LINUX WELT XXL

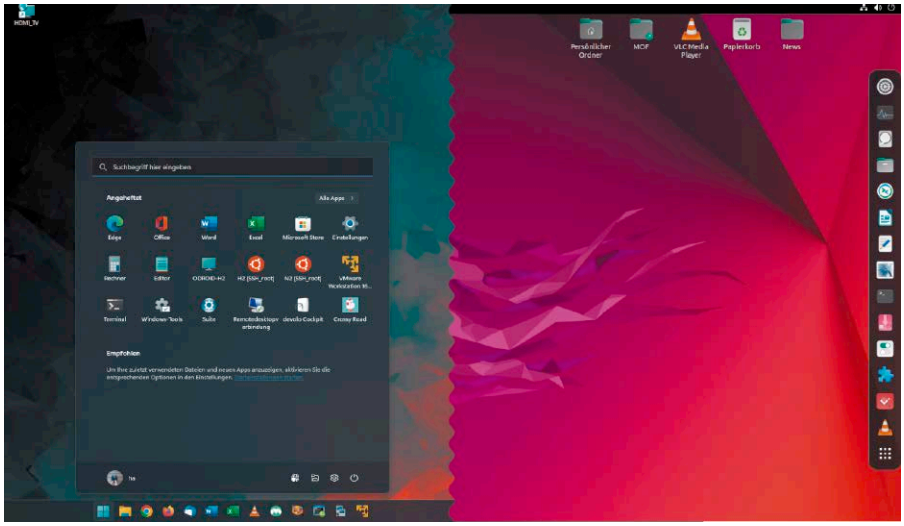
Das komplette Handbuch

Neue Fassung

Linux & Windows: Das Duell

Linux oder Windows – welches Betriebssystem ist besser? Die Frage ist beliebt, aber eigentlich schon im Ansatz verfehlt. Wir sammeln trotzdem in einem Punkteduell die jeweiligen Vorzüge und küren einen Sieger.

VON HERMANN APFELBÖCK



Linux oder Windows? Die bessere Frage lautet: Wo eignet sich Linux, wo Windows? Jedes der beiden Systeme hat seine Vorteile und am klügsten ist es, die beiden als Team zu sehen, das sich bestens ergänzt. Wir stellen Linux und Windows in wichtigen Kriterien gegenüber und versuchen eine objektive Bewertung. **Einen Punkt** gibt es für einen tendenziellen Sieg in der jeweiligen Kategorie, **zwei Punkte** für offensichtliche Überlegenheit in einer wichtigen Disziplin.

Die Entscheidung für oder gegen ein Betriebssystem wird Ihnen diese Wertung aber nicht abnehmen. Es gibt nämlich K-o.-Kriterien sowohl für Linux wie für Windows, die außerhalb jeder objektiven Wertung stehen. K.-o.-Kriterien für Windows sind kommerzielle Programme und Spiele, die es für Linux schlicht nicht gibt. Auch die Tatsache, dass unter Windows garantiert jede (aktuelle) Hardware funktioniert, ist für viele Nutzer ein entscheidendes Argument. Umgekehrt ist Linux praktisch alternativlos, wo es um ARM-basierte Hardware (Platinen), um leistungsschwache, ältere PCs/Notebooks oder um betagte Peripheriegeräte geht. Ferner bietet Linux konkurrenzlosen Schutz gegen digitale Schädlinge, besseren Datenschutz und jede portable Freiheit aufgrund der GPL-Lizenz.

1. Leistung (1): Der Bootprozess

Die Zeit, die ein eingeschaltetes Desktopsystem zum Log-in benötigt, sollte man nicht überbewerten, aber niemand hat etwas dagegen, wenn es schnell geht. Bei einer Rechnernutzung mit einem einzigen System, wie sie vermutlich für weit über 90 Prozent der Installationen zutrifft, ist Windows schneller am Log-in. Wir messen am selben Rechner (in Sekunden):

Windows 7,8
Ubuntu 13,6

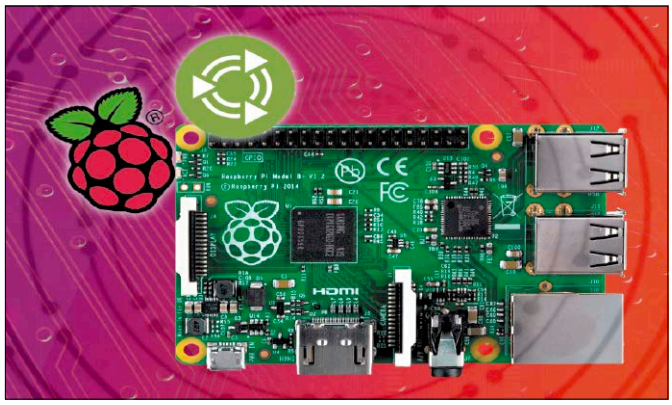
Das Ergebnis muss man aber interpretieren: Windows startet schneller, weil es beim „Herunterfahren“ nicht wirklich herunterfährt. Die Funktion „Fastboot (oder „Fast Startup“) nutzt einen Ruhezustand (Suspend to disk) für den Systemstatus und spart sich damit beim nächsten Start die Kernel- und Treiberinitialisierung. Ein tatsächlicher Windows-Start erfolgt nur über die Option „Neu starten“ und dieser Start ist mit 14,5 Sekunden etwa gleichauf mit Ubuntu – ein Stück langsamer aber doch. Zudem gibt es durchaus schnellere Distributionen, die annähernd Fastboot-Zeiten von Windows erzielen: Ein Arch-basiertes

Autostart-Anwendungen: Verglichen mit Windows bleibt das unter Linux stets überschaubar. Das liegt nicht zuletzt daran, dass sich die Software nicht selbst um Updates kümmern muss.

Endeavour-OS benötigt kaum zehn Sekunden, Bodhi Linux kaum neun Sekunden zur Anmeldung.
Windows bootet also „eigentlich" langsamer, durch Fastboot aber schneller. Dieser Windows-Vorteil gilt aber nur als alleiniges System. In Multiboot-Umgebungen ist Fastboot problematisch, denn die inaktive Windows-Partition befindet sich in einem hybriden Ruhezustand und darf von einem anderen System nicht beschrieben werden.
Ergebnis: 1 Punkt für Windows (weil Multiboot ein Minderheitenthema ist und weil Linux-Distributionen, die an Fastboot herankommen, nicht Mainstream sind).

2. Leistung (2): Betriebsperformance

Die Alltagsleistung zu objektivieren ist schwierig, da man letztlich nur die Startgeschwindigkeit von Programmen oder die Transferleistung von Hardwarekomponenten misst. Tatsache ist, dass größere Software wie Libre Office, Gimp, VLC oder Browser allesamt in einer Sekunde eingabebereit ist – unter Linux wie Windows. Dafür ist keine brandaktuelle Hardware nötig.
Beim Datentransfer zwischen lokalen Datenträgern scheint Linux geringe Leistungsvorteile bei SATA zu zeigen, Windows andererseits bei USB, die aber allesamt so minimal ausfallen, dass man sie als Messungenauigkeiten interpretieren muss. Bei Netzwerkfreigaben ist Windows deutlich langsamer als ein Linux-Client, sofern die Daten auf Linux-Servern liegen. In homogenen Verhältnissen kommuniziert Windows mit Windows ein Stück schneller als Linux mit Linux. Das alles sind Messungen und Erfahrungswerte aus einem gut ausgestattetem Homeoffice, das aber keine Testlabor-Präzision beanspruchen kann.
Defender-Bremse bei Windows: Bei Datentransfers, die ausführbare Dateien enthalten, schaltet sich der interne Defender zum Virencheck dazwischen. Dies ist unter Windows notwendig (siehe Punkt 9), kann aber die I/O-Leistung ausbremsen. Erfahrene Nutzer können „Ausschlüsse" definieren, um bestimmte Pfade von der Überwachung zu befreien.
Leistungsabfall bei Windows? Windows wird nachgesagt, dass es nach längerer Betriebszeit langsamer wird. Das kann tatsächlich eintreten, liegt aber nicht ursächlich am Windows-System. Der Grund ist eine Unmenge an Software, die sich im Windows-Autostart einnistet – zum einen Teil, um sofort einsatzbereit zu sein („Schnellstarter", „Preload"), zum anderen Teil, um sofort nach Programmupdates zu suchen. Hinzu kommt die Integration zahlloser Tools in die Explorer-Shell, die mindestens zu verzögerten Kontextmenüs führen kann. Das alles kostet Start- und Reaktionszeiten, die sich ebenso aufsummieren wie Speicherverbrauch und CPU-Zeit. Der Alterungsprozess von Windows gründet daher auf der Disziplinlosigkeit der Benutzer, jedes marginale Tool zu installieren und zum Dauertask zu erheben.
Linux bleibt stabil schnell: Unter Linux entfällt für Programme schon aufgrund der zentralen Updateversorgung ein wichtiges Motiv, sich als Autostart auszubreiten. Unter Linux trägt sich Software aber generell niemals ungefragt (oder als bereits voraktivierte Klickbox) als Autostart oder Shell-Erweiterung ein. Die Erlaubnis, dies zu tun, wird defensiv beim Benutzer abgefragt. Bei den meisten Linux-Programmen ist ein eigener Autostart bei der Einrichtung erst gar nicht vorgesehen.
Ergebnis: 1 Punkt für Linux



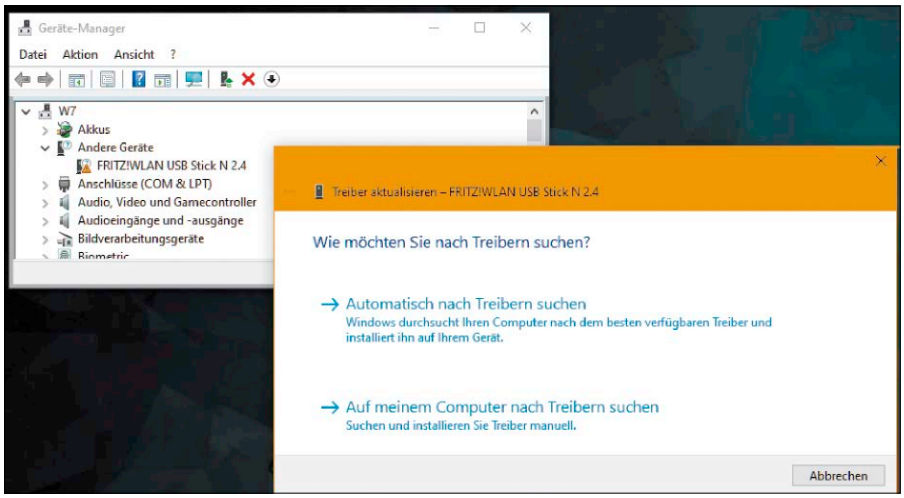
Linux läuft überall: Für ARM-Platinen oder x86-Altgeräte gibt es keine Windows-Alternativen.

3. Leistung (3): Skalierbarkeit

Ältere Notebooks und PCs kommen schon mit Windows 10 an ihre Grenzen. Das technisch kaum veränderte Windows 11 hat die Hardwarevoraussetzungen noch einmal künstlich hochgeschraubt. Selbst gut ausgestattete PCs und Notebooks fallen durch die „PC-Integritätsprüfung". Microsoft hat beim Windows-Desktop kein Interesse, ein skalierbares System anzubieten, das in verschiedenen Varianten auch leistungsschwächere Hardware unterstützt. Einzige nennenswerte Ausnahme ist das auf einigen preiswerten Geräten vorinstallierte „Windows S" mit reduziertem Umfang.
Linux läuft überall! Mit sehr verschiedenem Anspruch an CPU, RAM, GPU und Plattenplatz ist Linux konkurrenzlos flexibel. Mit der geeigneten Distribution lassen sich bis zu 20 Jahre alte PCs und Notebooks in Spezialrollen weiternutzen, bis zu zehn Jahre alte Geräte als vollwertiger Desktop mit ansprechender Leistung (etwa mit MX Linux, Q4-OS, Linux Mint LMDE, Xubuntu).
Jenseits vom Desktop hat die Linux-Bandbreite noch einen weiteren Aspekt: Wer sich in der englischsprachigen Wikipedia den Artikel „*Comparison_of_operating_system_kernels*" zumutet, wird feststellen, dass Windows die x86-PC-Architektur allenfalls versuchsweise verlassen hat. Auch „Windows IoT" für die ARM-Plattform (und für Raspberry 2) bleibt eine Marginalie. Linux spielt hingegen auf fast allen Architekturen mit, wobei ARM mit Raspberry & Co. für Endanwender sicher die wichtigste Plattform ist.
Ergebnis: 2 Punkte für Linux

4. Hardware (1): Allgemein

Computerhardware ist aufgrund der Verbreitung von Windows stets darauf zugeschnitten. Jedes aktuell im Handel verfügbare Gerät kann mit Sicherheit unter Windows genutzt werden, da wirklich jede exotische Peripherie einen Windows-Treiber bereitstellt.
Für Linux liefern nur wenige Hardwarehersteller proprietäre Treiber. Das Funktionieren der Hardware ist daher überwiegend auf die Treiberausstattung des Linux-Kernels angewiesen. Alle Kernkomponenten wie SATA, Grafikkarte, Ethernet, integrierter Wi-Fi-Chip, Monitor, Maus, Tastatur funktionieren immer. Nur bei brandaktuellen Kernkomponenten kann es sein, dass der Kernel diese (noch) nicht unterstützt. Als Grundregel kann gelten: Wo bislang das



Altperipherie unter Windows: Für diesen Wi-Fi-Stick ist unter Windows 10 kein Treiber mehr zu finden. Unter Linux funktioniert er sofort.

ältere Windows 10 lief, ist jede Linux-Distribution geeignet.

Bei neuen Peripheriegeräten wie USB-Druckern, Scannern, Multifunktionsgeräten, WLAN-USB-Adaptern, TV-Sticks sollte die Kompatibilität vor einem Kauf verifiziert werden. Die Chancen im Problemfall, anhand exakter Gerätekennungen und Chiprevisionen Abhilfe im Web zu finden, sind begrenzt und für Nicht-Profis knifflig. Präventive Problemerkennung bieten die Livesysteme der Linux-Distributionen. Alles, was im Livesystem funktioniert, wird im selben System auch nach der Installation funktionieren.

Ergebnis: 2 Punkte für Windows

5. Hardware (2): Ältere Peripherie

Hardwaretreiber für Windows sind selten NT-universell, sondern auf bestimmte Windows-Versionen zugeschnitten. Hersteller, die ehemals Treiber für Windows Vista oder 7 oder 8 anboten, aktualisieren diese oft nicht mehr für nachfolgende Windows-Versionen. In der Folge funktionieren ältere Geräte unter Windows 10 oder 11 nicht mehr. Unter Linux stehen die Chancen für einen Weiterbetrieb älterer Peripherie weit besser, weil die Treiberausstattung des Linux-Kernels äußerst konservativ gepflegt wird. Wenn Treiber aus dem Kernel entfernt werden, handelt es sich immer um moosalte und wirklich obsolete Hardware. Die Tatsache, dass Linux alte Rechner mit leistungsschwachen Kernkomponenten wie CPU und RAM unterstützt, hat bereits der Punkt 3 besprochen.

Ergebnis: 1 Punkt für Linux

6. Hardware (3): Notebooks

Auf Notebooks ist die Akkulaufzeit ein wichtiges Kriterium und hier ist Linux nicht in jedem Fall optimal. Standardmäßig bieten Linux-Distributionen unter „Energieverwaltung" nur fundamentale Stromspartechniken mit Time-outs für Bildschirm und Bereitschaftsmodus. Windows ermöglicht in enger Zusammenarbeit mit den Herstellern filigranere Regeln.

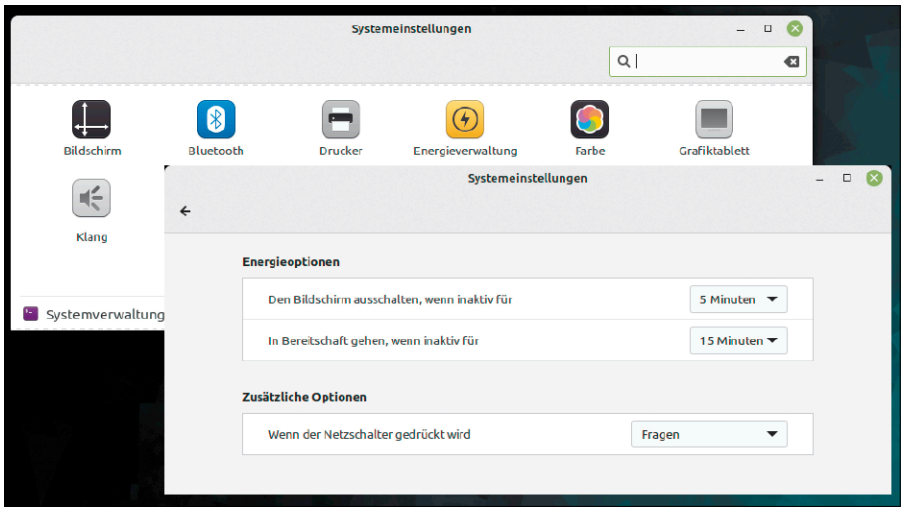
Manchmal werden auch Funktions- und Sondertasten von Notebooks von Linux nicht unterstützt. Mit Anleitungen aus dem Internet und etwas Aufwand lässt sich das Problem meistens beheben, sofern das Know-how des Nutzers ausreicht. Generell ist es ratsam, sich vor dem Notebookkauf über die Linux-Kompatibilität zu informieren. Denn natürlich gibt es auch Notebooks, die unter Linux optimale Ausdauer und alle Funktionen bieten.

Ergebnis: 1 Punkt für Windows

7. Software & Spiele

Windows hat das mit Abstand größte Softwareangebot. Es gibt kein renommiertes Programm oder Spiel, das nicht unter Windows läuft. Vorinstalliert ist nur eine Basisausstattung, die für Medienwiedergabe, Grafikbearbeitung, einfache Textformate und Internetzugang (Browser Edge) ausreicht. Aber alles was fehlt, kann man sich aus dem sicheren Microsoft Store oder aus zahllosen Hersteller- und Sammelquellen herunterladen. Das gilt für kommerzielle Software und Spiele aller Art, nebenbei aber auch für die komplette Open-Source-Prominenz.

Unter Linux bleibt das Angebot der Paketquellen bis auf wenige Ausnahmen auf Open-Source-Programme beschränkt. Mit Browser (alle), Thunderbird, VLC, Libre Office, Gimp, Calibre, Darktable, Scribus, Audacious & Co. können Sie auf einem Home-PC jede Aufgabe erledigen. Dennoch ist diese Beschränkung oft ein K.-o.-Kriterium: Wer Photoshop, Indesign, Autocad, Word oder Excel schlicht braucht, kann die Plattform Linux nicht nutzen – oder nur mit erheblichem Aufwand. Dabei muss es gar nicht um spezielle Fähigkeiten dieser Software gehen, die Alternativen wie Gimp oder Libre Office Calc nicht besitzen. Allein der unkomplizierte Workflow ohne eventuelle Nachbearbeitung ist ein schlagendes Argument. PC-Spiele bleiben unter Linux trotz Anbindung an die kommerzielle Spiel-



Linux-Desktops bieten nur fundamentale Stromsparfunktionen. Die Akkulaufzeiten von Notebooks sind in der Regel kürzer als unter Windows.

plattform Steam gegenüber Windows deutlich reduziert und auch leistungstechnisch kann selbst das Gaming-Linux Steam-OS ein Windows nicht schlagen.

Wine? Die Erfolge, die das Projekt Wine (*https://appdb.winehq.org/*) mit dem Nachbau der Windows-API vorweisen kann, fallen sehr unterschiedlich aus: Dass die benötigte Version einer Windows-Software einen störungsfreien „Platinum"- oder „Gold"-Status unter Linux erreicht, bleibt aber ein Glücksfall. Naturgemäß stehen dabei die Chancen bei älterer Software besser.

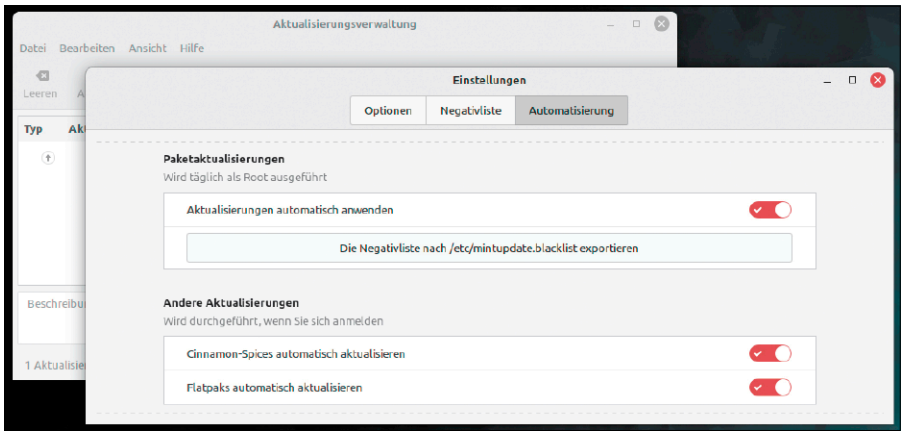
Ergebnis: 2 Punkte für Windows

8. Updates & Upgrades

Unter Windows werden Aktualisierungen automatisch und zwangsweise installiert und umfangreiche Updates zur Unzeit können eine erhebliche Produktivitätsbremse bedeuten. Immerhin ist bei Bedarf eine „Updatepause für 7 Tage" zu erzwingen. Windows-Updates berücksichtigen nur das Betriebssystem, Treiber und optional einige Microsoft-Programme wie Office. Die komplette sonstige Software muss sich mit eigenen Updatefunktionen behelfen, die entweder per System-Autostart arbeitet oder beim Programmstart das Update vorschlägt. Das ist umständlich, gegebenenfalls zeitlich unpassend und außerdem potenziell riskant, sofern diese Software ins Internet geht.

Windows-Upgrades auf eine neue Version erfolgen ebenfalls über das automatische Windows-Update. Während die Sicherheits- und Funktionsupdates in aller Regel problemlos sind, verlaufen Upgrades nicht immer fehlerfrei. Im schlimmsten Fall wird das System unbenutzbar, kann aber mit eingebauten Reparaturoptionen und Know-how meistens zurückgesetzt werden.

Linux-Updates sind frei konfigurierbar – was man wann installieren möchte. Bei einem Linux-Samba-Server, der nur im eigenen Heimnetz arbeitet, kann man sich durchaus entscheiden, jahrelang komplett ohne Sicherheits- und Funktionsupdates auszukommen. Ein weiterer, noch größerer Vorteil der Linux-Aktualisierung ist die Komplettversorgung inklusive Software. Der Updatedienst umfasst nämlich das Betriebssystem und jedes installierte Programm, das aus den Paketquellen der Distribution stammt. Dort, wo die Containersoftware Snap oder Flatpak zum Standard gehört, wird auch diese aktualisiert. Für



Updates für System, Software, Container und Zubehör: Eine generelle Einstellung genügt für automatische Vollversorgung. Ebenso einfach sind manuelle Updates mit apt & Co. im Terminal.

Server interessant sind ferner die Kernel-Updates über temporäre „Livepatches": Der Kernel wird dabei aktualisiert, ohne vorerst den fälligen Rechnerneustart zu erzwingen.

Linux-Upgrades auf eine neue Version werden ebenfalls über die Systemaktualisierung angeboten und bei Zustimmung ausgelöst. Wie bei Windows kosten Upgrades viel Zeit und sind nicht ohne Risiko. Im Fehlerfall sind Reparaturmöglichkeiten begrenzt und kompliziert. Es empfiehlt sich, vorher die persönlichen Dateien aus dem Home-Verzeichnis zu sichern.

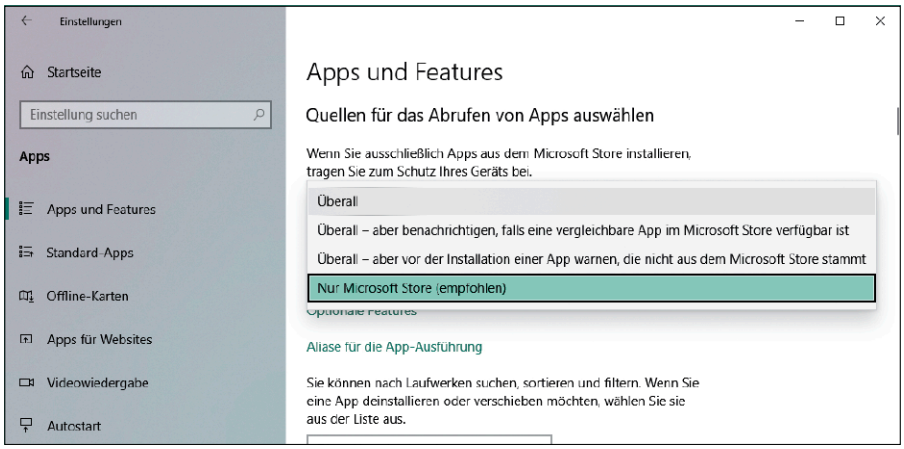
Ergebnis: 1 Punkt für Linux

9. Sicherheit im Web

Windows ist das erste Ziel für Schadsoftware. Das Einschleusen von Viren und Malware ist bei Windows-Systemen am erfolgversprechendsten – aufgrund der Verbreitung, aufgrund der Homogenität (der technisch unterschiedliche Linux-Distributionen gegenüberstehen), aufgrund des unkontrollierten Softwarebezugs aus jeder beliebigen Quelle. Schutzmaßnahmen wie der Smartscreen-Downloadfilter und der Windows Defender wehren das Schlimmste ab (soweit als Schädling bekannt oder heuristisch verdächtig), aber letztlich entscheidet der Nutzer, ob er eine Schadsoftware einlässt oder nicht.

Im Prinzip (aber verbunden mit deutlicher Softwarelimitierung) kann man Windows deutlich sicherer machen. Nach dem Vorbild von „Windows S" kann das System externe Downloads verbieten (siehe „Einstellungen → Apps & Features → Quellen") und nur noch Software aus dem Microsoft Store erlauben.

Linux ist theoretisch genauso angreifbar wie Windows, aber allein schon der ausschließliche Softwarebezug aus den sicheren Paketquellen der Distribution macht Schadsoftware so gut wie unmöglich. Sicherheitslecks im Browser gibt es natürlich



Riskante Software verbieten: Mit dieser Option würde Windows beim Programmdownload mit den sicheren Paketquellen von Linux gleichziehen. Sie ist aber zu imitierend und deshalb unpopulär.

auch unter Linux, aber Schädlinge, die solche zeitnah ausnutzen wollen, zielen fast ausschließlich auf das homogenere und verbreitetere Windows. Auf dem Linux-Desktop sind daher nur disziplinierte Updates Pflicht (inklusive Browser, Mail). Virenscanner und Firewall sind nicht erforderlich.

Ergebnis: 2 Punkte für Linux

10. Datenschutz & Verschlüsselung

Linux und Linux-Distributionen sind ganz große Ausnahmen: Es gibt sonst kaum Software, die kostenlos ist und dennoch datenschutzkonform und werbefrei arbeitet. Debian, Ubuntu & Co. möchten zwar gerne einige harmlose Nutzungsdaten und Problemberichte, aber das alles lässt sich abschalten, sofern man das will.

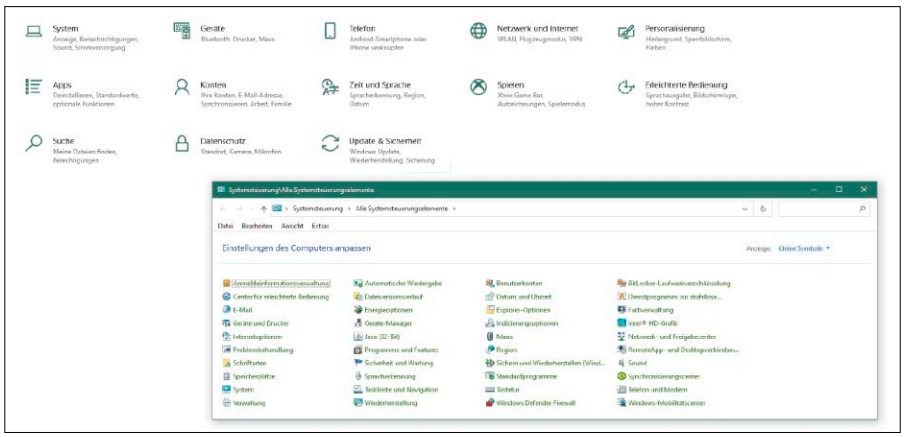
Windows sammelt anonyme Nutzungsdaten, eventuell auch personenbezogene Infos über Cortana, Defender, Aktivitätsverlauf. Wer die Onedrive-Anbindung kritiklos nutzt, übergibt Microsoft in jedem Fall persönliche Daten. Einiges kann man abschalten, aber nicht alles. In der Home-Edition von Windows 11 entsteht schon allein durch den neuen Zwang zur Onlineanmeldung eine Mindestüberwachung. Unabhängig davon kann natürlich jede Drittanbieter-Software Daten übermitteln. Das gilt im Prinzip auch für Linux, ist aber bei Open-Source-Programmen kontrollierbarer.

Für den lokalen Geräteschutz bietet Windows sichere Bitlocker-Verschlüsselung, dies allerdings nicht in der verbreiteten Home-Edition. Auf der anderen Seite gibt es in allen renommierten Linux-Distributionen bei der Installation die sichere Verschlüsselungsoption mit Luks/Cryptsetup. Diese ist im Betriebsalltag auch für mobile USB-Datenträger über das Laufwerkstool erreichbar.

Ergebnis: 1 Punkt für Linux

11. Mobilität auf USB

Eine Windows-Installation auf USB ist nicht vorgesehen und wird vom Setup nicht angeboten. Dass sie technisch möglich ist, beweist „Windows to go“, das allerdings Windows-Enterprise-Editionen vorbehalten ist. Ungeachtet dieser Einschränkung ist aber ein portables Windows mit speziellen Tools möglich. Wer sich auf dieses Thema einlässt, wird aber zu dem Schluss kommen, dass sich Windows gegen kompetente Tricks zwar nicht wehren kann, aber die Maßnahme in keiner Weise selbst unterstützt.



Irritierende Windows-Konfiguration: Alte Systemsteuerung und neue „Einstellungen“ stehen seit zehn Jahren nebeneinander. Wer beides durchsucht, wird irgendwo fündig.

Bei Linux ist mobiler Einsatz in doppelter Ausführung Standard: Die allermeisten Distributionen sind Livesysteme, die auf DVD wie USB funktionieren. Viele Livesysteme können durch Persistenzoptionen aufgewertet werden und somit auch Anpassungen und Softwareinstallationen ermöglichen. Zweitens ist für Linux eine reguläre Installation auf USB-Medien so selbstverständlich wie auf interne Datenträger.

Ergebnis: 1 Punkt für Linux

12. Systemkonfiguration (1): Die Zentralen

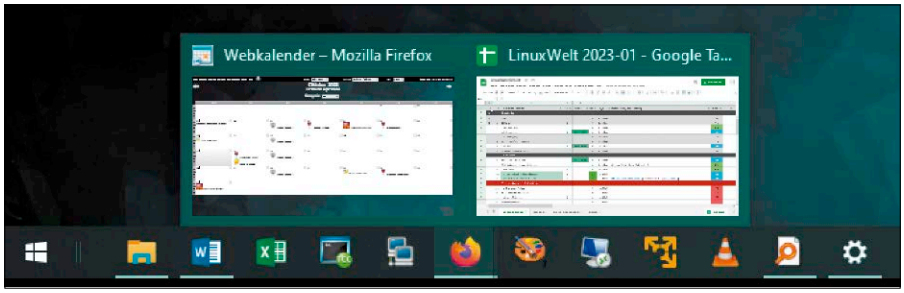
Systemeinstellungen und Anpassungen sollten nach kurzer Gewöhnung keine Suchrätsel aufgeben. Unter Linux hängt das Angebot zur Systemkonfiguration von der genutzten Desktopumgebung ab. Wer jahrelang bei einem Desktop wie Gnome, KDE oder Cinnamon bleibt, hat keine Mühe, wichtige Optionen unter „Anzeigeräte“, „Netzwerk“ oder „Darstellung“ zu finden. Im Allgemeinen sind diese Systemzentralen sehr übersichtlich, allerdings auch nicht so umfassend wie das Optionsangebot unter Windows. Pauschal gilt dies aber nicht, wie etwa die KDE-Einstellungen zeigen.

Windows hat das größere Angebot. Das wird aber so chaotisch präsentiert, dass selbst Windows-Profis immer wieder rätseln: Die Umstellung der alten Systemsteuerung auf die modernen „Einstellungen“ ist seit 2012 (Windows 8 mit „Modern UI“) und unter Windows 10 eine Dauerbaustelle. Bestimmte Punkte gibt nur in der Systemsteuerung, andere nur in den „Einstellungen“ und zum Teil ist das Angebot doppelt und redundant. Windows 11 hat die „Einstellungen“ weitgehend komplettiert und durch eine Navigationsspalte optimiert. Die parallele Systemsteuerung samt Redundanzen besteht aber weiterhin.

Ergebnis: 1 Punkt für Linux

13. Systemkonfiguration (2): Low Level

Hier stehen der zentralen Windows-Registry verstreute und kaum standardisierte Linux-Konfigurationsdateien im Textformat gegenüber. Letztlich ist es aber eine Frage der Gewöhnung, ob man sich in den Registry-Hauptschlüsseln „Hkey_Local_Machine“



Windows 10 mit Menü und Taskleiste: Das sieht einfach aus, ist es aber nicht. Linux-Nachahmer wie Cinnamon haben für analoges Verhalten erheblich investiert („Gruppierte Fensterliste“).

und „Hkey_Current_User“ oder in den Linux-Verzeichnispfaden „/etc“ und „/home/[user]/.config“ zu Hause fühlt. Die meisten Eingriffe hier wie dort erfolgen natürlich nicht manuell, sondern durch Klickoptionen in der grafischen Zentrale sowie in den jeweiligen Programmeinstellungen.

Allgemein spielt allerdings die Low-Level-Konfiguration unter Linux eine größere Rolle als unter Windows, weil wesentliche Linux-Systemdienste nur auf diesem Weg einzurichten und zu steuern sind. Selbst auf reinen Desktopsystemen sind manuelle Eingriffe in Konfigurationsdateien und Terminalaktionen mit Systemctl & Co. zur Dienste-Steuerung nicht dauerhaft zu vermeiden. Unterm Strich ist die Registry unter Windows zentraler, übersichtlicher und über API-Schnittstellen für jede Software und für die diversen Windows-Management-Konsolen erreichbar.

Mit Homogenität und Fehlertoleranz kommt noch ein weiterer Aspekt ins Spiel: Bei Windows ist alles aus einer Hand und mindestens bei Alltagsaufgaben einsteigerfreundlich. Linux-Distributionen kombinieren Komponenten unterschiedlicher Herkunft, die in Qualität und Fehlertoleranz variieren: Die eine Komponente warnt vor Fehlgriffen, die nächste erwartet Benutzer, die genau wissen, was sie tun.

Ergebnis: 1 Punkt für Windows

14. Oberfläche (1): Allgemein

Die Windows-Shell mit Desktop, Startmenü, Taskleiste, Einstellungen und Dateimanager (Explorer) ist ein beliebtes Shitstorm-Objekt. Tatsache ist aber andererseits, dass diese Oberfläche seit Jahrzehnten benutzerfreundliche Maßstäbe setzt, an denen sich viele Linux-Desktops orientieren. Die meisten Linux-Oberflächen (am wenigsten Gnome, am deutlichsten Cinnamon) folgen dem Windows-Konzept mit Startmenü, Desktopablage und multifunktionaler Leiste mit Taskübersicht und Programmfavoriten.

Auch der objektorientierte Ansatz von Windows, passende Aktionen per Kontextmenü an Ort und Stelle anzubieten, ist Vorbild für einsteigerfreundliche Linux-Distributionen. Hintergrundänderung, Leisteneinstellungen, Dateiaktionen per Kontextmenü unterscheiden sich bei Desktops wie KDE, Cinnamon, XFCE oder Mate nicht fundamental von Windows.

Ergebnis: 1 Punkt für Windows

15. Oberfläche (2): Flexibilität

Der Windows-Desktop wird puristischer und hat unter Version 11 nochmal einige Anpassungsoptionen über Bord geworfen. Neben Design, Hintergrundbild oder Akzentfarben, einfach ausbaufähiger Taskleiste und Systray-Zone gibt es aber alle Optionen zur Feineinstellung von Schriftgrößen, Maus- oder Tastatureigenschaften. Der Dateimanager bietet flexible Ansichtsoptionen und ist via Registry sehr einfach durch externe Tools erweiterbar.

Linux-Desktops bieten nicht in jedem Detail denselben Anpassungskomfort, aber deutlich mehr Optionen: In der Regel sind mehrere Systemleisten an beliebiger Position möglich, die wiederum mit beliebigen Applet-Modulen zu bestücken sind. Das Konzept der virtuellen Desktops ist unter Linux ausgereift und produktiv, unter Windows optional und fummelig („Aktive Anwendungen“). Zentrale Hotkeyverwaltung und mausaktive Ecken fördern Programmschnellstarts oder Multitasking-Übersicht.

Nicht zu vergessen: Der Desktop ist unter Linux nur eine austauschbare Software. Ein Linux-System kann daher mehrere Oberflächen installieren, die der Benutzer bei der Anmeldung auswählt. Das werden nicht viele Linux-Nutzer tatsächlich tun, aber diese Möglichkeit des Desktopwechsels besteht.

Ergebnis: 1 Punkt für Linux

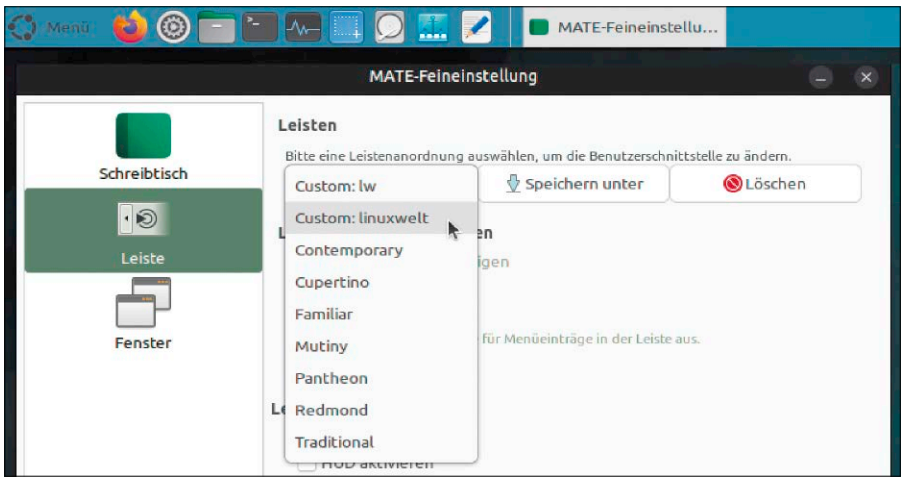
16. Kosten & Lizenzmodell

Haben wir etwas vergessen? Gewiss – die Kosten: Windows-Home- und Pro-Versionen sind kostenpflichtig, mit unterschiedlichen Preisen (Box, Download, nur Aktivierungsschlüssel). Typische vorinstallierte OEM-Lizenzen kosten etwa 80 Euro, Einzelhandelslizenzen mit Datenträger gerne das Doppelte. Linux-Distributionen sind für private Nutzer kostenlos. Einige Ausnahmen fordern eine Downloadgebühr oder bitten um freiwilligen Spende. Die freie GPL-Lizenz impliziert neben der Kostenfreiheit praktische Freiheiten, die in anderen Punkten schon angesprochen wurden: Die lästige Aktivierungspflicht etwa nach Neuinstallationen, Systemumzügen oder Hardwareumbauten entfällt komplett. Die unbegrenzte Mobilität gehört ebenfalls in diesen Kontext.

Ergebnis: 1 Punkt für Linux

LINUX GEGEN WINDOWS

Kriterien	Linux	Windows
Leistung (1): Booten		1
Leistung (2): Allgemein	1	
Leistung (3): Skalierbarkeit	2	
Hardware (1): Allgemein		2
Hardware (2): Altgeräte	1	
Hardware (3): Notebooks		1
Software & Spiele		2
Updates & Upgrades	1	
Sicherheit im Web	2	
Datenschutz & Verschlüsselung	1	
Mobilität (USB)	1	
Systemkonfiguration (1): Zentralen	1	
Systemkonfiguration (2): Low Level		1
Oberfläche (1): Allgemein		1
Oberfläche (2): Flexibilität	1	
Kosten & Lizenz	1	
Summe der erzielten Punkte	12	8



Anpassungen der Oberfläche: Die meisten Linux-Desktops (hier Mate) bieten deutlich mehr Konfigurationskonfekt als Windows.

Der Umgang mit ISO- und IMG-Dateien

Imagedateien benötigen Sie für die Linux-Installation und für den Raspberry Pi. Um aus heruntergeladenen Abbildern bootfähige DVDs, USB-Sticks oder SD-Karten zu erzeugen, ist spezielles Werkzeug erforderlich.

VON THORSTEN EGGELING

Linux-Nutzer kommen häufig in Kontakt mit Imagedateien unterschiedlichster Art. Für die Linux-Installation auf dem PC oder Notebook verwenden Sie eine DVD, die sich aus einer heruntergeladenen ISO-Datei brennen lässt. Viele ISO-Dateien eignen sich auch für bootfähige USB-Sticks. So können etwa die Livesysteme auf der Linux-Welt-DVD nicht nur von dort booten, sondern aus dem Ordner „Image-Dateien“ auch einzeln auf einen bootfähigen USB-Stick kopiert werden.

Nutzer von Ein-Platinen-PCs wie dem Raspberry Pi haben es mit einem anderen Abbildtyp zu tun. Beim Standardsystem Raspbian (*www.raspberrypi.org/downloads*) erhalten Sie nach dem Entpacken eine Imagedatei, deren Inhalt auf die SD-Karte gelangen muss. Diese enthält dann kein Live- und Installationsmedium, sondern bereits das komplette Betriebssystem.

Für alle Abbildtypen gibt es spezielle Werkzeuge, um den Inhalt auf einen Datenträger zu übertragen. Bevor wir den praktischen Umgang mit diesen Werkzeugen beschreiben (ab Punkt 4), erhalten Sie zunächst die wichtigsten Grundlagen zum Thema.

1. Dateisysteme auf DVDs und in ISO-Dateien

Auf allen Datenträgern sind Dateien in einem Dateisystem gespeichert, wenn auch teilweise in unterschiedlichen. Ein Dateisystem hat zuerst die Aufgabe, ein Verzeichnis der enthaltenen Objekte – Dateien und Ordner – bereitzustellen. Dazu gehören Metainformationen wie Erstellungszeitpunkt, letzter Zugriff und Größe.

Nicht alle Dateisysteme eignen sich für jeden Datenträger. Daten-CDs und -DVDs beziehungsweise ISO-Dateien verwenden ISO 9660, einen Standard, der bereits 1987 verabschiedet wurde. Zu der Zeit herrschten Dateinamen mit einer Länge von acht Zeichen (ISO 9660 Level 1) und Dateien waren selten mehrere Megabyte groß. Schließlich passten auf eine CD auch nur knapp 700 MB.

Die meisten Einschränkungen wurden nach und nach unter Beibehaltung des bereits als erweiterbar geplanten ISO-9660-Standards gemildert.

ISO 9660 Level 2 erlaubt bereits Dateinamen mit 31 Zeichen. Joliet ist eine Entwicklung von Microsoft, die 64 Zeichen in Dateinamen ermöglicht. Die Rock-Ridge-Erweiterungen erlauben es Unix-Systemen, Zugriffsrechte zu speichern, ermöglichen Dateinamen mit bis zu 255 Zeichen und beliebig tiefe Verzeichnisbäume. In einigen ISO-Dateien ist alles zusammen zu finden, also ein Standard ISO-9660- und ein Joliet-Dateisystem sowie Rock-Ridge-Erweiterungen.

UDF (Universal Disk Format) ist ein weiteres Dateisystem, das in der Regel für Video-DVDs verwendet wird. Es wird meist zusammen mit ISO 9660 eingesetzt (UDF/ISO-Bridge), damit auch ältere Systeme ohne UDF-Unterstützung die Scheibe lesen können. Windows-Installations-DVDs werden meist mit UDF ausgeliefert, auf Linux-Installations-DVDs ist UDF eher selten zu finden.

Bootsektoren auf DVDs: Damit ein Betriebssystem von DVD booten kann, ist aber noch mehr erforderlich. Die „El-Torito“-Spezifikation von 1995 legt drei Arten fest, wie sich von einer CD/DVD booten lässt: mit dem Image einer Festplatte, einer Floppy Disk oder einem Block mit Programmcode. Das Bios eines PCs erkennt dann beispielsweise das Floppy-Abbild auf der CD, das es wie ein Diskettenlaufwerk einbindet und den Bootloader davon startet. Aktuelle Linux-Systeme verwenden

praktisch nur noch Programmcode aus einem „El-Torito“-Bootsektor, den das Bios von der DVD in den Hauptspeicher lädt und startet. Darüber werden dann die anderen Dateien des Bootmanagers von der DVD geladen. Meist kommt dabei Isolinux zum Einsatz (*https://wiki.syslinux.org*). PCs, die im Uefi-Modus starten, benötigen einen zweiten Bootsektor auf der DVD, der in der Regel den Bootmanager Grub startet (*www.gnu.org/software/grub*).

2. Dateisysteme in Laufwerksabbildern

Mini-PCs wie der Raspberry Pi besitzen kein DVD-Laufwerk und das System lässt sich auch nicht über einen USB-Stick installieren. Da aber ein Linux-System wie Raspbian genau auf die Raspberry-Hardware zugeschnitten ist, kann die Arbeit eines Installers entfallen: Es ist nicht nötig, die Hardware zu identifizieren oder die Festplatte zu partitionieren.

In den Imagedateien etwa für den Raspberry Pi sind meist mehrere Partitionen untergebracht. Es gibt einen MBR-Bootsektor, eine FAT32-Boot-Partitition und eine Linux-Partition mit einem Ext4-Dateisystem. Wird das Image auf die SD-Karte übertragen (siehe Punkt 7), enthält diese eine 1:1-Kopie dieser Partitionen. Die Ext4-Partition ist nur etwa drei GB groß und belegt daher nur einen Teil der verfügbaren Kapazität. Beim ersten Start des Systems wird sie dann auf den gesamten noch freien SD-Speicher ausgedehnt.

3. Was steckt in der Abbilddatei?

An der Dateinamenserweiterung lässt sich erkennen, um welche Datei es sich handelt. Lautet die Endung „.iso“ handelt es sich um ein CD/DVD-Abbild, „.img“ wird meist für Festplattenabbilder verwendet. Das Universaltool für die genauere Analyse von Dateien heißt file. Verwenden Sie in einem Terminalfenster diese Befehlszeile:

```
file [Boot-DVD.iso]
```

Den Platzhalter ersetzen Sie durch den Namen der zu untersuchenden Datei gegebenenfalls zusätzlich mit Pfad. Für eine Ubuntu-Installations-DVD gibt das Tool folgendes aus:

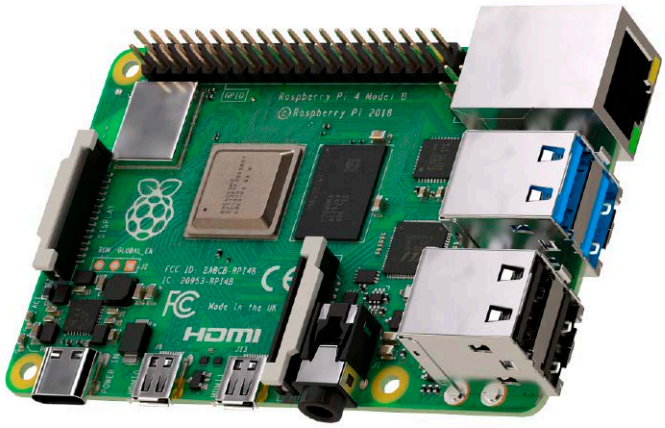
```
ubuntu-18.04.2-desktop-amd64.iso:
 DOS/MBR boot sector; partition 2 :
 ID=0xef, start-CHS
 (0x3ff,254,63), end-CHS
 (0x3ff,254,63), startsector
 3830956, 4928 sectors
```

Dieses Abbild enthält also einen DOS/MBR-Bootsektor und eine Partition mit der Nummer „2“. Genauere Auskunft über die Partitionen gibt fdisk:

```
fdisk -l [Boot-DVD.iso]
```

Tatsächlich gibt es bei im Ubuntu-ISO zwei Partitionen. Eine große mit etwa 1,9 GB und dem Typ „leer“ – eigentlich ist das Dateisystem ISO-9660, was fdisk aber nicht anzeigt – und eine kleinere mit 2,4 MB und dem Typ „EFI (FAT-12/16/32)“.

Start vom Installationsmedium: Damit ein Linux-System von DVD oder einem USB-Stick bootet, sind einige Voraussetzungen zu erfüllen, die man kennen sollte.



Booten von SD-Karte: Anders als bei einem PC, muss das Betriebssystem auf einem Platinenrechner nicht installiert werden. Es genügt eine Kopie der Imagedatei auf SD-Karte.

BACKUP: SD-KARTE UNTER LINUX SICHERN

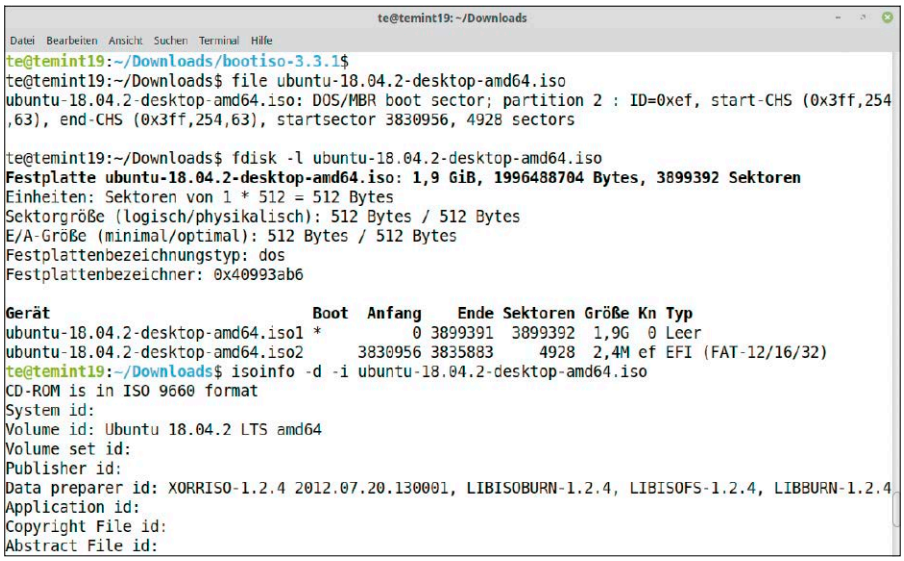
SD-Karten arbeiten im Raspberry Pi nicht immer zuverlässig. Manchmal kommt es zu Fehlern und das System startet nicht mehr. Es ist daher ratsam, ab und zu Backups zu erstellen. Fahren Sie den Raspberry Pi herunter, entnehmen Sie die SD-Karte und stecken Sie diese in den Kartenleser von PC oder Notebook. Ermitteln Sie den Pfad der SD-Karte und lösen Sie die Einbindung in das Dateisystem, entsprechend wie in Punkt 5 beschrieben. Für das Backup verwenden Sie diese zwei Befehle:

```
sudo apt-get install pv
sudo dd if=/dev/sd[X] | pv | gzip -c > ~/Backup_Raspian.img.gz
```

Das Tool pv sorgt dafür, dass eine Fortschrittsanzeige für dd erscheint. Den Platzhalter „[X]“ ersetzen Sie durch die zuvor ermittelte Laufwerksbezeichnung. Das Ergebnis ist eine komprimierte Abbilddatei der SD-Karte. Mit diesen zwei Befehlen

```
gunzip -c ~/Backup_Raspian.img.gz | pv | sudo dd of=/dev/sd[X]
sync
```

können Sie die Sicherung später wiederherstellen.



ISO-Datei untersuchen: Über die Tools file, fdisk und isoinfo erhalten Sie im Terminal Informationen zu den Dateisystemen und Partitionen, die in einer ISO-Datei untergebracht sind.

Weitere Informationen liefert das Tool isoinfo, das im Paket „genisoimage“ enthalten ist:

```
isoinfo -d -i [Boot-DVD.iso]
```

Es gibt aus, dass das Ubuntu-ISO mit dem Tool Xorriso im ISO-9660-Format mit Joliet und Rock-Ridge-Erweiterungen sowie El Torito erzeugt wurde. Auch diese Informationen sind noch nicht vollständig, denn Sie erfahren keine Details zu El Torito. Die liefert das Tool Xorriso, mit dem sich ISO-Dateien erstellen, bearbeiten und untersuchen lassen. Da es nicht standardmäßig installiert ist, holen Sie das mit

```
sudo apt install xorriso
```

nach und analysieren dann ein ISO-Abbild:

```
xorriso -indev [Boot-DVD.iso] -toc
```

Hinter „Boot record“ sehen Sie bereits bekannte Details wie „El Torito, MBR isohybrid“. Die Zeile „Boot image“ kommt zweimal vor: „/isolinux/isolinux.bin“ und „/boot/grub/efi.img“.

Es gibt ISO-Abbilder, die keinen MBR-Bootsektor enthalten und sich daher nicht für einen USB-Stick eignen. file gibt in diesem Fall nur „ISO 9660 CD-ROM filesystem“ aus. Der Bootsektor lässt sich aber nachträglich hinzufügen. Installieren Sie zuerst die nötige Software:

```
sudo apt install syslinux-utils
```

Dann bauen Sie den Bootsektor mit

```
isohybrid [Boot-DVD.iso]
```

ein.

Zusammenfassung: Die ermittelten Informationen geben genaue Auskunft über die Bootfähigkeiten einer ISO-Datei. Am Beispiel der Ubuntu-DVD ist zu sehen, dass der PC im Bios-Modus den Bootloader „/isolinux/isolinux.bin“ von der DVD lädt. Die Konfiguration, etwa für das angezeigte Menü, erhält er aus dem Verzeichnis „/isolinux“. Für den Uefi-Modus ist „/boot/grub/efi.img“ zuständig, das seine Konfiguration im Ordner „/boot/grub“ findet.

Wenn Sie aus dem ISO einen Bootstick erzeugen, etwa mit dem Startmedienersteller (siehe Punkt 5), werden beide Partitionen und der MBR-Bootsektor für den Bios-Modus kopiert. Eine ISO-Datei mit einem „DOS/MBR boot sector“ beziehungsweise „MBR isohybrid“ eignet sich daher für eine DVD und einen USB-Stick. Im Uefi-Modus lädt der PC automatisch den Grub-Bootloader aus dem Ordner „/EFI/BOOT“. Die für El Torito konfigurierten Bootloader kommen nicht zum Einsatz.

4. Installationsmedium aus ISO-Datei erstellen

Eine bootfähige DVD ist unter Ubuntu aus einer ISO-Datei schnell erstellt. Verwenden Sie im Dateimanager den Kontextmenüpunkt „Auf CD/DVD schreiben“. Windows-Nutzer gehen im Kontextmenü des Windows-Explorers auf „Datenträgerabbild brennen“. Sie können auch fast beliebige andere Brennprogramme benutzen, unter Linux beispielsweise Brasero oder K3B. Achten Sie dann aber darauf, dass Sie nicht die ISO-Datei auf die DVD brennen, sondern deren Inhalt. Dazu verwenden Sie etwa in Brasero den Punkt „Abbild brennen“.

5. USB-Stick für die Installation erstellen

Für USB-Sticks eignet sich unter Ubuntu der standardmäßig installierte „Startmedienersteller“. Nutzer von Linux Mint finden ein ähnliches Programm im Startmenü unter „Zubehör → USB-Abbilderstellung“. Ein alternatives Kopiertool unter Ubuntu und Linux Mint ist das grafische gnome-disks („Laufwerke“). Hier markieren Sie links das gewünschte Ziellaufwerk und wählen über das Zahnradsymbol die Option „Partitionsabbild wiederherstellen“. Sie erhalten dann ein Navigationsfenster, um das zu kopierende ISO-Image auszuwählen.

Wer die Kommandozeile bevorzugt, ermittelt folgendermaßen zuerst den Gerätepfad des USB-Laufwerks:

```
lsblk -p
```

In der Ausgabe sehen Sie beispielsweise „/dev/sdb1“ und dahinter „/media/[user]/[Kennung]“.

Hängen Sie den USB-Stick mit dieser Befehlszeile aus dem Dateisystem aus:

```
sudo umount /dev/sd[X]?
```

Der Platzhalter „[X]“ steht für die Gerätebezeichnung, beispielsweise „/dev/sdb“. „?“ sorgt dafür, dass alle Partitionen ausgehängt werden. Geben Sie im Terminal folgenden Befehl mit angepassten Pfaden ein:

```
sudo dd if=[Boot-DVD.iso] of=/dev/
  sd[X]
```

„[X]“ steht für die Laufwerksbezeichnung, die Sie schon zuvor bei umount verwendet haben. Warten Sie ab, bis die Eingabeaufforderung wieder erscheint. Achten Sie darauf, das richtige Zielgerät anzugeben, damit Sie nicht versehentlich eine Festplatte überschreiben.

Der analoge Rohkopierer (wie dd) unter Windows heißt Win 32 Disk Imager (auf Heft-DVD, Download unter *https://sourceforge.net/projects/win32diskimager*). Hier genügt es, die Quelldatei („Image Datei“) und das Zielgerät („Datenträger“) anzugeben. Die Schaltfläche „Schreiben“ startet den Kopiervorgang.

Die genannten Tools haben einen Nachteil. Die Partitionen aus dem ISO-Abbild werden einfach auf den Stick geschrieben und belegen den gesamten Speicherplatz. Wer den Stick für mehrere Installationen behalten, den Platz aber trotzdem nutzen will, greift zu elaborierten Alternativen. Eine davon ist Unetbootin, das Sie auch unter Windows verwenden können (auf Heft-DVD und Download unter *http://unetbootin.sour-*

ceforge.net). Der USB-Stick muss mit dem Dateisystem FAT32 formatiert sein. Sollte das nicht der Fall sein, sichern Sie alle Dateien und klicken unter Ubuntu 18.04 oder Linux Mint 19 im Navigationsbereich des Dateimanagers mit der rechten Maustaste auf das Laufwerk. Wählen Sie „Formatieren“, stellen Sie als Dateisystem „FAT32“ ein und klicken Sie auf „Formatieren“. Klicken Sie das Laufwerk an, um es ins Dateisystem einzuhängen.

Führen Sie diese drei Befehlszeilen im Downloadverzeichnis aus:

```
sudo apt install p7zip-full
chmod +x unetbootin-linux64-661.
 bin
sudo QT_X11_NO_MITSHM=1 ./
 unetbootin-linux64-661.bin
```

Aktivieren Sie die Option „Abbild“, wählen Sie über die Schaltfläche „...“ die ISO-Datei und klicken Sie auf „Open“. Nach einem Klick auf „OK“ kopiert Unetbootin die Dateien auf den Stick und macht ihn bootfähig. Der USB-Stick bleibt aber weiter nutzbar wie gewohnt.

6. USB-Stick per Bash-Script befüllen

Unter *https://github.com/jsamr/bootiso* finden Sie ein spannendes Bash-Script, das die Erstellung von bootfähigen USB-Sticks erleichtert. Es nutzt einige der in Punkt 3 beschriebenen Tools für die Analyse der ISO-Datei, um die passende Schreibmethode zu finden. Bevor Sie es nutzen, installieren Sie unter Ubuntu die erforderlichen Tools:

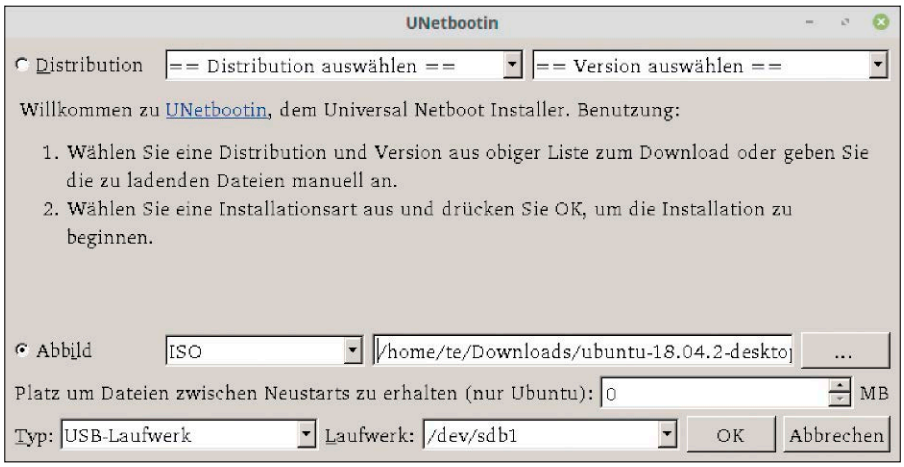
```
sudo apt install curl wimtools
 extlinux
```

Starten Sie das Script mit

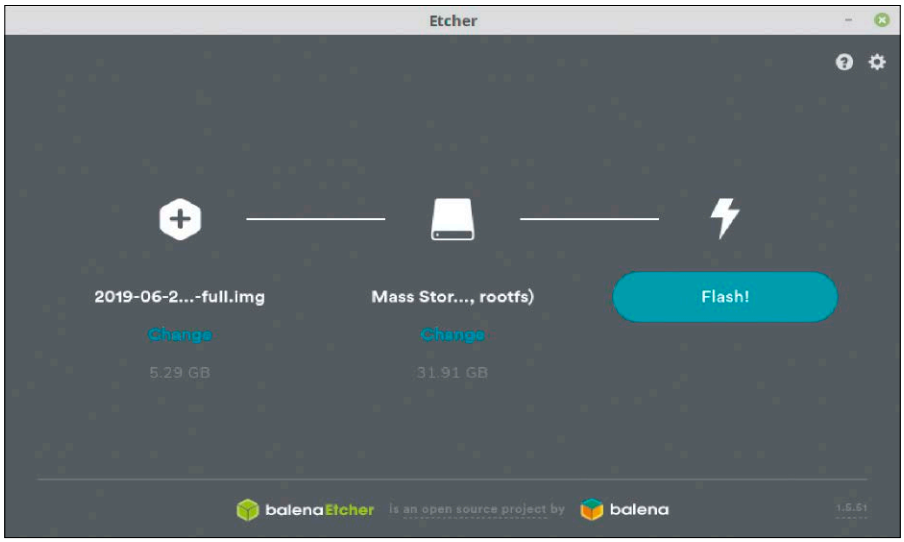
```
./bootiso -p [Boot-DVD.iso]
```

Für den Platzhalter setzen Sie Pfad und Name der ISO-Datei ein. Das Script untersucht die ISO-Datei und zeigt die möglichen Schreibmodi sowie vorhandene USB-Laufwerke an. Wenn das Script den USB-Stick erstellen soll, rufen Sie die Befehlszeile ohne die Option „-p“ erneut auf.

Bootiso kann auch mit ISO-Dateien für die Windows-Installation umgehen. Wenn die Datei „Install.wim“ enthalten ist, teilt es diese in kleinere Portionen auf. Dadurch lässt sich ein FAT32-Stick für die Bios- und Uefi-Installation verwenden. Eine „Install.wim“ mit mehr als vier GB würde ansonsten nur auf einen NTFS-Stick passen, der sich dann aber nicht im Uefi-Modus booten lässt.



Bootstick erstellen: Unetbootin schreibt die Dateien für die Linux-Installation direkt auf den USB-Stick. Dadurch bleibt Platz frei und Sie können den Stick weiter als Datenspeicher nutzen.



SD-Karte befüllen: Balena Etcher verwendet die gleiche Methode wie das Kommandozeilentool dd, bietet dafür aber eine komfortable grafische Oberfläche.

7. Images für Platinen-PCs kopieren

Systemabbilder, etwa für den Raspberry Pi, kopieren Sie auf eine SD-Karte wie in Punkt 5 für ISO-Dateien beschrieben. Sie benötigen dafür am PC einen Kartenleser, in den Sie die SD-Karte stecken.

Laden Sie das Abbild etwa über *www.raspberrypi.org/downloads/raspbian* herunter und entpacken Sie die ZIP-Datei. Unter Windows verwenden Sie den Win 32 Disk Imager (auf Heft-DVD), um die SD-Karte zu befüllen. Linux-Anwender nutzen einen dd-Befehl.

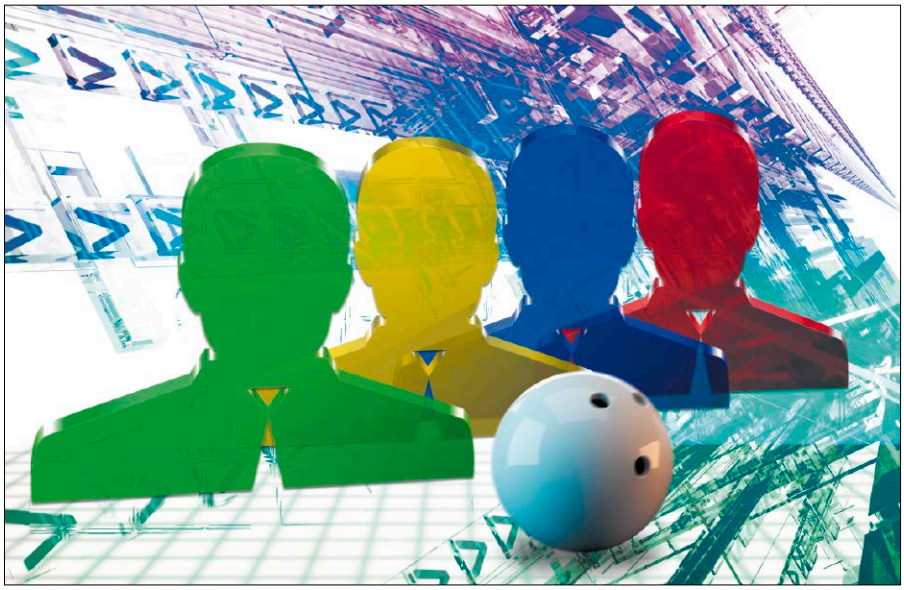
Wer eine grafische Oberfläche bevorzugt, lädt Balena Etcher für Windows oder Linux herunter (*www.balena.io/etcher*). Linux Anwender entpacken die ZIP-Datei und machen die Datei ausführbar. Dazu gehen Sie im Kontextmenü der Appimage-Datei auf „Eigenschaften“, wechseln auf die Registerkarte „Zugriffsrechte“, setzen ein Häkchen vor „Datei als Programm ausführen“ und schließen das Fenster. Starten Sie Etcher per Doppelklick auf die Appimage-Datei. Im Programm klicken Sie auf „Select Image“ und wählen die „img“-Datei mit dem Raspian-Systemabbild. Prüfen Sie das automatisch eingestellte USB-Laufwerk und ändern Sie es gegebenenfalls über „Change“. Nach Klick auf „Flash!“ schreibt Etcher das Abbild auf die SD-Karte.

Einige Distributionen für den Raspberry Pi bieten ein eigenes Tool für den Transfer auf die SD-Karte, beispielsweise Libre Elec (*https://libreelec.tv*). Der „LibreELEC USB-SD Creator“ lädt die Abbilddatei herunter und kopiert diese dann auf die SD-Karte. ■

Benutzer, Gruppen und Dateirechte

Unter Linux besitzt ein Standardbenutzer nur sehr begrenzte Zugriffsrechte. Das kann bei einigen Funktionen zu Einschränkungen führen, die sich mit der richtigen Konfiguration jedoch beseitigen lassen.

VON THORSTEN EGGELING



© David Wolski

Linux ist als Mehrbenutzersystem konzipiert und bietet ein ausgefeiltes Rechtesystem. Ein Standardbenutzerkonto erhält vollen Zugriff auf das eigene Home-Verzeichnis, aber sonst nur auf wenige andere Ordner. Das Systemverwalterkonto „root" hat dagegen alle Rechte im gesamten Dateisystem. Zwischen diesen Extremen liegen jedoch zahlreiche Abstufungen. Obwohl das Linux-Rechtesystem nicht besonders kompliziert ist, kommt es immer wieder zu Problemen aufgrund mangelnder Benutzerrechte. Dann ist beispielsweise kein Zugriff auf eine zweite Festplatte oder auf die Dateien einer Netzwerkfreigabe möglich.

Die Aussagen in diesem Artikel gelten für Ubuntu 18.04. Bei anderen Distributionen funktioniert es entsprechend, es gibt jedoch punktuelle Abweichungen bei der Verwendung einzelner Tools oder der Beschriftung von Menüpunkten.

Service: Der Artikel enthält Beispiele mit längeren Kommandozeilen. Die müssen Sie nicht vom Heft abtippen; sie sind unter *www.pcwelt.de/Ub3xvH* zusammengefasst und können von dort in das Terminal oder den Texteditor kopiert werden.

1. Systematik der Benutzerrechte unter Linux

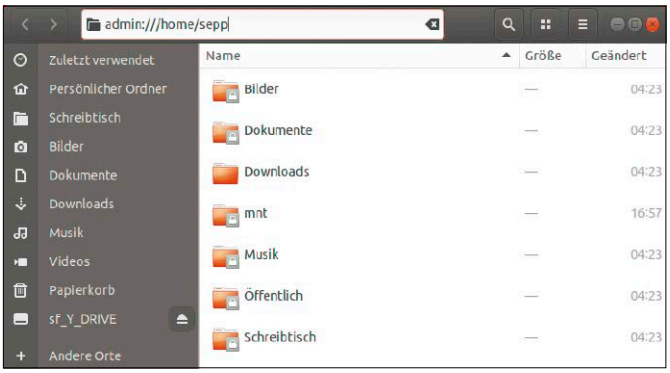
Jedes Element im Dateisystem hat unter Linux einen Eigentümer und es gehört einer Gruppe. Die Zugriffsrechte werden getrennt für Eigentümer und Gruppe über die Modi „Lesen", „Schreiben" und „Ausführen/Suchen" bestimmt. Letzterer bezieht sich bei Ordnern auf das fundamentale Recht, den Ordner zu öffnen, bei Dateien hingegen auf das Ausführungsrecht. Wenn dieses fehlt, lässt sich eine Datei nicht als Programm starten. Ist ein Benutzer weder Eigentümer noch Mitglied der definierten Gruppe, gehört er zu „Andere". Auch für ihn lassen sich die drei genannten Modi einstellen. Es lassen sich daher insgesamt neun Zugriffsrechte vergeben: „Lesen", „Schreiben" und „Ausführen/Suchen" jeweils für den Eigentümer, die Gruppe und für andere Benutzer. Die Rechte für Ordner wirken sich indirekt auch auf die darin liegenden Ordner aus. Wenn Sie „Ausführen/Suchen" verbieten, gilt das auch für die darunterliegenden Ordner. Es gibt eine Besonderheit: Ist dieses Recht bei einem Ordner erlaubt, aber „Lesen" nicht, kann ein anderer Benutzer eine darin befindliche Datei öffnen, wenn ihm der Pfad beziehungsweise Dateiname bekannt ist.

2. Benutzerrechte im Dateimanager verwalten

Welche Rechte für einen Ordner oder eine Datei gelten, ermitteln Sie unter Ubuntu im Dateimanager Nautilus („Dateien"). Wählen Sie eine Datei oder einen Ordner mit der rechten Maustaste aus, gehen Sie im Menü auf „Eigenschaften" und dann auf die Registerkarte „Zugriffsrechte". Hinter „Zugriff" können Sie die Rechte für „Besitzer", „Gruppe" und „Andere" festlegen, außerdem lässt sich die Gruppe ändern. Standardmäßig sind Gruppe und Benutzer im Home-Verzeichnis identisch. Per Klick auf die Schaltfläche „Zugriffsrechte der enthaltenen Dateien ändern" lassen sich bei Ordnern die Rechte rekursiv für alle enthaltenen Elemente setzen.

Sie werden bemerken, dass bei Ubuntu die Rechte für „Andere" mit „Auf Dateien zu-

Zugriffsrechte im Dateimanager: Über Nautilus ermitteln Sie, was Sie in welchem Ordner dürfen. Unter Ubuntu können Sie auch auf Dateien in fremden Home-Verzeichnissen zugreifen.



Maximale Rechte: Mithilfe der Nautilus-Erweiterung nautilus-admin lassen sich im Dateimanager Ordner mit administrativem Rechten öffnen und Dateien darin bearbeiten.

greifen“ eingestellt ist. Andere Benutzer können daher den Inhalt fremder Home-Verzeichnisse einsehen und Dateien darin öffnen, aber nicht ändern. Wenn Sie das nicht möchten, setzen Sie für Ihr Benutzerverzeichnis unter „/home“ die Rechte für „Andere“ hinter Zugriff auf „Keiner“. Das gilt dann auch für alle Unterverzeichnisse.

Rechte in fremden Ordnern setzen: Die Rechte lassen sich über den Dateimanager nur bei Elementen ändern, deren Eigentümer Sie sind. Für andere Dateiobjekte benötigen Sie daher den Dateimanager mit erhöhten Rechten. Das geht am einfachsten, indem Sie das Paket „nautilus-admin“ installieren und sich ab- und wieder anmelden. Im Kontextmenü von Ordner gehen Sie auf „Als Administrator öffnen“. Tippen Sie Ihr Passwort ein und klicken Sie auf „Anmelden“. Danach öffnet sich ein neues Nautilus-Fenster, in dem Sie administrative Rechte haben und Zugriffsrechte beliebig setzen können.

Wenn Sie den Ordner über die Seitenleiste wechseln, gehen die Admin-Rechte wieder verloren. Verwenden Sie zur Navigation daher einen Klick auf den Pfad-Bestandteil „/“ in der Adressleiste. Mit Strg-L lässt sich die Eingabezeile einblenden. Sie sehen dann, dass vor dem Pfad das Präfix „admin://“ steht. Tragen Sie einfach den gewünschten Pfad ein, beispielsweise „admin:///etc“ (drei Slashes), um den Ordner als Administrator zu öffnen.

3. Benutzerrechte auf der Kommandozeile verwalten

Im Terminalfenster lassen sich Zugriffsrechte flexibler kontrollieren als im Dateimanager. Mit chown ändern Sie den Eigentümer und mit chmod die Zugriffsrechte von Elementen im Dateisystem. Dazu ein Beispiel: Auf Ihrem Rechner läuft der Webserver Apache und Sie haben Wordpress im Ordner „/var/www/wordpress“ installiert. Sie haben die Wordpress-Dateien mit administrativen Rechten in diesen Ordner kopiert, deshalb gehören alle Elemente erst einmal dem Benutzer „root“. Die Gruppe ist ebenfalls auf „root“ gesetzt. Das Beispiel gilt sinngemäß für alle Ordner, die mehrere Nutzer gemeinsam nutzen wollen. Dazu gehören auch Serverdienste, die unter einem eigenen Konto laufen.

Apache wird unter Ubuntu über das Benutzerkonto „www-data“ gestartet, das zur gleichnamigen Gruppe gehört. Die Dateien und Ordner unter „/var/www/wordpress“ müssen jedoch dem Apache-Nutzer gehören, damit sich über das Wordpress-Back-End Updates und Plug-ins installieren lassen. Folglich müssen Sie die Rechte ändern:

```
chown -R www-data:www-data /var/
  www/wordpress
```

Der Parameter „-R“ steht für rekursiv. Damit wirkt sich der Befehl auf alle enthaltenen Ordner und Dateien aus. Dahinter stehen der neue Besitzer und die Gruppe. Indem Sie den Besitz aller Ordner und Dateien an „www-data“ übertragen, haben der Apache-Server und damit auch Wordpress das Recht, hier Konfigurationsdateien zu erzeugen und Dateien zu erstellen.

Sensible Dateien sollten Sie nach Abschluss der Wordpress-Einrichtung schützen, indem Sie Rechte wieder entziehen. Die grundlegende Wordpress-Konfigurationsdatei „wp-config.php“ beispielsweise sollten mögliche Angreifer nicht manipulieren dürfen.

Dem Server genügt der Lesezugriff, wenn Wordpress fertig eingerichtet ist. Mit den folgenden zwei Zeilen lässt sich das umsetzen:

```
chmod a-w /var/www/wordpress/wp-
  config.php
chmod go-r /var/www/wordpress/wp-
  config.php
```

Der Parameter „a“ bezieht sich auf „Alle“, also auf den Besitzer, die Gruppe und andere Benutzer. „-w“ entzieht das Schreibrecht. In der zweiten Zeile entfernen Sie das Recht „Lesen“ für die Gruppe und andere Benutzer. Es bleibt nur das Leserecht für den Eigentümer übrig. Die möglichen Angaben bei chmod sind „u“ für den Eigentümer, „g“ für die Gruppe und „o“ für andere. Diese kombinieren Sie mit den Rechten „r“ (Lesen), „w“ (Schreiben) und „x“ (Ausführen/Suchen). Ein „-“ entfernt das Recht, „+“ fügt es hinzu und „=“ setzt die Rechte neu.

Damit Sie nicht zwei Befehlszeilen verwenden müssen, empfiehlt sich die oktale Schreibweise:

```
chmod 400 /var/www/wordpress/wp-
  config.php
```

Der Wert „4“ steht für „Lesen“ und „0“ für keine Rechte. Die erste Stelle bezieht sich auf den Eigentümer, die zweite auf die Gruppe und die dritte auf alle anderen Benutzer. Verwenden Sie den Wert „600“, um dem Eigentümer wieder Schreibrechte zu gewähren. Eine Übersicht mit der Bedeutung der numerischen Werte finden Sie über *www.pcwelt.de/8P42PF*.

Im Terminalfenster prüfen Sie, welche Rechte für Dateien und Ordner gelten. Die gesetzten Rechte in einem Ordner prüfen Sie mittels des Befehls

```
ls -al /var/www/wordpress
```

ls zeigt die Rechte in der ersten Spalte mit „r“, „w“ und „x“ (Lesen, Schreiben, Ausfüh-

```
te@ub180407: ~
Datei  Bearbeiten  Ansicht  Suchen  Terminal  Hilfe
te@ub180407:~$ ls -al /var/www/wordpress/
insgesamt 224
drwxrwxr-x+  5 www-data www-data  4096 Mär  3 04:24 .
drwxrwxr-x   4 root     root      4096 Mär  3 01:38 ..
-rw-rw-r--+  1 www-data www-data   420 Mär  3 01:38 index.php
-rw-rw-r--+  1 www-data www-data 19935 Mär  3 02:42 license.txt
-rw-rw-r--+  1 www-data www-data  7425 Mär  3 02:43 readme.html
-rw-rw-r--+  1 sepp     sepp         0 Mär  3 04:24 test.txt
-rw-rw-r--+  1 www-data www-data  6919 Mär  3 03:57 wp-activate.php
drwxrwxr-x+  9 www-data www-data  4096 Feb 21 23:09 wp-admin
-rw-rw-r--+  1 www-data www-data   369 Mär  3 01:38 wp-blog-header.php
-rw-rw-r--+  1 www-data www-data  2283 Mär  3 01:44 wp-comments-post.php
-rw-rw-r--+  1 www-data www-data  2898 Mär  3 01:38 wp-config-sample.php
drwxrwxr-x+  4 www-data www-data  4096 Feb 21 23:09 wp-content
-rw-rw-r--+  1 www-data www-data  3847 Mär  3 01:38 wp-cron.php
drwxrwxr-x+ 19 www-data www-data 12288 Feb 21 23:09 wp-includes
-rw-rw-r--+  1 www-data www-data  2502 Mär  3 01:39 wp-links-opml.php
-rw-rw-r--+  1 www-data www-data  3306 Mär  3 01:39 wp-load.php
-rw-rw-r--+  1 www-data www-data 38883 Mär  3 01:38 wp-login.php
-rw-rw-r--+  1 www-data www-data  8403 Mär  3 01:39 wp-mail.php
```

Rechte prüfen: Das Terminal zeigt nach „ls -al [Ordner]“ alle Zugriffsrechte sowie Eigentümer und Gruppen für Dateien und Ordner detailliert an.

ren) in der Reihenfolge Eigentümer, Gruppe und andere Benutzer an. Um sich die Rechte zusätzlich in oktaler Schreibweise anzeigen zu lassen, verwenden Sie diese Befehlszeile:

```
stat -c '%A %a %U %G %n' /var/www/
  wordpress/*
```

Informationen zu einer einzelnen Datei lassen Sie sich mit *stat [Dateiname]* ausgeben.

Hinweis: Die Beschreibung gilt nur für den eigenen Ubuntu-Rechner zu Hause und für Rootserver im Rechenzentrum. Bei preisgünstigen Hostingangeboten erfolgt der Upload der Wordpress-Dateien per FTP. Die Zugriffsrechte sind dann automatisch so gesetzt, das Wordpress Lese- und Schreibzugriff erhält.

4. Zugriffsrechte mit chmod rekursiv ändern

Mit chmod lassen sich wie bei chown mit der zusätzlichen Option „-R“ Zugriffsrechte rekursiv setzen. Das wirkt sich dann auf Ordner und Dateien gleichermaßen aus. Wenn Sie beispielsweise den oktalen Wert „775“ verwenden, erlauben Sie bei Ordnern Lesen, Schreiben und Suchen für Eigentümer, Gruppe und andere Benutzer. Bei Dateien setzt „775“ jedoch das Recht „Ausführen“.

An sich ist das kein Problem, weil das etwa bei TXT- oder PHP-Dateien funktional zunächst nichts ändert. Auf einem über das Internet erreichbaren Server kann das aber von Hackern ausgenutzt werden. Aus der harmlosen Textdatei wird ein ausführbares Script, über das sich weiterer Schadcode absetzen lässt. Es ist daher sicherer, statt „chmod -R ...“ diese beiden Befehlszeilen zu verwenden:

```
sudo find /var/www -type d -exec
  chmod 775 {} +
sudo find /var/www -type f -exec
  chmod 664 {} +
```

Die erste Zeile wirkt sich auf alle Verzeichnisse („d“ für Directories) unterhalb von „/var/www“ aus und erlaubt Eigentümer und Gruppe den Vollzugriff. „Andere“ dürfen den Inhalt der Verzeichnisse sehen. Die zweite Zeile ändert die Rechte von Dateien („f“ für Files). Eigentümer und Gruppe erhalten Lese- und Schreibrechte, „Andere“ nur die Leseberechtigung.

5. Über Gruppen mehr Rechte einräumen

Standardnutzer erhalten im Beispiel aus Punkt 4 nur Leserechte im Ordner „/var/www“. Arbeiten mehrere Benutzer beispielsweise an Templatedateien oder CSS-Anpassungen, teilen Sie diesen aus Sicherheitsgründen in der Regel nicht das root-Passwort mit. Eine Möglichkeit ist es, Benutzer in die Gruppe des Webservers aufzunehmen und ihnen darüber Schreibrechte zu gewähren:

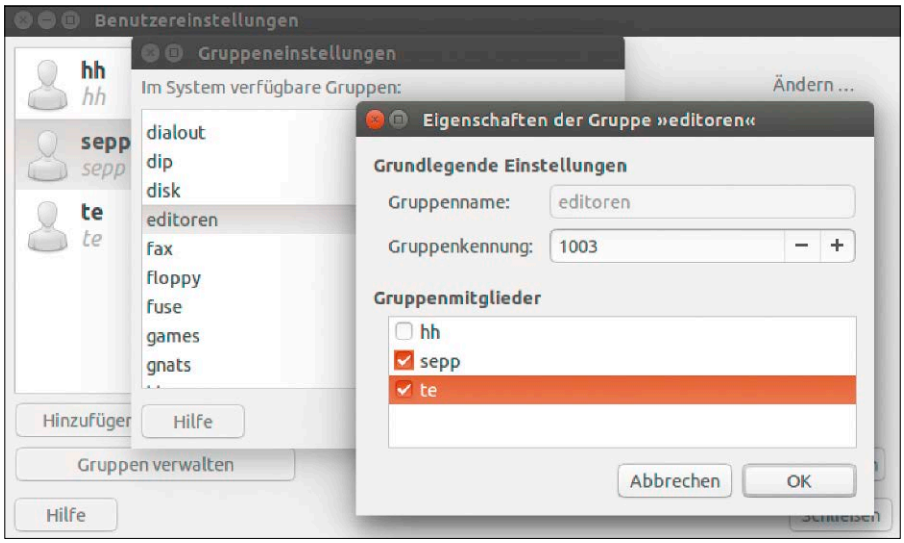
```
sudo usermod -a -G www-data [User]
```

Den Platzhalter „[User]“ ersetzen Sie durch die Anmeldekennung des Benutzers, der die Rechte erhalten soll.

Wer zur Verwaltung von Benutzern und Gruppen die grafische Oberfläche bevorzugt, installiert am besten das Paket gnome-system-tools („Benutzer und Gruppen“). Sie rufen es über eine Suche nach „Benutzer“ auf. Nach einem Klick auf „Gruppen verwalten“ erstellen Sie neue Gruppen und fügen Benutzer zur Gruppe hinzu.

Optimal ist diese Lösung jedoch nicht. Mitglieder der Gruppe „www-data“ haben Vollzugriff auf alle Dateien, die dieser Gruppe gehören. Neu angelegte Dateien gehören dem jeweiligen Benutzer, die Gruppe verliert das Schreibrecht.

Es gibt jedoch eine einfachere und zuverlässige Alternative, die wir in Punkt 6 beschreiben.



Benutzer und Gruppen verwalten: Installieren Sie gnome-system-tools („Benutzer und Gruppen“), wenn Sie Gruppen über die grafische Oberfläche erstellen und Benutzer zuweisen wollen.

6. Rechte über ACLs vergeben

Access Control Lists berücksichtigen die klassischen Unix-Rechte Eigentümer („user"), Gruppen („group") und Andere („other"). In aktuellen Linux-Systemen lassen sich ACLs standardmäßig verwenden (siehe Kasten „System für ACLs vorbereiten" auf dieser Seite unten).

Mit folgender Befehlszeile ermitteln Sie die geltenden Rechte:

```
getfacl /var/www/wordpress
```

Die Ausgabe enthält das, was aufgrund der bisher gesetzten Berechtigungen zu erwarten ist. „r" und „w" stehen für Lese- und Schreibrechte, „x" für ausführen/suchen.

Erstellen Sie die Gruppe „editoren", die Lese- und Schreibberechtigungen erhalten soll, und fügen Sie die gewünschten Benutzer („[User]") hinzu:

```
groupadd editoren
sudo usermod -a -G editoren [User]
```

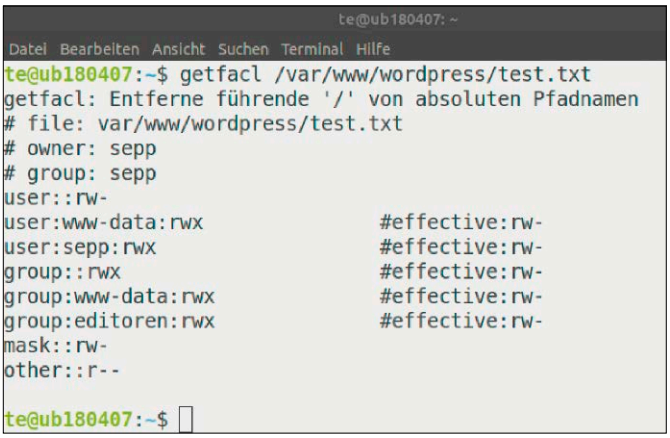
Melden Sie sich bei Linux ab und wieder an, damit die neue Gruppenzugehörigkeit wirksam wird. Mit folgender Befehlszeile geben Sie den Gruppen „www-data" sowie „editoren" und zusätzlich den Benutzern „www-data" sowie „sepp" Lese- und Schreibrechte („rwX") für den Ordner „/var/www/wordpress" und alle darin befindlichen Elementen („-R -m"). Der jeweils aktuelle Benutzer („u::rwW") und die Gruppe („g::rwX") erhalten Lese- und Schreibrechte.

```
sudo setfacl -R -m
  u::rwX,g::rwX,u:www-
  data:rwX,u:sepp:rwX,g:www-
  data:rwX,g:editoren:rwX /var/www/
  wordpress
```

Beachten Sie die Großschreibung bei „rwX". Mit „X" setzen Sie bei Ordnern das Recht „Suchen", bei Dateien bleibt „Ausführen" erhalten, wenn bereits vorhanden. Damit sich die Rechte auch auf neue Elemente auswirken, setzen Sie die „Default-ACLs". Dazu wiederholen Sie die Befehlszeile, ergänzen aber die Option „-d" vor „-m".

```
sudo setfacl -R -d -m
  u::rwX,g::rwX,u:www-
  data:rwX,u:sepp:rwX,g:www-
  data:rwX,g:editoren:rwX /var/www/
  wordpress
```

Um Fehler zu vermeiden, sollten Sie – wenn möglich – nur mit Gruppen arbeiten. Bei Bedarf erstellen Sie weitere Gruppen, fügen Benutzer hinzu und gewähren den Gruppen Vollzugriff auf unterschiedliche Verzeichnisse. Über die Option „-x" entfernen Sie einzelne ACLs:



ACLs verwenden: Das Tool getfacl zeigt Benutzer und Gruppe einer Datei an. Außerdem sehen Sie die geltenden Standardrechte und Access Control Lists.

```
sudo setfacl -R -x g:editoren /var/
  www/wordpress
```

Verwenden Sie danach die Optionen „-R -d -x", um auch die Standardberechtigungen zu entfernen. Einfacher geht es, wenn Sie

```
sudo setfacl -R -b /var/www/
  wordpress
```

nutzen. Damit löschen Sie alle ACLs und danach setzen Sie die Berechtigungen neu.

Rechte kontrollieren: Wenn der Benutzer „sepp" mit

```
touch /var/www/wordpress/test.txt
```

eine neue Datei erstellt, dann liefert

```
getfacl /var/www/wordpress/test.txt
```

die Liste mit den Zugriffsrechten. Die Datei gehört Benutzer und Gruppe „sepp", was sich gegenüber Punkt 5 nicht geändert hat. Durch die ACLs haben die Gruppen „editoren" und „www-data" jedoch weiterhin Lese- und Schreibrechte. Bei Mitgliedern der Gruppe „editoren" ist es entsprechend.

7. Rechte für Samba-Freigaben

Bei Samba Freigaben wirken zwei Rechtesysteme: Die Zugriffsrechte im Dateisystem gelten weiterhin, sekundär treten nun die Samba-Rechte beim Netzzugriff hinzu. Sie können daher Benutzern oder Gruppen den Zugriff im Dateisystem erlauben, über Samba aber verhindern (und umgekehrt).

Über den Dateimanager Nautilus lässt sich ein Ordner im eigenen Home-Verzeichnis über den Kontextmenüpunkt „Freigabe im lokalen Netzwerk" freigeben („usershare" im Unterschied zur administrativen Freigabe über „/etc/samba/smb.conf"). Sollte der Samba-Server nicht eingerichtet sein, wird die Installation angefordert. Damit ein Benutzer die Funktion verwenden darf, muss er Mitglied der Gruppe „sambashare" sein. Der bei der Installation eingerichtete Erstbenutzer ist bereits in dieser Gruppe. Andere Benutzer fügen Sie so hinzu:

```
sudo usermod -a -G sambashare [User]
```

Setzen Sie ein Häkchen vor „Diesen Ordner freigeben". Wenn Sie auch ein Häkchen vor „Anderen erlauben, Dateien in diesem Ordner zu erstellen und zu löschen" setzen, erscheint nach einem Klick auf „Freigabe erstellen" ein Dialog, in dem Sie auf „Die

SYSTEM FÜR ACLS VORBEREITEN

Access Control Lists (ACL) ergänzen das Rechtesystem von Linux. ACLs eigen sich vor allem für die Vergabe von vererbbaren Rechten für neue Dateien in Mehrbenutzerumgebungen. Access Control Lists gehören seit Ubuntu 12.04 zum Standard. Zur Sicherheit kontrollieren Sie das im Terminal:

```
sudo tune2fs -l /dev/sda1 | grep "Default mount options:"
```

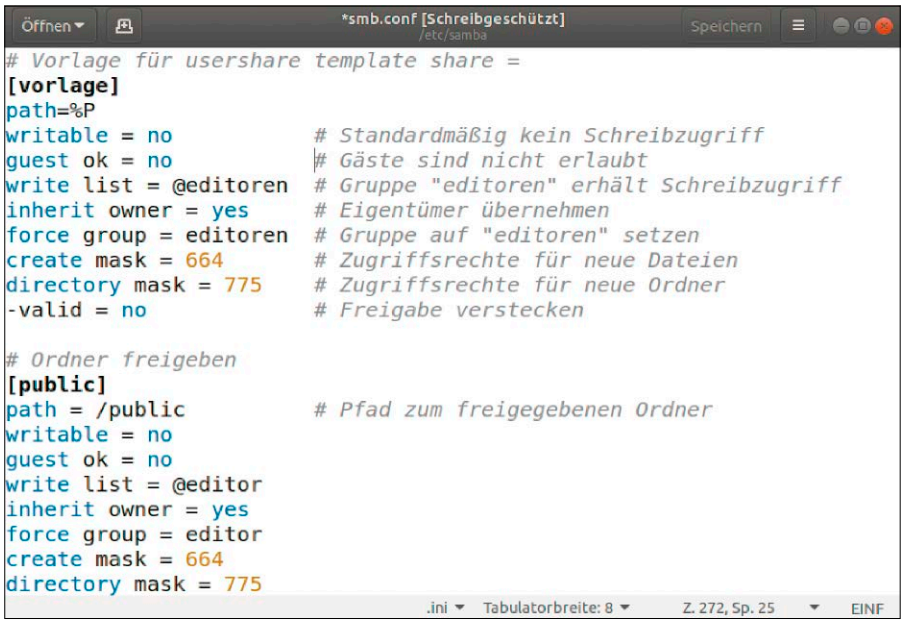
In der Ausgabe sollte der Wert „acl" auftauchen. Wenn nicht, verwenden Sie folgenden Befehl und starten danach Linux neu:

```
sudo tune2fs -o acl /dev/sda1
```

„/dev/sda1" ersetzen Sie durch den Pfad der Partition, auf der Sie ACLs nutzen wollen. Die nötigen Tools zur Verwaltung der Access Control Lists installieren Sie mit

```
sudo apt install acl
```

unter Ubuntu und verwandten Systemen.



Benutzerfreigaben konfigurieren: In der Datei „/etc/samba/smb.conf“ hinterlegen Sie eine Vorlage, welche die Rechtevergabe für neu erstellte Freigaben regelt.

Zugriffsrechte automatisch setzen“ klicken. Nautilus ändert dann selbständig die Rechte im Dateisystem, damit andere Benutzer Lese- und Schreibzugriff erhalten.

Bei Samba-Freigaben ergibt sich aber das gleiche Problem wie in Punkt 5 beschrieben. Dateien, die ein anderer Benutzer über das Netzwerk neu erstellt, gehören ihm. Ihnen selbst fehlt dann der Schreibzugriff. Auch hier lässt sich das Problem über ACLs lösen (siehe Punkt 6).

Samba bietet aber auch eigene Einstellungen für die Benutzerrechte, die sich einfacher anwenden lassen. Öffnen Sie die Samba-Konfigurationsdatei in einem Terminal mit dem Kommando

```
sudo gedit /etc/samba/smb.conf
```

In den Abschnitt „[global]“ fügen Sie diese Zeile ein:

```
usershare template share = vorlage
```

Fügen Sie am Ende der Datei die zehn Zeilen aus der Abbildung oben an. Danach starten Sie Samba neu:

```
sudo service smbd restart
```

In unserem Beispiel erhalten alle Mitglieder der Gruppe „editoren“ Schreibrechte über das Netzwerk („write list = @editoren“). Neue Dateien gehören dem Besitzer des Ordners („inherit owner = yes“) und der Gruppe „editoren“ („force group = editoren“). Die Zugriffsrechte von Dateien werden auf „664“ gesetzt („create mask = 664“), was dem Eigentümer und der Gruppe Schreibrecht einräumt. Bei Ordnern ergibt sich durch „directory mask = 775“ Vollzugriff für den Eigentümer und die Gruppe. „-valid = no“ sorgt dafür, dass die Vorlage nicht als Freigabe erscheint. Sie wird aber von allen Benutzerfreigaben über Nautilus berücksichtigt.

Globale administrative Freigaben lassen sich nach dem gleichen Schema konfigurieren. Hinter „path=“ tragen Sie den Pfad des Ordners ein, den Sie freigeben wollen. „-valid = no“ löschen Sie. Dann setzen Sie im Dateisystem die Rechte für diesen Ordner so, dass alle Benutzer zugreifen dürfen (siehe Punkt 4).

8. Rechte bei gemounteten Laufwerken

USB-Laufwerke, die mit dem Dateisystem NTFS oder FAT32 formatiert sind, erscheinen automatisch im Dateimanager. Jeder Benutzer hat Lese- und Schreibzugriff. Wenn Sie eine neue Festplatte in den PC einbauen und diese mit dem Dateisystem Ext4 formatieren, erhalten Sie standardmäßig nur Lesezugriff. Das Problem lässt sich über das Tool gnome-disks beheben, das Sie im Menü mit einer Suche nach „Laufwerke“ finden und starten.

Auf der linken Seite des Fensters wählen Sie die neue Festplatte, klicken dann im rechten Bereich des Fensters auf die Schaltfläche mit dem Zahnradsymbol und wählen „Partition formatieren“ (eventuell vorhandene Dateien vorher sichern!).

Hinter „Typ“ wählen Sie „Interne Disk für die ausschließliche Nutzung mit Linux Systemen (ext4)“ und hinter „Name“ geben Sie eine aussagekräftige Bezeichnung ein. Klicken Sie auf „Nächstes“ und danach auf „Formatieren“. Bestätigen Sie den Vorgang mit Ihrem Passwort.

Über die „Play“-Schaltfläche neben dem Zahnradsymbol lässt sich die neue Partition in das Dateisystem unterhalb von „/media/[User]/Data“ einbinden. Wenn Sie sich die Zugriffsrechte über den Dateimanager ansehen (siehe Punkt 2), stellen Sie fest, dass der Ordner Ihnen gehört und nur Sie Vollzugriff haben.

NETZWERKLAUFWERKE ALS „ROOT“ MOUNTEN

Netzwerkfreigaben lassen sich über das mount-Tool einbinden, was aber nur mit root-Rechten erfolgen kann:

```
sudo mount -t cifs -o vers=1.0,user=[Share-Benutzer],pass=[geheim],ui
  d=[Benutzer],gid=[Gruppe],dir_mode=0775,file_mode=0664 //
  [MeinServer]/[MeineFreigabe] /mnt
```

Für die Platzhalter setzen Sie die Werte für Ihr Netzwerk ein. Durch Angabe von „uid“ und „gid“ gehören alle Elemente im Mountpunkt zu „[Benutzer]“ beziehungsweise „[Gruppe]“. „dir_mode“ und „file_mode“ sorgen für Lese- und Schreibrechte. Ohne diese Parameter hätte nur root Vollzugriff.

Für die automatische Einbindung beim Systemstart verwenden Sie die entsprechende Zeile in der Datei „/etc/fstab“:

```
//[MeinServer]/[MeineFreigabe] /mnt username=[Benutzer],password=[ge
  heim],uid=[Benutzer],gid=[Gruppe],file_mode=0644,dir_mode=0755 0 0
```

Ob ein neuer Eintrag in der fstab funktioniert, können Sie vorab mit dem Befehl

```
sudo mount -a
```

testen.

Damit auch andere Nutzerkonten das Laufwerk verwenden können, hängen Sie die Partition über die „Stop“-Schaltfläche wieder aus. Klicken Sie auf das Zahnradsymbol und wählen Sie „Einhängeoptionen bearbeiten“. Setzen Sie den Schalter hinter „Vorgaben der Benutzersitzung“ auf „Aus“. Hinter „Einhängepunkt“ geben Sie das gewünschte Verzeichnis an, beispielsweise „/mnt/Data“. Das Verzeichnis muss nicht existieren, es wird automatisch erstellt. Klicken Sie auf „OK“, und bestätigen Sie mit Ihrem Passwort. Klicken Sie auf die „Play“-Schaltfläche, um das Laufwerk wieder einzubinden.

Das alleine genügt jedoch noch nicht, denn das Verzeichnis „/mnt/Data“ gehört auch jetzt dem Benutzer, der es angelegt hat. Damit auch andere Benutzer des PCs auf die Dateien zugreifen können, gehen Sie im Dateimanager auf „/mnt/Data“, wählen im Kontextmenü „Eigenschaften“ und gehen auf die Registerkarte „Zugriffsrechte“. Ändern Sie für „Andere“ hinter „Zugriff“ die Einstellung in „Auf Dateien zugreifen“. Soll auch der Schreibzugriff möglich sein, wählen Sie „Dateien erstellen und löschen“. Auch hier ergibt sich ein Problem mit den Zugriffsrechten: Legt ein Benutzer Ordner oder Dateien an, gehören sie ihm und allen anderen Benutzern fehlt der Schreibzugriff. Die Lösung heißt wieder „Access Control Lists“:

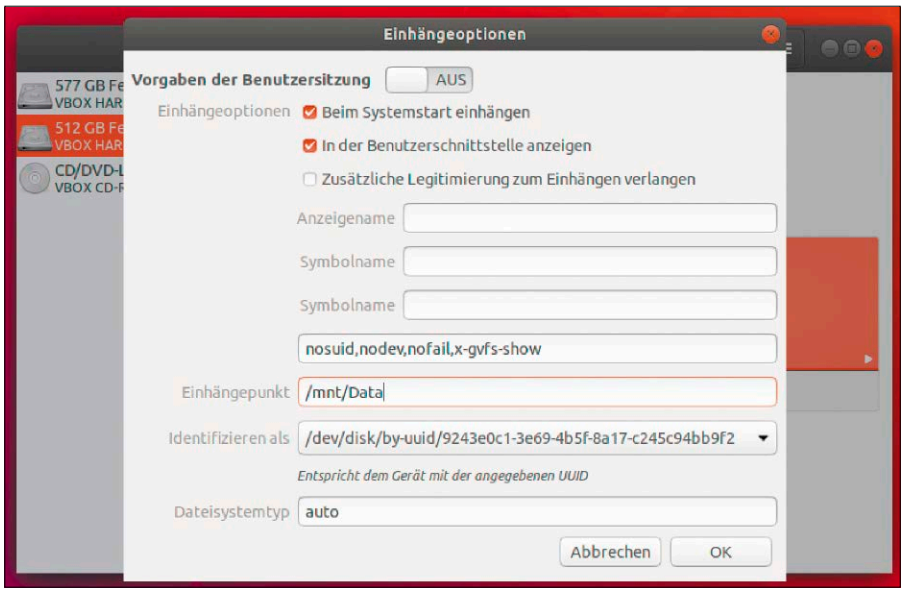
```
sudo setfacl -R -m u::rwX,
  g:editoren:rwX,o::rX /mnt/Data
sudo setfacl -R -d -m u::rwX,
  g:editoren:rwX,o::rX /mnt/Data
```

Der Besitzer und die Gruppe „editoren“ erhalten Lese- und Schreibrechte („u::rwX,g:editoren:rwX“). Andere Benutzer dürfen Dateien nur lesen („o::rX“).

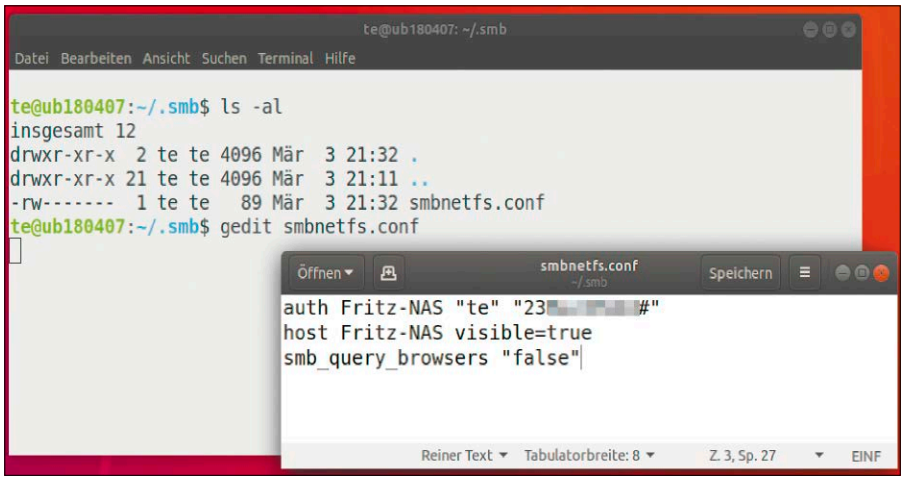
9. Netzwerkressourcen mounten

Netzwerkfreigaben lassen sich unter Ubuntu bequem über den Dateimanager in das Dateisystem einhängen („Andere Orte → Netzwerke“). In der Adressleiste erscheint ein Pfad in der Form „smb://[Server]/[Freigabe]“, im Dateisystem ist das Netzwerklaufwerk allerdings unterhalb von „/run/user/[User-ID]/gvfs/[...]“ zu finden.

Wem dieser Pfad zu lang ist, beispielsweise für die Verwendung in Backup-Scripts, verwendet alternativ das Tool smbnetfs (mit gleichnamigem Paketnamen). Damit können Sie einen Ordner im eigenen Home-Verzeichnis als Mountpunkt verwenden.



Festplatten einhängen: Das Tool Laufwerke kann Festplatten formatieren und dafür sorgen, dass Linux beim Systemstart Partitionen automatisch in das Dateisystem einbindet.



Freigabe als Benutzer mounten: Die Konfiguration von smbnetfs erfolgt über die Datei „~/.smb/smbnetfs.conf“. Darin legen Sie die Anmeldedaten für einen oder mehrere Server fest.

Das Tool benötigt die Konfigurationsdatei „~/.smb/smbnetfs.conf“ und einen Mountpunkt:

```
mkdir ~/.smb
mkdir -p ~/mnt/smb
gedit ~/.smb/smbnetfs.conf
```

Fügen Sie im Editor die folgenden drei Zeilen in die „smbnetfs.conf“ ein:

```
auth [Server] "[Benutzer]"
  "[Password]"
host [Server] visible=true
smb_query_browsers "false"
```

Die Platzhalter ersetzen Sie durch die Daten für Ihren Dateiserver. Um das Passwort vor unbefugten Zugriffen zu schützen, beschränken Sie die Zugriffsrechte:

```
chmod 0600 ~/.smb/smbnetfs.conf
```

Danach binden Sie die Freigabe mit

```
smbnetfs /home/[Benutzer]/mnt/smb
```

ein. Der Pfad ist dann bequem im Terminalfenster erreichbar und das Laufwerk taucht automatisch im Dateimanager auf. Soll die Einbindung beim Systemstart automatisch erfolgen, erstellen Sie für die Befehlszeile einen Autostarter über das Tool Startprogramme. Bei Bedarf lässt sich die Einbindung mit

```
fusermount -u ~/mnt/smb
```

wieder lösen.

Es gibt weitere spezialisierte Tools, über die Benutzer Netzwerklaufwerke einbinden können: sshfs eignet sich für SSH-Verbindungen, curlftpfs für den Zugriff auf FTP-Server. ■

Partitionen sichern und klonen

Die Livesysteme Clonezilla und Rescuezilla sichern Linux- oder Windows-Datenträger in komprimierte Abbilder und schreiben diese bei Bedarf wieder zurück. Dieser Ratgeber erklärt, wie Sie diese Werkzeuge nutzen und wo sich diese Aktion anbietet.

VON HERMANN APFELBÖCK

Rescuezilla und Clonezilla erledigen das Backup und Restore kompletter Datenträger oder ausgewählter Partitionen. Technische Basis ist bei beiden Tools das Kommandozeilenwerkzeug Partclone. Um die Verhältnisse vereinfacht zu skizzieren: Partclone ist ein Hardcorewerkzeug, das sich allenfalls Profis für automatisierte Datenträgersicherungen zumuten. Auf der komfortablen Gegenseite steht das klickfreundliche Rescuezilla, das auch Einsteiger mit wenigen Schaltflächen übersichtlich durch die anspruchsvolle Aktion führt. Etwa in der Mitte steht das textbasierte Clonezilla, das – besser mit Cursortasten, Tabulator, Eingabe- und Leertaste statt mit Maus – etwas antiquiert zu bedienen ist, aber andererseits funktional unübertroffen bleibt.

Clonezilla wie das seit Ende 2020 voll kompatible Rescuezilla beherrschen neben verbreiteten Linux-Dateisystemen (Ext2, Ext3, Ext4, BTRFS, XFS, JFS, F2FS, Reiser FS, Reiser4) auch Windows- und Apple-Partitionen wie FAT, exFAT, NTFS und HFS+. Die Images können auf lokalen (USB-)Datenträgern und auf Netzwerkfreigaben gespeichert werden. Im Netz beherrscht Clonezilla alle Protokolle (Samba, SSH, NFS, Webdav), während Rescuezilla sich auf Windows/Samba-Freigaben beschränkt.

Weitere Vorzüge von Clonezilla sind das direkte Klonen von Datenträger zu Datenträger, ferner die optionale Verschlüsselung der Imagesicherungen.

Clonezilla ist ohne Zweifel der Maßstab, Rescuezilla bleibt funktional auf eine Untermenge reduziert. Rescuezilla erfüllt aber die Ansprüche typischer Endanwender vollumfänglich, zumal einer Sicherung ins Netzwerk schon aus Geschwindigkeitsgründen meist lokales USB vorgezogen wird.

Warum sichern oder klonen?

Für das Sichern von Partitionen oder ganzen Festplatten gibt es mindestens drei starke Motive:

Systemsicherheit: Trotz Reparaturmechanismen von Linux- und Windows-Systemen sind manche Havarien gar nicht mehr zu beheben oder nur mit unzumutbaren Rechercheaufwand inklusiver stundenlanger Fehlversuche. Eine nicht allzu altes Plattenimage bietet Systemsicherheit auch in aussichtlosen Situationen und verkürzt Reparaturen auf eine einzige zuverlässige Aktion.

Systemumzug: Wenn der Platz des Systemdatenträgers nicht mehr ausreicht, kann das komplette bisherige System auf einen größeren Datenträger geschrieben werden.

Systemexperimente: Betriebssystembastler und Sicherheitsexperten benötigen oft einen genau definierten Systemzustand etwa vor einer Treiber- oder Softwareinstallation oder vor einer experimentellen (Un-)Sicherheitsaktion.

Imagesicherung versus Klonen

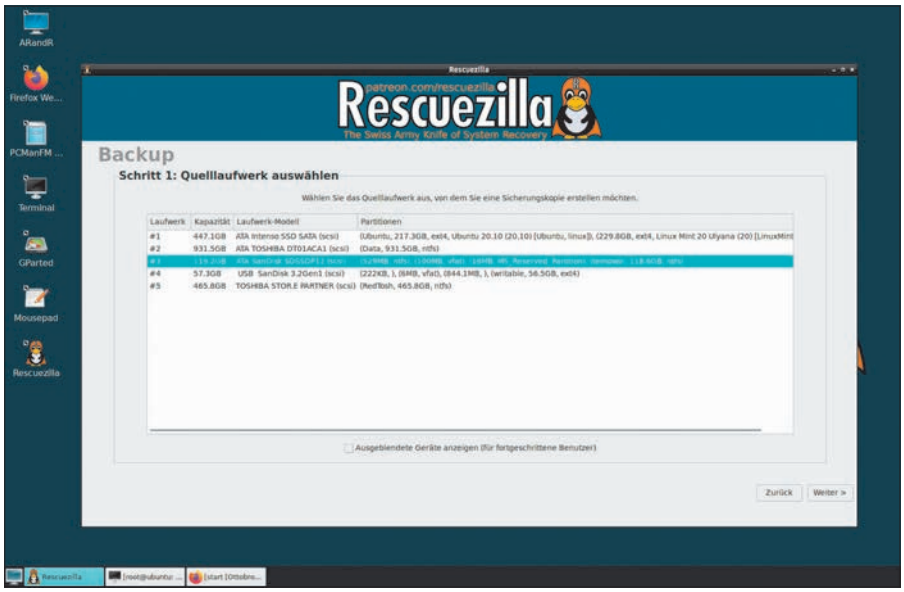
Sichern und Klonen sind zwei technisch klar unterschiedene Aktionen, wenngleich zweiteres im Prinzip nur eine Abkürzung bedeutet:

Imagesicherungen erstellen große komprimierte Dateien wahlweise eines kom-

pletten Laufwerks oder eines Laufwerks mit mehreren Partitionen oder nur einer bestimmten Partition eines Laufwerks. Sie können diese Dateien später zurückschreiben, um eine Systemhavarie zu beheben oder um das System auf einen früheren und besseren Zustand zurückzusetzen. Da die Imagedateien groß sind, sollten sie auf schnellen externen Laufwerken oder im Gigabit-Netz gespeichert werden. Images sind eine präventive Sicherheitsmaßnahme für den Fall einer späteren Hardware- oder Systemhavarie. Trotz der unvermeidlichen Größe arbeiten Clonezilla und Rescuezilla platzsparend, indem sie freien Platz von Datenträgern nicht sektorweise mitsichern: Eine zur Hälfte belegte 240-GB-SSD wird also nur 120 GB Sicherungsplatz erfordern, und nicht einmal dies, weil zusätzlich gzip-Komprimierung zum Einsatz kommt.

Klonen bedeutet eine exakte Datenkopie eines Laufwerks direkt auf ein zweites Laufwerk. Daher wird man Klonen nicht primär als Sicherheitsmaßnahme einsetzen, da es stets einen zweiten – identischen oder größeren – Datenträger erfordert, der dann eventuell über Monate unbenutzt bleibt. Klonen ist vielmehr die einschlägige Maßnahme, um den bisherigen Datenträger durch einen neuen (meist größeren) zu ersetzen. Direktes Klonen funktioniert nur mit Clonezilla. Wer mit Rescuezilla klonen will, benötigt zwei Schritte – erst das „Backup" des Datenträgers als Image und danach dessen „Wiederherstellung" auf den anderen Datenträger.

Benutzerdateien und Vorbereitungen: Für die Sicherung von Benutzerdaten brauchen Sie kein externes Livesystem – dafür gibt es einfachere Methoden im jeweiligen Betriebssystem. Einschlägig sind Rsync und Tar unter Linux, Robocopy oder Xcopy unter Windows (sowie diverse grafische Front-Ends oder Alternativen). Angesichts dieser Tatsache wäre es für schnelle Imagesicherungen optimal, Benutzerdateien weitgehend fernzuhalten. Bei unseren Imageaktionen hielt eine kleine SSD mit einem relativ frischen System und ohne nennenswerte Benutzerdaten den Rekord: Es war in drei Minuten auf USB gesichert und später in vier Minuten wiederhergestellt. Für ein Notebooksystem mit etwa 50 GB Benutzerdateien fiel bereits die zehnfache Sicherungs- und Wiederherstellungsdauer an. Da es bei der Imagesicherung um Boot- und Systemsicherheit geht, wäre eine strikte Trennung der Benutzerdaten optimal – etwa in einer expliziten Home-Partition, die nicht mitgesichert wird. Das wird sich nicht überall ideal realisieren lassen, aber wer notgedrungen ganze Film- und Musikarchive in die Imagesicherungen einbezieht, muss Geduld mitbringen.



Rescuezilla bei der Auswahl des Quelle: Für ein Low-Level-Werkzeug bietet das Livesystem maximalen Komfort. Über Quelle und Ziel muss dennoch zweifelsfreie Klarheit bestehen.

Rescuezilla kann nur Samba/Windows-Freigaben, das dürfte aber den meisten Nutzern völlig ausreichen. Häufigstes Sicherungsziel sind vermutlich USB-Laufwerke.

Der Umfang einer Sicherung lässt sich aber in jedem Fall reduzieren. Unter Linux entfernen Sie unnötige Programmpakete und räumen den Paketcache auf:

```
sudo apt autoremove
sudo apt autoclean
```

Ein Tool wie Bleachbit kann weitere überflüssige Datenlasten entsorgen.

Unter Windows verwenden Sie die Datenträgerbereinigung mit der Option „Systemdateien bereinigen", um temporäre Dateien, Updatesicherungen oder gar den eventuell noch vorhandenen Ordner „Windows.old" zu löschen (mit Vorversion). Beachten Sie unbedingt, Windows vor einer Imagesicherung über „Neu starten" zu beenden, denn nach normalem „Herunterfahren" erhalten Clonezilla oder Rescuezilla keinen Schreibzugriff.

Das einfache Rescuezilla

Rescuezilla ist der Nachfolger des eingestellten Redo Backup. Der circa 850 MB umfassende Download des ISO-Abbilds von *https://rescuezilla.com/* kann mit den üblichen Mitteln (dd, Gnome-Disks, Etcher, Win 32 Disk Imager) bootfähig auf USB-Stick kopiert werden. Es handelt sich um ein komplettes Ubuntu-Livesystem, das eine Basisausstattung einschlägiger Werkzeuge mitbringt, wie Browser, Gparted, Gnome-

Hübsche Rescuezilla-Funktion, aber kaum praxistauglich: Der „Image Explorer" will den Zugang auf die Dateiebene in den Sicherungsimages ermöglichen, ist aber zu langsam.

Rescuezilla und die Partitionswahl: Im Zweifel sichert man besser sämtliche Partitionen des Laufwerks. In Clonezilla heißt dieselbe Entscheidung „savedisk" (alles) oder „saveparts".

Disks. Nach „apt update" ist auch das Nachinstallieren zusätzlicher Programme möglich, allerdings nur temporär während der Laufzeit.

Im Zentrum steht das Tool Rescuezilla, das gemeinsam mit dem Desktop automatisch startet und die Imagesicherung und Wiederherstellung mit wenigen Schaltflächen einfach macht. Im Prinzip gibt es nur „Backup" und „Wiederherstellung", die wir nachfolgend genauer beschreiben.

Exkurs zur dritten Option: Eine dritte Schaltfläche „Image Explorer" ist neu und noch als „Beta" charakterisiert. Ihre Funktion ist es, den Inhalt vorhandener Sicherungsabbilder in den Dateimanager zu mounten. Dies wäre eine signifikante Funktionserweiterung, weil sich dann gezielt einzelne Dateiobjekte aus einer Sicherung holen ließen, ohne das gesamte Image zurückschreiben zu müssen. Da Rescuezilla (und Clonezilla) die Abbilder aber gzip-komprimieren, ist die Wartezeit für die Dekomprimierung größerer Images aktuell kaum zumutbar. In unserem Test benötigte das Mounten einer kleinen SSD-Sicherung (60 GB) etwa zehn Minuten, das Anzeigen des Inhalts im Dateimanager unter „/mnt/rescuezilla.image.explorer" sogar nochmal deutlich länger. Auch das anschließende Navigieren im Dateisystem des Abbilds ist unzumutbar zäh. Rescuezilla warnt daher bei dieser Funktion mit gutem Grund vor erheblichen Wartezeiten und kündigt für künftige Versionen ein anderes Kompressionsformat an, das schnellere Ergebnisse verspricht. Derzeit lohnt sich der „Image Explorer" allenfalls dann, wenn Sie ganz genau wissen, welche Einzeldateien Sie aus dem Image zurücksichern müssen.

Das Backup: Im automatisch gestarteten Haupttool „Rescuezilla" lädt die Schaltfläche „Backup" den Assistenten zum Schreiben eines neuen Abbilds:

„Schritt 1" ist die Auswahl des physikalischen Quell-Datenträgers, dessen Partitionen gesichert werden sollen. „Schritt 2" ermöglicht erlaubt die Auswahl der gewünschten Partitionen auf diesem Datenträger. Wenn Sie nicht genau wissen, dass eine bestimmte Partition keine Sicherung braucht, dann übernehmen Sie hier alle angezeigten Partitionen, wie es der Standard vorgibt. Andernfalls besteht die Gefahr, dass Sie eine wichtige Bootpartition unterschlagen und damit später ein nicht bootfähiges System zurückschreiben. In „Schritt 3" markieren Sie das Backupziel. Dabei zeigt die Standardoption „Direkt an meinen Computer angeschlossen" die internen Laufwerke sowie USB-Medien. Falls das Image auf einer Samba-Freigabe landen soll, aktivieren Sie oben die Option „Über das Netzwerk verbunden". In diesem Fall geben Sie den „Server oder Freigabeort" in dieser Form (also ohne Protokollangabe „smb" oder ähnlich)

```
//[IP]/[Zielverzeichnis]
```

ein, also etwa „//192.168.178.20/Data/". Falls Zugangsdaten erforderlich sind, lassen sich diese in den weiteren Zeilen ergänzen (Samba-Kontoname, Samba-Kennwort).

„Schritt 4" sollten Sie bei der Vorgabe belassen. Es handelt sich um das Mountverzeichnis im Livesystem, wohin das eigentliche Backupziel gemountet wird. In „Schritt 5" sollten Sie eventuell tätig werden, weil ein aussagekräftiger Sicherungsname die spätere Orientierung erleichtert. „Schritt 6" zeigt eine Übersicht für die Aktion und nach „Weiter" erfolgt in „Schritt 7" die eigentliche Aktion.

Die Wiederherstellung: Die Schaltfläche „Wiederherstellen" startet den Assistenten, der mit „Schritt 1" zunächst das Laufwerk abfragt, wo sich die Sicherung befindet. Wird das Laufwerk korrekt gewählt, zeigt „Schritt 2" die vorhandene(n) Imagesicherung(en). Mit der passsenden Auswahl und „Weiter" geht es in „Schritt 3" zum Zieldatenträger. Hier dürfen keine Zweifel bestehen, weil dieses Laufwerk komplett überschrieben wird. Die Angaben sind mit Größe, Hersteller und Partitionsangaben aber vorbildlich präzise. Mit „Schritt 4" folgt noch die Partitionsauswahl, wobei Sie wieder – wie beim Backup empfohlen – alle Partitionen übernehmen. Nach „Schritt 5" mit Zusammenfassung und „Weiter" startet die Wiederherstellung des Datenträgers.

Das mächtige Clonezilla

Anders als Rescuezilla hat das Livesystem Clonezilla keinen Desktop oder weitere Programme, sondern fokussiert sich ausschließlich auf seinen Spezialjob. Der Hersteller bietet im Downloadbereich von *https://clonezilla.org/downloads.php* mehrere Varianten.

Wir empfehlen die oberste Option „alternative stable", die auf Ubuntu basiert (aktuell „groovy", also Ubuntu 20.10). Ohne Desktop und sonstige Tools wiegt das Livesys-

tem nur etwa 350 MB und kann mit den üblichen Mitteln (dd, Gnome-Disks, Etcher, Win 32 Diskimager) bootfähig auf USB-Stick kopiert werden.

Im textbasierten Menü navigieren Sie mit Cursor- und Tabulatortasten und bestätigen „OK“ mit der Eingabetaste. Im allerersten Startschirm wählen Sie die erste Option „Clonezilla live“. Wenn Sie im Folgefenster „de-DE.UTF“ wählen, ist das Menü samt Erklärungen weitestgehend in deutscher Sprache. Im Folgefenster sollten Sie außerdem das Tastaturlayout auf „German“ setzen. Weitere Abfragen zur Tastatur beantworten Sie mit den Standardvorgaben. Danach laden Sie im Fenster „Starte Clonezilla“ das eigentliche Tool.

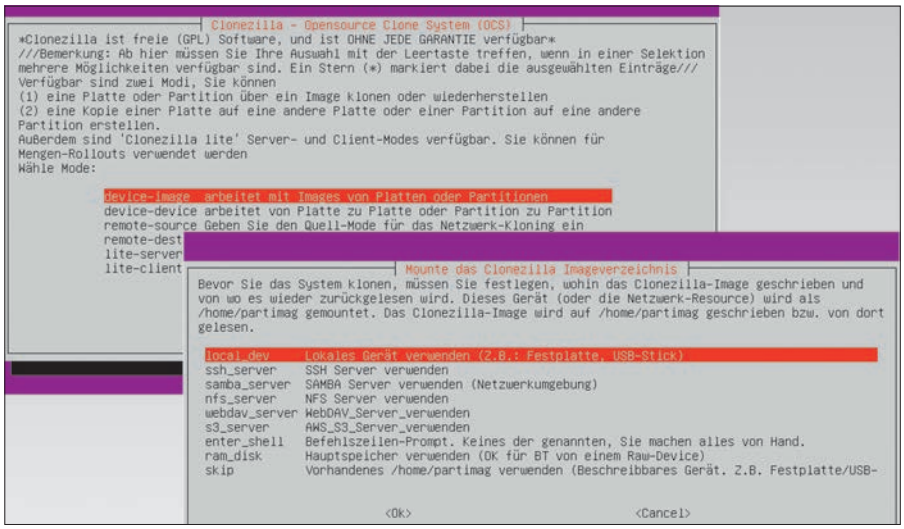
Das Backup: Wählen Sie im ersten Dialog die oberste Option „device-image“ und danach „local_dev“. Sie haben jetzt Gelegenheit, ein USB-Laufwerk anzuschließen. Drücken Sie die Eingabetaste. Clonezilla zeigt Ihnen die verfügbaren Laufwerke an. Warten Sie, bis das USB-Laufwerk erscheint, und drücken Sie dann die Tastenkombination Strg-C. Wählen Sie das Ziellaufwerk aus und danach ein Verzeichnis, in dem Clonezilla das Backup speichern soll. Gehen Sie mit den Pfeiltasten auf „Done“ und drücken Sie zweimal die Eingabetaste.

Wenn Sie ein Image im Netzwerk sichern wollen, wählen Sie statt „local_dev“ das gewünschte Netzwerkprotokoll – also „samba_server“ für Windows/Samba-Freigaben oder „ssh_server“ für eine Sicherung via SSH. Danach geben Sie die IP-Adresse des Servers an und die zugehörigen Anmeldedaten mit Kontonamen und Passwort. Im Anschluss fahren Sie fort, wie bei einem lokalen Ziel beschrieben.

Verwenden Sie den Modus „Beginner Einsteiger“ und dann die Option „savedisk“, sofern Sie ein Abbild der gesamten Festplatte erstellen möchten. Dies ist im Zweifel immer zu empfehlen, weil Clonezilla dann alle Partitionen inklusive Bootmanager sichert. Dabei spielt es keine Rolle, ob Windows, Linux oder beide Systeme installiert sind. Die weitere Option „saveparts“ sichert nur einzelne ausgewählte Partitionen.

Vergeben Sie einen aussagekräftigen Namen für das Image. Anschließend wählen Sie die Festplatte oder Partition aus, die Sie sichern möchten. Bei den folgenden Dialogen übernehmen Sie die Voreinstellungen.

Die Wiederherstellung: Starten Sie Clonezilla mit den Optionen „device_image“ und



Clonezilla: Die Menüs sind anspruchsvoll, aber ganz gut erklärt. Typischerweise arbeiten Sie mit Images (Bild oben) und mit lokalen Datenträgern (Bild unten).

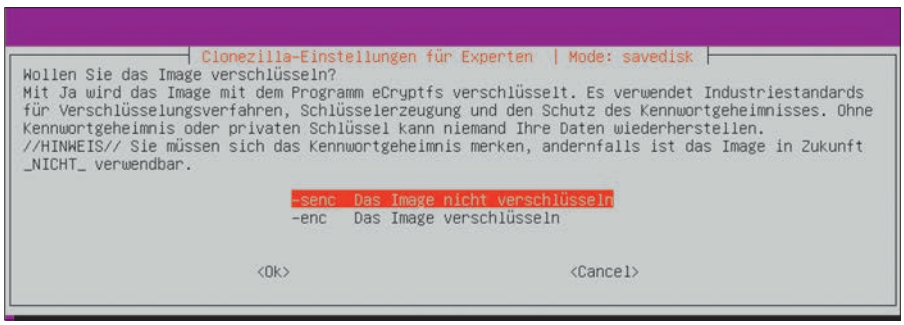
„local_dev“ (bei lokaler Sicherung). Wählen Sie die Partition und das Verzeichnis aus, in dem ein zuvor gesichertes Image liegt. Gehen Sie auf „Beginner“ und dann auf „restoredisk“. Wenn Sie vorher einzelne Partitionen gesichert haben, verwenden Sie „restoreparts“. Clonezilla findet auf dem Backupmedium alle Abbilder automatisch und präsentiert sie in einer Liste. Danach wählen Sie die Zielpartition aus, in die das Image zurückgeschrieben werden soll. Nach zwei Sicherheitsabfragen spielt Clonezilla das Backup zurück.

Eine Wiederherstellung aus dem Netzwerk läuft entsprechend ab. Hier wählen Sie aber statt „local_dev“ das passende Netzwerkprotokoll – also etwa „samba_server“– und geben danach die Anmeldedaten an.

Direktes Klonen: Beim Klonen spielt es keine Rolle, ob es sich bei Quelle und Ziel um Festplatten oder SSDs handelt. Wichtig sind nur die Datenträgergrößen. Wir gehen hier vom häufigen und einfacheren Fall aus, dass das neue Zielmedium gleich groß oder größer ist als das bisherige Laufwerk. In diesen Fällen benötigt Clonezilla keine Vorbereitung und nur geringe Nachbesserung:

Sie wählen zunächst „device-device“, dann „Beginner“ und anschließend „disk_to_local_disk“. Geben Sie zunächst den Datenträger an, den Sie kopieren wollen, im nächsten Schritt das neue Ziellaufwerk. Die folgenden beiden Dialoge bestätigen Sie mit Eingabetaste, um die Voreinstellungen zu übernehmen. Folgen Sie den weiteren Anweisungen des Assistenten. Prüfen Sie die Einstellungen und bestätigen Sie mit „y“, wenn Sie dazu aufgefordert werden.

Wenn der neue Datenträger mehr Kapazität besitzt als der ursprüngliche, dann bleibt nach der Clonezilla-Aktion, welche exakt die ursprünglichen Größen wiederherstellt, nach der letzten Partition ungenutzer Plattenplatz. Dies korrigieren Sie in einem beliebigen Linux-System mit Gparted, indem Sie die letzte Partition auf dem neuen Laufwerk maximal vergrößern. ■

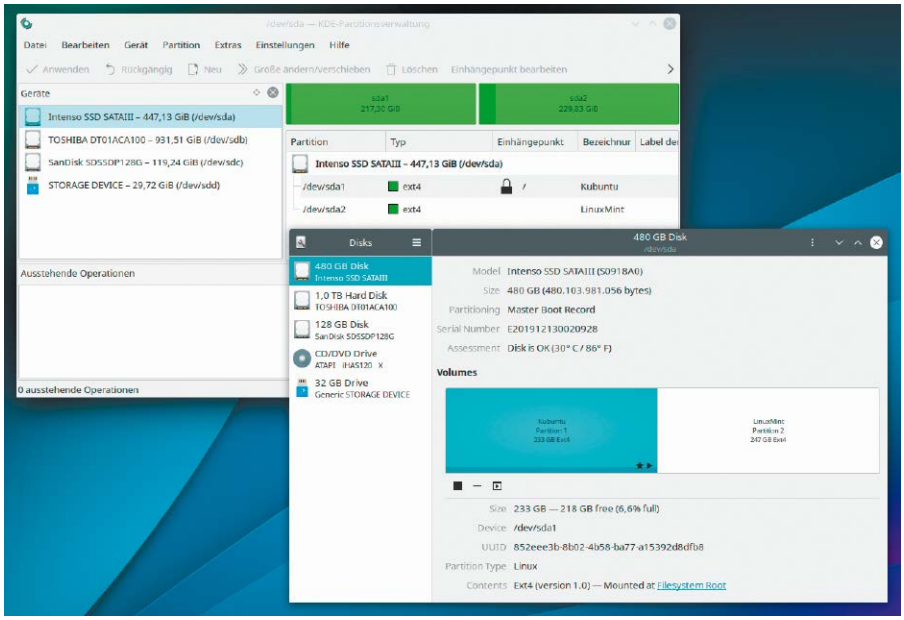


Clonezilla-Spezialitäten: Die Motive für das kompliziertere Clonezilla liegen nicht nur bei den Netzwerkfähigkeiten. Clonezilla kann verschlüsseln und direkt klonen.

Grafische Laufwerkstools

KDE- und Gnome-affine Desktops haben grafische Dienstprogramme an Bord mit weit größerem Aktionsradius als eine pure Partitionsverwaltung. Sie machen zahlreiche Terminaltools ebenso entbehrlich wie den Klassiker Gparted.

VON HERMANN APFELBÖCK



Im Umfeld von Linux-Ratgebern ist es Tradition, die Systemwartung mit Terminalkommandos zu erledigen. Das hat natürlich gute Gründe, erstens weil diese Methode distributions- und desktopunabhängig ist, zweitens weil sie auch per SSH-Fernwartung funktioniert, drittens weil die Terminaltools meistens die eigentlichen Dienstleister sind, welche grafische Programme nur entsprechend der Nutzerangaben füttern. Ganz irreführend wäre es aber, so zu tun, als sei der Weg ins Terminal alternativlos. Bei der Laufwerksverwaltung gibt es mit dem KDE-Partitionmanager („KDE-Partitionsverwaltung“) und mit Gnome-Disks („Laufwerke“) umfassende Werkzeuge für den grafischen Desktop.

Dieser Beitrag verzichtet aus Platzgründen auf etliche Unterfunktionen (Leistungstests, Dateisystemchecks, Schreddern, Verschieben von Partitionen), erklärt aber die wesentlichen Funktionen.

1. Die Gnome- und KDE-Tools: Ein Überblick

Alle Speichergeräte – Festplatte, SSD, DVD, USB, SD-Karte – werden in der linken Spalte unter „Geräte“ (KDE) beziehungsweise „Laufwerke“ (Gnome) aufgelistet. Beim markierten Gerät, das durch Größenangabe und Herstellerbezeichnung gut zu identifizieren ist, erhalten Sie alle Infos über Partitionen, Dateisystem, Partitionskennung (etwa „/dev/sda1“), Bezeichnung (Label), Gesamtkapazität, Füllzustand (bei KDE grafisch und in Zahlen, beim Gnome-Tool als Prozentangabe), Mountpunkt (falls eingehängt), aktuelle Temperatur, ferner auch die UUID-Kennung. Letztere zeigt Gnome-Disks standardmäßig, das KDE-Tool nach Rechtsklick auf die Partition im Unterdialog „Eigenschaften“.

Der KDE-Partitionmanager ist das funktional umfassendere Werkzeug. Er bietet eine klare Menüführung und bequeme, objektbezogene Kontextmenüs per Rechtsklick. Das KDE-Tool ist obendrein optisch schicker und erlaubt über „Einstellungen → KDE-Partitionsverwaltung einrichten“ angepasste Farben für Dateisysteme und eine individuell eingestellte Werkzeugleiste. Mehr noch: Auch die Infospalten in der Partitionsanzeige lassen sich einstellen und etwa durch die oft wichtige Info der „UUID“-Kennung ergänzen. Dies ist jedoch erst in der aktuellsten Version zuverlässig (21.08.3). Das Tool der Ubuntu-Langzeitversion 20.04 steht noch bei Version 4.1.0 und dort ist der Weg zum Unterdialog „Eigenschaften“ erforderlich. Auch andere Optionen arbeiten erst in jüngster Version zuverlässig: So ist es uns nicht gelungen, unter Kubuntu 20.04 und Partitionmanager 4.1.0 einen SMART-Status eingebauter Laufwerke zu erfragen. Erst im demnächst anstehenden Kubuntu 22.04 LTS wird das aktuelle Tool an Bord sein.

Der Partitionmanager fordert immer sudo-Recht, auch wenn man nur eine Info abholen will. Auch sonst orientiert sich der Partitionmanager an Gparted, das alle angeforderten Aktionen in einer To-do-Liste sammelt und erst nach „Bearbeiten → An-

wenden“ abarbeitet. Nach Aktionen werden alle Laufwerke stets komplett neu eingelesen. Neu angeschlossene Datenträger werden erst nach „Gerät → Geräte aktualisieren“ (oder Hotkey F5) erkannt.

Gnome-Disks ist das einfachere und eindeutig schnellere Werkzeug. Das beginnt mit dem einfachen Start ohne sudo-Recht, das erst bei tatsächlichen Systemeingriffen verlangt wird. Fachterminologie und Dateisystemkenntnisse werden nur in spezielleren Unterdialogen vorausgesetzt, um Desktopbenutzern die Bedienung zu vereinfachen. Das Mounten („Einhängen“) erledigt Gnome-Disks pragmatisch wie ein Linux-Dateimanager, indem es einfach den Standardpfad „/media“ annimmt. Der Partitionmanager will hier grundsätzlich einen statischen Mountpunkt in der „/etc/fstab“ („Einhängepunkt bearbeiten“), bevor er die Option „Einhängen“ anbietet. Natürlich kann auch Gnome-Disks statische Mountpunkte in der „fstab“ anlegen (Punkt 7), bietet aber auch einfaches Ad-hoc-Mounten.

Will man dem Gnome-Tool überhaupt Mängel vorwerfen, dann ist es eine etwas konfuse Oberfläche ohne Kontextmenüs, die immer wieder mal ein Suchspiel nach dem passenden Klick-Control erfordert. Dass Gnome-Disks eine LVM-Partitionierung zwar erkennt, aber nicht aktiv eingreifen kann, werden nur Profis vermissen (siehe Punkt 12).

2. Laufwerkstools: Unabhängig vom Desktop

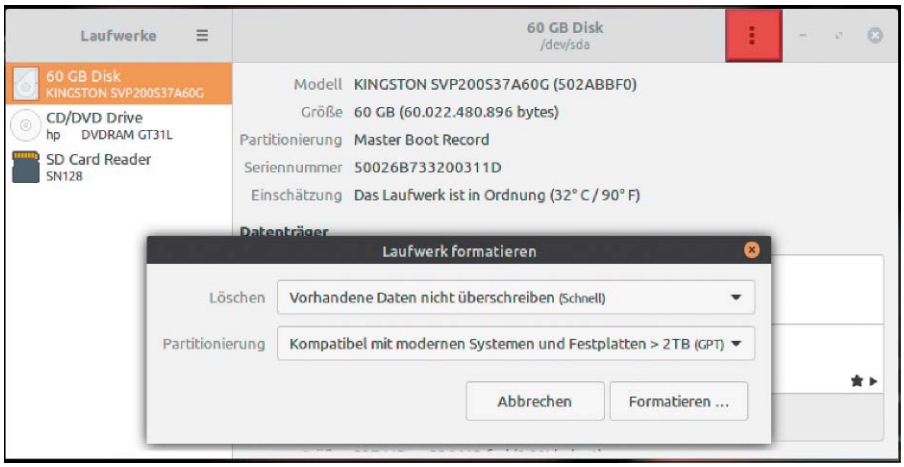
Für Linux-Nutzer, die nicht je nach Desktop ein unterschiedliches Laufwerkstool nutzen möchten, sind die beiden Programme auch für nicht-native Desktops installierbar. Der KDE-Partitionmanager lässt sich auch unter Oberflächen wie Gnome, XFCE oder Cinnamon installieren:

```
sudo apt install partitionmanager
```

Dabei zieht das Tool allerdings ein Menge KDE-Pakete mit. Umgekehrt ist die Installation des Gnome-Programms unter KDE mit

```
sudo apt install gnome-disk-utility
```

eine vergleichsweise leichtgewichtige Aktion. Solche Nachinstallation ist nicht nur unter KDE sinnvoll, denn Gnome-Disks ist auch auf Gnome-affinen Desktops nicht überall vorinstalliert. Wer das Systemtool etwa unter XFCE vermisst, kann es mit dem genannten Befehl nachinstallieren. Achten Sie auf den Paketnamen „gnome-disk-utility“ (nicht: „gnome-disks“).



Tabula rasa mit Partitionstabelle: Das – hier rot hervorgehobene – Drei-Punkt-Menü von Gnome-Disks enthält Überraschungen. „Laufwerk formatieren“ schreibt eine neue Partitionstabelle.

3. Partitionstabellen schreiben (MBR und GPT)

Grundlegendste Aktion bei der Festplattenverwaltung ist das Anlegen der Partitionstabelle. Der Partitionsstil (MBR oder GPT) spielt vor allem auf Systemdatenträgern eine Rolle, falls dort mehrere Systeme parallel installiert werden sollen. Der Stil der Partitionstabelle ist somit ein Thema der Installation und für alltägliches Formatieren von Datenpartitionen und externen USB-Laufwerken kaum relevant. Allerdings kann der alte MBR-Partitionsstil (Master Boot Record, auch „msdos“-Partitionstabelle) nur Partitionen bis maximal 2,2 TB verwalten. Für Laufwerke von vier bis 16 TB ist daher der GPT-Partitionsstil erforderlich, sofern solche Laufwerke ungeteilt als Ganzes genutzt werden sollen. Bei kleineren USB-Festplatten oder USB-Sticks können Sie den Partitionsstil ignorieren.

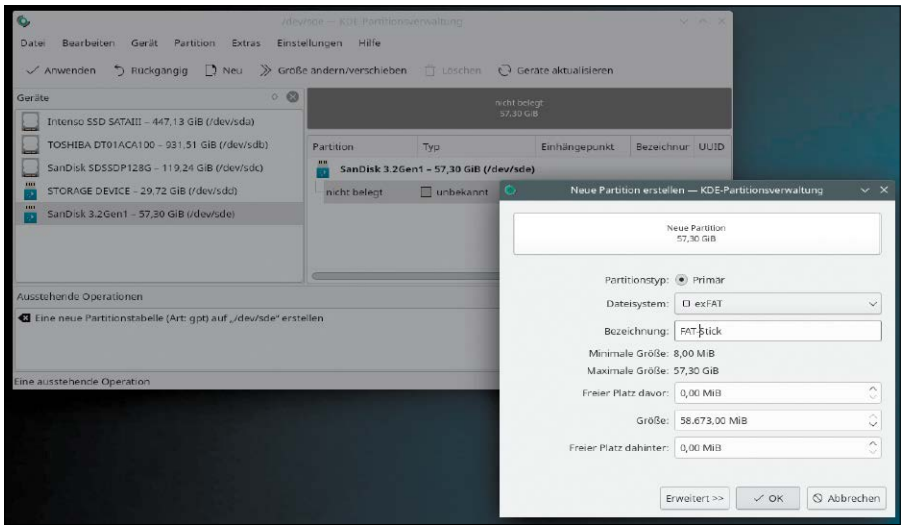
Gnome-Disks und der Partitionmanager können den Partitionsstil einer Festplatte festlegen. Die Umstellung des Partitionsstils geht immer mit komplettem Datenverlust einher.

LAUFWERKSTOOLS STATT TERMINAL

Wer den Informations- und Funktionsumfang von Gnome-Disks und KDE-Partitionmanager im Griff hat, kann auf eine ganze Truppe komplexer Terminaltools verzichten. Nicht für jeden Sonderfall, aber doch für 90 Prozent aller Alltagsaufgaben, ersetzen die grafischen Werkzeuge folgende Tools:

fdisk/gdisk	Partitionierung mit komplexen Parametern
mkfs	Formatierung für diverse Dateisysteme mit jeweils gesonderten Parametern
dd	Imagekopien mit zahlreichen Parametern
lsblk	Partitionsinfos mit 50 Parametern
blkid	Partitionsinfos mit 20 Parametern
mount	Partitionen einhängen mit 40 Parametern
df	Datenträgerbelegung
hddtemp	Temperaturinfo
hdparm	Bereitschaftsmodus für Festplatten mit 80 Schaltern und Optionen
smartctl	SMART-Abfragen mit 30 Parametern
lvm	Logical Volume Manager mit 50 Unterbefehlen und je weiteren Parametern

Nicht zuletzt ersparen Gnome-Disks und KDE-Partitionmanager das manuelle Bearbeiten der Laufwerkstabelle „/etc/fstab“.



Handwerk im KDE-Partitionmanager: Laufwerke einteilen und neue Dateisysteme schreiben ist hier wie im Gnome-Tool vorbildlich einfach.

Gnome-Disks will vereinfachen. Den Begriff „Partitionstabelle" sucht man hier vergeblich. Das kleine Drei-Punkt-Menü über dem Partitionsbereich zeigt aber den obersten Eintrag „Laufwerk formatieren" und hier die Auswahl „Kompatibel mit allen Systemen…(MBR / DOS)" und „Kompatibel mit modernen Systemen…(GPT)". Diese Aktion schreibt die Partitionstabelle, formatiert aber keineswegs mit einem Dateisystem. Es entsteht vorerst nur freier Speicherplatz ohne Partitionierung, ohne Dateisystem. Der aktuelle Partitionsstil eines Laufwerks ist im Partitionsfenster als „Master Boot Record" oder „GUID Partition Table" zu erkennen.

Im KDE-Partitionmanager gibt es dafür den Menüpunkt „Gerät → Neue Partitionstabelle", dessen Unterdialog die Optionen „GPT" und „MS-DOS" anbietet. Nach Auswahl und „Neue Partitionstabelle erstellen" muss die Aktion wie immer mit „Anwenden" ausgelöst werden. Der Vorgang ist sofort erledigt, weil der Partitionmanager nur die winzige Partitionstabelle schreibt. Der aktuelle Partitionsstil eines Laufwerks ist über „Gerät → Eigenschaften" als „gpt" oder „msdos" abzufragen.

4. Partitionen löschen, anlegen, aufteilen

Es gibt mindestens drei Gründe, Datenträger neu zu partitionieren: Der bisherige Inhalt soll gelöscht werden, das bisherige Dateisystem soll durch ein anderes ersetzt werden, die bisherige Partitionsaufteilung (eventuell noch keine) soll neu organisiert werden. Bei diesem Kerngeschäft zeigt sich Gnome-Disks nonchalanter als das KDE-Pendant. Kompliziert ist der Vorgang aber bei keinem der Programme, jedoch muss jedem Nutzer klar sein, dass Neupartitionierung mit Dateiverlust einhergeht und folglich die genaue Kontrolle des richtigen Laufwerks unter „Laufwerke" beziehungsweise „Geräte" vorausgehen muss.

Bei Gnome-Disks markieren Sie im Partitionsfenster per Mausklick die gewünschte Partition. Mit dem kleinen Minus-Symbol unter dem Partitionsschema löschen Sie die Partition, die sich umgehend als „Freier Platz" präsentiert. Bei einer geleerten Partition verschwindet automatisch das Minus-Symbol und mit dem jetzt angebotenen Plus-Symbol legen Sie die neue Partition an. Dabei folgen drei Entscheidungen:

1. Sie können die Größe der neuen Partition definieren, falls Sie den freien Platz nicht insgesamt nutzen, sondern aufteilen wollen. Dies lässt sich mit Schieberegler oder manueller Eingabe realisieren.

2. Nur beim MBR-Partitionsstil erscheint der zusätzliche Punkt „Erweiterte Partition". Sinnvoll wäre dies nur, wenn die maximal vier Partitionen des MBR-Stils nicht ausreichen.

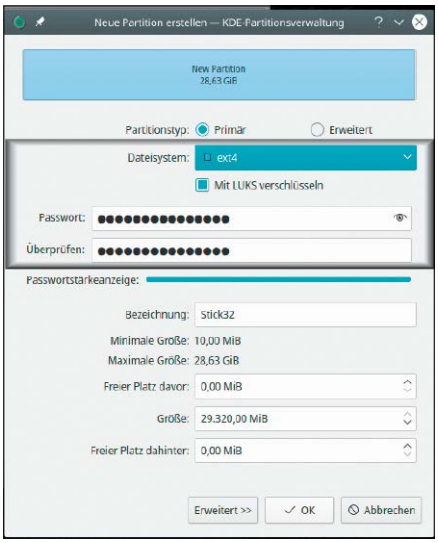
3. Im Folgedialog vergeben Sie optional ein beschreibendes Datenträger-Label, vor allem aber das Dateisystem. Hier ist Gnome-Disks anwenderfreundlich, indem es – knapp, aber gut erklärt – nur die verbreiteten Standards Ext4, NTFS und FAT anbietet und speziellere Dateisysteme in einen Unterdialog „Andere" verbannt. Was unter „Andere" angeboten wird, lässt sich durch Nachinstallationen erweitern (etwa „f2fs-tools", „exfat-utils").

Der KDE-Partitionmanager verlangt vor jeder Partitionsänderung das „Aushängen" der jeweiligen Partition. Technisch ist das korrekt, weil jede Partitionsbearbeitung vorheriges Aushängen voraussetzt (das Gnome-Tool erledigt dies automatisch). Erst danach werden im Menü „Partition" oder im Kontextmenü des Partitionsfensters die übrigen Befehle aktiviert. „Löschen" entfernt eine Partition, was die Partitionsdarstellung mit „nicht belegt" quittiert. Folgerichtig ist danach der Menüpunkt „Neu" aktiv, womit Sie eine Partition neu anlegen. Im Unterfenster „Neue Partition erstellen" sind alle Entscheidungen übersichtlich angeboten:

1. Oben erscheint der freie Speicherplatz als „Neue Partition". Diese Balkenrepräsentation funktioniert wie ein Schieberegler, um bei Bedarf den Datenträger aufzuteilen, benötigt aber sehr präzises Navigieren zum Partitionsende rechts. Nach unserer Erfahrung ist die Einteilung über die Felder „Größe" und „Freier Platz dahinter" einfacher.

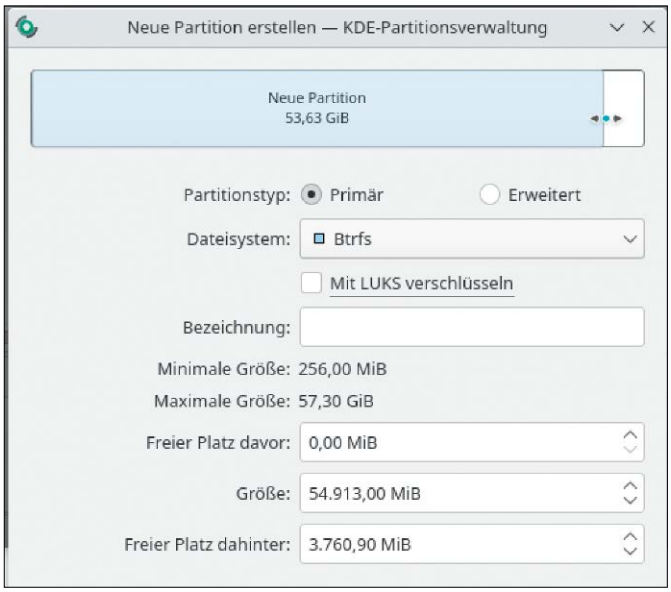
2. Nur beim MBR-Partitionsstil erscheint neben „Partitionstyp: Primär" der zusätzliche Punkt „Erweitert". Sinnvoll ist die Option nur dort, wo die maximal vier Partitionen des MBR-Stils nicht ausreichen.

3. Das Datenträger-Label vergeben Sie optional im Feld „Bezeichnung" und für das gewünschte Dateisystem gibt es eine



USB-Stick mit Luks verschlüsseln: Der KDE-Partitionmanager (im Bild) wie auch Gnome-Disks bieten Datenträgerverschlüsselung für externe Laufwerke.

gleichnamige Drop-down-Liste: So hübsch diese ist – das KDE-Tool setzt voraus, dass Sie mit Bezeichnungen wie „Btrfs“, „NTFS“, ext4“ etwas anfangen können. Einfachste Leitlinie ist, dass Linux-Systemdatenträger vorzugweise mit Ext4, mobile Laufwerke mit Benutzerdaten am einfachsten mit NTFS oder exFAT formatiert werden sollten.
Tipp für beide Tools: Wenn Sie einen Datenträger mit mehreren Partitionen komplett leeren wollen, ist es am einfachsten, die Partitionstabelle neu zu schreiben (siehe Punkt 3). In einigen Fällen mit Livesystemen in der primären Partition ist dies sogar notwendig, weil sich die Partitionen einzeln nicht löschen lassen.



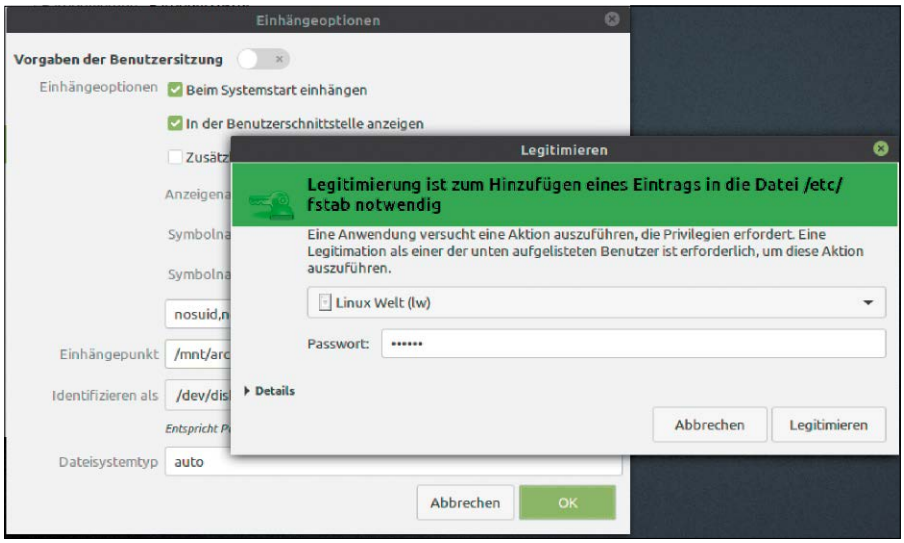
Größenänderung von Partitionen: Das KDE-Werkzeug ist in diesem Punkt Gnome-Disks überlegen.

5. Luks-verschlüsselte Datenträger

Punkt 5 ist nur eine Fußnote zum vorherigen Punkt, aber man kann diese wichtige Option leicht übersehen – vor allem in Gnome-Disks. Jede neue Partition lässt sich optional Luks-verschlüsseln und mit Passwort schützen. Das gilt auch für externe USB-Datenträger. Beachten Sie aber, dass Luks nicht bestehende Partitionen „on the fly“ verschlüsselt: Der Datenträger wird für die Verschlüsselung neu formatiert und dabei gelöscht.
In Gnome-Disks löschen Sie mit dem Minus-Symbol die bisherige Partition und legen mit dem Plus-Symbol eine neue an. Bei der Auswahl des Dateisystems gehen Sie zur Unterseite „Andere“. Im Folgedialog belassen Sie die Voreinstellung „XFS“ und aktivieren ganz unten die unscheinbare Option „Passwortgeschützter Datenträger (LUKS)“. Nach Klick auf „Weiter“ müssen Sie noch ein Kennwort eingeben und bestätigen.
Im KDE-Partitionmanager löschen Sie die bisherige Partition. Im Dialog „Neu“ muss neben „Dateisystem“ ein Linux-Dateisystem wie Ext4 oder XFS eingetragen sein, damit darunter die Option „Mit LUKS verschlüsseln“ erscheint. Wird diese aktiviert, erscheint die Kennwortabfrage. Der Vorgang wird mit „Bearbeiten → Anwenden“ abgeschlossen.

6. Partitionsgrößen ändern

Laufwerkstools beherrschen verlustfreie Größenänderungen von Partitionen. Allerdings sind nicht alle Aktionen ohne Datenverlust möglich, wie nachfolgend angesprochen. Typisches Motiv für Größenänderungen ist die Notwendigkeit, freien Speicherplatz für eine neue Partition zu schaffen, um dort ein weiteres System zu installieren. Dass dies vorbereitend mit Systemtools wie Gnome-Disks geschieht, ist aber eher die Ausnahme: Viele Linux-Installer beherrschen das im Zuge einer Multiboot-Installation eigenständig und haben dabei den Vorteil des externen Zugriffs. Wenn nämlich die Systempartition verkleinert und „ausgehängt“ werden muss, ist das im laufenden System ausgeschlossen.
Andere Motive für Größenänderungen sind eher selten, aber denkbar, so etwa der Wunsch nach einer verschlüsselten Partition auf einem USB-Laufwerk. Beachten Sie, dass beide Tools Größenänderungen auf Linux-Dateisystemen sowie auf NTFS und FAT beherrschen, aber nicht auf jedem Dateisystem-Exoten (etwa exFAT).
A. Im typischen und einfachsten Fall soll die Kapazität einer Partition verringert werden und auf dem frei werdenden Platz eine zweite entstehen:
In Gnome-Disk markieren Sie im Partitionsfenster die bestehende Partition und klicken darunter auf das kleine Zahnradsymbol (neuere Versionen verwenden ein Symbol, das eher einen Medienplayer assoziiert). Der Option „Größe ändern“ startet einen Dialog mit Schieberegler und einem Eingabefeld mit exakter MB/GB-Angabe. Nach der Verkleinerung mit der Schaltfläche „Größe verändern“ erhalten Sie eine



Gnome-Disks macht einen Eintrag in die Datei „/etc/fstab“: Diese Aktion muss mit einem Konto erledigt werden, das sich als Systemverwalter ausweisen kann.

zweite Partition als „Freier Platz“, wo Sie ein neues Dateisystem anlegen (siehe Punkt 4).

Beim KDE-Partitionmanager müssen Sie die Partition erst aushängen, erst dann wird die Option „Partition → Größe ändern/verschieben“ aktiv. Mit sehr exakter Mausnavigation am rechten Rand des Partitionsbalkens lässt sich dieser nach links ziehen und somit die Größe verringern. Einfacher ist es, im Eingabefeld „Freier Platz dahinter“ die gewünschte Größe der zweiten Partition anzugeben. Im dadurch geschaffenen Platz („nicht belegt“) erstellen Sie dann die neue Partition gemäß Punkt 4. Wie immer in diesem Tool ist die Arbeit erst nach „Bearbeiten → Anwenden“ tatsächlich getan.

B. Komplizierter sind Szenarien mit zwei bestehenden Partitionen (oder mehr), wo die Kapazität einer Partition zugunsten der anderen verringert werden soll. Wir beschränken uns auf ein Beispiel, wo die erste Partition vergrößert werden soll:

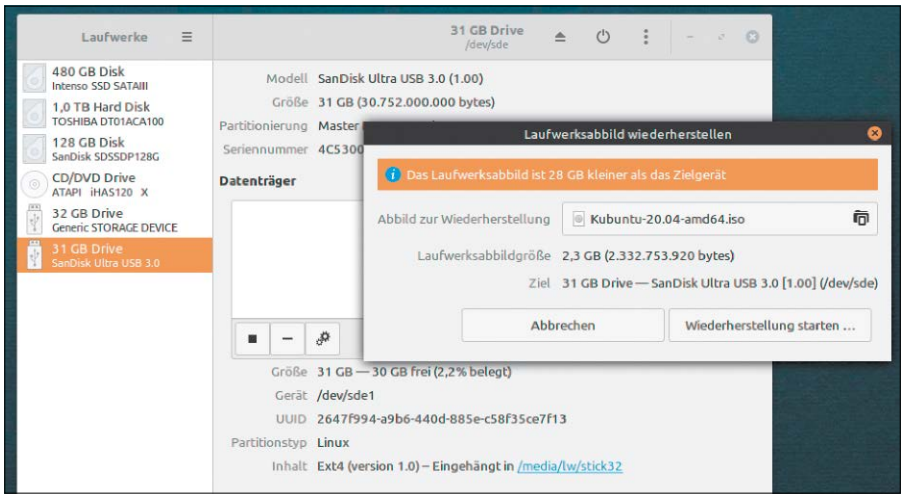
In Gnome-Disks ist das nach unserer Kenntnis ohne Datenverlust auf der zweiten Partition nicht zu realisieren. Sie können also die zweite Partition löschen, danach die erste vergrößern und auf dem restlichen Platz eine neue Partition schaffen.

Der KDE-Partitionmanager ist hier mächtiger: Sie verkleinern zunächst mit „Partition → Größe ändern/verschieben“ die zweite Partition, indem Sie den Partitionsbalken von links ziehen oder das Feld „Freier Platz davor“ verwenden. Dadurch entsteht zwischen den Partitionen ein „nicht belegter“ Bereich, den Sie dann durch eine zweite Größenänderung der ersten Partition zuschlagen. Dies arbeitet ohne Datenverlust, ist aber eventuell zeitaufwendig.

7. Datenträger standardmäßig mounten

Die einzige Partition, die bei jedem Systemstart eingebunden wird, ist die Systempartition. Dies wird bei Installation durch einen Eintrag in der Datei „/etc/fstab“ festgelegt. Insbesondere auf Servern, aber auch auf Desktop-PCs können weitere statische Mountaktionen sinnvoll bis notwendig werden. Die Laufwerkstools ersparen manuelles Hantieren in der „fstab“ mit UUID-Kennungen, Dateisystemen und Mountpunkten.

In Gnome-Disks markieren Sie die gewünschte Partition und klicken auf das Zahnradsymbol (oder Playersymbol). Hier erscheint der Punkt „Einhängeoptionen bearbeiten“, wo Sie die „Vorgaben der Benutzersitzung“ abschalten, die Option „Beim Systemstart einhängen“ sowie den nachfolgenden Punkt („Benutzerschnittstelle“) aktivieren. Im unteren Bereich des Dialogs geben Sie den Einhängepunkt an. Den nach wie vor notwendigen Eintrag in die Datei „/etc/fstab“ erledigt Gnome-Disks, nachdem Sie per Kennwort sudo-Recht nachweisen.



Bootfähige Kopie eines ISO-Abbilds auf USB-Stick: Gnome-Disks erledigt diesen Alltagsjob genau wie der KDE-Partitionmanager. Tools wie dd sind dafür nicht notwendig.

Im KDE-Partitionmanager verwenden Sie „Partition → Einhängepunkt bearbeiten“. Der Dialog zeigt mehr und brauchbar erklärte Optionen für die „Options“-Spalte in der „fstab“. Die Auswahl „Geräteknoten“ („/dev/…“), „UUID“ und „Bezeichnung“ (nur angeboten, falls ein Label vergeben) ist übersichtlicher als bei Gnome-Disks, außerdem gibt es hier eine Klicknavigation in das gewünschte Mountverzeichnis. Im Prinzip ersparen aber beide Tools die lästige Recherche nach UUID oder Devicekennung und vereinfachen den Eintrag in die „fstab“ erheblich.

8. Aussagekräftige Mountpunkte (Label)

Eine Kleinigkeit, die zu einer besseren Laufwerksübersicht beiträgt, ist die Datenträgerbezeichnung („Label“). Wenn automatisch eingehängte Partitionen (vor allem USB-Geräte) über ihre UUID identifiziert werden, entstehen Mountverzeichnisse wie „DEA5-B112“, die dem Systemnutzer keine Orientierung bieten. Ein sprechendes Laufwerkslabel macht die Identifizierung einfach.

In Gnome-Disks müssen Sie nur den betreffenden Datenträger markieren, auf das Zahnradsymbol (Playersymbol) klicken und hier die etwas irreführende Option „Dateisystem bearbeiten“ wählen. Dann geben Sie einen sprechenden Namen ein, klicken auf „Ändern“ und hängen den Datenträger danach wieder ein (erstes Symbol). Das Mountverzeichnis – standardmäßig unter „/media“ – erhält nun den Namen gemäß der vergebenen Bezeichnung.

Im KDE-Partitionmanager ist diese Funktion in das Untermenü „Partition → Eigenschaften“ ausgelagert. Hier gibt es das Feld „Bezeichnung“. Auch diese Kleinigkeit muss wie immer mit „Bearbeiten → Anwenden“ bestätigt werden.

9. Partitionsabbilder schreiben

ISO- oder IMG-Dateien auf USB-Sticks zu schreiben oder Partitionen als IMG-Datei zu sichern, erfordert kein dd, Etcher oder gar Clonezilla. Auch dafür sind die Standardtools gerüstet.

In Gnome-Disks zeigt im kleinen Drei-Punkt-Menü die Optionen „Laufwerksabbild erzeugen“ und „Laufwerksabbild wiederherstellen“. Die erste Aktion sichert den Inhalt des ausgewählten Laufwerks (oder SD-Karte) in eine Imagedatei („.IMG“). Weit häufiger werden Sie die zweite Aktion benötigen, um ISO- oder IMG-Dateien bootfähig auf UBS-Stick zu kopieren. Achten Sie darauf, dass in der Laufwerksliste der richtige Zieldatenträger markiert ist, wählen Sie „Laufwerksabbild wiederherstellen“ und navigieren Sie dann zur gewünschten ISO- oder IMG-Datei.

Im KDE-Partitionmanager verwenden Sie die Menüs „Partition → Sichern“ zum Schreiben von Imagesicherungen und „Partition

→ Wiederherstellen“ zum Kopieren von ISO- und IMG-Dateien auf die ausgewählte Partition. Hier gelten beim „Wiederherstellen“ dieselben Vorsichtsregeln wie bei Gnome-Disks.

10. SMART-Status abfragen

Moderne Festplatten folgen dem SMART-Standard (Self Monitoring, Analysis and Reporting Technology), der Auskunft über den aktuellen Zustand gibt. Gnome-Disks und der KDE-Partitionmanager können die SMART-Werte abgreifen und anzeigen.

Gnome-Disks bietet iwm Drei-Punkt-Menü die Option „SMART-Werte und Selbsttests“. Diese bietet ausführliche Auskunft zum markierten Laufwerk inklusive Temperaturangabe. Wichtigste Aussage oberhalb der Einzelwerte ist das Resümee „Das Laufwerk ist in Ordnung“. Das Gnome-Tool kann aber nur interne SATA-Laufwerke überprüfen, USB-Geräte derzeit nicht.

Der KDE-Partitionmanager äußert sich unter „Gerät → SMART-Status“ etwas knapper, jedoch sollte die Angaben „SMART-Status: Gut“ und „Gesamtbewertung: Gesund“, ferner die Angabe fehlerhafter Sektoren und die Temperaturmessung ausreichen. Anders als Gnome-Disks berücksichtigt das KDE-Tool auch per USB angeschlossene Festplatten.

11. Datenträger im Bereitschaftsmodus

Festplatten lassen sich bei längerer Nichtbenutzung in den Ruhemodus schicken. In den allgemeinen Systemeinstellungen werden Sie diese Option vermissen und auch der KDE-Partitionmanager muss hier passen: Dies ist der einzige Punkt, wo sich Gnome-Disks überlegen zeigt.

Gnome-Disks kann steuern, wann sich eine Festplatte abschalten soll. Wählen Sie das gewünschte Laufwerk und gehen Sie im Drei-Punkt-Menü auf „Laufwerkseinstellungen“. Unter „Bereitschaft“ setzen Sie den Schalter auf „An“ und stellen die Zeit ein, nach der die Festplatte sich abschalten soll. Die Zeitspanne reicht von „Niemals“ bis „3 Stunden“. Das funktioniert auch mit externen USB-Festplatten, nicht mit Sticks.

12. Laufwerke zusammenlegen (LVM)

LVM (Logical Volume Manager) ist eine Verwaltungsschicht für die Datenträgerorganisation. Die Technik erlaubt das Anlegen von

Das kann nur das Gnome-Tool: Unter den „Laufwerkseinstellungen“ lässt sich einstellen, dass nicht genutzte Laufwerke in den Ökomodus („Bereitschaft“) wechseln.

„Volume Groups“, die mehrere physische Datenträger zu einem logischen Laufwerk zusammenfassen. Ein angelegter Verbund ist erweiterbar, enthaltene Datenträger können wieder entnommen oder durch andere ersetzt werden. Voraussetzung für LVM ist das Paket „lvm2“, das sich mit

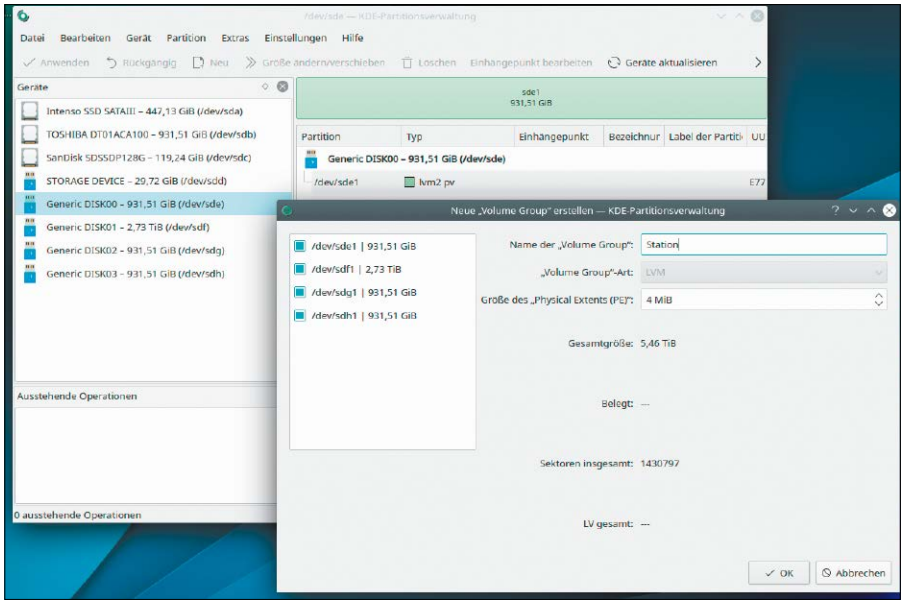
```
sudo apt install lvm2
```

nachrüsten lässt. Falls bei einer Linux-Installation LVM (oder Luks-Verschlüsselung) genutzt wurde, ist die Komponente bereits vorhanden.

Gnome-Disks erkennt LVM-Volumes, kann diese allerdings weder anlegen noch verändern.

Der KDE-Partitionmanager zeigt beim Erstellen einer neuen Partition das zusätzliche Format „lvm2 pv“. Datenträger, die Bestandteil einer LVM-Gruppe werden sollen, müssen mit diesem speziellen Dateisystem formatiert werden. Dies bedeutet natürlich vollständigen Datenverlust. Sind die gewünschten Laufwerke LVM2-formatiert, können Sie das Menü „Extras → Neue Volume Group“ nutzen. Dabei werden nun alle LVM2-formatieren Datenträger angeboten. Aktivieren Sie per Klickbox alle Laufwerke, die Sie zusammenlegen wollen. Vergeben Sie noch einen Namen für die Gruppe und bestätigen Sie mit „OK“. Wie immer muss die ausstehende Operation danach mit „Bearbeiten → Anwenden“ ausgelöst werden.

Danach erscheint in der Geräteliste das neue Gruppenvolume, das die Gesamtkapazität aller zusammengelegten Datenträger anbietet. Das virtuelle Volume benötigt nun noch eine reguläre Endformatierung und kann dann genutzt werden. Später ist es jederzeit möglich, ein Laufwerk aus der Gruppe wieder zu entnehmen oder ein weiteres hinzuzufügen. Die passende Option im KDE-Partitionmanager ist „Gerät → „Volume Group“-Größe ändern“. Dann erhalten Sie wieder die Liste der enthaltenen Laufwerke und können Geräte deaktivieren oder neue hinzufügen. Für ein Hinzufügen weiterer Datenträger muss das Laufwerk LVM2-formatiert sein, andernfalls taucht es in dieser Liste nicht auf. ■



LVM beherrscht nur der KDE-Partitionmanager: Hier entsteht aus vier kleineren Festplatten eine Volume Group mit etwa 5,5 TB, die später als ein einziges Laufwerk erscheint.

Laufwerke im Terminal

Wie formatiere ich einen USB-Stick, der an einen SSH-administrierten Platinenserver angeschlossen ist? Hinlaufen, das Laufwerk abziehen, an einem Desktoprechner formatieren und wieder an der Platine anschließen? Klar, das geht, muss aber nicht sein.

VON HERMANN APFELBÖCK

Am Desktop werden Linux-Nutzer für Datenträgeraufgaben die grafischen Werkzeuge Gnome-Disks und KDE-Partitionmanager bevorzugen. Wer deren Funktionsumfang im Griff hat, kann in der Tat auf eine ganze Truppe von Terminaltools verzichten. Ergänzend zu diesem Artikel verweisen wir daher auf den Beitrag im PDF „LinuxWelt Digital XXL 6/23“ auf Heft-DVD unter „Grundlagen → Grafische Laufwerktools“. Ganz hilflos sollte man aber nicht dastehen, wenn das Gnome- oder KDE-Tool nicht erreichbar ist: Auf einem Raspberry, der ohne Desktop läuft, ist das gelebter Standard, und auch auf einem Desktopsystem, das gerade repariert werden muss, gelegentlich Realität. Partitionieren, Formatieren, Analysieren von Datenträgern ist im Terminal etwas mühsamer, aber keine Wissenschaft. Dieser Artikel zeigt die wenigen wirklich wichtigen Werkzeuge, die 95 Prozent des Alltags abdecken.

Laufwerksüberblick mit Lsblk

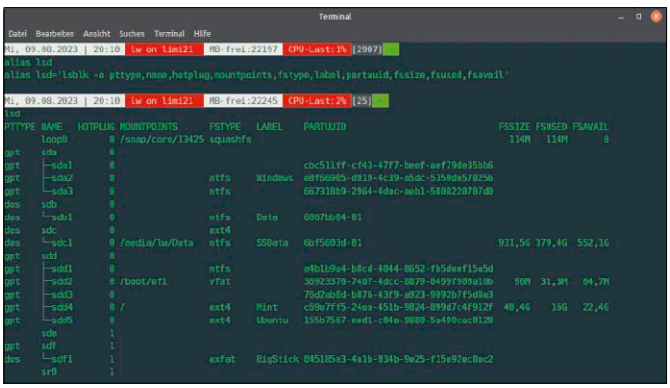
Präzise Informationen über die angeschlossenen Laufwerke sind unentbehrlich. Sie dienen nicht nur der Übersicht über Kapazität und Belegung, sondern schützen davor, potenziell destruktive Aktionen wie Partitionieren, Formatieren oder Schreiben von Laufwerkabbildern auf den falschen Datenträgern auszulösen. Die wichtigsten und sehr ähnlichen Infotools sind Lsblk und blkid. Wer grundsätzlich Lsblk benutzt, kann wenig falsch machen (Blkid aktualisiert allerdings die Laufwerkskennungen permanent und zuverlässiger):

```
lsblk -f
```

Der Schalter „-f“ ist ein Sammelschalter, der die Felder „name“, „fstype“, „fsver“, „label“, „uuid“, „fsavail“, „fsuse“, „mountpoints“ und damit alle Infos liefert, die man für eine eindeutige Zuordnung braucht. Wer will, kann sich auch eine eigene Felderkombination mit Schalter „-o“ zurechtlegen:

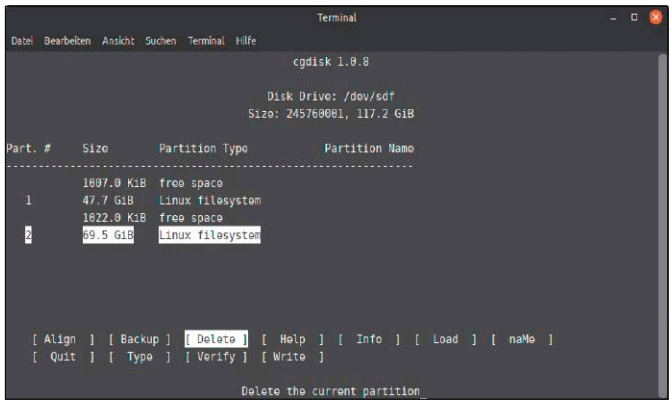
```
lsblk -o name,path,label,fstype,
  fssize,fsavail,mountpoints,
  hotplug,uuid,pttype
```

Der „path“ ist der Gerätename, den Tools



Hier ist Einiges los, aber Lsblk hat den Durchblick: Die Laufwerksinfos lassen sich nach Wunsch filtern.

wie Mkfs (Formatieren), Fdisk/Gdisk (Partitionieren) oder Hdparm (Hardwareinfo) als Angabe benötigen. Die Gesamtkapazität (Fssize) ist meistens aussagekräftiger als die freie (Fsavail) oder genutzte (Fsuse) Kapazität. Die UUID ist in jedem Fall unentbehrlich, um beim manuellen Mounteintrag in der „/etc/fstab" die eindeutige Laufwerkskennung angeben zu können. Das Feld „pttype" zeigt für jeden Datenträger, ob er das MBR/DOS- oder das GPT-Partitionsschema benutzt.



Cfdisk und Cgdisk (im Bild) sind reduziert, aber komfortabel: Das Löschen und Neuanlegen von Partitionen funktioniert menügeführt und entsprechend einfach.

Partitionieren im Terminal

Partitionieren, also das Anlegen der Partitionstabelle und das optionale Aufteilen von Datenträgern, wird in den meisten Fällen dem Installer der Linux-Distributionen überlassen. Was dann an Partitionierung und Formatierung von externen USB-Datenträgern anfällt, erledigt man in der Regel mit Gnome-Disks & Co. Trotzdem sind Grundkenntnisse der wichtigsten Terminalwerkzeuge nützlich, um im Falle des Falles nicht auf ein externes Livesystem angewiesen zu sein.

Terminalpartitionierer sind eine Zeitreise in die finsteren 90er-Jahre der PC-Nutzung. Hinzu kommt die Frage, welches der zahlreichen Werkzeuge Parted, Fdisk, Cfdisk, Sfdisk, Gdisk, Cgdisk, Sgdisk das geeignete ist? Wir sortieren aus:

Parted ist eignet sich nur für Hartgesottene und solche, die das Tool seit Jahren kennen.

Sfdisk und **Sgdisk** leisten dasselbe wie Fdisk und Gdisk, können aber komplett mit Eingabeparametern gefüttert werden und sind damit Script-fähig und automatisierbar. Für gelegentliche Partitionsaufgaben sind diese Fähigkeiten aber nicht erforderlich.

Fdisk und **Gdisk** sind trotz archaischer Bedienung die einschlägigen Terminalwerkzeuge, sofern die nachfolgend empfohlenen Ncurses-Varianten (Cfdisk, Cgdisk) nicht ausreichen. Nach etwa

```
sudo fdisk /dev/sde
```

fragen Sie mit „m" (Fdisk) oder „?" (Gdisk) die verfügbaren Optionen ab. Die Bedienung erfolgt über definierte Tasten wie „d", um eine Partition zu löschen, oder „n", um eine Partition neu anzulegen. „p" zeigt die aktuelle Partitionsaufteilung. Erst mit dem Befehl „w" schreiben die Tools die Änderungen tatsächlich auf die Festplatte. Mit „q" beenden Sie die Programme.

Cfdisk und **Cgdisk** sind reduzierte Versionen von Fdisk und Gdisk. Der Umfang ist zwar eingeschränkt, die Bedienung andererseits deutlich bequemer: Es handelt sich um Ncurses-Navigationsfenster, welche die wichtigsten Aktionen menüähnlich anbieten und die Steuerung mit Cursor-, Tab- und Eingabetaste ermöglichen. Wo das Angebot von Cfdisk und Cgdisk ausreicht (Partitionen löschen, neu anlegen), sind diese Tools komfortabler als Fdisk und Gdisk. Cfdisk bietet auch die Möglichkeit, eine Partition zu vergrößern, nachdem durch Löschen der nachfolgenden Platz geschaffen wurde.

Der Aufruf muss immer mit root-Recht und dem Gerätename erfolgen (Beispiel):

```
sudo cgdisk /dev/sde
```

Ohne „sudo" starten diese nicht (wie alle Partitionierungstools) und ohne Gerätenamen wählt Cfdisk automatisch „/dev/sda", während Cgdisk nach dem gewünschten Laufwerk fragt. Generell gilt bei Cfdisk und Cgdisk: Solange Sie nicht den Menüpunkt „Schreiben" beziehungsweise „Write" verwenden, bleibt der Datenträger unverändert. Dies muss auch noch ausdrücklich mit „yes" bestätigt werden. „Ende" oder „Quit" beendet die Tools.

Empfehlung: Für alle grundlegenden Aufgaben sind Cfdisk/Cgdisk ausreichend. Cfdisk ist die beste Wahl, weil es auch Partitionen verkleinern („Größe verändern") und vergrößern kann (sofern nachfolgend ein „Freier Bereich" geschaffen wurde). Für Cfdisk spricht außerdem, dass es nicht nur das alte MBR- („dos"-)Partitionsschema beherrscht, sondern in aktuellen Versionen auch GPT. Cgdisk hingegen beherrscht nur GPT-Partitionierung und bringt auch eine entsprechende Warnmeldung, sofern Sie damit einen MBR/DOS-Datenträger bearbeiten wollen. Die Abfrage, ob ein Datenträger eine MBR- oder GPT-Partitionstabelle besitzt, erledigen Sie am besten mit Lsblk und den oben genannten Felderkombination (inklusive „pttype"). Oder Sie verwenden grundsätzlich Cfdisk.

Tipp 1: Laufwerke, die man mit Partitionstools bearbeiten will, müssen vorher aus dem Dateisystem ausgehängt werden (Beispiel):

```
umount /dev/sde?
```

Wird dies vergessen, zeigen die meisten Tools keine Fehlermeldungen, können aber die Partitionsarbeit nicht erfolgreich durchführen.

Tipp 2: Partitionieren oder Ändern von Partitionsgrößen ist nicht notwendig destruktiv, sofern keine nachfolgende Formatierung folgt. Sich darauf zu verlassen, wäre aber ein heikles Experiment. Wir empfehlen Partitionierung ausschließlich auf Datenträgern, deren Daten Sie nicht mehr benötigen.

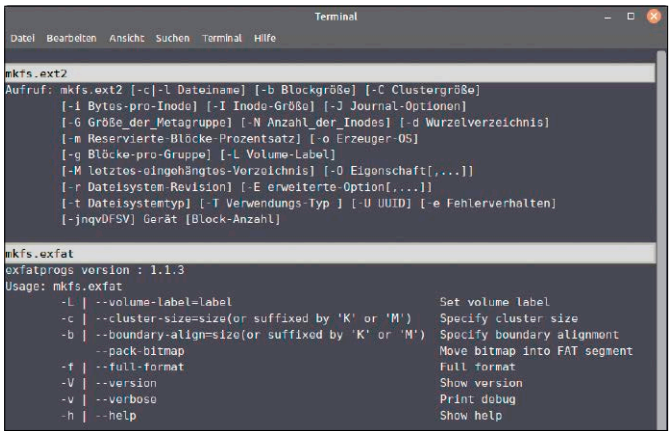
Tipp 3: Das Partitionieren teilt nur den Datenträger auf, schreibt aber keine Dateisysteme. Dies muss nachfolgend mit Mkfs geschehen (siehe unten „Formatieren").

Tipp 4: Bei textbasierten Tools kommt es auf jeden Buchstaben und jede Ziffer an. Ein Gerätepfad „/dev/sdd" ist statt „/dev/sde" schnell falsch eingegeben. Kontrollieren Sie immer zweimal, welches Laufwerk Sie gerade bearbeiten.

Formatieren: Dateisystem anlegen

Durch Partitionierung angelegte Festplattenbereiche können erst dann genutzt werden und Daten aufnehmen, wenn ein Dateisystem angelegt ist. Der Vorgang des Formatierens ist im Linux-Terminal relativ einfach mit Mkfs zu erledigen. Dabei gibt es zwei Syntaxvarianten, die dasselbe Ergebnis erzielen:

```
sudo mkfs.ext4 -L "Stick256"
  /dev/sde1
sudo mkfs -t ext4 -L "Stick256"
  /dev/sde1
```



Formatieren mit Linux- und Microsoft-Dateisystemen ist nicht kompliziert. Allerdings hat jedes Dateisystem-Modul seinen eigenen Umfang und seine eigenen Parameter.

Das gewünschte Dateisystem wird also direkt als Befehlsergänzung oder mit Schalter „-t“ (Type) angegeben. Je nach Dateisystem unterstützt das Kommando dann diverse Optionen (siehe etwa *mkfs.ntfs* oder *mkfs.vfat* ohne Parameter), die bei jedem Dateisystem etwas anders ausfallen. Schalter „-L“ (Label) ermöglicht bei den meisten Dateisystemen eine Partitionsbezeichnung. Bei NTFS empfiehlt sich immer Schalter „--quick“, der den Vorgang fundamental beschleunigt:

```
sudo mkfs.ntfs -L "Stick256"
  --quick /dev/sde1
```

Alle weiteren Optionen gehen bereits Richtung Expertenwissen. So kann etwa bei manchen reinen Datenfestplatten mit durchwegs sehr großen Dateien eine große Clustergröße jenseits des Standards erwünscht sein. Dafür ist in der Regel Schalter „-C“ oder „-c“ mit nachfolgender Größenangabe zuständig:

```
sudo mkfs.exfat -L "Stick256" -c 4M
  /dev/sde1
```

Hier würde eine Clustereinheit satte vier MB umfassen.

Tipp: Für den unkomplizierten Umgang mit externen USB-Laufwerken sollten Sie diese mit den Microsoft-Dateisystemen FAT32, NTFS oder ExFAT formatieren. Dort erhalten Systemverwalter wie Standardbenutzer Schreibzugriff, sofern das Einbinden per Automount oder mit dem richtigem Mountbefehl erfolgt (siehe unten). Auf Linux-Dateisystemen wie Ext4 oder BTRFS gibt es standardmäßig zunächst nur Lesezugriff.

Mount: Datenträger einhängen

Während man sich beim Partitionieren und Formatieren notfalls irgendwie grafisch behelfen kann (auf anderem Rechner oder mit einem Livesystem), sind Terminalkenntnisse beim Mounten kaum verzichtbar. Das gilt vor allem für permanente Laufwerke, die in die Datei „/etc/fstab“ eingetragen werden müssen, gelegentlich aber auch für USB-Laufwerke, die man an bestimmter Stelle im Dateisystem sehen möchte. Das Einhängen oder Mounten von Datenträgern erfordert root-Recht (oder sudo) und gehorcht im Prinzip folgender Syntax:

```
sudo mount -o [Optionen] [Gerät]
  [Mountordner]
```

Die Argumente für Gerät und Mountordner sind einfach: Der Mountordner muss nur existieren und kann an beliebiger Stelle im Dateisystem liegen – unter „/media“, unter „/mnt“, ebenso unter „/srv“ oder „/home“. Ob für das Erstellen des Ordners Benutzerrechte genügen oder sudo-Recht notwendig ist, spielt keine Rolle. Das Gerät kann auf unterschiedliche Weise angegeben werden, etwa als Gerätepfad „/dev/sd[xy]“ oder mit seiner UUID-Kennung („UUID=[...]“). Einschlägige Werkzeuge, den Gerätepfad oder die UUID („PARTUUID“) zu ermitteln, sind wie immer Lsblk oder Blkid.

Die nach Schalter „-o“ möglichen Optionen des Mountbefehls sind ein Handbuch für sich. Dabei geht es um die Benutzerrechte auf dem Datenträger, um das Recht, diesen einhängen und aushängen zu dürfen, um Dateiprotokolle und Authentifizierung für Netzressourcen. Für lokale Laufwerke ist folgende Syntax ausreichend und zu empfehlen:

```
sudo mount -o defaults /dev/sdc1 /
  mnt/stick256
```

Gerätepfad und Mountpunkt sind Beispiele, die entsprechend korrigiert werden müssen. Wenn es sich um Linux-Dateisysteme handelt, müssen Schreibrechte für Benutzerkonten in jedem Fall manuell mit Chmod explizit erlaubt werden. Bei allen Microsoft-Dateisystemen (NTFS, FAT, exFAT) kann man sich den Vorgang vereinfachen:

```
sudo mount -o uid=$UID,gid=$UID,
  defaults /dev/sdc1 /mnt/stick256
```

Die Mountoptionen „uid=$UID,gid=$UID“ stellen sicher, dass der aktuelle Benutzer, der diesen Befehl ausführt, auf dem Laufwerk sofort lesen und schreiben darf. Die Variable „$UID“ liefert dessen User-ID. Der Benutzer muss sudo-berechtigt sein – etwa als Hauptbenutzer des Systems.

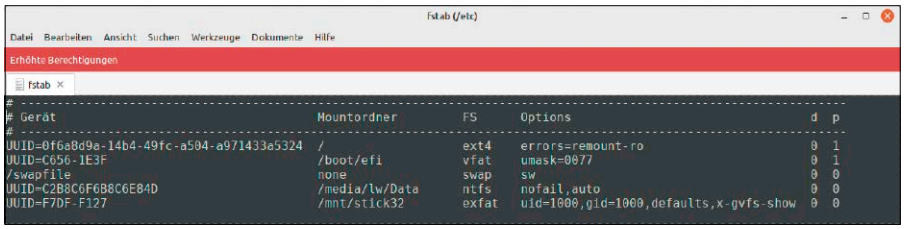
Manuelles Mounten eignet sich nur bei gelegentlich angeschlossenen externen Laufwerken. Einträge in der Datei „/etc/fstab“ sorgen für automatisches Einhängen lokaler Datenträger. Diese Einträge bestehen aus der UUID des Laufwerks (zu empfehlen, aber auch Gerätepfade wie „/dev/sd[xy]“ sind möglich), dem Mountpunkt, dem Dateisystem und den Mountoptionen. Die weiteren Felder „dump“ und „pass“ dürfen bei Datenpartitionen immer „0 0“ lauten. Über die UUID und das Dateisystem informiert wieder Lsblk, den Mountpunkt bestimmen Sie selbst und als Optionen halten Sie sich an die obigen Empfehlungen für den Mountbefehl. Nach

```
sudo nano /etc/fstab
```

tragen Sie als weitere, letzte Zeile etwa Folgendes ein:

```
UUID=E5FE-5015 /mnt/stick32 ntfs
  uid=1000,gid=1000,defaults 0 0
```

Das sind im Prinzip die gleichen Angaben wie beim manuellen Mounten, nur mit dem Unterschied, dass Fstab keine Variablen auflösen kann und daher UID (User-ID) und



Automatisches Mounten über die Datei „/etc/fstab“ folgt weitgehend den Pflichtargumenten und Optionen, wie sie auch der interaktive Mountbefehl verwendet.

GID (Gruppen-ID) als statische Zahl benötigt. Diese lautet für den Hauptbenutzer „1000“, kann aber mit

```
id $USER
```

ermittelt werden, falls sie abweicht.

Die Mounteinträge der Datei „/etc/fstab“ lassen sich mit

```
sudo mount –a
```

jederzeit interaktiv testen. Damit dies aussagekräftig ist, sollten Sie neu eingetragene Laufwerke vorher mit (Beispiel)

```
sudo umount /dev/sde?
```

aushängen. Funktioniert das Mounten mit *sudo mount -a*, wird das Laufwerk künftig beim Systemstart immer automatisch in das gewünschte Verzeichnis geladen.

Mount: Optionen & Tipps

Die zahlreichen, kombinierbaren Optionen für das Mounten im Terminal oder via Fstab sind hier nicht systematisch darstellbar. Wir ergänzen nur einige populäre Optionen:

Tipp 1: Der mount-Befehl lässt sich nicht nur für Partitionen auf Festplatten nutzen. Sie können auch einzelne Dateien mit unterstützten Dateisystemen einhängen. Typisches Beispiel dafür sind ISO-Abbilder, die sich mit

```
sudo mount -o loop Datei.iso
 /mnt/iso
```

mounten lassen. Das ISO-Dateisystem ist nur lesbar.

Tipp 2: Der Befehl Umount zum Aushängen von Geräten ist unkompliziert und akzeptiert jede eindeutige Angabe:

```
sudo umount /dev/sde1
sudo umount UUID=FF57-F124
sudo umount /mnt/stick32
```

Das Ergebnis ist identisch, wenn eine Partition „/dev/sde1“ unter „/mnt/stick32“ eingehängt ist und die UUID „FF57-F124“ besitzt.

Tipp 3: Wenn ein eingehängtes Laufwerk als Gerät in der Dateimanager-Navigation erscheinen soll, muss in der Datei „/etc/fstab“ die Option „x-gvfs-show“ angefügt werden (Beispiel):

```
UUID=E5FE-5015 /mnt/stick32 ntfs
 uid=1000,gid=1000,defaults,
 x-gvfs-show 0 0
```

Tipp 4: Bestimmte Mountoptionen können die Zugriffshäufigkeit reduzieren. Dies fällt bei reinen Datenhalden kaum ins Gewicht, kann aber Systemdatenträger entlasten:

```
UUID=[ID] / ext4
 defaults,noatime,nodiratime 0 0
```

Mit den Optionen „noatime“ und „nodiratime“ verzichtet das System darauf, die Zugriffszeiten für Dateien und Ordner im Dateisystem zu speichern.

Hdparm: Leistung & Ruhezustand

Das Terminalwerkzeug Hdparm bietet Hhardwarenahe Infos und Optimierungen für alle Datenträger an SATA und USB und ist detaillierter und universeller als grafische Alternativen. Einen Leistungstest startet dieser Befehl:

```
sudo hdparm -t /dev/sda
```

Dies ist hilfreich, um etwa den geeignetsten USB-Stick für eine bestimmte Ausgabe zu finden.

Hdparm kann Laufwerke bei Inaktivität nach gewisser Frist in den Bereitschaftsmodus versetzen. Sinnvoll ist das nur bei reinen Datenlaufwerken, nicht beim Systemdatenträger.

Das Tool unterstützt auch angeschlossene USB-Festplatten, was etwa bei Gnome-Disks nicht zutrifft. Ist die gewünschte Festplatte beispielsweise „/dev/sdb“, dann aktivieren Sie mit dem folgenden Befehl den Ruhezustand:

```
sudo hdparm -y /dev/sdb
```

Wenn das funktioniert, definieren Sie mit folgendem Befehl eine automatische Abschaltung (Schalter „-S“ für Spindown):

```
sudo hdparm -S 60 /dev/sdb
```

Der Wert hinter „-S“ muss mit „5“ multipliziert werden, in diesem Fall „60 mal 5“ Sekunden, also fünf Minuten. Da diese Einstellung nur bis zum nächsten Systemstart gilt, gibt es zwei Optionen für permanente Gültigkeit, entweder einen root-Cronjob (*sudo crontab -e*) mit obigem Befehl oder ein Eintrag in die Konfigurationsdatei „/etc/hdparm.conf“:

```
/dev/disk/by-uuid/[UUID] {
  spindown_time = 60
}
```

Die UUID liefern Lsblk oder Blkid.

Die Hdparm-Konfigurationsdatei ist komplizierter geworden. Alternativ kann man den Ruhemodus von Laufwerken auch als Cronjob anlegen (*@reboot /usr/sbin/hdparm -S 60 /dev/sda*).

SMART: Datenträgercheck

Technische Mängel von Laufwerken frühzeitig zu erkennen, kann Datenverlust und Ärger ersparen. Auch hier ist das Terminal – hier mit Smartctl – grafischen Werkzeugen überlegen, weil auch USB-Laufwerke unterstützt werden. Smartctl ist auf den meisten Distributionen Standard und kann bei Bedarf mit

```
sudo apt install smartmontools
```

nachinstalliert werden. Testen Sie die Laufwerke dann im Terminal (Beispiel):

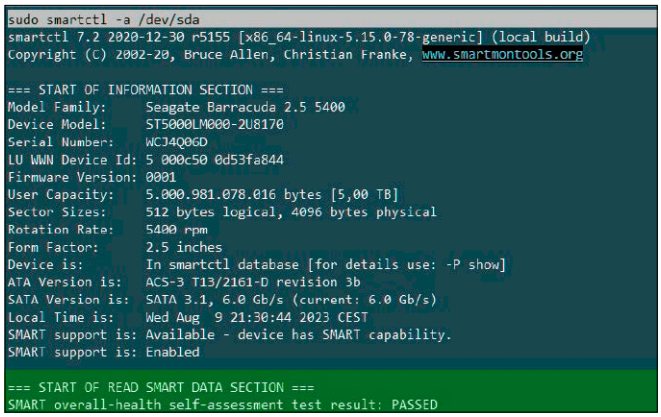
```
sudo smartctl -H /dev/sda
```

Wenn dieser kurze Health-Test mit „PASSED“ beantwortet wird, ist die allgemeine Tauglichkeit des Laufwerks schon erwiesen. Genauere Details liefert der Schalter „-A“

```
sudo smartctl -A /dev/sda
```

und noch ausführlicher der Schalter „-a“ („--all“). Ein wichtiger Wert ist „ Reallocated_Sectors_Ct“, der die Zahl defekter Sektoren anzeigt und im Optimalfall eine „0“ anzeigen sollte.

Gleiches gilt für „Spin_Retry_Count“, weil die hier gezählten, gescheiterten Anlaufversuche auf mechanische Mängel deuten. Seek- und Read-Errors sind eher weiche Mängelindizien und können auch bei hohen Werten toleriert werden. ■

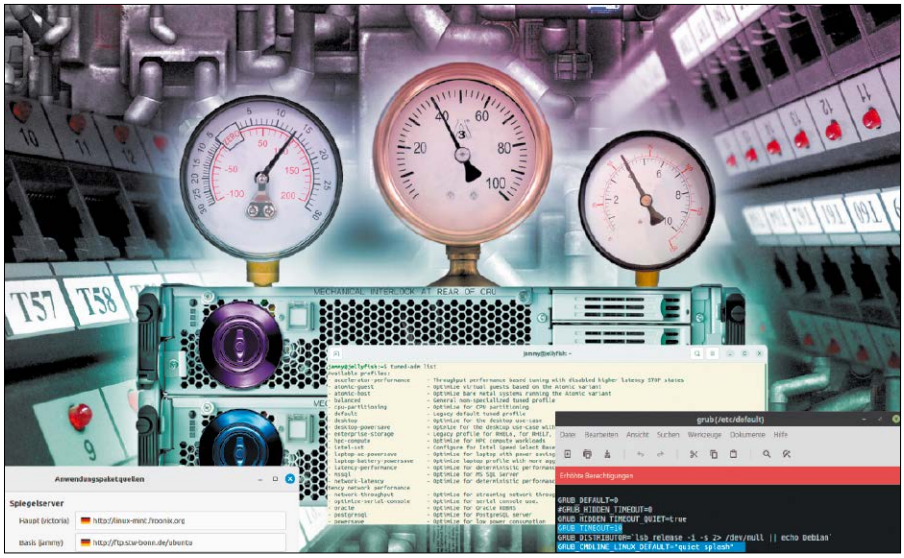


SMART-Test mit Smartctl: Laufwerksüberprüfungen im Terminal sind universeller als in grafischen Tools, weil sie auch bei USB-Datenträgern funktionieren (im Bild ist eine SATA-Festplatte).

20 Schritte zum optimalen System

Wenn Ubuntu oder Linux Mint auf aktuelle Hardware treffen, sind diese Distributionen schon nach der Standardinstallation überzeugend schnell. Mit den nachfolgenden Tipps gewinnen Sie aber Leistung, RAM- und Akkuressourcen hinzu.

VON HERMANN APFELBÖCK



Quelle: David Wolski

Die hier beschriebenen Methoden der Systemoptimierung eignen sich größtenteils für alle, zum kleineren Teil für fortgeschrittene Nutzer. Der Fokus liegt auf Ubuntu-Varianten und Linux Mint, jedoch funktionieren die meisten Optimierungen identisch oder sinngemäß auch unter anderen Linux-Distributionen. Die 20 Tuningmaßnahmen können selektiv oder Schritt für Schritt allesamt realisiert werden, weil sie sich nicht überschneiden und daher konfliktfrei funktionieren.

1. Hardware: SSD statt Festplatte

Software-Tuningaktionen können in der Summe das System signifikant beschleunigen. Einen Boost mit einer einzigen Maßnahme erzielen Sie aber nur durch schnellere Hardware. Eindeutig wichtigste Austauschkandidaten sind mechanische Festplatten, auf denen das Betriebssystem läuft. Für Benutzerdaten sind Festplatten aufgrund ihrer Kapazitäten nach wie vor konkurrenzlos, für tausendfache Systemzugriffe aber eine Bremse. Der Austausch durch eine SSD macht aus einem trägen, zehn Jahre alten Notebook sofort wieder eine alltagstaugliche Hardware.

Eine schnelle SSD mit 500 GB kostet heute weniger als 50 Euro und ist für ein Linux-System mehr als ausreichend, sofern keine große Datenarchive oder Spielesammlungen anfallen. Wenn bislang eine mechanische Platte arbeitet, bestehen beim Kauf keine Zweifel, dass eine klassische SSD im 2,5-Zoll-Format passt. Der Austausch ist auf PCs wie Notebooks nur eine Angelegenheit von wenigen Handgriffen. Die SSD wird genauso angeschlossen wie der vorherige Datenträger.

Was System und Software betrifft, gibt es mehrere Varianten:

1. Am einfachsten ist es, das Betriebssystem neu zu installieren. Wenn vorher das Home-Verzeichnis auf ein externes USB-Laufwerk gesichert und anschließend auf das neue System zurückkopiert wird, stehen Daten und Einstellungen schnell wieder zur Verfügung. Nur zusätzliche Software muss noch nachinstalliert werden. Der Anpassungsaufwand ist gering, wenn Distribution, Desktop und Software auf dem neuen Datenträger identisch sind.

2.1. Wer das bisherige System exakt übertragen will, kann es mit dem externen, unabhängigen Livesystem Clonezilla auf die neue SSD klonen („device-device“, dann „disk_to_local_disk“ und „savedisk“). Dies funktioniert aber nur auf PCs mit mehreren SATA-Ports. Die SSD muss dabei mindestens die Kapazität des bisherigen Laufwerks anbieten.

2.2. Wer das bisherige System auf Notebooks klonen will, muss den Umweg über eine Imagesicherung machen, in Clonezilla daher „device-image“ und „local_dev“ verwenden. Als vorübergehendes Imageziel kommt etwa eine USB-Festplatte in Frage. Das Image kann dann nach Tausch des Datenträgers mit Clonezilla („device_image“ → „local_dev“ → „restoredisk“) auf die SSD zurückgeschrieben werden.

Für **2.1** und **2.2** ist eventuell noch eine Nachbearbeitung nötig, sofern nämlich die neue SSD größer ist als die bisherige Festplatte. Dann muss die Systempartition auf die maximale Größe expandiert werden,

um den danach folgenden Platz nicht zu verschenken. Diese Expansion funktioniert mit der Software Gparted und deren Option „Größe ändern“ – und zwar sogar im laufenden System, dessen Systempartition erweitert werden soll.

2. Hardware: Optimale Treiber

Bei Grafikkarten und WLAN-Chips können Open-Source-Treiber mit Herstellertreibern nicht mithalten. Ubuntu & Co. machen es recht einfach, proprietäre Treiber nachzuinstallieren. In den Systemeinstellungen finden Sie den Punkt „Treiber“ oder „Treiberverwaltung“. Wenn Sie dieses Applet starten, beginnt automatisch eine Treibersuche. Wird ein passender Treiber gefunden, können Sie diesen nachinstallieren. Der neue Treiber wird ab dem nächsten Neustart verwendet.

Wer die aktuellsten Treiber verwenden will, kann diese auf eigene Gefahr aus externen Paketquellen installieren. Dies ist aber nur zu empfehlen, wenn die Grafikkarte offensichtlich nicht optimal unterstützt wird. Für Ubuntu und Mint gibt es ein PPA (Personal Package Archiv), das Sie über folgende Terminalbefehle einbinden:

```
sudo add-apt-repository
  ppa:graphics-drivers/ppa
sudo apt update
```

Anschließend gehen Sie in den Systemeinstellungen zur „Treiberverwaltung“. Hier stehen dann die neuesten Treiber aus dem PPA bereit.

Für Spieler relevant sind außerdem aktuelle Mesa-Bibliotheken für optimale Grafikbeschleunigung. Benutzer von Ubuntu, Linux Mint und Derivaten können dem System das folgende externe Repository (PPA) hinzufügen, das die aktuellen Mesa-Komponenten anbietet:

```
sudo add-apt-repository ppa:kisak/
  kisak-mesa
```

Danach sind die Mesa-Pakete mit den üblichen Terminalbefehlen

```
sudo apt update
sudo apt upgrade
```

oder mit der grafischen Aktualisierungsverwaltung zu aktualisieren.

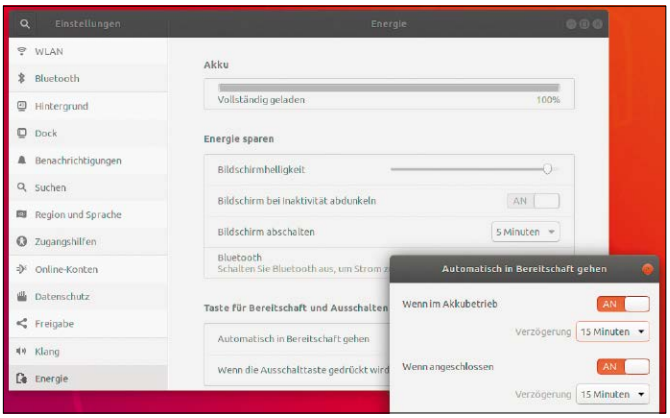
3. Hardware: Akku und Stromsparen

Ubuntu und Mint beschränken sich auf Stromsparoptionen, die das größte Einsparpotenzial besitzen – nämlich auf die Bildschirmabschaltung und den Suspend-Modus („Bereitschaft“). Unter „Systemeinstellungen → Energie“ (oder „Energieverwaltung“) finden Sie den Timer für den Bereitschaftsmodus („Automatisch in Bereitschaft gehen“ oder „Standby-Modus“). Nach der angegebenen Frist geht der Rechner in stromsparende Bereitschaft, sofern keine Aktivität festgestellt wurde. Optionen für das Verdunkeln und Ausschalten des Bildschirms bei Inaktivität finden Sie an gleicher Stelle.

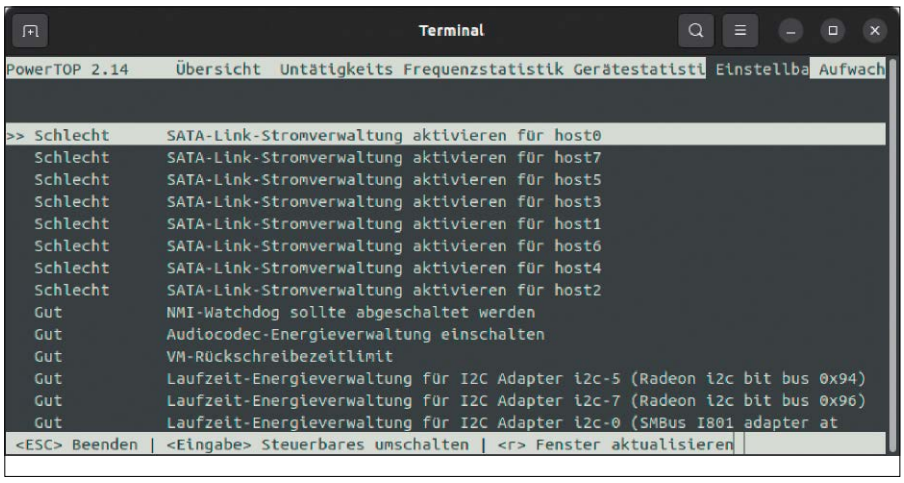
Im Bereitschaftsmodus verbrauchen Notebooks (mit geladenem Akku) und PCs nur noch minimale 0,5 bis 1,0 Watt die Stunde. Und die Leistungsaufnahme zwischen einem maximal hellen Noteboodisplay und einem maximal abgedunkelten unterscheidet sich um drei bis vier Watt.

Das **Tool Powertop** (mit gleichnamigem Paketnamen zu installieren) liefert auf der Seite „Einstellbarkeit“ eine Reihe von weiteren Empfehlungen zur stromsparenden Systemkonfiguration. Die Anzeigeseite wechseln Sie mit der Tab-Taste. Unter „Einstellbarkeit“ erscheinen aktivierte und deaktivierte Stromsparfunktionen. Temporär

Kaum mehr als ein Handgriff: Der Einbau einer SSD macht aus lahmen Altgeräten wieder alltagstaugliche Hardware.



Stromsparen: In den Energieeinstellungen (hier Ubuntu) legen Sie die Bildschirmhelligkeit fest und stellen die Zeit ein, wann der Rechner in den Bereitschaftsmodus schalten soll.



Powertop: Das Kommandozeilentool zeigt den aktuellen Energiebedarf und auf der Seite „Einstellbarkeit“ Sparoptionen, die Sie direkt aktivieren können.

für die aktuelle Sitzung und bis zum nächsten Neustart, aktiviert ein Druck auf die Eingabetaste eine einzelne Option. Um alle vorgeschlagenen Stromsparfunktionen für diese Sitzung einzuschalten, dient folgendes Kommando:

```
sudo powertop --auto-tune
```

Damit die Powertop-Einstellungen automatisch nach einem Neustart wirken, erstellen Sie einen Cronjob. Nach der Eingabe von

```
sudo crontab -e
```

tragen Sie in der Cronjob-Konfiguration die neue Zeile

```
@reboot /usr/sbin/powertop --auto-
  tune
```

ein, um diesen Befehl standardmäßig bei jedem Systemstart auszuführen.

4. Hardware: Rechner in Standby

Wer sein System jederzeit schnellstmöglich bedienen will, fährt es entweder gar nicht mehr herunter oder nur noch über Nacht. Wie schon unter Punkt 3 angemerkt, messen wir bei einem Notebook (dessen Akku geladen ist) im Standby-Bereitschaft 0,5 bis 1,0 Watt Stromverbrauch. Das sind auch bei heutigen Strompreisen gerade mal drei Euro im Jahr, sofern Sie das Gerät überhaupt nicht mehr abschalten. Und das Aufwachen aus dem Standby ist bekanntlich in zwei, drei Sekunden geschehen.

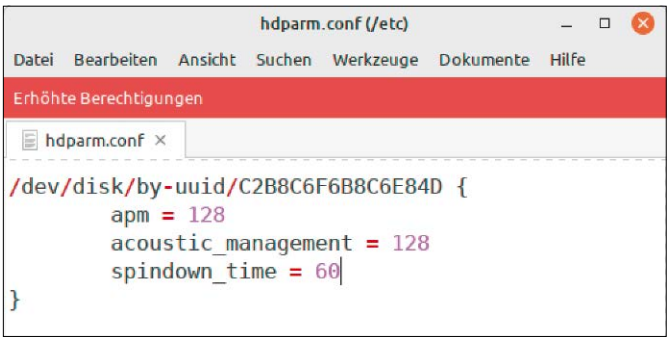
5. Hardware: Festplattenaktivität

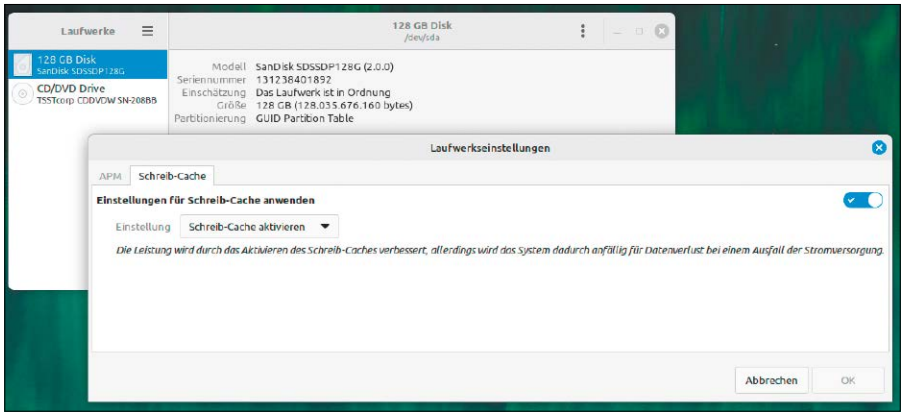
Datenträger lassen sich per Software in den Ruhemodus schicken. So können Ubuntu und Mint über das standardmäßig installierte Tool „Laufwerke“ (Gnome-Disks) einstellen, wann sich ein Laufwerk abschalten soll. Sinnvoll ist das nur bei reinen Datenlaufwerken, nicht beim Systemdatenträger. Wählen Sie im Tool das gewünschte Laufwerk aus und gehen Sie im Drei-Punkte-Menü auf „Laufwerkseinstellungen“. Auf der Registerkarte „Bereitschaft“ setzen Sie den Schalter auf „An“ und stellen die Zeit ein, nach der die Festplatte sich abschalten soll. Die Zeitspanne reicht von „Niemals“ (Ruhezustand deaktiviert) über „5 Minuten“ bis „3 Stunden“.

Für USB-Festplatten ist dieser Menüpunkt ausgegraut. Hier hilft das Tool Hdparm, das auch USB-Laufwerke bei Inaktivität in den Bereitschaftsmodus versetzt. Ist die gewünschte Festplatte beispielsweise „/dev/sdb“, dann aktivieren Sie mit diesem Befehl den Ruhezustand:

```
sudo hdparm -y /dev/sdb
```

Hdparm-Konfigurationsdatei mit Schlafanweisung für ein Laufwerk: Alternativ kann man den Ruhemodus von Laufwerken auch als Cronjob anlegen.





Der Schreibcache für Laufwerke ist standardmäßig meistens abgeschaltet. Mit dem Systemtool Gnome-Disks korrigieren Sie dieses Manko.

Wenn das funktioniert, definieren Sie mit folgendem Befehl eine automatische Abschaltung (Schalter „-S“ für Spindown):

```
sudo hdparm -S 60 /dev/sdb
```

Der Wert hinter „-S“ muss mit „5“ multipliziert werden, in diesem Fall also „60 mal 5“ Sekunden, also 5 Minuten. Da diese Einstellung nur für die aktuelle Sitzung gilt, gibt es zwei Optionen für permanente Gültigkeit: Ein root-Cronjob (*sudo crontab -e*) mit obigem Befehl

```
@reboot hdparm -S 60 /dev/sdb
```

kann das ebenso erledigen wie ein Eintrag in die Konfigurationsdatei „/etc/hdparm.conf“:

```
/dev/disk/by-uuid/[UUID] {
  spindown_time = 60
}
```

Die hier benötigte UUID-Kennung ermitteln Sie mit *lsblk -f*.

6. Hardware: Cache für Laufwerke

Die Kontrolle der internen Datenträger unter „Laufwerke“ (Gnome-Disks) kann einen erheblichen Mangel offenbaren: Klicken Sie jedes Laufwerk an und kontrollieren Sie über das Drei-Punkte-Menü und den Eintrag „Laufwerkseinstellungen“, ob dort der „Schreib-Cache“ aktiviert ist. Nach unserer Erfahrung ist das selbst beim Systemlaufwerk meistens nicht der Fall. Mit dem Schieberegler rechts oben ist das leicht zu korrigieren.

7. Booten: Schneller ohne Anmeldung

PCs und Notebooks zu Hause können eventuell ohne bremsende Anmeldung direkt zum Desktop durchstarten. Sie können daher eine automatische Anmeldung einrichten – etwa in Ubuntu unter „Systemeinstellungen → Details → Benutzer“, in Linux Mint unter „Anmeldefenster“. Um dadurch wirklich Zeit zu gewinnen, müssen Sie zusätzlich unter „Passwörter und Verschlüsselung“ nach Rechtsklick auf „Anmeldung“ und „Passwort ändern“ ein leeres Passwort definieren. Andernfalls würde der Schlüsselbund, der im Normalfall mit der Anmeldung geöffnet wird, spätestens dann nach dem Kennwort fragen, wenn ein Kennwort – etwa für eine Netzanmeldung – benötigt wird.

Ein Sonderfall, wo eine Anmeldung definitiv entfallen kann, ist ein Desktopsystem, das mit Luks-Datenträgerverschlüsselung installiert wurde: Hier muss das Systemlaufwerk bei jedem Bootvorgang sowieso durch

das unabhängige Luks-Kennwort aufgesperrt werden. Dieser Zugangsschutz genügt dann vollauf.

8. Booten: Kurze Bootloader-Wartezeit

In Multiboot-Umgebungen wartet der Grub-Bootloader standardmäßig zehn Sekunden auf eine Auswahl, bis er das erste, oberste Standardsystem automatisch wählt. Vor allem dann, wenn man überwiegend dieses System nutzt, ist es sinnvoll, den Eintrag

```
GRUB_TIMEOUT=10
```

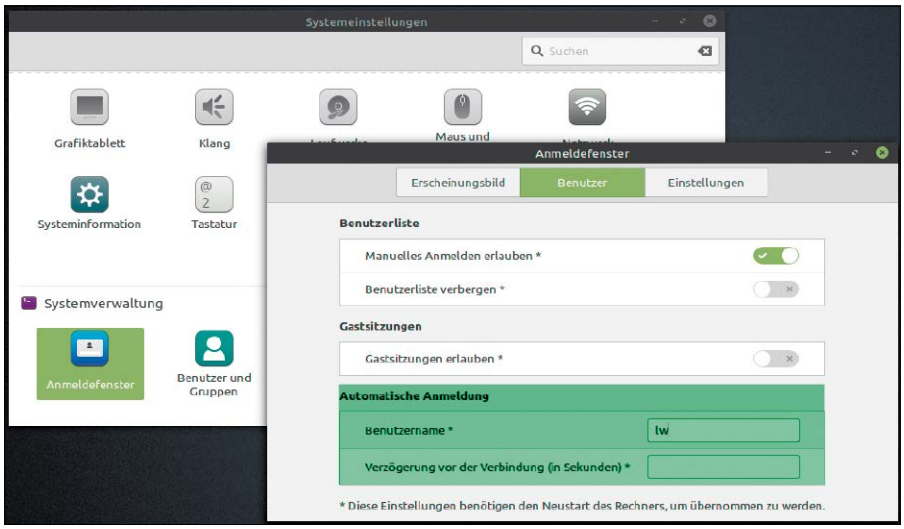
in der Datei /etc/default/grub etwa auf „3“ (Sekunden) zu verkürzen und danach mit *sudo update-grub* die Bootumgebung neu zu initialisieren.

9. Booten: Bootbremsen beseitigen

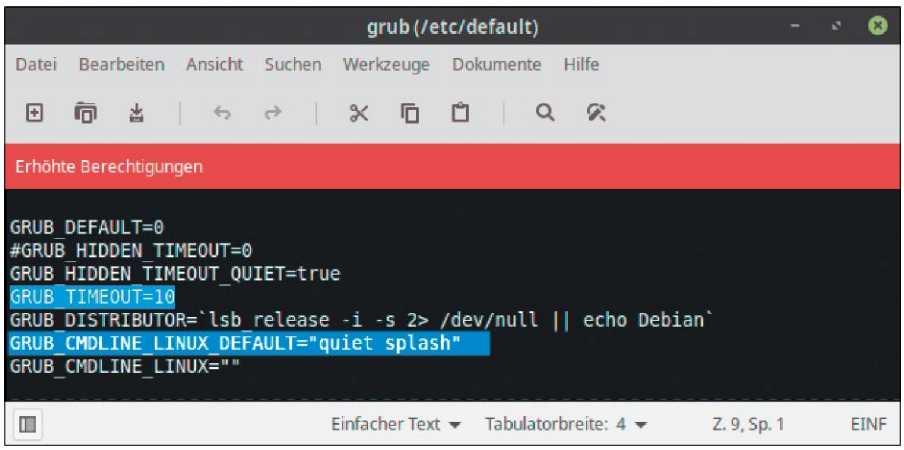
Unerklärliche Bootbremsen sind lästig: Eventuell ist der Bootvorgang komplett unterbrochen, wartet 20, 30 Sekunden und mehr und setzt erst dann fort. Um die Ursache herauszufinden, sollten Sie einen gesprächigen Bootvorgang erzwingen. Dauerhaft ist dies über die Datei „/etc/default/grub“ möglich, indem Sie die Zeile mit dem Eintrag „quiet splash“ mit dem Kommentarzeichen „#“ deaktivieren.

Eine Analyse erreichen Sie beim Systemstart, indem Sie „Erweiterte Optionen…“ wählen und darunter den Eintrag mit dem Hinweis „Recovery mode“. Ebenfalls erhellend kann die Abfrage der Kernel-Meldungen mit *dmesg -T* sein, wobei Sie sich beim Booten die exakte Uhrzeit mit Sekundenangabe notieren sollten, wann der Boothänger auftritt. Dmesg zeigt nämlich die Zeit aller Systemereignisse, die Sie dann genau zuordnen können.

Sehr lange Bootzeiten haben aber oft eine einfache Ursache, die sich leicht beheben lässt: Sie sprechen für einen fehlerhaften Eintrag in der Datei „/etc/ fstab“. Beweis dafür ist die Meldung „A start job is running for dev-disk-by…“, die sich beim hängenden Start durch Druck der Esc-Taste offenbart oder durch einen Systemstart über „Erweiterte Optionen → Recovery mode“. Das System will eine Festplatte mounten, die es nicht vorfindet. Erste Abhilfe ist ein Auskommentieren der betreffenden Zeile in der „fstab“ (mit „#“). Falls die Festplatte zwingend gemountet werden muss, kontrollieren Sie, ob der Mountpunkt



Auto-Log-in: Damit sich das zeitlich lohnt, muss der Standardbenutzer ein leeres Passwort verwenden. Jeder Kontenschutz entfällt damit, es sei denn, das System ist Luks-verschlüsselt.



Time-out ändern: Die Wartezeit bei Multiboot kann deutlich verkürzt werden. Zu empfehlen ist ferner ein gesprächiger Bootvorgang zur Fehleranalyse ohne „quiet“-Parameter.

existiert, und mit *lsblk -f*, ob die UUID-Kennung korrekt ist.

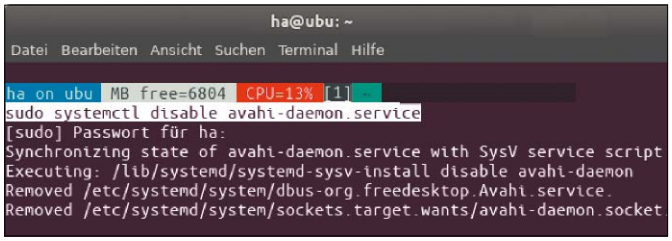
10. System: Schnelle, lokale Spiegelserver

Linux-Distributionen erhalten alle Updates und Programme von den zentralen Servern des Distributionsanbieters. Spiegelserver sind Alternativen, oft von Universitäten, die genau dasselbe Paketangebot bevorraten. Einen schnellen, lokalen Spiegelserver aus Deutschland einzustellen, ist eine klassische Win-win-Aktion und daher unbedingt zu empfehlen: Davon profitieren sowohl die Systembenutzer als auch die dadurch entlasteten Server des Distributionsanbieters. Je schneller die Internetverbindung ist, desto mehr lohnt sich ein richtig schneller Spiegelserver. Ubuntu & Co. können den geeignetsten deutschen Server selbst ermitteln: Dazu gehen Sie zu „Anwendungen & Aktualisierungen“ (Ubuntu) oder „Anwendungspaketquellen“ (Mint). Die dort vorangestellten Server können Sie anklicken, wonach automatisch die Suche nach einem deutschen Server beginnt. Die werden dabei automatisch nach der Downloadleistung sortiert – die schnellsten nach oben. Wählen Sie den schnellsten Server (den ersten in der Liste). Beachten Sie aber, dass der Geschwindigkeitstest eine Momentaufnahme ist, die gelegentliche Kontrolle verdient.

11. System: Systemdienste abschalten

Jedes Linux lädt zahlreiche Systemdienste, die nicht jeder Anwender benötigt. Einblick in die aktiven Dienste auf einem System mit Systemd-Daemon (Ubuntu, Mint)

Schnelle Spiegelserver für Updates und Installationen: Ubuntu und Linux Mint zeigen durch Schnelltests geeignete Kandidaten für den Softwarebezug.



Systemdienste abschalten: Unter Ubuntu und Mint (mit systemd) ist das Tool Systemctl das einschlägige Werkzeug zur Dienstverwaltung.

erhalten Sie folgendermaßen:

```
systemctl -a
```

Die Übersicht zeigt – unter anderem – die aktiven und inaktiven Dienste an. Dass Systemdienste in der Regel keine große Bootbremse darstellen, können Sie auf Ubuntu und Mint mit dem Befehl

```
systemd-analyze blame
```

kontrollieren, der die Ladezeiten absteigend (längste bis kürzeste) auflistet. Trotzdem können Sie Dienste abschalten, um Ressourcen einzusparen – vor allem solche, die tendenziell nur nerven: Whoopsie (Fehlerreport), Apport (Fehlerprotokoll), Apparmor (Sicherheitserweiterung), Ufw (Firewall), Brltty (Blindentastatur) sind auf dem Desktop selten notwendig:

```
sudo systemctl stop whoopsie
sudo systemctl disable whoopsie
```

Der Befehl „stop“ beendet den angegebenen Dienst in der aktuellen Sitzung, „disable“ deaktiviert ihn dauerhaft. Mit „enable“ und „start“ ist er bei Bedarf wieder zu aktivieren.

12. System: Manuelle Kernel-Optimierung

Das Kernel-Verhalten kann durch zahlreiche Parameter gesteuert werden. Interaktiv kann der Befehl Sysctl Kernel-Optionen für die aktuelle Sitzung ändern, dauerhaft ein Eintrag in die Systemdatei „/etc/sysctl.conf“. Welche Optionen insgesamt verfügbar sind, zeigt dieser Befehl:

```
sysctl -a
```

An dieser Stelle nennen wir nur zwei Beispiele: Das Protokoll IPv6 spielt im Heimnetz in der Regel keine Rolle. Da ältere Router und andere Netzwerkhardware für IPv6-Pakete oft schlechterem Datendurchsatz bieten, kann man IPv6 auch abschalten. Bei Ubuntu & Co. erledigt dies folgender Befehl

```
sudo sysctl net.ipv6.conf.all.
  disable_ipv6=1
```

interaktiv oder dauerhaft die zusätzliche Zeile

```
net.ipv6.conf.all.disable_ipv6=1
```

in der Datei „/etc/sysctl.conf“.

Swapping, also das Auslagern länger ungenutzter Speicherseiten vom Arbeitsspeicher auf die Festplatte, ist ein Verfahren, das auf die 90er-Jahre zurückgeht, als RAM notorisch knapp war: Der frei gewordene, schnelle Arbeitsspeicher steht dann wieder für Programme und für den Festplattencache zur Verfügung. Wie aktiv der Kernel auslagert, steuert der Parameter „Swappiness“, dessen aktuellen Wert Sie mit

```
cat /proc/sys/vm/swappiness
```

ermitteln. Unter Ubuntu & Co. voreingestellt ist „60“. Viel RAM bei langsamer mechanischer Festplatte legt es nahe, das Swappen stark zu reduzieren – etwa auf den Wert „10“. Bei wenig RAM, aber schneller SSD empfiehlt sich hingegen ein hoher Wert – etwa „90“:

```
sudo sysctl vm.swappiness=90
```

Dauerhaft gilt der Wert, wenn Sie die Zeile

```
vm.swappiness=90
```

mit root-Recht (sudo) in die „sysctl.conf“ eintragen.

13. System: Kernel-Optimierung mit Tuned

Der Systemdienst Tuned optimiert die Systemleistung mit einer Kombination von Sysctl-Parametern. Hinzu kommen eventuelle Anpassungen mit Hdparm (siehe Punkt 6), Powertop (siehe Punkt 3) sowie Netzwerkoptimierungen mit Ethtool. Dafür gibt es vorbereitete Profile für unterschiedliche Rechnerrollen wie Desktop, Dateiserver, virtuelle Maschinen oder Notebooks. Unter Ubuntu und Mint ist Tuned mit

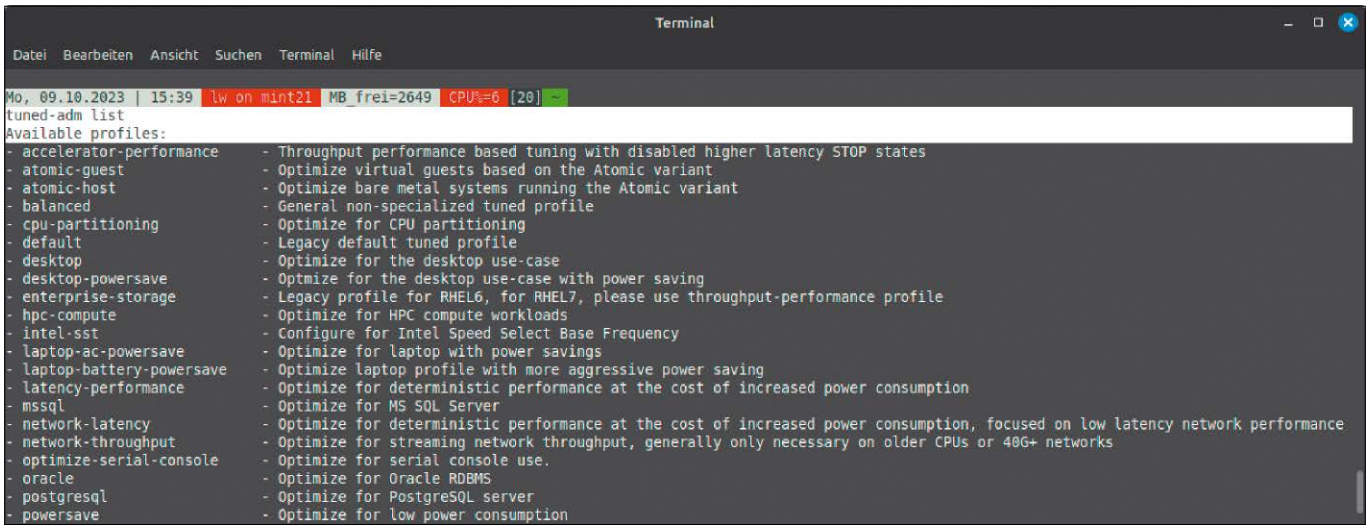
```
sudo apt install tuned tuned-utils
  tuned-utils-systemtap
```

zu installieren. Anschließend wird der Systemdienst mit

```
sudo systemctl enable tuned
```

via Systemd gestartet und aktiviert.

Der Parameter „vm.swappiness“ steuert die Auslagerungsaktivität. Bei viel RAM ist ein niedriger Wert angebracht, bei schneller SSD kann ein hoher Wert Leistungsvorteile bringen.



Optimierungsdienst Tuned: Hier sind zahlreiche Profile vorgegeben, die dann je nach Auswahl etliche Kernel-Parameter setzen und Sparmechanismen aktivieren.

Tuned tritt sofort in Aktion und aktiviert dabei das Standardprofil „balanced“, wie das zugehörige Werkzeug Tuned-adm mit diesem Kommando belegt:

```
tuned-adm active
```

Für ein Linux-Desktopsystem eignen sich die Profile „desktop“ oder „desktop-powersave“ und sind mit

```
sudo tuned-adm profile desktop
```

umweglos zu aktivieren. Eine Übersicht aller vorhandenen Profile liefert der Befehl *tuned-adm list*. Theoretisch kann man Tuned-Profile unter „/etc/tuned“ selbst definieren oder anpassen, was aber dann dem manuellen Weg nahekommt (Punkt 12).

14. System: Ext4 optimieren

Das Dateisystem Ext4 bietet viele Optionen über den Befehl Tune2fs, die zum Teil mit eingehängten, zum Teil nur mit ausgehängten Datenträgern funktionieren. Eine Übersicht für einen bestimmten Datenträger erhalten Sie mit diesem Befehl (root-Recht ist für tune2fs grundsätzlich erforderlich):

```
sudo tune2fs -l /dev/sda
```

Tuning für Ext4 wird kaum spürbaren noch messbaren Leistungsgewinn bringen. Das Motiv ist hier eher, die Hardware zu schonen. Die einzige Maßnahme, die gelegentlich den Bootvorgang beschleunigt, ist der Verzicht auf unnötig häufige Datenträger-Checks. Nach dem Befehl

```
sudo tune2fs -i60 -c100 /dev/sda
```

wird eine Festplattencheck nur noch alle 60 Tage („-i60“) oder nach 100 Neustarts („-c100“) erfolgen – je nachdem, welches Ereignis früher eintritt. Ein weitere Option ist das Abschalten der Journalingfunktion. Das Journaling dient zur Wiederherstellung von Dateien nach Abstürzen oder Stromausfällen und ist auf der Systempartition zu empfehlen, auf externen USB-Datenträgern oder reinen Datenpartitionen aber nicht notwendig:

```
sudo umount /dev/sdd?
sudo tune2fs -O ^has_journal /dev/
  sdd
```

Der erste Befehl ist notwendig, weil das Dateisystem bei dieser Änderung nicht eingehängt sein darf. Der zweite Befehl schaltet das Journaling für das Gerät „/dev/sdd“ ab, wovon Sie sich mit

```
sudo tune2fs -l /dev/sdd
```

in der Zeile „Filesystem features“ überzeugen können. Umgekehrt lässt sich das Journaling mit diesem Befehl aktivieren:

```
sudo tune2fs -O has_journal /dev/sdd
```

15. System: Ramdisk als Zwischendepot

16 GB RAM sind auf heutigen Rechnern eher die Regel als die Ausnahme. Für den typischen Einsatz mit Office, Mediaplayer, Bildbearbeitung ist das purer Luxus, mit dem sich aber Sinnvolles anfangen lässt. Wenn Sie einen zentralen Ordner, über den Sie den Datenaustausch inklusive Downloads abwickeln, in eine schnelle Ramdisk verlegen, entstehen mehrere Vorteile: mehr Leistung, Entsorgung beim Herunterfahren, Schonung von SSD/Festplatte, Nutzung des brachliegenden Speichers.

Eine Ramdisk ist unter Linux im Handumdrehen erstellt. Idealerweise liegt dieser Speicher zentral, etwa im Home-Verzeichnis oder gleich am Desktop:

```
sudo mount -t tmpfs -o size=2000M
  ramdisk ~/Ramdisk
```

Dieser Befehl genügt, um im Ordner „Ramdisk“ (der existieren muss), Platz für maximal zwei GB Daten zu schaffen. Die angegebene Kapazität wird dynamisch abgezweigt – je nach Bedarf bis zum angegebenen Maximum. Die Ramdisk verbraucht also immer nur so viel Speicher, wie die enthaltenen Dateien tatsächlich verursachen. Dauerhaft ist eine Ramdisk über die Datei „fstab“ einzurichten:

```
sudo nano /etc/fstab
```

Hier fügen Sie die weitere Zeile (Beispiel)

```
tmpfs /home/lw/Ramdisk tmpfs
  defaults,size=40%,mode=1777 0 0
```

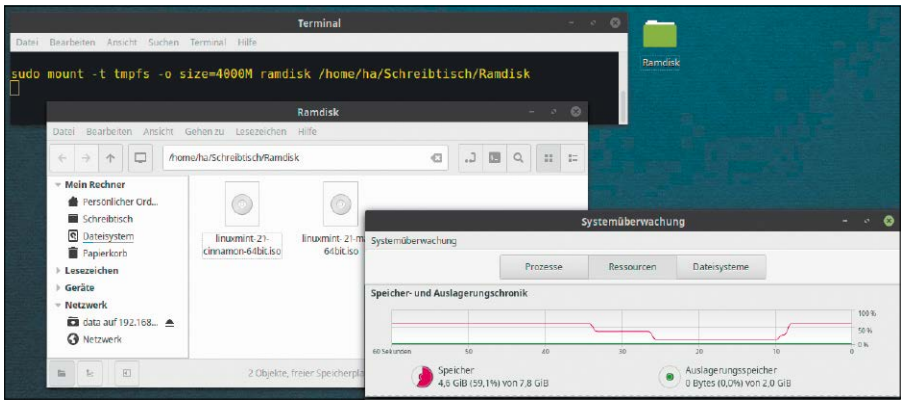
hinzu (der Mountpfad darf keine Variablen enthalten). Nach dem Speichern starten Sie Linux neu.

Achtung: Der Umgang mit Ramdisk-Daten erfordert disziplinierte Nutzer, weil die Daten beim Shutdown gelöscht werden. Ein praktischer Sonderfall für die Ramdisk-Nutzung ist der Einsatz als Browserverzeichnis, dessen Daten man nach Beenden des Browsers sowieso löschen will (siehe Punkt 19).

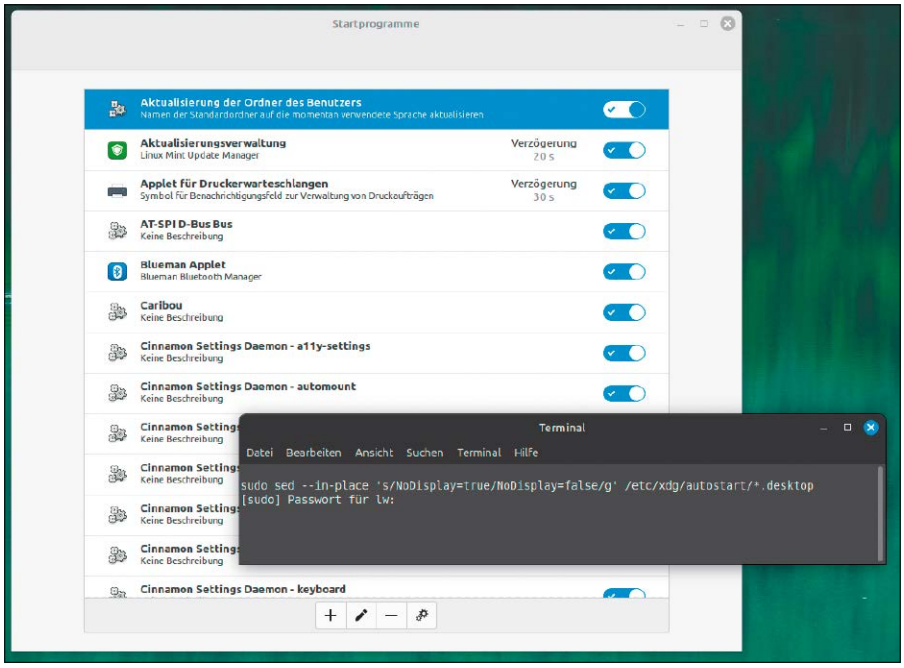
16. Software: Autostarts ausmisten

Desktops wie Gnome, KDE oder Cinnamon laden zahlreiche Programme bei der Desktopanmeldung.

Das Abschalten solcher Autostarts spart Speicher und beschleunigt den Desktopstart. Über das Tool „Startprogramme“ (Gnome-session-properties) können Sie bestehende Autostarts reduzieren.



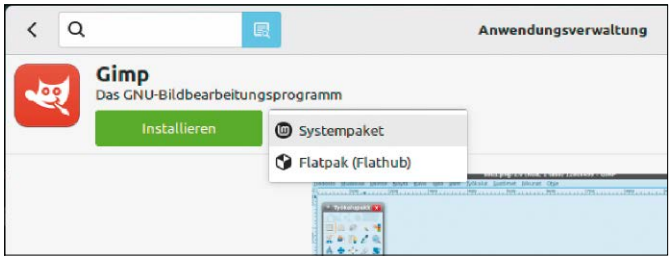
Der Ramdisk-Verbrauch ist nicht statisch, sondern richtet sich dynamisch nach dem Bedarf. Die Speicherchronik zeigt die Belegung nach Löschen und Kopieren großer ISO-Dateien.



Alle Autostarts: Das Tool „Startprogramme“ zeigt alle Selbststarter nur dann an, wenn Sie die Anweisung „NoDisplay“ in den Konfigurationsdateien abgeschaltet haben.

Besonders umfangreich fällt die Funktionalität unter KDE aus, das in den „Systemeinstellungen“ im Bereich „Starten und Beenden“ eine Reihe spezieller Optionen vorhält: So ist der Standard unter „Arbeitsflächen-Sitzung“, der alle Programme der letzten KDE-Nutzung automatisch wiederherstellt, in der Regel überflüssig und durch die Option „Mit leerer Sitzung starten“ zu ersetzen.

Wer rigoros ausmisten will, muss wissen, dass das Tool „Startprogramme“ die meisten systemnahen Komponenten ausblendet. Dafür sorgt die Anweisungszeile „NoDisplay=true“ in der jeweiligen Desktopdatei. Mit



Vorfahrt für klassische Pakete: Die Unterscheidung der Containerformate ist nicht überall so vorbildlich klar wie hier unter Linux Mint.

```
sudo sed --in-place 's/
 NoDisplay=true/
 NoDisplay=false/g' /etc/xdg/
 autostart/*.desktop
```

können Sie die Anweisung in allen Startern abschalten. Damit werden unter „Startprogramme“ alle Autostarts sichtbar und können deaktiviert oder komplett entfernt werden (die Programme selbst bleiben aber auf dem System). Theoretisch können Sie außer D-Bus, X-Settings-Plugin, Automount und den Sicherheitsdienst alles abschalten. Damit ist etwa auch ein Dickschiff wie Ubuntu Gnome auf deutlich unter 1 GB RAM zu verschlanken, ohne Cache auf unter 700 MB (siehe *free -m*).

Natürlich ist es Ermessensfrage, auf welche Module man tatsächlich verzichten kann und will: So ist ohne „Pulseaudio“ nur ein Audiostrom möglich, ohne „Dateien“ (nautilus-desktop) kein Desktop als Dateiablage, ohne „Aktualisierungsbenachrichtigung“ (update-notifier) kein Systemhinweis auf Updates.

17. Software: Snaps & Flatpaks

Der Tipp ist trivial und fordert nur etwas kritische Aufmerksamkeit: Klassische Programmpakete, die sich auf die vorhandenen Systembibliotheken verlassen, starten schneller als die Containerformate Snap, Flatpak oder Appimage. Denn diese müssen alle Abhängigkeiten mitbringen und bei jedem Start in ein virtuelles Dateisystem auspacken. Snaps & Co. konsequent aus dem Weg zu gehen, ist zwar auf Dauer kaum realisierbar, jedoch sollte die Wahl immer auf das klassische DEB- oder RPM-Paket fallen, sofern diese Alternative zur Verfügung steht.

18. Software: Preload-Beschleunigung

Das Tool Preload beschleunigt die Programmstarts oder Autostarts (unter „Startprogramme“), die Sie häufig oder regelmäßig nach jeder Anmeldung verwenden. Der einfache Dienst protokolliert die Programmvorlieben des Benutzers und lädt Komponenten dieser Softwarefavoriten vorab in den Arbeitsspeicher. Der eigentliche Programmstart verläuft dadurch deutlich schneller.

Preload ist in den Paketquellen verfügbar und etwa in Ubuntu mit

```
sudo apt install preload
```

schnell nachinstalliert und dann auch so-

fort aktiv. Theoretisch können Sie in die Konfiguration des einfachen Tools manuell eingreifen („/etc/preload.conf“), dies ist jedoch weder erforderlich noch inhaltlich ergiebig.

19. Software: Browser beschleunigen

Firefox: Zum Mozilla-Browser gibt es zahlreiche Detaileinstellungen über die Konfigurationszentrale „about:config“, die Firefox beschleunigen sollen. Seriöse, mit Messung belegte Leistungsvorteile durch geänderte Einstellungen unter „network.http.*“ oder „network.dns.*“ werden Sie jedoch kaum finden. Aus diesem Grund beschränken wir uns auf nachhaltige Maßnahmen.

• Einem langsamen Firefox helfen Sie durch ein neues Nutzerprofil auf die Sprünge. Nach

```
firefox --ProfileManager
```

und „Create Profile“ entsteht ein neues Profil mit Standardeinstellungen. Damit läuft der Browser wieder wie neu, Anpassungen und Lesezeichen gehen dabei aber verloren.

• Firefox lädt beim Start alle eingerichteten Erweiterungen. Der Menüpunkt „Add-ons“ zeigt die installierten Erweiterungen und kann diese wieder entfernen.

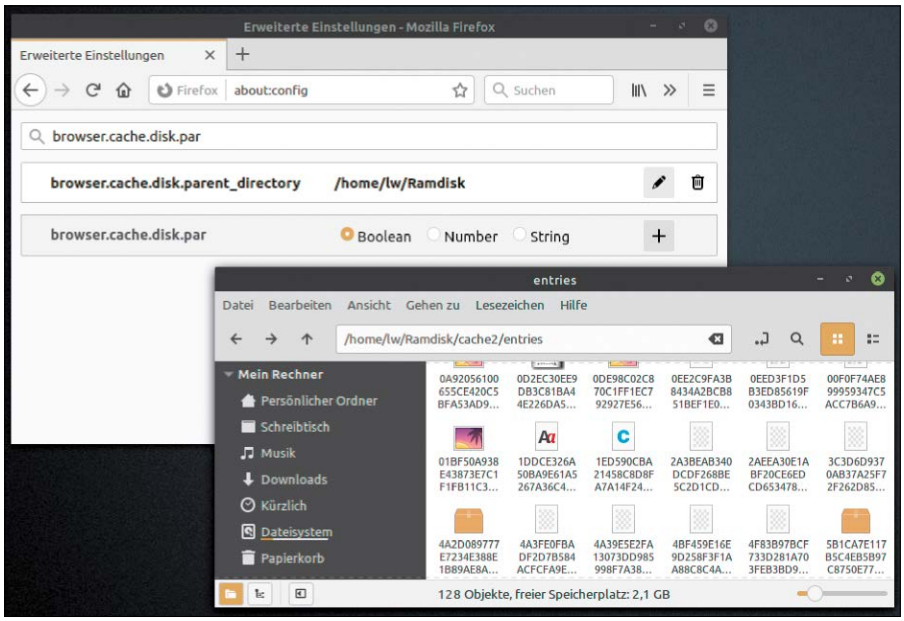
• Verlauf abschalten oder „Privates Browsen“: Wenn der Browser nichts aufzeichnen muss, läuft er schneller. Über „Einstellungen → Datenschutz & Sicherheit → Chronik“ entscheiden Sie, ob Firefox einen Verlauf anlegt oder eben nicht. Am genauesten sind hier die „benutzerdefinierten Einstellungen“, die „Immer den Privaten Modus“ (ohne Verlaufsaufzeichnung) vorsehen oder eine Option, um nur Suchbegriffe und Formulardaten zu speichern.

• Cache verlegen: Wenn Sie über die Adresse „about:config“ den zusätzlichen Parameter (als „String“)

```
browser.cache.disk.parent_
  directory
```

neu anlegen, können Sie danach den Ordner für die Verlaufsdaten manuell eintragen und somit frei wählen. Ideales Ziel ist eine Ramdisk, sofern der Verlaufsinhalt bei jedem System-Shutdown gelöscht werden darf (siehe Punkt 14).

Chrome/Chromium: Hier gilt Analoges wie beim Firefox: Die Chrome-Seiten und „chrome:about“ und „chrome:flags“ versprechen theoretisches Optimierungspotenzial. In der Praxis sollten folgende Tuningmaßnahmen ausreichen.



Browserverlauf in beliebigen Ordner schreiben: Firefox und Chrome/Chromium können die Surfchronik in einen benutzerdefinierten Ordner schreiben – etwa auf eine schnelle Ramdisk.

• Tabula rasa: Der Google-Browser hat zwar keinen Profilmanager, aber es ist trotzdem ganz einfach, den Konfigurationsballast abzuwerfen, indem Sie den Ordner „~/.config/google-chrome“ löschen oder verschieben. Ferner kann der Startschalter „--user-data-dir“ ein beliebiges Verzeichnis festlegen, in das der Browser seine Daten schreibt:

```
google-chrome --user-data-dir=/
  home/lw/chrome
```

Auch das ergibt ein komplett neues Chrome/Chromium-Profil.

• Erweiterungen abschalten: Im Google-Browser zeigt der Menüpunkt „Weitere Tools → Erweiterungen“ die Übersicht der installieren Add-ons, die sich per Schieberegler abschalten lassen.

• „Inkognito-Fenster“: Einstellungen für die Verlaufsaufzeichnung kennt Chrome nicht, aber bei konsequenter Verwendung des Inkognito-Modus geht die Schreibaktivität des Browser ebenso gegen null. Interaktiv verwenden Sie dazu den Menüpunkt „Neues Inkognito-Fenster“, einen generellen Inkognito-Modus erreichen Sie mit dem Browseraufruf „google-chrome --incognito“, den Sie als Starter oder Terminal-Alias ablegen können.

• Cache verlegen: Chrome kann wie Firefox alle Verlaufsdaten in ein beliebiges Verzeichnis schreiben. Der Google-Browser erledigt das über einen Aufrufschalter:

```
google-chrome --disk-cache-dir=/
  home/lw/Ramdisk
```

Geschwindigkeitsvorteile ergeben sich, wenn es sich beim neuen Ziel um ein schnelleres Medium handelt – etwa eine SSD oder Ramdisk (siehe Punkt 14).

20. Software: Libre Office beschleunigen

Wenn Libre Office durch eine fehlerhafte oder überladene Benutzerkonfiguration ausgebremst wird, lässt sich das mit diesem speziellen Startparameter leicht nachprüfen:

```
libreoffice
  -env:UserInstallation=file:///
  tmp/libreoffice
```

Damit entsteht ein neues Benutzerprofil im angegebenen Pfad. Wenn Office damit wieder einwandfrei läuft, sollten Sie das bisherige Profil unter „~/.config/libreoffice“ reparieren oder löschen. Dabei hilft dieser Start

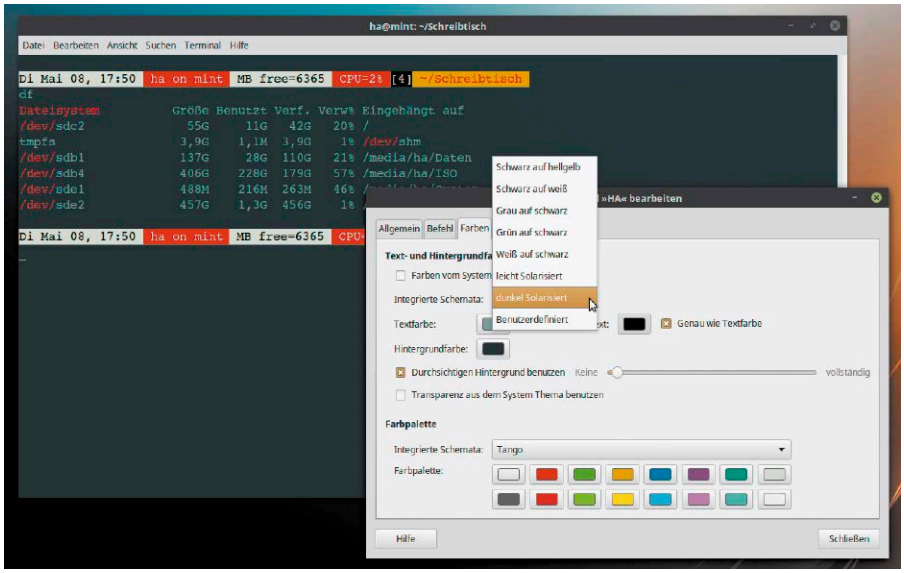
```
libreoffice --safe-mode
```

mit Reparaturoptionen wie „Benutzerkonfiguration [...] zurücksetzen“ oder „Auf Werkseinstellungen zurücksetzen“.

Als weitere Optimierung lassen sich alle Standardpfade von Libre Office, etwa für temporäre Dateien oder für automatische Sicherungskopien, über den Menüpunkt „Extras → Optionen → LibreOffice → Pfade“ in andere Ordner verlagern, die schneller zugänglich sind oder auf einem schnelleren Datenträger liegen. ■

Terminal- und Bash-Optimierung

Das Gnome-Terminal und die darin laufende Kommando-Shell bieten reichliche Optionen, um sie optisch und funktional zu optimieren. Das ist zum Teil einfach, zum Teil knifflig. Die notwendigen Tipps finden Sie hier.



VON HERMANN APFELBÖCK

Ohne Terminalbenutzung werden Sie mittelfristig nicht durch Linux (Mint) kommen. Es kommt unvermeidlich die Situation, wo Sie rekursiv Dateirechte ändern müssen, manuelles Kopieren durch rationales Rsync- oder Tar-Backup ersetzen wollen oder nur noch auf die Textkonsole des Systems gelangen. Und wer nicht nur ein Desktop-Mint, sondern auch einen Linux-Datenserver nutzen will, kommt ohne Terminal via SSH schon gar nicht aus. Dieser Artikel zeigt alle wichtigen Optionen, um das grafische Terminal, aber auch die virtuellen Konsolen und die SSH-Konsole komfortabel einzurichten. Punkt 1 bezieht sich ausschließlich das grafische Terminalfenster. Alle anderen Punkte 2 bis 5 zur Bash-Optimierung gelten auch für SSH und für die Konsolen (Strg-Alt-F1 und weitere). Bei den grafischen Terminalemulatoren nehmen wir das Gnome-Terminal als Referenz, wie es in der Hauptedition von Linux Mint zum Einsatz kommt. Das Mate-Terminal und das Xfce4-Terminal bieten ganz ähnliche Einstellungen, aber nicht immer an gleicher Stelle. Bei der Shell selbst, also dem eigentlichen Kommandointerpreter, ist überall die Bash-Shell Standard.

Dieser Beitrag kann keine Einführung in die Bash-Befehle leisten, sondern konzentriert sich auf den Bedienkomfort des Terminals. Beachten Sie in diesem Zusammenhang den Hefteinleger mit seiner Übersicht der wichtigsten Terminalkommandos.

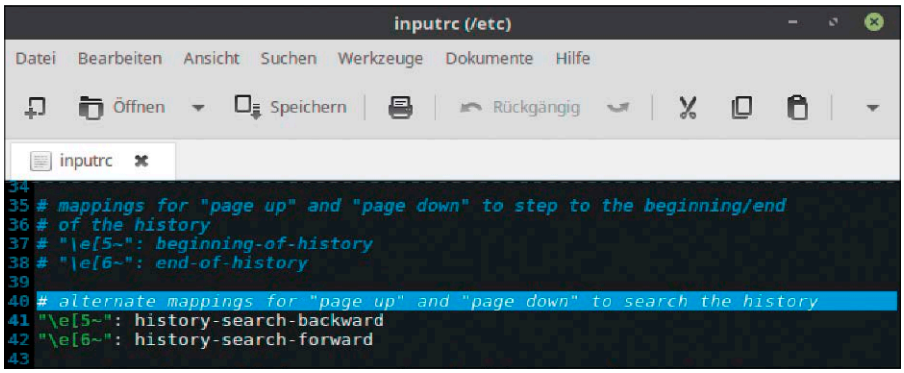
1. Das grafische Terminal

Terminalemulatoren sind grafische Programme mit zahlreichen Einstellungen. Sie sind unabhängig von der Shell, die im Terminal läuft. Die Optionen und Optimierungen, die Sie im grafischen Terminal vornehmen, haben daher mit der Bash-Shell zunächst nichts zu tun. Lediglich bei Farbeinstellungen für das grafische Terminal und solchen für die Bash-Shell gibt es Kombinationen, welche die Lesbarkeit fördern – oder eben nicht.

Insbesondere engagierte Nutzer, die sich das Terminal optisch bestmöglich einrichten möchten, sollten sich beim Aussehen des grafischen Terminals farblich festlegen, bevor sie Ausgabefarben und Prompt der Bash-Shell optimieren.

Einstellungen und Profile: Das Gnome-Terminal zeigt im Menü „Bearbeiten“ die Untermenüs „Einstellungen“ und „Profileinstellungen“. Beides sind benutzerspezifische Optionen: Was unter „Einstellungen“ festgelegt wird, gilt für jedes Terminal im aktuellen Benutzerkonto. Die „Profileinstellungen“ erlauben darüber hinaus verschiedene Layouts, die man entweder im Gnome-Terminal selbst mit „Terminal → Profil wechseln“ umschalten kann. Verschiedene Profile sind unnötiger Luxus, jedoch sollten Sie das als „Unbenannt“ betitelte Standardprofil unter „Bearbeiten → Profileinstellungen“ in jedem Fall bearbeiten. Die Registerkarte „Allgemein“ bestimmt die Größe des Terminalfensters über die Spaltenzahl (Breite) und Zeilenzahl (Länge) sowie die verwendete Schriftart. Beachten Sie, dass Sie das Terminalfenster unabhängig von der Schrift jederzeit mit Strg-+ und Strg-- skalieren können. Die Registerkarte „Farben“ definiert die Farb- und Transparenzeinstellungen. Wer Experimente mit eventuell kontrastarmen Ergebnissen vermeiden will, sollte bei den

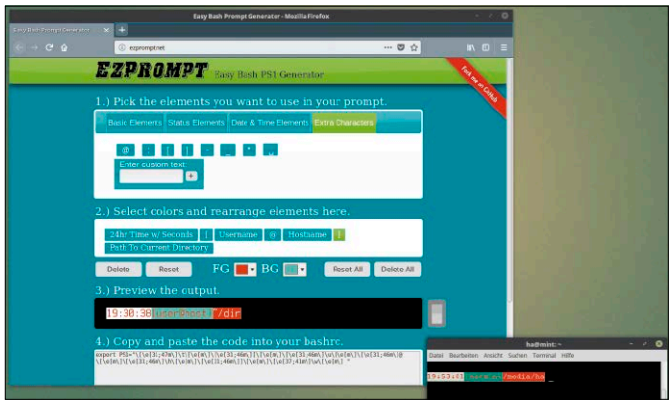
Vorgaben bleiben („Integrierte Schemata“) wie etwa „Schwarz auf hellgelb“ oder „Grün auf schwarz“.
Unter „Bildlauf“ sollte der „Zeilenpuffer“ deutlich vierstellig eingestellt sein, damit Sie auch bei umfangreichen Dateilisten (find, ls, rsync) bis zum Beginn der Ausgabe zurückblättern können.
Der allgemeinere Punkt „Bearbeiten → Einstellungen“ spielt für die Terminaloptik keine Rolle. Hier können Sie aber unter „Tastenkürzel“ die Hotkeys ermitteln oder neu bestimmen, die in Ihrem Terminal gelten. Der Tipp, hier auch die Hotkeys für Kopieren (Strg-Umschalt-C) und Einfügen (Strg-Umschalt-V) auf gebräuchliches Strg-C und Strg-V umzustellen, ist zweischneidig, weil Strg-C in der Bash-Shell traditionell für den Abbruch des aktuellen Befehls reserviert ist.



Historyfilter: Mit dieser Einstellung in der Datei „/etc/inputrc“ filtert die Bash nach Bild-oben/Bild-unten die Einträge, die mit dem bereits eingegebenen Teilbefehl übereinstimmen.

2. Bash-Zeileneditor und History

Kaum ein Terminalthema klingt langweiliger als die Regeln des „line editing“ – also Texteingabe, Textbearbeitung, Autovervollständigung und Befehlssuche am Bash-Prompt. Es entscheidet aber fundamental darüber, wie viel oder wenig Sie tippen müssen – und „Tippen“ bedeutet hier ja nicht das Schreiben von natürlicher Sprache, sondern von oft komplexen Befehlen. Eine Abkürzung hier vorab, da diese nachfolgend häufig erscheint: Die Tilde „~“ ist für die Bash-Shell die Variable für das Home-Verzeichnis des angemeldeten Kontos („/home/[kontoname]“). Die wichtigste Initialisierungsdatei bei jedem Terminalstart ist „~/.bashrc“, also „/home/[kontoname]/.bashrc“).



Diese Seite erspart das Hantieren mit den unzugänglichen Farbcodes: Auf *http://ezprompt.net/* stellen Sie sich die Basis des Bash-Prompts per Mausklicks zusammen.

Autocompletion: Lange Dateinamen müssen nicht getippt werden: Wenn Sie die ersten zwei, drei Buchstaben eingeben und dann die Tab-Taste drücken, ergänzt das Terminal den vollständigen Namen automatisch, desgleichen Ordnerpfade, sofern die eingegebenen Buchstaben stimmen (Groß- und Kleinschreibung beachten!).
History: Das Terminal vergisst nichts – jedenfalls nicht so schnell. Die Befehle werden im Speicher sowie dauerhaft in der „~/.bash_history“ gespeichert. Dafür die Befehle über Sitzungen und Neustarts hinaus gesammelt werden, sorgt diese Anweisung:

```
shopt -s histappend
```

Diese werden Sie in jeder Standardstartdatei „~/.bashrc“ antreffen. Bei welcher Zeilenmenge Schluss sein soll, also die ältesten Einträge gelöscht werden, bestimmen folgende Anweisungen:

```
HISTSIZE=5000
HISTFILESIZE=5000
```

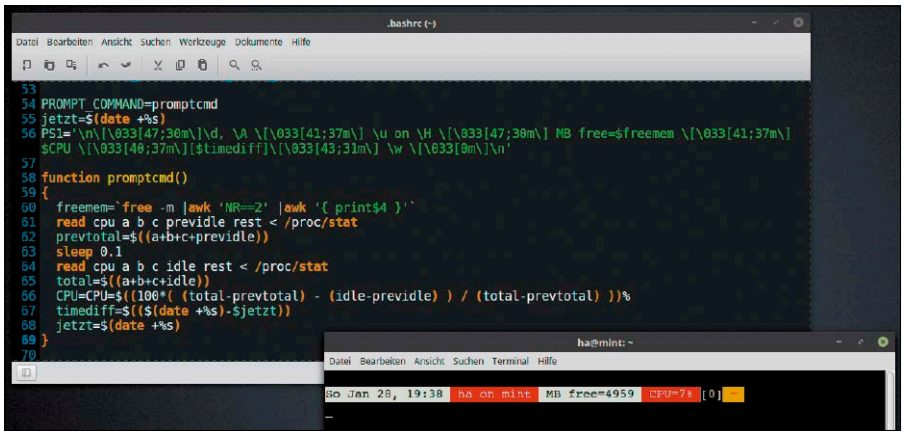
Auch diese stehen in jeder „~/.bashrc“, wenn auch eventuell mit geringeren Zeilenangaben. „HISTSIZE“ ist die maximale Zeilenmenge im Speicher, „HISTFILESIZE“ die maximale Zeilenmenge in der Datei „~/.bash_history“. Je höher die Zahlen, desto umfangreicher wird das Gedächtnis der Bash-Shell. Mit der Variablen

```
HISTCONTROL=ignoredups
```

können Sie verhindern, dass die History von Dubletten wimmelt: Bereits vorhandene identische Kommandos werden dann nicht aufgenommen.
Soviel zur Optimierung der History. Im praktischen Alltag gibt es mehrere Möglichkeiten. Fast jedem Anwender bekannt ist das Zurückblättern zu den letzten Kommandos mit der Taste Cursor-oben, die den gewünschten Befehl wieder auf den Prompt holt. Eine systematische Suche bietet der Hotkey Strg-R: Nach Eintippen etwa von „apt“ erscheint der letztgenutzte apt-Befehl in kompletter Länge. Ist dieser passend, kann er mit Eingabetaste sofort ausgeführt oder mit Alt-Eingabetaste zum Editieren auf den Prompt geholt werden. Ist der angezeigte Historytreffer nicht der passende, geht es mit Strg-R zum vorletzten und so fort.
Eine nützliche Ergänzung zur Rückwärtssuche mit Strg-R ist eine Filtersuche mit der Taste Bild-oben. Nach Eingabe etwa von *apt* befördert diese Taste den letzten kompletten apt-Befehl direkt auf den Prompt, ein weiteres Bild-oben den vorletzten und so fort. Diese Suche funktioniert aber nur, wenn Sie Bild-Tasten entsprechend belegen – und zwar in der Datei „/etc/inputrc“. Das Editieren erfordert root-Recht (*sudo xed /etc/inputrc*). Sie werden dort die beiden Zeilen

```
\"e[5~\": history-search-backward
\"e[6~\": history-search-forward
```

antreffen und müssen nur das führende Kommentarzeichen „#“ entfernen.
Zum Editieren vorhandener Zeilen, seien es selbst getippte oder aus der History gefischte, helfen Lösch- und Rücktaste, Pos1, Ende, Strg-Cursor-rechts/links (wortweise springen), Strg-K und Strg-U (Löschen nach und vor der Cursorposition, siehe dazu auch Punkt 4).



Hübsche Prompts sind hartes Handwerk. Ein funktionaler Prompt liefert aber automatisch Informationen, für die Sie sonst externe Systemwerkzeuge starten müssten.

3. Farben am Prompt und in Dateilisten

Der Prompt, also die Anzeige bei jeder Befehlseingabe, kann beliebige statische und dynamische Informationen anbieten. Die Promptanzeige definieren Sie temporär mit dem Befehl „PS1='...'". und dauerhaft in der Datei „~/.bashrc". Einige dynamische Variablen wie das aktuelle Verzeichnis, Datum oder Uhrzeit bietet der Prompt durch vordefinierte Escape-Zeichenfolgen selbst an, etwa „\w" für das aktuelle Verzeichnis, „\u" für das angemeldete Konto oder „\h" für den Rechnernamen. Einfache Prompts sehen dann so aus:

```
PS1="\w => "
PS1="\u@\h:\w => "
```

Eine gute Infoquelle für alle Promptoptionen ist die Seite *https://wiki.archlinux.de/title/Bash-Prompt_anpassen*. Über die eingebauten Codes hinaus können Sie jede allgemeine oder selbst definierte Variable einfach mit „$Variable" in die PS1-Definition setzen:

```
PS1="\w [$LOGNAME] => "
```

Um Infos gegeneinander abzugrenzen, sind ferner Farbdefinitionen vorgesehen, die stets mit der Sequenz „\[\033" starten. Ein Prompt wie

```
PS1="\n\[\033[47;30m\]\d, \A \
  [\033[41;37m\] \u on \H \
  [\033[47;30m\] MB free=$freemem \
  [\033[41;37m\] $CPU \
  [\033[40;37m\] [$timediff] \
  [\033[42;30m\] \w \[\033[0m\]\n"
```

ist aber praktisch unlesbar. Immerhin geht es Schritt für Schritt von einer Escape-Sequenz zur nächsten – „\n" bedeutet einen Zeilenumbruch, „\[\033" schaltet dann die Farben um, „\d" setzt das Datum ein, „\A" die Uhrzeit. Erläuternder Text oder Zeichen wie Komma oder Blank sind an jeder Stelle möglich, ferner auch Variablen mit „$". Wichtig ist, Farbdefinitionen am Ende wieder zurückzusetzen („\[\033[0m\]").

Easy Bash PS1 Generator: Bei den unsäglichen Farbsequenzen sollten Sie sich helfen lassen: Auf der Seite *http://ezprompt.net/* können Sie von ersten Position zur letzten durchgehen, was der Prompt zeigen soll. Dabei bestimmen Sie für das jeweils markierte Element Vorder- und Hintergrundfarbe („FG" und „BG"). Im untersten Feld erscheint dann der resultierende Code für die PS1-Variable, den Sie einfach kopieren, im Terminal einfügen und testen. Wenn das Ergebnis passt, übernehmen Sie diese Codezeile in Ihre Datei „~/.bashrc". Die Webseite deckt zwar längst nicht alle Möglichkeiten des Bash-Prompts ab, liefert aber die heiklen Farbcodes.

Dynamische Infos durch Prompt_Command: Wenn Variablen echtzeitaktuell im Prompt landen sollen (etwa die CPU-Auslastung), dann muss diese Variable unmittelbar vor der Promptdarstellung ermittelt werden. Dafür bietet die Bash einen speziellen Service: Mit

```
PROMPT_COMMAND=[function-name]
```

definieren Sie eine Funktion der Datei „~/.bashrc", die bei jedem Befehl in der Kommandozeile abgerufen wird. Da dies häufig geschieht, sollten Sie den Rechenaufwand in Grenzen halten. Ein Beispiel für einen selbst gebauten Prompt mit Echtzeitinfos aus einem Prompt_Command sehen Sie in der Abbildung auf dieser Seite. Den Code können Sie auch der Datei „bashrc" entnehmen, die wir auf *https://paste.ubuntu.com/p/cdBxTdvFgz/* bereitgestellt haben.

Farbige Dateien und Ordner: Das Terminal stellt Dateitypen und Ordner standardmäßig in unterschiedlichen Farben dar. Wenn Sie bestimmte Farben ändern möchten, erstellen Sie mit folgendem Befehl eine persönliche Konfigurationsdatei im Home-Verzeichnis:

```
dircolors -p > ~/.dircolors
```

Die versteckte Datei „.dircolors" können Sie dann mit einem beliebigen Editor bearbeiten. So werden zum Beispiel Ordnernamen gelb gefärbt:

```
DIR 01;33
```

Die Einstellungen dieser eigenen Farbtabelle dominieren über die Standardeinstellungen. Die Farbcodes können Sie der Seite *https://wiki.archlinux.de/title/Bash-Prompt_anpassen* entnehmen. Achten Sie auf die Tatsache, dass solche Farbdefinitionen durch Umstellen der allgemeinen Terminalfarben (siehe Punkt 1) unter Umständen unlesbar werden. Wer hier Zeit investiert, sollte an der allgemeinen Terminaloptik nichts mehr verändern.

4. Bash-Aliases und Bash-Hotkeys

Ohne in das Bash-Scripting einzusteigen, können einfachste Alias-Kurzbefehle und Bind-Hotkeys die Effektivität der Bash-Shell enorm steigern.

Bash-Hotkeys: Mit Tastendefinitionen sollte man sparsam umgehen, damit der Durchblick nicht verlorengeht, jedoch sind einige Nachbesserungen produktiv. So ist etwa beim Editieren am Prompt zwar das Löschen vor und nach der Cursorposition mit den Hotkeys Strg-U und Strg-K vorgesehen, aber nicht das Löschen der kompletten Zeile mit einem Hotkey. Folgendes Bind-Kommando

```
bind '"\C-l":kill-whole-line'
```

legt den internen Befehl „kill-whole-line" auf den Hotkey Strg-L. Die Strg-Taste ist mit „\C" einzugeben.

Folgender Befehl

```
bind '"\e[15~":"xdg-open . \n"'
```

belegt die Funktionstaste F5 so, dass sie im aktuellen Verzeichnis den Dateimanager startet. Die Funktionstasten sind mit „\e[nn~" anzugeben, wobei die Ziffer „nn" in der Regel den Wert plus 10 der tatsächlichen Taste benötigt. Im Zweifel kann der Befehl „read" und anschließendes Drücken der Funktionstaste über die Ziffer „nn" informieren.

Bind-Befehle können Sie interaktiv ausprobieren. Sie gelten bis zum Schließen des

Terminals. Für permanente Gültigkeit benötigen Sie einen Eintrag in der „~/.bashrc“.

Aliases: Kurzbefehle sorgen für schnelle Ordnernavigation oder vereinfachen komplexe Befehle. Der Platz für Aliases ist wieder die Datei „~/.bashrc“,und die Befehle werden in einfachsten Fällen so aussehen:

```
alias ini='xed ~/bashrc'
alias mc='mc /srv/dev-disk-by-
 label-Data /srv'
alias ll='ls -alF --group-
 directories-first'
```

Aliases entschärfen die interaktive Nutzung mächtiger Terminaltools erheblich. Ein Beispiel ist etwa folgendes Alias für den Find-Befehl:

```
alias fn='read -p "Dateimaske (z.B.
 *.pdf): " TMP; find . -type f -name
 "$TMP"'
```

Nach Aufruf des Kürzels „fn“ werden Sie mittels „read“ nach der Dateimaske gefragt, die dann etwa „*.odt“ oder auch „2018*.jpg“ lauten kann (ohne Anführungszeichen). Diese Eingabe wird mit der Variable „$TMP“ an find weitergereicht. Das Alias geht davon aus, dass man zuerst in das gewünschte Verzeichnis gewechselt hat, denn dort (Punkt nach „find .“) startet find die Suche. Ähnlich übergibt

```
alias ft='read -p "Alter in Tagen
 (z.B. 7): " TMP; find . -type f
 -mtime "-$TMP"'
```

die Variable „$TMP“ eine Zahl an find, das dann über den Schalter „-mtime“ alle Dateien ermittelt, die in den letzten Tagen erstellt wurden.

5. Ordnernavigation im Terminal

Verzeichniswechsel mit cd gehören zu den häufigsten Kommandos. Auch hier gibt es eine Reihe kleiner Optimierungen.

1. Die häufigsten Zielordner sind am besten über ein knappes Alias zu erreichen, um etwa nach

```
alias d='cd ~/Schreibtisch'
```

mit der Eingabe „d“ zum Desktop zu gelangen.

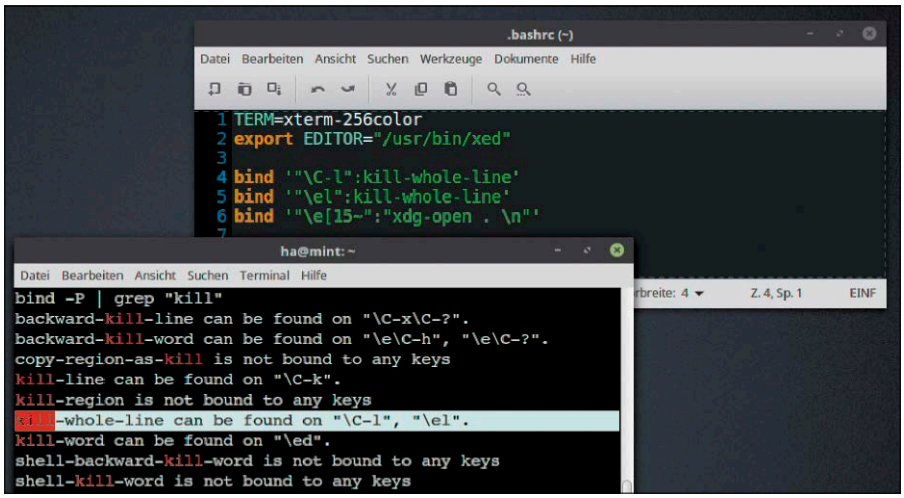
2. Eine hübsche Lösung für schnelles Springen in wichtige Verzeichnisse ist die Variable „CDPATH“. In ihr lassen sich mehrere Ordnerpfade speichern. Danach kann man überall mit „cd [Verzeichnis]“ in ein Unterverzeichnis eines der gespeicherten Verzeichnisse springen. Um also etwa den Pfad „/var/www/html“ in die Variable „CDPATH“ aufzunehmen, geben Sie

```
export CDPATH='.:/var/www/html/'
```

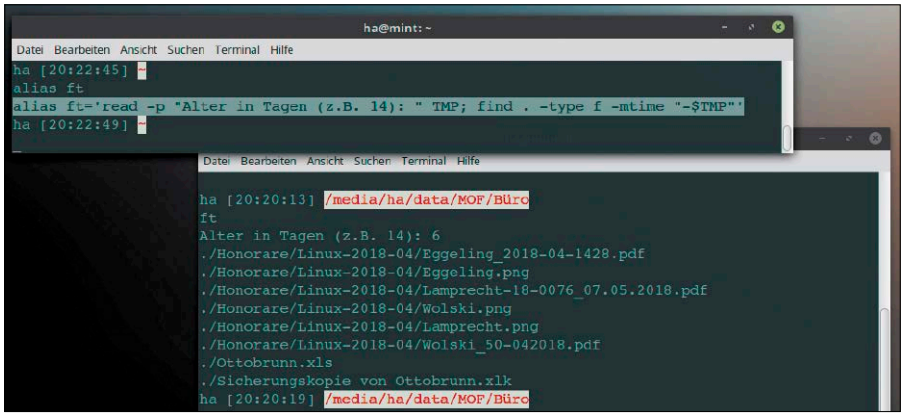
ein. Danach wechseln Sie von beliebiger Stelle mit *cd htdocs* und *cd logs* in Unterordner von „/var/www/html/“. Die CDPATH-Variable lässt sich durch eine beliebige Anzahl weiterer Verzeichnisse erweitern – jeweils durch Doppelpunkt getrennt:

```
export CDPATH='.:~:/var/www/
 html/:/media/985c9fb3-14a6-449e-
 bec5-4666a283fbf4/'
```

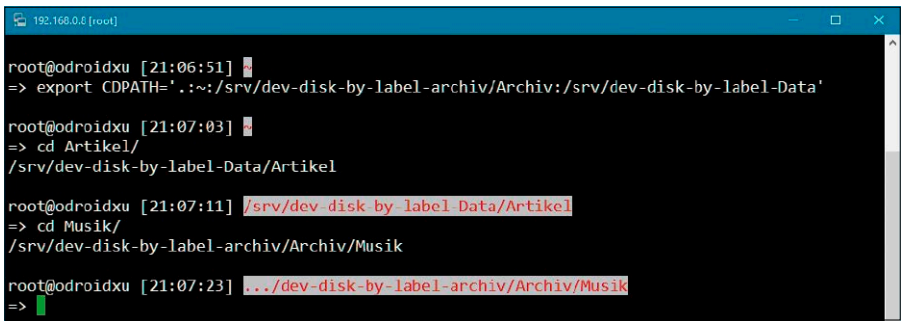
Hier besteht der „CDPATH“ aus dem aktuellen Verzeichnis („.“), dem Home-Verzeichnis („~“), dem Webserver-Verzeichnis und einem Mountordner. Am Anfang sollte mit „.:“ immer das aktuelle Verzeichnis stehen, damit dieses immer die höchste Priorität behält. Für einen dauerhaften „CDPATH“ müssen Sie die Exportanweisung in die Datei „~/.bashrc“ eintragen. ■



Hotkeys für die Bash-Shell: Mit bind können Sie Tasten und Tastenkombinationen neu definieren und Programme auslösen. „bind -P“ informiert über aktuelle Belegungen.



Weniger tippen und nicht über die Syntax nachdenken: Alias-Definitionen machen komplexe Bash-Kommandos – wie hier find – deutlich komfortabler.

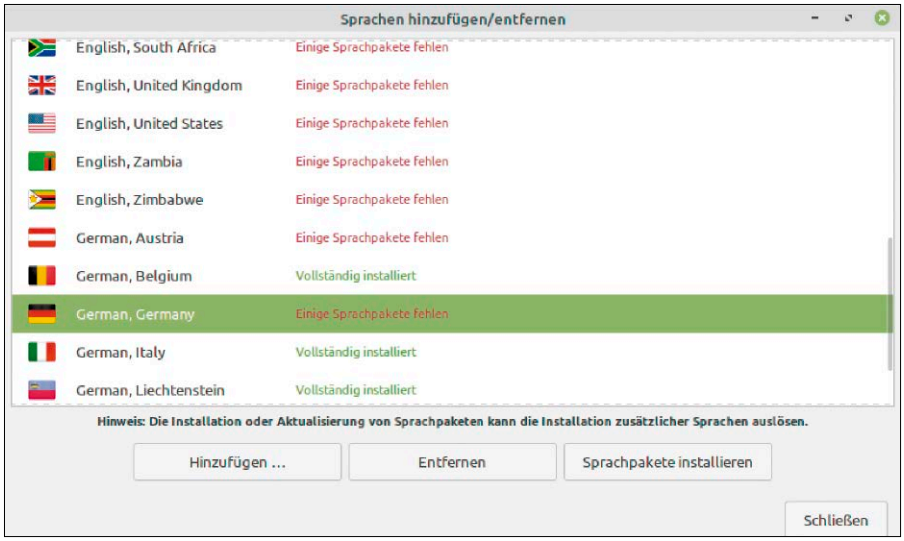


Effiziente Navigationshilfe: Einträge wichtiger Verzeichnisse in die Variable „CDPATH“ erlauben den direkten Ordnerwechsel quer über Verzeichnisstruktur und Laufwerke.

Alles Deutsch? Zeit, Sprache & Tastatur

Linux-Systeme sind in vielen Ländern und Sprachen heimisch. Mit ein paar Mausklicks stellen Sie eine andere Sprache für Desktop und Anwendungen ein oder Sie ändern die Tastaturbelegung.

VON THORSTEN EGGELING



Sprachpakete für Linux Mint: Oft ist die Sprachunterstützung nicht vollständig installiert. Nach der Linux-Installation sollten Sie daher die Konfiguration prüfen und fehlende Pakete nachinstallieren.

Die Linux-Basissprache ist Englisch und nicht jedes Programm zeigt sich auch mit einer deutschsprachigen Oberfläche. Meistens lässt sich das ändern, indem man ein passendes Sprachpaket nachinstalliert. In Einzelfällen kann es aber auch sinnvoll sein, das System oder ein einzelnes Programm auf Englisch umzustellen, etwa um eine englischsprachige Fehlermeldung zu erhalten. Eine Internetsuche danach liefert oft bessere Ergebnisse.

Die Zeitzone legen Sie bereits bei der Installation fest. Davon hängen beispielsweise auch die Regionaleinstellungen wie Datumsformat und Währung ab. Bei Bedarf lässt sich die Zeitzone ändern, etwa wenn Sie sich gerade im Ausland befinden. Probleme beziehungsweise Abweichungen bei der Uhrzeit kann es geben, wenn Sie mehrere Betriebssysteme auf dem Rechner verwenden. Die korrekte Uhrzeit ist aber wichtig, etwa für Updates oder die Anmeldung bei Websites, insbesondere bei der Zwei-Faktor-Authentifizierung etwa über die Smartphone-App Google Authenticator.

Spracheinstellungen kontrollieren

Nach einer Linux-Neuinstallation sollte der erste Weg in die Spracheinstellungen führen. Auch wenn die Sprache bereits bei der Installation festgelegt wird, sind oft nicht alle Sprachpakete für die aktivierten Sprachen installiert.

Unter Ubuntu 20.04 rufen Sie die „Einstellungen“ nach einem Mausklick auf den rechten Bereich der Leiste oben auf dem Bildschirm auf. Gehen Sie auf „Region und Sprache“ und klicken Sie auf „Installierte Sprachen verwalten“. Ubuntu sucht automatisch nach fehlenden Sprachpaketen und bietet deren Installation an.

Meist fehlen jedoch keine deutschen Sprachpakete, sondern englischsprachige. Die kommen in der Regel allerdings nicht zum Einsatz. Es kann aber vorkommen, dass bei einem Softwareupdate das deutsche Sprachpaket noch nicht verfügbar ist. Ubuntu aktualisiert dann die Software und das englische Sprachpaket. Das Programm startet mit einer englischsprachigen Oberfläche, bis auch ein Update für das deutsche Sprachpaket bereitsteht. Bei anderen Linux-Distributionen finden sich entspre-

Sprachpakete für Ubuntu: Ubuntu signalisiert fehlende Sprachpakete in einem eigenen Dialog. Meist fehlen nur Pakete für andere Sprachen als Deutsch, die Sie aber trotzdem installieren sollten.

chende Einstellungen, je nach verwendetem Desktop. In Linux Mint 20 Cinnamon beispielsweise gehen Sie im Menü auf „Einstellungen → Sprachen“ und klicken auf „Sprachen hinzufügen/entfernen“. Wenn hinter „German, Germany“ die Angabe „Einige Sprachpakete fehlen“ steht, klicken Sie die Zeile an und dann auf die Schaltfläche „Sprachpakete installieren“.

Spracheinstellungen ändern

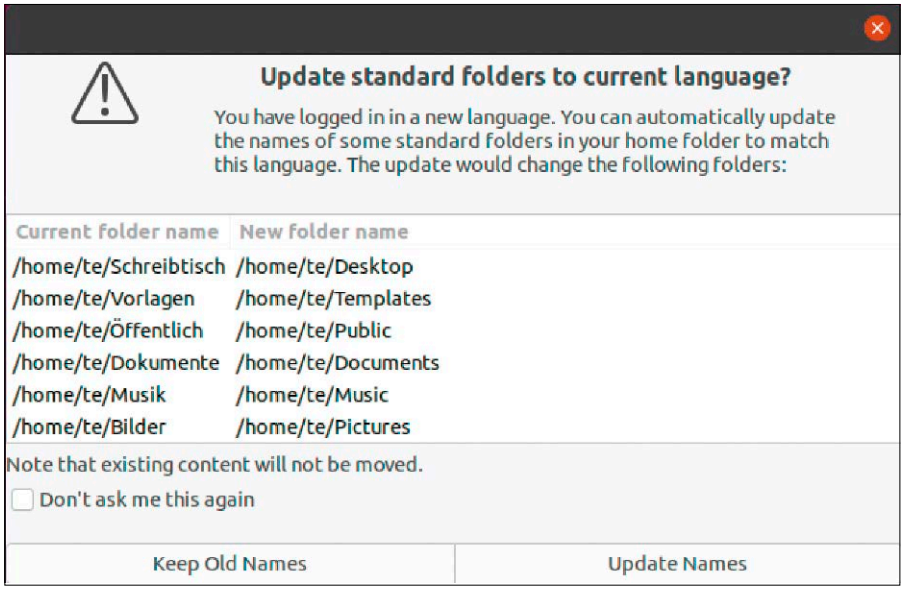
Die bei der Linux-Installation gewählte Sprache gilt systemweit und für alle Benutzerkonten. Wer etwas ändern möchte, geht unter Ubuntu 20.04 in den „Einstellungen“ auf „Region und Sprache“. Es öffnet sich das Fenster „Sprachen“, in dem man auf „Installierte Sprachen verwalten“ klickt. Unter „Sprache für Menüs und Fenster“ sind bei einer deutschsprachigen Ubuntu-Standardinstallation die Einträge „Deutsch (Deutschland)“, „English (United Kingdom)“ und „English“ zu sehen.

Die erste Sprache in der Liste ist der Standard für die Benutzeroberfläche. Sollte für ein Programm kein deutsches Sprachpaket vorhanden sein, verwendet es der Reihe nach die anderen Sprachen aus der Liste. Der letzte Eintrag ist immer „English“. Einträge darunter sind ausgegraut und werden ignoriert. Bei Bedarf lässt sich die Reihenfolge ändern, indem Sie eine Sprache mit der Maus an eine andere Position ziehen.

Die Einstellungen unter „Sprache für Menüs und Fenster“ gelten nur für den gerade angemeldeten Benutzer. Andere Benutzer des Systems können daher ihre eigenen Sprachpräferenzen festlegen. Änderungen werden erst wirksam, nachdem sich der Benutzer ab- und wieder angemeldet hat oder Linux neu gestartet wurde.

Per Klick auf „Systemweit anwenden“ übernehmen Sie die Spracheinstellungen für alle Benutzer sowie für den Start- und Anmeldebildschirm. Dafür ist das Passwort des Systemverwalters erforderlich. Ein Standardbenutzer kann diese Einstellung nicht ändern, aber für sein eigenes Konto eine beliebige Sprache wählen.

Die Umstellung der Sprache kann Auswirkungen auf einige Ordnernamen haben. Wenn Sie beispielsweise die Standardsprache auf „English (United States)“ ändern, fragt Ubuntu bei der nächsten Anmeldung, ob Sie die lokalisierten Bezeichnungen verwenden wollen. Wenn Sie auf „Update Names“ klicken, werden die Ordnernamen angepasst und leere Ordner gelöscht. Der Inhalt der bisherigen Ordner wird nicht verschoben. Das müssen Sie selbst erledigen und danach die nicht mehr benötigten Ordner löschen. Alternativ klicken Sie auf „Keep Old Names“, wenn Sie die deutschsprachigen Bezeichnungen behalten möchten. Auf Anwendungen hat das keine Auswirkungen. Dialoge wie „Datei öffnen“ oder „Datei speichern“ zeigen bei jeder Sprache automatisch einen passenden Ordner wie „Dokumente“ oder „Documents“, je nachdem, was vorhanden ist.



Sprachumstellung: Die Namen der Standardordner lassen sich für die jeweilige Sprache anpassen. Meist ist es besser, die bisherigen Namen zu behalten, damit Inhalte nicht verschoben werden müssen.

Im Fenster „Sprachen“ lassen sich auf der Registerkarte „Regionale Formate“ weitere Anpassungen vornehmen. Die Anzeige von Zahlen, Datumsangaben und Währungen erfolgt unabhängig von der Sprache der Oberfläche und kann hier geändert werden. Die Einstellungen gelten für den aktuellen Nutzer, nach einem Klick auf „Systemweit anwenden“ für alle Benutzerkonten.

Linux Mint 20 Cinnamon: „Einstellungen → Sprachen“ führt zum Fenster „Spracheinstellungen“, in dem Sie für „Sprache“, „Region“ und „Zeitformat“ jeweils eine andere

SPRACHEN UND ÜBERSETZUNGEN FÜR LINUX

Die meisten Programme und Tools unter Linux unterstützen mehrere Sprachen. In der ausführbaren Datei ist meist nur Englisch als Standardsprache enthalten. Die Sprachdateien mit den Übersetzungen werden je nach Spracheinstellung dynamisch geladen, wofür meist das Gettext-Framework zum Einsatz kommt.

Sprachdateien mit der Endung „.mo“, die in den einzelnen Programmpaketen enthalten sind, liegen in der Regel unterhalb von „/usr/share/locale“ in Ordnern mit der jeweiligen Länderkennung. „mo“-Dateien für Systemtools und die Desktopumgebungen werden über Sprachpakete installiert, beispielsweise „language-pack-[Länderkennung]“, „language-pack-gnome-[Länderkennung]“ „language-pack-kde-[Länderkennung]“. Die Datei liegen unter „/usr/share/locale-langpack“.

Für einige Anwendungen, beispielsweise Firefox, Thunderbird und Libre Office gibt es eigene Sprachpakete, beispielsweise „firefoce-locale-de“ oder „libreoffice-l10n-en-gb“.

In der Regel werden alle Sprachpakete automatisch installiert, wenn Sie eine neue Sprache hinzufügen. Sollte ein Programm nicht in der gewünschten Sprache erscheinen, sehen Sie nach, ob das zugehörige Pakete tatsächlich installiert ist und ob es dieselbe Versionsnummer trägt.

Sprache einstellen können. Nach einem Klick auf „Systemweit anwenden“ gelten die Einstellungen für alle Benutzer und den Anmeldebildschirm. Auch bei Linux Mint kann jeder Benutzer die eigenen Spracheinstellungen individuell ändern. Bei Standardbenutzern sind die Schaltflächen „Systemweit anwenden“ und „Sprachen hinzufügen/entfernen“ im Fenster „Spracheinstellungen“ nicht sichtbar.

Tastaturbelegung ändern

Die Belegung der Tastatur lässt sich bei Ubuntu 20.04 in den „Einstellungen“ unter „Region und Sprache“ unabhängig von der Sprache konfigurieren. Unterhalb von „Eingabequellen“ fügen Sie über die „+“-Schaltfläche weitere Belegungen hinzu. Die erste Sprache ist der Standard. Die Reihenfolge lässt sich per Klick und Ziehen mit der Maus ändern.

Rechts neben jedem Eintrag in der Liste befindet sich eine Schaltfläche mit einem Augen-Symbol. Nach einem Klick darauf erscheint ein Schema mit der zugehörigen Tastaturbelegung. Die meisten Tasten sind vierfach belegt. Die linke Spalte bei jeder Taste zeigt die Zeichen in Kombination mit der Shift-Taste, die rechte Spalte die zusammen mit der Alt-Gr-Taste (Super R).

Klicken Sie rechts neben „Eingabequellen“ auf die Schaltfläche mit dem Zahnradsymbol. Wählen Sie die Option „Verschiedene Quellen für jedes Fenster erlauben“, wenn Sie die Tastatur für unterschiedliche Fenster getrennt einstellen möchten. Die Eingabequelle lässt sich über das Menü der Schaltfläche mit dem Sprachkürzel am oberen rechten Bildschirmrand ändern.

Linux Mint 20 Cinnamon: Gehen Sie im Menü auf „Einstellungen → Tastatur“ und wechseln Sie auf die Registerkarte „Tastaturbelegungen“. Über die „+“-Schaltfläche fügen Sie weitere Sprachen hinzu, die Reihenfolge lässt sich über die Pfeil-Schaltflächen ändern. Im rechten Bereich des Fensters gibt es zwei Optionen. Sie können für alle Fenster die gleiche Tastaturbelegung verwenden oder unterschiedliche Belegungen für jedes Fenster. Die Umschaltung erfolgt über das Menü mit Landesflaggen in der Leiste am unteren Bildschirmrand.

Sprache im Terminal wechseln

Die bisher genannten Spracheinstellungen legen die Werte einiger Umgebungsvariablen fest. In einem Terminal (Strg-Alt-T) lassen Sie sich die Werte mit

```
locale
```

gefolgt von der Eingabetaste ausgeben. Bei einem deutschsprachigen Standardsystem enthalten alle LC_*-Variablen sowie „LANG“ den Wert „de_DE.UTF8“. „LANGUAGE“ besitzt den Wert „de_DE“ und „LC_ALL“ ist kein Wert zugewiesen. Die LC_*-Variablen sind für die unterschiedlichen Bereiche der Regionaleinstellungen zuständig.

Die Variablen lassen sich nutzen, um ein Programm schnell mit einer anderssprachigen Oberfläche zu starten oder die Sprache für nur ein Terminal zu ändern. Die Zeile

```
LANG=en_US.UTF-8 firefox
```

beispielsweise startet Firefox mit englischsprachiger Oberfläche. Programme im Terminal werten meist die Variable „LANGUAGE“ aus.

```
LANGUAGE=en_US.UTF-8 ping google.
 de
```

gibt Meldungen in englischer Sprache aus. Im Zweifelsfall verwendet man einfach beide Variablen:

```
LANGUAGE=en_US.UTF-8 LANG=en_US.
 UTF-8 gnome-terminal
```

Mit dieser Zeile öffnen Sie in neues Terminal, für das die geänderten Variablen gelten. Hier können Sie Programme mit grafischer Oberfläche oder Terminalprogramme starten und sehen Ausgaben in der angegebenen Sprache.

Schreibweisen: Variablen werden durchgehend in Großbuchstaben geschrieben, bei den Werten kann es unterschiedliche Schreibweisen geben. Der Befehl

```
locale -a
```

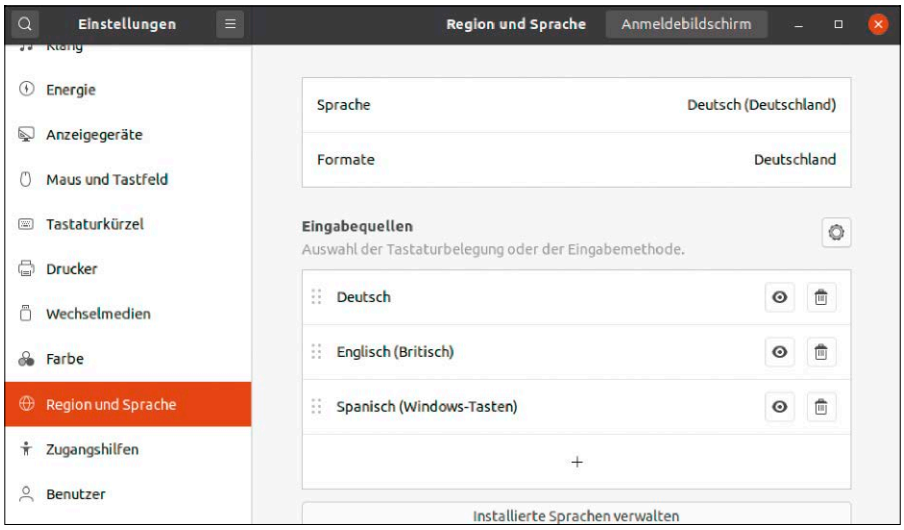
gibt Auskunft über die verfügbaren Locales. In der Ausgabe erscheint beispielsweise „en_US.utf8“, was als Wert für eine Variable ebenfalls gültig ist. Die durchgängige Kleinschreibung „en_us.utf8“ wird dagegen nicht akzeptiert.

Sprachunterstützung im Terminal einrichten: Eine Liste aller verfügbaren Locales ist in der Datei „/usr/share/i18n/SUPPORTED“ zu finden. Mit beispielsweise

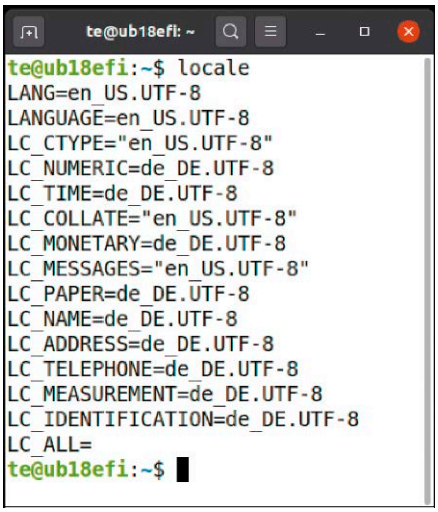
```
sudo locale-gen fr_FR.UTF-8
```

lässt sich eine neue Locale für Französisch erzeugen. Das wirkt sich jedoch nur auf Programme aus, für die bereits Sprachdateien vorhanden sind. Mit

```
sudo apt install language-pack-fr
```



Tastaturbelegung: Sie können mehrere Tastaturlayouts festlegen und die Belegung bei Bedarf schnell umstellen. Auf Wunsch funktioniert das auch für jedes Fenster individuell.



Umgebungsvariablen: Welche Spracheinstellungen gelten, wird über diese Variablen gesteuert. Programme lassen sich in einer anderen Sprache starten, indem Sie die Werte ändern.

installieren Sie beispielsweise das französische Sprachpaket.
Wer eine Sprache über die „Einstellungen“ und „Region und Sprache“ hinzufügt, muss keine Pakete manuell installieren. Die Einrichtung der Sprachunterstützung erfolgt dabei für Terminalprogramme und Desktopanwendungen automatisch.

Datum und Uhrzeit einstellen

Datum und Uhrzeit richten sich nach der Zeitzone, die Sie bei der Installation festgelegt haben. In den „Einstellungen“ lässt sich die Zeitzone bei Bedarf unter „Datum und Zeit“ ändern. Die Uhrzeit wird automatisch über einen NTP-Server (Network Time Protocol) synchronisiert, was eine Internetverbindung voraussetzt. Sollte die Uhrzeit zu stark abweichen, funktioniert das manchmal nicht. In diesem Fall setzen Sie unter „Datum und Zeit“ den Schalter hinter „Datum und Uhrzeit automatisch ermitteln“ auf „Aus“. Danach klicken Sie auf „Datum und Zeit“ und stellen die Uhr manuell ein. Anschließend setzen Sie den Schalter wieder auf „An“.
Bei Linux Mint 20 Cinnamon funktionieren die Zeiteinstellungen über „Einstellungen → Datum & Zeit“ entsprechend.
Wer auf einem Server beispielsweise über SSH die Zeit im Terminal korrigieren muss, verwendet diese drei Befehlszeilen:

```
timedatectl set-ntp false
timedatectl set-time "2020-10-10
 17:43"
timedatectl set-ntp true
```

Dies gilt für alle Systeme mit systemd (Debian, Ubuntu, Mint und viele mehr).

Uhrzeit bei Multiboot-Installationen

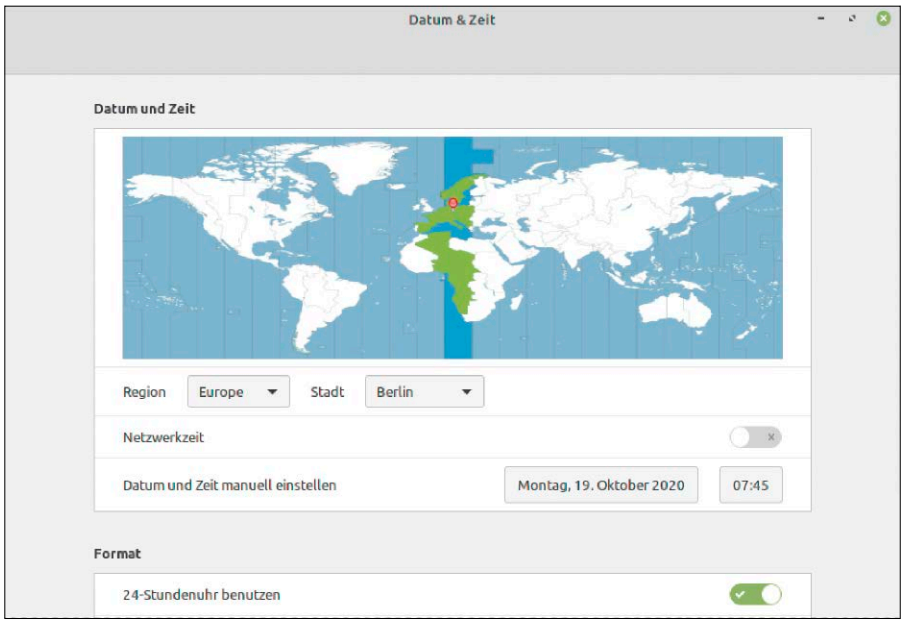
Datum und Uhrzeit erhalten Betriebssysteme von der Echtzeituhr auf der Hauptplatine (Real-Time Clock, RTC). Die Uhr geht meist nicht besonders genau, was die Synchronisierung mit einem NTP-Server erforderlich macht. Die korrigierte Uhrzeit wird auch an die Uhr auf der Hauptplatine übermittelt. Eine weitere Zeitkorrektur ist die Umstellung von Winter- auf Sommerzeit und wieder zurück. Dafür sorgt das Betriebssystem automatisch.
Linux und Windows interpretieren die Werte der Echtzeituhr auf der Hauptplatine unterschiedlich. Linux verwendet die koordinierte Weltzeit (UTC), Windows geht von der lokalen Zeit aus (Mitteleuropäische Zeit, MEZ, UTC+1). Zwischen beiden Zeitangaben liegen – je nach Sommer- oder Winterzeit – eine oder zwei Stunden. Im Terminal lässt sich mit

```
timedatectl
```

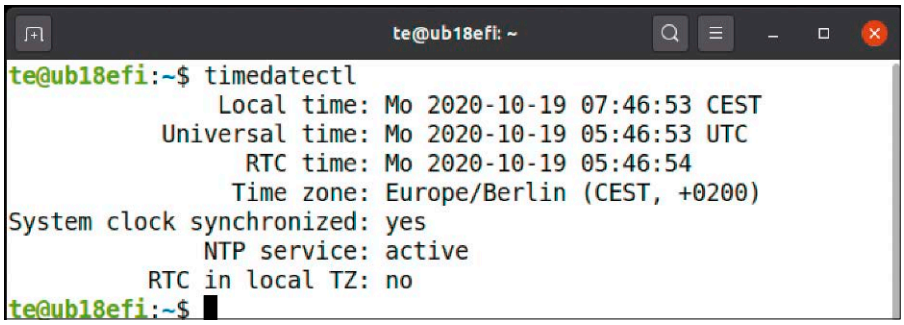
ermitteln, welche Zeiteinstellungen Linux verwendet. Steht hinter „RTC in local TZ:“ die Angabe „no“, basiert die Zeitangabe auf UTC.
Wenn Sie Windows starten, geht das System davon aus, das die Uhr auf UTC+1 eingestellt ist. Linux hat jedoch die UTC-Zeit eingestellt und die Uhr geht unter Windows eine Stunde oder bei Sommerzeit zwei Stunden nach. Windows korrigiert das mit einiger Verzögerung über NTP, was aber beim nächsten Linux-Start zu einer falsch eingestellten Uhr führt.
Zur Lösung des Problems können Sie unter Ubuntu oder Linux Mint das System mit

```
sudo timedatectl set-local-rtc 1
```

für die Verwendung der lokalen Zeit umstellen. Das hat jedoch den Nachteil, dass das System nicht mehr weiß, ob die Umstellung auf Sommer-/Winterzeit bereits erfolgt ist. Man muss dann erst auf den Abgleich mit dem Zeitserver warten, bis die korrekte Uhrzeit angezeigt wird.
Es erscheint daher sinnvoller, Windows UTC beizubringen. Dazu gehen Sie in der Registry auf „Hkey_Local_Machine\System\CurrentControlSet\Control\TimeZoneInformation“ und erstellen einen DWORD-Wert mit dem Namen „RealTimeIsUniversal“, den Sie auf „1“ setzen. Sollte Windows diesen nicht berücksichtigen, verwenden Sie einen QWORD-Wert.
Starten Sie Windows neu, öffnen Sie die „Einstellungen“ und gehen Sie auf „Zeit und Sprache → Datum und Uhrzeit“. Hier setzen Sie den Schalter unter „Uhrzeit automatisch festlegen“ auf „Aus“. ■



Uhrzeit einstellen (Linux Mint): Datum und Uhrzeit können Sie manuell ändern, nachdem Sie „Netzwerkzeit“ (NTP) deaktiviert haben. Die Zeitzone lässt sich hier ebenfalls wechseln.



Zeitquelle anpassen: Linux geht davon aus, dass die Hauptplatine die UTC-Zeit liefert. Wer parallel Windows nutzt, kann auch die lokale Zeit einstellen, um Konflikte zu vermeiden.

Sudo: Theorie & Praxis

Unter Linux ist sudo unentbehrlicher Standard. Sudo („Substitute user do“) ermöglicht den Wechsel zu anderen Benutzerkonten, in der Regel zu root, um (De-)Installationen, Dienste-verwaltung und Konfigurationsänderungen zu ermöglichen.

VON HERMANN APFELBÖCK

Wenn Systembenutzer alles dürften, könnten sie versehentlich beliebigen Schaden anrichten. Daher verbietet Linux standardmäßig praktisch alle Schreibzugriffe im Dateisystem außer unter „/home“ und „/tmp“. Für Installationen und Updates (unter „/usr“, „/opt“, „/snap“) sowie für Konfigurationseingriffe (hauptsächlich unter „/etc“) ist der explizite Einsatz von sudo erforderlich.

Sudo: Aufgabe und Reichweite

Um bei Bedarf root-Recht zu erhalten, genügt der Befehl „sudo“. Typisch ist etwa

```
sudo apt upgrade
```

zur Systemaktualisierung unter Debian/Ubuntu, wobei das eigene Kontokennwort erforderlich ist. Der obige Befehl entspricht genau genommen diesem Befehl:

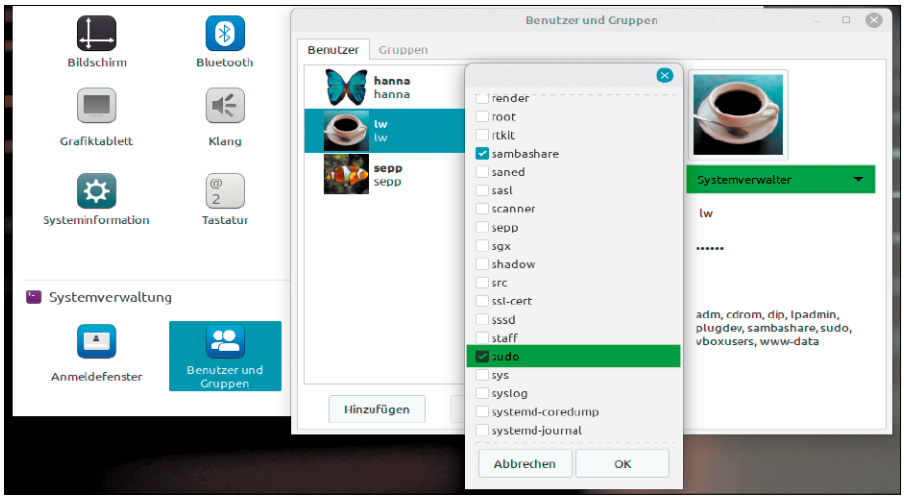
```
sudo --user=root apt upgrade
```

Es handelt sich um einen Wechsel in das root-Konto. Da dies der häufigsten sudo-Nutzung entspricht, darf die Kontenangabe bei root entfallen. Im Prinzip wechselt sudo aber auch zu beliebigen anderen Konten (hier die Kurzform statt „--user=sepp“):

```
sudo -u sepp bash
```

Das Prinzip von sudo ist der Benutzerkontensteuerung von Windows ähnlich: Der Systembenutzer soll nur dann mit root-Recht arbeiten, wenn dies zwingend notwendig ist. Das root-Konto selbst ist bei vielen Linux-Distributionen deaktiviert (unter anderem bei allen Ubuntus), damit Benutzer erst gar nicht in die Versuchung kommen, root als Standardkontext zu verwenden. Auch dies ist analog zu Windows und dem deaktivierten „Administrator“.

Linux ist aber ein Stück strenger als Windows: Erstens ist hier die Eingabe des Systemkennworts notwendig, während Windows nur einen „Ja“-Klick fordert. Zweitens



Wer „sudo“ darf, ist root und Systemverwalter: Alle anderen Berechtigungen sind letztlich sekundär und mit sudo bei Bedarf jederzeit einzufordern.

ist ein Systemkonto vom Typ „Standard“ generell nicht sudo-berechtigt. Das Konto muss den Typ „Systemverwalter“ verwenden, was eine Zugehörigkeit zur Gruppe „sudo“ impliziert. Genau genommen ist das Verhältnis von Systemverwalter und sudo ein-eindeutig: Der Kontotyp „Systemverwalter“ erhält immer sudo-Recht und sudo-Recht ist genau die Gruppenzugehörigkeit, die ein Konto zum Systemverwalter macht. Wenn Sie Systemverwalter-Konten in der grafischen Benutzerverwaltung (sofern vorhanden) oder mit

```
id sepp
```

abfragen, werden Sie neben „sudo“ weitere Gruppenzuweisungen finden (wie „adm“, „plugdev“, „sambashare“). Diese Gruppenrechte kann sich aber jedes Konto mit sudo-Recht bei Bedarf selbst besorgen:

```
sudo usermod -aG plugdev sepp
```

Letztlich ist es allein das sudo-Recht, was ein Konto zum Systemverwalter macht.

Konfigurationsdatei „/etc/sudoers“

Konten, Gruppen, root-Recht: Viele Desktopnutzer bekommen davon wenig zu sehen, denn das bei der Linux-Installation angelegte Erstkonto ist automatisch vom Typ „Systemverwalter“ mit sudo-Gruppenzugehörigkeit. Intimere Kenntnis kann aber den Benutzeralltag vereinfachen und ist spätestens nötig, wenn weitere Benutzerkonten angelegt werden sollen.

Die entscheidende Datei für die sudo-Nutzung ist „/etc/sudoers“, deren Bearbeitung natürlich ihrerseits root-Recht erfordert. Vor der ersten Bearbeitung dieser Datei empfiehlt es sich, mit

```
sudo cp /etc/sudoers /etc/sudoers.ori
```

eine Kopie des Originals anzulegen. Eine fehlerhafte „sudoers“ kann fatale Folgen haben, die Sie schlimmstenfalls über ein externes Livesystem und Wiederherstellen der Originaldatei beheben können.

Ein weiterer Standardtipp (auch in der „sudoers“-Datei selbst) ist die Editiermethode mit visudo. Statt eines Befehl wie *sudo nano /etc/sudoers* ist diese Methode die bessere:

```
sudo visudo
```

Visudo ist kein spezieller Editor, denn der Editor ist über Variablen oder mit

```
sudo update-alternatives --config
  editor
```

frei wählbar (in der Regel ist Nano voreingestellt). Vielmehr übergibt das Tool visudo den Inhalt der Datei als temporäre Datei an den Editor und macht nach dem Speichern im Editor einen Syntaxcheck (auch manuell möglich über *visudo -c*). Dies dient als Absicherung gegen fatale Fehler. Erst dann wird die eigentliche Systemdatei abgelegt.

Einige allgemeine Einstellungen in „/etc/sudoers" sind immer nützlich. Die zusätzliche Anweisung

```
Defaults pwfeedback
```

verhilft dazu, bei sudo-Kommandos die Eingabe des Systemkennworts durch Sternchen pro eingegebenem Zeichen zu beantworten. Dies erlaubt bessere Kontrolle der Eingabe. Eine weitere Anweisung im oberen Defaults-Bereich

```
Defaults timestamp_timeout=60
```

befreit für ganze 60 Minuten von der Eingabe des Systemkennworts bei sudo-Befehlen (Standard sind 15 Minuten). Beachten Sie aber, dass dies nur innerhalb eines laufenden Terminals gilt. Ein neu gestartetes Terminal wird angesichts von „sudo" das Kennwort erneut abfragen.

Die eigentlichen Konten- und Gruppenrechte (alle bezüglich sudo) sind anspruchsvoll. Die Zeile

```
root  ALL=(ALL:ALL) ALL
```

sollten Sie nie grundlos ändern, damit es nach *sudo* im root-Kontext keinerlei Beschränkungen gibt. Die diversen „ALL"s sind in aller Kürze als „Host=(Konto:Gruppe) Befehle" zu übersetzen und bleiben standardmäßig ohne Einschränkung.Eine naheliegende Idee, Ihrem Standardkonto etwa mit

```
sepp  ALL=(ALL:ALL) ALL
```

root-analoge Rechte zuzuweisen, ist nicht sinnvoll, weil die Gruppenrechte (Standard)

```
%sudo  ALL=(ALL:ALL) ALL
```

bereits dasselbe leisten, sofern „sepp" sudoberechtigt ist (Namen mit „%" wie „%sudo" sind stets Gruppenberechtigungen).

Ein einzelnes Systemkonto in die Datei einzutragen, kann aber durchaus sinnvoll sein. Damit wird es möglich, für ein sudo-berechtigtes Konto alle sudo-Kennwortabfragen abzuschalten:

```
sepp  ALL=(ALL:ALL) NOPASSWD: ALL
```

Diese reduzierten Kennwortabfragen lassen sich auch weniger radikal verfeinern:

```
sepp  ALL=(ALL:ALL) NOPASSWD: /usr/
 bin/apt, /usr/bin/apt-get, /usr/
 bin/systemctl
```

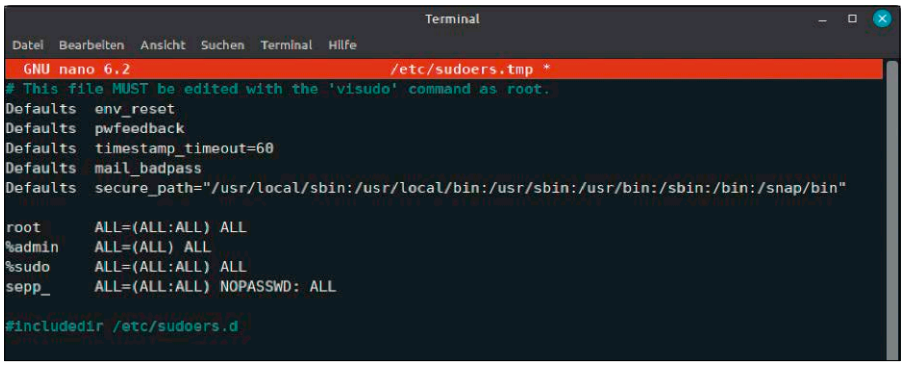
Das zweite Beispiel führt dazu, dass „sepp" für einige häufig benötigte Befehle (die ein sudo erfordern) kein Kennwort mehr eingeben muss, für alle übrigen aber schon.

Achtung: Solche Anweisungen für ein einzelnes Konto müssen **unterhalb der allgemeinen Gruppenrechte** („%sudo ALL [...]") erfolgen, weil bei abweichenden Angaben stets die letzte Anweisung der sudoers-Datei gewinnt. Die Abweichung entsteht hier dadurch, dass die Gruppenmitglieder von „sudo" standardmäßig nach dem Kennwort gefragt werden, das sudo-Gruppenmitglied „sepp" hingegen nicht (oder nicht immer).

Ist auf einem System überhaupt nur ein Konto relevant, können Sie sogar noch weitergehen und mit

```
%sudo ALL=(ALL:ALL) NOPASSWD: ALL
```

sämtlichen sudo-Konten (es gibt ja nur eines) die Kennworteingabe ersparen. ■



Konfigurationsdatei für sudo: Hier steht quantitativ recht wenig, die Relevanz ist aber kaum zu überschätzen. „root" und die Gruppe „%sudo" sollten alles oder viel dürfen.

WEITERE SUDO-TIPPS

Permanenter root-Kontext: Ein typisches sudo-Kommando wie

```
sudo apt install filezilla
```

erledigt genau eine Aufgabe im root-Konto und kehrt dann sofort wieder zum Benutzerkonto zurück. Für umfangreichere Arbeiten als root empfiehlt sich der Aufruf

```
sudo -s
```

oder – identisch – *sudo bash*. Danach bleiben Sie so lange „root", bis Sie „exit" eingeben oder das grafische Terminalfenster schließen.

Sudoedit: Mit einem Befehl wie

```
sudo gedit /etc/fstab
```

geben Sie einem bestimmten Editor das root-Recht zur Bearbeitung einer Systemdatei. Die Alternative *sudoedit* oder *sudo -e*

```
sudo -e /etc/fstab
```

ist erstens eine Abkürzung für Editierarbeiten an Konfigurationsdateien, verwendet zweitens den Standardeditor des Terminals (häufig Nano) und dies drittens in der Konfiguration des normalen Benutzerkontos (die Datei wird dazu temporär zwischengespeichert). Für den gewünschten Editor gibt es eine eigene Umgebungsvariable, die man mit

```
export SUDO_EDITOR="mcedit"
```

in der Datei „~/.bashrc" definieren kann.

Usermod/Gpasswd: Wie kommt ein neues Konto zur sudo-Gruppe? Wenn eine grafische Benutzerverwaltung wie unter Linux Mint vorliegt, dann einfach per Mausklick. Andernfalls hilft dies:

```
sudo usermod -a -G sudo sepp
```

Der umfangreichere Befehl für Gruppenzuweisungen ist allerdings gpasswd. Der kann nämlich

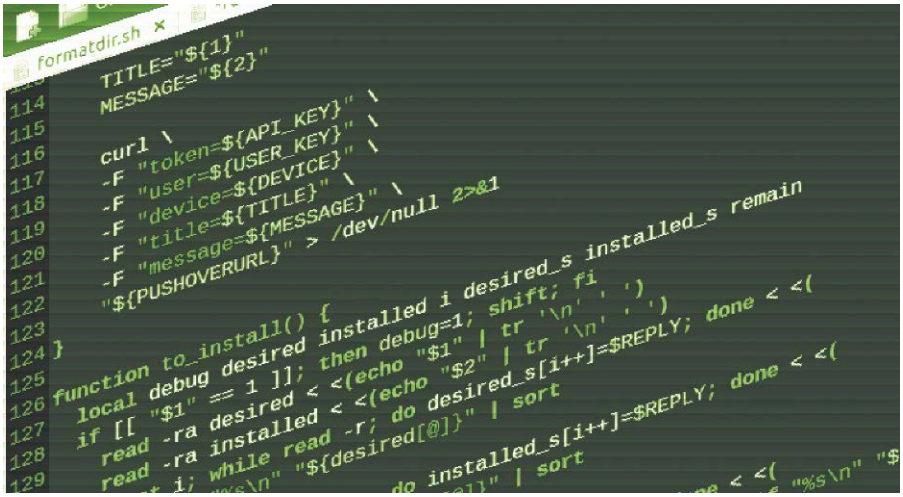
```
sudo gpasswd -a sepp sudo
sudo gpasswd -d sepp sudo
```

das sudo-Recht nicht nur gewähren („-a"), sondern bei Bedarf auch wieder entziehen („-d").

Bash-Script-Basics

Bash-Scripts können unter Linux alles erledigen, denn auch die grafische Oberfläche hört auf Terminalbefehle. Der Einstieg in die Ablauflogik und in die komplexen Regeln für Klammern und Quoting ist aber harte Arbeit.

VON HERMANN APFELBÖCK



Anlass dieses Beitrags sind Webrecherchen zur Bash-Syntax, die – obwohl am Ende auch mal erfolgreich – oft eine Mischung aus Ratlosigkeit und Ärger hinterlassen. Beliebte Antworten sind Exkurse in ganz andere Richtungen, gerne mit dem Hinweis auf Eleganz und Kürze. Ja – natürlich gibt es für jede Problemstellung zahlreiche Lösungsvarianten. Trotzdem wären punktgenaue Antworten hilfreicher als elegante Alternativen, die oft nur neue Fragen aufwerfen.

Ob wir es besser machen? Immerhin soll hier jeder angesprochene Aspekt möglichst auf den Kern reduziert werden. Die nächsten vier Seiten sind kein Lesestoff, eher eine Minireferenz zu den wichtigsten Bash-Prozeduren. Es geht ausschließlich um die Ablauflogik mit If, Case, For, While und Variablenverarbeitung. Für praxistaugliche Beispiele bleibt nur andeutungsweise Raum.

Info: Wer tiefer einsteigen will, dem sei das Openbook des Rheinwerk-Verlags empfohlen (*http://openbook.rheinwerk-verlag.de/shell_programmierung/*).

Service: Alle Script-Zeilen finden Sie unter *https://paste.ubuntu.com/p/ZqJqGjpKjF/*.

Zu allererst: Der Interpreter

Bash-Scripts sind reine Textdateien. Das Programm, das diese Texte zum aktiven Code macht, ist der Interpreter. Wir gehen hier immer von der Bash als Interpreter aus. Wenn Sie eine Codedatei mit

```
bash [datei]
```

starten, wird die Bash-Shell diese abarbeiten – egal, welchen Namen und welche Erweiterung diese trägt. Typischerweise erhalten solche Scripts die Erweiterung „.sh“, aber notwendig ist dies nicht, solange die obige Aufrufvariante gewählt wird. Ungeachtet der geltenden Standarderweiterung „.sh“ bildet die sh-Shell (Shell Command Language) nur eine Untermenge der Bash-Shell. Viele Scripts werden daher nicht oder fehlerhaft laufen, wenn sie mit

```
sh [datei]
```

den sh-Interpreter durchlaufen.

Wenn Bash-Scripts ohne explizite Nennung des Interpreters direkt starten sollen, benötigen sie

1. die Endung „.sh“

2. das Dateiattribut „ausführbar“ (*chmod +x [datei].sh*)

3. die Startzeile „#!/bin/bash“ im Script, um den Interpreter festzulegen.

If: Abfrage des root-Rechts

Für viele Script-Routinen ist root-Recht erforderlich. Folglich gehört eine entsprechende Abfrage in solchen Scripts zum Standard. Am einfachsten ist die Ermittlung der User-ID. Die ist nämlich für root gleich „0“:

```
if [ $UID -ne 0 ]
then
  echo "Das Script benoetigt root-
 Recht."
  sleep 5
  exit
fi
```

If: Existiert das Dateiobjekt?

Einschlägiger Operator, um die Existenz eines Ordners zu prüfen, ist „-d“ (Directory). Das abgefragte Verzeichnis kann ganz oder – wie nachfolgend – teilweise mit einer Variablen angegeben werden (hier $HOME):

```
if [ -d $HOME/.ssh ]
  then rm $HOME/.ssh/known_hosts
fi
```

Oft erspart es eine „else“-Anweisung, wenn der Operator mit „!“ umgekehrt wird. Wenn das Verzeichnis noch nicht besteht, wird es erstellt.

```
if [ ! -d $BASEDIR ]
  then mkdir $BASEDIR
  echo "Arbeitsverzeichnis $BASEDIR
  erstellt"
fi
```

Für Dateien gelten dieselben Regeln, jedoch ist hier der Operator „-f“ (File) einschlägig:

```
if [ ! -f $HOME/.nanorc ]
  then
  echo "set backup" >$HOME/.nanorc
 fi
```

Hinweis: Statt zwischen „-f“ und „-d“ zu differenzieren, kann für Dateien wie Ordner

auch allgemeines „-e“ verwendet werden, das für alle Dateiobjekte gilt.

If: Direkte Befehle in der Abfrage

If kann direkt das Ergebnis eines Kommandos auswerten. Das verkürzt Vorgänge wie den folgenden, der sich auch anders schreiben ließe, auf die halbe Schreibarbeit. Der „which“-Befehl sieht nach, ob das Programm VLC bereits vorliegt. Wenn die Abfrage nichts (Schalter „-z“) zurückliefert, dann fehlt der Player und wird installiert:

```
if [ -z $(which vlc) ]
  then echo "VLC fehlt. Wird
 installiert..."
  apt install vlc
fi
```

Eine vergleichbare Aktion ist folgende Abfrage einer Systemvariable. Wenn diese den Inhalt „64“ liefert, läuft das Script (nach „fi“) weiter. Andernfalls steigt es mit „exit“ aus:

```
if [ `getconf LONG_BIT` = "64" ]
  then echo "Bedingung erfüllt..."
else
  echo "Das Script funktioniert nur
 unter einem 64-Bit-System"
  sleep 5
  exit
fi
```

If: Exitcode abfragen

Die Standardvariable „$?“ liefert immer den Exitcode des zuletzt ausgeführten Befehls. Dieser Exitcode oder Errorlevel sollte „0“ sein, wenn alles funktioniert hat:

```
if [ "$?" != "0" ]
  then echo "Abbruch!"
  exit
fi
```

Das Script verabschiedet sich einfach, wenn der letzte Befehl nicht fehlerlos lief. In komplexeren Scripts sind auch gezielte Reaktionen auf den jeweiligen Fehlercode möglich – siehe etwa exemplarisch die „Exit Values“ eines Befehls wie Rsync in der Manpage.

If: Stringvergleich oder Grep?

Stringverarbeitung mit Bash ist kein Vergnügen. Sobald die einfacheren Operatoren (siehe Kasten „Wichtige Vergleichsoperatoren“) nicht mehr ausreichen, wird es heikel. Folgende If-Bedingung

```
ZEILE="#printers#"
if [[ $ZEILE = \#*\# ]]
```

zeigt, dass bei Stringverarbeitung mit regulären Ausdrücken eckige Doppelklammern erforderlich sind. Außerdem müssen Sonderzeichen wie hier das „#“ mit „\“ maskiert werden. Die Bedingung wäre für jede „Zeile“ wahr, die sowohl am Anfang wie am Ende ein „#“ enthält. Ein ähnliches Beispiel

```
if [[ $ZEILE =~ \# ]]
```

zeigt, wie man feststellt, ob ein String einen bestimmten Teilstring enthält: Die Bedingung wäre für jede „Zeile“ wahr, die an beliebiger Stelle ein „#“ enthält.

Wer sich hier nicht tiefer einlassen will, fährt oft einfacher, einen Grep-Befehl einzubauen und dessen Errorlevel abzufragen: Im nachfolgenden Fall werden Dateien mit der Endung „mkv“ verarbeitet, andere ignoriert. Grep meldet nämlich Errorlevel „1“, wenn der Textstring nicht gefunden wird:

```
echo $workfile | grep -i ".mkv"
if [ $? -eq 0 ]
  then echo "Weitermachen"
fi
```

Case: Ein Fall für viele

Überall dort, wo If-Elif-Else angesichts vieler Fallunterscheidungen unübersichtlich wird, sind Case-Esac-Klammern die klarere Prozedur mit weniger Schreibarbeit:

```
MIME=$(file --brief --mime-type
 $FILE)
case "$MIME" in
 "text/x-shellscript")
  xdg-mime default xed.desktop $MIME
  echo "Shellscript zugewiesen";;
 "video/x-matroska")
  xdg-mime default vlc.desktop $MIME
  echo "Matroska zugewiesen";;
# Und so weiter...
 *)
  echo "Nix zu tun..."
  exit;;
esac
```

In diesem – stark abgekürzten – Teil-Script sollen Dateitypen einem Standardprogramm zugewiesen werden.

Function: Ordnung und Schreibersparnis

Bash-Einsteiger schreiben selten so komplexe Scripts, dass dies gleich eine saubere Struktur von in sich abgeschlossenen Function-Einheiten erfordern würde. Strategisch wäre das aber sinnvoll: Eine kleine Function wie „dir_exist“ braucht man immer wieder und kann dann als Block in das nächste Script übernommen werden. Funktionen unterscheiden sich vom eigenständigen Script nur durch diesen Aufbau:

```
function name()
{
#Scriptcode...
}
```

WICHTIGE* VERGLEICHSOPERATOREN

Die folgenden Operatoren gelten für alle Prozeduren – egal ob in If-Abfragen oder in While- oder Until-Schleifen.

Zahlenvergleich (Ganzzahl)

Für arithmetische Zahlenvergleiche von Ganzzahlen gibt es zwei Schreibweisen. Am besten entscheiden Sie sich für eine Schreibweise und bleiben dann konsequent dabei:

Operator	Bedeutung	andere Schreibweise
-lt	kleiner als	<
-gt	größer als	>
-le	kleiner gleich	<=
-ge	größer gleich	>=
-eq	gleich	==
-ne	ungleich	!=

* Der Kasten zeigt bewusst nur einen Teil der Vergleichsoperatoren, da diese für 95 Prozent aller Aufgaben ausreichen.

Stringvergleich (Wörter)

Operator	Bedeutung
=	gleich
!=	ungleich
-z	leer, kein Inhalt
-n	nicht leer, hat Inhalt

Dateiabfragen

Operator	Bedeutung
-e	prüft Existenz eines Dateiobjekts (Datei oder Verzeichnis)
-d	prüft Existenz eines Verzeichnisses
-f	prüft Existenz einer Datei
-s	prüft Datei auf Inhalt (mehr als 0 Byte)
-x	prüft Datei auf Execute-Bit
!	Nicht-Operator, kehrt den Operator um (etwa „! -e“)

```
#!/bin/bash

function meldung ()
{
   echo ""
   echo "------------------------------------------------"
   echo $*
   echo "------------------------------------------------"
}

meldung Kopiere Datei ...
#cp ...
meldung Datei ist kopiert...
```

Die Function zeigt das Prinzip: Eine vorher abgelegte Function kann im weiteren Script-Verlauf mehrfach abgerufen werden – hier nur zur Ausgabe von Echo-Meldungen.

Die Abbildung oben zeigt eine ganz simple Function, die für einheitliches Aussehen aller Meldungen sorgt.

Functions müssen vor ihrem Aufruf abgelegt werden – etwa am Script-Anfang. Eine Ausnahme ist die Initialisierungsdatei „$HOME\.bashrc“. Alles, was dort definiert ist, gilt permanent bei der Terminalnutzung. Hier können Sie Funktionen (die nicht in der „bashrc“ selbst abgerufen werden) an beliebiger Stelle einsetzen und dann im Terminal interaktiv abrufen. Es kommt alles in Frage, was für ein Alias zu umfangreich wäre. Folgendes Beispiel sorgt für angenehmes Lesen von Manpages im grafischen Editor gedit:

```
function man ()
{
/usr/bin/man $* > ~/$*.man
 if [ -s ~/$*.man ]
#AUSGABE EXISTIERT, IST NICHT LEER
 then gedit ~/$*.man
 fi
}
```

Read: Einfache interaktive Fragen

Die Kommunikation mit dem Nutzer ist manchmal technisch erforderlich, oft auch nur ein Akt der Höflichkeit. Für eine einfache Entscheidung genügt Read, dessen Benutzerantwort als Variable (hier „$YESNO“) abgelegt wird und anschließend ausgewertet werden kann:

```
read -n 1 -p "Datei wirklich
 überschreiben (j/n)? " YESNO
if [ "$YESNO" = "J" ] || [ "$YESNO" =
 "j" ]
  then echo "Wir machen weiter..."
  cp $QUELLE $ZIEL
else
  echo "OK. Abbruch!"
fi
```

Schalter „-n 1“ ist optional, erspart aber dem Nutzer die Eingabetaste, „-p“ ist für interaktiven Abfrage notwendig. Beachten Sie ferner die If-Abfrage mit Oder-Operator („||“), um unabhängig von Groß- und Kleinschreibung zu entscheiden.

IF-KONSTRUKTIONEN

Der Haupttext geht auf kompliziertere If-Konstruktionen nicht ein. If-Elif-Else-Fi erlauben tief verschachtelte Entscheidungen, die allerdings schwerer zu schreiben und zu lesen sind als das für solche Fälle bevorzugte Case. Bei folgender sinnfreien If-Demo fragen wir Sie als Leser, welche Antwort das Script geben wird?

```
#!/bin/bash
if [ "a" = "e" ]
  then echo "Ja"
elif [ 1 -gt 2 ] || [ 2 -gt 1 ]
  then echo "Jein"
elif [ "b" = "b" ]
  then echo "Nein"
else
  echo "OK."
fi
```

Wenn Sie die Frage flott und eindeutig mit „Jein“ beantworten (weil „2“ größer „1“), dann haben Sie If-Konstruktionen gut im Griff. If bleibt eindeutig: Die nachfolgende Bedingung „b“ gleich „b“ trifft natürlich auch zu, kommt aber nicht mehr zum Zuge.

Select: Interaktive Auswahl

Soll der Benutzer aus einer ganzen Reihe von Optionen wählen, werden If und Read unpraktisch und schreibintensiv. Dafür gibt es das Spezialkommando Select. Dieses spielt in produktiven Scripts selten eine große Rolle, kann aber die interaktive Terminalnutzung erheblich vereinfachen:

```
select AUSWAHL in System Laufwerke
 Netzwerk
do
case $AUSWAHL in
 "System")
 inxi -SI;;
 "Laufwerke")
 inxi -dD;;
 "Netzwerk")
 inxi -ni;;
esac
exit
done
```

An der Auswertung mit Case oder If kommt man nicht vorbei, jedoch erspart Select die Präsentation der Optionen. Das wird noch deutlicher, wenn Select nach

```
select AUSWAHL in $(ls -A $HOME)
do rm $AUSWAHL
done
```

die Dateien eines Ordners präsentiert, um sie einfach per Eingabe der Kennziffer an einen bestimmten Befehl weiterzugeben.

While: Dateibearbeitung und Endlosschleife

While-Schleifen laufen solange, bis ein definierter Grenzwert erreicht ist. Im einfachsten Fall ist dies ein numerischer Wert:

```
i=1
while [ $i -ne 101 ]
do
echo "Durchlauf $1"
i=`expr $i + 1`
done
```

Dieses While läuft, während der Zähler pro Runde erhöht wird, genau bis „100“ – solange der Grenzwert „101“ nicht erreicht ist. Bezifferte Schleifen sind allerdings nicht die Domäne von While (sondern eher der For-Schleife). While-Do-Done mit Angabe der Eingabedatei ist hingegen die beste Lösung, um Dateilisten Zeile für Zeile abzuarbeiten:

```
find ~/ -iname "*.jpg" > ~/tmp.txt
while read ZEILE
  do
  convert "$ZEILE" "${ZEILE %.*}.
    png"
done < ~/tmp.txt
```

While eignet sich ferner auch als Endlosschleife, etwa um ein Dateiereignis zu überwachen oder ein Dauerbackup zu erledigen. Am einfachsten ist dabei die Schreibweise *while true*, aber natürlich funktioniert auch etwa *while [„a“ = „a“]*:

```
#!/bin/bash
while true
do
 rsync -auvP $HOME/Schreibtisch/ /
 media/Data/Schreibtisch
 sleep 300
done
```

Until-Schleife: Meist entbehrlich

Until ist in aller Regel entbehrlich, weil man mit While genauso ans Ziel kommt. Statt der Fortsetzungsbedingung wird hier die Endbedingung der Schleife festgelegt. Exakt dasselbe Ergebnis wie das erste Beispiel für While erzielt diese Until-Schleife:

```
until [ $i -eq 101 ]
  do
  ...
  done
```

Die Schleife läuft, bis der der Wert „101“ erreicht ist, folglich genau bis zum Wert „100“. Letztlich unterscheiden sich While und Until nur bei der Wahl des Vergleichsoperators.

For: Dateilisten und Zähler

Schleifen mit For-Do-Done erledigen mit wenigen Zeilen ganze Arbeit und eignen sich für definierte numerische Wiederholungen ebenso wie für Dateilisten unbekannter Menge. Im ersten Beispiel kann die Schrittfolge numerisch vorgegeben werden (Achtung: geschweifte Klammern):

```
for IP in {1..255}
do
  antwort=$(ping -c 1
 192.168.0.$IP)
  if [[ $antwort =~ "1 received" ]]
  then echo "192.168.0.$IP ist
 online..."
  fi
done
```

Im zweiten Beispiel verarbeitet die Do-Schleife alle Dateien im aktuellen Verzeichnis, die ihr der Hilfsbefehl ls liefert:

```
for PIC in `ls -A *.jpg`
do
 PICNAME=$(basename "$PIC" jpg)
 convert "$PIC" "$PICNAME.png";
done
```

Alle dort gefundenen JPG-Bilder werden in das Format PNG konvertiert.

Break & Exit: Shell raus hier!

Schleifen mit Do, While, Until lassen sich sicher sauber konstruieren – ohne speziellen Panikausstieg. Manchmal ist es aber pragmatischer und einfacher, einen seltenen Sonderfall nicht ausführlich einzubauen, sondern an der betreffenden Stelle einfach zwangsweise auszusteigen:

```
if [ $? -ne 0 ]
 then echo "Fehler. Abbruch!"
 break
fi
```

Die Standardvariable „$?“ meldet den Fehlercode des letzten Befehls. Ist dieser größer als „0“, war etwas schiefgegangen. Break macht nur Sinn in Schleifenkonstruktionen: Die Schleife wird verlassen, eventueller Code nach der Schleife aber weiter abgearbeitet.

Wenn ein Script zwangsweise komplett beendet werden soll, ist Exit der geeignete Ausstieg.

Dateiinhalt oder Befehlsoutput als Variable

Den Inhalt einer Datei schreibt der Befehl

```
VAR=$(cat $HOME/.bash_history)
```

oder noch kürzer

```
VAR=$(<$HOME/.bash_history)
```

umstandslos in eine Bash-Variable. Diese erhält in diesem Beispiel sämtliche Zeilen der Datei „.bash_history“. So einfach dies ist – praktikabel ist es oft nur bei einzeiligen Mini-Konfigurationsdateien wie etwa „/etc/timezone“, weil die Zeilen nicht einzeln bearbeitet werden können. Nach

```
echo $VAR
```

erscheint die Sammelvariable als Textbrei ohne die ursprüngliche Zeilenschaltung, diese lässt sich jedoch mit dieser Schreibweise erzwingen:

```
echo "$VAR"
```

```
#!/bin/bash
# WHILE oder UNTIL? Fast egal!

i=0
while [ $i -ne 21 ]
do
  echo "Durchlauf $i"
  i=`expr $i + 1`
done

# Dasselbe mit UNTIL...

i=0
until [ $i -eq 21 ]
do
  echo "Durchlauf $i"
  i=`expr $i + 1`
done
```

While- oder Until-Schleifen sind funktionsgleich und unterscheiden sich nur in der Logik des Operators.

Die Ausgabe eines Terminalbefehls ist ebenfalls problemlos in eine Variable zu übertragen

```
VAR=$(ping -c 1 192.168.178.1)
```

und danach unter „$VAR“ auszuwerten.

Array-Variablen

Mit Schleifenkonstruktionen mit indizierten Array-Variablen gerät Bash-Code schnell zur anspruchsvollen Programmierung. Arrays vom Typ „VAR[n]“ bieten die Möglichkeit, in eine einzige Variable beliebig viele Inhalte zu schreiben und per Indexnummer jeden einzelnen Inhalt gezielt zu bearbeiten. Mehr als das Prinzip können wir hier nicht andeuten: Die Abbildung unten zeigt ein kleines Beispiel-Script, das sich mit dem Echo-Beweis begnügt, dass man jeden einzelnen Inhalt „im Griff hat“. Ein praxistaugliches Script würde nun die gewünschten Zeilen suchen, diese mit oder ohne Benutzerinteraktion ändern und alle anderen Zeilen unverändert zurückschreiben. ■

Öffnen | array.sh ~/Schreibtisch | Speichern

```
#!/bin/bash
i=0
while read ZEILE
do
# Bedingung: Zeile nicht leer UND beginnt nicht mit "#"
  if [ -n "$ZEILE" ] && [[ $ZEILE != \#* ]]
# Zähler hochsetzen...
    then i=`expr $i + 1`
# Zeile in Array schreiben...
    VAR[$i]="$ZEILE"
  fi
done < /etc/samba/smb.conf

# for-Schleife beginnt bei 1, Schrittgröße 1, endet bei $i
for n in $(seq 1 1 $i)
do
   echo "$n ${VAR[$n]}"
done

echo "------------------------------------------------------------"
echo "$i gespeicherte Zeilen (leere und auskommentierte ignoriert)."
```

Prinzipielle Arbeitsweise mit Array-Variablen: Alle „aktiven“ Zeilen einer Konfigurationsdatei werden in die Variable „VAR[]“ geschrieben und danach über eine For-Schleife ausgegeben.

Distributionen im Check

Für Einsteiger ist es keine leichte Aufgabe, die passende Linux-Distribution für die anvisierte Aufgabe zu finden. Die folgende Übersicht klassifiziert wichtige tonangebende Systeme anhand ihrer Besonderheiten und Stärken.

Von **David Wolski**

Fragt man eine zufällige Anzahl an Linux-Anwendern, welche denn nun die beste Linux-Distribution sei, so bekommt man ein Vielfaches dieser Zahl an Meinungen, Einwürfe und Empfehlungen zurück. Und dazu eine Menge obskurer Geek-Weisheiten und mit religiösem Eifer verfochtene Überzeugungen zu Usability, Paketformaten und Entwicklungsmodellen. Abfällige Bemerkungen über die jeweils anderen Distributionen inklusive.

Auf Einsteiger wirkt das alles abschreckend bis arrogant und ist bei Anfängerproblemen selten hilfreich. Für Neuankömmlinge in der Linux-Welt bringt die gebotene Vielfalt nach wie vor die die Qual der Wahl, auch wenn das Einsatzgebiet wie Desktop oder Server klar ist. Nicht jedes System passt in jedes Umfeld, zu jedem Wissensstand und zu allen Geschmäckern.

Orientierungshilfe und Bewertung

Die Landkarte der Linux-Distributionen zeigt einige große bekannte Kontinente und unzählige kleinere Provinzen. Der folgende Distributions-Check nimmt sich die tonangebenden Systeme vor, die für sich eine eigene Kategorie darstellen. Bevor ein weitgereister Linux-Reisender fragt, warum das eigene Lieblingssystem nicht dabei ist, sei betont, dass diese Kategorisierung keinen Anspruch auf Vollständigkeit erhebt. Die großen Systeme, auf welchen viele andere Distributionen basieren, sind aber vertreten.

Auch Android hat es in der X86-Portierung in die Übersicht geschafft, während Mageia die Auswahl aufgrund seines Status als Randexistenz knapp verfehlt hat.

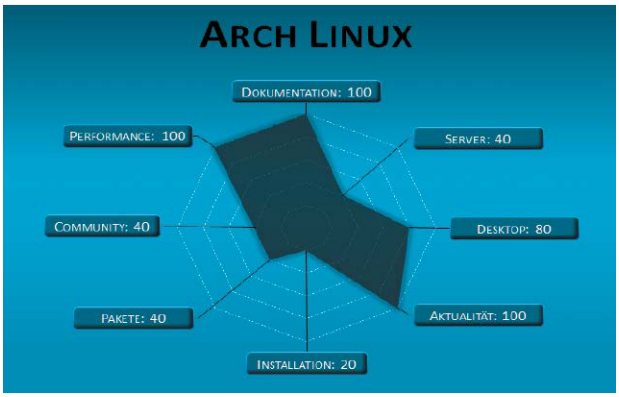
Die jeweiligen Stärken und Schwächen der Distributionen zeigt jeweils ein Radardiagramm mit den Bewertungskriterien, wie sie die Legende auf dieser Seite auflistet. Die „Leistung“ gibt den Erfahrungswert wieder, wie schnell und leistungsfähig ein System in der Standardkonfiguration ist. Was die Radargrafiken schnell auf den ersten Blick zeigen, sind die Stärken und Schwächen einer Distribution. Und auch, dass es das perfekte Universal-Linux nicht gibt, sondern immer das anvisierte Einsatzgebiet entscheidend für die richtige Wahl ist.

Ausschlaggebend ist in der Wertung der Zustand einer Distribution, wie sie sich im August 2018 gezeigt hat. Da die hier ausgewählten Systeme aber keinen umfangreichen Änderungen im Quartalsrhythmus unterliegen, wird die Bewertung und Einschätzung einige Jahre Bestand haben.

Legende zu den Radargrafiken

Server	Servertauglichkeit (bei Ubuntu Unterscheidung LTS-Version)
Desktop	Desktoptauglichkeit
Installation	Komfort der Systemeinrichtung
Performance	Leistung als Server und Desktop
Pakete	Umfang der angebotenen Softwarepakete
Aktualität	Programmversionen in den Standard-Paketquellen
Dokumentation	Ausführlichkeit / Einsteigerfreundlichkeit der Dokumentation (dt./engl.)
Community	Unterstützung durch Wikis und Foren

Arch Linux

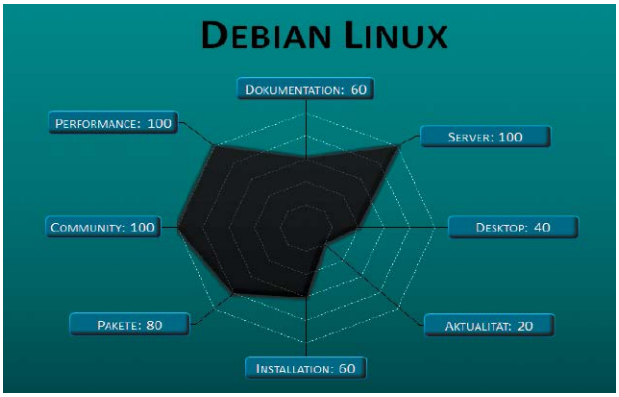


Obwohl Arch mit hohem Do-it-Yourself-Faktor, der schon bei der Installation beginnt, als Anachronismus erscheint, hat sich die Distribution enorm viele Freunde in der fortgeschrittenen Anwenderschaft gemacht: Arch legt Wert auf einen schlanken Aufbau und manuelle Konfiguration und versteckt die Innereien des Systems nicht hinter distributionsspezifischen Tools. Lohn der Mühe ist die volle Kontrolle darüber, was auf dem System installiert ist. Zum Bekanntheitsgrad von Arch trägt dessen hochkarätiges Wiki mit größtenteils englischsprachigen Anleitungen zu System und Software bei. Als „Rolling Release" lässt sich Arch über den Paketmanager auf dem neuesten Stand halten. Einen Standarddesktop gibt es nicht.

Der typische Arch-Anwender ist ein avantgardistischer Linux-Fan mit langjähriger Erfahrung, der sich selbst zu helfen weiß und Linux-Systeme aus den hochaktuellen Paketquellen selbst zusammenstellt.

Offizielle Webseite: *www.archlinux.de*

Debian GNU/Linux

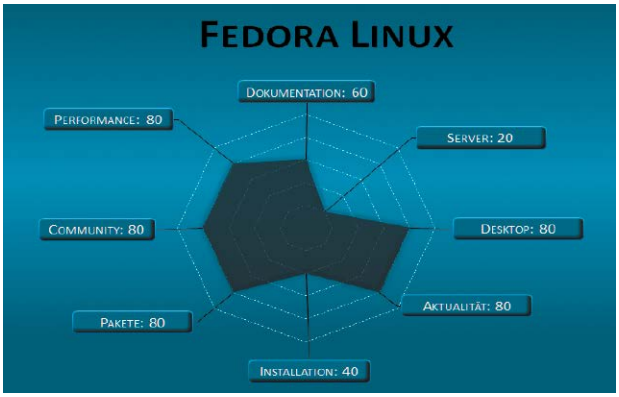


Das System für höchste Ansprüche an Stabilität ist in der turbulenten Linux-Entwicklung der Fels in der Brandung und mit 23 Jahren eine der dienstältesten Distributionen. Auf neueste Pakete legt die Entwicklergemeinde keinen Wert. Deswegen werden Programme und Komponenten langsamer aufgenommen als bei der Konkurrenz. Auf dem Debian-Paketformat DEB und der Paketverwaltung APT ist auch Ubuntu aufgebaut. Neue Debian-Ausgaben erscheinen rund alle zwei Jahre und die Entwicklung erfolgt in mehreren Zweigen: Debian Unstable bietet neueste Software, die für weitere Tests in Debian Testing aufgenommen wird, das wiederum die Vorstufe zu Debian Stable ist.

Der typische Debian-Anwender braucht ein grundsolides Serversystem für professionelle Aufgaben oder bevorzugt konservative Desktops. Die Programmversionen dürfen dabei auch älter sein – Hauptsache, alles ist gründlich getestet.

Offizielle Webseite: *www.debian.org*

Fedora

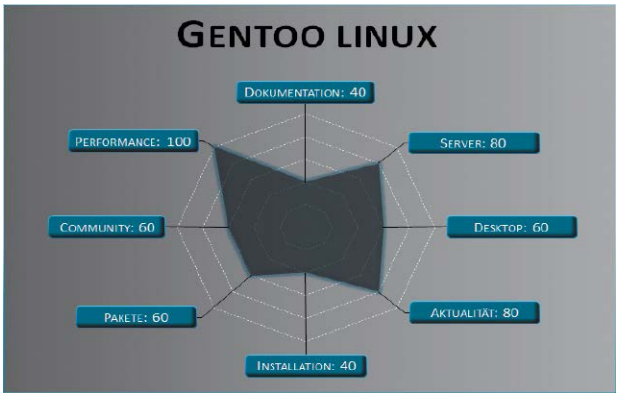


Das von Red Hat gesponserte Fedora ist ein Trendsetter mit topaktueller Programmauswahl. Es spricht ambitionierte Anwender an, die eine möglichst aktuelle Desktopdistribution suchen. Wenn sich eine Technologie wie der neue Init-Daemon Systemd bei Fedora bewährt hat, wandert sie später zu Red Hat Enterprise Linux. Fedora nutzt das RPM-Paketformat und ist vornehmlich für den Desktopeinsatz geschaffen, da sich das System mit häufigen Updates oft ändert. Die typische Desktopumgebung ist Gnome 3, aber auch Mate, LXDE und KDE können sich unter Fedora sehen lassen. Die Installation erfolgt über Livesysteme oder mit der universellen DVD-Ausgabe. Der Installer ist eher umständlich.

Der typische Fedora-Anwender hat beruflich oft mit Red Hat Enterprise Linux oder Cent-OS zu tun oder ist sogar Administrator, will aber zu Hause lieber ein aktuelleres Fedora, das schon mal eine Vorschau auf das nächste Red Hat bietet.

Offizielle Webseite: *http://fedoraproject.org*

Gentoo Linux

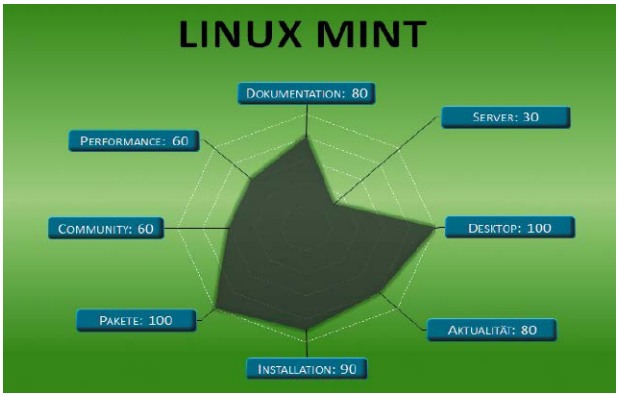


Auch wenn der Stern Gentoos langsam sinkt, ist diese Distribution kein Fall für die Geschichtsbücher. Das liegt auch an Google Chrome-OS, das seit 2010 auf das anpassungsfähige Gentoo als Basis setzt. Gentoo zeichnet sich wie Arch durch ein eigenes Paketformat aus, das mit dem Paketmanager Portage an die „Ports“ von Free BSD erinnert. Dies erlaubt die Kompilierung von Programmen nach Bedarf aus einem Repository mit mehr als 10 000 Quellpaketen. Dies ist natürlich eher für Fortgeschrittene interessant, die sich um jedes Detail und die Konfiguration selbst kümmern, aber es gibt auch Binärpakete. Gentoo ist ein „Rolling Release“, das sich über den Paketmanager auf dem neuesten Stand halten lässt.

Der typische Gentoo-Anwender scheut keine hohen technischen Ansprüche, weil er die Anpassungsfähigkeit und Quelltextpakete schätzt, die Gentoo zu einem besonders schnellen System machen. Die Installation erfolgt per Scripts.

Offizielle Webseite: *www.gentoo.org*

Linux Mint

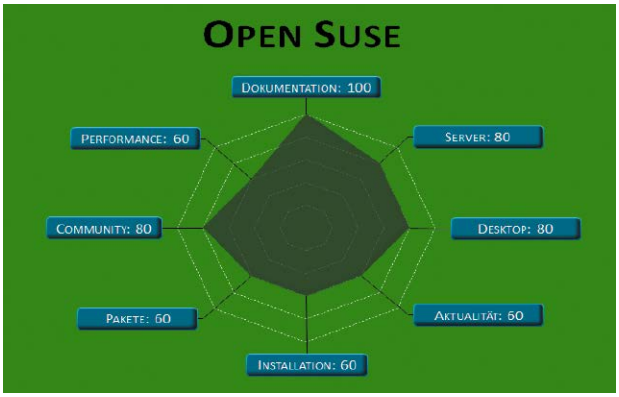


War Linux Mint anfangs eine inoffizielle Ubuntu-Variante mit umgestaltetem Desktop, so tritt Mint heute mit zahlreichen Eigenentwicklungen langsam aus dem Schatten des Vorbilds. Mint basiert immer noch auf Ubuntu LTS und erscheint stets eine Weile nach einem neuen Ubuntu, setzt aber genügend eigene Akzente, um hier als eigene Distribution durchzugehen. Eigene Entwicklungen gehen von Konfigurationstools bis hin zur Arbeitsumgebung Cinnamon und den neuen X-Apps. Linux Mint ist in der undogmatischen Linux-Anwenderschaft sowie unter Umsteigern beliebt, die ein unkompliziertes Desktop-Linux suchen. Für den anspruchsvollen Servereinsatz ist es aufgrund der Softwareauswahl und vereinzelt auftretenden Paketkonflikte ungeeignet.

Der typische Mint-Anwender sucht ein anwenderfreundliches Desktop-Linux, dessen Entwickler weitgehend alle Entscheidungen zur Softwareausstattung getroffen haben.

Offizielle Webseite: *www.linuxmint.com*

Open Suse

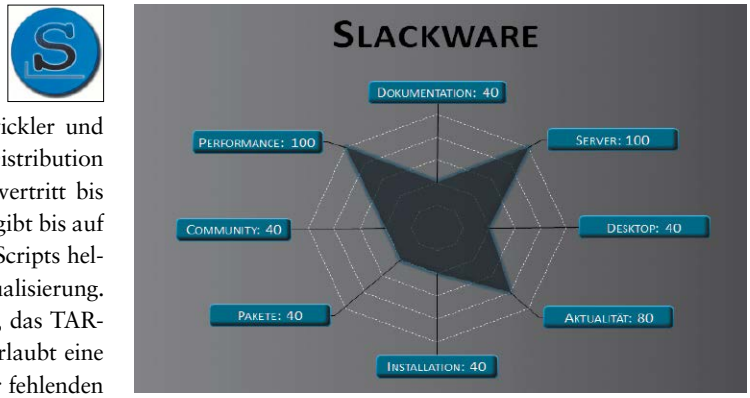


Einen langen gewundenen Weg hat Open Suse hinter sich, das bereits 1992 in Deutschland entstand und auf dem RPM-Paketformat basiert. Seit der Übernahme durch Novell 2005 ist es wie Fedora ein von der Community entwickeltes Projekt. Aktuell ist es beim Mainframespezialisten Microfocus untergekommen, der mit Suse Linux Enterprise auch eine kommerzielle Variante unterhält. Seit der Ausgabe „Leap“ nutzt Open Suse dessen Paketquellen, die es durch neuere Software ergänzt. Die Paketauswahl ist nicht brandaktuell, lässt sich aber durch inoffizielle Paketquellen des Build Service erweitern. Open Suse hat den Pokal für Einsteigerfreundlichkeit an Mint und Ubuntu abgegeben, punktet aber mit exzellentem KDE-Desktop und grafischen Konfigurationshilfen.

Der typische Suse-Anwender setzt auf das grafische Menüsystem von Yast zur Administration oder ist ein Traditionalist, der mit Suse zu Linux kam und Suse bis heute treu bleibt.

Offizielle Webseite: *http://de.opensuse.org*

Slackware

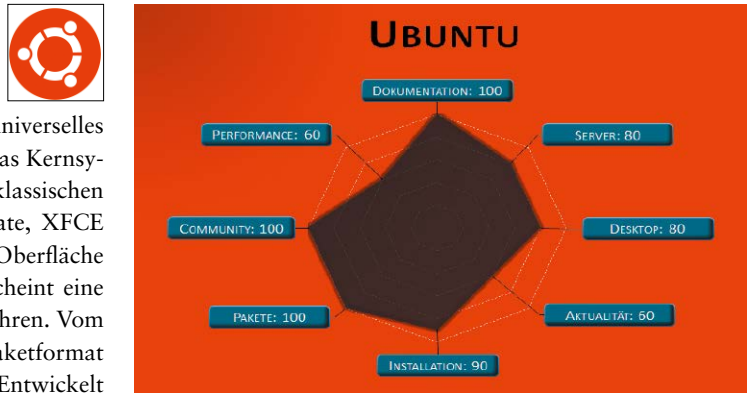


Als lebendiges Fossil hat sich Slackware in eine Nische zurückgezogen, in der hauptsächlich Entwickler und Administratoren zu Hause sind. Die älteste aktive Distribution war anfangs die Basis für Suse Linux. Slackware vertritt bis heute die reine Lehre der Linux-Administration: Es gibt bis auf den Installer kaum Konfigurationshilfen. Lediglich Scripts helfen bei der Programminstallation und Systemaktualisierung. Dies ist auch auf das Paketformat zurückzuführen, das TAR-Archive ohne ausführliche Metadaten nutzt. Dies erlaubt eine sehr freie Systemeinrichtung mit dem Nachteil einer fehlenden Abhängigkeitsprüfung. Slackware ist sehr schnell und schlank und mit seinen stabilen Programmversionen servertauglich.

Der typische Slackware-Anwender hat meist schon ein paar graue Haare mehr auf dem Kopf oder im Gesicht, ist bei Linux-Systemen auf ausführlich getestete, stabile Versionen bedacht und will maximale Konfigurationsmöglichkeiten.

Offizielle Webseite: *www.slackware.com*

Ubuntu

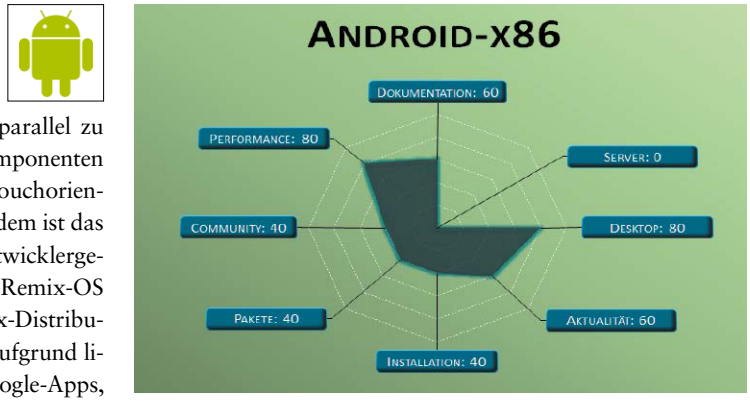


Die Distribution mit ungebrochener Popularität auf dem Desktop verfolgt den Anspruch, ein universelles System für PCs, Server und Mobilgeräte zu sein. Das Kernsystem basiert aber weiterhin auf Debian. Auf dem klassischen Desktop-PC genießen offizielle Varianten mit Mate, XFCE und LXDE seit der Einführung der kontroversen Oberfläche Unity mehr Aufmerksamkeit. Alle zwei Jahre erscheint eine Ubuntu-Ausgabe mit Langzeitsupport von fünf Jahren. Vom Vorbild Debian übernimmt Ubuntu das DEB-Paketformat und APT, ist aber zu Debian nicht kompatibel. Entwickelt wird Ubuntu von einer Community und der Firma Canonical. Für den Servereinsatz sind nur die LTS-Versionen sinnvoll.

Der typische Ubuntu-Anwender will ein einsteigerfreundliches, von Debian abstammendes Allround-Linux mit großer Community und häufiger Erscheinungsfrequenz für Server und Desktop.

Offizielle Webseite: *www.ubuntu.com*

Android-x86



Android ist keine herkömmliche Linux-Distribution. Von Google wurde Android ursprünglich parallel zu Chrome-OS für Smartphones geschaffen; Kernkomponenten wie die Android Runtime für Java-Apps und die touchorientierte Oberfläche sind dafür maßgeschneidert. Trotzdem ist das System so anpassungsfähig, dass OEMs und Entwicklergemeinden eigene Ausgaben bauen. Android-x86 und Remix-OS sind Vertreter dieser Gattung und werden wie Linux-Distributionen als installierbare Livesysteme ausgeliefert – aufgrund lizenzrechtlicher Beschränkungen allerdings ohne Google-Apps, zu welchen auch der App Store Google Play gehört. Wer Android-x86 auf PCs einsetzen will, muss APKs manuell installieren oder mit dem App-Store-F-Droid vorlieb nehmen.

Der typische Android-X86-Anwender will eine simple Oberfläche auf einem Zweit- oder Drittrechner, muss aber für die Einrichtung Experimentierbereitschaft mitbringen.

Offizielle Webseite: *www.android-x86.org*

Dauerläufer: Rolling Releases

Einst galten stetig aktualisierte Linux-Systeme als fragile Gebilde, die höchstens für Entwickler interessant sind. Diese „Rolling Releases“ haben sich mittlerweile als stets aktuelle Systeme für fortgeschrittene Linux-Anwender etabliert.

VON DAVID WOLSKI

Hier geht es nicht um konservative Distributionen wie Debian und Ubuntu LTS, die ohne Änderungen an der initialen Konfiguration einige Jahre laufen sollen. Vielmehr werden die hier vorgestellten Systeme laufend aus ihren Paketquellen auf dem neuesten Stand gehalten. Dieses Modell ist als „Rolling Release“ bekannt und erfordert von den Distributionsmachern viel Aufmerksamkeit für Updates, die ein Linux-System nie in einem funktionsunfähigen Zustand hinterlassen dürfen. Wer ein System dieser Bauart einsetzt, ist stets am Puls der Entwicklungen und erhält frische Kernel samt Modulen, Treibern und aktualisierten Anwendungsprogrammen.

Der Nachteil: Die Pakete sind weniger ausgiebig getestet. Im Laufe der Zeit werden über die Lebensdauer eines Rolling Release unvermeidlich Inkompatibilitäten zwischen Systemkomponenten auftreten. Bei größeren Änderungen kann es durchaus sein, dass Anwender eingreifen und die Konfiguration manuell anpassen müssen. Deshalb eignen sich „Rolling Releases“ eher für Fortgeschrittene. Für eine Rolle als Server-Dauerläufer sind sie nicht die beste Wahl, denn dafür sind die Versionssprünge der Pakete hin und wieder zu groß. Die Wahrscheinlichkeit, dass ein Serverdienst nach einem Update stehenbleibt, ist durchaus gegeben.

Die Auswahl: Bewährte Systeme

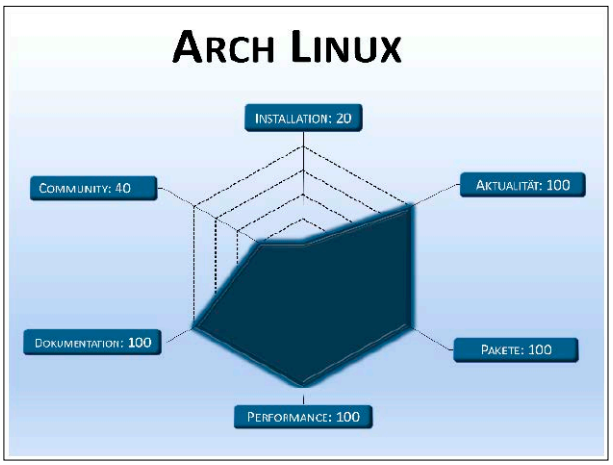
Gut geeignet sind Rolling Releases für anspruchsvolle Desktopsysteme, denn die gelegentliche Mühe sporadischer Korrekturen wird durch ein besonders aktuelles System belohnt. Es ist aber nicht jedes Rolling Release für den Einsatz auf einem Arbeitsrechner geeignet. So ist die Entwicklerversion Ubuntus nicht stabil genug, sondern lediglich eine Teststation für zukünftige Ubuntu-Ausgaben. Die hier getroffene Auswahl umfasst bewährte und bereits etablierte Distributionen, die dem Prinzip fortlaufender Updates folgen und sich über Jahre pflegen lassen: Arch Linux, das davon abstammende Manjaro, Debian Sid, Open Suse Tumbleweed, Gentoo und Solus-OS sind auf den nächsten Seiten vertreten.

Stärken & Schwächen im Radar

Die Unterschiede zwischen den Distributionen zeigt eine Bewertungsgrafik aus dem Blickwinkel eines fortgeschrittenen Linux-Kenners – sicher keine exakte Wissenschaft, aber eine solide Einschätzung. In die Wertung fließen folgende Kriterien ein:

Installation: Wie komfortabel gestaltet sich die Einrichtung? Welche Konfigurationswerkzeuge bringt der Installer mit?
Aktualität: Wie schnell gelangen frische Programmpakete in die Standardquellen?
Performance: Wie schnell ist die Distribution in der Standardkonfiguration?
Pakete: Wie viele Softwarepakete gibt es in offiziellen und inoffiziellen Repositorys?
Dokumentation: Wie sorgfältig ist die Distribution in Wikis und Community-Webseiten erklärt?
Community: Wie groß ist die Nutzer- und Entwicklergemeinde?
Das Thema der Hardwareunterstützung hat keine separate Wertung bekommen, da sich alle genannten Distributionen heute dank großer Fortschritte des Linux-Kernels gut schlagen und mit seltenen Ausnahmen mit allen aktuellen PCs und Notebooks klarkommen.

Arch Linux



Arch Linux hat sich in den letzten 19 Jahren aus einer kleinen Variante von „Linux from Scratch“ plus Paketmanager zu einer illustren Linux-Distribution entwickelt, die vor allem fortgeschrittene Linux-Enthusiasten schätzen. Ein wichtiges Motiv für Arch Linux neben der Anpassungsfähigkeit und dem puristischen Ansatz bei Einrichtung und Administration ist auch das informative Arch Wiki, das Linux-Anwender weit über Arch Linux hinaus mit praxisrelevanter Dokumentation versorgt.

Unter der Haube gibt es ein robustes eigenes Paketsystem mit dem Kommandozeilen-Paketmanager Pacman, das Entwicklern die Erstellung von Arch-Paketen mit sehr wenig Überbau erlaubt.

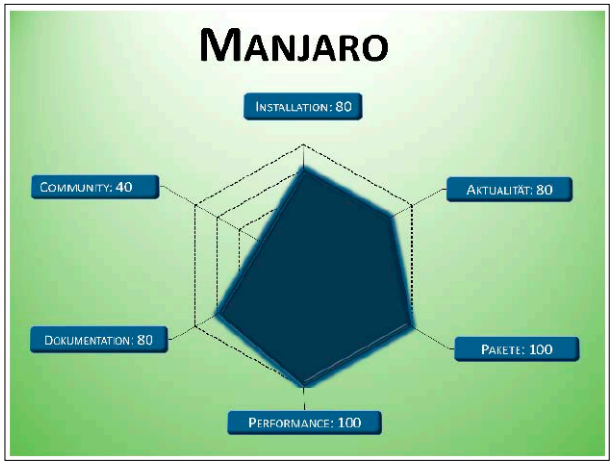
Alle Bestandteile in den offiziellen Repositorys sind deshalb stets sehr aktuell, wenn auch auf das Kernsystem begrenzt. Zahlreiche weitere Pakete liefern inoffizielle AURs („Arch User Repositories“), die es über ein ausgefeiltes Buildsystem erlauben, aus dem Quellcode von Programmen fertige Pakete zu kompilieren. Dazu gibt es separate Paketmanager, wobei sich derzeit Yay durchgesetzt hat.

Eine gehörige Einstiegshürde bleibt die Installation von Arch Linux, die per minimalem Installationssystem mit viel Handarbeit und wenigen helfenden Scripts erfolgen muss. Die Dokumentation dazu im Arch Wiki (*https://wiki.archlinux.org*) ist aber eine enorme Erleichterung und ein genaues Studium der Installationsanleitungen ist Pflicht.

Eine Arch-Variante mit niedrigerer Einstiegshürde ist – neben dem nachfolgenden Manjaro – Endeavour-OS (*https://endeavouros.com*), das einen grafischen Installer in einem Livesystem bereitstellt.

Mehr Infos zu Arch Linux:
Webseite: *www.archlinux.de*
Dokumentation:
https://wiki.archlinux.org

Manjaro Linux



Manjaro ist ein System für angehende Experten, denen pures Arch zu umständlich ist. Manjaro legt regelmäßig neue Ausgaben eines installierbaren Livesystems vor. Zum Einsatz kommt dabei der Installer Calamares, der sich inzwischen auch in Lubuntu und Kubuntu um die Einrichtung des Systems kümmert.

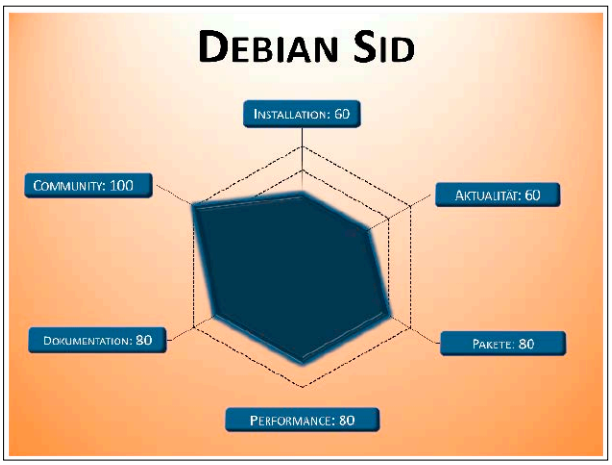
Zwar handelt es sich bei Manjaro im prinzipiellen Aufbau und beim Paketsystem um einen Abkömmling von Arch Linux, allerdings geht die kleine Distribution inzwischen doch viele eigene Wege, sodass sie nicht mehr mit Arch gleichzusetzen ist. Die Unterschiede beginnen damit, dass Manjaro nicht aus den gleichen Paketquellen wie Arch schöpft, sondern eigene Repositorys bereitstellt. Hier landen neue Paketversionen mit ein paar Wochen Verzögerung. Dies ist ein Umstand, der Manjaro seitens der Arch-Gemeinde in der Vergangenheit schon harsche Kritik eingebracht hat, wenn sicherheitsrelevante Aktualisierungen nicht früh genug zu den Nutzern kamen. Diese Entschleunigung gibt den Manjaro-Machern aber theoretisch noch die Möglichkeit, Bugs und Probleme auszumerzen oder ein Update vorerst zurückzuziehen.

Manjaro sucht die Balance zwischen frischen Paketen und Stabilität. Aus der Sicht von Arch-Linux-Fans ist Manjaro eine eigenständige Distribution, im Alltag gibt es aber so viele Gemeinsamkeiten, dass die Dokumentation im ausführlichen Arch Wiki in weiten Teilen auch für Manjaro gilt.

Manjaro liegt in Form installierbarer Livesysteme mit XFCE, KDE und Gnome vor. Die Gemeinde um diese Distribution veröffentlicht zudem auf unregelmäßiger Basis Medien mit weniger bekannten bis exotischen Desktops.

Mehr Infos zu Manjaro:
Webseite: *https://manjaro.org*
Dokumentation: *https://wiki.manjaro.org*

Debian Sid



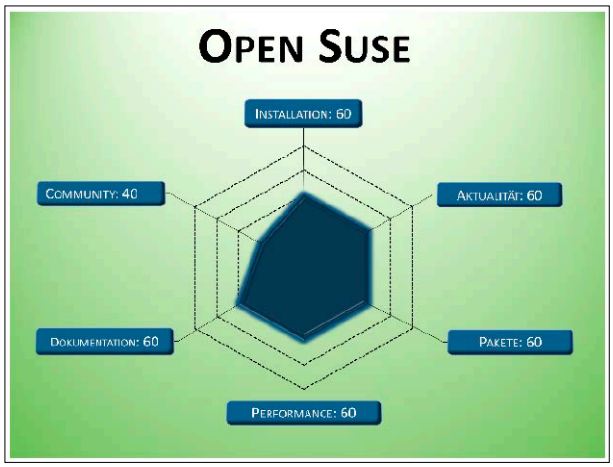
Der Weg eines Pakets zu einer neuen Debian-Ausgabe verläuft von den Zweigen „Experimental“ zu „Unstable“ und dann „Testing“. In „Unstable“ liegt Debian als Rolling Release vor und hat von den Debian-Machern den Codenamen „Sid“ bekommen, der sich wie alle Namen im Debian-Universum auf einen Charakter aus den Filmen „Toy Story“ bezieht. Unter den Rolling Releases nimmt Debian Sid eine Sonderstellung ein, da es sich um eine Vorstufe zum stabilen Debian handelt und um keine eigenständige Distribution. Vorstufe heißt, dass hier die Paketquellen des noch instabilen Debian-Zweigs zusammengefasst sind, aus welchen das zukünftige Debian bestehen wird. „Unstable“ bedeutet aber nicht, dass ein Debian-System aus diesen Paketversionen allenthalben von großen Bugs heimgesucht wird. Die Softwareversionen sind dabei nicht so weit vorauseilend wie etwa bei Arch Linux und im Vergleich eher konservativ, vom Kernel abgesehen.

Ein reguläres, stabiles Debian kann durch den Wechsel der Paketquellen zu einem Debian Sid gemacht werden.

Auch andere Distributionen schöpfen aus diesen Quellen, beispielsweise Ubuntu. Mit Parrot-OS Home (*https://parrot-linux.org*) gibt es auch eine eigene Distribution, die ein pures Debian Sid aus einem installierbaren Livesystem einrichtet. Im Dauerbetrieb verlangen diese Linux-Systeme vergleichsweise häufig eine Korrektur, um Paketabhängigkeiten zu reparieren. Aktualisierungen kommen üblicherweise in größeren zusammengefassten Portionen. Dann sind gute Kenntnisse mit dem Paketmanager apt in der Kommandozeile nötig, um eine Installation durch umfangreiche Änderungen zu bugsieren.

Mehr Infos zu Debian Sid:
Webseite: *www.debian.org/releases/sid*
Dokumentation:
https://wiki.debian.org/DebianUnstable

Open Suse Tumbleweed

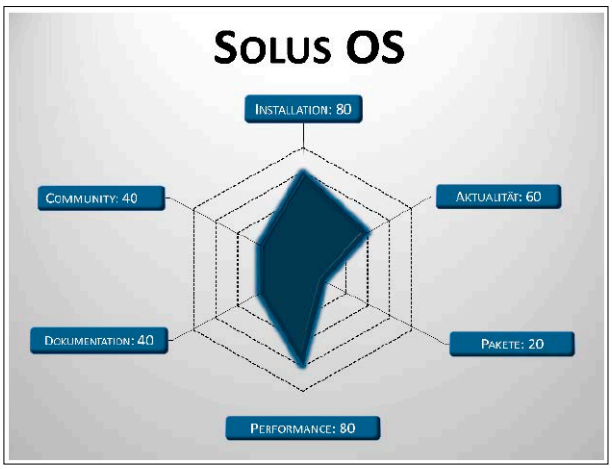


„Tumbleweeds“ sind Steppenläufer, die der Wind mal hierhin, mal dorthin weht. So wie die umherwehenden Wüstensträucher ist Open Suse Tumbleweed stets in Bewegung, da hier die neuesten, nicht immer ausgiebig getesteten Programmpakete ankommen. Eigentlich hat Open Suse nicht den Ruf, ein System mit den neuesten Paketen zu sein. Open Suse macht gar den Eindruck, dass die Entwicklung seit Leap, welches Kernkomponenten vom konservativen Suse Enterprise Live übernimmt, gerne mal ein paar Versionsnummern gegenüber vergleichbaren Distributionen hinterherhinkt. Dazu kommen eine langsame jährliche Veröffentlichungsfrequenz.

Der muss man aber nicht folgen: Open Suse Tumbleweed ist ein Rolling Release, das sich aus fortwährend aktualisierten Paketrepositorien zusammensetzt. Tumbleweed ist ein eigener Zweig von Open Suse und kann recht komfortabel aus einem eigenen Livesystem mit dem üblichen Installer Yast eingerichtet werden. Der Umbau eines stabilen Open Suse Leap zu Tumbleweed ist technisch möglich, empfiehlt sich aber nicht, da erfahrungsgemäß Paketkonflikte viel Kopfzerbrechen bereiten. Das System sollte besser anhand des Livesystems frisch installiert werden. Wie das reguläre Open Suse, so ist auch Tumbleweed ein Aushängeschild für KDE Plasma 5 als Desktop, der in Leap in Version 5.18 enthalten ist, im Rolling Release hingegen schon in Version 5.20. Neben Fedora ist Open Suse die derzeit einzige Distribution, die BTRFS als Standard-Dateisystem anbietet – komplett mit Subvolumes und Snapshots. Um in den Genuss der Vorteile zu kommen, ist eine geduldige Auseinandersetzung mit der Dokumentation nötig.

Mehr Infos zu Open Suse Tumbleweed:
Webseite: *https://software.opensuse.org/distributions/tumbleweed*
Dokumentation:
https://de.opensuse.org/Portal:Tumbleweed

Solus-OS



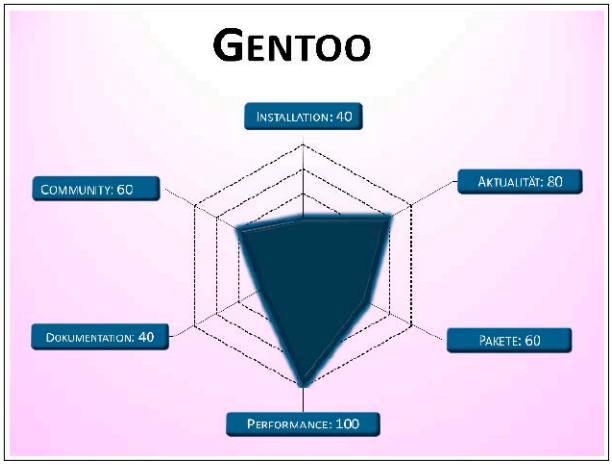
Bescheidener Neuanfang: Solus-OS trat ursprünglich dazu an, eine große Nummer auf dem Linux-Desktop zu werden. Der ehemalige Hauptentwickler ersann dazu den Desktop Budgie als Gnome-Abspaltung und ließ etliche Optimierungen für die typische Arbeitslast grafischer Anwendungen in den verwendeten Linux-Kernel einfließen.

Dann ereilte das schon beinahe etablierte Solus-OS das Schicksal vieler kleiner Linux-Distributionen: Der charismatische Hauptentwickler kam abhanden und überließ der Community die Weiterführung der Distribution. Das ist dank der kritischen Masse von Fans tatsächlich gelungen – Solus-OS wird weiter gepflegt und es gibt etwa im Jahresrhythmus aktualisierte Medien mit eigenem Installer, die als Livesystem konzipiert sind.

Die letzte dieser Ausgaben stammt vom Januar 2020, bekam im Oktober ein großes Update und liefert wahlweise den hauseigenen Budgie-Desktop, Gnome, KDE oder Mate. Das Ziel des Rolling Release ist bewusst eng definiert: Solus ist für den Desktop von klassischen PCs und Notebooks gedacht – also nicht für Server oder Cloud. Die Softwareausstattung ist schmal, umfasst aber die herkömmlichen Gnome-Applikationen, die den Linux-Desktop derzeit dominieren: Firefox ist der Browser, Libre Office ist das Office-Programm, Thunderbird ist das Mailprogramm und als Mediaplayer kommt VLC zum Einsatz. Über die typischen Desktopanwendungen hinaus ist das Paketangebot eher spärlich. Von allen hier vorgestellten Rolling Releases ist der Updatevorgang über die grafische Aktualisierungsverwaltung aber am einfachsten.

Mehr Infos zu Solus-OS:
Webseite: *https://getsol.us*
Dokumentation:
https://getsol.us/help-center/home

Gentoo Linux



Gentoo zeichnet sich wie Arch durch ein eigenes Paketformat aus, das mit dem Gentoo-Paketmanager Portage an die „Ports“ von Free BSD erinnert. Dies sind Quellcode-Pakete, die eine Kompilierung von Programmen ganz nach Bedarf aus einem Repository mit mehr als 10 000 Quellpaketen erlaubt. Eine Paketinstallation kommt damit einer Neukompilierung gleich – optimiert für den Prozessor des Rechners. Es gibt auch genügend Binärpakete für verbreitete Plattformen. Der weitgehend manuelle Installationsprozess eines puren Gentoo-Systems stellt allerdings nach wie vor eine nicht gerade kleine Hürde dar.

Über diese Distribution, die als Vorläufer von Arch gelten darf, wird nur noch selten berichtet. Und dennoch ist Gentoo eine feste Größe, zumal sich Greg Kroah-Hartman als illustrer Kernel-Entwickler mit darum kümmert, dieses Rolling Release am Leben zu halten. Google hat die Distribution als technische Grundlage für das immens erfolgreiche Chrome-OS gewählt und neuralgische IT-Systeme der Wall Street arbeiten damit auf ihren oft hochspezialisierten Servern. Gentoo zeichnet sich durch sein Paketmanagement aus, welches von Free BSD inspiriert ist und Programme bei der Installation auf Wunsch frisch und optimal kompiliert. Gentoo ist das einzige Rolling Release, das sich eventuell auch für Server eignet – vorausgesetzt, der Administrator bringt das nötige Durchhaltevermögen mit, sich in Gentoo einzuarbeiten.

Mit der Distribution Sabayon gibt es einen leichter beherrschbaren Abkömmling (*www.sabayon.org*). Das ehemals hervorragende Gentoo-Wiki befindet sich nach einem katastrophalen Serververlust 2008 seitens des damaligen Hosters wieder im Aufbau.

Mehr Infos zu Gentoo:
Webseite: *www.gentoo.de*
Dokumentation:
https://wiki.gentoo.org

Linux „immutable“: Sicher und stabil

Auch wenn meist alles gut geht, sind Systemupdates und Softwareinstallationen eine potenzielle Gefahr für die Stabilität des Systems. Wer sich maximale Systemsicherheit wünscht, sollte sich einen anderen Distributionstyp ansehen.

VON THORSTEN EGGELING

Linux-Distributionen gibt es hauptsächlich in drei Geschmacksrichtungen: besonders stabile Langzeitversionen (LTS), Versionen mit aktuellerer Software und Kurzeitunterstützung (STS) sowie Distributionen, die kontinuierlich aktualisiert werden („Rolling Releases“).

Relativ neu hinzugekommen sind „immutable“ Distributionen, was sich mit „unveränderlich“ übersetzen lässt. Ähnlich wie bei einer Linux-Live-DVD ist das System schreibgeschützt, Konfigurationsdateien und das Home-Verzeichnis werden jedoch auf der Festplatte gespeichert. Die meisten dieser Systeme enthalten nur eine minimale Softwareausstattung. Was man zusätzlich benötigt, muss man selbst zusammenstellen. Der Artikel zeigt, für wen sich Immutable-Distributionen eignen, stellt die wichtigsten Distributionen vor und zeigt, welche Vorteile und Einschränkungen zu erwarten sind.

Zielgruppen und Einsatzzwecke

Immutable-Distributionen bieten ein reduziertes und damit schnelles Betriebssystem, das sich für fast jedes Einsatzgebiet eignet. Die Hauptzielgruppe sind Installationen in Unternehmen auf zahlreichen Rechnern, bei denen es auf einen einheitlichen und verlässlichen Systemunterbau ankommt. Privatanwender profitieren von der Technik, wenn ein besonders stabiles und sicheres System gewünscht wird.

Einige der in diesem Artikel vorgestellten Distributionen sind relativ neu und teilweise auch noch nicht komplett auf Deutsch übersetzt. Wer etwas Erfahrung mit den neuen Systemvarianten gesammelt hat, kann die Systeme jedoch beispielsweise auf Rechnern installieren, die möglichst wartungsarm laufen sollen. Der Einsatz als Server ist derzeit nicht zu empfehlen, weil die Konfiguration des schreibgeschützten Systems dafür nicht flexibel genug ist.

Am weitesten fortgeschritten ist die Entwicklung bei Endless OS, das es bereit seit 2017 gibt. Als Alleinstellungsmerkmal bietet die Distribution ein Setupprogramm für Windows, über das sich eine Parallelinstallation durchführen lässt. Die Installation neben einem bereits vorhandenen Linux auf der gleichen Festplatte ist bei Endless OS und auch bei den anderen in diesem Artikel erwähnten Distributionen zurzeit nicht vorgesehen, aber immerhin auf einer zweiten Festplatte möglich. Wer die Syste-

Komfortable Installation: Endless OS ist eine der wenigen Linux-Distributionen, die sich von Windows aus installieren lassen. Über das Setuptool kann man auch einen USB-Stick erstellen.

me nur ausprobieren möchte, sollte für die Installation eine virtuelle Maschine in Virtualbox verwenden.

Vorteile und Einschränkungen

Das Immutable-Konzept ist mit Chrome-OS oder Android vergleichbar. Betriebssystem, Anwendungen, Konfiguration und Benutzerdaten sind voneinander getrennt. Programme laufen in einem geschützten Bereich und können an den Systemkomponenten nichts ändern. Die Installation von Flatpak-Paketen erfolgt als Standardbenutzer ohne erhöhte Rechte. Alles zusammen gewährleistet eine hohe Betriebssicherheit und Schutz vor Schadsoftware.

Updates des Basissystems erfolgen erst beim Neustart in einer Transaktion. Sollte beispielsweise während der Aktualisierung der Strom ausfallen, ist das Update entweder bereits vollständig installiert oder gar nicht. Bei Fehlern erfolgt ein erneuter Updateversuch beim nächsten Neustart.

Die Distributionen verwenden unterschiedliche Methoden für die Sicherung des jeweiligen Zustands. Bei Fedora Silverlight und Endless OS kommt Ostree (*https://github.com/ostreedev/ostree*) zum Einsatz, Open Suse Micro-OS setzt auf die Snapshot-Funktion des Dateisystems BTRFS.

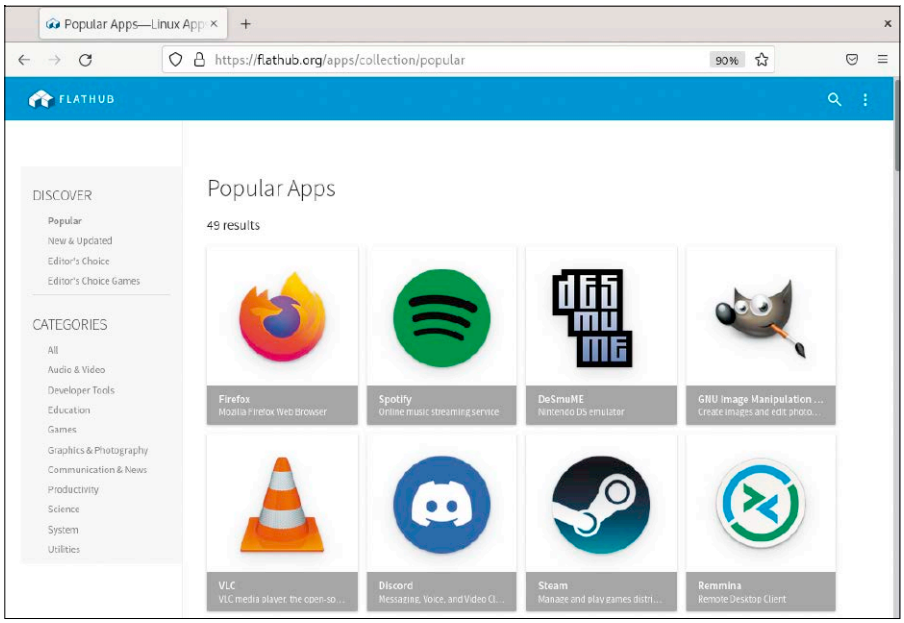
Einschränkungen: Wer ein Immutable-Linux verwenden möchte, muss sich in einigen Bereichen umstellen. Ein einfaches Desktopsystem mit den üblichen Anwendungen wie Firefox, Libre Office und dem VLC Media Player ist schnell eingerichtet. Das Softwareangebot ist jedoch beschränkt. Auf einfache Weise lassen sich nur Anwendungen installieren, die als Flatpak-Paket (siehe *https://flathub.org*) zur Verfügung stehen. Es ist aber möglich, einzelne Pakete zum schreibgeschützten Systemabbild hinzuzufügen (nicht bei Endless OS).

Zusätzliche Kernel-Module, etwa Treiber für Nvidia-Chips oder WLAN-Sticks, lassen sich nicht wie gewohnt einrichten. Man ist auf das angewiesen, was das Repositorium des Distributors bietet. Für Anwender mit sehr neuer Hardware sind Immutable-Distributionen daher nicht zu empfehlen.

Fedora Silverblue: Schlichter Gnome-Desktop

Auf der Downloadseite *https://silverblue.fedoraproject.org/download* wird eine ISO-Datei für die Installation angeboten und auf der gleichen Seite das Tool „Fedora Media Writer" für Linux, Windows und Mac-OS X, mit dem sich ein Installationsstick erstellen lässt. Die Installation erfolgt, indem Sie den PC vom Installationsmedium booten. Sie stellen zunächst Sprache und Tastaturbelegung ein, wählen nach einem Klick auf „Installations-Ziel" das Zielaufwerk aus und klicken auf „Fertig". Sollten darauf bereits Partitionen vorhanden sein, erscheint ein Fenster, in dem Sie auf „Speicherplatz freigeben" klicken und alle Partitionen löschen. Alle Daten darauf gehen verloren. Wenn eine zweite Festplatte alleine für Fedora zur Verfügung steht, wählen Sie diese. Der Bootloader wird auf der zweiten Festplatte eingerichtet, das Bootlaufwerk legen Sie nach der Installation im Firmwaresetup fest oder Sie verwenden das Firmware-Bootmenü.

Beim ersten Start des Systems öffnet sich ein Fenster, in dem man auf „Ersteinrichtung starten" klickt. Über den Assistenten legt man Benutzernamen und Passwort fest und kann danach den Gnome-Desktop nutzen. Der Desktop zeigt im Wesentlichen den Gnome-Standard; an Software ist nur



Programme im Container: Immutable-Distributionen setzen allesamt auf Flatpak. Welche Anwendungen verfügbar sind, lässt sich auf *https://flathub.org* herausfinden.

LINUX-PROGRAMME IM CONTAINER (TOOLBOX)

Auch wenn die Installation von Programmen im schreibgeschützten Basissystem möglich ist, gibt es eine bessere Methode. Das Hilfsprogramm Toolbox, das bei allen Immutable-Distributionen vorinstalliert ist, kann ein weiteres Linux in einem Container einrichten. Im Terminal erstellt man zunächst mit

```
toolbox create
```

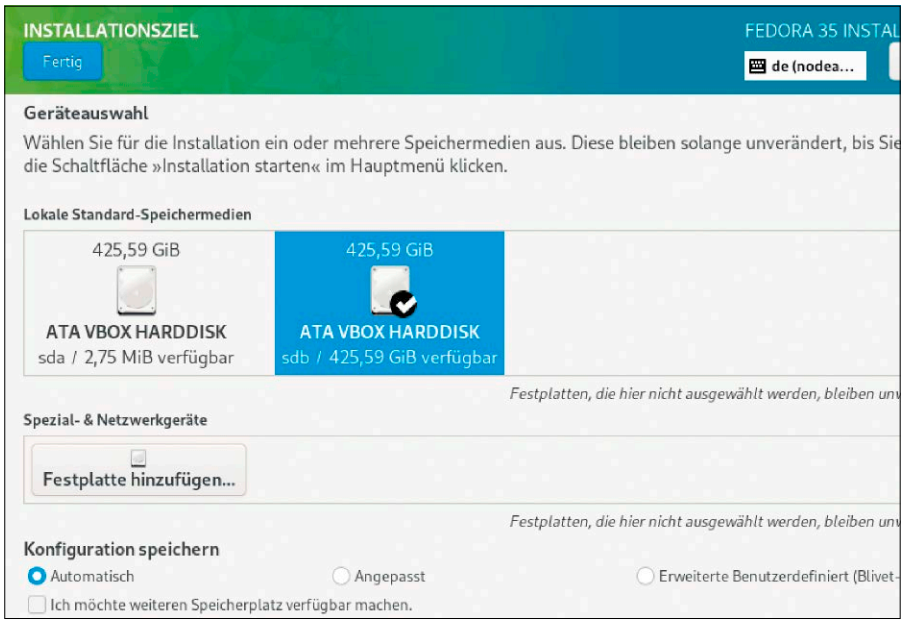
den Container. Fedora Silverblue und Endless OS richten dabei ein Fedora-System ein, Open Suse Micro-OS ein weiteres Open Suse. Mit

```
toolbox enter
```

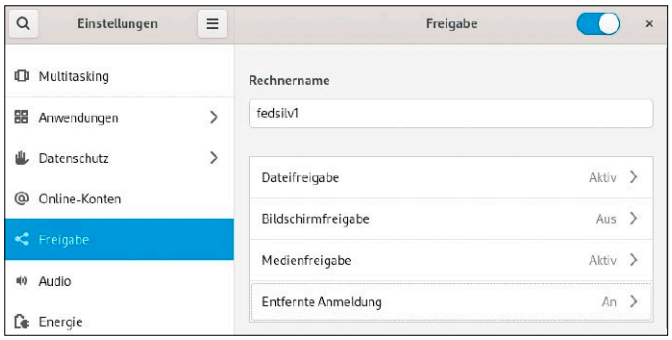
wechselt man in das Containersystem. Hier kann man mit dem standardmäßigen Paketmanager Software installieren, unter Fedora beispielsweise den Midnight Commander:

```
sudo dnf install mc
```

Anwendungen für die grafische Oberfläche lassen sich ebenfalls installieren. Serverdienste sind allerdings nicht nutzbar, weil sich Systemdienste nicht starten lassen. Der Container ist nicht völlig vom Hauptsystem getrennt. Das Home-Verzeichnis beispielsweise wird gemeinsam genutzt.



Installationsassistent: Fedora beansprucht eine eigene Festplatte. Eine Parallelinstallation neben Windows oder Linux ist im Setuptool nicht vorgesehen.



Netzwerkfreigaben: In den „Einstellungen“ lässt sich bei Fedora Webdav aktivieren („Dateifreigabe“). „Medienfreigabe“ aktiviert UPnP und „Entfernte Anmeldung“ den SSH-Zugriff.

wenig Software: Mit dabei ist Firefox, ansonsten nur Gnome-Tools wie der Dateimanager, der Texteditor Gedit und der Archivmanager. Was fehlt, muss man sich selbst zusammenstellen.

In Fedora sollte daher der erste Weg zur „Software“ (gnome-software) führen. Auf der Registerkarte „Aktualisierungen“ stehen nach einen Neuinstallation wahrscheinlich einige Systemupdates bereit, die man per Klick auf „Neu starten und Aktualisierungen installieren“ einrichtet. Nach dem Neustart öffnet man Software erneut und installiert per Klick auf „Alle aktualisieren“ die Softwareupdates. Ein Neustart ist danach nicht erforderlich.

Über „Erkunden“ oder die Suchfunktion wählt man die gewünschten Anwendungen. Zur Verfügung stehen beispielsweise Libre Office, Gimp und Gnome Musik. Da die Softwareauswahl im Flatpak-Repositorium von Fedora noch etwas eingeschränkt ist, sollten Sie im Terminal mit

```
sudo flatpak remote-add --if-not-exists flathub https://flathub.org/repo/flathub.flatpakrepo
```

flathub.org als Quelle hinzufügen. In gnome-software finden Sie dann beispielsweise auch die Flatpak-Pakete von VLC Media Player, Smplayer, Chromium und Skype.

Das Softwareangebot lässt sich außerdem durch Anwendungen im Appimage-Format vergrößern. Eine unvollständige Übersicht finden Sie unter *https://appimage.github.io/apps*, ansonsten bieten zahlreiche Open-Source-Projekte Anwendungen in diesem Format an. Appimage-Dateien müssen Sie nach dem Download nur ausführbar machen, um sie starten zu können.

Software im System installieren: Sollte es kein Flatpak für ein Programm geben, was etwa bei fast allen Terminaltools der Fall ist, kann die Installation direkt im System erfolgen. Den Dateimanager Midnight Commander beispielsweise richten Sie im Terminal mit

```
sudo rpm-ostree mc
```

ein. Danach müssen Sie Linux mit

```
sudo systemctl reboot
```

neu starten. Entsprechend lassen sich fehlende Tools wie htop (Infos zu Tasks und Tasksteuerung) oder inxi (Infos zu System, Hardware, Software, Netz) installieren. Die Installation mit rpm-ostree dauert relativ lange und Sie müssen Linux neu starten, bevor Sie das neue Tool nutzen können. Die Verwendung von Toolbox ist daher in den meisten Fällen vorzuziehen (siehe Kasten „Linux-Programme im Container“).

Netzwerkfreigaben: Bei Bedarf lässt sich der Samba-Server mit rpm-ostree installieren (Paket: „samba“). Alternativ verwenden Sie die Optionen in den „Einstellungen“ unter „Freigabe“. Aktivieren Sie „Dateifreigabe“ für den Datenaustausch über Webdav, was den Zugriff auf den Ordner „Öffentlich“ im Home-Verzeichnis über das Netzwerk ermöglicht. Bei anderen Linux-Rechnern taucht die Freigabe im Dateimanager unter „Andere Orte“ auf (Linux Mint: „Netzwerk“). „Medienfreigabe“ stellt ausgewählte Ordner mit Medieninhalten über UPnP bereit (Universal Plug and Play). Audio- und Videodateien lassen sich über den UPnP-Player eines Smart-TV oder am Computer mit VLC wiedergeben („Ansicht → Wiedergabeliste → Universal Plug'n'Play“). Die Option „Entfernte Anmeldung“ aktiviert den SSH-Server.

Endless OS: Zahlreiche Softwarepakete

Endless OS ist ein System auf der Basis von Debian. Der Schwerpunkt der Entwicklung liegt bei einem System, das bereits mit den wichtigsten Anwendungen ausgestattet ist und auch ohne Internetverbindung genutzt werden kann, etwa für den Einsatz in Gebieten mit unzureichender Internetabdeckung.

Im Downloadbereich (*https://endlessos.com/download*) gibt es einen Installer für Windows-Nutzer, der die Parallelinstallation ermöglicht und auch einen USB-Stick erstellen kann. Nutzer anderer Systeme laden unter „Try or Install on your Computer“ eine ISO-Datei herunter, außerdem gibt es Abbilder für virtuelle Maschinen und den Raspberry Pi 4. Aus der ISO-Datei lässt sich etwa mit Etcher (*https://www.balena.io/etcher*) ein Installationsstick er-

stellen. Beim Download wählen Sie „Basic Multilanguage“, das auch eine deutschsprachige Oberfläche bietet. Die deutlich größeren Downloads für andere Sprachen enthalten mehr Software, die sich aber beim Basic-System nachinstallieren lässt.

Nach dem Start vom Installationsmedium klicken Sie nach der Sprachauswahl für ein Livesystem auf „Ausprobieren“ oder für die Installation auf „Formatieren“. Die danach ausgewählte Festplatte wird neu formatiert und alle Daten gehen verloren. Nach dem ersten Start legen Sie Sprache, Benutzernamen und Kennwort fest.

Endless OS zeigt einen Gnome-Desktop, der sich an Chrome-OS orientiert. Ein Anwendungsmenü gibt es nicht, Programme lassen sich über die zugehörigen Desktopicons oder die Suche starten. Um die Übersichtlichkeit zu erhöhen, sind einige Aufgaben in Gruppen zusammengefasst, etwa „Arbeiten“ für Libre Office und „Hilfsprogramme“ für Systemtools. Beim Basic-System werden der Browser Chromium, Libre Office und Totem für die Medienwiedergabe eingerichtet.

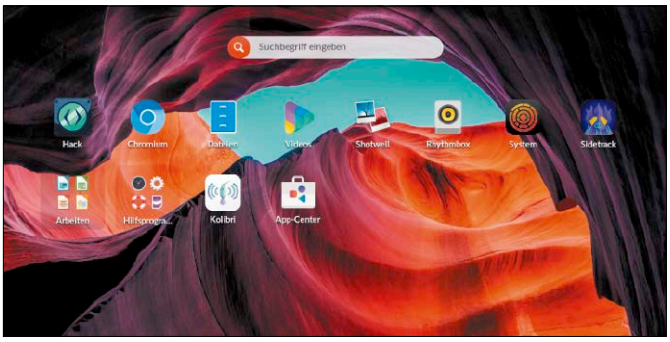
Das Tool gnome-software heißt bei Endless OS „App-Center“ und über dessen Registerkarte „Aktualisierungen“ lassen sich anstehende Updates installieren. Das System verwendet standardmäßig *https://flathub.org* sowie eigene Repositorien. Es stehen daher zahlreiche Anwendungen für die Installation bereit. Im Basissystem lässt sich bei Endless OS nichts installieren (siehe aber Kasten „Linux-Programme im Container“).

Netzwerkfreigaben: Wer Dateien über das Netzwerk bereitstellen möchte, geht in den „Einstellungen“ auf „Freigabe“. Mit der „Dateifreigabe“ lässt sich Webdav aktivieren, ferner SSH mit der Option „Entfernte Anmeldung“.

Open Suse Micro-OS: Mit Gnome oder KDE

Open Suse Micro-OS lässt sich über *https://en.opensuse.org/Portal:MicroOS/Downloads* als ISO-Abbild für den PC herunterladen („x86_64“). Außerdem gibt es Imagedateien für den Raspberry Pi, Virtualbox und Vmware. Aus der ISO-Datei lässt sich etwa mit Etcher (*www.balena.io/etcher*) unter Linux oder Windows ein Installationsstick erzeugen.

Booten Sie den PC vom Installationsmedium und wählen Sie im Menü „Installation“.



Endless OS: Das System enthält bereits bei einer Standardinstallation die wichtigsten Anwendungen als Flatpaks. Das Basissystem lässt sich allerdings nicht erweitern.

Nach der Sprachauswahl geben Sie die Systemrolle an. Für ein Desktopsystem wählen Sie „MicroOS Desktop Gnome (BETA)“ oder „MicroOS Desktop KDE Plasma (ALPHA)“. Wir haben uns wegen der besseren Stabilität für Gnome entschieden. Danach legen Sie Benutzernamen und Passwort fest. Setzen Sie ein Häkchen vor „Dieses Passwort für den Systemadministrator verwenden“. Bei den Installationseinstellungen wählt der Assistent automatisch die erste Festplatte, auf der alle Daten gelöscht werden. Nach Klicks auf „Partitionierung“ und „Geführtes Setup“ kann man – sofern vorhanden – auch eine andere Zielfestplatte angeben.

Beim ersten Start des Systems richtet Open Suse einige Flatpak-Pakete ein. Neben den üblichen Gnome-Tools ist nur Firefox installiert. Auch wenn man bei der Installation „Deutsch“ gewählt hat, ist die Oberfläche englischsprachig, was sich in den „Einstellungen“ unter „Region & Language“ ändern lässt. Die deutsche Lokalisierung ist jedoch noch nicht überall abgeschlossen.

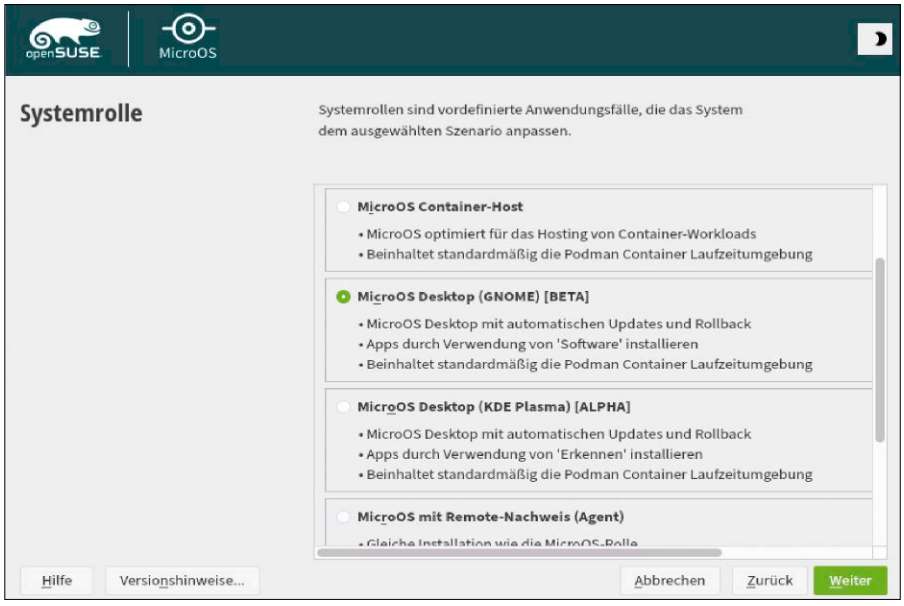
Wie bei Fedora beschrieben, sollte man über Software (gnome-software) zuerst System und Anwendungen aktualisieren. Danach richtet man die gewünschten Anwendungen ein. Open Suse Micro-OS verwendet standardmäßig *https://flathub.org* mit breiter Softwareauswahl.

Software im System installieren: Open Suse Micro-OS verwendet das Tool pkcon im Terminal. Mit beispielsweise

```
sudo pkcon install mc
```

installieren Sie den Midnight Commander, der Ihnen nach einem Neustart des Systems zur Verfügung steht (siehe auch Kasten „Linux-Programme im Container“).

Netzwerkfreigaben: In den „Einstellungen“ lässt sich unter „Freigabe“ der Fernzugriff über SSH aktivieren. Weitere Optionen gibt es nicht. Für einen Dateiserver lässt sich aber das Paket „samba“ über pkcon nachrüsten. ■



Open Suse Micro-OS: Bei der Installation kann man zwischen Gnome- und KDE-Desktop wählen. KDE ist allerdings noch als „Alpha“ gekennzeichnet und daher unvollständig.

Problemlösungen für Ubuntu 22.04

Auch LTS-Versionen Ubuntus sind nicht frei von Versäumnissen der Entwickler oder von eigenwilligen, unpraktischen Standardeinstellungen. Die folgende Sammlung präsentiert häufige Probleme und deren Lösungen in Ubuntu 22.04 LTS und Varianten.

VON DAVID WOLSKI

Kaum eine andere Distribution bekommt bei jeder Ausgabe so viel Aufmerksamkeit wie Ubuntu. Die Entwicklung von Ubuntu und die einzelnen Softwarepakete sind weiterhin eng mit Debian GNU/Linux verbunden, da dies die Basis für Ubuntu stellt. Auch im Entwicklerteam gibt es einige personelle Überschneidungen. Die Größe der Ubuntu-Community erlaubt eine Veröffentlichung alle sechs Monate und eine Ausgabe mit Langzeitsupport von fünf Jahren im Zweijahresrhythmus. Die praktische Erfahrung seit April hat gezeigt, dass Ubuntu 22.04 nicht weniger Probleme macht als noch die LTS-Version 22.04. Einige Schwierigkeiten mit Firefox als Snap-Paket und mit dem aggressiven Out-of-Memory-Killer von Systemd verlangen Nacharbeiten, die eine LTS-Version Ubuntus eigentlich vermeiden sollte. Einige dieser Probleme und Lösungen sind keine Fehler, sondern einfach auf einem Desktopsystem unpraktische Standardeinstellungen. Canonical hat mit seiner Linux-Distribution heute eher Server- und Cloud-instanzen als den Endanwender-Desktop im Fokus.

Die folgenden Themen behandeln Stolperfallen und Ungereimtheiten, die uns in der Redaktion selbst in Ubuntu 22.04 begegnet sind oder für welche auf der Frage-Antwort-Webseite *https://askubuntu.com* besonders häufig nach Lösungen gesucht wird. Einige der präsentierten Lösungen sind auch für Ubuntu 22.10 beziehungsweise im kommenden 23.04 relevant, denn auch dort werden wieder Snap-Pakete zu bändigen sein.

OOMD: Aggressiver Programmkiller

Server sollen auch in Situationen mit wenig freiem Arbeitsspeicher weiterlaufen und dürfen im Falle eines Speichermangels nicht einfach stehenbleiben. Systemd hat deshalb den Out-of-Memory-Dämon (OOMD) für Server eingeführt, der besonders speicherhungrige Prozesse bei knappem Arbeitsspeicher radikal beendet. Ab Ubuntu 22.04 ist dieser Programmkiller auch auf Desktopinstallation aktiviert und verursachte vielen Anwendern Probleme, weil vor allem Browserinstanzen auf Rechnern mit weniger als vier GB RAM oft abgeschossen wurden.

```
jammy@jellyfish: ~
            0 htop
[ 4498.074931] oom-kill:constraint=CONSTRAINT_NONE,nodemask=(null),cpuset=/,mems_allowed=0,global_oom,task_memcg=/user.slice/user-1000.slice/user@1000.service/app.slice/app-gnome-libreoffice\x2dwriter-2859.scope,task=soffice.bin,pid=2943,uid=1000
[ 4498.074977] Out of memory: Killed process 2943 (soffice.bin) total-vm:2232568kB, anon-rss:766672kB, file-rss:0kB, shmem-rss:0kB, UID:1000 pgtables:2996kB oom_score_adj:0
[ 4503.384477] audit: type=1400 audit(1672730570.606:258): apparmor="ALLOWED" operation="connect" profile="libreoffice-soffice" name="/run/user/1000/at-spi/bus" pid=8472 comm="soffice.bin" requested_mask="wr" denied_mask="wr" fsuid=1000 ouid=1000
[ 4503.429405] audit: type=1400 audit(1672730570.650:259): apparmor="ALLOWED" operation="file_perm" profile="libreoffice-soffice" name="/run/user/1000/at-spi/bus" pid=8472 comm="soffice.bin" requested_mask="r" denied
```

Übereifriger Programmkiller: OOMD ist in Ubuntu 22.04, 22.10 und 23.04 unterwegs. Auf Desktopsystemen mit weniger als vier GB RAM hilft ein Abschalten des Dienstes.

In Ubuntu 22.04.1 LTS und 22.10 gab es deshalb außerplanmäßige Updates für OOMD: Der Out-of-Memory-Dämon hat in der Konfigurationsdatei „/usr/lib/systemd/system/-.slice.d/10-oomd-root-slice-defaults.conf“ die Ergänzung „ManagedOOM Swap=auto“ erhalten und ignoriert deshalb zumindest Auslagerungsaktivitäten. Auf Systemen mit wenig Arbeitsspeicher wird OOMD auf Desktops aber weiterhin Programme beenden, die plötzlich sehr viel RAM beanspruchen. Um das Verhalten zurückverfolgen, dient folgendes Kommando, das die letzten Aktionen des automatischen Programmkillers in den Kernel-Meldungen mit den Zeilen „Out of memory“ zeigt:

```
sudo dmesg
```

Um OOMD in Ubuntu dauerhaft zu deaktivieren, dient dieser Befehl:

```
systemctl disable --now systemd-oomd
```

Nach unserer Einschätzung ist OOMD auf Desktopsystemen nicht hilfreich und nicht notwendig.

Snaps: Updates anhalten

Über ein gewöhnliches Systemupdate mittels apt wird Snap-Software nicht aktualisiert. Stattdessen verfügen Snaps über eine separate Updatefunktion, die alle installierten Pakete dieser Art täglich automatisch viermal aktualisieren will. Im Terminal zeigt das Kommando

```
snap refresh --time
```

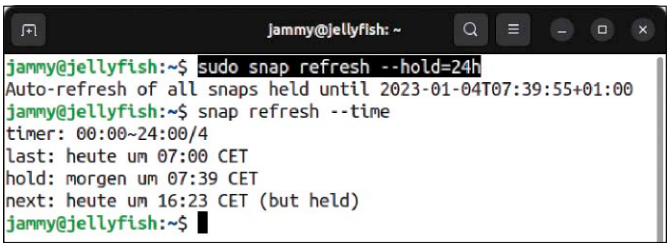
an, wann der nächste Check erfolgen soll. Diese kurze Frequenz hat einen Haken: Läuft eine Snap-Anwendung, so kann das Paket nicht aktualisiert werden und wird seit Ubuntu 22.04 auf den nächsten Updatecheck verschoben. Um neue Versionen installierter Snaps manuell zu installieren, kann dann der eingegebene Befehl

```
sudo snap refresh
```

manuell eine Aktualisierung ausführen. Unterwegs mit einem Notebook, wenn eine Internetverbindung deutlich langsamer ist, sorgt das automatische Update von Snaps wegen der knappen Bandbreite für Ungemach und wird eventuell gar nicht fertig. Für diesen Fall gibt es die neue Möglichkeit, Updates auszusetzen. Dafür ist eine aktuelle Version des Snapd-Rahmenwerks nötig, welche der Befehl

```
sudo snap refresh snapd --channel=latest/edge
```

installiert. Anschließend kann die Eingabe des Kommandos



Einen Tag lang anhalten: Damit Snap-Aktualisierungen im Hintergrund nicht Bandbreite verschwenden, können diese Updates mit diesem Befehl aufgeschoben werden.

Wo bleibt der Sound? Die Mixeranwendung Pavucontrol kann die Audioeinstellungen, Geräte und Ausgänge überprüfen. In diesem Beispiel fehlt in Ubuntu 22.04 eine Konfigurationsdatei.

```
sudo snap refresh --hold=24h
```

die automatische Installation von neuen Snap-Versionen für 24 Stunden anhalten.

Pipewire und Pulseaudio

Bei der Wahl der Soundserver setzt Ubuntu 22.04 auf einen Mix aus dem herkömmlichen Pulseaudio und dem modernen Pipewire. Letzteres ist im System für Screensharing und Web RTC in Browsern unter Wayland zuständig. Die sonstigen Aufgaben bei der Soundausgabe erledigt weiterhin Pulseaudio.

Es passiert vor allem bei Upgrades von älteren Ubuntu-Systemen auf 22.04, dass Pulseaudio in diesem Gespann zunächst nicht funktioniert. Die Mixeranwendung Pavucontrol ist zur Überprüfung nötig, ob die Ausgabe überhaupt unter „Konfiguration“ eingeschaltet ist. Sie muss aber zunächst mit

```
sudo apt install pavucontrol
```

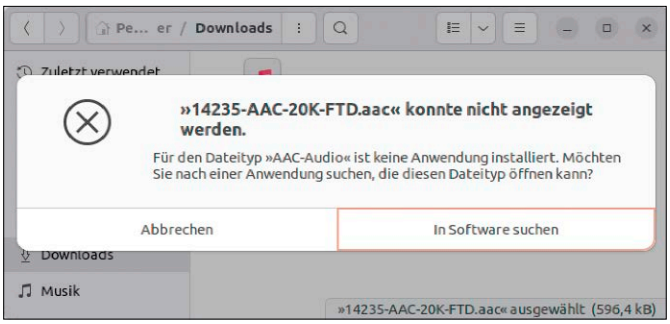
installiert werden. Gibt es keine Ausgänge für Pulseaudio beziehungsweise nur ein Ausgabegerät namens „dummy“, so ist meist die Konfiguration nach einem Upgrade nicht komplett. Die beiden Befehle

```
sudo touch /usr/share/pipewire/media-session.d/with-pulseaudio
systemctl --user restart pipewire-session-manager
```

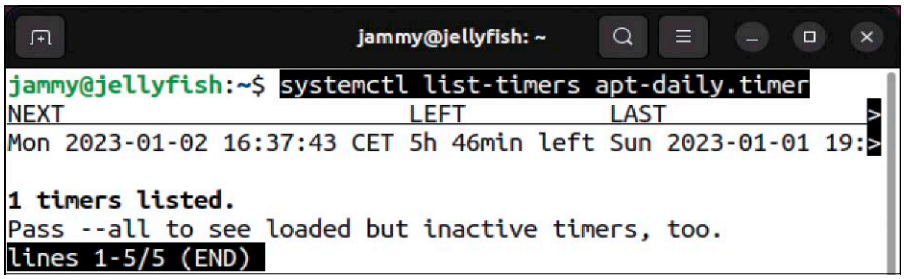
korrigieren das Problem.

Nachrüsten: Codecs und Extras

Ubuntu liefert in seinen Paketquellen nicht nur Open-Source-Programme aus, sondern auch Linux-Software, die einer kommerziellen oder auch unklaren Lizenz unterlie-



Diese Suche läuft oft ins Leere: Gnome versucht, ein passendes Programm für eine Mediendatei zu finden, und kann auch nach Codecs suchen, aber dies gelingt meistens nicht.



Wann ist die nächste Systemaktualisierung? Die von Haus aus aktivierten „Unattended Upgrades" blockieren den Paketmanager bei umfangreichen Updates eine ganze Weile.

gen. Dazu zählen einige Audio- und Videocodecs und Truetype-Fonts von Microsoft, die für die Darstellung einiger Webseiten und Dokumente vorteilhaft sind. Die von einigen Gnome-Programmen angebotene Suche nach Codecs in den Paketquellen ist nicht immer erfolgreich. Zuverlässiger ist es, gleich nach der Ubuntu-Installation alle häufig benötigten Codecs und Extras in einem Terminalfenster mit diesem Befehl

```
sudo apt-get install ubuntu-
 restricted-extras gstreamer1.0-
 plugins-bad gstreamer1.0-plugins-
 ugly
```

nachzurüsten.

Blockiertes apt: Unattended Upgrades

Eher für Server interessant, aber auch in der Desktopausgabe von Ubuntu 22.04/22.10 aktiviert, ist die automatische Installation von Sicherheitsupdates im Hintergrund über den Dienst „Unattended Upgrades". Damit die Server der Paketquellen dabei nicht überlastet werden, lösen Ubuntu-Systeme den Download an zufälligen Zeiten aus. Wann das eigene System wieder ein Hintergrundupdate startet, zeigt das Kommando

```
systemctl list-timers apt-daily.
 timer
```

in der Kommandozeile an.

Bei langsamen Internetverbindungen oder im WLAN führt dies nach dem Start des Systems immer wieder dazu, dass der Paketmanager apt längere Zeit nicht für andere Aktionen verfügbar ist, weil im Hintergrund Updates installiert werden. Der Hinweis von apt in der Kommandozeile lautet dann „E: Could not get lock /var/lib/dpkg/lock - open (11: Ressource unavailable)".

Wenn dies ein immer wieder auftretendes Problem ist, dann empfiehlt es sich, die Aktualisierungen besser regelmäßig manuell mit *sudo apt upgrade* einzuspielen und die automatischen Sicherheitsupdates abzuschalten. Auf Desktopsystemen ist dies völlig legitim. Um den Dienst zu konfigurieren, dient der Aufruf dessen Konfigurations-Scripts:

```
sudo dpkg-reconfigure -plow
 unattended-upgrades
```

In einem angezeigten textbasierten Menü schaltet dann die Auswahl „Nein" die automatischen Updates aus.

Paketmanager: Werbung abschalten

Wer in Ubuntu 22.04 mit apt in der Kommandozeile Updates und das Paketmanagement vornimmt, erhält beim Aufruf im Terminal hin und wieder Werbung für Ubuntu Pro. Dies ist ein Extraservice Canonicals, welcher nach einer Registrierung insgesamt zehn Jahre Updates für Ubuntu LTS verspricht. Nach Kritik an den zusätzlichen Nachrichten hat Canonical verraten, dass sich diese Werbeeinblendungen mit dem Kommando

```
sudo pro config set apt_news=false
```

sehr einfach abschalten lassen.

Server: Einfachere Netzwerkkonfiguration

Während Debian-Server ihre Netzwerkeinstellungen im alten Stil über die Datei „/etc/network/interfaces" erledigen, nutzt der Ubuntu Server schon seit Ausgabe 18.04 LTS seine eigene Konfigurationsmethode über Netplan.io. Es handelt sich dabei um einen Parser für das YAML-Format, um auch komplexe Netzwerkkonfigurationen abzubilden. Netplan.io ist aber speziell für die Ubuntu-Server-Ausgabe gemacht und in keiner anderen Linux-Distributionen per Standard eingerichtet. Von Canonical gibt es auf der Webseite *https://netplan.io* eine Vorstellung mit englischsprachigen Beispielen zum Einstieg.

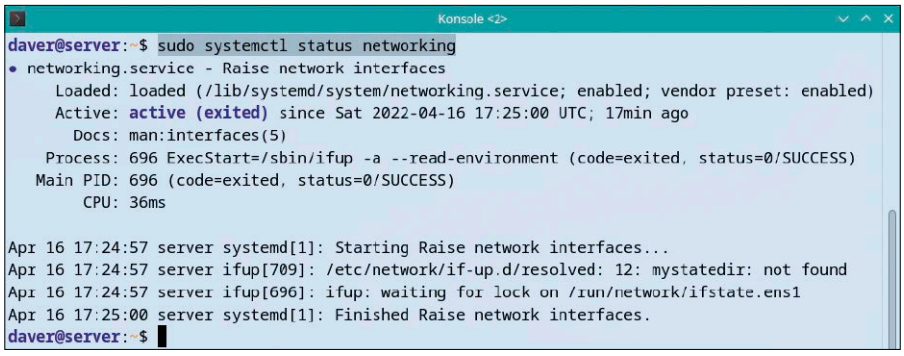
Netplan.io ist nur eine Abstraktionsschicht mit eigener Syntax. Wer diese nicht verwenden will, kann wieder die herkömmliche Netzwerkkonfiguration im Debian-Stil auf einem Ubuntu-Server nutzen, der dabei aber vorübergehend offline geht. Das ist beim Wechsel zu bedenken. Zuerst gilt es, den Hardwarenamen der Netzwerkschnittstelle zu ermitteln, die der Befehl

```
ip a
```

im Abschnitt „2:" für Ethernet anzeigt und die beispielsweise „enp3s0" lautet. Diese Angabe muss man sich notieren, denn sie ist für die herkömmliche Konfigurationsdatei wichtig.

ALTERNATIVE NETZWERK-KONFIGURATION

```
#loopback
#Datei /etc/network/interfaces
auto lo
iface lo inet loopback
#Ethernet, "enp3s0" bitte anpassen
auto enp3s0
allow-hotplug enp3s0
iface enp3s0 inet dhcp
```



Herkömmliche Netzwerkkonfiguration in Ubuntu 22.04 nutzen: Die Ausgabe von systemctl zum traditionellen Netzwerkdienst zeigt, ob der Umstieg geklappt hat, und hilft bei der Fehlersuche.

Den herkömmlichen Debian-Netzwerkdienst installiert dann dieses Kommando:

```
sudo apt install ifupdown
```

Wie bei Debian erwartet dieser Dienst eine klassische Konfigurationsdatei namens „/etc/network/interfaces“, die mit root-Recht erstellt wird:

```
sudo nano /etc/network/interfaces
```

Diese Datei erhält den Inhalt, wie er im Kasten „Alternative Netzwerkkonfiguration“ hier abgebildet ist. Die Angabe „enp3s0“, also der vorher ermittelte Hardwarename der Schnittstelle, muss unbedingt angepasst werden. Damit die Netzwerkschnittstelle automatisch über DHCP ihre IPv4- und IPv6-Adressen bezieht, verlangt auch noch die Datei „/etc/dhcp/dhclient.conf“ eine Ergänzung: Ganz unten fügt man hier diese Zeile ein:

```
send dhcp-client-identifier =
  hardware;
```

Nun kann vor dem Neustart des Serversystems der Systemd-Dienst für Netplan.io mit folgendem Kommando deaktiviert werden:

```
sudo systemctl mask networkd-
  dispatcher systemd-networkd-wait-
  online systemd-networkd.socket
  systemd-networkd
```

Danach steht der Neustart des Ubuntu-Systems mit *sudo reboot* an und dort zeigt dann die Eingabe von

```
sudo systemctl status networking
```

an, ob alles geklappt hat. Schlägt die Initialisierung des Netzwerks fehl, so liegt dies meist an einer ungültigen Hardwareadresse der Ethernet-Schnittstelle und es lohnt sich hier eine erneute Kontrolle auf die Ausgabe von „ip a“.

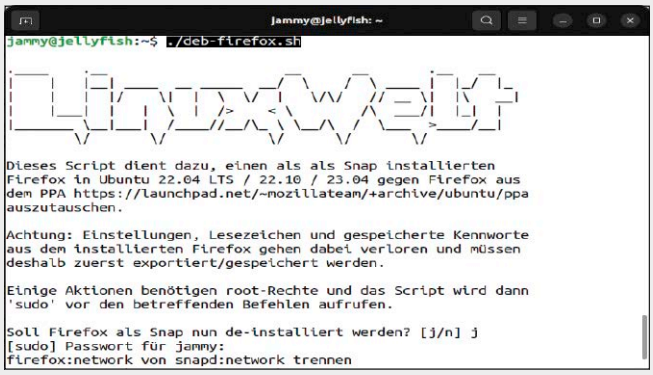
Ubuntu-Server bei Internetprovidern: Ist ein Ubuntu-Server nur per SSH erreichbar, dann ist diese Operation durchaus riskant, denn schlimmstenfalls ist die Maschine erst mal nicht erreichbar. Es empfiehlt sich deshalb zuvor als Nothaken, die Möglichkeiten einer Verbindung zum Server per KVM oder webbasierter Konsole zu aktivieren oder auch gleich alle Schritte über eine Notfallkonsole auszuführen. Die meisten Serveranbieter und Clouddienste bieten diese an. ■

FIREFOX UND CHROMIUM ALS DEB-PAKET

Als Canonical ausgerechnet Chromium und dann auch noch den Standardbrowser Firefox als Snap-Paket in Ubuntu auslieferte, war die Skepsis bei vielen Anwendern zu Recht groß. Denn die Browser starten als Snap zu langsam und einige Add-ons wollten auch nicht mehr funktionieren, weil Berechtigungen fehlen. Mittlerweile hat Canonical bei der Einbindung von Firefox nachgebessert – der Start ist deutlich flotter und viele Erweiterungen wie etwa die Gnome-Browsererweiterung zur Einbindung von Gnome-Shell-Extensions von *https://extensions.gnome.org* funktionieren wieder. Dennoch bleibt der Start auf Systemen mit schwächeren CPUs zunächst bei beiden Browsern schleppend, denn Snaps liefern ein gepacktes Dateisystem mit, das erst mal dekomprimiert werden will.

Firefox und Chromium gibt es in den aktuellen Ubuntus nicht mehr in den offiziellen Paketquellen. Allerdings liefern weiterhin PPAs, also externe Paketquellen, die Webbrowser stets aktuell in der üblichen Form als DEB-Paket aus: Für Firefox gibt es von der Mozilla Foundation das PPA *https://launchpad.net/~mozillateam/+archive/ubuntu/ppa* und für Chromium bietet sich *https://launchpad.net/~phd/+archive/ubuntu/chromium-browser* an. Eine Schwierigkeit ist es aber, Firefox oder Chromium als Snap erst einmal loszuwerden. Denn bei dem vorhandenen DEB-Paket in den Standard-Paketquellen handelt es sich um einen Platzhalter, der immer wieder das Snap installiert. Auch ein Systemupdate würde den als DEB installierten Firefox wieder gegen das Snap-Paket austauschen.

Es ist also mehr zu beachten: Per apt-Pinning muss das nachträglich installierte DEB eine höhere Priorität bekommen als das Snap-Paket aus den regulären Quellen. Gut ist es außerdem, falls die unbeaufsichtigten Updates aktiviert sind, diese auf Firefox beziehungsweise Chromium automatisch auf den neusten Stand bringen. Insgesamt kommen hier eine Menge kleine Handgriffe im Terminal zusammen, die in der Wiederholung auf mehreren Ubuntu-Systemen lästig werden. Wir haben deshalb für die Installation von Firefox und Chromium über die



Firefox als DEB-Paket: Das Script von Heft-DVD deinstalliert das Snap-Paket in Ubuntu 22.04 und holt den Browser vom offiziellen PPA der Mozilla Foundation.

genannten PPAs jeweils ein Shell-Script erstellt, dass diese Handgriffe übernimmt und dabei gut nachvollziehbar ist. Für Firefox ist das Script „deb-firefox.sh“ im Unterverzeichnis „Software“ auf der Heft-DVD und für Chromium erledigt „deb-chromium.sh“ die Installation. Zuvor werden die Browser als Snap erst deinstalliert, falls vorhanden. Diese Aktionen verlangen nach dem sudo-Passwort und fragen dies im Terminal zuvor ab. Um eines der Scripts zu starten, kopiert man es in einen beliebigen Ordner, macht es mit

```
chmod +x deb-firefox.sh
```

ausführbar und ruft es dann mit

```
./deb-firefox.sh
```

auf. Das Script „deb-chromium.sh“ verlangt die gleiche Behandlung. Die weiteren Schritte sind in der Ausgabe des jeweiligen Scripts erläutert und es gibt auch eine kurze Anleitung, wieder das Snap zu installieren, falls gewünscht.

Hinweis: Eine Deinstallation des Snap-Pakets löscht alle vorhandenen Profildaten, Lesezeichen und eventuell gespeicherten Passwörter. Diese Daten sollte man deshalb zuvor exportieren und danach im klassischen DEB-Browser wieder importieren.

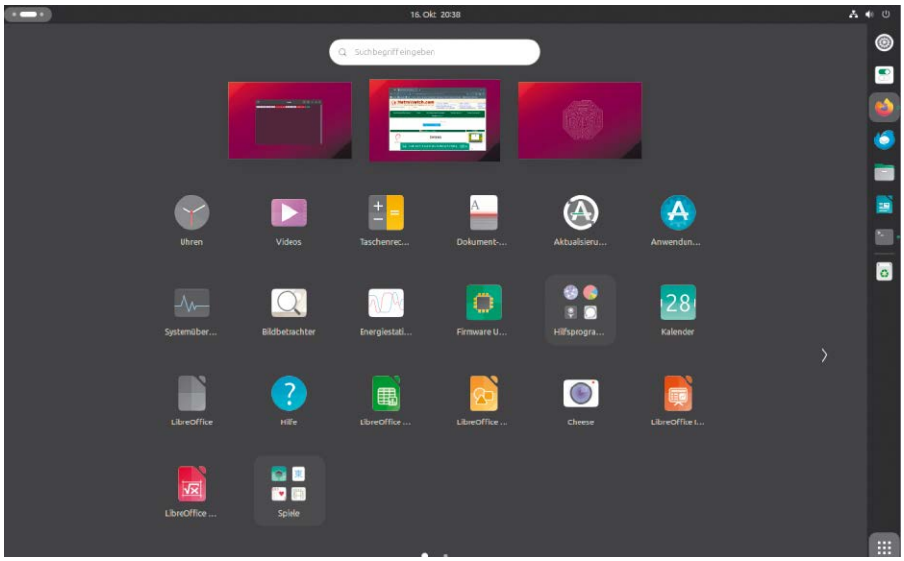
Das neue Ubuntu 23.10

Mit etwas Verspätung hat Canonical die Oktoberausgabe Ubuntu 23.10 veröffentlicht. Es handelt sich um eine STS-Zwischenversion mit neun Monaten Support bis Juli 2024, die jedoch ab April 2024 per Upgrade auf Version 24.04 (LTS) gehievt werden kann.

VON HERMANN APFELBÖCK

Neben der neuen Ubuntu-Hauptedition von Canonical mit Gnome-Desktop sind wie immer zeitgleich auch die offiziellen Ubuntu-Flavours Kubuntu, Xubuntu & Co. in neuer Version 23.10 erschienen. Alle Editionen stehen auf der Systembasis der Ubuntu-Hauptedition, unterscheiden sich aber in ihrer Desktopumgebung inklusive der zugehörigen Tools und verwenden zum Teil auch einen anderen Installer (Kubuntu, Lubuntu). Wegen der kurzen Laufzeit von neun Monaten ignorieren viele Anwender diese STS-Ausgaben (Short Term Support) und konzentrieren sich auf LTS-Versionen (Long Term Support). Die nächste LTS-Version ist schon im April 2024 fällig: Lohnt sich noch ein Intermezzo mit der Version 23.10?

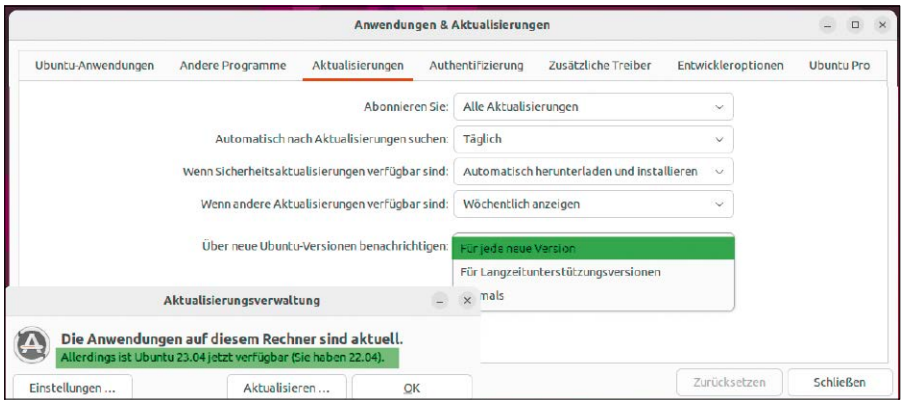
Die Verspätung: Die Hauptedition von Ubuntu (Gnome) und Ubuntu Budgie verspäteten sich um eine knappe Woche. Ursache war antisemitische Hetze, die in die ukrainische Lokalisierung des neuen Installers mit Flutter-Oberfläche eingebaut war. Da nur Ubuntu und Ubuntu Budgie diesen Flutter-Installer verwenden, waren die restlichen Flavours nicht betroffen. Canonical stellte bis zur Bereinigung des Installers temporär (sechs Tage lang) ein „Legacy"-ISO zur Verfügung, das die Ubuntu-Hauptedition mit dem alten Installer auf den Rechner brachte. Der Schmutz ist inzwischen auch aus dem Flutter-Installer vollständig entfernt, mahnt aber eindrücklich, wie verwundbar Open-Source-Projekte sein können, wenn an Kontrollmechanismen gespart wird …



STS-Zwischenversion: Ja oder nein?

Ubuntu 23.10 ist wie alle Zwischenversionen keine Sackgasse, sondern kann im Frühjahr 2024 auf die LTS-Langzeitversion 24.04 upgraden. Diese bietet dann drei Jahre (Kubuntu, Xubuntu, Lubuntu etc.) oder fünf Jahre (Hauptedition von Canonical mit Gnome) Updatesupport via Aktualisierungsverwaltung. Bei kurzlebigen Ubuntu-Zwischenversionen stellt sich dennoch die Frage, ob sich die Installation oder das Upgrade einer älteren Version auf 23.10 tatsächlich lohnt. Dazu folgende Empfehlungen:

- Neueinsteiger können ohne Bedenken zur Version 23.10 greifen, weil im nächsten Jahr das Upgrade auf die LTS-Version 24.04 möglich ist. Bevor Version 23.10 abläuft, bleiben drei Monate Zeit, um sie per Upgrade auf Version 24.04 zu befördern. Ubuntus „Aktualisierungsverwaltung" bietet dies aktiv an, sobald der Nachfolger vorliegt (siehe dazu den Kasten „Installation und Upgrade").
- Wer aktuell die Zwischenversion Ubuntu 23.04 installiert hat, muss auf Version 23.10 upgraden, denn 21.04 läuft im Januar 2022 ab.
- Für aktuelle Nutzer der Langzeitversion Ubuntu 22.04 gibt es wenige Gründe für ein Upgrade auf 23.10, es sei denn, Kernel 6.5 wird dringend benötigt, um ein Problem mit aktueller Hardware aus dem Weg zu schaffen. Der aktuellere Kernel bringt tatsächlich relevante Verbesserungen mit (siehe unten), akute Hardwareprobleme wird er aber kaum beheben, zumal die LTS-Version 22.04 durch Aktualisierung inzwischen bei Point Release 22.04.3 angelangt ist, das auch bereits den Kernel Version 6.2 enthält.



Upgrade zur Zwischenversion Ubuntu 23.10: Die Langzeitversion 22.04 wird diesen Vorgang nicht anbieten, solange hier nicht explizit „Für jede Version“ eingetragen ist.

Ubuntu 23.10: Allgemeine Neuerungen

Brandaktueller Kernel: Alle Ubuntus 23.10 erhalten den Linux-Kernel 6.5. Das ist dieses Mal, wie es der zeitliche Zufall will, die aktuellste Basis, die eine Linux-Distribution derzeit anbieten kann. Brandneue Kernel sorgen immer für ein Plus an unterstützter, neuer Hardware. An erster Stelle steht, dass Ubuntu 23.10 über den aktualisierten Kernel erstmals Unterstützung für Wi-Fi 7 mitbringt. Auf AMD-Ryzen-CPUs unterstützt Kernel 6.5 alle P-States (CPU-Leistungszustände) und arbeitet damit stromsparender. Durch gleichzeitige Auslastung aller CPU-Kerne sollen sich außerdem die Bootzeiten generell verkürzen. Noch deutlicher wird dies mit virtuellen Linux-Systemen, weil diese den zugewiesenen Arbeitsspeicher jetzt nicht mehr komplett sofort adressieren müssen, sondern dynamisch – erst sobald er in der virtuellen Maschine gebraucht wird.

Mehr Sicherheit für PPA-Software: Personal Package Archives (PPAs) erlauben Ubuntu-Distributionen seit vielen Jahren, das Softwareangebot durch externe Quellen zu erweitern. Die Methode unterscheidet sich substanziell vom Windows-Wildwuchs beliebiger Installationspakete, weil der Weg immer über die Site *https://launchpad.net* führt, die vom Ubuntu-Distributor Canonical betrieben wird. Trotzdem wurde mittlerweile als theoretisches Sicherheitsrisiko eingestuft, dass die Zuordnung einer PPA-Quelle zu ihrem Schlüssel nicht eindeutig ist. Dies könnte theoretisch genutzt werden, einen vorhandenen GPG-Schlüssel zur Installation einer falschen PPA-Software zu missbrauchen. Daher wird das bisherige Verfahren schrittweise abgeschafft und die Schlüsselinformation jeweils mit der Paketquelle gespeichert. Die Zuordnung ist somit eineindeutig und das Entfernen eines PPA entfernt auch den zugehörigen Schlüssel. Bis dies für alle PPA-Pakete abgeschlossen ist, ist gelegentlich mit Warnmeldungen über ungültige „Apt-Keys“ zu rechnen.

Konsolidierte Netzwerkverwaltung: Wenngleich das normale Desktopanwender kaum mitbekommen dürften, konkurrieren unter Ubuntu seit sechs Jahren zwei Konzepte zur Netzwerkkonfiguration – der Network-Manager und Netplan. Diese Koexistenz bleibt zwar bestehen, sodass Systembenutzer weiterhin die Basiseinstellungen über den grafischen Networkmanager (in der Systemleiste) erledigen können. Aufgehoben wurde aber die Konkurrenz der Methoden: Die Netplan-Konfiguration ist bestimmend und der Network-Manager wird zum Front-End degradiert, das im Hintergrund Netplan verwendet. Damit sollten

INSTALLATION UND UPGRADE

Die ISO-Images mit den Ubuntu-Live- und Installationsmedien sind erheblich angewachsen. Unter drei Gigabyte geht nichts mehr, und die Hauptedition geht Richtung fünf GB. Dies ist der Grund, warum wir Ihnen auf der DVD nur noch diese Hauptedition mit Gnome anbieten können. Infos und Downloads für alle weiteren Ubuntu-Flavours finden Sie auf der Sammelseite *https://ubuntu.com/desktop/flavours*. Flavours mit unterschiedlichen Desktops gibt es mittlerweile fast zu viele: Kubuntu (KDE), Lubuntu (LXQT), Xubuntu (XFCE), Ubuntu Budgie, Ubuntu Cinnamon, Ubuntu Mate und Ubuntu Unity.

Es handelt sich bei allen ISO-Downloads um hybride Abbilder, die sowohl von DVD wie von USB booten. Statt dafür einen DVD-Rohling zu verschwenden (etwa mit Brasero, Infrarecorder), können Sie das gewünschte ISO-Image mit den bewährten Werkzeugen auf USB-Stick kopieren (u. a. Etcher, Gnome-Disks, unter Windows mit USB Imager oder ebenfalls mit Etcher). Diese Werkzeuge sind selbsterklärend und verlangen nur die Angaben der ISO-Datei und des USB-Sticks als Kopierziel.

Wir empfehlen nach dem Booten des ISO-Livesystems auf dem Zielrechner für Installationen immer die Option „Ausprobieren“ (statt direktes „Installieren“) und den anschließenden Start des Installationslinks am Desktop des Livesystems. Das Livesystem im Hintergrund bietet in Zweifelsfällen bessere Kontrolle: So kann dann etwa das Terminal oder die Laufwerksverwaltung Unsicherheiten hinsichtlich der Laufwerkskennungen beseitigen, bei Bedarf kann vor der Installation noch eine Datensicherung erfolgen.

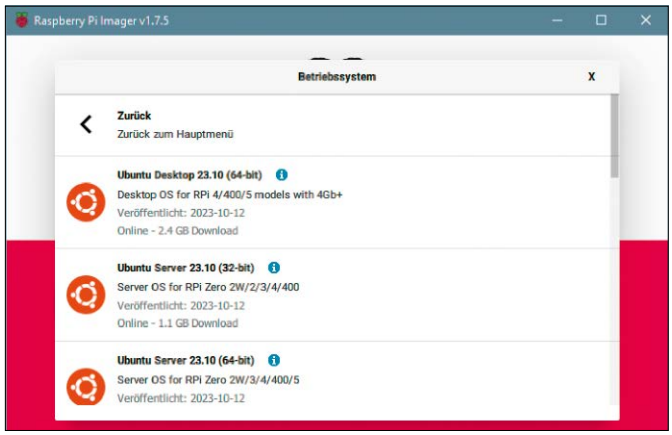
Upgrade älterer Versionen: Alle Ubuntu-Editionen bieten über das Systemtool „Aktualisierungsverwaltung“ das Upgrade auf die jeweils aktuelle Version an. Dazu muss vorher mit der „Aktualisierungsverwaltung“ oder im Terminal mit

```
sudo apt update
sudo apt upgrade
```

eine vollständige Systemaktualisierung erfolgt sein. Außerdem muss unter „Anwendungen & Aktualisierungen → Aktualisierungen“ der unterste Punkt „Auf jede neue Version“ gesetzt sein. Beim Start der „Aktualisierungsverwaltung“ erhalten Sie dann das Upgradeangebot gemäß Abbildung. Auf genau dieselbe Weise bringen Sie Version 23.10 im nächsten Frühjahr auf die LTS-Version 24.04.

Systemverwalter künftig konfliktfrei arbeiten können, unabhängig davon, ob sie Einstellungen in Netplan oder im Network-Manager ändern.

Raspberry Pi 5: Ubuntu 23.10 läuft von Haus aus auf dem neuen Raspberry Pi 5. Der einschlägige Raspberry Pi Imager (*www.raspberrypi.com/software)* für den Systemdownload und die Einrichtung bietet als Ubuntu 23.10 erstaunlicherweise die relativ anspruchsvolle Gnome-Hauptedition an. Laut ersten Testberichten bedient der neue Raspberry 5 diesen Desktop aber jederzeit flüssig.

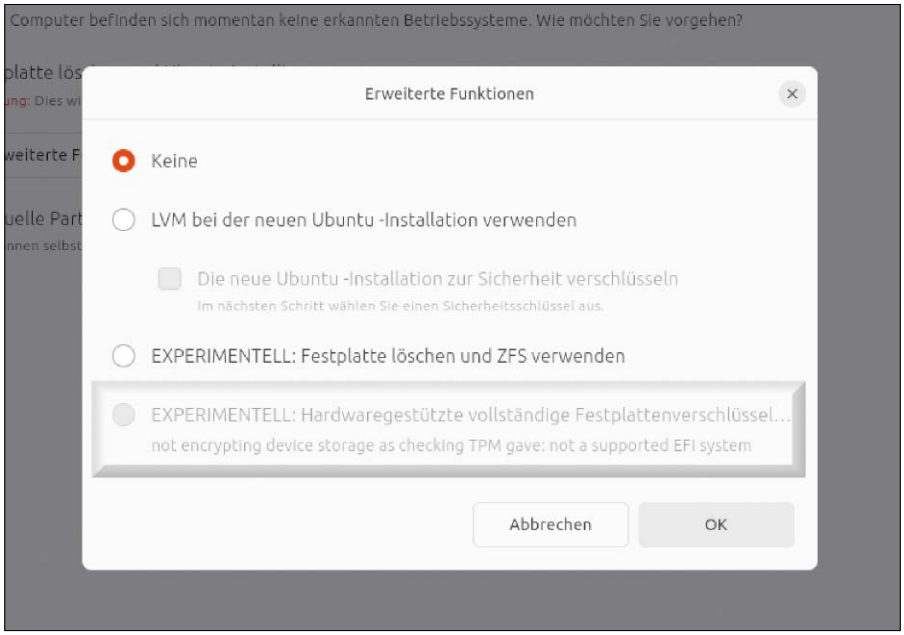


Der Raspberry 5 packt das anscheinend: Beim vom Pi Imager angebotenen Ubuntu 23.10 handelt es sich um die Hauptedition mit Gnome-Desktop.

Ubuntu-Hauptedition mit Gnome 45

Festplattenverschlüsselung mit TPM: Der Installer von Ubuntu 23.10 liefert eine Vorschau auf die hardwaregestützte Festplattenverschlüsselung. Da dies vorläufig nur beim Flutter-basierten, neuen Installer der Fall ist (also Hauptedition und Budgie-Edition), führen wir diese Neuheit an dieser Stelle und nicht als allgemeine Neuerung. Sie wird aber wahrscheinlich künftig auch in anderen Flavours Einzug halten.

Die Option findet sich beim Installationsschritt „Art der Installation" unter „Erweiterte Funktionen", wird hier noch als „Experimentell" bezeichnet und bleibt bei nicht kompatibler Hardware inaktiv. Ziel der Funktion ist es, die Eingabe komplexer Kennwörter zu ersparen. Der Entsperrschlüssel wird im Trusted Platform Module (TPM) der Hardware gespeichert und eröffnet damit einfachere Authentifizierungsmethoden, etwa durch einen Fingerabdruck-Leser. Die Funktion soll erst ab Ubuntu 24.04 LTS uneingeschränkt verfügbar sein.



Laufwerksverschlüsselung via TPM-Chip: Diese Funktion erscheint im Ubuntu-Installer noch als „Experimentell", soll aber demnächst die Authentifizierung vereinfachen.

Reduzierte Standardinstallation: Die frühere Installeroption „minimale Installation" ist jetzt die voreingestellte „Standard-Installation". Das sollte man wissen, wenn man typische Kandidaten wie Libre Office, Thunderbird oder Shotwell mitinstallieren will. Zu diesem Zweck muss nun explizit die Option „Vollständige Installation" gewählt werden. Der neue Standard gilt nur für die Hauptedition und ist insofern erstaunlich, als die genannten Softwarekandidaten (und weitere mehr) auf dem Installationsmedium und im Livesystem durchaus vertreten sind.

Neues Ubuntu App Center: Die Softwarezentrale zur Installation zusätzlicher Software („Anwendungszentrale" oder intern „Gnome-Software") ist in der Hauptedition komplett erneuert. Das mit Googles Flutter gestaltete Systemwerkzeug ist beim ersten Aufruf auffällig schneller am Start. Eindeutig positiv zu bewerten ist ferner die klare Unterscheidung zwischen Snap- und Debian-Paketen, sobald man in der Suche einen Softwarenamen eingibt.

Ansonsten ist die Zentrale aber schlichter als der Vorgänger und mit lediglich drei Kategorien „Produktivität", „Entwicklung", „Spiele" aktuell wohl noch unfertig. Dies lässt sich vorläufig nur durch zielsichere Paketsuche kompensieren. Ein weiteres absolutes Manko ist das Fehlen der bisherigen Übersicht „Installiert". Insgesamt ist die neue Anwendungszentrale in Ubuntu 23.10 eher ein Versprechen für die Zukunft als ein produktives Werkzeug.

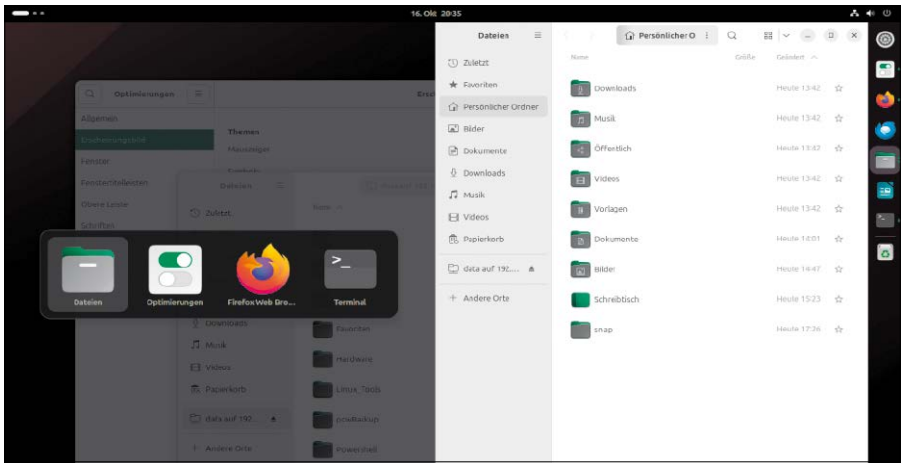
Firmware-Updater: Die Aktualisierung von Firmware der Systemhardware und Komponenten lagert Ubuntu 23.10 jetzt in ein Extra-Tool aus – den Firmware-Updater. Das braucht man nicht täglich, aber das zusätzliche Werkzeug macht das Installieren und Aktualisieren unter Ubuntu nicht übersichtlicher.

Gnome-„Aktivitäten": Das neue dynamische Schaltflächendesign für den vorher statischen „Aktivitäten"-Eintrag in der Systemleiste dient jetzt als Arbeitsflächen-Indikator und stellt die Anzahl der Arbeitsflächen (Punkte) sowie die aktuell genutzte Arbeitsfläche (kleiner Balken) visuell dar. Dabei behält das Control aber seine bisherige Funktion: Klickt man darauf, öffnet sich die bekannte Aktivitätenübersicht mit Fenster, Programmsuche und Arbeitsflächen.

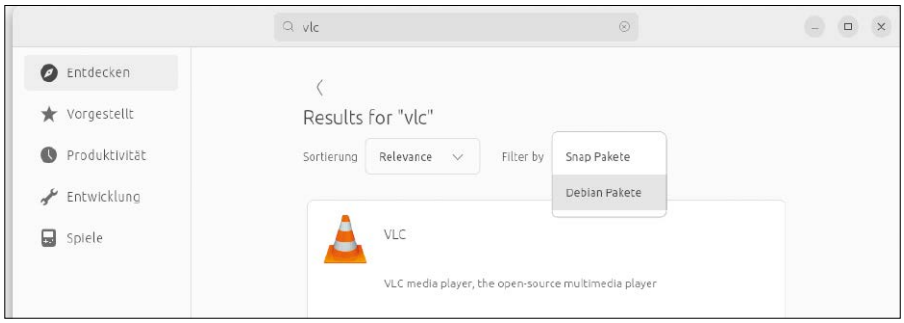
Erweitertes Fenster-Tiling: Windows-ähnlich ist das neue Gnome-Verhalten, nach einem an den Bildschirmrand gezogenen Fenster (das dann hier einrastet), eine Taskliste zu erhalten, um dort ein anderes Programmfenster auszuwählen. Dieses rastet dann in der anderen Bildschirmhälfte ein. Außerdem sind nun Viertelkacheln für vier Fenster möglic, und im Gnome-Control-Center erscheint unter „Multitasking" ein neuer Abschnitt „Tiling". Hier kann der Anwender einstellen, inwieweit er diese Gnome-Funktion nutzen will. So lässt sich etwa das Pop-up, das die anderen geöffneten Fenster anbietet, auch abschalten.

Schnelleinstellungen (Quick Settings Menu): Das kleine Systray-Menü in der Systemleiste ganz links wird unter Gnome immer wichtiger. Es führt bekanntlich zu den Netzwerk- und Audioeinstellungen, zum allgemeinen Kontrollzentrum, zu den Abschaltfunktionen, Themen und Energieeinstellungen. Jetzt kommt auch noch ein Control zu Tastaturbeleuchtung hinzu (falls solche Hardware vorhanden). Zur noch schnelleren Erreichbarkeit erhält das Mini-Menü den neuen Hotkey Super-S.

Dateimanager Nautilus: Die Suchfunktion für Dateien im Dateimanager wurde beschleunigt und die Optionen, welche die Suche schon länger anbietet, werden durch ein neues Filtersymbol deutlicher als bisher angeboten und visualisiert.



Windows-analoges Fensterarrangement („Tiling"): Gnome 45 bietet nach Ziehen an einen Bildschirmrand die übrigen Fenster an, um das gewünschte daneben zu platzieren.



Renovierte Softwarezentrale: Die deutliche Unterscheidung zwischen Snap- und DEB-Paket ist gut, alles andere noch eher Betastadium.

Die Ubuntu-Flavours: Ein Kurzdurchgang

Alle offiziellen Ubuntus 23.10 erhalten die Neuerungen, die der Punkt „ Ubuntu 23.10: Allgemeine Neuerungen" anspricht. Da am Desktop der Flavour-Distribution jeweils folgende Versionen

- Kubuntu mit KDE 5.27
- Lubuntu mit LXQT 1.3.0
- Xubuntu mit XFCE 4.18
- Ubuntu Cinnamon mit Cinnamon 5.8.4
- Ubuntu Unity mit Unity 7.7
- Ubuntu Mate mit Mate 1.26.2

zum Einsatz kommen, ist dort wenig Neues zu erwarten. Beim Cinnamon-Flavour gibt es kleine Neuerungen im Vergleich zum Ubuntu-Vorgänger 23.04, bei Mate minimale Verbesserungen seit 1.26.

Bei der bisher nicht genannten Budgie-Variante (mit Budgie 10.8) bleibt einiges seltsam bis fehlerhaft: Das Livesystem lässt den Installer-Link am Desktop und auch im automatisch startenden „Welcome" vermissen: Immerhin erscheint hier der Hinweis, den Link „Install Release" im Hauptmenü aufzusuchen. Danach startet der Installer in neuer Flutter-Optik. Die Installation verläuft aber ohne die üblichen Infos, das Installer-Fenster bleibt einfach leer.

In virtueller Maschine bringen einige Aktionen den Budgie-Desktop zuverlässig zum Absturz, so etwa der Aufruf des wichtigen Budgie-Control-Center („Einstellungen") oder ein Ändern des Desktophintergrunds. Damit ist das virtuelle System nicht produktiv nutzbar.

Nativ installiert treten diese Fehler zwar nicht auf, trotzdem können wir Ubuntu Budgie 23.10 aktuell nicht empfehlen. ■

Hübsche Gnome-Variante: Ubuntu Budgie zähmt viele Gnome-Eigenheiten, scheint aber in Version 23.10 an etlichen Ecken unfertig und fehlerhaft.

Manjaro für alle?

Arch gilt als System für Linux-Kenner. Distributionen wie Manjaro und Antergos öffnen Arch Linux inzwischen aber auch für normale Desktopnutzer. Insbesondere Manjaro erreicht laut Distrowatch erstaunliche Beliebtheit. Zu Recht?

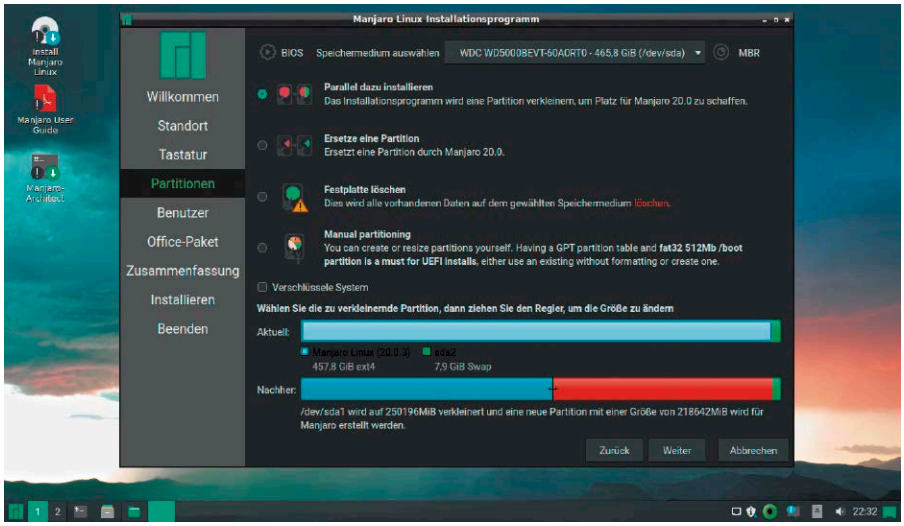
VON HERMANN APFELBÖCK

Den Linux-Desktop beherrschen die Debian-Systeme Ubuntu inklusive Derivaten wie Mint oder Elementary. Manjaro, aktuell in Version 20, ist hingegen ein Arch-basiertes Linux. Ungeachtet der sonstigen Debian-Dominanz ist dessen Top-Position in der Liste auf *https://distrowatch.com* inzwischen fast ein Dauerzustand: Offensichtlich macht Manjaro vieles richtig. Unser Fazit vorneweg: Wer Manjaro mit einem traditionellen Desktop wählt und auf experimentelle Paketquellen verzichtet, erhält einen ernsthaften Ubuntu-Konkurrenten.

Motive für Manjaro

Manjaro ist über den auch sonst bekannten Calamares-Installer (siehe Kubuntu, Lubuntu und andere mehr) bequem zu installieren und bringt im System grafische Verwaltungstools mit, deren Reichweite vom gewählten Desktop anhängt. Die „Flavour"-Auswahl auf der Webseite *https://manjaro.org/download* unter „Editions" ist beeindruckend: Die offiziellen Editionen bieten Gnome, KDE und XFCE. Weitere Community-Editionen erweitern das Angebot um Cinnamon, Mate, Budgie, LXDE, LXQT, um nur die prominentesten zu nennen.

Zusätzlich zu dieser großen Auswahl fertiger Live- und Installationsmedien gibt es auch noch den „Architect"-Baukasten. Manjaro Architect ist ein reiner Netinstaller (kein Livesystem) und erlaubt ein System nach Maß – unter anderem die Wahl zwischen 14 Linux-Oberflächen, genaue Kernel-Version und Softwareausstattung, Konten- und Treibereinrichtung sowie optionale „Tweaks" schon vorab. Dieser Installer geht deutlich darüber hinaus, was etwa ein Ubuntu-Netinstaller anbietet. Architect ist ein Highlight für Kenner, typische Desktopnutzer sollten jedoch die normale Installation mit Calamares vorziehen. Diese Entscheidung müssen Sie im Livesystem am Desktop bewusst treffen, denn die Manjaro-Livesysteme bieten dort beide Setupvarianten an („Install Manjaro" und „Manjaro Architect"). Architect gibt es auf *https://manjaro.org/download/* außerdem auch solo als Nur-Installer.



Calamares-Installer: Das Standard-Setup von Manjaro ist – auch bei Multiboot wie hier – nicht schwieriger als bei Ubuntu & Co. Für Kenner gibt es obendrein den „Architect"-Installer.

Manjaro kann als „Rolling Release" dauerhaft über die Systemaktualisierung auf dem neuesten Stand gehalten werden. Die von anderen Distributionen bekannte „Upgrade"-Prozedur auf die nächste Version entfällt also. Ein weiterer genereller Vorteil aller Arch-Systeme ist deren Aktualität: Das Paketformat erlaubt es den Entwicklern, fertige Pakete ohne großen Aufwand aus dem Quellcode zu erzeugen. Das sorgt für aktuelle Versionen für Kernel und Anwendungssoftware.

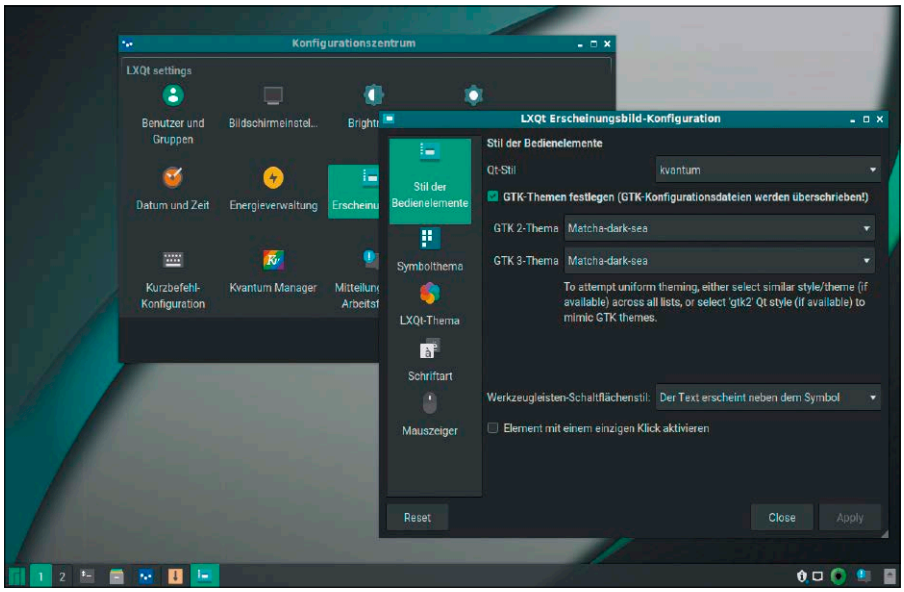
Die hohe Aktualität von Manjaro hat aber auch Schattenseiten: Bei umtriebiger Software mit vielen Neuentwicklungen können auch unzureichend getestete Pakete im System landen, die dann Stabilitätsprobleme verursachen. Typischen Desktopnutzern ist daher ein Manjaro mit konservativer Software zu empfehlen. Aus unserer Sicht die favorisierte Manjaro-Edition ist die XFCE-Edition – obendrein eine der drei offiziellen Varianten. Auf der Heft-DVD haben wir uns für die ebenfalls solide Community-Edition mit LXQT entschieden, aus dem einfachen Grund, dass diese um 600 MB kleiner ausfällt als Manjaro XFCE. Die Manjaro-Abbilder sind mit 2,2 bis 3,1 GB allesamt relativ groß, weil sie Livesystem plus Calamares-Installer plus Architect-Installer kombinieren.

Manjaro: Installation und Start

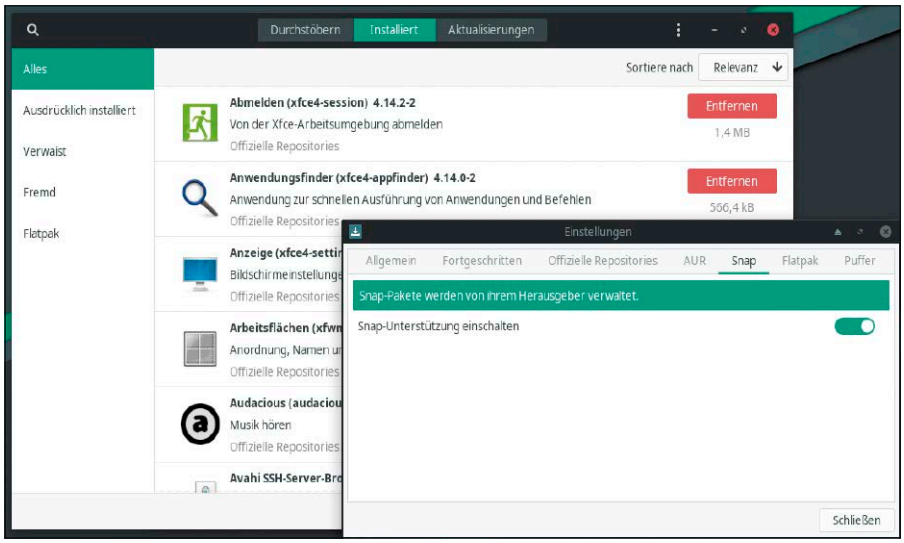
Beim Start des Livesystems sollten Sie das frühe Angebot nutzen, auf deutsche Tastatur und Sprache umzustellen. Dann weiß der spätere Installer automatisch, welche Sprache man installieren will. Die normale Installation über den Desktoplink startet Calamares (auf Architect gehen wir hier nicht näher ein). Dieser Installationsassistent stellt selbst Anfängern keine Rätsel

und beherrscht auch das Umpartitionieren für Multiboot. Im maßgeblichen Schritt „Partitionen“ wird ein vorhandenes System erkannt und die Verkleinerung der Partition (mit Größenregler) angeboten, um eine neue Partition für Manjaro zu schaffen. Ungewöhnlich ist lediglich die Abfrage einer Swappartition mit oder ohne Ruhezustand. Falls Sie diese Option übersehen oder ignorieren, ist das aber kein kritisches Problem. Auch Luks-Komplettverschlüsselung ist mit der unscheinbaren Option „Verschlüssele System“ vorgesehen. Bei der Einrichtung des Erstbenutzers will Manjaro auch ein Passwort für das root-Konto. Die spätere Systemverwaltung erfolgt aber wie bei Debian/Ubuntu über die „sudo“-Berechtigung des Erstbenutzers.

Nach erfolgter Installation gibt es einen schicken Bootscreen und – dies zumindest bei der Manjaro XFCE – eine vollständig deutschsprachige Oberfläche. Bei anderen Editionen müssen Sie eventuell noch fehlende Sprachpakete nachinstallieren. In den allgemeinen „Einstellungen“ des Desktops finden Sie den Unterpunkt „Manjaro-Einstellungen“ und dort wiederum „Sprachpakete“. Die „Manjaro-Einstellungen“ sind wichtig, denn sie versammeln noch weitere systemnahe Punkte wie die Benutzer-, Treiber- und Kernel-Verwaltung.



Manjaro LXQT startet von der Heft-DVD. Die Desktopanpassung folgt den sonstigen Regeln des LXQT-Desktops. Systemnahes bietet der Einstellungspunkt „Manjaro-Einstellungen“.



Grafischer Paketmanager: Dieses Manjaro-Tool erledigt die Updates und die Softwareverwaltung. Neben den offiziellen Quellen stehen optional auch AUR, Flatpak und Snap zur Verfügung.

Umfassende Paketverwaltung

Als grafischer Paketmanager für Systemaktualisierung plus Softwareinstallation ist der Pamac-Manager zuständig. Der ist sowohl im Hauptmenü als auch in den „Einstellungen“ anzutreffen und dies aufgrund seiner Zwitterfunktion doppelt – als „Software-Aktualisierungen“ und „Software hinzufügen/entfernen“. Das Tool ist einfach, aber fix, zeigt die installierten Programme und bietet mit „Durchstöbern“ eine kategorisierte Suche in den Paketquellen. Über das Lupensymbol links oben erhalten Sie ein Suchfeld für die manuelle Suche nach einem Programmnamen.

Der Pamac-Manager kann aber noch mehr: Ein Klick auf das unscheinbare Menüsymbol in der Titelleiste (drei Punkte) öffnet die „Einstellungen“. Hier finden Sie neben den offiziellen Paketquellen auch noch die Register „Snap“, „Flatpak“ und „AUR“. Die bekannten Containerformate Snap und Flatpak lassen sich hier für den Pamac-Manager einschalten, wonach dieser beim „Durchstöbern“ auch Software aus diesen Quellen anbietet. Auf der Kommandozeile sind diese standardmäßig einsatzbereit. Das Register „AUR“ meint die „Arch User Repositories“ mit Zugriff auf brandaktuelle Versionen. Hinter diesen Paketquellen stecken aber keine fertigen Pakete, sondern Bauanleitungen, aus denen der Paketmanager die Programme aus dem Quellcode kompiliert. Die AUR-Quellen sollten deshalb nur solche Benutzer einschalten, die notfalls auch mal mit einer fehlerhaften Programmversion und mit Paketkonflikten klarkommen.

Der Pamac-Manager sollte den Gang zum Terminaltool Pacman weitgehend erübrigen. Trotzdem ist ein Hinweis auf Pacman (das Pendant zu Apt unter Debian) unerlässlich, weil Arch-Kenner Pacman als Effizienz-Perle schätzen. Umsteigern von anderen Linux-Distributionen kostet die Syntax von Pacman aber erst einmal Einarbeitung.

An einige Befehle wie

```
sudo pacman -Syu
```

sollte man sich aber gewöhnen, weil es das komplette System einschließlich Software aktualisiert. Mit Schalter „-S“

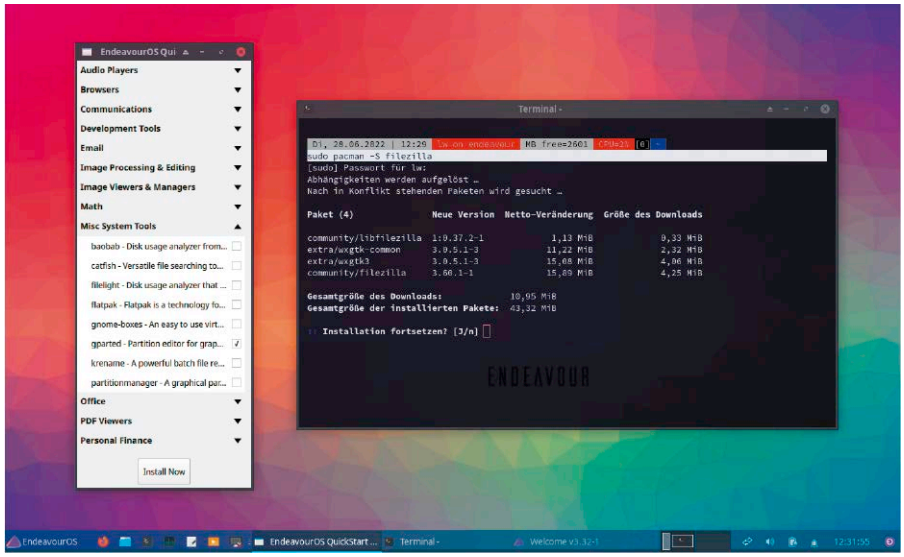
```
sudo pacman -S plank
```

installiert Pacman umstandslos – hier das Paket „Plank“. ■

Endeavour-OS: Flottes Arch

Wie alle Linux-Fans macht die LinuxWelt-Redaktion periodisch den Klick nach distrowatch.com zum Distributionsranking. Dass derzeit (Anfang Juli) Endeavour-OS ganz vorne liegt, trifft sich gut: Das System ist soeben in neuer Version erschienen.

VON HERMANN APLELBÖCK



Schnelles Arch: Das reaktionsfreudige Endeavour-OS (hier mit XFCE) ist komfortabel zu installieren, fordert aber früher oder später Terminalkompetenz.

Das jüngste Endeavour-OS 22.6 (ab hier kurz „EOS“) hat vor allem die ARM-Unterstützung für Raspberry- und Odroid-Platinen ausgebaut. EOS ist Nachfolger des eingestellten Antergos und hat denselben Anspruch wie das bekanntere Manjaro, nämlich mit einem grafischen Installer den Zugang zu Arch Linux zu vereinfachen. Laut Distrowatch hat EOS Manjaro inzwischen den Rang abgelaufen und liegt aktuell auf Platz 2 vor Mint, Manjaro, Ubuntu, Debian & Co. Generell scheinen Arch-Derivate und deren Rolling-Release-Modell derzeit hoch im Kurs: Sie gelten als besonders schnell und stets aktuell. Nachteile sind gelegentliche Paketkonflikte, eine Fokussierung auf das Terminal und eventuell nicht vollständig deutsch lokalisierte Komponenten. Die Frage dieses Artikels ist daher, ob sich EOS als das derzeit wohl beste Arch als Alltags-Desktop eignet?

Bezug und Installation

Das Installations-ISO und Livesystem erhalten Sie auf *https://endeavouros.com/latest-release* (1,8 GB) und als LinuxWelt-Leser sofort bootfähig auf der Heft-DVD. Dieser Live-Installer bringt standardmäßig den XFCE-Desktop mit, jedoch sind Sie nicht zwingend auf diese Oberfläche festgelegt. Der „Welcome“-Dialog des Livesystems zeigt mehrere Optionen, und im Normalfall wird die Installation mit „Start the Installer“ ausgelöst. Alle anderen Optionen können Sie ignorieren, allenfalls die Option „Endeavour community editions“ ist für Nutzer interessant, die sich für exotische bis experimentelle Oberflächen interessieren (Sway, Qtile, Openbox sowie die Endeavour-Eigenentwicklung Worm).

Die primäre Option „Start the Installer“ eröffnet dann wiederum die zwei Möglichkeiten „Offline“ und „Online“. Wer den mitgelieferten XFCE möchte, kann „Offline“ rein vom Installationsmedium installieren. Dies ist der schnellste und einfachste Weg. „Online“ bezieht Teile des Systems aus dem Web und erlaubt die Auswahl zwischen neun prominenten Oberflächen (Gnome, KDE, Cinnamon etc.).

Verantwortlich für das Setup ist der Calamares-Installer, den auch Manjaro und einige Ubuntu-Varianten nutzen. Die typischen Fragen betreffen Sprache, Zeitzone, Tastatur, Partitionierung (mit optionaler Systemverschlüsselung) und Erstbenutzer. Setzt man hier, wie vorgeschlagen, das Benutzerpasswort mit dem des Administrators identisch, erzielt man ein sudo-Verhalten genau wie bei Ubuntu & Co.

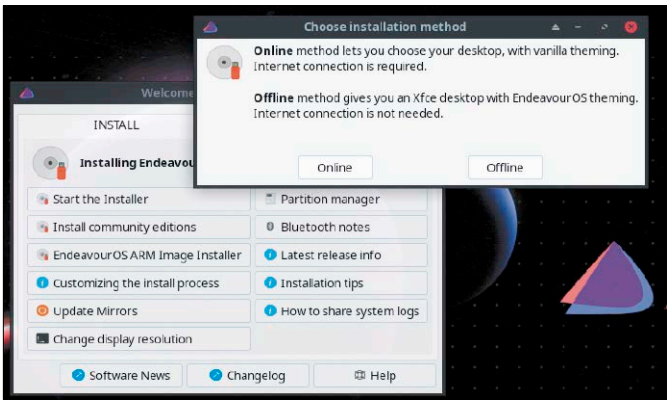
EOS: Ein erster Rundgang

Das System präsentiert sich am XFCE-Desktop und allen installierten Programmen komplett deutschsprachig mit ganz wenigen Ausnahmen bei EOS-eigenen Tools. Thema der neuen „Artemis“-Version ist die Apollo-Mission und Standardhintergrund am Anmeldebildschirm und am Desktop dazu passend eine steil startende Rakete: Hier wird der Mythos vom schnellen Arch gepflegt, der sich dann tatsächlich bestätigt: Das System bootet auf einem älteren Rechner (allerdings auf SSD) in zehn Sekunden. Da kann ein Ubuntu 22.04 nicht

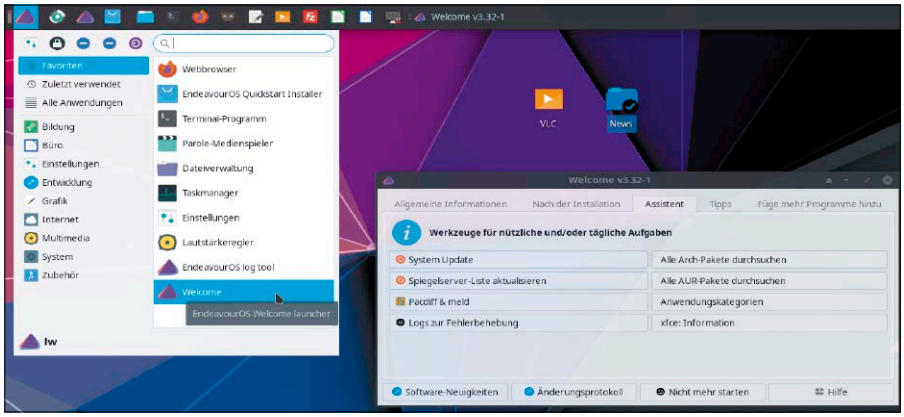
mithalten (13 Sekunden). Wie flink ein klassisch installierter Firefox agieren kann, wird Snap-geschädigte Ubuntu-Nutzer ebenfalls positiv überraschen. Auch der Start von Software-Schwergewichten wie Gimp ist praktisch per Mausklick geschehen. Wir kennen mit Bodhi Linux nur ein einziges Debian/Ubuntu mit vergleichbaren Reaktionszeiten.

Ressourcentechnisch fordert EOS mit dem Standarddesktop XFCE nicht mehr, aber auch nicht weniger als ein Debian/Ubuntu, nämlich etwa 650 MB ab Anmeldung. Auf der Festplatte bleibt es nach der Installation deutlich unter fünf GB, sollte aber für den Dauerbetrieb wie jedes Linux wenigstens 50 bis 100 GB auf der Systempartition vorfinden (Benutzerdaten nicht eingerechnet). Hardwaretechnisch gibt es mit den von uns genutzten Standardkomponenten keinerlei Einschränkungen. EOS verwendet Kernel 5.18 und arbeitet problemlos im Multimonitorbetrieb, erkennt alle Medien, akzeptiert Linux-bewährte WLAN-Adapter, beherrscht ACPI-Ruhezustände und erkennt Funktions-Sondertasten auf Notebooks.

Nach der Anmeldung meldet sich der komplett deutsch lokalisierte „Welcome“-Dialog (eos-welcome). Die Angebote „Spiegelserver“ und „System-Update“ sollte man nach der Installation umgehend aufgreifen. EOS ist terminaldominiert, aber viele Aktionen wie eben auch die Systemaktualisierung kann man sich mit „Welcome“ vereinfachen. Es handelt sich um eine umfangreiche Kommando- und Script-Sammlung, die man als Autostart zwar abschalten („Nicht mehr starten“), aber als Favorit im Menü oder in der Systemleiste bereithalten sollte. EOS arbeitet wie die allermeisten neueren Distributionen mit dem Init-Dienst systemd. Komponenten und Kommandos von systemctl, journalctl funktionieren daher wie gewohnt.



„Welcome“ im EOS-Livesystem: „Start the Installer“ startet das Setup mit Calamares wahlweise „Offline“ oder „Online“ mit Desktopwahl.



„Welcome“ im installierten System: Diese nützliche Sammlung von URLs und Verwaltungskommandos erspart einige Terminalausflüge.

Paketmanager und Installationen

EOS nutzt die Arch-Paketquellen, bietet für den Softwarebezug aber nur ein sehr einfaches grafisches Programm. eos-quickstart („EndeavourOS Quickstart Installer“) zeigt eine kategorisierte Auswahl prominenter Software, die nach Markierung und „Install Now“ umstandslos installiert wird. Schwergewichte wie Chromium, Gimp, Libre Office, Thunderbird, VLC sind hier in jedem Fall anzutreffen. Im Dauerbetrieb und für die Installation speziellerer Tools wird das aber nicht ausreichen: Schon die Suche nach einem SSH-Server oder einem Werkzeug wie Filezilla bleibt hier vergeblich.

Basiskommandos des Terminal-Paketmanagers pacman sind daher unerlässlich. Dieser bezieht die Software aus den offiziellen Arch-Quellen. Ein zweiter Paketmanager yay kann zusätzlich die inoffiziellen AUR-Quellen nutzen. Wir empfehlen Arch-Einsteigern, zunächst bei den Arch-Quellen und bei pacman zu bleiben. Fürs Erste genügt (Beispiel)

```
pacman -Ss filezilla
```

zur Suche nach Software, ferner

```
sudo pacman -S filezilla
```

zur Installation und

```
sudo pacman -R filezilla
```

zur Deinstallation. Das komplette Systemupdate mit

```
sudo pacman -Syu
```

kann man alternativ auch mit dem Terminallink im Hauptmenü „System → UpdateIn-Terminal“ erledigen oder mit dem freundlichen „Welcome“. Letzteres weist unter „Assistent → Alle Arch-Pakete durchsuchen“ außerdem auf das Inventar unter *https://archlinux.org/packages*, das eine bequeme Onlinesuche erlaubt. Passendes kann dann mit *pacman -S […]* installiert werden.

Systemverwaltung und Desktop

Neben den genannten grafischen EOS-Werkzeugen eos-quickstart (limitierter Software-Installer) und eos-welcome (wichtige klickfreundliche Script-Sammlung) bleibt es Arch-typisch spartanisch. Nahezu alles, was unter „/usr/bin/eos-*“ an Systemprogrammen zu finden ist, sind terminalnahe Helfer.

An grafischen EOS-Tools, die auch im Menü auftauchen, ist neben den bereits genannten nur noch der eos-update-notifier zu erwähnen, der die Frequenz der Systemaktualisierung einstellen kann. Im Übrigen überlässt EOS die grafische Systemverwaltung dem jeweils benutzten Desktop. Wer Terminaldefizite hat, ist daher mit Desktops wie Gnome, KDE oder Cinnamon am besten beraten, die eine große Reichweite auch in Richtung Systemverwaltung besitzen. Nutzern ohne Terminalaffinität wird man diese beeindruckend schnelle Distribution dennoch nicht empfehlen können. ■

Chrome-OS für alle

Googles Chrome-OS gilt als schlank und besonders schnell. Eigentlich gibt es das System nur zusammen mit neuer Hardware. Es lässt sich aber auch auf fast beliebigen Notebooks oder PCs installieren.

VON THORSTEN EGGELING

Alternatives System: Chrome-OS ist von Google nur zusammen mit einem Chromebook erhältlich. Es gibt aber Wege, das System auch auf anderer Hardware zu installieren.

Quelle:www.google.com

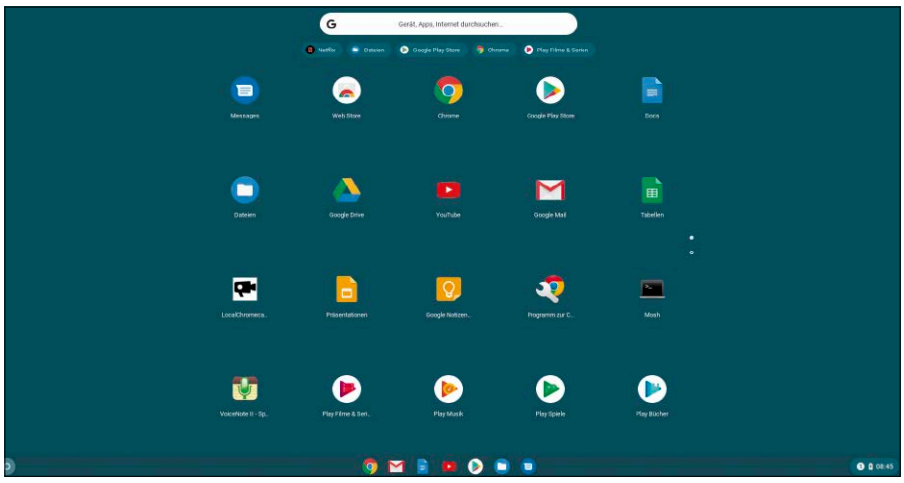
Chrome-OS ist ein Betriebssystem von Google, das als Basis einen Linux-Kernel verwendet. Google liefert das System nur vorinstalliert zusammen mit Chromebooks aus (*www.google.com/chromebook*). Die Hardware unterscheidet sich kaum von herkömmlichen Notebooks. In der Regel steckt ein Intel-Prozessor im Gerät, seltener eine AMD- oder ARM-CPU. Als Grafikchip dienen passend dazu Intel UHD Graphics oder AMD Vega. Chromebooks gibt es zu Preisen zwischen etwa 250 und knapp 1000 Euro.

Chrome-OS selbst ist nicht frei verfügbar, die Open-Source-Bestandteile mit dem Namen Chromium-OS dagegen schon (*www.chromium.org*). Es liegt daher nahe, eine angepasste Linux-Distribution auf der Basis von Chromium-OS zu erstellen. Das System ist aufgrund des geringen Ressourcenbedarfs gut für etwas ältere Hardware geeignet. Die Installation kann aber auch für Nutzer interessant sein, die eine besonders übersichtliche Oberfläche bevorzugen.

1. Diese Funktionen bietet Chrome-OS

Die ersten Chromebooks stammen aus dem Jahr 2011. Die einzige Anwendung war der Chrome-Browser, über den sich beispielsweise Google Mail oder Google Drive aufrufen ließen. Das funktionierte jedoch nur bei bestehender Internetverbindung. Zusätzliche Anwendungen konnte man nicht installieren, nur Chrome-Erweiterungen und Chrome-Apps. Für ein Betriebssystem mit Aussicht auf Marktchancen war das wohl zu wenig. Google hat daher relativ schnell einen Offlinemodus eingebaut, damit sich Dokumente auch ohne Internetverbindung bearbeiten lassen. Inzwischen ist bei vielen Chromebooks auch Google Play verfügbar, über das sich Apps wie unter Android lokal installieren lassen. Es sind jedoch nicht alle Apps auch für Chrome-OS verfügbar. Die wichtigsten und beliebtesten lassen sich aber einrichten, beispielsweise Instagram, Pinterest, Netflix, Amazon Prime Video oder der VLC Media Player.

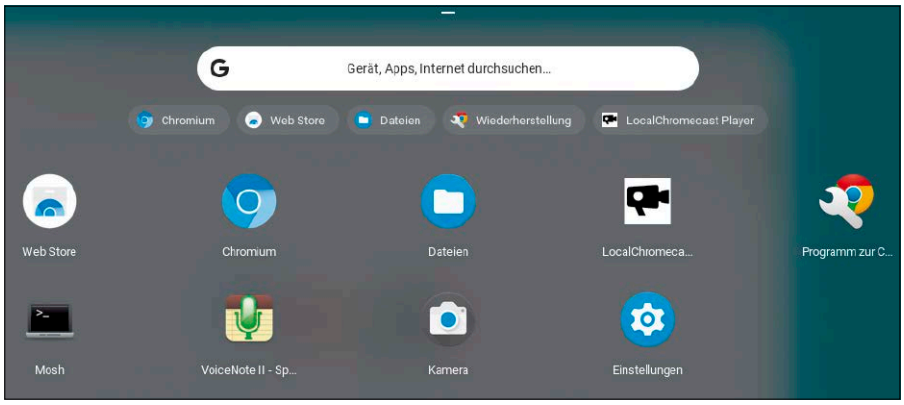
Chrome-OS lässt sich über einen Touchscreen, ein Touchpad und/oder mit Maus und Tastatur bedienen. Programme erscheinen wie unter Linux in einem eigenen Fenster oder werden innerhalb des Chrome-Browsers ausgeführt. Die Anwendungen startet man über die untere Leiste



Ähnlichkeiten mit Android: Apps lassen sich über den Launcher starten. Bei einigen Apps, beispielsweise Google Drive oder Google Mail, öffnet sich ein Tab im Chrome-Browser.

(„Ablage“) oder den „Launcher“ links unten in der Ecke. Die Schaltfläche mit dem Aufwärtspfeil führt zu einer Übersicht aller Apps. Nach einem Klick auf die Uhr rechts unten öffnet sich ein Menü, über das Sie beispielsweise in die „Einstellungen“ gelangen, eine WLAN-Verbindung herstellen oder Chrome-OS herunterfahren. Weitere Infos zu Chrome-OS finden Sie auf *www.google.com/chromebook*, hilfreich sind insbesondere die „Tipps zum Chromebook“ (*www.google.com/chromebook/howto*).

Linux-Programme laufen ebenfalls unter Chrome-OS, zumindest auf neueren Geräten ab ungefähr 2018 (siehe *https://m6u.de/coss*). Zuerst muss man in den Einstellungen auf „Linux (Beta)“ gehen und auf „Aktivieren“ klicken. Über die App „Terminal“ lässt sich ein Linux-Terminal starten. Das Debian-Subsystem läuft zwar abgeschottet in einer Sandbox, über apt im Terminal installierte Programme für die grafische Oberfläche integrieren sich aber trotzdem in den Launcher und müssen daher nicht über das Terminal gestartet werden.



Reduziertes System: Chromium-OS ist die Open-Source-Basis von Chrome-OS. Standardmäßig gibt es hier aber nur wenige Apps. Das Meiste läuft im Chromium-Browser.

2. Chrome-OS und Chromium-OS im Vergleich

Chromium-OS verwendet die gleiche Basis wie Chrome-OS, es fehlen aber alle proprietären Google-Apps. Das System ist also im Wesentlichen auf den Chromium-Browser und die dafür verfügbaren Erweiterungen und Apps beschränkt. Das damit sehr reduzierte System mag den Wünschen einiger Nutzer sehr entgegenkommen, wer mehr will, kann aber die fehlenden Funktionen nachrüsten und Chromium-OS in Chrome-OS verwandeln (siehe Punkt 4).

Es gibt jedoch keine Garantie dafür, dass sich auf Anhieb ein startfähiges Chrome-OS für jedes Gerät erstellen lässt. Manchmal muss man mit unterschiedlichen Konfigurationen experimentieren, damit das System rund läuft.

Hinweise: Im Firmwaresetup muss Secure Boot deaktiviert sein, sonst starten die Systeme nicht. Die im Folgenden genannten Systemvarianten erfordern in jedem Fall die Anmeldung mit einem Google-Benutzerkonto, das Sie schon bei der Installation angeben oder neu erstellen.

3. Ein angepasstes Chromium-OS verwenden

Chrome-OS ist speziell auf das jeweilige Chromebook zugeschnitten. Der Kernel enthält nur die wirklich nötigen Module (Treiber) für die verbaute Hardware, was zur Beschleunigung des Systems beiträgt. Das Betriebssystem lässt sich daher nicht einfach auf ein Gerät mit abweichender Hardware übertragen. Um das zu ändern, baut man in das System einen neuen Linux-Kernel ein, der Module für jede gängige Hardware mitbringt. Zusätzlich sind weitere Anpassungen etwa für den Bootloader, das Soundsystem oder WLAN-Treiber erforderlich. Chrome-OS unterstützt von Haus aus keine Nvidia-Grafikchips. Treiber dafür müssen also ebenfalls eingebaut werden.

CHROME-OS ALS ZWEITSYSTEM

Chrome-OS verwendet ein relativ komplexes Partitionsschema. Deshalb sind Installationen neben einem anderen Betriebssystem auf der gleichen Festplatte schwierig. Das System lässt sich über Grub jedoch aus einer Imagedatei booten, die Sie auf der Linux-Partition ablegen.

Bereiten Sie Chrome-OS vor wie in Punkt 4 beschrieben und starten Sie dann das System vom USB-Stick. Öffnen Sie nach der Anmeldung ein crosh-Terminal mit der Tastenkombination Strg-Alt-T. Tippen Sie *shell* ein und bestätigen Sie mit der Eingabetaste. Mit der Befehlszeile

```
sudo /sbin/fdisk -l
```

lassen Sie sich eine Partitionsübersicht ausgeben. Wenn die Linux-Partition beispielsweise unter „/dev/sda2“ zu finden ist, dann verwenden Sie die folgenden vier Befehlszeilen:

```
mkdir -p ~/tmpmount
sudo mount /dev/sda2 ~/tmpmount
sudo bash /usr/sbin/chromeos-install.sh -dst ~/
  tmpmount/chromeos.img -s 20
sudo umount ~/tmpmount
```

Der Wert hinter „-s“ legt die Größe der Imagedatei in GB fest. Das Minimum sind 14 GB. Das Script gibt die Zeilen für die Grub-Konfiguration aus, die Sie markieren und dann in einem Dokument auf Google Drive speichern.

Starten Sie dann das installierte Ubuntu oder Linux Mint von der Festplatte. Über ein Terminal öffnen Sie die Konfigurationsdatei in einem Editor:

```
sudo gedit /etc/grub.d/40_custom
```

Fügen Sie unterhalb des Kommentars die Zeilen für die Grub-Konfiguration ein, die Sie unter Chrome-OS kopiert haben. Wenn Sie den Entwicklermodus deaktivieren möchten, entfernen Sie „cros_debug“ (siehe Punkt 5). Speichern Sie die Datei und beenden Sie den Editor. Aktualisieren Sie dann die Grub-Umgebung mit diesem Befehl:

```
sudo update-grub
```

Danach starten Sie neu und wählen „Chrome-OS“ im Grub-Bootmenü.

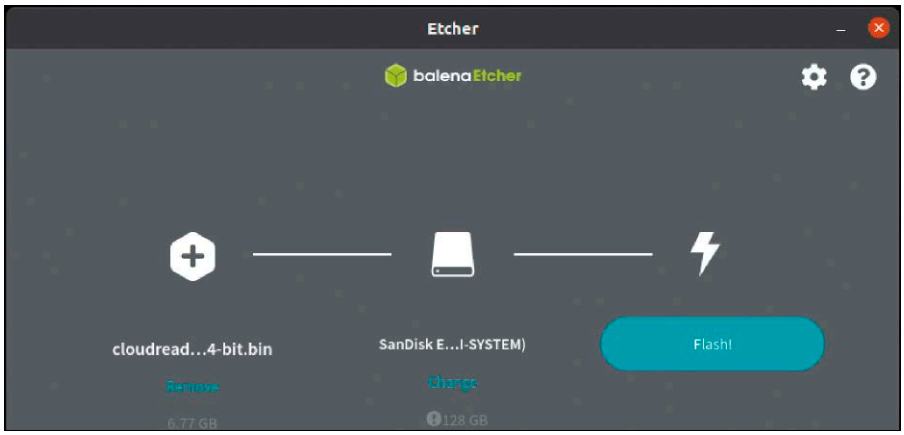


Image flashen: Wer nicht dd im Terminal verwenden mag, greift zu Etcher. Damit übertragen Sie den Inhalt einer Imagedatei bequem auf einen USB-Stick oder eine SD-Karte.

Ohne Google-Konto geht nichts: Ob CloudReady, Chromium-OS oder Chrome-OS – die Google-Anmeldung während der Installation ist bei allen Betriebssystemen Pflicht.

Es ist jedoch nicht garantiert, dass das System mit jedem Grafikchip problemlos zusammenarbeitet.

Ein fertig angepasstes Chromium-OS gibt es unter dem Namen „CloudReady" kostenlos bei *www.neverware.com*. Das Unternehmen bietet auch kostenpflichtige Lizenzen inklusive Support für Firmen und Schulen an. Über *https://guide.neverware.com/supported-devices* lässt sich eine Datenbank mit unterstützten Geräten abfragen. Nach einem Klick auf ein Modell erfahren Sie weitere Details, so etwa, was bei der Installation zu beachten ist und welche Einschränkungen es gibt. Sollte Ihr Gerät nicht aufgeführt sein, können Sie Cloudready trotzdem ausprobieren. Der Computer sollte mindestens zwei GB Arbeitsspeicher und eine 64-Bit-CPU besitzen sowie im Uefi-Modus booten können. Sehr alte Geräte (mehr als zehn Jahre) sind daher für Cloudready/Chromium-OS nicht geeignet.

Die testweise Installation ist ohne Gefahr möglich, weil dafür nur ein USB-Stick verwendet wird. Dieser sollte mindestens 16 GB Speicherplatz bieten, USB 3.0 ist von Vorteil. Wenn dort alles funktioniert, kann man das System auch auf der Festplatte installieren. Dualboot mit einem anderen System wird von Cloudready allerdings nicht unterstützt.

Schritt 1: Gehen Sie auf *www.neverware.com/freedownload*, klicken Sie auf „Download 64-Bit Image" und entpacken Sie die ZIP-Datei.

Schritt 2: Sichern Sie gegebenenfalls alle Daten, die sich auf dem USB-Stick befinden. Diese gehen mit den folgenden Aktionen verloren. Mit

```
sudo parted -l
```

ermitteln Sie den Gerätepfad des USB-Sticks und hängen ihn dann mit

```
sudo umount /dev/sd[X]?
```

aus. Der Platzhalter „[X]" steht für die Gerätebezeichnung, beispielsweise „b" für „/dev/sdb". „?" sorgt dafür, dass alle Partitionen ausgehängt werden. Geben Sie dann im Terminal folgenden Befehl ein, wobei Sie die Pfade für Ihr System anpassen:

```
sudo dd if=~/Downloads/cloudready-
  free-80.4.1-64-bit.bin of=/dev/
  sd[X] bs=4M
```

„[X]" steht für die Laufwerksbezeichnung, die Sie schon zuvor bei umount verwendet haben. Warten Sie ab, bis die Eingabeaufforderung wieder erscheint. Achten Sie darauf, das richtige Zielgerät anzugeben, damit Sie nicht versehentlich eine Festplatte überschreiben. Wer zum Schreiben des Abbilds eine grafische Oberfläche bevorzugt, verwendet statt dd beispielsweise Balena Etcher für Windows oder Linux (*www.balena.io/etcher*).

Schritt 3: Booten Sie den Computer vom USB-Stick. Dafür müssen Sie meist die Bootreihenfolge im Bios-Setup ändern oder Sie verwenden das Bios-Bootmenü. Starten Sie dort den Eintrag mit einem vorangestellten „UEFI".

Schritt 4: Im Startbildschirm klicken Sie auf „English (United States)" und stellen als Sprache „German – Deutsch" ein, für die Tastatur wählen Sie „Deutsch – Deutsch". Klicken Sie auf „OK" und dann auf „Los geht's". Folgen Sie den weiteren Anweisungen des Assistenten. Nach der Anmeldung mit einem Google-Konto ist das System einsatzbereit.

Cloudready startet und läuft auf einem USB-Stick in der Regel ausreichend schnell. Sie können es aber auch auf der Festplatte installieren. Dazu klicken Sie auf die Uhr unten rechts und dann auf „Install OS". Die Festplatte wird dabei gelöscht. Die Installation neben einem weiteren Betriebssystem ist nicht vorgesehen.

4. Chrome-OS mit dem Brunch-Framework installieren

Chrome-OS für beliebige Hardware gibt es zwar nicht zum Download, dafür aber Wiederherstellungsabbilder für Chromebooks. Mit dem Brunch-Framework lässt sich daraus ein Chrome-OS erzeugen, das mehr Hardware unterstützt. Die Voraussetzungen sind ähnlich wie in Punkt 3 beschrieben. Nvidia-Grafikchips werden nicht unterstützt, auf Notebooks mit hybrider Grafik lässt sich das System oft trotzdem verwenden, wenn die Umschaltung auf die Intel-CPU-Grafikeinheit funktioniert. Dafür läuft das angepasste System auch auf Geräten mit AMD-Prozessoren aus der Serie A4 bis A6, nicht jedoch mit Ryzen-CPUs. Intel-CPUs/GPUs lassen sich ab Nehalem (erste Generation, 2008) verwenden. Insgesamt ist die Hardwareunterstützung etwas schlechter als bei Cloudready, aber wenn es läuft, erhält man ein vollwertiges Chrome-OS.

Laden Sie Brunch über *https://github.com/sebanc/brunch/releases* herunter. In der Versionsnummer steht, für welche Version der Wiederherstellungsabbilder sich die Software eignet (r83 oder r81).

Entpacken Sie die ZIP-Datei und verschieben Sie den Inhalt in einen Ordner in Ihrem Home-Verzeichnis, beispielsweise nach „~/brunch“.

CPU-Typ ermitteln: Starten Sie ein Linux, beispielsweise das Livesystem Ubuntu Mate (auf Heft-DVD), auf dem Rechner, wo Sie Chrome-OS installieren wollen. In einem Terminal verwenden Sie die folgende Befehlszeile

```
cat /proc/cpuinfo
```

Sie sehen in der Ausgabe die Modellbezeichnung der CPU. Unter *https://en.wikipedia.org/wiki/Intel_Core* finden Sie eine Liste mit Intel-Core-CPUs, in der Sie nach der Modellbezeichnung suchen. Entscheidend ist nur, ob die CPU zur vierten Generation (Haswell) und neuer gehört oder älter ist.

Schritt 1: Entsprechend dem Ergebnis laden Sie ein Wiederherstellungsabbild über *https://cros-updates-serving.appspot.com* herunter.

Verwenden Sie Abbilder mit dem Codenamen „rammus“ für CPUs der vierten Generation oder neuer, „sammus“ für die dritte Generation oder älter und „grunt“ für AMD-CPUs. Klicken Sie in der Spalte „Recovery“ auf die Versionsnummer, die zur Brunch-Version passt (81 oder 83). Entpacken Sie die heruntergeladene ZIP-Datei und verschieben Sie die enthaltene „bin“-Datei in den Ordner „~/brunch“.

Schritt 2: Für Brunch sind zwei Tools erforderlich, die Sie unter Ubuntu/Mint mit dieser Befehlszeile installieren:

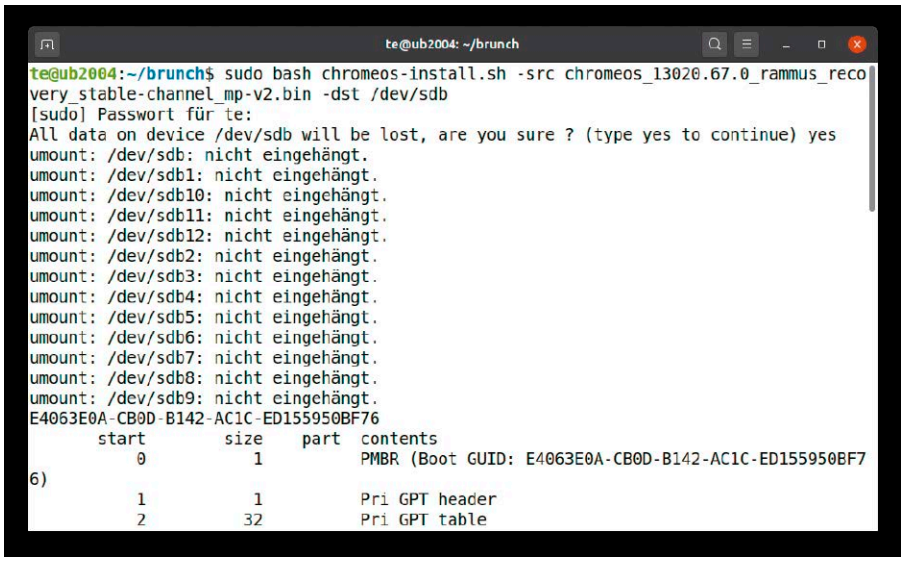
```
sudo apt install pv cgpt
```

Schritt 3: Hängen Sie den USB-Stick aus dem Dateisystem aus (siehe Punkt 3) und führen Sie im Terminal diese zwei Befehlszeilen aus:

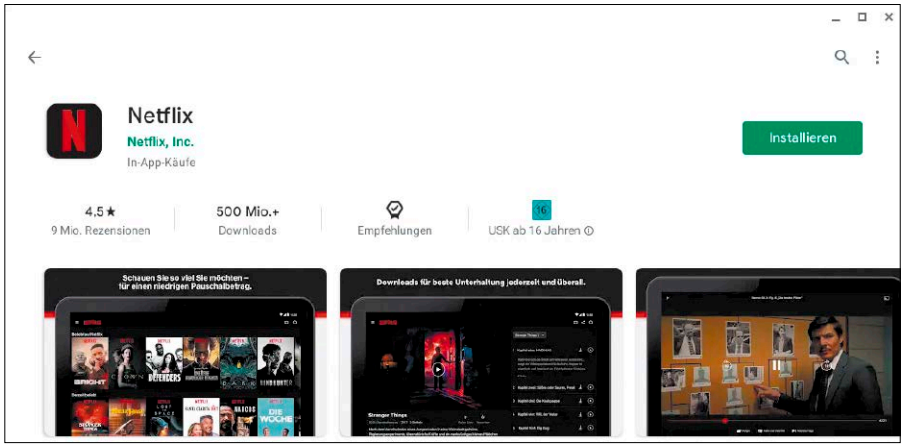
```
cd ~/brunch
sudo bash chromeos-install.sh -src
  [bin-Datei] -dst /dev/sd[X]
```

Die Platzhalter in eckigen Klammern passen Sie für Ihr System an. Tippen Sie als Bestätigung „yes“ ein, wenn Sie sicher sind, das richtige Ziellaufwerk angegeben zu haben.

Booten Sie dann den Rechner vom USB-Stick. Der erste Start dauert etwas länger, weil das Dateisystem zuerst angepasst und einige Patches installiert werden müssen. Danach sehen Sie den Bildschirm „Welcome“, von wo aus es wie in Punkt 3 (Schritt 4) weitergeht. Über Google Play installieren Sie die gewünschten Apps oder Sie verwenden Linux unter Chrome-OS.



Chrome-OS anpassen: Das Script des Brunch-Frameworks ändert eine Google-Wiederherstellungsdatei so, dass Chrome-OS auch auf Standardhardware laufen kann.



Mehr Programme: Apps wie Netflix lassen sich unter Chrome-OS nur installieren, wenn der Entwicklermodus abgeschaltet ist. Dafür müssen Sie die Datei „grub.cfg“ ändern.

5. Bei Bedarf: Entwicklermodus abschalten

Ein über Brunch eingerichtetes Chrome-OS läuft im Entwicklermodus. Das erlaubt Zugriffsrechte in Bereichen des Systems, die einem Standardbenutzer verwehrt sind. Allerdings erhöht sich dadurch das Sicherheitsrisiko und einige Apps lassen sich nicht installieren, so beispielsweise Netflix. Wenn Sie unter Chrome-OS persönliche Dateien lokal gespeichert haben, sichern Sie diese. Beim Zurücksetzen des Systems in den Standardmodus gehen die Dateien verloren.

Unter Linux mounten Sie die EFI-Partition auf dem USB-Stick. Wo diese zu finden ist, ermittelt dieser Befehl:

```
sudo fdisk -l
```

Die Partition vom Typ „EFI-System“ beispielsweise auf „/dev/sdb12“ ist die gesuchte. Hängen Sie diese mit

```
sudo mount /dev/sdb12 /mnt
```

in das Dateisystem ein. Öffnen Sie die Grub-Konfigurationsdatei mit

```
sudo gedit /mnt/efi/boot/grub.cfg
```

im Editor (Linux Mint: xed). Entfernen Sie den Parameter „cros_debug“. Speichern Sie die Datei und starten Sie Chrome-OS neu. Klicken Sie auf die Uhr rechts unten im Bildschirm und dann auf das Zahnradsymbol („Einstellungen“). Hier gehen Sie auf „Gerät“, klicken auf „Erweitert“ und unter „Einstellungen zurücksetzen“ auf „Zurücksetzen“. Danach wählen Sie „Neu starten“. Sobald sich das System wieder meldet, gehen Sie auf „Powerwash“ und „Weiter“. Danach müssen Sie noch einmal dieselbe Prozedur absolvieren wie bei der Ersteinrichtung. ■

Knoppix 8.6: Der Live-Klassiker

Livesysteme sind nicht rar: Moderne Linux-Distributionen kombinieren das Installationsmedium mit einem Livesystem, das sich zum Ausprobieren, zum Hardwaretest und zur Reparatur eignet. Der Allrounder Knoppix behält dennoch seine Berechtigung.

VON HERMANN APFELBÖCK

„Initiating startup sequence“ meldet eine Frauenstimme beim Desktopstart. Extravagante Compiz-Effekte im Standarddesktop LXDE mit „wackeligen“ Fenstern und wechselnde Knoppix-Screensaver garnieren den Desktop. Darunter wartet eine unfassbar umfangreiche Softwaresammlung auf ihren Einsatz – eine Sammlung mit nützlichsten Werkzeugen für Netzwerk, Surfen, Office, Medien, Reparaturen, die allerdings auch vor fragwürdiger B-Ware und funktional redundanten Dubletten nicht zurückschreckt.

Das nach Klaus Knopper benannte Knoppix ist eine ganz spezielle Distribution – und dabei in der technischen Basis vom Feinsten. Das Livesystem bootet praktisch auf jedem alten wie neuen Rechner, hat einen absolut zuverlässigen Assistenten zur Einrichtung und kann optional Daten und Einstellungen durch Verschlüsselung schützen. Das inzwischen fast 20 Jahre gereifte Debian-Linux ist der Live-Klassiker: Knoppix ermöglichte den Livebetrieb lange vor den heute verbreiteten Live-Installationsmedien von Ubuntu & Co. Mit exzellenter Hardwareerkennung, deutschsprachiger Arbeitsumgebung, opulenter Softwareausstattung und variabler Einrichtung bleibt Knoppix die erste Wahl für ein universelles Zweitsystem auf USB.

Download und Einrichtungsvarianten

Knoppix-Downloads werden via *http://www.knopper.net/knoppix-mirrors/* hauptsächlich über Universitäten angeboten. Der Download der aktuellsten Version 8.6 (Mitte 2019) beträgt circa 4,3 GB. Eine schlanke CD-Version (circa 700 MB) gibt es zwar auch noch, wird aber seit 2013 nicht mehr gepflegt und stagniert seither bei Version 7.2. Es empfiehlt sich also der Griff zur großen DVD-Variante. Achten Sie in der Liste der ISO-Dateien auf „-DE“ im Dateinamen (KNOPPIX_V8.6-2019-08-08-DE.iso), um das System mit deutscher Benutzerführung herunterzuladen.

Knoppix live: Ungeachtet mancher irreführender Hinweise ist das originale Knoppix-ISO nicht auf den DVD-Start reduziert, sondern bietet eine moderne hybride Startumgebung. Ein Zwischenschritt über einen DVD-Rohling ist daher nicht nötig, Knoppix bootet auch von einer Rohkopie auf USB-Stick. Als Werkzeug für diese Rohkopie taugen die üblichen Tools wie dd, GnomeDisks („Laufwerksabbild wiederherstellen“), Etcher (*https://etcher.io*) oder der Win 32 Disk Imager unter Windows.

Nach dem Schreiben als Rohkopie ist Knoppix ein pures Livesystem, das keinerlei Änderungen speichert – egal ob auf DVD oder auf USB. Das Dateisystem wird in den Arbeitsspeicher geladen und somit gehen die in der Sitzung getätigten Änderungen beim Herunterfahren wieder verloren. Typischerweise erkennen Sie ein laufendes Livesystem mit dem mount-Befehl im Terminal, der ein „loop0“-Device, ein „cloop“-Device (komprimiert), ein „squashfs“ (komprimiert) oder auch ein „aufs“-Dateisystem anzeigt (Another Union File System). Im Falle von Knoppix gibt es mehrere cloops- und unionfs-Geräte.

Das originale Knoppix live ist ausreichend, wenn Sie gelegentlich ein transportables Zweitsystem für Reparaturen, zum Surfen oder Spielen benötigen.

Knoppix live mit Overlaypartition: Die ideale Knoppix-Einrichtungsvariante für den Dauerbetrieb ist der Einsatz einer zusätzlichen beschreibbaren Overlaypartiti-

on. Diese speichert und transportiert nicht nur persönliche Dokumente, sondern erlaubt auch dauerhafte Anpassungen, Installation, Deinstallationen. Diese Variante ist nach unserer Kenntnis nur aus einem bereits laufendem Knoppix zu erreichen, dies aber ganz einfach: Das maßgebliche Tool liegt standardmäßig als Link „Flash Knoppix“ auf dem Desktop. Im Menü ist es unter „Knoppix → Knoppix auf Flash kopieren“ zu erreichen. Wie der Name sagt, ist Flash Knoppix der Installationsassistent für Kopien auf beschreibbare USB- und SD-Medien, kann aber auch für die Einrichtung auf Festplatten genutzt werden.

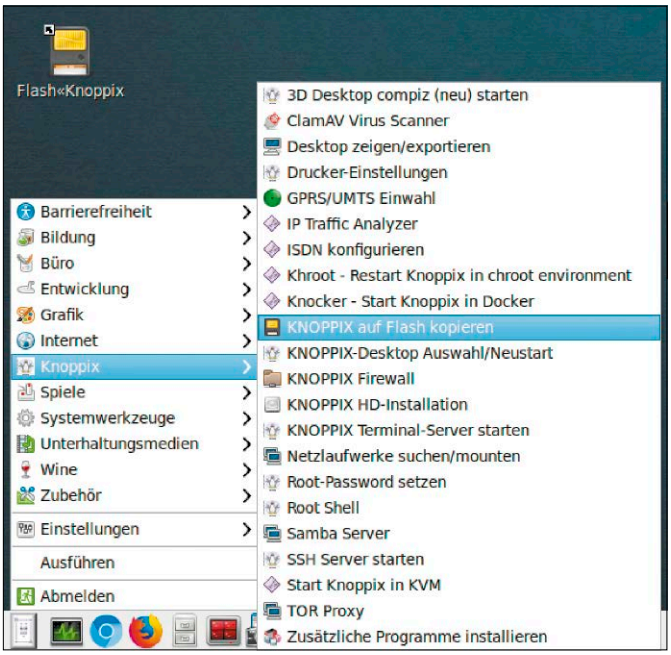
1. Der erste Dialog fragt ab, ob lediglich Wechselmedien oder auch interne Festplatten als Ziel infrage kommen. Je nach Ihrer Antwort ermittelt das Tool anschließend die passenden Datenträger. Das Medium, auf dem Knoppix gerade läuft, wird erfreulicherweise nicht angeboten – ein logischer, aber nicht selbstverständlicher Service des Tools.

2. Nach Auswahl des gewünschten Zieldatenträgers wählen Sie die Option „Installation auf FAT32 mit zusätzlicher Overlay-Partition“. Um das Dateisystem FAT32 der Systempartition müssen Sie sich nicht kümmern, dafür sorgt das Tool automatisch. Die Overlaypartition („Knoppix-Data“) erhält das Dateisystem Reiser FS.

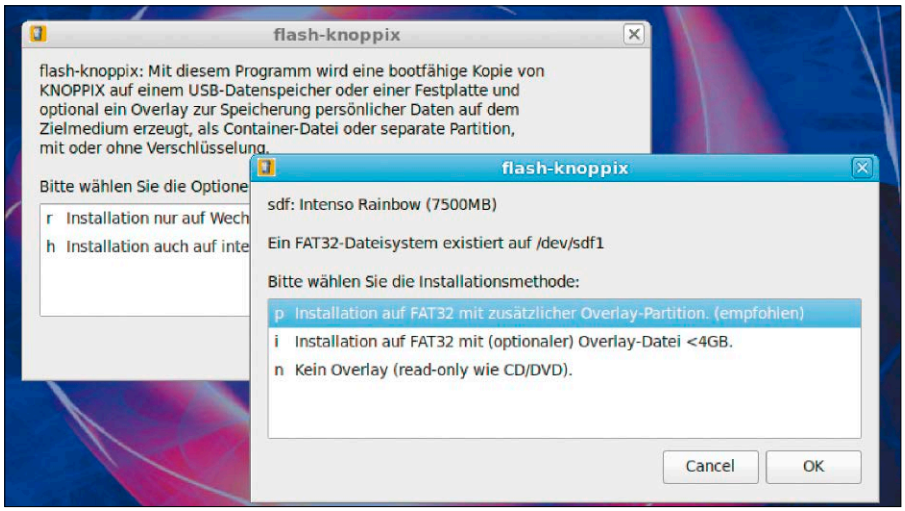
3. Die nächste Abfrage „Möchten Sie Knoppix remastern?“ ist nur relevant, wenn Sie das Knoppix-System, mit dem Sie gerade installieren, bereits individuell angepasst haben. Mit anderen Worten: Wenn Sie gerade Ihr erstes Knoppix mit Overlaypartition erstellen, beantworten Sie die Frage mit „Nein“. In einem späteren angepassten Knoppix ist diese Option jedoch umso wichtiger: Mit der Antwort „Ja“ erreichen Sie, dass Ihre nächste Knoppix-Kopie wieder alle persönlichen Einstellungen mitbringt.

4. Die Abfrage zur Größe der Overlaypartition können Sie auf einem USB-Stick normaler Größe einfach mit „OK“ übernehmen. Dann erhält die Overlaypartition auf dem Stick die komplette Restkapazität, die das eigentliche Knoppix-System übrig lässt. Bei Installation auf Festplatte schränken Sie die Größe mit dem Schieberegler auf Wunsch ein.

5. Die letzte Frage betrifft den optionalen Verschlüsselungsschutz der Overlaypartition. Es handelt sich um die einzige Möglichkeit, ein Knoppix-System systemweit zu schützen. Knoppix als Livesystem hat nämlich keine Benutzerverwaltung. Der Liveuser „knoppix“ kommt ohne Anmeldung an den Desktop und ist sudo-berechtigt. Wählt man bei der Einrichtung hingegen die Verschlüsselung, dann stoppt später der Bootvorgang relativ früh (vor dem Umschalten in den grafischen Textmodus) und fragt nach dem Kennwort („passphrase“). Dieses muss ohne Feedback eingegeben werden. Ein Start des Systems ohne Kennwort ist nicht möglich; ebenso erfolglos bleibt der Versuch, die Daten mit einem Fremdsystem auszulesen. Diese Verschlüsselung ist für USB-Sticks sehr zu empfehlen, umso mehr, wenn die Overlaypartition nicht nur Systemeinstellungen, sondern auch persönliche Daten speichert.

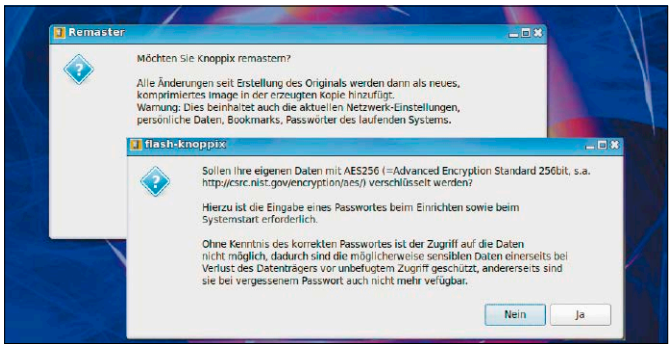


Das wichtigste Knoppix-Tool: Nicht ohne Grund ist Flash Knoppix Dauergast auf dem Desktop. Damit machen Sie aus einem Livesystem ein flexibles Linux.



Empfohlene Einrichtungsvariante mit Persistenz: Die Overlaypartition ermöglicht dem Livesystem Desktopanpassungen, Installationen und Deinstallationen.

Knoppix auf Festplatte: Trotz ausufernder Software und verspielter Effekte ist Knoppix mit seinem pragmatischen Standarddesktop LXDE äußerst bescheiden und fordert nur circa 300 MB RAM für System plus Oberfläche. Damit ist Knoppix mit LXDE, eventuell auch mit KDE, auch ein geeigneter Kandidat für eine Festplatteninstallation auf älteren Notebooks/PCs. Der dafür vorgesehene Assistent unter „Knoppix → Knoppix HD-Installation“ ist im Vergleich mit dem Tool Flash Knoppix allerdings konfus, fehlerträchtig, wahrscheinlich fehlerhaft. Wir raten definitiv davon ab und empfehlen



Entscheidungen bei der Einrichtung: „Remastern“ ist praktisch, wenn bereits ein angepasstes (Overlay-)Knoppix vorliegt, das identisch kopiert werden soll. Verschlüsselung kompensiert die fehlende Benutzersicherheit.

auch für die Festplatteninstallation das Tool Flash Knoppix. Dabei erhalten Sie ein Livesystem mit üppiger Overlaypartition, das im Alltag wie ein normal installiertes Linux arbeitet – nur ohne Benutzerkonten und Anmeldesicherung.

Die Overlaypartition erhält das Dateisystem Reiser FS, das keinerlei Beschränkungen für Dateigrößen besitzt. Die fehlende Benutzersicherheit können Sie bei der Einrichtung durch die Verschlüsselungsoption kompensieren.

Knoppix individuell einrichten

Mit Overlaypersistenz erlaubt Knoppix Anpassungen aller Art, auch Nachinstallationen und Entfernen überflüssiger Pakete. (De-)Installationen sind über apt im Terminal zu realisieren, auf Wunsch auch über „Einstellungen → Synaptic-Paketverwaltung“. Voraussetzung ist zunächst das übliche

```
sudo apt update
```

zum Einlesen der Paketquellen. Danach können Sie aufräumen

```
sudo apt remove cheese evolution
  gerbera scribus […]
```

oder auch Fehlendes nachrüsten.

Um das sehr umfangreiche Hauptmenü nicht für jeden Softwarefavoriten bemühen zu müssen, empfiehlt sich nach Rechtsklick auf die „Anwendungsstartleiste“ die Einrichtung der wichtigsten Programme in der Hauptleiste. Alternativ sind auch Desktoplinks möglich, indem Sie im Hauptmenü nach Rechtsklick auf ein Tool die Option „Der Arbeitsfläche hinzufügen“ nutzen.

Wenn Sie den Knoppix-LXDE-Desktop versachlichen möchten, finden Sie mit „Einstellungen → CompizConfig-Einstellungsverwaltung“ unter „Effekte“ die zuständigen Optionen. Zumindest die „wackeligen Fenster“ sind nicht jedermanns Geschmack. Weitere LXDE-Anpassungen zeigen die „Einstellungen“ unter „Desktop-Einstellungen“ und „Erscheinungsbild anpassen“.

Knoppix hat neben LXDE noch zwei weitere Desktops an Bord. Alternativ lassen sich auch die anspruchsvolleren Oberflächen Gnome 3 oder KDE Plasma 5 starten, dies aber, da es keine Systemanmeldung gibt, nur im laufenden System über den Menüpunkt „Knoppix-Desktop Auswahl/Neustart“. Gnome halten wir unter Knoppix für unproduktiv, weil die opulente Softwareausstattung in der großen Gnome-Anwendungsübersicht sehr unübersichtlich wird. Außerdem ist der Gnome-Desktop für USB-Sticks (2.0) eine erhebliche Last. KDE Plasma ist mit seinem durchsuchbaren Hauptmenü die bessere und schlankere Alternative.

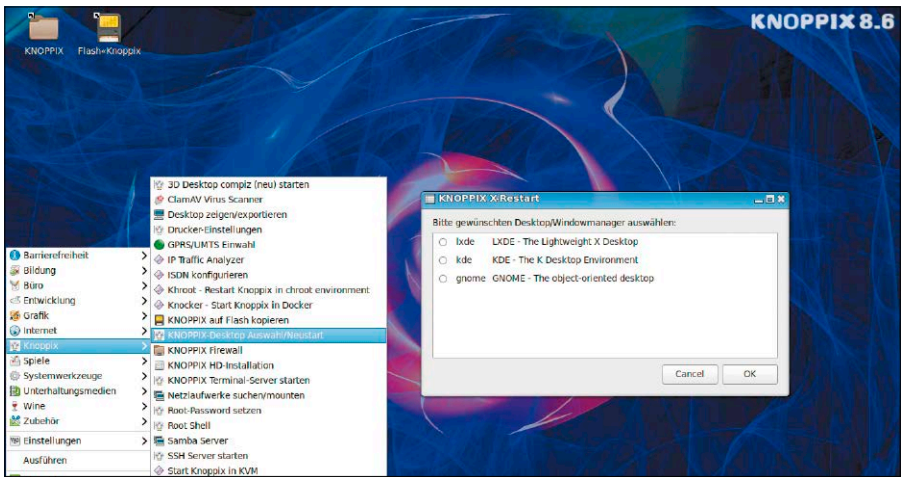
Knoppix startet künftig so lange mit einem einmal gewählten Desktop, bis Sie über den genannten Menüpunkt wieder zu einer anderen Oberfläche wechseln.

Die interessantesten Knoppix-Tools

Das wichtigste Knoppix-Werkzeug ist Flash Knoppix, das wir bereits im obigen Punkt ausführlich beschrieben haben. Das Menü „Knoppix“ versammelt aber eine Reihe weiterer nützlicher Tools: Mit „Knoppix → Netzlaufwerke suchen/mounten“ startet das System eine sehr zuverlässige Suche nach Samba-Freigaben. Zur Verbindung zu einem der dann angezeigten Server ist dann nur noch die Eingabe des Kontonamens und des Samba-Passworts nötig. Die danach automatisch eingehängte Freigabe erscheint im Dateimanager.

Umgekehrt kann Knoppix auch schnell mal selbst Daten freigeben. Während sich das veraltete Script „Sambastart“ („Knoppix → Samba Server“) in einer Endlosschleife verfängt, gelingt der Start des SSH-Servers über „Knoppix → SSH Server starten“ problemlos. Zugriff erhält das Konto „knoppix“ mit dem zu vergebenden Kennwort. Linux-Rechner im lokalen Netz können sich dann mit dem Dateimanager und der Adresse „sftp://[IP-Adresse]“ bequem verbinden. Für Windows-Rechner ist der Datenzugriff über typische SSH-Clients wie Putty etwas umständlicher, weil man dann – etwa über den Midnight Commander – erst eine Shell-Verbindung zu einem dritten Rechner als Übergangsstation aufbauen muss. Die Option „Knoppix → TOR Proxy“ bereitet den Weg in das anonymisierende TOR-Netzwerk vor. Sobald das Tool die Erfolgsmeldung „TOR wurde gestartet“ bringt, können Sie über „Internet → TOR Browser“ den Browser laden. Beim allerersten Mal muss dieser erst aus dem Web nachgeladen werden.

Eine interessante Sicherheitsfunktion bietet der Punkt „Knoppix → Start Knoppix in KVM“. Sofern die Rechnerhardware mitspielt, lädt Knoppix hier eine Originalkopie seiner selbst (ohne Overlayanpassungen) als virtuelle Maschine mit dem Virtualisie-



Der schlanke LXDE-Desktop ist Knoppix-Standard. Als Alternativen sind Gnome und KDE an Bord, wobei uns Gnome aus mehreren Gründen für ein Knoppix-Livesystem ungeeignet erscheint.

rer Qemu. Start wie Betrieb der VM verlaufen auch auf USB frappierend flott. Die VM kann etwa für den doppelt gesicherten Surfausflug mit dem Browser dienen (VM unter einem Livesystem!). Nebenbei haben Sie mit der VM immer ein originales Knoppix zur Hand, falls Sie das Overlaysystem zu weitreichend abgespeckt haben.

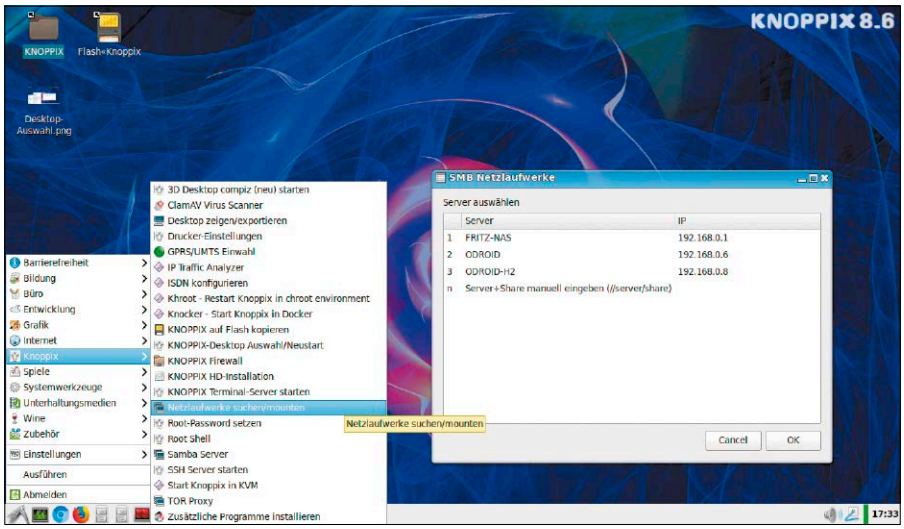
Die Option „Knoppix → Desktop zeigen/exportieren“ erlaubt die Remotefreigabe des Knoppix-Desktops. Dabei benutzt Knoppix das VNC-Protokoll, unterscheidet bei der Freigabe zwischen „Nur beobachten“ und „Steuerung erlauben“ und sichert die Freigabe durch ein optionales Kennwort, das Sie vor der Desktopfreigabe eingeben. Der zugreifende Rechner benötigt einen Client wie das verbreitete Remmina, das Knoppix natürlich auch an Bord hat („Internet → Remmina“). Remmina benötigt für den Zugriff nur die IP-Adresse, das Kennwort und die Protokollangabe „VNC“. Das unter Knoppix installierte Remmina hat neben VNC und SSH auch das RDP-Plug-in an Bord, das Windows für die Desktopfreigabe verwendet.

Systemwerkzeuge und Zubehör

Unter den Kategorien „Systemwerkzeuge“ und „Zubehör“ versammelt Knoppix alle Gnome- und KDE-Kandidaten, die für Datenträger-, Datei-, Task- und Netzwerkverwaltung Rang und Namen haben. Knoppix will jeden Nutzer versorgen, egal von welcher Distribution und welchem Desktop er kommt. Das führt zu erheblicher Redundanz und erschwert den Durchblick gerade für weniger Erfahrene, denen Namen wie „Dolphin“, „Htop“ oder „Leafpad“ nicht auf Anhieb etwas sagen. Außerdem geht es im Hauptmenü munter hin und her zwischen beschreibenden Bezeichnungen und tatsächlichen Programmnamen. Wer hier mehr Klarheit haben will, kann auf seinem Overlay-Knoppix selbst aufräumen und aus dem jeweils halben Dutzend an Dateimanagern, Systemmonitoren, Terminals oder Texteditoren die irrelevanten herausfiltern. Ein „apt remove…“ ist die radikale Antwort, etwas sanfter ist nach

```
sudo pcmanfm /etc/share/
 applications
```

das Löschen oder Umbenennen von Desktopdateien. Geht es nur um das Entschlacken des Menüs, ist unter „Zubehör → Hauptmenü“ der Menüeditor Alacarte an Bord. Änderungen mit diesem Editor gelten erst nach einer Abmeldung vom Desktop.



Komfortables Systemtool: „Netzlaufwerke suchen/mounten“ findet Samba/Windows-Freigaben im lokalen Netz.

Ungeachtet dieser eher kritischen Bemerkungen steht auf der positiven Seite außer Frage, dass jeder Linux-Nutzer unter Knoppix sein favorisiertes Systemtool vorfindet: Klassiker wie Gparted, Gnome-Disks („Laufwerke“), Hardinfo („System Profiler“) oder Gnome-System-Monitor („Systemüberwachung“) sind ebenso an Bord wie bewährte Editoren (Kate, Kwrite, Bluefish, Geany, Emacs, Leafpad), kleine Helfer wie Sweeper (Aufräumen), Baobab (Festplattenbelegung), Ark (Archivmanager) oder die Wine-Umgebung für Windows-Programme.

Office, Medien, Unterhaltung und Spiele

Das Livesystem versammelt auf komprimierten 4,3 GB eine Armada an Anwendungssoftware – auch hier mit bewusster funktionaler Redundanz, um jedem das Gewohnte anbieten zu können. Mit Alternativen wie Firefox und Chromium, Thunderbird und Evolution, VLC und MPV Player, Kdenlive und Openshot, Eog und Gpicview, Evince, Xournal, Okular (Dokumentenbetrachter) fallen die Doppelungen aber dosierter aus als bei den Systemwerkzeugen. Ansonsten steht mit Libre Office, Calibre (E-Book-Verwaltung), Gimp (Bildbearbeitung), Amarok, Audacity, Blender, Brasero, Freecad, Handbrake, Mediathekview, Inkscape, Keypassx, Ktorrent Pidgin, Remmina, Putty wirklich alles parat, was ein Linux-Nutzer für den Medienkonsum und für den produktiven Alltag benötigt (wobei unsere kleine Liste nur die prominentesten Programme erwähnt).

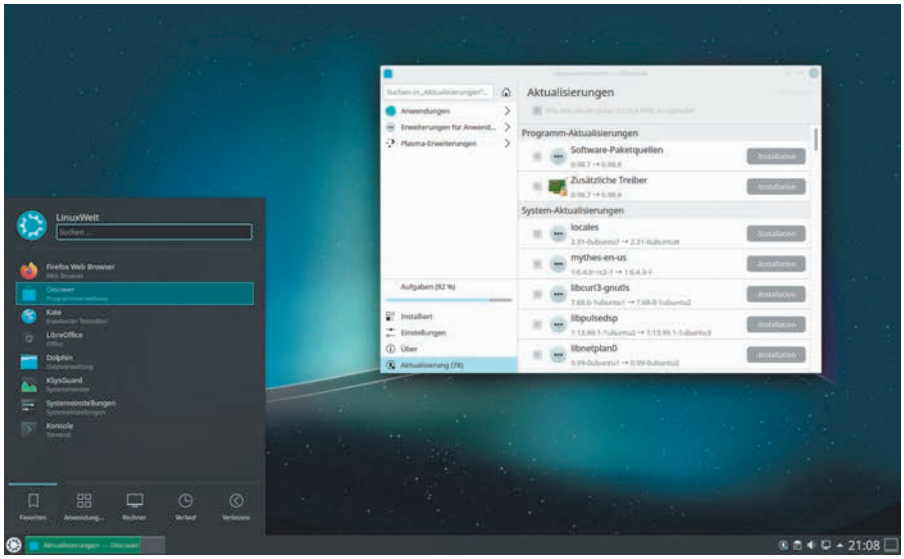
Nicht zu vergessen: Annähernd 80 Spiele bringt Knoppix auch noch unter. Da ist – freundlich formuliert – auch Krimskrams dabei, aber auch viel Unterhaltsames. Spiele wie Kobi Deluxe, Kapman oder Kblocks sind nicht ganz der aktuelle Stand der Spieleentwicklung, haben aber das Suchtpotenzial für viele verlorene Stunden (dieser Artikel wurde trotzdem rechtzeitig fertig). ■

Auch das ist Knoppix: Das Livesystem bringt nicht nur Nutzwert pur, sondern auch eine ganze Menge Spielspaß mit.

Linux-Desktopsysteme

Der Heftschwerpunkt liefert auf den nächsten 20 Seiten Distributionsempfehlungen für diverse Rollen. Den Start macht der PC- und Notebookdesktop. Für diese Rolle konkurriert eine große Zahl von Linux-Systemen und die Entscheidung ist besonders heikel.

VON HERMANN APFELBÖCK



Heißt die Frage wirklich „Debian, Arch, Ubuntu, Mint, Mageia, Solus …"? Oder nicht vielleicht eher „KDE, Gnome, Cinnamon, XFCE, Mate, Budgie …"? Die grafische Oberfläche ist es, die das Benutzererlebnis prägt, und manchem Anwender mag es sogar egal sein, ob unter dem vom ihm bevorzugten KDE oder Cinnamon ein Arch oder Debian läuft.

Die Oberfläche ist fundamental, weil es ja nicht nur um Menü, Systemleiste und Arbeitsoberfläche geht: Grafische Systemeinstellungen, Dateimanager, Taskmanager kommen allesamt vom Desktop und bestimmen den Benutzeralltag. Daher beziehen wir bei den Empfehlungen für PC und Notebook den zugehörigen Desktop in knappster Charakterisierung mit ein.

1. Die offiziellen Ubuntus

Ubuntu-Varianten beherrschen den PC-Desktop. Die Systembasis ist schnell, aber abgesehen vom Derivat Bodhi Linux (siehe ab Seite 28) nicht rekordverdächtig schnell. Arch-basierte Distributionen sowie Solus-OS sind ein Stück schneller. Ubuntus bieten aktuellere Software als die Stammmutter Debian, können aber auch hier mit Arch nicht konkurrieren. Dafür gibt es aber hier erweiterte Softwarequellen mit PPAs. Snap- und/oder Flatpak-Unterstützung ist als zusätzliche Quelle meist vorinstalliert. Eine Ubuntu-Installation ist immer komfortabel und findet entweder mit dem angestammten Ubiquity oder mit Calamares statt (Kubuntu, Lubuntu). Attraktiv sind ferner ein Supportzeitraum von mindestens drei Jahren und ein zuverlässiges Upgradeverfahren nach Ablauf einer Version.

Von Ubuntu gibt es sechs offizielle Editionen für den Desktop. „Offiziell" bedeutet, dass die Entwickler mit der Ubuntu-Firma Canonical zusammenarbeiten und deshalb ihre Derivate gleichzeitig mit Erscheinen der Hauptversion anbieten können (anders als Mint, Zorin & Co.).

Ubuntu: Die Hauptedition von Canonical nutzt einen angepassten Gnome – eine innovative Oberfläche mit bildschirmfüllender Programmübersicht (Windows-A) statt Hauptmenü, „Aktivitäten" (Windows-Taste) zu Programmsuche, Fensterwechsel und Wechsel der virtuellen Desktops. Das Gnome-Einstellungen-Center sowie Softwarecenter, Laufwerkstool und Dateimanager erlauben eine weitgehend lückenlose grafische Bedienung des Systems. Mit Anpassungsoptionen geizt die Oberfläche und die Arbeitsoberfläche wird nur durch Erweiterungen zur universellen Dateiablage. Das Starterdock für Programmfavoriten ist ebenfalls Gnome-fremd und von Ubuntu hinzugefügt.

Kubuntu: Die Edition mit KDE Plasma ist das Ubuntu mit dem universellsten Desktop. Kontrollzentrum, Softwarecenter „Discover", Laufwerksmanager, Dateimanager Dolphin, Desktop als Ablage für Datei und Widget sowie minutiöse Anpassungsfähigkeit machen Terminalausflüge unter KDE zur Option, kaum zur Pflicht.

Ubuntu Mate: Desktop als Ablage, multifunktionales Menü, anpassungsfähige Systemleiste, umfassende Konfigurationszentrale („Steuerzentrale"): Alles ist aufgeräumt und einfach zu bedienen, zudem reaktionsfreudig. Hinzu kommt ein funktionsreicher Dateimanager Caja. Ein Laufwerkstool fehlt, kann aber nachinstalliert werden (gnome-disk-utility). Dennoch ist die Standortbestimmung des konservativen Ubuntu Mate problematisch: Wer ein sparsames System sucht, wird eher zu Xubuntu mit XFCE-Desktop greifen.

Ubuntu Budgie: Die Eigenschaften des namengebenden Budgie-Desktops sind unter „Solus-OS" skizziert.

Xubuntu/Lubuntu: Diese Ubuntus werden ab Seite 34 kurz beschrieben („Linux für

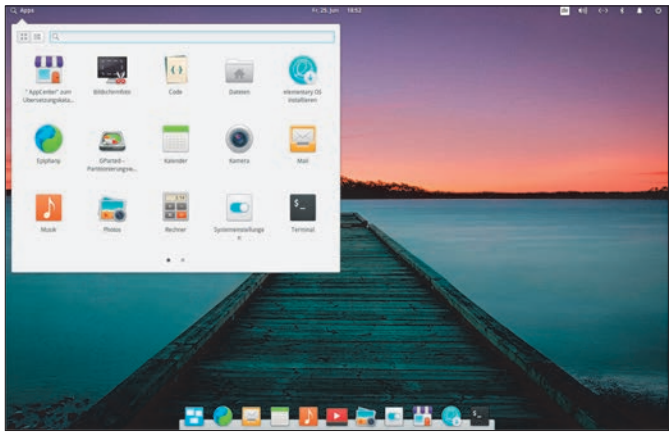
ältere Hardware“). Lubuntu hat seit dem Umstieg vom extrem sparsamen LXDE auf das schickere, aber austauschbare LXQT gewissermaßen seinen Fokus verloren. Xubuntu (mit XFCE) hingegen hat bei pragmatischen Nutzern durchaus auch einen Platz auf moderner Hardware. Überall anpassungsfähig, mit einer Arbeitsflache als Datei- und Starterablage, dem grafischen Softwarecenter von Gnome und einer weitreichenden (nicht ganz an Gnome oder KDE heranreichenden) Konfigurationszentrale ist die ausgereifte Oberfläche hier und in anderen Distributionen jederzeit ein Empfehlung. Ein Laufwerkstool fehlt, kann aber nachinstalliert werden (gnome-disk-utility).

2. Prominente Ubuntu-Derivate

Inoffizielle Ubuntus verwenden die Ubuntu-Basis, ohne von Canonical unterstützt zu werden. Allen diesen Derivaten ist gemeinsam, dass sie einige Monate hinterherlaufen müssen. Kein Mint, Elementary, Zorin kann ein Trendsetter im technischen Unterbau sein (Linux-Kernel, Ubuntu-Basis). Andererseits profitieren sie wie die offiziellen Derivate vom dreijährigen Supportzeitraum.

Linux Mint: Das Ubuntu-Derivat ist bei Linux-Kennern wie Einsteigern erste Wahl am PC-Desktop. Ungeachtet einiger Tool-Eigenentwicklungen ist der eindeutige Hauptgrund die Oberfläche Cinnamon. Gemeinsam mit Softwarezentrale und Konfigurationszentrale bildet sie die komplette Systemverwaltung mit grafischen Mitteln ab, ist dabei anpassungsfähig, bietet eine Arbeitsoberfläche als Datei- und Gadget-Ablage und kommt nebenbei Windows-Umsteigern mit vielen Detailanalogien entgegen (siehe auch Neuvorstellung der Version 20.2 ab Seite 18).

Elementary OS: Diese Distribution ist ideal für Anwender, die ihre Standardprogramme auf einem ästhetischen und aufgeräumten Desktop nutzen wollen – und nicht viel mehr. Die Desktop-Eigenentwicklung Pantheon orientiert sich am Mac und gehört zu den attraktivsten Linux-Desktops. Oberste Prämisse ist allerdings Reduktion: Die Systemleiste bietet ein schickes Programm-Menü und fundamentale Indikatoren (Lautstärke, Netz, Shutdown), ist aber nicht erweiterbar. Die Konfigurationszentrale ist auf Fundamentales reduziert und der Desktop hat keine Ordnerfunktionalität. Für (notwendige) Nachinstallationen gibt es ein hübsches „Appcenter“. Elementary OS will beim Download einen freiwilligen Obulus, gibt sich aber auch mit „0 Euro“ zufrieden.



Das schöne Elementary OS mit Pantheon: Es muss aber so gefallen, wie es ist, denn Anpassungen sind kaum vorgesehen.

Zorin-OS will 39 Euro für den Download der „Ultimate“-Variante, die kleinere „Core“-Variante gibt es aber kostenlos. Oberfläche ist ein ausgesprochen eleganter, tiefgreifend angepasster Gnome ohne „Aktivitäten“, mit klassischem Menü und Ordnerfunktionalität. Das übliche Gnome-Verhalten ist aber mit Windows-Taste („Aktivitäten“) und Windows-A (Programmübersicht) ebenfalls erreichbar. Alle Gnome-Komponenten wie Gnome-Software oder Gnome-Control-Center sind weitgehend original enthalten. Die Paketverwaltung hat sowohl Snaps wie Flatpaks integriert. Komponenten wie das AWN-Dock in der Systemleiste richten sich speziell an Umsteiger und bilden das Windows-Verhalten ab. Unterm Strich ist Zorin weit anpassungsfähiger als Elementary und in der Nähe von Linux Mint einzuordnen.

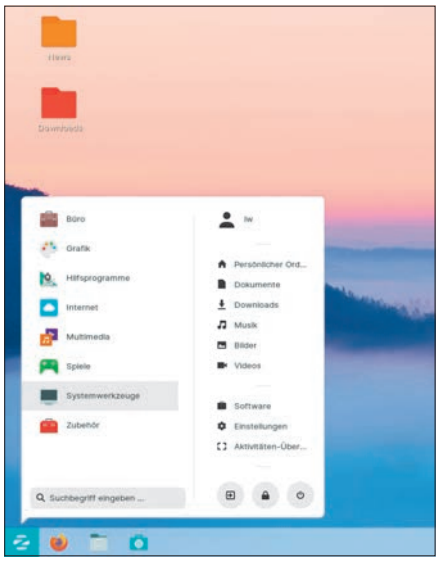
Voyager Live: Das Attribut „Live“ im Distributionsnamen ist nicht technisch gemeint, da es sich um ein normal zu installierendes Ubuntu handelt. Die Distribution demonstriert mit ihrer XFCE-Edition, was man aus dem konservativen Klassiker XFCE machen kann – eine beeindruckend hübsche und reaktionsschnelle Oberfläche: Hunderte von Wallpapers, Dutzende von Farbthemen, moderne Iconsets inklusive Farbwechsler. Voyager Live baut bekannte Kom-

INFOS ZU LINUX-DISTRIBUTIONEN

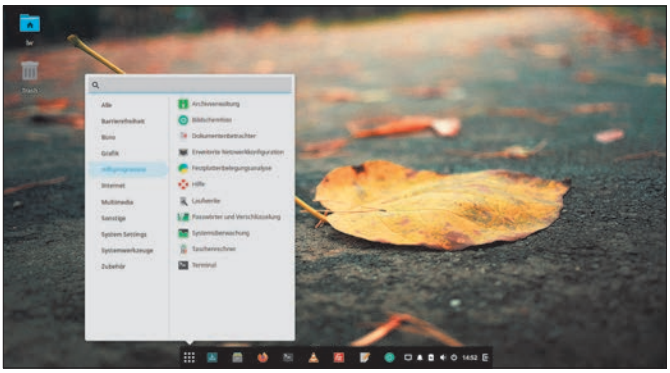
Die deutschsprachige Wikipedia-Seite „Liste von Linux-Distributionen“ (*https://de.wikipedia.org/wiki/Liste_von_Linux-Distributionen*) bietet einen Gesamtüberblick über die Derivate aller Linux-Hauptzweige. Neben Stammbäumen zu Arch, Debian & Co. gibt es eine Kurzcharakterisierung des Hauptstamms und einen Mini-Steckbrief zu den einzelnen Derivaten. Für eine Erstorientierung ist dieser Überblick nützlich, als praxisnahe Entscheidungshilfe zu dünn.

Die englischsprachige Wikipedia-Seite „Comparison_of_Linux_distributions“ (*https://en.wikipedia.org/wiki/Comparison_of_Linux_distributions*) zeigt auf anspruchsvollen Tabellen fundierte Infos zu einer Auswahl wichtiger Distributionen. Hier ist etwa die Existenz eines installierbaren Livesystems oder eines grafischen Installers, der Standarddesktop, die installierte Standardsoftware recherchierbar. Abgesehen von der begrenzten Vorauswahl und Menge leisten diese Tabellen die beste Entscheidungshilfe für eine strategische Distributionssuche.

Distrowatch (*https://distrowatch.com*) liefert Basisdaten über Herkunft und Ausrichtung und knappe, selten tiefschürfende Charakterisierungen. Hier ist aber alles anzutreffen, Exoten und längst begrabene Projekte inklusive. Außerdem ist die Rangliste auf der Distrowatch-Startseite (rechts) ein vielbeachtetes Bewertungssystem für die aktuelle Popularität der Distributionen, wenngleich sie über die tatsächliche Verbreitung nichts aussagt.



Konkurrenz für Linux Mint: Zorin-OS bedient auch Windows-Umsteiger und macht aus Gnome eine klassische Oberfläche.



Schnelles Solus mit ruhigem Budgie: Der Desktop ist besonders reduziert und aufgeräumt. Solus-Nutzer müssen aber mit begrenzter Softwareauswahl auskommen.

ponenten mit viel Sorgfalt zusammen, erweitert die XFCE-Einstellungszentrale sinnvoll und bringt das Gnome-Laufwerkstool mit. Mit Systemleisten, Desktop- und Themenanpassungen übertreibt es die Distribution ein wenig. Wer nicht mehr durchblickt, erreicht die meisten der Distributions-Spezialitäten über die „Voyager Box", die überall nach Rechtsklick angeboten wird.

3. Debian und Derivate

Die Desktop-dominierenden Ubuntus fußen allesamt auf Debian. Anspruchslose Debian-Derivate wie Bunsenlabs, Q4-OS, MX Linux oder Antix haben ihren wichtigen Platz auf älterer Hardware und werden an anderer Stelle besprochen (ab Seite 34 und 38). Debian selbst spielt aber am Desktop nur eine marginale Rolle. Das liegt am System selbst mit seiner konservativen Ausrichtung und zum Teil veraltetem Softwareangebot, außerdem an älteren Desktopumgebungen, die ohne Feintuning installiert werden. Beim kleinen Netinstaller-ISO von Debian stehen aber alle namhaften Desktops zur Auswahl (Gnome, KDE, XFCE, Cinnamon, Mate, LXDE, LXQT). Wer mit älteren Desktop- und Softwareversionen klarkommt und sich den Desktop selbst optimieren kann, erhält mit Debian einen grundsoliden Desktop.

Netrunner: Diese Distribution stellt sich in den Dienst des KDE-Desktops. Dafür gibt es sogar zwei Ausgaben, eine auf Debian basierend, die zweite auf Manjaro. Manjaro-Netrunner bietet dabei stets das noch aktuellere KDE Plasma. Beide Ausgaben sind näher am KDE-Puls als Kubuntu. Absolute KDE-Fans erhalten allerdings mit KDE Neon stets das ganz brandneue KDE (siehe ab Seite 28). Weiteres Merkmal von Netrunner ist eine besonders umfangreiche Softwareausstattung ab Installation.

LMDE: Die Linux Mint Debian Edition führt neben dem Ubuntu-basierten Linux Mint nur ein Nischendasein. Generell ist hier alles ein Stück älter und unkomfortabler als beim originalen Linux Mint. LMDE ist daher keine Empfehlung für Benutzer, sondern ein strategisches Fallback-Projekt des Mint-Teams, falls Linux Mint eines Tages die Ubuntu-Basis nicht mehr nutzen könnte.

Steam-OS: Dieses Debian-System ist auf Spiele der Steam-Plattform spezialisiert. Die Kombination mit passender Gaminghardware blieb jedoch unter den Erwartungen, da sie weder den Umfang noch die Leistung von Windows erreicht. Da zum Spielen die Software Steam genügt, ist Steam-OS nur ein System für Hardcoregamer unter Linux.

4. Manjaro: Arch für den Desktop

Arch gilt als System für Kenner, das bei der Installation und Systemwartung souveräne Terminalkenntnisse verlangt. Manjaro (sowie Endeavour-OS, ab Seite 28) bringt Arch auf den Desktop normaler Anwender. Auf die Oberfläche legt sich Manjaro nicht fest: Offizielle Editionen mit Gnome, XFCE und KDE, ferner sieben weitere Desktops als „Community Releases" sorgen für freie Auswahl. Neben diesen Livemedien gibt es auch noch den Extra-Installer „Manjaro Architect", der die interaktive Auswahl von Desktop und Software vorsieht.

Der Manjaro-Installer „Thus" ist ein leicht geänderter Klon des bekannteren Calamares (auch in Kubuntu, Lubuntu). Als grafische Softwarezentrale arbeitet der schmucklose, aber funktionale Pamac-Manager. Ansonsten gelten für die Paketverwaltung die Regeln von Arch: Mindestens an Basisbefehle des Terminaltools Pacman sollten sich Manjaro-Nutzer gewöhnen.

Der Befehl

```
sudo pacman -Syu
```

aktualisiert das komplette System einschließlich Software.

Achtung, Manjaro ist ein „Rolling Release": Es wird also über Funktionsupdates ständig aktuell gehalten, ist aber als Rolling-System anfälliger für Paketkonflikte.

5. Solus-OS: Chancenreicher Außenseiter

Solus-OS ist ein unabhängiges Desktop-Linux – schnell wie ein Arch-System und mit dem eigenen interessanten Budgie-Desktop, der inzwischen auch von anderen Distributionen aufgegriffen wurde. Budgie bietet eine aufgeräumte, kontrastive Benutzerführung ohne Schnickschnack, ist dabei noch einfacher und reduzierter als Gnome oder Pantheon (Elementary OS), dafür aber anpassungsfähiger. Die Arbeitsoberfläche hat keine Funktion als Datei- oder Starterablage. Typische Gnome-Komponenten wie Gnome-Control-Center („Einstellungen") oder Dateimanager Nautilus kombiniert Budgie mit einem eigenen, relativ einfachen grafischen Softwarecenter. Im Terminal muss man sich an den Paketmanager eopkg gewöhnen, der aber ähnlich wie apt (Debian/Ubuntu) arbeitet. Die Paketquellen von Solus sind wesentlich ausgedünnter als jene von großen Distributionen, enthalten aber die Softwareprominenz.

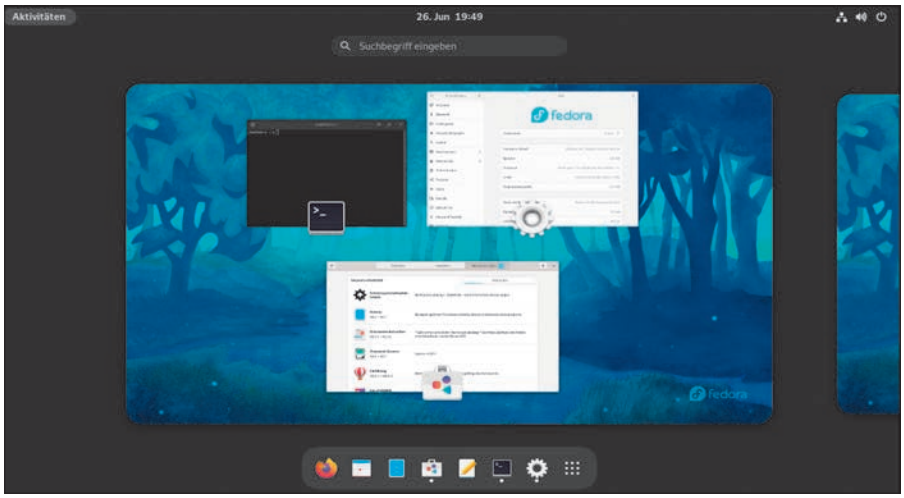
Achtung, Solus-OS ist wie Manjaro ein „Rolling Release": Es wird also über Funktionsupdates ständig aktuell gehalten, ist aber wie jedes Rolling-System anfälliger für Paketkonflikte.

6. Fedora Workstation: Avantgarde

Fedora Workstation ist quasi die experimentelle Vorstufe von Red Hat Enterprise Linux. Wer Fedora nutzt, schätzt aktuelle Kernel-, Desktop- und Softwareversionen sowie innovative Linux-Entwicklungen. So ist Fedora Vorreiter beim neuen Displaymanager Wayland oder beim Dateisystem BTRFS. Mit Fedora ist man in der Linux-Avantgarde, aber nicht immer auf einem soliden Produktivsystem. Standarddesktop beim Fedora-Livemedium ist ein Gnome (original ohne Anpassungen), jedoch sind unter *https://spins.fedoraproject.org* auch Editionen mit KDE, Cinnamon & Co. Zu erreichen. Der Fedora-eigene Installer verkürzt die Prozedur auf das Einfachste, auch die Anlage des Erstbenutzers wird auf den ersten Systemstart verlegt.

Fedora liefert prinzipiell nur freie Open-Source-Software aus. Weitere Codecs und Player sind aber über RPM Fusion erhältlich (*https://rpmfusion.org*).

Da alle Versionen von Fedora Workstation stets nur ein gutes Jahr (circa 13 Monate) Updates erhalten, ist periodisch ein Upgrade auf die nächste Version erforderlich, was aber sowohl grafisch wie auf der Kommandozeile unterstützt wird.



Fedora Workstation mit Gnome (Standard): Wer Fedora einsetzt, muss mit experimentellen Systemfunktionen einverstanden sein.

7. Mageia: Alles etwas anders

Mageia geht über das stillgelegte Mandriva auf Red Hat Linux zurück und ist somit dem weiteren Dunstkreis von Open Suse und Fedora zuzurechnen (mit RPM-Paketierung). Als Installationsmedien stehen Editionen mit KDE Plasma, Gnome und XFCE zur Verfügung. Ergänzt wird die grafische Oberfläche durch die eigenen „Drak"-Tools. Dies beginnt bereits mit dem ungewohnten Installer „Draklive", der einerseits Partitionierungsmöglichkeiten vermissen lässt, andererseits bereits Feineinstellungen für den Bootmanager vorsieht. Die Installeroption, „Onlinemedien" einzurichten, meint die Definition der Paketquellen, der dann auch gleich eine „Distributionsaktualisierung" folgen kann. Die Einrichtung des Erstbenutzers erfolgt hingegen nicht bei der Installation, sondern beim ersten Start des installierten Systems. Für Verwaltungsaufgaben fordert Mageia ein klassisches root-Konto. Als grafisches Softwarecenter dient das komfortable „Drakrpm". Mageia zeigt beim Booten keine Eile, ist aber im Betrieb ein flottes System. Der Support einer Mageia-Version endet in der Regel einige Monate nach Erscheinen der Folgeversion. Dann ist ein Upgrade erforderlich und vorgesehen. Mageia ist solide, bietet aber unterm Strich wenige Anreize, ein- oder umzusteigen. Es ist eine Distribution für treue Fans, die es seit Jahren kennen und nutzen. ■

PROMINENTE LINUX-DESKTOPSYSTEME

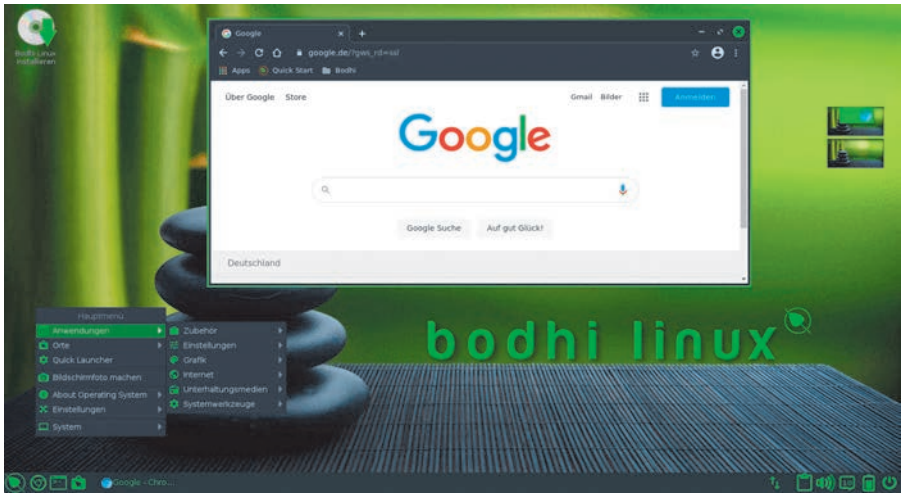
Distribution	Aktuell	Webseite	Download (MB)	Basis	Beschreibung
Debian	10	*www.debian.org*	340–3700	–	konservative Basis vieler Desktopdistributionen
Fedora Workstation	34	*https://getfedora.org/de*	1900	Red Hat	innovativer, aber kurzlebiger Desktopableger von Red Hat Enterprise
Mageia	8	*www.mageia.org*	2700–3400	Red Hat	solides, aber unspektakuläres Desktopsystem
Manjaro	21	*https://manjaro.org*	2400–2700	Arch	schnelles Arch mit Installer und Softwarezentrale; Rolling Release
Netrunner	21.01	*www.netrunner.com*	2600	Debian	umfangreiche Standardsoftware auf aktuellem KDE-Desktop
Solus-OS	4.2	*https://getsol.us/home/*	1800–2100	–	unabhängiges Linux mit eigenem Budgie-Desktop; Rolling Release
Steam-OS	2.195	*http://repo.steampowered.com/*	1400	Debian	Debian-Derivat mit vorinstalliertem Client für die Spieleplattform Steam
Ubuntu	20.04	*www.ubuntu.com*	2700	Debian	Ubuntu-Originalversion von Canonical mit angepasstem Gnome
Ubuntu Budgie	20.04	*https://ubuntubudgie.org*	2100	Ubuntu	offizielles Ubuntu-Derivat mit Budgie-Desktop
Ubuntu Mate	20.04	*https://ubuntu-mate.org*	2300	Ubuntu	offizielles Ubuntu-Derivat mit Mate-Desktop
Kubuntu	20.04	*www.kubuntu.org*	2300	Ubuntu	offizielles Ubuntu-Derivat mit KDE Plasma
Xubuntu	20.04	*https://xubuntu.org*	1600	Ubuntu	offizielles Ubuntu-Derivat mit XFCE-Desktop
Elementary OS	6.0	*https://elementary.io/de/*	2500	Ubuntu	inoffizielles Ubuntu-Derivat mit eigenem Pantheon-Desktop
Linux Mint	20.2	*www.linuxmint.com*	2100	Ubuntu	inoffizielles Ubuntu-Derivat mit eigenem Cinnamon-Desktop
Voyager Live	20.04	*https://voyagerlive.org/*	1900	Ubuntu	inoffizielles Ubuntu-Derivat mit angepasstem XFCE (wahlweise Gnome)
Zorin-OS (Core)	15.3	*https://zorinos.com*	2300	Ubuntu	inoffizielles Ubuntu-Derivat mit stark angepasstem Gnome-Desktop

Spezielle Desktop-distributionen

Mainstream-Distributionen sind die richtige Wahl für Linux-Einsteiger wie für pragmatische Linux-Kenner. Wer – aus verschiedenen Motiven – Exotischeres sucht, findet spannende Alternativen, muss aber eventuell mit Risiken und Nebenwirkungen rechnen.

VON HERMANN APFELBÖCK

Zu weit abseits von der sicheren Mitte sollte man sich ein Desktopsystem, mit dem man produktiv arbeiten will, nicht auswählen. Zuverlässigkeit und langjährige Nachhaltigkeit sind ein wichtiges Kriterium. Einfache Installation, komfortable Systemverwaltung und gut gefüllte Paketquellen sind weitere Kriterien, die nicht überall erfüllt werden. Pures **Arch** zum Beispiel will einfach nicht unter die Leute, indem es ihnen das Setup möglichst schwer macht. Bei **Gentoo**, selbst im weichgespülten **Sabayon**-Derivat, sind Systemaktualisierung und Softwareinstallationen so zäh, dass man sich lieber auf das Notwendigste beschränkt. Die nachfolgenden Kandidaten bleiben der mehrheitstauglichen Mitte näher: Abstriche, die der Nutzer eventuell machen muss, werden durch spezielle Vorzüge ausgeglichen.



Schnellstes Ubuntu (Linux?): Bodhi ist sehr klein, sehr schnell, verzichtet aber auf etliche Konfigurationshilfen.

Bodhi Linux: Schnell anstrengend

Bodhi Linux muss auf jede Linux-Rechnung: Ungeachtet mancher Arch-Mythen ist das Ubuntu-basierte Bodhi das vermutlich schnellste Linux. Die aktuelle Version 6.0 ist auf Heft-DVD und erhält ihren Steckbrief in den DVD-Distributionsvorstellungen ab Seite 10. An dieser Stelle fassen wir uns kurz: Version 6.0 bestätigt alle Vor- und Nachteile vergangener Bodhi-Ausgaben. Der Footprint im RAM bleibt mit unter 250 MB absolute Ökoliga. Bodhi läuft auf alter Hardware und auf USB (2.0/3.0) richtig schnell, auf moderner Hardware frappierend: Selbst auf einem uraltem Notebook (mit SSD) messen wir zehn Sekunden Bootzeit zum Log-in-Bildschirm. Browser, VLC, Libre Office sind per Klick eingabebereit. Die Nachteile sind altbekannt: Der Desktop Moksha ist anstrengend und jetzt obendrein schwarz-moosgrün-düster – eine Moorwanderung mit Nachtsichtgerät. Die Konfigurationszentrale („Einstellungen → Einstellungskonsole“) kann hier vieles korrigieren, fordert aber Einarbeitungszeit. Gravierender aber als der eigenwillige Desktop, an den man sich gewöhnen kann, sind fehlende Konfigurationszentralen à la Gnome, KDE, XFCE, Cinnamon. Wer Monitoreinstellungen, Partitionen, Benutzerkonten bearbeiten will, ist auf das Terminal und auf externe Programme wie Gparted und Arandr angewiesen. Wer das beherrscht, erhält mit Bodhi einen Sprinter.

Endeavour-OS: Flottes Arch

Dieses System hat denselben Anspruch wie das bekanntere Manjaro, mit einem grafischen Installer den Zugang zu Arch Linux zu vereinfachen. Es verwendet den bekannten und komfortablen Calamares-Installer. Hinzu kommt die benutzerfreundliche Wahl zwischen Online- und Offline-Installation. „Offline“ ist schneller und installiert standardmäßig das auf dem ISO enthaltene XFCE, mit „Online“ besteht die Auswahl zwischen allen prominenten Linux-Desktops. Sie werden keine Mühe haben, ein Endeavour-OS mit bevorzugtem Desktop einzurichten. Das System ist schnell am Log-in und reaktionsschnell im Betrieb. Ein schlichter, aber nützlicher Welcome-Dialog hilft bei der Ersteinrichtung. Endeavour-OS nutzt die originalen Arch-Paketquellen, bietet dafür aber kein grafisches Programm. Eine Einarbeitung in pacman (offizielle Quellen) und yay (inoffizielle Quellen) ist also unerlässlich, aber nicht allzu anstrengend. Wer auf grafische Hilfe gar nicht verzichten kann, holt sich mit

```
sudo yay -S pamac
```

den grafischen Paketmanager Pamac auf das System.

KDE Neon: Nur für KDE-Fans

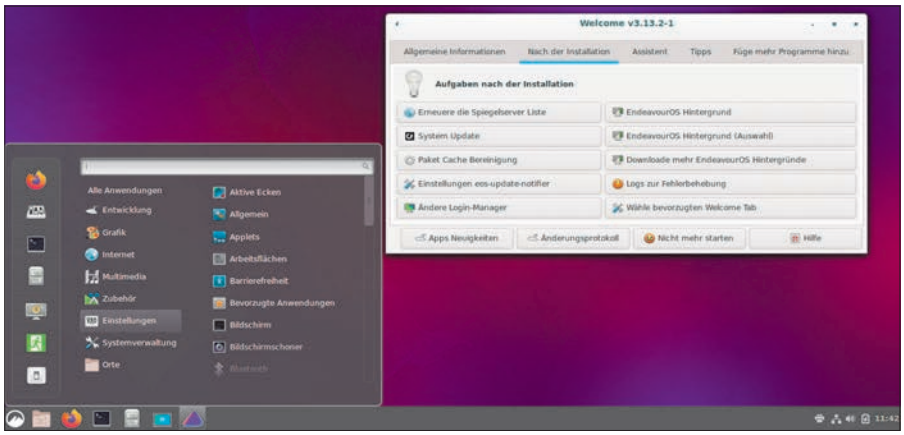
Die KDE Neon User Edition basiert auf Ubuntu und ist somit nicht mehr als ein aktuelleres Kubuntu. Für den hier immer hochaktuellen KDE-Plasma-Desktop gibt es laufend Funktionsupdates, während Kubuntu nur Sicherheitsupdates einspielt und der Desktop folglich funktional stagniert. KDE Neon ist eindeutig und ausschließlich eine Distribution für KDE-Fans!

Ubuntu Studio: Mit Spezial-Kernel

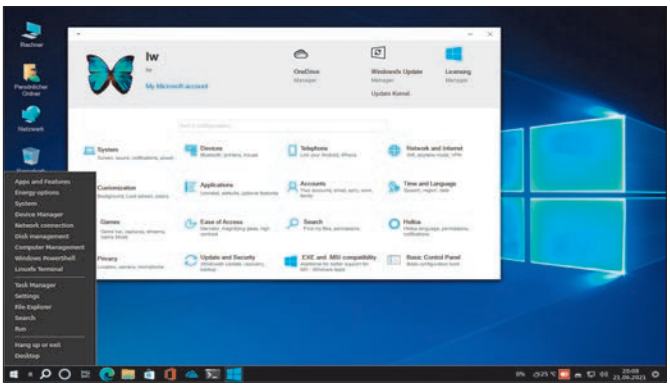
Manches Ubuntu-Derivat, das sich nur durch einige zusätzliche Software definierte, ist zurecht wieder von der Bildfläche verschwunden. Auch bei der Spezialdistribution Ubuntu Studio (*https://ubuntustudio.org*) steht allgemein verfügbare Software im Vordergrund, die ein Linux-System zur Digital Audio Workstation (DAW) ausbaut: Mit Ardour und Rosegarden sind wichtige Programme für die Aufnahme und das Mischen von Musik dabei, außerdem Werkzeuge für die Produktion von Podcasts und für die Konfiguration der verschiedenen Sound- und Filtersysteme. Sequenzer, Sampler, Midi-Programme und Drumcomputer sind ab Installation betriebsbereit.
Neben opulenter DAW-Software verwendet Ubuntu Studio aber auch standardmäßig einen speziellen Low-Latency-Kernel, der für die zeitgenaue Verarbeitung von Audiosignalen nötig ist. Ein weiterer Unterschied zum gewohnten Ubuntu besteht in der vorinstallierten Wine-Umgebung. Viele Soundbearbeitungsprogramme von Windows lassen sich damit auch unter Linux betreiben. Trotz aller Spezialisierung handelt es sich um ein Ubuntu, mit dem Sie jederzeit auch im Internet surfen oder Texte schreiben können.

Windows FX: Ist das Linux?

Diese Ubuntu-Distribution brasilianischer Herkunft ist spektakulär. Ob sie nutzwertig, nachhaltig und seriös ist, sollen die Benutzer entscheiden – und Microsoft. Was das Projekt nämlich aus Ubuntu/Mint/KDE/Cinnamon/Calamares/Wine produziert, ist eine Windows-10-Karosserie mit Linux-Motor. Alles an der Oberfläche ist offensichtliche, dreiste, aber technisch aufwendige Windows-Nachahmung. Mit einer pixeltreuen Kopie von Iconthema, Hintergrund, Anmeldung und Explorer-Optik ist es nämlich nicht getan: Windows FX schafft es, von der Installation bis zu Verwaltung alle Windows-Standards weitestgehend mit Cinnamon- oder KDE-Mitteln abzubilden. Auch ein „.exe and .msi compatibility mode“ wird nach der Installation angeboten, also die Ausführbarkeit von Windows-Programmen. Linux-Kennern wird klar sein, was das ist: Ja, hier wird Wine installiert – mit allen Fähigkeiten und Defiziten, das es auch sonst hat.
Eine Bewertung ist gespalten: Unbestritten wird sich ein Windows-Umsteiger erst mal zu Hause fühlen. Eine vergleichbare Windows-Mimikry gibt es nicht. Aber am Ende startet dann eben ein Gparted statt der Datenträgerverwaltung, ein Hardinfo statt dem Gerätemanager – und ein EXE-Programm eventuell nicht, weil es von Wine nicht unterstützt wird. Somit sind Umstiegsprobleme nur von der Oberfläche auf die Programmebene verschoben.
Nebenbei: Microsoft könnte gegen das seit 2016 existierende Windows FX zweifellos rechtlich vorgehen, wird das aber voraussichtlich weiter unterlassen, um sich keine Gegner in der falschen Liga zu schaffen. ■



Schnelles Arch-Derivat: Endeavour ist komfortabel zu installieren, fordert aber später Terminalkompetenz.



Minutiöse Mimikry: Windows FX scheut keine Mühe, den Windows-10-Desktop detailliert nachzubauen.

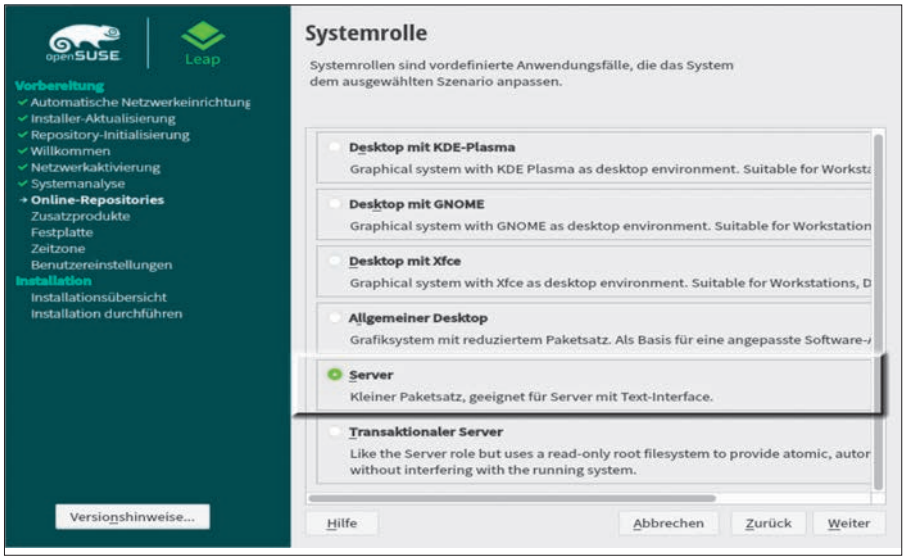
ALTERNATIVE DESKTOPDISTRIBUTIONEN

Name	Aktuell	Webseite	Download (MB)	Beschreibung
Bodhi Linux	6.0	*https://www.bodhilinux.com/*	850 bis 1400	schnell und klein: Speed-Desktop auf Ubuntu-Basis mit Moksha-Desktop
Endeavour-OS	2021.04.17	*https://endeavouros.com*	1900	schnelles Arch-nahes System mit Calamares-Installer
KDE Neon	2021-06-15	*https://neon.kde.org*	1700	Community-Ubuntu mit stets aktuellstem KDE Plasma
Ubuntu Studio	20.04	*https://ubuntustudio.org/*	3500	Ubuntu als Digital Audio Workstation
Windows FX	10.8	*www.windowsfx.org/*	4500	Windows 10 mit Ubuntu und Cinnamon/KDE nachgebaut

Serverdistributionen

Serverdienste sind Softwarekomponenten und somit auf jedem Linux-System bei Bedarf nachrüstbar. Trotzdem sind Distributionen, die auf den Servereinsatz spezialisiert sind, eine gute Wahl, wenn der Einsatzzweck eines Systems von vornherein feststeht.

VON HERMANN APFELBÖCK



Serverdistributionen haben oft einen besonders langen Supportzeitraum, unterscheiden sich aber nicht grundsätzlich von Desktop- und Allzwecksystemen. Sie fokussieren sich nur auf ihre Rolle: Am Desktop und an grafischer Software wird total oder graduell gespart, auf der anderen Seite sind Serverkomponenten wie SSH, Samba, Apache, PHP gleich standardmäßig an Bord.

Je nach Ausrichtung dient zur Verwaltung schlichtes SSH, ein eingebauter Webserver mit Browseroberfläche oder auch die spezielle Serversoftware (etwa Kodi, Volumio), dem das System dient. Der Einsatz einer Serverdistribution ist sinnvoll, wenn Sie wissen, dass ein Gerät – oft auch ein Platinenrechner – ausschließlich als Web-, Samba-, FTP- oder Streamingserver arbeiten soll. Welche Distribution sich am besten eignet, hängt vom Einsatzzweck, von der Hardware und vom Know-how des Systemverwalters ab.

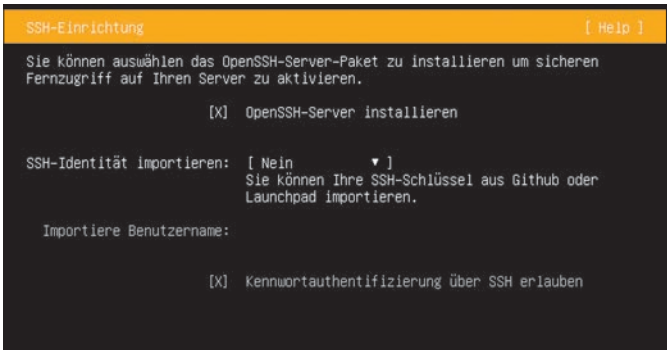
Minimale Serverinstallationen

Wer die Systemverwaltung per Kommandozeile beherrscht, kommt mit einem Headless-Server klar, der ausschließlich per SSH konfiguriert wird. Für leistungsschwache Hardware ist das ideal und falls der Server nur eine statische und einfache Konfiguration etwa als Samba- oder Webserver benötigt, hält sich auch der Aufwand in Grenzen. Solide Kandidaten für solche Server sind **Debian, Open Suse Leap** oder **Ubuntu Server**. Das Deployment unterscheidet sich fundamental: Während etwa Debian 10/11 und Open Suse Leap 15.3 einen allgemeinen Installer ausliefern, der dann während der Installation die Entscheidung über den Servereinsatz anbietet, trennt Ubuntu von vornherein Desktop- und Serverimages. Tendenziell benutzerfreundlicher ist die Methode von Debian und Open Suse. Open Suse hat außerdem für die spätere SSH-Fernwartung das großartige Yast2 an Bord, das bekanntlich auch als textbasierte Variante in der Konsole läuft.

Bei Ubuntu Server ist der Installer textbasiert, entspricht aber zunächst weitgehend dem grafischen Ubuntu-Installer. Dass es sich um eine Serverdistribution handelt, zeigt aber die frühe Abfrage zur Open-SSH-Komponente, die jeder Headless-Server unbedingt benötigt. Danach werden typische Dienste wie Nextcloud oder Minidlna als Snap-Container angeboten. Alles Weitere, selbst einen Samba-Server, muss sich der Administrator bei Bedarf nachträglich manuell nachinstallieren.

NAS-ähnliche Serversysteme

Wer seinen Server lieber in einer Weboberfläche mit dem Browser verwaltet, hat die Wahl zwischen mehreren NAS-ähnlichen Distributionen. Obwohl solche klickfreundliche Bedienung Einsteigern leichter fallen wird als die souveräne SSH-Fernwartung, ist auch die Orientierung in solchen Konfigurationsoberflächen kein Selbstläufer. Auf den Punkt gebracht, ist eine mono-



Ubuntu Server installiert ein minimales Basissystem ohne grafische Oberfläche. Die SSH-Serverkomponente wird explizit abgefragt.

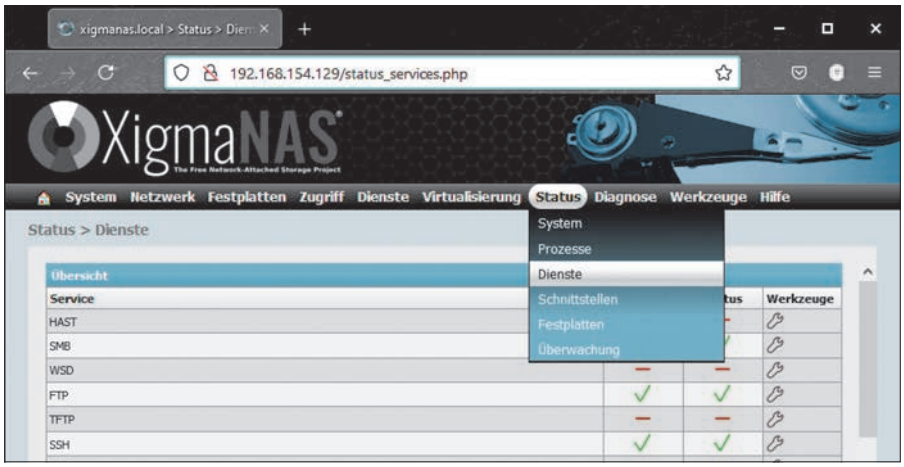
funktionale Rolle etwa als Samba-Homeserver, die obendrein wenig Benutzerkonten erfordert, per SSH wahrscheinlich schneller eingerichtet als in der Weboberfläche eines NAS-Systems.

Die Vorteile dieser Distributionen wachsen aber proportional mit den Ansprüchen: Wenn ein Gerät mehrere/viele Dienste für mehrere/viele Konten anbieten soll, ist ein NAS-System erste Wahl.

NAS-Distributionen mit moderaten Hardwareansprüchen sind Rockstor, Xigma NAS und Open Media Vault. Das an sich vielversprechende und schicke Rockstor stellen wir vorerst in die zweite Reihe: Es nutzt als Systembasis das Serversystem Cent-OS. Nach dem Aus von Cent-OS (siehe Kasten) muss sich Rockstor nach einer neuen Basis umsehen.

Xigma NAS dürfte jedem Linux-Nutzer geläufig sein, sobald man seine Herkunft klärt: Die Free-BSD-basierte Serverdistribution war bis 2018 unter dem Namen „NAS-4Free“ bekannt. Wie für NAS-Systeme typisch, wird das System nicht auf Festplatte installiert, da alle großen Datenträger für Medien und Benutzerdateien reserviert bleiben. Ziel ist vielmehr ein USB-Stick mit etwa acht GB Kapazität – mehr ist eigentlich Verschwendung, bringt aber andererseits meist schnellere Leseleistung. Nach der Installation ist das System „headless“ über die IP-Adresse erreichbar, ein SSH-Server läuft aber standardmäßig ebenfalls. Der voreingestellte Log-in-Standard für die Weboberfläche ist „admin“ mit dem Passwort „xigmanas“. Die wichtigsten und anspruchsvollsten Menüpunkte sind „Festplatten“ (Einrichten der Datenträger mit Mountpunkt), „Zugriff“ (Einrichten der Benutzer) und „Dienste“ (Aktivieren und Konfigurieren von zahlreichen Serverdiensten wie Samba, SSH, NFS, FTP, UPnP).

Open Media Vault (OMV) ist der vermutlich ideale NAS-Kandidat für kleine Homeserver und Platinenrechner. Mit dem unverwüstlichen und nachhaltigen Debian als Basis hat OMV geringe Ansprüche an die Hardware. Ein GB RAM und vier GB auf dem USB-Datenträger sind die bescheidenen Mindestvoraussetzungen. Eigene Installationsmedien gibt es allerdings nur noch für PCs und Notebooks (64 Bit), während sich OMV auf Platinen wie Raspberry Pi nur noch nachträglich als Software installieren lässt – das Basissystem (hier Raspberry-Pi-OS) muss also bereits vorliegen.



Xigma NAS (vormals „NAS4free“): NAS-Systeme sind über klickfreundliche Oberflächen im Browser zu verwalten. Das ist bequemer als das SSH-Terminal, aber durchaus anspruchsvoll.

Das laufende OMV-System steuern Sie NAS-typisch über seine Konfigurationsoberfläche im Browser. Voreingestellter Anmeldestandard ist hier „admin“ und Kennwort „openmediavault“. Nebenher ist ab Installation immer noch ein zusätzlicher SSH-Zugang aktiv („root“ mit Kennwort „openmediavault“). Die Weboberfläche lässt sich komplett deutschsprachig einstellen.

OMV mountet angeschlossene Datenträger (alle verbreiteten Dateisysteme Ext3, Ext4, FAT, NTFS, XFS, UFS) beim Systemstart automatisch ins Dateisystem und zeigt sie als physische Festplatten („Datenspeicher → Reale Festplatten“) sowie als logische Partitionen („Datenspeicher → Dateisysteme“). Wesentliche erste Konfigurationswege führen in der Regel zu den Netzdiensten („Dienste“). So muss etwa für plattformunabhängige Netzfreigaben „SMB/CIFS“ (Samba) aktiviert werden. Mit aktiviertem Samba kann dann im Register „Freigaben“ ein Datenträger oder Ordner freigegeben werden.

Die Systemkonten richten Sie unter „Zugriffskontrolle → Benutzer“ ein.

Nethserver mit Groupware

Eine Distribution, die über NAS-Dienste deutlich hinausführt, ist der auf Cent-OS basierende **Nethserver.** Es handelt sich um eine umfassende, deutsch lokalisierte Zusammenstellung mit allen Serverdiensten, mit Konfigurationsoberfläche und Groupwarekomponenten. Nethserver kann daher als Mail-, Datenbank-, Druck-, FTP-, Samba-, SSH-, LDAP- und Groupwareserver dienen (Kalender, Kontakte, Adressen). Diese und weitere nachladbare Dienste sind im „Software-Center“ zusammengefasst. Wenn die integrierten Groupwarefunktionen nicht ausreichen oder nicht gefallen, kann Nethserver über das „Software-Center“ auch noch eine zusätzliche Nextcloud einbinden. Aktuelle Updates installieren Sie ebenfalls über das „Software-Center“.

DAS AUS FÜR CENT-OS

Das langbewährte Serversystem Cent-OS ist ein Klon von Red Hat Enterprise Linux (RHEL). Das für Ende 2021 angekündigte Aus ist nicht nur an sich ein großer Verlust, sondern bringt auch eine Reihe weiterer Serverdistributionen in Verlegenheit, die bisher auf Cent-OS basieren. Neben den in der Tabelle genannten NAS-ähnlichen Systemen Rockstor und Nethserver müssen sich auch noch Blue Onyx, Baruwa Enterprise und SME Server nach einer neuen Basis umsehen. Erklärter Nachfolger von Cent-OS ist Alma Linux, als weiterer Red-Hat-Klon kommt aber auch noch Scientific Linux in Betracht.

Es ist davon auszugehen, dass die genannten Serversysteme mit neuer Basis weiterhin angeboten werden. Trotzdem entstehen im Dunstkreis von Cent-OS quantitative wie qualitative Fragezeichen für die Zukunft.

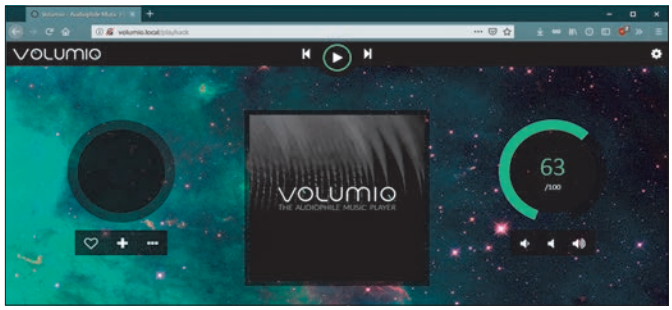
Libre Elec mit Kodi für zahlreiche Plattformen und Platinen: Der USB-SD Creator macht Auswahl, Download und Schreiben auf USB-Stick sehr einfach.

Da die Zukunft aller Cent-OS-Derivate wie Nethserver durchaus ungewiss ist (siehe Kasten), nennen wir an dieser Stelle nur die wichtigsten Merkmale dieser Serverdistribution.

Libre Elec: Das Mediencenter

Für das Mediencenter Kodi gibt es mehrere Linux-Distributionen, um die Software auf einem unabhängigen System zu starten. Eine schlanke Variante für zahlreiche Platinenrechner, aber auch für x86-PCs, ist Libre Elec, das unter *https://libreelec.tv* ein kleines USB-SD-Creator-Tool für alle Plattformen anbietet. Das Tool holt das gewünschte Installerimage aus dem Netz und schreibt es auf USB oder SD-Karte. Nach dem Booten dieses Images kopiert der Installer das System auf einen zweiten, endgültigen USB-Stick. Eine Installation auf interne Festplatten ist nicht vorgesehen. Diese sollen vielmehr die Film- und Musikmedien anbieten.

Kodi arbeitet bekanntlich sowohl als Abspielstation als auch als Samba- und UPnP-Server, auf den andere Netzwerkgeräte zugreifen können, sofern diese Serverdienste unter „Einstellungen → Dienste“ aktiviert werden.



Hübsche und intuitiv bedienbare Musikstation: Volumio ist am Gerät selbst und übers Netzwerk genau identisch zu bedienen.

Volumio: Die Soundstation

Volumio ist eine Musikstation, kein Musikserver. Das heißt, es spielt auf seinem lokalen Gerät die Musik ab, liefert aber keine Medien an andere Geräte. Jedoch ist es über das Netzwerk von jedem Smartphone, Tablet, PC zu bedienen. Mehr als ein Browser ist nicht nötig, um die Musikstation über die Adresse *http://volumio.local* (oder mit IPv4-Adresse) zu steuern. Mit identischer Oberfläche kann es auch direkt am Gerät konfiguriert und bedient werden. Volumio ist für Raspberry Pi, Tinkerboard und x86/x64-Architektur verfügbar. Letzteres macht es auch für ungenutzte Altgeräte interessant (Notebook, PC), hier allerdings nur mit brauchbarem Soundchip. Wer nicht eine Hardware monofunktional zur Soundstation machen will, kann Volumio auch mobil auf USB-Festplatte installieren (inklusive Musiksammlung).

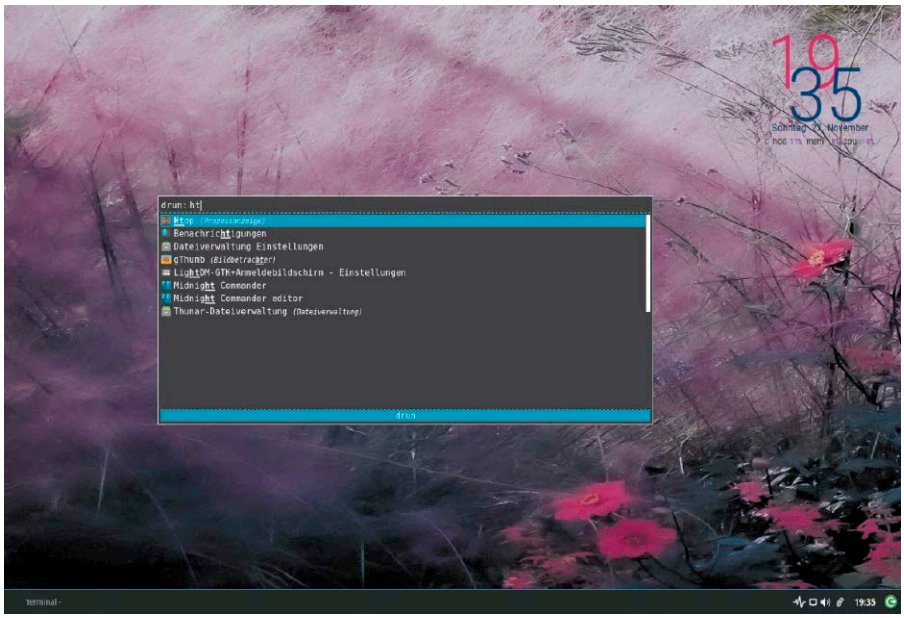
Die Oberfläche ist einfach und übersichtlich: Das Zahnrad-Control rechts oben führt zu den System- und Basiseinstellungen, bietet dort auch die Option „Herunterfahren“ und unter „System“ eine Installation auf Festplatte. Der Punkt „Meine Musik“ verwaltet die internen Laufwerke oder Netzfreigaben der Musikquellen. Auswahl und Abspielen der Musik erfolgt mit den drei großen Schaltflächen am unteren Bildschirmrand – „Durchsuchen“, „Wiedergabe“ und „Warteschlange“. Volumio verwaltet und präsentiert auch große Musikbibliotheken performant und ästhetisch überzeugend. ■

SPEZIALISIERTE SERVERDISTRIBUTIONEN

Name	Aktuell	Webadresse	Download (MB)	Beschreibung	Support
Alma Linux	8.4	*https://almalinux.org/*	ab 1800	Nachfolger für Cent-OS, Klon von Red Hat Enterprise Linux (RHEL)	8 Jahre
Cent-OS 8	8	*www.centos.org*	1000	Klon von Red Hat Enterprise Linux (RHEL), wird Ende 2021 eingestellt	–
Debian 10	10/11	*www.debian.org*	330	solider Server mit konservativen Paketen	5 Jahre
Fedora 34 Server	34	*https://getfedora.org/de/server*	ab 600	Server mit aktuellen Paketen, aber kurzem Supportzeitraum	1 Jahr
Libre Elec 9.2	9.2	*https://libreelec.tv/*	ab 130	reduziertes Basissystem für das Kodi-Mediencenter	manuell
Nethserver 7.9	7.9	*www.nethserver.org*	1100	Serverdistribution mit Web-Administrationsoberfläche (Basis: Cent-OS)	–
Open Media Vault 5.5	5.5	*www.openmediavault.org*	600	NAS-System mit Web-Administrationsoberfläche (Basis: Debian)	5 Jahre
Open Suse Leap 15.3	15.3	*hhtps://get.opensuse.org/leap*	ab 150	allgemeiner Installer mit Benutzerentscheidung über Serverrolle (oder Desktop)	3 Jahre
Raspberry-Pi-OS	2021-05-07	*www.raspberrypi.org/software/*	ab 440	Standardsystem des Rasberry Pi (Basis: Debian)	5 Jahre
Rockstor 3.9	3.9	*http://rockstor.com*	830	NAS-System mit Administrationsoberfläche und Dateisystem BTRFS (Basis: Cent-OS)	–
Ubuntu Server 20.04	20.04	*www.ubuntu.com/download/server*	1,1	solider minimaler Server mit SSH und optionalen Serverdiensten als Snap	5 Jahre
Volumio 2.8	2.8	*https://volumio.org/*	400–700	Musikstation für x86, Raspberry, Tinkerboard (Basis: Debian)	manuell
Xigma NAS 12 („NAS4free“)	12	*https://xigmanas.com/*	580	Serverdistribution mit Web-Administrationsoberfläche (Basis: FreeBSD)	manuell

Schnelles Linux auf USB

Zweitsysteme auf USB eignen sich als mobile Allzwecksysteme, als sichere Surfsysteme oder als Reparatur- oder Backup-Dienstleister. Für die erstgenannten Einsatzgebiete ist Geschwindigkeit Pflicht, aber auch generell darf es gerne schnell gehen.



VON HERMANN APFELBÖCK

Gesucht wird das schnellste und beste Linux auf USB als Allzweck-Zweitsystem. Was wir in diesem Beitrag empfehlen werden, sind dann allerdings nicht die typischen Minimalisten oder Live-Spezialisten, die sich als Kandidaten scheinbar aufdrängen. Denn das Ergebnis sollte mehrheitstauglich und halbwegs komfortabel ausfallen – und das wirft diverse typische Mobil-Spezialisten aus dem Rennen.

Zur Info: Alle aufgeführten USB-Bootzeiten wurden mit einem 64-GB-Stick Sandisk Ultra 3.20 gemessen, allerdings auf einem älteren PC mit USB 3.0 (Gen1). Die Leistung kann auf ganz moderner Hardware besser ausfallen als hier gemessen, schlechter nur mit USB 2.0.

Aussortiert: Spezialsysteme für Bastler

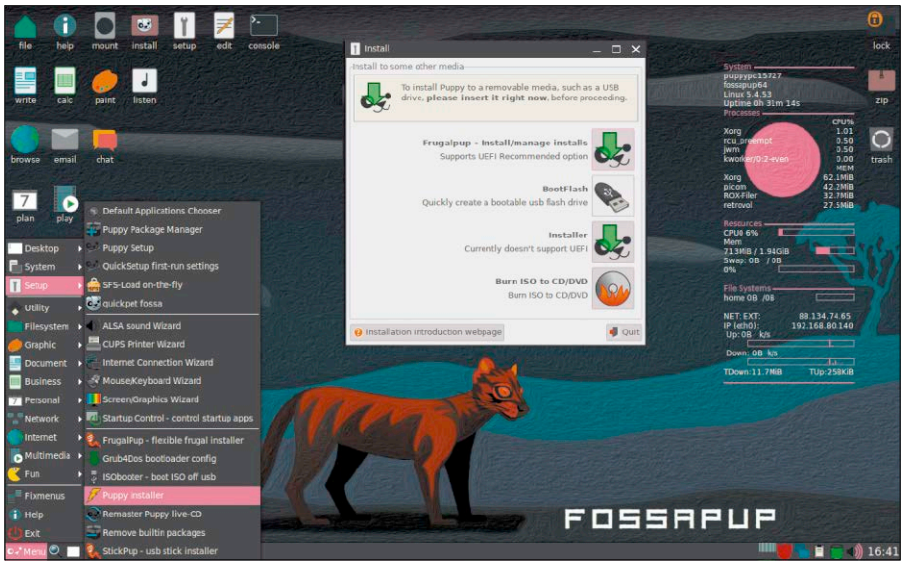
Es gibt einige bekannte Minimalisten, die sich auf den Livebetrieb als Zweit- oder Servicesystem spezialisiert haben. Ursprüngliche Zielsetzung von Live-Pionieren wie Knoppix und Puppy war allerdings eine Lösung für eine extreme Mangelsituation, die eigentlich aus der Zeit gefallen ist: Das System sollte mit CD-Kapazität zurechtkommen, die Nur-Lesbarkeit dieses Mediums muss mit virtuellen Dateisystemen im RAM kompensiert werden und dabei noch mit wenig RAM auf alter Hardware auskommen. Das sind Mangelbedingungen, die auf moderner Hardware und auf heutigen USB-Sticks eigentlich hinfällig sind. Minimalisten wie Porteus, Slax, Slitaz, Sparky, Tiny Core, Trisquel Mini oder Watt-OS setzen diese Techniken dennoch im Sinne einer Spezialisierung fort.

Aus diesem Grund sortieren wir außer Knoppix alle oben genannten Kandidaten aus, obwohl ein Slax ein USB-Schnellbooter ist (10 bis 12 Sekunden) und ein Puppy Linux wieselflink im Alltagsbetrieb arbeitet. Es gibt aber noch weitere Gründe: Slitaz (*www.slitaz.org/de*) und Tiny Core (*http://tinycorelinux.net*) sind Reduktionsrekorde ohne echte Alltagsrelevanz. Slax (*www.slax.org*), Puppy Linux (*http://distro.ibiblio.org/puppylinux*) und Porteus (*http://porteus.org*) sind allenfalls für Bastler relevant: Allein schon, deren nicht-hybride ISO-Images (nur auf CD/DVD-bootfähig) auf USB zu befördern, nötigt zu manuellen Schritten (Slax) oder zum Umweg über eine CD oder eine virtuelle Maschine (Puppy, Porteus). Weiterführende Anpassungen des Livesystems sind entweder kompliziert (Slax, Porteus) oder inhaltlich unbefriedigend: Die Puppy-Systeme bieten für ihr eigenes Paketformat wenig Software und diese praktisch nur englischsprachig.

Bei etlichen weiteren Minimalisten wie Sparky (*https://sparkylinux.org*), Trisquel (*https://trisquel.info*) oder Watt-OS (*http://planetwatt.com*) ergeben sich keine offensichtlichen Vorteile gegenüber einem Debian oder Derivaten wie MX Linux und Q4-OS.

Livesysteme: Ubuntu oder Knoppix?

Ein pures, unveränderliches Livesystem taugt nicht als Zweitsystem. Erst eine Persistenzoption für eigene Dateien, Anpassun-



Klein, schnell und eingebaute Persistenz: Puppy-Livesysteme können technisch überzeugen, sind aber nicht pflegeleicht und lassen (deutschsprachige) Software vermissen.

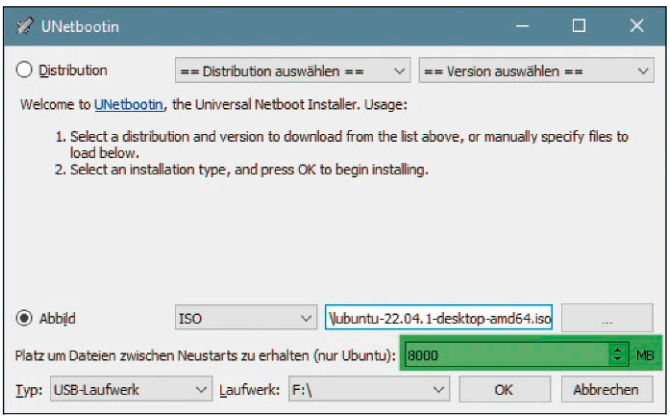
gen und Nachinstallationen macht das Zweitsystem attraktiv. Die Auswahl solcher anpassungsfähiger Livesysteme wäre trotz der oben aussortierten Live-Spezialisten enorm, weil jedes Ubuntu-basierte ISO-Installationsmedium über das Tool Unetbootin (auf Heft-DVD) mit Persistenz auf USB geschrieben werden kann. Sie müssen dazu im Unetbootin-Fenster neben der Option „Platz um Dateien zwischen Neustart zu erhalten" nur eine MB-Angabe eintragen. 2000 bis 8000 MB sind je nach Kapazität des USB-Sticks sinnvolle bis großzügige Werte. Unetbootin meldet dann beim Aktionsschritt 3 („Installiere Startverwalter") zusätzlich die Aktion „Erstellen der Persistenz".

Optimal sind Live-Ubuntus allerdings nicht, weil sie aufgrund eines standardisierten Checks des Livemediums nicht sonderlich schnell booten. 40 Sekunden sind auch bei kleinem Lubuntu oder Xubuntu für jeden Start einzurechnen. Aus Leistungsgründen sind Ubuntu-Distributionen daher eher ein Fall für ordentliche Installation auf USB. Noch ein zweiter Grund spricht gegen Live-Ubuntu auf USB: Es gibt dabei keine Möglichkeit, das USB-Medium durch Verschlüsselung zu schützen.

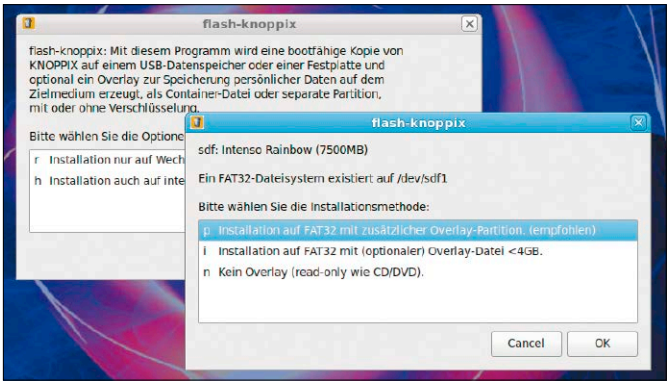
Das Debian-basierte Knoppix ist der Live-Klassiker schlechthin und ein „No-Brainer". Wem der relativ einfache LXDE-Desktop nicht zu schlicht ist, kann mit Knoppix definitiv nichts falsch machen. Deutschsprachig, mit exzellenter Hardwareerkennung, opulenter Softwareausstattung und anspruchslosem LXDE-Desktop ist Knoppix erste Wahl für ein Zweit- oder Surfsystem. Mit USB-Bootzeiten von 20 Sekunden zum eingabebereiten Desktop gehört Knoppix zu den schnellen Livestartern, wenngleich er mit Spezialisten wie Slax oder Porteus nicht ganz mithalten kann. Im laufenden Betrieb und beim Start von Programmen ist die Knoppix-Leistung durchschnittlich, aber jederzeit agil. Knoppix hat aber zusätzlich den unschätzbaren Vorteil, dass weder der LXDE-Desktop viel Eingewöhnung fordert noch Software nachinstalliert werden muss. Knoppix hat wirklich alles an Software und Tools am Start.

Der Download von einem der Mirrorserver unter *www.knopper.net/knoppix-mirrors* beträgt für die aktuellste Version 9.1 circa 4,4 GB. Achten Sie in der Liste der ISO-Dateien auf „-DE" im Dateinamen („Knoppix_V9.1DVD-2021-01-25-DE.iso"). Das hybride ISO-Abbild kann mit den üblichen Tools auf USB-Stick kopiert werden.

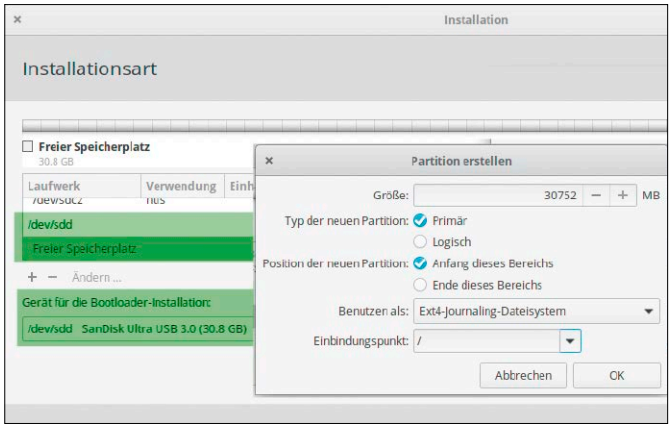
Für häufige Nutzung ist die Persistenzoption unentbehrlich, die bei Knoppix „Overlay-Partition" heißt. Dazu müssen Sie aber aus einem bereits laufenden Knoppix ein zweites erstellen. Das maßgebliche Tool „Flash Knoppix" finden Sie unter „Knoppix → Knoppix auf Flash kopieren". Nach Auswahl des Zieldatenträgers folgt die „Installation auf FAT32 mit zusätzlicher Overlay-Partition". Die Abfrage zur Größe der Overlaypartition können Sie auf einem USB-Stick einfach mit „OK" übernehmen. Dann erhält die Overlaypartition auf dem Stick die komplette Restkapazität, die das eigentliche Knoppix-System übriglässt. Eine letzte Frage betrifft den optionalen Verschlüsselungsschutz der Overlaypartiti-



Unetbootin und Ubuntu live mit Persistenz: Das ist besser als ein pures Livesystem, aber kaum optimal. Kleine Ubuntus sind regulär auf USB-Stick installiert schneller und flexibler.



Live-Klassiker Knoppix mit Persistenz: Die Overlay-Partition ermöglicht dem Livesystem Desktop-Anpassungen, Installationen und Deinstallationen.



USB-Installationen: Systempartition und Bootloader müssen als Ziel den USB-Stick erhalten. Mehr ist bei der Partitionierung nicht nötig, wenn die Installation im Bios-Modus erfolgt.

on. Es handelt sich um die einzige Möglichkeit, einen USB-Stick mit Knoppix systemweit zu schützen, weil Knoppix als Livesystem keine Benutzerverwaltung hat. Die Verschlüsselung schützt neben dem Knoppix-System auch die persönlichen Daten auf dem USB-Stick.

Mit Overlaypersistenz erlaubt Knoppix Anpassungen aller Art, auch Nachinstallationen und Entfernen überflüssiger Pakete. (De-)Installationen sind wahlweise über apt im Terminal zu realisieren oder auch über Synaptic.

USB-Installation: Schnelle Kandidaten

Jedes Linux lässt sich regulär auf USB-Stick installieren. Ein installiertes mobiles Linux auf USB oder SD-Karte ist genauso updatefähig, ausbau- und anpassungsfähig wie auf Festplatte. Anders als beim Livesystem (mit oder ohne Persistenz) ist hier ein USB-Stick mit mindestens 32 GB Kapazität zu empfehlen, besser größer.

Die Installation geschieht typischerweise im Livesystem, dessen ISO-Image Sie zunächst herunterladen, kopieren und dann im Bios-Modus starten. Bei der Partitionierung während der Installation müssen Sie dann den USB-Datenträger als Zielpartition für das System angeben, zweitens unbedingt auch als Zielort für den Bootloader. Die Vorgehensweise ist für die empfohlenen Systeme anschließend noch genauer beschrieben.

Bei der Wahl der Distribution gibt es keine prinzipiellen Beschränkungen. Aber im Sinne eines möglichst schnellen Bootvorgangs und einer agilen Systemnutzung gibt es besser und schlechter geeignete Distributionen.

Kleine Ubuntus: Im Gegensatz zum Livebetrieb booten auf USB installierte Ubuntus recht flott zum Desktop. Schnellster Starter ist das Ubuntu-basierte Bodhi Linux (*www.bodhilinux.com*), das in 13 Sekunden zum Desktop lädt. Bodhi ist auch im Betrieb und bei Programmstarts überragend schnell, lässt aber bequeme Konfigurationszentralen vermissen und hat einen gewöhnungsbedürftigen Moksha-Desktop. Unsere Ubuntu-Empfehlung ist daher das unkomplizierte Lubuntu, das – installiert auf USB 3.x – nach 21 Sekunden am Log-in ist.

Für die Lubuntu-Installation benötigen Sie das ISO-Image von *https://lubuntu.me/downloads/* (2,5 GB). Das hybride ISO-Abbild kann mit den üblichen Tools (Etcher, Gnome-Disks, USB-Imager et cetera) auf einen USB-Stick kopiert werden. Damit booten Sie einen Rechner, laden das Bios-Bootmenü (Esc, F8, F9, seltener F10, F11, F12) und dort den Stick im Bios-Modus (ohne „Uefi"). Das Livesystem bietet dann die Installation mit dem Tool Calamares an, die Sie auf einen zweiten und eigentlichen USB-Stick absolvieren. Der beim Setup wesentliche Punkt „Partitionen" muss also oben bei „Speichermedium" auf den USB-Stick verweisen. Über „Manuelle Partitionierung" löschen Sie dann eventuell vorhandene Partitionen des Sticks und erstellen auf dem nun „freien Platz" eine primäre Ext4-Partition mit Einhängepunkt „/". Die unscheinbare Option „Verschlüsseln" sorgt bei Bedarf für Vollverschlüsselung des Sticks. Zurück im Hauptdialog muss ganz unten die Option „Installiere Bootloader auf" unbedingt ebenfalls auf das USB-Laufwerk gesetzt werden, damit das USB-System später an jedem Rechner starten kann.

Hinweis: Andere Ubuntus wie Xubuntu oder Bodhi Linux verwenden einen anderen Installer (Ubiquity). Die Vorgehensweise unterscheidet sich dort deutlich, die prinzipielle Vorgehensweise ist aber entsprechend. Die Abbildung auf dieser Seite zeigt den einschlägigen Installer-Dialog.

Q4-OS ist mit Debian-Unterbau und Trinity-Desktop schnell und anspruchslos (Download unter *http://q4os.org*, auf Trinity-Variante achten!). Für einen reinen Livebetrieb ist es nicht ideal, weil es nach der Auswahl der deutschen Lokalisierung die nötigen Pakete stets erst aus dem Internet nachlädt und damit kaum unter einer Minute zu starten ist. Es ist aber ein idealer Kandidat für die reguläre Installation auf USB. Dazu muss das hybride Download-ISO erst auf einen USB-Stick kopiert und im Livesystem Q4-OS, das im Bios-Modus gestartet werden muss, auf einen zweiten und endgültigen USB-Stick installiert werden.

Die Installation erledigt hier ein eigener, aber Calamares-ähnlicher Installer, wobei unter „Software" am besten „Q4OS-Desktop" mit vollständiger Programmausstattung zu wählen ist. Unter „Partitionen" muss ganz oben unbedingt das richtige Speichermedium aktiviert werden, wobei Sie dann alles Vorhandene „Löschen" und mit „Erstellen" die Systempartition mit Einhängepunkt „/" anlegen. Eine Partitionsverschlüsselung mit Luks ist hier ebenfalls vorgesehen. Nach „OK" muss noch der Bootloader im Dialog ganz unten auf das USB-Laufwerk gesetzt werden.

Nach der Installation holen Sie die deutsche Lokalisierung nach, was das System selbst anbietet. Danach startet der „Desktop-Profiler", um die Softwareausstattung zu komplettieren.

Das installierte System startet auf USB-3.0-Stick in 15 Sekunden und belegt nach der Anmeldung für System und Desktop knapp 400 MB RAM. Der Desktop Trinity basiert auf dem eingestellten KDE 3 und wirkte lange Zeit reichlich retro. In den jüngsten Versionen (aktuell 4.10) hat sich die Oberfläche optisch gründlich modernisiert, und eingängig, übersichtlich sowie anpassungsfähig war sie schon immer. Die Arbeitsfläche ist eine klassische Dateiablage, das Menü ähnelt dem Stil älterer Windows-Versionen und die Systemleiste („Kontrollleiste") enthält mit Schnellstarter, Fensterliste und Indikatoren die typischen Elemente.

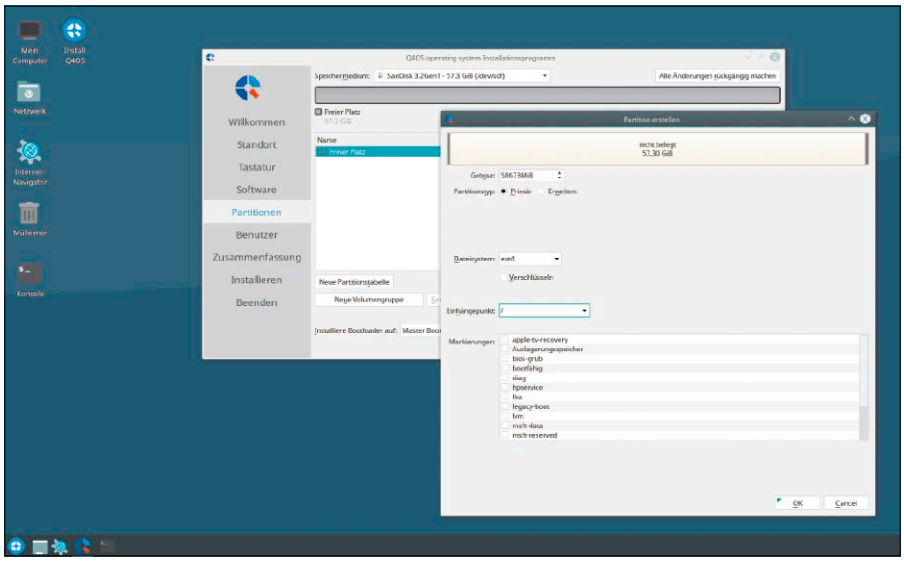
MX Linux: Diese Distribution (Download unter *https://mxlinux.org*) nutzt auf Debian-Basis entweder den klassischen XFCE-Desktop (1,7-GB-ISO) oder den besonders schlanken Fenstermanager Fluxbox (1,4-

GB-ISO), der sich lediglich einige XFCE-Anleihen wie den Xfce4-Appfinder leistet (als Menüersatz). Die Fluxbox-Variante ist für ein mobiles Zweitsystem eine schlanke Wahl, XFCE die komfortablere. Die eine oder andere englischsprachige Beschreibung oder Menübezeichnung muss man bei MX Linux aber in beiden Desktops in Kauf nehmen.

Auch für MX Linux muss zunächst das hybride Download-ISO auf einen USB-Stick kopiert werden. Mit dem Livesystem von MX Linux, das im Bios-Modus gestartet werden muss, wird es dann auf den zweiten und endgültigen USB-Stick installiert.

Das Setup verläuft einfach und linear, wenngleich ein paar Fragen mehr gestellt werden: Im Bootmenü des Livesystems wählen Sie zunächst mit F2 die Sprache „Deutsch“ und mit F3 die Zeitzone „Berlin“. Dann starten Sie den obersten Eintrag „MX-21.2“. Eventuelle Fragen nach der Grafikkarte quittieren Sie ohne Auswahl mit Eingabetaste, starten zum Desktop des Livesystems und klicken auf den Installer-Link am Desktop. Als „Art der Installation“ verwenden Sie „Normale Installation“ und wählen dann im Drop-down-Feld darunter sorgfältig den USB-Stick, der das Installationsziel ist. Beachten Sie darunter die Option „Verschlüsseln“, die System und Stick durch Luks-Datenträgerverschlüsselung schützt. Während der Installer dann bereits kopiert, werden die Daten für den Erstbenutzer, die Sprache und die Zeitzone, ein root-Kennwort, ein Computername sowie die Samba-Arbeitsgruppe abgefragt. Der Vorgang ist etwas umständlicher als bei Ubuntu & Co., aber letztlich einfacher, als diese Einstellungen später im laufenden System zu suchen.

Nach ordentlicher Installation auf USB 3.0 beträgt die Startzeit zur Desktopanmeldung etwa 18 Sekunden. Der RAM-Bedarf liegt unter 500 MB. Alle Programme, auch größere Brocken wie Browser oder LibreOffice-Komponenten, sind frappierend reaktionsschnell. Die Fluxbox-Variante von MX Linux ist tempomäßig mit Bodhi Linux vergleichbar, dabei aber deutlich pflegeleichter.



Q4-OS bei der USB-Installation: Die Distribution mit klassischem Trinity-Desktop hat sich optisch modernisiert und ist schneller und schlanker als jedes Ubuntu.

Systemoptimierung: Ausmisten und erweitern

Für ein ordentlich auf USB installiertes Linux-System gibt es nur eine nennenswerte Einschränkung: Installieren Sie besser keine proprietären Treiber, wenn das System auf unterschiedlicher Hardware funktionieren soll. Ansonsten haben Sie alle Möglichkeiten, Software zu installieren, Software zu entfernen sowie das System zu optimieren.

Software installieren und beseitigen: Alle hier empfohlenen Kandidaten verwenden das Debian-Paketformat und lassen sich über den apt-Paketmanager erweitern und entschlacken. Folglich können Sie in allen genannten Systemen in der üblichen Manier etwa mit

```
sudo apt install filezilla
```

Software ergänzen und Unnötiges mit *sudo apt remove […]* entsorgen.

Autostarts und Dienste: Um den Desktopstart und den Speicherbedarf zu optimieren, suchen Sie die „Startprogramme“ auf. Wenn eine solche Zentrale fehlt, hilft auch direkte Dateibearbeitung unter „/etc/xdg/autostart“ und „~/.config/autostart“. Komponenten, die Sie auf einem Mobilsystem nicht benötigen (Datensicherung, Blueman, Orca, Welcome …) deaktivieren Sie per Mausklick in der Zentrale oder durch Umbenennen auf Dateiebene.

Wer noch einen Schritt weiter gehen will, kann die gestarteten Dienste durchforsten:

```
sudo service --status-all
```

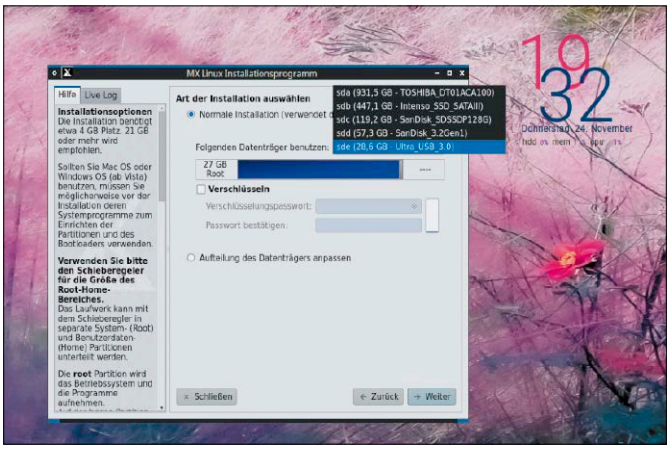
Dieser Befehl (statt systemctl) funktioniert sowohl unter systemd als auch ohne systemd – so etwa unter MX Linux. So sind die Dienste Cups (Drucken), Whoopsie (Fehlerreport), Apport (Fehlerprotokoll) oder Apparmor (Sicherheitserweiterung) auf einem Mobilsystem vermutlich entbehrlich. Einen Dienst stoppen Sie mit

```
sudo service whoopsie stop
```

und entfernen ihn später mit

```
sudo rm /etc/init.d/whoopsie
```

komplett, sofern er sich dauerhaft als überflüssig erweist. ■

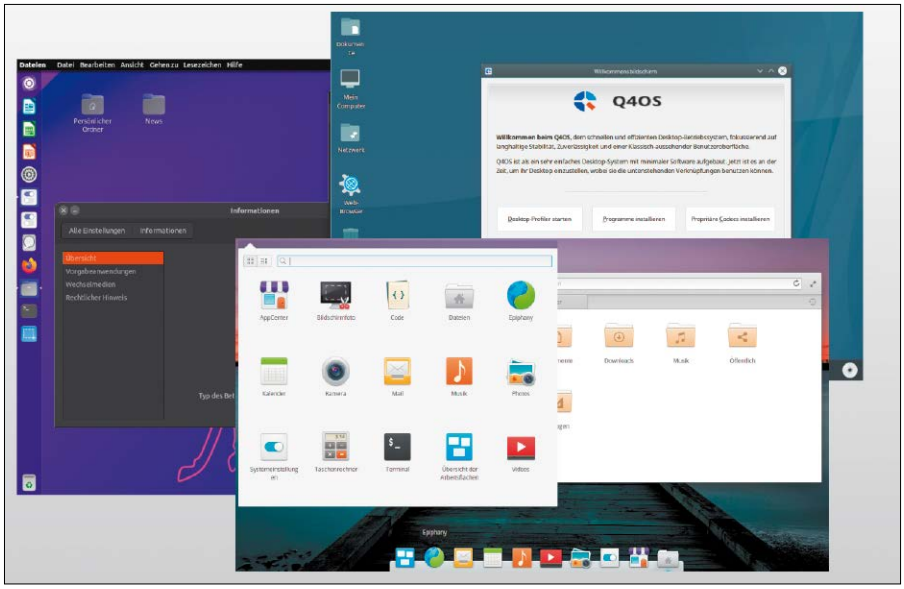


Unser Favorit bei der Installation auf USB: MX Linux mit Fluxbox garantiert einen überaus agilen Programmalltag auf USB-Stick.

Wahlpflicht Linux-Desktop

Wie viele Linux-Desktops gibt es insgesamt? Tatsächlich annähernd 30, wenn man auch eigenartige Exoten mitzählt. Dieser Wucher hat Vorteile, aber noch mehr Nachteile. Ein Nachteil aus Anwendersicht ist schlicht der nagende Zweifel, richtig zu wählen.

VON HERMANN APFELBÖCK



2023 ist der Linux-Desktop fragmentierter denn je. Neben den prominentesten Desktops KDE, Gnome, Cinnamon und XFCE stehen weitere namhafte Oberflächen wie Budgie, LXDE, LXQT, Mate, Moksha/E, Pantheon, Trinity, Unity. Und wer sich auf Exoten und Minimalisten einlassen will, kann es mit Fluxbox, Gnome-Flashback, Icewm oder Openbox versuchen. Die Desktops werden nicht weniger, weil Totgeglaubte wie Unity sich erneuern und Abspaltungen und Modernisierungen ihre Vorgänger nicht ersetzen, wie an den Beispielen LXQT (versus LXDE), Cinnamon und Budgie (versus Gnome) zu sehen ist.

Vielfalt bedeutet Auswahl, und wo Vielfalt funktional begründet ist, ist Auswahl willkommen. Die Wahl zwischen prinzipiell ähnlichen, im Detail aber doch wieder unterschiedlichen Produkten kann aber durchaus nerven. Das folgende Special zu Linux-Oberflächen (und deren Optimierung) wird daher kein Loblied auf die Desktop-Vielfalt, sondern ein Ratgeber mit einer bewusst engen Auswahl der Kandidaten. Es handelt sich nach unserer Einschätzung um die Desktops mit den besten Bedienkonzepten und Konfigurationszentralen. Außerdem sind anspruchslose Kandidaten dabei, die sich für ältere oder schwächere Hardware anbieten.

Linux-Desktops: Ein Überblick

Gnome, KDE, XFCE und **Cinnamon** sind die bevorzugten Desktopoberflächen vieler Linux-Nutzer und erhalten nachfolgend ihre eigenen Vorstellungen und Optimierungstipps. Daneben gibt es weniger bekannte Desktops wie beispielsweise Mate, der eine Mischung zwischen Gnome und Cinnamon darstellt und durch das offizielle Ubuntu Mate gewisse Verbreitung gefunden hat. Auch Mate erhält eine eigene Besprechung.

LXQT hat mit Lubuntu ebenfalls eine starke Distribution im Rücken, hat aber gewissermaßen seinen ursprünglichen Fokus verloren: Er ist und wird kein „großer" Desktop, wiegt aber trotzdem kaum noch weniger als ein XFCE oder Mate.

Der **Pantheon-Desktop** ist praktisch nur über seine halbkommerzielle Vorzeigedistribution Elementary OS bequem zu erreichen (außerdem noch über ein PPA). Mit seiner von Mac-OS inspirierten Oberfläche ist Pantheon ästhetisch ansprechend, bietet andererseits aber kaum Anpassungsoptionen. Fenster lassen sich standardmäßig nur per Klick auf das zugehörige Icon im Dock minimieren. In den Fensterleisten gibt es nur eine Schaltfläche für die Darstellung im Vollbild.

Einen ähnlichen Ansatz, Gnome konservativer, aber ästhetisch ansprechend umzuformen, verfolgt der optisch ebenfalls überzeugende **Budgie-Desktop:** Der ist um Einiges flexibler als Pantheon, nutzt aber keine intuitiven Kontextoptionen, sondern Konfigurationszentralen, an die man sich erst gewöhnen muss.

Der **Moksha-Desktop** ist praktisch nur in Bodhi Linux anzutreffen (theoretisch gibt es noch eine abgelegene PPA-Quelle). Trotz klassischem Konzept mit Startmenü und Taskleiste ist diese Oberfläche mehr als

eigenwillig und individuelle Anpassungen sind gewöhnungsbedürftig bis kompliziert. Dank seiner Anspruchslosigkeit und Schnelligkeit sollte man Moksha und die Distribution Bodhi aber immer auf dem Radar behalten.

In der Liga „Nicht mehr Desktop als nötig", die vor allem für Altgeräte und für schwache Platinenrechner optimal ist, konkurrieren diverse und zum Teil interessante Kandidaten: **Openbox** verdient den Namen „Desktop" kaum, kann aber als Programmstarter und Fenstermanager ausreichen. Anpassungen der schlichten Oberfläche sind möglich, führen aber schnell in manuelles Editieren von Konfigurationsdateien. Den ebenfalls minimalen Icewm werden Sie bei keiner Distribution als Standarddesktop antreffen, jedoch ist dieser Fenstermanager in einigen Distributionen nach wie vor als Not- und Basisdesktop zu wählen (etwa bei Open Suse als „Allgemeiner Desktop"). Deutlich hübscher fällt das funktionale **Fluxbox** aus, das passenderweise beim Oldie-Spezialisten Antix als grafische Shell dient, weil es kaum Hardwareressourcen fordert.

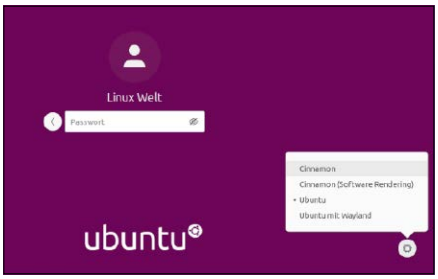
Wer auf Platinenrechnern oder Oldies auf solche Minimalisten angewiesen ist, ist wahrscheinlich am besten bei **Trinity** aufgehoben. Diese Abspaltung des längst verblichenen KDE3 bietet bei aller Anspruchslosigkeit einen zwar altmodischen, aber ansehnlichen und erstaunlich vielseitigen Desktop. Trinity ist aber praktisch nur über seine Vorzeige-Distribution Q4-OS zu beziehen, sonst nur über ein externes PPA.

Aus der Kategorie der Minimalisten berücksichtigt dieses Special nur den **LXDE-Desktop.** Als Standard ist er nur noch im Livesystem Knoppix anzutreffen, aber weiterhin eine Option bei vielen Distributionen wie etwa Debian oder Fedora. LXDE ist einfach und unkompliziert und hat gegenüber dem vielleicht sogar besseren Trinity einen entscheidenden Vorteil: Der Desktop ist in allen Paketquellen erreichbar und bei Bedarf auf jedem System leicht nachzuinstallieren.

Desktop nachinstallieren?

Keine Frage: Die solideste Desktopwahl ist die Wahl der passenden Distribution inklusive Standardoberfläche – etwa ein Kubuntu mit KDE oder ein Linux Mint mit Cinnamon. Nichtsdestotrotz ist ein einmal installierter Desktop-Linux keine Einbahnstraße: Für alle namhaften Linux-Desktops gibt es Metapakete, die sich auch später nachinstallieren lassen. Der zweite (oder dritte) alternative Desktop ist dann am Anmeldefenster nach Bedarf auszuwählen. Ohne explizite Wahl startet jeweils der zuletzt genutzte Desktop. Einige Regeln und Einschränkungen sollte man dabei aber beherzigen:

• Den primären Standarddesktop sollte man nie entfernen, selbst wenn ein sekundärer Desktop einwandfrei läuft.



Nachinstallierter Desktop: Die Anmeldung erlaubt die Auswahl eines sekundären Desktops. Der bleibt dann Standard bis zur nächsten manuellen Auswahl.

• Die Nachinstallation großer Desktops wie Gnome und KDE ist umso umfangreicher und unkalkulierbarer, je weniger Verwandtschaft mit dem bereits vorhandenen Desktop besteht. Eine KDE-Installation neben einem Gnome oder einem Gnome ähnlichen Desktop wie Budgie, Unity (oder umgekehrt ein Gnome neben einem bestehenden KDE) ist ein erheblicher Eingriff und funktioniert nicht überall konfliktfrei.

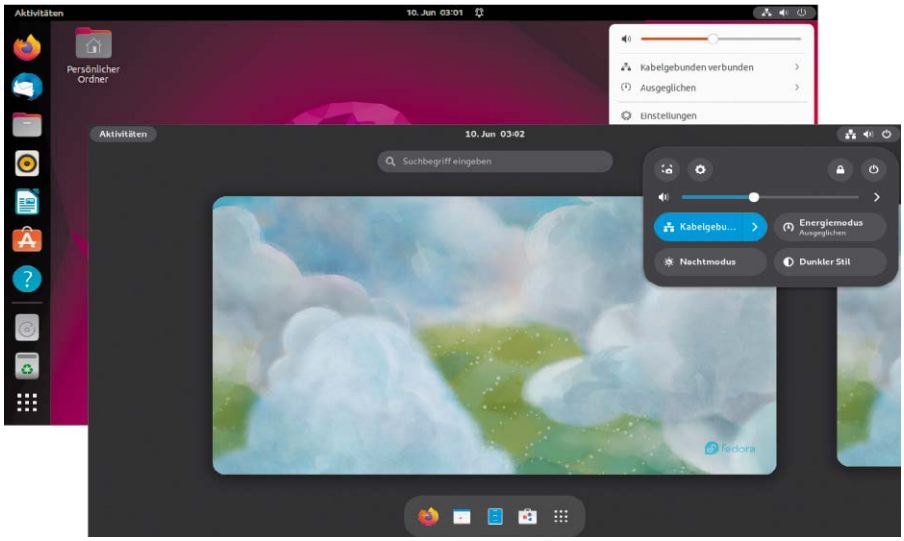
• Um tatsächlich nur die Desktop-Bedienoberfläche zu installieren, sollte eine Recherche mit Synaptic, *apt search* oder ähnlich vorausgehen. Die Tabelle auf dieser Seite zeigt Paketnamen (für Ubuntu-Paketquellen), die sich auf die Oberflächen und deren Konfigurationswerkzeuge beschränken. Metapakete, die eine ganze Desktopumgebung einschließlich Anwendungssoftware mitbringen, bringen nur Ballast und unnötiges Konfliktpotenzial. ■

WICHTIGE LINUX-DESKTOPS

	Artikel	Stammdesktop für	Hardware-anspruch	Flexibilität	Bemerkungen	Paketname
Budgie	–	Ubuntu Budgie / Solus-OS	relativ hoch	mittel	gezähmter Gnome mit klassischer Bedienung	budgie-desktop
Cinnamon	S. 46	Linux Mint / Ubuntu Cinnamon	mittel	hoch	klassische Bedienung, anpassungsfreundlich	cinnamon-core
Fluxbox	–	Antix / MX Linux	minimal	gering	sehr einfach, funktional, altmodische Optik	fluxbox
Gnome	S. 38	Ubuntu / Fedora / Tails	hoch	gering	elegant, einfach, aber gewöhnungsbedürftig	gnome-shell
Gnome-Flashback	–	[nachinstallierbar]	hoch	gering	klassische Retro-Bedienung für Gnome 3	gnome-session-flashback
Icewm	–	[optional – etwa bei Open Suse]	minimal	gering	spartanischer Minimaldesktop	icewm
KDE	S. 42	Kubuntu / KDE Neon / Open Suse	moderat bis hoch	exzellent	klassisches Konzept, komplexe Anpassung	kde-plasma-desktop
LXDE	S. 54	Knoppix	gering	mittel	sehr einfach und funktional, altmodische Optik	lxde-core
LXQT	–	Lubuntu	mittel	mittel	einfach, klassisch, funktional	lxqt-core
Mate	S. 52	Ubuntu Mate	mittel	hoch	klassische Bedienung und flexible Anpassung	mate-core
Moksha (E19)	–	Bodhi Linux	gering	mittel	exotisch bis konfus, aber sparsam und sehr schnell	enlightenment (PPA)
Openbox	–	Bunsenlabs	sehr gering	mittel	minimalistisch, Anpassungen anspruchsvoll	openbox
Pantheon	–	Elementary OS	mittel	gering	elegant, einfach, aber hermetisch (Mac-like)	elementary-desktop (PPA)
Trinity	–	Q4-OS	gering	hoch	klassisch, funktional, altmodische Optik	tde-trinity (PPA)
Unity	–	Ubuntu Unity	relativ hoch	gering	sehr einfach, intuitiv, aber reduziert	ubuntu-unity-desktop
XFCE	S. 49	Xubuntu / Voyager-OS	mittel	hoch	klassische Bedienung, ausgereift, etwas altmodisch	xfce4

Der schlichte Desktop Gnome

Gnome eignet sich für Nutzer, die einen einfach bedienbaren Desktop bevorzugen. Standardmäßig gibt es nur wenige Optionen für individuelle Anpassungen, was man jedoch für mehr Komfort durch Erweiterungen ändern kann.



Zweimal Gnome: Je nach Konfiguration sieht der Gnome-Desktop unterschiedlich aus. Ubuntu (links) blendet das Dash dauerhaft ein, Fedora zeigt es nur nach Klick auf „Aktivitäten“.

VON THORSTEN EGGELING

Gnome (*www.gnome.org*) gehört zu den Desktopumgebungen mit langer und wechselvoller Geschichte seit 1997. Zwischendurch gab es Stagnation, Brüche und Verzögerungen, die Gnome nicht immer ein gutes Image bescherten. Inzwischen ist Gnome der Standarddesktop bei einigen Distributionen und auch häufig als Variante („Flavour“) verfügbar.

Die aktuelle Version ist Gnome 44, LTS-Distributionen nutzen in der Regel etwas ältere Versionen. Der Ressourcenbedarf von Gnome ist höher als bei KDE Plasma oder Cinnamon, deutlich höher als etwa bei XFCE oder LXDE. Typisch ist ein RAM-Bedarf von einem Gigabyte. An CPU und Grafikchip werden keine hohen Ansprüche gestellt, ein Dualcore-Prozessor ab zwei GHz Taktfrequenz ist aber empfehlenswert.

Distributionen und Pakete

Gnome ist der Standarddesktop etwa von Ubuntu und Fedora und damit weit verbreitet. Für viele andere Distributionen, beispielsweise Debian, Manjaro Linux oder Open Suse, ist Gnome ebenfalls verfügbar. Wer sich für den Gnome-Desktop entscheidet, sollte bevorzugt ein Installationsmedium wählen, das diesen bereits enthält. Die Nachinstallation ist möglich, kann aber unerwünschte Nebenwirkungen haben.

Bei Linux Mint mit Cinnamon Desktop beispielsweise lässt sich die Gnome-Desktopumgebung im Terminal mit

```
sudo apt update && sudo apt upgrade
sudo apt install gnome
```

installieren. Debian-Nutzer können ebenfalls das Metapaket „gnome“ verwenden.

Die typischen Gnome-Anwendungen wie Texteditor (Gedit), Dateimanager (Nautilus) und Videos (Totem) werden automatisch eingerichtet. Sie werden gefragt, welchen Displaymanager Sie verwenden möchten. Wählen Sie „gdm3“ für einen Anmeldebildschirm im Gnome-Stil. Starten Sie Linux neu, klicken Sie im Anmeldebildschirm auf Ihren Benutzernamen, dann auf das Zahnradsymbol und wählen Sie im Menü „Ubuntu“.

Ein auf diesem Wege installierter Gnome-Desktop entspricht weitestgehend den Gnome-Standards und sieht daher etwas anders aus als unter Ubuntu. Der Programmstarter – bei Gnome „Dash“ genannt – erscheint bei Linux Mint wie bei Fedora als Leiste am unteren Bildschirmrand, bei Debian links. Sichtbar ist das Dash nur nach einem Klick auf „Aktivitäten“. Eine Konfiguration oder Änderung der Position ist nicht vorgesehen (siehe Abschnitt „Nützliche Gnome-Anpassungen“).

Gnome wieder deinstallieren? Eine zusätzliche Desktopumgebung lässt sich nicht einfach wieder entfernen.

```
sudo apt remove gnome
```

deinstalliert nur das Metapaket selbst, jedoch nicht die automatisch installierten Pakete. Erst nachfolgendes

```
sudo apt autoremove
```

entfernt weitere Pakete, der Gnome-Desktop bleibt jedoch weitestgehend erhalten und taucht auch in der Sitzungsauswahl auf. Auf die Deinstallation anderer, zu Gnome gehörigen Pakete sollte man verzichten, weil aufgrund der Abhängigkeiten auch Pakete für die ursprüngliche Desktopumgebung entfernt werden und diese dadurch unbrauchbar wird.

Konzept und Funktionsumfang

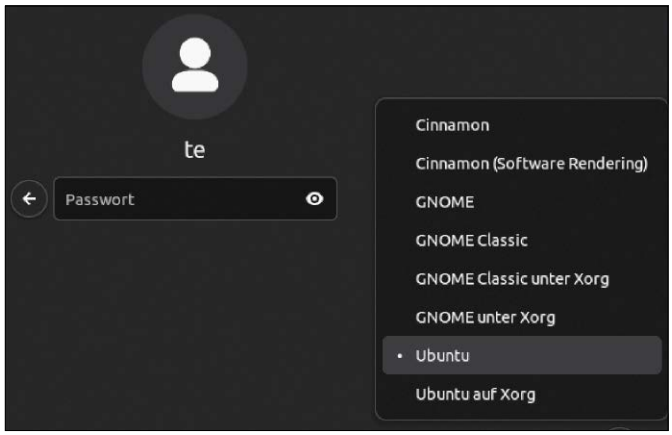
Viele Desktops orientieren sich an Windows, einige auch an Mac-OS. Vor allem für Windows-Umsteiger wird der Wechsel zu Linux erleichtert, wenn das Bedienkonzept zumindest ähnlich ist. Die Gnome-Entwickler haben sich für einen anderen Weg entschieden, an den sich Benutzer erst einmal gewöhnen müssen. Ein unveränderter Gnome-3-Desktop zeigt beim Start eine eher sinnfreie Desktopvorschau mit dem Hintergrundbild. Am unteren Bildschirmrand ist das Dash untergebracht. Es dient als Programmstarter und zeigt einige Icons, beispielsweise für den Dateimanager und Kalender. Über das Icon „Anwendungen anzeigen“ ganz rechts ruft man eine Liste aller installierten Programme auf und startet das Gewünschte per Mausklick. Alternativ tippt man einen Suchbegriff in das Eingabefeld ein.

Wurde ein Programm gestartet, verschwindet das Dash und man sieht nur noch das Programmfenster. Ein Klick auf „Aktivitäten“ blendet Dash und Suchfeld wieder ein. Die Vorschau zeigt jetzt die geöffneten Fenster, die man per Mausklick aktivieren kann.

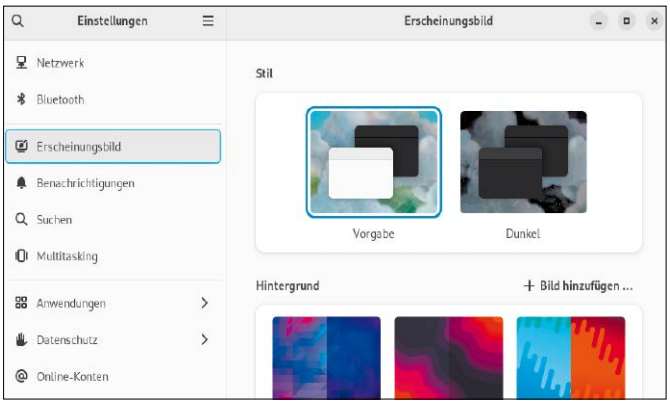
Laufende Anwendungen werden im Dash als Icons mit einem Punkt darunter dargestellt. Per rechtem Mausklick und „An Dash anheften“ kann man ein Programm dauerhaft in das Dash aufnehmen. Eine Taskleiste im eigentlichen Sinn gibt es bei Gnome nicht. Die obere Leiste zeigt nur die gerade aktive Anwendung an und bietet ein Menü, das je nach Programm unterschiedliche Einträge zeigt.

Der „Schreibtisch“, also die Oberfläche des Desktops, ist bei Gnome fast ohne Funktion. Man kann ihn mit einem Hintergrundbild verzieren, ein rechter Mausklick führt zu den Menüpunkten „Hintergrund ändern“, „Anzeigeeinstellungen“ und „Einstellungen“. Ordner, Dateien oder Verknüpfungen lassen sich nicht auf dem Desktop ablegen oder erstellen. Die Gnome-Entwickler argumentieren, dass man den Desktop ohnehin fast nie sieht, weil Fenster ihn verdecken.

Besonderheiten bei Ubuntu: In Ubuntu sind die strengen Gnome-Vorgaben etwas entschärft, was die Bedienbarkeit für viele Nutzer verbessern dürfte. Nach dem Start sind Desktop sowie Dash zu sehen und die Leiste bleibt dauerhaft sichtbar. Auf dem Desktop lassen sich über das Kontextmenü neue Ordner anlegen und man kann vom Dateimanager Ordner und Dateien auf den Desktop ziehen.



Desktopauswahl: Wenn mehrere Desktopumgebungen installiert sind, erfolgt die Auswahl nach einem Klick auf den Benutzernamen im Anmeldebildschirm.



Wenig Auswahl: Ein Standard-Gnome bietet nur wenige Einstellungen für die Optik. Es lassen sich zwei Desktop-Stile und Hintergrundbilder konfigurieren.

Die Bedienung ist allerdings nicht konsistent. Zieht man eine Datei im Dateimanager bei gedrückter Alt-Taste in einen anderen Ordner und lässt die Maustaste dann los, erscheint ein Menü mit den Einträgen „Hierher verschieben“, „Hierher kopieren“ und „Hierher verknüpfen“. Die gleiche Aktion bewirkt beim Desktop immer „Hierher verschieben“ (gleiches Laufwerk), das Menü erscheint nicht. Man kann sich aber damit behelfen, den Ordner „Schreibtisch“ in einem zweiten Fenster des Dateimanagers zu öffnen. Kopieren Sie die gewünschten Dateien oder Ordner hinein oder erstellen Sie Verknüpfungen, die auf dem Desktop erscheinen sollen.

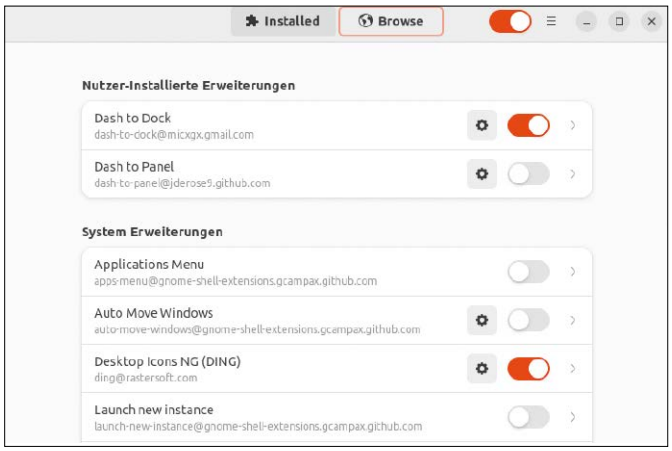
Wer Programme über ein Desktopicon starten möchte, kopiert die zugehörige „.desktop“-Datei aus dem Ordner „/usr/share/applications“ in den Ordner „Schreibtisch“. Im Kontextmenü des Icons ist danach noch ein Klick auf „Start erlauben“ erforderlich.

Die Ubuntu-Anpassungen ziehen weitere Änderungen nach sich. Das Kontextmenü des Desktops bietet beispielsweise „Symbole anordnen“ und „Anordnen nach → Sortiert nach Name“. In den „Einstellungen“ kann man unter „Darstellung“ beispielsweise die Größe der Schreibtischsymbole einstellen und die Position des Dash-Docks mit „Links“, „Unten“ oder „Rechts“ festlegen.

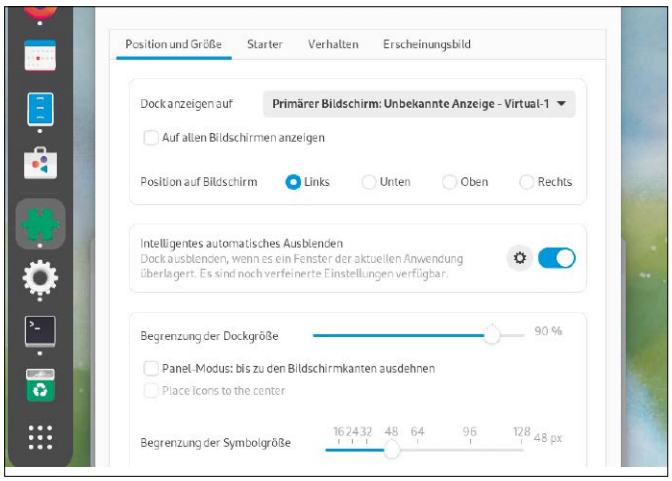
Nützliche Gnome-Anpassungen

Gnome bietet absichtlich wenige Einstellungen, um die Oberfläche individuell anzupassen. Beim Standard-Gnome kann man in den „Einstellungen“ unter „Erscheinungsbild“ lediglich zwischen den Stilen „Vorgabe“ (hell) und „Dunkel“ wählen und ein anderes Hintergrundbild einstellen. Unter „Barrierefreiheit“ sind einige Optionen zu finden, etwa für die Größe von Schrift und Mauszeiger. Ubuntu bietet unter „Darstellung“ zusätzlich die Möglichkeit, Akzentfarben für Icons und andere Fensterelemente einzustellen.

Gnome-Erweiterungen nutzen: Was Gnome fehlt, lässt sich teilweise über Erweiterungen nachrüsten. Auf *https://extensions.gnome.org* kann man nach Erweiterungen suchen und installieren. Damit die Installation über den Browser funktioniert, instal-



Mehr Funktionen für Gnome: Das Tool Extension-Manager ermöglicht die Verwaltung, Konfiguration und Installation neuer Erweiterungen.



Dash konfigurieren: Die Erweiterung Dash to Dock bietet umfangreiche Einstellungen für die Favoritenleiste. Sie können dann auch die Position und das Verhalten konfigurieren.

lieren Sie zuerst das Firefox-Add-on „Gnome Shell-Integration“ (*https://addons.mozilla.org/de/firefox/addon/gnome-shell-integration*). Nutzer von Ubuntu oder Debian installieren danach zwei zusätzliche Pakete mit

```
sudo apt install chrome-gnome-shell
  gnome-shell-extension-prefs
```

Ab Ubuntu 23.04 heißt das erste Paket „gnome-browser-connector“. Für andere Systeme oder Browser folgen Sie dem Link „Siehe wiki page“ auf *https://extensions.gnome.org*. Das Paket „gnome-shell-extension-prefs“ richtet ein Tool ein, das man unter dem Namen „Erweiterungen“ findet. Darüber lassen sich installierte Erweiterungen deaktivieren, aktivieren und konfigurieren. Bei Fedora heißt das Paket „gnome-extensions-app“.

https://extensions.gnome.org zeigt beim Aufruf unter Ubuntu zurzeit einen Fehler an, der die nicht vorhandene Unterstützung für API v6 bemängelt. Installation und Verwaltung der Erweiterungen funktionieren aber trotzdem. Alternativ kann man Erweiterungen über das Tool Erweiterungs-Manager installieren, den man unter Ubuntu 22.04 mit

```
sudo apt install gnome-shell-
  extension-manager
```

einrichtet. Nach einem Klick auf „Browse“ kann man nach Erweiterungen suchen und diese installieren. Unter „Installed“ lassen sich Erweiterungen deaktivieren, aktivieren und konfigurieren.

Mehr Optionen für das Dash: Ubuntu verwendete standardmäßig die Gnome-Erweiterung Ubuntu-Dock für die Leiste am linken Rand des Bildschirms. Dabei handelt es sich um eine modifizierte Version von Dash to Dock. Das Original bietet jedoch mehr Funktionen. Zur Installation gehen Sie auf *https://extensions.gnome.org/extension/307*, setzen den Schalter rechts oben auf „On“ und klicken auf „Installieren“.

Starten Sie das Tool „Erweiterungen“ und klicken Sie unter „Dash to Dock“ auf „Einstellungen“. Auf der ersten Registerkarte „Position und Größe“ lässt sich die Position des Docks auf dem Bildschirm festlegen. Alle vier Seiten sind möglich. Standardmäßig stellt ein Klick auf ein Dock-Icon das minimierte Fenster einer Anwendung wieder her. Ein weiterer Mausklick auf das Icon hat keine Wirkung. Sind mehrere Fenster einer Anwendung geöffnet, wechselt jeder Mausklick zwischen den Fenstern. Auf der Registerkarte „Verhalten“ lässt sich das hinter „Wirkung bei Mausklick“ ändern. Ist „Minimieren“ eingestellt, werden alle Fenster per Mausklick minimiert und bei einem erneuten Klick wiederhergestellt.

Taskleiste für Gnome: Eine traditionelle Taskleiste lässt sich mit der Erweiterung Dash to Panel nachbilden, die das Dock mit dem Hauptpanel zusammenführt. Installieren Sie dazu die Erweiterung über *https://extensions.gnome.org/extension/1160*. Dash to Panel lässt sich auf dem gleichen Weg konfigurieren wie zuvor bei Dash to Dock beschrieben. Es lassen sich die Position der Leiste, deren Höhe und Länge festlegen.

Startmenü für Gnome: Die Erweiterung Applications Menu (*https://extensions.gnome.org/extension/6*) ist in der Regel standardmäßig installiert und lässt sich über das Tool „Erweiterungen“ aktivieren. Per Klick auf die Schaltfläche „Anwendungen“ lässt sich dann ein einfaches Menü mit Kategorien wie „Büro“ und „Internet“ aufrufen. Das Arc Menu (*https://extensions.gnome.org/extension/3628*) bietet ein Menü im Stil von Windows 7 mit Suchfunktion. In der Konfiguration sind umfangreiche Anpassungen möglich.

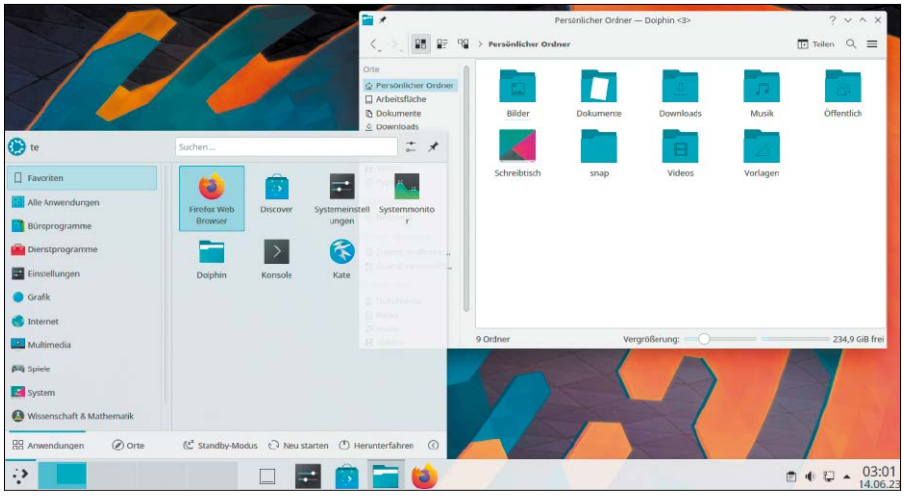
Zusätzliche Gnome-Einstellungen: Das Tool „Optimierungen“ aus dem Paket „gnome-tweaks“ kann die Schaltflächen „Minimieren“ und „Maximieren“ in den Titelleisten der Fenster aktivieren (bei Ubuntu Standard). Außerdem kann man damit Desktopthemes und Schriftarten konfigurieren.

Tastenkombinationen: Als Programmwechsler dient das übliche Alt-Tab, ferner auch Super-Tab („Windows“-Taste). Mit Super-Taste allein öffnet man die „Aktivitäten“. Wer die Tastatur gegenüber der Maus bevorzugt, kann in den „Einstellungen“ die Belegung unter „Tastatur → Tastenkombinationen anzeigen und anpassen“ einsehen und eigene Tastenkombinationen festlegen. Nützlich ist beispielsweise „Alle normalen Fenster verbergen“ unter „Navigation“. Damit kann man alle Fenster verbergen und wiederherstellen. In Ubuntu ist hierfür bereits Strg-Super-D konfiguriert. Bei anderen Systemen legen Sie selbst eine Tastenkombination fest. ■

KDE Plasma: Der individuelle Desktop

Der KDE-Desktop ist sinnvoll vorkonfiguriert und lässt sich intuitiv schnell nutzen. Zahlreiche Einstellungen für Themes und Oberfläche ermöglichen außerordentlich viele Anpassungen und funktionale Erweiterungen.

VON THORSTEN EGGELING



KDE Plasma (*https://kde.org*) gehört zu den Desktopumgebungen im klassischen Stil. Das KDE-Startmenü zeigt Kategorien wie „Büroprogramme“ und „Grafik“ und bietet eine Suchfunktion. Die Leiste am unteren Bildschirmrand nimmt Programmstarter sowie die Icons von Systemprogrammen auf und dient als Taskleiste. Optisch erscheint KDE Plasma mit fein gezeichneten Elementen sowie dezenten Farben klar und modern.

Der KDE-Desktop galt in der Vergangenheit als schwerfällig und leistungshungrig. Das trifft inzwischen nicht mehr zu. Der RAM-Bedarf liegt um die 600 bis 800 MB bei einem neu installierten und frisch gestarteten System. Auch auf älterer Hardware mit einer CPU ab zwei GHz und vier GB RAM sollte KDE Plasma flüssig laufen. Zu den Anforderungen an den Grafikchip gibt es vom KDE-Projekt keine Aussagen. Da KDE jedoch standardmäßig nur wenige Desktopeffekte nutzt, sollte das System auch mit älterer Grafikhardware zurechtkommen. Etwas aktuellere Grafikchips sind wahrscheinlich bei Nutzung des moderneren Displayservers Wayland erforderlich. Bisher kommt dieser aber nur bei Fedora standardmäßig zum Einsatz. Die meisten anderen Distributionen mit KDE setzen weiter auf X11.

Distributionen und Pakete

Wer Ubuntu mit KDE Plasma installieren möchte, greift zu Kubuntu (*https://kubuntu.org*). Auch von den meisten anderen Distributionen gibt es KDE-Varianten, beispielsweise Fedora (*https://spins.fedoraproject.org/kde*) oder man wählt den KDE-Desktop bei der Installation, etwa bei Debian (*www.debian.org*) oder Open Suse (*www.opensuse.org*). Eine Alternative ist die User-Edition von KDE Neon (*https://neon.kde.org*), die auf Ubuntu basiert, aber stets die aktuellste KDE-Version verwendet.

Eine nachträgliche Installation von KDE Plasma ist möglich, aber aufgrund möglicher Unverträglichkeiten nicht empfehlenswert.

Wer es versuchen möchte, verwendet beispielsweise unter Ubuntu mit Gnome-Desktop diesen Befehl:

```
sudo apt install kubuntu-desktop
```

Aus Ubuntu wird damit Kubuntu, der Start einer Gnome-Sitzung ist über die Sitzungsauswahl im Anmeldebildschirm weiter möglich. Alternativ ist mit

```
sudo apt install plasma-desktop
```

die Installation des Desktops ohne umfangreiche Anwendungssoftware.

Konzept und Funktionsumfang

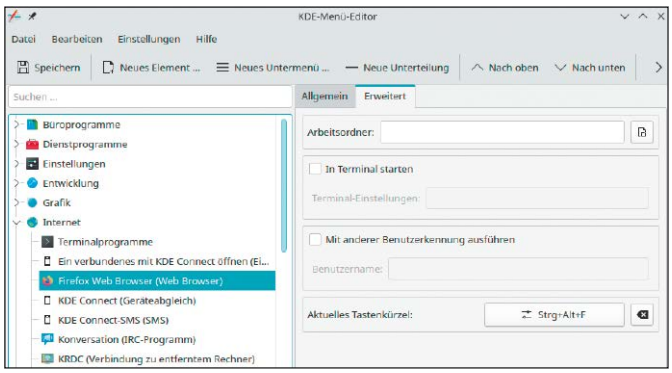
Bei KDE Plasma sollten sich Windows-Umsteiger von Anfang an wohlfühlen. Das KDE-Menü mit Suchfunktion („Anwendungsstarter“) sieht ähnlich aus wie das Startmenü von Windows 7, die Taskleiste ist am gewohnten Platz und die Oberfläche des Desktops bietet die üblichen Funktionen als Ablage von Ordnern, Dateien und Verknüpfungen. Im Detail gibt es jedoch deutliche, aber meist nützliche Unterschiede.

Nach einem rechten Mausklick auf den Anwendungsstarter beispielsweise geht man auf „Menüeinträge bearbeiten“. Sie können neue Elemente hinzufügen, Kategorien umbenennen oder neu organisieren. Bei den einzelnen Programmen lässt sich auf der Registerkarte „Erweitert“ jeweils ein Tastaturkürzel für den Schnellstart festlegen. Klicken Sie auf „Keiner“ und drücken Sie danach die gewünschte Tastenkombination. Zum Abschluss klicken Sie auf „Spei-

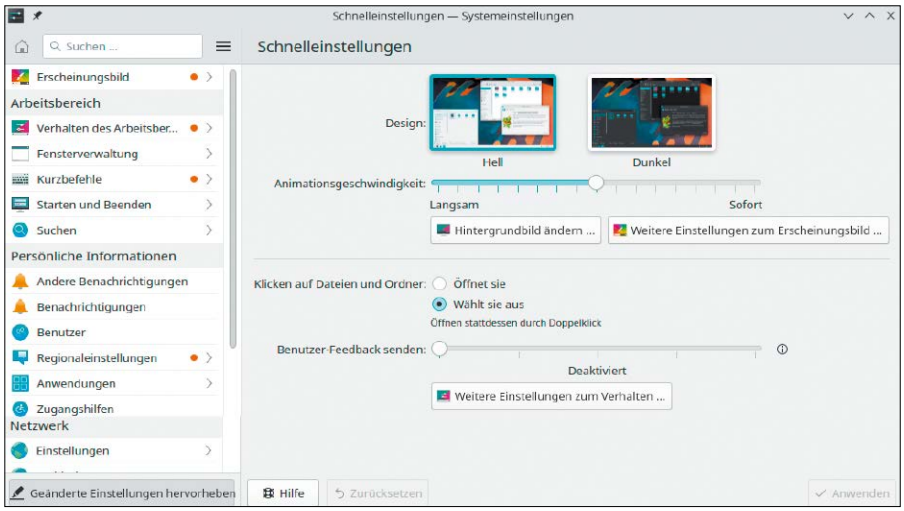
chern“. Alle selbst definierten und voreingestellten Tastaturkürzel kann man in den „Systemeinstellungen“ unter „Kurzbefehle“ einsehen und anpassen.

Über den Kontextmenüpunkt „Anwendungsstarter einrichten“ lässt sich das Aussehen des Menüs konfigurieren. Alternativ klicken Sie auf die Schaltfläche rechts oben neben dem Eingabefeld für die Suche. Setzen Sie ein Häkchen vor „Kompakten Listenstil verwenden“, wenn KDE die Elemente mit knapper einzeiliger Beschreibung anzeigen soll.

Die Beispiele zeigen, dass KDE oft mehrere Wege zu einer Konfiguration bietet und dass sich auch Kleinigkeiten detailliert einstellen lassen. Kaum eine Desktopoberfläche bietet mehr Einstellungen und Optionen als KDE. Wer das System bis ins Kleinste individuell anpassen möchte, weiß das zu schätzen. Die schiere Menge macht KDE aber auch etwas unübersichtlich. Wer in den „Systemeinstellungen“ das eine oder andere ändert, kann später Schwierigkeiten haben, eine Option wiederzufinden. Das haben auch die Entwickler erkannt und deshalb links unten die Schaltfläche „Geänderte Einstellungen hervorheben“ untergebracht (Kubuntu 22.04). Nach einem Klick darauf markiert KDE alle Rubriken mit einem farbigen Punkt, in denen etwas geändert wurde. Bei neueren KDE-Versionen ist die Funktion in das „Hamburger“-Menü (drei horizontale Linien) gewandert. Außerdem gibt es bei fast allen Einstellungen die Schaltfläche „Voreinstellungen“, die alle Optionen auf den Standard zurücksetzt.



KDE-Menü: Die Menüeinträge lassen sich in einem Editor bearbeiten und neu ordnen. Tastaturkürzel für Anwendungen kann man ebenfalls vergeben.



Was wurde geändert? Nach einem Klick auf „Geänderte Einstellungen hervorheben“ sieht man in den „Systemeinstellungen“ die Bereiche mit geänderten Optionen.

Nützliches KDE-Tuning

Skalierung des Bildschirms: HD-Monitore mit hoher Auflösung stellen Desktopoberflächen vor eine Herausforderung. Für Nutzer mit sehr guter Sehkraft mögen die sehr kleinen Schriftzeichen und Symbole noch erkennbar sein. Andernfalls muss man die Skalierung ändern, um die Darstellung zu vergrößern. Bei KDE geht man dafür in den „Systemeinstellungen“ auf „Anzeige und Monitor“. Über den Schieberegler lässt sich die Skalierung in Schritten um jeweils 25 Prozent vergrößern und über die Schaltflächen neben dem Eingabefeld mit jedem Klick jeweils um 6,25 Prozent. Bei Fedora 38 mit Wayland sind sogar Fünf-Prozent-Schritte möglich.

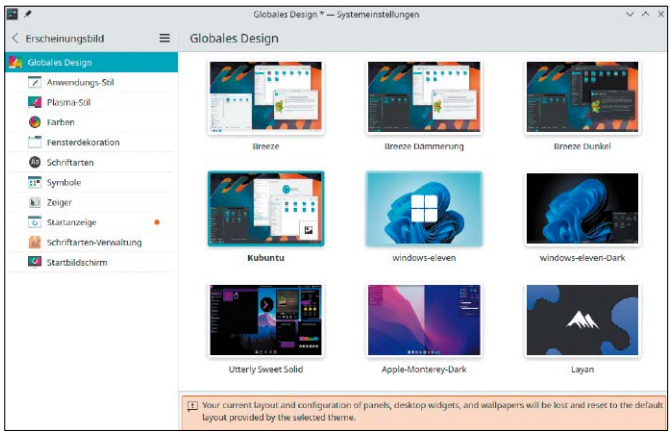
Unter „Erscheinungsbild → Schriftarten“ lässt sich „DPI für Schriften erzwingen“ aktivieren und dahinter ein anderer Wert einstellen. Mit den Einstellungen von Skalierung und DPI sollte man etwas experimentieren, um die optimalen Werte für Display und Anwendungen zu finden. Damit die Änderungen wirksam werden, muss man sich ab- und wieder anmelden.

Themen und Stile: Wie KDE Plasma aussehen soll, lässt sich in den „Systemeinstellungen“ unter „Erscheinungsbild“ konfigurieren. Unter „Globales Design“ kann man ein Theme-Paket auswählen. Über „Neue globale Designs holen“ können Sie weitere Themes herunterladen und installieren.

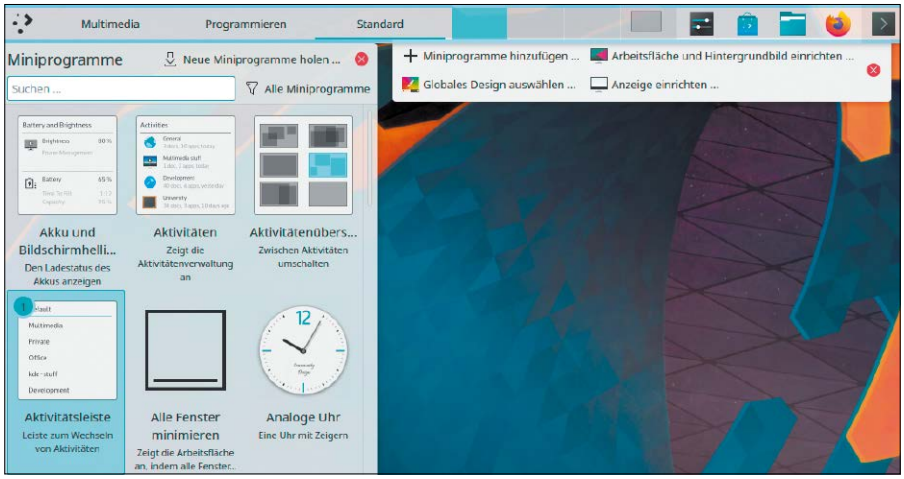
Ein Theme kann Hintergrundbilder, neue Icons, Fensterdekorationen und Miniprogramme („Widgets“) enthalten. Wenn Sie ein anderes Theme auswählen und auf „Anwenden“ klicken, wird nur ein Teil davon aktiviert. Um alle Funktionen eines Themes zu nutzen, setzen Sie ein Häkchen vor „Arbeitsflächen-Layout des Designs verwenden“ und klicken auf „Anwenden“. Bei neueren KDE-Versionen, etwa unter Fedora 38, genügt es, ein Theme anzuklicken. Es erscheint ein Fenster, in dem Sie ein Häkchen vor „Arbeitsflächen- und Fenster-Layout“ setzen und dann auf „Anwenden“ klicken. Ist diese Option aktiviert, werden beispielsweise zuvor festgelegte Hintergrundbilder und Miniprogramme durch die des Themes ersetzt.

Unterhalb von „Globales Design“ sind mehrere Rubriken zu sehen, über die sich die einzelnen Bereiche unabhängig vom aktivierten Theme beeinflussen lassen. „Anwendungs-Stil“ bezieht sich auf die Gestaltung von Elementen für Gnome/GTK-Anwendungen, „Plasma-Stil“ auf KDE-Anwendungen. In fast jedem Bereich gibt es eine Schaltfläche, um weitere Elemente/Pakete herunterzuladen.

Virtuelle Desktops: Virtuelle Arbeitsflächen sind praktisch, wenn man nur über einen Monitor verfügt, aber häufig viele Fenster geöffnet hat. Bei KDE ist standardmäßig nur eine Arbeitsfläche konfiguriert. In den „Systemeinstellungen“ lassen sich unter „Verhalten des Arbeitsbereichs → Virtuelle Arbeitsflächen“ weitere hinzufügen.



Theme aktivieren: Neue Designs können alle Bereiche des Desktops inklusive Miniprogrammen verändern, wenn ein Häkchen vor „Arbeitsflächen-Layout des Designs verwenden“ gesetzt ist.



Kontrollleisten erstellen: Leisten lassen sich beliebig anpassen und mit neuen Miniprogrammen für bestimmte Aufgaben ausstatten, etwa für die Steuerung von Aktivitäten.

Danach erscheint automatisch das Miniprogramm „Arbeitsflächen-Umschalter“ in der Leiste am unteren Bildschirmrand, über das man die Arbeitsflächen per Mausklick wechseln kann. Der Wechsel gelingt auch per Mausrad oder mit den Tastenkombination Strg-F1, Strg-F2 und so weiter. Im Kontextmenü der Titelleiste einer Anwendung können Sie unter „Arbeitsflächen“ Häkchen vor die Arbeitsflächen setzen, auf denen das Fenster auch erscheinen soll. Es handelt sich um eine Kopie des Fensters, nicht um eine zweite Instanz. Wenn Sie eins der Fenster schließen, werden auch alle anderen geschlossen. Sie können beispielsweise auch „Arbeitsflächen → Verschieben nach 2 Arbeitsfläche 2“ anklicken, um ein Fenster auf eine andere Arbeitsfläche zu verschieben.

KDE-Aktivitäten: KDE bietet eine weitere Funktion zur Organisation von Fenstern und Desktops. In den „Systemeinstellungen“ lassen sich unter „Verhalten des Arbeitsbereichs → Aktivitäten“ mehrere Arbeitsbereiche einrichten. Dabei handelt es sich um unabhängige Desktops, die jeweils auch ihre eigenen virtuellen Arbeitsflächen enthalten. Wenn man beispielsweise vier Aktivitäten und vier virtuelle Arbeitsflächen erstellt, erhält man 16 Desktops.

Zwischen den Aktivitäten wechselt die Tastenkombination Meta-Tab („Windows“-Taste und Tab-Taste). Zur besseren Unterscheidung lässt sich für jede Aktivität ein eigenes Hintergrundbild festlegen. Dazu klicken Sie mit der rechten Maustaste auf einen freien Bereich des Desktops, gehen auf „Arbeitsfläche und Hintergrundbild einrichten“ und wählen das gewünschte Bild aus. Programmstarter in der Leiste kann man gezielt für die jeweilige Aktivität einrichten und hat dann die für die Aufgabe passenden Anwendungen parat. Bei einem angehefteten Programmsymbol dient dazu das Kontextmenüpunkt „In Aktivitäten anzeigen → [Name der Aktivität]“.

Im Kontextmenü der Titelleiste eines Fensters finden Sie unter „In Aktivitäten anzeigen“ ähnliche Optionen wie bei den Arbeitsflächen. Ein Fenster kann zugleich in mehreren Aktivitäten erscheinen und Sie können es verschieben.

Tastenkombinationen: Die Einstellungen für Tastenkürzel sind in den „Systemeinstellungen“ unter „Kurzbefehle“ zu finden. Wer mit virtuellen Desktops arbeitet, kann bei „Fenster auf nächste Arbeitsfläche verschieben“ und „Fenster auf vorherige Arbeitsfläche verschieben“ beispielsweise Strg-Umschalt-Alt-Cursor rechts/links konfigurieren.

Zusätzliche KDE-Anpassungen

Die Leiste am unteren Bildschirmrand – bei KDE „Kontrollleiste“ genannt – ist modular aufgebaut und besteht aus einzelnen Miniprogrammen. Die Standardleiste enthält „Anwendungs-Starter“, „Fensterleiste nur mit Symbolen“, „Symbolabschnitt der Kontrollleiste“, „Digitale Uhr“ und „Blick auf die Arbeitsfläche“ (alle Fenster aus- und einblenden). Jedes Modul lässt sich entfernen oder austauschen und Sie können neue Miniprogramme hinzufügen.

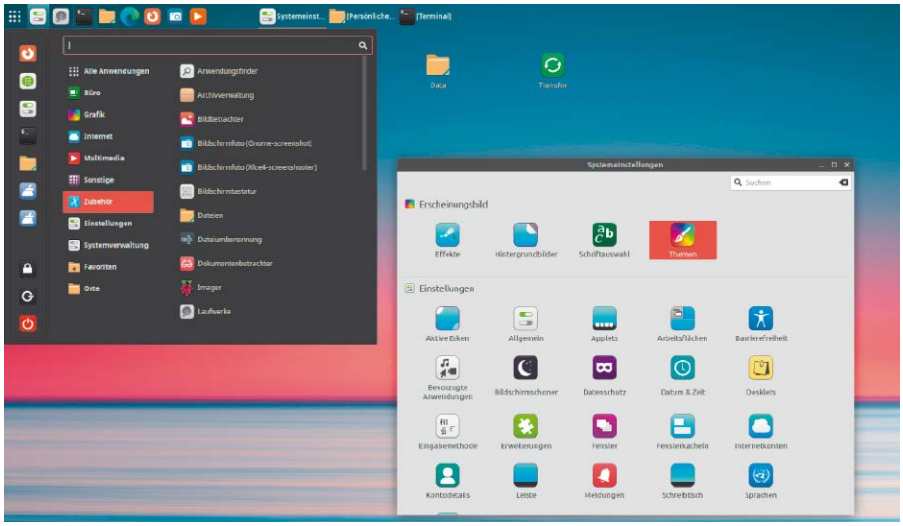
KDE ist nicht auf eine Leiste beschränkt. Ein rechter Mausklick auf einen freien Bereich des Desktops und „Kontrollleiste hinzufügen → Leere Kontrollleiste“ erstellt eine weitere Leiste. Klicken Sie die neue Leiste mit der rechten Maustaste an und wählen Sie „Bearbeitungsmodus starten“. Klicken Sie in den Bereich „Ziehen zum Verschieben“ oder „Drag to Move“ und ziehen Sie die Leiste mit der Maus an die gewünschte Position. Nach einem Klick auf „+ Miniprogramme hinzufügen“ füllen Sie die bisher leere Leiste mit Inhalt. Wer Aktivitäten verwendet, kann „Aktivitäten“, „Aktivitätsübersicht“ oder „Aktivitätsleiste“ per Mausklick in die Leiste einbauen. Darüber kann man schnell zwischen den Aktivitäten wechseln beziehungsweise die Liste der Aktivitäten einblenden. Es gibt Miniprogramme für den Wetterbericht, Systemmonitore und die Zwischenablage. Wem die Auswahl nicht ausreicht, kann über „Neue Miniprogramme holen“ weitere herunterladen.

Fährt man im Bearbeitungsmodus mit dem Mauszeiger über ein Miniprogramm, sieht man meist den Menüpunkt „Alternativen anzeigen“. Der zeigt eine Liste mit anderen Miniprogrammen für die gleiche Aufgabe, aber mit unterschiedlichen Funktionen. Der Menüpunkt „Einrichten“ führt zur Konfiguration des jeweiligen Miniprogramms. ■

Cinnamon: „Wie es euch gefällt!“

Gnome oder ein Windows-Explorer stellen Benutzer vor vollendete Tatsachen. Cinnamon versteht sich eher als offenes Angebot mit vielen Anpassungsoptionen. Bastelzwang besteht allerdings nicht: Cinnamon kommt „out of the box“ attraktiv und funktional.

VON HERMANN APFELBÖCK



Cinnamon ist – ähnlich wie Mate – eine Antwort auf das eigenwillige Gnome-3-Konzept und wird mit konservativer Ausrichtung auf Gnome-2-Basis weiterentwickelt. Der Desktop ist aufgeräumt, dank moderner Themes elegant und bietet viele und beinahe KDE-minutiöse Optionen für Optik, Fensterverhalten und Dateimanager. Im Fokus stehen die optimale, individuelle Wandlungsfähigkeit und viele Windows-Analogien. So baut etwa das Leistenapplet „Gruppierte Fensterliste“ die Funktionalität der Windows-Taskleiste praktisch identisch nach. Dass das nicht nur Windows-Umsteigern, sondern auch vielen Linux-Fans gefällt, ist eine Erfolgsgeschichte für sich.

Cinnamon ist anspruchsloser als Gnome oder Windows 10/11, benötigt aber halbwegs aktuelle Hardware. Mindestens vier GB RAM sollten vorliegen, weil Desktop plus System ab Anmeldung 800 bis 900 MB Speicher fordern. Cinnamon benötigt einen Grafikchip mit 3D-Beschleunigung, was aber bei Intel/AMD/Nvidia seit mehr als zehn Jahren Standard ist. Als CPU genügt eine Dualcore-CPU ab zwei GHz.

Distributionen und Pakete

Die bekannteste Distribution, die Cinnamon als Standarddesktop verwendet, ist Linux Mint, dessen Team diesen Desktop auch entwickelt. Inzwischen etabliert sich Cinnamon auch als offizieller Ubuntu-Flavour unter dem Namen Ubuntu Cinnamon (*https://cdimage.ubuntu.com/ubuntucinnamon*). Als optionaler Desktop wird Cinnamon inzwischen praktisch überall angeboten, etwa bei Arch-Varianten (Endeavour, Manjaro), Debian, Fedora, Open Suse.

Soll Cinnamon auf einem bereits bestehenden System nachinstalliert werden, stehen in den meisten Repositorys die Pakete „cinnamon“ oder „cinnamon-core“ (fast identisch), ferner die komplette Umgebung samt Anwendungssoftware zur Auswahl („cinnamon-desktop-environment“). Für den Desktop und dessen Kernkomponenten wie die „Einstellungen“ (cinnamon-control-center) und den Dateimanager Nemo sind die kleineren Pakete völlig ausreichend.

Aber Achtung: In manchen Quellen liegen Cinnamon-Pakete in moosalten Versionen, was sich am besten vorab mit Synaptic ermitteln lässt. Der mit Linux Mint ausgelieferte Cinnamon erreicht inzwischen Version 5.8 und uralte Versionen mit einer 4.x sind nicht zu empfehlen, weil damit viele „Spices“ (Erweiterungen und Leistenapplets) nicht mehr kompatibel sind. Der Desktop ist dann nicht nur angestaubt, sondern funktioniert in Teilen auch nicht korrekt.

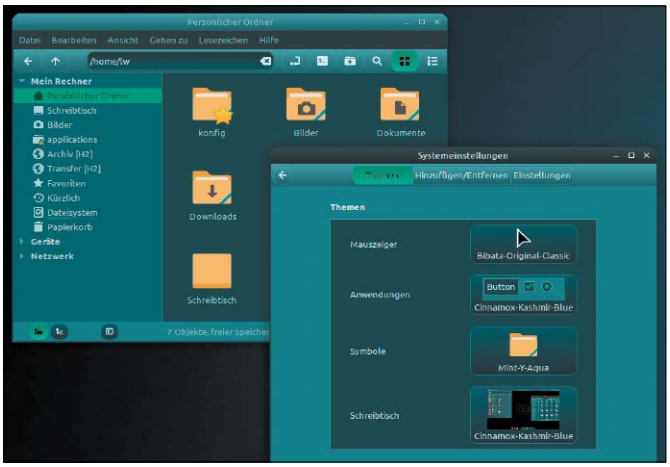
Besonders frische Pakete sind bei aktuellen Ubuntu-basierten Systemen zu finden, und zwar mit Paketnamen, die sich bereits auf das neue offizielle Ubuntu Cinnamon beziehen: „ubuntucinnamon-desktop“ und „ubuntucinnamon-environment“. Zu empfehlen ist das erste und kleinere Paket, das für die vollständige Installation des Desktops genügt und derzeit den recht aktuellen Cinnamon 5.6.7 mitbringt.

Konzept und Funktionsumfang

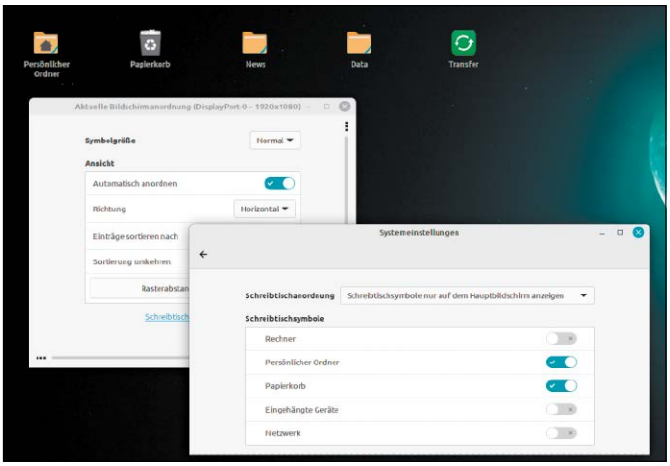
Cinnamon ist eine klassische Oberfläche mit Systemleiste(n), Hauptmenü und multifunktionalem Desktop als Ablage für Standardsymbole, Ordner, Dateien, Starter und Minianwendungen. Das Menü mit Suchfeld bietet sehr variable Optionen und sogar

einen eigenen Menüeditor. Die „Systemeinstellungen“ (cinnamon-settings) gehören zum komplettesten Angebot (neben KDE), was Linux-Desktops an grafischer Systemverwaltung zu bieten haben. Die Notwendigkeit für Terminal-Ausflüge reduziert sich auf ein Minimum. Cinnamon liefert zahlreiche objektorientierte Kontextmenüs, um Konfigurationsdialoge für Desktop, Leiste, Dateiobjekte intuitiv zu erreichen. Beim angestammten und sehr anpassungsfähigen Dateimanager Nemo ist eine Reduktion des Angebots („Einstellungen → Werkzeugleiste/Kontextmenü/Module“) zu empfehlen, um es übersichtlich zu halten. Generell tendiert Cinnamon dazu, Vorgaben zu meiden und Desktopelemente als möglichst flexibles Angebot auszuliefern. Daher gerät mancher Einstellungsdialog (etwa Themenwahl, Konfiguration von Leistenapplets) zur intellektuellen Herausforderung.

Auch technisch ist Cinnamon nicht perfekt: Die Einrichtung der Systemleiste ist zwar so offen wie bei vielen Linux-Desktop üblich, aber handwerklich deutlich fummeliger als etwa bei XFCE. Bei der Bildschirmskalierung sind standardmäßig nur unpraktikable 25-Prozent-Schritte möglich. Auch das können andere besser.



Die Einstellungen unter „Themen“ bestimmen die Optik. Damit alles harmonisch zusammenpasst, ist unter „Anwendungen“ und Schreibtisch“ dasselbe Thema zu empfehlen.



Arbeitsfläche einrichten: Hierfür sind zwei unabhängige Dialoge zuständig – der Punkt „Schreibtisch“ in den Systemeinstellungen und der Desktopkontext „Anpassen“.

Nützliches Cinnamon-Tuning

Bildschirm und Schriften: Wie schon angesprochen, erlaubt die Bildschirmskalierung unter „Systemeinstellungen → Bildschirm“ nur grobe Schrittstufen und allenfalls „125%“ ist eine eventuelle Option. Eine weitere Möglichkeit der Darstellungsoptimierung ist der „Skalierungsfaktor der Schrift“ unter „Einstellungen → Schriftauswahl“. Ein Verändern des Standardwertes „1.0“ auf „0,9“ oder „1,1“ beeinflusst Darstellung und Lesbarkeit der Desktopelemente wesentlich.

Themen bestimmen das Aussehen entscheidend. Unter „Systemeinstellungen → Themen → Schreibtisch“ legen Sie die Farben des Hauptmenüs und der Systemleiste fest. Der weitere Unterpunkt „Symbole“ bestimmt die Optik des Desktops und des Dateimanagers erheblich. Bei der Auswahl des allgemeinen Fensterthemas („Anwendungen“) ist dasselbe Thema wie bei „Schreibtisch“ zu empfehlen.

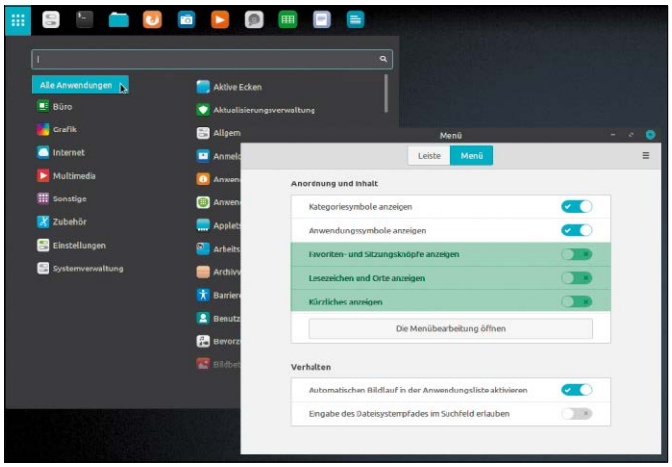
Der Punkt **Schreibtisch** (nicht zu verwechseln mit „Themen → Schreibtisch“) ist insofern wichtig, weil Cinnamon hier die Auswahl der Standardsymbole am Desktop anbietet („Papierkorb“, „Netzwerk“, „Eingehängte Datenträger“). Dem Dialog fehlt aber ein wichtiger Aspekt: Größe, Anordnung und Symbolabstand der Desktopelemente können nur nach einem Rechtsklick auf dem Desktop und „Anpassen“ eingestellt werden.

Hintergrundbild: Den Desktophintergrund ändern Sie über „Systemeinstellungen → Hintergrundbilder“, noch einfacher durch Rechtsklick am Desktop und „Hintergrund […] ändern“. Abgesehen von den mitgelieferten Bildern können Sie mit dem kleinen Plus-Symbol (unten links) einen eigenen Bilderordner vorgeben.

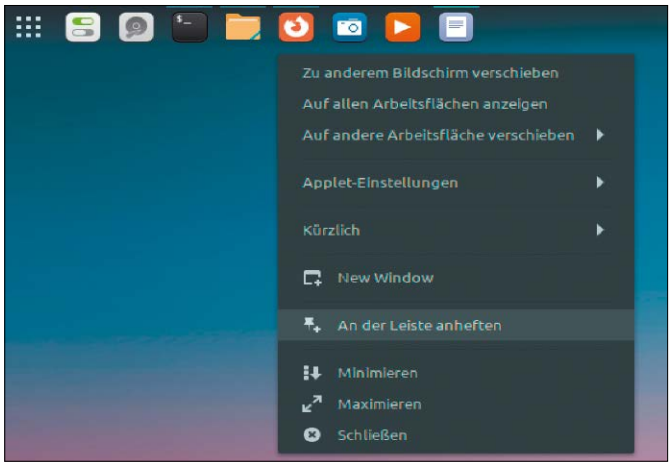
Aktive Ecken lösen durch Mausbewegung in eine Bildschirmecke eine Desktopaktion oder ein Programm aus. Aktive Ecken neben wichtigen Klickzielen wie dem Hauptmenü oder Programmtitelleisten sind allerdings kontraproduktiv. Da Titelleisten standardmäßig oben sind, die Systemleiste standardmäßig unten, gibt es eigentlich keinen störungsfreien Platz für aktive Ecken. Wenn Sie allerdings die Systemleiste nach oben verlegen (Rechtsklick auf die Leiste und „Verschieben“), können unten zwei aktive Ecken scharf gestellt werden. Als Aktionen bieten „Aktive Ecken“ typische Fensteraktionen wie „Alle Fenster anzeigen“ oder „Alle Arbeitsflächen anzeigen“.

Virtuelle Arbeitsflächen: Das Handling unter Cinnamon ist vorbildlich. Als Standardhotkeys dienen Strg-Alt-Cursor rechts/links zum Wechsel und Strg-Alt-Cursor-oben zur Übersicht. Die zusätzlich gedrückte Umschalt-Taste verschiebt das aktuelle Fenster auf die nächste Arbeitsfläche. Die Anzahl der virtuellen Desktops können Sie in der Arbeitsflächenübersicht (Strg-Alt-Cursor-oben) verringern oder erhöhen– durch Schließen eines Desktops („X“-Symbol) oder durch Klick auf das Plus-Symbol ganz rechts. Auch das optionale Leistenapplet „Arbeitsflächenwechsler“ bietet Kontextmenüs, um die Anzahl der Desktops zu vergrößern oder zu verringern.

Tastenkombinationen: Eine Übersicht aller Cinnamon-Hotkeys finden Sie unter „Systemeinstellungen → Tastatur → Tasten-



Flexibles Menü-Applet: Wenn andere Applets die Rolle übernehmen, kann das Hauptmenü Angebote wie „Favoriten“ oder Shutdown-Optionen ausblenden.



Applet „Gruppierte Fensterliste“: Die Windows-ähnliche Taskleiste hat komplexe Einstellungsoptionen, aber das Anheften von Programmen könnte nicht einfacher sein.

kombinationen“. Um eigene Tastenkombinationen zu definieren, klicken Sie auf die Kategorie „Eigene Tastenkombinationen“ und „ Eigene Tastenkombination erstellen“. Nun geben Sie „Name“ und „Befehl“ ein. Der Befehl könnte etwa „cinnamon-settings“ lauten (also die „Systemeinstellungen“). Der neue Hotkey erscheint dann im Dialog und im unteren Bereich „Tastenkombinationen“ klicken Sie nun zweimal auf „nicht zugeordnet“. Danach drücken Sie den Hotkey Ihrer Wahl.

Die Cinnamon-„Spices“

Cinnamon kann durch vier Spices-Kategorien („Gewürze“) erweitert werden. Im Prinzip können Sie alle Spices von der Sammelstelle *https://cinnamon-spices.linuxmint.com* beziehen und in jene Ordner entpacken, wie es die Webseite beschreibt.

Der einfachere Weg führt aber über die „Systemeinstellungen“ nach „Themen“, „Applets“, „Desklets“ und „Erweiterungen“. Dort zeigt das Register „Herunterladen“ (für Themen das Register „Hinzufügen/Entfernen“) das Spices-Angebot. Nach dem Download durch Klick auf das Pfeil-Symbol erscheint es in der lokalen Liste unter „Verwalten“ (oder „Themen“) und kann dann aktiviert werden.

Themen-Spices: Hier lautet die Devise: nicht übertreiben! Andernfalls wird der Katalog unter „Systemeinstellungen → Themen“ so unübersichtlich, dass die Auswahl und vor allem die Abstimmung zwischen den Elementen kompliziert wird.

Desklet-Spices: Desklets sind kleine, frei platzierbare Info-Gadgets für die Arbeitsfläche – etwa der „Digitale Bilderrahmen“ für kleine Diashows oder das „Uhr-Desklet“. Unter den nachladbaren Desklets gibt es aber wenig Lohnendes, das sich nicht effizienter als Leistenapplet realisieren ließe.

Erweiterungen: Die Spices-Kategorie unter „Einstellungen → Erweiterungen“ bietet hauptsächlich optische Ergänzungen wie „Desktop Cube“ oder „Opacify Windows“. Unterm Strich sind diese „Erweiterungen“ marginal, aber es gibt Ausnahmen. Die beliebteste Erweiterung **„Transparent Panels“** macht die Systemleiste(n) transparent – auf Wunsch mit Schattenwurf, um die Leiste etwas abzuheben. **„Smart Panel“** ist komplizierter und erlaubt Komfortklicks für die (primäre) Systemleiste. In den Einstellungen ist an oberster Stelle unter „Mouse scroll options“ eine „Action on scrolling“ angegeben (Mausrolltaste). Wenn Sie hier „Switch between workspaces“ einstellen, dürfte dies die bequemste Möglichkeit sein, zwischen virtuellen Arbeitsflächen zu wechseln. Unter den „Click options“ kann man für den Doppelklick und den Mittelklick (Mausrad) auf der Systemleiste eine Fensteraktion wie die „Arbeitsflächenübersicht“, aber auch einen beliebigen Programmstart definieren.

Applets: Das Angebot der Systemleiste(n) wird durch modulare Applets geregelt. Die derzeit aktiven und sonstigen verfügbaren Applets verwalten Sie in der Übersicht „Systemeinstellungen → Applets“. Aktive Applets zeigen ein Häkchen. Mit der Minus-Schaltfläche schalten Sie das Element ab, mit der Plus-Schaltfläche ein. Viele Applets bieten eine eigene kleine Konfiguration („Einrichten“ oder „Einstellungen“). Positionell verschieben lassen sich Applets nur, wenn Sie nach Rechtsklick auf die Leiste den „Leistenbearbeitungsmodus“ aktivieren.

Unentbehrliche Applets sind das „Menü“ und eine „Fensterliste“ – vorzugsweise die „Gruppierte Fensterliste“. Alles Weitere ist geräteabhängig oder nutzungsspezifisch. Es gibt weitere optionale Applets, die kleine Aufgaben funktionsreicher anbieten, als dies das Menü oder die Standard-Applets tun: So liefert der „Session Manager“ („Sitzungsmanager“) alle Optionen zum Abschalten und Abmelden. Applets wie „Places Center“ erlauben den Sofortzugriff auf lokale Datenträger und Netzwerkfreigaben.

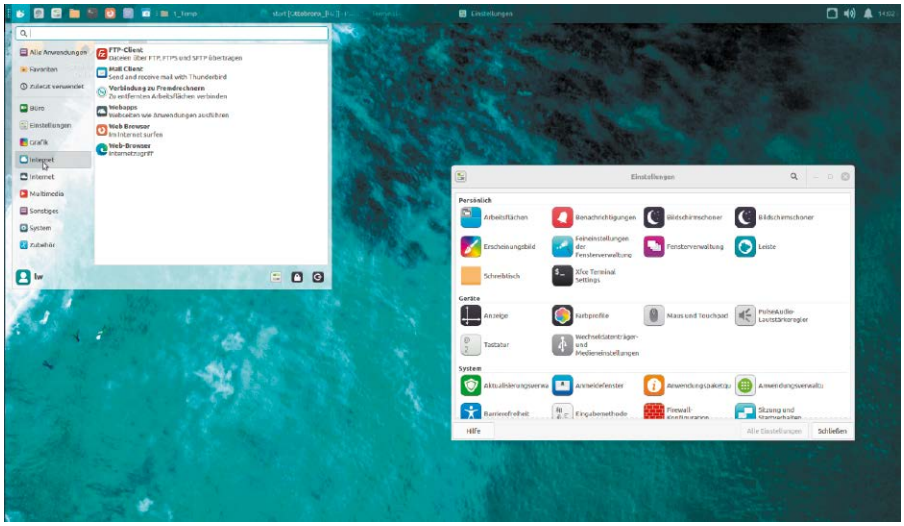
Das Applet „Gruppierte Fensterliste“ kombiniert eine dynamische Taskliste der laufenden Programme mit einem Favoritenstarter und ist praktisch funktionsidentisch mit der Windows-Taskleiste. Zum dauerhaften Anheften eines Programms wählen Sie bei einem laufenden Task nach Rechtsklick einfach „An der Leiste anheften“. Alternativ bestücken Sie die Favoriten über das Hauptmenü durch Rechtsklick auf ein Programm und „Zur Leiste hinzufügen“. Die Position der Icons können Sie hier ohne „Leistenbearbeitungsmodus“ einfach mit der Maus ändern. ■

XFCE: Ein Allzweck-Desktop

Wer einen klassischen, funktionsreichen und anpassungsfähigen Desktop sucht, ist bei XFCE („X-Face“) gut aufgehoben. Die seit 1996 entwickelte Oberfläche ist logisch, intuitiv und zudem anspruchslos – ein Desktop für alle und für fast jede Hardware.

VON HERMANN APFELBÖCK

XFCE (*www.xfce.org*) hat im Feld der Linux-Desktops sein eigenes Podest. Der XFCE-Desktop ist zwar nicht modern, aber klarer als KDE und flexibler als Gnome, Cinnamon, Mate, zudem ein Stück sparsamer. Damit hält XFCE seinen unbestrittenen Platz auf älterer (wenn auch nicht uralter) Hardware sowie bei Nutzern, die einen pragmatischen Desktop suchen. XFCE stellt keine Ansprüche an CPU und Grafik und verbraucht nur ab etwa 450 MB ab Anmeldung (je nach RAM-Ausstattung auch mehr). XFCE ist aktuell bei Version 4.18, entwickelt sich nur langsam weiter, ist konservativ, jedoch funktional, hervorragend konfigurierbar und nach Anpassungen richtig schick. Moderne Entwicklungen wie fraktionale Monitorskalierung macht der Desktop jederzeit mit, wenn auch langsamer als Gnome & Co. So steckt der Wechsel von Displayserver Xorg zu Wayland bei XFCE noch in den frühesten Anfängen.



Altmodischer XFCE? Der Desktop-Klassiker bietet ein flexibles Systemleistenkonzept und sehr viele Optionen für Oberflächenkosmetik und Fensterverhalten.

Distributionen und Pakete

Zum XFCE-Desktop kommt man am einfachsten durch Installation einer Distribution, die den Desktop mitbringt. Es gibt kaum ein prominentes Desktop-Linux, das auf eine XFCE-Variante verzichtet. Arch, Debian, Endeavour, Fedora, Linux Mint, Manjaro, Ubuntu – allesamt bieten XFCE mindestens als Flavour oder Installeroption. Als primärer Standarddesktop dient er unter anderen bei Xubuntu, MX Linux, Peppermint-OS, Endeavour-OS, Voyager-OS.

Wenn ein System bereits vorliegt und XFCE nachgerüstet werden soll, erweist sich das Paket „xfce4“ etwa unter Debian/Ubuntu mit

```
sudo apt install xfce4
```

als relatives Leichtgewicht. Dies installiert nur die Oberfläche mit den wesentlichsten Komponenten (Dateimanager, Einstellungen). Für Ubuntu-basierte Systeme ist das umfangreichere Metapaket „xubuntu-core“ zu empfehlen, während das noch größere Paket „xubuntu-desktop“ nur zusätzliche Anwendungssoftware installiert.

Das relativ kleine Paket „xfce4“ unter den anderen Distributionen mag ausreichen, verzichtet aber auf etliche Komponenten wie das Terminal (xfce4-terminal) und diverse Plug-ins (siehe unten: Whisker-Menü). Speziell unter Linux Mint installieren Sie mit

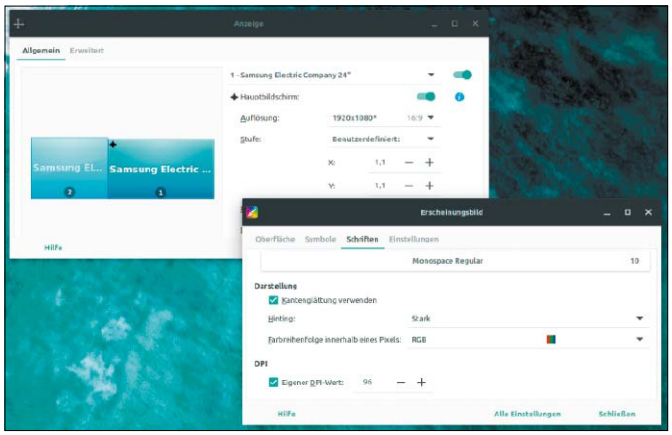
```
sudo apt install mint-meta-xfce
 xfce4-terminal
```

am besten das Metapaket aus den eigenen Mint-Paketquellen plus Terminal.

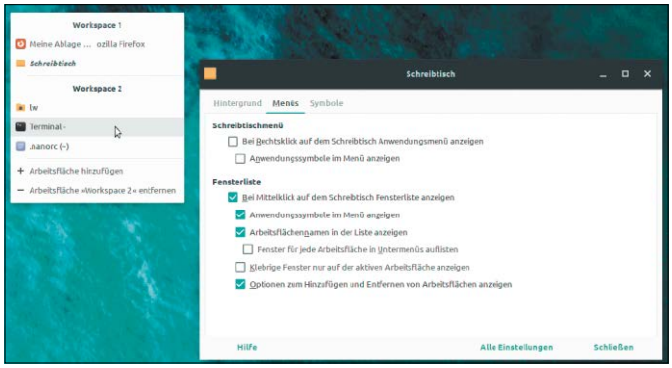
Konzept und Funktionsumfang

XFCE ist intuitiv und logisch organisiert, so dass die meisten Anpassungen direkt am Objekt (Leiste, Leistenapplets, Arbeitsfläche) per Kontextmenü erledigt werden können. Die Systemleiste enthält als Standardapplets ein einfaches Kategorienmenü (zum Teil auch das funktionsreichere Whisker-Menü), die Taskübersicht (Applet „Fensterknöpfe“) und die typischen Systemapplets für Netzwerk, Lautstärke und Zeitanzeige. Wie üblich dient die Leiste als offener Container für weitere Applets, der nach Rechtsklick auf der Leiste über „Leiste → Leisteneinstellungen → Objekte“ nach Bedarf zu ändern ist.

Für Programmfavoriten bietet XFCE zwar kein Sammelapplet, aber ein Starterdock ist mit mehreren „Starter“-Applets nebeneinander leicht zu arrangieren.



Monitore und Schriften skalieren: XFCE kann für jede Display-Situation und Monitorauflösung optimale Lösungen einstellen.



Mittelklickmenü am Desktop: Diese Option ist der kürzeste Weg, Fenster auf virtuellen Arbeitsflächen zu erreichen und zu wechseln.

An der Desktopoberfläche zeigt Xubuntu standardmäßig die Icons „Papierkorb“, „Dateisystem“ und „Persönlicher Ordner“. Der XFCE-Desktop arbeitet aber als klassische Dateiablage und kann folglich beliebige Dateiobjekte aufnehmen. Nach Rechtsklick am Desktop lassen sich neue Ordner, Dateien, Programmstarter („Starter“) oder URLs („Adressverknüpfung“) erstellen. Bei Verwendung des Whisker-Menüs können alle installierten Programme noch einfacher via „Zum Schreibtisch hinzufügen“ am Desktop abgelegt werden. Das Whisker-Menü bietet zusätzlich die Option, ein Programm als Starter in der Systemleiste abzulegen („Zur Leiste hinzufügen“).

Die „Einstellungen“ (xfce4-settings-manager) unter XFCE sind eine funktionsreiche Konfigurationszentrale, mit der Sie über die Punkte „Anzeige“, „Erscheinungsbild“, „Schreibtisch“ und „Fensterverwaltung“ jedes Anzeigegerät optimal einstellen. Fast alle Einstellungen wirken sich sofort aus und werden automatisch gespeichert. Per Klick auf „Alle Einstellungen“ gelangen Sie von einer Unterrubrik wieder zurück zur Hauptübersicht. Ein kleiner Mangel ist die fehlende grafische Benutzerverwaltung (dazu unten mehr).

Bei der XFCE-Standardsoftware sind der Dateimanager (Thunar) und der Terminalemulator (xfce4-terminal) tadellose Kandidaten, der Mediaplayer Parole, der Texteditor Mousepad und der Taskmonitor xfce4-taskmanager verdienen eventuell Ersatz (VLC, Gnome-Editor, Htop?).

Nützliche XFCE-Anpassungen

Einige Distributionen investieren viel Detailarbeit in eine attraktive XFCE-Oberfläche. Herauszuheben sind hier Xubuntu oder Voyager-OS, während Fedora oder Open Suse den Desktop praktisch unbearbeitet anbieten. In solchen Fällen – oder auch bei einer manuellen Nachinstallation – präsentiert sich XFCE hingegen sehr schmucklos. Erstaunlich attraktiv wird er dann erst durch entsprechende Anpassungen. Diese und weitere Optimierungen, die sich generell lohnen, nennt der nachfolgende Durchgang.

Whisker-Menü: Ein nachinstalliertes XFCE lässt einige Leistenapplets vermissen. Ärgerlichstes Defizit ist das sehr einfache Kategorienmenü („Anwendungsmenü“) statt des Whisker-Menüs. Das deutlich komfortablere Whisker-Applet mit Suchfeld, Verlinkungsoptionen und minutiöser Anpassung können Sie sofort in die Leiste einbauen, nachdem Sie es mit

```
sudo apt install xfce4-whiskermenu-plugin
```

nachinstalliert haben.

Grafische Benutzerverwaltung: Nach der Installation von

```
sudo apt install gnome-system-tools
```

gibt es das Tool users-admin („Benutzer und Gruppen“) als grafische Benutzerverwaltung. Dieses wird allerdings nicht in die „Einstellungen“ des XFCE-Desktops integriert und muss daher als eigenständiges Programm im Startmenü (unter „System“) genutzt werden.

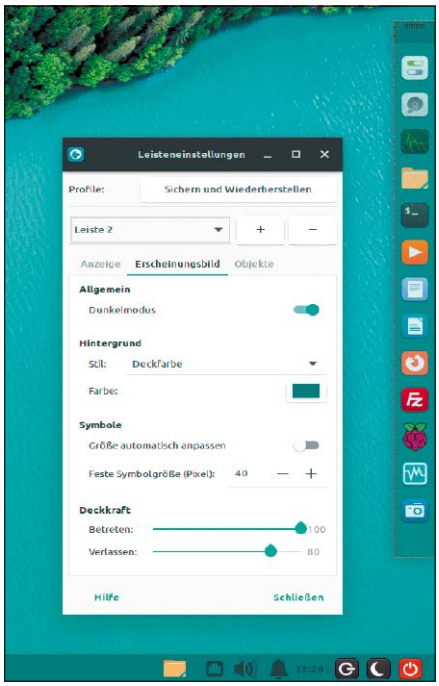
Monitoroptimierung: Unter „Einstellungen → Anzeige“ folgt XFCE dem Vorbild anderer Desktops und bietet dort mit dem Unterpunkt „Stufe“ eine flexible Monitorskalierung. Vorgegeben sind eher unbrauchbare Faktoren wie „1,5“ und „2“, aber der Klick auf „Benutzerdefiniert“ ermöglicht beliebige Werte wie „1,2“ oder „0,8“. Die Einstellung ist sogar unabhängig für mehrere Monitore möglich.

Fensteroptik und Verhalten: Relevante Punkte in den „Einstellungen“ zur Desktopgestaltung sind „Erscheinungsbild“, „Fensterverwaltung“ und „Feineinstellungen der Fensterverwaltung“.

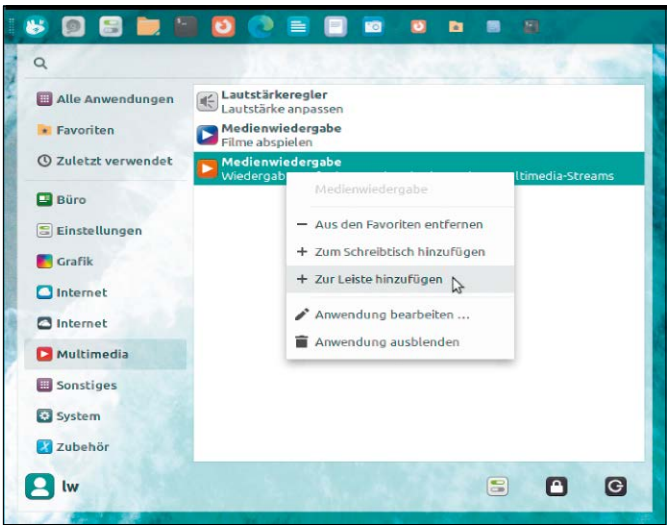
1. Mit „Erscheinungsbild → Oberfläche“ bestimmen Sie die Farbgebung von Menüs und Fensterelementen. Es empfiehlt sich, parallel ein Programm wie etwa den Dateimanager zu beobachten, um die geänderte Optik sofort vor Augen zu haben. Dem aktuellen Trend folgend gibt es dunkle Themen wie „Greybird-dark“, die den kompletten Fensterinhalt betreffen. Unter „Erscheinungsbild → Schriften“ lässt sich die Skalierung des kompletten Desktops über den DPI-Wert ändern. Dies bietet weiteres Feintuning neben der oben genannten Monitorskalierung.

2. Die „Fensterverwaltung“ bestimmt unter „Stil“ das Aussehen der Titelleisten. Wählen Sie hier etwa „Greybird-dark-acessibility“ für eine größere und dunkle Titelleiste, die damit griffiger und kontrastiver wird. Weitere Feinheiten zum Fokus und zum Einrastverhalten („Erweitert“) sind manchen Nutzern wichtig, um Windows-konformes Verhalten beim Verschieben der Fenster abzuschalten.

3. Die „Feineinstellungen der Fensterverwaltung“ zeigen auf der Registerkarte „Fensterwechsel“ Optionen für den Pro-



Exzellentes Leistenkonzept: Hier dient Leiste 1 (unten horizontal) als eigentliche Systemleiste, Leiste 2 (rechts vertikal) ausschließlich als Starter.



Hübsch und funktional: Das Whisker-Menü legt Programmstarter auf dem Schreibtisch, in der Systemleiste oder in den eigenen Favoriten ab.

grammwechsler Alt-Tab. Setzen Sie ein Häkchen vor „Fensterzyklus durch alle Arbeitsflächen“, wenn Alt-Tab auch Fenster anderer virtueller Arbeitsflächen anzeigen soll. Für optimale Darstellung müssen auf der Registerkarte „Komposit“ der Effektkompositor und dessen Transparenz- und Schatteneffekte aktiviert sein.

Der Punkt „Schreibtisch“ eröffnet die Auswahl eines Hintergrundbilds, wobei über „Ordner → Andere“ jeder beliebige Ordner mit eigenen Bildern gewählt werden kann. XFCE kann im Multimonitor-Betrieb für jeden Monitor ein eigenes Bild vergeben und mehr noch: Sogar für virtuelle Desktops ist ein je eigener Hintergrund möglich. Dabei verwenden oder verschieben Sie den „Schreibtisch“ einfach auf oder zum gewünschten Monitor oder virtuellen Desktop. Im Register „Symbole“ legen Sie fest, welche Icons auf dem Schreibtisch zu sehen sind und welche Größe sie besitzen sollen. Sehr nützlich ist es, die Symbolanordnung positionell festzulegen („Symbol Orientierung“), weil die Symbole dann am Desktop mit Rechtsklick und „Schreibtischsymbole anordnen“ jederzeit wieder in Reih und Glied stehen. Diese Aktion berücksichtigt auch selbst angelegte Ordner, Dateien, Verknüpfungen. Das Register „Menüs“ ist ebenfalls von Interesse, insbesondere der Abschnitt „Fensterliste“: Die Option, beim Mittelklick (Mausrad) die Fensterliste inklusive virtuelle Desktops anzuzeigen, ermöglicht eine sehr effiziente Navigation und Fensterkontrolle beim Einsatz virtueller Arbeitsflächen.

Systemleisten: Die Systemleiste(n) konfigurieren Sie in der Konfigurationszentrale mit dem Punkt „Leiste“ oder nach Rechtsklick auf die Leiste und „Leiste → Leisteneinstellungen“. Mit dem Plus-Symbol rechts oben erstellen Sie eine weitere Leiste, die XFCE vertikal, horizontal oder als freies Desktopelement darstellen kann. Optik und Größe sind unter „Anzeige“ und „Erscheinungsbild“ minutiös zu steuern. Ist die Option „Leiste sperren“ gesetzt, bleibt die Leiste stets an der konfigurierten Position, andernfalls lässt sie sich verschieben. Auf der Registerkarte „Objekte“ lässt sich die Anordnung der Leistenapplets verändern. Das funktioniert im Prinzip auch direkt am Objekt mit „Verschieben“ (auch in andere Leisten), aber für mehrere Verschiebe-Aktionen ist der Leistendialog effizienter.

Über „Hinzufügen“ fügen Sie neue Objekte ein. Falls es sich dabei um Programmstarter („Starter“-Applet) handeln soll, ist der Weg über das Whisker-Menü („Zur Leiste hinzufügen“) die einfachere Alternative.

Leistenprofile: Das nützliche Applet ist im Leistendialog („Sichern und Wiederherstellen“) oder in den „Einstellungen“ zu erreichen und bietet an, eine aktuelle Leistenkonfiguration dauerhaft zu sichern. Außerdem gibt es eine ganze Anzahl von vorgegebenen Leistenarrangements, die sich per Klick wechseln lassen. Das Werkzeug arbeitet auch im Multimonitorbetrieb exakt und zuverlässig.

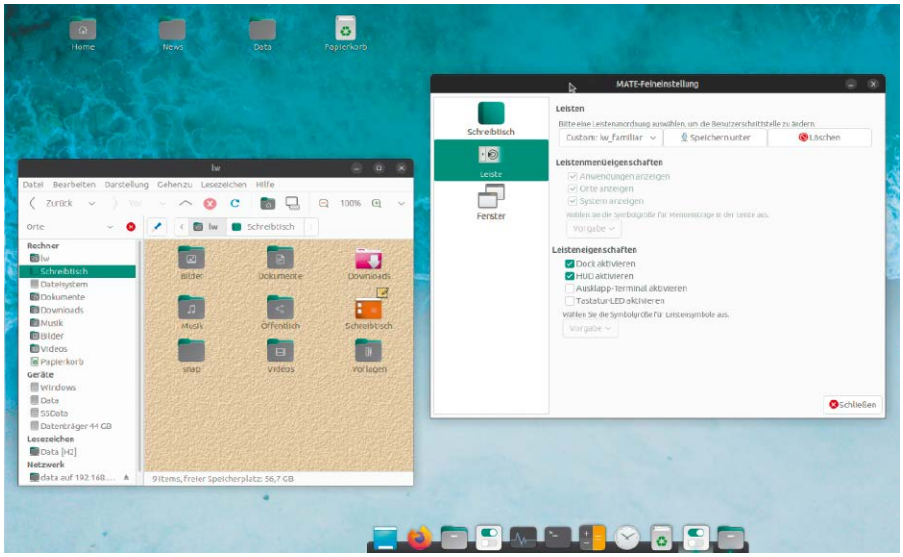
Whisker-Menü: Dieses Leistenapplet ist der schlichten Alternative („Anwendungsmenü“) klar vorzuziehen. Allein das Instant-Search-Suchfeld, das auch die deutschen Programmbeschreibungen berücksichtigt, rechtfertigt diesen Kandidaten. Neben Verlinkungsoptionen zum Desktop und zur Leiste gibt es nach Rechtsklick auf das Menüsymbol und „Eigenschaften“ alle Optionen, um die Größe der Menü- und Kategorien-Einträge sowie Transparenz („Hintergrunddeckkraft“) individuell festlegen. Was Whisker unter „Favoriten“ anzeigt, bestimmen Sie dadurch, dass Sie ein Programm im Menü rechts anklicken und dann die Option „Zu Favoriten hinzufügen“ wählen. Die zusätzliche Option „Menü bearbeiten“ zur inhaltlichen Anpassung von Kategorien und Programmen steht nur zur Verfügung, wenn das zusätzliche Werkzeug Menulibre installiert wurde (mit identischem Paketnamen).

Tastenkombinationen: Eine Übersicht der voreingestellten Hotkeys finden Sie unter „Einstellungen → Tastatur → Tastenkürzel für Anwendungen“. Hier besteht auch die Möglichkeit, eigene Hotkeys zu definieren. Um eine Zuweisung zu ändern, klicken Sie doppelt auf einen Eintrag in der Spalte „Tastenkürzel“ und drücken dann die gewünschte Tastenkombination. Über „Hinzufügen“ definieren Sie eigene Programm-Hotkeys. Es gibt außerdem einen Satz von Tastenkombinationen für die Fenstersteuerung. Deren Konfiguration finden Sie unter „Einstellungen → Fensterverwaltung → Tastatur“. Die voreingestellten Hotkeys folgen den üblichen Standards, beispielsweise Alt-Tab für „Fenster durchwechseln“ und Alt-F4 für „Fenster schließen“. ■

Mate: Spezialitäten inklusive

Der Mate-Desktop hat keine Eigenschaften, die ihn für eine bestimmte Zielgruppe als alternativlos auszeichnen würde. Die Oberfläche ist aber einerseits unkompliziert und anpassungsfähig und bietet zudem einige Spezialitäten.

VON HERMANN APFELBÖCK



Mate ist – deutlicher als Cinnamon – eine Weiterentwicklung der alten Gnome-2-Basis. Das wird überdeutlich bei nachinstalliertem Mate-Desktop, der mit seinen beiden horizontalen Systemleisten einem Gnome-Flashback (Retro-Paket für Gnome) täuschend ähnelt. Bei Distributionen mit Mate wird dies weniger deutlich, weil diese schon in die Desktopanpassung investieren. Denn Mate ist ausgesprochen wandlungsfähig und nach einigen Optimierungen optisch zwischen XFCE und Cinnamon einzuordnen.

Mate ist ein unkomplizierter Desktop für alle Einsatzzwecke. Die Anpassungen fallen hier fast immer objektorientiert und oft intuitiver aus als anderswo. Ressourcentechnisch liegt Mate dort, wie es der optische Eindruck nahelegt – zwischen XFCE und Cinnamon. Je nach Speicherausstattung etwa 600 MB aufwärts fordert der Mate-Desktop plus System ab Anmeldung. Die Anforderungen an CPU und Grafik erfüllt jede ältere Hardware der letzten zehn Jahre.

Distributionen und Pakete

Mate ist fast für jede Distribution als optionales Flavour bei der Installation zu haben. Als Standarddesktop dient er aber nur selten: Die bekanntesten Distributionen mit Mate-Desktop sind Ubuntu Mate und Parrot-OS. Wenn das System bereits vorliegt und Mate nachgerüstet werden soll, finden sich in jedem Repository Pakete unterschiedlicher Größe. Eine Suche etwa mit Synaptic kann verwirren, weil sich unter die Paketvarianten auch Dummypakete mischen, die nur auf andere verweisen. Nach unserer Erfahrung sind außerhalb des Ubuntu-Biotops die Pakete „mate-desktop-environment-core“ (genügt als Desktop) oder „mate-desktop-environment“ zu empfehlen. Für Ubuntu-Systeme sind die Pakete „ubuntu-mate-core“ (genügt als Desktop) und „ubuntu-mate-desktop“ die zwar deutlich umfangreichere, aber dennoch die bessere und aktuellere Wahl.

Konzept und Funktionsumfang

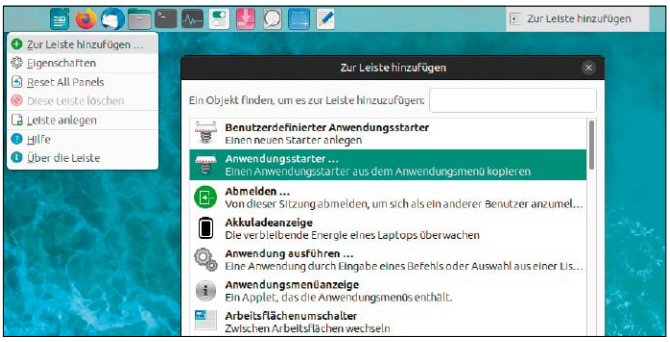
Dem alten Gnome 2 folgend, ist Mate ein konservativer Desktop mit Hauptmenü, zwei Systemleisten und einem offenen Desktop für Standardsymbole, Ordner, Dateien, Programmstarter. Wie bei jedem größeren Linux-Desktop gibt es eine Konfigurationszentrale, die sich hier „Steuerzentrale“ nennt (mate-control-center). Hier sind die typischen Applets zur Geräteeinrichtung, Systemaktualisierung, Benutzerverwaltung oder Sprachunterstützung zu finden. Die Steuerzentrale verlinkt aber auch externe Tools wie „Laufwerke“, „Mate Tweak“ oder die Einstellungen für das Plank-Favoritendock.

Der Punkt „Erscheinungsbild“ (mate-appearance-properties) zur optischen Anpassung ist vorbildlich und klarer als etwa bei Cinnamon. Die wichtigsten Desktopanpassungen können unter Mate praktisch durchgängig intuitiv über Kontextmenüs an den Elementen erledigt werden. So verzichtet Mate auch komplett auf ein eigenes Programm zur Leistenkonfiguration und erledigt alles direkt am Objekt.

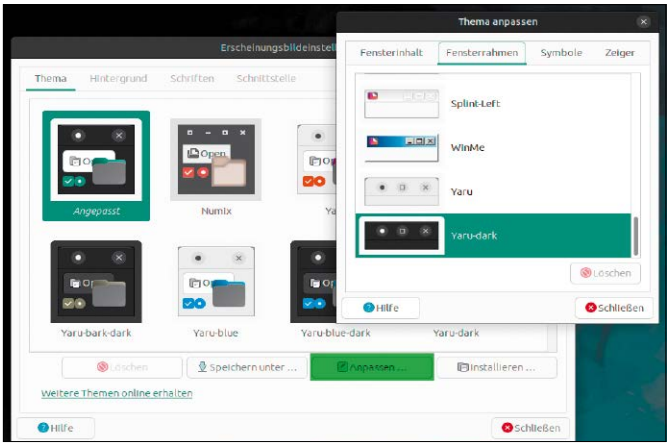
Das Tool „Mate Tweak“ (unter Ubuntu Mate auch im Willkommen-Dialog integriert) beherrscht einen fundamentalen Wechsel der

Leistenkonfiguration, wobei je nach Stil bei Bedarf das externe Plank-Dock integriert wird. Das ist keine Zauberei, aber auch nicht ganz trivial, funktioniert aber tadellos. Das sonstige Mate-Zubehör folgt weitgehend den Gnome-Standards. Die meisten Extras bietet der Nautilus-Fork Caja: Der Dateimanager hat diverse Auszeichnungsmöglichkeiten für Dateiobjekte und eine wandlungsfähige Navigationsleiste.

Der Mate-Desktop unter Ubuntu Mate bietet standardmäßig neben der ordentlichen Benutzeranmeldung eine Gastsitzung, die alle Aktionen wieder verwirft. Das kann praktisch sein, um Webaktionen ohne Dateireste und Protokollierung in einem temporären Konto zu absolvieren.



Systemleisten bestücken: Nach Rechtsklick auf eine freie Leistenstelle starten Sie den Konfigurationsdialog „Zur Leiste hinzufügen“.



Themes bringen andere Farb- und Iconthemen auf den Mate-Desktop. Feineinstellungen für Fensterinhalt und Fensterrahmen gibt es unter „Anpassen“.

Nützliche Mate-Anpassungen

„Mate Tweak“: Das schon erwähnte Tool ist mehr als nur ein Zusatztool, denn es ist für die Leistenarrangements und für die Standards der Schreibtischsymbole zuständig. Bei Mate-Nachinstallationen ist es nicht immer dabei und sollte dann mit

```
sudo apt install mate-tweak
```

nachgerüstet werden. Eine der frühesten Anpassungen unter Mate sollte die gewünschte Leistenanordnung sein, weil sich mit einem Leistendesign wie „Cupertino“ oder „Pantheon“ (beide mit Plank-Dock) eine andere Optik und Bedienung ergibt. Bestehende und bereits optimierte Leisten lassen sich mit „Speichern unter“ als benutzerdefiniertes Leistendesign sichern.

Hauptmenü: Bei manuell installiertem Mate sind als Menüapplets eventuell nur spartanische Menüs verfügbar („Klassisches Menü“). Jüngerer Standard und unbedingt zu empfehlen ist das Brisk-Menü. Das ist ebenfalls vergleichsweise einfach, hat aber ein Suchfeld und wechselt die Kategorien per Mouse-over (ohne Klick). Mit

```
sudo apt install mate-applet-brisk-menu
```

kann es nachinstalliert werden und ist nach Neuanmeldung einbaufähig.

Leistenkonfiguration: Systemleisten sind an allen vier Bildschirmrändern möglich. Alle optischen und inhaltlichen Optionen stehen nach Rechtsklick auf eine freie Leistenstelle über die Optionen „Zur Leiste hinzufügen“ und „Eigenschaften“ bereit. Ein neue Leiste erstellen Sie ebenfalls mit Rechtsklick auf eine bereits bestehende, indem Sie „Leiste anlegen“ wählen. Der kleine Dialog „Eigenschaften“ bietet alles zur Positionierung und Größe, zum Ausblendverhalten und zur optischen Verfeinerung. Leistenmodule lassen sich nach Rechtsklick verschieben, sofern das Modul nicht gesperrt ist (Option „Auf der Leiste sperren“). Die weitere Kontextoption „Aus der Leiste entfernen“ beseitigt ein unnötiges Element.

In der Systemleiste zu empfehlen sind die Applets „Brisk-Menü“, „Fensterliste“, „Benachrichtigungsfeld“ (mit Netzwerk, Lautstärke, Sitzungsverwaltung) und „Anwendungsstarter“: Letzterer erlaubt bequemes Anlegen einer Favoritensammlung. Zur späteren Erweiterung dieser Sammlung verwenden Sie „Zur Leiste hinzufügen“ und „Anwendungsstarter“ erneut, übernehmen das gewünschte Programm und „Verschieben“ dessen Icon dann zu den bestehenden. Wer ein Leistenlayout mit Plank-Dock verwendet, hat es noch ein Stück bequemer.

Optik- und Themenanpassungen sind in der Steuerzentrale unter „Erscheinungsbild → Thema“ kompakt versammelt. Die wichtige Schaltfläche „Anpassen“ erlaubt für jedes Schema Feineinstellungen zum Stil der Programmfenster („Fensterinhalt“) und der Titelleisten („Fensterrahmen“).

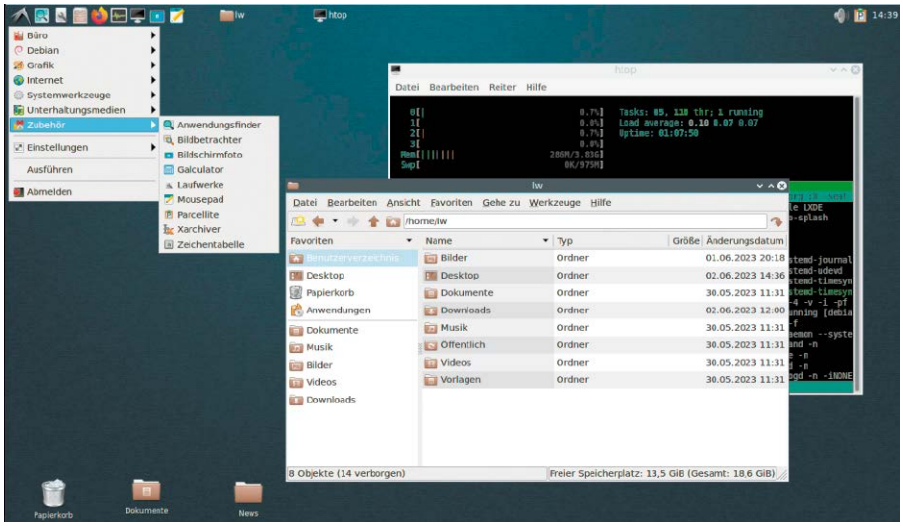
Desktop als Dateiablage: Mate versteht den Desktop als klassische Dateiablage. Der Rechtsklick am Desktop zeigt daher die Optionen „Ordner anlegen“ und „Starter anlegen“. Für Programmstarter genügt ein Name und der Programmbefehl. Das passende Symbol holt sich Mate automatisch. Zur Ausrichtung der Desktopsymbole verwenden Sie nach Rechtsklick die Option „Anordnung fixieren“. Wie fast jeder Desktop-Linux zeigt Mate nach Rechtsklick das Angebot „Hintergrund des Schreibtischs ändern“.

Dateimanager: Caja kann Dateiobjekte durch Farbe und Symbole hervorheben. Mehr noch: Er kann auch den Ordnerhintergrund verändern. Voraussetzung ist die Symbolansicht („Ansicht → Symbole“) oder die Kompaktansicht. Zum Ändern des Hintergrunds wählen Sie „Bearbeiten → Hintergründe und Symbole“ und ziehen ein Muster oder eine Farbe auf den Ordner. Um den Standard wiederherzustellen, ziehen Sie den Eintrag „Zurücksetzen“.

Cajas Navigationsspalte zeigt unter anderem die Option „Notizen“, die sich auf den aktuellen Ordner bezieht. Das eröffnet die Möglichkeit, Zusatzinformationen über den Inhalt von Verzeichnissen abzulegen. Wenn für einen Ordner „Notizen“ existieren, erscheint über der Navigationsspalte ein kleines Symbol. ■

Der kleine Desktop LXDE

An LXDE („Lightweight X11 Desktop Environment“) ist nichts Aufregendes oder Spannendes. Trotzdem hat dieser brave Desktop seine Rolle auf Platinen, Servern und Altgeräten, weil er maximal unkompliziert und überall verfügbar ist.



VON HERMANN APFELBÖCK

Obwohl mit LXQT längst ein Nachfolger feststeht, wird der LXDE-Desktop erfreulicherweise weiterentwickelt. LXDE (*www.lxde.org*) ist ein Oldie und basiert auf der alten Gnome-Version 2, die schon vor 12 Jahren durch Gnome 3 abgelöst wurde. Der Desktop stellt daher keinerlei Ansprüche an CPU und Grafikchip und ist mit 250 bis 300 MB RAM-Bedarf am Start (inklusive System und Dienste). Dies kann zwar so mancher Minidesktop wie Fluxbox, Moksha oder Trinity noch locker unterbieten, aber LXDE hat gegenüber solchen Kandidaten klare Vorzüge: Er ist so einfach zu benutzen, wie es ein einfacher Desktop sein sollte, und er ist überall als Softwarepaket verfügbar.

Auf moderner Hardware werden – trotz klarer und mit etwas Anpassung ansprechender Optik – nur ganz trockene Pragmatiker ein LXDE einsetzen wollen. Der Desktop ist aber ideal zum Wiederbeleben alter Notebooks mit zwei bis vier GB RAM. Außerdem eignet er sich hervorragend als Starter und Lieferant grafischer Programme auf kleinen Linux-Servern, die sonst überwiegend per SSH und ohne Monitor und Tastatur verwaltet werden: Es ist einfach angenehmer, Laufwerke mit einem Gnome-Disk zu verwalten oder Konfigurationsdateien mit einem grafischen Mousepad zu bearbeiten als mit Terminaleditoren wie Nano. Der Headless-Betrieb ist ja weiter möglich, weil SSH auch grafische Fenster vermittelt.

Distributionen und Pakete

Als Standarddesktop dient LXDE nur noch beim Livesystem Knoppix (*www.knopper.net/knoppix-mirrors*) und beim kleinen Ubuntu-Derivat LXLE (*www.lxle.net*). Bei den namhaften Distributionen Debian, Fedora und Open Suse ist der Desktop immerhin noch als Option beim Netinstaller vorgesehen.

Auf die Desktopvorgabe von Distributionen ist man aber nicht angewiesen: LXDE ist nach wie vor bestens etabliert und daher in allen Paketquellen als nachinstallierbare Software verfügbar. Um nur den LXDE-Desktop als alternative Oberfläche zu verwenden, genügt das kleine Metapaket „lxde-core“. Handelt es sich bislang um ein Headless-Serversystem ohne Oberfläche, dann ist die komplette Desktopumgebung zu empfehlen, um wenigstens schon mal die grafischen Basisprogramme (Dateimanager, Terminalemulator, Editor) zu erhalten:

```
sudo apt install lxde
```

Das noch deutlich umfangreichere Metapaket „lubuntu-desktop“ ist nicht geeignet, weil es schon seit Jahren den immer noch relativ schlanken, aber eben doch anspruchsvolleren LXQT-Desktop mitbringt.

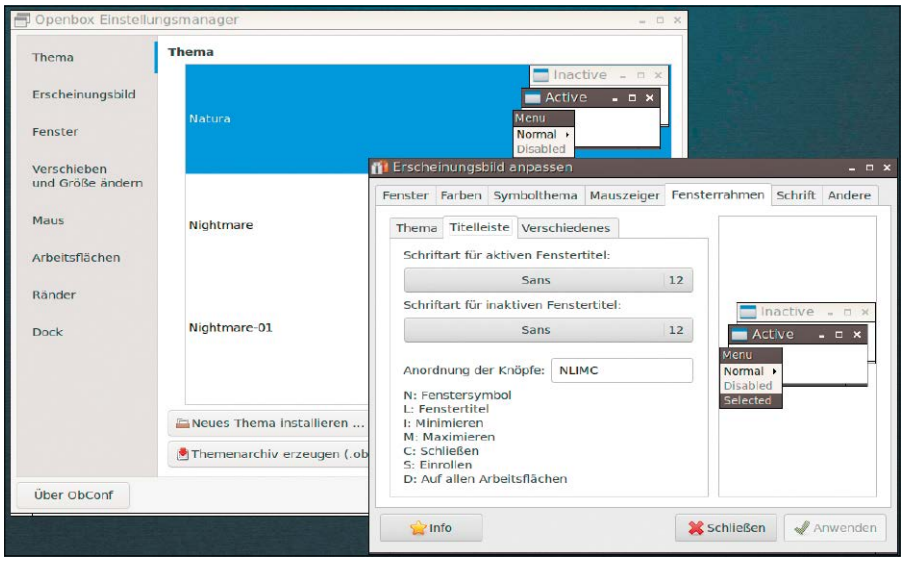
Konzept und Funktionsumfang

Die LXDE-Oberfläche kommt mit wenigen Elementen aus: Das Lxpanel liefert eine typische Systemleiste mit Appletmodulen. Standard sind hier Applets für das Hauptmenü, den Favoritenstarter, die Fensterliste sowie die üblichen Systemcontrols für Lautstärke, Netzwerk und Uhrzeit. Lxappearance („Erscheinungsbild anpassen“) ist die wesentliche Konfigurationszentrale, um die Fensteroptik oder das Iconthema umzustellen. Daneben gibt es noch Obconf, den „Openbox Einstellungsmanager“, der das Aussehen der Titelleisten, Fensterfokus und die virtuellen Arbeitsflächen definiert. Diese Trennung in zwei Tools ergibt sich zwangsläufig, weil der Fenstermanager Openbox unter LXDE als Leihgabe arbeitet. Die LXDE-Arbeitsfläche dient als offene Ablage für Dateien, Ordner und Verknüpfungen, wofür der LXDE-Dateimanager Pcmanfm verantwortlich ist. Auch das Kon-

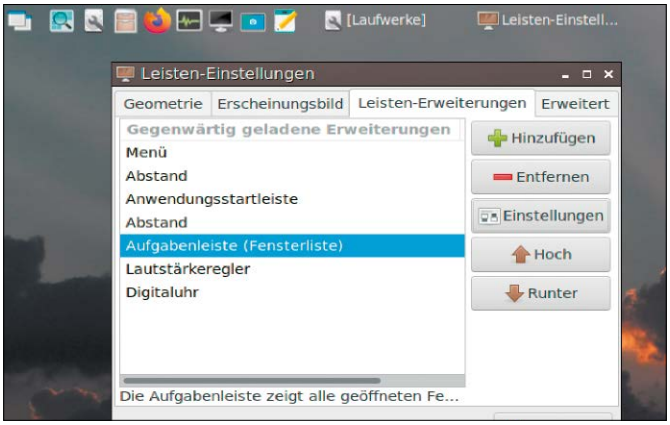
textmenü „Desktop-Einstellungen“, das die Schreibtischsymbole und das Hintergrundbild definiert, liefert dieser Dateimanager.
Im einfachen Hauptmenü gibt es unter „Einstellungen“ die typischen Systemtools der Benutzerverwaltung (users-admin), Bildschirmkonfiguration (lxrandr) oder Autostart-Kontrolle (lxsession-edit). Hier geht es optisch etwas schlichter zu als bei großen Desktops, aber funktional sind diese grafischen Werkzeuge völlig zufriedenstellend.

Anpassungen am LXDE-Desktop

Die **Systemleiste** ist nach intuitivem Rechtsklick optisch wie inhaltlich gut anpassbar und beliebig zu positionieren („Leisten-Einstellungen → Geometrie“). Dabei gelingen Leistenanpassungen im Vergleich zu XFCE oder Mate sogar einfacher, insbesondere bei vertikaler Anordnung. Transparenz ist im Register „Erscheinungsbild“ zu erreichen, indem eine „Durchgehende Farbe“ ohne „Deckkraft“ (0) gewählt wird. Bei der Leistengröße kann sowohl die der Leiste selbst als auch die der enthaltenen Icons eingestellt werden.
Beim Angebot der Leistenapplets („Leisten-Erweiterungen → Hinzufügen“) beschränkt sich LXDE auf Klassiker, die zum Großteil auch schon standardmäßig aktiviert sind. Theoretisch sind alle Applets optional und lassen sich auch „Entfernen“. Als notwendige Desktopstandards sind aber „Menü“, „Anwendungsstartleiste“ und „Fensterliste“ zu empfehlen. Je nach Nutzung kann sich der zusätzliche „Desktop-Pager“ für virtuelle Arbeitsflächen lohnen, auf Notebooks der „Akku-Monitor“. Um Applets visuell zu trennen, gibt es ein Applet „Abstand“, das sich pixelgenau dehnen lässt.
Das Menüapplet ist ein schlichter, einfacher Programmstarter mit gliedernden Kategorien. Elegantere Alternativen gibt es nicht. Wer im Hauptmenü zumindest ein Suchfeld erwartet, kann das XFCE-Tool xfce4-appfinder nachinstallieren und an die erste Stelle der „Anwendungsstartleiste“ platzieren (und später eventuell auf das LXDE-Menü-Applet ganz verzichten).
Das Leistenapplet, das in jedem Fall individuelle Anpassung verdient, ist die eben angesprochene „Anwendungsstartleiste“ für die Programmfavoriten. Nach Rechtsklick darauf und „Anwendungsstartleiste-Einstellungen“ erhalten Sie die Liste aller Programme und können die gewünschten mit „Hinzufügen“ eintragen. Die Reihenfolge der Icons ist mit „Hoch“ und „Runter“ leicht zu optimieren.



Lxappearance und Obconf enthalten zum Teil identische Angebote. Nehmen Sie zur Optikanpassung das LXDE-Werkzeug. Den Openbox-Manager brauchen Sie nur für spezielle Fensteroptionen.



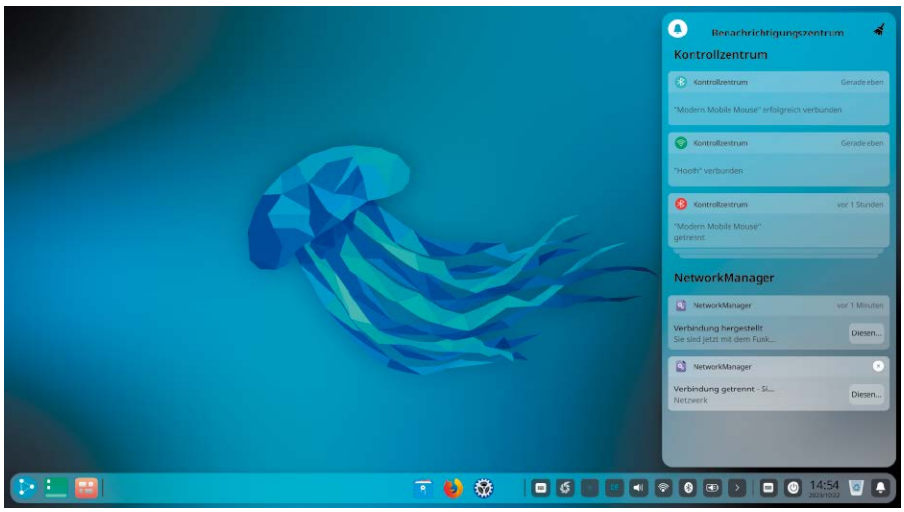
LXDE-Systemleiste: Das Anpassen der Leiste gelingt beim LXDE-Desktop intuitiv. Das Appletangebot bleibt zwar begrenzt, enthält aber alles Wesentliche.

Für das **allgemeine Erscheinungsbild** sind die genannten Werkzeuge Lxappearance und Obconf zuständig und dabei zum Teil redundant. Das LXDE-Tool Lxappearance („Erscheinungsbild anpassen“) integriert unter „Fensterrahmen“ die Themen, die der Fenstermanager Openbox anbietet. Diese Einstellung betrifft die Farben der Titelleisten und das Aussehen der Klick-Controls. Eine sachliche Empfehlung für die Fensterrahmen sind die Themen „Breeze-ob“ oder „Natura“. Wer die Titelleisten größer und griffiger haben will, kann im Unterpunkt „Titelleiste“ größere Schriften vergeben. Dies erzwingt dann größere Titelleisten. Diese Anpassungen sind ebenso mit Obconf („Openbox Einstellungsmanager“) zu erreichen. Wirklich notwendig wird Obconf nur für einige Feinheiten des Fensterverhaltens, etwa wann diese den Eingabefokus erhalten (Punkt „Maus“), wie neue Fenster platziert werden (Punkt „Fenster“) und wie viele virtuelle Desktops angeboten werden (Punkt „Arbeitsflächen“).
Das **Aussehen des Desktops** im engeren Sinn, also der Arbeitsfläche, ist über „Einstellungen → Desktop-Einstellungen“ oder einfacher mit Rechtsklick am Desktop zu bestimmen. Das LXDE-Angebot beschränkt sich auf die Auswahl des Hintergrundbildes, die Vorgabe weniger Standardicons und eine Option unter „Erweitert“, die beim Rechtsklick am Desktop das Openbox-Mini-Menü öffnet. Diese Option ist kaum zu empfehlen, weil damit die normale Rechtsklick-Funktion am Desktop verlorengeht. ■

Deepin: Der schönste Desktop?

Das „Deepin Desktop Environment“ (DDE) zählt aktuell wohl zu den optisch ansprechendsten Oberflächen für Linux-Systeme. Wir erklären dessen Installation und stellen den Desktop vor.

VON STEPHAN LAMPRECHT



Der Deepin-Desktop hat viele Anleihen von Windows 11 und vor allem Mac-OS. Das zeigt sich auch an der zentralen Rolle des Docks.

Dass eine ansprechende Gestaltung der Benutzeroberfläche mehr ist als Zuckerwerk für die Augen, wusste bereits Steve Jobs. Wer viele Stunden mit einem System zubringt, möchte auch visuell angesprochen werden. Eine attraktive Oberfläche ist das Deepin Desktop Environment (DDE) – eigentlich die Benutzerschnittstelle für Deepin Linux. Da Deepin wird von einer chinesischen Firma entwickelt wird, steht schnell die rufschädigende Diskussion im Raum, dass hier Daten abgezogen werden. Der immanente Vorwurf lautet, dass die Distribution genau deswegen so schick aussieht, um möglichst viele Nutzerinnen und Nutzer zur Installation zu bewegen, um anschließend möglichst viele Daten absaugen zu können. Wer mit Deepin trotzdem arbeiten will, kann dies auch, ohne die chinesische Distribution installieren zu müssen.

Deepin unter Ubuntu installieren

Für alle Ubuntu-basierten Distributionen ist die Installation der Umgebung einfach. Im Web finden Sie vermutlich verschiedene Angaben zu einer Paketquelle. Einige davon funktionieren aber anscheinend nicht mehr. Das nachfolgende Repository funktioniert aber problemlos:

```
sudo add-apt-repository
  ppa:ubuntudde-dev/stable
sudo apt update
sudo apt install ubuntudde-dde
```

Damit fügen Sie die Paketquelle hinzu, aktualisieren die Paketverwaltung und beginnen die Installation. Im Laufe der Einrichtung werden Sie dazu aufgefordert, sich für einen Fenstermanager zu entscheiden, der als Standard verwendet werden soll. Wählen Sie unter Ubuntu am besten „gdm3“ aus. Der ist dort Standard und erspart weitere Konfigurationsarbeiten.

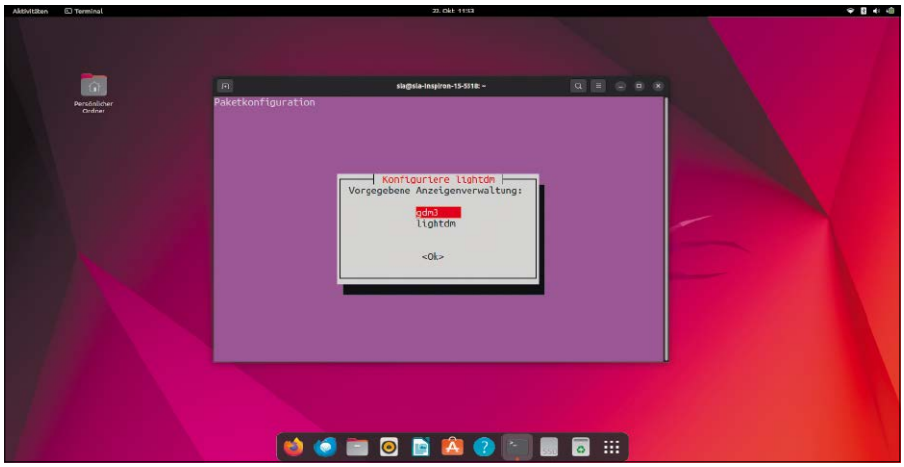
Danach setzt die Installationsroutine die Arbeit fort. Starten Sie danach den Rechner einmal komplett neu. Danach steht Ihnen der neue Desktop zur Verfügung. Auf der Anmeldeseite befindet sich am unteren Ende ein Zahnradsymbol. Mit einem Klick wechseln Sie dort zwischen parallel installierten Oberflächen, hier also für Deepin. Bei der Anmeldung gibt es eine Einschränkung, die für die meisten keine ist: Deepin unterstützt keine Anmeldung per Fingerabdruck. Ihr System verhält sich also korrekt, wenn diese Option verschwindet. Wechseln Sie zum Standarddesktop von Ubuntu zurück, ist die Option wieder zurück.

Ein Mix aus Windows 11 und Mac-OS

Wer sich auf dem Desktop umschaut, erkennt unschwer die Inspirationsquellen. Zu Deepin gehören Stilelemente aus Windows 11 und der Apple-Welt. Am unteren Rand des Bildschirms dominiert ein Dock (oder Startleiste), auf der die Icons der laufenden Anwendungen wie unter Windows 11 zentriert sind. Die ersten drei Schalter ermöglichen den Zugriff auf die installierten Anwendungen, blenden den Desktop ein oder wechseln zu einer Exposé-Ansicht aller laufenden Programme und Fenster. Eine Besonderheit ist die Touchtastatur, die Sie über das entsprechende Icon auf der rechten Seite der Leiste aufrufen. Links davon sind die Icons von Minianwendungen angeordnet, über die Sie das WLAN aktivieren, dessen Verbindung wechseln oder Verbindungen zu Bluetooth-Geräten herstellen.

Das zentrale Bedienelement des Desktops ist wie unter Mac-OS das Dock am unteren

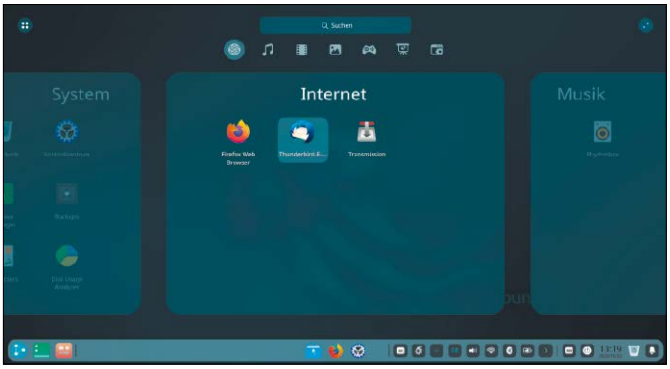
Bildschirmrand. Es kennt zwei Betriebsarten: Der „Design-Modus“ nutzt eine andere Bildsprache und legt den Fokus auf opulente grafische Gestaltung. Das kostet natürlich auch Ressourcen. Deswegen gibt es auch einen „Leistungs-Modus“, der weniger verschwenderisch mit Icons und Effekten umgeht. Zwischen beiden wechseln Sie mit einem Rechtsklick auf das Dock und der Auswahl von „Modus“ aus dem Kontextmenü. Die Größe und das Verhalten des zentralen Elements verändern Sie am besten über die „Dock-Einstellungen“, die ebenfalls via Kontextmenü zu erreichen sind. Der nachfolgende Dialog ist typisch für Deepin: Die Programmfenster und Dialoge nutzen abgerundete Ecken, wie sie unter Mac-OS Standard sind. Über den „Pluginbereich“ in der rechten unteren Ecke können Sie auch die Zahl der angezeigten Elemente reduzieren. Optional wechseln Sie zwischen einer permanenten Darstellung oder dem automatisierten („intelligenten“) Ausblenden.



Während der Installation werden Sie nach dem Fenstermanager (Anmeldefenster) gefragt. Bleiben Sie am besten beim vorhandenen Fenstermanager – unter Ubuntu ist „gdm“ der Standard.

Das Startmenü kann mehr

Das Startmenü ist vielseitiger, als es zunächst den Anschein hat. Die klassische Ansicht präsentiert die Anwendungen als einfaches Menü. Der Launcher kennt ebenfalls verschiedene Modi. Klicken Sie darauf, sehen Sie in der rechten oberen Ecke des Dialogs einen Doppelpfeil. Damit vergrößert sich die Ansicht und die Programmicons werden wie unter Gnome oder auf dem Mac bildschirmfüllend präsentiert. Wenn Sie in dieser Ansicht in die linke obere Ecke klicken, sind die Programme nach Kategorien sortiert. Mit einem Klick in der rechten oberen Ecke kehren Sie zur klassischen Ansicht zurück.



Das Startmenü im Dock kann mehr als nur ein Menü darstellen. Mit einem Mausklick rufen Sie eine Ansicht wie das Launchpad auf dem Mac auf.

Deepin anpassen

Im Dock erreichen Sie mit einem Klick auf das Zahnrad das Gnome-ähnliche Kontrollzentrum zur Anpassung vieler Optionen. Unter „Personalisierung“ nehmen Sie Einfluss auf die Gestaltung durch den Wechsel des Themes. Sie möchten stärkere Transparenz oder weniger gerundete Fensterecken? Dann nutzen Sie einfach die Schieberegler dort. Das Kontrollzentrum ermöglicht über „Standardanwendungen“ auch, das von Ihnen bevorzugte Terminal, Mailprogramm oder den Browser auszuwählen. Die vielen Soundeffekte, die jede Systemmeldung untermalen, werden den einen oder anderen Nutzer stören, und unter „Ton“ legen Sie für jeden Effekt einen individuellen Klang fest.

Deepin bringt Abwechslung auf die Arbeitsfläche, sieht schön aus und arbeitet auf halbwegs aktuellen Rechnern flott. Wer eine Gnome-Alternative sucht und nicht auf KDE ausweichen will, findet auch hier genügend „Eye Candy“. Wenn Ihnen die Arbeit mit Deepin trotzdem nicht gefällt, können Sie den Desktop recht unkompliziert entfernen. Sofern Sie bei der Auswahl des Fenstermanagers „lightdm“ gewählt hatten, müssen Sie aber zunächst „gdm3“ wieder als Displaymanager aktivieren. Das erledigen Sie mittels

```
sudo dpkg-reconfigure lightdm
```

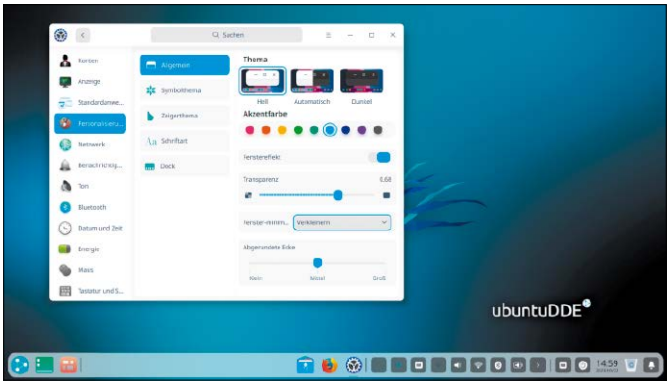
und Auswahl von „gdm3“. Danach führen Sie die Befehle

```
sudo apt remove startdde ubuntudde-dde
sudo apt autoremove
```

aus. Zusätzlich können Sie auch die Paketquelle mittels

```
sudo add-apt-repository –remove ppa:ubuntudde-dev/stable
```

wieder entfernen. ■



Im Kontrollzentrum haben Sie Zugriff auf viele Systemoptionen, visuelle Effekte und Fensterdekorationen und legen bevorzugte Anwendungen fest.

Fernwartung mit SSH

Dieser Heftschwerpunkt mit dem Thema Homeserver bringt Grundlagen und die wichtigsten Einsatzbeispiele für Linux-Systeme im Heimnetz und Intranet. Aufgrund der herausragenden Bedeutung starten wir hier mit der Fernwartung mit SSH.

VON HERMANN APFELBÖCK

In privaten Netzen und Kleinbetrieben, wo komplizierte Rechteregeln ganz oder teilweise entfallen können, sind Daten-, Web- und Streamingserver mit Linux schnell eingerichtet. Und angesichts geringer Benutzerzahlen genügen als Hardware kostengünstige Platinenrechner oder ausrangierte Notebooks.

Das Special zeigt die wichtigsten Rollen für Linux-Homeserver und beschränkt sich dabei auf den Betrieb im heimischen Netzwerk. Das sicherheitskritische Thema der Internetfreigabe, die heimische Serverdienste für das World Wide Web öffnet, bleibt außen vor. Dafür legen wir fundierte Grundlagen für die Einrichtung von (Apache-)Webdiensten und Datenservern mit Samba.

Den Beginn macht der stets unentbehrliche Serverdienst Open SSH, der nicht nur zur Fernwartung dient, sondern auch unkomplizierten Datenaustausch und Softwareverteilung ermöglicht.

1. SSH: Weit mehr als nur Fernwartung

SSH, die „Secure Shell", ist zuverlässig, schnell, sicher und multifunktional. Kein Server, auch wenn seine Hauptaufgabe woanders liegt, sollte auf diesen Dienst verzichten. Wenn nur oder hauptsächlich Linux-Systeme kommunizieren, stellt sich eher die umgekehrte Frage, ob SSH nicht manchen anderen Dienst überflüssig macht. Ein SSH-Server ist letztlich für jedes Linux zu empfehlen – auch auf dem Desktop. Immerhin erfüllt SSH gleich drei Aufgaben:

1. Man erhält im Fernzugriff das voll funktionsfähige Terminal des „Servers" inklusive der dort geltenden Konfiguration (Aliases, Variablen, Prompt et cetera) und allen dort installierten Terminalprogrammen (Htop, Midnight Commander, Inxi et cetera).

2. SSH verwendet sein eigenes Dateiübertragungsprotokoll SFTP (das mit FTP und FTPS nichts zu tun hat). Da alle grafischen Linux-Dateimanager dieses Protokoll beherrschen, eröffnet dies den unkomplizierten Datenaustausch am Desktop. Freigaben sind nicht nötig: Jeder Benutzer, der ein Systemkonto auf dem Server besitzt, darf beim Fernzugriff via Dateimanager genau das, wozu er auch direkt am Server mit seinem Konto berechtigt wäre.

3. SSH erlaubt via X11-Forwarding den Start grafischer Programme der „Server", die beim zugreifenden Netzwerkclient angezeigt und dort uneingeschränkt (eventuell etwas zäher) genutzt werden können. Das ist attraktiv für Anwender, die sich in einer grafischen Konfigurationszentrale wohler fühlen als in den Konfigurationsdateien eine Ebene darunter. Es ermöglicht aber auch die Verteilung von Software, weil dann nicht jedes Programm und Tool auf jedem System installiert sein muss.

2. SSH: Einrichtung am Server

Auf Serverseite ist die einzige Voraussetzung für den SSH-Zugriff ein laufender Open-SSH-Server. Wenn Sie sich von vornherein für ein Serversystem entschieden haben, ist SSH in der Regel schon vorinstalliert und aktiv. Im Zweifel lässt sich dies mit

```
service ssh status
```

abfragen. Ist der SSH-Server noch nicht installiert, holen Sie das unter Debian/Ubuntu-Systemen mit diesem Kommando nach:

```
sudo apt install openssh-server
```

Nach erfolgter Installation ist der SSH-Server sofort mit Standardeinstellungen aktiv.

Exkurs zur SSH-Konfiguration: Die Standardkonfiguration ist sinnvoll und benötigt keine dringende Anpassung. Einsteiger tun gut daran, diese Standards erst mal zu belassen, da Änderungen die Komplexität erhöhen.

Trotzdem ist es gut zu wissen, woher der SSH-Server seine Einstellungen bezieht. Es handelt sich um die Konfigurationsdatei „/etc/ssh/sshd_config", welche die Standards auskommentiert mit „#" anzeigt. Nach

Entfernen dieses Kommentarzeichens können Sie die Voreinstellung ändern. Die vielleicht interessanteste Änderung auch für weniger Erfahrene ist die Korrektur des Standards „#X11Forwarding no“:

```
X11Forwarding yes
```

Dies eröffnet den Fernstart grafischer Programme, wie später für die zugreifende Clientseite noch genauer erklärt wird. Die meisten weiteren Zeilen dienen in erster Linie dazu, die Sicherheitsstandards zu erhöhen oder zu senken. Zum Beispiel verhindert der Standard

```
#PermitRootLogin prohibit-password
```

eine Anmeldung des root-Kontos mit Passwort (eine Schlüsselanmeldung von root ist hingegen erlaubt). Im Heimnetz ist eine Lockerung zu

```
PermitRootLogin yes
```

vertretbar und vereinfacht viele Administrationsaufgaben. Änderungen an der Datei „/etc/ssh/sshd_config“ werden nach einem Systemneustart oder nach manuellem Neustart des Dienstes mit

```
sudo service ssh restart
```

gültig.

3. SSH-Terminal: Linux/Mac-OS als Client

Die Client-Komponente für den Zugriff auf SSH-Server ist auf allen Linux-Systemen und unter Mac-OS X standardmäßig vorinstalliert. Im Terminal und mit dem Tool ssh kommen Sie daher ohne Umschweife an den SSH-Server. Alles was Sie brauchen, ist ein Systemkonto auf dem Server und dessen Kennwort, ferner wahlweise die IP-Adresse oder den Hostnamen:

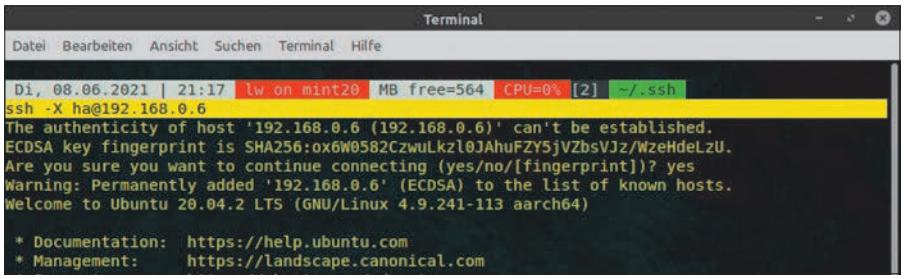
```
ssh ha@192.168.178.20
ssh ha@raspberry
```

Das Kennwort wird abgefragt. Wenn Sie mit

```
ssh 192.168.178.20
```

kein Konto angeben, wird erst das Konto und danach dessen Kennwort abgefragt. Beim allerersten Zugriff ist dem Clientsystem der Server noch nicht bekannt und Sie müssen die Verbindung mit „yes“ bestätigen. Künftig entfällt diese Abfrage, weil der Fingerabdruck des Servers auf dem Clientsystem unter „~/.ssh/known_hosts“ gespeichert wird.

Anmerkung: Die Datei „~/.ssh/known_hosts“ sollten Sie kennen, weil es nach Änderungen am Serversystem nötig werden kann, sie einfach zu löschen. Der SSH-Client interpretiert nämlich geänderte Servereinstellungen (mit dadurch geänderten Fingerprint) als mögliches Sicherheitsrisiko und verweigert den Zugang. Nach Löschen der Datei gilt der Server wieder als unverdächtiger Neuling, und nach Bestätigung mit „yes“ wird die Datei „known_hosts neu“ angelegt.



Erstanmeldung mit SSH: Der dem Clientsystem noch unbekannte Server muss mit „yes“ explizit akzeptiert werden und wird dann in die Liste der Server aufgenommen („~/.ssh/known_hosts“).

Über SSH arbeiten Sie auf dem entfernten System genauso wie im lokalen Terminal jedes Linux-Systems. Sie bearbeiten Konfigurationsdateien, installieren Programme oder versorgen das System mit Updates:

```
nano ~/.bashrc
sudo apt install mc
sudo apt update & apt upgrade
```

Diese klassische SSH-Fernwartung bleibt Terminalarbeit und fordert Terminal-Know-how, lässt sich aber immerhin durch pseudografische Werkzeuge wie Midnight Commander, Htop oder Ncdu vereinfachen. Weitere komfortable SSH-Optionen beschreiben die nachfolgenden Punkte. Diesen Abschnitt beschließen wir mit zwei wichtigen Hinweisen:

1. Sie beenden eine SSH-Verbindung mit dem Befehl „exit“ oder mit der Tastenkombination Strg-D.

2. SSH benutzt den Netzwerkport 22 als Standard. Einen abweichenden Port (siehe „/etc/ssh/sshd_config“) geben Sie typischerweise – so etwa im Midnight Commander oder in grafischen Dateimanagern – nach einem Doppelpunkt nach der IP-Adresse an, also etwa 192.168.178.20:2222. Das Tool ssh benötigt aber mit

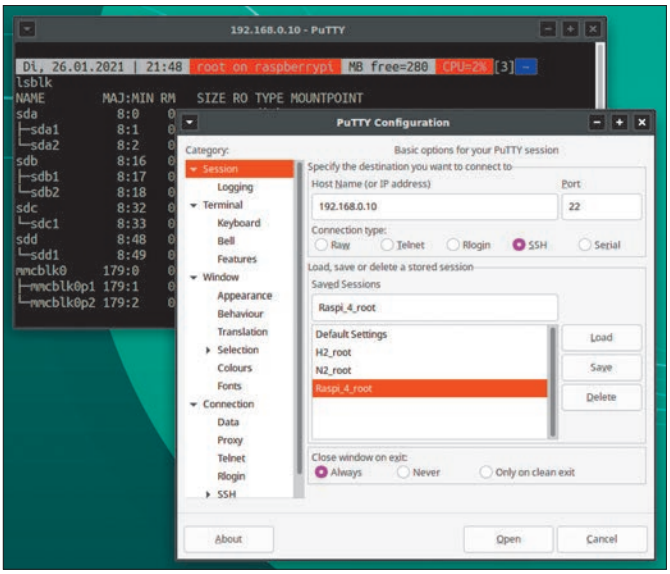
```
ssh -p 2222 ha@192.168.178.20
```

den expliziten Schalter „-p“.

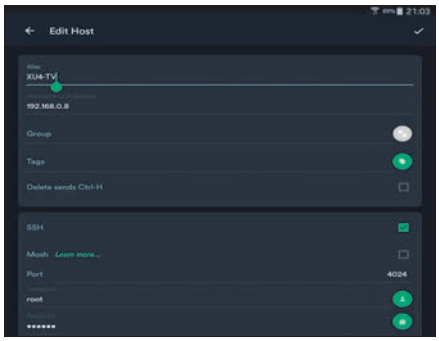
4. SSH-Terminal: Windows als Client

Die Optionen unter Windows, sich mit SSH-Servern zu verbinden, sind die letzten Jahre inflationär gewachsen, wonach der SSH-Klassiker Putty (Kitty) längst nicht mehr alternativlos ist. Dennoch bleiben wir aus Gründen der Vereinfachung hier bei Putty/Kitty. Ganz intuitiv ist Putty nicht, weil es fundamentale Einstellungen neben exotische Details stellt. Unterm Strich gewährleistet es dennoch die komfortable Verwaltung von SSH-Verbindungen.

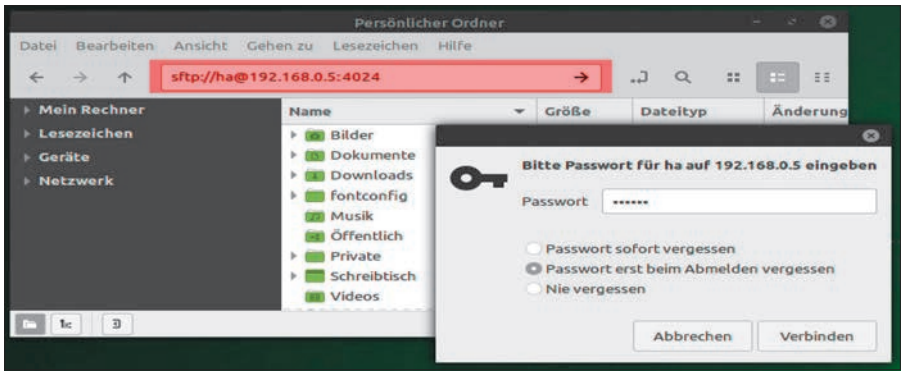
Die Basiskonfiguration ist einfach: Sie geben unter „Host Name“ entweder den Host-



Unter Windows ist Putty der SSH-Klassiker, unter Linux eher Exot. Putty und sein Klon Kitty sind nicht überall intuitiv, aber für SSH-Verbindungen unter Windows immer noch erste Wahl.



SSH-Client für Android und iOS: Die englischsprachige App Termius verwaltet beliebig viele Server übersichtlich und optisch ansprechend.



Datenzugriff und Mediennutzung per SFTP: Praktisch alle grafischen Linux-Dateimanager sprechen SFTP und verbinden sich mit einem SSH-Server.

namen oder die IP-Adresse des Servers an. Mit „Connection type: SSH“ und dem vorgegebenen Standardport 22 können Sie sich mit „Open“ bereits verbinden. Für häufigeren Zugriff und Feineinstellungen lohnt es sich aber, unter „Saved Sessions“ eine aussagekräftige Bezeichnung zu verwenden und jeden Server mit „Save“ dauerhaft zu speichern. Unter „Window → Translation → Remote character set“ sollten Sie immer den Eintrag „UTF-8“ wählen, damit Sonderzeichen in der SSH-Konsole korrekt angezeigt werden. Unter „Window → Colors“ (sowie „Fonts“) bestimmen Sie Erscheinungsbild und Schriftgröße. Beachten Sie nach allen Änderungen, in der Übersichtsspalte auf „Session“ zu navigieren und mit „Save“ die Einstellungen zu speichern.

Neben Putty gibt es den Klon Kitty (ebenfalls auf Heft-DVD, *http://www.9bis.net/*). Er unterscheidet sich nur dadurch, dass er die automatische Übergabe des Passworts erlaubt („Connection → Data“) und die Serverdaten in Klartextdateien unter „\Kitty\Sessions“ ablegt (statt in der Windows-Registry). Damit ist Kitty komfortabler, etwas unsicherer, aber für Heimnetzserver erste Wahl.

5. SSH-Terminal: Mobilgeräte als Client

Mobile Geräte sind nicht unbedingt erste Wahl für die SSH-Fernwartung. Der Bildschirm von Smartphones ist zu klein, zumal die Tastatur eingeblendet bleiben muss. Trotzdem ist ein schneller Eingriff in eine Konfigurationsdatei oder das Abholen einer wichtigen Datei auch mit Smartphones oder Tablets realisierbar. Entsprechende Apps finden Sie mit der Suche nach „SSH“ im Apple- wie im Google Store. Die englischsprachige App „Termius“ ist mit der beste Kandidat für Android wie iOS. Unter „Host“ legen Sie mit dem Plus-Zeichen einen Eintrag an („New host“). Im Prinzip genügt der Eintrag der IP-Adresse, falls der Server den Standardport 22 nutzt. Man kann bei geringen Sicherheitsansprüchen im lokalen Netz auch gleich das Benutzerkonto und das Kennwort hinterlegen. Allgemeine Einstellungen zu Schriftgröße und Farben werden unter den „Settings“ eingetragen, die für alle Hosts gelten. Um Einstellungen an einem bereits eingetragenen Server („Host“) zu ändern, hilft längeres Drücken des Host-Eintrags, was den Host markiert und in der kleinen Symbolleiste den Editierstift einblendet. Für bereits eingetragene Rechner genügt ein Fingertipp, um die SSH-Verbindung zu starten.

6. SFTP-Datenaustausch: Linux/Mac-OS als Client

Wie schon in Punkt 1 angesprochen, bietet SSH sein eigenes Dateiprotokoll SFTP. Da Linux-Dateimanager dieses Protokoll beherrschen, ist zwischen Linux-Rechnern Samba oder NFS entbehrlich. Mit der Syntax

```
sftp://[Benutzer]@[IP-
 Adresse]:[Port]/[Ordner]/
```

oder wahlweise auch

```
ssh://[Benutzer]@[IP-
 Adresse]:[Port]/[Ordner]/
```

in der Adresszeile eines Dateimanagers (Strg-L) haben Sie – nach Kennworteingabe – umstandslos die Dateien des entfernten Rechners vor sich. Port und Ordner können entfallen, falls Standardport 22 genutzt wird und das gesamte Dateisystem angezeigt werden soll – also etwa:

```
sftp://ha@192.168.178.20
```

Diese Methode eignet sich für Datensicherungen oder das Editieren von Konfigurationsdateien ebenso wie für das Abspielen von Musik- oder Filmmedien und ist einem Samba-Zugriff mindestens ebenbürtig. Theoretisch lässt sich das Dateisystem eines SSH-Servers mit

```
sshfs ha@192.168.178.20 ~/Raspi4
```

auch in das lokale Dateisystem einbinden, sofern das Paket „sshfs“ installiert ist. In den meisten Fällen wird aber der Weg über den grafischen Dateimanager völlig befriedigen, zumal Sie die einmal gemountete SFTP-Quelle einfach als Lesezeichen ablegen können.

7. SFTP-Datenaustausch: Windows als Client

Um es auf den entscheidenden Punkt zu bringen: Der Datentransport zwischen Windows und SSH-Servern ist möglich, eine direkte Daten- oder Mediennutzung am Server hingegen nicht: Wer mit Windows Dateien vom SSH-Server bearbeiten, ändern oder einfach abspielen will, kommt an einer zusätzlichen Samba-Lösung nicht vorbei. Geht es hingegen nur um reine Dateiaktionen, also das Kopieren, Verschieben und Löschen von Daten, dann hilft unter Windows das externe Tool Filezilla (*www.filezilla-project.org*). Filezilla ist den meisten Nutzern als FTP-Client geläufig, beherrscht aber auch SFTP. Sie können daher den SSH-Server mit seiner IP, den Authentifizierungsdaten („Verbindungsart: Normal“) und SFTP-Protokoll in den Servermanager eintragen und sich verbinden. Die Zwei-Fenster-Anordnung erlaubt einfache Navigation im lokalen Dateisystem und am Server sowie Datenaustausch per Doppelklick oder Drag & Drop.

8. SSH: Grafische Programme

Sofern der SSH-Dienst entsprechend konfiguriert ist (siehe Punkt 2), lassen sich via SSH auch grafische Programme starten, die

dann auf dem Client angezeigt werden (X11-Forwarding). Mit Linux-Clients ist der Aufwand am geringsten: Hier verwenden Sie beim ssh-Start einfach den zusätzlichen Schalter „-X“ (Großschreibung):

```
ssh –X [benutzer]@[hostname]
```

In der SSH-Konsole starten Sie dann das gewünschte Programm. Auf Wunsch lässt sich das auch schon beim SSH-Aufruf anfordern (Beispiel):

```
ssh -X ha@192.168.178.20
  thunderbird
```

Auch unter Windows bringen Sie grafische Programme des SSH-Servers auf den Clientdesktop. Putty/Kitty muss unter „Connection → SSH → X11 → Enable X11 forwarding“ und ebenda „X display location“ mit der Angabe „localhost:0“ darauf vorbereitet werden. Ferner benötigen Sie aber noch den kostenlosen X-Server Xming (*https://sourceforge.net/projects/xming/*). Xming muss laufen, bevor Sie die SSH-Session starten. Xming ist nicht anspruchsvoll und kann unter Windows auch dauerhaft mitlaufen (10 bis 20 MB im Wartezustand).

9. SSH-Anmeldung ohne Passworteingabe

Die Eingabe eines kurzen Systemkennworts beim Start einer SSH-Sitzung ist an sich eine zumutbare Pflicht. Es gibt aber Szenarien, die – jenseits des Komfortaspekts – einen passwortlosen Zugang sinnvoll machen. Das gilt besonders für automatisierte Datensicherung (etwa mit rsync), die ohne Interaktion ablaufen soll, aber auch für den störungsfreien Start von ausgelagerter Software. Mit

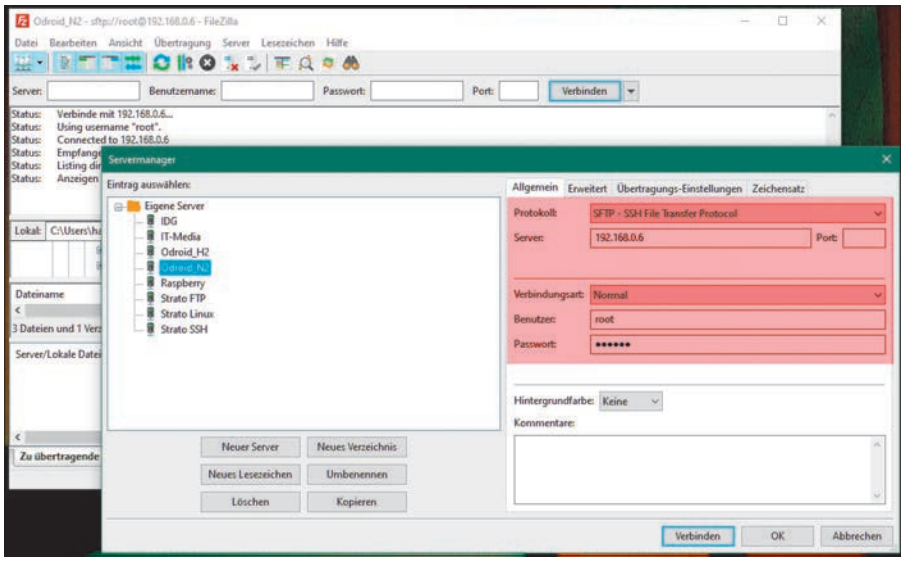
```
ssh-keygen
```

erstellen Sie zunächst auf Linux-Client-PC (nicht auf dem Server!) einen Zugangsschlüssel. Weitere Optionen sind dabei möglich, aber nicht zwingend. Der Schlüssel wird standardmäßig unter „~/.ssh/id_rsa.pub“ gespeichert, was Sie bestätigen müssen. Das ferner abgefragte Passwort zum Schutz des Schlüssels können Sie mit Eingabetaste ignorieren. Anschließend kopieren Sie den Schlüssel zum Server (Beispiel):

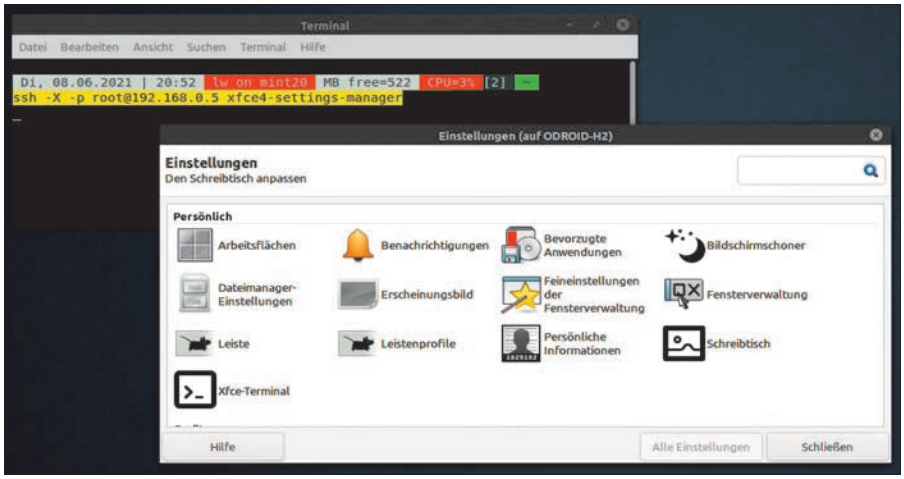
```
ssh-copy-id -i ~/.ssh/id_rsa.pub
  root@192.168.178.20
```

Beachten Sie, dass der Schlüssel für das Konto am Server gilt, das Sie vor der Server-IP angeben – hier „root“. Auf Clientseite gilt es wiederum für das Konto, mit dem Sie gerade arbeiten. Falls der Server einen vom Standardport 22 abweichenden Port verwendet, kann das Tool ssh-copy-id diesen über den Schalter „-p [Port]“ mitteilen.

Starten Sie danach die erste SSH-Sitzung mit Schlüsselanmeldung. Das System fragt nach dem vorher vergebenen Schutzpasswort für den Schlüssel – also genügt die Eingabetaste, falls Sie das Schutzpasswort bei der Schlüsselerstellung ignoriert haben. Alle künftigen Verbindungen funktionieren dann ohne interaktive Eingabe. Auch Putty unter Windows kann sich mit einem Schlüssel beim Server authentifizieren, benötigt dafür aber die zusätzlichen Tools Puttygen und Pageant. Einfacher ist es im Heimnetz, statt Putty das nonchalantere Kitty zu verwenden, das die Passwortübergabe unter „Connection → Data“ direkt anbietet: Hier tragen Sie das Konto einfach neben „Auto-login username“ und das Passwort neben „Auto-login password“ ein. ■



Filezilla beherrscht SSH-Dateiprotokoll SFTP. Dies ermöglicht unter Windows den Datenaustausch mit SSH-Servern, jedoch keine Mediennutzung oder direkte Dateibearbeitung.



Optional zeigt SSH grafische Programme des Servers am Client. Die XFCE-Einstellungszentrale läuft nicht auf dem Desktop-PC, sondern auf dem Server, wie auch die Titelleiste bestätigt.

SSH ohne Kennwortabfrage: Der Clientrechner muss einen Schlüssel erzeugen (ssh-keygen), der dann zum Server kopiert wird (ssh-copy-id).

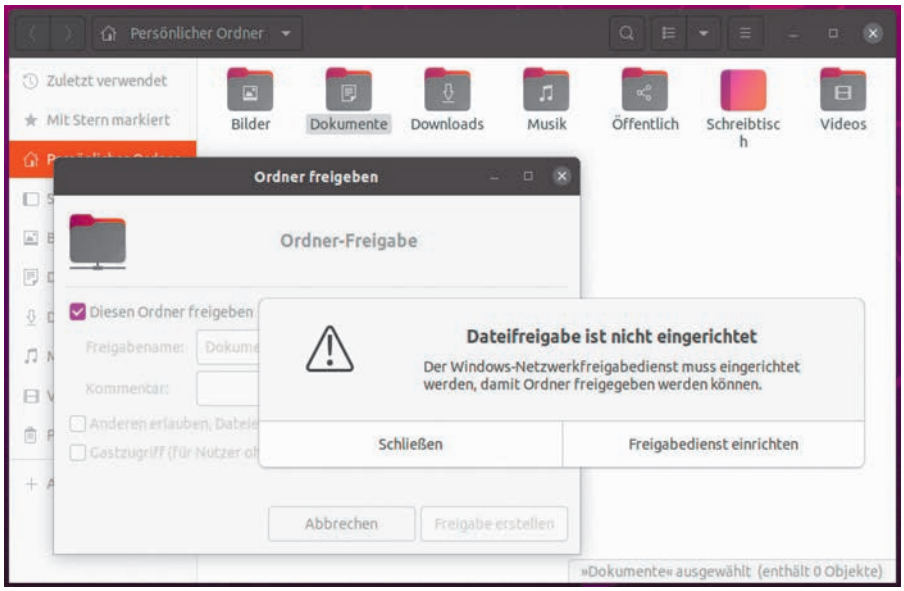
```
ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:z1LFEDr6iEDoPML8/NGPnPML8ZcoapXPML8oXEDVWG4 root@odroid
ssh-copy-id -i ~/.ssh/id_rsa.pub root@192.168.0.5
```

Netzwerken mit Samba

Netzwerkfreigaben mit SMB/CIFS sind die gebräuchlichste Methode für den Dateitransfer zwischen PCs im gemischten Netzwerk. Linux, Windows und Mac-OS unterstützen das Protokoll standardmäßig.

VON THORSTEN EGGELING

Linux-Dateimanager können ohne zusätzliche Software auf Netzwerkfreigaben von Windows- und Linux-Rechnern zugreifen. Soll der Linux-PC ebenfalls Freigaben anbieten, installiert man den Samba-Server. Die Basiskonfiguration ist nicht kompliziert, das Zusammenspiel von Samba-Einstellungen, Benutzerkonten und Rechten im Dateisystem erfordert jedoch einen gewissen Aufwand. Wie hoch der ist, hängt davon ab, ob Sie nur einen Ordner im Home-Verzeichnis freigeben wollen oder einen beliebigen anderen Ordner, ferner ob mehrere Benutzer nur Lese- oder auch Schreibzugriff erhalten sollen. Hilfe bei der Samba-Konfiguration bieten Tools beziehungsweise Webanwendungen, die wir ab Seite 62 vorstellen. Aber auch damit sind Kenntnisse der manuellen Konfiguration von Vorteil.



Freigabe einrichten: Ubuntu fordert bei der Ersteinrichtung einer Benutzerfreigabe zur Installation des Samba-Servers auf. Mint-Nutzer müssen die Komponente manuell installieren.

1. Samba-Server installieren

Wer Ordner im lokalen Netzwerk freigeben möchte, muss in jedem Fall die Samba-Serverkomponente installieren.

Die Vorgehensweise ist entweder geführt oder manuell:

Ubuntu: Freigaben aus dem Home-Verzeichnis kann unter Ubuntu direkt der Dateimanager erledigen (Benutzerfreigabe). Klicken Sie den gewünschten Ordner mit der rechten Maustaste an und wählen Sie im Kontextmenü „Freigabe im lokalen Netzwerk“. Setzen Sie ein Häkchen vor „Diesen Ordner freigeben.“ Nun erscheint eine Meldung, in der Sie auf „Freigabedienst einrichten“ klicken, danach auf „Installieren“ und dies mit Ihrem Passwort bestätigen. Zurück im Fenster „Ordner freigeben“ können Sie nun ein Häkchen vor „Gastzugriff (für Nutzer ohne Benutzerkonto)“ setzen. Damit erlauben Sie anderen PCs im Netzwerk ohne Anmeldung Lesezugriff auf den freigegebenen Ordner. Ansonsten gibt es Lesezugriff nach vorheriger Anmeldung für Sie selbst und für andere Nutzer, die ein Konto auf dem PC mit der Freigabe besitzen. Schreibzugriff ist möglich, wenn Sie ein Häkchen vor „Anderen erlauben, Dateien in diesem Ordner zu erstellen und zu löschen“ setzen. Damit die Anmeldung funktioniert, müssen Sie zusätzlich ein Samba-Passwort vergeben (siehe Punkt 2).

Linux Mint und andere Distributionen: Mint-Nutzer müssen den Samba-Server manuell installieren, selbst wenn sie nur Benutzerfreigaben verwenden wollen. Auch Ubuntu-Nutzer installieren den Samba-Server oft besser manuell, entweder weil zunächst keine Benutzerfreigabe erstellt werden soll oder weil eine grafische Oberfläche fehlt. Die Installation über einen SSH-Fernzugriff ist auf diesem Weg natürlich auch möglich, etwa bei Raspberry-Pi-OS (Raspberry Pi). Führen Sie im Terminal diese drei Zeilen aus:

```
sudo apt update
sudo apt upgrade
sudo apt install samba
```

Unter Linux Mint lässt sich anschließend im Dateimanager über den Kontextmenüpunkt „Freigabeoptionen“ eines Ordners die Freigabe aktivieren. Die Optionen sind die gleichen wie oben für Ubuntu beschrieben.

2. Gruppenzugehörigkeit und Samba-Passwort

Nur das Systemverwalterkonto, das Sie bei der Linux-Installation als Erstbenutzer erstellt haben, darf Benutzerfreigaben über den Dateimanager erstellen. Hintergrund dafür ist die Tatsache, dass ein Benutzerkonto zur Gruppe „sambashare“ gehören muss, um Ordner freigeben zu dürfen. Das bei der Installation eingerichtete Erstbenutzerkonto ist automatisch Mitglied von „sambashare“. In den Mint-Systemeinstellungen können Sie über „Benutzer und Gruppen“ weitere Konten zum Mitglied von „sambashare“ machen. Ubuntu-Nutzer benötigen dafür das Terminal:

```
sudo usermod -aG sambashare [User]
```

Ersetzen Sie den Platzhalter „[User]“ durch die Bezeichnung des Benutzerkontos, das Benutzerfreigaben erstellen darf. Die Terminalmethode funktioniert natürlich auch unter Mint.

Samba-Passwort: Samba verwendet bei der Anmeldung zwar die Linux-Benutzerkonten, aber eine eigene Passwort-Datenbank. Sie müssen daher den gewünschten Benutzerkonten folgendermaßen ein Samba-Passwort zuweisen:

```
sudo smbpasswd -a [User]
```

Den Platzhalter „[User]“ ersetzen Sie durch die Bezeichnung des Benutzerkontos. Tippen Sie das Passwort ein und bestätigen Sie es. Das Samba-Passwort darf identisch mit dem Linux-Anmeldepasswort sein, kann aber auch abweichen. Es ist jedoch empfehlenswert, auf allen Linux- und Windows-PCs die gleiche Kombination von Benutzernamen und Passwörtern zu verwenden.

3. Samba-Konfiguration und globale Freigaben

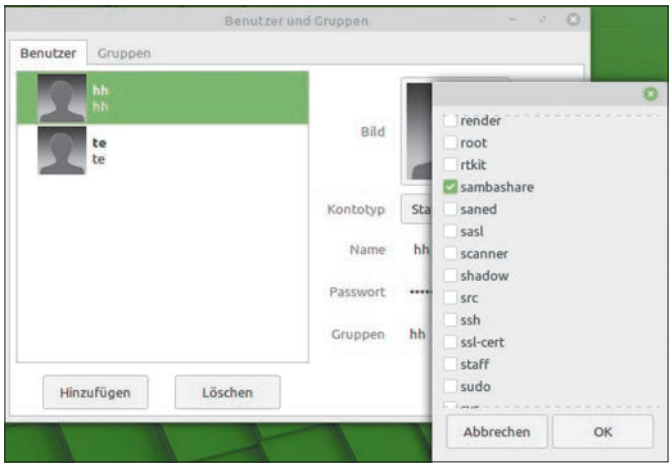
Die gesamte Samba-Konfiguration erfolgt in der Datei „/etc/samba/smb.conf“. Die standardmäßig installierte Beispielkonfiguration enthält Kommentare in englischer Sprache, die die Funktion der einzelnen Optionen erläutert. Der Hauptabschnitt ist mit „[global]“ eingeleitet. Alle weiteren Abschnitte in eckigen Klammern sind Freigabedefinitionen.

Änderungen in der „smb.conf“ werden wirksam, wenn Sie den Samba-Server die Konfigurationsdatei neu einlesen lassen:

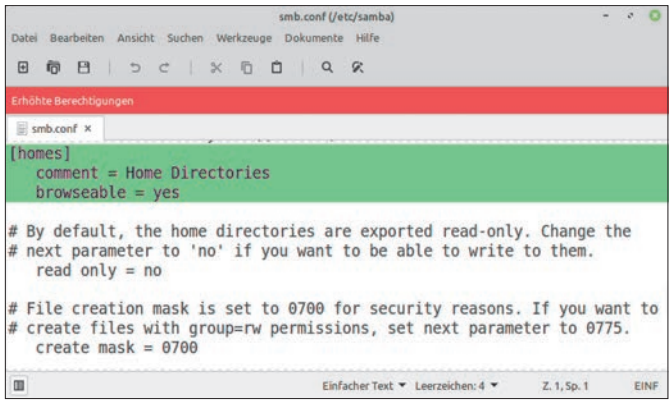
```
sudo systemctl restart smbd
```

Alle Home-Verzeichnisse freigeben: In der „smb.conf“ gibt es einen auskommentierten Abschnitt, der mit „;[homes]“ beginnt. Entfernen Sie die Kommentarzeichen, um die Home-Verzeichnisse aller Benutzer standardmäßig freizugeben. Soll Schreibzugriff erlaubt sein, ändern Sie „read only = yes“ auf „read only = no“. Wenn ein authentifizierter Benutzer auf den Server zugreift, sieht er nur sein eigenes Home-Verzeichnis als Freigabe.

Allgemeine Freigaben: Eine globale Freigabe lässt sich beispielsweise über diese



Nicht jeder hat das Recht: Damit ein Benutzer Freigaben erstellen darf, muss er zur Gruppe „sambashare“ gehören. Mint-Nutzer legen die Gruppe über „Benutzer und Gruppen“ fest.



Freigaben für alle Benutzer: Entfernen Sie die Kommentarzeichen beim Block „[homes]“. Dann kann jeder Benutzer von anderen PCs aus auf sein Home-Verzeichnis zugreifen.

WINDOWS UND LINUX-FREIGABEN

Damit ein Samba-Server bei Windows unter „Netzwerk“ auftaucht, muss man Linux das Windows-Protokoll WS-Discovery beibringen. Eine Lösung für die Anzeige von Windows-Servern im Linux-Dateimanager gibt es bisher nicht.

Laden Sie über *https://github.com/christgau/wsdd/releases* das aktuelle „tar.gz“-Paket herunter und entpacken Sie das Archiv in einen beliebigen Ordner. Das Python-Script „src/wsdd.py“ benennen Sie in „wsdd“ um. Kopieren Sie die Datei in den Ordner „/usr/bin“. Öffnen Sie die Datei „etc/systemd/wsdd.service“ in einem Editor. Ändern Sie Benutzer und Gruppe hinter „User=“ und „Group=“ für Ubuntu, Linux Mint oder Debian jeweils auf „daemon“. In der Zeile „ExecStart“ fügen Sie am Ende die Bezeichnung des Netzwerkadapters an, etwa „-i eth0“ oder „-i enp0s3“. Den Namen finden Sie über *ip addr* heraus.

Kopieren Sie die Datei „wsdd.service“ in den Ordner „/etc/systemd/system“.Danach starten Sie den Dienst mit diesen Befehlen:

```
sudo systemctl daemon-reload
sudo systemctl start wsdd
sudo systemctl enable wsdd
```

Unter Windows 8.1/10 taucht der Linux-Server dann sofort unter „Netzwerk“ auf.

drei Zeilen erstellen, die Sie am Ende der Datei „smb.conf“ einfügen:

```
[data1]
path = /data1
writeable = no
```

Damit wird das Verzeichnis „/data1“ unter der Bezeichnung „data1“ freigegeben. Der Ordner „/data1“ muss existieren und die Benutzer müssen auf der Ebene des Dateisystems wenigstens Leserechte besitzen. Das ist standardmäßig der Fall, wenn Sie das Verzeichnis mit

```
sudo mkdir /data1
```

erstellen. Mit der zusätzlichen Zeile

```
guest ok = yes
```

ergänzen Sie die Freigabedefinition für den Fall, dass Sie auch Benutzern ohne Konto den Zugriff erlauben wollen.

4. Freigaben mit Schreibberechtigung erstellen

Damit Benutzer Dateien über das Netzwerk neu erstellen oder ändern können, genügt aus der Sicht von Samba die Änderung von „writeable = no“ auf „writeable = yes“. Das allein reicht jedoch noch nicht für den vollen Zugriff aus. Der Ordner „/data1“ im Beispiel aus Punkt 3 gehört Benutzer und Gruppe „root“, alle anderen Benutzer haben auf der Ebene des Dateisystems nur Leserechte. Um das zu ändern, verwenden Sie folgende vier Befehlszeilen:

```
sudo groupadd smbadmin
sudo chown -R root:smbadmin /data1
sudo find /data1 -type d -exec chmod
 775 {} +
sudo find /data1 -type f -exec chmod
 664 {} +
```

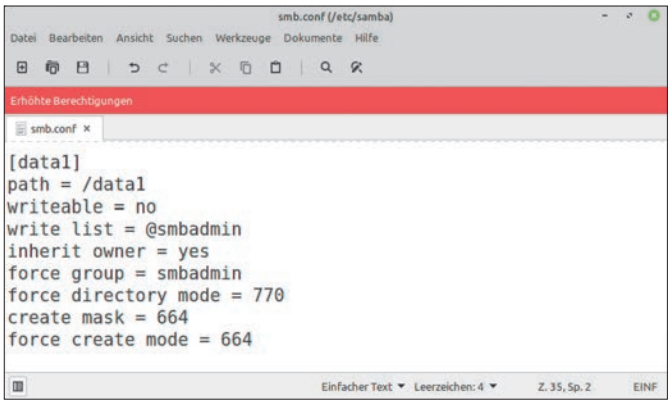
Die letzten drei Befehlszeilen arbeiten rekursiv, berücksichtigen also auch unter „/data1“ bereits vorhandene Ordner und Dateien. Die neu erstellte Gruppe „smbadmin“ – die Bezeichnung können Sie frei wählen – und der Besitzer „root“ erhalten Vollzugriff, andere Benutzer inklusive Gäste dürfen weiterhin nur lesen.

Fügen Sie Ihr eigenes Benutzerkonto und weitere Konten, die eine Schreibberechtigung erhalten sollen, zur Gruppe „smbadmin“ hinzu:

```
sudo usermod -aG smbadmin
 [Benutzer]
```

Den Platzhalter „[Benutzer]“ ersetzen Sie dabei jeweils durch den Benutzernamen. Melden Sie sich ab und wieder an, damit Linux die neue Gruppenzugehörigkeit berücksichtigt.

Zugriffsrechte festlegen: Damit neue Elemente im Dateisystem auch für andere Benutzer Schreibrechte erhalten, müssen die Freigabeoptionen angepasst werden.



Berechtigungen korrekt setzen: Der Schreibzugriff durch mehrere Benutzer auf Elemente des Dateisystems hat unerwünschte Nebenwirkungen. Erstellt ein Benutzer Dateien neu oder ändert er deren Inhalt, wird er zum Eigentümer. Danach haben andere Benutzer nur noch Leserechte. Um das zu ändern, erstellen Sie eine Freigabedefinition mit diesen neun Zeilen:

```
[data1]
path = /data1
writeable = no
write list = @smbadmin
inherit owner = yes
force group = smbadmin
force directory mode = 770
create mask = 664
force create mode = 664
```

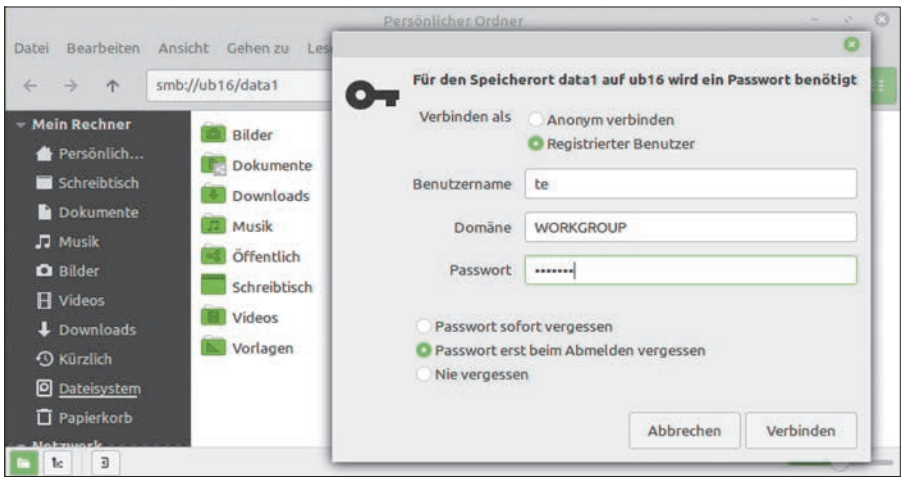
„write list = @smbadmin“ gewährt der Gruppe „smbadmin“ Schreibzugriff.

Für alle anderen Benutzer und Gruppen bleibt es durch „writeable = no“ bei der Berechtigung „Nur lesen“. Die weiteren Optionen sorgen dafür, dass neu erstellte Elemente dem Besitzer des darüberliegenden Ordners („inherit owner“) sowie der Gruppe „smbadmin“ gehören und beide Vollzugriff erhalten.

5. Zugriff auf Netzwerkfreigaben

Unter Linux greifen Sie über den Dateimanager auf Samba-Freigaben zu. Mint-Nutzer gehen auf „Netzwerk“, Ubuntu-Nutzer auf „Andere Orte“. Sie sehen dann die Namen der Samba-Server im lokalen Netzwerk. Ob auch eine Liste mit freigegebenen Ordnern erscheint, wenn Sie einen Server öffnen, hängt von der Samba-Version des Servers ab. Ab einschließlich Version 4.11 erhalten Sie nur die Fehlermeldung „Empfangen der Freigabeliste vom Server ist gescheitert“. Andernfalls können Sie den gewünschten Ordner öffnen und sich mit einem Benutzerkonto auf dem Server und dem zugehörigen Samba-Passwort anmelden (siehe Punkt 2).

Windows-Rechner sind im Dateimanager nicht zu sehen. Wenn Sie den Ordner „Windows-Netzwerk“ öffnen, bleibt das Fenster leer. Samba- und Windows-Server bezie-



Zugriff auf Freigaben: Über eine URL in der Form „smb://[Servername oder IP-Adresse]]/[Freigabename]“ lässt sich jede Freigabe im Dateimanager direkt aufrufen.

hungsweise Freigaben werden nicht angezeigt, weil inzwischen aus Sicherheitsgründen die dafür nötige Unterstützung durch das Protokoll SMB 1.0 fehlt. Sie können aber eine Freigabe über die Adressleiste des Dateimanagers (Strg-L) direkt ansprechen. Verwenden Sie eine URL in der Form

```
smb://[Servername oder IP-
 Adresse]/[Freigabename]
```

Erstellen Sie für die Freigabe mit Strg-D ein Lesezeichen, um Sie künftig mit einfachem Mausklick zu erreichen. Wie Sie einen unbekannten Freigabenamen herausfinden, lesen Sie in Punkt 7.

Windows sieht Samba-Server ebenfalls nicht (siehe Kasten „Windows und Linux-Freigaben"). Hier tippen Sie in die Adressleiste eine URL in der Form

```
\\[Servername oder IP-Adresse]]\
 [Freigabename]
```

ein. Wenn Benutzername und Passwort bei Windows und Linux (Samba-Passwort) identisch sind, erfolgt die Anmeldung automatisch. Andernfalls werden Sie nach den Anmeldeinformationen gefragt.

6. SMB-Version 1 reaktivieren

Aktuelle Netzwerkgeräte kommunizieren über die Protokolle SMB 2.0 oder 3.0. Bei älteren NAS-Geräten kann es aber sein, dass nur SMB 1.0 zur Verfügung steht. In diesem Fall aktivieren Sie unter Linux SMB 1.0 für den Client, also für den Zugriff auf die Freigaben. In die Datei „/etc/samba/smb.conf" tragen Sie in den Abschnitt „[global]" die Zeile

```
client min protocol = NT1
```

ein. Falls der Rechner selbst Freigaben auch über SMB 1.0 bereitstellen soll, konfigurieren Sie zusätzlich

```
server min protocol = NT1
```

Speichern Sie die Datei und starten Sie Samba mit

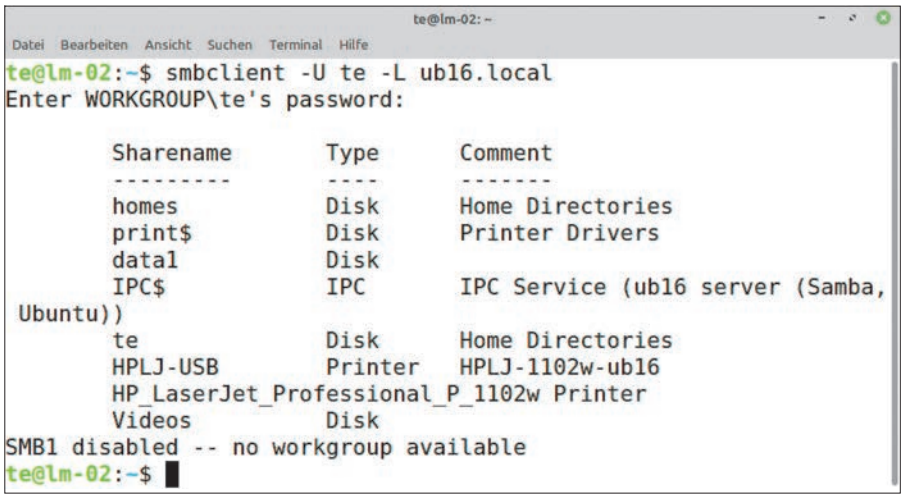
```
sudo serviceclt restart smbd
```

neu.

Sicherheit: SMB 1.0 ist angreifbar, weil die Datenübertragung – auch von Benutzernamen und Passwörtern – unverschlüsselt erfolgt. In einem privaten Netzwerk mit einer übersichtlichen Anzahl von Benutzern ist das jedoch nur ein geringes Risiko. Trotzdem sollte man mittelfristig Geräte austauschen, die nur SMB 1.0 bieten.

7. Samba-Tool für das Terminal

Die Bezeichnungen der Freigaben lassen sich unter Linux mit der Befehlszeile



Welche Freigaben gibt es im Netz? Das Tool smbclient zeigt im Terminal, welche Freigaben Linux- oder Windows-Systeme im Netzwerk bereitstellen.

```
smbclient -U [Benutzer] -L
 [Servername oder IP-Adresse]
```

herausfinden. Tippen Sie das Passwort ein, das für die Freigabe auf dem Server erforderlich ist. Sollte das Tool nicht gefunden werden, installieren Sie unter Ubuntu/Mint das Paket „smbclient". Smbclient kann Arbeitsgruppen beziehungsweise SMB-1.0-Freigaben anzeigen, auch wenn Sie Samba nicht wie in Punkt 6 beschrieben konfiguriert haben. Dazu verwenden Sie die Befehlszeile

```
smbclient -U [Benutzer] -L
 [[Servername oder IP-Adresse]
 --option="client min
 protocol"="NT1"
```

Unter Windows zeigt der Befehl

```
net view \\[[Servername oder IP-
 Adresse]
```

die Freigaben des angegebenen Rechners an.

8. Samba-Freigaben mounten

In der Regel genügen Lesezeichen im Dateimanager, um Samba-Freigaben bei Bedarf komfortabel zu mounten. Wer Freigaben aber permanent im Dateisystem erreichen will, installiert das Paket „cifs-utils". Eine Freigabe lässt sich dann mit einer Befehlszeile nach diesem Muster einbinden:

```
sudo mount -t cifs -o
 username=[Share-
 Benutzer],password=[Samba-
 Passwort] //[Server]/[Freigabe]
 [Zielverzeichnis]
```

Für die Platzhalter setzen Sie die Werte für Ihr Netzwerk ein. Das „[Zielverzeichnis]" muss bereits existieren. Da „root" der Eigentümer ist, ist kein Schreibzugriff möglich. Das lässt sich aber mit dem folgenden Aufruf ändern:

```
sudo mount -t cifs -o
 username=[Share-
 Benutzer],password=[Samba-Passwo
 rt],uid=[Benutzer],gid=[Gruppe],
 dir_mode=0775,file_mode=0664 //
 [MeinServer]/[MeineFreigabe]
 [Zielverzeichnis]
```

Die UID Ihres Linux-Benutzerkontos bekommen Sie mit

```
id -u [Benutzername]
```

heraus und die GID so:

```
id -g [Benutername]
```

Die Optionen sind nötig, damit der Standardbenutzer „[Benutzer]" auf eine mit sudo eingehängte Freigabe auch Schreibzugriff erhält. Verwenden Sie eine derartige Konfiguration möglichst mit der Freigabedefinition aus Punkt 4. Nur so stellen Sie sicher, dass sich die Zugriffsrechte nicht unerwünscht ändern. Soll die Freigabe sogar automatisch beim Systemstart eingebunden werden, tragen Sie eine Zeile nach diesem Muster in die Datei „/etc/fstab" ein:

```
//[MeinServer]/[MeineFreigabe] /
 mnt cifs rw,_netdev,auto,nofail,
 user,username=[Share-
 Benutzer],password=[Samba-Passwo
 rt],uid=[Benutzer],gid=[Gruppe],
 file_mode=0644,dir_mode=0755 0 0
```

Zum Testen führen Sie diese Befehlszeile aus:

```
sudo mount -a
```

Die Option „nofail" ist ratsam, damit das System nicht auf den Samba-Server wartet, falls dieser einmal nicht erreichbar ist.

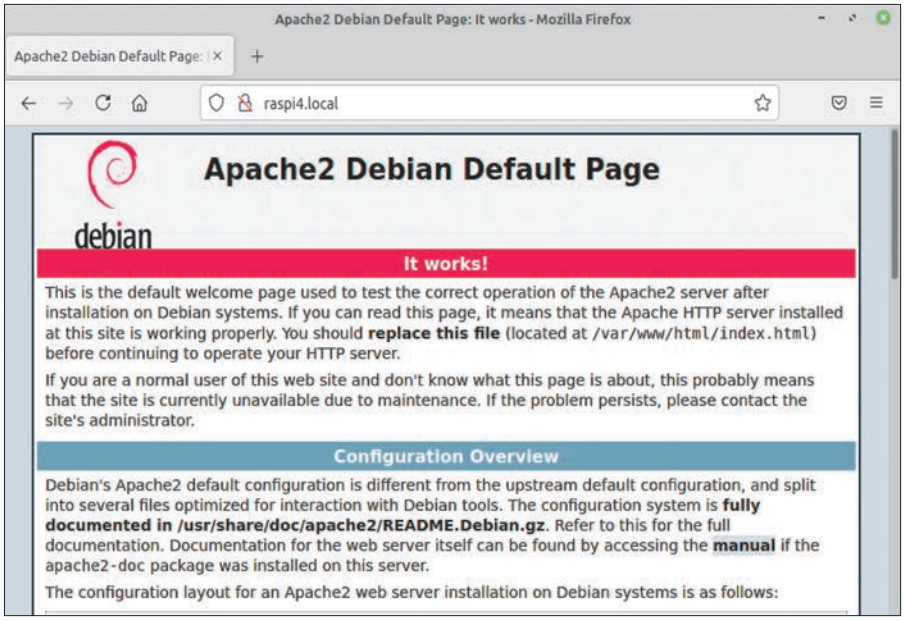
Apache: Installation und Konfiguration

Ein Webserver ermöglicht die Nutzung zahlreicher Webanwendungen von der Fotogalerie bis zum Content-Management-System. Im eigenen Netzwerk lassen sich die Dienste für alle Rechner und Betriebssysteme bereitstellen.

VON THORSTEN EGGELING

Zu den zahlreichen Vorzügen von Linux gehört die Möglichkeit, Serverdienste schnell und einfach zu installieren. Schließlich läuft ein Großteil aller Internetserver ebenfalls unter Linux, weshalb ausgereifte Software vor allem für dieses Betriebssystem verfügbar ist. Das gilt nicht nur für den Webserver selbst, sondern auch für Webanwendungen, die auf dem Server laufen sollen. Sie können damit beispielsweise einen Webserver als Dateispeicher, Fotogalerie oder das Medienstreaming im eigenen Netzwerk einrichten (siehe ab Seite 54).

In diesem Artikel beschreiben wir die manuelle Installation und Konfiguration des Webservers Apache nebst Zusatzprogrammen unter Ubuntu 20.04, Linux Mint 20 und Raspberry-Pi-OS (Raspberry Pi). Eine Alternative ist die Installation und Konfiguration über ein Tool für die Serververwaltung (siehe ab Seite 62). Die Voraussetzung dafür ist ein frisch installiertes System. Sie sollten sich daher vorher überlegen, ob Sie den Server selbst einrichten oder dafür ein Tool verwenden wollen. Grundlegende Kenntnisse der Apache-Konfiguration sind auch beim Einsatz eines Konfigurationstools von Vorteil.



Es funktioniert: Nach der Installation des Apache-Webservers lässt sich die Standardseite gleich im Browser aufrufen. Dafür ist keine besondere Konfiguration erforderlich.

1. Installation der Software für den Server

Den Webserver Apache installiert man in der Regel zusammen mit dem Script-Interpreter PHP und der Datenbank My SQL oder Maria DB. Was man genau benötigt, hängt von der jeweiligen Webanwendung ab. PHP dient zur dynamischen Erzeugung von Webinhalten, als Quelle kommt meist eine Datenbank zum Einsatz. Die Datenbank Maria DB ist eine Abspaltung von My SQL und steht vollständig unter einer Open-Source-Lizenz, weshalb die Installation zu bevorzugen ist. Beide Datenbanken sind kompatibel zueinander und verwenden gleichnamige Tools für die Verwaltung. Daher lässt sich My SQL einfach durch MariaDB ersetzen.

Schritt 1: Für die Installation des Webservers Apache verwenden Sie im Terminal

```
sudo apt install apache2
```

Der Serverdienst wird automatisch aktiviert und gestartet. Im Webbrowser rufen Sie *http://localhost* auf und sehen dann die Startseite („/var/www/index.html“). Auf allen anderen Rechnern im Netzwerk ersetzen Sie „localhost“ durch die IP-Adresse des Servers. Oder Sie verwenden den Hostnamen des Servers, an den Sie in den meisten Netzwerken „.local“ anhängen, damit der Rechner gefunden wird.

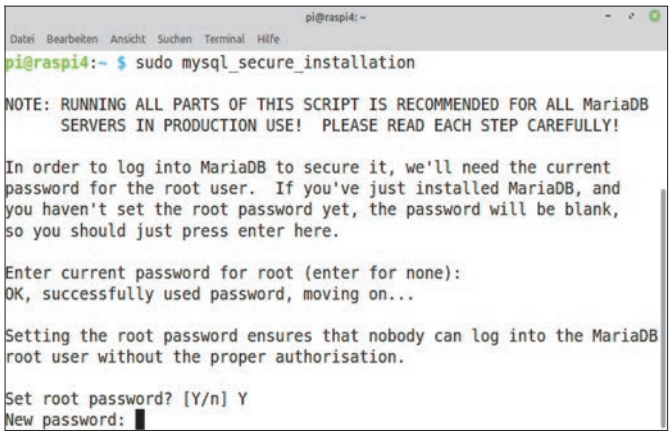
Wenn Sie später etwas in der Apache-Konfiguration ändern oder weitere Websites erstellen, müssen Sie die Konfiguration neu einlesen:

```
systemctl reload apache2
```

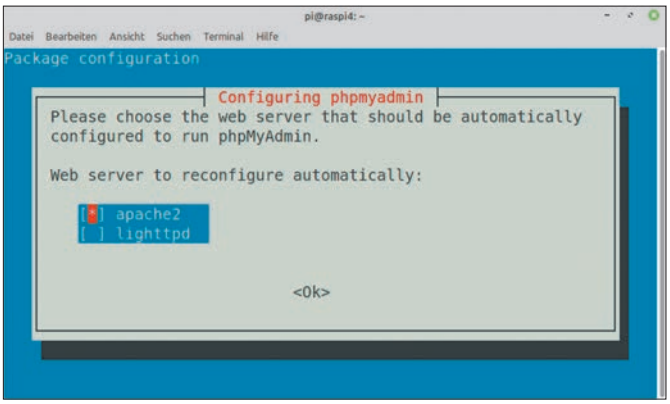
Schritt 2: Für eine PHP-Basisinstallation genügt dieser Befehl:

```
sudo apt install php
```

Schritt 3: Installieren Sie die Datenbank Maria DB, sofern das für die gewünschte Webanwendung erforderlich ist:



Datenbankserver: Maria DB wird standardmäßig ohne Passwort installiert. Über „mysql_secure_installation“ vergeben Sie ein Passwort für den Benutzer „root“.



Maria-DB-Front-End: Das Datenbank-tool Phpmyadmin unterstützt mehrere Webserver. Wählen Sie bei der Installation „apache2“ für die automatische Konfiguration aus.

```
sudo apt install mariadb-server
```

Vergeben Sie ein Passwort für den Maria-DB-Nutzer „root“. Dazu starten Sie

```
sudo mysql_secure_installation
```

Sie werden nach dem bisherigen Passwort gefragt. Da noch keines vergeben ist, bestätigen Sie mit der Eingabetaste. Legen Sie dann ein Passwort fest und beantworten Sie alle folgenden Fragen mit „Y“. Danach aktiveren Sie mit den folgenden vier Zeilen das Plug-in „mysql_native_password“, weil sonst nur eine Anmeldung mit administrativen Rechten möglich wäre:

```
sudo mysql -u root -p mysql
update user set plugin='mysql_
 native_password' where
 User='root';
flush privileges;
exit;
```

Nach der ersten Zeile tippen Sie das zuvor vergebene root-Passwort ein.

Schritt 4: Für Maria DB sollten Sie das Konfigurationstool phpmyadmin installieren. Darüber können Sie neue Datenbanken erstellen sowie Benutzer und Zugriffsrechte verwalten. Zur Installation verwenden Sie

```
sudo apt install phpmyadmin
```

Sie werden nach dem verwendeten Webserver gefragt und wählen „apache2“. Beantworten Sie die Frage nach „dbconfig-common“ mit „Ja“ und geben dann das in Schritt 3 gewählte Maria-DB-root-Passwort ein. Danach müssen Sie ein weiteres Passwort festlegen, mit dem sich phymyadmin in Zukunft bei My SQL anmelden soll. Rufen Sie das Tool im Browser über *http://localhost/phpmyadmin* auf und melden Sie sich probehalber an.

Wofür sich das Tool nutzen lässt, erfahren Sie ab Seite 54.

2. Feste IP-Adresse für den Server

Server im eigenen Netzwerk sollten möglichst immer über die gleiche IP-Nummer ansprechbar sein. Das ist nicht zwingend erforderlich, wenn der Server auch über seinen Namen erreichbar ist. Mit einer festen IP-Adresse vermeiden Sie aber Probleme, wenn Sie in einer Konfiguration die IP-Adresse eintragen müssen oder wollen. Die Zuweisung der IP-Adresse erfolgt per DHCP (Dynamic Host Configuration Protocol) über den DSL-Router oder das Kabelmodem. In der Regel ist eine Ablaufzeit für die IP-Adressen eingestellt, damit unbenutzte Adressen nach einiger Zeit wieder freigegeben werden. Meist lässt sich aber eine IP-Adresse dauerhaft zuweisen. Bei einer Fritzbox rufen Sie die Konfigurationsoberfläche über *http://fritz.box* oder standardmäßig *http://192.168.178.1* auf und melden sich an. Gehen Sie auf „Heimnetz → Netzwerk“. Auf der Registerkarte „Netzwerkverbindungen“ klicken Sie in der Zeile für Ihren Server auf das Stift-Symbol, setzen ein Häkchen vor „Diesem Netzwerkgerät immer die gleiche IPv4-Adresse zuweisen.“ und klicken auf „OK“.

Sollte Ihr Router keine entsprechende Option bieten, konfigurieren Sie die feste IP-Adresse am Linux-Server selbst (siehe Seite 80).

3. Die Struktur der Apache-Konfiguration

Die Apache-Konfigurationsdateien liegen unter „/etc/apache2“. Die Standardkonfiguration ist in der Datei „/etc/apache2/apache2.conf“ abgelegt. Diese sollte nur in Ausnahmefällen geändert werden. Anpassungen nehmen Sie in den anderen Konfi-

NGINX: DER ALTERNATIVE WEBSERVER

Nginx gilt als leistungsstarke Alternative zu Apache. Gerade auf limitierter Hardware wie dem Raspberry Pi bietet die Software einige Vorteile. Wenn Sie Nginx verwenden wollen, müssen Sie Apache deinstallieren oder für andere Ports konfigurieren. Die Installation von Nginx und PHP kann dann mit

```
sudo apt install nginx php-fpm
```

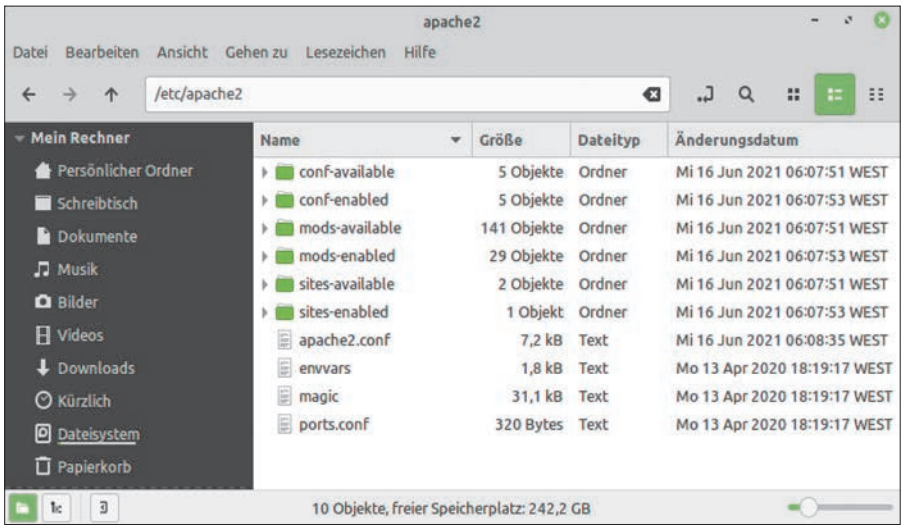
erfolgen. In der Konfigurationsdatei „/etc/nginx/sites-enabled/default“ tragen Sie für PHP in die Liste hinter „index“ zusätzliche „index.php“ ein. Der auskommentierte Abschnitt für PHP-Scripts muss so aussehen:

```
location ~ \.php$ {
include snippets/fastcgi-php.conf;
fastcgi_pass unix:/run/php/php7.3-fpm.sock;
}
```

Starten Sie den Webserver mit

```
systemctl restart nginx
```

neu. Weitere Informationen zu Nginx finden Sie ab Seite 62.



Alles an einem Ort: Die Apache-Konfiguration ist im Ordner „/etc/apache2“ untergebracht. Die Dateien lassen sich nur mit administrativen Rechten bearbeiten.

gurationsdateien vor, die „apache2.conf“ einbindet. Die Standardwerte lassen sich damit überschreiben. Es gilt das, was in der zuletzt geladenen Datei steht.

ports.conf: Hier ist festgelegt, auf welchen Ports der Webserver lauscht. Standardmäßig sind das Port 80 (HTTP) und Port 443 (HTTPS). Meist gibt es keinen Grund, das zu ändern, außer wenn ein anderer Webserver für diese Ports zuständig sein soll.

magic: In dieser Datei stehen Definitionen, die für die Auslieferung bestimmter Dateitypen erforderlich sind. Anhand einer Kennung erkennt der Browser, dass er beispielsweise ein JPG-Bild anzeigen und nicht als Textdatei darstellen soll. In der Regel ändern Sie auch hier nichts.

envvars: Die Datei enthält Umgebungsvariablen, die das Script „apache2ctl“ beim Start des Webservers auswertet. Mit „APACHE_RUN_USER“ beispielsweise ist festgelegt, unter welchem Benutzerkonto Apache läuft („www-data“).

Ordner „mods-enabled“: Der Ordner enthält symbolische Links auf Konfigurationsdateien im Ordner „mods-available“. Im Terminal lassen sich mit a2enmod Module aktivieren, mit a2dismod deaktivieren, einfach indem der Symlink erstellt beziehungsweise entfernt wird. Das ermöglicht eine flexible Konfiguration, ohne dass ein Apache-Modul deinstalliert werden muss. Es gibt „*.load“-Dateien, die ein bestimmtes Apache-Modul beim Start laden, beispielsweise „php7.3.load“ für PHP. Die „*.conf“-Dateien enthalten die Konfiguration der Module.

Ordner „conf-enabled“: Hier liegen symbolische Links auf globale Konfigurationsdateien im Ordner „conf-available“. Mit a2enconf und a2disconf lassen sich die Symlinks erstellen beziehungsweise entfernen. Phpmyadmin beispielsweise legt hier seine Konfiguration ab, in der der Pfad zu den zugehörigen Dateien unter „/usr/share/phpmyadmin“ zu finden ist.

Ordner „sites-enabled“: Dies ist der wichtigste Ordner für die Konfiguration. Er enthält Symlinks auf „conf“-Dateien im Ordner „sites-available“, die zugehörigen Tools sind a2ensite und a2dissite. Bisher ist hier nur die Datei „000-default.conf“ zu finden, die für die Auslieferung von Inhalten aus dem Ordner „/var/www/html“ sorgt. Unter „sites-available“ ist außerdem die Datei „default-ssl.conf“ zu finden. Sie enthält eine Beispielkonfiguration für die SSL-Verschlüsselung (HTTPS). Darauf gehen wir in diesem Artikel nicht weiter ein, weil das im Heimnetz unnötig ist. Bei einem aus dem Internet erreichbaren Webserver sollte Sie in jedem Fall SSL aktivieren. Kostenlose SSL-Zertifikate erhalten Sie von Let’s Encrypt. Auf *https://letsencrypt.org/getting-started/* finden Sie Links zu Anleitungen und den erforderlichen Tools.

4. Konfigurationsdateien bearbeiten

Alle Dateien unterhalb von „/etc/apache2“ und „/var/www“ gehören dem Benutzer „root“ und lassen sich nur mit administrativen Rechten ändern. Im Terminal können Sie dafür den Editor nano verwenden:

```
sudo nano [Pfad und Dateiname]
```

Die wichtigsten Tastenkombinationen zur Steuerung des Editors sind in der Leiste unten eingeblendet. Drücken Sie Strg-O und bestätigen Sie den Dateinamen mit der Eingabetaste, um eine Datei zu speichern. Mit Strg-X beenden Sie den Editor.

Desktopeditor verwenden: Wenn Sie einen Editor für die grafische Oberfläche bevorzugen, öffnen Sie unter Linux Mint (Cinnamon) den Dateimanager und klicken mit der rechten Maustaste auf einen Ordner oder einen leeren Bereich. Wählen Sie im Kontextmenü „Als Systemverwalter öffnen“. Bestätigen Sie mit Ihrem sudo-Passwort. Navigieren Sie zum gewünschten Ordner und öffnen Sie eine Datei per Doppelklick oder über den Kontextmenüpunkt „Öffnen mit Textverarbeitung“.

Nutzer von Ubuntu 20.04 (Gnome-Desktop) installieren ein Zusatzpaket

```
sudo apt install nautilus-admin
```

und starten Nautilus mit

```
nautilus -q
```

neu. Im Kontextmenü des Dateimanagers sehen Sie jetzt den Eintrag „Als Systemverwalter öffnen“. Bei Dateien gibt es außerdem „Als Systemverwalter bearbeiten“.

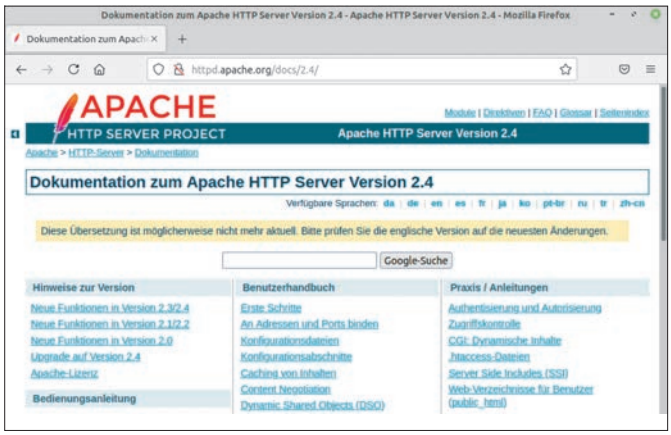
5. Die Standardkonfiguration „000-default.conf“

Öffnen Sie die Konfigurationsdatei „/etc/sites-available/000-default.conf“ in einem Editor. In der ersten Zeile steht „<VirtualHost *:80>“. Das Konzept der virtuellen Hosts ermöglicht, dass mehrere Websites mit unterschiedlichen IP-Adressen und/oder Domainnamen unter einem Apache-Webserver laufen.

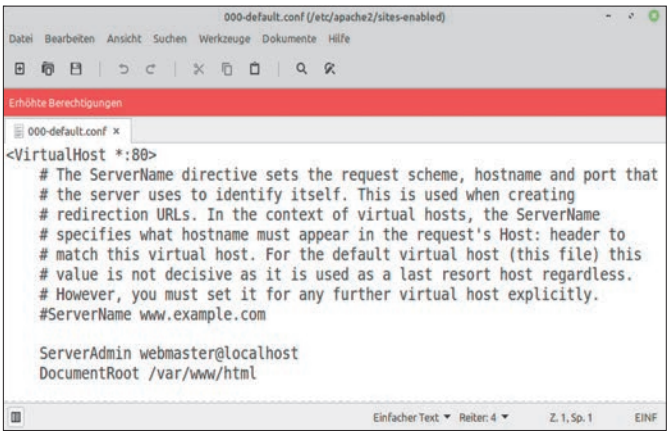
Die Angabe „*:80“ bewirkt, dass Apache für alle IP-Adressen zuständig ist, für die Anfragen auf Port 80 eingehen.

Die Datei endet in der letzten Zeile mit „</VirtualHost>“ – eine Struktur, die Sie vielleicht von HTML-Seiten kennen. „<...> ... </...>“ bilden einen Container. Dazwischen stehen Direktiven, die die Konfiguration des virtuellen Hosts festlegen.

Bei den meisten Bezeichnungen unterscheidet Apache nicht zwischen Groß- und Kleinschreibung, bei Argumenten für Direktiven und Variablen dagegen schon. Es ist daher besser, die gemischte Groß-Kleinschreibung beizubehalten, wie Sie sie in den vorhandenen Dateien und der Apache-Dokumentation finden (*http://httpd.apache.org/docs/2.4/*)



Informationen über Apache: Unter *http://httpd.apache.org/docs/2.4/* finden Sie eine umfangreiche Dokumentation zum Webserver – größtenteils in Deutsch.



Standard-Webseite: In der Datei „000-default.conf“ ist die Standard- und Beispielkonfiguration für Inhalte aus dem Ordner „/var/www/html“ enthalten.

Speicherort der Webseiten: Die Direktive „DocumentRoot“ gibt das Verzeichnis an, aus dem Apache Webseiten ausliefert. Liegt hier eine Datei mit dem Namen „index.html“ wird diese verwendet. Wenn PHP installiert ist und die Datei „index.php“ vorhanden ist, kommt diese zum Einsatz. Wie die Dateien heißen können, ist in „/etc/apache2/mods-available/dir.conf“ festgelegt. Ist keine der aufgeführten Dateien vorhanden, zeigt Apache einfach den Verzeichnisinhalt. Man kann die Dateien dann herunterladen und beispielsweise Bilder direkt im Browser öffnen. Sollte das nicht erwünscht sein, baut man

```
<Directory /var/www/html>
Options -Indexes
</Directory>
```

an beliebiger Stelle zwischen „<VirtualHost *:80>“ und „</VirtualHost>“ ein. Die Anzeige des Verzeichnisinhalts samt Unterverzeichnissen wird dann verweigert. Eine einfache Alternative ist, eine leere Datei mit dem Namen „index.html“ in jedem Ordner unterzubringen, dessen Inhalt nicht angezeigt werden soll. Der Zugriff auf Dateien ist trotzdem möglich, wenn man den exakten Namen kennt.

Logdateien: Apache protokolliert Fehlermeldungen und Zugriffe. In welchen Dateien die Meldungen landen, ist hinter „ErrorLog“ (Fehler) und „CustomLog“ (Zugriffe) definiert.

Die Variable „APACHE_LOG_DIR“ aus der Datei „envvars“ verweist auf den Basisordner „/var/log/apache2“. Wenn Sie mehrere virtuelle Hosts erstellen, empfiehlt es sich, unterschiedliche Logdateien zu verwenden. Das ist bei der Suche nach Fehlern übersichtlicher.

6. Neue Konfigurationsdatei erstellen

Im Prinzip können Sie mehrere „VirtualHost“-Blöcke in einer einzigen Datei unterbringen. Ein besserer Stil ist jedoch, dem modularen Ansatz von Apache zu folgen und jede Konfiguration in einer eigenen Datei unterzubringen.

Wenn Sie einen weiteren virtuellen Host benötigen, erstellen Sie einfach eine Kopie der Standarddatei:

```
cd /etc/apache2/sites-available
sudo cp 000-default.conf 001-test.
  conf
```

Öffnen Sie „001-test.conf“ in einem Editor. Bei einem Server im Rechenzentrum würde man jetzt die Internetdomäne hinter „ServerName“ eintragen. Denn hier kann man mehrere Domains und Subdomains registrieren, deren DNS-Eintrag auf dieselbe IP-Adresse verweist. Im privaten Netzwerk hat der Server nur einen Namen und Subdomains sind nicht ohne Weiteres möglich. Deshalb kann „ServerName“ mit vorangestelltem „#“ auskommentiert bleiben. Mehrere Webanwendungen sind trotzdem möglich, wenn man diese in unterschiedliche Ordner unterhalb von „/var/www“ installiert. Alternativ kann man einem Rechner auch mehrere IP-Adressen geben (siehe Seite 80) und dann bei einem virtuellen Host statt „*:80“ die Angabe „[IP-Adresse]:80“ verwenden.

Es ist aber einfacher, einen anderen Port zu verwenden, den Sie beispielsweise mit

```
<VirtualHost *:8088>
```

festlegen. In die Datei „ports.conf“ tragen Sie zusätzlich die Zeile

```
Listen 8088
```

ein.

Hinter „DocumentRoot“ geben Sie das Verzeichnis für die neue Website an (Beispiel):

```
DocumentRoot /var/www/html2
```

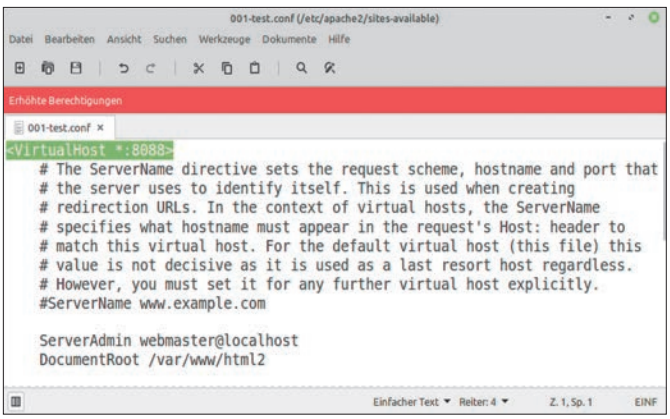
Erstellen Sie in diesem Ordner eine „index.html“. Dann aktivieren Sie die neue Website mittels

```
a2ensite 001-test
```

und informieren Apache über die Änderung:

```
sudo systemctl reload apache2
```

Sie können die Seite jetzt mit *http://[Server]:8088* im Browser aufrufen. ■



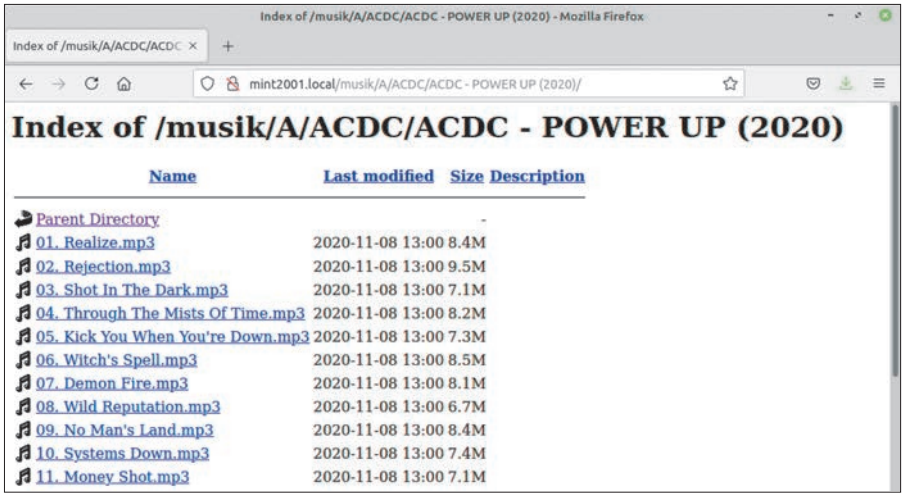
Zweite Website: In der weiteren Site-Konfiguration „001-test.conf“ verwenden Sie als Port beispielsweise „8088“, außerdem geben Sie einen anderen Ordner hinter „DocumentRoot“ an.

Anwendungen für Webserver

Ein Webserver kann im heimischen Netzwerk viele Aufgaben übernehmen. Er kann beispielsweise Fotos präsentieren, Audio- und Videodateien streamen oder eine Zentrale für Dokumente und Notizen anbieten.

VON THORSTEN EGGELING

Dienste auf einem Webserver stehen allen Geräten im lokalen Netzwerk zur Verfügung, etwa auf dem Smartphone, TV-Gerät oder anderen PCs. Ohne besonders aufwendige Konfiguration lassen sich Dateien vom Webserver herunterladen oder Audio- und Videodateien streamen. Für mehr Funktionen installieren Sie passende Webanwendungen, von denen wir hier einige vorstellen. Wir gehen in diesem Artikel davon aus, dass Apache, PHP und Maria DB installiert sind, wie ab Seite 50 beschreiben, und dass Sie die Standardkonfiguration nicht geändert haben.



Einfach und schlicht: Apache zeigt automatisch den Inhalt von Ordnern an, wenn die Datei „index.html“ fehlt. MP3-Dateien lassen sich auch direkt im Browser abspielen.

Webserver für den Zugriff auf Dateien

Es muss nicht immer Samba sein: Auch Apache kann bereits ohne zusätzliche Software für den Download von Dateien dienen, Audio- und Videodateien streamen oder Bilddateien ausliefern. Dazu genügt es, unter „/var/www/html“ einen neuen Ordner anzulegen, beispielsweise mit dem Namen „Musik“. Kopieren Sie dann die gewünschten Verzeichnisse mit Audiodateien in diesen Ordner. Damit Apache die Dateien lesen kann, ändern Sie den Eigentümer:

```
sudo chown -R www-data:www-data /
  var/www/html/Musik
```

Öffnen Sie dann in einem Browser die Adresse „http://[IP oder Servername]/Musik“, so zeigt Apache mit Hilfe des Moduls „Autoindex“ den Inhalt des Ordners an. Was beim Klick auf eine Datei passiert, hängt vom Inhalt ab. Formate wie MP3, OGG oder Flac lassen sich streamen und der Browser kann die Dateien im integrierten Player abspielen. Bei Videos funktioniert das mit MP4-Dateien. Bilddateien (in den Formaten JPG, PNG, GIF) sowie PDFs zeigt der Browser ebenfalls an. Bei allen anderen Formaten lädt der Browser die Dateien herunter oder bietet die Option „Öffnen mit“, hinter der Sie die gewünschte Anwendung wählen.

Webdav für den Zugriff auf Dateien

Webdav (Web-Distributed Authoring and Versioning) ist eine Erweiterung des HTTP-Protokolls. Sie erhalten darüber Lese- und Schreibzugriff auf den Webserver. Für Webdav aktivieren Sie zwei Apache-Module:

```
sudo a2enmod dav
sudo a2enmod dav_fs
```

Erstellen Sie dann einen Ordner, den Sie für den Datenaustausch verwenden wollen, und geben Sie dem Webserver Zugriffsrechte (Beispiel):

```
sudo mkdir /srv/webdav
sudo chown -R www-data:www-data /
  srv/webdav
```

Bearbeiten Sie die Apache-Konfiguration „/etc/apache2/sites-enabled/000-default.conf“. Bauen Sie oberhalb von „</VirtualHost>“ die folgenden neun Zeilen ein:

```
<Directory /srv/webdav/>
Options Indexes MultiViews
Require all granted
</Directory>
Alias /webdav /srv/webdav/
<Location /webdav>
DAV on
Options +Indexes
</Location>
```

Danach starten Sie den Webserver neu:

```
sudo systemctl restart apache2
```

Auf Webdav-Freigaben zugreifen: In den Dateimanagern Nautilus oder Nemo tippen

Sie in die Adresszeile (Strg-L) eine URL in dieser Form ein:

```
dav://[IP oder Servername]/webdav
```

Sicherheit: Jeder Rechner im lokalen Netzwerk hat bei dieser Konfiguration Lese- und Schreibzugriff auf den Webdav-Ordner. Solchen globalen Schreibzugriff können Sie einfach mit

```
sudo chown -R root:root /srv/webdav
```

unterbinden.

Fotogalerie mit Piwigo

Piwigo (*https://piwigo.org*) ist eine funktionsreiche Galerieanwendung, mit der sich Bilder in Alben organisieren und mit Schlagwörtern und Beschreibungen versehen lassen. Sie können einzelne Bilder betrachten oder eine Diashow starten.

Vorbereitungen: Piwigo benötigt einige zusätzliche PHP-Module, die Sie mit

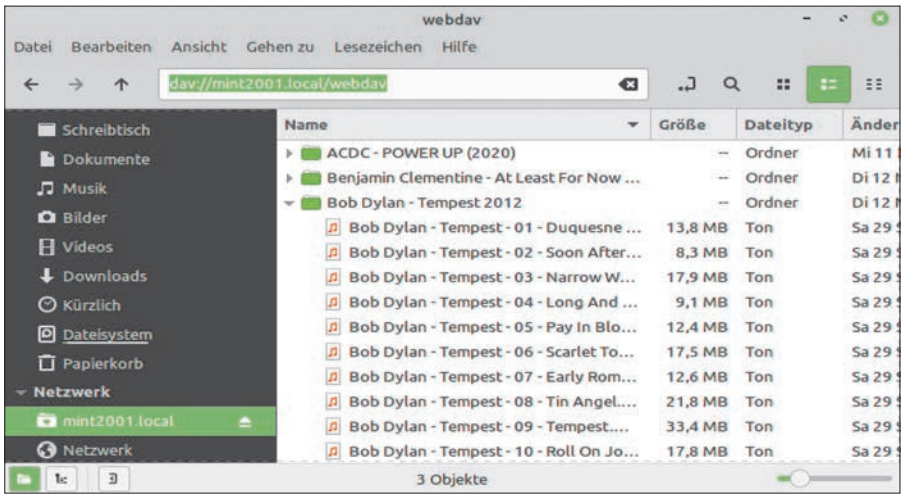
```
sudo apt install php-mbstring php-
  xmlrpc php-gd php-xml php-intl
  php-mysql php-cli php php-ldap
  php-zip php-curl
```

installieren. Eine Datenbank für Piwigo müssen Sie selbst erstellen. Öffnen Sie im Browser „http://[IP oder Servername]/phpmyadmin“ und melden Sie sich an (siehe Artikel ab Seite 50). Klicken Sie auf „Benutzerkonten“ und dann auf „Benutzerkonto hinzufügen“. Erstellen Sie einen Benutzer mit dem Namen „piwigo“ und vergeben Sie ein Passwort. Setzen Sie ein Häkchen vor „Erstelle eine Datenbank mit gleichem Namen und gewähre alle Rechte“ und klicken Sie auf „OK“.

Piwigo installieren: Laden Sie das ZIP-Archiv über *https://piwigo.org/get-piwigo* herunter, entpacken Sie die Datei und kopieren Sie den kompletten Ordner „piwigo“ nach „/var/www/html“. Als Eigentümer des Ordners bestimmten Sie dann „www-data“:

```
sudo chown -R www-data:www-data /
  var/www/html/piwigo
```

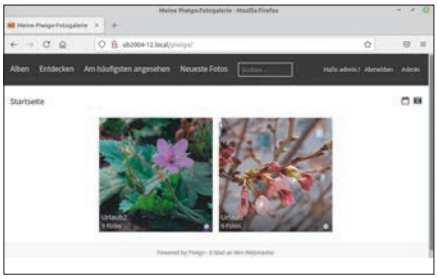
Rufen Sie im Browser die URL „http://[IP oder Servername oder IP]/piwigo“ auf. In das Formular tragen Sie hinter „Benutzer“ den Namen „piwigo“ ein, darunter das beim Anlegen der Datenbank vergebene Passwort sowie den Datenbanknamen „piwigo“. Unter „Administrationseinstellungen“ legen Sie Benutzernamen und Passwort für Piwigo fest. Klicken Sie auf „Start der Installation“ und danach auf „Fotos hinzufügen“ und „Erstes Album hinzufügen“. Dann vergeben Sie einen Namen für das neue Album und laden die Dateien hoch.



Webdav-Freigaben: Im Linux-Dateimanager greifen Sie über eine URL mit vorangestelltem „dav://“ auf einen Webdav-Ordner zu – bei Bedarf auch mit Schreibzugriff.

Streamingserver für Audio und Video

Ampache (*https://ampache.org*) ist eine Streaming-Anwendung vor allem für Audiodateien. Die Weboberfläche zeigt Coverbilder für Alben und MP3-Tags an. Die Audiowiedergabe kann im Browser über den HTML5-Webplayer von Ampache erfolgen. Der Zugriff von anderen Geräten aus ist über UPnP (Universal Plug and Play) möglich. Webdav bietet Ampache ebenfalls, was den Zugriff über den Dateimanager ermöglicht. Ampache kann auch Videos streamen und nicht streambare Formate wie MKV-Dateien automatisch konvertieren. Die Systembelastung ist dabei relativ hoch, weshalb Ampache etwa für große HD-Videodateien nur eingeschränkt zu empfehlen ist. Andere Lösungen eignen sich dafür besser (siehe Kasten „ Weitere Server“).



Fotos komfortabel präsentieren: Piwigo organisiert Bilder in Alben, die Sie sich im Browser anzeigen lassen. Eine Diashow ist ebenfalls möglich.

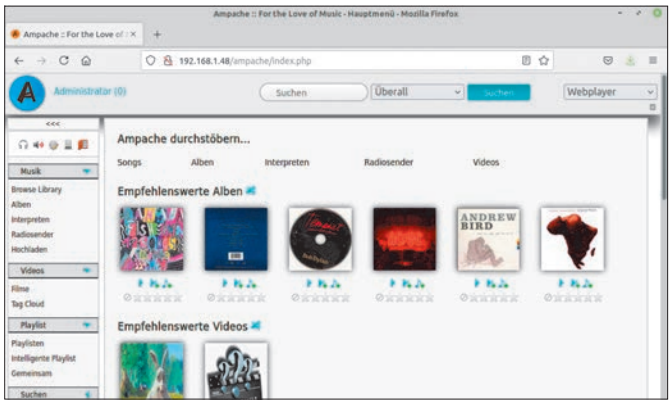
Vorbereitungen: Die Webanwendung benötigt einige zusätzliche PHP-Module und Programme, die Sie mit

```
sudo apt install ffmpeg php-mysql
  php-curl php-xml php-gd
```

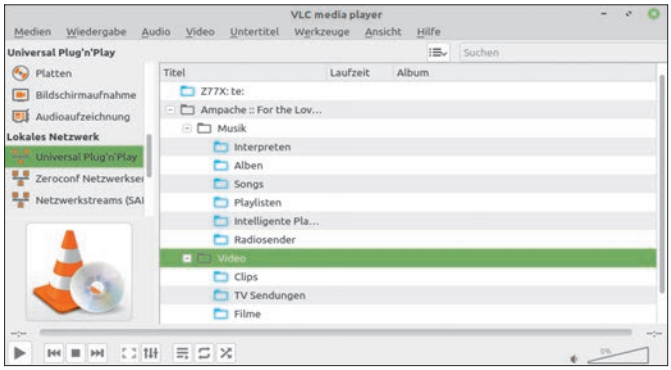
WEITERE SERVER FÜR MULTIMEDIA

Apache plus geeignete Webanwendung ist vielseitig einsetzbar. Für manche Aufgaben sind jedoch Spezialisten noch besser: Kodi (*https://kodi.tv*) ist eine Multimedia-Oberfläche für den PC, den man am besten ans TV-Gerät anschließt. Als eigenes Mini-Betriebssystem für Kodi eignet sich Libre Elec (*https://libreelec.tv*) besonders gut für den Raspberry Pi. Die Steuerung ist über eine Infrarotfernbedienung, Smartphone-Apps oder eine Browseroberfläche möglich. Via UPnP stellt Kodi die Medien anderen Abspielgeräten zur Verfügung. Allerdings kann Kodi Videoformate für das Streaming nicht in Echtzeit konvertieren, weshalb die UPnP-Wiedergabe zwar etwa mit VLC, aber meist nicht mit TV-Geräten funktioniert.

Eine Alternative ist der Plex Media Server (*www.plex.tv*) mit ähnlichen Funktionen wie Kodi, der aber die Videos auch konvertieren kann. Die dazu passende Plex-App gibt es beispielsweise für Android, iOS, Amazon Fire TV und zahlreiche TV-Geräte. Wer sich für eine dieser Lösungen interessiert, findet ausführliche Beschreibungen unter *www.pcwelt.de/2301815* und *www.pcwelt.de/2033800*.



Musik mit Ampache: Die Webanwendung zeigt in einer aufgeräumten Oberfläche Alben und Musiktitel an. MP3-Dateien lassen sich über HTML5 im Browser abspielen.



Es muss nicht immer der Browser sein: Ampache kann Medien per UPnP freigeben, der Zugriff erfolgt dann etwa mit dem VLC Player oder anderen UPnP-Apps.

installieren. Aktivieren Sie zunächst das Apache-Rewrite-Modul:

```
sudo a2enmod rewrite
```

In der Apache-Konfiguration „/etc/apache2/sites-enabled/000-default.conf“ bringen Sie dann folgenden Block unter:

```
<Directory /var/www/html/ampache>
AllowOverride All
Require all granted
</Directory>
```

Danach starten Sie Apache neu:

```
systemctl restart apache2
```

Ampache installieren: Laden Sie das ZIP-Archiv aus dem Downloadbereich von *https://ampache.org* herunter und entpacken es nach „/var/www/html/ampache“. Ändern Sie die Zugriffsrechte mit diesen zwei Befehlen:

```
sudo chown -R www-data:www-data /
  var/www/html/ampache
sudo chmod -R 774 /var/www/html/
  ampache/config
```

Rufen Sie im Browser „http://[[IP oder Servername]/ampache“ auf. Folgen Sie den Anweisungen des Installationsassistenten. Dieser prüft zuerst die Voraussetzungen und weist Sie auf fehlende Module hin. Danach geben Sie die Verbindungsdaten zum Maria-DB-Server ein, setzen ein Häkchen hinter „Erstelle Datenbankbenutzer“ und vergeben für den neuen Benutzer „ampache“ ein Passwort. In „Schritt 2 – Erstellen der Konfigurationsdateien“ wählen Sie „Standard“ als Installationstyp und „ffmpeg“ hinter „Beispielkonfiguration“. Unter „Player“ setzen Sie Häkchen vor „UPnP“ und „Webdav“, sofern Sie diese Funktionen nutzen möchten. Im letzten Schritt erstellen Sie einen administrativen Benutzer für Ampache, mit dessen Konto Sie sich danach anmelden.

Musik hinzufügen: Klicken Sie links oben auf das vorletzte Symbol „Admin“ und dann auf „Katalog hinzufügen“. Vergeben Sie hinter „Katalogname“ eine aussagekräftige Bezeichnung, hinter „Katalogtyp“ stellen Sie „local“ ein und hinter „Medientyp des Kataloges:“ wählen Sie „Musik“. Tippen Sie hinter „Pfad:“ den Pfad zum Ordner ein, in dem die Musikdateien liegen.

Wechseln Sie über das erste Symbol links oben zurück ins Hauptmenü. Über „Browse Library“ oder „Alben“ können Sie jetzt Musiktitel ansehen und abspielen.

Videos hinzufügen: Gehen Sie auf das „Admin“-Menü und dann auf „Optionen“. Hinter „Videofunktionen erlauben“ stellen Sie „An“ ein, setzen ein Häkchen in der Spalte „Für alle anwenden“ und klicken auf „Einstellungen aktualisieren“.

Erstellen Sie einen neuen Katalog über „Katalog hinzufügen“. Hinter „Medientyp des Kataloges:“ wählen Sie „Film“ oder „TV-Sendung“ aus. Sollten sich größere Videodateien nicht abspielen lassen, erhöhen Sie in der Datei „/var/www/html/ampache/config/ampache.cfg.php“ den Wert hinter „memory_limit“, beispielsweise auf „1024M“ oder „4096M“.

UPnP aktivieren: Gehen Sie im „Admin“-Menü auf „System“ und setzen Sie „UPnP Backend verwenden“ auf „An“. In der Konfigurationsdatei „/var/www/html/ampache/config/ampache.cfg.php“ entfernen Sie das Kommentarzeichen „;“ vor „http_host“ und tragen Sie dahinter den Namen Ihres Servers mit angehängtem „.local“ ein:

```
http_host = "servername.local"
```

Statt „Servername“ können Sie auch die IP-Adresse verwenden.

Entfernen Sie das Kommentarzeichen vor der folgenden Zeile

```
websocket_address = "ws://
  localhost:8100"
```

und speichern Sie die Datei.

Die von uns getestete Ampache-Version 4.4.3 enthält einen Fehler, der im Zusammenhang mit neueren PHP-Versionen auftritt. Um ihn zu beheben, ändern Sie in der Datei „/var/www/html/ampache/lib/class/upnp_api.class.php“ in Zeile 272 den Code

```
$result =
  XMLReader::XML($prmRequest);
```

in

```
$result = $reader-
  >XML($prmRequest);
```

Rufen Sie im Browser die URL „http://[IP oder Servername]/ampache/upnp/?btnSend=Send+SSDP+broadcast“ auf und klicken Sie auf „Send SSDP broadcast every second“. Starten Sie dann den VLC Media Player und gehen Sie auf „Ansicht → Wiedergabeliste“, danach auf „Universal Plug'n'Play'. Der Ampache-UPnP-Server ist unter dem Namen „Ampache :: For the Love of Music“ zu sehen. Öffnen Sie einen Ordner wie „Musik → Alben“, um Dateien in VLC wiederzugeben.

Damit sich der UPnP-Server automatisch im Netzwerk bekanntmacht, öffnen Sie die Datei „/etc/crontab“ in einem Editor und fügen diese neue Zeile ein:

```
* * * * * www-data /usr/bin/php /var/
  www/html/ampache/bin/broadcast.
  inc
```

Mit diesem Cronjob wird minütlich eine Nachricht im Netzwerk versendet.

Webdav nutzen: Gehen Sie im „Admin"-Menü auf „System" und stellen Sie „WebDAV Backend verwenden" auf „An". Im Linux-Dateimanager verwenden Sie dann in der Adresszeile eine URL in der Form „dav://[IP oder Servername]/ampache/webdav/index.php".

Webanwendung für Notizen und Bilder

Dokuwiki (*www.dokuwiki.org*) ist ein Content-Management-System, das nur geringe Systemressourcen und keine Datenbank erfordert. Sie können darin Notizen, Bilder und andere Informationen speichern. Neben Apache und PHP sind drei zusätzliche PHP-Module erforderlich:

```
sudo apt install php-gd php-xml php-
 json
```

Laden Sie das Installationspaket über *https://download.dokuwiki.org* herunter und entpacken Sie es. Kopieren Sie den Ordner „dokuwiki" nach „/var/www/html", und setzen Sie dort die Zugriffsrechte:

```
sudo chown -R www-data:www-data /
 var/www/html/dokuwiki
```

Rufen Sie im Browser „http://[IP oder Servername]/dokuwiki/install.php?l=de" auf. Geben Sie dem Wiki einen Namen und legen Sie einen administrativen Benutzer mit Passwort fest. Klicken Sie auf „Speichern" und dann auf den Link „Ihr neues DokuWiki". Die Willkommensseite zeigt eine kurze Einführung in englischer Sprache, mit weiterführenden Links etwa zur „syntax page". Hier wird Ihnen erklärt, wie sich Wiki-Seiten formatieren lassen.

Cloudserver für das Heimnetz

Die Zielgruppe von Nextcloud (*https://nextcloud.com*) sind vor allem Teams, die online zusammenarbeiten. Nextcloud ist aber auch für das Heimnetz attraktiv. Die Webanwendung bietet Speicherplatz für Dateien jeder Art inklusive einem Online-Office-Paket (Collabora Office). Module für Bildergalerien, Aufgaben, Kalender sowie ein HTML5-Player für Audio- und Videoinhalte sind ebenfalls dabei. Die Software erfordert zahlreiche PHP-Module – welche genau, hängt von den verwendeten Apps ab. Die komplette Liste finden Sie über *https://m6u.de/nxcp*.

Schritt 1: Klicken Sie auf der Seite *https://nextcloud.com/install* auf „Download for Server" und dann auf „Download Nextcloud". Entpacken Sie das ZIP-Archiv und kopieren Sie den Ordner „nextcloud" nach „/var/www/html". Hier setzen Sie die Zugriffsrechte:

```
chown -R www-data:www-data
 nextcloud
```

Schritt 2: Fügen Sie in die Apache-Konfiguration „/etc/apache2/sites-enabled/000-default.conf" diese neun Zeilen ein:

```
<Directory /var/www/html/
 nextcloud/>
Options +FollowSymlinks
AllowOverride All
<IfModule mod_dav.c>
Dav off
</IfModule>
SetEnv HOME /var/www/html/
 nextcloud
SetEnv HTTP_HOME /var/www/html/
 nextcloud
</Directory>
```

Schritt 3: Öffnen Sie die Datei „/etc/php/7.4/apache2/php.ini" (Pfad je nach PHP-Version anpassen). Ändern Sie dort den Wert für „memory_limit":

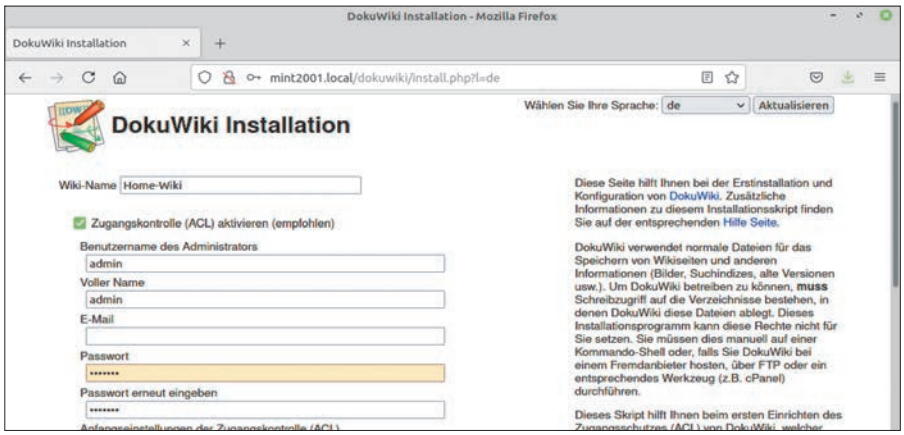
```
memory_limit = 512M
```

Schritt 4: Starten Sie Apache dann neu:

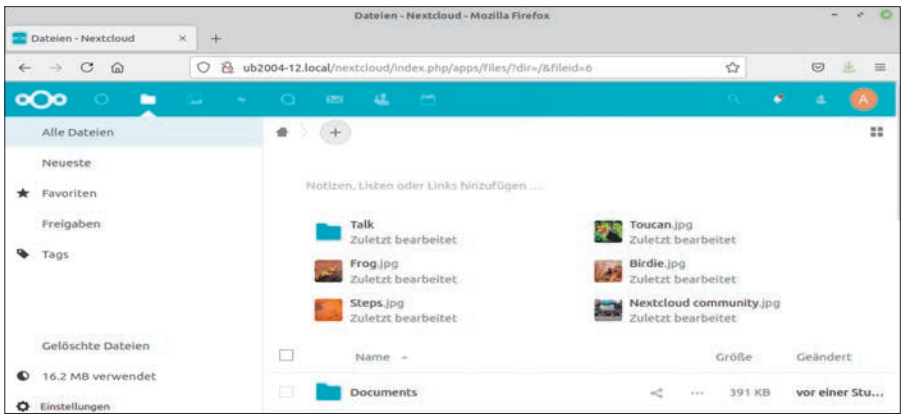
```
sudo systemctl restart apache2
```

Schritt 5: Öffnen Sie im Browser „http://[IP oder Servername]/nextcloud". Tragen Sie Benutzername und Passwort für den Administrator ein, außerdem den Datenbank-Benutzer („root") und sein Passwort. Als Datenbanknamen vergeben Sie beispielsweise „nextcloud". Klicken Sie auf „Installation abschließen".

Bei unserer Installation versuchte Nextcloud anschließend, die Adresse „http://nextcloud/index.php/core/apps/recommended" zu öffnen. Das ist ein erwartbarer Umleitungsfehler, weil eine Einrichtung in einem Unterverzeichnis eigentlich nicht vorgesehen ist. Ergänzen Sie daher die URL mit „http://[IP oder Servername]/nextcloud/index.php/core/apps/recommended", um mit der Installation fortzufahren. Danach können Sie Nextcloud verwenden. Eine Benutzeranleitung finden Sie unter *https://m6u.de/nxum*. ■



Wiki für Notizen, Dokumente und Bilder: Dokuwiki benötigt keine Datenbank und auch nicht viel Konfiguration. Sie müssen nur einen administrativen Nutzer mit Passwort erstellen.



Nextcloud bietet viele Funktionen, benötigt dann aber auch einige Systemressourcen. Wer auf einige Apps verzichtet, kann Nextcloud auch auf schwächerer Hardware einsetzen.

Nextcloud: Der eigene Cloudserver

Dateien lassen sich über viele unterschiedliche Methoden im eigenen Netzwerk und im Internet bereitstellen. Die durchdachte Weboberfläche eines Cloudservers wie Nextcloud bietet jedoch den meisten Komfort.

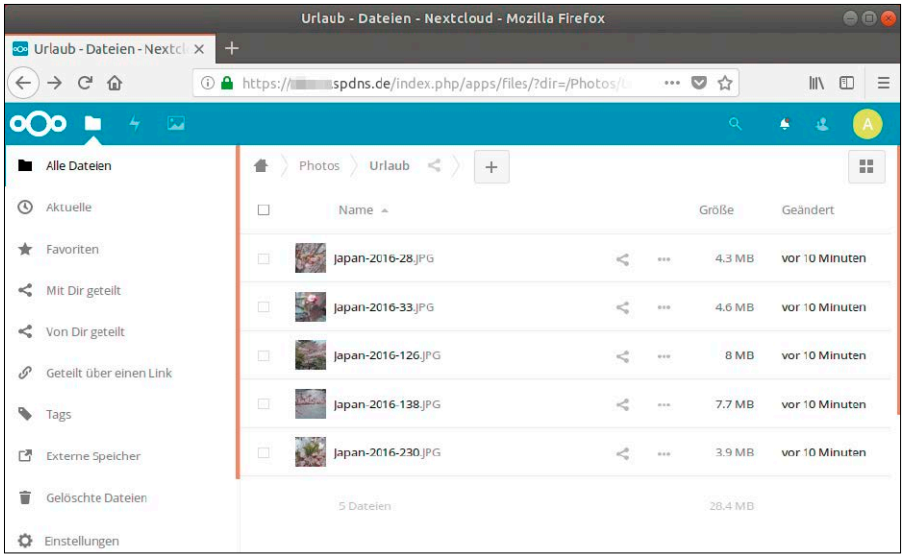
VON THORSTEN EGGELING

Der Begriff „Cloud“ ist in der Werbung allgegenwärtig. Bilder, Dokumente, Backups, virtuelle Maschinen und Anwendungen – alles ist Cloud und gehört in die Cloud. Letztlich verbirgt sich hinter dem Begriff aber nichts anderes als Speicherplatz auf einem Server im Internet oder Anwendungen, die auf einem Server laufen. In der Regel befindet sich der Server in einem Rechenzentrum.

Je nach Tarif steht Ihnen nur Onlinespeicher zur Verfügung, oder Sie nutzen vorinstallierte Webdienste, oder Sie mieten ein voll ausgestatteten Server, auf dem Sie selbst Webanwendungen einrichten. Ist eine schnelle Internetanbindung vorhanden, kann für kleine Firmen beziehungsweise Teams auch ein Server zu Hause im eigenen Netzwerk ausreichen.

Wer nur ab und zu Dateien auf einem Server ablegen oder anderen Personen zur Verfügung stellen möchte, benötigt keine spezielle Software. Dafür genügen Tools, die bei einer Linux-Standardinstallation bereits vorhanden sind (siehe Artikel ab Seite 42). Für mehr Komfort verwenden Sie eine Webanwendung, die sich über den Browser bedienen lässt. Neben dem Austausch von Dateien gehören Diashows und eingebettet Videoplayer zum Funktionsumfang. Für die Teamarbeit gibt es Kalender, To-do-Listen, eine Versionskontrolle für Dateien und eine Benutzerkontenverwaltung.

Über Plug-ins lassen sich weitere Funktionen nachrüsten, etwa für die gemeinsame Arbeit an Office-Dokumenten (siehe Beitrag ab Seite 37).



Cloudserver: Nextcloud bietet eine übersichtliche Weboberfläche, über die sich Dateien hochladen und teilen lassen. Für Fotos gibt es auch eine Galerieansicht.

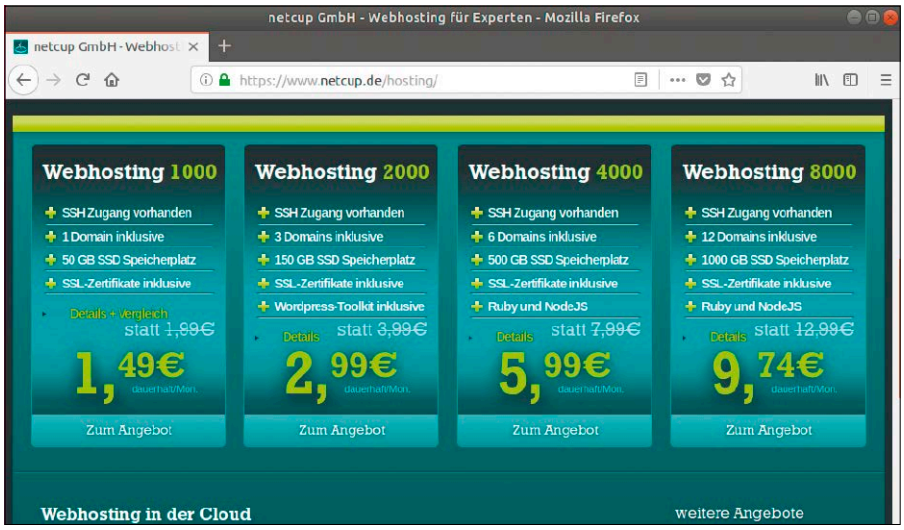
Hinweis: Eine Textdatei mit allen Befehlszeilen aus diesem Artikel sowie weiteren Anleitungen können Sie über *www.pcwelt.de/Z6an9V* herunterladen.

1. Der Server für die eigene Cloud

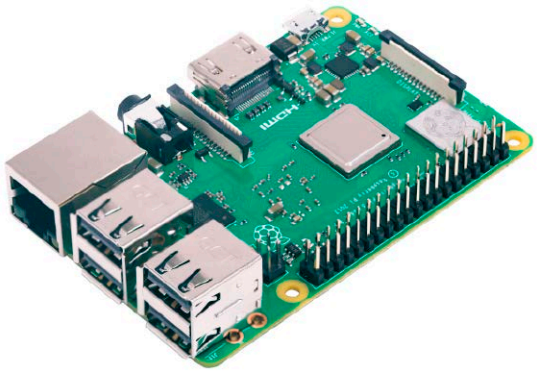
Dank schneller Internetanbindung ist es möglich, Teile der Netzwerkinfrastruktur aus dem eigenen Netzwerk auf Server in Rechenzentren zu verlagern. Lohnend ist das vor allem für Firmen, die auf diesem Weg flexibel Speicherplatz und Rechenleistung anmieten können, etwa um Leistungsspitzen abzufangen. Wird der Dienst nicht mehr benötigt, lässt er sich schnell kündigen, was Kosten einspart.

Es gibt jedoch Bedenken: Die eigenen Dateien landen auf einem Server irgendwo im Internet. Es ist ungewiss, welche Personen in welchem Land Zugriff auf die Daten erlangen können und ob die Datenschutzbestimmungen tatsächlich eingehalten werden. Die Betreiber garantieren zwar die Sicherheit, was sich aber kaum zweifelsfrei überprüfen lässt. Eine Alternative ist die eigene Cloud. Die erforderliche Software kann auf einem PC zu Hause laufen, wenn die Internetanbindung schnell genug ist (Upload!). Andernfalls müssen sich Nutzer, die etwas von Ihrem Server herunterladen möchten, in Geduld üben. Für schnellere Downloads mieten Sie einen Server bei einem der zahlreichen Webhoster.

Bei einem Server im Rechenzentrum können Sie sich zwar auch nicht sicher sein, wer Zugriff auf Ihre Dateien hat, Sie haben jedoch volle Kontrolle über die installierte Software und die verwendete Verschlüsse-



Server im Internet: Webhosting-Pakete gibt es schon für wenige Euro im Monat. Die Server eignen sich als Datenspeicher sowie für die Installation einer eigenen Cloudsoftware.



Sparserver: Ein Mini-PC wie der Raspberry Pi kostet nicht viel und ist sparsam im Betrieb. Die Leistung ist für die Basisfunktionen von Nextcloud ausreichend.

lung. Allerdings sind Sie dann selbst für die Sicherheit des Servers verantwortlich. Das gilt auch, wenn Sie den Server zu Hause im eigenen Netzwerk betreiben.

Wichtiger Hinweis: Wenn der heimische Server von außen über das Internet erreichbar sein soll, richten Sie vor der Nextcloud-Installation einen Domainnamen und Portfreigaben ein, wie im Kasten „Kostenlose Domains" sowie in Punkt 3 beschrieben.

2. Software für die eigene Cloud

Eine erste Version von Owncloud erschien im Jahr 2010 (*https://owncloud.org*). Inzwischen bietet die Software fast alles, was für den Datenaustausch erforderlich ist, beispielsweise Kalender, Adressbuch, Fotogalerie, Wiedergabe von und Musik- und Videos sowie gemeinsames Arbeiten an Dokumenten. Über Plug-ins lassen sich die Funktionen erweitern. Der Zugriff erfolgt über eine Weboberfläche oder Sie verwenden eine Clientsoftware für Windows, Mac-OS, Linux, Android oder iOS, um einen lokalen Ordner mit dem Cloudserver zu synchronisieren.

Nextcloud (*https://nextcloud.com*) ist eine Abspaltung von Owncloud, die erstmals 2016 erschien. Ein genauer Vergleich ist schwierig, weil beide Anbieter regelmäßig Updates veröffentlichen. Nextcloud bietet zur Zeit einige Funktionen mehr als Owncloud, weshalb wir die Nextcloud-Installation in diesem Artikel behandeln. Die Anleitung gilt aber weitestgehend auch für Owncloud.

Als Betriebssystem für den Server haben wir Ubuntu 18.04 auf einem PC im heimischen Netzwerk gewählt. Als Alternative zu Ubuntu bietet sich ein Raspberry Pi mit Raspbian an. Soll der Server 24 Stunden in Betrieb sein, ist das eine besonders energiesparende Lösung. Allerdings bietet der Mini-PC wenig Leistung und eignet sich daher nur für die private Nutzung und kleine Arbeitsgruppen. Die meisten Nextcloud-Funktionen lassen sich auch auf dem Raspberry Pi nutzen. Für ein Cloud-Office mit Collabora oder Onlyoffice, die beide viel Hauptspeicher benötigen (siehe folgenden Artikel ab Seite 37), ist der Raspberry Pi ungeeignet.

3. Portfreigaben für den Server einrichten

Wer einen heimischen Cloudserver über das Internet erreichen will, muss einen oder mehrere Ports nach außen öffnen. Damit sich auch IPv6 für Freigaben nutzen lässt, ändern Sie zuerst die Linux-Konfiguration. Standardmäßig kommen bei fast allen Systemen IPv6-Adressen zum Einsatz, die per Zufall erzeugt werden und sich regelmäßig ändern. Für die Portfreigabe sind

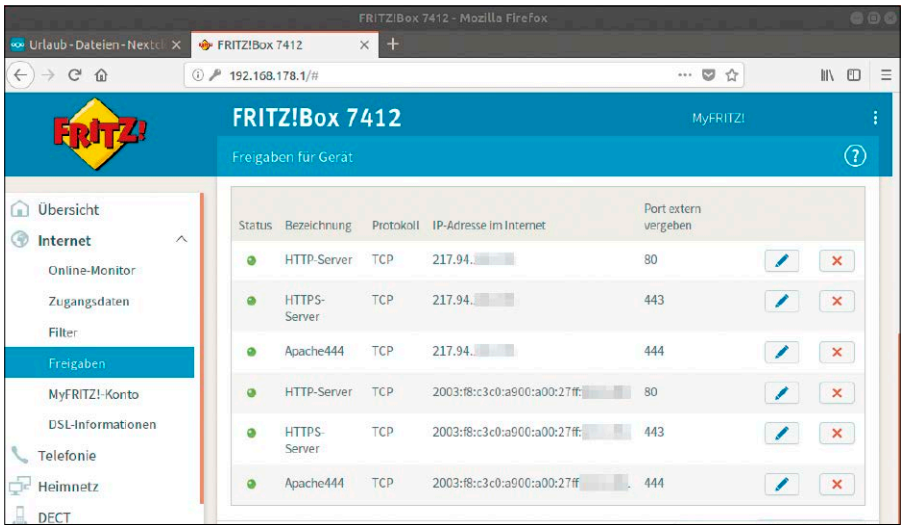
KOSTENLOSE DOMAINS FÜR DYNAMISCHE IP-ADRESSEN

Bei den meisten DSL-Anschlüssen ändert sich die IP-Adresse automatisch in regelmäßigen Abständen. Damit der Server im Heimnetzwerk immer über die gleiche URL erreichbar ist, verwenden Sie einen kostenlosen Dienst für dynamische IP-Adressen, beispielsweise *https://spdyn.de*. Dabei gibt es jedoch eine Einschränkung: Ihr DSL-Router muss über eine öffentliche IPv4-Adresse verfügen, damit er sich über IPv4 von jedem Gerät im Internet ansprechen lässt. Wenn Ihr DSL-Anbieter nur Dual Stack Lite (DS-Lite) zur Verfügung stellt, besitzen Sie nur eine öffentliche IPv6-Adresse, die dann auch nur für Computer nutzbar ist, die Zugang zum Ipv6-Internet haben – und das ist nicht an jedem Ort der Welt gewährleistet.

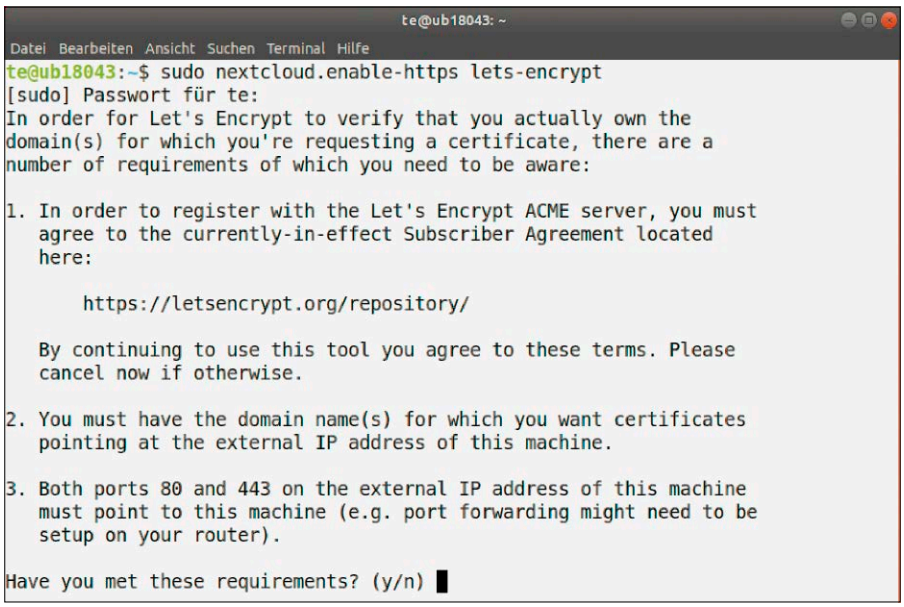
Was für Ihren DSL-Anschluss gilt, finden Sie über die Konfigurationsoberfläche des Routers heraus. Bei einer Fritzbox (*http://fritz.box*) beispielsweise sehen Sie auf der Übersichtsseite die IPv4- und IPv6-Adresse. Sollte die IPv4-Adresse fehlen (DS-Lite) können Sie nur IPv6 für Internetfreigaben nutzten.

Nach der Registrierung und Anmeldung bei *https://spdyn.de* legen Sie Ihre Wunschdomain über „IPv4-Host hinzufügen" und/oder „IPv6-Host hinzufügen" an. Tragen Sie dabei die in der Routeroberfläche ermittelten IP-Nummern ein.

Damit für Ihre Domain stets die aktuelle IP-Adresse hinterlegt ist, kann der DSL-Router die Informationen automatisch übermitteln. Anleitungen für mehrere Routermodelle finden Sie unter *https://wiki.securepoint.de/SPDyn/Hostverwenden*.



Fritzbox konfigurieren: Damit Ihr Cloudserver über das Internet erreichbar ist, sind Portfreigaben nötig. Fritz-OS legt automatisch IPv6-Portfreigaben an, wenn Sie IPv4-Freigaben erstellen.



SSL-Verschlüsselung: Das kostenlose Let's-Encrypt-Zertifikat lässt sich schnell in die Snap-App einbinden. Für die regelmäßige Erneuerung des Zertifikats sorgt Nextcloud automatisch.

jedoch Adressen erforderlich, deren gerätespezifischer Teil immer gleich bleibt. Unter Ubuntu führen Sie im Terminal diese Befehlszeile aus:

```
sudo gedit /etc/
  sysctl.d/10-ipv6-privacy.conf
```

Ändern Sie die Werte in der Datei:

```
net.ipv6.conf.all.use_tempaddr = 0
net.ipv6.conf.default.use_
  tempaddr = 0
```

Speichern Sie die Datei und laden Sie dann die nächste Datei:

```
sudo gedit /etc/network/interfaces
```

Tragen Sie hier diese vier Zeilen ein:

```
auto enp0s3
iface enp0s3 inet dhcp
iface enp0s3 inet6 auto
pre-up modprobe ipv6
```

„enp0s3" ersetzen Sie durch den Gerätenamen Ihres Netzwerkadapters (siehe „ip addr"). Speichern Sie die Datei und starten Sie Linux neu.

Wenn Sie einen Raspberry Pi verwenden, ändern Sie in der Datei „/etc/dhcpd.conf" die Option „slaac private" auf „slaac hwaddr" und starten Linux neu.

Ermitteln Sie im Terminalfenster die IPv6-Adresse:

```
ip -6 addr
```

Hinter „inet6" steht jetzt beispielsweise

```
2003:f8:c3c6:4f00:a00:27ff:fe54:
  cf81
```

Portfreigaben konfigurieren: Wie genau die Konfiguration des Routers durchzuführen ist, hängt vom jeweiligen Modell ab. Auf *https://portforward.com* finden Sie Anleitungen für zahlreiche Geräte in englischer Sprache.

Bei einer Fritzbox mit aktuellem Fritz-OS (Version 06.83 oder höher) gehen Sie auf „Internet → Freigaben" und dann auf die Registerkarte „Portfreigaben". Klicken Sie auf „Gerät für Freigaben hinzufügen" und wählen Sie hinter „Gerät" Ihren Server aus. Tragen Sie die „IPv6 Interface-ID" ein. Das sind die letzten vier Buchstaben-Ziffern-Gruppen, die Sie zuvor über *ip -6 addr* ermittelt haben. Klicken Sie auf „Neue Freigabe" und wählen Sie die Option „Portfreigabe". Wählen Sie hinter „Anwendung" den Eintrag „HTTP-Server" und bei „Port an Gerät" sowie „Port extern gewünscht" jeweils „80". Klicken Sie auf „OK" und danach noch einmal auf „OK". Fritz-OS erstellt dann automatisch eine Portfreigabe für IPv4 und IPv6.

4. Nextcloud als Snap-Paket installieren

Die Nextcloud-Installation gelingt am einfachsten als Snap-App. Dabei wird automatisch alles eingerichtet, was Sie für Nextcloud benötigen. In Ubuntu 18.04 ist Snapd bereits enthalten. Sollte das bei Ihrem System nicht der Fall sein (etwa bei Raspbian), holen Sie die Installation nach:

```
sudo apt update && sudo apt install
  snapd
```

Starten Sie Linux danach neu. Preisgünstige Webhoster bieten bisher meist keine Snap-Apps an und die Installation muss manuell erfolgen. Eine Anleitung dafür können Sie über *www.pcwelt.de/Z6an9V* herunterladen. Sollte der Apache-Webserver für andere Webanwendungen bereits auf dem PC installiert ist, deaktivieren Sie ihn in einem Terminalfenster vorübergehend mit

```
sudo systemctl stop apache2
```

Nextcloud bringt im Snap-Container seinen eigenen Apache-Server mit, der die Standardports 80 (HTTP) und 443 (HTTPS) nutzt. Nach der Ersteinrichtung lassen sich die Ports ändern und Sie können Apache dann wieder aktivieren (siehe Punkt 6).

Installieren Sie Nextcloud in einem Terminal mit dieser Zeile:

```
sudo snap install nextcloud
```

Der Server ist aus dem Internet erreichbar: Aktivieren Sie die SSL-Verschlüsselung und verwenden Sie ein allgemein gültiges Zertifikat. Dafür muss der Server über einen Domainnamen und Port 80 erreichbar sein (siehe Kasten „Kostenlose Domains"). Führen Sie in einem Terminal den folgenden Befehl aus:

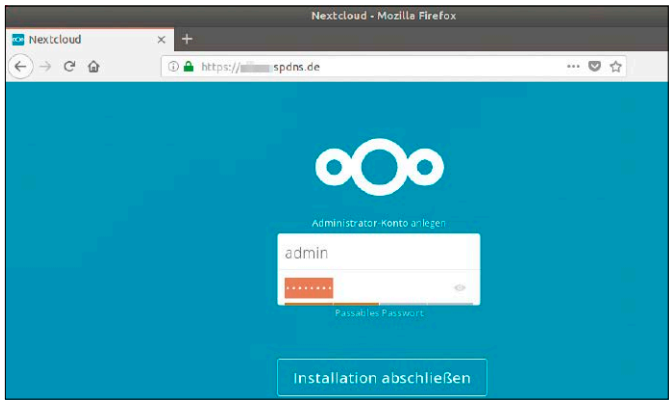
```
sudo nextcloud.enable-https lets-
  encrypt
```

Es startet ein Assistent, der Sie durch die nötigen Schritte führt. Sie müssen den Domainnamen eintippen und eine E-Mail-Adresse, an die Let's Encrypt (*https://letsencrypt.org*) Informationen etwa über den Ablauf des Zertifikats schicken kann. Die SSL-Zertifikate von Let's Encrypt sind kostenlos und gelten jeweils für drei Monate. Sie müssen sich aber um nichts kümmern, weil die Nextcloud-Instanz das Zertifikat automatisch rechtzeitig erneuert.

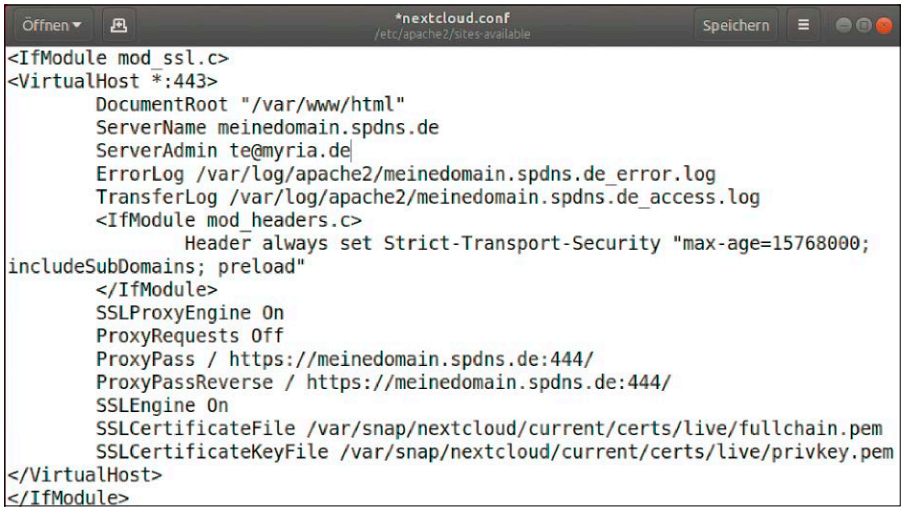
Sie verwenden den Server nur im lokalen Netzwerk: Wenn Sie die SSL-Verschlüsselung aktivieren wollen, verwenden Sie ein selbst signiertes Zertifikat. Dazu starten Sie im Terminalfenster

```
sudo nextcloud.enable-https self-
  signed
```

Im Browser müssen Sie nun für dieses Zertifikat eine Ausnahmeregel festlegen (Firefox: „Ich kenne das Risiko", „Ausnahme hinzufügen...", Sicherheits-Ausnahmeregel bestätigen").



Schnelle Installation: Sie müssen nur die Infos für das Administratorkonto eintippen und auf „Installation abschließen" klicken. Danach ist Nextcloud sofort einsatzbereit.



Zwei Webserver: Wenn Sie Apache auch für andere Webanwendungen benötigen, leiten Sie die Anfragen an den Nextcloud-Server einfach an die gewünschte Adresse und den Port weiter.

5. Die Nextcloud-Installation komplettieren

Die Snap-Installation ist schnell einsatzbereit. Rufen Sie im Browser die URL „https://[MeineDomain]" beziehungsweise ohne SSL „http://[MeineDomain]" auf. Den Platzhalter „[MeineDomain]" ersetzen Sie durch den Domainnamen (siehe Kasten „Kostenlose Domains"). Wenn Sie den Server nur im lokalen Netzwerk verwenden, ersetzen Sie den Platzhalter durch die IP-Adresse oder den Hostnamen des Servers. Sie sehen die Weboberfläche von Nextcloud, in der Sie den Benutzernamen und das Passwort für das Administratorkonto eintippen und mit „Installation abschließen" bestätigen.

Nextcloud speichert die Domain oder IP-Adresse, von der aus Sie die Installation durchgeführt haben, als vertrauenswürdige Domain. Wenn Sie beispielsweise zuerst den Domainnamen verwendet haben und dann auf den Server über die IP-Adresse im lokalen Netzwerk zugreifen, sehen Sie im Browser einen Zertifikatfehler, denn das Zertifikat gilt nur für den gewählten Domainnamen. Nachdem Sie die Ausnahmeregel bestätigt haben, beschwert sich Nextcloud wegen des Zugriffs über eine nicht vertrauenswürdige Domain. Klicken Sie auf „[IP-Adresse] als vertrauenswürdige Domain hinzufügen", damit die Fehlermeldung verschwindet.

6. Nextcloud hinter Apache betreiben

Ein Vorteil von Snap-Apps ist es, dass sie alle benötigten Programme enthalten und schnell konfiguriert sind. Der Nachteil ist jedoch, dass sich auch nicht viel konfigurieren lässt. Den mitgelieferten Apache-Webserver beispielsweise können Sie nicht gleichzeitig für andere Webanwendungen nutzen. Das Problem lässt sich jedoch lösen, indem Sie einen herkömmlich auf dem System installierten Webserver als Reverse Proxy nutzen. Wir gehen davon aus, dass Apache bereits konfiguriert und einsatzbereit ist. Infos und Tipps zu Installation finden Sie unter *www.pcwelt.de/1607540*. Nextcloud muss mit einem Let's-Encrypt-Zertifikat gesichert und über einen Domainnamen erreichbar sein.

Aktivieren Sie in einem Terminalfenster die nötigen Apache-Module:

```
sudo a2enmod proxy proxy_http
  proxy_wstunnel ssl headers
```

Danach ändern Sie den SSL-Port der Nextcloud-Snap-App:

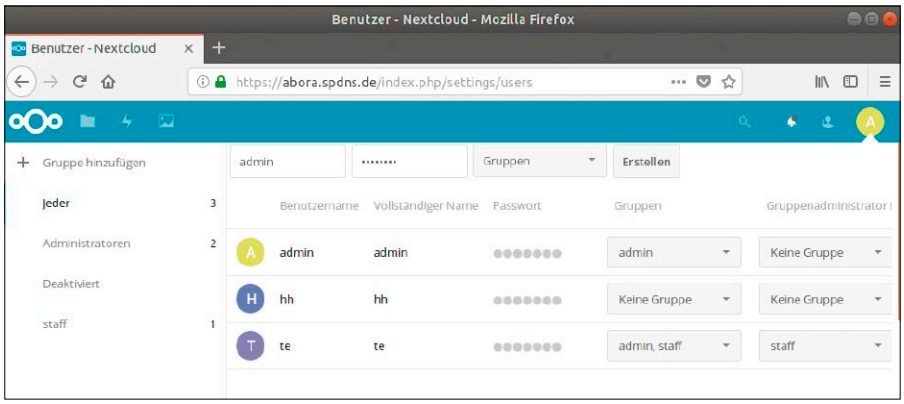
```
sudo snap set nextcloud ports.
  https=444
```

Wählen Sie eine andere Portnummer als „444", wenn dieser Port bereits belegt ist.

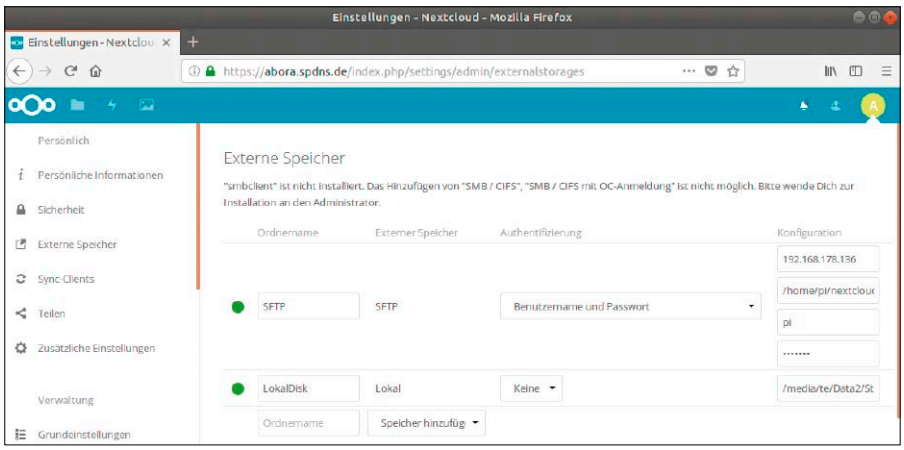
Erstellen Sie eine Apache-Konfigurationsdatei für den Nextcloud-Server:

```
sudo gedit /etc/apache2/sites-
  available/nextcloud.conf
```

Füllen Sie die Datei mit dem Inhalt aus der Abbildung oder laden Sie die Datei über *www.pcwelt.de/Z6an9V* herunter. Passen Sie alle Vorkommen von „meinedomain.spdns.de" für Ihre Domain an. Aktivieren



Multiuser: In Nextcloud lassen sich Benutzerkonten einrichten, die jeweils über eigene Ordner im Datenspeicher verfügen. Gruppen erleichtern die Freigabe für mehrere Benutzer gleichzeitig.



Speicher erweitern: Nextcloud kann Speicherplatz von einem anderen Server beispielsweise über SFTP einbinden. Für höhere Sicherheit lassen sich die Dateien verschlüsseln.

Sie dann die Konfiguration und starten Sie den Webserver neu:

```
sudo a2ensite nextcloud
sudo systemctl restart apache2
```

Da die Umleitung auf die Internetdomain und den Port 444 erfolgt, müssen Sie noch eine zusätzliche Portfreigabe für diesen Port einrichten, wie in Punkt 3 beschrieben. Der Cloudserver ist danach über „https://[MeineDomain]“ und „https://[MeineDomain]:444“ erreichbar.

7. Erste Schritte in Nextcloud

Als erste Aktion sollten Sie weitere Nextcloud-Benutzer anlegen. Klicken Sie auf das Symbol in der rechten oberen Ecke und gehen Sie im Menü auf „Benutzer“. Tippen Sie den gewünschten Benutzernamen sowie ein Passwort ein. Unter „Gruppen“ setzen Sie ein Häkchen bei „admin“, wenn der neue Benutzer administrative Rechte erhalten soll. Wählen Sie „+ Gruppe hinzufügen“ und tippen Sie eine Bezeichnung für die Gruppe ein, wenn Sie Freigaben nicht nur für einzelne Benutzer, sondern auch für Benutzergruppen erstellen möchten. Zum Anschluss klicken Sie auf „Erstellen“.

Fügen Sie dann über „+Apps“ Plug-ins hinzu, beispielsweise Calendar, Contacts und Notes aus der Rubrik „Büro und Text“. Die Erweiterungen für Bilder (Gallery) und Dateien (File sharing) sind standardmäßig installiert.

Nextcloud lässt sich weitestgehend intuitiv bedienen. Über das „+“-Zeichen legen Sie neue Ordner an oder laden einzelne Dateien hoch. Per Drag & Drop vom Dateimanager lassen sich mehrere Dateien übertragen. Damit andere Benutzer Dateien betrachten oder herunterladen können, klicken Sie auf das Teilen-Symbol neben einer Datei oder einem Ordner und tippen dann den Benutzernamen ein. Setzen Sie ein Häkchen vor „Link teilen“, um beliebigen Personen ohne Benutzerkonto den Zugriff auf ein Element zu ermöglichen. Diese müssen dann nur den Link kennen, den Nextcloud Ihnen anzeigt.

8. Mehr Sicherheit für Ihre Daten

Nextcloud bietet von Haus aus bisher nur eine serverseitige Verschlüsselung. Die ist zwar nützlich, wenn Dateiinhalte vor unbefugten Augen geschützt werden sollen, bietet aber keine nachhaltige Sicherheit, da die Sicherheitsschlüssel auf dem Server liegen. Das Verfahren kann jedoch als weitestgehend sicher gelten, wenn Nextcloud die Dateien auf einem anderen Server ablegt. Dafür benötigen Sie Speicherplatz im Internet oder im lokalen Netzwerk, beispielsweise ein NAS, der per SFTP erreichbar ist.

Um den Speicher einzubinden, gehen Sie in Nextcloud auf „+ Apps“ und dann auf „Deaktiviert Apps“. Aktivieren Sie „External storage support“ und „Default encryption module“. Gehen Sie auf „Einstellungen“ und klicken Sie unter „Verwaltung“ auf „Externe Speicher“. Tippen Sie eine aussagekräftige Bezeichnung unter „Ordnername“ ein. Unter „Externer Speicher“ wählen Sie beispielsweise „SFTP“. Tragen Sie unter „Konfiguration“ die Anmeldedaten ein, „Root“ ersetzen Sie durch das Verzeichnis, das Sie für den Datenspeicher vorgesehen haben. Sie speichern die Einstellungen per Klick auf das Häkchen ganz rechts im Fenster.

Gehen Sie dann auf „Einstellungen“ und „Verschlüsselung“. Setzen Sie ein Häkchen vor „Serverseitige Verschlüsselung aktivieren“ und klicken Sie auf „Verschlüsselung aktivieren“. Entfernen Sie das Häkchen vor „Benutzerverzeichnis verschlüsseln“, wenn Sie nur Dateien auf dem externen Speicher verschlüsseln wollen. Andernfalls werden alle neu hinzugefügten Dateien verschlüsselt. Melden Sie sich bei Nextcloud ab und wieder an.

Auf der Nextcloud-Startseite sehen Sie jetzt einen neuen Ordner, über den Sie auf den Inhalt des SFTP-Servers zugreifen. Er lässt sich wie alle anderen Ordner verwenden.

Alternativen: Nextcloud wird demnächst auch eine Ende-zu-Ende-Verschlüsselung bieten, die sich zur Zeit aber noch nicht für produktiv eingesetzte Server eignet (*https://apps.nextcloud.com/apps/end_to_end_encryption*).

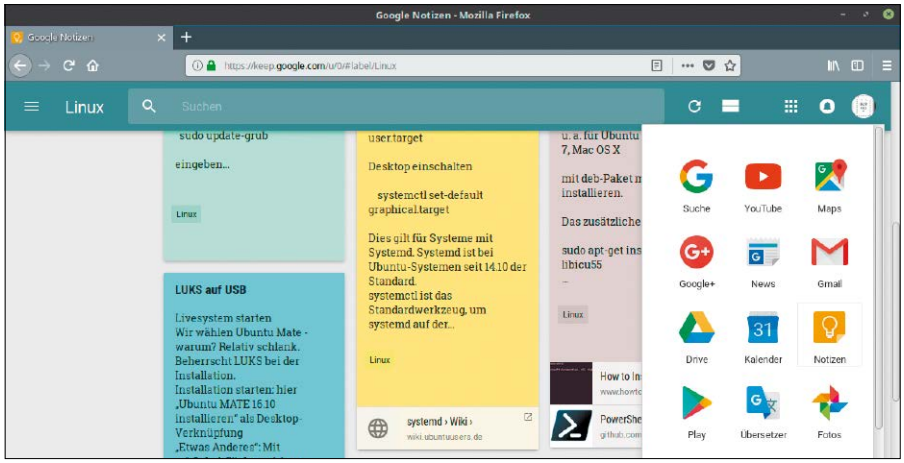
Wer mehr Sicherheit möchte – auch unabhängig von der Nextcloud-Installation – sollte die komplette Linux-Systempartition verschlüsseln. Das ist ohne erheblichen Aufwand jedoch nur bei der Installation des Systems möglich. Mehr Infos zum Thema Verschlüsslung unter Linux finden Sie auf *www.pcwelt.de/2116961*. ■

Zentrale Infos, Texte und Notizen

Eine Heimnetzzentrale für Notizen, Adressen, technische Infos und oft benötigte Dateien ist eine hervorragende Einrichtung. Im Optimalfall sollte dieser Serverdienst einfach zugänglich und hardwaretechnisch anspruchslos sein.

VON HERMANN APFELBÖCK

Es sind Kriterien der Textmengen, der Datenschutz-Sensibilität und der Anzahl der Clientgeräte, die darüber entscheiden, ob man für seine Infos einen Netzwerkdienst braucht. Wer ausschließlich an einem PC arbeitet, kann seine Notizen dort auch lokal ablegen. Für unsensible Einkaufsnotizen genügen sicher auch die „Google Notizen". Wenn aber Adressen, Kennwörter, technische Infos, Scripts, Webrecherchen von mehreren Personen auf mehreren Geräten zentral, bequem und sicher zugänglich sein sollen, ist das ein Fall für eine Infozentrale. Dies steht im Zentrum dieses Artikels, der aber zunächst auch andere populäre Lösungen streift.

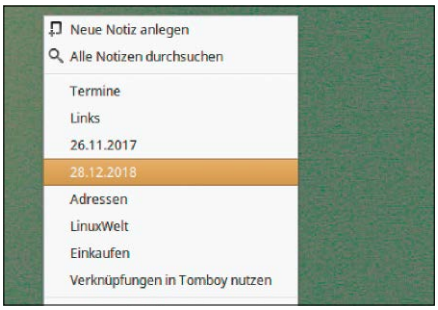


Google Notizen („Google Keep"): Solche Cloudlösungen sind für viele Nutzer technisch völlig ausreichend. Für persönliche oder sensible Daten sind solche Angebote aber ungeeignet..

Lokale Notizen und Cloudnotizen

Komfortable Notizenprogramme gibt es in Menge für jedes System. Wenn es unter Linux eine rein lokale Rechnerlösung sein darf, ist Tomboy (Paketname „tomboy") erste Wahl: Das Tool organisiert Einzelnotizen in Notizbüchern, bietet reichhaltige Textformatierungen und eine schnelle Suchfunktion. So wirklich zeitgemäß sind aber lokale Lösungen wie Tomboy oder „Klebezettel" nicht mehr. Die populärsten Notizsammler sind plattformübergreifend und nutzen einen externen Cloudspeicher – so etwa Evernote (*https://evernote.com*), Google Keep (*https://keep.google.com/*) oder Microsofts One Note (*https://onedrive.live.com*). Diese Text- und Infosammler sind ausgereift und elegant (die „Google-Notizen" eher simpel), haben aber zwei Nachteile: Alle Infos lagern auf amerikanischen Servern. Außerdem sind sie auf die persönliche Infoablage einer Person mit einem Zugangskonto ausgerichtet, nicht primär für Personengruppen.

Wer es komplexer haben will, landet schnell bei Kollaborationssoftware wie Google Docs, Nextcloud oder Feng Office. Diese Lösungen ermöglichen natürlich auch einfache Infosammlungen, schießen aber mit zahlreichen weiteren Funktionen und einem zum Teil beträchtlichen Einrichtungsaufwand (Nextcloud, Feng Office) weit übers Ziel hinaus.



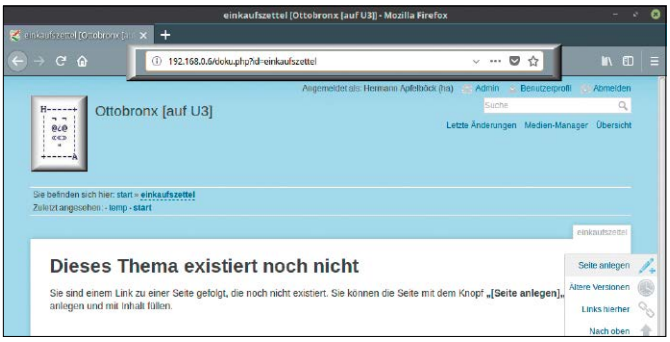
Lokale Notizen mit Tomboy: Technisch ist das nicht mehr zeitgemäß, aber wo dies genügt, ist Tomboy eine ausgereifte Lösung.

Empfehlenswerte Wiki-Lösungen

Wikis sind eine ideale Plattform, um umfangreiche Textsammlungen zu sammeln und zu organisieren. Selbst bei der Einschränkung auf kostenlose Angebote ist die Anzahl solcher Wiki-Lösungen mittlerweile unübersichtlich, wie die Wikipedia-Seite *https://de.wikipedia.org/wiki/Liste_von_Wiki-Software* zeigt. Die populärsten Lösungen basieren auf PHP, und das gilt auch für die beiden hier empfohlenen Kandidaten Mediawiki (*www.mediawiki.org*) und Dokuwiki (*www.dokuwiki.org*). Beide bieten weit mehr als nur Textsammlungen, wobei die meisten Audio-, Video- und Bildfunktionen durch zahlreiche externe Plug-ins gelöst werden. Das Mediawiki ist die angestamm-

te Basis der Wikipedia und kann daher exzellente Pflege und Zukunftssicherheit garantieren. Das Dokuwiki steht dem aber kaum nach und hat wesentliche Vorteile für Heimanwender, da es auf mehreren Ebenen einfacher ist als das Mediawiki:

- Das Dokuwiki benötigt keine Datenbank und speichert alles in einfachen Textdateien.
- Die Trennung der Daten von der Software und ist rigoros, sodass die Sicherung oder Synchronisierung des kompletten Datenbestands des Unterverzeichnisses „data“ (typischerweise „/var/www/dokuwiki/data/“) sehr einfach wird.
- Die Struktur in gliedernde Namensräume (auf Dateiebene Verzeichnisse) und Seiten (auf Dateiebene TXT-Dateien) ist simpel.
- Auszeichnungssprache und Editor sind relativ einfach. Wysiwyg bietet der Standardeditor nicht, kann aber über einen Plug-in-Editor nachgerüstet werden.
- Für Nutzer, die auch Windows verwenden, gibt es ein absolut einfaches Gesamtpaket mit integriertem Apache.



Seiten anlegen: Wenn Sie als Dokuwiki-Adresse eine nicht existierende ID eingeben, erscheint diese Meldung und mit „Seite anlegen“ entsteht eine neue Seite (und Datei).

Vorbereitungen für das Dokuwiki

Ideales Gerät für ein Wiki ist ein ständig laufender Server von der Sorte Raspberry & Co. Im Falle des Dokuwiki können Raspberry & Co. diese zusätzliche Aufgabe mühelos neben sonstigen Serverdiensten übernehmen, denn das Dokuwiki stellt geringe Ansprüche an die Hardware. Voraussetzung ist jedoch ein laufender Apache-Server mit PHP. Sofern dieser noch nicht vorliegt, installieren Sie diesen unter Raspbian, Debian oder Ubuntu mit diesem Kommando:

```
sudo apt install apache2 php5
  libapache2-mod-php5 php5-curl
```

Das nur gut drei MB große Installationspaket von Dokuwiki holen Sie mit wget ab.

```
wget http://download.dokuwiki.org/
  src/dokuwiki/dokuwiki-stable.tgz
```

Unter den Debian/Raspbian-Distributionen liegt das Standardverzeichnis für Apache-Webdienste unter „/var/www/“, bei Ubuntu unter „/var/www/html“. Entpacken Sie mit

```
sudo tar xzvf dokuwiki-stable.tgz
  -C /var/www/[html/]
```

das Archiv an die richtige Stelle. Das dort

(WIKI-)FREIGABE IM INTERNET

Die Anleitungen in diesem Kasten beantworten die Frage, wie Sie heimische Serverdienste wie etwa ein Wiki für den Fernzugriff aus dem Internet öffnen. Sie gelten analog auch für andere Serverdienste, die in diesem Special vorgestellt werden.

Generell gibt es für Webfreigaben zwei Gegenanzeigen: Erstens bietet jeder nach außen geöffnete Port (und ohne solchen geht es nicht) eine Angriffsfläche. Hier müssen strikte Zugangsregeln und sichere Passwörter benutzt werden. Zweitens ist der Datendurchsatz in der Regel bescheiden, weil alles, was über das Internet als Download angefordert wird, am heimischen Router als Upload verschickt wird – und die Uploadbandbreite typischer DSL-Verträge liegt selten über 1–2 MBit/s.

Technisch entstehen drei Aufgaben:

1. Der Router benötigt eine Portfreigabe. Welchen Port (1 bis 65535) Sie nach außen öffnen, ist unerheblich – Sie müssen sich die Zahl nur merken. Die Portfreigabe geschieht in der Fritzbox unter „Internet -> Freigaben -> Portfreigaben“, bei anderen Routern unter „Portforwarding“, „Portmapping“ oder „Virtual Server“. Das Prinzip ist überall gleich: Sie tragen neben „von Port“ und „bis Port“ eine frei gewählte Portnummer ein, die nach außen geöffnet wird. Unter „an Port“ müssen Sie genau den Port angeben, mit dem der Serverdienst arbeitet. Das kann Port 22 für SSH, Port 80 für einen Webserver wie das Dokuwiki oder Port 25565 für einen Minecraft-Server sein.

2. Der Heimserver benötigt eine feste lokale IP, damit der Router die Anfrage aus dem Web an das richtige Gerät schickt. Die Fritzbox vergibt feste IPs unter „Heimnetz -> Heimnetzübersicht -> Netzwerkverbindungen“ mit der Option „Diesem Netzwerkgerät immer die gleiche IPv4-Adresse zuweisen“.

3. Für den Fernzugriff auf den heimischen Server benötigen Sie die öffentliche WAN-IP. Der Fernzugriff auf ein Heim-Wiki sieht dann im entfernten Browser so aus

```
http://[WAN-IP]:[Freigegebener Port]/dokuwiki/
```

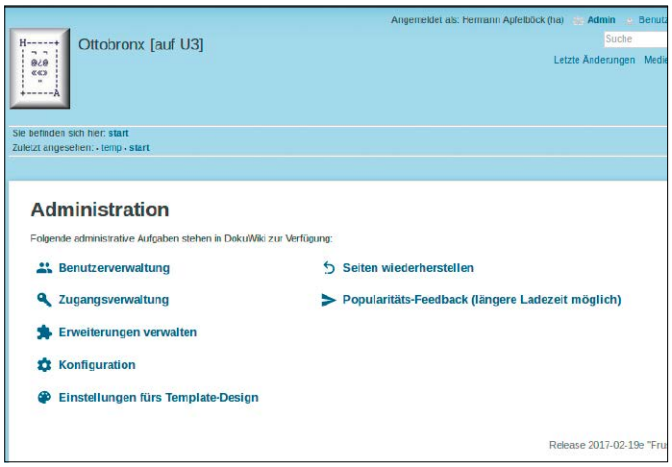
und könnte in einem konkreten Beispiel so lauten:

```
http://178.27.67.34:80/dokuwiki/
```

Dabei stellt sich jedoch das Problem, dass Sie die WAN-IP Ihres Heimnetzes nicht ermitteln können, wenn Sie sich außerhalb Ihres Netzwerks befinden. Dafür gibt es zwei Lösungen:

3a. Sie registrieren eine Pseudodomain etwa bei *www.noip.com*, *www.dlinkddns.com* (für D-Link-Router) oder über das Myfritz-Konto (für Fritzbox-Router). Kontodaten und Pseudohost geben Sie dann in die dafür vorgesehenen Eingabefelder des Routers ein. Bei der Fritzbox finden Sie diese unter „Internet -> Freigaben -> Dynamic DNS“. Der Router wird ab sofort bei jeder Neueinwahl die WAN-IP sofort an diesen Dienst weitergeben. Folglich bringt Sie die Angabe der Pseudodomain in Ihr Heimnetz.

3b. Sie sorgen selbst dafür, dass die aktuelle WAN-IP Ihres Netzwerks stets im Internet hinterlegt ist. Dafür ist im Prinzip nur eine kleine Textdatei auf einem Cloud- oder Webspeicher erforderlich. Eine genauere Anleitung würde jedoch den Rahmen dieses kleinen Exkurses sprengen.



Der Dokuwiki-Link „Admin“ führt zur Konfiguration: Es empfiehlt sich, sich zunächst auf Basiseinstellungen unter „Konfiguration“ und Farb-einstellungen für das Design zu beschränken.

entstandene Verzeichnis mit Versionsangabe im Namen benennen Sie mit

```
sudo mv /var/www/[html/]dokuwiki* /
  var/www/[html/]dokuwiki
```

nach „dokuwiki“ um und setzen die Zugriffsrechte für Apache:

```
sudo chown -R www-data:www-data /
  var/www/[html/]dokuwiki
```

Ab sofort ist das Wiki betriebsbereit und die weitere Einrichtung erfolgt im Browser mit der Adresse „http://[IP-Adresse]/dokuwiki/install.php?l=de“, wobei als „[IP-Adresse]“ diejenige des Serverrechners einzugeben ist. Beim Start des Install-Scripts mit Firefox kommt es vor, dass der Browser den Script-Inhalt anzeigt, anstatt das Script zu starten: Verwenden Sie in diesem Fall einfach einen beliebigen anderen Browser.

Die Grundkonfiguration erfordert nur wenige Schritte: Notwendig sind das Einrichten eines Administratorkontos und die Vergabe eines Wiki-Namens. Weitere Einstellungen wie das Festlegen der Startseite oder der Sprache finden Sie jederzeit auch später unter „Admin -> Konfiguration“.

Dokuwiki: Seiten anlegen und organisieren

Eine neue Wiki-Seite entsteht dadurch, dass Sie in der Browseradresse hinter „[IP]/dokuwiki/doku.php?id=“ einen bisher nicht benutzten Seitennamen eintragen und dann auf „Seite anlegen“ klicken. Der Editor erlaubt Auszeichnungen wie fett oder kursiv, Überschriftenebenen und das Einfügen von Bildern und Dateien. Für das Einfügen von internen Links innerhalb des Wikis und externen URL gibt es Schaltflächen, welche die Eingabe deutlich vereinfachen. Der Editor entspricht weitgehend demjenigen anderer Wikis oder Blogeditoren wie Wordpress. Einige Eigenheiten sollte man aber kennen:

Beachten Sie, dass ein Return im Editor keinen Zeilenumbruch auf der Ergebnisseite bewirkt. Sie müssen im Editor mit zwei Returns eine sichtbare Leerzeile erzeugen oder das Zeilenende durch Doppelbackslash (\\) erzwingen. Bei Listen aller Art (Telefonliste, Adressen, Scripts) wäre es nicht zumutbar, die notwendigen Zeilenumbrüche manuell einzutragen. Formatieren Sie in solchen Fällen den gesamten Text mit dem Button „Listenpunkt“.

Ohne weitere Gliederung landen alle Seiten auf oberster Ebene, was selbst bei kleinen Sammlungen schnell unübersichtlich wird. Um hierarchische Ebenen zu organisieren, gibt es „Namensräume“ (Namespaces). Um einen Namensraum anzulegen, verwenden Sie den Befehl

```
[IP-Adresse]/dokuwiki/doku.
  php?id=[Namensraum:][Seitenname]
```

oder als konkretes Beispiel „[IP-Adresse]/

RECOLL: INFOSUCHE IM NETZWERK

Wikis eignen sich für den Aufbau zentraler Texte und leisten dabei unter der Haube automatisch eine Indexierung für schnelle Textsuche (Mediawiki, Dokuwiki). Eine spezialisierte Suchsyntax gibt es aber nicht und außerdem müssen alle Texte neu eingepflegt werden. Die Rolle eines zentralen Suchservers für Texthalden aller Art können solche Wikis daher nicht erfüllen.

Die empfohlene Software für diese Aufgabe ist das Programm Recoll: Es lässt sich nicht nur am lokalen Rechner, sondern über eine Weboberfläche im gesamten Netzwerk nutzen. Außerdem verarbeitet es alle relevanten Dateiformate. Recoll ist überall in den Standard-Paketquellen (*sudo apt install recoll*), jedoch oft veraltet. Wer die aktuelle Version nutzen will, kann ein externes PPA einbinden:

```
sudo add-apt-repository ppa:recoll-backports/recoll-
  1.15-on
sudo apt update
sudo apt install recoll
```

Da es hier ausschließlich um den Recoll-Server im Netzwerk geht, überspringen wir hier alle Hinweise zur Erstellung des Index, die unter „Einstellungen -> Index-Einstellungen“ gut strukturiert und weitgehend selbsterklärend ist.

Als Webserver kann Recoll sowohl unterhalb unter Apache laufen als auch „stand-alone“. Die nachfolgende Kurzanleitung beschreibt die einfachere Stand-alone-Variante: Zuerst laden Sie über *https://github.com/koniu/recoll-webui* die passende Version der Weboberfläche herunter. Suchen Sie dort weiter unten nach „Download“. Hier finden Sie zwei Varianten – eine für Recoll 1.18.2 und neuer, ein zweite für alle ältere Recoll-Versionen (Ihre Recoll-Version verrät der Terminalbefehl *recoll --version*). Erstellen Sie etwa im Home-Verzeichnis einen Ordner „recoll“ und entpacken Sie dort das heruntergeladene ZIP-Archiv. Der Ordner enthält eine Reihe von Python-Scripts, unter anderem „webui-standalone.py“ für den Miniserver. Damit dieses funktioniert, benötigen Sie noch folgendes Paket:

```
sudo apt install python-recoll
```

Danach funktioniert der Recoll-Server, sobald Sie das genannte Script mit

```
python webui-standalone.py
```

dokuwiki/doku.php?id=Anna:Adressen“. Die neue Wiki-Seite „Adressen“ wird dann unter der neuen Ebene „Anna“ eingerichtet.

Da Namensräume auf Dateiebene durch Verzeichnisse, Wiki-Seiten durch TXT-Dateien repräsentiert werden, ist es für den Basisaufbau oder bei Umbauten des Wikis oft einfacher, die Grundstruktur unter „/var/www/[html/]dokuwiki/data/pages“ auf Dateiebene zu unternehmen. Die Wiki-Ansicht im Browser folgt solchen Änderungen sofort oder spätestens nach dem Seitenrefresh mit Taste F5.

Für das Löschen oder Umbenennen von Seiten gibt es keine Option. Zum Löschen öffnen Sie die Wikiseite und gehen auf „Diese Seite bearbeiten“. Nach Löschen des kompletten Inhalts und „Speichern“ ist die Seite entfernt. Namensräume verschwinden automatisch, wenn alle Seiten unterhalb des Namensraums gelöscht werden. Zum Umbenennen von Seiten kopieren Sie den kompletten Inhalt in eine neue Seite mit dem gewünschten Namen und löschen dann die ursprüngliche Seite auf die beschriebene Weise.

Dokuwiki: Anpassung und Erweiterungen

Über „Admin -> Konfiguration“ erreichen Sie die zahlreichen Basiseinstellungen. Ganz oben unter „Basis“ definieren Sie die Designvorlage. Das ist beim Dokuwiki nicht nur eine optische Entscheidung, sondern bestimmt auch, ob und wo die Wiki-Übersicht, die Editieraktionen und die Konfiguration erreichbar sind. Beachten Sie, dass jedes Design im allerletzten Punkt „Template“ der Konfiguration noch diverse Detailanpassungen vorsieht: Das betrifft nicht nur die Farben, sondern auch die gewünschte Position der Elemente.

Über „Admin -> Erweiterungen verwalten -> Suchen und Installieren“ ist das Dokuwiki erweiterbar. Es gibt zahlreiche funktionale Erweiterungen und Templates. Wer in den Plug-ins stöbern will, sollte zunächst die Seite *www.dokuwiki.org/extensions* aufsuchen und danach die gewünschte Erweiterung über „Suchen und Installieren“ in der Konfigurationsoberfläche einrichten. Ein auf diese Weise heruntergeladenes Template können Sie dann unter „Admin -> Konfiguration -> Designvorlage“ auswählen und dann ganz unten auf „Speichern“ gehen. In der Regel benötigt der Browser mit Taste F5 einen Seitenrefresh, um das neue Theme anzuzeigen.

Dokuwiki: Portabel für Windows

Sowohl das Dokuwiki als auch das Mediawiki gibt es auch als portables Windows-Paket, jedoch ist hier das Dokuwiki erneut ungleich einfacher einzurichten. Diese Option ist nützlich für ein gemischtes Heimnetz, um auf einfachste Weise ein vollständiges Windows-Backup vorzuhalten. Den Download finden Sie unter *https://download.dokuwiki.org/* und hier ganz nach unten als „MicroApache“. Dieses Paket enthält das Dokuwiki komplett mit einem minimalen Apache-Webserver – einfach entpacken und im entstandenen Ordner die Batchdatei „run.cmd“ aufrufen.

Das Wiki lädt automatisch im Standardbrowser am lokalen Rechner, andere Rechner erreichen es über die Adresse „http://[IP-Adresse]:8800/doku.php“. ■

Versionsverwaltung: Dokuwiki speichert Bearbeitungszustände und kann auf ältere Seitenversionen zurückkehren.

starten. Allerdings läuft die Recoll-Suchmaske erst mal nur mit der Adresse „http://127.0.0.1:8080“ im lokalen Browser. Damit es auf jedem Browser im Netzwerk funktioniert, müssen Sie eine Zeile im Python-Script modifizieren: Statt

```
default='127.0.0.1'
```

tragen Sie

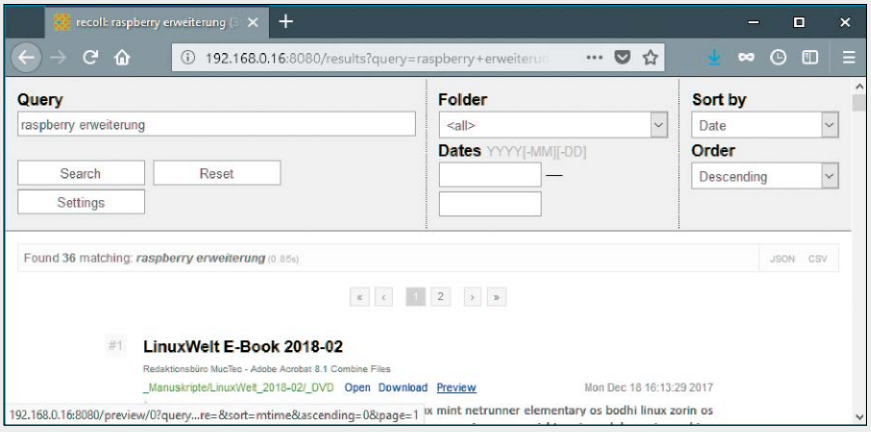
```
default='[IP-Adresse des Servers]'
```

ein, also beispielsweise

```
default='192.168.178.12'
```

Der Recoll-Server sollte (wie jeder Server) eine feste IP-Adresse beziehen, damit die hier eingetragene IP dauerhaft gilt.

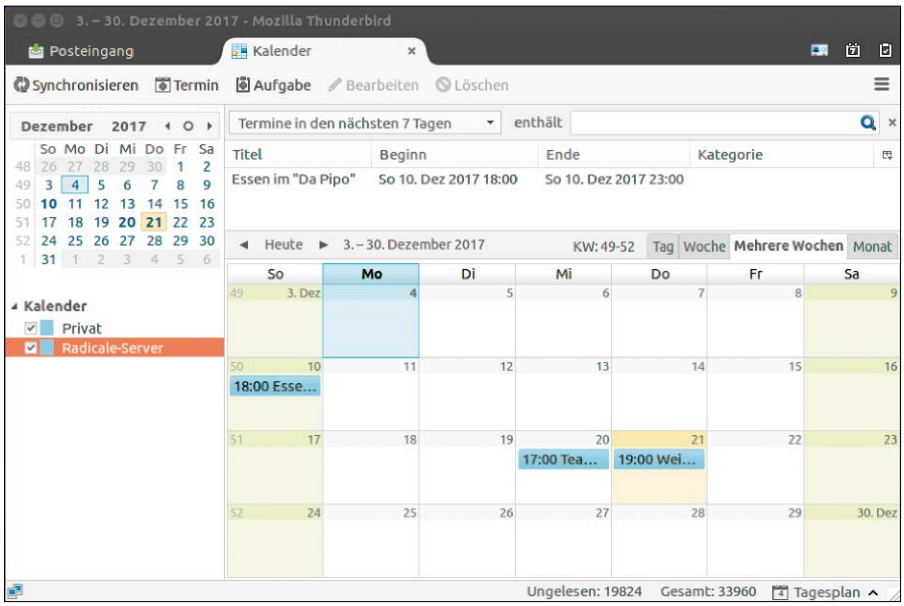
Bei gestartetem Stand-alone-Server erreicht nun jeder Browser die Recoll-Weboberfläche. Die entspricht dem lokalen Suchdialog und erlaubt alle Filter und Operatoren. Wenn der Recoll-Server immer erreichbar sein soll, sollte der Aufruf des Scripts „webui-standalone.py“ als Autostart-Programm oder in die Crontab eingetragen werden.



Differenzierte Recoll-Suche auch über das Netzwerk: Der Recoll-Server läuft entweder unter Apache oder noch einfacher als Stand-alone-Server über ein winziges Python-Script.

Server für Termine und Adressen

Ein Kalenderserver im eigenen Netzwerk hilft bei der Verwaltung Ihrer Termine. Er ist schnell eingerichtet und lässt sich auch von mehreren Personen verwenden.



Termine im Netz. Das Thunderbird-Add-on Lightning bietet einen lokalen Terminkalender, kann die Daten aber auch mit einem Kalenderserver abgleichen.

VON THORSTEN EGGELING

Kostenlose Online-Terminkalender gibt es mehrere, etwa von Google oder Microsoft. Wer sich nicht an diese Anbieter binden und persönliche Daten lieber auf dem heimischen Rechner speichern möchte, installiert sich einen eigenen Kalenderserver. In diesem Artikel beschreiben wir unkomplizierte Lösungen, die sich relativ schnell einrichten lassen. Wer mehr Funktionen benötigt, etwa zusätzlich den Austausch von Dateien, den gemeinsamen Zugriff auf Dokumente und mehrere Benutzerkonten, sollte sich beispielsweise Nextcloud ansehen (siehe Seite 56).

Die Anleitungen in diesem Artikel gelten für Ubuntu 16.04 und verwandte Systeme wie Linux Mint 18. Die Installation der genannten Software funktioniert auch auf einem Raspberry Pi unter Raspbian beziehungsweise OSMC (siehe Seite 46). Wie Sie auf den Heimserver über das Internet zugreifen, lesen Sie auf Seite 32.

Serversoftware für Caldav und Carddav

Welche Serversoftware für Sie infrage kommt, hängt davon ab, ob Sie Termine oder Adressbücher nur für einen Nutzer oder für ein Team bereitstellen wollen. Sind mehrere Personen beteiligt, besteht wahrscheinlich der Wunsch, die Zugriffsrechte festzulegen. Mit steigenden Ansprüchen an Funktion und Bedienbarkeit erhöht sich auch der Installations- und Wartungsaufwand.

Bei Radicale (*http://radicale.org*), das wir im nächsten Punkt ausführlicher vorstellen, ist der Aufwand relativ gering, der Funktionsumfang ist für private Anwender und kleine Teams ausreichend. Webserver und Datenbank sind nicht erforderlich, die Konfiguration ist daher schnell erfolgt. Wer möchte, kann aber auch Radicale zum Mehrbenutzersystem ausbauen. Anleitungen dazu gibt es auf der Website des Anbieters.

Baikal (*http://baikal-server.com*) geht einen Schritt weiter. Die Software ist in PHP programmiert und bietet eine Weboberfläche, über die sich Benutzerkonten anlegen und verwalten lassen. Das setzt jedoch die Installation eine Apache-Webservers und eine Datenbank wie My SQL oder Sqlite voraus (siehe Seite 59).

Wenn es auf eine detaillierte Rechtevergabe für größeren Teams ankommt, ist Davical die richtige Wahl (*www.davical.org*). Auch hier kommt PHP zum Einsatz. Sie benötigen den Apache-Webserver und die Datenbank Postgre SQL. Die Verwaltung von Davical erfolgt über eine Weboberfläche. Hier lassen sich Benutzer und Gruppen in „Benutzerfunktionen -> Prinzipalen anlegen“ erstellen und Rechte zuweisen. Eine Installations- und Bedienungsanleitung finden Sie auf der Website des Anbieters.

Radicale: Einfacher und schlanker Server

Radicale (*http://radicale.org*) ist ein Server für Caldav (Kalender) und Carddav (Kontakte). Die Software ist in Python programmiert und benötigt weder Webserver noch Datenbank. In der Grundkonfiguration gibt es keine Benutzerkonten und keine Anmeldung. Radicale eignet sich daher für Einzelanwender oder Teams mit wenigen Personen, wo Zugriffsbeschränkungen keine Rolle spielen. Die Software ist im Terminal-

fenster mit

```
sudo apt install radicale
```

schnell installiert. Öffnen Sie die Konfigurationsdatei mit

```
sudo nano /etc/default/radicale
```

Entfernen Sie das Kommentarzeichen „#“ vor der Zeile „ENABLE_RADICALE=yes“. Speichern Sie die Datei mit Strg-O, bestätigen Sie mit der Enter-Taste und schließen Sie den Editor mit Strg-X. Starten Sie den Serverdienst über die Befehlszeile

```
sudo service radicale start
```

Bei einem Linux-Neustart wird der Radicale-Server automatisch aktiviert.

Testen Sie die Installation, indem Sie im Webbrowser die Adresse „http://localhost:5232“ aufrufen. Auf einem anderen PC ersetzen Sie „localhost“ durch den Namen Ihres Linux-Servers oder dessen IP-Adresse. Es erscheint dann die Meldung „Radicale works!“.

Clientsoftware für Radicale konfigurieren

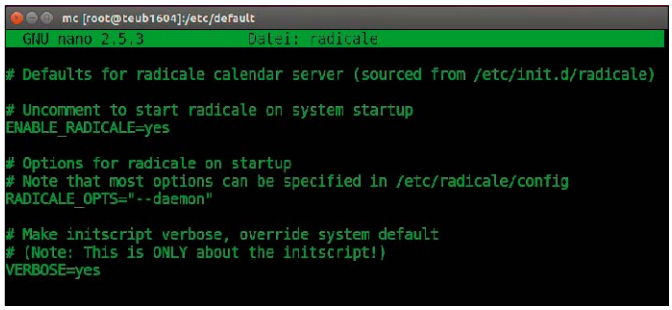
Wenn Sie beispielsweise das Add-on Lightning in Thunderbird installiert haben, gehen Sie im Menü auf „Datei -> Neu -> Kalender“. Wählen Sie die Option „Im Netzwerk“ und klicken Sie auf „Weiter“. Klicken Sie darauf die Option „CalDAV“ an und tippen Sie unter „Adresse“ die URL für den Radicale-Server ein:

```
http://[IP]:5232/[User]/kalender.
 ics/
```

Den Platzhalter „[IP]“ ersetzen Sie durch den Namen oder die IP-Adresse Ihres Linux-PCs und „[User]“ durch den gewünschten Benutzernamen. Dieser ist frei wählbar. Auch der Dateiname „kalender.ics“ kann beliebig lauten. Wichtig: Am Ende der Adresse muss das Zeichen „/“ stehen – sonst funktioniert der Zugriff nicht. Klicken Sie dann auf „Weiter“ und tippen Sie hinter „Name:“ eine aussagekräftige Bezeichnung für den neuen Kalender ein. Klicken Sie auf „Weiter“ und auf „Fertig stellen“.

Gehen Sie auf „Termine und Aufgaben -> Kalender“, um einen Tab mit der Kalenderansicht zu öffnen. Per Doppelklick auf einen Tag oder eine Uhrzeit sowie über das Menü „Termine und Aufgaben -> Neuer Termin“ erstellen Sie einen neuen Kalendereintrag. Achten Sie dabei darauf, dass hinter „Kalender:“ der Onlinekalender eingestellt ist.

Ein Onlineadressbuch lässt sich in Thunderbird über das Add-on Cardbook nutzen.



Radicale-Konfiguration: Damit der Radicale-Server automatisch startet, entfernen Sie in der Datei „/etc/default/radicale“ das Zeichen „#“ vor „ENABLE_RADICALE=yes“.

Netzwerkadressbuch: Onlineadressbücher binden Sie in Thunderbird über das Add-on Cardbook ein. Sie müssen hier nur die URL zum Radicale-Adressbuch konfigurieren.

Erstellen Sie das Adressbuch, indem Sie im Browser die Adresse

```
http://[IP]:5232/[User]/adressen.
 vcf/
```

aufrufen. „[User]“ ist ein beliebiger Benutzername, den Dateinamen können Sie ebenfalls frei wählen. Beachten Sie wieder den Slash „/“ am Ende der Zeile.

Gehen Sie in Thunderbird auf „Extras - > Cardbook“. Klicken Sie die Menüschaltfläche links oben in der Symbolleiste an und gehen Sie auf „Adressbuch -> Neues Adressbuch“. Wählen Sie „Im Netzwerk“ und klicken Sie auf „Weiter“. Aktivieren Sie die Option „CardDAV“ und tippen Sie hinter „URL“ Folgendes

```
http://[IP]:5232/[User]/adressen.
 vcf/
```

ein. Die Platzhalter ersetzen Sie wie oben beschrieben. Hinter „Benutzername“ und „Passwort“ tragen Sie dann beliebige Zeichen ein, klicken auf „Überprüfen“ und dann auf „Weiter“. Vergeben Sie einen Namen für das neue Adressbuch, klicken Sie auf „Weiter“ und auf „Fertigstellen“. Bitte beachten Sie: Cardbook verwendet eigene Adressbücher, die nicht mit dem Standardadressbuch synchronisiert werden. ■

CLIENTSOFTWARE FÜR KALENDER & ADRESSEN

Die meisten Kalender- und Adressbuchanwendungen unterstützen die Standardprotokolle Caldav (Calender Distributed Authoring and Versioning) und Carddav (vCard Extensions für Webdav). Verbreitete Programme sind die Thunderbird-Add-ons Lightning und Cardbook, die sich schnell über „Extras -> Addons“ und einer Suche nach dem Programmnamen installieren lassen. Alternative Desktopanwendungen sind Evolution und Korganizer, die Sie über die Paketverwaltung Ihrer Linux-Distribution installieren. Für Android gibt es beispielsweise Caldav-Sync (*www.pcwelt.de/Ela8LZ*, 2,59 Euro) und Carddav-Sync (*www.pcwelt.de/AzBOV*, 1,90 Euro). iPhone-Nutzer können die Standardkalender- und Kontakte-App für die Verwendung von Netzwerkressourcen konfigurieren.

Der eigene Fotoserver

Einfache PHP-Scripts für eine Fotogalerie sind schnell installiert und genügen für heimische Präsentation oder für Webfreigaben für den Freundeskreis. Es gibt aber auch Bilderserver für größere Personengruppen.

VON THORSTEN EGGELING

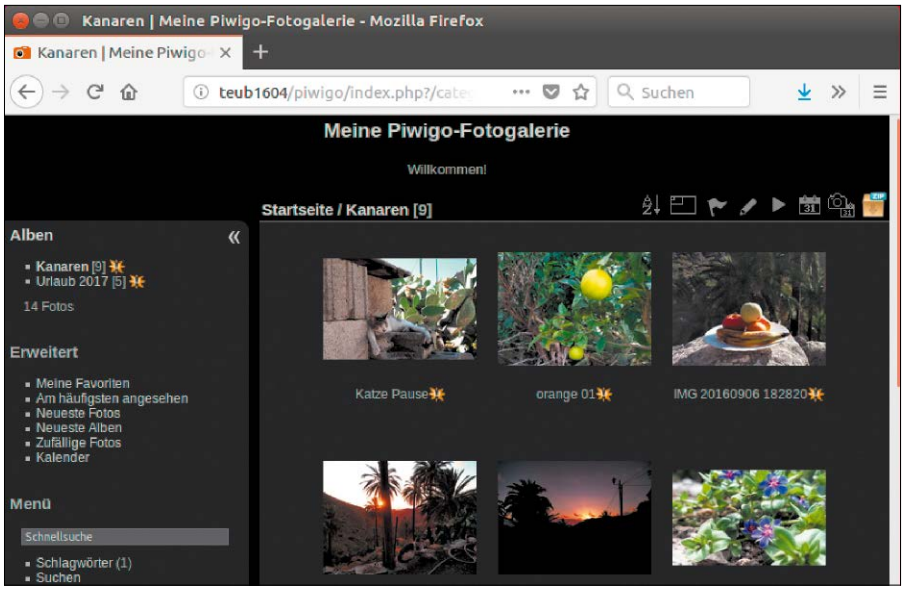
In einer Fotogalerie lassen sich Bilder perfekt organisieren und für die Präsentation vorbereiten. Dieser Artikel nennt sehr einfache bis anspruchsvollere Lösungen für die Bildverwaltung. Wer seine Bildersammlung nicht nur zu Hause zeigen, sondern online dem Freundeskreis zugänglich machen will, sorgt dafür, dass der Webserver zu Hause auch über das Internet erreichbar ist (siehe Seite 32).

Galerien mit und ohne Datenbank

Single File PHP Gallery ist besonders einfach gehalten (*https://sye.dk/sfpg*) und benötigt nur einen Apache-Server und PHP. Die private Nutzung ist kostenlos, von kommerziellen Anwendern erwartet der Hersteller eine Spende ab zehn Dollar. Diese Galerie besteht nur aus einer einzigen PHP-Datei (siehe nächster Punkt) und bietet eine schlichte Ordner- und Bilderübersicht. Bei Bedarf lassen sich auch Admin-Funktionen aktivieren, über die sich Dateien hochladen oder löschen lassen.

Auch Tiny Web Gallery (*www.tinywebgallery.com*) kommt ohne Datenbank aus. Die Software ist für Privatpersonen kostenlos. Über eine Gratisregistrierung lassen sich weitere Funktionen freischalten. Für 19 Euro erhalten Sie eine Standardlizenz für eine Domain und ab 39 Euro auch kommerziell verwendbare Lizenzen für mehrere Domains.

Tiny Web Gallery bietet eine gefällige Oberfläche und kann auch MP3s und Videos streamen (Flashplayer erforderlich). Außerdem besteht die Möglichkeit, mehrere Benutzer einzurichten und Kommentare sowie Bewertungen auf der Webseite zu hinterlassen. Auf der Webseite des Herstellers gibt es mehrere Demos, über die Sie die Funktionen ausprobieren können.



Fotos auf dem eigenen Server: Piwigo bietet fast alles, was man von einer Online-Bildergalerie erwartet. Zusatzfunktionen lassen sich über Plug-ins ergänzen.

Die Fotogalerie Piwigo (*http://piwigo.org*) steht unter einer Open-Source-Lizenz und bietet umfangreiche Funktionen. Sie lässt sich durch Plug-ins erweitern, etwa für den Download von Fotoalben als ZIP-Datei. Zu den Standardfunktionen gehören eine Benutzerverwaltung, Rechtevergabe für Fotoalben, Kommentare, Schlagwörter und eine Diashow. Neben einem Webserver und PHP benötigt Piwigo auch die Datenbank My SQL oder Maria DB. Eine Anleitung zur Installation finden Sie am Ende des Artikels.

Single File PHP Gallery installieren und nutzen

Wenn noch nicht geschehen, installieren Sie den Webserver Apache und PHP in einem Terminalfenster unter Ubuntu mit folgender Zeile:

```
sudo apt install apache2 php
 libapache2-mod-php php-gd
```

Dann starten Sie Apache

```
sudo service apache2 restart
```

und erstellen das Verzeichnis, das die Bildergalerie aufnehmen soll:

```
sudo mkdir /var/www/html/fotos
```

Laden Sie die Dateien „Single_File_PHP_Gallery_4.7.0.zip“ und „sfpg_test_1.5.1.zip“ von *https://sye.dk/sfpg/* herunter und entpacken Sie die Dateien. Starten Sie den Dateimanager über das Terminalfenster mit root-Recht:

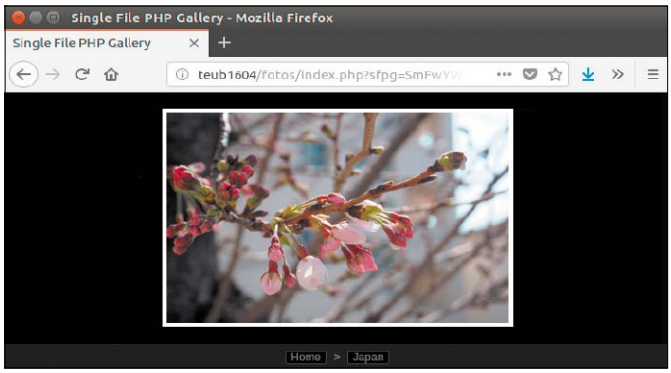
```
sudo nautilus &
```

Kopieren Sie die Dateien „index.php“ und „sfpg_test.php“ nach „/var/www/html/fotos“. Erstellen Sie ein Unterverzeichnis, das bereits einige Bilder enthält. Geben Sie dann dem Webserver die Schreibrechte in diesem Ordner:

```
chown -R www-data:www-data /var/
 www/html/fotos
```

Starten Sie dann in einem Browser im lokalen Netz folgenden Test:

```
http://[IP]/fotos/sfpg_test.php
```



Minigalerie mit Single File PHP Gallery: Das Tool besteht aus einem einzigen PHP-Script und bietet nur einfache, aber oftmals ausreichende Funktionen.

Piwigo verwalten: Im übersichtlichen Administrationsbereich organisieren Sie Alben und Bilder, legen Benutzer und Gruppen an und vergeben Zugriffsrechte.

Das Test-Script prüft, ob alle Voraussetzungen erfüllt sind. Wenn nicht, erhalten Sie eine Fehlermeldung mit Hinweisen zur Beseitigung des Problems. Den Platzhalter „[IP]“ ersetzen Sie durch die IP-Adresse oder den Namen Ihres Linux-Servers.

Öffnen Sie dann die Adresse *http://[IP]/fotos* im Browser. Sollte die Meldung „You have to set the SECURITY_PHRASE in the top of the script! “ erscheint, laden Sie die Seite neu, indem Sie die Taste F5 drücken. Sie sehen dann den Bilderordner, den Sie zuvor nach „/var/www/html/fotos“ kopiert haben. Nach einem Klick darauf öffnen Sie die Bilder oder Sie starten per Klick auf „Slideshow“ eine Diashow.

Single File PHP Gallery konfigurieren: Öffnen Sie die Datei „index.php“ in einem Editor, im Terminalfenster beispielsweise mit

```
gedit /var/www/html/fotos/index.
 php &
```

Gleich zu Beginn finden Sie Variablen, die das Verhalten des Scripts steuern. Tragen Sie beispielsweise in die Zeile

```
define('PASSWORD', '');
```

ein Passwort zwischen den einfachen Anführungszeichen ein. Der Zugang zur Bildergalerie ist dann nur noch nach Passworteingabe möglich.

Wenn Sie bei „define(‚ADMIN‘, FALSE);“ den Wert „FALSE“ durch „TRUE“ ersetzen, blendet das PHP-Script die Schaltfläche „Admin“ ein. Nach einem Klick darauf sehen Sie weitere Schaltflächen, um Bilder hochzuladen, umzubenennen oder zu löschen. Auf einem öffentlich zugänglichen Server sollten Sie diese Option aus Sicherheitsgründen nicht aktivieren.

Piwigo unter Ubuntu installieren

Da Piwigo eine Datenbank benötigt, ist die Installation etwas komplizierter. Installieren Sie zuerst in einem Terminalfenster die nötigen Pakete:

```
sudo apt install apache2
 libapache2-mod-php mysql-common
 mysql-server php php-cli php-mysql
 php-imagick php-gd
```

Dabei legen Sie ein My-SQL-Passwort für den Benutzer „root“ fest. Erstellen Sie eine My-SQL-Datenbank und einen Datenbanknutzer (fünf Zeilen):

```
mysql --default-character-set=utf8
 -uroot -p
CREATE DATABASE piwigo DEFAULT
 CHARACTER SET utf8 DEFAULT COLLATE
 utf8_general_ci;
GRANT USAGE ON piwigo.* TO dbuser@
 localhost IDENTIFIED BY
 '[Passwort]';
GRANT ALL PRIVILEGES ON piwigo.* TO
 dbuser@localhost;
FLUSH PRIVILEGES;
```

Nach der ersten Zeile tippen Sie das Passwort des My-SQL-Benutzers „root“ ein. Den Platzhalter „[Passwort]“ ersetzen Sie durch das Passwort des neuen My-SQL-Benutzers „dbuser“. Das My-SQL-Tool beenden Sie über die Tastenkombination Strg-D.

Laden Sie Piwigo von *http://piwigo.org/basics/downloads* per Klick auf „Download Package“ herunter. Entpacken Sie die ZIP-Datei und kopieren Sie den Inhalt als „root“ beispielsweise nach „/var/www/html/piwigo“. Ändern Sie dort die Zugriffsrechte mittels des Kommandos

```
chown -R www-data:www-data /var/
 www/html/piwigo
```

Rufen Sie dann im Browser die URL

```
http://[IP]/piwigo
```

auf. In das Formular tragen Sie hinter „Benutzer“ den Namen „dbuser“ ein, darunter das beim Anlegen der Datenbank vergebene Passwort sowie den Datenbanknamen „piwigo“.

Unter „Administrationseinstellungen“ legen Sie Benutzernamen und Passwort für Piwigo fest. Klicken Sie auf „Start der Installation“ und danach auf „Galerie ansehen“. Per Klick auf „Tour starten“ verschaffen Sie sich einen Überblick über die Grundfunktionen. ■

PHP-KONFIGURATION ANPASSEN

Bei Ubuntu 16.04 beträgt die maximale Größe beim Dateiupload nur zwei MB. Das ist für Bildergalerien in der Regel zu wenig. Um das zu ändern, öffnen Sie die PHP-Konfiguration im Editor:

```
sudo nano /etc/php/7.0/php.ini
```

Passen Sie den Pfad für Ihre PHP-Installation an. Ändern Sie die Variablen in der Datei wie folgt:

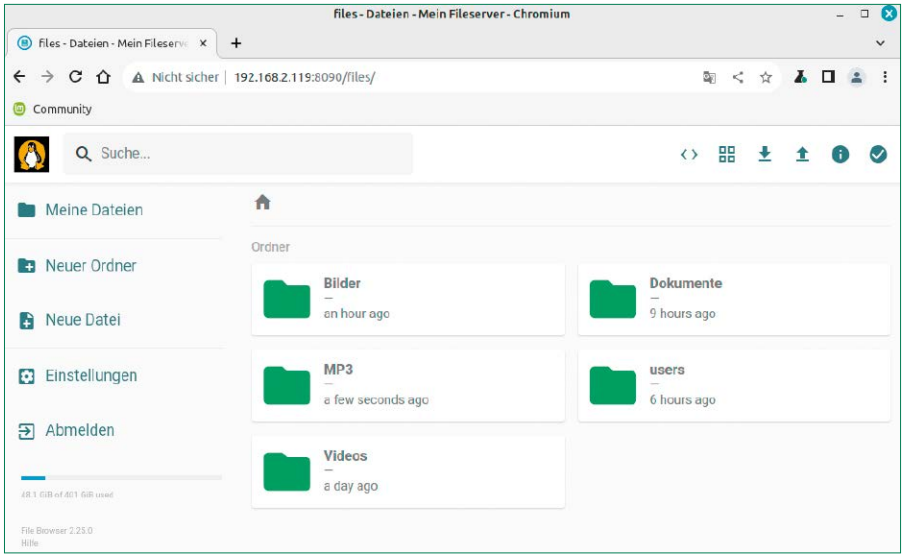
```
upload_max_filesize = 64M
post_max_size = 64M
max_execution_time = 300
```

Sie erhöhen damit das Dateilimit auf 64 MB und geben außerdem Scripts etwas mehr Zeit für die Ausführung.

Mini-Cloud mit Filebrowser

Wer keinen der bekannten Clouddienste für den Dateiaustausch einrichten möchte, verwendet Filebrowser auf dem eigenen PC. Die Software lässt sich einfach installieren und komfortabel nutzen.

VON THORSTEN EGGELING



Die Oberfläche und die Bedienung von Filebrowser erschließt sich sofort. Viele Funktionen gibt es nicht, aber für einen kleinen privaten Cloudserver kann dieser Minimalismus genau richtig sein.

Für eine eigene Cloud gibt es umfangreiche Lösungen, die auch den Ansprüchen von Firmenkunden genügen, beispielsweise Nextcloud (siehe ab Seite 74). Für private Nutzer reicht aber oft eine einfachere Software. Filebrowser (*https://filebrowser.org*) ist schnell installiert, bringt einen eigenen Webserver mit und benötigt keine zusätzliche Datenbanksoftware. Dateien lassen sich in Ordnern organisieren und es ist möglich, Textdateien online in einem Editor zu bearbeiten. Außerdem lassen sich Links für den Download generieren – mit und ohne Passwortschutz.

Service: Die Befehlszeilen und die Beispielkonfiguration für diesen Artikel können Sie über *https://tinyurl.com/FBROWS* abrufen.

Filebrowser installieren

Mit dem Terminalbefehl

```
curl -fsSL https://raw.
 githubusercontent.com/
 filebrowser/get/master/get.sh |
 bash
```

wird das Tool im Ordner „/usr/local/bin“ installiert. Grundsätzlich lässt sich Filebrowser ohne weitere Konfiguration einfach mit den Standardvorgaben starten oder man verwendet Optionen in der Befehlszeile. Über die verfügbaren Optionen gibt der Befehl

```
filebrowser -h
```

Auskunft. Es ist jedoch übersichtlicher, eine Konfigurationsdatei zu erstellen. Legen Sie beispielsweise im Home-Verzeichnis Arbeitsverzeichnisse mit diesen Befehlen an:

```
mkdir -p ~/filebrowser/db
mkdir -p ~/filebrowser/files
```

Im Hauptordner „~/filebrowser“ erstellen eine Textdatei mit dem Namen „filebrower.json“ und folgendem Inhalt:

```
{
"port": 8090,
"baseURL": "",
"address": "[IP]",
"log": "stdout",
"database": "/home/[User]/
 filebrowser/db/filebrowser.db",
"root": "/home/[User]/filebrowser/
 files"
}
```

Für den Platzhalter „[IP]“ setzen Sie die tatsächliche lokale IP des PCs ein („ip a“) und statt „[User]“ setzen Sie Ihren Benutzernamen ein.

Filebrowser konfigurieren und nutzen

Starten Sie das Programm dann immer so:

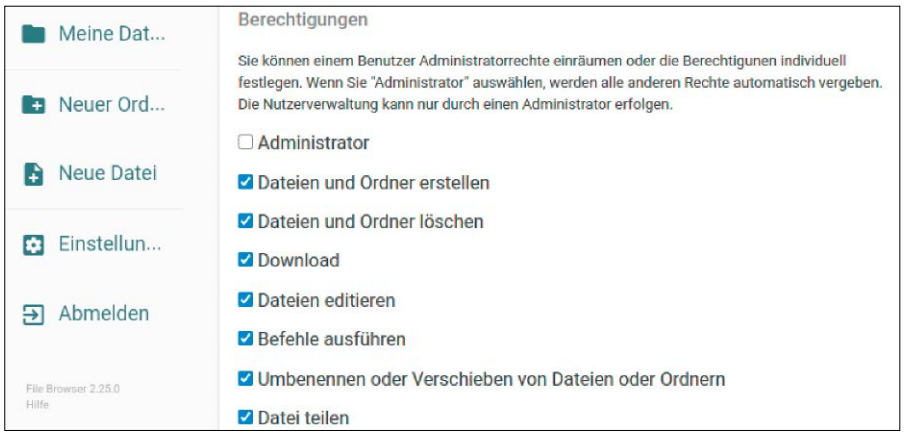
```
filebrowser -c /home/[User]/
 filebrowser/filebrowser.json
```

Danach erreichen Sie die Weboberfläche des Serverdienstes mit

```
http://[IP]:8090
```

im Browser. Den Platzhalter „[IP]“ ersetzen Sie durch die tatsächliche IP-Nummer des PCs. Melden Sie sich mit Benutzername „admin“ und Passwort „admin“ an. Klicken Sie auf „Settings“, wählen Sie unter „Language“ als Sprache „Deutsch“ und klicken Sie auf „Update“. Unter „Passwort ändern“ können Sie ein eigenes Passwort für den Benutzer „admin“ vergeben.

Gehen Sie auf „Globale Einstellungen“. Wenn jeder neu erstellte Benutzer sein eigenes Verzeichnis erhalten soll, setzen Sie ein Häkchen vor „Automatisches Erstellen des Home-Verzeichnisses beim Anlegen neuer Benutzer“. Der Zugriff auf Dateien in anderen Ordnern ist dann nicht möglich. Unter „Benutzer Standard Einstellungen“



Zugriff beschränken: Entfernen Sie Berechtigungen bei Benutzern, die Dateien zwar herunterladen dürfen, aber keine neuen Ordner oder Dateien erstellen sollen.

Sind mehrere Dateien oder Ordner ausgewählt, erstellt Filebrowser ein gepacktes Archiv für den Download. Das Format kann man wählen.

geben Sie die Sprache der Benutzeroberfläche und die Standardberechtigungen vor.
Gehen Sie auf „Benutzerverwaltung“ und erstellen Sie nach einem Klick auf „Neu“ einen weiteren Benutzer. Abweichend vom Standard lassen sich dabei Berechtigungen deaktivieren.

Dateien hoch- und herunterladen: Filebrowser lässt sich auf zwei Wegen mit Daten füllen. Sie können über den Dateimanager einfach Ordner im konfigurierten Verzeichnis („/home/[User]/filebrowser/files“) erstellen und Dateien hineinkopieren.
In der Weboberfläche verwenden Sie „Neuer Ordner“, um einen Ordner zu erstellen. Mit „Neue Datei“ erstellt Filebrowser eine Textdatei, die sich zum Bearbeiten im Editor öffnet. Wurde eine Datei per Mausklick markiert, kann man sie über „Herunterladen“ rechts oben lokal speichern. Mehrere Dateien lassen sich mit gedrückter Strg-Taste markieren. Mit Klick auf die Schaltfläche „Hochladen“ erhält man die Auswahl „Datei“ und „Ordner“. Sie können dann eine Datei (mehrere bei gedrückter Strg-Taste) oder einen Ordner auswählen, den Sie in Filebrowser hochladen.

Dateien oder Ordner freigeben: Ist ein Ordner oder eine Datei markiert, erscheint in der Symbolleiste das Teilen-Icon. Nach einem Klick darauf, kann man die Dauer festlegen, wie lange der Link gültig sein soll. Bleibt das Feld leer, gibt es kein Ablaufdatum. Bei Bedarf lässt sich auch ein Passwort vergeben.

Anpassungen der Weboberfläche

Es gibt begrenzte Möglichkeiten, das Aussehen von Filebrowser anzupassen. Öffnen Sie die Weboberfläche, melden Sie sich als Administrator an und gehen Sie auf „Einstellungen“. Über „Globale Einstellungen“ können Sie unter „Instanzname“ eine Bezeichnung für den Server vergeben, die im Anmeldebildschirm erscheint. Unter „Designverzeichnispfad“ geben Sie einen Ordner an, in dem Sie weitere Dateien für Anpassungen speichern, beispielsweise „/home/[User]/filebrowser/branding“.
Für ein individuelles Logo erstellen Sie in diesem Ordner das Verzeichnis „img“ und darin eine SVG-Datei mit ungefähr 64 x 64 Pixeln. Dieses Bild erscheint als Logo auf der Anmeldeseite und links oben in der Weboberfläche.
Filebrowser berücksichtigt die Datei „branding/custom.css“, in der Sie eigenen CSS-Code unterbringen. So färbt beispielsweise die Anweisung

```
.file-icons [data-dir=true] i {
color: #2ecc71 }
```

die Ordnericons grün statt blau. Für weitere Anpassungen analysieren Sie den Quellcode im Browser.

Filebrowser über Systemd starten

Damit Filebrowser nach dem Systemstart automatisch verfügbar ist, erstellen Sie das Service-Unit „filebrowser.service“ mit diesem Inhalt:

```
[Unit]
Description=Filebrowser
After=network-online.target
[Service]
Type=simple
User=[User]
Group=[User]
ExecStart=/usr/local/bin/
  filebrowser -c /home/[User]/
  filebrowser/filebrowser.json
[Install]
WantedBy=default.target
```

Den Platzhalter „[User]“ ersetzen Sie jeweils durch Ihren Benutzernamen.
Kopieren Sie die Datei mit administrativen Rechten in den Ordner „/etc/systemd/system“. Folgende Befehle

```
sudo systemctl daemon-reload
sudo systemctl enable filebrowser.
  service
sudo systemctl start filebrowser.
  service
```

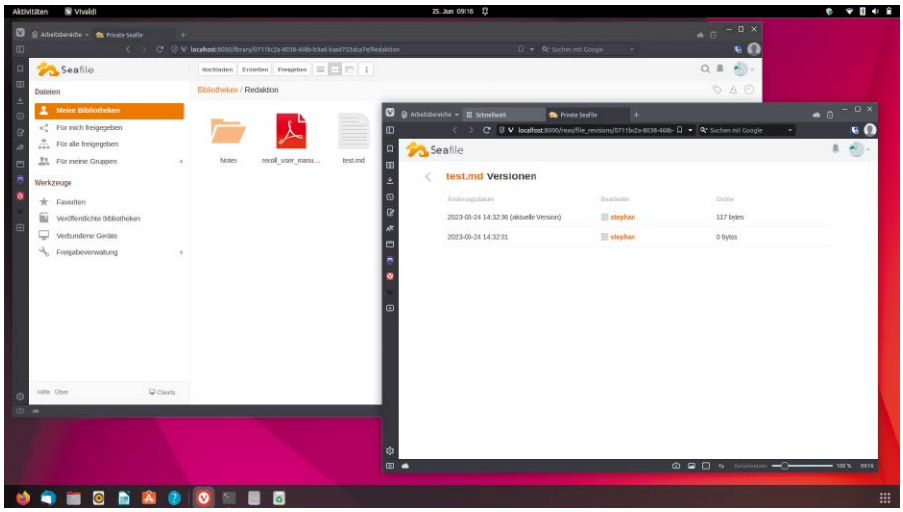
aktivieren den Dienst dann dauerhaft:

Filebrowser über das Internet erreichen

Mit der bisherigen Konfiguration lässt sich Filebrowser nur im lokalen Netzwerk nutzen. Soll der Server über das Internet erreichbar sein, empfiehlt sich der Einsatz von Nginx als Proxyserver. Eine Beschreibung der Konfiguration lesen Sie ab Seite 78. Der Vorteil: Filebrowser ist hinter dem Proxyserver besser gegen Angriffe geschützt und es lässt sich eine SSL-Verschlüsselung mit einem kostenlosen Lets-Encrypt-Zertifikat konfigurieren. Außerdem müssen Sie im Router nur einen Port freigeben (siehe *https://www.pcwelt.de/1198519*), selbst wenn mehrere Serverdienste auf dem PC arbeiten.
Zusätzlich benötigen Sie einen Dienst für dynamische DNS, von dem Sie einen Domainnamen erhalten, etwa *www.noip.com*. Fritzbox-Nutzer finden eine Anleitung für den Myfritz-Dienst unter *https://www.pcwelt.de/1148201*. ■

Datensynchronisation mit Seafile

Wenn es in erster Linie um die Synchronisation von Dateien zwischen verschiedenen Rechnern geht, gibt es mit Seafile eine schlankere und schnellere Alternative zu Nextcloud (oder schlichtem Samba).



VON STEPHAN LAMPRECHT

Nextcloud ist eine hervorragende und beliebte Groupware, die in den vergangenen Jahren intensiv weiterentwickelt wurde. Geht es allerdings nur um die Datensynchronisation zwischen mehreren Clients, also um eine unabhängige Alternative zu Dropbox, Google Drive oder Onedrive, werden die zahlreichen Funktionen gar nicht benötigt. Seafile ist auf den Datenabgleich fokussiert und bietet für diesen Einsatzzweck eine Sammlung von Clients für die verschiedenen Plattformen an. Wenn Sie also auf die weitergehenden Funktionen von Nextcloud verzichten können, kommen Sie mit Seafile schneller ans Ziel.

Die Seafile-Installation

Seafile kann auf einem Raspberry Pi, als virtuelle Maschine oder auf einem Linux-Desktop/Server installiert werden. Entsprechend viele Möglichkeiten für die Installation gibt es auch. Wenn Sie sich mit der Installation und Konfiguration von Serveranwendungen ungern beschäftigen, könnten Sie auf einem Rechner auch das von uns bereits vorgestellte Yunohost installieren (siehe LinuxWelt 3/2022, ab Seite 80, PDF auf DVD). Zu den installierbaren Anwendungen gehört auch Seafile.

In diesem Artikel wird Seafile manuell, aber in Minimalkonfiguration unter Ubuntu eingerichtet. Zur Verwaltung der Dokumente und Versionsstände benötigt Seafile eine Datenbank. Theoretisch können Sie auch Sqlite verwenden, was aber von den Entwicklern selbst nicht mehr empfohlen wird. Als Voraussetzung sollten Sie also erst eine Datenbank installieren und einrichten. Dazu installieren Sie Maria DB, legen einen Seafile-User an sowie die drei Datenbanken für die Software:

```
sudo apt install mariadb-server
sudo mysql_secure_installation
```

Danach melden Sie sich in My SQL mit root-Recht an und erstellen die folgenden drei Datenbanken:

```
sudo mysql -u root -p
CREATE DATABASE seafile_server;
CREATE DATABASE ccnet_server;
CREATE DATABASE seahub_server;
```

Nun folgt noch die Einrichtung des Nutzers („seafile“):

```
CREATE USER 'seafile'@'localhost'
  IDENTIFIED BY '[PASSWORT]';
GRANT ALL ON seafile_server.* TO
  'seafile'@'localhost';
GRANT ALL ON ccnet_server.* TO
  'seafile'@'localhost';
GRANT ALL ON seahub_server.* TO
  'seafile'@'localhost';
QUIT;
```

Seafile ist von Python abhängig. Nachdem Sie die Paketverwaltung auf den aktuellen Stand gebracht haben, installieren Sie eine Reihe von Paketen:

```
sudo apt install ffmpeg memcached
  libmemcached-dev python3 python3-
  {pip,pil,ldap,urllib3,setuptools
  ,mysqldb,memcache,requests}
sudo pip3 install --upgrade pip
sudo pip3 install Pillow pylibmc
  captcha jinja2 sqlalchemy django-
  pylibmc django-simple-captcha
  python3-ldap mysqlclient
```

Es gibt von Seafile keine Binärpakete, sondern nur ein Installations-Script. Das besorgen Sie sich von der Seite des Projekts (*www.seafile.com/en/download/*, hier „Server for generic Linux“ oder auch „Raspberry“). Die einzelnen Schritte sind dabei identisch. Sind die Voraussetzungen erfüllt, legen Sie auf dem System zusätzlich das Systemkonto „seafile“ an. Das ist eine

Sind die Voraussetzungen geschaffen, können Sie das Installations-Script aufrufen. Das erfragt dann automatisch die Daten für die Seafile-Installation.

reine Schutzmaßnahme, da es nie eine gute Idee ist, eine Anwendung als Root auszuführen. Dann legen Sie das Programmverzeichnis an, verleihen dem Nutzer „seafile“ die Rechte

```
sudo mkdir /opt/seafile
sudo chown -R seafile: /opt/seafile
```

und entpacken den Download der Projektseite. Den Inhalt verschieben Sie in das neue Programmverzeichnis unter „/opt“ und starten dort das Installations-Script

```
./setup-seafile-mysql.sh
```

Wenn Seafile wissen möchte, ob es einen bestehenden SQL-Server nutzen will, bejahen Sie dies und tragen die Details der Maria-DB-Installation ein. Danach können Sie Seafile mit *./seafile.sh start* und *./seahub.sh start* aus dem Installationsverzeichnis starten.

Das Konzept von Seafile

Nach erfolgreichem Start können Sie sich mit jedem Browser mit der IP-Adresse am System anmelden. Standardportnummer ist 8000 – also insgesamt „[IP]:8000“. Als Admin-Nutzer erreichen Sie die Verwaltung mit einem Klick auf das Profil-Icon am oberen Bildschirmrand. Über die verschiedenen Menüpunkte steuern Sie die Verwaltung neuer Nutzer (Anlage, Bearbeitung, Löschen), die Organisation der Benutzer in Form von Gruppen, verwalten verbundene Geräte und die Bibliotheken.

Die Bibliotheken sind das Herzstück von Seafile. Jeder Nutzer besitzt seine eigene Bibliothek, die sich mit einem Home-Ordner vergleichen lässt. Darin gespeicherte Inhalte darf er auch selbständig teilen. Dazu klickt er lediglich in der Ansicht auf „Freigeben“. Als Ziel hat er die Wahl zwischen anderen Nutzern der gleichen Instanz, einer Gruppe des Systems, aber auch externen Personen, die dann Inhalte herunterladen oder auch hinzufügen können. Bei der Anlage solcher Links können eine zeitliche Befristung und ein optionales Passwort hinzugefügt werden. Wie er seine Bibliotheken organisiert, steht jedem Nutzer frei. Optional lässt sich eine Bibliothek auch veröffentlichen. Sie ist dann direkt über ihre URL erreichbar. Das alles funktioniert auch ohne die Installation eines Clients auf einem anderen System. Um Wildwuchs auf dem System zu vermeiden, sollten Sie als Admin über eine Dateistruktur nachdenken, um diese in Form von Bibliotheken zu organisieren, denen Sie dann Gruppen oder Nutzer zuweisen. Bei der Anlage der Bibliothek erreichen Sie in der Liste über die drei Punkte weitere Funktionen. Eine der wesentlichsten ist sicherlich die Aktivierung der Versionierung. Hierbei entscheiden Sie, ob alle Versionen gespeichert werden oder sich die Überwachung auf einen Zeitraum beschränken soll. Im Browser erreichen Sie die Versionsübersicht mittels eines Rechtsklicks auf die Datei. Über das Kontextmenü legen Sie bei Bedarf auf Kommentare an.

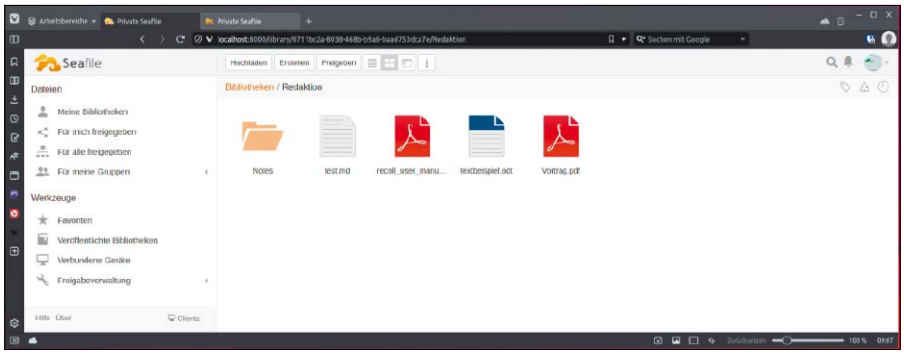
Mit Clients zugreifen

Zur Synchronisierung mit einem zentralen Datenbestand ist der Einsatz dieser Clientprogramme zu empfehlen, die es für Windows, Linux und Mac gibt (*www.seafile.com/en/download*). Im Downloadbereich der Seafile-Homepage gibt es zwei verschiedene Clientvarianten. Mit „Drive Clients“ binden Sie eine Seafile-Instanz und deren Bibliotheken wie ein Netzlaufwerk ein. Es findet in diesem Fall aber keine permanente Synchronisierung statt. Sie öffnen eine Datei also wie bei einer Windows/Samba-Freigabe und bearbeiten sie. „Syncing Clients“ bieten hingegen eine Synchronisation wie etwa bei Dropbox oder Onedrive. Lokale Änderungen werden also automatisch zum Server gepusht und dann an die anderen Clients übermittelt.

Wie bei ähnlichen Lösungen gilt auch in diesem Fall: Nicht jedes Programm kommt mit dieser Echtzeit-Synchronisierung zurecht.

Schlank und schnell

Wenn Sie auf zentrale Telefonbücher, Terminkalender oder Kanban-Boards verzichten können, ist Seafile eine schnelle Methode zum Datenabgleich mit verschiedenen Systemen und Nutzern. Beim Scrollen durch umfangreichere Fotosammlungen wird Sie Seafile in Hinblick auf die Geschwindigkeit überraschen. Dank des Markdown-Formats und eines integrierten Editors ist auch der schnelle Austausch von Textinformationen einfach möglich. Und wenn es um Office-Dokumente geht, können Sie optional auch Only Office und Collabora integrieren, um darüber dann direkt diese Formate zu bearbeiten. ■



Zentrales Element bei Seafile sind die Bibliotheken, in denen die Dokumente organisiert werden. Über Nutzer- und Gruppenverwaltung legt der Administrator die Zugriffsrechte fest.

Linux-Hardware und Treiber

Meist lässt sich Linux auf PCs oder Notebooks problemlos installieren. Sehr neue oder exotische Hardware wird von Linux jedoch manchmal nicht erkannt. Prüfen Sie daher möglichst vor dem Kauf, ob die Hardware mit Linux kompatibel ist.

VON THORSTEN EGGELING

Die Linux-Installation bereitet auf den meisten PCs und Notebooks kaum Probleme. Zusätzliche Treiber sind oft nicht erforderlich, weil alles Nötige bei Linux bereits dabei ist. Peripheriegeräte, zumindest von bekannten Herstellern, werden von Linux ebenfalls gut unterstützt (siehe ab Seite 28). Es gibt jedoch keine Garantie dafür, dass ein bestimmtes Gerät von einem Linux-System erkannt und auch optimal eingebunden wird. Gegenwärtige und zukünftige Linux-Nutzer sollten daher vor dem Kauf neuer Hardware genau hinsehen und detaillierte Informationen einholen. Wenn Hardware, beispielsweise von Ubuntu 20.04 oder Linux Mint 20, nicht standardmäßig unterstützt wird, gibt es aber auch dafür Lösungen. Mit etwas Bastelarbeit lässt sich auch standardmäßig nicht unterstützte Hardware in Betrieb nehmen, wenn passende Treiber in einem neueren Linux-Kernel enthalten sind. Eine einfache Alternative ist der Umstieg auf eine andere Linux-Distribution mit aktuellerem Kernel.

1. Linux-Treiber und Kernel

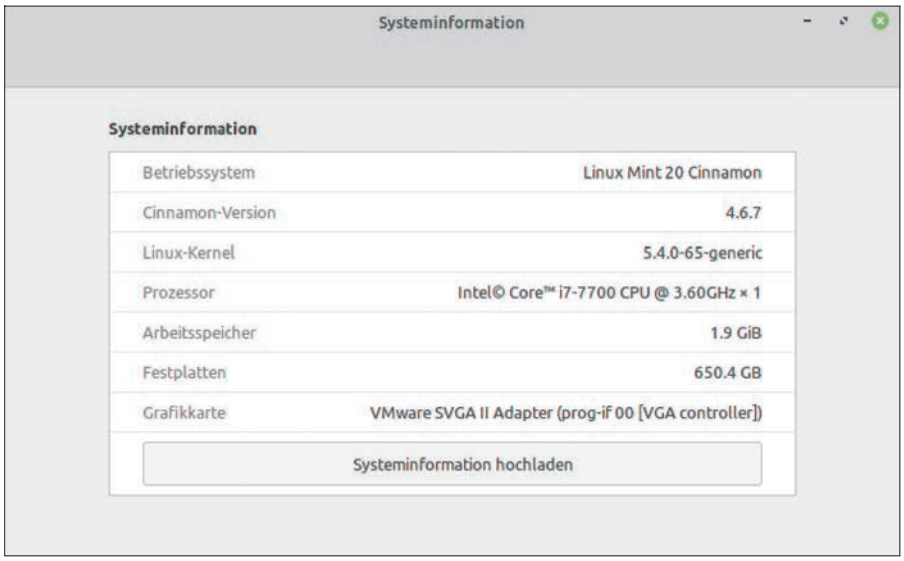
Ein Computer besteht aus zahlreichen Hardwarekomponenten und für alle ist ein eigener Treiber erforderlich. Unter Linux sind Treiber, die hier als Kernel-Module bezeichnet werden, im Betriebssystemkern (Kernel) enthalten oder werden von diesem bei Bedarf geladen. Neue Kernel erscheinen alle zwei bis drei Monate und enthalten neben Fehlerkorrekturen und Verbesserungen auch neue Module für aktuellere Hardware.

LTS-Distributionen (Long Term Support) wie Ubuntu 20.04 oder Linux Mint 20 sind auf lange Laufzeiten von fünf Jahren ausgelegt. Um die Stabilität des Systems sicherzustellen, beseitigen Updates nur Fehler und Sicherheitslücken. Die Hauptversionsnummern von Kernel und anderer Basissoftware bleiben standardmäßig gleich. Das hat zur Folge, dass Hardware nicht unterstützt wird, die vor Erscheinen des Kernels auf den Markt kam oder für die zu diesem Zeitpunkt noch kein Linux-Treiber verfügbar war.

Im ungünstigsten Fall ist eine LTS-Version bei der Neuinstallation knapp zwei Jahre alt, der Kernel sogar noch etwas älter. Damit das auf neuer Hardware nicht zu Problemen führt, erscheint etwa alle sechs Monate ein Point Release von Ubuntu (18.04.4, 18.04.5, 20.04.1, 20.04.2). Die Version enthält alle bisherigen Updates und meist auch einen neueren Kernel. Das letzte Point Release einer Version wird mit dem Kernel des Nachfolgers ausgeliefert. Für Linux Mint, das auf Ubuntu basiert, gibt es ebenfalls Point Releases, wenn auch in etwas größeren Abständen.

Bestehende Installationen lassen sich bei Bedarf auf den Stand des jeweils aktuellen Point Release bringen (siehe Punkt 5). Ein Kernel-Upgrade ist sinnvoll, wenn zusätzlich eingebaute Hardware vom bisherigen Kernel nicht unterstützt wird oder Treiber eine neuere Kernel-Version erfordern.

Die von Ubuntu angebotenen Updates und Upgrades sind ausreichend getestet und gelten daher als sicher. Es ist aber möglich, noch neuere Kernel zu installieren (siehe Punkt 5). Damit ist jedoch nicht garantiert, dass das System stabil läuft und alle Komponenten zusammenpassen. Ein großes Risiko besteht jedoch nicht, weil man im Problemfall zum vorherigen Kernel zurückkehren kann.



Nicht wirklich aktuell: LTS-Versionen kommen mit sehr aktueller Hardware teilweise schlecht zurecht. Der Kernel 5.4 von Linux Mint 20 („Ulyana“) wurde bereits Ende 2019 veröffentlicht.

2. Distributionen mit besserer Hardwareunterstützung

Linux Mint und Ubuntu sind bewährte Distributionen, die sich auch für Einsteiger eignen. Wer Probleme mit sehr neuer Hardware vermeiden möchte, greift jedoch besser zu einer Distribution mit kürzeren Updatezyklen. Als Favorit kann Fedora (*https://getfedora.org*) gelten, das sich bei Installation und Nutzung nicht wesentlich von Ubuntu unterscheidet, aber aktuellere Kernel als regelmäßige Updates anbietet.

Für aktuelle Hardware ebenfalls empfehlenswert ist Open Suse Tumbleweed (*https://de.opensuse.org/Portal:Tumbleweed*), das als Rolling Release ständig auf dem aktuellsten Stand gehalten wird. Linux-Profis greifen gerne zu Arch Linux (*www.archlinux.de*), das für Einsteiger jedoch schwer zu installieren ist. Ein grafischer Installer fehlt und daher ist viel Handarbeit erforderlich. Eine Arch-Variante mit niedrigerer Einstiegshürde ist Endeavour-OS (*https://endeavouros.com*), das einen grafischen Installer in einem Livesystem bereitstellt.

Allen genannten Alternativen ist gemeinsam, dass sich Aktualität nur auf Kosten der Stabilität erreichen lässt. Damit ist nicht gemeint, dass sich die Systeme nicht produktiv nutzen lassen. Man muss jedoch aufgrund neuer und weniger getesteter Softwarepakete eher mit Problemen rechnen als beim konservativen Ubuntu oder Linux Mint.

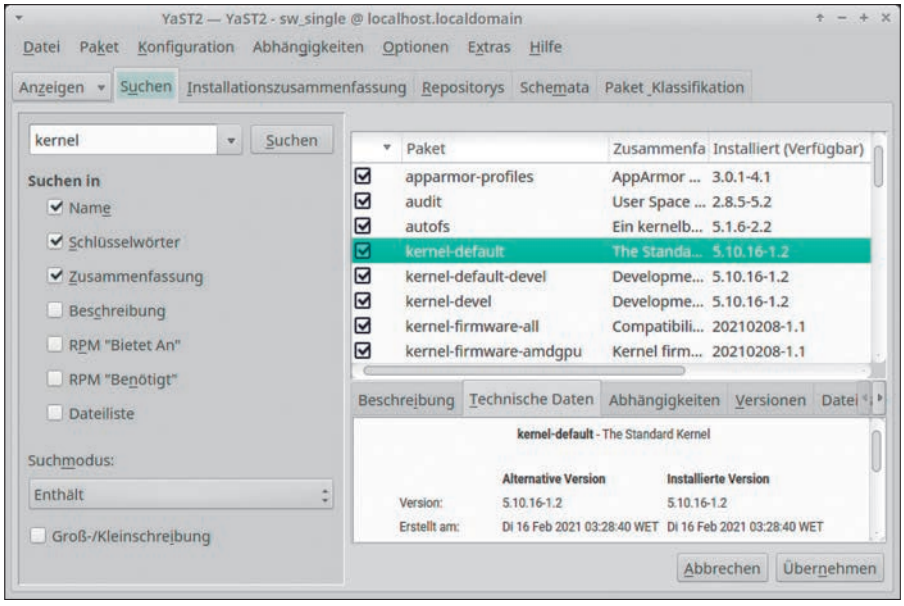
Ein Spezialfall liegt vor, wenn das Installationssystem den Netzwerkadapter nicht erkennt. Dann ist auch kein Update auf einen neueren Kernel möglich, der die Hardware unterstützt.

In diesem Fall ist es am einfachsten, vorübergehend einen externen Ethernet- oder WLAN-Adapter am USB-Port anzuschließen. Ältere oder besonders preisgünstige USB-Adapter für zehn bis 20 Euro funktionieren unter Linux meist problemlos (siehe auch ab Seite 28). Sollte das nicht möglich sein, laden Sie die Kernel-Pakete (siehe Punkt 5) auf einem anderen PC herunter und die Installation erfolgt dann manuell über einen USB-Stick.

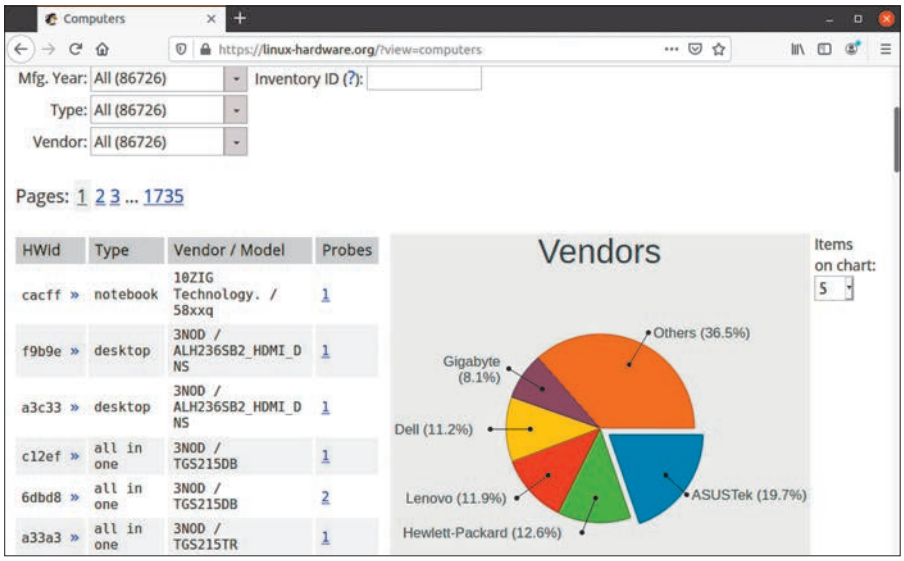
3. Geeignete Hardware für Linux finden

Wer sich mit der Hardware des PCs nicht selbst eingehend beschäftigen möchte, überlässt die Arbeit den Experten. Mehrere Hersteller bieten PCs und Notebooks mit vorinstalliertem Linux an oder sichern zumindest die Linux-Tauglichkeit zu. Canonical, das Unternehmen hinter Ubuntu, pflegt unter *https://certification.ubuntu.com/desktop* eine Liste mit zertifizierter Hardware. Die genannten Hersteller sind zurzeit Dell, Lenovo, HP, Intel und Acer. Zu jedem Gerät gibt es Angaben, mit welcher Ubuntu- und Kernel-Version es getestet wurde und welche Komponenten enthalten sind. Da Linux Mint auf Ubuntu basiert, sollte die Hardware auch mit dieser Distribution einsetzbar sein.

Einige Firmen und Händler bieten die Vorinstallation von Linux an, entweder auf Geräten bekannter Marken oder selbst zusammengestellter Hardware. Für Debian gibt es eine Liste von Firmen unter *https://www.debian.org/distrib/pre-installed*. Es handelt sich dabei aber meist um Anbieter für Unternehmens- und Serverlösungen. Ein umfangreiches Angebot für Firmen wie Privatkunden ist bei *https://www.tuxedocomputers.com* zu finden. Hier gibt es Linux-PCs und Notebooks für jeden Anwendungsbereich. Das System ist optimal auf die Hardware abgestimmt. Sollte doch einmal etwas klemmen, erhalten Sie Support per E-Mail oder Telefon.



Immer auf dem neuesten Stand: Rolling Releases wie Open Suse Tumbleweed werden ständig aktualisiert und eignen sich besonders gut für sehr aktuelle Hardware.



Was läuft unter Linux? Die Daten auf *https://linux-hardware.org* stammen von Einsendungen der Nutzer und liefern Information zu Hardware, die Linux unterstützt.

Bei einem beliebigen Gerät aus dem aktuellen Angebot eines Onlinehändlers oder lokalen Discounters kann niemand für die Linux-Unterstützung garantieren. Bis auf seltene Ausnahmen wird Ihnen auch der Händler nichts über Linux-Erfahrungen berichten können. Zurzeit gibt es keine zentrale Datenbank, in der die Kompatibilität jeder Hardware mit Linux-Distributionen oder Linux-Kerneln erfasst ist. Es ist daher nicht einfach möglich zu ermitteln, ob ein bestimmter PC oder ein Notebook in jeder Hinsicht perfekt unter Linux arbeitet. Trotzdem gibt es Hilfe und Infos:

Als Erstes sollte man eine Websuche nach dem gewünschten Computermodell kombiniert mit dem Suchbegriff „Linux" starten. Vielleicht haben andere Nutzer bereits Erfahrungen sammeln können und berichten von Erfolgen oder möglichen Problemen.

https://linux-hardware.org kann ebenfalls nützliche Informationen liefern. Die Datenbank basiert auf von Linux-Nutzern eingesendeten Testdaten und enthält daher nicht unbedingt die neusten Modelle. Über „Find Computer" kann man per Auswahl von „Type", „Vendor" (Hersteller) und „Model" eine Abfrage starten. Wählen Sie hinter „Mfg. Year" ein Jahr aus, um das Ergebnis auf einen Herstellungszeitraum zu beschränken.

https://linux-hardware.org zeigt an, mit welcher Linux-Distribution und welcher Kernel-Version der Test durchgeführt wurde. Unter „Devices" sind die einzelnen Komponenten aufgelistet. In der Spalte „Status" signalisiert „works", dass die Komponente funktioniert. Steht hier „detected", wird die Hardware zwar erkannt, es gibt jedoch noch keinen Test. Ein Ausrufungszeichen weist auf kleinere Probleme oder zusätzliche Anmerkungen hin. Per Klick auf das Feld gelangen Sie zur Detailansicht für das Gerät. Beim Status „failed" gibt es meist den Hinweis, dass kein Linux-Kernel diese Hardware unterstützt. Manchmal sind aber auch weiterführende Infos zu finden, wie man eine Komponente dennoch in Betrieb nehmen kann.

Eigene Hardware testen: Wer die Daten des PCs bei *https://linux-hardware.org* einsenden möchte, findet Informationen dazu über den Link „creating a probe". Nutzer von Ubuntu oder Linux Mint installieren das nötige Tool im Terminal:

```
sudo apt install hw-probe
```

Nach dem Start mit

```
sudo -E hw-probe -all -upload
```

erhalten Sie eine URL, die Sie im Webbrowser aufrufen.

4. Gezielte Suche nach Einzelkomponenten

Eine weitere Website, über Sie die Linux-Kompatibilität ermitteln können, ist *https://cateee.net/lkddb*. Die „Linux Kernel Driver Data Base" enthält Namen und numerische IDs von Hardware sowie deren Vorkommen im Kernel-Quellcode. Damit lässt sich ermitteln, ab welcher Kernel-Version eine Hardware unterstützt wird. Nutzbar ist das jedoch nur, wenn Sie die genaue Bezeichnung oder Hardware-ID einer Komponente kennen.

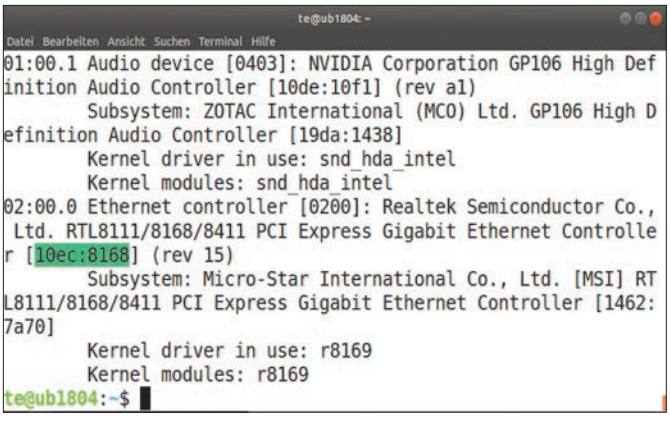
Letztere bekommen Sie heraus, wenn Sie bei *https://linux-hardware.org* nach einem PC oder Notebook suchen oder wenn Sie die Hardware bereits besitzen und Linux oder Windows auf dem Rechner läuft (siehe Kasten „Die Bedeutung von PCI- und USB-IDs" auf der nächsten Seite).

Ein Beispiel: lspci gibt folgende Info aus: „Realtek Semiconductor Co., Ltd. RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller [10ec:8168]", ferner den Hersteller des Mainboards mit „Subsystem: Micro-Star International Co., Ltd. [MSI] RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller [1462:7a70]". „Kernel driver in use: r8169" zeigt an, dass die Hardware erkannt und dafür das Kernel-Modul „r8169" geladen wurde.

Wichtig ist die Hardware-ID „10ec:8168". Eine Google-Suche bei *https://cateee.net/lkddb* kann dann mit der folgenden Suchanfrage erfolgen:

```
10ec 8168 site:cateee.net
```

Im ersten Suchergebnis sehen Sie im Abschnitt unter „LKDDb" mehrere Zeilen, die mit „lkddb pci 10ec 8168" beginnen. Am Ende jeder Zeile steht, in welchen Kerneln



Was steckt im PC? lspci gibt Bezeichnungen und Hardware-IDs der PC-Komponenten aus. Außerdem zeigt es an, welches Kernel-Modul geladen wurde.

die Hardware-ID gefunden wurde. In diesem Fall sind das die Versionen 3.17 bis 5.11.Bei USB-Geräten gibt es nur eine Hersteller- und Geräte-ID, aber keine Subsystem-ID. lsusb liefert die IDs, jedoch keine Infos über den geladenen Treiber. Dafür verwenden Sie

```
sudo usb-devices
```

Taucht in der Ausgabe „Driver=(none)“ auf, wurde kein Treiber geladen. Die Google-Suche beispielsweise für einen USB-WLAN-Adapter (TP-Link TL-WDN5200 T2U) mit

```
148f 761a site:cateee.net
```

zeigt, dass das passende Kernel-Modul „MT76x0U“ heißt und die Hardware erst ab Kernel-Version 4.20 unterstützt wird (siehe auch ab Seite 28).

5. Neue Kernel für neue Hardware

Abhängig von Ihren Recherchen installieren Sie einen neueren Kernel, um die Hardwareunterstützung zu verbessern. Vielleicht reicht der offizielle HWE-Kernel (Hardware Enablement) des nächsten Point Releases schon aus (siehe Punkt 1). Welcher Kernel aktuell verwendet wird, ermitteln Sie im Terminal:

```
uname -a
```

Mit der Zeile

```
apt search linux-generic-hwe
```

finden Sie Version des HWE-Kernels heraus. Ist der HWE-Kernel neuer als der installierte, installieren Sie ihn zusammen mit dem aktuellen X-Server:

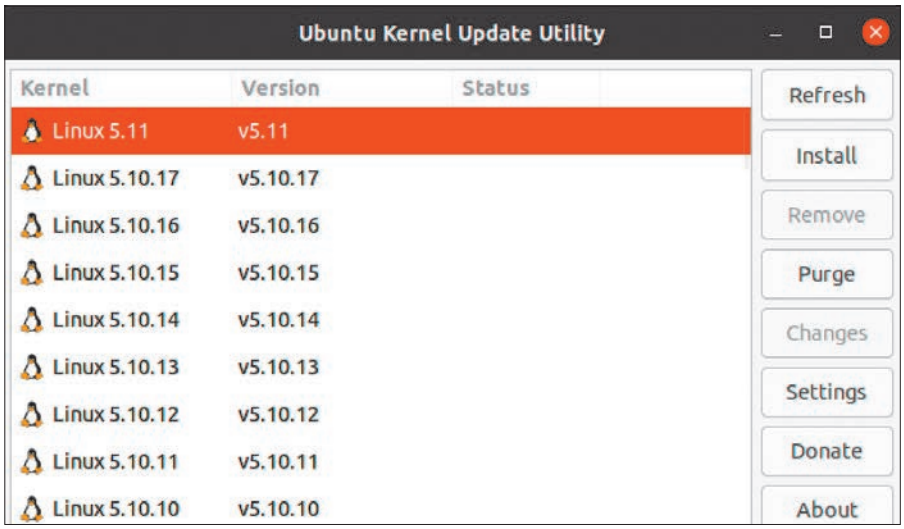
```
sudo apt-get install --install-
  recommends linux-generic-
  hwe-20.04 xserver-xorg-hwe-20.04
```

Die Versionsnummern passen Sie für andere Versionen an. Statt „20.04“ verwenden Sie beispielsweise „18.04“ für Ubuntu 18.04. Wer den HWE-Kernel unter Linux Mint installieren möchte, geht im Menü auf „Systemverwaltung → Aktualisierungsverwaltung“ und dann auf „Ansicht → Linux-Kernel“.

Die aktuellsten Kernel finden Sie unter *https://kernel.ubuntu.com/~kernel-ppa/mainline*. Bei Redaktionsschluss waren Kernel bis Version 5.11 als DEB-Pakete zum Download verfügbar. Für ein 64-Bit-System laden Sie unter „amd64“ alle Pakete herunter, die „generic“ enthalten, und die Datei mit der Endung „all.deb“. Neuere 32-Bit-Kernel werden nicht mehr bereitgestellt.

Im Terminal erfolgt die Installation im Downloadverzeichnis:

```
sudo dpkg -i *.deb
```



Kernel-Upgrade: Auch in LTS-Versionen lassen sich deutlich aktuellere Kernel installieren. Die gibt es bei *https://kernel.ubuntu.com*. Das Tool Ukuu vereinfacht die Installation.

Beachten Sie, dass bei sehr neuem Kernel die Wahrscheinlichkeit geringer ist, dass sich zusätzliche Treiber damit kompilieren lassen. Das kann Nutzer betreffen, die den proprietären Nvidia-Treiber (siehe ab Seite 24) oder Virtualbox verwenden.

Bei Problemen rufen Sie das Grub-Bootmenü auf. Sollte es nicht automatisch erscheinen, halten Sie die Umschalttaste nach dem Einschalten des PCs gedrückt. Im Menü gehen Sie auf „Erweiterte Optionen für Ubuntu“ beziehungsweise „Erweiterte Option für Linux Mint“ und wählen einen älteren Kernel. Danach deinstallieren Sie die neuere Version über die Paketverwaltung.

Wer neuere Kernel über die grafische Oberfläche installieren möchte, lädt sich das Tool Ukuu herunter (*https://github.com/teejee2008/ukuu*). Es ermöglicht die einfache Installation und Deinstallation der Kernel von *https://kernel.ubuntu.com* in Ubuntu und Linux Mint. ■

DIE BEDEUTUNG VON PCI- UND USB-IDS

Jede Hardware besitzt eine eindeutige ID, über die sich Hersteller und Gerätetyp ermitteln lassen. Die Verkaufsbezeichnung ist meist weniger eindeutig, weil einige Hersteller im Laufe der Fertigung andere Chips verbauen, ohne die Modellnummer zu ändern. Die Hardware-IDs ermitteln Sie unter Linux im Terminal mit diesen drei Befehlszeilen:

```
sudo lshw -numeric -html > lshw.html
sudo lspci -knn > lspci.txt
sudo lsusb -v > lsusb.txt
```

In der Datei „lshw.html“ finden Sie danach allgemeine Informationen zum PC, Typ der Hauptplatine, Bios-Version sowie Prozessor. „lspci.txt“ enthält Informationen zu den über PCI angebundenen Komponenten wie Soundchips („Audio device“), Grafikkarten („VGA compatible controller“) und Netzwerkchips („Ethernet controller“). In der Datei „lsusb.txt“ sehen Sie, welche Geräte mit den USB-Ports verbunden sind.

Unter Windows öffnen Sie den Gerätemanager (devmgmt.msc), rufen per rechten Mausklick die „Eigenschaften“ eines Gerätes auf und wechseln auf die Registerkarte „Details“. Unter „Eigenschaft“ stellen Sie „Hardware-IDs“ ein.

Eine Hardware-ID besteht aus der Vendor-ID (Chip-Hersteller) und einer Device-ID (Gerät). Beide nutzt der Linux-Kernel, um den passenden Treiber zu finden. Dazu kommt eine zweiteilige Subsystem-ID, die den Hersteller des Komplettgerätes enthält und die Sie nicht weiter beachten müssen.

Grafikkarten & Monitore optimal nutzen

Auch Grafikadapter benötigen Treiber und davon gibt es unter Linux gleich mehrere. Abhängig vom Einsatzbereich kann sich die Installation eines neueren und optimierten Treibers lohnen.

VON THORSTEN EGGELING

Die Anzahl der Anbieter von Grafikchips ist überschaubar. Die Basisausstattung steckt meist bereits im Hauptprozessor, der von Intel oder AMD stammt. Die Leistung genügt für Desktopanwendungen, Videowiedergabe in HD-Qualität und einfache Spiele. Wer mehr benötigt, vor allem für grafisch anspruchsvolle Spiele, greift zu Geräten mit einem zusätzlichen Grafikchip von Nvidia oder AMD. Der sitzt bei Notebooks auf der Hauptplatine, PCs lassen sich mit einer separaten Grafikkarte ausstatten. Aktuelle Linux-Systeme unterstützen alle genannten Grafikchips. Lediglich bei sehr neuen Modellen kann es zu Problemen bei der Linux-Installation kommen, was sich aber leicht beheben lässt. Die standardmäßig installierten Open-Source-Grafiktreiber reichen für die meisten Anwender aus, für optimale Leistung empfiehlt sich die Installation eines Treibers vom Hersteller.

1. Grafikchips und Treiber

Prozessorgrafik von Intel und AMD funktioniert dank Unterstützung durch die Hersteller in der Regel gut. Bei Grafikkarten geben viele Linux-Nutzer Nvidia-Chips den Vorzug, weil die Installation eines optimierten Treibers unter Ubuntu oder Linux Mint mit wenigen Mausklicks erledigt ist. Bei AMD-Grafikchips bietet allerdings schon der standardmäßige Open-Source-Treiber eine ausreichend gute Unterstützung. Wer möchte, kann trotzdem auch hier einen neueren Treiber installieren.

Eine Besonderheit bei Linux: Das System benötigt zwei Treiber. Der erste gehört zum Kernel und sorgt für die Darstellung der Textkonsole. Meist kommt der standardmäßige Vesa-Framebuffer-Treiber zum Einsatz. Der unterstützt keine speziellen Fähigkeiten des Grafikchips, genügt aber für eine höhere Auflösung in der Textkonsole. Die bekommen Sie in der Regel gar nicht zu sehen, weil das System gleich die grafische Oberfläche startet, deren Basis der Xserver ist. Hier wird ein Xorg-Treiber verwendet, der 2D-Beschleungigung für die bessere Darstellung der Fensterelemente und 3D-Beschleunigung für grafische Anwendungen bieten kann. Zudem kann der Treiber zusammen mit einigen Programmbibliotheken den Prozessor der Grafikkarte (GPU, Graphics Processing Unit) für die Decodierung (Abspielen) und Encodierung (Umwandeln) von Videos nutzen. Das entlastet den Hauptprozessor (CPU, Central Processing Unit) des Rechners und sorgt für die ruckelfreie Wiedergabe auch von hochauflösenden Videoinhalten.

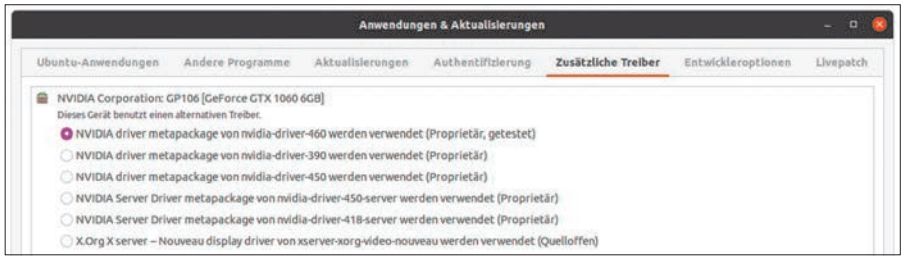
2. Grafikprobleme bei der Installation beheben

Ubuntu 20.04 und Linux Mint 20 verwenden bei der Installation einen Standardtreiber für Nvidia-Grafikchips („nouveau“). Der funktioniert in der Regel, bei einigen sehr neuen Chips startet das Livesystem jedoch nicht bis zum Desktop oder friert ein. Das Problem lässt sich umgehen, indem man beim Start vom Installationsmedium nach der Sprachauswahl „Ubuntu ohne Installation ausprobieren (abgesicherter Grafikmodus)“ wählt. Unter Linux Mint heißt die Option „Start in compatibility mode“). Im Uefi-Modus wählen Sie den Eintrag „safe graphics“, bei Linux Mint „compatibility mode“. Ubuntu-Nutzer setzen bei der Installation ein Häkchen vor „Installieren Sie Software von Drittanbietern für Grafik- und Wi-Fi-

Hardware und zusätzliche Medienformate". Die Installation sollte dann reibungslos ablaufen. Ubuntu richtet den proprietären Nvidia-Treiber automatisch ein und der Desktop erscheint wie erwartet.

Unter Linux Mint müssen Sie zuerst das Grub-Bootmenü aufrufen, indem Sie beim Neustart des PCs die Umschalt-Taste gedrückt halten. Drücken Sie die Taste E, um den Standardmenüeintrag zu bearbeiten. Gehen Sie in die Zeile, die mit „linux" beginnt, tragen Sie hinter „ro" die Option „nomodeset" ein und starten Sie dann Linux Mint mit Taste F10. Nach dem Systemstart gehen Sie im Menü auf „Systemverwaltung → Treiberverwaltung", wählen dort den Treiber mit der höchsten Versionsnummer und dem Zusatz „empfohlen", klicken auf „Änderungen anwenden" und schließlich auf „Neustarten".

Beim Start im abgesicherten Grafikmodus lädt Ubuntu keine Treiber, die den Start der grafischen Oberfläche verhindern. Der passende Treiber wird dann automatisch eingerichtet.



Verbesserte Treiber installieren: Ubuntu bietet mehrere Herstellertreiber zur Installation an. In der Regel wählen Sie die höchste Versionsnummer mit dem Zusatz „getestet".

3. Den optimalen Grafiktreiber nutzen

Für viele Nutzer ist der Nouveau-Standardtreiber für Nvidia-Chips ausreichend. Wenn Sie Spiele oder Videobearbeitungssoftware nutzen oder die Videowiedergabe ruckelt, sollten Sie aber auf den proprietären Nvidia-Treiber umsteigen. Der Weg führt unter Ubuntu über „Aktivitäten", die Suche nach „Treiber" und Klick auf „Zusätzliche Treiber", bei Linux Mint über „Systemverwaltung → Treiberverwaltung". Wählen Sie den Treiber mit der höchsten Versionsnummer und dem Zusatz „Proprietär, getestet" (Linux Mint „empfohlen"). Klicken Sie auf „Änderungen anwenden" und starten Sie Linux nach Abschluss der Installation neu.

Grafikchips von AMD: Linux-Distributionen verwenden automatisch den passenden Standardtreiber. Das Paket „xserver-xorg-video-ati" unterstützt sehr alte Grafikchips wie AMD/ATI Mach64, Rage128, Radeon, FireGL oder FireMV. „xserver-xorg-video-radeon" kommt bei Modellen wie R100 bis RV790 zum Einsatz. Der neueste Treiber steckt im Paket „xserver-xorg-video-amdgpu" und eignet sich für die Chipsatz-Familien Bonaire, Hawaii, Kaveri, Kabini Mullins, Iceland, Tonga, Carrizo, Fiji und Stoney. Nicht bei jedem Chipsatz werden bisher alle Funktionen unterstützt. Detaillierte Infos dazu liefert die Webseite *https://www.x.org/wiki/RadeonFeature*.

Grafikchips von Intel: Bei Chips ab Baujahr etwa 2007 wird nur der Kernel-Treiber geladen. Es ist zwar bei Ubuntu und Linux Mint auch das Paket „xserver-xorg-video-intel" installiert, die Treiber kommen aber bei neuerer Hardware nicht mehr zum Einsatz.

MONITORANSCHLÜSSE, KABEL UND 4K-AUFLÖSUNG

Einen Monitor verbinden Sie am besten über die digitalen Anschlüsse Displayport, HDMI oder DVI. Ubuntu oder Linux Mint erkennen die maximal mögliche Auflösung dann automatisch. Analoge VGA-Kabel sollten Sie nur benutzen, wenn ein älterer PC oder Monitor nichts anderes anbietet. Die Qualität ist schlechter, außerdem wird die passende Auflösung oft nicht erkannt und muss manuell justiert werden.

Für Auflösungen bis 1920 × 1200 Pixel genügt ein Single-Link-DVI-Kabel mit 18+1 Kontakten; für höhere Auflösung muss es ein Dual-Link-DVI-Kabel mit 24+1 Kontakten sein. Für einen hochauflösenden Monitor (Ultra-HD, 4K) nutzen Sie ein HDMI-2.0-Kabel, das den Hinweis „4k", „UHD" oder „2160p" auf der Verpackung trägt. Andernfalls liegt die Bildwiederholfrequenz nur bei 30 statt 60 Hz, was zu einer schlechteren Bildqualität führt. Bei der Grafikkarte ist dafür ein HDMI-2.0-Ausgang erforderlich. Alternativ verwenden Sie ein Displayport-Kabel. Für 60 Hz muss die Grafikkarte mindestens den Displayport-Standard 1.2 beherrschen.

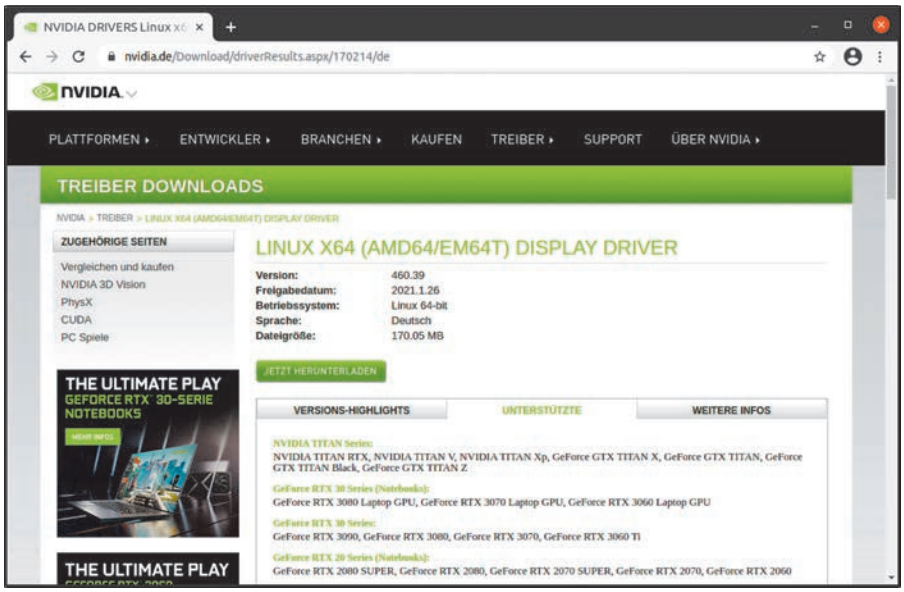
Bei voller 4K-Auflösung von 3840 × 2160 Pixeln sehen zwar Videos prima aus, Desktopelemente sind aber oft schwer zu erkennen. Bei Ubuntu 20.04 können Sie in den „Einstellungen" unter „Anzeigegeräte" die „Fraktionelle Skalierung" aktivieren. Hinter „Skalieren" stellen Sie dann beispielsweise „125 %" ein. Auf der gleichen Einstellungsseite lassen sich auch weitere Monitore aktivieren und bei Bedarf mit unterschiedlichen Auflösungen konfigurieren.

Linux-Mint-Nutzer finden die entsprechenden Optionen über „Einstellungen → Bildschirm".

Weitere Einstellungen ändern Sie unter Ubuntu über das Tool gnome-tweaks, das Sie per

```
sudo apt install gnome-tweaks
```

im Terminal installieren. Starten Sie das Tool über eine Suche nach „Optimierungen" unter „Aktivitäten". Gehen Sie auf „Schriften" und stellen Sie den gewünschten Skalierungsfaktor ein. Unter Linux Mint ist die Konfiguration über „Einstellungen → Schriftauswahl" möglich.



Welcher Treiber passt? Im Downloadbereich informiert Nvidia darüber, welche Grafikchips beziehungsweise Grafikkarten eine bestimmte Treiberversion unterstützt.

4. Herstellertreiber für Grafikchips verwenden

Ubuntu und Linux Mint bieten relativ aktuelle Treiber zur Installation an. Es ist daher nur in Ausnahmefällen erforderlich oder sinnvoll, einen neueren Treiber zu installieren, etwa für die Unterstützung eines sehr neuen Grafikchips. Aufgrund der zahlreichen Abhängigkeiten zum Xserver und anderen Programmbibliotheken kann die Installation eines Herstellertreibers leicht fehlschlagen und ist daher nur erfahrenen Linux-Nutzern zu empfehlen.

Für Nvidia-Chips rufen Sie *www.nvidia.de* auf und gehen auf „Treiber → Gforce-Treiber“. Wählen Sie das gewünschte Modell und hinter „Betriebssystem“ den Eintrag „Linux 64-Bit“. Klicken Sie auf „Suchen“ und dann auf „Unterstützte“. Vergewissern Sie sich, dass Ihre Grafikkarte in der Liste zu finden ist, und merken Sie sich die Versionsnummer. Gehen Sie dann zur Seite *https://launchpad.net/~graphics-drivers/+archive/ubuntu/ppa*. Hinter „Published in:“ wählen Sie die Ubuntu-Version, beispielsweise „Focal“ für Ubuntu 20.04/Linux Mint 20 oder „Bionic“ für Ubuntu 18.04/Linux Mint 19. Klicken Sie auf „Filter“ und prüfen Sie, ob die neueste Version der bei *www.nvidia.de* ermittelten entspricht.

Fügen Sie im Terminal das PPA hinzu:

```
sudo add-apt-repository
 ppa:graphics-drivers/ppa
sudo apt update
sudo apt upgrade
```

Ein Nvidia-Treiber mit der passenden Hauptversionsnummer wird damit aktualisiert. War ein älterer Treiber installiert, gehen Sie vor wie oben in Punkt 3 beschrieben, und installieren die neuste Version.

Über *https://www.nvidia.de/Download/Find.aspx?lang=de* finden Sie auch noch neuere Treiber, wenn Sie unter „Aktuelle“ den Eintrag „Beta“ wählen. Nvidia bietet einen Installer zum Download an. Klicken Sie auf „Weitere Infos“, um Informationen zum Treiber zu erhalten. Folgen Sie dem Link „See the README for more detailed instructions.“ für eine ausführliche Installationsanleitung.

Treiber von AMD nutzen: AMD bietet ebenfalls aktualisierte Treiber für Linux an. Auch hier lohnt sich die Installation nur, wenn die Hardware nicht standardmäßig unterstützt wird. Gehen Sie auf *https://www.amd.com/de/support* und wählen Sie die Grafikkarte in der Liste aus.

Nach einem Klick auf „Absenden“ gehen Sie auf „Ubuntu x86 64-Bit“ und laden „Radeon Software for Linux“ für Ubuntu 20.04 oder 18.04 herunter.

Eine Anleitung zur Installation finden Sie unter *https://amdgpu-install.readthedocs.io/en/latest*.

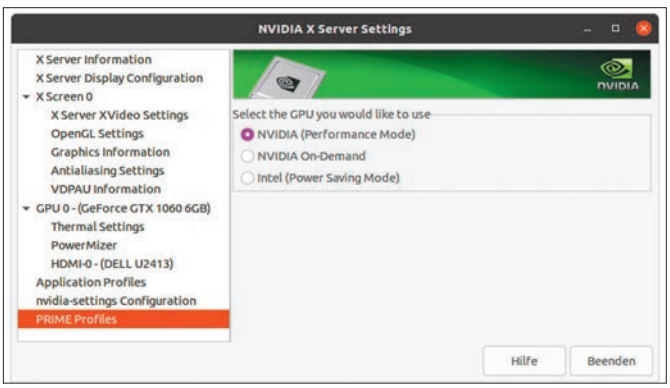
5. Energiesparen durch Treiberwechsel

In vielen Notebooks stecken zwei Grafikchips. Die CPU-Grafik bietet weniger Leistung, dafür hält der Akku länger. Der zusätzliche Grafikchip verbessert die Darstellung von Spielen oder grafikintensiven Anwendungen, nimmt aber auch mehr Leistung auf. Wenn die Open-Source-Treiber für die Grafikchips installiert sind, kommt standardmäßig die CPU-Grafik zum Einsatz, solange ein Programm nichts anderes fordert. Um einem Programm mehr Grafikleistung zuzuweisen, starten Sie es so:

```
DRI_PRIME=1 [Programmname]
```

Es verwendet dann den leistungsstärkeren Grafikchip von AMD oder Nvidia.

Ist der proprietäre Nvidia-Treiber installiert, kann man zwischen Nvidia- und CPU-Grafik umschalten. Linux Mint zeigt dafür ein Applet, über dessen Menü Sie den gewünschten Modus wählen. Ubuntu-Nutzer suchen über „Aktivitäten“ nach Nvidia, starten „Nvidia X Server Settings“ und gehen auf „PRIME Profiles“. Standardmäßig ist „Nvidia (Performance Mode)“ eingestellt. Wählen Sie „Intel (Power Saving Mode)“, wenn die Leistung nicht erforderlich ist. Die Option „Nvidia On-Demand“ – im Linux-Mint-Applet mit „Wechseln zu Nvidia auf Abruf“ bezeichnet – aktiviert ebenfalls die Intel-GPU. Anwendungen oder Spiele können dann bei Bedarf den Nvidia-Chip nutzen. Damit die Änderung wirksam wird, müssen Sie sich mindestens ab- und wieder anmelden.



GPU wählen: Über „Nvidia X Server Settings“ lässt sich wählen, welcher Grafikchip als Standard gelten soll. Der Intel-Chip bietet weniger Leistung, verlängert aber die Akkulaufzeit.

6. Feintuning für AMD-Grafikkarten

Das grafische Tool „Radeon-Profile“ dient zum Feintuning der AMD-Grafikchips über die Open-Source-Treiber unter Linux. Es unterstützt über den Treiber „radeon“ ältere AMD-Chips mit einer Handvoll Tuningoptionen.

Deutlich mehr Einstellungen gibt es, wenn der Treiber „amdgpu“ zum Einsatz kommt. Damit kann man beispielsweise manuell die Lüfterdrehzahl einstellen. Installieren Sie Radeon-Profile über ein PPA:

```
sudo add-apt-repository
 ppa:radeon-profile/stable
sudo apt update
sudo apt install radeon-profile
```

Zum Starten des Tools mit

```
sudo -H radeon-profile
```

sind root-Rechte erforderlich:

Tool für AMD-Grafikchips: Radeon-Profile zeigt Leistungsdaten sowie die Temperatur an und erlaubt auf vielen Karten die Anpassung der Energieprofile und der Lüfterdrehzahl.

7. Videos mit GPU-Unterstützung konvertieren

Schwächere Prozessoren sind mit der Darstellung hochauflösender Videos überfordert. Mediaplayer, Videoeditoren und Webbrowser nutzen daher – sofern vorhanden – die Hardwarebeschleunigung des Grafikprozessors. Die Programme erkennen, was der Grafikchip bietet, und passen die Einstellungen automatisch an. Die GPU lässt sich auch zum Encodieren von Videos nutzen, also für die Umwandlung in andere Formate. Im Vergleich zu einem Codec, der nur die CPU verwendet, ist die Geschwindigkeit etwa um den Faktor vier bis fünf höher. Allerdings leidet meist die Qualität etwas, weshalb viele Programme die GPU-Fähigkeiten nicht automatisch nutzen.

Wem es jedoch auf Geschwindigkeit ankommt, der kann beispielsweise den Videokonverter Handbrake verwenden. Sehen Sie zuerst unter *https://handbrake.fr/docs/en/1.3.0/technical/system-requirements.html* nach, ob die GPU in Kombination mit dem verwendeten Treiber unterstützt wird. Folgen Sie den Links im Abschnitt „Hardware encoders“.

Um die aktuellste Version zu erhalten, installieren Sie das Flatpak-Paket.

```
sudo apt install flatpak
flatpak --user install https://
 flathub.org/repo/appstream/fr.
 handbrake.ghb.flatpakref
```

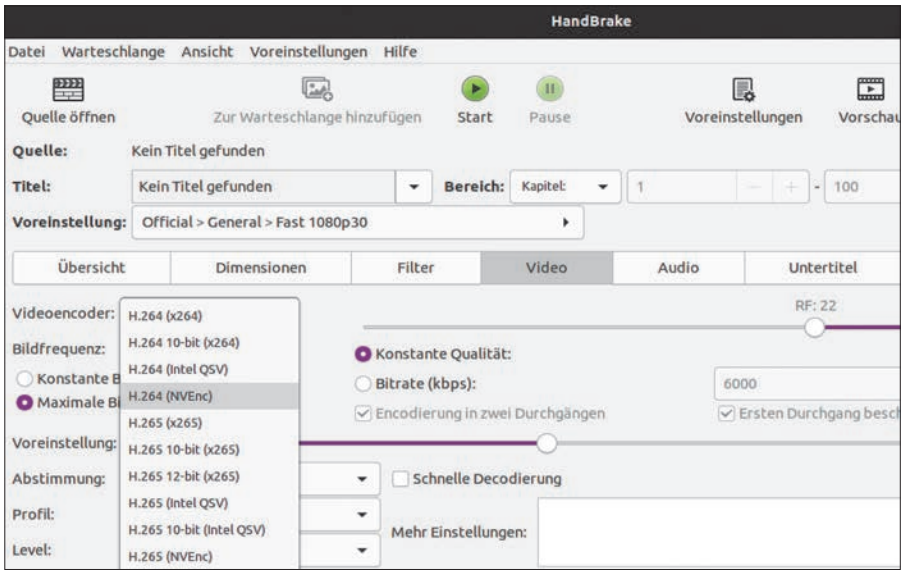
Nutzer von Linux Mint 20 können den ersten Befehl weglassen, weil dort Flatpak standardmäßig vorhanden ist. Wer die Intel-GPU (ab Intel Skylake, sechste Generation mit Intel HD Grafik oder besser) verwenden möchte, klickt zusätzlich unter *https://handbrake.fr/downloads.php* auf „QuickSync Plugin Download (64bit)“. Die Installation erfolgt mit

```
flatpak --user install Plugin.
 HandBrake.IntelMediaSDK-
 1.3.3-x86_64.flatpak
```

Anschließend starten Sie das Programm mittels

```
flatpak run fr.handbrake.ghb
```

Nach einem Klick auf „Open Source“ wählen Sie die Videodatei aus, die Sie konvertieren wollen. Klicken Sie auf „Video“ und stellen Sie hinter „Video Encoder“ beispielsweise „H.264 (NVEnc)“ (Nvidia), „H.264 (Intel QSV)“ (Intel-GPU) oder „H.264 (AMD VCE)“ (AMD-GPU) ein. Handbrake zeigt die Optionen nur an, wenn diese von Hardware und Treiber unterstützt werden. Prüfen Sie die anderen Einstellungen und klicken Sie abschließend auf „Start“. Bei einem Nvidia-Chip können Sie über „Nvidia X Server Settings“ (siehe Punkt 5) unter „GPU-0“ beobachten, wie die Auslastung hinter „Video Engine Utilization“ während der Verarbeitung steigt. ■



Videos umwandeln: Der Videokonverter Handbrake kann die Hardwarebeschleunigung des Grafikchips verwenden, was die Verarbeitung deutlich beschleunigt.

USB-Geräte: Drucker und Scanner

An PCs und Notebooks lassen sich etliche Geräte anschließen. Fast alles läuft unter Linux ohne spezielle Konfiguration oder besondere Software – von wenigen Ausnahmen abgesehen.

Schneller Anschluss: Aktuelle Notebooks besitzen meist Typ-C-Buchsen für USB 4.0/Thunderbolt 4. Daran lässt sich ein Monitor oder USB-Hub für weitere USB-Geräte und Monitore verbinden.

VON THORSTEN EGGELING

Was nicht in den Rechner passt, lässt sich extern anschließen. Dafür findet – abgesehen von HDMI und Displayport für Monitore – fast nur noch der Universal Serial Bus (USB) Verwendung, der seinem Namen inzwischen alle Ehre macht. Ursprünglich fast nur für Maus und Tastatur geeignet, kann USB heute Drucker, Scanner, Festplatten und Monitore. Daneben gibt es mit Thunderbolt 3 und 4 weitere Standards für ähnliche Aufgaben.

Beim Neukauf sollte man genau auf die Logos am Gerät oder auf der Verpackung achten und in den technischen Spezifikationen nachlesen. Was man tatsächlich benötigt, hängt von gewünschten Einsatzzweck ab. Drucker und Scanner geben sich mit USB 2.0 zufrieden. Für schnelle externe Festplatten oder mehrere Monitore sollte man auf aktuelle Hardwarestandards achten.

Unklarheiten bei den USB-Bezeichnungen

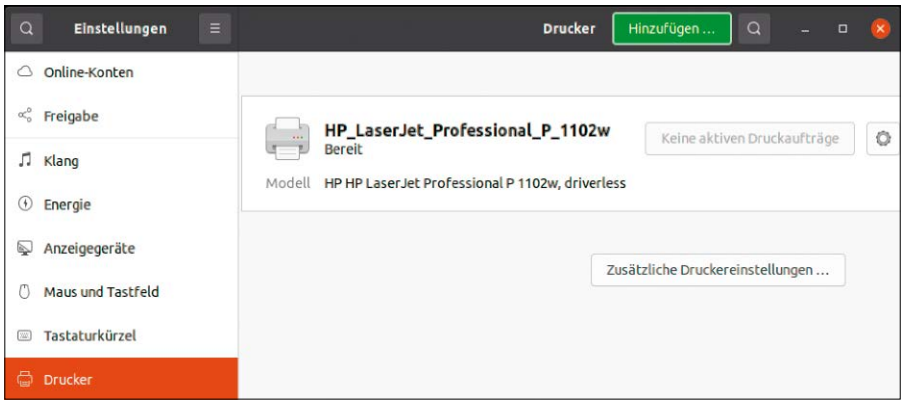
Aktuelle PCs und Notebooks sind fast immer mit einer USB-Buchse vom Typ C ausgestattet. Buchse und Stecker vom Typ C sagen alleine sagen jedoch nichts über die unterstützten USB-Standards aus. Es kann sich um relativ langsames USB 3.2 Gen 1×1 mit fünf GBit/s (vorherige Bezeichnung: USB 3.1 Gen 1 oder USB 3.0) oder um USB 4 (20/40 GBit/s) handeln. Ein Thunderbolt-3-Anschluss ist ebenfalls möglich, der auch USB 3.2 Gen 2×1 bietet. Sehr neue Geräte können auch mit Thunderbolt 4 ausgestattet sein, was USB 4 mit 40 GBit/s einschließt. Bei allen Geräten sollte das USB-Logo auf der Verpackung, an der Buchse oder auf dem Stecker über den genauen Typ Auskunft geben, was jedoch nicht immer gewährleistet ist. Thunderbolt-Buchsen sind mit einem kleinen Blitz gekennzeichnet, manchmal auch mit dem Zusatz „20“ oder „40“ (GBit/s).

Dazu kommen Logos, die über die Stromversorgung mit Hilfe der Typ-C-Buchse Auskunft geben. Meist ist es ein kleines Batteriesymbol oder die Zusätze „Charger“ oder „Fast Charger“. Teilweise ist auch die mögliche Leistung in Watt angegeben. Interessant ist das vor allem für Dockingstationen oder Monitore, die über ein Typ-C-Kabel das Notebook mit Strom versorgen können. Man benötigt dann nur ein Kabel für

USB-STANDARDS UND -LOGOS IM ÜBERBLICK

Version	USB 2.0	USB 3.2 Gen 1x1	USB 3.2 Gen 2x1	USB 3.2 Gen 2x2	USB 4 20 Gbps	USB 4 40 Gbps
Früher bekannt als	–	USB 3.0/3.1 Gen 1	USB 3.1 Gen 2	–	–	–
Geschwindigkeit	480 MBit/s	5 GBit/s	10 GBit/s	20 GBit/s	20 GBit/s	40 GBit/s
Schnittstellen	Typ A/B, Mini/Micro-USB	Typ A/C, Micro-USB	Typ A/C, Micro-USB	nur Typ C	nur Typ C	nur Typ C
Paket-Logo						
Port-Logo						

USB statt HDMI: Monitore mit USB-Hub erhalten über ein Typ-C-Kabel Bildsignale, ferner können sie Notebooks mit Strom versorgen und es lassen sich USB-3.0-Geräte anschließen.



Druckereinrichtung: Sobald Sie in den Einstellungen auf „Drucker“ gehen, erkennt Ubuntu das Gerät automatisch. Das funktioniert auch mit Netzwerkdruckern, deren Netzzugang konfiguriert ist.

die Verbindung zum Notebook und die anderen Geräte inklusive Monitor hängen an der Dockingstation. Voraussetzung dafür ist, dass das Notebook sich auch über USB laden lässt. Sie erkennen das an Angaben wie „Power Delivery DC-In“ in der Dokumentation zum Gerät.

Monitore per USB anschließen

Monitore werden in der Regel über ein HDMI- oder Displayport-Kabel mit Signalen versorgt. Neuere Geräte haben auch eine USB-Typ-C-Buchse, die den eingebauten USB-Hub versorgt und Bildsignale zum Monitor leitet. Die Typ-C-Buchse am Rechner muss jedoch die erforderlichen Signale liefern, was im Gerätehandbuch an Angaben wie „DisplayPort Alt Mode“ oder „Video über USB Type C“ zu erkennen ist.

Mit welcher Auflösung und mit wie vielen Monitoren das funktioniert, ist auch bis USB 4 nicht genau festgelegt. Erst ab Thunderbolt 4 schreibt der Standard zwingend vor, dass man mindestens zwei 4K-Monitore gleichzeitig oder alternativ einen 8K-Monitor ansteuern kann. Das kann jedoch nur funktionieren, wenn eine Grafikeinheit in die CPU integriert ist. Andernfalls muss ein Displayport-Eingang vorhanden sein, der extern per Kabel mit dem Ausgang der Grafikkarte verbunden wird. Darüber lässt sich dann allerdings nur ein zusätzlicher Monitor ansteuern.

Sollte der Monitor am USB-Anschluss unter Linux kein Bild zeigen, obwohl die Hardware dazu in der Lage wäre, fehlt wahrscheinlich ein Treiber. Die nötige Software lässt sich für Ubuntu 20.04 und Linux Mint 20 über *https://m6u.de/DPGRA* herunterladen. Auf der Downloadseite ist ein Link zur Installationsanleitung zu finden. Benutzer anderer Distributionen finden den Quellcode unter *https://github.com/DisplayLink/evdi*.

Für schnelleres USB aufrüsten

Für den PC gibt es Steckkarten, mit denen sich USB 3.2 Gen 2×2 nachrüsten lässt. Dafür ist ein Steckplatz mit mindestens PCIe-3.0-×4 erforderlich. Verfügbar sind zur Zeit Karten von Orico (PE20-1C, *https://m6u.de/PE20*) für 45 Euro und von Icy Box (IB-PCI1901-C32, *https://m6u.de/IBPCI*) für 35 Euro. Auf beiden Karten ist der Chip Asmedia ASM3242 zu finden, der vom Linux-Kernel direkt unterstützt wird.

Die schnelleren USB-Ports lassen sich nur mit einer dazu passenden externen Festplatte ausnutzen – beispielsweise für USB 3.2 Gen 2×2 die Western Digital WD-Black P50 Game Drive SSD 1 TB für knapp 200 Euro oder die Seagate Firecuda Gaming SSD 1 TB für etwa 220 Euro. Beide Laufwerke erreichen knapp 2000 MB/s beim sequenziellen Lesen und Schreiben. Externe SSDs mit USB 3.2 Gen 2×1 sind zahlreicher und kosten etwa 60 Euro weniger. Die Geschwindigkeit liegt hier bei knapp 1000 MB/s. Die Steckkarten unterstützen nur den Datentransfer! Ein Monitor lässt sich nicht anschließen und man kann auch nicht von einem damit verbundenen Laufwerk booten.

Drucker und Scanner

Bei den weit verbreiteten Geräten von Markenherstellern stehen die Chancen gut, dass sich ein Drucker, Scanner oder Multifunktionsgerät unter Linux ohne Aufwand in Betrieb nehmen lässt.

Bei Ubuntu 20.04 gehen Sie in den Einstellungen auf „Drucker“, Nutzer von Linux Mint gehen im Menü auf „Systemverwaltung → Drucker“. Schalten Sie den Drucker ein. Ubuntu erkennt das Gerät automatisch und richtet die passende Software ein. Wenn nicht, klicken Sie auf „Hinzufügen“ und wählen den Drucker aus. Bei Linux Mint richten Sie den Drucker in jedem Fall über „Hinzufügen“ ein. Das funktioniert auch mit Netzwerkdruckern. Die Ersteinrichtung der Netzwerkkonfiguration muss aber unter Windows erfolgen, sofern sich die Einstellungen nicht am Drucker selbst vornehmen lassen. Bei Scannern und Multifunktionsgeräten mit Scaneinheit genügt es, das Programm Dokument-Scanner (simple-scan) zu starten. Es sucht automatisch nach Scannern.

Zusätzliche Treiber sind in der Regel nicht erforderlich. Einige Hersteller bieten jedoch Treiber an, die zum Teil zusätzliche Funktionen unterstützen. Suchen Sie im Supportbereich danach, beispielsweise für Geräte von Brother (*https://m6u.de/BROPR*), Canon (*https://m6u.de/CNPR*), Epson (*https://m6u.de/EPPR*), HP (*https://m6u.de/HPPR*), Lexmark (*https://m6u.de/LEXM*) oder Samsung (*https://m6u.de/SSPR*). ■

Platinenrechner und Mini-PCs

Platinenrechner und Mini-PCs sind preiswert, stromsparend und meist lautlos. Damit eignen sie sich ausgezeichnet für den Server-Dauerbetrieb. Bevorzugte Rollen sind die als Samba-Datenserver, Intranet-Webserver oder Mediencenter im heimischen Netz.

VON HERMANN APFELBÖCK

Dieser Beitrag bespricht mit Ein-Platinen-Rechnern, Mini-PCs, Barebones und NAS mehrere Geräteklassen, in denen Hunderte von Produkten konkurrieren. Es ist ausgeschlossen, einen umfassenden Marktüberblick mit Stärken und Schwächen einzelner Geräte zu leisten. Was wir hier leisten können, ist lediglich eine strategische Abgrenzung dieser Geräteklassen mit einigen Einzelempfehlungen. Da vor allem Mini-PCs und Ausbau-Barebones gewaltig skalieren hinsichtlich Leistung, Ausstattung und Preis, ziehen wir den Kreis noch enger: Hier soll es nicht um leistungsstarke Desktop- oder gar Gamingrechner gehen (die es in Form von Mini-PCs auch gibt), sondern ausschließlich um preisgünstige Hardware im Leistungs- und Preissegment von Platinenrechnern, die sich für einen Servereinsatz im Heimnetz anbieten.

Mini-PCs und Barebones

Mini-PCs und Barebones sind gegenüber Ein-Platinen-Computern eine veredelte Form, die vor allem Nicht-Bastler anspricht. Intels NUCs („Next Unit of Computing“) sind die bekanntesten Vertreter solcher Mini-PCs und Barebone-Kits. Eine brauchbare Übersicht über diese extrem fragmentierte Geräteklasse bietet Intel auf *www.pcwelt.de/nucpc*. Im preisgünstigen Segment kommen aber auch noch Acer Chromebox, CSL Narrow Box, Gigabyte Brix sowie günstigere Zotac-Zboxen in Frage. Diese Geräte sind nicht speziell für Linux ausgelegt, können aber auf ihrer x86-Plattform jedes beliebige System aufnehmen – Linux wie Windows. Soll Linux installiert werden, gilt die generelle Regel, dass etwas ältere Geräte mit Standardkomponenten von Intel ganz neuer Hardware und Exoten aus Fernost vorzuziehen sind.

Mini-PCs sind zusammenfassend nur grob äußerlich so zu charakterisieren, dass es sich um kompakte x86-Rechner im schicken Gehäuse mit typischen Abmessungen wie etwa 12 × 12 × 5 Zentimeter handelt. Solche Mini-PCs werden in der Regel aktiv gekühlt, aber mit großem Lüfter über das komplette Gehäuse und mit niedrigen Drehzahlen (daher leise). Die enthaltene Hardware ist sehr variabel, was sich in so unterschiedlichen Preisen von 200 bis 1500 Euro niederschlägt. Prinzipiell sind Mini-PCs vom kleinen Heimserver bis zum Gaming-PC zu skalieren.

Den Unterschied zwischen Mini-PCs und Barebones oder „Kits“ erkennen Sie in der Regel (aber nicht eindeutig) schon am Preis: Im Prinzip handelt es sich um dieselben Geräte, einmal aber vollständig bestückt und startklar inklusive System („Mini-PCs“, meist mit Windows), im anderen Fall nur mit Mainboard und CPU („Barebone“, „Kit“). Mindestens Arbeitsspeicher und Datenträger müssen beim Barebone/Kit also ergänzt (mindestens zusätzliche 100 bis 150 Euro) und eingebaut, ferner das gewünschte Betriebssystem installiert werden. Günstiger als ein kompletter Mini-PC ist der eigene Ausbau eines Barebone-Kits in der Regel nicht, aber für Linux-Nutzer entfällt immerhin die Lizenzgebühr für Windows und der Kunde hat freie Wahl bei RAM und Laufwerk.

Für den Servereinsatz genügt als CPU theoretisch ein Intel Atom/Celeron oder AMD A9-9600. Besser ist die nächsthöhere Leistungsklasse mit Intel i3 oder AMD-A12. Beim Speicher genügen für einen Daten- wie Medienserver vier GB RAM.

Quelle: minipc.de

Intel NUC: Diese Mini-PCs sind skalierbar vom kleinen Datenserver bis zum Gaming-PC. Die Intel-Hardware ermöglicht die Installation beliebiger Betriebssysteme.

Leiser Mini-PC:
Die Zotac Zbox CI329 Nano kommt ohne Lüfter aus und arbeitet lautlos. Die Wärmeabfuhr erfolgt über das Gehäuse.

Reichlich Schnittstellen: Bei Mini-PCs (hier ein älteres Zotac-Modell) gehören USB, HDMI, Displayport und Ethernet meist zum Standard.

Ein konkretes Beispiel: Das ältere Intel NUC 8i3BEH (also ein NUC der achten Generation mit i3-CPU) ist aktuell für 330 Euro erhältlich, plus RAM und SSD liegt der Endpreis dann je nach Anspruch etwas oder auch deutlich über 400 Euro. Dafür erhalten Sie keinen Sprinter, zumal neben der durchschnittlichen CPU auch noch SATA II (SATA 300) verbaut ist. Für einen Daten- oder Medienserver ist dies aber ausreichend. Aufgrund der Standard-Intel-Hardware ist die Installation eines beliebigen Linux oder einer Kodi-Distribution wie Libre Elec problemlos. Für die Medienwiedergabe ist ein HDMI-Ausgang vorhanden.

Wer auf lautlose passive Kühlung Wert legt, findet ebenfalls Kandidaten: Die Zotac Zbox CI329 Nano wird für knapp 300 Euro als Barebone angeboten, muss also noch durch RAM, SSD und Betriebssystem ergänzt werden. Auch hier ist also insgesamt mit 400 Euro zu rechnen. HDMI und Displayport 1.2 befähigen das Gerät zur Rolle als Mediencenter und mit insgesamt vier USB-3.0- und zwei Gigabit-Anschlüssen eignet sich das Gerät auch als Dateiserver.

Mini-PCs versus Platinenrechner

Was ist nun „besser" – ein Mini-PC oder ein Platinenrechner?

Schnittstellen: Im Vergleich mit Platinen bieten Mini-PCs mehr, je nach Preis auch deutlich mehr Schnittstellen. Die für einen Serverbetrieb wesentlichen I/O-Schnittstellen SATA II oder III, USB-3.x und Gigabit-Ethernet sind immer anzutreffen. Zum Anschluss an Monitore oder TV-Geräte ist mindestens HDMI, oft zusätzlich Displayport, DVI oder VGA vorhanden. Die Geschwindigkeit liegt bei USB-3.0, SATA und Ethernet in etwa auf dem Niveau beliebiger anderer PCs mit ähnlicher Hardware.

Betriebssystem: Aufgrund der x86-Architektur gibt es bei Mini-PCs keinerlei Einschränkungen. Das ist ein klarer Vorteil gegenüber ARM-basierten Platinenrechnern, wo die Auswahl an tauglichen Betriebssystemen oft eng begrenzt bleibt und die Systeme zum Teil Qualität und Nachhaltigkeit vermissen lassen.

CPU/GPU und RAM: Die im Vergleich zu Ein-Platinen-Rechnern höhere Leistung prädestiniert Mini-PCs als direkte Zuspieler an TV-Geräte via HDMI etwa mit Kodi-Mediencenter. Dank Hardwarebeschleunigung durch die GPU gewährleisten auch die preisgünstigen Intel-CPUs der N-, G- oder J-Serie die ruckelfreie Wiedergabe von HD-Videos. Das funktioniert auch mit 4K-Videos, beispielsweise 3840 × 2160 Pixeln (HEVC, H.265), an einem 4K-Monitor. Unter Linux lassen sich jedoch keine Ultra-HD-Videostreams etwa von Netflix abspielen. Hier ist maximal 1920 × 768 möglich.

Optik und Ausbauflexibilität: Mini-PCs sind aufgeräumter und schicker als die typischen Plastikgehäuse von Platinen. Das hat aber auch Nachteile: In Mini-PCs lässt sich nur eine 2,5-Zoll-Festplatte oder SSD einbauen (SATA II oder III), was die interne Speicherkapazität beschränkt. Diesen Nachteil können aber die wenigsten Platinenrechner zu ihren Gunsten nutzen, da größtenteils SATA fehlt. Ausnahmen sind der nicht mehr erhältliche Odroid H2+ sowie Banana Pi Pro mit echtem SATA III. Manche Platinen wie einige Cubieboards bieten zwar SATA-Anschlüsse, verwenden dafür aber einen langsamen SATA-USB-Adapter.

Das Fazit ist klar: Mini-PCs der Einsteigerklasse ab 300 bis 400 Euro sind den allermeisten Ein-Platinen-Rechnern eindeutig überlegen. Punkten können Raspberry & Co. allenfalls mit geringerem Stromverbrauch (etwa die Hälfte) und natürlich dem wesentlich niedrigeren Preis. Ein echter Killer von NUC & Co. und Verkaufsschlager im unteren Preissegment war lediglich der Barebone-ähnliche Odroid H2+. Den musste der Hersteller Hardkernel jedoch Mitte November 2021 einstellen, weil Intel die Produktion des dort genutzten Celeron-CPU J4105 stoppte.

NAS-Heimserver (Network Attached Storage)

Neben Ein-Platinen-Rechnern und Mini-PCs gibt es mit NAS-Geräten (Network Attached Storage) eine wichtige Geräteklasse im Umfeld von Heimservern. NAS für dem Heimbereich sind mehr oder weniger attraktive Gehäuse mit Festplatteneinschüben. Als Betriebssystem läuft fast immer ein angepasstes Linux, das „headless" über eine Weboberfläche bedient wird. Manche Geräte bringen zusätzlich ein kleines Display für Basisfunktionen mit. NAS-Hardware ist aber grundsätzlich auf den Servereinsatz spezialisiert und verzichtet auf Peripherieanschlüsse für Monitor oder Eingabegeräte.

Bekannte Hersteller sind Synology, QNAP, Western Digital, Buffalo, D-Link, Asustor. Typische Home-NAS-Server nehmen ein,

Quelle: qnap.com

Hübsche NAS-Box (QNAP-TS-451) statt Platinenlösung mit Kabelsalat: Der höhere Preis ist gerechtfertigt, wenn der Nutzer Bedienkomfort, Optik und unkomplizierte Administration schätzt.

Quelle: amazon.de

NAS-Geräte sind pure Server: Die Rückseite dieses Synology-NAS bietet zwei Ethernet-Anschlüsse, ferner USB und eSata. Ausgabeports wie HDMI gibt es nicht.

zwei oder vier Festplatten auf und kosten zwischen 100 und 500 Euro. Bei diesen Preisen sind keine Festplatten inbegriffen. Beim Kauf eines NAS-Geräts sollten Sie nicht nur auf die Anzahl der Festplatten-„Bays" achten, sondern auch auf die Maximalkapazität pro Festplatte.

NAS-Server versus Platinenrechner

Was ist denn nun „besser" – ein kommerzielles NAS oder eine Bastellösung mit Raspberry & Co?

I/O-Leistung: Bei einem aktuellen NAS muss man sich um den Datendurchsatz keine Gedanken machen, weil stets SATA (600) für die Festplatten kombiniert ist mit einem Netzwerktransport via Gigabit-Ethernet (zum Teil 2,5-Gigabit-Ethernet). Ab Mittelklasse und etwa 300 Euro bieten NAS-Geräte zwei Gigabit-Ports.

Komfort und Optik: Ein NAS ist eine aufgeräumte Einheit. Wer statt eines NAS mit zwei oder vier Schächten einen Platinenrechner nutzt, muss mit erheblichen Kabelsalat rechnen. Angesichts beschränkter Anschlussports ist oft noch zusätzlicher Aufwand durch Hubs oder Dockingstations erforderlich und mithin auch erhöhter Stromverbrauch.

Betriebssystem: Auf NAS-Geräten ist alles vorinstalliert und auf die Hardware abgestimmt. Damit entfallen Suche und Einrichtung eines passenden Systems. Anspruchsvollere Aufgaben wie Raid, Internet-Portfreigaben, UPnP-Medienstreaming, Benutzerverwaltung sind in der Konfigurationsoberfläche vorgegeben und einfacher zu realisieren als bei einem Platinensystem. Insbesondere Synology-Geräte verdanken ihre Popularität nicht zuletzt dem exzellenten DSM-Betriebssystem (Disk Station Manager).

CPU und RAM: Die Leistung von Platinenrechnern wie dem Raspberry Pi 4 erreichen Home-NAS-Geräte erst ab Preisen von 400 Euro aufwärts.

Flexibilität: Das Betriebssystem auf Home-NAS-Geräten ist meist ein Embedded Linux, das sich durch Apps und Add-ons erweitern lässt, aber im Prinzip geschlossen ist. Definitionsgemäß bleibt ein NAS auch hardwaretechnisch auf die Serverrolle beschränkt (kein Displayausgang) und ist nicht als direkter Zuspieler für TV oder Monitor einsetzbar. Platinenserver sind flexibler, ob nun als nur SSH-administrierter Datenserver, als Webserver, UPnP-Server oder TV-Zuspieler mit Kodi-Mediencenter. Zudem ist das komplette System auf SD-Karte jederzeit austauschbar.

Stromverbrauch und Kühlung: Platinen arbeiten fast alle lüfterlos und somit lautlos, während NAS-Geräte in der Regel einen (leisen) Lüfter besitzen. Platinenrechner verbrauchen außerdem deutlich weniger Strom als NAS-Geräte. Allerdings sind Serverlösungen mit Platinen und mehreren Datenträgern meistens auf externe Stromversorgung der Festplatten angewiesen.

Vor- und Nachteile halten sich die Waage. Raspberry & Co. sind deutlich preisgünstiger, lautlos, theoretisch stromsparender, flexibler und bei der Rechnerleistung einem NAS im unteren Preissegment überlegen. Hinsichtlich Komfort, Bedienung und Aufgeräumtheit können Platinenlösungen aber nicht annähernd mithalten und sind auch beim Datendurchsatz tendenziell unterlegen.

Platinenrechner: Zum Teil überschätzt

Der Raspberry-Hype seit 2012 hat auf Herstellerseite viele Nachahmer, auf Nutzerseite viele Projekte mit oft überzogenen Ansprüchen ausgelöst. Inzwischen ist realistische Ernüchterung eingekehrt. Etliche Platinen konnten hardwaretechnisch von vornherein nicht überzeugen. Für einen NAS-ähnlichen Serverbetrieb kommt nur USB 3.x oder SATA in Kombination mit Gigabit-Ethernet in Betracht. Gigabit-Ethernet ist zwar inzwischen auf vielen Platinen zu finden, jedoch bleiben die erreichbaren Geschwindigkeiten meist unter jenen, die ein NAS oder Desktop-PC erreicht. Beim älteren Raspberry Pi Modell 3+ ist der Ethernet-Port intern über USB 2.0 angebunden und kommt daher nur auf etwa 220 MBit/s. Beim Banana Pro und Odroid XU4 sind es gut 460 MBit/s.

SATA und USB 3.0 bringen ebenfalls nicht überall den erwarteten Durchsatz: So bieten Cubieboards zwar SATA-Anschlüsse, die aber über USB 2.0 laufen und entsprechend enttäuschen. An USB 3.x angeschlossene Datenträger teilen sich bei den meisten Platinen die Schnittstellenleistung, sodass mit zwei oder mehr USB-Festplatten kaum mehr als 600 MBit/s zu erreichen sind.

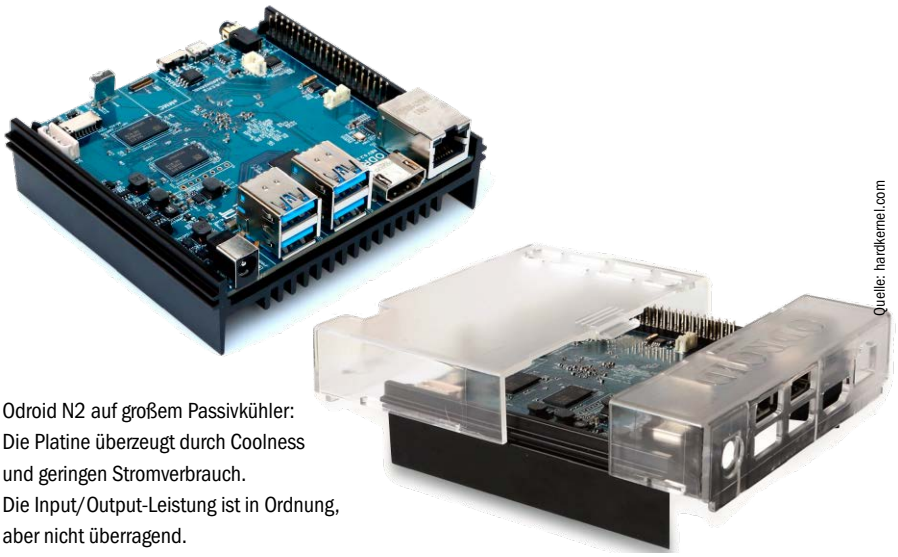
Eine weitere Schwäche sind mangelnde oder mangelhafte Betriebssysteme. Die hardwaretechnisch ansprechenden Banana-Platinen haben mit dem inzwischen eingestellten Bananian ein besonders unrühmliches Negativbeispiel.

Für Odroid-Platinen ist die Auswahl ebenfalls nicht üppig (*https://wiki.odroid.com*), aber ein halbwegs aktuelles System sollte zu finden sein. Große Ausnahme und Vorbild ist das Raspberry-Pi-OS (*www.raspberrypi.org*), das nachhaltig und abwärtskompatibel weiterentwickelt wird. Diese Tatsache ist entscheidender als manche Hardwarespezifikation.

Die generelle Leistung von Platinenrechnern ist mit der von Smartphones oder Tablets vergleichbar, weil hier ähnliche Hardware zum Einsatz kommt. Die ARM-CPUs takten zwischen ein bis zwei GHz und als Arbeitsspeicher sind ein bis acht GB RAM verbaut. Die Leistungsaufnahme von Platinen-PCs liegt im Leerlauf um die zwei bis drei Watt, bei Volllast je nach Gerät zwischen vier und acht Watt. Für die Videowiedergabe ist die Grafikeinheit der

Platinen-PCs wichtiger als die CPU. Da die schwachen CPUs beim Decodieren von HD-Videos an ihre Grenzen geraten, muss die GPU diese Aufgabe übernehmen. Das Problem dabei: Unter Linux lässt sich die Hardwarebeschleunigung in der Regel nicht standardmäßig nutzen, weil die nötigen Treiber aus lizenzrechtlichen Gründen fehlen. Ungeachtet mancher nominell leistungsstärkerer Platinen ist als Videoabspieler der Raspberry Pi 4 mit dem Broadcom-Chip BCM2711B0 der beste Kandidat, weil der Chiphersteller Broadcom die Software für die Hardwarebeschleunigung zur Verfügung stellt.

Im Hinblick auf Serverfunktionalität schrumpft der Zoo der Platinenrechner dann schnell zusammen: Verbleibende Kandidaten sind unter anderen der Raspberry Pi 4, Odroid XU4, Odroid N2, Banana Pi M2 Berry (alle unter 100 Euro). Die wahrscheinlich interessanteste Alternative zu NAS und Mini-PCs, der Odroid H2+, ist hingegen leider Geschichte. Restposten der gefragten Hardware dürften nur noch schwer zu finden sein.



Quelle: hardkernel.com

Odroid N2 auf großem Passivkühler: Die Platine überzeugt durch Coolness und geringen Stromverbrauch. Die Input/Output-Leistung ist in Ordnung, aber nicht überragend.

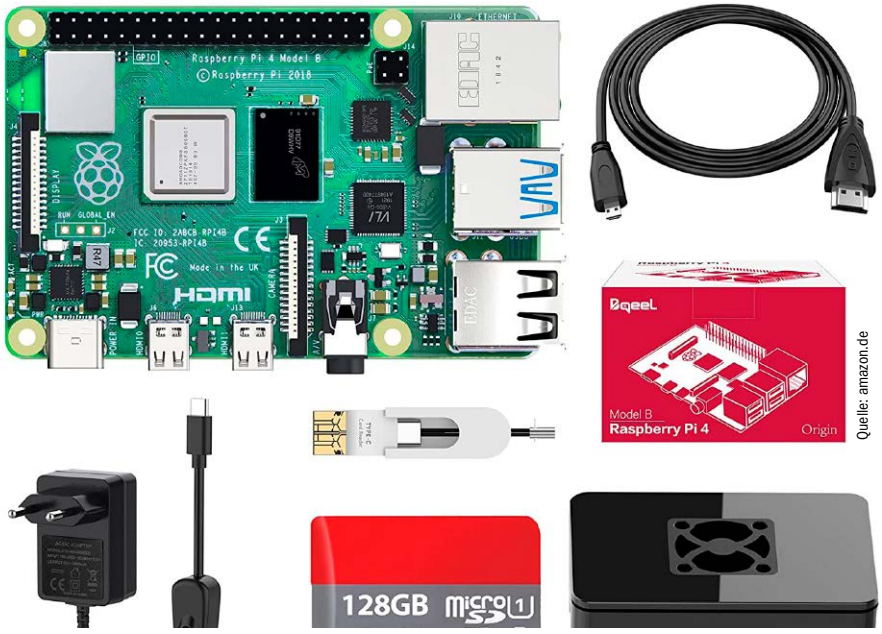
Raspberry Pi 4: Der Universelle

Der Raspberry Pi 4 ist keine originelle, aber eine grundsolide Empfehlung für kleine Heimserver. Das aktuelle Modell 4 hat bis zu acht GB RAM (vier GB sollten genügen), die CPU läuft mit 1500 MHz. Mit zwei USB-3.0-Ports, Gigabit-Ethernet sowie WLAN- und Bluetooth-Chip erfüllt der Modell 4 erstmals die fundamentalen Server-Durchsatzpflichten. Im Bestfall erreicht die Platine im Netz knapp 100 MB pro Sekunde, in der Regel liegt der Durchsatz bei ordentlichen 55 bis 60 MB pro Sekunde. Für Serveraufgaben ist verkabeltes Gigabit-Ethernet alternativlos, aber auch die Leistung des WLAN-Chips (802.11ac) ist alltagstauglich und erreicht bis zu zehn MB/s beim Versenden von Daten, beim Empfang bis zu sechs MB/s. Das ist mehr als genug zum Abspielen von Filmen auf Tablets.

Der Preis für die pure Platine liegt bei knapp 60 Euro. Damit ist die Hardware aber nicht betriebsbereit.

Folgendes Zubehör ist unentbehrlich oder zu empfehlen:

- Das notwendige Netzteil kostet knapp zehn Euro (Netzteile älterer Pi-Modelle passen nicht).
- Für das Betriebssystem ist eine Micro-SD-Karte mit mindestens acht GB erforderlich. Wer die Leistung des neuen Raspberry nicht durch den Flaschenhals einer Billigkarte verschenken will, sollte eine schnelle Karte ab 32 GB mit dem Zusatz „SDXC“ oder „UHS“ wählen. Der Preis kann je nach Kapazität den der Raspberry-Platine erreichen.
- Das schicke Alluminiumgehäuse Flirc für circa 20 Euro dient als passiver Kühlkörper (eine Google-Suche „flirc raspberry“ genügt) und ist eine echte Empfehlung, da der Raspberry Pi 4 erfahrungsgemäß relativ heiß läuft.
- Für HDMI-Monitoranschluss ist ein kleiner Zwischenstecker von Micro-HDMI auf HDMI erforderlich (circa zwei Euro) oder ein Direktkabel vom Micro-HDMI-Anschluss zum Monitor (circa sieben Euro).



Quelle: amazon.de

Platinenklassiker Raspberry Pi 4 mit Zubehör: Solche Bundles sind praktische „Nobrainer“ für Einsteiger, Erfahrene wählen das Zubehör besser gezielt.

Einsteiger greifen am einfachsten zu einem Raspberry-Bundle. Die bieten für 120 Euro aufwärts das komplette Zubehör, allerdings keine Auswahl bei SD-Karte oder Kühlgehäuse. ■

Gute Kühllösung: Das Alu-Gehäuse Flirc kühlt den hitzigen Raspberry Pi 4 lautlos.

Festplatten und SSDs unter Linux

Speicherlaufwerke jeder Art arbeiten unter Linux praktisch immer zuverlässig und ohne Auffälligkeiten. Einige Stellschrauben für die Optimierung bietet das System aber dennoch.

VON THORSTEN EGGELING

Festplatten und SSDs sind die wichtigsten Komponenten im Computer, weil sie für die verlässliche Datenspeicherung zuständig sind. Es ist mehr als ärgerlich, wenn eine Festplatte ausfällt und dabei wichtige Dateien verloren gehen. Die mechanischen Laufwerke sind empfindlich gegen Sturz oder Stoß und auch zu hohe Temperaturen können einen Ausfall herbeiführen. SSDs sind deutlich robuster, obwohl auch hier – wie bei allen elektronischen Bauelementen – die Wärmeabfuhr gewährleistet sein muss. Wie es um die Gesundheit eines Laufwerks bestellt ist und ob es die erwartbare Transferrate liefert, kann man unter Linux mit Bordmitteln und zusätzlichen Tools ermitteln.

Laufwerke und Kernel-Treiber

SATA-Controller für den Anschluss von Festplatten und SSDs sind in jedem PC oder Server zu finden. Die nötigen Treiber sind im Linux-Kernel enthalten und sorgen dafür, dass die Laufwerke frühzeitig beim Systemstart angesprochen werden können. Auch relativ neue Adapter für das schnelle USB 3.2 Gen2x2 oder für Thunderbolt bereiten unter Linux keine Probleme. Bei externen USB-Laufwerken sollte die grundsätzliche Inbetriebnahme immer gelingen. Wenn ein USB-Laufwerk sich im Betrieb spontan aushängt oder nicht automatisch erkannt wird, hat das meist andere Gründe: fehlerhafte USB-Ports, qualitativ minderwertige Kabel oder eine unzureichende Stromversorgung. Davon sind dann alle Betriebssysteme betroffen.

Laufwerke und Partitionen verwalten

Einen guten Überblick über die Laufwerke liefert das Tool Gnome-Disks (Paket: „gnome-disk-utility“). Ubuntu-Nutzer finden es mit einer Suche nach „Laufwerke“ über „Aktivitäten“, bei Linux Mint gehen Sie im Menü auf „Zubehör → Laufwerke“. Das Werkzeug kann Partitionen formatieren, löschen und die Größen ändern. Die Optionen erreichen Sie nach Auswahl einer Partition per Klick auf die Schaltfläche mit den Zahnrädern oder Umschalt-F10. Hier gibt es auch den Menüpunkt „Leistungstest für Partitionen“, über den Sie Lese- und Schreibgeschwindigkeit messen.

Weitere interne Festplatten erreichen Sie im Dateimanager unter „Andere Orte“ (Linux Mint: „Gehe zu → Rechner“). Soll eine Partition bereits beim Systemstart eingebunden werden, klicken Sie die gewünschte Partition an und gehen nach Umschalt-F10 auf „Einhängeoptionen bearbeiten“. Schalten Sie „Vorgaben der Benutzersitzung“ aus. Bei Bedarf ändern Sie den Pfad hinter „Einhängepunkt“ beispielsweise auf die Bezeichnung der Partition. Danach können Sie die Partition über die „Play“-Schaltfläche einhängen.

Gnome-Disks zeigt – sofern ein Sensor verfügbar ist – die Temperatur von Laufwerken an und gibt Infos zum Zustand. Wer es genauer wissen will, drückt die Tastenkombination Strg-S und kann dann die SMART-Werte ermitteln (Self-Monitoring, Analysis and Reporting Technology). Hinter „Allgemeine Einschätzung“ sollte „Das Laufwerk ist in Ordnung“ stehen. Andernfalls ist es Zeit, an einen Austausch zu denken. Bei SSDs sehen Sie sich die Zeile „wear-leveling-count“ an. In der Spalte „Normalisiert“ steht bei neuen SSDs der Wert „100“, der sich mit der Zeit reduziert. Bevor er nahe „0“ ist, sollten Sie das Laufwerk ersetzen.

Unbenutzte Laufwerke abschalten

Eine zweite Festplatte, die beispielsweise nur bei Backups zum Einsatz kommt, muss nicht ständig laufen. In Gnome-Disks rufen

Sie mit Strg-E die „Laufwerkseinstellungen“ auf. Aktivieren Sie die Option „Einstellungen für Bereitschaft-Wartezeit anwenden“ und stellen Sie darunter den Zeitraum ein, nach dem das Laufwerk automatisch in den Stand-by-Modus wechseln soll. Zusätzlich kann es auch die Registerkarte „APM“ (Advanced Power Management) geben, auf der Sie alternativ den Regler in Richtung „Energie sparen“ (schnelleres Stand-by) oder „Leistung verbessern“ schieben. Wenn Laufwerke diese Optionen nicht anbieten, sind die Einstellungen nicht verfügbar.

Über Strg-E und „Jetzt in Bereitschaft gehen“ lässt sich die Festplatte sofort abschalten, was in der Regel auch hörbar ist. Beachten Sie, dass zu viele Start/Stop-Zyklen zu vorzeitigem Verschleiß führen. Im Terminal lässt sich mit

```
sudo hdparm -C /dev/sd[x]
```

kontrollieren, ob die Abschaltung tatsächlich erfolgt ist. Bei einer laufenden Festplatte gibt das Tool „active/idle“ aus, „standby“ zeigt den Bereitschaftsmodus.

Sollte der Bereitschaftsmodus nicht funktionieren, hilft das Tool hd-idle weiter. Wie es sich installieren und verwenden lässt, lesen Sie auf der englischsprachigen Webseite *http://hd-idle.sourceforge.net*. hd-idle unterstützt auch USB-Laufwerke.

Tipp: Wer umgekehrt eine ständige Abschaltung von USB-Laufwerken verhindern möchte (um Wartezeiten beim Zugriff zu vermeiden), kann dafür einen Cronjob verwenden. Nach

```
sudo crontab -e
```

fügen Sie folgende Zeile an:

```
*/5 * * * * /bin/touch /dev/sd[x] &>/
 dev/null
```

Im Beispiel erfolgt ein Zugriff alle fünf Minuten. Ersetzen Sie den Platzhalter „[x]“ durch die Bezeichnung des Laufwerks.

Firmwareupdates unter Linux

Für Festplatten und SSDs gibt es Firmwareupdates, die Fehler beheben oder die Leistung verbessern. Die Hersteller stellen meist nur Windows-Tools bereit. Ubuntu 20.04 und Linux Mint 20 bringen ein Tool mit, über das sich die Updates auch unter Linux durchführen lassen. Es sollte standardmäßig installiert sein. Wenn nicht, holen Sie das mit

```
sudo apt install fwupdate
```

nach. Unter Gnome läuft fwupd automatisch im Hintergrund und das Gnome-Software-Center informiert über verfügbare Firmwareaktualisierungen. Wer das kontrollieren möchte, erhält im Terminal mit

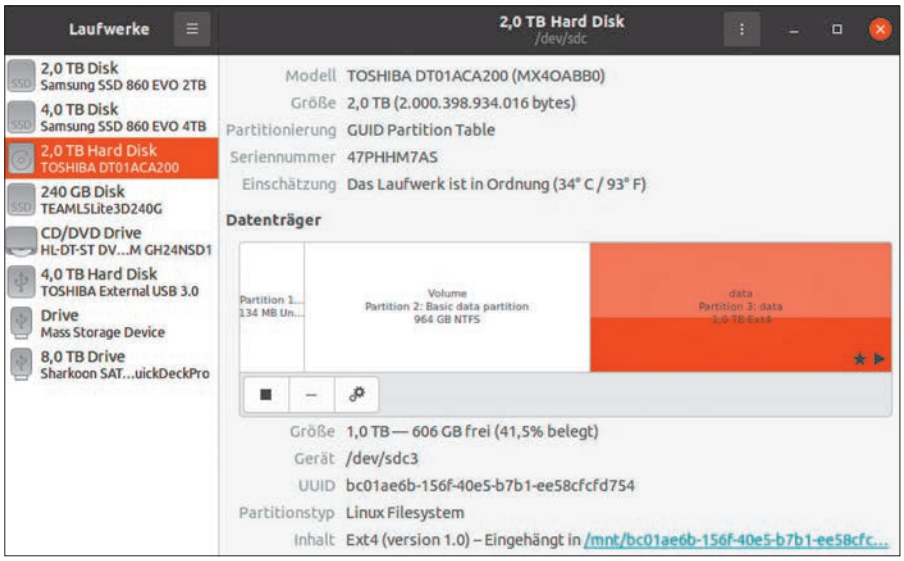
```
sudo fwupdmgr get-devices
```

eine Liste der erkannten Geräte. Die drei Befehlszeilen

```
sudo fwupdmgr refresh
sudo fwupdmgr get-updates
sudo fwupdmgr update
```

bringen die Firmwaredatenbank auf den neuesten Stand, laden Updates herunter – wenn vorhanden – und führen die Installation durch. Bisher steuern noch nicht alle Hersteller zur Firmwaredatenbank bei. Zur Zeit sind vor allem Dell, HP, Lenovo und Logitech vertreten.

Für eine Suche in der Datenbank nach Hersteller und Gerätenamen gehen Sie auf *https://fwupd.org*. ■



Werkzeug für Laufwerke: Das Tool Gnome-Disks bietet die wichtigsten Funktionen rund um Festplatten und SSDs. Sie können Partitionen verändern oder Einhängepunkte festlegen.

Festplatten abschalten: Über Gnome-Disks legen Sie fest, wann ein Laufwerk automatisch in den Stand-by-Modus wechseln soll. Das funktioniert allerdings nicht mit allen Geräten.

SSDS MIT TRIM-BEFEHL OPTIMIEREN

Wenn Sie eine Datei löschen, wird der Platz im Dateisystem als wiederbeschreibbar markiert. Die SSD weiß davon jedoch nichts, daher muss zur Optimierung dem Controller ab und zu eine Liste mit den freien Blöcken übermittelt werden. Das funktioniert jedoch nur, wenn die SSD den Trim-Befehl unterstützt, was Sie mit

```
sudo hdparm -I /dev/sd[x] | grep -i TRIM
```

herausfinden. Die Ausgabe sollte „Data Set Management TRIM supported“ oder ähnlich lauten. Wenn nicht, lässt sich daran nur etwas über ein Firmwareupdate ändern. Andernfalls überlassen Sie Ubuntu oder Linux Mint die automatische Optimierung. Sie können fstrim auch manuell ausführen, etwa um sich von der korrekten Funktion zu überzeugen:

```
sudo fstrim -v -a
```

In der Ausgabe sehen Sie, wie viele Bytes freigegeben wurden. Es sollte sich nur um einen geringen Wert handeln, wenn das Tool periodisch und automatisch vom System ausgeführt wird.

Notebooks für Linux

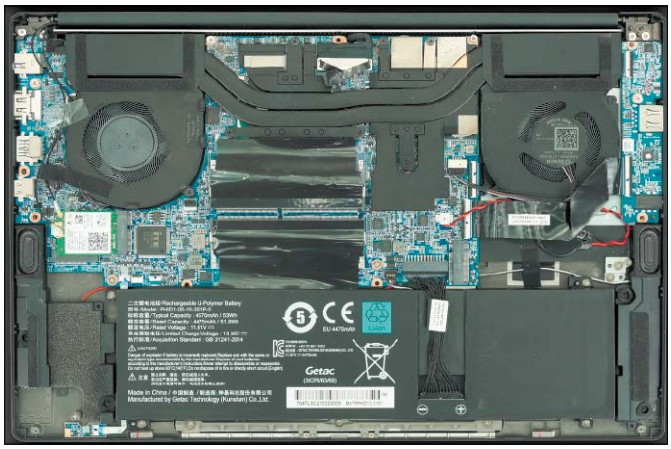
Hardware unterliegt stetem Wandel und Hersteller folgen bei der Treiberentwicklung meist den Vorgaben für Microsoft Windows. Der folgende Leitfaden für 2022 zeigt, worauf Linux-Anwender schon beim Erwerb eines Notebooks achten sollten.

VON DAVID WOLSKI

Transportabel, leistungsfähig, langes Durchhaltevermögen und kompakte Formate: Mit schrumpfenden Platinengrößen sind Notebooks in den letzten drei Jahren dünner und leichter geworden. Dabei haben sich Akkus beständig weiterentwickelt und konnten die Energiedichte erhöhen, während Mobile-CPUs durch eine Fertigung im Zehn-Nanometer- (Intel) beziehungsweise Sieben-Nanometer-Bereich (AMD) energiesparender wurden.

Wer heute ein Notebook der besseren Mittelklasse mit einem Modell von vor drei Jahren vergleicht, wird schon Aufklappen beziehungsweise Anheben enorme Unterschiede in Gewicht und Abmessungen feststellen. Moderne Notebooks haben mehr mit Tablets gemein als mit den einstigen kantigen Mobilrechnern.

Linux-Anwender tun gut daran, bei der Auswahl eines Geräts genau auf Hersteller, Modellgeneration, Hardwarespezifikationen und sogar auf Typenbezeichnungen einzelner Komponenten zu achten. Denn obwohl sich die Unterstützung weit verbreiteter Hardware durch den Linux-Kernel zusehends bessert, läuft Linux nicht gleich auf jedem Notebook optimal. Zu groß sind die Unterschiede bei verbauten Chipsatz-Serien und ihrer Firmware, die für den Massenmarkt mit Windows gemacht sind.



Geöffnetes Notebook von Tuxedo: Sehr flache Notebook-Chassis bringen viel Leistung auf wenig Platz unter. Der Akku ist dabei von außen nicht mehr mit einem Handgriff wechselbar.

CPU: Auf die Frequenz kommt es an

Wie leistungsfähig Notebooks sind, ist hauptsächlich vom Prozessor abhängig und dessen Taktfrequenz. Probleme bei der der Unterstützung durch den Linux-Kernel gibt es kaum, solange eine aktuelle Linux-Distributionen auf neuen Notebooks verwendet wird. Intel und AMD steuern regelmäßig Patches zum Kernel bei, aber es dauert eine Weile, bis die neuen Kernel in Linux-Distributionen vorliegen. Bei einem ganz neuen Notebook, beispielsweise mit Intels Prozessorgeneration Alder Lake oder AMDs Grafikeinheit Yellow Carp, sind Distributionen mit Langzeitsupport und älterem Kernel nicht geeignet. Besser sind bei brandneuer Hardware die regulären Ausgaben oder auch eine vorauseilende Distribution wie Fedora Linux. Stromsparfunktionen und Temperaturkontrolle kommen aber auch für etwas ältere Prozessoren des letzten Jahres hin und wieder erst nachträglich in den Kernel. Hier gilt generell die Regel, je neuer die Linux-Distribution, desto besser. Hersteller von Linux-Notebooks wie Tuxedo und Dell liefern zwar LTS-Versionen von Ubuntu vorinstalliert aus, ergänzen aber die dann nötigen Treiber – Dell sogar selbst mit einem Custom-Kernel.

Tipp: Der Linux-Kernel steuert den CPU-Takt seit Version 3.9 über den „CPU-Governor" und dessen Standardeinstellung „Ondemand", um die Frequenz nach Auslastung dynamisch anzupassen. Auch einem aktuellen Linux-System gelingt es nicht immer optimal, die Prozessorfrequenz passend zu wählen. Eine Hilfe ist das Tool Auto-Cpufreq (*https://github.com/AdnanHodzic/auto-cpufreq*), das die dynamische Taktung des Prozessors nach eigenen Statusabfragen vornimmt und dabei auch den „Turbo-Boost" auf Intel-CPUs beziehungsweise AMDs „Turbo Core" aktivieren kann. Auto-Cpufreq betrachtet dabei auf Laptops, ob das Ladekabel angeschlossen ist oder der Computer mit Akku läuft. Im ersteren Fall aktiviert das Tool den Performance-Modus, andernfalls den Energiespar-Modus des Prozessors.

Das Tool ist noch zu neu, um in den Paketquellen der großen Linux-Distributionen vertreten zu sein. Aber der der Entwickler hat ein Installations-Script auf Github veröffentlicht sowie ein Snap-Paket für Ubuntu, das die Installation vereinfacht. In Ubuntu installiert das Kommando

```
sudo snap install auto-cpufreq
```

das Snap-Paket und der Befehl

```
sudo systemctl enable --now snap.
  auto-cpufreq.service.service
```

setzt den zugehörigen Hintergrunddienst in Gang, welcher die CPU überwacht und die Frequenz anpasst. Die doppelte Endung „.service" ist kein Fehler, sondern ein Merkmal des Snap-Pakets.

Auto-Cpufreq ist auch direkt aus dem Github-Repository installierbar und verlangt dann keine Snap-Runtime. Dazu holt

```
git clone https://github.com/
  AdnanHodzic/auto-cpufreq.git
```

den Quellcode und die Kommandos

```
cd auto-cpufreq
sudo ./auto-cpufreq-installer
```

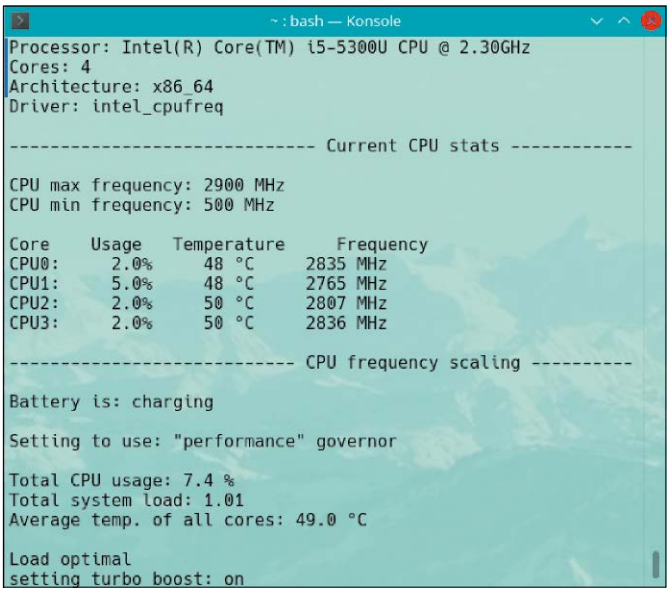
installieren das Tool. Allerdings muss nun noch der Systemd-Dienst mit dem separaten Befehl

```
sudo auto-cpufreq --install
```

aktiviert werden. Damit ist die Einrichtung komplett. Übrigens ist Auto-Cpufreq nicht nur ein unsichtbarer Dienst im Hintergrund, sondern lässt sich mit der Eingabe von

```
auto-cpufreq –stats
```

in die Karten schauen, welcher CPU-Governor aktiv ist und wie es um die aktuelle Temperatur, Auslastung und Frequenz des Prozessors bestellt ist.



Optimale Prozessorleistung bei angeschlossenem Ladekabel: Auto-Cpufreq sorgt dafür, dass die höchste CPU-Leistung über den Modus „Performance Governor" zur Verfügung steht.

Grafikchip: Interne GPU bevorzugt

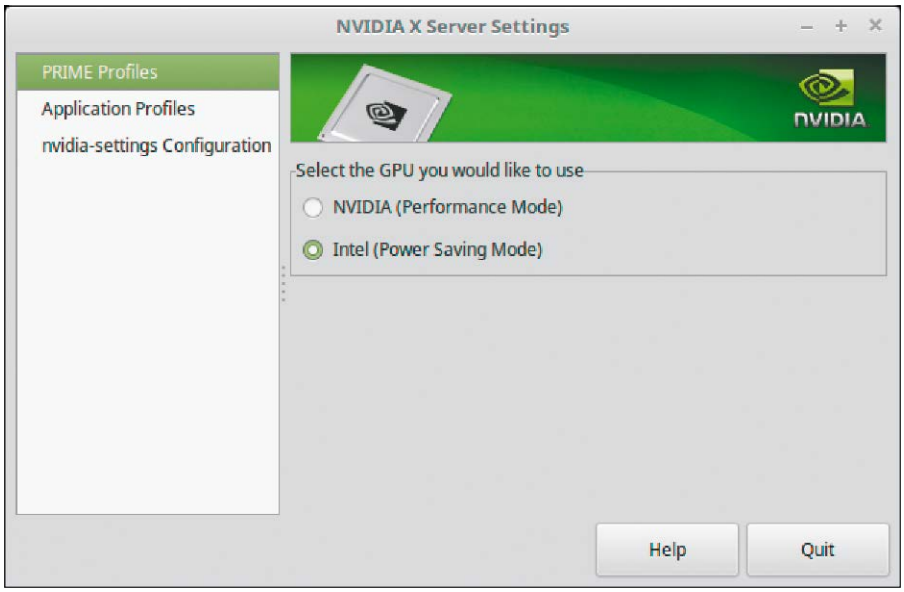
Die Leistung des integrierten Grafikchips in einigermaßen aktuellen Intel- und AMD-Prozessoren der letzten sieben Jahre reicht vollkommen aus für den reibungslosen Betrieb auch aufwendiger Linux-Desktops. Die Open-GL-Treiber von Gnome und KDE, die mit aktivierten Desktopeffekten eifrig Gebrauch der GPU machen, sind effizient und flott. Für Spieletitel mit aufwendiger Grafik reicht die integrierte GPU-Einheit von Intel- und AMD-Prozessoren jedoch bei hohen Auflösungen wie 1080p nicht aus. Teurere Notebookmodelle ab der gehobenen Mittelklasse setzen deshalb auf Hybridlösungen, um spieletauglich zu sein. Bei

GEBRAUCHTMARKT: LEASINGRÜCKLÄUFER UND ALTGERÄTE

Gerade jetzt in Zeiten langer Lieferzeiten und steigender Hardwarepreise durch Euro-Inflation werden viele Anwender vor der Anschaffung eines neuen Geräts zurückschrecken. Linux ist aber im Vorteil, wenn es um Gebrauchtgeräte geht, denn ein älteres Notebook der letzten fünf Jahre ist stark genug auch für KDE Plasma oder Gnome. Gegebenenfalls ist aber mehr RAM (ab vier GB) immer eine gute Idee. Mate, XFCE und LXQT laufen als schlankere Oberflächen auch auf älterer Hardware der letzten sieben Jahre gut.

Generell haftet Gebrauchtgeräten nicht zu Unrecht ein schlechter Ruf an, denn die Akkus sind meistens nur noch Schatten ihrer selbst. Es empfiehlt sich daher, bei Amazon oder Ebay gezielt nach Leasingrückläufern von Händlern zu suchen, die eine gewisse Gewährleistung, ein Widerrufsrecht und eine Rückgabe im gesetzlichen Rahmen einhalten. Alte, zuverlässige Notebooks sind so schon für 180 bis 300 Euro aufzutreiben, wobei Lenovo-Thinkpads, Dell-Geräte und HP Probook gebraucht oft echte Schnäppchen sind, die noch mehrere Jahre gute Arbeit verrichten.

Ein älterer Dell Latitude mit einem i5-Prozessor der dritten Generation: Mit einer nachgerüsteten SSD ist das Gerät von 2014 schnell genug etwa für Xubuntu (Gebrauchtpreis ca. 130 Euro).



Nicht so einfach, wie es hier aussieht: Ein Umschalten von der internen Grafikeinheit zur schnellen GPU, hier über den proprietären Nvidia-Treiber, funktioniert in Linux nicht auf Anhieb.

Anwendungen, die weniger anspruchsvoll sind, kommt nur die sparsame Grafikeinheit des Prozessors zum Einsatz. Nvidia nennt die hybride Grafik „Optimus“ und AMD „PowerXPress“. Die separate GPU muss manuell zugeschaltet werden, was grundsätzlich auch unter Linux funktioniert, aber Nacharbeiten erfordert.

Tipp: In der Praxis funktioniert Nvidia Optimus unter Linux mit der Technik „Prime“ etwas besser mit den proprietären Nvidia-Treibern. Die Situation der Treiber, auch der proprietären Nvidia-Treiber, bleibt aber schwierig und mit der Installation einiger Pakete ist es nicht getan. Bei dieser Notebookhardware bleibt weniger versierten Nutzern meist nur, die Intel-GPU zu deaktivieren und das Gerät nur mit dem energiehungrigen separaten Grafikchip zu betreiben. Damit gibt es dann zwar kein dynamisches Umschalten zwischen zwei GPUs wie unter Windows und folglich kürzere Akkulaufzeiten. Aber immerhin funktioniert dann die schnelle Grafikausgabe mit dem proprietären Treiber.

Akku: Ersatz hilft unterwegs weiter

Notebooks müssen Langläufer sein und aktuelle Geräte zeigen beeindruckende Akkulaufzeiten – zumindest unter Windows, Mac-OS und Chrome-OS. Die meisten Hersteller entwickeln eben für den Massenmarkt, den Windows dominiert. Unter Windows übernehmen nachinstallierte Treiber vom Hardwarehersteller das Zusammenspiel von Geräten und Betriebssystem über die Stromsparfunktionen von ACPI (Advanced Configuration and Power Interface). Unter Linux muss der Kernel diese Aufgabe übernehmen und das nicht immer standardkonforme Verhalten von Windows imitieren.

Tipp: Zahlreiche Feineinstellungen eines Linux-Systems zum Betrieb mit möglichst wenig Energiebedarf fasst das Projekt Linux Advanced Power Management (TLP) zusammen. Die Konfiguration von TLP ist nicht nur im Web in deutscher Sprache dokumentiert (*http://thinkwiki.de/TLP_-_Linux_Stromsparen*), sondern liegt als fertiges, installierbares Paket in allen Linux-Distributionen vor. Die Installation von TLP ist in Debian, Ubuntu und Linux Mint mittels des Kommandos

```
sudo apt-get install tlp
```

schnell erledigt und aktiviert bereits ein grundlegendes Set an Stromsparfunktionen. Auch bei perfekter Konfiguration wird ein Linux-Notebook nicht ganz auf die Laufzeiten eines Windows-Geräts kommen. Mit 20 bis 40 Prozent weniger Laufzeit ist zu rechnen. Bei aktuellen Geräten, etwa dem Tuxedo Infinity Book Pro 14, sind es dann trotzdem noch vier bis sechs Stunden, je nach Systemauslastung. Kommt es auf mehr Laufzeit an, so sollte man sich ein Gerät zulegen, das einen leicht zugänglichen, leicht austauschbaren Akku hat, und einen aufgeladenen Reserveakku mitnehmen.

WLAN: 802.11ac macht Laune

Wer 2022 nach einem neuwertigen Laptop sucht, sollte auf den Standard 802.11ac, auch „Wi-Fi 5“ genannt. Denn Router und Access Points mit dem schnellen Wi-Fi 5 sind jetzt keine Seltenheit mehr. Die effektiv erreichbare Datenrate ist damit signifikant und spürbar höher als mit 802.11n.

Der Linux-Kernel gewinnt in jeder Version neue Treiber für Netzwerkkarten und WLAN-Chipsätze hinzu. Die Zahl der Hersteller der Chips für Notebooks ist überschaubar: Intel, Qualcomm Atheros, Broadcom und Mediatek (Ralink) liefern üblicherweise die Chipsätze.

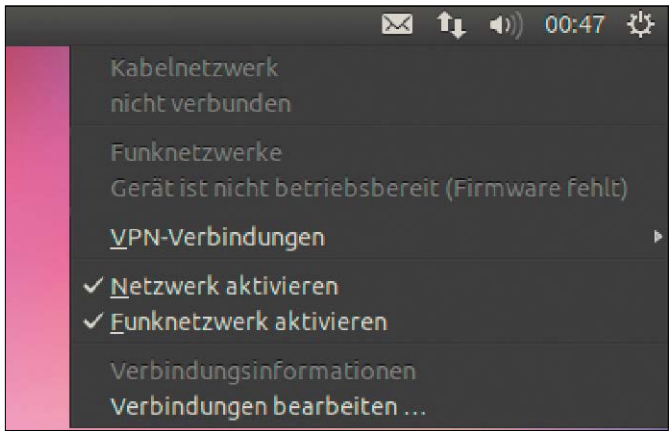
Leider machen es einige wenige Ausreißer nötig, bei der Suche nach geeigneten Notebooks auf die genaue Typenbezeichnung des WLAN-Chips achten und dann im Inter-

Extragroßer Akku für Reisen: Links ein leicht auswechselbarer Austauschakku eines No-Name-Herstellers für ein Thinkpad T450s mit höherer Kapazität als der Originalakku rechts.

WLAN-Modul eines Notebooks: Meist sitzen die WLAN-Karten in einer M.2-Schnittstelle. Ein Austausch ist wegen Kompatibilität mit der Notebookfirmware nur selten sinnvoll.

net gezielt nach der Linux-Unterstützung zu forschen.

Tipp: Die Erfahrung zeigt, dass WLAN-Chipsätze von Intel die wenigsten Probleme bereiten. Meiden sollte man neue Chipsätze von Realtek, denn diese bereiten häufiger Ärger mit Linux. Generell gilt: Je neuer der WLAN-Chip, desto frischer sollte auch die eingesetzte Distribution beziehungsweise der enthaltene Linux-Kernel sein. Bei problematischen WLAN-Chips hilft zur ersten Einrichtung ein Ethernet-Kabel, falls ein Port vorhanden ist, beziehungsweise ein separater WLAN-USB-Dongle mit älterem Chipsatz.



WLAN lahmt: Der Network-Manager meldet, dass proprietäre Firmware fehlt. Diese gibt es in Ubuntu im Standard-Repository „Multiverse“ und wird in der Treiberverwaltung installiert.

Datenträger: NVMEs haben die Nase vorn

Nachdem SSDs und NVMEs als Flash-NAND-Speicher ohne drehende Teile auskommen, ist es keine Frage, dass sie längst zur Pflichtausstattung von Notebooks gehören. Bei der Installation einer Linux-Distributionen aus dem Debian- und Ubuntu-Umfeld, eines Fedora oder einer Arch-Variante wie Manjaro sind zunächst keine Besonderheiten im Zusammenspiel mit SSDs zu beachten – die Systeme treffen die sinnvollen Einstellungen zum Dateisystem selbst. Das Dateisystem Ext4 eignet sich auch für Flashspeicher gut und kann sich auch bei diesen Laufwerken als Quasistandard behaupten. Die beste Leistung liefert mit Abstand NVME, denn es handelt sich um eine PCI-E-Schnittstelle direkt auf der Notebookplatine, die für Multithreading optimiert ist (siehe auch Artikel ab Seite 36).

Tipp: Zum Austausch eines NVME-Speichers ist aber meist die Demontage des gesamten Notebooks nötig, weil diese Speicher platzsparend im Gehäuse untergebracht sind. Einfacher ist der Austausch von SSDs bei älteren Notebooks, etwa bei Geräten von Dell der Precision-Serie oder von LenovoThinkpads: Der SATA-III-Schacht ist hinter einer verschraubten Klappe auf der Unterseite verborgen. Kauft man ein Notebook zum Aufrüsten, so sind Businessmodelle mit diesen Eigenschaften am besten geeignet.

Bei der Formatierung reserviert das Ext4-Dateisystem eine bestimmte Anzahl an Inodes für Systemdateien und privilegierte Systemprozesse. Standardmäßig liegt der reservierte Platz bei fünf Prozent – bei einer 200-GB-NVME sind das also schon wertvolle zehn GB. Bei den heute üblichen Größen von SSDs/NVMEs von über 100 GB lässt sich der Platz gefahrlos verringern. Das gelingt mit dem Tool tune2fs, das viele Parameter von Ext4-Dateisystemen nachträglich ohne Datenverlust anpassen kann: Das Kommando

```
sudo tune2fs -m 1 /dev/nvme0n1p2
```

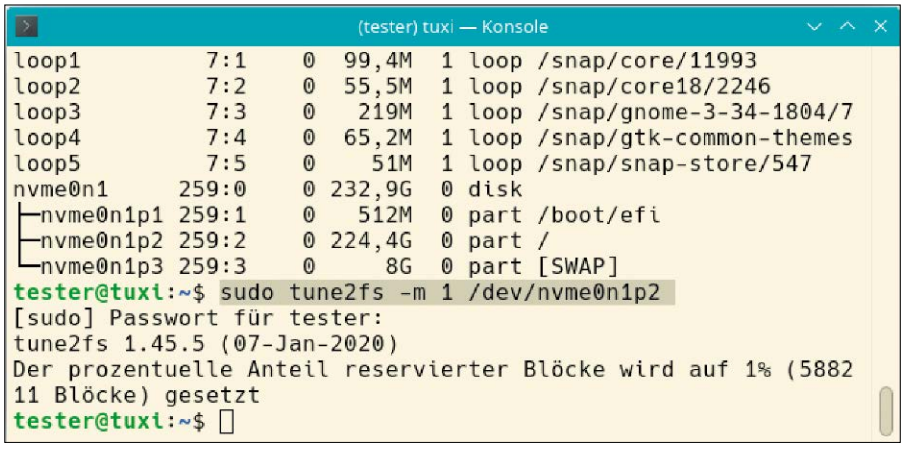
reduziert die Anzahl der reservierten Blöcke auf der Partition „/dev/nvme0n1p2“ auf ein Prozent.

Bildschirm: Hi-DPI und Touchscreens

Notebooks mit Touchscreen sind zwar keine Exoten mehr, aber eine herausragender Erfolg sind berührungsempfindliche Displays bei dieser Geräteklasse nicht geworden. Viele Linux-Anwender ignorieren die Touchbildschirme ihres Notebooks meist und arbeiten konventionell mit Maus und Tastatur. Aus gutem Grund: Finger am Bildschirm sind unpraktisch. Selbst der Gnome-Desktop, der mit seinen großen Menüelementen und Touchgesten noch am ehesten für Touchscreens geeignet ist, bringt wenig Vorteile bei Touchscreens.

Tipp: Bei der Bestellung eines Notebooks vom Händler oder Hersteller ist genau auf die Spezifikationen des Bildschirms zu achten. Denn Hersteller wie Dell liefern einige Modelle wahlweise mit oder ohne Touchscreen, wie beispielsweise das XPS 13.

Ob matt oder glänzend, ist sicherlich Geschmacksfrage. Wichtiger ist für die Lesbarkeit bei Tageslicht die effektive Helligkeit des Bildschirms. Diese geben Hersteller meist in Candela pro Quadratmeter an (cd/m²). In der Regel sollte die Helligkeit bei einem entspiegelten Notebookdisplay bei rund 220 cd/m² liegen, für die Arbeit draußen besser bei 250 cd/m² . Für Innenräume reichen dagegen schon 130 bis 150 cd/m² aus. Mit Linux sind bei den Desktops Gnome, Budgie, KDE Plasma, eingeschränkt auch bei XFCE und Mate, 4K-Bildschirme mit Auflösung bis 3840 × 2160 Pixel nutzbar. Die Hi-DPI-Unterstützung der Desktops skaliert die Elemente der Arbeitsfläche. Java-Programme brauchen aber eigene Parameter. ■



Wertvollen Platz sparen: Bei Ext4 werden fünf Prozent der Blöcke für root für den Notfall reserviert. Das kann das Tool tune2fs gefahrlos auf ein Prozent reduzieren.

Problemlöser für Bluetooth

Der Bluetooth-Kopfhörer bleibt stumm und Bluetooth-Geräte in der Nähe sind unsichtbar? Unter Linux kann man mit Bluetooth sein blaues Wunder erleben, denn die Einrichtung klappt selten reibungslos. Die folgenden Schritte helfen weiter.

VON DAVID WOLSKI

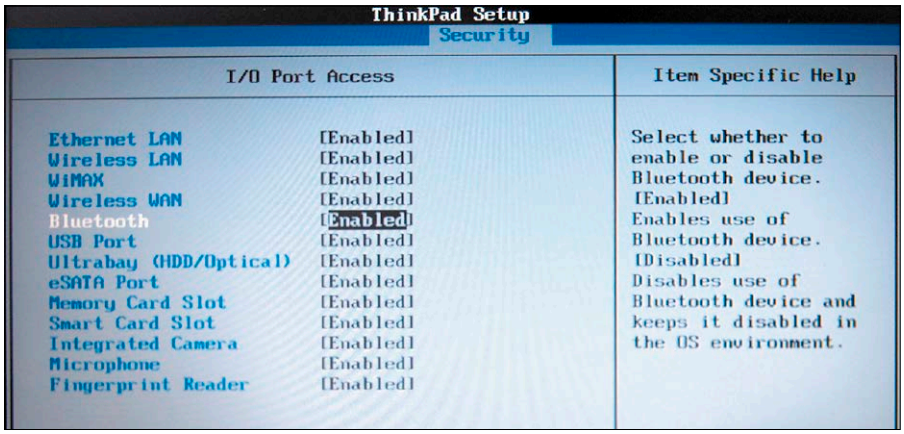
Bluetooth scheint längst etabliert: Schon 1996 stellte der damalige Mobilfunkriese Ericsson das Nahfunk-Protokoll vor, das übrigens nach dem Wikingerkönig Harald Blåtand (910–987) benannt ist.
Der Name „Blåtand" (Blauzahn) ist sogar im offiziellen Bluetooth-Logo festgehalten, das einem altnordischen Runenzeichen ähnelt. Und nach wie vor kann eine Verbindungsaufnahme zwischen Geräten eine raue Angelegenheit sein – wie eine Seereise auf einem Wikingerschiff. Denn ganz problemlos klappt die Verbindung zwischen Bluetooth-Geräten selten: Ungünstige Konstellationen von Treibern, Hardwarespezifikationen und nachlässig programmierter Firmware verhindern oft den einwandfreien Verbindungsaufbau.
Darunter haben übrigens nicht nur Linux-Anwender zu leiden. Auch wenn es unter Linux einige spezielle Bluetooth-Probleme mehr gibt als bei Betriebssystemen, die von Herstellern mit Treibern verwöhnt werden. Immerhin aber finden sich in Linux-Systemen mehrere Analysemethoden und Tools, um Verbindungsproblemen auf den Grund zu gehen. Die folgenden Schritte helfen systematisch dabei, Bluetooth bei einer Reihe von typischen Schwierigkeiten flottzumachen.

Hardware: Kein Bluetooth gefunden

Es klingt trivial, aber hinter vielen Anlaufschwierigkeiten stehen oft Einstellungen im Bios des Rechners, die Bluetooth erst einmal komplett abschalten. Zwar sind Bluetooth- und WLAN-Fähigkeiten auf Hauptplatinen meistens im gleichen Chip untergebracht, aber das Bios kann dennoch beide Funktionen getrennt ein- oder ausschalten.
Lösung: Einen wichtigen Hinweis darauf, ob Bluetooth komplett per Bios-Einstellung abgeschaltet ist, liefern die Kernel-Meldungen eines Linux-Systems, die den Systemstart und damit auch die Hardwareinitialisierung durch das Betriebssystem protokollieren. Mit dem Befehl

```
dmesg | grep -i bluetooth
```

im Terminal zeigt sich, ob Bluetooth vom Kernel überhaupt erkannt wurde. Falls das Kommando gar kein Resultat anzeigt, dann findet der Kernel gar keine Bluetooth-Hardware. Jetzt sollte als erster Schritt ein Besuch im Bios erfolgen, um die Einstellungen zu überprüfen.
Die Einstellung zu Bluetooth findet sich je nach Mainboardhersteller in den Untermenüs „Onboard Device Configuration", „Security → I/O Port Access" oder auch „Config → Network", da Bluetooth und WLAN in Notebooks meist vom Netzwerkchip bedient werden.
Tipp: Nach einem Bios/Uefi-Update kann es sein, dass Bluetooth erst mal komplett ausfällt. Ist dies passiert, dann hilft meistens ein Abschalten und Einschalten dieser



Bluetooth macht blau: Falls die Bluetooth-Funktion per Bios deaktiviert ist, findet sich der Bluetooth-Chip unter Linux schon mal gar nicht. Das ist trivial, aber leicht zu übersehen.

Funktion im Bios, jeweils gefolgt von einem Neustart.

Treiberprobleme: Fehlende Firmware

Ein Sonderfall sind Bluetooth-Chips, die nicht direkt seitens des Linux-Kernels Unterstützung finden, sondern auf zusätzlich geladene Firmware angewiesen sind. Zwar taucht dann das Bluetooth-Modul in den Kernel-Bootmeldungen auf, trotzdem kann das Linux-System Bluetooth nicht in Betrieb nehmen.

Lösung: Bevor Bluetooth funktioniert, benötigt das Linux-System die passende Firmware zum Chipsatz. Das Kommando

```
hciconfig --all
```

zeigt die Kennung der Bluetooth-Schnittstelle an, meist „hci0“, sowie den Hersteller und die Anschlussart. Auf der üblichen PC-Hardware handelt es sich bei der Anschlussart entweder um PCI oder um USB. Je nachdem, was der obige in der ersten Zeile anzeigt, ist dann entweder der Befehl „lsusb“ einschlägig, der alle USB-Geräte anzeigt, oder Sie benötigen das Kommando „lspci“, sofern das Bluetooth-Modul am PCI-Bus hängt.

Beide Kommandos zeigen zwar alle USB- beziehungsweise PCI-Geräte des Systems an, allerdings meist ohne eindeutige Bezeichnung für Bluetooth-Module. Erst der zuvor ermittelte Hersteller macht die Identifikation des Bluetooth-Chips mit Typennummer möglich.

Die Seite *https://wiki.ubuntu.com/HardwareSupportComponentsBluetoothUsbAdapters* ist eine gute Anlaufstelle, um Firmware für problematische Bluetooth-Chips zu finden. Die Anleitungen sind zwar für Ubuntu maßgeschneidert, gelten aber häufig so oder ähnlich auch für andere Distributionen.

Flugmodus: Bluetooth wieder einschalten

Alle Notebooks erlauben es, den Bluetooth- und WLAN-Sender abzuschalten, etwa um das Gerät auch an Bord eines Flugzeugs während Start und Landung zu betreiben. Neben einem Schalter beziehungsweise einer Tastenkombination zum Abschalten der Sender gibt es auch eine Methode, den Bluetooth-Chip einzeln per Software zu deaktivieren.

Lösung: Auf vielen Notebooks kann der Bluetooth-Sender zwar wieder per Hardwareschalter oder mit der vorgesehenen Tastenkombination eingeschaltet werden, bleibt aber trotzdem softwareseitig blockiert. Klarheit darüber, ob und wie ein Bluetooth-Chip blockiert ist, verschafft das nützliche Kommandozeilentool rfkill, das nach der Eingabe des Befehls

```
rfkill list all
```

in einem Terminalfenster den Status aller Sendereinheiten des Computers meldet. Es gibt dabei für jeden Sender zwei Typen von Blockaden: „Soft blocked: yes“ bedeutet, dass der Sender über den Treiber deaktiviert wurde. Das Kommando

```
sudo rfkill unblock all
```

schaltet alle Sender softwareseitig wieder ein. Eine zweite Art von hardwareseitiger Blockade zeigt der Status „Hard blocked: yes“ an. In diesem Fall muss man am Notebook auf einen Schalter oder eine Taste mit Antennensymbol absuchen, um die Sender damit wieder in Betrieb zu nehmen. Viele Hersteller sparen sich auch eine gesonderte Taste dafür und bringen den Antennenschalter als FN-Tastenkombination auf einer der Funktionstasten unter.

Systemdienste: Bluetooth-Status überprüfen

Auch diese Situation ist häufig anzutreffen: Der Bluetooth-Chip ist zwar erkannt und wäre betriebsbereit, trotzdem fehlt im Infobereich der verwendeten Desktopumgebung das Symbol für Bluetooth-Verbindungen. Jeder Versuch, eine Verbindung mit anderen Tools aufzubauen, scheitert mit der Fehlermeldung, dass der Bluetooth-Dämon nicht liefe.

Lösung: Das Problem tritt auf, wenn der Bluetooth-Chip nachträglich nach der Installation eines Linux-Systems aktiviert wurde. Typischerweise auch dann, wenn die Bluetooth-Fähigkeiten durch einen später eingesteckten USB-Dongle zum System kamen.

Im Terminal kontrolliert das Kommando

```
sudo systemctl status bluetooth
```

den Status des Bluetooth-Dämons (Systemdienstes). Zeigt die dritte Zeile nur „Active: inactive (dead)“ an, so läuft der Dienst nicht. Die beiden Kommandos

```
sudo systemctl enable bluetooth
sudo systemctl start bluetooth
```

setzen den Bluetooth-Systemdienst in Gang. Danach ist eine erneute Anmeldung am Desktop ratsam, damit dort das Bluetooth-Symbol für die weiteren Funktionen auftaucht.

Wir können auch anders: Wenn die einfachen Bluetooth-Applets von Gnome oder KDE nicht genügen, so gibt es noch den Bluetooth-Manager (blueman) als fortgeschrittenes Werkzeug.

```
() thunkpad — Konsole
[Bluetooth Audio]# pair 00:02:3C:03:81:E1
Attempting to pair with 00:02:3C:03:81:E1
Failed to pair: org.bluez.Error.ConnectionAttemptFailed
[CHG] Device 00:02:3C:03:81:E1 RSSI: -38
[Bluetooth Audio]# pair 00:02:3C:03:81:E1
Attempting to pair with 00:02:3C:03:81:E1
[CHG] Device 00:02:3C:03:81:E1 Connected: yes
[CHG] Device 00:02:3C:03:81:E1 UUIDs: 00001108-0000-1000-8000-00805f9b34
[CHG] Device 00:02:3C:03:81:E1 UUIDs: 0000110b-0000-1000-8000-00805f9b34
[CHG] Device 00:02:3C:03:81:E1 UUIDs: 0000110c-0000-1000-8000-00805f9b34
[CHG] Device 00:02:3C:03:81:E1 UUIDs: 0000110e-0000-1000-8000-00805f9b34
[CHG] Device 00:02:3C:03:81:E1 UUIDs: 0000111e-0000-1000-8000-00805f9b34
[CHG] Device 00:02:3C:03:81:E1 ServicesResolved: yes
[CHG] Device 00:02:3C:03:81:E1 Paired: yes
Pairing successful
[CHG] Device 00:02:3C:03:81:E1 ServicesResolved: no
[CHG] Device 00:02:3C:03:81:E1 Connected: no
[Bluetooth Audio]# trust 00:02:3C:03:81:E1
[CHG] Device 00:02:3C:03:81:E1 Trusted: yes
Changing 00:02:3C:03:81:E1 trust succeeded
[Bluetooth Audio]# connect 00:02:3C:03:81:E1
Attempting to connect to 00:02:3C:03:81:E1
[CHG] Device 00:02:3C:03:81:E1 Connected: yes
Connection successful
```

Bluetooth-Verbindungen zu Fuß: Schön es ist nicht, Bluetooth manuell in der Kommandozeile mit bluetoothctl herzustellen, aber bei Problemen sind die Meldungen sehr aufschlussreich.

Blueman: Alternative für jeden Desktop

Gnome und KDE Plasma bieten ihre eigenen Bluetooth-Applets auf dem Desktop. Das Applet von Gnome ist dabei äußerst einfach gehalten: Entweder es funktioniert mit den erkannten Geräten oder eben nicht – was leider recht häufig vorkommt.

Lösung: Es gibt eine grafische Alternative, die deutlich mehr Funktionen zur Fehleranalyse hat und unter jedem Linux-Desktop funktioniert. Der Bluetooth-Manager ermöglicht eine genauere Kontrolle darüber, als welche Art von Gerät eine Bluetooth-Peripherie angebunden werden soll. So kann man beispielsweise festlegen, ob ein Headset nur als Kopfhörer oder auch als Eingabegerät dienen soll. Zudem erlaubt es der Bluetooth-Manager, die Suche nach Geräten manuell erneut anzustoßen. Er zeigt die Verbindungsqualität und die aktuelle Datenrate des Bluetooth-Funkmoduls an.

Auf den sparsamen Desktops wie Mate, XFCE, LXDE, und LXQT ist der Bluetooth-Manager meist vorinstalliert. Wer das fortgeschrittene Tool auch unter Gnome und KDE verwenden will, muss es aus den Paketquellen der Linux-Distribution noch nachrüsten. In Debian und Ubuntu genügt dazu folgendes Terminalkommando:

```
sudo apt-get install blueman
```

Der Bluetooth-Manager ist dann sofort einsatzbereit und kollidiert nicht mit den Bluetooth-Applets der Desktopumgebung. Nach dem Start des Tools, etwa mit „blueman-manager“ über den Ausführen-Dialog, zeigt das Hauptprogrammfenster die bereits erkannten Geräte in der Nähe an. Ein Klick auf „Suche“ startet einen erneuten Suchlauf und mit „Einrichten“ beginnt mit der Pairingprozess für ein ausgewähltes Gerät. Das Stern-Symbol steht für die Vertrauenswürdigkeit eines Gerätes. Generell verlangen Eingabegeräte wie Tatstatur und Maus diesen Status.

Fehlersuche: Exkurs in die Kommandozeile

Der Bluetooth-Manager gibt einen guten, hardwarenahen Überblick, welche Geräte sich verbinden können. Scheitert die Verbindungsaufnahme aber, so gibt auch dieses grafische Tool wenig Aufschluss darüber, woran dieses Problem liegen könnte.

Lösung: Bei besonders hartnäckiger Bluetooth-Peripherie kann es immer noch helfen, die Geräte in der Shell mit dem Kom-

BLUETOOTH-VERBINDUNGEN: DER ÜBLICHE WEG

Es muss ja nicht immer etwas schiefgehen – auch mit Bluetooth nicht. Gutmütige Geräte sprechen ohne Klimmzüge über die übliche Konfiguration von Bluetooth-Peripherie miteinander. So funktioniert die Verbindung ganz exemplarisch unter dem Gnome-Desktop:

1. Im aufklappenden Benutzermenü rechts oben findet sich unterhalb des Bluetooth-Symbols der Punkt „Bluetooth-Einstellungen“. Über diesen gelangt man zur Bluetooth-Verwaltung von Gnome.

2. Nach einem recht langen Suchlauf listet Gnome die gefunden Bluetooth-Geräte mit Status auf. Ein Klick darauf startet die Verbindungsaufnahme – das „Pairing“. Wichtig ist in diesem Menü außerdem der leicht zu übersehende Schalter „An/Aus“ rechts oben im Fensterrahmen, der den Bluetooth-Sender ein- und ausschalten kann.

3. Zu Geräten, die kein Pairing verlangen, verbindet sich Gnome im Idealfall ohne weiteres Zutun. Alle anderen Bluetooth-Gegenstellen, die eine Bestätigung verlangen, warten auf die Eingabe der Nummer, die Gnome nun anzeigt.

Gleich ein glückliches Paar: Alle Arten von Eingabegeräten sowie Smartphones und andere Computer verlangen zur Verbindungsaufnahme die Bestätigung per eingegebenem Code.

4. Für jedes verbundene Gerät öffnet Gnome bei einem Klick darauf ein Untermenü mit weiteren Optionen. Hier kann man das Gerät wieder entfernen, temporär abschalten oder die Klangeinstellungen für Lautsprecher, externe Verstärker oder Headsets ändern.

mandozeilentool bluetoothctl zu verbinden, das in jeder Linux-Distribution vorliegt. Auf diesem Weg erhält man zudem auch aussagekräftige Fehlermeldungen, die beispielsweise auf Inkompatibilität zwischen alten und neuen Bluetooth-Klassen hinweisen. Auf einem Raspberry Pi 3 ohne grafische Benutzeroberfläche ist bluetoothctl der übliche Weg, Peripherie per Bluetooth anzusprechen. Die Eingabe von *bluetoothctl* in der Kommandozeile öffnet ein textbasiertes Menüsystem, das wiederum von Befehlen gesteuert wird. Die Eingabe von

```
agent on
discoverable on
pairable on
```

macht zunächst den Bluetooth-Chip für andere Geräte sichtbar. Nun startet der Befehl

```
scan on
```

einen Suchlauf, den man nach einigen Minuten mit

```
scan off
```

wieder anhält. Die gefundenen Geräte zeigt dann die Eingabe von

```
devices
```

mit Name und Adresse an. Diese Adresse wird zur Verbindung benötigt: Mit

```
pair [Adresse]
```

beginnt das Pairing, wobei Eingabegeräte und Smartphones die Eingabe der angezeigten Nummer zur Bestätigung erwarten. Dann vertraut man dem Gerät mit dem Befehl

```
trust [Adresse]
```

und verbindet es schließlich:

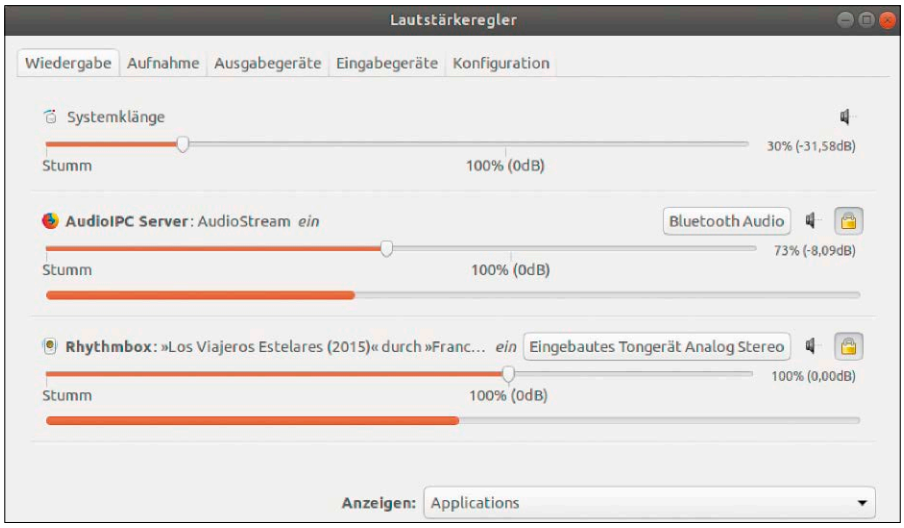
```
connect [Adresse]
```

Jeder einzelne Schritt liefert dabei recht ausführliche Debugginginformationen. Die so verbundenen Geräte bleiben dem System übrigens auch nach einem Neustart bekannt, sofern sie in Reichweite bleiben.

Pulse Audio: Zum richtigen Ausgang

Wenn ein Headset, ein Kopfhörer oder ein externer Lautsprecher per Bluetooth verbunden ist, so bleibt das Gerät meist ohne weitere Konfiguration vorerst stumm.

Der Soundserver Pulse Audio, der in den meisten Linux-Distributionen für die Soundausgabe zuständig ist, muss erst mit den neu hinzugefügten Bluetooth-Ausgabeports bekannt gemacht werden. Auch wenn mehrere Audiogeräte verbunden sind, verlangen diese noch manuell nach einer Aktivierung.



Getrennte Wege: Das Konfigurationstool Pavucontrol zaubert noch einige Tricks mehr aus dem Hut. So kann es verschiedene Soundquellen gezielt an getrennte Ausgabegeräte weitergeben.

Lösung: Auf dem Gnome-Desktop gibt es in den Systemeinstellungen unter „Klang" ein Untermenü, das bei „Ausgabe" und „Eingabe" per Klick ein Umschalten zwischen Audiogeräten erlaubt. Zur Ergänzung weiterer Funktionen und auf anderen Desktops kommt das Pulse-Audio-Tool Pavucontrol in Frage, das in allen Linux-Distributionen zur nachträglichen Installation bereitsteht. In Debian, Ubuntu und seinen Varianten ist diese im Terminal schnell erledigt:

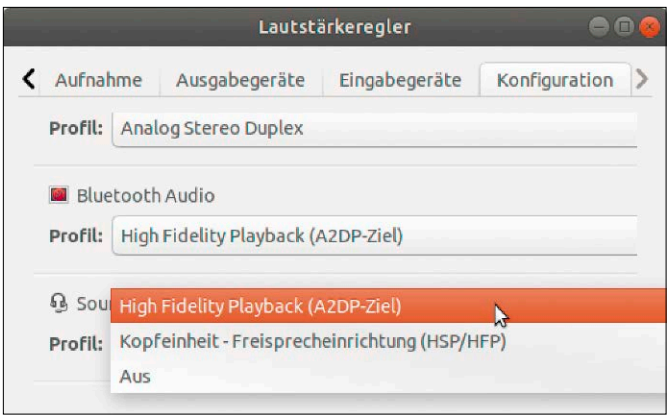
```
sudo apt-get install pavucontrol
```

Nach dem Start zeigt Pavucontrol das Menü „Wiedergabe" an. Hier sind alle aktuell laufenden Anwendungen mit Soundausgabe auf dem System aufgelistet. Für jede dieser Quellen kann ein Klick auf das nebenstehende Auswahlfeld ein Ausgabegerät gezielt ausgewählt werden. Während dann etwa das „Eingebaute Tongerät" Systemklänge und Browsersound wiedergibt, kann ein Audioplayer über ein externes Bluetooth-Gerät abspielen. Eine Liste aller verfügbaren Geräte zeigt Pavucontrol im Untermenü „Ausgabegeräte".

Profile: Bessere Soundqualität

Nach der Verbindung eines Bluetooth-Headsets und dem ersten Soundcheck ist die Enttäuschung oft groß: Die Kopfhörer scheppern wie ein altes Transistorradio und liefern nicht annähernd Hi-Fi-Qualität.

Lösung: Um dies zu ändern, hilft wieder das Konfigurationstool Pavucontrol, das in den meisten Distributionen noch auf seine Installation wartet. Nach dem Aufruf von Pavucontrol über den Ausführen-Dialog oder im Terminalfenster zeigt die Registerkarte „Konfiguration" den Status aller verbundenen Audiogeräte an. Im Feld „Profil" eines Bluetooth-Kopfhörers steht üblicherweise „Aus" oder „Kopfeinheit - Freisprecheinrichtung (HSP/HPF)". Genau das ist der Fehler, denn erst die Auswahl des Profils „High Fidelty Playback" veranlasst das Gerät zur Soundausgabe in Hi-Fi-Qualität. ■

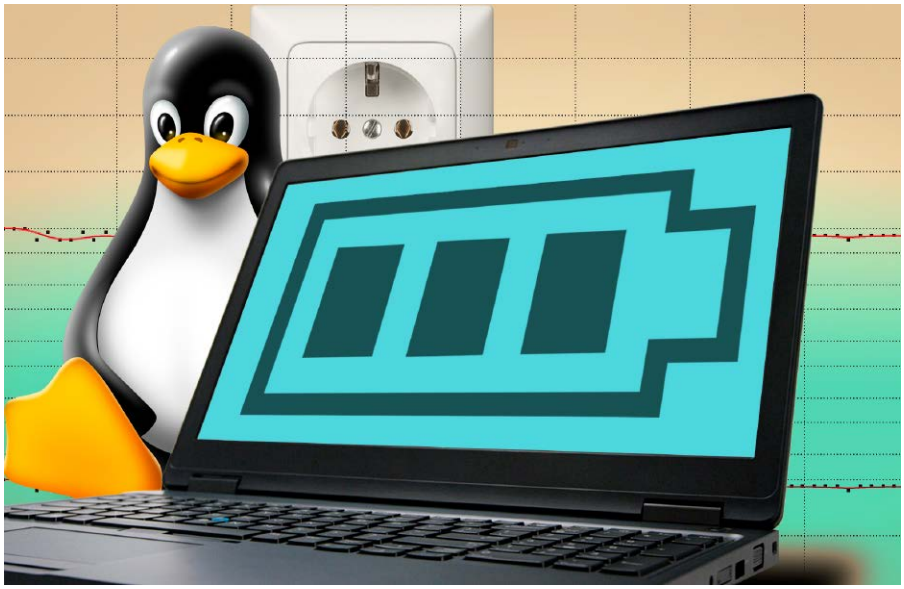


Hi-Fi statt Soundbrei: Linux-Distributionen sprechen Bluetooth-Headsets zunächst nur in Radioqualität an. Das Tool Pavucontrol schaltet die Ausgabe auf „High Fidelity Playback" um.

Tipps zum Stromsparen

Weder Desktop-PCs noch Server noch Router oder Receiver müssen permanent laufen, wenn es eindeutige Zeiten gibt, wo sie keiner nutzt. Abschalten, ACPI-Ruhezustände und Deaktivieren von Komponenten senken die Kosten und schonen die Geräte.

VON HERMANN APFELBÖCK



Als IT-Magazin hat die LinuxWelt Notebooks, PCs, Server, Router, Monitore, Tablets, Smartphones, Datenträger im Fokus. Jede solche Hardware benötigt Strom, und wenn Datenserver oder Router nachts nicht genutzt werden, liegt es nahe, diese für etliche Stunden abzuschalten. Konsequent verfolgt, können akkumulierte Sparmaßnahmen bei der heimischen IT jährlich einen dreistelligen Eurobetrag einsparen.

Darum wird es hier gehen – jedoch sollte man die Relationen klarstellen: Allein mit dem Ersatz einer veralteten Kühl-Gefrier-Kombination durch eine neue mit Effizienzklasse A ist locker dasselbe zu erreichen. Ähnliches gilt für den Verzicht auf TV-Größen von 80 Zoll und mehr. Man bedenke: Ein Display wird umso größer, je näher man sitzt. Vier Meter vor einem 80-Zoll-TV ist das Bild kleiner als mit einem 11- oder 12-Zoll-Tablet in der Hand. Aber schon klar: Das ist ein Spartipp für Singles.

1. Nützliches Hardwarezubehör

Zweckmäßige Steckerleisten, Zeitschaltuhren und Messgeräte für wenige Euro können den Stromverbrauch analysieren und signifikant reduzieren. Überlegen Sie sich den Einsatz folgender Hilfsmittel:

Leistungsmessgerät: Mit einem Messgerät können Sie überprüfen, wie viel Strom ein Gerät verbraucht und ob sich geänderte Einstellungen positiv auswirken. Einfache Messgeräte sind schon ab acht Euro erhältlich und zeigen die Leistungsaufnahme in Watt an. Rechnen müssen Sie dann selbst, denn die Watt-Angaben sind für Verbraucher eher nichtssagend. Was hilft die Info, dass ein Notebook 20 bis 30, ein Büro-PC 50 bis 60, ein 32-Zoll-TV 50, ein Router etwa 10 bis 15 Watt verbraucht? Dieser Wert zeigt den Verbrauch pro Stunde. Den Jahresverbrauch im Dauerbetrieb berechnen Sie dann so:

```
[Watt-Angabe]/1000*24*365*0,30
```

Als Kilowatt-Preis sind hier 30 Cent angenommen. Ein permanent laufender Büro-PC mit 60 Watt schlägt also im Jahr mit 157,68 Euro zu Buche.

Steckerleiste mit Gesamtschalter oder Einzelschalter pro Port: Damit trennen Sie mit einem Knopfdruck alle angeschlossenen Geräte vom Netz oder per Einzelschalter ein ganz bestimmtes. Drucker, TV, Receiver müssen nachts nicht laufen, auch nicht im Standby. Selbst Router müssen nachts nicht durchlaufen – es sei denn, das Telefon-Festnetz hängt etwa per DECT-Funk am Router und ist nachts unentbehrlich. Achtung: PCs und Server müssen vorher sauber heruntergefahren werden!

Steckdosen mit Zeitschaltuhr: Einfache analoge Zeitschaltuhren in Form von Zwischensteckern kosten nur fünf bis zehn Euro, bessere digitale etwa 10 bis 30 Euro. Sinnvoll sind solche Helfer für tendenziell „dumme" Geräte wie Beleuchtung, Drucker, TV oder Router. Bei PCs, Notebooks, NAS-Geräten und sonstigen Servern sind harte Zeitschaltungen meistens zu unflexibel: Denn wenn Sie ausnahmsweise länger als gewohnt arbeiten und die Uhr automatisch den Strom abdreht, ist Datenverlust vorprogrammiert.

Master-Slave-Steckerleiste: Solche Steckerleisten ab etwa 20 Euro schalten automatisch alle Geräte an den Slave-Anschlüssen ab, sobald am Masteranschluss kein Strom mehr fließt. Typischerweise kommt der PC oder auch das TV-Gerät an den Master-Port. Beim Abschalten des Mastergeräts gehen dann auch alle Peripheriegeräte an den Slave-Ports vom Stromnetz (Drucker, Monitor, USB-Platte, Receiver, gegebenenfalls auch Beleuchtung). Bei hochwertigeren Master-Slave-Leisten ab etwa 50 Euro kann die zur Abschaltung führende Spannung mit einem Regler exakt justiert werden. Dies ist etwa dort zweckmäßig, wenn ein ACPI-Ruhezustand wie „Energie sparen"

oder „Ruhezustand“ die Geräte an den Slave-Ports nicht abschalten soll.

Wenn an die Leiste auch Geräte angeschlossen werden, die unabhängig vom Master funktionieren sollen, gibt es bei den meisten – jedoch nicht bei allen – Master-Slave-Leisten unabhängige „Permanent“-Stecker.

IP-Steckerleiste mit Zeitschaltung: Erstaunlicherweise gibt es kaum preiswerte Stromsteckerleisten mit integrierter Zeitschaltuhr für sämtliche Stromanschlüsse oder gar für jeden einzeln. Seltene Ausnahmen gehen dann gleich einen Schritt weiter und integrieren einen Webserver und Ethernet-Port. Somit lassen sich die Ports der Steckerleiste professionell im Browser zeitprogrammieren oder auch manuell schalten. Solche Produkte wie etwa Gembird EG-PMS2-LAN (circa 80 Euro bei *conrad.de*) oder die IP-Steckdosenleiste Allnet ALL4176 (circa 240 Euro bei *reichelt.de*) sind entsprechend hochpreisig und dürften für normale Stromsparansprüche überdimensioniert ausfallen.

Master-Slave-Steckerleiste und Zeitschaltung: Bei einer passenden Konstellation an einer Steckerleiste lassen sich alle angeschlossenen Geräte zeitgesteuert abschalten, ohne dass hierfür eine dumme Zeitschaltuhr oder eine teure IP-Steckerleiste notwendig wäre. Es genügt eine erschwingliche Master-Slave-Steckerleiste mit einem Heimserver am Masterport. Wenn dieser Server (etwa ein Raspberry Pi) täglich abends per Cronjob abgeschaltet wird, gehen auch die restlichen Geräte an den Slave-Ports vom Stromnetz. Wie Sie einen Linux-Server zeitgesteuert abschalten – und im Optimalfall auch automatisch wieder aktivieren – lesen Sie in Punkt 7.

Stromstecker mit Zeitschaltung: Zubehör wie die Funksteckdose Fritz Dect 200 ist eine anspruchsvolle Lösung (40 Euro), einfache mechanische oder digitale Zeitschaltuhren kosten 5 bis 20 Euro.

Quelle: conrad.de / avm.de

Quelle: obi.de

Master-Slave-Steckerleiste: Solche Leisten schalten alle Geräte an den Slave-Dosen ab, sobald das Hauptgerät am farbigen Masterport heruntergefahren wird (typischerweise der PC).

Steckerleiste der absoluten Oberklasse: Diese Allnet All4176 ist ein Ethernet/WLAN-Gerät mit Webserver, der Zeitprogrammierung und manuelle Schaltung für jeden Anschluss ermöglicht.

Quelle: allnet.de

2. Allgemeine Stromspartipps für Hardware

Wenn Sie Kaufentscheidungen energiebewusst treffen wollen, gibt es einige Grundregeln für die Wahl der Hardware.

• Multifunktionsgeräte sind sparsamer als Einzelgeräte: Eine Drucker-Scanner-Kopierer-Fax-Kombi verbraucht deutlich weniger Strom als mehrere Einzelgeräte. Ein gutes Smartphone ersetzt Handy, Digitalkamera und MP3-Player. Abgesehen von Farblaserdruckern liegt aber der Standby-Verbrauch aller dieser Peripheriegeräte unter, meist deutlich unter 5 Watt. Handlungsbedarf besteht nur, wo sich der Verbrauch allzu vieler Geräte aufsummiert.

• Monitore und TVs verbrauchen umso mehr Strom, je größer die Bildfläche ausfällt. Heutige TV-Statussymbole mit über 80 Zoll benötigen bei HDR-Qualität bis zu 300 Watt. Mit den 2021 von der EU neu definierten Effizienzklassen fallen solche Geräte jetzt praktisch alle in das tiefrote G-Label.

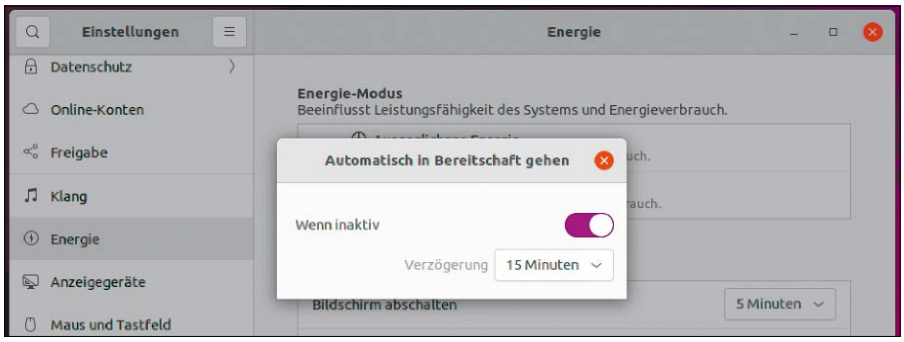
Ein weiterer entscheidender Faktor bei Displays ist die Helligkeit: Am Notebook können Sie bei Inaktivität das Display über die Energieoptionen des Betriebssystems automatisch verdunkeln (siehe Punkt 3). PC-Monitore bieten ebenso wie Smart-TVs detaillierte Optionen zu Helligkeit, Kontrast, Schärfe, die oft ungenutzt bleiben. Ein reduzierter, aber immer noch ausreichend guter Helligkeitswert, kann den Verbrauch dauerhaft um 25 Prozent und mehr senken.

• Röhrenmonitore sind zu Recht am Aussterben: Während ein 24-Zoll-LCD-Monitor mit 15 bis 20 Watt auskommt, verbraucht eine gleich große alte CRT-Röhre schnell das Vierfache. Im Dauerbetrieb amortisiert sich ein neuer Monitor nach kaum zwei Jahren.

• PC-Komponenten: Am sparsamsten arbeitet eine Hauptplatine, die alle wesentlichen Komponenten enthält – Grafikchip, WLAN, LAN, USB, Sound. 2,5-Zoll-Festplatten sind sparsamer als 3,5-Zoll-Platten, Platten mit großer Kapazität sparsamer als mehrere kleine. Beim Netzteil sparen Sie kaum Strom, wenn Sie eines mit geringer Ausgangsleistung wählen. Eine Nennleistung von 600 Watt bedeutet nämlich keineswegs 600 Watt im Mittel, sondern nur den absoluten Spitzenwert.

3. PC & Notebook: Linux-Energieverwaltung

Bei den Stromsparoptionen des Betriebssystems ist es kein Geheimnis, dass Linux ein ganzes Stück hinter den Möglichkeiten bleibt, die Windows in enger Zusammenarbeit mit den Hardwareherstellern bieten kann. Die wirksamsten Funktionen gibt es



Eingebaute Stromsparoptionen: Ubuntu-Systeme können dort sparen, wo es sich am meisten lohnt – beim Bildschirm und beim Time-out für den Bereitschaftsmodus.

Displayverdunkelung nach kurzer Inaktivität: Diese Maßnahme ist neben der „Bereitschaft“ die wirksamste Stromsparoption. Beachten Sie auch analoge „Öko“-Einstellungsoptionen bei PC-Monitoren und Smart-TVs.

aber auch unter Linux. Ubuntu und Linux Mint beschränken sich auf die Stromsparoptionen mit dem größten Einsparpotenzial – die Bildschirmabschaltung und den ACPI-S3-Modus („Bereitschaft“, technisch „Suspend to RAM“). Unter „Systemeinstellungen → Energie“ (oder „Energieverwaltung“) finden Sie den Timer für den Bereitschaftsmodus („Automatisch in Bereitschaft gehen“ oder „Standby-Modus“). Nach der angegebenen Frist geht der Rechner in stromsparende Bereitschaft, sofern in dieser Frist keine Aktivität festgestellt wurde (Maus und Tastatur). Das Verdunkeln und Ausschalten des Bildschirms bei Inaktivität finden Sie an gleicher Stelle.

Auch andere Linux-Oberflächen bieten vergleichbare Zentralen, sehr übersichtlich etwa der Xfce4-Power-Manager für XFCE, der nach der Installation als „Energieverwaltung“ im Startmenü zu finden ist. Das Tool Powerdevil5 für KDE („Systemeinstellungen → Erweitert → Energieverwaltung“) ist mit Abstand das Werkzeug mit den differenziertesten, aber auch kompliziertesten Einstellungsmöglichkeiten.

Im S3-Modus verbrauchen Notebooks und PCs nur noch zwei bis drei Watt die Stunde. Und die Leistungsaufnahme zwischen einem maximal hellen Notebookdisplay und einem maximal abgedunkelten unterscheidet sich um drei bis vier Watt, das sind 25 Prozent bezogen auf den typischen Verbrauch eines Notebooks insgesamt. Der genaue Wert hängt nicht zuletzt von der Größe des Bildschirms ab.

Manuelle „Bereitschaft“: Wenn man gerade vorhat, den Rechner zu verlassen, kann man den Bereitschaftsmodus auch manuell anfordern. Diese Option bietet in Ubuntu das Sitzungsmenü in der Systemleiste („Ausschalten/Abmelden → Bereitschaft“), in Linux Mint verwenden Sie im Hauptmenü das Symbol „Beenden“ und dann „Bereitschaft“.

4. PC & Notebook: Datenträger in Bereitschaft

Auch Festplatten lassen sich bei längerer Nichtbenutzung in den Ruhemodus schicken. Beim Systemlaufwerk ist die Maßnahme kontraproduktiv, hingegen gut geeignet für reine Datenspeicher – auch für externe USB-Festplatten. In den allgemeinen Systemeinstellungen werden Sie diese Option allerdings vermissen, jedoch kann das auf vielen Gnome-affinen Desktops (Gnome, Cinnamon, Budgie) vertretene Gnome-Disks steuern, wann sich Festplatten abschalten sollen. Wählen Sie dort das gewünschte Laufwerk und gehen Sie im Drei-Punkt-Menü auf „Laufwerkseinstellungen“. Unter „Bereitschaft“ setzen Sie den Schalter auf „An“ und stellen die Zeit ein, nach der die Festplatte sich abschalten soll. Die Zeitspanne reicht von „Niemals“ bis „3 Stunden“.

5. PC & Notebook: Powertop-Tuning

Der Energiemonitor Powertop liefert zahlreiche Informationen zum Stromverbrauch der Hardwarekomponenten und hilft aktiv zur optimierten Systemkonfiguration. Das Tool liegt in den Standardquellen aller wichtigen Linux-Distributionen bereit. Nutzer von Ubuntu/Mint installieren Powertop mit

```
sudo apt install powertop
```

und erhalten nach dem Aufruf

```
sudo powertop
```

nach einigen Sekunden das Ergebnis. Sie sehen die Entladungsrate in Watt und den Energiebedarf einzelner Prozesse. Mit Tab-Taste navigieren Sie zur jeweils nächsten Kategorie. Im Register „Einstellbarkeit“ gibt Powertop eine Reihe von Empfehlungen für optimierte Stromsparfunktionen. Temporär aktiviert die Eingabetaste eine einzelne Option. Um alle vorgeschlagenen Stromsparfunktionen zu aktivieren, verwenden Sie besser diesen Befehl:

```
sudo powertop --auto-tune
```

Auch dies gilt nur für die aktuelle Sitzung, kann aber mit einem Cronjob für jeden Systemstart angefordert werden. Nach *sudo crontab -e* tragen Sie den zusätzlichen Job

```
@reboot /usr/sbin/powertop --auto-
  tune
```

als letzte zusätzliche Zeile ein.

6. Router: Abschalten und Funk reduzieren

Wenn komplettes Abschalten des Routers über Nacht organisatorisch möglich ist (und komfortabel etwa per Kippschalter auf der Steckerleiste zugänglich), dann ist dies die einfachste Sparmaßnahme. Sie nehmen dabei lediglich in Kauf, dass der Internetzugang beim morgendlichen Einschalten nicht sofort, sondern erst nach zwei, Minuten funktioniert.

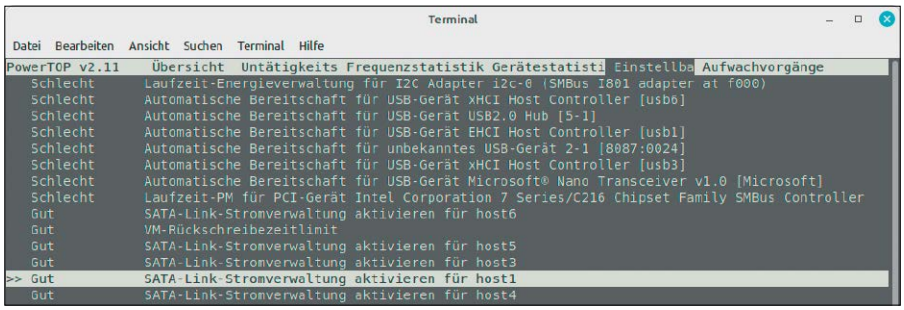
Heimrouter besitzen aber weitere Optionen, um den Stromverbrauch zu reduzieren. Die Konfigurationsoberfläche des Routers erreichen Sie bekanntlich mit jedem Browser und der IP4-Adresse [xxx.xxx.xxx].1, wobei [xxx.xxx.xxx] identisch ist mit der IP, die Ihr PC meldet (zum Beispiel nach „ip adress“).

Die Fritzbox ist alternativ auch mit „fritz.box“ erreichbar. Die Möglichkeiten der Routerkonfiguration sind nicht nur aus ökologischen Gründen zu empfehlen, sondern fast mehr noch, um das Multifunktionsgerät vor Dauerstress und Überhitzung zu bewahren.

Eine Zeitschaltung für das Funknetz bietet jeder Router, die Fritzbox unter „WLAN → Zeitschaltung“. Aktivieren Sie dort das entsprechende Kästchen „Zeitschaltung“, das darunter hingegen nicht: Wenn der Router in einem Haushalt mit mehreren Mobilgeräten tolerant auf die Abmeldung des letzten warten muss, kann dies die Abschaltung verzögern, selbst wenn alle Smartphones und Tablets nicht mehr aktiv genutzt werden. Darunter geben Sie dann einfach die zwei Uhrzeiten an, zwischen denen Sie kein Funknetz benötigen. Es gibt auch eine zweite Option mit einem komplexen Wochenplan; der wäre aber nur sinnvoll, wenn Sie an verschiedenen Wochentagen stark divergierende Nutzungszeiten haben.

Router, die als Basisstation für DECT-Telefone arbeiten, können das DECT-Signal optional verringern. Nach unserer Erfahrung ist das schwächere Signal für durchschnittliche Wohnungsgrößen völlig ausreichend. In der Fritzbox finden Sie die Einstellungen unter „Telefonie → DECT → DECT-Funkleistung verringern“. Die zusätzliche Option „DECT Eco“ ist ebenfalls zu empfehlen, wenn das genutzte DECT-Telefon dabei mitspielt.

Ein reduziertes DECT-Signal spart Strom und kühlt den Router auch deutlich um etliche Grad.



Powertop: Das Tool zeigt den aktuellen Energiebedarf und bietet im Register „Einstellbarkeit“ Feineinstellungen, die Sie einzeln schalten können oder per „auto-tune“ allesamt.

7. Server: Automatisches Abschalten

Daten- oder Webserver müssen nachts nicht durchlaufen, in der Regel nicht einmal in Firmen – zu Hause schon gar nicht. Es ist eine ganz einfache Übung, einen Linux-Server täglich zur bestimmten Zeit sauber zu beenden. Dazu genügt eine Zeile in der Crontab des root-Kontos. Nach *sudo crontab -e* tragen Sie dort folgende Zeile ein:

```
0 23 * * * /sbin/shutdown now
```

Der Abschaltzeitpunkt wäre hier 23:00 Uhr. Besonders schick wird es, wenn der Server nicht täglich manuell gestartet werden muss, sondern dies automatisch erledigt. Platinenrechner der Klasse Raspberry haben typischerweise keinen Powerknopf, sondern booten einfach, sobald der Strom fließt. Daher kann man sich für den zeitgesteuerten Neustart mit einer Zeitschaltuhr oder einer Funksteckdose wie Fritz Dect 200 behelfen (siehe Punkt 1).

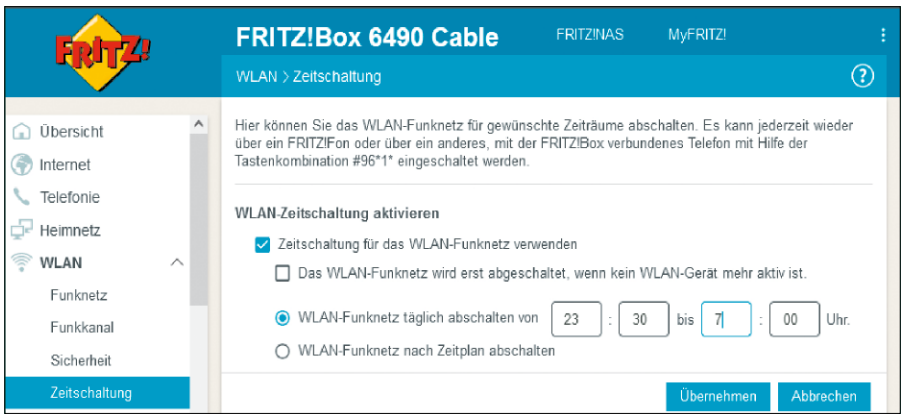
Oft geht es aber noch einfacher: Das Tool Rtcwake – Bestandteil des Standardpakets „util-linux“ – ist auf praktisch jedem Linux-System vorinstalliert. „RTC“ steht für Real Time Clock, die auch im ausgeschalteten Zustand über eine kleine Platinenbatterie weiterläuft. Im einfachsten Fall sieht ein Kommando so aus:

```
sudo rtcwake -m off -s 180
```

Der Befehl ist gut geeignet, um zu testen, ob die Hardware mitspielt (das ist nicht bei allen Platinenrechnern der Fall). Der Schalter „-m“ bestimmt den ACPI-Modus, hier schlicht „off“, um das System komplett herunterzufahren. Als zweiter Parameter ist „-s“ („seconds“) mit einer nachfolgenden Zeitangabe in Sekunden angegeben. Der Befehl wird also das System komplett beenden und dann nach drei Minuten neu starten (180 Sekunden). Wir empfehlen, den geplanten Neustart immer mit Parameter „-s […]“ anzugeben, selbst wenn es sich um viele Stunden handelt. Dies ist einfacher als mit Schalter „-t“ („time) eine exakte RTC-taugliche Zeitangabe anzugeben. Für dauerhaften Einsatz ist ein Cronjob mit root-Recht erforderlich. Nach *sudo crontab -e* genügt folgende Zeile:

```
0 23 * * * /usr/sbin/rtcwake -m
  off -s 28800
```

Dieser Befehl schaltet den Rechner um 23:00 Uhr ab und startet ihn wieder um 7:00 Uhr (nach 28 800 Sekunden, also acht Stunden). ■



Ausgefunkt: Das WLAN können alle Router zeitgesteuert ein- und ausschalten. Beim DECT-Signal für Telefone erlaubt die Fritzbox zumindest eine Reduktion der Signalstärke.

Hardware für spezielle Aufgaben

Ein aktueller Desktop-PC eignet sich für so gut wie jede Aufgabe, wäre aber für den Einsatz etwa alleine als Samba-Server überdimensioniert. Altgeräte, Mini-PCs oder Ein-Platinen-Rechner können diese Rolle ebenfalls übernehmen.

VON THORSTEN EGGELING

Abhängig von der Hardwareausstattung eignen sich Computer für unterschiedliche Aufgabenbereiche. Für einige Rollen reichen eine schwache CPU und wenig RAM aus, andere benötigen mehr Rechenleistung und Hauptspeicher. Die Grafikleistung kann ebenfalls eine Rolle spielen, etwa beim Multimedia-PC am Fernseher. Bei der Gerätewahl sollte man auch die Leistungsaufnahme berücksichtigen, wenn die Hardware pro Tag viele Stunden oder sogar dauerhaft laufen soll. Ein älterer PC kann durchaus die Rolle etwa als Dateiserver übernehmen, treibt die Stromrechnung jedoch mit ungefähr 60 Watt Leistungsaufnahme in die Höhe. Ein-Platinen-Computer, neuere Mini-PCs, Notebooks oder NAS sind in der Regel deutlich sparsamer.

In der Übersichtstabelle finden Sie Informationen zur Einordnung. Bei den Watt-Angaben handelt es sich um ungefähre Werte. Was ein Gerät tatsächlich benötigt, hängt von der durchschnittlichen CPU/GPU-Belastung, dem Speicherausbau und den Festplatten ab. Dazu kommt noch die Leistung für Netzteile, die eventuell USB-Laufwerke versorgen. Die Preisangaben sind Momentaufnahmen vom März 2023. Einige Geräte waren zu diesem Zeitpunkt nicht lieferbar, der Raspberry Pi 4 mit 4 GB RAM wurde in Deutschland ohne Zubehör für 200 Euro angeboten. Vor einigen Jahren lag der Preis noch bei ungefähr 70 Euro.

Prozessor und Hauptspeicher

Ein 64-Bit-Prozessor mit zwei Kernen, einer Taktrate von 1 GHz aufwärts und 4 GB RAM reicht für viele einfache Serveraufgaben völlig aus. Im Heimnetz ist keine besonders hohe Last zu erwarten, auch nicht mit mehreren zugreifenden PCs. Es ist somit möglich, Altgeräten, auf denen die Arbeit mit Office-Programmen und Browser keinen Spaß mehr macht, zu einer neuen Rolle zu verhelfen.

Preisgünstige PCs: Die Leistung eines neuen Mini-PCs mit Celeron-CPU unterscheidet sich kaum von der eines um die zehn Jahre alten Desktop-PCs oder Notebooks. Die Neuanschaffung lohnt sich, wenn es auf eine kleine Bauform ankommt und wenn das Gerät für die geplante Aufgabe ausreicht. Es sind auch Mini-PCs mit deutlich schnelleren Prozessoren verfügbar, die dann aber mit 600 bis 800 Euro ähnlich viel kosten wie ein entsprechender Desktop-PC oder ein Notebook.

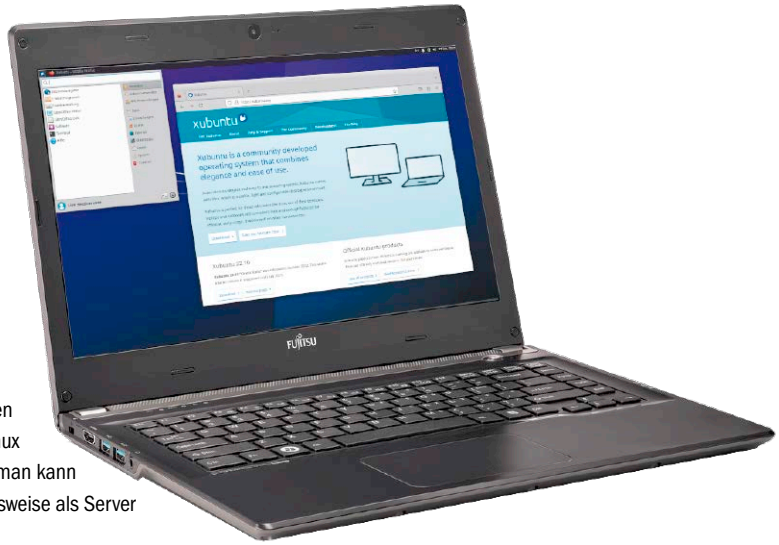
Die Mini-PCs Intel NUC11ATKC2 und Zotac ZBOX CI331 Nano enthalten nur die CPU, RAM (16 GB etwa für 60 Euro) und Festplatte/SSD muss man zusätzlich erwerben. Ein Netzteil ist im Lieferumfang enthalten. Beim Odroid H3+ kauft man nur die Platine inklusive CPU, alles andere erwirbt man als Zubehör. Mit 11 × 11 Zentimetern entspricht die Abmessung der Platine in etwa der in den anderen Mini-PCs. Der Intel-Celeron-N6005-Prozessor ist jedoch etwas leistungsstärker.

Die Ein-Platinen-Rechner mit ARM-CPU spielen in einer anderen Liga. Die Prozessoren sind durchweg weniger leistungsfähig als ein Intel Celeron, die RAM-Ausstattung liegt meist bei nicht erweiterbaren 2 bis 4 GB, lediglich vom Raspberry Pi 4 gibt es ein Modell mit 8 GB. Für den ursprünglichen anvisierten Einsatz als besonders preiswerte Lehr- und Lerncomputer ist das ausreichend. Ein Apache-Webserver oder Dateifreigaben über Samba sind für die kleinen Geräte aber kein Problem, sofern man keine besonders hohe Geschwindigkeit unter Last erwartet. Besondere Vorteile bieten die frei programmierbaren GPIO-Pins (General-Purpose Input/Output) beim Raspberry Pi, Banana Pi und Beaglebone Black, über die sich Geräte steuern oder

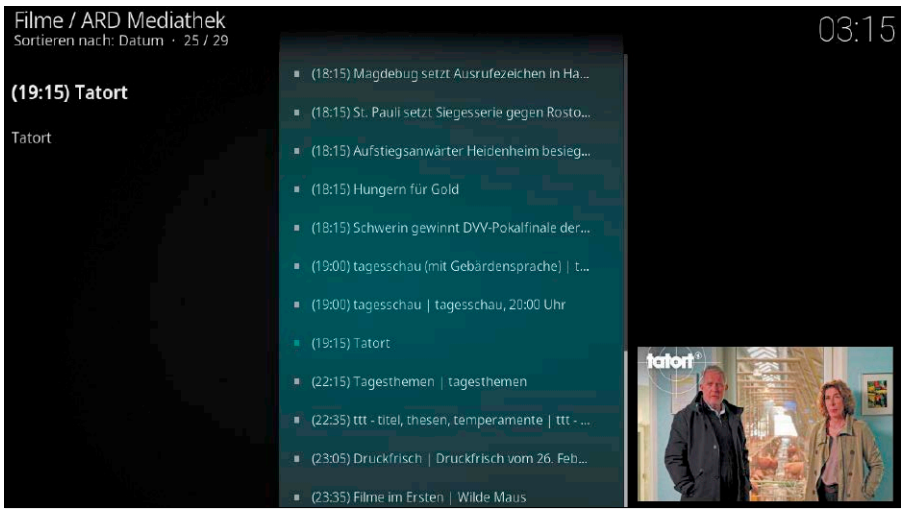
Sensoren abfragen lassen (siehe *www.pcwelt.de/1357080*).

Intel oder ARM? Geräte mit Intel-CPU sind flexibel. Linux wie Windows lassen sich installieren und man hat eine breite Auswahl von Software für x86-Prozessoren. Für ARM-CPUs stehen vor allem die Distributionen Debian und Ubuntu sowie Android zu Verfügung. Das Standardsystem für den Raspberry Pi ist Raspberry-Pi-OS (*www.raspberrypi.com/software*), das auf Debian basiert. Fast alle Linux-Tools und -Programme lassen sich auch auf ARM-Systemen installieren. Einschränkungen gibt es nur bei wenig Spezialsoftware, die nur Intel-CPUs unterstützt.

NAS als bequemere Lösung? Die flexibelste Variante eines Netzwerkspeichers – Network Attached Storage, kurz NAS – ist ein Leergehäuse. Denn hier bestücken Sie das NAS-Gehäuse mit Festplatten Ihrer Wahl. Die Preisangaben in der Übersichtstabelle verstehen sich daher ohne Festplatten. Um CPU und RAM müssen Sie sich wenige Gedanken machen. Der Hersteller hat eine Konfiguration gewählt, die ausreichend Leistung bietet. Auf- oder Umrüstung sind aber in der Regel nicht vorgesehen. Aktuelle NAS dienen nicht nur als Datenspeicher. Die komfortable Oberfläche lässt sich im Browser aufrufen und ermöglicht auch die Organisation von Bild-, Audio- und Video-Dateien. Die Inhalte lassen sich per App auf dem Smartphone oder Tablet abrufen oder auf TV-Geräte streamen.



Neues Leben für alte Hardware: Auf Notebooks, die vor zehn Jahren auf den Markt kamen, läuft Linux immer noch flott und man kann die Hardware beispielsweise als Server nutzen.



Mediacenter-PC am TV: Kodi kann Inhalte von Freigaben im lokalen Netzwerk abspielen und unterstützt über Add-ons auch Streaminganbieter und einige Mediatheken.

Grafikchip und Multimedia

Aktuelle TV-Geräte bieten bereits standardmäßig Netflix, Amazon Prime Video, Youtube und andere Streamingdienste. Aufbau und Reaktionszeit der Oberfläche sind jedoch oft nicht befriedigend. Der Zugriff auf Mediaserver im lokalen Netzwerk (DLNA, UPnP) ist zwar möglich, die Navigation ist jedoch nicht besonders komfortabel. Außerdem spielen TV-Geräte längst nicht jedes Format ab. Ein PC als Mediacenter ist deutlich flexibler und schneller. Ältere PCs bieten jedoch oft nur einen wenig leistungsfähigen Grafikchip. Für die Wiedergabe von SD-Videos reicht die Prozessorgrafik aus, meist aber nicht mehr für HD- oder 4K-Filme. Allerdings möchte man einen lärmenden Desktop-PC nicht gerne im Wohnzimmer unterbringen.

Kleine PCs mit Celeron-CPU können auch 4K-Videos ohne Ruckeln abspielen und von den passive gekühlten Geräten (Zotac ZBOX CI331 Nano, Odroid H3+) ist keine Lärmbelästigung zu befürchten. Der Nachteil: Damit sich eine Multimediaoberfläche wie Kodi (*https://kodi.tv* oder Komplettpaket *https://libreelec.tv*) bequem vom Sofa aus per TV-Fernbedienung steuern lässt, benötigt man einen HDMI-CEC-Adapter (*www.pulse-eight.com*). Eine Alternative ist ein Infrarot-USB-Adapter (beispielsweise FLIRC USB *https://amzn.to/3SyXCjv*). Kodi lässt sich außerdem über eine Smartphone-App fernbedienen (*http://bit.ly/3m7O3vU*).

Der Raspberry Pi 4 unterstützt HDMI-CEC von Haus aus, sodass sich Kodi über die TV-Fernbedienung steuern lässt. Der Grafikchip reicht auch für 4K-Videos aus, und mit Modellen mit 4 oder 8 GB RAM ist die Oberfläche flüssig bedienbar.

Kodi spielt Inhalte von Samba-Freigaben oder von einem per USB angeschlossenen Laufwerk ab. Für Netflix & Co. nutzt man die Apps des Smart-TV. Ist das Gerät an einen PC-Monitor angeschlossen oder kein Smart-TV verfügbar, kann man auch Netflix und Amazon Prime Video in Kodi einbinden (siehe *www.pcwelt.de/1172212*).

Bei den aktuellen Preisen des Raspberry Pi ist ein Amazon Fire TV Stick 4K für ungefähr 70 Euro zurzeit die bessere Alternative. Netflix und Amazon Prime Video sind vorinstalliert, weitere Anbieter lassen sich über Apps aus dem Amazon App Store nachinstallieren. Das kleine Gerät wird direkt mit dem HDMI-Anschluss des Fernsehers oder Monitors verbunden, es spielt 4K-Videos ab und die Bedienung ist angenehm flüssig. Eine Fernbedienung gehört zum Lieferumfang, die TV-Fernbedienung lässt ich per HDMI-CEC ebenfalls nutzen. Die Installation der Android-Kodi-App ist nur über Umwege möglich. Eine Beschreibung finden Sie unter *www.pcwelt.de/1177253*.

Für besonders schnellen Datentransfer kann man einen PC mit 10-Gigabit-Ethernet aufrüsten. Das lohnt sich aber nur, wenn die Festplatten mit diesem Netzwerktempo mithalten.

Mehr Speicherplatz: Externe USB-Festplatten im 2,5-Zoll-Format gibt es zurzeit mit bis zu 5 TB. Die Geräte sind ausreichend schnell und leise, die Leistungsaufnahme ist gering.

Ethernet und WLAN

Aktuelle PCs und Notebooks verfügen durchweg über Gigabit-Ethernet. In der Praxis sind Transferraten von circa 100 MB pro Sekunde erreichbar. Beim Kopieren vieler kleiner Dateien bricht die Übertragungsrate deutlich ein. Mit einer SSD laufen die Daten meist flüssiger durch das Netzwerk. Schnellere Ethernet-Adapter mit 2,5 oder 10 Gigabit sind in einigen NAS zu finden und als Netzwerkkarten für den PC. Sie versprechen mehr Geschwindigkeit, setzen aber einen dazu passenden Router oder Switch voraus. Eine Magnetfestplatte liefert jedoch nur um die 120 MB/s, weshalb sich Multi-Gigabit erst beim Einsatz von SSDs oder bei Festplatten in einem Raid-0-Verbund lohnt.

Sollte kein Ethernet-Kabel verfügbar sein, lässt sich auch das WLAN nutzen. Bei optimaler Aufstellung in der Nähe des WLAN-Routers sollte die Geschwindigkeit ausreichen. Wer einen Wi-Fi-6-Router und dazu passenden WLAN-Adapter besitzt, kann über das Funknetzwerk theoretisch 1201 MBit/s abrufen. In der Praxis bleiben davon unmittelbar neben dem Sender um die 730 MBit/s übrig, bei größerer Entfernung sinkt die Übertragungsrate deutlich. Mit Routern und WLAN-Adaptern, die mit älteren Standards arbeiten, lassen sich oft nur um die 100 MBit/s erreichen. WLAN ist daher für einen Server im Vergleich zu Gigabit-Ethernet eher eine Notlösung.

Festplatten und SSDs

Ähnlich wie Notebooks, bieten Mini-PCs oft nur Platz für eine Festplatte oder SSD im 2,5-Zoll-Format. Die Speicherkapazität ist damit zur Zeit auf 5 TB beschränkt. Ein Tower-PC kann meist vier oder mehr 3,5-Zoll-Festplatten jeweils mit bis zu 18 TB aufnehmen. Das genügt sicher auch als Backupspeicher für mehrere PCs. Viele große Festplatten treiben aber die Stromrechnung in die Höhe und erhöhen den Geräuschpegel. An Notebooks, Mini-PCs und Ein-Platinen-Computer lassen sich externe Laufwerke über USB anschließen. In der Regel sind Ports nach dem Standard USB 3.0 verfügbar (neue Bezeichnung USB 3.2 Gen 1), die bis zu 5 GBit/s liefern. In der Praxis sind das um die 450 MB/s, was auch für mehrere USB-Festplatten ausreicht.

Beim Raspberry Pi 4 hat man keine Wahl. Das Gerät bietet für die Laufwerke nur USB-Buchsen. Auf dem Banana Pi M2U oder Odroid H3+ befinden sich auch SATA-Anschlüsse, was eine flexiblere Ausstattung ermöglicht. Die Stromversorgung erfolgt über ein SATA-Adapterkabel. Bei den ansonsten sparsamen Geräte steigt durch externe Festplatten die Leistungsaufnahme um einige Watt.

Ein-Platinen-Computer starten das Betriebssystem von einer SD-Karte. Man sollte auf gute Qualität von einem Markenhersteller achten, damit die Karte eine ausreichende Geschwindigkeit bietet und zuverlässig arbeitet. Der Kartenslot des Raspberry Pi ist eine Schwachstelle. Vor allem nach längerer Benutzung kommt es manchmal zu Abstürzen des Systems oder zu Start-

BETRIEBSSYSTEME FÜR BESONDERE ROLLEN

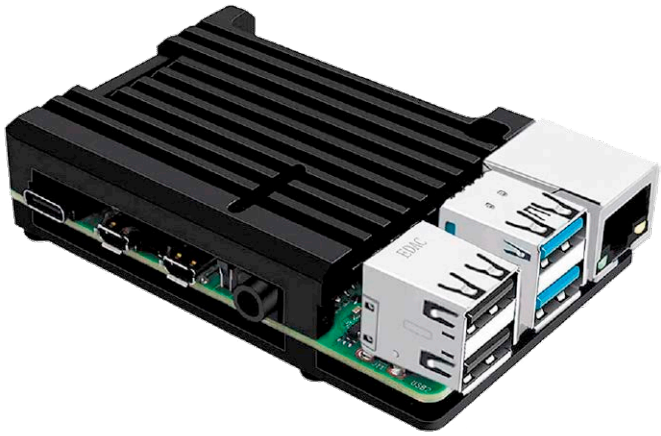
Für einen Mini-PC oder ein Altgerät sollte man ein Betriebssystem wählen, das sparsam mit den Ressourcen umgeht. Geeignet sind beispielsweise MX Linux (*https://mxlinux.org*), Q4-OS (*https://q4os.org*) oder Xubuntu (*https://xubuntu.org*). Spezialisierte Oldie-Unterstützer wie Antix (*https://antixlinux.com*), Bodhi Linux (*www.bodhilinux.com*), Puppy Linux (*https://puppylinux.com*) sind noch anspruchsloser, erfordern jedoch mehr Einarbeitung bei der Konfiguration und Nutzung. Infrage kommen außerdem Systeme wie Ubuntu Server (*https://ubuntu.com*). Bei einer Standardinstallation wird keine Desktopumgebung eingerichtet, die Administration erfolgt bevorzugt über das Netzwerk mit SSH. Ansonsten unterscheidet sich das System nicht wesentlich von Ubuntu Desktop.

Wer für einen Datenserver eine Konfigurationsoberfläche bevorzugt, ist mit dem NAS-System Open Media Vault (OMV) gut beraten (*www.openmediavault.org*). Der Start des Rechners von der heruntergeladenen ISO-Datei bietet einen textbasierten Installer. Das System belegt immer die komplette Festplatte, obwohl es nur wenig Platz benötigt. Verwenden Sie daher als Installationsziel besser eine kleine SSD, die Sie sonst nicht mehr benötigen, oder einen USB-Stick. 16 GB reichen aus. Nach der Installation erfolgt die Konfiguration über das Netzwerk via Browser in einer Weboberfläche. Dafür benötigen Sie lediglich die IP-Adresse des OMV-Rechners.

problemen, die auf mangelhafte Kontakte des Lesegerätes zurückzuführen sind. Bei USB-Sticks treten diese Fehler nicht auf. Allerdings blockiert man damit einen USB-Anschluss.

Kühlung und Gehäuse

Für Celeron und ARM-CPUs reicht auch unter Volllast eine passive Kühlung aus. Zur effektiven Wärmeabfuhr kommen am besten großflächige Kühlkörper zum Einsatz. Bei der Zotac ZBOX CI331 Nano dient das gesamte Gehäuse der geräuschlosen Kühlung. Intel verbaut in der NUC-Serie kleine Lüfter, die nicht oft anspringen und deren Drehzahl geregelt ist. Unter Last kann das Gerät aber unangenehme Geräusche produzieren. Odroid H3+ wird mit einem voluminösen Kühlkörper ausgeliefert, das vom Hersteller angebotene passende Gehäuse lässt sich mit einem 92-mm-Lüfter versehen. Beim Raspberry Pi 4 gibt es kleine Kühlkörper als Zubehör, die man auf die Chips klebt. Effektiver sind große Kühlkörper, die alle Chips auf der Ober- und Unterseite abdecken. Ein zusätzliches Gehäuse ist nicht mehr notwendig. Gehäuse mit einem kleinen Lüfter sind aufgrund der Geräuschentwicklung nicht zu empfehlen. ■



Kühler Raspberry Pi: Der Kühlkörper dient hier zugleich als Gehäuse. Beim Raspberry Pi 4 ist ausreichende Kühlung damit auch unter hoher Last gewährleistet.

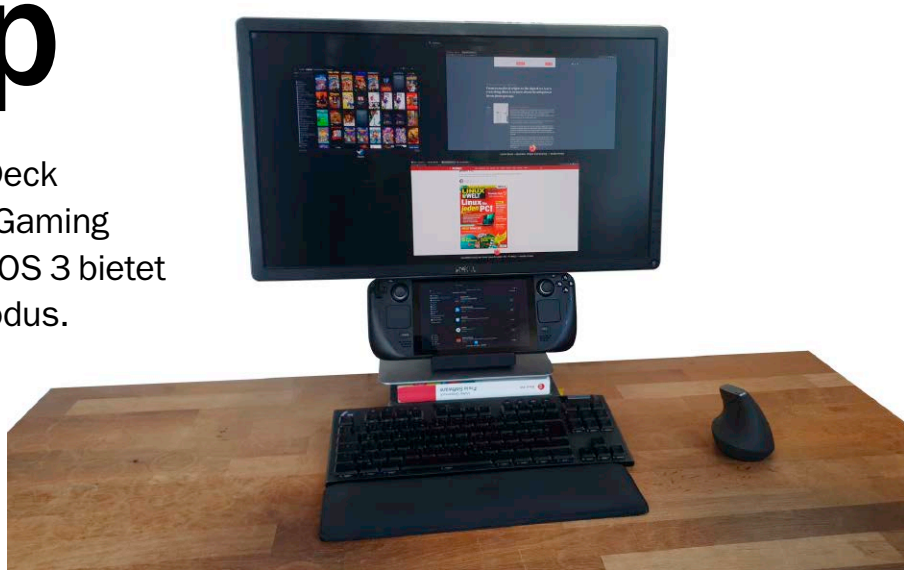
Odroid H3+ im Gehäuse: Damit die CPU kühl bleibt, empfiehlt der Hersteller ein Gehäuse mit aufgesetztem Lüfter für die Abfuhr der Wärme aus dem Gehäuse.

EIN-PLATINEN-COMPUTER UND MINI-PCS (AUSWAHL)

Gerät	CPU Core	CPU GHz	RAM GB	Ethernet	USB 2.0/3.0	Extras	Watt (Leerlauf/Last)	Vertrieb	Betriebssysteme	Preis € (ca.)
Amazon Fire TV Stick 4K	Quad (ARM)	1,7	1,5	100 MBit/s mit Ethernet-Adapter	–	WLAN, Fernbedienung	3/3	Amazon	Android	70
Asustor Drivestor 2 Pro AS3302T (NAS)	Quad (Realtek ARM)	1,4	2	2,5 Gigabit/s	0/3	2× SATA	6/13	Amazon, Reichelt	Asustor Data Master (Linux, vorinstalliert)	250
Banana Pi M2U	Quad (ARM)	1,5	2	1 Gigabit/s	3/0	SATA, WLAN, Bluetooth	2/5	Reichelt, Conrad	Ubuntu, Debian, Android	92
Banana Pi M5	Quad (ARM)	2	4	1 Gigabit/s	0/4	Infrarotempfänger	2/5	Reichelt, Conrad	Ubuntu, Debian, Android	100
Beaglebone Black	Single	1	0,5	100 MBit/s	1/0	HDMI, viele I/O-Ports	1/3	Reichelt, Pollin	Debian, Android	70
Intel NUC11ATKC2	Dual (Intel)	2,9	bis zu 32	1 Gigabit/s	2/4	Celeron N4505, M.2-Steckplatz (SSD), WLAN, Bluetooth	2/20	Amazon, Reichelt	jedes Linux, Windows	170
Odroid H3+	Quad (Intel)	bis 3,3	bis zu 64	2× 2,5 Gigabit/s	2/2	Jasper Lake N6005, 2× SATA 3	2/18	Reichelt, Pollin	jedes Linux, Windows	270
Odroid N2+	Quad/Dual (ARM)	bis 2,4	4	1 Gigabit/s	0/4	Infrarotempfänger	2/7	Reichelt, Pollin	Ubuntu, Android	135
Raspberry Pi 4	Quad (ARM)	1,5	1 bis 8	1 Gigabit/s	2/2	WLAN, Bluetooth, 2× HDMI	2/5	Amazon, Conrad, Reichelt	Raspberry-Pi-OS, Debian, Ubuntu, Windows IoT	70-200
Synology NAS DS223	Quad (Realtek ARM)	1,7	2	1 Gigabit/s	0/3	2× SATA	5/18	Amazon, Conrad, Reichelt	Disk Station Manager (Linux, vorinstalliert)	290
Zotac ZBOX CI331 Nano	Quad (Intel)	1,1 bis 2,8	bis zu 16	2× 1 Gigabit/s	4/1	Celeron N5100, 1× SATA, WLAN, Bluetooth	6/18	Amazon, Conrad, Reichelt	jedes Linux, Windows	245

Steam Deck als Desktop

Valves Spielekonsole Steam Deck revolutioniert gerade mobiles Gaming und Gaming mit Linux. Steam-OS 3 bietet jedoch auch einen Desktopmodus. Wird die Konsole mit Dockingstation zum passablen Desktopersatz?



Steam Deck mit internem und externem Display: Der kleine Sieben-Zoll-Bildschirm der Spielekonsole genügt nur im Notfall für einen Desktopeinsatz.

VON CLAUDIUS GRIEGER

2015 hatte der US-Konzern Valve schon einmal Gamingsysteme mit Linux veröffentlicht. Steam-OS basierte damals auf Debian und die Hardware wurde von Firmen wie Dell oder Alienware gebaut. Trotz der flexiblen Preisspanne zwischen 400 und 6000 US-Dollar geriet die Idee zum finanziellen Flop. Zudem mangelte es am Spieleangebot und einem funktionierenden Compatibility Layer wie Proton. Auch der Desktopmodus war kaum zu gebrauchen – doch das ist jetzt anders.

Das Steam Deck ist eine mobile Spielekonsole mit PC-Hardware und Linux im Hintergrund. Derzeit ist die günstigste Variante für 419 Euro zu haben. Wenn die Leistung dieser Hardware für aktuell 6000 Spiele ausreicht, die als „verified" oder „playable" für die Konsole zertifiziert sind, dann sollte das auch für einen Desktopersatz genügen.

Steam-OS basiert auf Arch Linux

Valve hat aus vergangenen Fehlern gelernt. Die Steam Deck ist nicht nur ein mobiles Gaming Device, sondern Steam-OS 3 basiert nun auf Arch Linux. Das wird ähnlich wie Manjaro nicht als Rolling Release veröffentlicht, sondern in periodischen Abständen ausgeliefert. Die Distribution profitiert durch die schnelleren Releases von Treibern und Grafik-APIs gegenüber der alten Debian-Basis. Die Systemsoftware mit Linux-Kernel 5.13 (aktuell 6.1), KDE Plasma 5.26 (aktuell 5.27) und Qt-Toolkit 5.15 (aktuell 6.4) könnte jedoch noch etwas aktueller sein. Dank Proton laufen für Windows entwickelte Spiele unter Linux zudem problemlos(er) als nur mit Wine. Auch der Desktopmodus ist jetzt definitiv gut nutzbar.

Steam Deck: Hardware und Benchmarks

Der verwendete AMD-APU basiert auf der Zen-2- und RDNA-2-Architektur und soll die Leistung eines Ryzen der 3000er-Serie oder einer Radeon der RX 6000er-Serie liefern. Die Vierkern-CPU mit acht Threads taktet zwischen 2,5 und 3,5 GHz. Der Arbeitsspeicher mit 16 GB Low-Power-DDR5 ist ebenfalls guter Standard. Diese Ausstattung ist bei allen Deck-Varianten identisch.

Der Benchmark Geekbench 6 attestiert für die teuerste Steam-Deck-Version mit NVME einen Singlecore-Wert von 1191, für Multicore 4209 – nicht exorbitant, aber doch mehr als manch gebrauchter Laptop und damit absolut desktopttauglich.

Die verschiedenen Modelle unterscheiden sich vor allem in einem anderen Display-Glas (die 512-GB-Variante ist entspiegelt, geätzt und soll bessere Farbwerte liefern) und unterschiedliche Festplatten: 64 GB eMMC, 256 GB NVMe SSD und 512 GB NVMe SSD. Alle lassen sich mit einer Micro-SD-Karte erweitern.

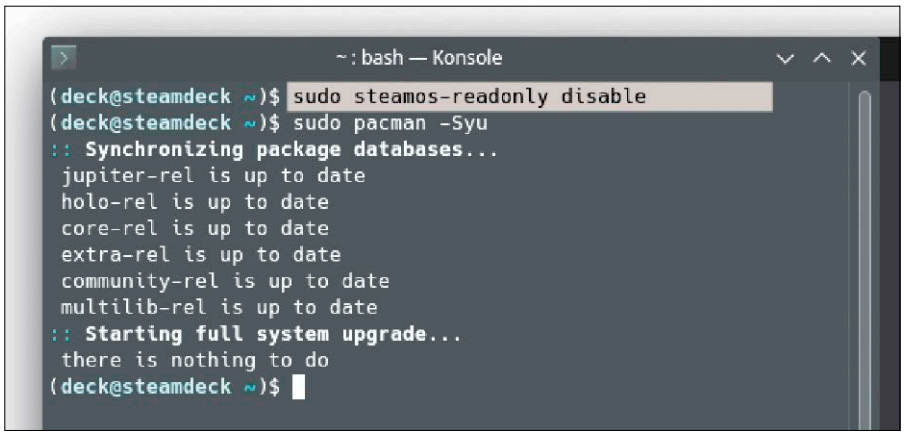
Eine Webcam ist nicht verbaut, Sprachkonferenzen sind aber dank Stereo-Mikrofonarray und Stereolautsprechern problemlos umsetzbar. Die Lautsprecher klingen bei Musik eher dünn, dafür ist das Sprachverständnis gut. Es sollte dennoch ein Headset via Bluetooth, am Klinkenstecker oder via USB-Adapter genutzt werden, denn der Lüfter wird wegen der nahen Lüftungsschlitze auf den integrierten Mikros deutlich hörbar. Zudem neigt der verbaute Lüfter der Marke Delta zum Fiepen. Der leisere Huaying-Lüfter ist für circa 25 Euro zum Selbsteinbau bestellbar. (*www.ifixit.com/Device/Steam_Deck*).

Dockingstation für Desktopbetrieb

Peripherie kann über den USB-C Anschluss mittels Adapter, Hub oder einer passenden Dockingstation angeschlossen werden. Damit wird das Steam Deck zum zweiten Monitor. Das hauseigene Steam Deck Dock bietet drei USB 3.1-Anschlüsse, Gigabit-Ethernet, Displayport 1.4, HDMI 2.0 und unterstützt damit maximal zwei externe

Quelle: amazon.de

Ohne Dockingstation ist das Steam Deck kaum als Desktop zu gebrauchen. Das hauseigene Valve-Dock kostet etwa 50 Euro.



Pacman im Terminal: Der Arch-Paketmanager ist standardmäßig deaktiviert, kann aber mit einem Befehl freigeschaltet werden.

Monitore bis 4K bei 60 Hz oder 1440 p mit 120 Hz. Ein externer Bildschirm ist für den Desktopbetrieb in jedem Fall Pflicht. Ohne angeschlossenes Netzteil geht dem Akku je nach Nutzung nach zwei bis acht Stunden der Saft aus. In der Praxis eher früher als später. Generell gibt es keinerlei Probleme bei Alltagsprogrammen wie Libre Office, Firefox, Thunderbird, Gimp, Kdenlive, Darktable, Obsidian und natürlich Steam: Alle typischen Desktopprogramme können installiert werden und laufen einwandfrei. Speicher und Zugriffszeiten sind auf externen Micro-SD-Karten und Festplatten ohne merkliche Verzögerung. Steam-OS 3 (oder Steam-Deck-OS) setzt auf den Desktop KDE und zusätzliche Programme installiert man standardmäßig nur als Flatpak über den App Store Discover oder im Terminal. Der Zugriff auf den Terminalpaketmanager pacman ist ab Werk deaktiviert, kann aber mit

```
sudo steamos-readonly disable
```

auf Wunsch freigeschaltet werden. Das lohnt sich vor allem für Nutzer, die im Terminal mehr als das vorinstallierte Minimalpaket nutzen möchten. Den Steam-Paketquellen fehlen allerdings etliche populäre Programme wie etwa das Infotool inxi.

In Problemfällen oder zum Einbau einer größeren Festplatte gibt es ein „SteamOS Recovery-ISO“ nebst Anleitung (*https://help.steampowered.com/en/faqs/view/1B71-EDF2-EB6D-2BB3*).

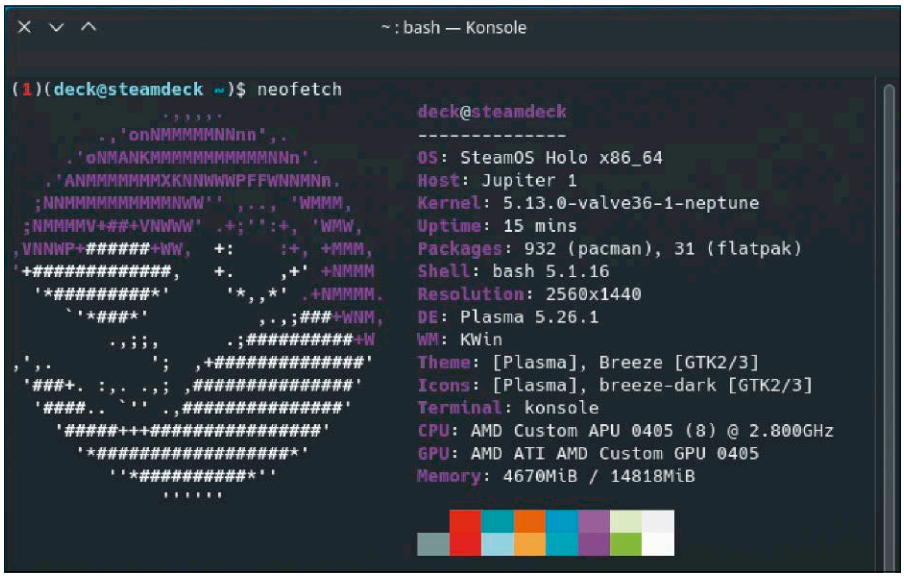
Sicherheitsdefizite: Valve bietet als Sicherheitsoption lediglich eine Pin-Funktion an, die beim Start, beim Aufwachen aus der Bereitschaft und beim Aktivieren des Desktopmodus aktiv wird. Eine ausgebaute Festplatte oder SD-Karte mit Home-Ordner kann daher leider problemlos ausgelesen werden. Eine komplette Verschlüsselung des Dateisystems (Full Disk Encryption) ist nur manuell möglich. Dann muss allerdings beim Neustart der Konsole immer eine Tastatur verfügbar sein. Für sensible Daten über die Nutzungsdaten von Browser und Dateiverlauf hinaus sollten Lösungen wie Veracrypt in Erwägung gezogen werden.

Passwörter für root und für den Standardbenutzer „deck“ sind nicht vergeben und sollten daher beim ersten Desktopstart mit *passwd* im Terminal für das Benutzerkonto sowie mit *sudo su* und anschließendem *passwd* für root angelegt werden.

Steam Deck: Gaming und Allround-PC?

Das Steam Deck ist ein vielseitiges Stück Hardware. Valve bleibt zwar ein gewinnorientierter Konzern und will Nutzer ins Steam-Universum locken, dennoch zeigt Valve, wie man es richtig macht – mit akzeptablen Preisen, austauschbarer Hardware, offiziellen Ersatzteilen, Drittherstellerprodukten und Linux als freiem Unterbau mit zugänglichem Desktopmodus.

Die Leistung reicht jederzeit für alltägliche Aufgaben. Mit einer Dockingstation wird es zu einem brauchbaren Begleiter für Browsen, Streamen, Mail, Text-, Grafik-, Foto-, Audio- und Videobearbeitung. In seltenen Fällen hängt das System den Eingaben für ein, zwei Sekunden hinterher, fängt sich aber wieder. Einen stationären Arbeitslaptop kann das Steam Deck spielend ersetzen. Lediglich die teils veraltete Softwarebasis und mangelnde Verschlüsselungsmöglichkeiten trüben den insgesamt positiven Eindruck. Immerhin soll aber mit Steam-OS 3.5 ein neuer Kernel Einzug halten. ■

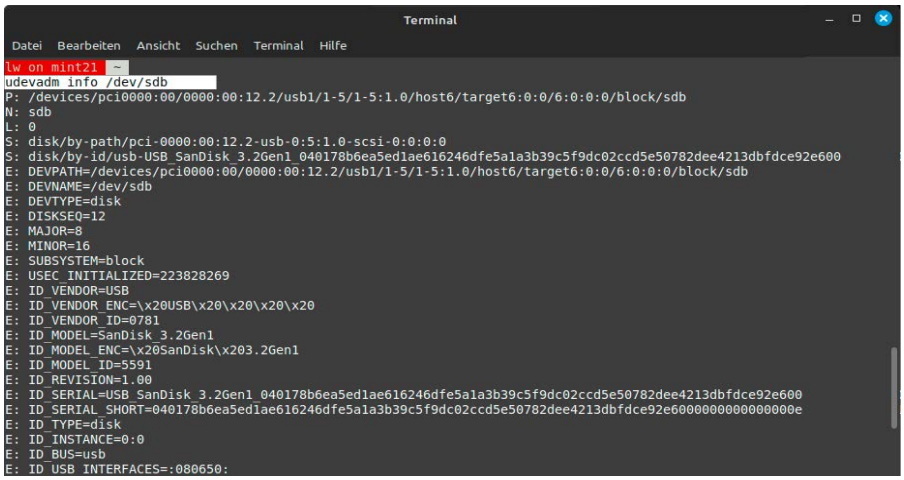


Das Tool Neofetch zeigt es: Die aktuell verwendete Softwarebasis ist nicht mehr auf dem neuesten Stand.

Linux-Gerätemanager Udev

Der Systemd-Dienst Udev ist ein umfangreiches Linux-Subsystem zur Kontrolle und Steuerung aller Hardwarekomponenten. Trotzdem sind kompetente Ratgeber und sprechende Beispiele zu diesem Thema rar – und das kann kaum verwundern.

VON HERMANN APFELBÖCK



Geräteeigenschaften ermitteln: Der Befehl *udevadm info* liefert die Informationen, die Sie für eine exakte Udev-Regel benötigen.

Das zum Udev-Dienst gehörige Werkzeug udevadm ist im Prinzip vergleichbar mit dem Gerätemanager unter Windows, allerdings nicht mit dessen grafischer Ausführung, sondern mit dessen optionalem Kommandowerkzeug devcon (nicht Standard). Wenn Sie im Linux-Terminal den Überwachungsbefehl

```
udevadm monitor
```

starten, wird dieser auf Hardwareereignisse aller Art antworten – auf das Einstecken eines USB-Sticks ebenso wie auf den Anschluss eines Notebook-Netzteils, auf das Abschalten des Wi-Fi-Adapters oder den Druck einer Notebook-Sondertaste. Einen Eindruck über die Reichweite des Udev-Dienstes gewinnen Sie unter „/lib/udev/rules.d“, wo die Standardregeln Ihrer Linux-Distribution in Dateien mit der Endung „.rules“ vorliegen. Der Dateibestand ist dreistellig, wobei aber viele Regeln nur für ganz bestimmte Hardware, Hersteller und Modelle gelten. Die Einsicht in diese „Rules“ dürfte jeden PC-Anwender überfordern. Udev ist katastrophal verkopft, erfordert präziseste Syntax, Operatoren und Gerätespezifikationen, bietet aber weder die Debug-Möglichkeiten noch die Dokumentation, die für so exaktes Arbeiten notwendig wären. Die systematischen, aber allzu knappen Manpages udev.html und udevadm.html unter *www.freedesktop.org/software/systemd/man/* sind eine Orientierung, aber mehr nicht. Das sind insgesamt einige Gründe, die normale PC-Benutzer abschrecken dürften. Für Bastler ist Udev aber durchaus ergiebig. Dieser Beitrag liefert einige Grundlagen und praktische Beispiele.

Grundlegende Infos

Udev-„Rules“ geben vor, wie sich permanente Geräte beim System anmelden und was beim Anschluss oder Trennen einer Hardware geschehen soll (Hotplug). Der Ablauf und die Priorität der „Rules“-Dateien ist nicht ganz einfach: Selbst angelegte (oder dorthin kopierte) Dateien unter „/etc/udev/rules.d/“ haben stets Vorrang vor gleichnamigen Standarddateien unter„/lib/udev/rules.d“. Alle Rules-Dateien werden nach ihrem Dateinamen alphanumerisch abgearbeitet, daher die typische (allerdings nicht notwendige) Bezifferung von „01-*“ bis „99-*“. Wenn sich dort enthaltene Regeln inhaltlich widersprechen, gewinnt die letzte. Mit einer Datei „99-xyz.rules“ unter „/etc/udev/rules.d“ ist die Priorität so gut wie gewiss, mit einer Datei „xyz.rules“ ohne Bezifferung noch sicherer, weil diese alphanumerisch noch später gelesen wird. Eigene Regeln muss man grundsätzlich mit root-Recht (sudo) unter „/etc/udev/rules.d“ anlegen – nicht nur wegen der Priorität dieses Ortes, sondern auch aus dem Grund, dass die Rules-Dateien unter „/lib/udev/rules.d“ durch Systemupdates wieder in den Originalzustand versetzt werden.

Eine Regel besteht immer aus einer Zeile, jedoch kann eine Rules-Datei auch mehrere oder viele Regeln enthalten. Eine Regelzeile besteht aus mit Komma getrennten Anweisungen, die zunächst das Gerät oder eine Geräteklasse definieren und für diese Hardware danach einen neuen Namen, andere Zugriffsrechte, Verbote oder ein externes Programm anfordern.

Eigene Udev-Regeln benötigen folglich eine exakte Definition der Geräteeigenschaften. Um die Eigenschaften eines Geräts zu ermitteln, gibt es unterschiedliche Methoden. Auch allgemeine Systemtools wie lsusb, lsblk oder blkid können Eigenschaften wie Laufwerkskennungen liefern, die dann in Udev-Regeln verarbeitet werden. Wir verweisen hier der Kürze halber auf das Tool udevadm, das in jedem Fall alle benötigten Infos ausgibt:

```
udevadm monitor --property
```

Diese Methode reagiert auf Hardwareänderungen wie etwa den Anschluss eines USB-Sticks. Dann flutet der Befehl Informatio-

nen über das betreffende Gerät, scheint damit zunächst sehr unübersichtlich, ist aber andererseits eine universelle Methode. Gezielter auf ein Gerät gerichtet ist diese Methode, die keine Änderung des Gerätestatus erfordert:

```
udevadm info /dev/sdb
```

Zusätzliche Schalter „udevadm info -a -n“ machen die Ausgabe sehr redselig, sind aber nicht notwendig, wenn etwa nur eine Geräte-ID ermittelt werden soll wie etwa „ID_SERIAL“ oder „ID_MODEL“.

Mit exakten Geräteangaben wie

```
ATTR{ID_SERIAL_SHORT}==
  "4C530001080716117381", […]
```

lässt sich dann die Anschlussreaktion eines ganz bestimmten USB-Laufwerks verändern und mit sehr allgemeinen Angaben wie

```
SUBSYSTEMS=="usb", […]
```

das Verhalten einer ganzen Geräteklasse.

Hinweise auf Syntaxfehler in einer Rules-Datei kann der Befehl

```
udevadm test /dev/sda
```

ausgeben, wobei das angegebene Gerät keine Rolle spielt. Dabei werden sämtliche „Rules“-Dateien durchlaufen – dies in der oben erklärten Reihenfolge und mit Hinweisen auf fehlerhafte Einträge. Die Befehle

```
sudo udevadm control --reload
sudo udevadm trigger
```

sind hilfreich, um neue Regeln im laufenden Betrieb zu aktivieren und damit ohne lästige Neustarts zu testen.

Praktische Beispiele

1. Partitionen verstecken: Dateimanager zeigen unter „Geräte“ grundsätzlich alle angeschlossenen Datenträger, auch jene von parallel installierten Systemen (Linux oder Windows), auf die man in der Regel nicht zugreifen sollte. Eine einfache Udev-Regel, etwa gespeichert als „/etc/udev/rules.d/no_win.rules“, kann die betreffende Partition ausblenden:

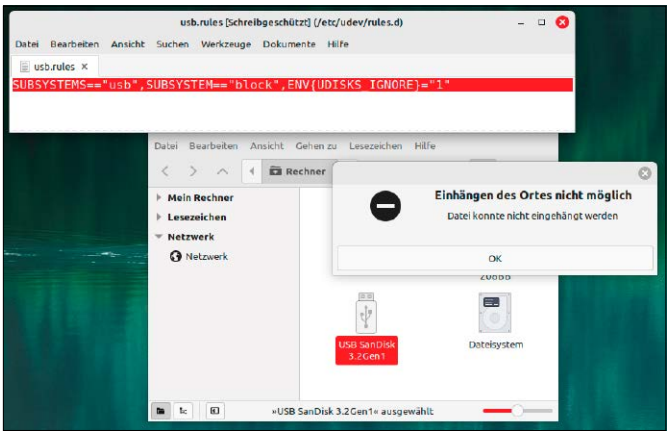
```
KERNEL=="sda2", ENV{UDISKS_
  IGNORE}="1"
```

Dasselbe Ergebnis erzielt folgende Regel, welche die Partition anhand ihrer eindeutigen Kennung anspricht:

```
ENV{ID_FS_UUID}=="5cb95212-b894-
  4e57-91ff-7ba2faf48ad5",
  ENV{UDISKS_IGNORE}="1"
```

Die ID kann mit *blkid* oder *udevadm info* ermittelt werden.

Hinweis: Für ältere Distributionen gültig und daher vielfach in älteren Udev-Anleitungen immer noch anzutreffen ist obsoletes „UDISKS_PRESENTATION_HIDE“ statt dem heute gültigen „UDISKS_IGNORE“.



Ein simples, aber grobes Verbot: Diese Udev-Regel (oben) verbietet jegliche USB-Datenträger.

2. USB-Datenträger verbieten: Mit folgender Udev-Regel, etwa abgelegt als „/etc/udev/rules.d/no_usb.rules“, ignoriert jeder grafische Desktop den Anschluss von USB-Laufwerken (Subsystem im Plural und Singular ist so korrekt):

```
SUBSYSTEMS=="usb",SUBSYSTEM==
  "block",ENV{UDISKS_IGNORE}="1"
```

Andere USB-Geräte wie Maus oder Netzadapter funktionieren weiter. Die Aktion hat wie das erste Beispiel nur Auswirkung auf den grafischen Dateimanager. Mit mount im Terminal bleiben USB-Datenträger erreichbar, aber eben nur mit root-Recht.

3. Netzwerkadapter umbenennen: Folgende einfache Regel kann zwei Motive haben, entweder dass Ihnen eine Standardbezeichnung wie „enp0s1“ für die Ethernet-Schnittstelle schlicht nicht gefällt oder – und technischer motiviert –, dass mehrere Adapter ihren Namen wechseln und daher nicht eindeutig anzusprechen sind:

```
SUBSYSTEM=="net", ATTR{address}==
  "e8:03:9a:33:32:ea", NAME="eth0"
```

Als „address“-Eigenschaft ist die MAC-Adresse gemeint, die etwa mit *ip address* zu ermitteln ist.

4. Touchpad ein- und ausschalten: Die folgende Regel ist komplexer, aber nach unseren Tests ist hier tatsächlich keine der Komma-getrennten Angaben verzichtbar.

```
SUBSYSTEM=="input",KERNEL=="mou
  se[0-9]*",ACTION=="add",ENV{DISP
  LAY}=":0", ENV{XAUTHORITY}="/
  home/sepp/.Xauthority",RUN+="/
  usr/bin/xinput --disable 12"
```

Die „ACTIONS“ add und remove meinen den Anschluss (add) und das Entnehmen (remove) eines Geräts. „RUN“ erlaubt den Start eines externen Programms. In Kürze übersetzt heißt dies, dass beim Anschluss („add“) eines Inputgeräts „Maus“ das Inputgerät mit der Kennung 12 abgeschaltet wird (nämlich das Touchpad). Das Ganze gilt nur für den angegebenen Benutzer – im Beispiel das Konto „sepp“. Nun muss es noch eine sehr ähnliche zweite Regel geben, die das Touchpad wieder aktiviert, sobald die Maus abgesteckt wird („remove“):

```
SUBSYSTEM=="input",KERNEL==
  "mouse[0-9]*",ACTION=="remove",
  ENV{DISPLAY}=":0",
  ENV{XAUTHORITY}="/home/sepp/.
  Xauthority",RUN:="/usr/bin/
  xinput --enable 12"
```

Diese Regeln sollte auf jedem Notebook mit Touchpad funktionieren, wenn die Pfadangabe „/home/sepp“ für den tatsächlichen User angepasst wird und die Ziffer „12“ am Ende durch die Kennzahl ersetzt wird, die der Befehl

```
xinput list
```

für das Touchpad liefert.

5. Backup bei USB-Anschluss: Das letzte Beispiel zeigt eine weitere Udev-Hürde. So kann zwar eine Regel

```
ACTION=="add", ATTRS{idVendor}
  =="1d6b", ATTRS{idProduct}
  =="0002", ENV{DEVTYPE}=="usb_
  device", RUN+="/[Pfad]/backup-
  start.sh"
```

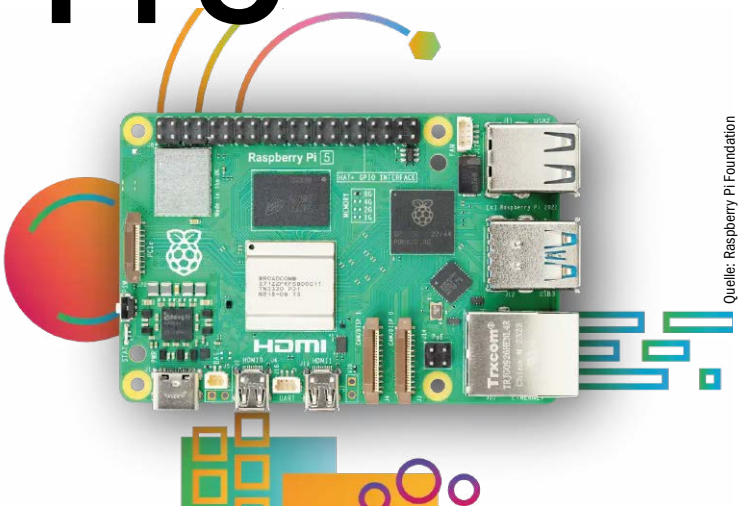
bei Anschluss eines definierten USB-Sicherungslaufwerks sofort ein Backup-Script auslösen, dieses wird aber scheitern, weil Udev solchen RUN-Tasks nur wenige Sekunden einräumt (wohl um zu vermeiden, dass Geräteanschlüsse das System blockieren). Das Script backup-start.sh muss daher mit

```
/[Pfad]/backup.sh &
```

ein weiteres Script starten, das dann den tatsächlichen Backupcode (etwa mit rsync, tar) auslöst. ■

Raspberry Pi 5

Überraschung zum Jahresende: Die Raspberry Pi Foundation hat ohne lange Ankündigung das Modell 5 des Raspberry Pi vorgestellt. Dieser verspricht bei Prozessor- und I/O-Leistung einen ordentlichen Satz nach vorne.



Quelle: Raspberry Pi Foundation

VON DAVID WOLSKI

Wie immer hielt sich die Raspberry Pi Foundation sowie Gründer und Chefentwickler Eben Upton bei Fragen nach neuen Modellen bedeckt, um dann unvermittelt einen ganz neuen Raspberry Pi vorzustellen. Vor etwas mehr als vier Jahren erfolgte die Präsentation des Raspberry Pi 4 und 400 ähnlich unerwartet. Dahinter steckt nicht nur Marketing per Überraschungseffekt, sondern auch eine Vertriebsstrategie: In der allgemeinen Nachschubkrise bei Halbleitern seit 2020 und der schlechten Verfügbarkeit von Raspberry-Platinen bis in dieses Jahr hinein wäre eine lange Liste an Vorbestellungen eine schwere Geduldsprobe geworden.

Erste Benchmarks des Herstellers

Vier Jahre sind bei den Halbleitern, ARM-Prozessoren und SoCs (System-on-Chip) von Ein-Platinen-Computern eine lange Zeit. Und so sind die Erwartungen an den Raspberry Pi 5 entsprechend hoch. Zu einem praktischen Test mit Benchmarks unter realen Bedienungen kommen wir erst in der kommenden LinuxWelt. Die Vorstellung der Raspberry Pi Foundation zeigt aber schon, welche Verbesserungen sich die fünfte Generation der Platine vorgenommen hat.

Wie nicht anders zu erwarten, beschert der neuere ARM-Prozessor, ein Broadcom BCM2712 mit vier Kernen und bis zu 2,4 GHz Taktfrequenz, ein ansehnliches Leistungsplus. Die veröffentlichten Benchmarks der Raspberry Pi Foundation (*www.raspberrypi.com/news/benchmarking-raspberry-pi-5*) bescheinigen der fünften Generation bei der Messung mit Geekbench ein Leistungsplus um 220 Prozent gegenüber dem Vorgängermodell 4. Die RAM-Bausteine, nun vom Typ LPDDR4X, sind mit etwas mehr als 4,2 GHz getaktet, beim älteren Raspberry Pi 4 noch mit maximal 3,2 GHz.

Bei der Grafikeinheit des System-on-Chip geht es von Videocore VI zur Version VII, die zwei Monitore mit 4K-Auflösung über Micro-HDMI bedienen kann. Unterstützt werden dabei die Standards Open GL ES 3.1 und Vulkan 1.2 für die hardwarebeschleunigte Grafikausgabe, wobei die Raspberry Pi Foundation die dafür nötigen Patches erst kurz vor der Vorstellung der neuen Platine an den Linux-Kernel und die Grafikbibliothek Mesa weitergegeben hat. In diesem Punkt wird es also noch ein paar Monate zum Kernel 6.7 dauern, bis der Raspberry Pi 5 sein ganzes Potenzial zeigen kann.

RP1: Eine echte Southbridge

An Anschlüssen präsentiert der neue Raspberry Pi einen verbesserten Micro-SD-Slot, der bis zu 100 MB pro Sekunde Durchsatz liefern soll. Die Aufteilung der USB-Ports ist mit zwei USB-3-Anschlüssen und zwei USB-2-Buchsen nur augenscheinlich gleich geblieben, denn bei USB 3 liefert der neue Raspberry Pi jetzt simultan bis zur vollen USB-3-Geschwindigkeit von 5 Gbit pro Sekunde.

Das Highlight des Raspberry Pi ist aber eine neu entwickelte I/O-Einheit als eigenständige Southbridge wie auf PC-Hauptplatinen. Dieser Chip mit der Bezeichnung RP1 dürfte der aufwendigste Teil der Entwicklung gewesen sein, deren Kosten die Foundation mit 25 Millionen US-Dollar beziffert. Der RP1 verschafft der Platine nun PCI Express über insgesamt vier PCIe-2.0-Lanes für flotte Datenträger wie SSDs. Die Raspberry Pi Foundation ist bei der Veröffentlichung der Spezifikationen zum RP1-Chip noch zurückhaltend. Den Anschluss von SSDs wird erst weiteres Zubehör im Frühjahr 2024 möglich machen, das wiederum die Unterstützung von Kernel-Modulen braucht.

Der neue Chip und die zwei unabhängigen USB-Controller verlangen nach mehr Leistung: Der Raspberry Pi 5 benötigt ein geändertes Netzteil mit mindestens 27 Watt. Empfohlen wird ferner ein aktiver Kühler. ■

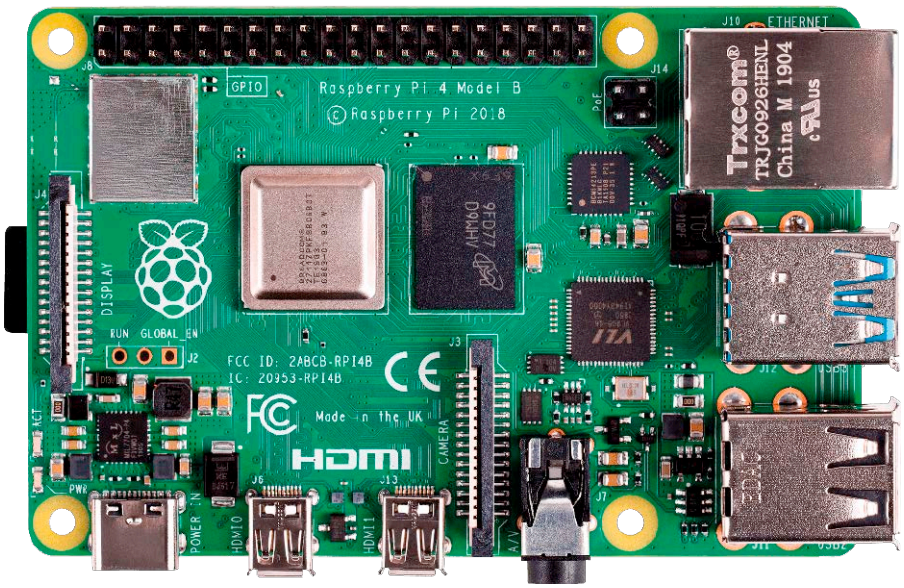
STECKBRIEF: RASPBERRY PI 5

ARM Prozessor Cortex-A76 (4× 2,4 GHz)
2× USB 2, 2× USB 3
1× Gigabit-Ethernet
Wi-Fi 7 (802.11ac)
Bluetooth 5.0
2× Micro-HDMI
Preis ohne Zubehör:
circa 70 Euro mit 4 GB RAM,
93 Euro mit 8 GB RAM
Versand: *https://www.berrybase.de*
Webseite:
www.raspberrypi.com/products

10 Jahre Raspberry Pi

Die Gratulation zum zehnten Geburtstag des Ein-Platinen-Rechners kann nicht anders als begeistert ausfallen. Der Raspberry Pi hat seit 2012 eine ehemals nischige Geräteklasse im Massenmarkt etabliert und mit seinem Erfolg zahlreiche Nachahmer inspiriert.

VON HERMANN APFELBÖCK



Der Rechnerwinzling Raspberry war 2012 als Entwicklerboard und Programmiereinstieg konzipiert, hätte aber in dieser Rolle gewiss keine 40 Millionen Exemplare verkauft. Der Raspberry und seine Konkurrenten haben sich zu preisgünstigen Heimservern entwickelt und sich als attraktive Alternative zu NAS-Geräten etabliert. Dem aktuellen Status quo mit dem Raspberry Pi 4 darf man bescheinigen, dass es wenige Produkte mit einem derart überzeugendem Preis-Leistungs-Verhältnis gibt. Trotzdem wäre es falsch, die Platine als ein Must-have-Produkt zu preisen. Wir nehmen zehn Jahre Raspberry zum Anlass, ein herausragendes Produkt zu porträtieren, dabei aber auch Fehlentwicklungen und Fehleinschätzungen zu benennen.

Der Weg zur aktuellen Version 4

Der Raspberry Pi begann 2012 als ein Arduino-ähnliches Board mit einer Einkern-CPU (700 MHz) und 256 MB RAM. Eine frühe Modellunterscheidung führte zur kleineren A-Reihe ohne Netzwerkadapter und zum etwas größeren Formfaktor der B-Reihe, die von Beginn an einen Ethernet-Port anbot. Wer heute vom Raspberry Pi spricht, meint fast immer ein Raspberry-Modell B. Die kleinere A-Platine wurde mit der Raspberry-Version 3 praktisch (wenn auch nicht offiziell) aufgegeben und durch die winzigen Sondermodelle Raspberry Zero (ab 2015) und Pico (ab 2021) kompensiert. Beim aktuellen Raspberry Pi 4 B ist die Modellkennzeichnung „B“ mittlerweile hinfällig, weil alternativlos.

Die ersten Versionsschritte der Modellreihe B hatten vor allem sukzessive RAM-Erweiterung und CPU-Beschleunigung im Fokus. Beim – unfairen – Vergleich des ersten Raspberry 1 mit einem maximal ausgestatteten Raspberry 4 von heute ergibt sich ein Faktor 32 beim Arbeitsspeicher (256 MB gegenüber acht GB) und sogar ein Faktor 60 bei der CPU-Leistung (0,2 gegenüber 13,5 Gigaflops). Spätestens mit Version 2 (2015), die mit einem GB RAM ausgestattet war und mit übertakteter CPU die Ein-GHz-Hürde nahm, blieb es nicht mehr bei kleinen Daten- und Webserver-Diensten und der Platinenrechner wurde auf Desktoptauglichkeit geprüft.

Die Raspberry-Version 3 im Jahr 2016 brachte mit neuer Vierkern-CPU (ARM Cortex-A53) erneut eine signifikante Leistungssteigerung und hatte nun auch erstmals neben der Ethernet-Schnittstelle einen WLAN-Chip dabei.

Während es also bei der Leistungsfähigkeit (CPU, RAM) und Alltagstauglichkeit (WLAN) kontinuierlich voranging, stagnierten die I/O-Schnittstellen über viele Jahre: Für das von vielen Nutzern bevorzugte Einsatzgebiet als Homeserver blieb es bis 2018 beim relativ langsamen Fast Ethernet (100 MBit/s) und bei USB 2.0.

Das Versionsupgrade Raspberry Pi 3 B+ im Jahre 2018 war ein halbgarer Kompromiss, denn der lang erhoffte Gigabit-Ethernet-Port wurde an USB 2.0 gekoppelt, was die möglichen 1000 MBit/s auf USB-2.0-Geschwindigkeit drosselte, also auf etwa 300 MBit/s (circa 30 MB/s).

Keine Frage: Als Bastlerplatine mit seinen flexiblen Möglichkeiten, die GPIO-Pins selbst zu programmieren oder einfach fertige HAT-Erweiterungsplatinen (Hardware Attached on Top) aufzustecken, war der Raspberry Pi auch schon vor Version 4 ein faszinierendes und dabei preisgünstiges Produkt. Auch alle Serveroptionen, die mit durchschnittlichem Datendurchsatz auskommen, wie etwa Intranet-Webserver oder kleine Clouddienste, konnte die Platine schon mit seinen Vorgängerversionen bedienen. Nicht zu vergessen sind die erstaun-

lichen Fähigkeiten als Videospieler, die der Raspberry Pi seit jeher dem Broadcom-Videocore-Chip verdankt: Als Mediaplayer, Streamingdienst, aber auch bei der Desktop-Grafikausgabe ist der Raspberry besser als viele Platinenkonkurrenten mit scheinbar leistungsstärkeren Komponenten.

Trotz allem blieb vor dem aktuellen Raspberry Pi 4 (seit Juni 2019) so manches Serverprojekt in einem zwar tolerierbaren, aber gefühlt defizitären Bereich. Erst der Raspberry Pi 4 mit Gigabit-Ethernet und USB 3.0, verbesserter CPU und GPU sowie skalierbarem RAM von zwei bis acht GB ist gewissermaßen die Einlösung (fast) aller Versprechen, die ältere Raspberry-Versionen noch überfordert hatten.

Der Raspberry Pi 4: Leistung und Preis

Seit fast drei Jahren ist der tadellose Raspberry Pi 4 auf dem Markt. Zum Nachfolger mit der Versionsziffer 5 gibt es nach wie vor weder konkrete Ankündigungen, geschweige denn einen Erscheinungstermin. Tatsächlich muss man schon sehr kritisch suchen, wo sich das aktuelle Modell noch signifikant verbessern ließe: Gut – der WLAN-Chip ist nur mittelmäßig, aber durchaus alltagstauglich. SATA ist auf der Platine schon aus Platzgründen kaum realisierbar, außerdem gibt es bereits HAT-Lösungen zum Aufstecken und natürlich USB-to-SATA-Kabelverbindungen. Daher spricht viel dafür, dass sich Version 5 nach dem großen Wurf des Vorgängers wieder mit einer moderaten Leistungsevolution bescheiden wird.

Der aktuelle Raspberry Pi 4 kann jede Rolle als Homeserver übernehmen, auch mehrere gleichzeitig – etwa als Samba-Datenserver und als Webserver. Seine Tauglichkeit als Desktopsystem bleibt hingegen eingeschränkt: Einen Film mit VLC ansehen oder mit dem Browser ins Web gehen – das geht durchaus flüssig. Multitasking – also etwa im Hintergrund das System zu aktualisieren und gleichzeitig Medien zu nutzen –, überfordert die Platine hingegen. Die Aussage von Eben Upton, Gründer der Raspberry Pi Foundation, dass der Raspberry Pi 4 als Allzweck-PC tauge, ist daher eher kritisch zu bewerten.

Daher halten wir auch das für den Desktopeinsatz spezialisierte Sondermodell Raspberry Pi 400 tendenziell für einen Irrweg: Der Pi 400 integriert die Platine in eine Tastatur und muss dann nur noch durch einen Monitor zur vollwertigen Arbeitsstation ergänzt werden.

In Tastatur integrierter Raspberry: Das Sondermodell Pi 400 kostet etwa 100 Euro und benötigt nur noch einen Monitor. Die Ausrichtung auf den Desktopbetrieb ist aber grenzwertig.

Quelle otto.de

Bundles sind nicht verkehrt, zumal die pure Platine aktuell praktisch ausverkauft ist. Das hier angebotene Set für 189 Euro bietet aber nur Zubehör minderer Qualität und ist um 90 Euro zu teuer.

Halten wir fest: Der Raspberry Pi 4 taugt notfalls als Allzweck-PC oder als Zweitsystem, ist uneingeschränkt als NAS-Datenserver, als Webserver und als Medienlieferant zu empfehlen und eröffnet mit Kameraschnittstelle und HAT-Erweiterungen zahlreiche Spezialisierungen (etwa Wettersensoren, Gebäudeüberwachung, Hi-Fi, SATA, DVB-TV, Power-over-Ethernet, Mini-Display). Der Stromverbrauch ist legendär gering und liegt selbst unter Hochlast nur bei etwa fünf Watt.

Was darf eine derart flexible Hardware kosten? Wir fragen deshalb, weil mittlerweile Bundles angeboten werden, die locker über 200 Euro liegen. Was Sie wirklich in jedem Fall brauchen, ist aber nur Folgendes:

- die Platine selbst (vier GB sollten genügen)
- das passende Netzteil (Netzteile älterer Pi-Modelle passen nicht)
- eine schnelle SD-Karte (UHS) mit mindestens 16 GB
- ein Gehäuse mit Kühlfunktion (optimal: Aluminiumgehäuse „Flirc“)

Eventuell kommt noch ein Micro-HDMI-Kabel hinzu, falls für die Ersteinrichtung oder dauerhaft ein Monitor benötigt wird. Bundles mit diesen Komponenten gibt es im Prinzip noch unter 100 Euro, dies aber selten in der wünschenswerten Qualität aller Teile. Ein Raspberry mit dem notwendigen und dabei hochwertigen Zubehör ist daher heute nicht mehr ganz das 60-, 70-Euro-Schnäppchen wie vor zehn Jahren, sondern liegt eher bei 120 bis 150 Euro. Damit bleibt das Preis-Leistungs-Verhältnis dieser Platine aber weiterhin unübertroffen. ■

Raspberry Pi 400 – Desktop für Bastler?

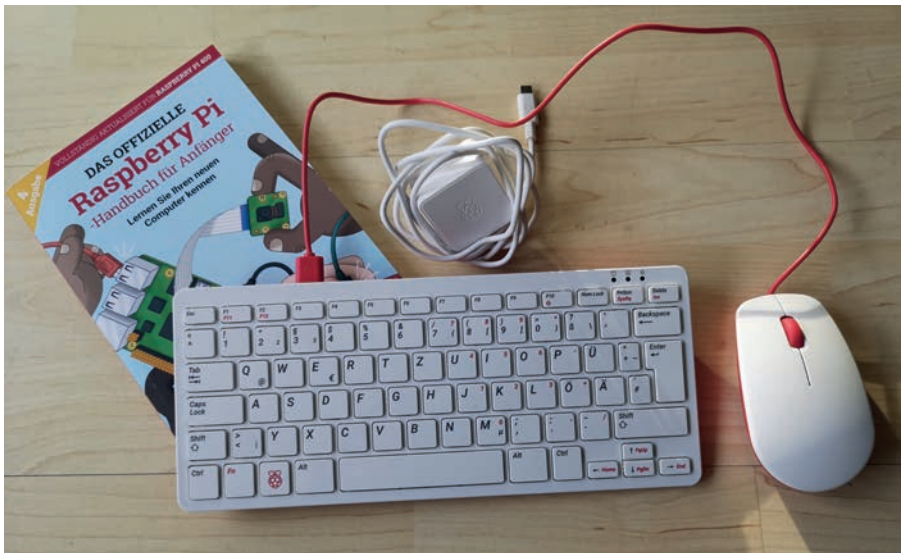
Mit dem Pi 400 hat die Raspberry-Foundation einen kleinen Rechner gebaut, der in erster Linie den Bildungssektor im Blick hat. Für sehr wenig Geld gibt es einen vollwertigen kleinen Desktoprechner. Wir haben uns das Gerät angesehen.

VON STEPHAN LAMPRECHT

Man nehme eine Platine, versorge sie mit Anschlüssen und baue sie in ein Gehäuse mitsamt Tastatur ein. Das Konzept des Raspberry Pi 400 ist nicht neu. Computerveteranen werden sich an den Commodore C64 erinnern. Auch der Pi 400 will zu einem erschwinglichen Preis moderne Computertechnik anbieten, damit vor allem Schüler ihre ersten Schritte in Sachen Informatik absolvieren.

Im Kit ist alles Notwendige dabei

Im Fachhandel wird der Pi 400 in zwei Varianten angeboten. Das Kit (unbedingt darauf achten, dass Sie die DE-Variante erwerben) umfasst alles, was zum sofortigen Start benötigt wird. In der kompakten Verpackung sind der Rechner, eine Maus, ein Netzteil, eine Speicherkarte mit Betriebssystem sowie ein HDMI-Kabel und ein Handbuch zusammengepackt. Es ist vielleicht Jammern auf hohem Niveau, aber das HDMI-Kabel wirkt etwas steif und besonders lang ist es auch nicht. Aber natürlich kann mittels eines passenden Adapters, der die Minibuchse in das große Format verwandelt, jedes beliebige Kabel angeschlossen werden. Es wird also nur noch ein passender Monitor benötigt und schon kann es zum Preis von rund 100 Euro losgehen (ohne Monitor). Unterschiedliche Preise für das Kit ergeben sich in erster Linie durch unterschiedliche SD-Karten-Kapazitäten. Günstiger ist nur die Bulkware, die lediglich den Rechner selbst bietet. Wer Maus, Kabel und Netzteil besitzt, kann damit etwas Geld sparen.



Raspberry Pi 400: Die einfachste Wahl ist ein komplettes Kit für etwa 100 Euro. Hier ist alles dabei, was für den Start benötigt wird: HDMI-Monitor anschließen und los geht's!

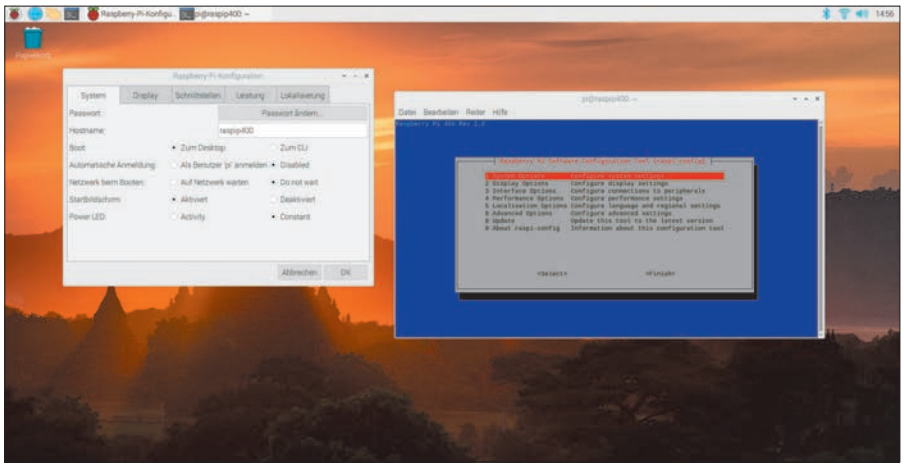
Einschränkungen für Bastler: Ist der Pi 400 der erste Raspberry im Haushalt, werden die Einschränkungen gegenüber der üblichen Platine nicht auffallen. Auf der Rückseite der „Tastatur" sind alle Anschlüsse verbaut. Von rechts nach links sind dies eine Kensington-Buchse zur Diebstahlsicherung, ein Ethernet-Anschluss, ein USB-Anschluss 2.0, zwei USB-Anschlüsse 3.0, einmal USB-C für die Stromversorgung, zwei Mini-HDMI-Buchsen sowie der Einschub für die Micro-SD-Karte. Unter einer Gummiabdeckung befindet sich die GPIO-Leiste. Für ambitionierte Bastler bedeutet dies im Vergleich zum Pi 4 eine deutliche Einschränkung. Es fehlen der zweite USB-Anschluss Typ 2.0 sowie der kleine Klinkenstecker für Audiowiedergabe, Kamera (CSI) und Display (DSI). Auch PoE (Power-over-Ethernet) ist mit dem Pi 400 nicht möglich. Die GPIO-Leiste ist gedreht vorhanden, aber Orientierung auf dem Gehäuse bieten die gekennzeichneten Pins 1 und 40. Am pragmatischsten dürfte es sein, die Anschlüsse über ein Flachbandkabel nach außen zu führen, um am anderen Ende ein Steckboard anzuschließen.

Aufgrund der Bauform lassen sich die beliebten Aufsteckboards (HAT, Hardware Attached on Top) nicht einsetzen. Der Pi 400 taugt also nicht dazu, beispielsweise mit einem DAC-Board das Signal der Stereoanlage per WLAN zu verteilen. Alle im Handel erhältlichen Hi-Fi-Boards sind als HAT konzipiert. Die Bauform schmälert also die Einsatzmöglichkeiten der Platine, die hier eindeutig als Desktop konzipiert ist. Das Fehlen der 3,5-Millimeter-Buchse

lässt sich dagegen verschmerzen, weil das Audiosignal auch via HDMI oder USB abgeschöpft werden kann.

Vier GB RAM sind fix: Neben der Bauform unterscheidet sich der Pi 400 vom normalen Pi 4 auch in Sachen Hardware. Zwar kommt der gleiche ARM-Prozessor zum Einsatz, doch ist die Vierkern-Broadcom BCM2711 im Pi 400 in einer neueren Version verbaut. Die bietet statt 1,5 GHz standardmäßig 1,8 GHz. Während es beim Raspberry Pi 4 allerdings bis zu acht GB RAM gibt, sind im 400 stets vier GB verbaut. Das sollte aber den meisten Nutzern genügen.

Zielgruppe: Flexibler für Bastlerprojekte dürfte nach wie vor eine nackte Platine sein, etwa wenn es um Kamera- oder Audioprojekte geht. Grundsätzlich gefällt der kleine Computer aber: Für Office und Internet genügt der Pi 400 auf jeden Fall. Preiswerter kann man in die Linux-Welt kaum einsteigen. Auch im Kinder- und Jugendzimmer macht der 400er eine gute Figur. So laufen darauf beispielsweise alle von uns schon einmal vorgestellten Anwendungen für das Homeschooling auch auf dem kompakten Computer. Wer den Pi 400 als ersten „richtigen" Computer verschenken will, sollte zum Kit greifen, denn das beiliegende Handbuch ist so geschrieben, dass auch jüngere Leser damit zurechtkommen werden. Mit zunehmenden Alter wachsen auch die Ansprüche, deswegen dürften Schüler der Mittel- und Oberstufe wohl weniger begeistert sein. Für eine Spielemaschine ist der Desktop zu schwach und intensives Videoconferencing dürfte ihn auch an seine Grenzen treiben. Mit seinen kompakten Abmessungen und der Ähnlichkeit mit Rechnern wie dem C64 werden aber Retrogamer am Pi 400 viel Freude haben.



Nach Anschluss des Netzteils startet der Desktop sofort durch. Mit seinem Standardsystem Pi-OS ist der Pi 400 ein vollwertiger Rechner für Internet und Office.

Eines der buntesten und vielseitigsten Systeme für den Raspberry Pi: Twister-OS ist ideal für Retrogamer und bringt sogar grafische Hilfe zum Übertakten mit.

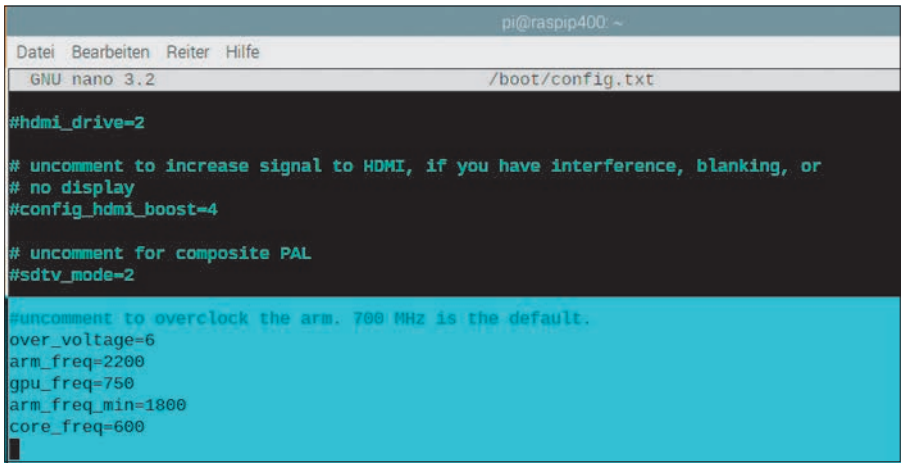
Kompakt und solide gearbeitet

Wer den Pi 400 aus der Schachtel holt, wird wahrscheinlich angenehm vom Gewicht überrascht sein. Auf den ersten Blick sieht der viele Kunststoff alles andere als stabil aus, aber der durch den integrierten Kühlkörper und die Anschlüsse auf einer Seite resultierende Schwerpunkt sorgt dafür, dass der kleine Rechner auf dem Schreibtisch während der Eingaben nicht herumrutscht. Von seinen Abmessungen (circa 30 × 12 Zentimeter) ist der Pi 400 erstaunlich kompakt. Die Größe des Gehäuses entspricht etwa dem Magic Keyboard von Apple. Apropos Tastatur: Die Tasten sind aus Kunststoff, die Beschriftung einfach aufgedruckt. Die Tasten besitzen einen recht guten Druckpunkt mit niedrigem Hub, wie von Notebooktastaturen gewohnt. Damit lassen sich tatsächlich auch längere Texte bearbeiten (dieser Artikel entsteht gerade auf dem Pi 400). Wer von einer großen Tastatur umsteigt, wird sich trotzdem etwas umgewöhnen müssen.

Eine Besonderheit ist der erstmals verbaute Geräteschalter. Mittels Fn-F10 wird der Raspberry Pi 400 ein- und ausgeschaltet. Aber Achtung: Direkt nach dem Auspacken aus dem Kit ist die SD-Karte mit Betriebssystem bereits eingesteckt. Wird der Rechner mit Strom versorgt, startet er sofort durch. Ist in diesem Moment noch kein Display angeschlossen, wird dies auch nicht erkannt. Der Pi wäre somit nur via Terminal zu erreichen. Damit das Gerät eingerichtet werden kann, ist es also von Vorteil, erst alle physischen Verbindungen vor dem ersten Start herzustellen. Hier zeigt sich eine weitere kleine Schwäche: Die Buchsen sind nicht beschriftet. Und bei der Ersteinrichtung blieb der Bildschirm dunkel, weil offenbar der falsche Ausgang genutzt wurde. Erst beim Anschluss an die Buchse, die sich direkt neben dem SD-Kartenschlitz befindet, wird ein Bild sichtbar. Dabei könnte es sich aber um ein bereits gefixtes Problem handeln. Denn nach einem Update des Systems spielte der verwendete Anschluss keine Rolle mehr.

Die Ersteinrichtung ist problemlos

Findet die Platine beim ersten Systemstart ein Display, verläuft der Start einsteigerfreundlich. Nach wenigen Sekunden wird bereits der Desktop sichtbar und führt den



Mit zwei Zeilen Code übertakten Sie den Pi 400. Dank der großen Kühlkörper sollte dies keine Probleme bereiten.

Nutzer durch die ersten Schritte, also die Auswahl des WLANs und die Vergabe eines Passworts für den Nutzer. Danach rät das System dazu, erst einmal eine automatische Aktualisierung durchzuführen. Das ist bei allen Betriebssystemen immer eine gute Idee, noch dazu in diesem Fall, wo es um völlig neue Hardware geht. Zum Einsatz kommt Raspberry-Pi-OS, also das ehemals als Raspbian bekannte System.

Alternative Betriebssysteme: Ein großer Vorteil der Pi-Plattform liegt darin, durch das Flashen einer SD-Karte rasch ein anderes System nutzen zu können. Genau das haben wir auch mit dem Pi 400 ausprobiert. Die Erfahrungen damit waren zum Teil schlecht, zum Teil positiv. Das von Microsoft für die ARM-Plattform gedachte Windows lässt sich zwar installieren, mehr aber auch nicht. „Out of the Box" läuft hier nichts. Es bedarf also einer gehörigen Portion Enthusiasmus, um hier ein System zusammenzustellen, das dann aber kein vollwertiges Windows ist. Und als Zentrale für IoT-Projekte ist der 400 wegen des Formfaktors zu schade.

Die Desktopvariante von Ubuntu 20.10 für den Raspberry dagegen funktioniert. Gefühlt ist dieser Desktop aber deutlich langsamer als das angestammte Pi-OS. Wer aber auf seinen gewohnten Desktop nicht verzichten will, kann auch Ubuntu auf der Plattform nutzen. Sehr positiv waren die Erfahrungen mit Twister-OS (*https://twisteros.com/*). Zwar haben die Entwickler keine separate Version für den 400 produziert, aber die bekannte Variante für den normalen Pi 4 kann problemlos installiert werden. Gefällig ist dabei nicht nur die Optik. Was für Twister-OS in erster Linie spricht, ist die Zusammenstellung der Pakete, denn viele Emulatoren und Umgebungen für das Retrogaming sind hier von Haus aus dabei. Das erspart einige Installationsarbeit. Da Twister-OS im Kern auf Raspbian basiert, lassen sich Konfigurationsarbeiten wie gewohnt durchführen. Wer also eher eine kleine Spielemaschine sucht, ist mit diesem System bestens bedient.

Übertakten und Sound ausgeben

Wer auf dem Pi 400 spielen will, kann die ohnehin höhere Taktung im Vergleich mit der Platine noch einmal ausreizen. Wegen seiner Bauform ist der Pi 400 für das Übertakten prädestiniert, denn der Kühlkörper reicht fast über die gesamte Breite der Tastatur. Wenn Sie Ihren Rechner mit mehr Spannung höherer Taktung betreiben, tun Sie dies auf eigene Gefahr.

Das Übertakten erledigen Sie in einer Konfigurationsdatei des Systems. Öffnen Sie ein Terminal und geben Sie dort

```
sudo nano /boot/config.txt
```

ein. Suchen Sie im Editor den Eintrag „#uncomment to overclock". Ersetzen Sie die vorhandenen Werte und Einträge mit den nachfolgenden Zeilen. Die Kombination hat sich in unseren Tests als stabil erwiesen und kitzelt auch nicht das allerletzte Quäntchen aus der Hardware:

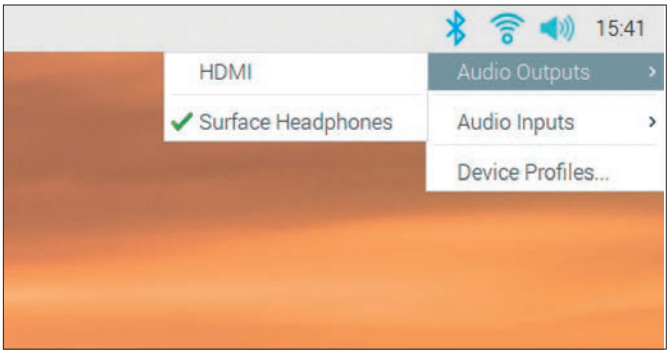
```
over_voltage=6
arm_freq=2200
```

Mit Strg-O und Strg-X speichern Sie und verlassen den Editor. Sie können den Rechner dann neu starten, um die Optionen zu verwenden.

Das beigefügte Netzteil liefert stabil die notwendige Leistung. Sollte der Rechner wider Erwarten nicht starten oder nicht stabil laufen, können Sie die Datei „config.txt" auf der SD-Karte auch mit einem anderen System editieren. Kommentieren Sie die Einträge notfalls einfach wieder aus. Mit *watch -n 1 vcgencmd measure_clock arm* in einem Terminal können Sie sich die aktuelle Taktrate anzeigen lassen. Wundern Sie sich nicht, wenn der Wert zunächst niedrig erscheint. Dann wird gerade nicht so viel Leistung benötigt. Öffnen Sie weitere Programme und arbeiten Sie damit, dann werden die Werte nach oben gehen.

Audioausgabe: Wie bereits erwähnt, besitzt der Pi 400 keine Kopfhörerbuchse. Sie können dennoch Audiosignale auf externen Systemen wiedergeben. Sowohl eine ältere Soundbar als auch ein Anker-BT-Lautsprecher konnten problemlos mit dem Pi 400 gekoppelt werden. Bevor ein Audiosignal zu hören ist, muss aber über das Kontextmenü des Lautsprechersymbols aus der oberen Navigation der externe Lautsprecher gewählt werden. Hier ist HDMI vorbelegt.

Allerdings gab und gibt es wohl Probleme bei der Wiedergabe mit Chromium, was aber nicht direkt am Betriebssystem oder dem Rechner liegt. Die Wiedergabe der gleichen Quelle mit einem anderen Player wie dem VLC funktioniert. Sofern Sie mit Chromium keinen Sound hören, ist ein Softwareupdate zu empfehlen, oder Sie weichen auf eine Alternative aus. ■



Via Bluetooth können Sie das Audiosignal auch ohne Buchse ausgeben lassen. Ein häufiger Fehler: Sie müssen HDMI für die Audioausgabe ausschalten.

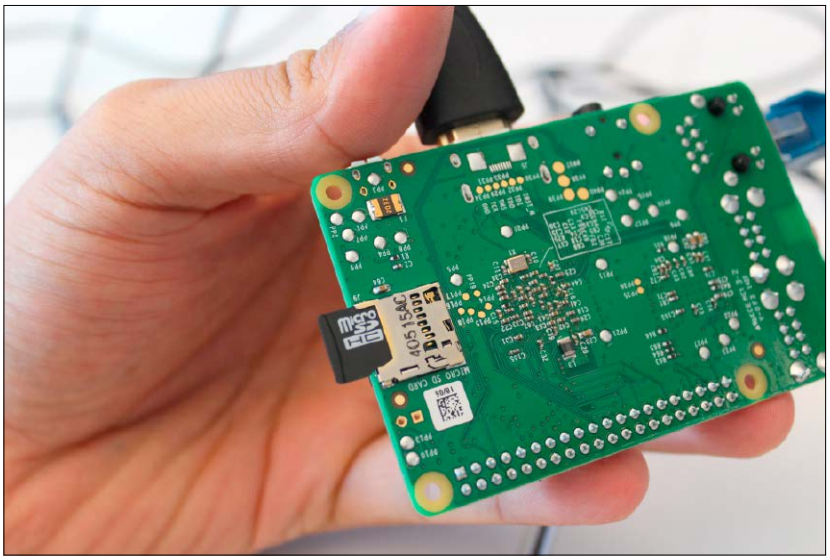
Tipps für den Raspberry Pi

Aufgrund seiner speziellen Hardware ist beim Raspberry Pi einiges anders als beim herkömmlichen Linux-PC. Vor allem bei der Installation und Konfiguration gibt es deutliche Unterschiede.

Von **Thorsten Eggeling**

Der Raspberry Pi ist klein, arbeitet geräuschlos und kostet nur etwa 40 Euro. Das aktuelle Modell Raspberry 3 ist mit einem Ethernet-Anschluss, vier USB-2.0-Ports, WLAN und Bluetooth ausgestattet. Es gibt allerdings nur ein GB RAM und der ARM-Prozessor ist nicht besonders schnell. Trotzdem eignet sich das Gerät für Desktopanwendungen und als Server. Eine gute Figur macht der Raspberry Pi auch als Multimedia-PC, denn dank Hardwarebeschleunigung ist sogar die Wiedergabe von HD-Videos möglich.

Für den Raspberry Pi gibt es speziell für den ARM-Prozessor angepasste Linux-Versionen, bei deren Installation einige Besonderheiten zu beachten sind. Wenn das System läuft, gibt es jedoch kaum Unterschiede zu Linux auf einem x86-PC, außer wenn es die spezielle Raspberry-Hardware betrifft. Unsere Tipps basieren auf der verbreiteten Raspberry-Distribution Raspbian und einem Raspberry Pi 3. Die meisten Tipps sollten aber so oder ähnlich auch mit älteren Modellen und anderen Distributionen funktionieren.



Quelle: pcworld.com

Mini-PC: Der Raspberry Pi ist nur so groß wie eine Scheckkarte, bietet aber ausreichend Leistung für viele Einsatzgebiete. Das Betriebssystem findet auf einer SD-Karte Platz.

1. Die richtige SD-Karte finden

Der Raspberry Pi bootet das Betriebssystem von einer SD-Karte. Wie schnell das Gerät arbeiten kann, hängt auch von den maximalen Transferraten der Karte ab. SD-Karten wurden für Kameras und große Bilddateien entwickelt. Häufige Schreibzugriffe und viele kleine Dateien, wie sie für Betriebssysteme typisch sind, bringen eine SD-Karte an ihre Leistungsgrenzen. In Ermangelung technischer und preislicher Alternativen blieb den Raspberry-Entwicklern aber nichts anderes übrig, als einen SD-Kartenleser einzubauen. In der Praxis ist die Lebensdauer einer SD-Karte jedoch ausreichend lang und Lese- und Schreibvorgänge laufen für fast alle Anwendungsbereiche schnell genug ab. Auf dem Raspberry Pi 2 befindet sich seit Modell A+ ein Micro-SD-Kartenleser. Die Vorgänger waren mit einem SD-Kartenleser ausgestattet. Die kleineren Micro-SDs sollen für mehr Stabilität sorgen, denn bei den älteren Modellen wurden die Kontakte des Kartenlesers als Quelle für häufige Abstürze ermittelt.

SD-Karten der Klasse 10 bieten beim mindestens zehn MB pro Sekunde, beim Lesen lassen sich Geschwindigkeiten von bis zu 90 MB/s erreichen („sequenziell“). Das gilt aber nur für große Dateien, die Sie beispielsweise von der SD-Karte auf den PC kopieren. Der Raspberry Pi liest maximal nur mit etwa 20 MB/s, unabhängig von der Geschwindigkeit der Karte. Ein Betriebssystem fordert vom Speichermedium jedoch meist viel kleine Dateien an, wobei die Transferrate beim Lesen von 4K-Blöcken („random read“) auf unter zehn MB/s absinkt, beim Schreiben sind es nur noch um die zwei MB/s.

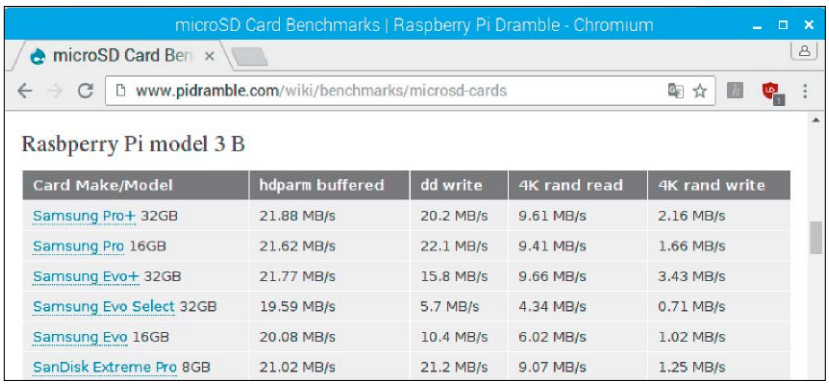
Trotzdem empfiehlt sich eine Karte der Klasse 10, weil sich dann am PC die Installationsimages schneller auf die Karte kopieren lassen (-> Punkt 4). Außerdem benötigen Backups weniger Zeit (-> Punkt 7). Im Hinblick auf Qualität, Haltbarkeit und Leseleistung sollten Sie zu SD-Karten von Markenherstellern wie Samsung oder Sandisk greifen (-> Punkt 2). In der Regel sind 32 GB völlig ausreichend, minimal sind acht GB erforderlich.

2. So schnell ist die SD-Karte wirklich

Aktuelle SD-Karten bieten Leseraten um die 90 MB/s. Der Raspberry Pi kann zwar nur deutlich weniger nutzen, trotzdem gibt es deutliche Unterschiede bei der Leistung.

Auf der Webseite *www.pidramble.com* finden Sie aktuelle Tests von SD-Karten für den Raspberry Pi. Klicken Sie auf „Benchmarks“ und dann auf „microSD Card Benchmarks“. Die Tabellen zeigen nicht nur SD-Karten, sondern teilweise auch USB-Sticks für den Vergleich. Beim Test mit hdparm (sequenzielles Lesen) liegen die Karten meist dicht beieinander. Deutlicher ist das Bild beim wichtigeren Test „4k random write“. Die schnellste SD-Karte liefert im Raspberry Pi 3 eine knapp fünfmal höhere Schreibleistung als die langsamste. Sehr gute Werte zeigen Samsung Pro + mit 32 GB und Sandisk Extreme mit 16 GB, die mit etwa 28 Euro und 13 Euro aber auch im oberen Preissegment liegen.

Wer die Geschwindigkeit der eigenen SD-Karte nach der Installation von Raspbian (-> Punkte 3 und 4) prüfen möchte, kann den Benchmarktest selbst durchführen und mit den Werten von *www.pidramble.com* vergleichen.



Card Make/Model	hdparm buffered	dd write	4K rand read	4K rand write
Samsung Pro+ 32GB	21.88 MB/s	20.2 MB/s	9.61 MB/s	2.16 MB/s
Samsung Pro 16GB	21.62 MB/s	22.1 MB/s	9.41 MB/s	1.66 MB/s
Samsung Evo+ 32GB	21.77 MB/s	15.8 MB/s	9.66 MB/s	3.43 MB/s
Samsung Evo Select 32GB	19.59 MB/s	5.7 MB/s	4.34 MB/s	0.71 MB/s
Samsung Evo 16GB	20.08 MB/s	10.4 MB/s	6.02 MB/s	1.02 MB/s
SanDisk Extreme Pro 8GB	21.02 MB/s	21.2 MB/s	9.07 MB/s	1.25 MB/s

Leistungsunterschiede: Beim sequenziellen Lesetest (hdparm) schneiden alle SD-Karten gut ab. Deutliche Unterschiede gibt es jedoch beim zufälligen Schreiben kleiner Blöcke.

3. Betriebssysteme über Noobs installieren

Die Installation von Systemen auf dem Raspberry ist mit wenigen Mausklicks erledigt. Sie benötigen dazu einen SD-Kartenleser am PC, über den Sie die SD-Karte unter Linux befüllen. Am einfachsten ist die Verwendung von Noobs, das Sie im Downloadbereich von *www.raspberrypi.org* herunterladen. Es gibt zwei Varianten: Noobs Lite ist nur etwa 30 MB groß und der Download des gewünschten Systems erfolgt erst später auf dem Raspberry Pi. Verwenden Sie diesen Download vorzugsweise, wenn Sie ein anderes System als Raspbian installieren möchten. Noobs ist 1,2 GB groß und enthält bereits das Abbild für Raspbian, sodass der spätere Download entfällt. Über beide Noobs-Varianten lassen sich zurzeit neben Raspbian auch Libre Elec, Raspbian Lite, Lakka_RPi2, OSMC und Windows 10 IoT Core herunterladen und installieren.

Die SD-Karte muss für Noobs mit dem Dateisystem FAT32 formatiert sein. Sie sollten jede SD-Karte neu formatieren, weil der Raspberry Pi sonst manche Karten nicht als bootfähig erkennt. Starten Sie unter Linux das Programm Gparted. Sollte es nicht installiert sein, holen Sie das mit folgender Befehlszeile nach:

```
sudo apt install gparted
```

Wählen Sie den Kartenleser in der Liste an der rechten Seite des Fensters aus. Kontrollieren Sie die Einstellung genau, damit Sie nicht versehentlich das falsche Laufwerk formatieren. Sollte die SD-Karte eingehängt sein, wählen Sie im Kontextmenü „Aushängen“. Gehen Sie im Menü auf „Gerät -> Partitionstabelle erstellen“. Hinter „Neuen Partitionstabellentyp auswählen“ muss „msdos“ eingestellt sein. Klicken Sie auf „Anwenden“. Danach erstellen Sie über den Kontextmenüpunkt „Neu“ eine primäre FAT32-Partiton. Klicken Sie anschließend auf „Bearbeiten - > Alle Vorgänge ausführen“ und auf „Anwenden“. Schließen Sie Gparted und binden Sie die SD-Karte im Dateimanager per Klick auf das Laufwerk in das Dateisystem ein. Entpacken Sie dann den Inhalt der Noobs-ZIP-Datei auf die SD-Karte.

Geschwindigkeit der SD-Karte testen

Ob die SD-Karte im Raspberry Pi etwas taugt, lässt sich mit einem Benchmarktest schnell prüfen. Verwenden Sie in einem Terminalfenster folgende Befehlszeile:

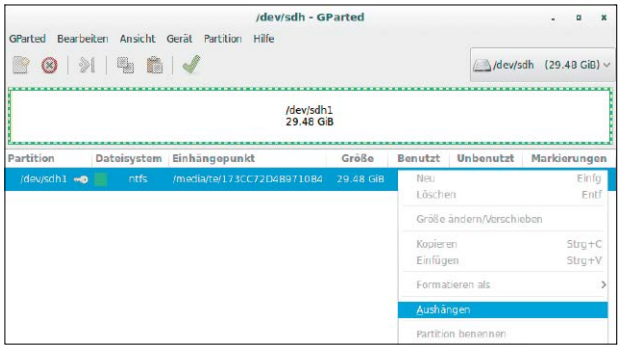
```
curl -L http://www.pcwelt.de/sdbench | sudo bash
```

Das Script lädt einige Tools herunter und führt dann Leistungstests mit hdparn, dd und iozone durch. Bei iozone beziehen sich die letzten ausgegebenen Werte auf „4k random read“ und „4k random write“ in KB/s. Diese Werte sind am aussagekräftigsten für die Beurteilung der Arbeitsgeschwindigkeit. Das Tool iozone lässt sich auch unter Ubuntu installieren (Paket: „iozone3“). Sie können dann die Leistung des Speichermediums im PC und Raspberry Pi vergleichen. Verwenden Sie die Befehlszeile

```
iozone -e -I -a -s 100M -r 4k -i 0 -i 1 -i 2
```

Die sequenzielle Schreib- und Lesegeschwindigkeit ist bei einer Festplatte deutlich höher und liegt bei etwa 100 MB/s. Zufällige Daten lassen sich auf Festplatte jedoch kaum schneller lesen und schreiben als auf Speicherkarte. Insofern schneidet der Raspberry Pi mit einer SD-Karte nicht schlecht ab.

Wer die Geschwindigkeit dennoch optimieren möchte, kann das System von einem schnellen USB-Stick booten (-> Punkt 5).



SD-Karte vorbereiten: In Gparted melden Sie die Speicherkarte über „Aushängen“ beim System ab. Danach erstellen Sie eine neue FAT32-Partition.

```
te@te-Z87-HD3: ~/Downloads
te@te-Z87-HD3:~$ df -h
Dateisystem    Größe Benutzt Verf. Verw% Eingehängt auf
udev           3,4G       0  3,4G    0% /dev
tmpfs          690M    9,9M  680M    2% /run
/dev/sda1      104G     84G   15G   86% /
tmpfs          3,4G    416K  3,4G    1% /dev/shm
tmpfs          5,0M    4,0K  5,0M    1% /run/lock
tmpfs          3,4G       0  3,4G    0% /sys/fs/cgroup
tmpfs          690M     68K  690M    1% /run/user/1000
/dev/sdb1       30G     16K   30G    1% /media/te/DDB3-6C5E
te@te-Z87-HD3:~$ sudo umount /dev/sdb1
[sudo] Passwort für te:
te@te-Z87-HD3:~$ cd ~/Downloads
te@te-Z87-HD3:~/Downloads$ sudo dd bs=4M if=2016-11-25-raspbian-jessie.img
 of=/dev/sdb && sync
```

Imagedatei kopieren: Lösen Sie zuerst die Laufwerkseinbindung und übertragen Sie dann die Abbilddatei des Betriebssystems mit dd auf die SD-Karte.

Werfen Sie das Laufwerk über die zugehörige Schaltfläche im Dateimanager aus und setzen Sie die SD-Karte in den Raspberry Pi ein. Jetzt müssen Sie nur noch das Netzteil mit dem Gerät verbinden. Nach kurzer Zeit erscheint die Noobs-Oberfläche. Setzen Sie ein Häkchen vor das gewünschte Betriebssystem. Sie können auch mehrere Systeme auswählen, wenn auf der SD-Karte genügend Platz ist. Nach einem Klick auf „Install“ richtet Noobs die gewählten Systeme ein.

Die Auswahl ist endgültig: Sie können keine weiteren Systeme nachträglich installieren. Noobs lässt sich zwar kurz nach dem Start des Raspberry Pi per Druck auf die Shift-Taste erneut aufrufen, in diesem Recoverymodus installiert Noobs jedoch alle gewählten Systeme neu und die bisherigen Einstellungen und Daten gehen verloren. Sind mehrere Systeme installiert, sehen Sie nach dem Start des Raspberry Pi ein Auswahlmenü. Nach zehn Sekunden startet das zuletzt verwendete System automatisch.

4. Systeme über Imagedateien installieren

Wer Noobs nicht verwenden oder ein dort nicht angebotenes System einrichten möchte, geht einen anderen Weg. Schreiben Sie die Imagedatei des gewünschten Betriebssystems direkt auf die SD-Karte. Im Downloadbereich von *www.raspberrypi.org* finden Sie unter „Third Party Operating System Images“ Links zu weiteren Systemen.

Die Imagedateien sind meist in ZIP-, gz- oder xz-Archive gepackt. Extrahieren Sie den Inhalt über den Dateimanager und den Kontextmenüpunkt „Hier entpacken“. Die Raspbian-Datei beispielsweise heißt „2016-11-25-raspbian-jessie.zip“ und nach dem Entpacken sehen Sie die Datei „2016-11-25-raspbian-jessie.img“.

Öffnen Sie ein Terminalfenster und ermitteln Sie über den Befehl df, ob die SD-Karte in das Dateisystem eingebunden ist. Sollte das der Fall sein, hängen Sie die Karte aus:

```
sudo umount /dev/sdx1
```

„sdx1“ ersetzen Sie durch den über df ermittelten Gerätepfad. Alternativ lässt sich der Pfad auch mit *sudo parted -l* in Erfahrung bringen, wenn die SD-Karte nicht eingehängt ist.

Wechseln Sie in das Verzeichnis, in dem die entpackte „img“-Datei liegt, und schreiben Sie das Abbild auf die SD-Karte. Verwenden Sie dafür folgende Kommandos:

```
cd ~/Downloads
sudo dd bs=1M if=2016-11-25-ras
 pbian-jessie.img of=/dev/sdx
sync
```

„sdx“ ersetzen Sie durch den Gerätepfad der SD-Karte. Kontrollieren Sie die Angabe genau, damit Sie nicht versehentlich das falsche Laufwerk überschreiben. Die Angabe „bs=1M“ sorgt für eine zuverlässige Blockgröße beim Kopieren.

Bitte beachten Sie: Die für den Raspberry Pi verfügbaren alternativen Desktopbetriebssysteme sind nicht auf dem gleichen technischen Stand wie das Referenzsystem Raspbian (*www.raspbian.org*). Sie müssen teilweise mit Einschränkungen rechnen. Beispielsweise funktionieren WLAN oder Bluetooth nicht immer zuverlässig. Wenn es keine besonderen Gründe etwa für ein Ubuntu Mate (*https://ubuntu-mate.org*) oder Fedora (*https://fedoraproject.org/wiki/Raspberry_Pi*) gibt, sollten Sie Raspbian wählen. Multimedia-Systeme wie Open Elec (*http://openelec.tv*), Libre Elec (*https://libreelec.tv*) und Osmc (*https://osmc.tv*) arbeiten ebenfalls stabil.

5. Raspbian über USB oder Netzwerk booten

SD-Karten sind nicht besonders schnell und eher schlecht zu handhaben. Die Installation des Betriebssystems auf einem USB-Laufwerk verspricht mehr Geschwindigkeit und unterschiedliche Systeme lassen sich bequemer durch einfachen Wechsel des USB-Sticks starten. Der Raspberry Pi 3 kann das System auch von USB laden, ohne dass sich eine SD-Karte im Gerät befindet. Ältere Modelle können zwar einen USB-Stick mit dem System einbinden, die SD-Karte bleibt aber weiter das

Bootmedium. Wie das funktioniert, ist auf *www.pcwelt.de/2131569* beschrieben.

Das neue Bootverfahren für den Raspberry Pi 3 befindet sich noch in der Betaphase und es gibt Einschränkungen. USB-Festplatte oder Stick müssen nach etwa zwei Sekunden betriebsbereit sein, damit der Raspberry Pi die Bootpartition findet. Deshalb kann es sein, dass vor allem USB-Festplatten nicht korrekt funktionieren. Verwenden Sie besser einen schnellen USB-Stick. Außerdem darf Raspbian nicht über Noobs installiert worden sein.

Installieren Sie zuerst Raspbian auf einer SD-Karte wie in -> Punkt 4 beschrieben. Aktualisieren Sie das System, indem Sie im Terminal diesen Befehl ausführen:

```
sudo apt-get update && sudo apt-
  get -y upgrade
```

Danach installieren Sie die Betafirmware und starten das System neu:

```
sudo BRANCH=next rpi-update
sudo reboot
```

Jetzt aktivieren Sie die USB-Bootfunktion und starten Raspbian neu:

```
echo program_usb_boot_mode=1 | su
  do tee -a /boot/config.txt
sudo reboot
```

Prüfen Sie im Terminalfenster, ob der Bootmodus korrekt gesetzt ist:

```
vcgencmd otp_dump | grep 17:
```

Die korrekte Antwort muss „17:3020000a“ lauten – nicht „17:1020000a“. Andernfalls wiederholen Sie die vorherigen Schritte.

System auf USB übertragen: Verbinden Sie das USB-Laufwerk mit dem Raspberry Pi. Gehen Sie im Menü auf „Zubehör -> SD Card Copier“. Hinter „Auf Gerät kopieren“ wählen Sie den USB-Stick aus und klicken auf „Start“. Danach müssen Sie mit „Ja“ bestätigen, dass Sie die Daten auf den Stick kopieren möchten und alle darauf befindlichen Dateien verlorengehen. Ist der Vorgang abgeschlossen, binden Sie die Partitionen auf dem USB-Stick in das Dateisystem ein:

```
sudo mount /dev/sda2 /mnt
sudo mount /dev/sda1 /mnt/boot
```

Jetzt müssen Sie für das System auf dem USB-Stick die geänderten Partitionsbezeichnungen konfigurieren:

```
sudo nano /mnt/boot/cmdline.txt
```

Tragen Sie im Editor hinter „root=“

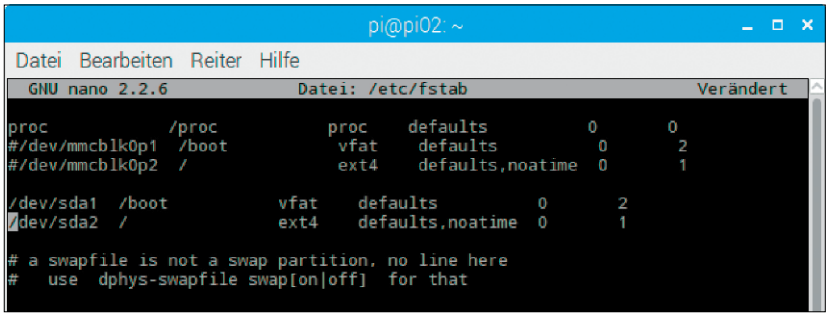
```
/dev/sda2
```

ein statt bisher „/dev/mmcblk0p2“. Mit Strg-S speichern Sie die Datei, bestätigen dies mit Eingabetaste und beenden den Editor mit Strg-X. Nach dem gleichen Muster öffnen Sie die Datei „/mnt/etc/fstab“ im Editor nano. Hier ändern Sie „/dev/mmcblk0p1“ auf „/dev/sda1“ und „/dev/mmcblk0p2“ auf „/dev/sda2“. Hängen Sie den USB-Stick aus:

```
sudo umount /mnt/boot /mnt
```

Beenden Sie Raspbian und trennen das Gerät von der Stromversorgung. Entnehmen Sie die SD-Karte und schließen Sie das Netzteil wieder an. Das System startet jetzt vom USB-Stick.

Netzwerkboot: Der aktualisierte Bootloader des Raspberry Pi sucht im Netzwerk nach einem DHCP/TFTP-Server, wenn keine SD-Karte und kein USB-Stick vorhanden ist. Damit lässt sich das System theoretisch über das Netzwerk laden. Bei unseren Tests konnten wir den Raspberry Pi jedoch nicht dazu bewegen, zuverlässig über das Netzwerk zu booten. Deshalb verzichten wir in diesem Artikel auf eine ausführliche Beschreibung. Wer es selbst ausprobieren möchte, findet über *www.pcwelt.de/K6Z4lZ* eine englischsprachige Anleitung.



Laufwerkskonfiguration ändern: Damit das System die Partitionen vom USB-Stick einbinden kann, müssen Sie die Einträge in der Datei „/etc/fstab“ ändern.

6. Erste Schritte nach der Systeminstallation

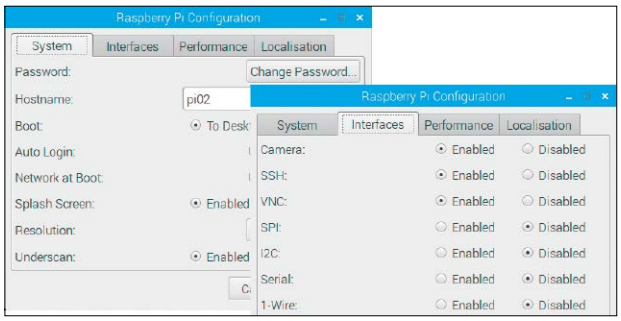
Nach der Installation startet Raspbian mit englischsprachiger Oberfläche und Tastaturbelegung. Über die Einstellungen können Sie das ändern, ein neues Passwort festlegen sowie zusätzliche Dienste aktivieren. Installieren Sie außerdem die verfügbaren Updates oder konfigurieren Sie die automatische Updateinstallation.

Klicken Sie links oben auf die Menüschaltfläche und gehen Sie auf „Preferences -> Raspberry Pi Configuration“. Unter „Localisation -> Set Locale“

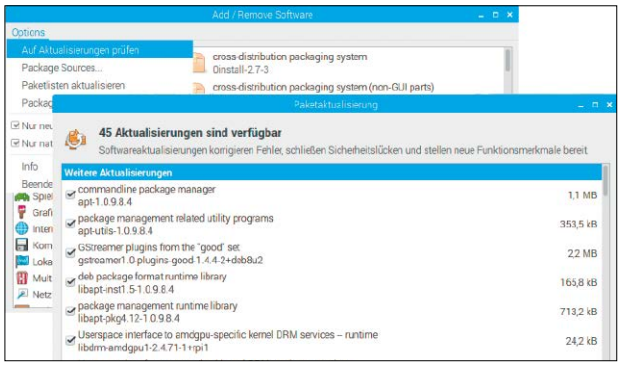
Instabilität durch schwaches Netzteil

Das System bleibt regelmäßig hängen und Sie sehen beim Start rechts oben auf dem Bildschirm ein buntes Kästchen oder einen gelben Blitz? Mit den genannten Symbolen signalisiert der Raspberry Pi eine zu geringe Stromversorgung.

Der Raspberry Pi 3 benötigt ein Netzteil mit mindestens 2,5 A, für die älteren Modelle reichen zwei A. Das Gerät startet zwar meist auch, wenn das Netzteil eine geringere Leistung hat, es kann dann aber zu Fehlfunktionen kommen. Sind beispielsweise WLAN und Bluetooth aktiviert und ist vielleicht noch eine USB-Festplatte angeschlossen, reicht die Stromversorgung nicht mehr aus. Sehen Sie sich daher nach einem passenden Netzteil mit 2,5 A für den Raspberry Pi 3 um, oder greifen Sie zu einem Gerät mit drei A, um Reserven zu haben. Im Onlinehandel gibt es geeignete Netzteile für circa zehn Euro.



Basiskonfiguration: Über „Preferences -> Raspberry Pi Configuration“ ändern Sie das Passwort des Benutzers „pi“ und aktivieren beispielsweise „SSH“ für den Fernzugriff.



System aktualisieren: Über den Menüpunkt „Auf Aktualisierungen prüfen“ rufen Sie im Paketmanager („Add/Remove Software“) die Aktualisierungsverwaltung auf.

stellen Sie hinter „Language“ den Wert „de (German)“ ein; bei „Country“ wählen Sie „DE (German)“ und hinter „Character Set“ geben Sie „UTF-8“ ein. Klicken Sie auf „OK“. Über die Schaltflächen „Set Timezone“, „Set Keyboard“ und „Set WiFi Country“ konfigurieren Sie weitere Einstellungen für ein deutschsprachiges System.

Auf der Registerkarte „Interfaces“ können Sie Dienste wie „SSH“ und „VNC“ für den Fernzugriff einschalten. Auf der Registerkarte „System“ ändern Sie das Passwort für den vorkonfigurierten Benutzer „pi“ (Standardpasswort: „raspberry“) und bei Bedarf auch der Rechnernamen. Klicken Sie zum Abschluss auf „OK“ und beantworten Sie die Frage „Would you like to reboot now?“ mit „Yes“.

Raspberry bietet ein weiteres Konfigurationstool, das Sie im Terminal folgendermaßen starten:

```
sudo raspi-config
```

Es bietet die gleichen Optionen wie das Werkzeug für die grafische Oberfläche, jedoch unter „Advanced Option“ zwei zusätzliche Einstellungen. Über „Audio“ legen Sie fest, ob die Audioausgabe über HDMI oder die 3,5-Millimeter-Klinkenbuchse erfolgen soll. Über „GL Driver“ lässt sich ein experimenteller Treiber für die hardwarebeschleunigte OpenGL-Ausgabe aktivieren. Sie können dann Spiele wie Neverball oder Oolite ausprobieren.

Updates und Upgrades: Über den Punkt „Einstellungen -> Add/Remove Software“ rufen Sie die Paketverwaltung auf. Darüber installieren Sie zusätzliche Software oder suchen über „Options -> Auf Aktualisierungen prüfen“ nach Updates. Wer das Terminalfenster bevorzugt, verwendet folgende Befehlszeile:

```
sudo apt update
sudo apt upgrade
```

Wer den Raspberry als Server nutzt, kann die Sicherheitsupdates automatisieren. Installieren Sie die dafür nötige Software:

```
sudo apt install unattended-upgrades
```

Das System aktualisiert dann täglich die Paketlisten und installiert Sicherheitsupdate automatisch.

7. Backup des Systems erstellen

Wenn Raspbian wunschgemäß eingerichtet ist, sollten Sie eine Sicherungskopie des Systems erstellen. Das Backup lässt sich auf einer zweiten SD-Karte anlegen, die Sie über einen USB-Kartenleser unter Raspbian verwenden. Die Backup-Karte muss genau so groß wie die System-Karte oder größer sein. Gehen Sie im Menü auf „Zubehör -> SD Card Copier“ und wählen Sie hinter „Auf Gerät kopieren“ das Laufwerk mit der zweiten SD-Karte. Klicken auf „Start“ und dann auf „Ja“.

Alternativ erstellen Sie das Backup mit dem Tool dd auf einem Linux-PC. Dazu verwenden Sie am PC einen Kartenleser, in den Sie die SD-Karte einsetzen. Mit df oder mount ermitteln Sie den Laufwerkspfad. Erstellen Sie dann das Backup mit dieser Befehlszeile:

```
sudo dd if=/dev/sdx of=raspbian.img bs=4M
```

„/dev/sdx“ ersetzen Sie durch den zuvor ermittelten Laufwerkspfad. Bei Bedarf stellen Sie die SD-Karte aus dem Backup später wieder her, indem Sie die Parameter für „if“ und „of“ austauschen.

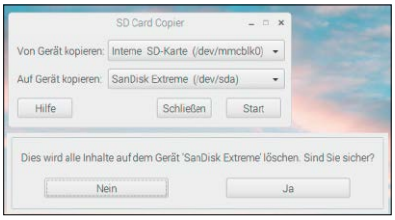
8. Multimedia-Funktionen nachrüsten

Raspbian bietet nach der Installation keine Programme, mit denen sich Audio- und Videodateien abspielen lassen. Über die Standard-Repositorien lassen sich Anwendungen wie VLC-Player oder Smplayer installieren. Gehen Sie im Menü auf „Einstellungen -> Add/Remove Software“ und suchen Sie nach dem gewünschten Programm.

Für MP3s und SD-Videos sind VLC oder Smplayer ausreichend. Bei HD-Videos kommt es jedoch zu hoher CPU-Belastung und die Wiedergabe ruckelt. Beide Programme können die Hardwarebeschleunigung nicht nutzen. Besser geht es mit dem standardmäßig installierten Omxplayer, der sich allerdings nur über die Kommandozeile aufrufen und mit Tastaturkürzeln bedienen lässt. Um ein Video abzuspielen, verwenden Sie folgende Befehlszeile:

```
omxplayer -o local meinvideo.mkv
```

Die Audioausgabe erfolgt dabei über die Buchse für den 3,5-Millimeter-Klinkenstecker. Für HDMI setzen Sie



Backup erstellen: Mit dem Tool SD Card Copier erstellen Sie eine Kopie der Systemspeicherkarte auf einer zweiten SD-Karte, die in einem USB-Kartenleser steckt.

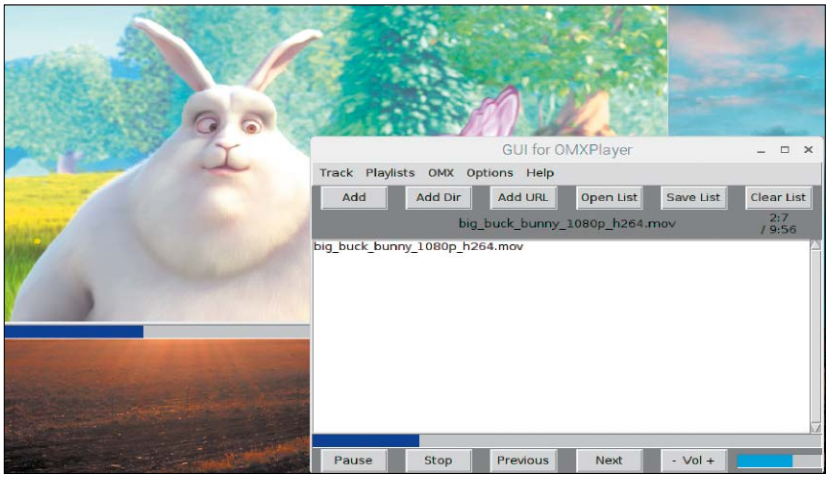
„-o hdmi“ ein. Die Wiedergabe erfolgt im Vollbildmodus, mit der Q-Taste beenden Sie den Player. Eine Übersicht mit weiteren Optionen und den Tastaturkürzeln finden Sie unter *https://github.com/huceke/omxplayer*.

Tboplayer ist eine nicht besonders hübsche, aber funktionale Oberfläche für den Omxplayer. Die Befehlszeile für die Installation über ein Setup-Script finden Sie auf *https://github.com/KenT2/tboplayer*. Das Tool integriert sich in den Dateimanager und Sie können Videos über den Kontextmenüpunkt „TBOPlayer“ abspielen. Das Wiedergabefenster hat zwar keinen Rahmen, es lässt sich aber auf dem Bildschirm mit der linken Maustaste verschieben. Um die Größe des Videobereichs zu ändern, halten Sie die Strg-Taste gedrückt.

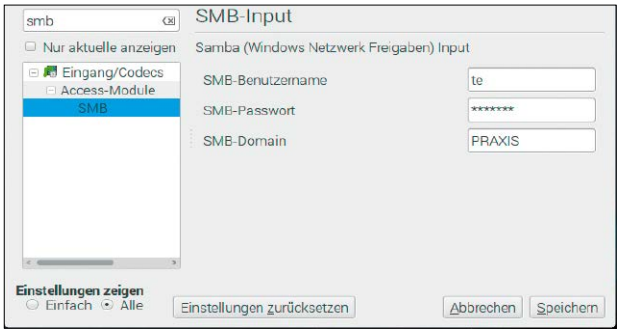
9. MP3s und Videos über das Netzwerk abspielen

Dieses Problem tritt häufig auf: Die Audio- und Videosammlung liegt auf einem Netzwerklaufwerk und die Wiedergabe funktioniert nicht, wenn Sie eine Multimedia-Datei etwa im VLC-Player öffnen. Der Grund: VLC kann nicht auf eine Datei zugreifen, wenn sie auf einem passwortgeschützten Netzwerklaufwerk liegt. Das funktioniert nur, wenn Sie Benutzernamen und Passwort im VLC-Player konfigurieren. Dazu gehen Sie im Menü auf „Werkzeuge -> Einstellungen“ und aktivieren unter „Einstellungen zeigen“ die Option „Alle“.

Tippen Sie *smb* in das Suchfeld ein, klicken Sie auf „SMB“, tragen Sie die



HD-Videos auf dem Desktop: Tboplayer nutzt das Kommandozeilentool Omxplayer, das auch hochauflösende Videos ruckelfrei abspielt.



Netzwerkzugriff: Der VLC-Player kann Dateien von passwortgeschützten Freigaben nur öffnen, wenn Sie die Anmeldeinformationen in den Einstellungen hinterlegen.

Anmeldeinformationen ein und klicken Sie auf „Speichern“.

Alternativ können Sie die Netzwerkfreigabe auch in das Dateisystem einhängen. Dann haben auch andere Programme wie Smplayer oder Tboplayer Zugriff. Verwenden Sie im Terminal beispielsweise folgende Befehle:

```
sudo mkdir /mnt/nas
sudo mount.cifs //[IP-Adresse]/
  [Freigabe] /mnt/nas -o
  user=[Benutzer]
```

Die Platzhalter in eckigen Klammern ersetzen Sie durch den Freigabepfad und Benutzernamen. Tippen Sie das Anmeldepasswort ein, um sich mit dem Server zu verbinden. Im Dateimanager öffnen Sie dann den Ordner „/mnt/nas“, um auf die Dateien zuzugreifen.

Soll die Einbindung automatisch beim Systemstart erfolgen, öffnen Sie die Konfigurationsdatei fstab:

```
sudo nano /etc/fstab
```

Tragen Sie folgende Zeile ein:

```
//[IP-Adresse]/[Freigabe] /mnt/nas
  cifs username=[Benutzer],passwd=
  [Passwort]
```

Die Platzhalter ersetzen Sie wieder durch die Daten für Ihre Systemkonfiguration.

Bitte beachten Sie: Wenn auf dem Server der Schreibzugriff auf die Freigabe erlaubt ist, wird diese über die Benutzer- und Gruppen-ID gesteuert. Sie haben beispielsweise auf einem Linux-Server Schreibrechte für den bei der Installation erstellten Benutzer erlaubt. Dieser hat die Benutzer-ID „1000“. Da der Benutzer „pi“ unter Raspbian ebenfalls die ID „1000“ besitzt, ist auch hier der Schreibzugriff möglich. Weichen die IDs ab, verwenden Sie folgende Zeile in „/etc/fstab“:

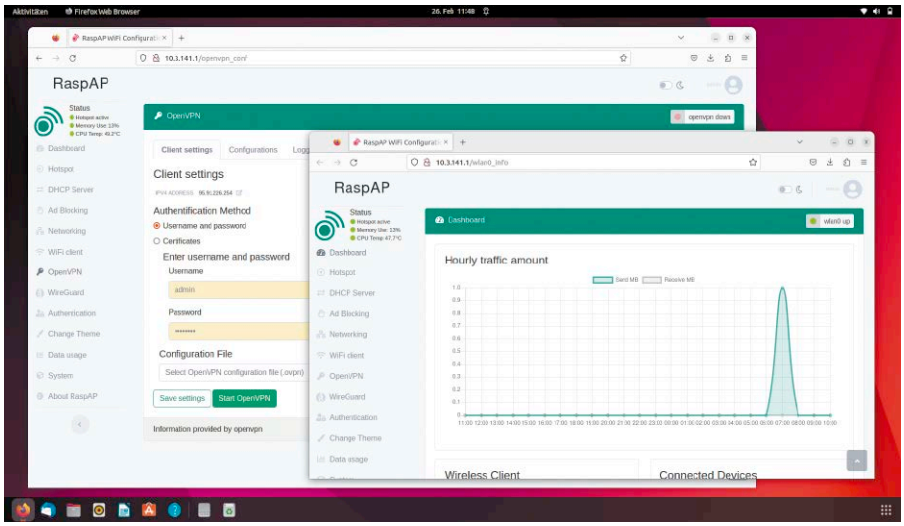
```
//[IP-Adresse]/[Freigabe] /mnt/nas
  cifs username=[Benutzer],passwd=
  [Passwort],uid=1000,gid=1000
```

Die Angaben „uid“ und „gid“ sind auch notwendig, wenn sich die Freigabe auf einem Windows-Rechner befindet. ●

Raspberry als WLAN-Router

Zu den vielseitigen Einsatzmöglichkeiten des Ein-Platinen-Computers zählt auch der Einsatz als WLAN-Router und Access Point. Mit einer cleveren Software klappt die Einrichtung problemlos. Wir zeigen, wie das geht.

VON STEPHAN LAMPRECHT



Üblicherweise kümmert sich der heimische Router um das Aufspannen eines Funknetzes. Einen weiteren Wi-Fi-Router oder Access Point in Betrieb zu nehmen, ist aber mehr als nur Redundanz. So kann es etwa sinnvoll sein, alle Geräte des IoT und Smarthome in einem separaten Netz zu betreiben. Bekanntlich werden smarte Glühbirnen, Thermostate und andere Devices nicht so häufig mit Updates versehen wie Office-Programme. Laufen diese in einem eigenen Netz, trägt das zur Sicherheit des Heimnetzes bei. Die Lösung Rasp AP stellt alles bereit, um einen Raspberry in einen WLAN-Router zu verwandeln.

Wozu ein separates WLAN?

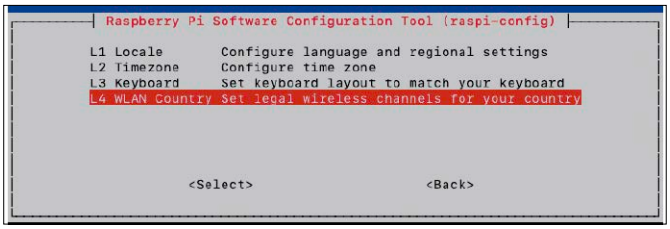
Einmal eingerichtet, kann der Raspberry Pi mit Rasp AP vielfältige Aufgaben übernehmen. Neben der Trennung aller IoT-Devices vom heimischen Netz ist die Platine klein genug und energieeffizient, um unterwegs nützlich zu sein – zum Beispiel im Urlaub, um ein kleines privates WLAN im Hotelzimmer aufzubauen. Auch eine Verbindung des Raspberry mit einem mobilen Modem ist denkbar. Damit wären Sie dann auch von (teuren) Hotspots unabhängig.

Der Raspberry benötigt zwei Netzwerkschnittstellen: Es liegt auf der Hand, soll aber zur Sicherheit an dieser Stelle erwähnt werden, dass der Raspberry zwei Netzwerkadapter benötigt, wenn er als Router arbeiten soll. Über die erste verbinden sich alle Geräte im Heimnetzwerk. Die zweite stellt die Verbindung zum Internet her. Im heimischen Netzwerk kontaktiert sie etwa eine Fritzbox. Die Modelle 3 und 4 des Raspberry besitzen eine Ethernet-Buchse und eine integrierte WLAN-Schnittstelle, somit alles, was es für den Einsatz als Router benötigt. Bei älteren Modellen müssen Sie die zweite Schnittstelle (WLAN) durch einen externen USB-Dongle nachrüsten.

Den Raspberry vorbereiten

Die Konfiguration der Software erledigen Sie später ganz bequem per Browser. Für die Installation benötigen Sie weder Tastatur noch Bildschirm, wenn der Raspberry entsprechend vorbereitet ist. Das geht am einfachen mit dem offiziellen Raspberry Pi Imager (*www.raspberrypi.com/software/*). Suchen Sie sich damit eine aktuelle Version des Raspberry-Pi-OS aus. Bevor Sie es auf die Karte schreiben, klicken Sie auf das Zahnrad mit den Einstellungen. Dort aktivieren Sie die Option „SSH aktivieren“ und nutzen Sie die Option, die Anmeldung mittels Passwort zu erlauben.

Danach setzen Sie den Benutzernamen und ein Passwort für den Zugriff. Speichern Sie und schreiben Sie nun das Image auf die Karte. Davon starten Sie den Raspberry und warten einen Moment. Als



Vor der eigentlichen Installation legen Sie noch die Landeskennung für die Funkkanäle via raspi-config fest.

Nächstes ermitteln Sie in der Konfigurationsoberfläche Ihres Routers die aktuelle IP-Adresse des Systems. Jetzt starten Sie ein Terminal auf einem beliebigen Computer innerhalb des gleichen Netzes und rufen die Verbindung via SSH auf:

```
ssh [benutzer]@[IP-Adresse]
```

Sofern das System Sie nach Aufnahme des Fingerprints fragt, bestätigen Sie mit „Yes“. Verwenden Sie das Passwort, das Sie vorher mit dem Imager angelegt haben. Sie sind jetzt mit dem Pi auf einer Konsole verbunden.

Rasp AP installieren

Steht die Verbindung, bringen Sie das System auf den neusten Stand. Dazu sind im Terminal drei Schritte notwendig, die Sie nacheinander abarbeiten.

```
sudo apt-get update
sudo apt-get full-upgrade
sudo reboot
```

Nun kommt noch eine wichtige Aufgabe. Starten Sie in der Konsole das Programm raspi-config. Wechseln Sie in den Menüpunkt „Localisation Options“ und anschließend zu „WLAN Country Set“. Im nächsten Dialog wählen Sie mit der Tastatur den Eintrag „De“ aus und bestätigen dies.

Danach können Sie die Software verlassen. Damit ist alles vorbereitet. Jetzt besorgen Sie sich die aktuelle Version von Rasp AP:

```
curl -sL https://install.raspap.com | bash
```

Es handelt sich um eine Schnellinstallation. Belassen Sie alles bei den Voreinstellungen und beantworten Sie die Fragen mit „Y“. Jetzt müssen Sie einen Moment warten, weil das System alle notwendigen Dateien aus dem Internet lädt und die Konfiguration schreibt. Beobachten Sie das Terminal aber weiter, da gelegentlich weitere Fragen gestellt werden, die Sie alle bejahen. Am Ende fordert das System zum Neustart auf.

Rasp-AP-Oberfläche und WLAN-Zugang

Der Raspberry spannt nach dem Reboot bereits sein eigenes WLAN auf. Mit diesem müssen Sie sich zunächst verbinden. Suchen Sie nach einem Netzwerk „raspi-webgui“ und verbinden Sie sich unter Benutzung des Schlüssels „ChangeMe“. Nun können Sie sich auch mit der Administrationsoberfläche verbinden. Stellen Sie mit einem Browser Ihrer Wahl eine Verbindung mit „10.3.141.1“ her. Als Benutzernamen verwenden Sie „admin“ und als Passwort „secret“. Es versteht sich fast von selbst, dass Sie dies im ersten Schritt ändern sollten. Das erledigen Sie mit einem Klick auf das Icon am rechten oberen Rand. Im nachfolgenden Dialog vergeben Sie dann das neue Passwort.

Nach wenigen Schritten läuft das System. Alle weiteren Einstellungen nehmen Sie über den Browser im Subnetz von Rasp AP vor.

Sie benötigen einen Bridge-Mode?

Rasp AP ist standardmäßig so konfiguriert, dass die Software im Modus „Access Point“ läuft. Das bedeutet, dass der Raspberry ein eigenes Subnetz aufbaut und den sich anmeldenden Clients ihre eigene IP-Adresse zuweist. Der Vorteil dieser Konstruktion kann auch ein Nachteil sein. Denn durch das getrennte Netzwerk sind die Clients im heimischen Netz so abgeschirmt, dass sie darin geteilte Ressourcen nicht nutzen können.

Wollen Sie das ändern, können Sie in den „Bridge Modus“ umschalten. Wenn Sie sich intensiver mit Netzwerken beschäftigt haben, werden Sie die Folgen nicht überraschen. Allen anderen sei gesagt, dass der Raspberry sich nun nicht mehr als Wi-Fi-Client in einem Netzwerk anmelden kann, deshalb ist die entsprechende Option unter „Hotspot → Advanced“ ausgeblendet. Den Abschnitt „DHCP-Server“ erreichen Sie auch nicht mehr, denn die Vergabe der IP-Adressen erledigt dann der übergeordnete Router (in der Fachsprache „Upstream-Router“). Sofern Sie auf den Clients bisher Open VPN aktiviert haben, läuft der Traffic auch nicht mehr über den Raspberry Pi. Nur dessen eigener Netzwerkverkehr ist dann noch mit Open VPN geschützt.

Um den Bridge-Modus zu aktivieren, wechseln Sie in das Menü „Hotspot“ und rufen das Register „Advanced“ auf. Dort können Sie den Modus via Schiebeschalter aktivieren, müssen anschließend aber noch den Hotspot neu starten.

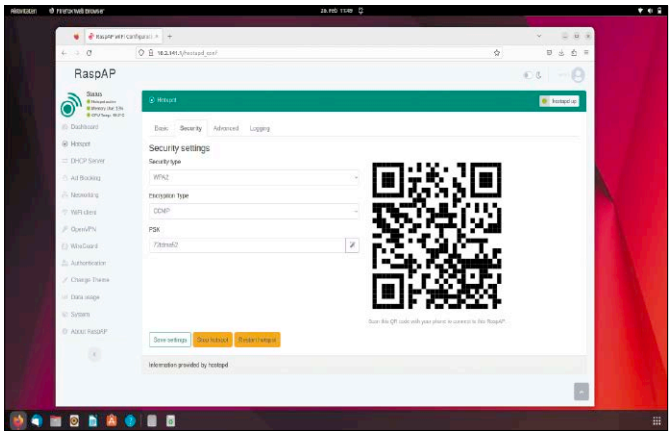
Über die Einträge im Abschnitt „Hotspot“ (linke Navigation) haben Sie die Möglichkeit, die Details des vom Raspberry aufgespannten WLANs zu regeln. Unter „Basic“ verändern Sie den Namen des Netzwerks (SSID) und können hier sogar den Wireless-Mode verändern. Auf Wunsch dürfen Sie hier, wie Sie es vermutlich von Routern gewohnt sind, das schnellere 5-GHz-Netz einschalten und den Funkkanal bestimmen. Mehr als empfehlenswert ist es, im Register „Security“ unter „PSK“ die Phrase für den Netzwerkschlüssel zu ändern. Danach verändert sich auch der QR-Code, der Ihnen bei der Einrichtung von Geräten hilft. Mit einem Klick auf den Zauberstab können Sie Rasp AP auch einen neuen Schlüssel vorschlagen lassen – der hat es von der Länge dann aber auch tatsächlich in sich.

Besitzen Sie gute Kenntnisse im Aufbau von Netzwerkstrukturen, finden Sie im Abschnitt „DHCP Server“ die Option, die von Rasp AP angebotenen Adressbereiche zu verändern oder andere DNS-Server einzustellen. Da sich gerade Anfänger in die Thematik hier schnell verbasteln können, sollen diese Optionen an dieser Stelle keine größere Rolle spielen.

Anzeigen blockieren – auch mit Pi Hole

Haben Sie die Standardinstallation gewählt, bringt Rasp AP eine Besonderheit mit. Denn die daran angeschlossenen Clients können werbefrei surfen.

Möglich macht dies der während der Installation eingerichtete Adblocker. Es ist

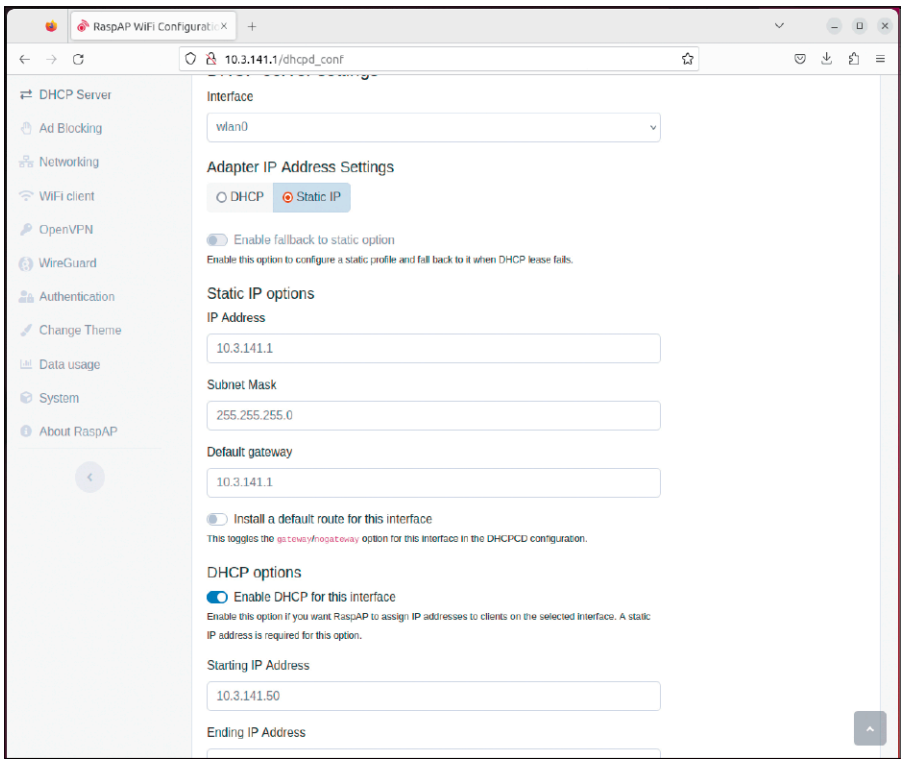


Im Menü „Hotspot“ verändern Sie Funknetz, Kennung, Passphrase und andere Optionen. Dank eines QR-Codes lassen sich mobile Geräte schnell auf das neue Netz einrichten.

auch möglich, diesen später nachträglich zu installieren, das erfordert allerdings eine Reihe von Kommandos, die ausführlich in der Dokumentation des Projekts beschrieben sind (*https://docs.raspap.com/manual*). Über die linke Navigation erreichen Sie die übersichtlichen Einstellungen. Diese beschränken sich auf den Wechsel des Verwalters von Blocklisten und die Bearbeitung der Listen durch eigene Einträge.

Sofern Sie das Blockieren von Anzeigen und Trackern in Ihrem Netz bereits mit Pi Hole gelöst haben, nutzen Sie dessen Möglichkeiten einfach weiter. Dazu haben Sie zwei Möglichkeiten. Um die Vorzüge in Hinblick auf die Sicherheit zu nutzen, müssen Sie Rasp AP dazu zwingen, die externe Ressource des Pi Hole zu nutzen. Pi Hole selbst arbeitet ja als DNS-Server im Netzwerk. Darin liegt dann auch bereits der Trick. Sie rufen in der linken Navigation von Rasp AP den Abschnitt „DHCP Server“ auf und wechseln in das Register „Advanced“. Dort haben Sie die Möglichkeit unter „Add upstream DNS Server“ die Adresse des Pi Hole zu hinterlegen.

Die Alternative dazu ist der Betrieb von Rasp AP im Bridge-Modus. Hier wird ja ohnehin der DNS-Server des Netzwerks verwendet, zu dem eine Brücke aufgebaut wird. Es ist sogar möglich, Pi Hole und Rasp AP auf dem gleichen Raspberry zu betreiben. Das würde allerdings etwas den Rahmen des Artikels sprengen. So könnte man Rasp AP etwa nachträglich auf dem Gerät von Pi Hole in Form eines Docker-Containers installieren.



Rasp AP bietet viele Einstellmöglichkeiten, um eigene Netze zu konfigurieren, etwa um einen Upstream-DNS einzurichten oder individuelle DNS-Server einzutragen.

Rasp AP im Zusammenspiel mit Open VPN

Wer Rasp AP als Access Point zusammen mit einem unsicheren Netzwerk als Upstream nutzt, etwa in einem Hotel, wird seine Bankgeschäfte oder andere private Dinge mit Unbehagen über dieses Netzwerk abwickeln. Mit der Integration von Open VPN können Sie dieses Problem lösen. Voraussetzung dafür ist, dass Sie bereits über ein Konto auf einem VPN-Server verfügen. Ob es sich um einen kommerziellen Anbieter handelt oder einen eigenen Server, spielt keine Rolle. Rasp AP stellt aber keinen eigenen VPN-Server zur Verfügung, sondern kann lediglich dafür genutzt werden, dass die Anfragen der Clients an den VPN-Server weitergereicht werden.

Ein VPN-Anbieter, der als Basis Open VPN benutzt, stellt Ihnen in der Regel eine Konfigurationsdatei mit der Endung „ovpn“ zur Verfügung. Diese Datei sowie die Zugangsdaten des Anbieterunternehmens benötigen Sie. Die Einrichtung nehmen Sie anschließend im Abschnitt „OpenVPN“ in der linken Navigation vor. Sind die Felder gesperrt, haben Sie unter Rasp AP den Bridge-Modus aktiviert. Fehlt der Menüeintrag vollständig, wurde während der Standardinstallation die Komponente abgewählt. Wie im Falle des Adblockers lässt sich das nachträglich korrigieren. Das erklärt die Dokumentation.

Die Aktivierung des Tunnels erfordert den Benutzernamen und das Passwort für den VPN-Zugang. Auch die Absicherung via Zertifikate ist möglich, allerdings bei kommerziellen Angeboten eher die Ausnahme. Auf der Startseite des Abschnitts „OpenVPN“ tragen Sie die Daten ein. Anschließend müssen Sie die „ovpn“-Datei des Zugangs hochladen. Die Einstellungen speichern Sie zunächst und aktivieren danach den Service. Es ist sogar möglich, mehrere Profile und Zugänge zu hinterlegen, um zwischen ihnen zu wechseln. Somit stellt Rasp AP ein sehr bequemes und leicht zu konfigurierbares System für eigene Wi-Fi-Access-Points respektive Router zur Verfügung, das auch Einsteiger vor keine unüberwindlichen Hürden stellt. ■

Odroid M1: Neue Raspi-Konkurrenz

Seit Erscheinen des Raspberry-Modells 4 ist es für andere Platinenhersteller eine echte Herausforderung, zu einem angemessenen Preis ein überzeugendes Konkurrenzprodukt anzubieten. Der neue Odroid M1 will mit SATA-3-Port und NVMe-Slot punkten.

VON HERMANN APFELBÖCK

Die Platinenfamilie Odroid des koreanischen Herstellers Hardkernel (*www.hardkernel.com*) gehört seit Jahren zu den größten Raspberry-Konkurrenten. Die Odroid-Hardware ist robust und in der Regel ausgewogen konzipiert. Das einfache Grundkonzept war schon immer, für etwas mehr Geld mehr Leistung als der gerade aktuelle Raspberry zu liefern oder andere Anschlussmöglichkeiten als dieser. Die bisherige Palette mit Odroid XU4, Odroid HC4, Odroid N2 und Odroid H2 (nicht mehr verfügbar) wird neuerdings ergänzt durch die Platine Odroid M1. Wir hatten den Platinenrechner im Test und zeigen, was ihn auszeichnet und ob er sich einen Platz neben dem dominierenden Raspberry 4 verdient.

Odroid M1: Schnell ausverkauft

Vorneweg: Mit 150 Euro muss man mindestens rechnen, sofern man neben der eigentlichen Platine (etwa 100 Euro oder 120 Euro mit vier oder acht GB RAM) das unentbehrliche Netzteil (etwa 7 Euro), ein Gehäuse (etwa 13 Euro) und ein Kabel- und Montageset für SATA (etwa 13 Euro) benötigt. Und Achtung: Dies waren die Preise einschlägiger Elektronik-Versandhändler wie Pollin oder Reichelt im April und Mai. Seit der Odroid M1 in erster Marge schnell vergriffen war, stiegen umgehend die Preise. Es ist nicht auszuschließen, dass das genannte Bundle bis Erscheinen dieses Artikels bei 180 oder 200 Euro liegt. Preisdynamik, Lieferengpässe und eventuelle Wartezeiten zeigen, dass der Odroid M1 seine Nische sofort gefunden hat.

Die nachfolgenden Eckdaten versprechen in der Tat ein besonders flott laufendes Betriebssystem dank Installation auf NVMe, SATA oder eMMC sowie einen rasanten Serverbetrieb dank SATA-Laufwerk. Ein Sorglospaket für Einsteiger ist die Platine im Unterschied zum universellen Raspberry 4 indes nicht: WLAN- und Bluetooth-Chip fehlen, beim Einsatz eines SATA-Laufwerks gibt es Bedingungen, die man vorab kennen sollte, und auch bei USB ist nicht jede beliebige Anschlussoption möglich. Nicht zuletzt gibt es vorläufig nur ein schmales Angebot bei der Systemsoftware, sodass der Käufer bei der Auswahl des Betriebssystems eventuell Kompromisse eingehen muss. Aber das lohnt die Hardware allemal.

Anschlussfreudiger Odroid M1: Die Standardports oben bieten Gigabit-Ethernet, HDMI, je zweimal USB 2.0 und USB 3.0. Darunter gibt es den Slot für eine NVMe-SSD, rechts unten SATA-Datenport und SATA-Stromversorgung, unten Mitte den eMMC-Anschluss. GPIO-Pins und Audio-Klinkenbuchse sind ebenfalls vertreten.

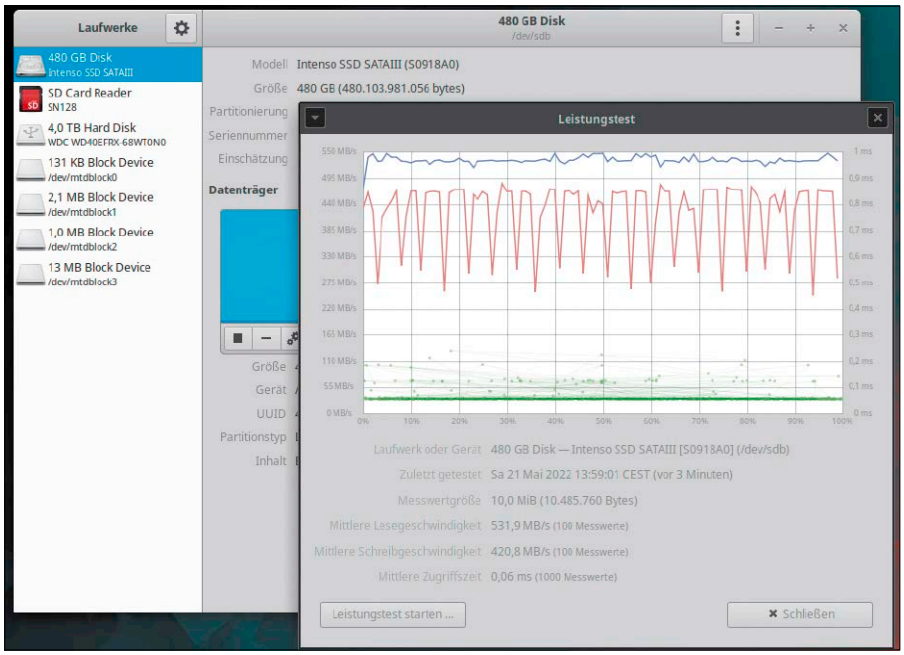
Odroid M1: Die technischen Eckdaten

Die ARM-Hardware läuft mit einem leicht angepassten Rockchip-Prozessor (RK3568B2) mit vier Cortex-A55-Kernen und einer Taktfrequenz von knapp zwei GHz. Diese CPU bringt die Platine in die Liga des Raspberry 4, erreicht dessen Leistung aber nicht ganz (siehe Kasten „Mini-Benchmark“ auf dieser Seite). Für den fest verbauten LPDDR4-Arbeitsspeicher gibt es zwei Varianten der Platine mit vier oder acht GB RAM. Der Preisunterschied beträgt gut 20 Euro. Nach unserer Marktbeobachtung wurde die Acht-GB-Variante am schnellsten ausverkauft und fordert derzeit auch die längeren Wartezeiten auf die nächsten Margen. Im Prinzip sollten für typische Serverrollen im Heimnetz aber auch vier GB RAM völlig ausreichen.

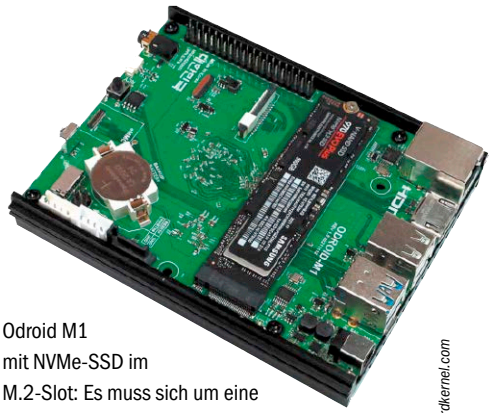
Für den Netzwerkanschluss ist ein Gigabit-Ethernet-Port vorhanden und zur Monitorausgabe ein HDMI-Anschluss. Für die sehr ordentliche bis gute Soundausgabe kann neben HDMI auch ein 3,5-Millimeter-Klinkenstecker dienen. Für Bastler und Industrieeinsatz kommt ferner noch ein DSI-Anschluss für einen kleinen LCD-Bildschirm hinzu. Ebenfalls für Bastlerprojekte kann eine Kamera über CSI angeschlossen werden. Auch die vom Raspberry bekannte 40-Pin-GPIO-Leiste ist verbaut.

Interessant für den Servereinsatz wird es bei den Anschlüssen für Datenträger: USB darf nicht fehlen und ist im Prinzip fünfmal vertreten – zweimal USB 3.0, zweimal USB 2.0 sowie ein Micro-USB-Anschluss (OTG). Der untere der beiden USB-3.0-Ports wird allerdings deaktiviert, falls der kleine OTG-Anschluss genutzt wird. Das ist kein großes Limit, aber man sollte dieses Detail nicht vergessen. Für an USB 3.0 angeschlossene Laufwerke gilt wie bei allen ähnlichen Platinen die Empfehlung, besser Datenträger mit eigener Stromversorgung anzuschließen. Zwei 2,5-Zoll-Laufwerke an USB und eventuell noch ein zusätzliches SATA-Laufwerk kann das Netzteil der Platine nicht stabil versorgen.

Das optionale SATA-Laufwerk versorgen die zwei Standardanschlüsse für das Daten- und das Stromkabel. Letzterer ist ein Fünf-Volt-Anschluss für 2,5-Zoll-HDDs oder SSDs. Eine große 3,5-Platte mit 12-Volt-Anschluss kann die Platine folglich nicht versorgen,



Leistungstest mit Gnome-Disks: Die (ältere) SATA-SSD liefert im Odroid M1 den erwarteten Datendurchsatz.



Odroid M1 mit NVMe-SSD im M.2-Slot: Es muss sich um eine PCIe-SSD handeln (Stichwort „M-Key“ oder „Key M“). Ebenfalls im M.2-Faktor erhältliche SATA-Laufwerke funktionieren nicht.

Quelle: www.hardkernel.com

MINI-BENCHMARK MIT RASPBERRY UND ODROID

Ein kleiner Vergleich mit der simplen arithmetischen Iteration

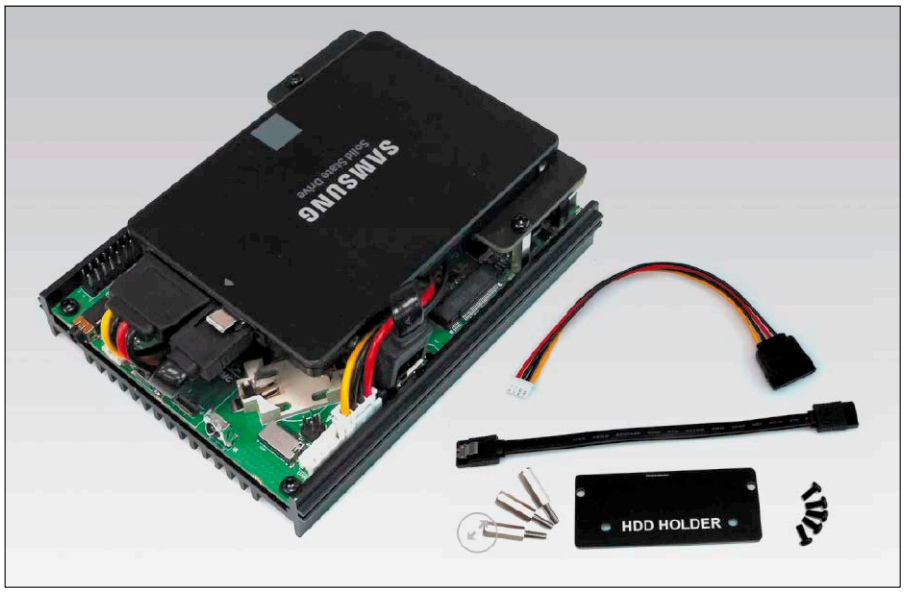
`time $(i=0; while (( i < 9999999 )); do (( i ++ )); done)`

auf etlichen Geräten ordnet die CPU-Leistung des neuen Odroid M1 ganz gut ein. Diese primitive Methode haben wir gewählt, weil auf den diversen Geräten mit diversen Betriebssystemen eine andere einheitliche Methode zu viel Aufwand erfordert hätte. Über die Aussagekraft des simplen Benchmarks lässt sich streiten, aber die Rangfolge deckt sich mit unserer praktischen Alltagserfahrung mit diesen Geräten. Der Raspberry Pi 4 liegt vor der neuen Odroid-Platine, deutlicher noch der Odroid N2 und der nicht mehr erhältliche Odroid H2. Der Fokus des neuen Raspberry-Konkurrenten Odroid M1 liegt eindeutig beim Angebot der Datenträgeranschlüsse, nicht bei der CPU-Leistung.

CPU-MINI-BENCHMARK

Gerät	Prozessor	Architektur	Zeit*
PC-System	Intel i7 (3,2 GHz)	x86	23,61
Odroid H2	Intel Celeron J4105 (2,5 GHz)	x86	45,45
Altes Notebook	AMD Phenom Dual (3,0 GHz)	x86	55,94
Odroid N2	Amlogic (1,8 GHz) / A53 (1,9 GHz)	ARM	67,99
Raspberry Pi 4	Cortex A53 (1,4 GHz)	ARM	113,11
Odroid M1	Rockchip RK3568B2 (2 GHz)	ARM	129,55
Odroid XU4	Cortex A7/A15 (1,4/2,0 GHz)	ARM	144,86
Odroid U3	Exynos 4 (1,7 GHz)	ARM	216,30
Raspberry Pi 3	Cortex A53 (1,2 GHz)	ARM	317,33

*kleiner ist schneller (Angabe in Sekunden)



Odroid M1 mit montierter SSD: Das Montageset für etwa 13 Euro ist unter Umständen entbehrlich, wenn SATA-Standardkabel vorrätig sind. Das Standardgehäuse ist bei einem SATA-Einbau in jedem Fall überflüssig, weil es dafür keinen Platz bietet.

diese müsste dann also mit externem Netzteil betrieben werden. Das von Hardkernel angebotene SATA-Montage-Set für circa 13 Euro umfasst nur die beiden Standardkabel und einen Hartplastik-„HDD-Holder“, um die SATA-Platte mit der Platine zu verschrauben. Das Zubehör ist verzichtbar, sofern Standardkabel vorliegen und der Datenträger nicht befestigt werden muss.

Für das Betriebssystem (oder Daten) gibt es neben dem üblichen Slot für eine Micro-SD-Karte und dem SATA-Laufwerk noch weitere Optionen: Es ist ein eMMC-Slot vorhanden (Embedded Multimedia Card) sowie ein Anschluss für ein SSD-Laufwerk vom Typ NVMe M.2. Letzteres muss eine PCIe-NVMe sein, eine NVMe mit SATA-Controller funktioniert dort nicht.

Wichtige Infos zur Systeminstallation

Auf *https://wiki.odroid.com/odroid-m1/odroid-m1* gibt es bislang nur einige wenige Systemimages zum Download (siehe dort „os_images“), die dann mit einschlägigen Tools wie Etcher oder Gnome-Disks auf SD-Karte zu übertragen sind. Zum Redaktionsschluss war die Auswahl verfügbarer Systeme noch sehr bescheiden und überdies unglücklich gewählt: Wer – naheliegend – die Hardware für Serveraufgaben nutzen will, wird nicht unbedingt zu Android 11 greifen. Ansonsten gibt es ein Ubuntu 20.04 ausgerechnet mit der anspruchsvollen Gnome-Oberfläche, die für die Hardware nicht angemessen erscheint. Zum Zeitpunkt des Produkttests erschien uns daher als einzig passende Wahl ein purer Ubuntu Server 20.04, auf den wir anschließend ein sparsames XFCE nachinstallierten. Die Zugangsdaten für fertige Odroid-Images lauten seit jeher „odroid“ mit Kennwort „odroid“.

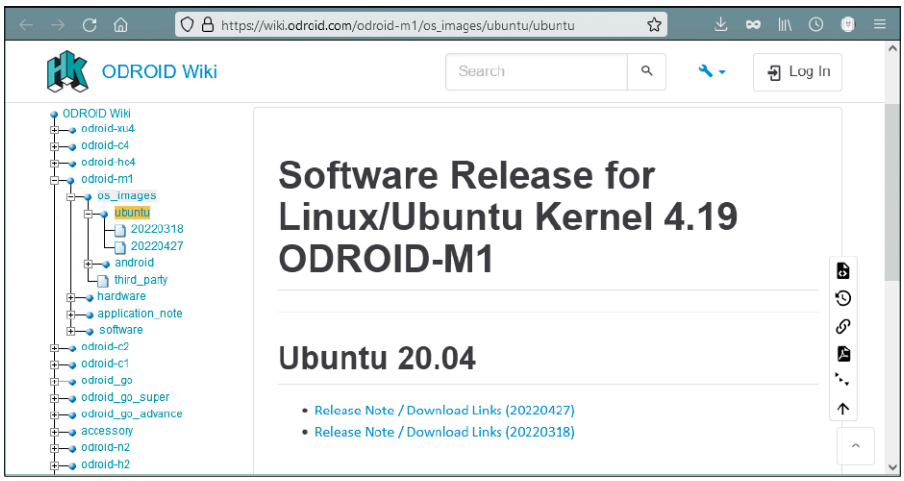
Diese traditionelle Systembestückung für Platinenrechner ist aber auf SD-Karten (eventuell noch eMMC) beschränkt. Wer das System auf SATA oder NVMe installieren will, muss einen anderen Weg einschlagen. Und dieser Weg erweist sich insgesamt als der klügere, weil er ein sauberes System ohne „odroid“-Konto, eine größere Systemauswahl, eine individuelle Desktopauswahl und vor allem die freie Wahl des Systemdatenträgers eröffnet.

Beim Start der Platine (mit oder ohne installiertes Betriebssystem) meldet sich das integrierte Minimalsystem Petitboot, das einige wesentliche Systeminfos anzeigt und ferner eine Multiboot-Auswahl des Betriebssystems erlaubt (falls etwa auf SD, SATA und NVMe verschiedene Systeme bereitstehen). Entscheidender ist aber die Fähigkeit von Petitboot, Betriebssysteme über das Internet zu laden und zu installieren. Diese Fähigkeit wird bei Hardkernel- oder Vertreiber-Dokumentationen lapidar vorausgesetzt, ist aber bislang nirgendwo prominent dokumentiert.

Um die im Netz verfügbaren Systeme aufzulisten, müssen Sie in Petitboot zunächst die unterste Option „Exit to shell“ wählen und dann die folgenden zwei Befehle eingeben:

```
udhcpc
netboot_default
```

Der erste stellt die Verbindung zum Netzwerk sicher, der zweite setzt die Bootpriorität auf die Netzwerkinstallation. Nach „exit“ und Verlassen der Mini-Shell zeigt das Petitboot-Menü oben die verfügbaren Betriebssysteme. Dies sind mehr, als die Downloadseite als traditionelle Images anbietet, allerdings ist von Kandidaten mit dem Hinweis „Work in Progress“ oder „Experimental“ eher abzuraten, da dies in unserem Fall prompt in einem fatalen Boothänger nach dem ersten Systemstart endete. Zum Zeitpunkt dieser Recherche waren nur Ubuntu 20.04 und Debian 10 als stabi-

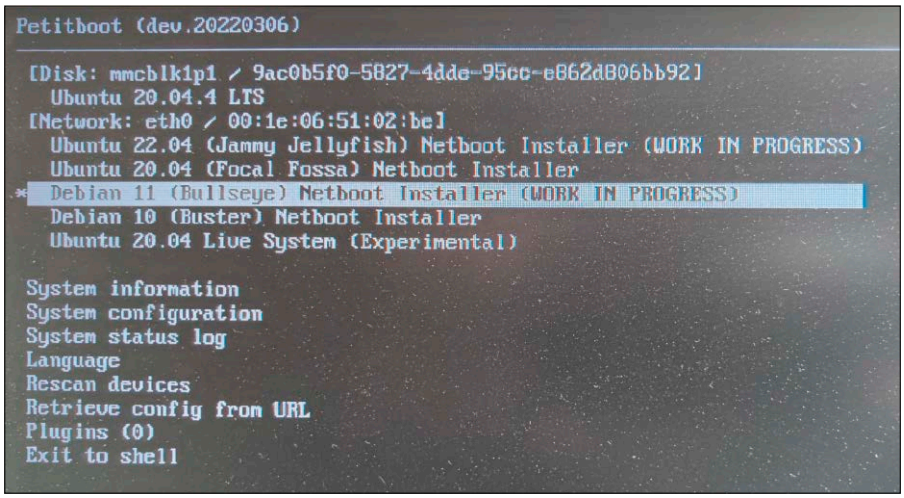


Klassische Images auf *https://wiki.odroid.com*: Dieser Weg eignet sich nur für den Transport auf SD-Karte. Eine Installation auf SATA oder NVMe muss über das Minisystem Petitboot erfolgen.

le Kandidaten erreichbar. Mindestens Ubuntu 22.04 und Debian 11 werden umgehend folgen.

Die weiteren Vorteile dieser Installationsweise sind offensichtlich: In den bekannten textbasierten Installern von Ubuntu und Debian sorgen Sie vorab für eine saubere Lokalisierung des Systems, für ein individuelles Systemkonto und entscheiden gegen Ende der Installation im Tasksel-Dialog über Desktop und gewünschte Serverdienste (SSH, Apache).

Für den Systemdatenträger gibt es beim Partitionierungsdialog kein Verbot – SD-Karte, NVMe-, SATA-, eMMC- oder auch USB-Laufwerke sind möglich.



Besser und flexibler als ein Imagedownload: Im integrierten Odroid-Minimalsystem können Sie die Netboot-Option freischalten und dann das gewünschte System aus dem Internet beziehen.

Odroid M1: Praxis, Tipps und Einordnung

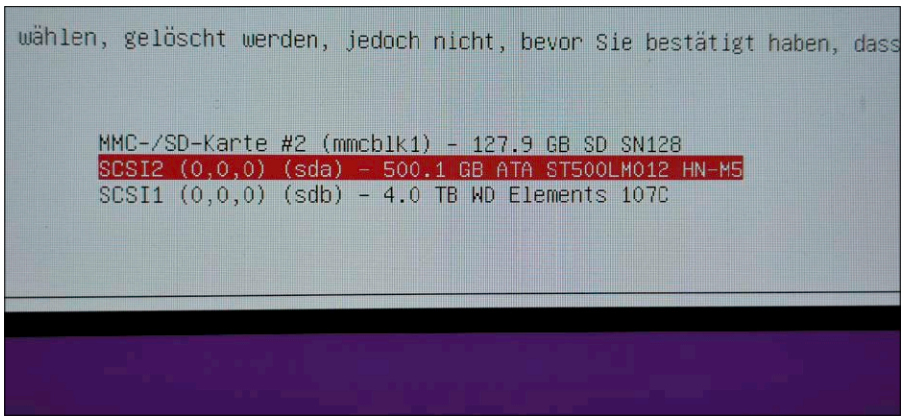
Die Platine arbeitet lüfterlos und somit absolut lautlos. Ähnlich dem Odroid N2 sitzt die gesamte Hardware auf einem großen passiven Kühlkörper und nach Ausweis des Sensortools des von uns genutzten XFCE-Desktops erreicht die Platine selbst bei Last kaum 40 Grad. Dies bestätigen auch eine haptische Kontrolle sowie der sehr niedrige Stromverbrauch: Wir messen etwa zwei Watt im Leerlauf und bringen den Odroid M1 selbst unter hoher Last nicht über 3,5 Watt Leistungsaufnahme – eventuelle mechanische Laufwerke oder Displays sind hier natürlich nicht eingerechnet.

Tipp zur Desktopwahl: Sofern man dem allzu anspruchsvollen Desktop Gnome aus dem Weg geht, arbeitet der Minirechner mit einem XFCE, LXDE oder LXQT jederzeit auch mit grafischer Oberfläche flüssig. Selbst für einen Odroid M1 in reiner Serverrolle empfehlen wir die Installation eines Desktops, der dann per HDMI oder VNC neben der SSH-Fernwartung auch eine bequeme Oberfläche anbietet. Bei vier oder sogar acht GB RAM fällt der meist ungenutzte Desktop kaum ins Gewicht.

Tipp für Datenfreigaben: Mechanische SATA-HDDs, auch wenn sie ausschließlich als Datenfreigabe dienen, sollten unbedingt mit dem Standard-Dateisystem Ext4 formatiert werden. Das von Hardkernel früh angebotene Ubuntu 20.04 hat einen relativ betagten Kernel mit mäßiger NTFS-Unterstützung. Der Datendurchsatz kommt damit kaum über 30 bis 40 MB/s und liegt damit sogar unter den etwa 80 MB/s, die per USB angeschlossene Datenträger erreichen. Es wäre daher kontraproduktiv, die M1-Platine wegen der SATA-Schnittstelle zu erwerben und dann mit NTFS auszubremsen. SSDs am SATA-Port sind hingegen mit jedem beliebigen Dateisystem schnell genug, um im Gigabit-Netzwerk die Daten mit den maximalen 110 bis 120 MB/s auszuliefern.

Tipp zum Zubehör: Für den Odroid M1 gibt es ein hübsches blaues Aluminiumgehäuse, das als Staubschutz prinzipiell zu empfehlen wäre. Es wird einfach auf die passende Rille des großen Kühlkörpers aufgeschoben und dann auf beiden Seiten mit Endabdeckungen verschraubt. Ganz zu Ende gedacht ist das nicht, weil sich das Gehäuse mit dem interessantesten Hardwareangebot der Platine nicht verträgt: Ein SATA-Laufwerk bringen Sie nämlich nicht unter, wenn Sie das Gehäuse nutzen. Es ist nicht einmal möglich, die SATA-Kabel nach außen zu legen und das Laufwerk außerhalb zu nutzen, denn allein schon die eingesteckten SATA-Kabel machen es unmöglich, das Gehäuse auf die Platine zu schieben. Kurz: Wer vorhat, am Odroid M1 ein SATA-Laufwerk anzuschließen, kann sich den Kauf des Gehäuses von vornherein sparen.

Einordnung: Im Umfeld des Raspberry Pi 4 und den weiteren aktuellen Odroid-Platinen wird das Modell Odroid M1 aufgrund seiner Flexibilität mühelos seinen Platz finden. Daran lässt sich praktisch alles anschließen und einbauen, was man in der Schublade liegen hat. Da wird dann die kleine SSD, die für den Desktoprechner längst unterdimensioniert war, zum idealen Systemdatenträger. Als Datenserver garantiert die Platine jederzeit volle Gigabit-Leistung (120 MB/s), wenn die Daten auf einem SATA-Laufwerk liegen. Laufwerke an USB 3.0 liefern die Daten nicht schneller, aber auch nicht langsamer aus als beim Raspberry Pi 4 – also je nach Datengrößen etwa mit 40 bis 80 MB/s. ■

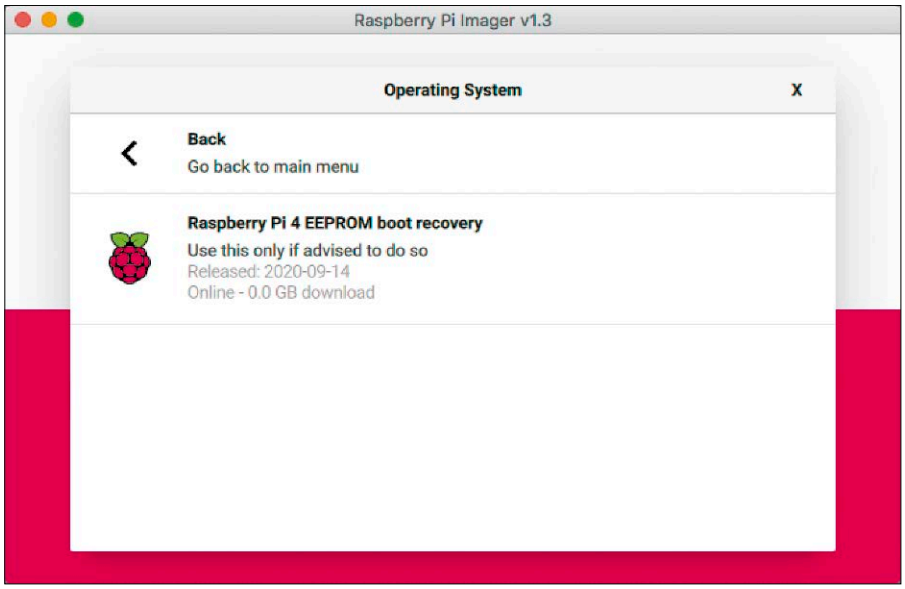


Mit Petitboot gestarteter Netinstaller (hier Debian): Damit bringen Sie das Betriebssystem auf jedes beliebige Laufwerk, das an der Odroid-Platine angeschlossen ist.

Raspberry Pi 4 bootet von USB

Die Entwickler des Raspberry Pi 4 haben der Platine die Bootoption von einem USB-Speicher spendiert. Damit können Sie Startprobleme wegen defekter SD-Karte vergessen. Wir erklären Ihnen, wie Sie den Raspberry via USB zum Laufen bekommen.

VON STEPHAN LAMPRECHT



Mit dem Imagerprogramm schreiben Sie das Eeprom-Update auf eine SD-Karte, um damit eine Aktualisierung durchzuführen.

Einer der Gründe dafür, dass ein Raspberry Pi nicht richtig startet, kann eine defekte SD-Karte sein. Und nicht immer ist dann passender Ersatz zu Hause, während der eine oder andere USB-Stick sicher noch in der Schublade liegt. Der Raspberry Pi 4 wird durch die Aktualisierung von Betriebssystem und Firmware flexibler und kann auch von einem USB-Massenspeicher booten. Dies wird vorzugsweise ein USB-Stick, kann aber auch eine externe Festplatte sein. USB-Festplatten ohne eigene Stromversorgung sind allerdings eine Fehlerquelle für sich und daher eher nicht zu empfehlen.

Vielleicht ist USB-Boot bereits an Bord?

Wenn Sie einen Raspberry Pi 4 gerade gekauft haben, ist USB-Boot vielleicht schon aktiv und folglich keine Änderungen an der Konfiguration erforderlich. Um dies vorab zu überprüfen, schließen Sie die Platine einfach an einen Monitor und die Stromversorgung an – ohne externen USB-Datenträger und ohne SD-Karte. Der Rechner zeigt auf dem Display seine Diagnosemeldungen an. Dazu gehört auch die Version des Bootloaders im Eeprom am oberen Rand des Bildschirms. Bootfähig von USB sind alle Versionen, die ein Datum vom 3. September 2020 oder neuer zeigen. Ist das der Fall, können Sie die USB-Startoption sofort nutzen.

Eeprom vor einer Installation aktualisieren

Erfüllt die Platine die Voraussetzungen nicht, ist eine Aktualisierung des Eeproms erforderlich – dies am besten vor einer Installation des Betriebssystems. Besorgen Sie sich zunächst den Raspberry Pi Imager von der Seite des Projekts (*https://www.raspberrypi.org/software/*). Sie benötigen außerdem eine SD-Karte. Unter „Choose OS“ entscheiden Sie sich für „Misc. utility Images“. Dort nutzen Sie „EEPROM boot recovery“ für den Pi 4. Dieses Images übertragen Sie auf die Karte und starten anschließend damit den Raspberry. Das angeschlossene Display signalisiert den Erfolg.

Neuinstallation des Betriebssystems

Nachdem das Eeprom der Platine die Voraussetzungen erfüllt, sind die Installation eines Betriebssystems und der Startvorgang per USB problemlos umzusetzen. Dazu laden Sie sich von der Projektseite die gewünschte Version des Betriebssystems lokal auf Ihren Hauptrechner herunter. Anschließend erfolgt die übliche Kopie des Systemabbilds auf das USB-Medium – zum Beispiel mit dem Tool Etcher (*https://etcher.io*): Schließen Sie Festplatte oder USB-Stick an den PC an und starten Sie Etcher. Wählen Sie als Quelle die Abbilddatei und als Ziel das USB-Laufwerk. Bei der Übertragung werden alle vorhandenen Daten auf dem USB-Gerät gelöscht. Nach erfolgreicher Übertragung mit Etcher entnehmen Sie den USB-Speicher und verbinden ihn mit der Raspberry-Platine. Schließen Sie die gewünschten externen Geräte wie Display, Maus und Tastatur an und versorgen Sie den Pi mit Strom. Der erste Start dauert im

Vergleich mit der Installation auf SD-Karte etwas länger, verläuft aber problemlos.

System auf USB-Boot umstellen

Auf den meisten Raspberry-Platinen läuft wahrscheinlich bereits ein bewährtes Betriebssystem, das man nicht einfach ersetzen will. Auch existierende Systeme lassen sich auf die neue Startoption umrüsten. Das funktioniert mit wenigen Handgriffen am Raspberry selbst. Dazu bringen Sie das System zunächst auf den aktuellsten Stand – am einfachsten in einem Terminal mit diesen Kommandos:

```
sudo apt-get update
sudo apt-get full-upgrade
```

Anschließend muss das Eeprom aktualisiert werden. Auch das können Sie in einem Terminal erledigen. Führen Sie dazu das Kommando

```
sudo rpi-eeprom-update
```

aus. Danach starten Sie das System zur Sicherheit einmal neu, um zu kontrollieren, dass alles korrekt vorbereitet ist. Der Raspberry Pi sollte nach dem Update so eingerichtet sein, dass er von USB startet, sofern keine SD-Karte gefunden wird. Diese Bootreihenfolge sollten Sie kontrollieren und gegebenenfalls ändern. Dazu rufen Sie sich mit root-Recht

```
sudo raspi-config
```

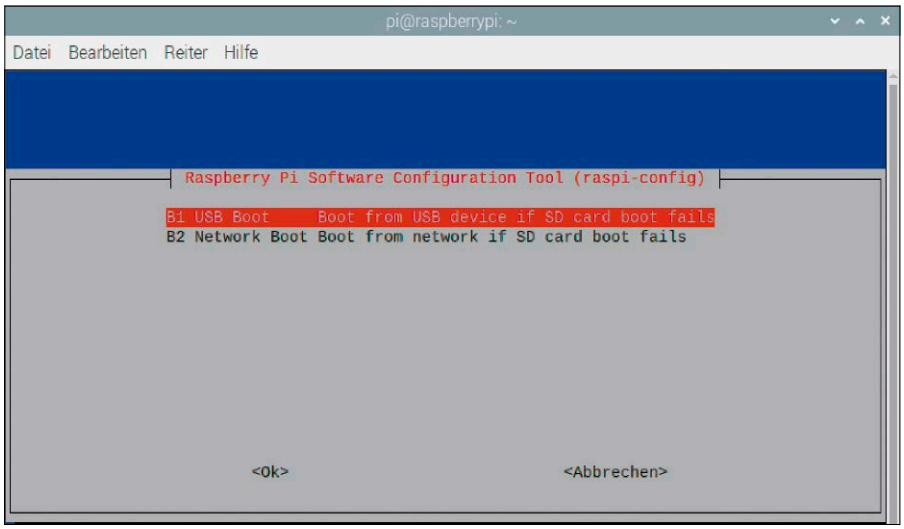
das Programm raspi-config auf. Öffnen Sie den dritten Menüpunkt „Boot Options“ und anschließend „Boot Order“. Dort sollte „USB-Boot“ aktiviert sein. Ist das nicht der Fall, ändern Sie die Option entsprechend. Kontrollieren Sie aus einem Terminal heraus, was in den Parametern für den Systemstart hinterlegt ist. Dies erfahren Sie in der Datei der Bootkonfiguration:

```
cat /boot/cmdline.txt
```

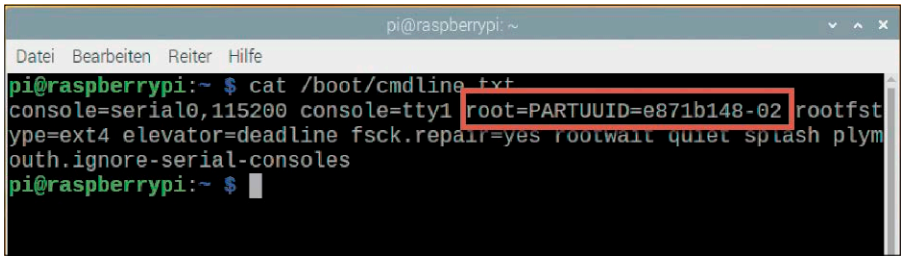
Kontrollieren Sie, ob hinter dem Wert „root=“ die UUID-Kennziffer der Bootpartition hinterlegt ist. Eine absolute Pfadangabe sollte dort nicht mehr stehen.

Einige Anleitungen im Internet empfehlen neben der Aktualisierung von Betriebssystem und Eeprom auch noch die Aktualisierung des Kernels via rpi-update. Dieser Schritt war bei keiner unserer Testplatinen notwendig.

Der Raspberry ist nun vorbereitet. Jetzt muss die aktuelle Konfiguration auf den USB-Datenträger übertragen werden. Dazu schließen Sie USB-Stick oder -Festplatte an die Platine an. In der Programmgruppe „Zubehör“ finden Sie die Anwendung „SD Card Copier“. Hier wählen Sie Ihre Rootpartition aus, im Normalfall „/dev/mmcblk0“. Als Ziel nutzen Sie den angeschlossenen USB-Datenträger. Dies überschreibt vorhandene Daten auf dem USB-Laufwerk. Hat das Kopierprogramm seine Arbeit erfolgreich beendet, fahren Sie den Raspberry herunter. Danach unterbrechen Sie dessen Stromversorgung, entfernen die SD-Karte und starten durch Anschluss des Netzteils die Platine neu. Der Raspberry bootet jetzt vom USB-Medium.



Prüfen Sie mit raspi-config, ob die USB-Option für das Booten bereits vorliegt. Dann können Sie sich Konfigurationsarbeit ersparen.

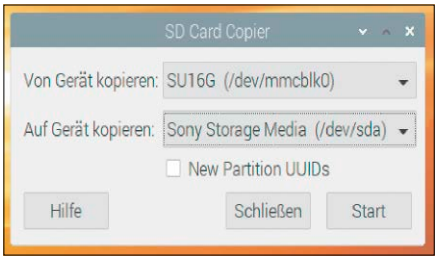


Überprüfen Sie die Bootoptionen. In diesem Fall ist alles in Ordnung, denn es wird keine absolute Pfadangabe, sondern die UUID für das Bootmedium verwendet.

Einschränkungen bei externen Festplatten

Das beschriebene Verfahren hat bei allen getesteten USB-Sticks problemlos funktioniert. Mit externen USB-Festplatten waren unsere Bemühungen nicht ganz so erfolgreich: Bei einer SSD-Festplatte von Samsung, die per USB-Kabel angeschlossen wurde, startete der Rechner bis zum Desktop. Bei zwei weiteren externen Festplatten, die mittels eines SATA-Adapters an einen USB-Port angeschlossen werden, blieb der Startvorgang bei einer Platte regelmäßig hängen, beim zweiten Modell wurde – nicht reproduzierbar – der Desktop fallweise gestartet oder auch nicht. Der erfolgreiche Startvorgang scheint noch wesentlich von eventuell verwendeten Adaptern abzuhängen.

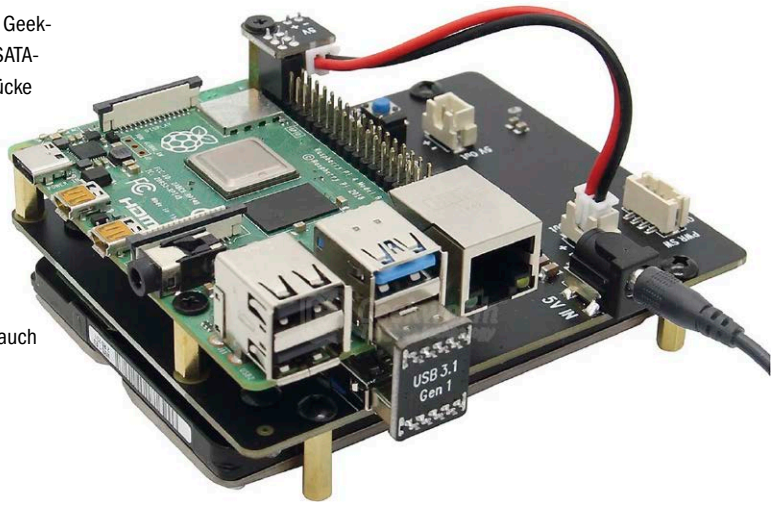
Sollten bei Ihnen Probleme auftreten, ist eine Rückkehr zum bisherigen Startvorgang jederzeit möglich, indem Sie die funktionierende SD-Karte einfach wieder einstecken und von dort starten. Durch das Kopieren auf den USB-Datenträger hat sich an diesem Teil der Konfiguration nichts verändert. ■



SD Card Copier: Mit dem Kopierprogramm des Raspberry Pi übertragen Sie eine vorhandene Installation von der SD-Karte auf das USB-Medium.

Raspberry Pi: SATA nachgerüstet

Die SD-Karte eines Raspberry Pi ist als Datenspeicher nicht ideal. Während SSDs mit einen USB-Adapter auf SATA zufrieden sind, reicht diese sparsame Lösung für mechanische Festplatten nicht aus. Wir haben verschiedene Möglichkeiten getestet.



Zusatzplatine von Geekworm mit einem SATA-Port: Die Steckbrücke zum USB-Port stellt die Datenverbindung her. Ein separates Netzteil (5 V/4 A) versorgt sowohl das Laufwerk als auch den Raspberry.

VON DAVID WOLSKI

Für kleinere oder temporäre Dateiablagen im Netzwerk ist ein älterer Raspberry Pi mit großzügiger SD-Karte oder besser noch mit USB-Stick ohne weiteres Zubehör völlig ausreichend. Raspberry-Pi-OS (vormals Raspbian) liefert in seinen Paketquellen zudem den Samba-Server für das CIFS/SMB-Protokoll mit, um Windows-Freigaben bereitzustellen. Die Einrichtung als Dateiserver ist damit nicht anders als mit einem regulären Debian. Ein zuverlässiges Linux-System macht aber allein noch keinen Dateiserver, geschweige denn ein großzügiges NAS. Mit dem Raspberry Pi 4 mit echtem Gigabit-Ethernet sowie schnelleren USB-3.0-Ports erscheint dieser Einsatzzweck attraktiver als mit den Vorgängermodellen. Aber was dem Raspberry Pi weiterhin fehlt, ist ein SATA-Anschluss zur Anbindung von SATA-Festplatten. Verschiedene hier getestete Ansätze können dieses Manko ausgleichen.

Einfache Adapter: USB auf SATA

Die einfachste Lösung stellen passive Adapter dar, die alle SATA-Konnektoren inklusive der Stromversorgung für den externen Datenträger einfach an den USB-Port führen. Adapter dieser Art sind schon ab sieben Euro plus Versandkosten zu haben (*https://amzn.to/2Gr3pas*). Dieses Zubehör hat aber kein eigenes Netzteil – der USB-Port muss den benötigten Strom liefern. Dies funktioniert im Prinzip schon ab dem Raspberry Pi 2, denn ab diesem Modell liefern die USB-Ports bis zu 1,2 A. Das gilt für alle Ports zusammengenommen. Ein einzelner USB-Anschluss ist dabei nicht begrenzt, versorgt ein angeschlossenes Gerät aber maximal mit diesem Strom. Die Spezifikation ist in der Dokumentation der Raspberry Pi Foundation unter *www.raspberrypi.org/documentation/hardware/raspberrypi/usb/README.md* dargelegt. In der Praxis reicht diese Stromversorgung allenfalls für eine einzelne SSD oder eine 2,5-Zoll-Festplatte bis zwei TB. Mehr als ein SATA-Laufwerk kann man via USB und USB-Stromversorgung aber nicht betreiben – selbst der Raspberry Pi 4 wird instabil, wenn er zwei USB-Laufwerke mit Strom versorgen soll.

Mit Stromversorgung: SATA-Docks

Soll der Raspberry 4 mehr als ein SATA-Laufwerk per USB ansprechen, so sind Dockingstationen für 2,5-Zoll- oder 3,5-Zoll-Festplatten mit USB-Anschluss eine Option. Entsprechende Geräte gibt es im Versandhandel ab 25 Euro (*https://amzn.to/35WOwp7*) oder auch mit zwei Einschüben ab 30 Euro (*https://amzn.to/34PZHQW*). Eine um wenige Euro günstigere Alternative sind kleine Ansteckadapter mit eigenem Netzteil (*https://amzn.to/35WPmSN*), die besser in beengte Standorte und in Schubladen passen. Auf diese Weise können zwei SATA-Laufwerke über den schnellen USB-Port am Raspberry Pi 4 angeschlossen werden.

Achtung: Die beigelegten, oft sehr billig hergestellten Netzteile haben meist einen sehr schlechten Wirkungsgrad und erhöhen den Energiebedarf pro Festplatte um etwa vier bis sechs Watt.

SATA-Platinen: Fest montiert

Ein genereller Nachteil von Adaptern und Docks sind bei beengten Verhältnissen die rasch ausufernden Kabelknäuel. Diese sind auf Dauer immer auch eine nicht zu unterschätzende Fehlerquelle.

Eine etwas teurere, aber aufgeräumtere dritte Möglichkeit, dem Raspberry Pi 4 einen SATA-Anschluss zu verpassen, sind kompakte Zusatzplatinen. Diese bringen als Sandwich die Adapterschaltung, ein

Einfacher Adapter: Der Raspberry Pi 4 liefert maximal 1,2 A per USB. Es genügt für kleine Notebookfestplatten bis zwei TB und sparsame SSDs. Andere Laufwerke brauchen ein Netzteil.

Mit eigenem Netzteil: 3,5-Zoll-Laufwerke und 2,5-Zoll-Festplatten ab zwei TB können per USB nicht mitversorgt werden und verlangen eine separate Stromversorgung.

2,5-Zoll-Laufwerk sowie den eigentlichen Platinenrechner zusammen. Auch diese SATA-Platinen verbinden sich schließlich mit einer Steckbrücke zu einem der USB-3.0-Ports für den Datentransfer, denn die GPIO-Pins sind generell nicht für hohe Bandbreiten geeignet.

Die im Aufmacherbild dieses Beitrags abgebildete Platine Geekworm X825 (*https://amzn.to/3n0qmB5*, 40 Euro) kann auf diese platzsparende Weise ein 2,5-Zoll-Laufwerk über den USB-Port des Raspberry Pi 4 verfügbar machen. Für einen stabileren Betrieb oder eine stromhungrige Festplatte mit mehr als zwei TB muss diese Platine mit einem zusätzlichen Netzteil zu 5V/4A (DC) betrieben werden, das nicht im Lieferumfang enthalten ist und separat bestellt werden muss. Der Clou dabei ist jedoch, dass auch der Raspberry Pi mit an diesem Netzteil hängt und über die entsprechenden GPIO-Pins mitversorgt wird.

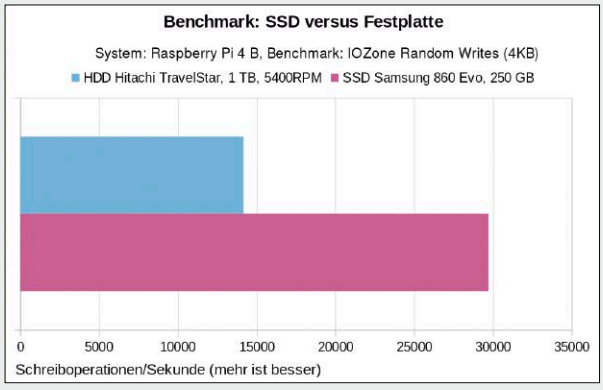
In den letzten Monaten hatten Onlineshops für den Raspberry Aufsteckplatinen der Firma Radxa Limited aus Schenzhen, China, angepriesen. Die Produkte mit dem Namen Dual-SATA-HAT sowie Quad-SATA-HAT sollen einem Raspberry Pi 4 zwei, respektive sogar vier SATA-Anschlüsse bescheren. Eine offenkundig baugleiche Platine ist auch als„Seeed Studio Dual SATA HAT in Onlineshops vertreten. Allerdings ließ sich in Deutschland und einschlägigen Onlineshops keine einzige dieser Platinen auftreiben. Andere Onlinehändler in Europa stornierten die Bestellung nach einigen Wochen ohne weiteren Kommentar. Es ist nach unseren Recherchen davon auszugehen, dass diese HATs nur in kleinen Stückzahlen gefertigt wurden, die erst gar nicht auf den hiesigen Markt gelangten.

Raid: Nur Level 1 ist sinnvoll

Ein Raid-1-Verbund, also eine Spiegelung geschriebener Daten auf zwei Datenträgern, war auf den bisherigen Raspberry Pis in der Praxis nicht gut zu machen, denn die Platine lieferte nicht genug Leistung. Unsere Versuche mit einem Raspberry Pi 3 B und zwei 3,5-Zoll-Festplatten in einem Raid-0-Verbund mit jeweils eigener Stromversorgung zeigen nach etwa einem Tag Betriebszeit schon die ersten Fehler im Kernel-Protokoll. Mit dem Raspberry Pi 4, USB 3.0 und mehr Rechenpower wird der Betrieb zweier Festplatten als Raid 1 realistisch (Mirroring). Bei einem Raid-Wiederaufbau ist die Platine allerdings über Stunden ausgelastet und sollte über eine gute Kühlung verfügen. Raid 5 (Parität) verlangt der kleinen Platine zu viel Rechenleistung ab, Raid 0 (Striping) bringt am USB-Port keine messbaren Vorteile bei den Zugriffsgeschwindigkeiten. ■

LAUFWERKSTYP: USB ODER HDD?

Weil alle extern angeschlossenen SATA-Laufwerke am USB-Controller des Raspberry Pi zusammenkommen, liegt die Vermutung nahe, dass eine SSD hier keinen Geschwindigkeitsvorteil gegenüber einer Festplatte hat. Bis zum Raspberry Pi 3 trifft dies zu, denn die Geschwindigkeit der USB-2.0-Ports begrenzt den Datendurchsatz auf 60 MB/s. In der Praxis sind kaum mehr als 30 MB/s von einem externen Laufwerk zu erwarten. Der Raspberry Pi 4 kennt mit seinem USB-3.0-Controller diese Limitierung nicht mehr und liefert an diesem Bus unter realen Bedingungen bis zu 360 MB/s Durchsatz. Ab dieser Generation macht es durchaus einen Unterschied, ob man eine HDD oder SSD per USB anbindet.



Schön schnell dank USB 3.0: Diese Schnittstelle ist auf dem Raspberry Pi 4 kein Flaschenhals mehr. Trotz eines potenziell bremsenden SATA-Adapters lohnt sich daher eine flotte SSD.

Zubehör für den Raspberry Pi

Für den Raspberry Pi gibt es viel interessantes Zubehör. Statten Sie das Gerät mit einer Kamera oder einem Minidisplay aus oder verwenden Sie Sensoren und Aktoren für Bastelprojekte.

Standardzubehör: Ein Netzteil benötigen Sie in jedem Fall. Es muss aber nicht das Original sein. Ein Gehäuse schützt das Gerät und per HDMI-Kabel erfolgt die Verbindung zum Monitor.

VON THORSTEN EGGELING

Der Raspberry Pi gehört mit mehr als 20 Millionen verkauften Geräten zu den erfolgreichsten Ein-Platinen-PCs. Der ursprünglich als Lehr- und Lerncomputer entwickelte Raspberry Pi kann durch seinen günstigen Preis und die zahlreichen Einsatzmöglichkeiten überzeugen. Ein weiteres Argument ist, dass die Raspberry-Modelle hardwareseitig weitestgehend abwärtskompatibel sind. Das meiste Zubehör lässt sich weiterverwenden, auch wenn Sie auf ein neueres und schnelleres Modell umsteigen wie etwa aktuell auf den Raspberry Pi 4 (außer Gehäuse, Netzteil und HDMI-Kabel). Alles zusammen trägt dazu bei, dass ein breites Zubehörangebot verfügbar ist. Einiges ist für jeden Raspberry-Besitzer interessant, manches nur für Nutzer, die den Raspberry Pi als Experimentier- und Bastel-PC verwenden.

Gehäuse und Netzteil

Der Raspberry Pi wird als einzelne Platine verkauft oder als Starterkit inklusive Gehäuse, Netzteil und SD-Karte. Teilweise gibt es auch noch einen USB-Kartenleser für den PC, HDMI-Kabel und Kühlkörper dazu. Nur die Platine kostet zwischen etwa 35 Euro für den älteren Raspberry Pi 3 Modell B+, 40 Euro für den Raspberry 4 Modell B mit einem GB RAM und etwa 60 Euro für das neueste Modell mit vier GB RAM. Starterkits mit unterschiedlicher Ausstattung kosten um die 75 Euro inklusive Raspberry Pi 3 oder 4.

Ob man das nötige Zubehör selbst auswählt oder ein Starterkit bestellt, ist Geschmackssache. Es ist auf jeden Fall flexibler, alle Teile einzeln zu bestellen. Beim Gehäuse beispielsweise haben Sie die Wahl zwischen Modellen aus Kunststoff oder aus Metall. Letztere ermöglichen eine bessere Wärmeableitung. Der Raspberry Pi 4 wird relativ heiß (siehe Artikel ab Seite 54), weshalb wenigstens Kühlkörper, vielleicht sogar Gehäuse mit Lüfter erforderlich sind.

Für die passive Kühlung gibt es kleine Einzelkühlkörper, die man einfach auf die Chips klebt. Eine effektivere Wärmeableitung versprechen große Kühlkörper, die die gesamte Platine abdecken und gleichzeitig als einfaches Gehäuse dienen.

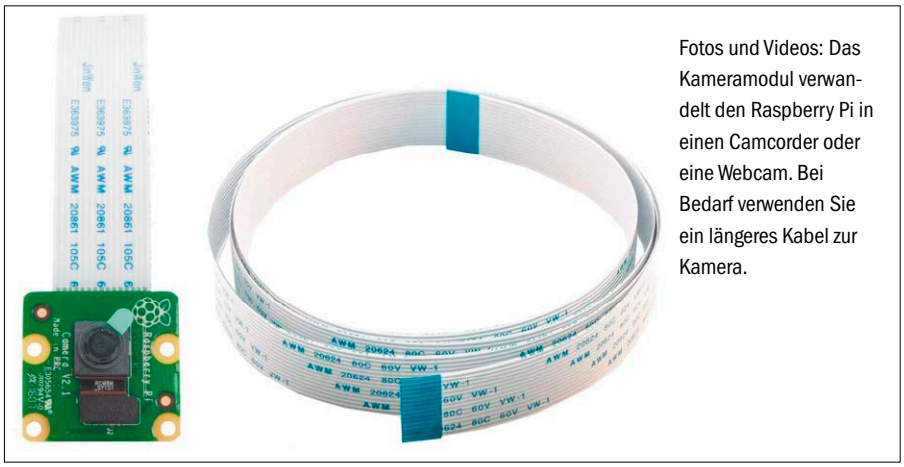
Beim Netzteil kann man zum original Raspberry-Pi-Netzteil greifen, für den Raspberry Pi 4 muss es bei fünf Volt mindestens drei Ampere liefern. Es kostet knapp neun Euro und ist von angenehm kleiner Bauform. Es funktioniert auch jedes andere Netzteil mit den gleichen oder besseren Leistungswerten.

Kameras für den Raspberry Pi

Es gibt mehrere Kameramodelle, die Sie an den Mini-PC anschließen können. Die erste Version war mit einem Fünf-Megapixel-Sensor ausgestattet (2952 x 1944 Pixel). Restbestände sind im Handel teilweise für unter 20 Euro zu bekommen. Das aktuelle Modell trägt Versionsnummer 2.1, besitzt einen Acht-Megapixel-Sensor (3280 x 2464 Pixel) und ist für etwa 25 Euro zu haben.

Es ist in zwei Varianten mit und ohne Infrarotfilter erhältlich. Letztere ist an der dunklen Platine zu erkennen und für Aufnahmen in der Dämmerung und bei Nacht mit zusätzlicher Infrarotbeleuchtung gedacht. Es liegt ein kleiner IR-Filter aus Kunststoff bei, der Aufnahmen auch bei Tageslicht ermöglicht.

Der Anschluss der Kameras erfolgt über ein flaches Kabel an die 15-polige CSI-Schnittstelle (Camera Serial Interface) auf dem



Fotos und Videos: Das Kameramodul verwandelt den Raspberry Pi in einen Camcorder oder eine Webcam. Bei Bedarf verwenden Sie ein längeres Kabel zur Kamera.

Raspberry Pi. Der Pi sollte dann in einem Gehäuse untergebracht sein, das eine Durchführung für das Kabel besitzt. Es gibt auch Gehäuse mit einer Aussparung im Deckel, die ein aufklappbares Kameragehäuse aufnehmen können. Alternativ verwenden Sie ein eigenes Gehäuse für die Kamera. Sollte das Kabel zu kurz sein, gibt es im Handel längere Ersatzkabel.

Da sich an dem Anschluss seit der ersten Raspberry-Ausgabe nichts geändert hat, eignen sich die Kameras für die Modelle 1 bis 4. Damit das System die Kamera erkennt, gehen Sie im Menü auf „Einstellungen → Raspberry-Pi-Konfiguration“ und dann auf die Registerkarte „Schnittstellen“. Setzen Sie bei „Kamera“ die Option auf „Aktiviert“. Starten Sie Raspbian neu.

Im Terminalfenster nehmen Sie dann mit

```
raspistill -o bild.jpg
```

ein Bild auf oder mit

```
raspivid -t 10000 -o testvideo.mp4
```

ein Video mit einer Länge von zehn Sekunden. Wie Sie die Kamera für ein Überwachungssystem verwenden, lesen Sie unter *www.pcwelt.de/1925151*, die Anleitung für eine einfache Webcam finden Sie unter *www.pcwelt.de/2300255*.

Displays für den Raspberry Pi

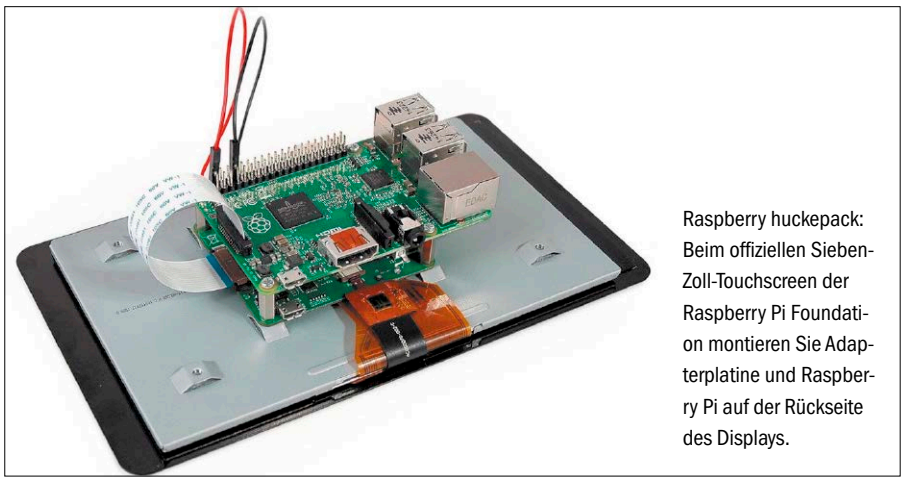
Der Raspberry Pi verfügt über eine HDMI-Buchse, an die Sie einen PC-Monitor oder ein TV-Gerät anschließen. Für spezielle Einsatzzwecke, etwa in Kraftfahrzeugen oder als öffentliches Infoterminal oder als Multimedia-Station, empfehlen sich kleinere Displays mit sieben bis zehn Zoll. Die gibt es auch als Touchscreen, was eine Bedienung ohne Maus und Tastatur erlaubt. Allerdings sollten Sie davon nicht allzu viel erwarten, weil sich die Raspbian-Oberfläche nicht besonders gut für die Fingerbedienung eignet. Ein Touchscreen kann jedoch sinnvoll sein, wenn Sie spezielle Anwendungen benutzen, die sich über große Bedienelemente bequem steuern lassen.

Der offizielle Touchscreen der Raspberry Pi Foundation misst sieben Zoll und bietet eine Auflösung von 800 x 480 Pixeln (etwa 70 Euro). Im Lieferumfang ist eine Adapterplatine enthalten, die hinten auf das Display geschraubt wird. Der Raspberry Pi wird darüber angebracht und per Flachbandkabel verbunden (siehe Abbildung). Zur Stromversorgung dienen zwei Kabel, die zu den GPIO-Pins führen. Es genügt dann ein Netzteil für beide Geräte.

Wer einen größeren Touchscreen benötigt, findet im Handel Geräte mit HDMI-Anschluss (um die 100 Euro). Die Touchscreen-Signale gelangen über ein USB-Kabel zum PC. Der Vorteil: Diese Geräte sind nicht nur für den Raspberry Pi, sondern für beliebige PCs geeignet. In der Regel ist ein Treiber für die Steuerung erforderlich, den der Hersteller für Raspbian beziehungsweise Linux liefern muss. Informieren Sie sich vor dem Kauf, ob das gewünschte Gerät Linux unterstützt und welche Erfahrungen andere Benutzer damit gesammelt haben.

Spezialdisplays: Wenn der Raspberry Pi zur Steuerung von Geräten oder zur Erfassung von Messwerten eingesetzt wird, kann ein Minidisplay in Scheckkartengröße ausreichend sein. Die gibt es als LCD-, OLED- oder besonders stromsparende E-Paper-Module in Größen etwa zwischen 1,3 und 4,3 Zoll (Diagonale), LCDs wahlweise auch als Touchscreen. Die Platine bei Displays mit 2,7 bis vier Zoll entspricht in etwa der Größe der Raspberry-Pi-Platine. Die Module kosten je nach Größe und Ausstattung etwa zwischen 20 und 100 Euro.

Die Displaymodule sitzen meist auf einer HAT-Platine (Hardware Attached on Top), die auf die GPIO-Pins (General Purpose Input Output) gesteckt wird. In ein normales Gehäuse passt die Sandwich-Konstruktion in der Regel nicht. Sie benötigen ein Gehäuse mit einer Aussparung über den GPIO-Pins und Abstandsbolzen, auf denen sich das Display verschrauben lässt.



Raspberry huckepack: Beim offiziellen Sieben-Zoll-Touchscreen der Raspberry Pi Foundation montieren Sie Adapterplatine und Raspberry Pi auf der Rückseite des Displays.

Stromsparende Anzeige: Ein E-Paper-Hat wird direkt auf die GPIO-Pins des Raspberry Pi gesteckt. Es eignet sich für die Anzeige von Benachrichtigungen oder Messwerten.

Für die kleinen Displays sind in der Regel spezielle Treiber erforderlich. Hersteller wie Waveshare (*www.waveshare.com/wiki/*) bieten in ihrem Wiki Links zum Treiberdownload sowie Raspbian-Images mit bereits integriertem Treiber. E-Paper-Displays lassen sich nur mit eigenen Programmen sinnvoll nutzen. Beispielcode in C++ und Python gibt es unter *https://github.com/waveshare/e-Paper*.

Mediacenter-PC fernbedienen

Die Mediacenter-Oberfläche Kodi (*https://libreelec.tv*) steuert man am bequemsten über eine Infrarot-Fernbedienung. Da die meisten TV-Geräte HDMI-CEC beherrschen, können Sie auch einfach die Fernbedienung des Fernsehers verwenden. Bei einigen Geräten müssen Sie die Funktion erst aktivieren. Weitere Infos dazu finden Sie im Handbuch des TV-Gerätes.

Sollte das nicht funktionieren oder wenn Sie den Raspberry Pi an einem PC-Monitor betreiben, können Sie die Infrarot-Fernbedienung Hama MCE Remote einsetzen (etwa 30 Euro). Der Infrarotempfänger wird per USB mit dem Raspberry Pi verbunden und die Fernbedienung ist sofort einsatzbereit.

Wer kein Geld ausgeben möchte, aber ein Smartphone besitzt, verwenden eine kostenlose App wie Kore (Official Remote for Kodi, *www.pcwelt.de/M2BG6x*) für das Android-Smartphone. Benutzer eines iPhones suchen im App Store nach „Official Kodi Remote“.

Baukästen, Sensoren und Aktoren

Der Raspberry kann Elektronikbasteleien und den Einstieg in die Programmierung verbinden. Für circa 80 Euro gibt es Starterkits inklusive Raspberry Pi 3, die ein Steckbrett („Breadboard“), Verbindungskabel, Widerstände, Schalter und LEDs enthalten. Starterkits mit unterschiedlicher Ausstattung ohne Raspberry Pi kosten etwa zwischen 20 und 50 Euro. Teilweise sind bereits einige Sensoren enthalten, für die aber auch eigene Sensorkits in ähnlicher Preislage verfügbar sind.

Diese Sensoren messen Temperatur und Feuchtigkeit, es gibt aber auch Schallsensoren, Fotowiderstände, Hallsensoren, Flammensensoren und vieles mehr. Das Angebot wird mit Aktoren wie Berührungsschalter, Infrarotempfänger und -Sender, Potentiometer, Joystick und Display abgerundet.

Die Bauteile sitzen auf kleinen Platinen mit Steckkontakten und lassen sich über das Steckbrett mit dem Raspberry Pi verbinden. Wer nur ein spezielles Projekt verwirklichen möchte, kann alle genannten Bauteile auch einzeln erwerben. Meist kosten diese nur wenige Euro. Zum Ausprobieren muss man Sensoren auch nicht auf Platinen lösten. Das Steckbrett reicht aus. Einen kleinen Überblick mit den 50 wichtigsten Sensoren und Modulen für den Raspberry Pi finden Sie über *www.pcwelt.de/rpimod*.

Es gibt direkte Links zu Shops, über die Sie die Bauteile beziehen können, Bilder vom Aufbau und Tutorials mit Programmierbeispielen. ■

Mediacenter: Mit einer Infrarotfernbedienung lässt sich Kodi komfortabel bedienen. Die Hama MCE Remote wird von Kodi automatisch erkannt und muss nicht konfiguriert werden.

Basteln mit dem Raspberry Pi: Starterkits bieten alle Bauteile für den Einstieg in die hardwarenahe Programmierung und Steuerung von Geräten. Sensorkits erweitern die Möglichkeiten.

RASPBERRY PI UND ZUBEHÖR ONLINE KAUFEN

Wer nach Raspberry-Zubehör sucht, wird am schnellsten im Internet fündig. Fast alle bekannten Onlinehändler haben die in diesem Beitrag genannten Geräte und Starterkits im Angebot.

Das breiteste Angebot findet man bei einem offiziellen „Raspberry Pi Approved Reseller“. Welche das sind, erfahren Sie auf *www.raspberrypi.org/products* nach der Produktauswahl („More info“) und Klick auf „Buy now“. Wählen Sie das gewünschte Modell und Land, um sich die Shops anzeigen zu lassen.

Der Raspberry Pi ist übrigens „Made in Wales“ und auch das Zubehör kommt teilweise aus Großbritannien. Im Moment ist noch nicht abzusehen, wie sich ein ungeregelter Brexit auf die Preise auswirken wird. Wer direkt bei einem britischen Versender bestellt, muss dann mit Einfuhrsteuern rechnen. Durch Zoll, Steuer und längere Transportzeiten könnten sich die Produkte auch in deutschen Shops verteuern.

Gehäuse für jedes Raspberry-Projekt

Der Raspberry Pi beschäftigt uns in seinen vielen Varianten seit der ersten Version. Das Thema „Gehäuse“ stand bislang nicht im Fokus, gewinnt aber beim Modell 4 an Bedeutung. Denn der aktuelle Raspberry ist ein kleiner Heizkörper.

VON STEPHAN LAMPRECHT

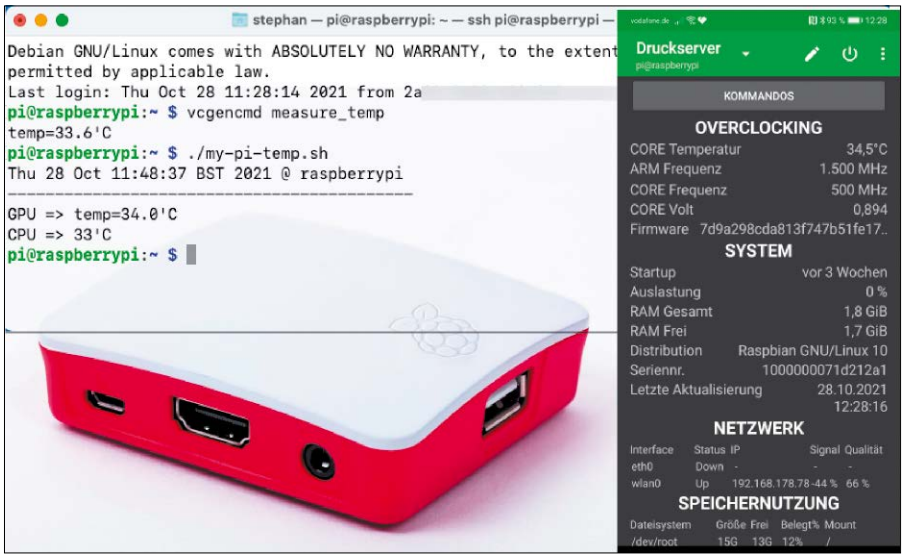
Seit seiner ersten Vorstellung hat der Raspberry Pi einen ordentlichen Leistungssprung gemacht. So kann der Raspberry Pi im Heimnetzwerk energieeffizient zentrale Serverdienste zur Verfügung stellen. Ein passendes Gehäuse ist Pflicht, wenn der kleine Rechenknecht zuverlässig laufen soll. Für den Dauerbetrieb ist eine Lösung mit passiver oder aktiver Kühltechnik zu empfehlen.

Warum Sie ein Gehäuse brauchen

Es mag auf den ersten Blick das Umfeld beeindrucken, wenn das selbst gebastelte NAS aus einem Wirrwarr an Kabeln und Festplatten besteht. Dieser Zustand sollte aber nur die Zeit eines Funktionstests überdauern. Danach ist ein Gehäuse nicht nur aufgeräumter: Sie verlängern auch die Lebensdauer des kleinen Computers, wenn Sie ihn vor Staub schützen. Denn der legt sich wie eine Decke auf CPU und Speicherchips und behindert den Wärmeaustausch. Ein Gehäuse schützt auch davor, aus Versehen einen Kurzschluss auszulösen.

Überzeugt? Die Suche nach einem Gehäuse führt Sie schnell zum offiziellen Gehäuse der Raspberry-Entwickler im Vanille-Himbeer-Look. Allerdings besteht dieses Gehäuse aus Kunststoff, der keine Wärme ableitet. Mit diesem oder einem ähnlichen Case lösen Sie zwar die Problematik mit Staub und Kurzschlüssen, nehmen der Platine aber die Luft zum Atmen.

Tipp: Zur Kontrolle der Temperatur bietet sich für alle Nutzer eines Android-Smartphones der Einsatz von Raspi Check an. Es überwacht eine oder mehrere Platinen im Heimnetz. Dazu muss der Open-SSH-Server im Raspberry-System aktiviert sein. Einmalig werden in der App die IP-Adresse oder Hostname sowie die Zugangsdaten für den SSH-Nutzer hinterlegt. Dann kann jederzeit ein Blick auf die vom Gerät diagnostizierte Temperatur geworfen werden.



Die Temperatur des Raspberry Pi 4 sollte bei hoher Last häufiger kontrolliert werden. Das geht per SSH im Terminal ebenso wie mit einer Android-App.

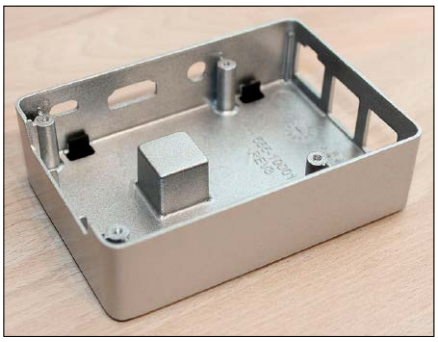
Kühle Platine, coole Leistung

Wenn Sie im Internet mit den Stichwörtern „Raspberry Thermal“ nach Bildern suchen, werden Sie viele Fotos von Wärmebildkameras finden, die beeindruckende Temperaturen der Platine zeigen, was insbesondere die Zentraleinheit (SoC) betrifft. Der Pi selbst taktet bei einer Temperatur von 85 Grad Celsius automatisch herunter. Temperaturen unter diesem Wert sind problemlos, alles darüber mehr oder weniger tödlich. Unter Volllast zieht ein Raspberry 4 etwa sechs Watt. Das klingt nicht nach viel, ist aber beachtlich. Dient die Platine dann als NAS oder Druckerserver, erhitzen sich auch noch die Bauteile für USB und WLAN. Grob vereinfacht erhitzt sich das SoC im Verhältnis zu seiner Größe stärker als die Herdplatte Ihres Ceranfeldes in der Küche. Glauben Sie nicht? Dann teilen Sie die 2000 Watt des Herdes durch die Fläche der kleinen Platte mit 20 Zentimetern Durchmesser. Danach vergleichen Sie es mit den sechs Watt des Raspberry, geteilt durch die Fläche der etwa 1,4 Zentimeter großen Zentraleinheit.

Eine passive Kühlung nutzt das physikalische Prinzip der Wärmeleitung. Kurz gesagt, fließt „Wärme“ immer in Richtung geringerer Temperatur. Je größer die Kon-

Quelle: Amazon

Das optisch ansprechende Gehäuse von Flirc ist solide gearbeitet und bietet eine gute passive Kühlung für den Raspberry Pi 4.



Das Flirc-Case hat eine würfelförmige Einbuchtung, die exakt auf SOC und CPU der Platine drückt und die Wärme auf das gesamte Gehäuse ableitet.

Quelle: Amazon

Geekworm NASPi: Diese teure Lösung (über 60 Euro) macht aus dem Raspberry ein Mini-NAS. Ein einfaches Alu-Gehäuse gibt es von Geekworm ab circa 13 Euro.

taktfläche zwischen der Wärmequelle und je größer die Temperaturdifferenz, desto mehr Wärme kann abfließen. Aluminium bietet eine hohe Leitfähigkeit, zudem sind Gehäuse aus diesem Material robust und temperaturbeständig. Im Fachhandel werden in der Regel zweiteilige Konstruktionen angeboten: Die Platine wird fest mit Spezialschrauben mit der Unterschale verbunden. Der obere Gehäuseteil dient der Wärmeabgabe. Ein aus der Oberschale hervorstehender Zapfen stellt die Verbindung mit dem SoC her.

Gehäuse mit Passivkühlung: Bei uns leistet in verschiedenen Projekten das Aluminium-Case von **Flirc** zuverlässige Dienste (circa 21 Euro). Auch das Modell von **Geekworm** hat sich im Praxiseinsatz bewährt. Das einfache Geekworm-Aluminiumgehäuse gibt es ab etwa 13 Euro. Wer möchte, kann den Raspberry für gut 60 Euro in ein NAS-artiges Gehäuse einbauen (Geekworm NASPi). An weiteren Alternativen herrscht im Fachhandel kein Mangel. Auf jeden Fall prüfen Sie am besten anhand von Bewertungen oder einer Sichtung des Lieferumfangs, ob das Gehäuse die daran gestellten Aufgaben auch erfüllt. Bei besonders preiswerten Importen aus China sind die mitgelieferten Klebepads, die der besseren Wärmeübertragung an das Gehäuse dienen sollen, nichts anderes als Teppichklebebänder. Die haften zwar gut, leiten aber keine Wärme ab.

Achtung WLAN: Den Raspberry in ein passiv kühlendes Metallgehäuse zu stecken, ist unter dem Gesichtspunkt der Wärmeableitung eine vielversprechende Idee. Allerdings darf ein Problem nicht übersehen werden. Da der Raspberry Pi keine separaten Antennen für den Empfang von WLAN besitzt, kann das Gehäuse den WLAN-Empfang stören. Metallgehäuse sind also nur dort erste Wahl, wo kein WLAN benötigt wird.

Aktive Kühlung für Hochleistung: Die mit einem hochwertigen Gehäuse zu erzielende passive und lautlose Kühlung dürfte für die meisten Szenarien als Homeserver ausreichen. Wenn die Platine allerdings dauerhaft unter Volllast läuft oder weitere Bauteile für zusätzliche Wärme sorgen, dann genügt passive Diffusion eventuell nicht mehr. Dann muss ein aktiver Lüfter her, der die entstehende Wärme einfach fortbläst, was der Physiker vornehmer als „Konvektion" bezeichnet. Die meiste Wärme schaffen Sie demzufolge mit einem Aluminiumgehäuse fort, das zusätzlich einen Lüfter besitzt.

Auch hier hält der Handel unzählige Modelle parat. Aber Achtung: In den Produktbeschreibungen wird gerne der Eindruck erweckt, es sei alles Notwendige in der Box. Der erstaunte Kunde wundert sich dann, wenn der versprochene Lüfter fehlt. High-End, solide verarbeitet plus die Möglichkeit, auch von außen an die GPIO-Pins zu gelangen, ist das Gehäuse **Argon One Case** (circa 26 Euro). Es kombiniert aktive und passive Kühlung. Das als Kickstarter-Projekt gestartete Gehäuse sieht gut aus und lässt die Platine auch bei besonders fordernden Aufgaben kühl. Eine klare Empfehlung unsererseits.

Sonderfälle: Die obige Auswahl orientiert sich am typischen Heimserver: Der Raspberry versieht ohne Erweiterungsplatinen seine Dienste in einem geschlossenen Raum. Wenn Sie den Raspberry als Streamingclient für die Stereoanlage verwenden und ein DAC aufgesteckt wurde, benötigen Sie ein Gehäuse, das die Anschlüsse der Huckepack-Platine nach außen führt und mit der Abwärme umgehen kann. Hier sollten Sie sich für Modelle aus Metall und Kühlkörpern entscheiden.

Andere Spezialfälle sind Einsätze in freier Natur. Abgesehen von der Stromversorgung müssen Sie sich in diesem Fällen auch mit dem Nässeproblem befassen, also nach Gehäusen mit einer entsprechenden IP-Schutzklasse suchen. ■

Das Gehäuse Argon One ist etwas teurer als einfache Plastik-Cases, aber mit aktivem Lüfter gekühlt.

Software und Paketverwaltung

Neue Anwendungen und Updates beziehen Sie unter Linux in der Regel aus dem Software-Repository der jeweiligen Distribution. Für die Verwaltung gibt es mehrere Tools mit unterschiedlichen Funktionen.

VON THORSTEN EGGELING

Fast alle Linux-Distributionen verwenden eine zentrale Paketverwaltung, über die Sie die gewünschte Software beziehen, installieren und aktualisieren. Die Vorteile: Sie erhalten geprüfte und virenfreie Programmpakete, die reibungslos mit dem Betriebssystem zusammenarbeiten. Sicherheitsupdates gibt es automatisch für jedes installierte Programm.

Es gibt aber auch Nachteile. Bei Distributionen wie Ubuntu, Linux Mint oder Debian sind Sie in der Regel auf die Programmversionen festgelegt, die zur jeweiligen Version des Betriebssystems gehören. Neuere Versionen gibt es erst beim nächsten Upgrade der Distribution. Ausnahmen sind beispielsweise Firefox und Thunderbird. Wer aktuellere Programme benötigt oder in der Paketverwaltung nicht fündig wird, kann jedoch zusätzliche Paketquellen einbinden oder Software auf anderen Wegen installieren (siehe Artikel ab Seite 46 und 48).

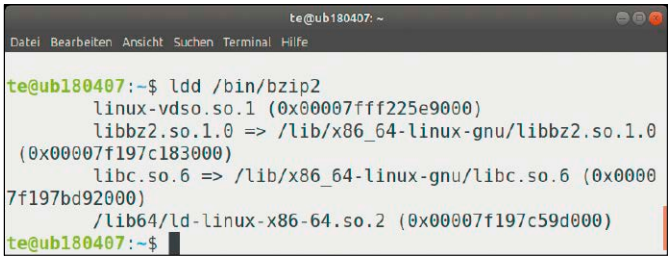
Für die Paketverwaltung bieten Ubuntu und verwandte Distributionen mehrere Tools für unterschiedliche Zielgruppen und mit unterschiedlichen Funktionen. Teilweise ist es Geschmackssache, welchem Programm der Vorzug zu geben ist. Es gibt aber auch Aufgaben, die sich nur mit einem bestimmten Tool erledigen lassen.

1. Programme und Bibliotheken

Ausführbare Programmdateien enthalten unter Linux in der Regel nicht alle nötigen Komponenten. Meist ist zusätzlich wenigstens eine Standardbibliothek erforderlich, die Funktionen für in der Programmiersprache C geschriebene Programme enthält. Genauere Informationen liefert beispielsweise diese Befehlszeile:

```
ldd /bin/bzip2
```

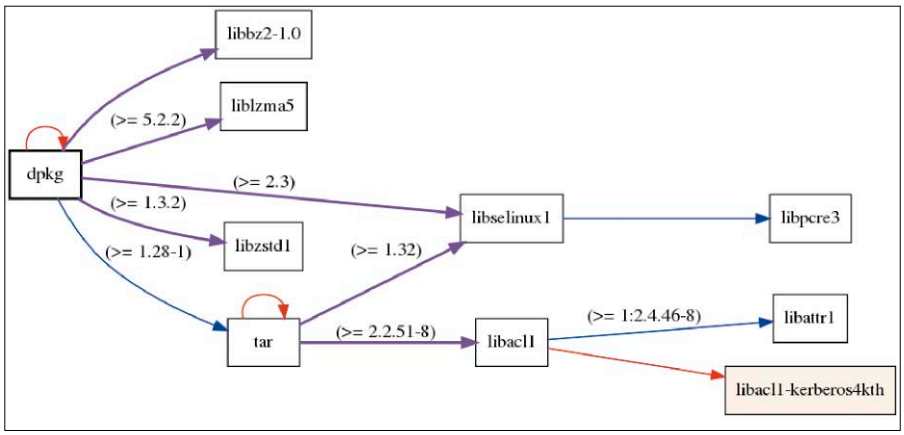
In der Ausgabe sehen Sie alle Programmbibliotheken, die das Komprimierungstool bzip2 benötigt. Darunter ist die Standardbibliothek „libc.so.6“ zu finden, „linux-vdso.so.1“ stellt einige Kernel-Funktionen bereit und „ld-linux-x86-64.so.2“ ermöglicht es, Bibliotheken bei Bedarf zu laden („dynamic shared“). Die Komprimierungsfunktion ist in der Bibliothek „libbz2.so.1.0“ zu finden, die auch andere Programme nutzen können. Programme benötigen genau die Bibliotheken, mit den denen sie erstellt wurden, oder eine höhere, abwärtskompatible Version. Das Konzept der dynamisch ladbaren, gemeinsam genutzten Bibliotheken verringert die Größe der Programmdateien und ermöglicht eine effiziente Hauptspeichernutzung.



Abhängigkeiten: Die meisten Programme benötigen zusätzliche Bibliotheken. Die Paketverwaltung sorgt für die automatische Installation der abhängigen Pakete.

2. Das Debian-Paketformat

Bei Installation oder Update lädt die Paketverwaltungssoftware bei Debian/Ubuntu-Systemen eine „deb"-Datei herunter. Es handelt sich um ein gepacktes Archiv, das ausführbare Dateien, Bibliotheken und Konfigurationsdateien enthalten kann, die bei der Installation in das Dateisystem kopiert werden. Ebenfalls enthalten sind meist einige Scripts, über die sich beim Setup beispielsweise Konfigurationsdateien anpassen oder Systembenutzer erstellen lassen. Ein weiterer Bestandteil ist eine Textdatei mit Informationen über die Abhängigkeiten von anderen Paketen sowie optionalen Empfehlungen für zusätzliche Pakete.



Dependency Tree: Damit ein Linux-Programm läuft, sind meist zusätzliche Tools und Bibliotheken ab einer bestimmten Version erforderlich. Welche das sind, lässt sich mit debtree ermitteln.

3. Die Paketverwaltung bei Ubuntu

Bei der Softwareinstallation muss die Paketverwaltung die ausführbaren Dateien auf die Festplatte kopieren und dafür sorgen, dass alle benötigten Bibliotheken und Tools vorhanden sind. Bei komplexeren Programmen ergibt sich ein verzweigter Baum von Abhängigkeiten („dependency tree") und die Paketverwaltung installiert mehrere Pakete.

Wer es genauer wissen möchte, kann mit dem Befehl

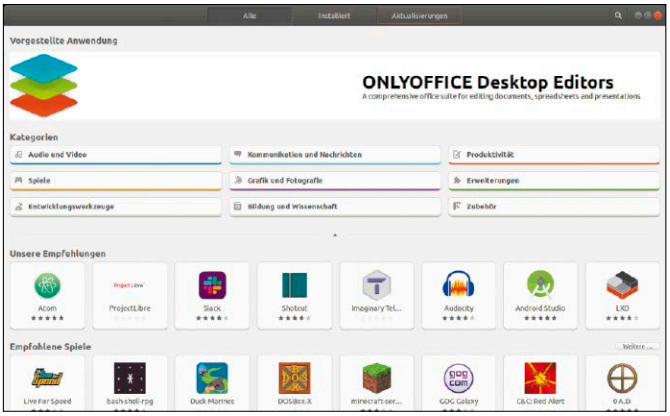
```
debtree [Paketname] | dot -Tpng >
 bild.png
```

eine grafische Darstellung der Abhängigkeiten eines Pakets erstellen. Die Pakete „debtree" und „graphviz" müssen dafür installiert sein.

Das zentrale Programm zur Paketverwaltung heißt unter Ubuntu und verwandten Systemen dpkg. Es verwendet Datenbanken, in denen verfügbare und installierte Pakete gespeichert sind. dpkg lädt jedoch keine Paketdateien herunter und prüft keine Abhängigkeiten. Deshalb werden Sie das Tool nur selten direkt nutzen (siehe auch ab Seite 48). Stattdessen verwenden Sie eines der Programme, die wir in den nächsten Punkten beschreiben.

4. Die Standard-Paketverwaltung von Ubuntu

Anwendungen für die grafische Oberfläche lassen sich in Ubuntu mit Ubuntu-Software installieren, entfernen und aktualisieren. Sie starten es über das Icon in der Starterleiste. Auf der Registerkarte „Alle" zeigt das Tool Kategorien wie „Audio und Video" und „Grafik und Fotografie". Klicken Sie eine Kategorie an und stöbern Sie in der Liste nach für Sie interessanten Anwendungen. Wenn Sie den Namen eines Programms kennen, können Sie auch die Suchfunktion verwenden (Lupensymbol auf der Startseite). Empfehlenswert ist auch ein Blick in die



Programme installieren: Ubuntu-Software ermöglicht eine komfortable Programmauswahl. Das Angebot ist hier aber nicht vollständig und enthält beispielsweise keine Terminaltools.

PAKETVERWALTUNG IN ANDEREN DISTRIBUTIONEN

Bei allen verbreiteten Linux-Distributionen erfolgt die Paketverwaltung ähnlich wie bei Debian/Ubuntu. Es gibt jedoch andere Paketformate und Tools für deren Verwaltung. Bei Fedora dient Gnome-Software als Standardtool, das auch die Basis von Ubuntu-Software bildet. Nutzer des KDE-Desktops nutzen Plasma Discovery. Im Terminalfenster kommt hier dnf, der Nachfolger von yum, zum Einsatz. dnf ähnelt in der Bedienung apt. Für die Installation beispielsweise verwendet man

```
sudo dnf install [Paketname]
```

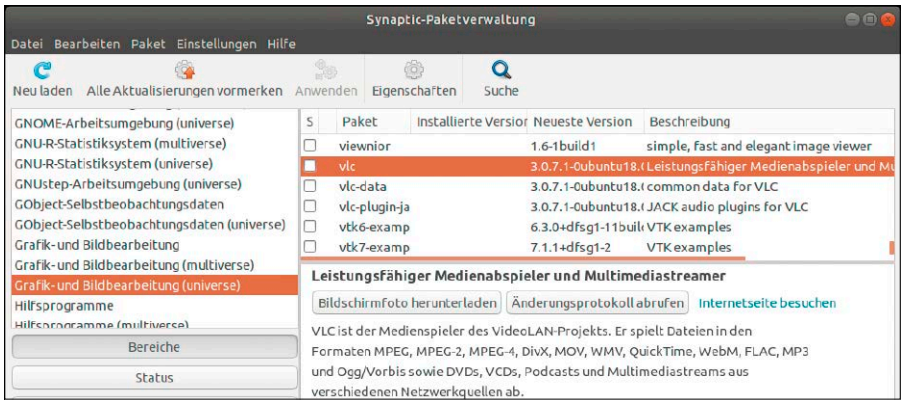
Als Paketformat verwendet Fedora RPM (RPM Package Manager, früher Red Hat Package Manager). RPM wird auch von Open Suse genutzt, zur Paketverwaltung dient hier Yast2 und auf der Kommandozeile Zypper.

Auch Gentoo Linux kennt eine Softwareverwaltung, die allerdings etwas anders funktioniert. Das Tool emerge greift auf einen täglich aktualisierbaren Portage-Tree zu, in dem Infos zu Quelltextarchiven und Abhängigkeiten hinterlegt sind. Bei der Installation werden die Binärdateien aus dem Quelltext erstellt. Das ermöglicht sehr aktuelle Softwareversionen, birgt aber auch ein hohes Fehlerpotenzial. Letztlich ist der Benutzer selbst dafür verantwortlich, dass alles reibungslos zusammenpasst.

Kategorie „Erweiterungen“. Hier finden Sie neue Schriftarten und nützliche Shell-Erweiterungen.

Ein Klick auf das Programmsymbol führt zu weiteren Informationen (häufig mit Screenshot), Beschreibungen und Rezensionen. Unter „Details“ erfahren Sie jeweils, um welchen Pakettyp es sich handelt. Wenn hinter „Quelle“ beispielsweise „ubuntu-bionic-universe“ oder ähnlich steht, handelt es sich um ein herkömmliches „deb“-Paket. Sollte die Angabe „Snap-Store“ lauten, dann handelt es sich um einen Snap-Container (siehe ab Seite 46).

Klicken Sie auf „Installieren“, um eine Software einzurichten. Sollte diese bereits vorhanden sein, sehen Sie die Schaltflächen „Starten“ und „Entfernen“. Die Registerkarte „Installiert“ (Startseite) zeigt Ihnen eine Liste der installierten Anwendungen, per Klick auf „Entfernen“ können Sie ein Programm deinstallieren. Auf der Registerkarte „Aktualisierungen“ sehen Sie die verfügbaren Updates. Klicken Sie auf die Schaltfläche links oben im Fenster, um die Paketdatenbank zu aktualisieren.



Alles installieren: Synaptic bietet eine schnelle Suche nach allen verfügbaren Anwendungen, Tools und Bibliotheken. Software lässt sich außerdem über „Bereiche“ auswählen.

5. Softwarepakete mit Synaptic verwalten

Synaptic ist bei Linux Mint 19 bereits vorinstalliert, Ubuntu-Nutzer können das Tool über Ubuntu-Software nachinstallieren. Synaptic bietet eine Suchfunktion und mehrere Filter, über die sich die Ansicht auf die gewünschte Software einschränken lässt. Das Tool ist im Vergleich zu Ubuntu-Software etwas unübersichtlicher, dafür liefert aber die Suche schnellere Ergebnisse. Anders als mit Ubuntu-Software lassen sich mit Synaptic alle verfügbaren Programme installieren, also auch Tools für die Kommandozeile, Bibliotheken und Entwicklerpakete.

Nach dem Start von Synaptic klicken Sie zuerst auf „Neu laden“, um die Paketdatenbank zu aktualisieren, und danach auf die Schaltfläche „Suche“. Tippen Sie einen Suchbegriff ein und klicken Sie auf „Suchen“. Sie können den Namen eines Programms verwenden oder einen Begriff, der in der Beschreibung vorkommen sollte. Synaptic kann auch alle verfügbaren Programme aus einer Kategorie anzeigen. Dazu klicken Sie auf „Bereich“ und wählen beispielsweise „Grafik- und Bildbearbeitung“. In der Regel ist alles aus dieser Kategorie bereits installiert. Weitere Software gibt es unter „Grafik- und Bildbearbeitung (universe)“ sowie „Grafik- und Bildbearbeitung (multiverse)“. Programme aus dem Bereich „multiverse“ unterliegen lizenzrechtlichen Einschränkungen, was beispielsweise für Multimedia-Codecs gelten kann. In der Kategorie „universe“ ist freie Software ohne solche Einschränkungen zu finden. Für Endanwender in Deutschland hat diese Unterscheidung jedoch keine Konsequenzen. Sie können alle installierbaren Programme uneingeschränkt und kostenlos nutzen. Es kann jedoch Länder oder Einsatzbereiche geben, die Programme aus dem Bereich „multiverse“ nicht erlauben.

Software installieren und entfernen: Wenn Sie fündig geworden sind, klicken Sie das gewünschte Paket mit der rechten Maustaste an und wählen „Zum Installieren vormerken“. In der Regel öffnet sich ein Fenster, das eine Liste mit weiteren erforderlichen Paketen anzeigt. Klicken Sie auf „Vormerken“ und danach in der Synaptic-Symbolleiste auf „Anwenden“. Das Fenster „Zusammenfassung“ zeigt ihnen die anstehenden Änderungen. Klicken Sie auf „Anwenden“, um die Installation anzustoßen.

Für die Deinstallation wählen Sie im Kontextmenü eines Pakets „Zum Entfernen vormerken“ und klicken danach auf „Anwenden“. Prüfen Sie im Fenster „Zusammenfassung“ die Angaben unter „Zu entfernen“. Hier sollten nur das gewählte Paket und wenige weitere Pakete aufgeführt sein.

PROBLEME BEI DER INSTALLATION BEHEBEN

Bei der Vielzahl der Softwarepakete ist nicht ausgeschlossen, dass es bei Installationen oder Updates zu Fehlern kommt. Meist sind nur Pakete betroffen, die selten installiert werden und nicht ausreichend gepflegt sind. Die Installation kann beispielsweise fehlschlagen, wenn eine Abhängigkeit besteht, die nicht erfüllt werden kann. Das Problem lässt sich meist mit

```
sudo apt-get -f install
```

lösen. Dabei wird das defekte Paket entfernt. Sollte das nicht funktionieren, verwenden Sie

```
sudo dpkg -r [Paketname]
```

Damit löschen Sie das Paket ohne Prüfung der Abhängigkeiten.

Bei Problemen mit Abhängigkeiten können Sie nur darauf warten, dass der Paketbetreuer den Fehler behebt. Oder Sie suchen nach einer alternativen Quelle für die Software (siehe ab Seite 48).

Eine häufige Fehlermeldung bei der Verwendung von apt ist „Konnte Sperre /var/lib/dpkg/lock-frontend nicht bekommen“ oder ähnlich. Ursache dafür ist meist ein automatisches Update im Hintergrund. Warten Sie einige Zeit, bis das Update abgeschlossen ist, und versuchen Sie es dann erneut. Die Meldung erscheint auch, wenn ein anderes Tool die Paketverwaltung gesperrt hat (beispielsweise Synaptic) oder wenn Sie apt ohne vorangestelltes „sudo“ starten.

Ist die Liste sehr lang, besteht die Gefahr, dass wichtige Pakete dabei sind, und die Deinstallation die Funktionen des Betriebssystems beeinträchtigt. In diesem Fall sollten Sie die Deinstallation besser abbrechen. Bei systemrelevanten Programmen gibt Synaptic ohnehin eine Warnmeldung aus. Die Frage „Sind Sie sicher, dass Sie das tun wollen?“ sollte Sie immer alarmieren und ist besser mit „Nein“ zu beantworten.

Im Kontextmenü gibt es außerdem den Punkt „Zum vollständigen Entfernen vormerken“. Damit entfernen Sie Programmdateien inklusive Konfiguration. Verwenden Sie diese Funktion, wenn Sie ein Programm auch in Zukunft nicht mehr verwenden wollen oder wenn Sie Fehler in der Konfiguration vermuten, die sich auch nach einer Neuinstallation auswirken können. Synaptic löscht jedoch nur die systemweite Konfiguration. Konfigurationsdateien in den Benutzerverzeichnissen unter „/home“ müssen Sie manuell entfernen.

6. Softwarepakete im Terminalfenster verwalten

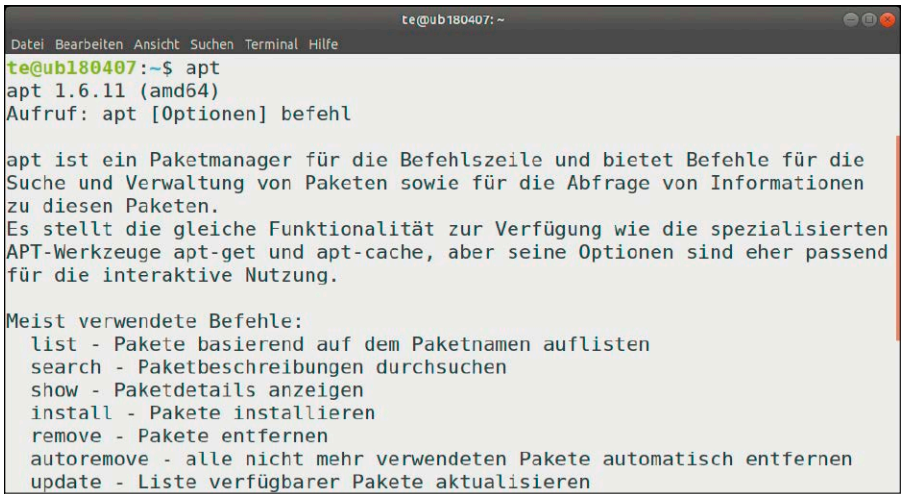
Bei der SSH-Fernwartung eines Servers im Netzwerk sind Sie auf Kommandozeilentools angewiesen. Diese leisten aber auch auf einem Arbeitsrechner gute Dienste, weil Installationen über die Kommandozeile schneller und bequemer ablaufen als über die Tools für die grafische Oberfläche. Meist werden Sie unter Ubuntu, Linux Mint oder Debian das Tool apt einsetzen. Starten Sie es in einem Terminalfenster ohne weitere Optionen, um einen kurzen Hilfetext zu erhalten. Für die Installation einer Software verwenden Sie

```
sudo apt update
sudo apt install [Paketname]
```

Die erste Zeile aktualisiert die Paketdatenbank, die zweite installiert das im Platzhalter „[Paketname]“ angegebene Paket. Sie können auch mehrere Paketnamen hintereinander verwenden – durch schlichtes Leerzeichen getrennt. Für die Deinstallation verwenden Sie

```
sudo apt remove [Paketname]
```

Auch hier sollten Sie vorsichtig sein, wenn apt mehr als ein Paket entfernen möchte. apt gibt jedoch eine deutliche Warnung aus, wenn Sie versuchen, systemrelevante Pakete zu entfernen. Wenn bei der Deinstallation unnötige Pakete zurückbleiben, gibt apt eine Liste unter „Die folgenden Pakete wurden automatisch installiert und



Schnelle Paketverwaltung: apt ist im Terminal einfach zu verwenden und bietet den meisten Komfort, wenn Sie mehrere Programme auf einmal einrichten wollen (apt install [Paketnamen]).

werden nicht mehr benötigt:“ aus. Diese Pakete lassen sich mit

```
sudo apt autoremove
```

entfernen. Diesen Befehl sollten Sie in regelmäßigen Abständen verwenden, besonders nach mehreren Kernel-Updates. Wenn der aktuelle Kernel stabil läuft, entfernen Sie damit alte Kernel-Pakete, was Platz auf der Festplatte einspart. Mit dem Befehl

```
apt list [Suchmuster]
```

können Sie nach Softwarepaketen suchen. Verwenden Sie für den Platzhalter „[Suchmuster]“ beispielsweise *gimp*. apt gibt dann alle Paketnamen aus, in denen „gimp“ an beliebiger Stelle vorkommt. Entsprechendes leistet

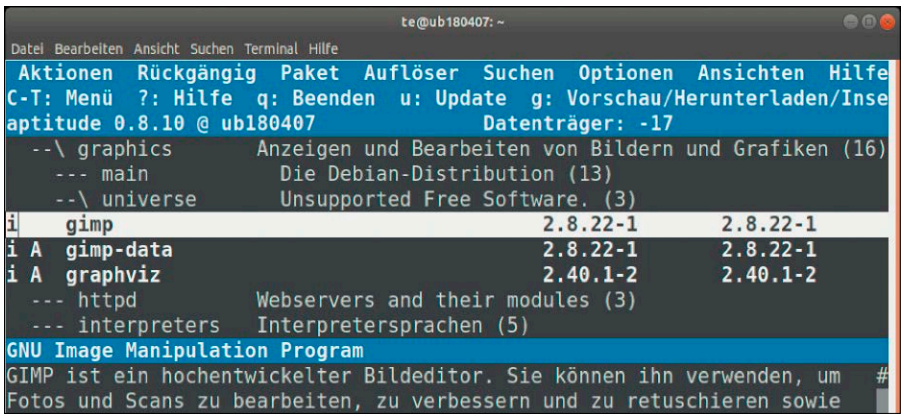
```
apt search [Suchmuster]
```

für die Suche in den Paketbeschreibungen. Das Kommandozeilentool apt-get bietet alle für apt beschriebenen Funktionen und noch ein paar mehr. Es gibt beispielsweise „purge“ für die vollständige Entfernung von Paketen und „download“, wenn Sie ein „deb“-Paket vorerst nicht installieren, sondern nur herunterladen wollen. Ebenfalls nützlich ist dieser apt-Befehl:

```
sudo apt-get clean
```

Dies löscht den Paketcache und räumt damit Festplattenplatz frei.

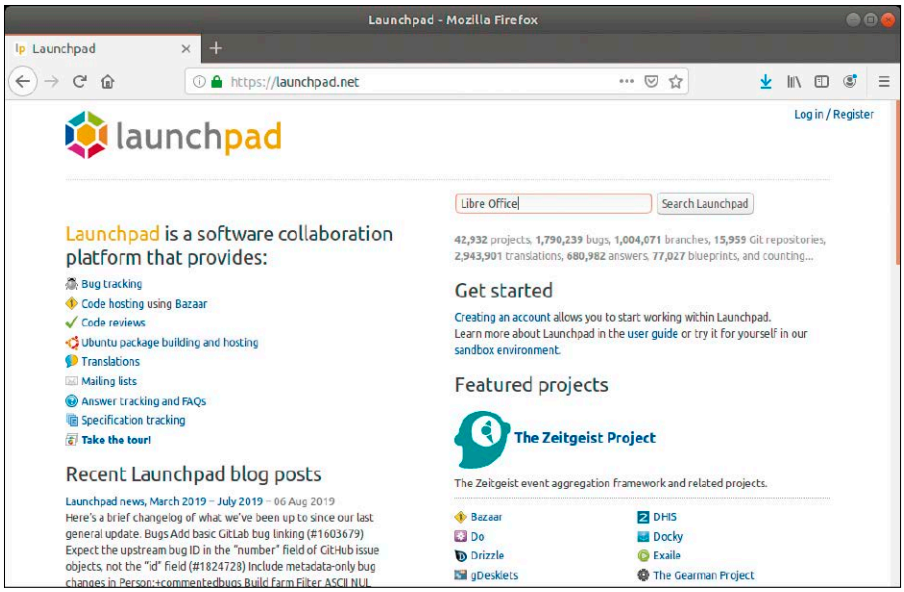
Wer eine Paketverwaltung mit Menüsteuerung im Terminal bevorzugt, kann aptitude installieren. Das Menü rufen Sie per Strg-T auf. Alternativ verwenden Sie Tastaturkürzel, die aptitude bei den einzelnen Menüpunkten anzeigt. Drücken Sie die Taste „/“, um nach Paketen zu suchen, und die Taste „N“ für „Weitersuchen“. Mit der Plus-Taste („+“) markieren Sie ein Paket für die Installation, dann drücken Sie die Taste „G“ für eine Vorschau der Änderungen und noch einmal die Taste „G“, um die Installation durchzuführen. Über die Minus-Taste („-“) lassen sich Pakete für die Deinstallation auswählen. ■



Alternative fürs Terminal: aptitude ist nicht besonders übersichtlich, bietet aber im Terminal eine menügeführte Paketverwaltung mit Programminfos und eine Suchfunktion.

Zusätzliche Paketquellen verwenden

Die Standard-Paketquellen von Ubuntu stellen die wichtigsten Programme bereit. Sollten Sie hier etwas nicht finden, binden Sie weitere Paketquellen ein oder Sie installieren Pakete manuell.



Neue Softwarepakete: Was Sie in den Ubuntu-Paketquellen nicht finden, gibt es wahrscheinlich bei Launchpad. Binden Sie für Installation und Updates die gewünschte Paketquelle ein.

VON THORSTEN EGGELING

Die Softwareinstallation über die Ubuntu-Paketverwaltung aus den Standardrepositorien ist der bequemste und sicherste Weg. Manchmal fehlt jedoch das gewünschte Programm oder es gibt nur eine veraltete Version. Sie sind jedoch nicht auf das angewiesen, was der Distributor bereitstellt. Für neue Software lassen sich weitere Paketquellen konfigurieren oder deb-Pakete manuell installieren.

Service: Eine Textdatei mit allen Befehlszeilen aus diesem Artikel laden Sie über *http://www.pcwelt.de/mQYUqt* herunter.

Zusätzliche Paketquellen einbinden

Sie können jede Paketquelle einbinden, die ein Repository im Ubuntu/Debian-Format betreibt und für Ihre Systemversion passende Software bereitstellt. Beim Update der Paketdatenbank prüft die Paketverwaltung die Gültigkeit der GPG-Schlüssel von Paketquellen und Paketlisten. In den Paketlisten sind Hash-Werte der „deb"-Pakete hinterlegt, die ebenfalls berücksichtigt werden. Sollte der GPG-Schlüssel einer Softwarequelle nicht vorhanden oder ungültig sein, lässt sich die Paketquelle nicht verwenden und die darüber angebotene Software nicht installieren.

Am einfachsten ist die Installation von Fremdpaketen über ein Launchpad-PPA (Personal Package Archive). Die Website *https://launchpad.net* wird vom Ubuntu-Distributor Canonical betrieben und ist die bevorzugte Plattform für Entwickler, die Softwarepakete für Ubuntu und verwandte Distributionen bereitstellen möchten.

Verwenden Sie die Suchfunktion auf der Startseite, um herauszufinden, ob es ein PPA für die gewünschte Software gibt. Die Suche beispielsweise nach „Libre Office" und Klick auf den Link „LibreOffice Packaging in Launchpad" führt zu einer Übersichtsseite. Unter „Personal package archives" klicken Sie auf „LibreOffice 6.3.x", wenn Sie die zurzeit aktuellste Version von Libre Office installieren möchten. Unter „Overview of published packages" öffnen Sie hinter „Published in:" eine Liste mit den Ubuntu-Versionen, für die Pakete verfügbar sind. Bei diesem PPA ist die älteste Version „Bionic" (Ubuntu 18.04). „LibreOffice 6.2.x" gibt es dagegen auch für Xenial (Ubuntu 16.04). Wenn die Version passt, verwenden Sie im Terminalfenster die Befehlszeile unter „Adding this PPA to your system", beispielsweise

```
sudo add-apt-repository
  ppa:libreoffice/libreoffice-6-3
```

Bestätigen Sie mit Eingabetaste, dass Sie das PPA verwenden wollen. Es wird dann über die Textdatei „/etc/apt/sources.list.d/libreoffice-ubuntu-libreoffice-6-3-bionic.list" als neue Paketquelle eingebunden, der zugehörige GPG-Schlüssel ist unter „/etc/apt/trusted.gpg.d" zu finden. Abweichend von der Ubuntu-Dokumentation aktualisiert add-apt-repository bei Ubuntu 18.04 die Paketdatenbank automatisch. Sollte das bei Ihnen nicht der Fall sein (oder unter einer älteren Ubuntu-Version), dann verwenden Sie diesen Befehl:

```
sudo apt update
```

Da Libre Office wahrscheinlich bereits installiert ist, genügt dann

```
sudo apt upgrade
```

für das Upgrade. Andernfalls verwenden Sie folgende Zeile

```
sudo apt install libreoffice
```

für unser Beispiel.

Paketquellen manuell einbinden

Sollte es kein Launchpad-PPA für die gewünschte Software geben, finden Sie bei Anbietern von Linux-Software oft Adressen für deren eigene Repositorien. Der Ablauf ist immer der gleiche: Zuerst importieren Sie den GPG-Schlüssel und konfigurieren dann die neue Paketquelle.

Wer beispielsweise Google Chrome verwenden möchte (siehe auch den übernächsten Punkt), importiert zunächst den Schlüssel:

```
wget -q -O - https://dl-ssl.google.
 com/linux/linux_signing_key.pub
 | sudo apt-key add -
```

Mit folgendem Befehl erzeugen Sie eine Textdatei für die neue Paketquelle:

```
echo deb [arch=amd64] http://
 dl.google.com/linux/chrome/deb/
 stable main | sudo tee /etc/apt/
 sources.list.d/google_chrome.
 list
```

Danach verwenden Sie

```
sudo apt update
sudo apt install google-chrome-
 stable
```

für die Installation der Software.

Paketquellen wieder entfernen

Paketquellen, die Sie nicht mehr benötigen, sollten Sie entfernen. Die darüber installierte Software bleibt erhalten und muss manuell deinstalliert werden (*apt remove [Paketname]*). Verwenden Sie diesen Befehl:

```
sudo add-apt-repository -r
 ppa:[Launchpad-Nutzername/PPA-
 Name]
```

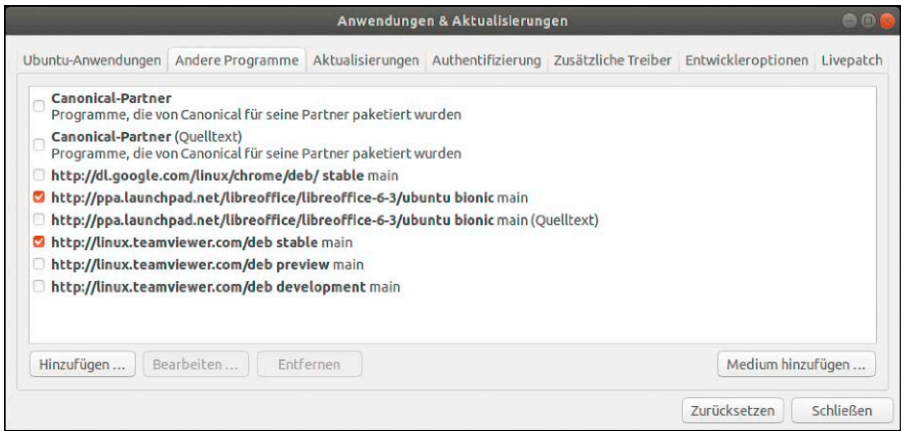
Den Platzhalter ersetzen Sie durch die Angaben, die Sie auch bei der Installation verwendet haben. Sie können auch das grafische Tool „Anwendungen & Aktualisierungen“ nutzen, das Sie über „Aktivitäten“ finden. Gehen Sie dort auf die Registerkarte „Andere Programme“, entfernen Sie das Häkchen vor der Paketquelle und klicken Sie auf „Entfernen“.

Alternativ verwenden Sie das Tool ppa-purge, das Sie mit

```
sudo apt install ppa-purge
```

installieren.

Mit dem Befehl



Paketquellen verwalten: Paketquellen lassen sich mit Hilfe von „Anwendungen & Aktualisierungen“ entfernen. Die installierte Software müssen Sie selbst deinstallieren.

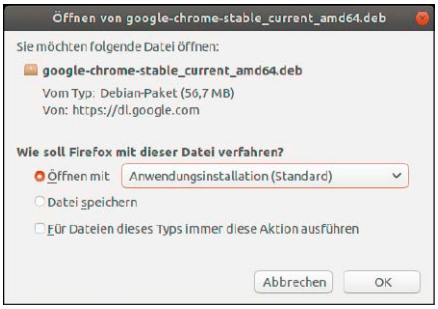
```
sudo ppa-purge ppa:[Launchpad-
 Nutzername/PPA-Name]
```

deaktivieren Sie die PPA-Quelle. Sollte eine andere Version der Software in den offiziellen Quellen zu finden sein, wird diese automatisch als Ersatz installiert.

Das ist beispielsweise der Fall, wenn Sie Libre Office über das PPA auf die Version 6.3.x aktualisiert haben wie zuvor beschrieben. ppa-purge richtet dann erneut die Vorgängerversion ein. Ist das Paket über die Standard-Paketquellen nicht installierbar, bleibt es erhalten und Sie deinstallieren es manuell.

Heruntergeladene „deb“-Pakete installieren

Ubuntu-Software kann auch Pakete installieren, die Sie aus dem Internet herunterladen. Ein Beispiel ist Google Chrome (*www.google.de/chrome*). Beim Download über Firefox ist hinter „Öffnen mit“ standardmäßig „Anwendungsinstallation“ eingestellt. Nach einem Klick auf „OK“ öffnet sich Ubuntu-Software und Sie klicken auf „Installieren“. Das Chrome-Paket weist eine Besonderheit auf: Es richtet eine neue Paketquelle für den Google-Browser ein und installiert den Google-GPG-Schlüssel. Sie erhalten daher auch regelmäßig Updates für den Browser. Einige „deb“-Pakete aus dem Internet bieten diesen Komfort eventuell nicht. Für ein Update installieren Sie dann – wenn verfügbar – eine neue Version des „deb“-Pakets. ■



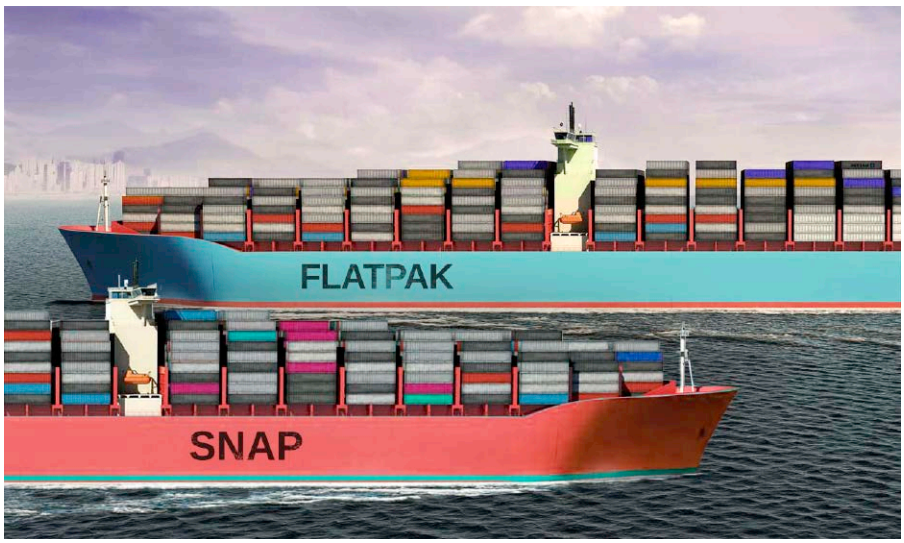
Pakete installieren: „deb“-Dateien, die Sie über den Browser herunterladen, öffnen Sie gleich mit Ubuntu-Software („Anwendungsinstallation“) und klicken auf „Installieren“.

FREMDPAKETE KÖNNEN DAS SYSTEM GEFÄHRDEN

Grundsätzlich ist jede Softwareinstallation immer Vertrauenssache. Die GPG-Schlüssel dürfen nicht kompromittiert und die Downloadserver müssen sicher sein. Bei den offiziellen Ubuntu-Servern können Sie von professioneller Wartung und umfangreichen Sicherungsmaßnahmen ausgehen. Launchpad (*https://launchpad.net*) wird zwar ebenfalls von Ubuntu-Distributor Canonical betrieben, Software kann hier jedoch jeder einstellen. Die Wahrscheinlichkeit, dass Schadsoftware frühzeitig entdeckt und gemeldet wird, ist aber sehr hoch. Launchpad darf daher als ausreichend sicher gelten. „deb“-Dateien aus dem Internet sollten Sie nur vertrauen, wenn diese von bekannten Anbietern stammen. Alles andere ist als unsicher anzusehen und das Risiko bei der Installation müssen Sie selbst verantworten.

Tipps zu Snaps und Flatpaks

Kompilieren war gestern: App-Container vereinfachen unter Linux die Installation neuer Programme, die nicht in den Paketquellen liegen. Zwei Formate buhlen dabei um die Gunst der Anwender: Flatpaks und Snaps.

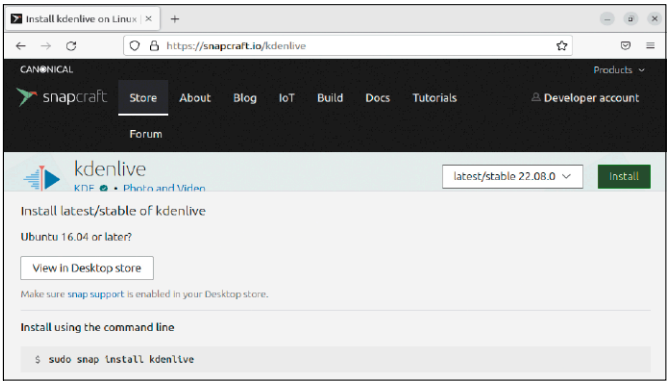


VON DAVID WOLSKI

Zwischen den App-Formaten Snap von Canonical für Ubuntu und dem allgemeiner gehaltenen Flatpak der Gnome Foundation ist eine Rivalität entstanden. Beide wollen die Softwareinstallation unter Linux für Anwender erleichtern und Entwicklern einen einfacheren Weg bieten, Programme in universellen Containern auszuliefern. Diese Container setzen auf einer Runtime auf, die in einer Linux-Distribution als Voraussetzung vorhanden sein muss, dürfen aber anders als herkömmliche Linux-Pakete ihre eigenen Bibliotheken mitbringen. Jeder App-Container ist von anderen Apps sowie vom Kernsystem abgeschottet und installiert sich in sein eigenes Verzeichnis, damit keine Konflikte entstehen.

Zwei Formate mit einem Ziel

Der Vorteil ist also die Verfügbarkeit von Programmen oder Programmversionen, die nicht im Kanon einer Linux-Distributionen erscheinen. Verlangt eine Software neuere oder nicht vorhandene Bibliotheken, so ist damit die Installation in Linux dennoch möglich, weil Flatpaks oder Snaps auch diese individuellen Komponenten enthalten. Es muss auch nicht zwingend Open Source sein, weil Entwickler diese App-Formate selbst veröffentlichen und nicht über eine Linux-Distribution. Anwender müssen daher Einzelteile wie Bibliotheken und Binärdateien nicht selbst zusammensuchen, sondern holen sich den kompletten Container vom Hersteller oder von einem moderierten App Store. Es gibt dabei selbstverständlich Überschneidungen an Bibliotheken und deshalb eine grundlegende App-Infrastruktur bei Snaps und Flatpaks: Beispielsweise müssen GTK oder Gnome-Bibliotheken nicht immer in jedem Container neu mitgeliefert werden, sonst wären diese Apps noch größer (und langsamer). Stattdessen gibt es über die Snap- oder Flatpak-Runtime auch übergreifende Basispakete. Es handelt sich bei beiden App-Formaten um Open-Source-Technologien, die Linux-Distributionen ergänzen können und nachrüstbar sind. Die Snap-Runtime ist auch in Debian, Fedora, Arch Linux und anderen Systemen installierbar – desgleichen auch Flatpak. Auch die Koexistenz auf demselben System ist völlig in Ordnung – in Ubuntu Mate 22.04 sind beide Laufzeitumgebungen sogar schon vorinstalliert. Ein komplet-



Snapcraft.io: Die Webseite ist wie ein App Store aufgebaut und bietet eine durchsuchbare Übersicht zu Snaps, ferner auch Anleitungen zur Installation der Snap-Runtime.

ter Ersatz für die bewährten Paketsysteme sind diese Container nicht und alle Distributionen verwenden auch weiterhin ihr natives Paketformat. Während Ubuntu für Snaps vorbereitet ist und einige dieser Container bereits mitliefert, bevorzugen alle anderen Linux-Distributionen Flatpak. In diesem Beitrag geht es aber nicht um eine Gegenüberstellung, sondern um Installation und Verwaltung dieser App-Formate.

Snapcraft.io: Snaps finden

Ubuntu macht es ab Ausgabe 22.04 dem eigenen Snap-Format nicht leicht, seine Vorteile auszuspielen. Ausgerechnet der Browser Firefox ist nicht mehr als natives Paket installiert, sondern als Snap. Der Browser ist dabei schlicht ein ungünstiger Kandidat für die Vorzüge von Snap-Paketen. Denn einer der Vorteile ist eben Verfügbarkeit von Programmen als Snap, die nicht als DEB-Paket vorliegen – oder nur in alten Versionen. Gelungene Beispiele für die Paketierung als Snap sind Skype, Spotify für Linux oder der umfangreiche Videoeditor Kdenlive mit seinen vielen speziellen Bibliotheken. In der Kommandozeile kann der Befehl

```
snap search [Begriff]
```

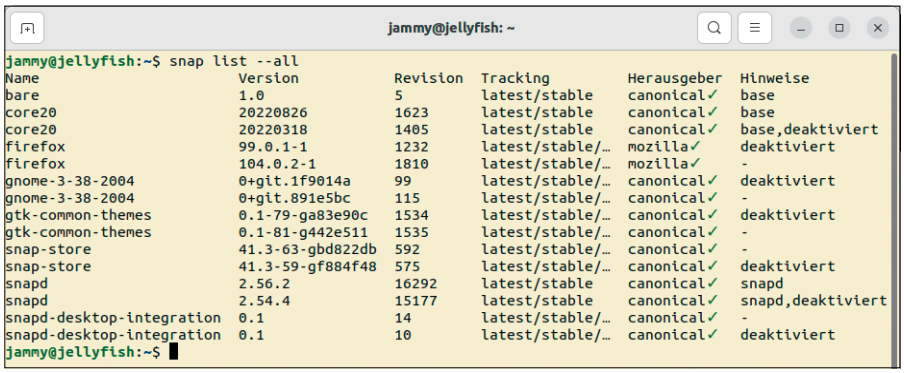
verfügbare Snap-Pakete zu dem angegeben Suchbegriff auflisten. Das geht aber auch noch einfacher: Um das Angebot von Snaps kennenzulernen, lohnt sich ein Besuch der Website *https://snapcraft.io*. Neben einer Vorstellung von populären Snaps auf der Einstiegsseite gibt es links oben eine Suchfunktion für Programmnamen und Stichwörter. Zu jedem Programm zeigt die betreffende Seite unter „Install" eine kurze Befehlszeile oder aber eine Verknüpfung, um das Programm in Ubuntu über das Softwarecenter zu öffnen.

Alle installierten Snaps auflisten

Ubuntu 22.04 und dessen offizielle Varianten liefern neben dem erwähnten Firefox einige vorinstallierte Snaps bereits mit. In einem Terminalfenster zeigt der Befehl

```
snap list --all
```

die vorhandenen Snap-Pakete und deren Versionen an. Die Snap-Runtime behält nämlich bis zu drei Versionen einer so installierten Programms auf dem System, um bei Bedarf den Schritt zurück zu einer älteren Version zu ermöglichen. Dies verschärft die allgemein unangenehme Eigenschaft von Containern: Sie benötigen sehr viel



Was ist installiert? Eine Auflistung aller Snaps gelingt nur in der Kommandozeile. Zur Berechnung des Platzbedarfs ist ein Blick ins Verzeichnis „/var/lib/snapd/snaps" nötig.

Platz auf dem Datenträger, der auf kleinen SSD- und NVME-Laufwerken schon mal zum Problem wird.

Das Kommando

```
du -h /var/lib/snapd/snaps/*
```

listet alle Snap-Verzeichnisse mit ihrem jeweiligen Platzbedarf auf und

```
du -sh /var/lib/snapd/snaps
```

zeigt, auf wie viel Platz sich das insgesamt aufaddiert.

Snaps: Manuell aktualisieren

Snaps sind als Containerformat von der üblichen Paketverwaltung mit apt komplett entkoppelt. Sie verlangen zur Installation sowie zur Aktualisierung eine andere Vorgehensweise. Über ein gewöhnliches Systemupdate werden diese alternativen Programmpakete nämlich nicht aktualisiert. Stattdessen verfügt das Snap-Rahmenwerk über eine separate Updatefunktion, die alle installierten Snaps täglich automatisch aktualisieren will. Auf Rechnern, die nicht dauernd eingeschaltet sind, beispielsweise auf Notebooks, wird das automatische Update nicht immer zuverlässig ausgeführt. Mit dem Befehl

```
sudo snap refresh
```

können Sie die Aktualisierung aller Snaps jederzeit manuell ausführen.

FLATPAK UND SNAPD NACHRÜSTEN

Auch wenn sich Ubuntu auf das eigene Snap-Format festgelegt hat, so ist ein Nachrüsten von Flatpaks auch hier leicht möglich. Einem Mix aus Snaps und Flatpaks steht nichts entgegen, denn die unabhängig voneinander entwickelten App-Container kommen sich nicht in Quere. Ein eventuelles Limit, wie viele Snaps und Flatpaks auf einem System sinnvoll sind, ist aber deren Platzbedarf. Denn der ist bei beiden Formaten erheblich – einige dieser Apps belegen schnell etliche Gigabyte Plattenplatz. In Ubuntu und Debian liegen die Flatpak-Voraussetzungen in den Standard-Paketquellen. Das Kommando

```
sudo apt install flatpak
```

holt das Flatpak-Verwaltungstool ab, um anschließend für die Installation von Apps eine Flatpak-Quelle einzurichten.

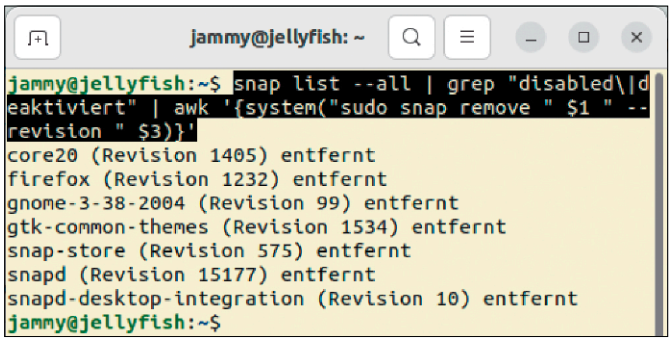
Umgekehrt ist es in Debian, Fedora oder Manjaro kein Problem, Snapd als Runtime für Snap-Pakete auf das System zu holen. Das Paket „snapd" findet sich in den Standardquellen und ist in Debian beispielsweise mit

```
sudo apt install snapd
```

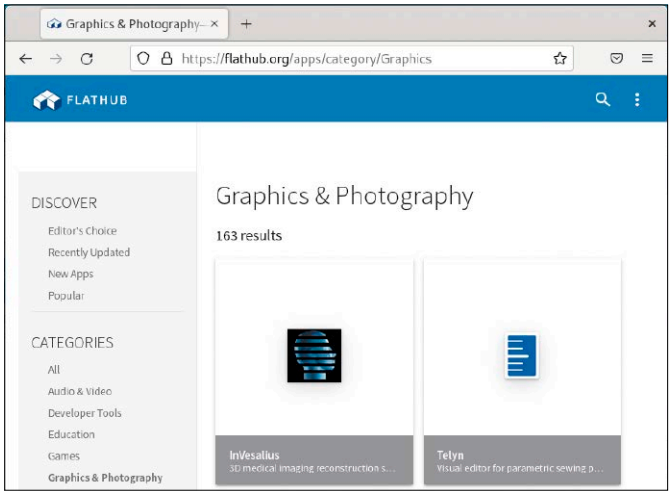
schnell nachgerüstet. Das trifft auch für die Ubuntu-Varianten Kubuntu und Lubuntu zu, bei welchen Snapd auch erst mal fehlt. Eine Ausnahme ist Linux Mint, auf welchem die Installation von Snapd durch eine Regel des Paketmanagers apt blockiert ist. Wer unter Linux Mint Snaps möchte, muss erst mit dem Befehl

```
sudo mv /etc/apt/preferences.d/nosnap.pref ~/nosnap.backup
```

die Blockadedatei verschieben. Der genannte Befehl verschiebt die Konfigurationsdatei dazu in das Home-Verzeichnis.



Snaps aussortieren: Ein länger genutztes Ubuntu-System behält auch die letzten zwei älteren Versionen von installierten Snaps. Dieser Befehl entfernt diese Versionen.



Zentrale für Flatpaks: Flathub ist nur eine von vielen Flatpak-Quellen. Unter der Ägide der Gnome Foundation entsteht unter *https://flathub.org* aber das umfangreichste Repository.

Snaps: Alte Versionen entfernen

Laufen alle installierten Snaps unproblematisch, ist es nicht nötig, die älteren Versionen zu behalten. Archivierte, aber inaktive Snaps sind in der tabellarischen Übersicht von „snap list --all“ in der letzten Spalte „Notes“ mit dem Begriff „disabled“ beziehungsweise „deaktiviert“ versehen. Eine gezielte Deinstallation eines dieser Snaps gelingt mit diesem Kommando:

```
sudo snap remove [Name] --revision
  [Revision]
```

Den korrekten „Namen“ erfahren Sie in der gleichnamigen Spalte „Name“ des list-Befehls und den Wert von „Revision“ aus der gleichnamigen Spalte „Revision“. Um beispielsweise das Snap „gnome-calculator“ in der Revision 260 zu entfernen, dient dieser Befehl:

```
sudo snap remove gnome-calculator
  --revision 260
```

Diese Aktion ist in der Befehlszeile per verknüpften Kommandos auch automatisierbar. Die Zeile

```
snap list --all | grep
  "disabled\|deaktiviert" | awk
  '{system("sudo snap remove " $1 "
  --revision " $3 ")}'
```

deinstalliert alle archivierten und inaktiven Snaps in einem Durchgang.

Flatpaks: Ein Programm installieren

Die Idee hinter Flatpaks geht auf Red Hat und die Gnome Foundation zurück und vorgestellt wurden diese App-Container erstmals 2016 in Fedora 24 und Gnome 3.22. Dieses zweite verbreitete Containerformat Flatpak hat aktuell ein höheres Momentum als Snap, ist offener, benötigt allerdings noch mehr Plattenplatz als Snap. Unter anderem favorisiert Linux Mint Flatpak als Containerformat und in Ubuntu Mate ist es ebenfalls von Haus aus nutzbar. Flatpaks sind also weder an eine Distribution gebunden noch an die Desktopumgebung Gnome.

Im Gegensatz zu Snaps (zentraler Canonical-Snapstore *snapcraft.io*) sind Flatpaks nicht zentralisiert. Linux-Distributionen wie auch Softwareentwickler veröffentlichen eigene Flatpaks auf verschiedenen Repositorys und liefern Installationsanleitungen auf ihren eigenen Web- oder Github-Seiten. Aktuell ist die Site *https://flathub.org* die eindeutig wichtigste Anlaufstelle für die Suche nach Flatpaks. Rund 1700 Einträge finden sich dort mit Beschreibung. Das Wachstum ist konstant und die Site soll mit Hilfe der Gnome Foundation zu einem App Store für Linux wachsen. Die Seite bietet eine Suchfunktion, eine Liste an neu vorgestellten Flatpaks sowie Programmkategorien zum Durchstöbern. Die Unterseite zu einem Programm liefert Versionsangaben und ganz unten die Kommandozeilen zur Einrichtung in der Shell.

In Linux-Distributionen ist in der Regel wenig mehr vorinstalliert als das Verwaltungstool flatpak für die Kommandozeile. Um etwas installieren zu können, ist zuerst die Einbindung einer externen Quelle nötig. Das Kommando

```
flatpak remotes
```

listet die vorhandenen Paketquellen auf. Um das empfehlenswerte und gut gefüllte Repository Flathub aufzunehmen, dient dieser Befehl:

```
sudo flatpak remote-add flathub
  https://flathub.org/repo/
  flathub.flatpakrepo
```

Danach kann die Abfrage

```
flatpak search [Begriff]
```

nach Programmen suchen. Wichtig ist in dieser Auflistung die „Application ID“, anhand derer sich ein Programm mit

```
flatpak install [Application ID]
```

installieren lässt. Dies funktioniert ohne vorangestelltes „sudo“, denn um die Rechteverwaltung im Dateisystem kümmert sich flatpak selbst. Das Programm steht deshalb nicht nur dem aktuell angemeldeten Konto zur Verfügung.

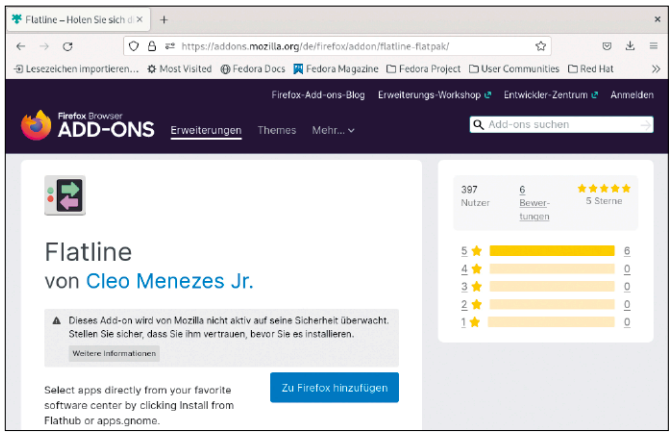
Flatline: Flatpaks über den Browser

Auf flathub.org bietet jede Seite zu einem Programm auch gleich die Schaltfläche „Install“, die aber nicht viel mehr tut, als eine Datei mit der Endung „.flatpakref“ herunterzuladen. Diese dient zunächst zur Weiterverarbeitung im Terminal mit diesem Befehl:

```
flatpak install --from [Datei].
  flatpakref
```

Der Sprung ins Terminal zur Flatpak-Installation ist aber nicht unbedingt nötig, denn es gibt für Flathub eine Browsererweiterung für Firefox, um die Einrichtung von Flatpaks zu vereinfachen: Das Add-on Flatline steht im Erweiterungsverzeichnis Mozillas unter *https://addons.mozilla.org/de/firefox/addon/flatline-flatpak* bereit. Damit

sich nach einem Klick auf „Install“ zu einem Programm auf Flathub etwas tut, muss dazu auch das Repository *https://flathub.org/repo/flathub.flatpakrepo* hinzugefügt sein wie vorher gezeigt. Der Install-Button bietet dann an, die Installationsprozedur über den grafischen Paketmanager (etwa Gnome Software oder Discover) zu öffnen, und der Exkurs in die Kommandozeile kann daher entfallen. Ein Dialog bietet außerdem an, diese Verknüpfung immer auf diese bequeme Weise zu öffnen.



Flatline: Diese Browsererweiterung für Mozilla ist eine Installationshilfe für Flathub und kann direkt die grafischen Werkzeuge Gnome Software oder Discover aufrufen.

Inventur: Verwaltung in der Shell

Genau wie bei Snaps so fällt auch die Verwaltung von Flatpaks nicht an den nativen Paketmanager der Distribution. In Gnome-Software sowie in Discover (KDE) ist es aber möglich, Flatpaks auf grafischem Weg wieder zu deinstallieren. Eine Filterfunktion, die nur Flatpaks zeigt, fehlt allerdings, daher muss die Auflistung der Flatpaks und ihrer Runtimes weiterhin in der Kommandozeile erfolgen. Die Eingabe

```
flatpak list
```

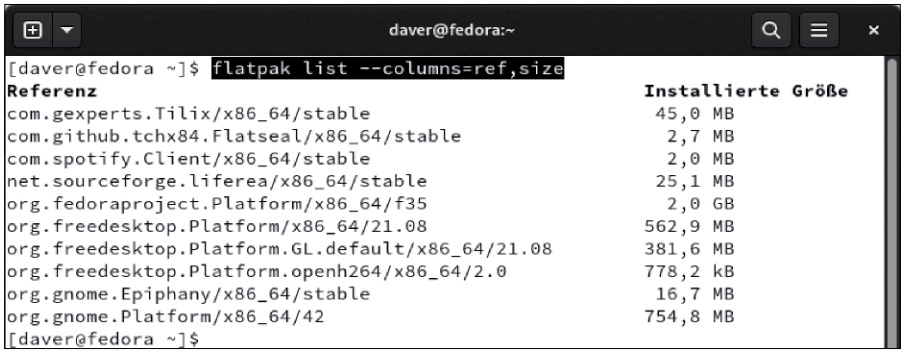
zeigt die schon installierten Flatpaks an. Geht es um die Einschätzung des Platzbedarfs aller Flatpaks, dann hilft dieses Kommando

```
flatpak list --columns=ref,size
```

weiter, das eine tabellarische Liste der Apps und ihrer jeweiligen Größe ausgibt. Über den Befehl

```
flatpak uninstall [Name]
```

ist ein Flatpak im Terminal ohne lange Suche auch wieder deinstalliert, wobei hier keine genaue Angabe der Applikations-ID notwendig ist – der Name reicht aus. Auch hier ist kein „sudo“ nötig.



Flatpaks und der Umfang auf dem Datenträger: Eine Auflistung der Flatpak-Apps mit Größenangabe ist auch bei diesem Format nur in der Kommandozeile möglich.

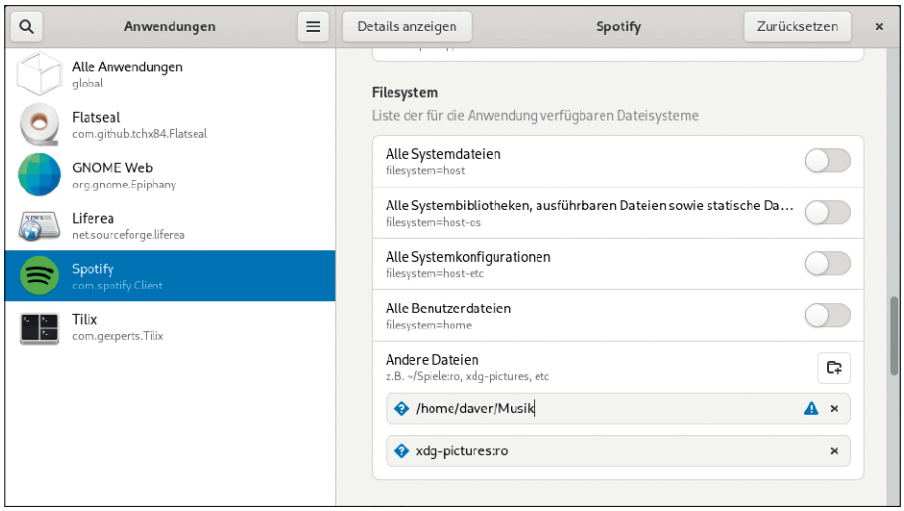
Flatseal: Berechtigungen von Flatpaks

Die Ziele von Flatpak sind recht hoch gesteckt: Als abgeschottete Programme, die Cgroups und Namespaces des Linux-Kernels zur Prozessorisolierung nutzen, sollen Flatpak-Apps auf dem Desktop in einer sicheren Sandbox mit Rechteverwaltung laufen. Anwender können bestimmen, welche Ressourcen ein Flatpak nutzen darf. Zur Anzeige und Verwaltung der Berechtigungen installierter Flatpaks gibt es das grafische Tool Flatseal, das seinerseits als Flatpak vorliegt. Um das Tool zu installieren, ist es am einfachsten, wieder Flathub als Quelle zu nutzen. Flatseal findet sich dort unter *https://flathub.org/apps/details/com.github.tchx84.Flatseal*, ist aber auch im Terminal mittels

```
flatpak install flathub com.github.tchx84.Flatseal
```

zu installieren. Nach einem Aufruf zeigt das Tool links alle installierten Flatpaks an, rechts jeweils deren Berechtigungen. Die meisten Apps liefern eine Standardkonfiguration mit allen nötigen Rechten, um korrekt zu funktionieren. Eine Berechtigung, die gelegentlich Anpassungen verlangt, ist der Zugriff auf Verzeichnisse außerhalb von Home.

Diese Rechte sind in Flatseal in der Kategorie „Filesystem“ untergebracht und das Ordnersymbol unter „Andere Dateien“ kann hier weitere Pfade hinzufügen, auf die der aktuelle Benutzer selbst Zugriff hat. ■

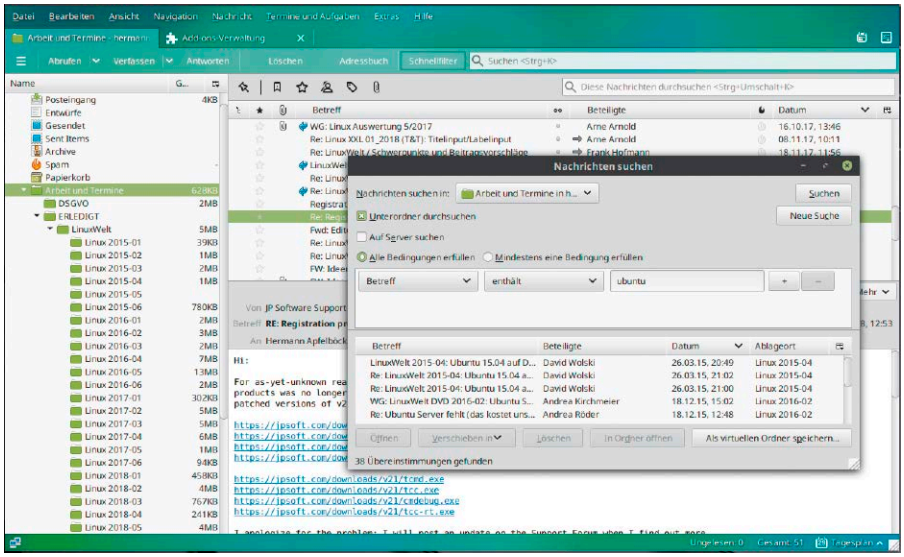


Wer darf was? Flatseal kann die Flatpak-Zugriffsrechte anpassen. Das ist beispielsweise nützlich, wenn Programme den Zugriff auf Ordner jenseits des Home-Verzeichnisses verlangen.

Die besten Tipps für Thunderbird

Thunderbird ist eines der beliebtesten Mailprogramme. Selbst viele Windows-Nutzer, die auch ein Outlook auf dem Rechner hätten, bevorzugen Thunderbird. Funktionalität, Layout und Optik sind ausgereift, die Konfiguration ist aber zum Teil verschnörkelt.

VON HERMANN APFELBÖCK



Braucht man heutzutage überhaupt noch ein Mailprogramm? Uneingeschränkt ja, sofern man beruflich mit Mails arbeitet und eventuell mehrere Konten mit einer Software verwalten will. Aber auch private Nutzer mit nur einem Konto arbeiten übersichtlicher, komfortabler und sicherer, wenn sie statt Webmail im Browser ein spezialisiertes Mailprogramm verwenden.

Konten und Konteneinstellungen

Starten Sie Thunderbird zum ersten Mal, öffnet sich der Einrichtungsassistent. Gleiches geschieht, wenn Sie über „Einstellungen → Konteneinstellungen“ unter „Konten-Aktionen“ ein „E-Mail-Konto hinzufügen“. Bei allen namhaften Mailprovidern (Google, GMX, Hotmail, Vodafone, Telekom, Strato, 1&1 etc.) genügt es, den eigenen Namen einzutragen (technisch irrelevant), ferner die Mailadresse und das Passwort für das Konto. Nach „Weiter“ kontaktiert Thunderbird seine Datenbank und konfiguriert die Einstellungen für Eingangs- und Ausgangsserver automatisch.

Eingerichtete Mailkonten finden Sie unter „Einstellungen → Konten-Einstellungen“ versammelt. An den grundlegenden „Server-Einstellungen“ müssen Sie nichts ändern, wenn die Verbindung funktioniert. Gibt es beim Verbindungsaufbau einen Fehler, dann könnte es an einem falschen Passwort oder an falschen Ports liegen. Die richtigen Einstellungen erfahren Sie normalerweise vom Provider. Die üblichen Standardports für verschlüsseltes SSL/TLS sind 995 für POP3 und 993 für IMAP.

Die Einstellungen für „Kopien & Ordner“ sind wichtig, da Sie insbesondere für berufliche Mails einen Nachweis für gesendete Nachrichten brauchen. Daher muss die Option „Eine Kopie speichern“ (für gesendete Mails) aktiviert sein. Wer mehrere Konten benutzt, kann die Sendekopien aller Konten an einer Stelle sammeln. Dazu kann ein „Anderer Ordner“ definiert werden, der in einem anderen Mailkonto liegt. Derselbe Zielordner kann dann unter „Kopien & Ordner“ für alle Konten festgelegt werden.

Wichtig für IMAP-Konten ist ferner der Punkt „Synchronisation & Speicherplatz“. Mit der Option „Nachrichten [...] bereithalten“ bestimmen Sie, ob überhaupt Nachrichten lokal abgelegt werden. Unter „Speicherplatz“ konfigurieren Sie, ob Sie alle Mails, nur jüngere oder solche bestimmter Größe lokal herunterladen wollen. Auf dem IMAP-Server bleiben alle Mails erhalten, es sei denn, Sie definieren im untersten Bereich dieses Fensters bestimmte Löschoptionen (maximale Anzahl, maximales Alter). Wir empfehlen keinerlei Löschoption, weil das Kontingent von Mailprovidern meist jahrelange intensive Nutzung erlaubt, ohne an die Grenzen zu stoßen. Den aktuellen Füllstand eines Mailkontos ermitteln Sie am einfachsten durch Rechtsklick auf den „Posteingang“ eines Kontos und „Eigenschaften“. Die Registerkarte „Kontingent“ zeigt die absolute und prozentuale Belegung.

Bei einem IMAP-Konto erscheint nach Rechtsklick auf das Konto in der Navigationsleiste die Option „Abonnieren“. Im Unterschied zur Synchronisation legt diese Option keine lokalen Kopien an. Hier geht es nur um die Ordner auf dem Server, die

Sie in Thunderbird sehen wollen. Eventuell gibt es alte Archive, die Sie am Server erhalten wollen, aber nicht tagtäglich vor Augen haben müssen. Das sind dann Kandidaten, die Sie nicht „abonnieren".

Globale Thunderbird-Einstellungen

Unter „Extras → Einstellungen" (klassisches Menü) oder „Einstellungen → Einstellungen" (neues Menü) kommen Sie zu den globalen Thunderbird-Einstellungen. Diese sind längst nicht so fundamental wie die Kontenoptionen: Die Registerkarte „Verfassen" bietet Schreibhilfen sowie die Prüfung auf „fehlende Anhänge", die automatische Speicherung beim Schreiben längerer Nachrichten und die Rechtschreibprüfung. Die Prüfung auf fehlende Anhänge ist immer sinnvoll, alle anderen Optionen Geschmackssache. Eine aktivierte Rechtschreibprüfung, die ausnahmsweise nervt, lässt sich im Editor-Fenster über „Optionen → Sofort-Rechtschreibprüfung" auch ad hoc abstellen.

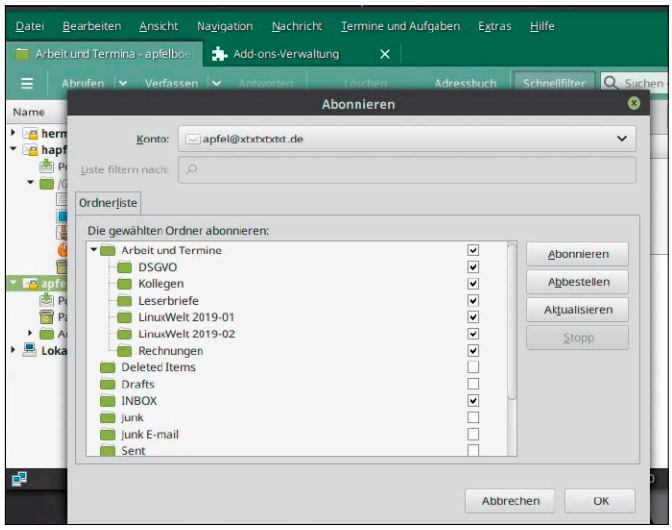
Unter „Sicherheit" verwalten Sie die globalen Einstellungen für Junknachrichten, wobei Sie unter „Betrugsversuche" bestimmen, ob die Software Nachrichten automatisch auf Phishing untersuchen und warnen soll. Hinter „Passwörter" finden Sie – oder jeder, der an das System kommt – alle gespeicherten Mailkennwörter. Auf mobilen Notebooks ist dies riskant: Hier definieren Sie am besten an gleicher Stelle ein Masterpasswort („Master-Passwort verwenden"), das die Mailkennwörter verschlüsselt. Dieses Passwort müssen Sie einmal pro Thunderbird-Sitzung eingeben.

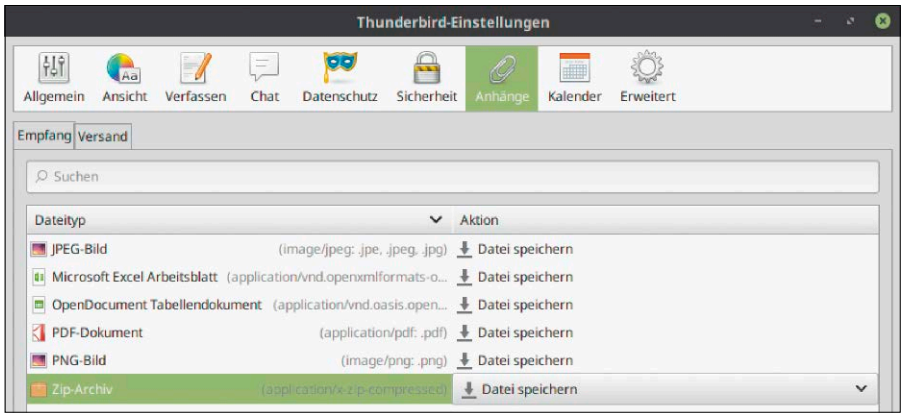
Auf der Registerkarte „Anhänge" werden Sie bei den meisten Dateitypen die Option „Jedes Mal nachfragen" vorfinden. Nutzen Sie stattdessen „Datei speichern" und unten neben „Datei speichern unter" einen festen Zielordner – bevorzugt den Desktop. Global gilt diese Einstellung für Anhänge dann aber immer noch nicht: Bei bislang noch nicht eingetragenen Dateitypen müssen Sie die Option „Datei speichern" anklicken und dies für den Dateityp „immer" anfordern.

Thunderbird 60 installieren

Zum Zeitpunkt dieses Artikels war es nicht möglich, über das Update eine ältere Version 52.x auf Thunderbird 60 zu hieven. Eventuell ist dieser Mangel bei Erscheinen dieses Hefts behoben. Falls nicht, erhalten Sie die neueste Version als direkten Download unter *https://www.thunderbird.net/de/*. Beachten Sie dort unter der großen Schaltfläche „Kostenloser Download" den Link „System und Sprachen", um die deutsch lokalisierte Version auszuwählen („German"). Hier gibt es neben Windows und Mac-OS auch den Download von „Linux in German" sowie „Linux 64-Bit in German". Dabei handelt es sich um keine Installationspakete, sondern um Tar-Archive, die Sie nach dem Download einfach entpacken – etwa ins Home-Verzeichnis. Über das enthaltene Programm „thunderbird" starten Sie den Mailclient. Die neue Version übernimmt die Konteneinstellungen und Konfi-

„Abonnieren" von IMAP-Ordnern: Wählen Sie nur aus, was Sie in Thunderbird tatsächlich sehen müssen. Das verbessert die Übersicht in der Navigationsspalte.

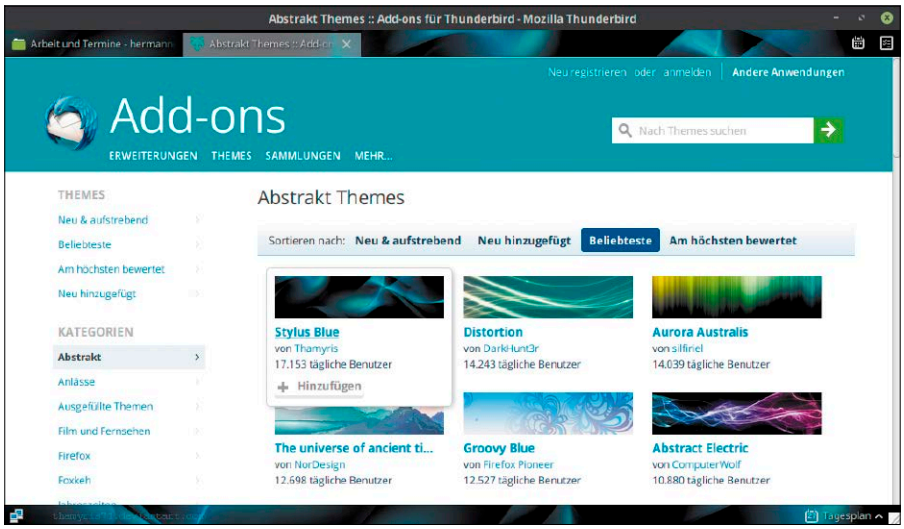




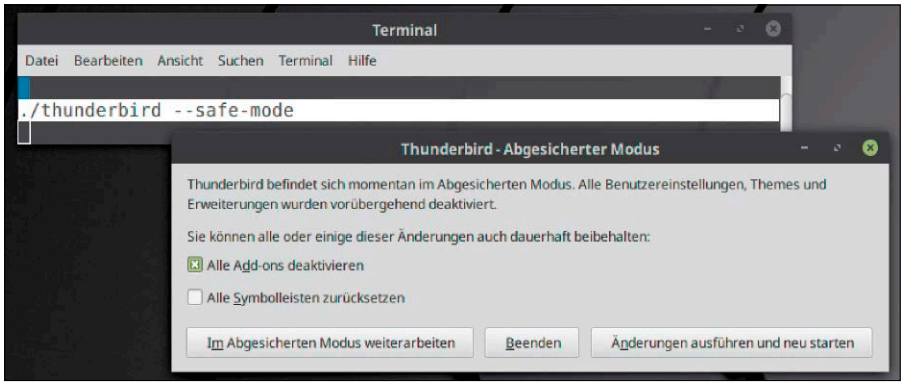
Standard für Anhänge: Sie sparen Klicks bei jedem Anhang-Download, wenn Sie alles grundsätzlich auf den Desktop speichern.

DIE VORTEILE VON IMAP GEGENÜBER POP3

IMAP (Internet Message Access Protocol) und POP3 (Post Office Protocol) sind die verbreiteten Empfangsprotokolle für Mails und die meisten Provider bieten beides wahlweise. Aus technischer Sicht ist IMAP klar vorzuziehen. POP3 lädt nämlich die Mails immer auf das aktuelle Gerät herunter. Das wird zum Problem, sobald Sie mehr als ein Empfangsgerät nutzen: Für das zweite Notebook oder Smartphone ist die einmal gelesene Mail dann nicht verfügbar. Bei IMAP verbleiben hingegen die Nachrichten auf dem Server, die zusätzliche Synchronisation mit dem lokalen Gerät ist möglich, aber nicht zwingend. Sie kommen folglich mit jedem Gerät auf alle Nachrichten, und haben – neben optionalen lokalen Kopien – das Mailarchiv auf einer externen Quelle gesichert.



Optik ändern: Standardmäßig ist es kein Aufwand, über die Add-ons-Verwaltung andere Themen zu installieren. Aktuell kann dies daran scheitern, dass die Themenauswahl im Browser startet.



Thunderbird-Startparameter: Neben dem hier angeforderten „Safe Mode“ ohne Add-ons gibt es auch einen Profilmanager für Anwender mit vielen Mailkonten.

guration der bisherigen Version. Die volle Systemintegration fehlt dieser „portablen“ Installation jedoch. Wenn Sie einen grafischen Starter am Desktop oder in einem Starterdock einrichten wollen, müssen Sie das manuell erledigen. Dabei können Sie sich an den Dateien mit der Endung „.desktop“ unter „/usr/share/applications“ orientieren. Unter Linux Mint ist es am einfachsten, die Starterdatei mit der Desktopoption „Neuen Starter hier erstellen“ zu erstellen. Jede Menge Icons für den Starter gibt es unter „/usr/share/icons“.

Themes für Thunderbird

Das Mailprogramm hat wie der Browser Firefox unzählige Themes zu bieten, um das Standardoutfit aufzufrischen oder an das des Browsers anzugleichen. Der Weg dazu führt über das Menü „Add-ons“ zu „Add-ons entdecken“. Hier finden Sie zahlreiche „Vorgestellte Themes“, die Sie durch „Hinzufügen“ (und anschließendes „Erlauben“) herunterladen und damit auch sofort aktivieren.

Solcher Theme-Wechsel wird jedoch durch einen Bug derzeit mindestens bei den älteren Versionen 52.x verhindert. Dort öffnet sich nämlich beim Klick auf „ Vorgestellte Themes“ oder auf eines der einzeln vorgeschlagenen Themen der Browser. Eine Integration in Thunderbird ist auf diesem Weg nicht möglich. In der neuen Version 60.x funktioniert der Theme-Wechsel in der Regel wieder wie gewohnt, jedoch kann der Bug auch hier noch auftreten.

Wer von diesem Fehler betroffen ist, hat immerhin noch die Option, unter „Add-ons entdecken“ den Link „Alle vollständigen Themes anzeigen“ zu nutzen. Der führt dann zwar fehlerhaft in den Browser, aber die vollständigen Themes erlauben einen manuellen Download einer XPI-Datei auf den Rechner. Achten Sie vor dem Download auf die Angabe „Kompatibel mit...“, um ein für Ihre Thunderbird-Version passendes Thema zu laden. Die heruntergeladene XPI-Datei können Sie dann in Thunderbird im Fenster „Add-ons → Erweiterungen“ mit dem Zahnradsymbol und der Option „Add-on aus Datei installieren“ integrieren.

Backups und Umzüge

Die komplette Thunderbird-Installation einschließlich aller Mailkonten und Mails lässt sich sehr einfach sichern und auf andere Rechner übertragen. Unabhängig vom Programmordner sind diese Daten unter Linux im Ordner „~/.thunderbird“ versammelt, wobei der Unterordner „[xxxxxxxx].default“ den wesentlichen Profilordner ausmacht. Die acht „x“-Zeichen werden zufällig generiert. Um die Thunderbird-Umgebung auf einen anderen Rechner umzuziehen, kopieren Sie einfach den gesamten Ordner „~/.thunderbird“ in das Home-Verzeichnis auf dem neuen PC und installieren danach, falls nötig, Thunderbird auf diesem Rechner.

Adressbuch: Wer nur das Adressbuch mit den gesammelten Mailadressen auf einem anderen PC benötigt, öffnet mit Strg-Umschalt-B oder mit „Extras → Adressbuch“ die Sammlung und nutzt dort das Menü „Extras → Exportieren“. Als Ausgabeformat empfiehlt sich LDIF oder CSV. Die Liste können Sie dann am nächsten Rechner in das Thunderbird-Adressbuch einlesen, indem Sie dort „Extras → Importieren“ wählen und zur gespeicherten Liste navigieren.

Interessante Startparameter

Thunderbird berücksichtigt zahlreiche Startparameter, wie der Terminalbefehl *thunderbird --help* zeigt. Die meisten Schalter richten sich an Entwickler, aber einige sind durchaus auch für fortgeschrittene Endbenutzer interessant. Der Troubleshooting-Parameter

```
thunderbird --safe-mode
```

startet das Programm ohne Erweiterungen, wonach Sie eventuell problematische Add-ons entfernen oder deaktivieren können.

Wie Firefox hat auch Thunderbird eine Profilverwaltung. Das heißt, dass Sie innerhalb desselben Benutzerkontos verschiedene Thunderbird-Konfigurationen anlegen können. Sinnvoll ist das etwa bei sehr vielen Mailkonten, die der Übersicht halber in ein privates und berufliches Profil getrennt

werden sollen. Aber auch auf einem typischen Familienrechner, den mehrere Personen ohne Multiuser-Verwaltung nutzen, machen Thunderbird-Profile Sinn.

Und so funktioniert's: Sie eröffnen mit

```
thunderbird --ProfileManager
```

und „Profil erstellen" ein neues Profil und vergeben den gewünschten Namen. Thunderbird startet dann jungfräulich mit dem Einrichtungsassistenten. Dort legen Sie das Mailkonto oder auch mehrere Konten für das zweite Profil oder den anderen Benutzer an. Um die beiden Profile mit zwei Startern aufrufen zu können, benötigen Sie folgende Startparameter:

```
thunderbird -P default
thunderbird -P [name]
```

Der erste Befehl lädt das primäre Defaultprofil, der zweite das neu angelegte.

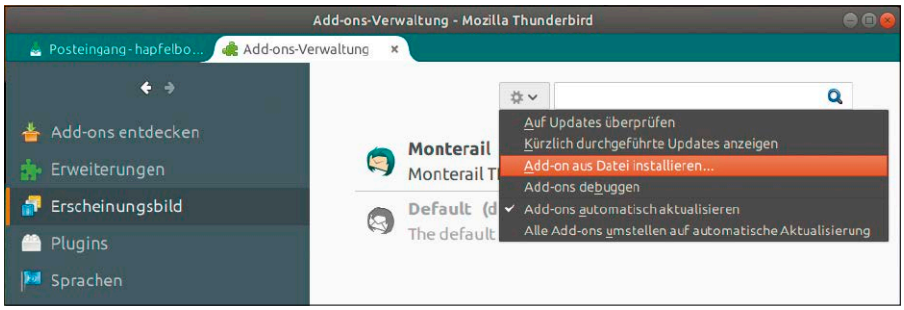
Es geht sogar noch besser: Der Befehl

```
thunderbird --new-instance -P
  [name]
```

kann eine zweite Instanz des Mailclients neben der ersten starten; somit können beide Profile gleichzeitig laufen.

Add-ons und Kalender

Über „Add-ons → Erweiterungen" rüsten Sie Thunderbird funktional auf. Das Suchfeld erlaubt hier eine gezielte Suche. Da Thunderbird hier auf die Seite *https://addons.mozilla.org/de/thunderbird/* zugreift, ist der direkte Weg über den Browser meistens übersichtlicher und komfortabler. Nach dem Download einer Erweiterung erhalten Sie eine Datei im XPI-Format. In Thunderbirds Add-ons-Verwaltung („Erweiterungen") verwenden Sie dann das Zahnradsymbol und die Option „Add-on aus Datei installieren". Danach ist regelmäßig ein Neustart von Thunderbird erforderlich.



Add-ons manuell installieren: Die Seite *https://addons.mozilla.org/de/thunderbird/* bietet alle Erweiterungen, die Sie dann als XPI-Datei in Thunderbird integrieren.

Beispiel 1: Der beliebte Thunderbird-Kalender Lightning ist ein Add-on, das Sie in beschriebener Weise nachinstallieren. Er erscheint auf Platz eins der genannten Add-ons-Webseite. Nach der Einrichtung rufen Sie den Kalender über das Menü oder mit Strg-Umschalt-C auf. Links in der Seitenleiste sehen Sie den Standardkalender „Privat", der sich lokal auf dem Rechner befindet. Mit einem Rechtsklick darunter können Sie weitere Kalender anlegen. Es öffnet sich ein Fenster und Sie haben die Wahl zwischen „Auf meinem Computer" oder „Im Netzwerk". Lightning kann externe Webkalender im ICS.- oder Caldav-Format importieren und synchronisieren.

Beispiel 2: Um sämtliche Google-Kontakte mit dem Thunderbird-Adressbuch zu synchronisieren, hilft das Add-on „gContactSync". Bei dem einfachen Tool geben Sie lediglich die Google-Mailadresse und das Google-Kennwort an und klicken auf „Weiter". ■

MINITIPPS ZU THUNDERBIRD

Menüleiste einblenden: Die traditionelle Menüleiste ist standardmäßig ausgeblendet und im – weniger übersichtlichen – Hauptmenü-Symbol mit den drei Balken komprimiert. Um die Menüleiste dauerhaft einzublenden, klicken Sie mit der rechten Maustaste auf einen leeren Bereich in der Tab-Leiste von Thunderbird (unterhalb der Titelleiste) und aktivieren im Auswahlmenü den Eintrag „Menüleiste".

Das klassische Menü lässt sich zudem mit der Taste F10 ad hoc einblenden, unter Windows auch mit der Alt-Taste.

Symbolleiste anpassen: Angebot und Anordnung der Hauptsymbolleiste („Abrufen", „Verfassen"…) sind frei einstellbar. Nach Rechtsklick auf der Leiste erscheint die Option „Anpassen". Über „Anzeigen" bestimmen Sie das grundsätzliche Aussehen der Schaltflächen (nur Symbol, nur Text oder beides). Umfang und Position ändern Sie durch Drag & Drop.

So können „Schnellfilter", „Löschen", „Antworten" in der stets erreichbaren Symbolleiste echte Zeitsparer sein.

Ansichtssachen: Die grundlegende Fensteranordnung finden Sie im Hauptmenü weder unter „Ansicht" noch unter „Einstellungen → Einstellungen → Ansicht".

Das klassische Menü (F10) ist hier logischer („Ansicht → Fensterlayout"), jedoch ist die Option auch im Hauptmenü zu finden – unter „Einstellungen → Fensterlayout". Hier gibt es unter anderem die „3-Spalten-Ansicht".

Eine weitere fundamentale Option für mehrere Konten ist die Einstellung „Ordner → Gruppiert". Dann fasst Thunderbird unter „Posteingang" (Papierkorb etc.) die betreffenden Mails aller Konten zusammen.

Suchoptionen: Die diversen Suchmethoden in Thunderbird sind verwirrend.

Die im Normalfall in der Symbolleiste vertretenen Varianten „Schnellfilter" und „Globale Suche" sind auch über die Hotkeys Strg-Umschalt-K und Strg-K zu erreichen. Der Schnellfilter sucht nur im Ordner der aktuell angezeigten Mails, die globale Suche hingegen in allen Ordnern aller Konten.

Es geht aber noch differenzierter: Strg-Umschalt-F öffnet ein Suchfenster mit exakten Filtern (Betreff, Inhalt, Datum, Absender etc.). Der Hotkey Strg-F dient hingegen nur als Textsuche in der aktuellen Mail.

Adressbuch: Das Adressbuch (Strg-Umschalt-B) speichert automatisch alle Mailempfänger unter „Gesammelte Adressen". Über „Neue Liste" können Sie Verteilerlisten erstellen. Beim Versenden genügt dann als Adressat („An") der Eintrag des Listennamens, um alle Listenteilnehmer zu erreichen.

Libre Office „persönlich“

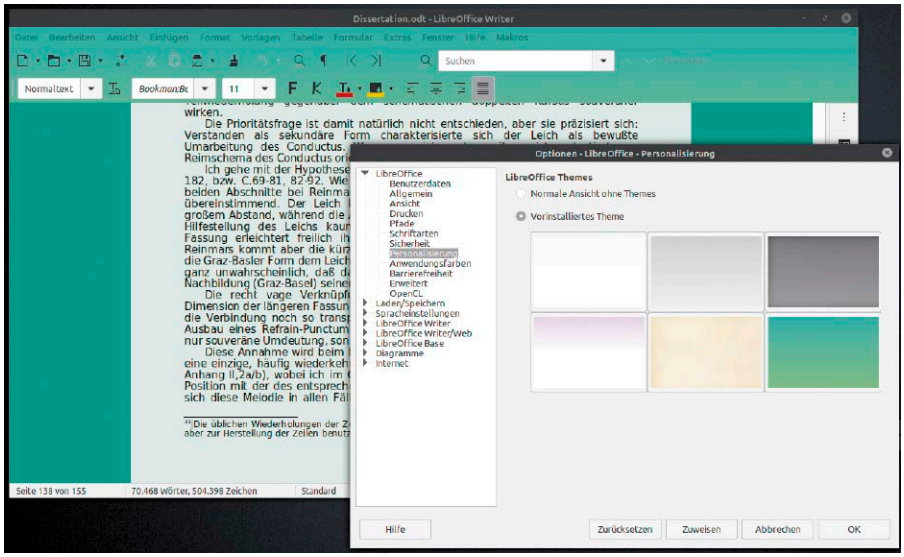
Ein knapper Beitrag zu einer hochkomplexen Software wie Libre Office muss sich fokussieren: Hier geht es ausschließlich um Optik und Einstellungskomfort, die den Einsatz der Office-Programme persönlicher und individueller gestalten.

VON HERMANN APFELBÖCK

Hinsichtlich Optik und Benutzeroberfläche ist Libre Office derzeit recht aktiv und was noch für die Versionen 5.x oder frühes 6.0 galt, ist nicht mehr aktuell. Obwohl einige der nachfolgenden Tipps auch für ältere Versionen gelten, müssen wir hier eine aktuelle Version 6.3.x voraussetzen, um uns nicht in den Details der Versionsunterschiede zu verlieren. Falls eine ältere Version vorliegt, erhalten Sie die jüngste Version unter *https://de.libreoffice.org* oder über das PPA (ppa:libreoffice/ppa):

```
sudo add-apt-repository
 ppa:libreoffice/ppa
sudo apt update
sudo apt dist-upgrade
```

Die zweite Methode hat den Vorteil, dass Sie das Office-Paket künftig über die Aktualisierungsverwaltung automatisch updaten können.



Ein wenig Farbe, angepasste Symbolleisten und moderneres Iconset: Libre Office hat viele Stellschrauben für eine personalisierte Optik.

1. Alternatives Farbschema verwenden

Die Option, die Office-Komponenten mit Firefox-Themes zu verzieren, funktioniert schon lange nicht mehr, auch wenn sie in älteren Office-Versionen noch als Angebot auftaucht. Als kleine Entschädigung finden Sie unter „Extras → Optionen → LibreOffice → Personalisierung“ einige vorinstallierte Themen, die nach Markieren und Klick auf „Zuweisen“ den Menübereich dezent einfärben. Die Maßnahme gilt für alle Komponenten. Das Ergebnis im Einzelnen ist aber nicht zuletzt davon abhängig, was unter „Ansicht → Benutzeroberfläche“ eingestellt ist: Für die beiden „Register“-Darstellungen hat das Farbthema keine Auswirkung (siehe Punkt 3).

2. Allgemeine Ansichtsoptionen

Die Einstellungen unter „Extras → Optionen → LibreOffice → Ansicht“ gelten ebenfalls für alle Komponenten. Auf großen Bildschirmen mit hoher Auflösung empfiehlt sich für alle drei aufgeführten Symbolkategorien die Einstellung „Groß“. Die wichtigere Option ist jedoch der „Symbolstil“. Das voreingestellte Symbolthema für Leisten und Menü wirkt buntscheckig und unruhig. Ruhiger und sachlicher ist demgegenüber das Thema „Breeze“. Falls das Drop-down-Feld unter „Symbolstil“ keine Alternativen anbietet, können Sie diese nachinstallieren: Im Angebot sind die Pakete „libreoffice-style-breeze“, „libreoffice-style-hicontrast“, „libreoffice-style-human“, „libreoffice-style-oxygen“, „libreoffice-style-galaxy“, „libreoffice-style-sifr“ und „libreoffice-style-tango“. Das empfohlene „Breeze“ ist mit dem Terminalbefehl

```
sudo apt install libreoffice-style-
 breeze
```

schnell eingerichtet.

Weitere globale Einstellungen zur Optik bietet der Punkt „Extras → Optionen → LibreOffice → Anwendungsfarben“. Dieser Dialog zeigt detaillierte Farbeinstellungen für Texte, Tabellen und allgemeine Elemente wie den „Dokumenthintergrund“ oder den „Hintergrund der Anwendung“. Diese Sektion „Allgemein“ ermöglicht es zum Beispiel, den Anwendungshintergrund farblich an ein Farbschema des Menübereichs (siehe Punkt 1) anzugleichen.

3. Mehrere Menükonzepte zur Auswahl

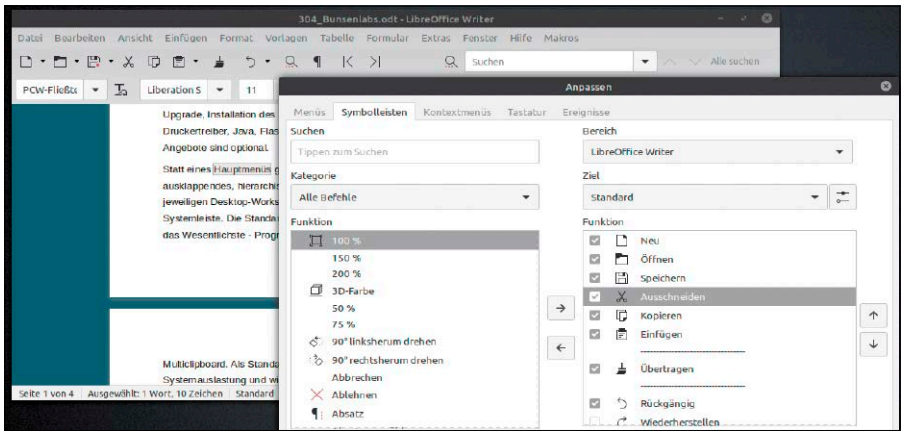
Was neueres Libre Office unter „Ansicht → Benutzeroberfläche“ anbietet, ist verwirrend und zum Teil kontraproduktiv. Von den insgesamt sieben Optionen halten wir nur drei für alltagstauglich: Die Option „Symbolleisten“ ist die klassische Bedienung mit statischem Hauptmenü und Symbolleisten. Mit der Option „Gruppiert kompakt“ lässt sich das Meiste gut erledigen, für Spezielleres kann man über „Menü → Menüleiste“ das klassische Hauptmenü einblenden. Die weitere Option „In Registern“ orientiert sich am Menükonzept der Microsoft-Suite, was ebenfalls praktikabel ist. Wer dort nicht findet, was er braucht, kommt über „Ansicht → Ansicht → Menüleiste“ zum klassischen Hauptmenü.

Generell sehen die neuen Menükonzepte besser aus und haben für Alltagsaufgaben kürzere Klickwege. Wer aber das klassische Menü plus Symbolleisten über Jahre gewöhnt ist, wird damit produktiver arbeiten. Ein Kompromiss könnte so aussehen, dass Sie eine schicke Register- oder Kompaktansicht wählen und sich das Hauptmenü auf eine einprägsame Tastenkombination wie etwa Strg-M legen. Das geht über „Extras → Anpassen → Tastatur“, Scrollen zur gewünschten Tastenkombination, Klick auf „Ändern“, gefolgt von der Auswahl „Ansicht“ (unter „Bereich“) sowie „Menüleiste“ (unter „Funktion“). Nach neuerlichem Klick auf „Ändern“ ist der Hotkey aktiv.

Achtung: Das Menü- und Bedienkonzept muss für jede Office-Komponente einzeln eingestellt werden.

4. Symbolleisten und Menüs bearbeiten

Die klassische Benutzerführung mit Hauptmenü und Symbolleisten hat einen großen Vorzug: Das Angebot kann maßgeschneidert den eigenen Arbeitsabläufen angepasst werden. Insbesondere bei den Symbolleisten ist eine Anpassung dringend zu empfehlen. Die Standardbestückung kommt arg überladen daher, obwohl nur zwei von den zahlreichen verfügbaren Symbolleisten aktiv sind („Standard“ und „Formatierungen“). Alle vorangestellten Leisten sind über „Ansicht → Symbolleisten“ einsehbar und dort auch zu aktivieren oder abzuschalten. Die meisten Leisten sind relativ speziell, lediglich „Suchen“ kommt neben „Standard“ und „Formatierungen“ für den normalen Einsatz



Reduzierte Symbolleisten: Was Sie nicht tagtäglich und mit einem Klick brauchen, können Sie ausmisten und damit Platz und Übersicht schaffen.

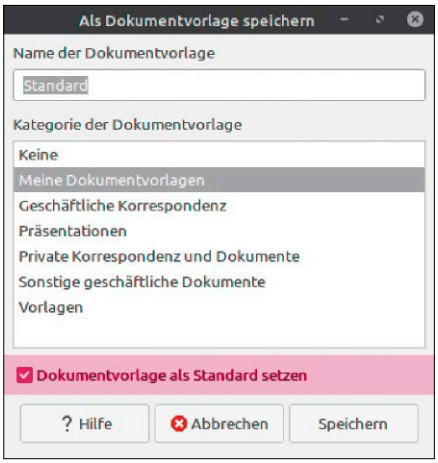
in Betracht. Das Angebot einer Leiste bearbeiten Sie entweder über „Extras → Anpassen → Symbolleisten“ oder – direkter – nach Rechtsklick auf die gewünschte Leiste und „Symbolleiste anpassen“. Letzteres hat den Vorteil, dass Sie sich sofort in der richtigen Leiste befinden. Im rechten Teil des Dialogs unter „Funktion“ erkennen Sie die aktuell aktivierten Symbole am Häkchensymbol. Jede Funktion lässt sich über das Häkchen abschalten oder mit dem Pfeilsymbol in der Dialogmitte komplett aus der Leiste entfernen. Umgekehrt fügen Sie fehlende Funktionen ein, indem Sie in der Liste links eine Funktion markieren und mit dem Pfeilsymbol in die Symbolleiste holen. Nachträgliche Positionsänderungen sind jederzeit per Drag & Drop möglich oder mit den Positionspfeilen ganz rechts.

Analog zu den Symbolleisten können Sie das Hauptmenü über „Extras → Anpassen → Menüs“ ebenfalls individuell optimieren. Allzu rigoroses Abspecken ist hier aber nicht ratsam, da Sie nicht wissen, ob Sie eine heute vermeintlich entbehrliche Unterfunktion künftig nicht doch noch benötigen. Ein besserer Kandidat zur Bearbeitung ist das Kontextmenü („Extras → Anpassen → Kontextmenüs“).

Beachten Sie, dass dieses objektbezogen ist und für das gewünschte Objekt („Ziel“) bearbeitet werden muss. In Writer wäre das primäre Ziel „Text“, in Calc „Zelle“ oder auch „Spaltenkopf“.

5. Standard-Dokumentvorlagen einrichten

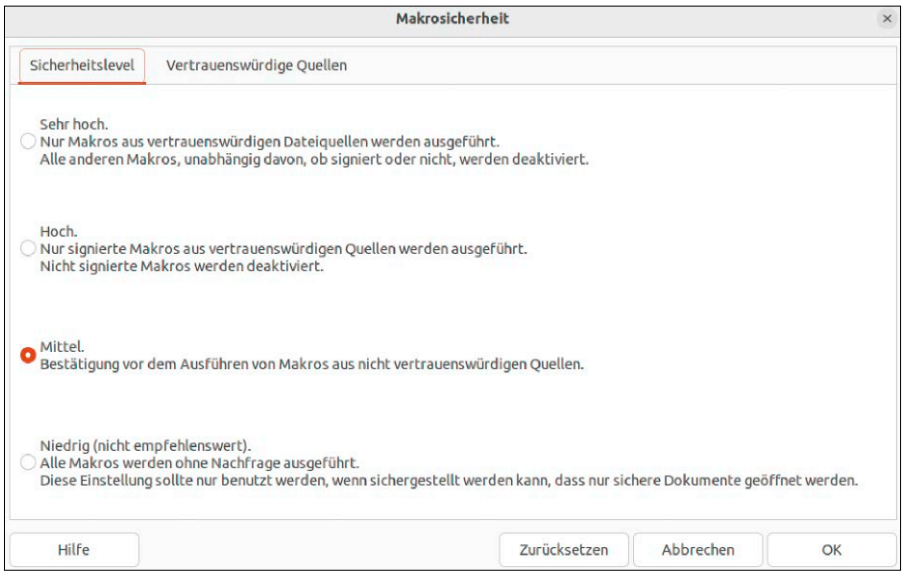
Wenn Sie im Writer über „Datei → Neu →Textdokument“ eine neue Datei erstellen, formatiert Libre Office mit Standardeinstellungen, die im Programm hinterlegt sind. Anders als bei Microsoft Word gibt es zunächst keine Standardvorlage, die Sie individuell einrichten könnten. Ein solcher Standard lässt sich aber in allen Komponenten mühelos erstellen: Nehmen Sie in einem Textdokument oder einer Tabelle alle gewünschten Änderungen vor: Das kann enthaltene Formatvorlagen, Standardschrift, Schriftgröße, Absatzabstände, Zeilenhöhe, Spaltenbreite, Zahlenformate, Zoomfaktor und vieles mehr betreffen. Inhaltlich sollte die Datei allerdings am Ende der Vorbereitungen geleert werden. Die „leere“, aber mit Formatvorgaben versehene Datei speichern Sie dann über „Datei → Dokumentvorlagen → Als Dokumentvorlage speichern“, wobei Sie ganz unten die Option „Dokumentvorlage als Standard setzen“ aktivieren. ■



Eine globale Dokumentvorlage ist im Handumdrehen angelegt und gespeichert. Dies erspart das Einstellen von Schrift, Absatzabstand, Zellhöhe, Zoomfaktor und vielem mehr.

Erweiterungen & Makros für Libre Office

Erweiterungen für Libre Office ergänzen nützliche Funktionen oder automatisieren Arbeitsschritte. Wie sich Erweiterungen einrichten und selbst erstellen lassen, lesen Sie in diesem Artikel.



Makroeinstellungen: Makros aus Erweiterungen stuft Libre Office automatisch als sicher ein. Für Makros aus Dokumenten müssen Sie den Sicherheitslevel auf „Mittel“ einstellen.

VON THORSTEN EGGELING

Fertige Erweiterungen für Libre Office gibt es zum kostenlosen Download auf *https://extensions.libreoffice.org*. Außerdem finden Sie hier Vorlagenpakete, die ebenfalls als Erweiterungen ausgeliefert werden. Meist funktionieren auch Erweiterungen für Open Office (*https://extensions.openoffice.org*). Vorlagen werden unter *https://templates.openoffice.org* angeboten.

Eine Auswahl nützlicher Erweiterungen und Vorlagen haben wir auf die Heft-DVD gepackt. In diesem Artikel zeigen wir, wie sich die Erweiterungen installieren lassen, wie Sie eigene Erweiterungen erstellen und Probleme mit Erweiterungen beheben. Auf die Grundlagen der Makroprogrammierung gehen wir nicht ein. Dazu finden Sie auf der Heft-DVD einige einführende Dokumente, zumeist in englischer Sprache.

Libre Office vorbereiten

Bevor Sie Erweiterungen installieren oder mit Makros arbeiten, sollten Sie eine Sicherungskopie des Libre-Office-Profils erstellen. In seltenen Fällen kann Libre Office nach der Installation von Erweiterungen abstürzen oder sich nicht mehr starten lassen. Für ein Backup beenden Sie Libre Office, starten den Dateimanager, gehen in Ihr Home-Verzeichnis und drücken die Tastenkombination Strg-H (Ubuntu Nautilus oder Linux Mint Nemo). Damit blenden Sie die verborgenen Dateien und Verzeichnisse ein. Kopieren Sie den Ordner „~/.config/libreoffice“ in ein Backup-Verzeichnis.

Gehen Sie in Libre Office auf „Extras → Optionen → LibreOffice → Erweitert“. Aktivieren Sie die Java-Laufzeitumgebung, die von einigen Erweiterungen benötigt wird. Wenn keine angezeigt wird, installieren Sie unter Ubuntu/Linux/Mint das Paket „libreoffice-java-common“. Danach starten Sie Libre Office neu und konfigurieren dann die Java-Laufzeitumgebung.

An der gleichen Stelle können Sie unter „Optionale Funktionen“ ein Häkchen vor „Makroaufzeichnung ermöglichen (eingeschränkt)“ setzen. Über „Extras → Makros → Makro aufzeichnen“ können Sie dann Aufrufe von Menüs oder Funktionen sowie Tastenanschläge als Makro speichern. Das funktioniert aber meist nicht zuverlässig und das aufgezeichnete Makro erfordert manuelle Nacharbeit.

Gehen Sie in den „Optionen“ auf „LibreOffice → Sicherheit“ und klicken Sie auf „Makrosicherheit“. Hier stellen Sie den Sicherheitslevel auf „Mittel“. Für Erweiterungen ist das nicht erforderlich, aber für Makros, die aus Dokumenten installiert werden. Wenn Sie ein Dokument öffnen, das Makros enthält, bestätigen Sie mit „Makros aktivieren“. Aktivieren Sie Makros aber nur in Dokumenten sicherer oder eigener Herkunft.

Erweiterungen installieren

Erweiterungen für Libre Office tragen die Dateinamenserweiterung „.oxt“. Öffnen Sie die gewünschte Erweiterung per Doppelklick im Dateimanager. Der Dialog „Extension-Manager“ erscheint und Sie bestätigen die Installation per Klick auf „OK“. Bei einigen Erweiterungen müssen Sie danach die Lizenzvereinbarungen bestätigen. Klicken Sie auf „Schließen“, danach auf „Jetzt neu starten“. Nach der Installation von Erweite-

rungen muss Libre Office immer neu gestartet werden.

Alternativ gehen Sie in Libre Office auf „Extras → Extension-Manager“ (ab Libre Office 7.5 heißt der Menüpunkt „Erweiterungsverwaltung“). Nach dem Klick auf „Hinzufügen“ wählen Sie die gewünschte Erweiterungsdatei. In dem Fenster können Sie Erweiterungen auch deinstallieren, deaktivieren oder nach Updates suchen.

Erweiterungen integrieren sich unterschiedlich in das Büropaket. Oft wird eine neue Symbolleiste oder ein Menüeintrag erzeugt (siehe Tabelle auf Seite 59). Wenn nicht, lassen sich die enthaltenem Makros über „Extras → Makros → Makro ausführen“ oder in der Basic-IDE (Integrated Development Environment) starten („Extras → Makros → Makro → Makros bearbeiten“ oder „Extras → Makros → Makro → Makros verwalten → Basic). Der Inhalt der Vorlagenpakete ist über „Datei → Dokumentvorlagen → Dokumentvorlagen verwalten“ erreichbar.

Installation im Terminal: Im Basic-Editor tauchen im „Objektkatalog“ zwei Rubriken auf. „Meine Makros und Dialoge“ zeigt Elemente, die im Libre-Office-Profil des Benutzers gespeichert sind. Die Makros und Dialoge lassen sich bearbeiten und speichern. „LibreOffice-Makros und -Dialoge“ zeigt gemeinsam in jedem Benutzerkonto genutzte Elemente. Die Inhalte sind schreibgeschützt und lassen sich nur mit administrativen Rechten ändern.

Im Terminal verwenden Sie das Tool unopkg für die Installation und Deinstallation von Erweiterungen. Der Aufruf mit

```
unopkg add [.oxt-Datei]
```

installiert eine Erweiterung für den aktuellen Nutzer. Für den Platzhalter setzen Sie Pfad und Dateinamen der gewünschten Erweiterung ein.

Der Befehl

```
unopkg list
```

zeigt die installierten Erweiterungen an. Hinter „Identifier:“ erscheint die ID einer Erweiterung, meist in der Form „my.domain.my_extension-id“ oder ähnlich. Diese Information benötigen Sie für die Deinstallation, die mit

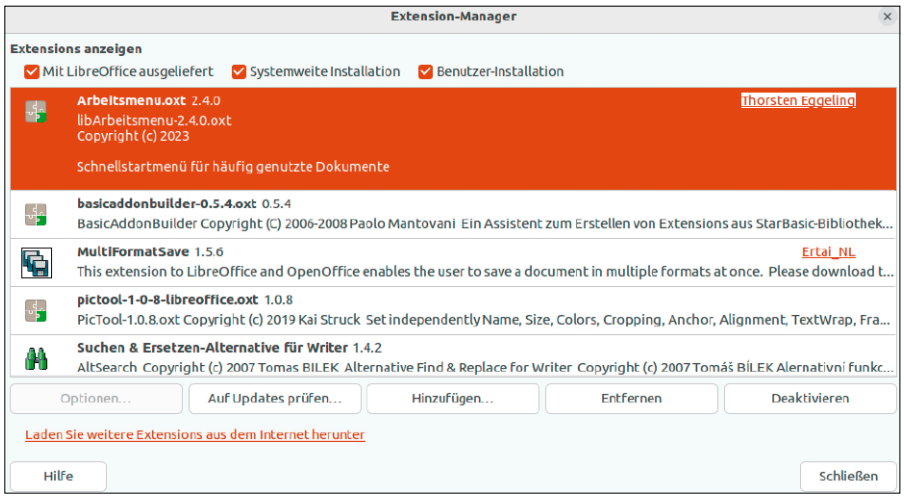
```
unopkg remove [ID]
```

erfolgt.

Der Befehl

```
sudo unopkg add --shared [.oxt-
  Datei]
```

installiert eine Erweiterung schreibgeschützt für alle Benutzerkonten und



Erweiterungen verwalten: Über den „Extension-Manager“ lassen sich Erweiterungen in Libre Office installieren und auch entfernen oder deaktivieren.

```
sudo unopkg list --shared
```

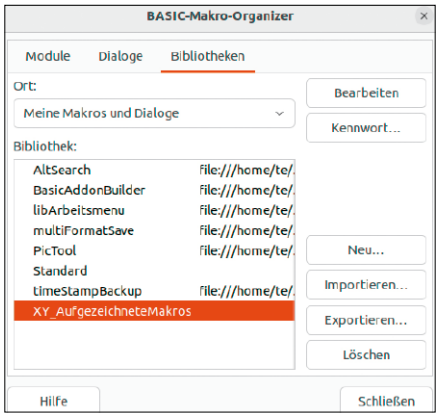
zeigt die gemeinsam genutzten Erweiterungen an, die sich wiederum mit

```
sudo unopkg remove [ID]
```

entfernen lassen.

Einfache Erweiterungen selbst erstellen

Selbst erstellte oder aufgezeichnete Makros lassen sich in Erweiterungen speichern. Das ist für ein Backup nützlich oder für die schnelle Installation von Makros nach einer Neuinstallation oder auf einem anderen Rechner. In der Basic-IDE („Extras → Makros → Makro → Makros bearbeiten“) lassen sich die Makros in Bibliotheken organisieren, die mehrere Module enthalten können. Von Haus aus ist unter „Meine Makros und Dialoge“ die Bibliothek „Standard“ mit dem Basic-Modul „Module1“ vorhanden. Es empfiehlt sich, die Bibliothek „Standard“ nur für die Entwicklung oder Tests zu verwenden, da sie sich nicht exportieren lässt. Über „Extras → Makros verwalten → Basic“ können Sie mit Klick auf „Verwalten“ auf der Registerkarte „Bibliotheken“ eine neue Bibliothek erstellen. Verwenden Sie aussagekräftige Bezeichnungen für Ihre Bibliotheken mit einem vorangestellten Präfix, beispielsweise „XY_AufgezeichneteMakros“. Das erleichtert später die Organisation der Bibliotheken.



Bibliotheken sichern: Der „BASIC-Makro-Organizer“ ermöglicht den Export von Bibliotheken als Erweiterung oder als einzelne Dateien in einen Ordner.

Für den Export gehen Sie auf „Extras → Makros verwalten → Basic → Verwalten → Bibliotheken“. Klicken Sie die gewünschte Bibliothek an und dann auf „Exportieren“. Belassen Sie die Option „Als Extension exportieren“, klicken Sie auf „OK“ und geben Sie Speicherort und Namen der Erweiterung an. Mit der Option „Als BASIC-Bibliothek exportieren“ speichern Sie die Module einer Bibliothek in einem Ordner. Die Dateien lassen sich über „Importieren“ wieder laden, allerdings nur einzeln. In einer Erweiterung speichern Sie alle Module auf einmal.

Erweiterungen bearbeiten

Eine „oxt“-Datei ist ein ZIP-Archiv, das sich im Terminal entpacken lässt. Wenn die zuvor exportierte Erweiterung beispielsweise „XY_AufgezeichneteMakros.oxt“ heißt, verwenden Sie dafür die Befehlszeile

```
unzip XY_AufgezeichneteMakros.oxt
  -d XY_AufgezeichneteMakros
```

Sollten unzip und zip auf Ihrem System nicht installiert sein, holen Sie das mit

```
sudo apt install unzip zip
```

nach.

Beschreibung für Erweiterungen: In der Datei „META-INF/manifest.xml“ stehen Pfade zu Ordnern und Dateien. Sie können eine Datei mit Beschreibungen ergänzen.

Im Zielordner „XY_AufgezeichneteMakros“ finden Sie einen Ordner mit dem gleichen Namen, der die Makrodateien im XML-Format enthält. In „Module1.xba“ ist der Basic-Code untergebracht, auf den der Inhalt von „script.xlb“ verweist. Die Datei „manifest.xml“ im Ordner „META-INF“ enthält den Pfad zu den Basic-Dateien.

Sie können eine Beschreibung hinzufügen, die bei der Installation in der Erweiterungsverwaltung erscheint. Erstellen Sie den Ordner „pkg-desc“ und darin die Textdatei „pkg-description.txt“ mit der Beschreibung. Damit die Datei berücksichtigt wird, bauen Sie in die Datei „META-INF/manifest.xml“ unterhalb von „<manifest:manifest>“ die folgende Zeile ein:

```
<manifest:file-entry
 manifest:full-path="pkg-desc/
 pkg-description.txt"
 manifest:media-
 type="application/vnd.sun.star.
 package-bundle-description"/>
```

Achten Sie beim Bearbeiten stets auf die korrekt gesetzten XML-Tags, sonst bricht Libre Office die Installation mit einer Fehlermeldung ab. Abschließend erzeugen Sie ein neues ZIP-Archiv der Erweiterungen

```
cd XY_AufgezeichneteMakros
zip -r ../XY_AufgezeichneteMakros_
 v2.oxt *
```

Es ist wichtig, zuerst mit *cd* in den Ordner zu wechseln, weil zip sonst den Ordner selbst einpackt und Libre Office die Dateien dann nicht findet.

Erweiterungen reparieren

Erweiterungen für Open Office funktionieren in der Regel auch unter Libre Office. Es gibt jedoch eine Änderung ab Open Office 4.x, die die Einrichtung einer Symbolleiste unter Libre Office verhindert. Ein Beispiel dafür ist Pepito Cleaner Fork (*http://bit.ly/3HKpM6h*). Bei der Version auf Heft-DVD haben wir den Fehler bereits korrigiert. Sollte das Problem bei einer Erweiterung auftreten, entpacken Sie diese wie im vorherigen Abschnitt beschrieben. Öffnen Sie die Datei „addon.xcu“ in einem Editor. Sie finden in der Datei einen Abschnitt, der mit

```
<node oor:name="OfficeToolBar">
```

beginnt. Am Anfang muss die Definition entfernt oder auskommentiert werden, die mit „<prop oor:name=“Title“ beginnt. Die Klammer „<node oor:name=“ToolBarItems“> […]</node>“ muss ebenfalls entfernt werden. Sehen Sie sich die Datei „addon.xcu“ von Pepito Cleaner Fork zum Vergleich an, in der wir die Zeilen auskommentiert haben. Nach den Änderungen packen Sie den Ordner wieder in eine „.oxt“-Datei und die Erweiterung installiert auch in Libre Office eine Symbolleiste.

Assistenten für komplexe Erweiterungen nutzen

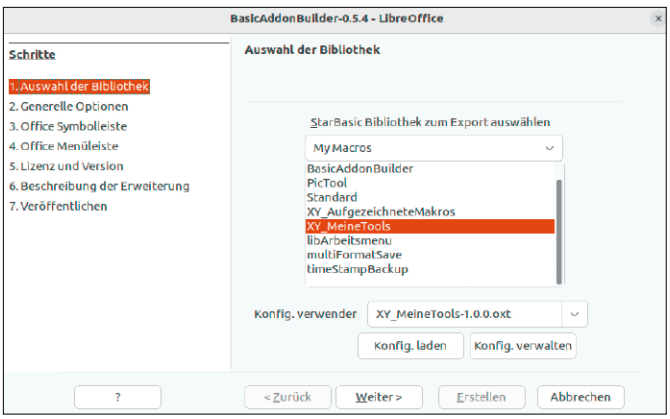
Auf die Heft-DVD haben wir die Erweiterung Basic Addon Builder 0.5.4 gepackt, die Erweiterungen inklusive Symbolleisten und Menüs erstellen kann. Das Original stammt von *https://extensions.openoffice.org/de/project/basicaddonbuilder-extensions-packager*. Die Entwicklung wurde aber nie ganz fertiggestellt und unter Libre Office 7.x funktioniert das Tool nicht korrekt. Die Version 0.5.4 auf der Heft-DVD haben wir angepasst und um Funktionen erweitert.

Der Basic Addon Builder lässt sich nach der Installation über eine Symbolleiste starten. Im Assistenten wählen Sie die Bibliothek, aus der Sie eine Erweiterung erstellen möchten. Im nächsten Schritt geben Sie Optionen wie „eigene Office-Symbolleiste hinzufügen“ und/oder „Hauptmenüeintrag hinzufügen“ an. Die dafür nötigen Informationen werden in den nachfolgenden Schritten abgefragt. Im letzten Schritt vergeben Sie einen Dateinamen und klicken auf „Erstellen“.

Die Erweiterungen auf der Heft-DVD nutzen

Zu den meisten Erweiterungen auf der Heft-DVD finden Sie eine Beschreibung, indem Sie die Weblinks gemäß der Tabelle aufrufen. Wir ergänzen hier nur die Beschreibungen für Erweiterungen der Linux-Welt-Redaktion.

Arbeitsmenü: Die Erweiterung baut den Menüpunkt „Arbeitsmenü“ in die Module Writer, Calc und das Startcenter ein. Über „Arbeitsmenü → Zum Menü hinzufügen“ fügen Sie den Pfad des aktuell geöffneten Dokuments in das Menü ein. Nach einem Neustart von Libre Office können Sie das als Favoriten gespeicherte Dokument darüber schnell wieder aufrufen. Gehen Sie auf „Arbeitsmenü → Optionen“. Das Fenster zeigt eine Liste der gespeicherten Favoriten. Sie können die Reihenfolge ändern und einzelne oder alle Einträge löschen. Das erste Dokument in der Liste lässt sich außerdem schnell über die Symbolleiste mit der Schaltfläche „Dokument öffnen“ aufrufen. „Arbeitsmenü → Öffne Dokument-Ord-



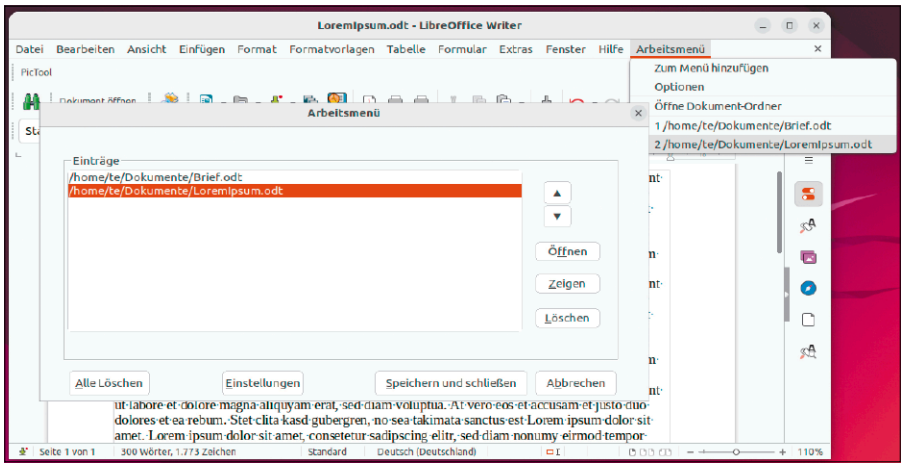
Erweiterungen erstellen: Mit Basic Addon Builder erstellen Sie Erweiterungen aus Bibliotheken und bauen bei Bedarf Menüeinträge und Symbolleisten ein.

ner“ öffnet den Speicherort des aktuellen Dokuments im Dateimanager. Für Ubuntu ist „nautilus“ voreingestellt. Wenn Sie einen anderen Dateimanager verwenden, passen Sie im Makro die Angabe hinter „Const strLinuxFileManager=“ an.

Backup-Libs: Das Dokument enthält Makros, über die sich alle Basic-Bibliotheken in einem Dokument oder im Dateisystem speichern lassen. Lesen Sie den Beschreibungstext und nehmen Sie bei Bedarf Anpassungen im kommentierten Makrocode vor.

Sample Extension: Das Beispiel demonstriert, wie sich Menüs und Symbolleisten bei der Installation einer Erweiterung oder per Makrocode erstellen lassen.

Sample Config Extension: Libre Office speichert seine Konfiguration im Benutzerprofile in der Datei „registrymodifications.xcu“. Um herauszufinden, welche Werte zu welcher Option gehören, startet man Libre Office mit einem frischen Benutzerprofil, passt Optionen an und sucht in der Datei nach Änderungen. Die gewünschten Optionen kann man dann in einer Erweiterung unterbringen, die alle Einstellungen etwa auf einem anderen PC automatisch vornimmt. Unsere Beispielerweiterung setzt die Makro-Sicherheitsstufe auf „Mittel“ und aktiviert die Speicherung von Autowiederherstellungs-Informationen. Eine kurze Anleitung finden Sie über *https://bit.ly/3RPYpMI*. ■



Favoritenmenü erstellen: Über die Arbeitsmenü-Erweiterung nehmen Sie Dokumente in das Menü auf. Häufig benutzte Dateien sind dann schnell erreichbar.

ERWEITERUNGEN & VORLAGEN FÜR LIBRE OFFICE

Name	Modul	Beschreibung	Aufruf mit	Sprache	Internet
Add Pics 2.5.0	Writer	mehrere Bilder aus Ordner einfügen	Symbolleiste	Deutsch	*http://bit.ly/40D9FA4*
Alt Search 1.4.2	Writer	verbesserter Ersatz für „Bearbeiten → Suchen und ersetzen“	Symbolleiste	Deutsch	*http://bit.ly/40xLuDf*
Arbeitsmenü 2.4	Office	Favoriten-Menü	Menü „Arbeitsmenü“	Deutsch	*https://bit.ly/3RHgrRb*
Backup-Libs 1.0	Basic-IDE	Basic-Module sichern	Schaltflächen im Dokument	Deutsch	*https://bit.ly/3XjUlW1*
Basic Addon Builder 0.5.4	Office	Erweiterungen erstellen	Symbolleiste	Deutsch	*https://bit.ly/3XtUVAZ*
Copy only visible cells 2.0	Calc	nur sichtbare Zellen kopieren	Symbolleiste	Deutsch	*http://bit.ly/3IfTFDY*
EPC 0.9.2	Draw	Symbole für Diagramme	Gallery → EPC	Englisch	*http://bit.ly/3YQOw3V*
Export As Images 1.0.1	Impress/Draw	Folien als Bilder speichern	„Datei → Export as images“	Englisch	*http://bit.ly/3DSBVVw*
Jahreskalender 1.0	Calc	konfigurierbares Kalenderblatt	Dokument	Deutsch	*http://bit.ly/3JSGqU8*
Multi Format Save 1.5.6	Writer	Dokument in mehreren Formaten speichern	„Datei → Multi Speichern“	Deutsch	*http://bit.ly/3JM4ms9*
Oxygen Office Extra – German Templates 2.6.0.2	Writer	Dokumentvorlagenpaket	„Datei → Neu → Dokumentvorlagen“	Deutsch	*http://bit.ly/3HMAjhe*
Pepito Cleaner Fork 0.1.17	Writer	Dokument bereinigen	Symbolleiste	Englisch	*http://bit.ly/3HKpM6h*
Photo Album 3.5	Impress	Fotoalbum aus Folien erstellen	„Extras → Plug-ins → Create Photo Album“	Englisch	*http://bit.ly/3HDzQOq*
Pictool 1.0.8	Writer	Bilder im Dokument bearbeiten	Symbolleiste	Englisch	*http://bit.ly/3XiLfca*
Poemenia 0.4.0	Writer	deutsche Oberfläche für Pepito Cleaner	„Extras → Plug-ins → Poemenia“	Deutsch	*http://bit.ly/3XtV4o1*
Professional Template Pack – German 1.0	Writer	Dokumentvorlagenpaket	„Datei → Neu → Dokumentvorlagen“	Deutsch	*http://bit.ly/3JUFK0i*
Professional Template Pack II – German 1.0	Writer	Dokumentvorlagenpaket	„Datei → Neu → Dokumentvorlagen“	Deutsch	*http://bit.ly/3JRnBke*
Review Toolbar 20131006.0.1	Writer	Symbolleiste für „Änderungen aufzeichnen“	Symbolleiste	Englisch	*http://bit.ly/3JRnCEO*
Sample Config Extension 1.0	Office	Demo der Konfiguration über eine Erweiterung	Basic-IDE	Englisch	*https://bit.ly/40Fqsm9*
Sample Extension 1.0.0	Office	Demo einer Erweiterung mit Menü, Symbolleiste und Makros	Basic-IDE	Englisch	*https://bit.ly/3x8CpDe*
Timestamp Backup 1.2.2	Office	zusätzlich Sicherungskopie mit Zeitstempel speichern	Symbolleiste	Deutsch	*https://bit.ly/3DUe47Z*
Writer2ePub 1.1.28	Writer	speichert Dokumente im Epub-Format	Symbolleiste	Deutsch	*http://writer2epub.it*
Xray-Tool 6.0	Basic-IDE	Objekte im Basic-Editor untersuchen	Befehl „Xray“	Deutsch	*http://bit.ly/3YB3o5Y*

Docfetcher: Der Textindexer

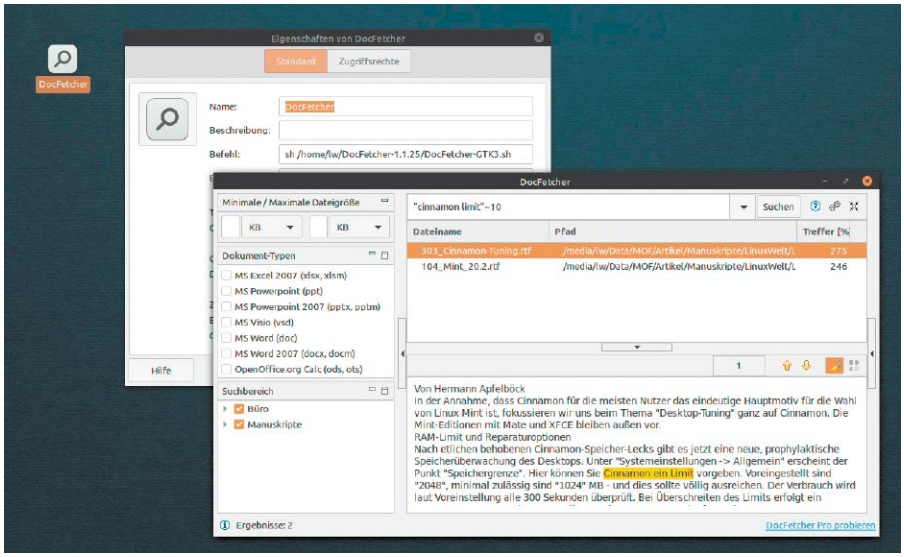
Nicht nur Textproduzierende benötigen eine schnelle Suche in Dateiinhalten. Im Prinzip profitieren Büroangestellte, Studenten und Datensammler jeder Ausrichtung von einer präzisen Textrecherche im vorhandenen Datenbestand.

VON HERMANN APFELBÖCK

Wenn es um Textsuche geht, ist der unkomplizierte Docfetcher ein Top-Favorit. Das Java-Tool leistet schnelle Volltextsuche für Text-, Script und HTML-Dateien, Libre-Office- und Microsoft-Office-Formate, RTF, PDF, Epub, ferner auch eine „Tag"-Suche in MP3, Flac und JPG. Da das clevere Programm sogar Packarchive (ZIP, 7Z, RAR, TAR) durchsucht, kann man es auf jedes heterogene Datenarchiv ansetzen.

Docfetcher arbeitet mit einem Index, den Sie für ein oder mehrere gewünschte Verzeichnis(se) erstellen. Die Suchsyntax unterstützt logische AND/OR/NOT-Operatoren, Nachbarschaftssuche (Wortvorkommen in einem definierten Abstand) sowie Fuzzy-Suche (ähnliche Wörter).

Exzellent ist ferner die großzügige und kopierbare Vorschau der Fundstellen, die das Aufsuchen der eigentlichen Quelldatei überflüssig macht.



Top-Tool für Inhaltssuche: Docfetcher ist schnell, präzise und unkompliziert, denn er verarbeitet alle prominenten Dokument-, Audio-, Bildformate und Archivformate.

Installation und Voraussetzungen

Docfetcher ist in Java geschrieben, benötigt daher auf dem System eine Java-Umgebung, aber keine Installation. Damit ist das Suchprogramm plattformunabhängig und funktioniert auf Linux, Windows und Mac-OS. Welche Java-Version Ihr Linux-System benötigt, müssen Sie nicht wissen, denn der Befehl

```
sudo apt install default-jre
```

installiert automatisch die zum System passende Java-Version, mit der alle Anwendungen und auch Docfetcher funktionieren. Falls diese Version bereits vorliegt, erhalten Sie nach diesem Kommando die Meldung „[...] ist schon die neueste Version" und die die Installation entfällt.

Laden Sie dann die portable Version von Docfetcher über *http://docfetcher.sourceforge.net* herunter (für alle Betriebssysteme). Unter Linux entpacken Sie die ZIP-Datei einfach in Ihrem Home-Verzeichnis in einen separaten Ordner. Damit ist die Einrichtung bereits erledigt, und im Prinzip starten Sie im Terminal das Programm mit diesem Befehl (bei sehr alten Desktops *Docfetcher-GTK2.sh*):

```
sh Docfetcher-GTK3.sh
```

Für häufigen Einsatz lohnt sich aber in jedem Fall ein komfortablerer Desktopstarter mit dem „Befehl" (Beispiel)

```
sh /home/lw/DocFetcher-1.1.25/
  DocFetcher-GTK3.sh
```

gemäß Aufmacherbild.

Desktops wie KDE oder Cinnamon unterstützen dies vorbildlich, bei Gnome ist etwas Handarbeit erforderlich.

Docfetcher als Snap: Wer sich weder um Java noch um einen bequemen Starterlink kümmern will, kann Docfetcher auch als Snap-Paket installieren:

```
sudo snap install docfetcher
```

Als Snap fällt Docfetcher deutlich umfangreicher aus (300 MB), bringt dann aber alles mit einschließlich Startmenü-Eintrag.

Docfetcher Pro: Es gibt eine Pro-Version von Docfetcher (*https://docfetcherpro.com/demo-purchase*) mit zusätzlichen Filtermöglichkeiten für Ordner und Dateitypen und verbesserter Outlook- und Ebook-Unterstützung. Linux-Nutzer oder generell Nicht-Outlook-Nutzer haben aber wenig Grund für die Bezahlversion (40 US-Dollar).

Indexierung von Ordnern

Wir empfehlen vor dem ersten Einsatz des Programms eine Anpassung im Start-Script. Für den Index größerer Datenbestände benötigt der Docfetcher (eigentlich Java) sehr viel Arbeitsspeicher. Mit Standardeinstellungen werden viele begonnene Indexläufe mit einer Meldung über mangelnden Speicher einfrieren und scheitern. Öffnen Sie daher die Datei „DocFetcher-GTK3.sh“ in einem beliebigen Editor und ändern Sie in deren letzten Zeile die beiden Einträge für „-Xmx“ und „-Xss“ wie folgt (siehe auch Abbildung rechts):

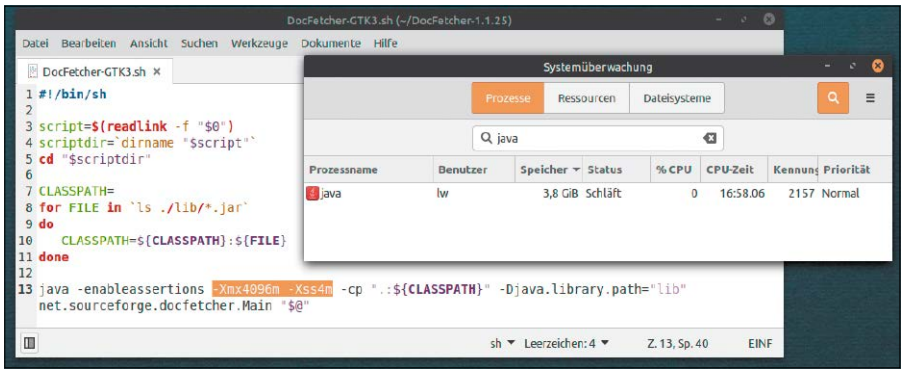
```
[…] -Xmx4096m -Xss4m […]
```

Dies ist eine Anweisung für Java und bedeutet, dass für den Prozess insgesamt vier GB RAM, für einzelne Threads vier MB RAM bereitstehen sollen. Wenn der Rechner so großzügige Werte nicht zulässt, verwenden Sie „-Xmx2048m -Xss4m“. Beachten Sie, dass Docfetcher solchen Speicherhunger nur bei Indexaufgaben zeitigt und beim späteren Suchalltag mit etwa 200 MB auskommt.

Indexierung: Um einen Index zu erstellen, klicken Sie mit der rechten Maustaste in das Feld unter „Suchbereich“ und gehen im Menü auf „Index erstellen aus → Ordner“. Navigieren Sie zum Ordner, in dem die Dateien liegen, die Sie durchsuchen wollen. Danach genügt ein Klick auf „OK“, um die Indexierung zu starten. Docfetcher arbeitet grundsätzlich rekursiv, berücksichtigt also alle Unterordner. Bei Bedarf wiederholen Sie den Vorgang für weitere Datenordner.

Index aktualisieren: Wenn Docfetcher läuft, bemerkt das Programm geänderte oder neue Dateien automatisch und nimmt sie sehr schnell in den Index auf. Wenn das Programm länger läuft, sollte der Index folglich stets aktuell sein. Sie können aber auch aktiv im Kontextmenü eines Eintrags im Suchbereich auf „Aktualisieren“ gehen. Zusätzlich gibt es für Linux und Windows einen Hintergrunddienst zur Indexaktualisierung – für Linux das Programm docfetcher-daemon-linux. Nach unserer Erfahrung ist es aber nicht notwendig, dieses Tool in den Autostart des Systems aufzunehmen.

Index für portablen Docfetcher: Da Docfetcher auf jedem System mit Java-Runtime läuft, ist auch ein Einsatz auf (zum Beispiel) USB möglich und die gemeinsame Nutzung unter Linux und Windows. Dazu muss der USB-Datenträger ein Dateisystem verwenden, das jedes Betriebssystem versteht – etwa NTFS. Ferner ist eine Option bei der Indexerstellung erforderlich: Wenn Sie nach Rechtsklick im „Suchbereich“ einen neuen Index erstellen, erscheint nach Auswahl des gewünschten Datenordners das Fenster „Indizierungs-Prozesse“. Ganz unten (scrollen!) gibt es die Option „Relative Pfade speichern, wenn möglich (zwecks Portabilität)“.



RAM-Fresser bei der Indexerstellung: Es ist zu empfehlen, dem Java-Programm via Startdatei großzügig Speicher bereitzustellen. Die Standards sind oft nicht ausreichend.

Suchfilter und Suchsyntax

Tippen Sie in das zentrale Suchfeld oben ein Wort ein und klicken Sie auf „Suchen“. Das Vorschaufenster unten zeigt die Fundstellen mit Kontext an und hebt sie farblich hervor. Über die Schaltfläche mit dem Pfeil-nach-unten-Symbol gehen Sie zur nächsten Fundstelle. Die Suche lässt sich nicht nur durch die Sucheingabe steuern, sondern ganz grob auch durch die globalen Filter im linken Fensterbereich: Deaktivieren Sie dort etwa ganze Ordner unter „Suchbereich“ oder die Mehrzahl der „Dokument-Typen“, falls Sie diese für die aktuelle Suche nicht benötigen.

Mehrere durch Leerzeichen getrennte Wörter verknüpft Docfetcher mit logischem „OR“. Sie können das durch ein explizites „AND“ zwischen den Wörtern ändern. In den Einstellungen (Zahnradsymbol) gibt es außerdem eine Option, ob „OR“ oder „AND“ der Standard sein soll (wir empfehlen „AND“). Stehen die Suchwörter

```
"linus torvalds"
```

in Anführungszeichen, dann sucht Docfetcher diese exakte Wortfolge. Sehr nützlich ist auch die Nachbarschaftssuche. Der Suchbegriff

```
"ubuntu nautilus" ~20
```

findet alle indexierten Dateien, die beide Wörter enthalten, der Abstand dieser Wörter aber höchstens 20 Wörter beträgt. Falls Sie einen Text suchen, der ein bestimmtes Wort, ein anderes jedoch nicht enthalten soll, verwenden Sie „NOT“:

```
cinnamon NOT "linux mint"
```

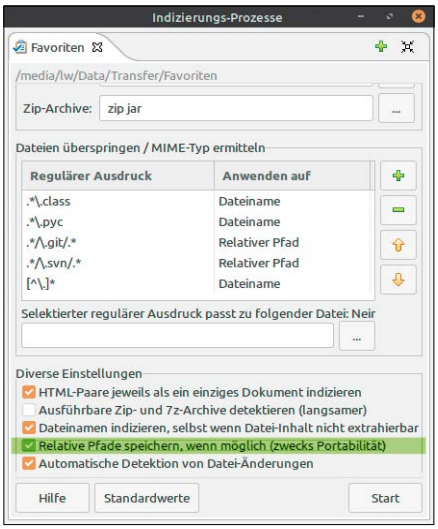
Falls die Schreibung oder Flexion eines Suchwortes nicht klar ist oder die Suche so weitreichend wie möglich bleiben soll, gibt es Wildcards wie

```
xcfe?
münchen*
```

oder noch unschärfer die Fuzzy-Suche:

```
selfie~
```

„AND“, „OR“, „NOT“, Wortfolgen und Nachbarschaftssuche werden den meisten Nutzern vollauf genügen. Wer noch präziser suchen will, kann darauf vertrauen, dass Docfetcher auch eine Suchsyntax mit Klammersetzungen und Kombination von unterschiedlichen Operatoren beherrscht. ■

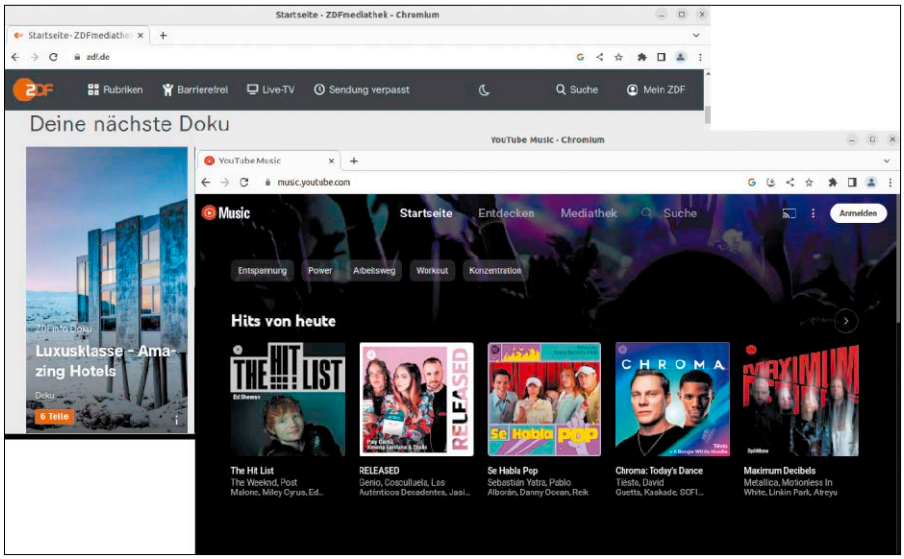


Relative Pfade: Diese Option ist entscheidend, wenn Docfetcher auf einem Datenträger unter Linux wie Windows funktionieren soll. Achten Sie außerdem auf ein kompatibles Dateisystem.

Musik & Filme laden

Musik und Filme werden im Internet oft nur zeitlich begrenzt angeboten. Wer die medialen Schätze dauerhaft speichern möchte, stößt jedoch schnell auf technische Hindernisse. Mit geeigneten Tools lassen sich die meisten Inhalte jedoch archivieren.

VON THORSTEN EGGELING



Video und Audio im Browser: Fast alles, was flimmert und lärmt, kann man sich über das Internet ansehen. Downloads sind meist nicht vorgesehen, aber mit geeigneten Tools dennoch möglich.

Filme und Musik gelangen inzwischen vor allem über das Internet auf die TV-Geräte und Computer. Etliche Streaminganbieter bieten Abos an, daneben gibt es kostenlose beziehungsweise werbefinanzierte Angebote. Die öffentlich-rechtlichen Anstalten liefern neben dem linearen TV-Angebot eigene Mediatheken und zahlreiche Inhalte auf Youtube und anderen Plattformen. Diese Inhalte sind nicht immer zeitlich unbegrenzt verfügbar. Dabei sind eher lizenzrechtliche oder bei den Mediatheken gesetzliche Beschränkungen, warum Filme wieder aus dem Angebot verschwinden. Daher ist der Wunsch verständlich, zumindest Lieblingssongs und Top-Videos auf der eigenen Festplatte zu archivieren. Offiziell werden Downloads meist nicht angeboten beziehungsweise nach Möglichkeit verhindert.

Auf rechtliche Fragen gehen wir hier nicht ein. Nur so viel: Das Urheberrecht (§ 53 UrhG) erlaubt Kopien für den Privatgebrauch. Wirksame technische Maßnahmen zum Schutz eines Werkes dürfen dabei nicht umgangen werden (§ 95a UrhG). Wie ein wirksamer Schutz genau aussieht, ist jedoch umstritten.

In diesem Artikel geht es um Tools, die multimediale Inhalte speichern. Die folgenden Beiträge in diesem Special zeigen, wie Sie Audio- und Videodateien bearbeiten und konvertieren sowie im heimischen Netzwerk bereitstellen.

Service: Alle Befehlszeilen zu diesem Artikel finden Sie als kopierbaren Text unter *https://m6u.de/MEDS*.

1. Streaming ja, Download nein?

Onlineanbieter möchten, dass Sie möglichst viel Zeit auf deren Website verbringen. Das ist verständlich, weil sich die kostenlosen Angebote über Werbung finanzieren. Einige Inhalte sind nicht dauerhaft verfügbar, etwa weil ein Youtube-Nutzer seinen Kanal aufgibt oder der Kanal gesperrt wird. In den Mediatheken der öffentlich-rechtlichen TV-Sender sind Filme maximal 12 Monate online, Dokumentation 24 Monate und Kulturdokumentationen bis zu fünf Jahre. Eingekaufte Filme und Serien werden oft nur über Satellit und DVB-T gesendet oder stehen im Internet nur einmalig als Livestream zur Verfügung. Über die Mediatheken sind sie nicht abrufbar.

Im Browser zeigen sich Filme, Musik und Podcasts eingebettet in eine Webseite. Die Videostreams stammen von einer bestimmten URL, über die der Player im Browserfenster den Inhalt bezieht und abspielt. Kennt man diese URL, lässt sich der Stream auch in einer Datei auf der Festplatte ablegen – man muss die URL nur herausfinden. Dabei hilft ein Tool (siehe Punkt 2), das den Inhalt der Webseite mit dem eingebetteten Player untersucht, die Video-URL ermittelt und den Stream herunterlädt.

Bei Diensten, die eine Anmeldung erfordern, beispielsweise Netflix und Amazon Prime Video, funktioniert das nicht. Die Streams sind verschlüsselt und lassen sich daher nicht ohne Weiteres speichern. Theoretisch wäre es möglich, den Stream nach der Entschlüsselung abzufangen und aufzuzeichnen. Aus rechtlichen Gründen sollte man darauf aber besser verzichten. Als unproblematisch gilt dagegen die simple Bildschirmaufnahme (siehe Punkt 5).

2. Streaminginhalte direkt herunterladen

Lange Zeit war youtube-dl (*https://youtube-dl.org*) das bevorzugte Tool für den Download bei öffentlich zugänglichen Streamingangeboten. Es lässt sich bei Ubuntu und Linux Mint über die Paketverwaltung installieren, wurde aber seit Ende 2021 nicht mehr aktualisiert. Mit yt-dlp gibt es jedoch

einen Ableger, der aktiv gepflegt wird. Updates sind bei diesem Tool besonders wichtig, weil die Anbieter häufig das Format der URLs ändern und der Download dann ohne Anpassungen nicht mehr funktioniert. yt-dlp ist zwar auf Youtube spezialisiert, funktioniert aber auch mit zahlreichen anderen Diensten, beispielsweise den Mediatheken von ARD, ZDF und Arte sowie Vimeo, Spiegel und Facebook (siehe *https://m6u.de/ytsup*).

Im Downloadbereich von yt-dlp (*https://github.com/yt-dlp/yt-dlp*) finden Sie unter „Releases“ die Datei „yt-dlp_linux“, die Sie nach dem Download im Terminal mit

```
chmod a+rx y t-dlp_linux
```

ausführbar machen.

Damit das Programm systemweit verfügbar ist und sich einfach aufrufen lässt, kopieren Sie es nach „/usr/local/bin“:

```
sudo cp yt-dlp_linux /usr/local/
  bin/yt-dlp
```

Für regelmäßige Updates verwenden Sie diesen Befehl:

```
sudo /usr/local/bin/yt-dlp -U
```

Das Tool benötigt für einige Aufgaben ffmpeg, das sich über das gleichnamige Paket installieren lässt. Ebenfalls nützlich ist die Installation von aria2, womit sich Downloads beschleunigen lassen. Um einen Stream herunterzuladen, verwenden Sie diese einfache Syntax:

```
yt-dlp '[URL]'
```

Den Platzhalter ersetzen Sie durch den in der Adressleiste des Browsers angezeigten Pfad, etwa wenn Sie sich ein Youtube-Video ansehen. Es ist nicht zwingend erforderlich, aber meist ratsam, die URL in einfache Anführungszeichen zu setzen. Andernfalls interpretiert yt-dlp enthaltene Sonderzeichen eventuell falsch.

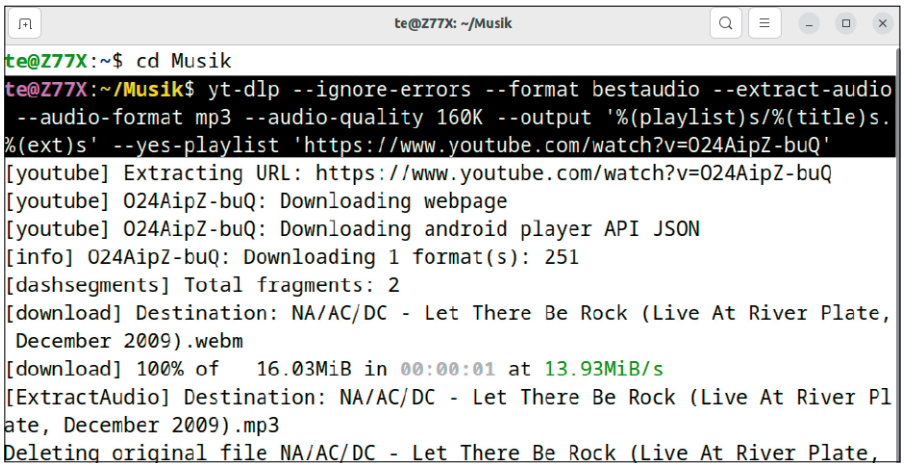
Das Tool kennt zahlreiche Optionen, mit denen sich fast jede Aufgabe erledigen lässt. Bringen Sie längere Befehlszeilen am besten in einem Shell-Script unter. Das folgende Beispiel speichern Sie in der Datei „yt-mkv.sh“, die Sie ausführbar machen:

```
yt-dlp --remux-video mkv --merge-
  output-format mkv $1
```

Der Aufruf erfolgt mit

```
./yt-mkv.sh '[URL]'
```

Die URL wird im Script mit der Variablen „$1“ übergeben. Der Videostream wird durch die Optionen nicht umgewandelt, sondern nur in einen MKV-Container umgepackt (ffmpeg erforderlich), was ohne Qualitätsverlust und schnell erfolgen kann.



Downloads im Terminal: Das Tool yt-dlp kann Inhalte von Youtube und vielen anderen Websites herunterladen. Es bietet auch Optionen, um etwa Musikvideos nur als MP3-Datei zu speichern.

Das folgende Beispiel lädt alle Dateien einer Youtube-Playlist als MP3-Dateien:

```
yt-dlp --ignore-errors --format
  bestaudio --extract-audio
  --audio-format mp3 --audio-
  quality 160K --output '%(playlist)
  s/%(title)s.%(ext)s' --yes-
  playlist '[Playlist-URL]'
```

Die Vorlage hinter „--output“ legt fest, dass Dateinamen in der Form „Titel.Extension“ gebildet und in einem Ordner mit dem Titel der Playlist abgelegt werden. „--ignore-errors“ setzt den Download fort, falls sich ein Stream gerade nicht laden lässt. Ohne diesen Schalter bricht das Tool den Download sonst komplett ab.

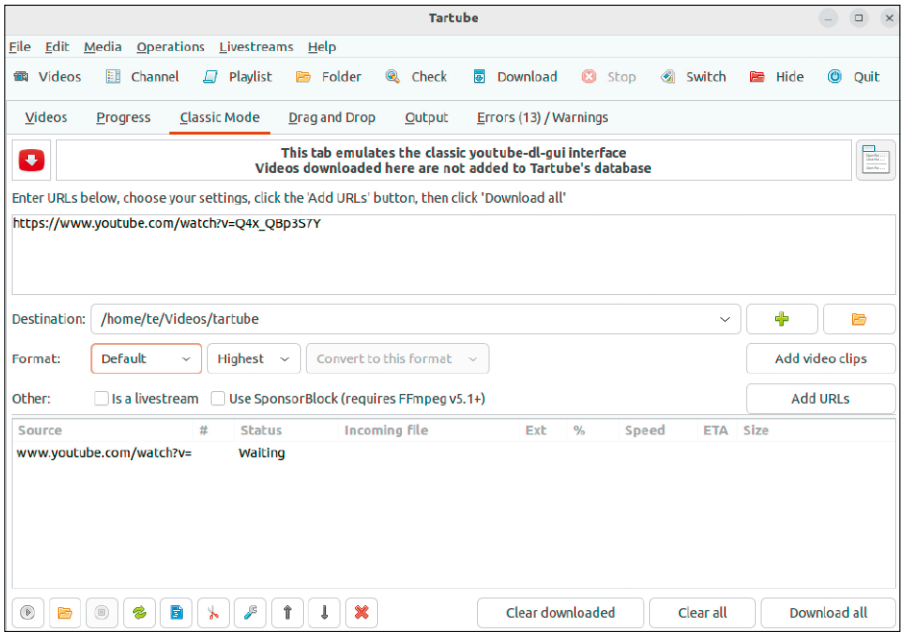
Vor allem für umfangreiche Downloads empfiehlt sich die Nutzung von aria2:

```
yt-dlp --ignore-errors --external-
  downloader aria2c --external-
  downloader-args aria2c:'-c -j 3 -x
  3 -s 3 -k 1M' --output '%(playlist)
  s/%(title)s.%(ext)s' --yes-
  playlist '[Playlist-URL]'
```

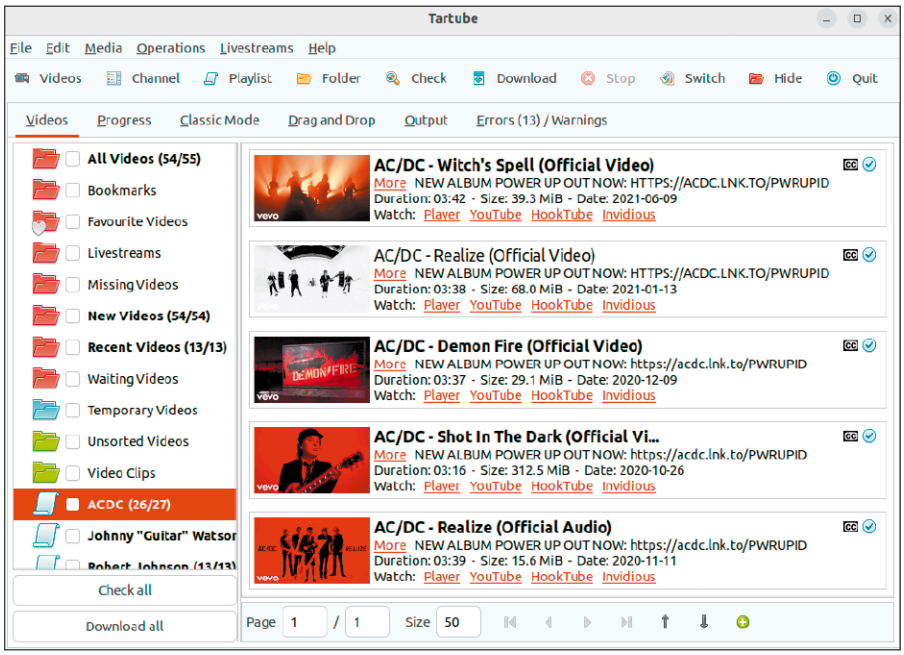
Es versteht sich von selbst, dass derart komplexe Befehlszeilen als Script- oder Alias-Vorlagen vorbereitet sein sollten.

3. Grafische Oberfläche für yt-dlp nutzen

Im Terminal bietet yt-dlp die höchstmögliche Flexibilität, bei täglicher Nutzung ist



Einfache Tartube-Oberfläche: Im „Classic Mode“ fügen Sie die gewünschte URL der Streamingseite ein und klicken auf „Download all“. Bei Bedarf lässt sich ein Speicherformat festlegen.



Übersichtliche Sammlung: In der Ansicht „Videos“ sortiert Tartube die Inhalte in eine Datenbank ein. Man sieht Vorschaubilder und Beschreibungen und startet über „Player“ die Wiedergabe.

eine grafische Oberfläche jedoch komfortabler. Tartube (*https://github.com/axcore/tartube*) ermöglicht einen vereinfachten Zugang zu yt-dlp, bietet aber bei Bedarf trotzdem zahlreiche Optionen. Unter „Releases“ laden Nutzer von Ubuntu oder Linux Mint die DEB-Datei herunter. Beim ersten Start nach der Installation meldet sich ein Assistent, über den Sie das Arbeitsverzeichnis konfigurieren und yt-dlp herunterladen.

Gehen Sie auf „Classic Mode“. Über die „+“-Schaltfläche geben Sie den Downloadordner an. Fügen Sie eine oder mehrere URLs der Videoseiten ein und klicken Sie auf „Add URLs“. Hinter „Format:“ können Sie das gewünschte Video- und Audioformat einstellen. Die Einstellung „Default“ lädt immer die beste Qualität herunter. Klicken Sie zum Abschluss auf „Download all“.

Wenn Sie Ihre Mediensammlung mit Tartube verwalten möchten, klicken Sie auf „Videos“, „Channels“ oder „Playlist“. Geben Sie jeweils die URL zum gewünschten Inhalt an. Vergeben Sie eine Bezeichnung, wenn danach gefragt wird, beispielsweise den Namen der Playlist.

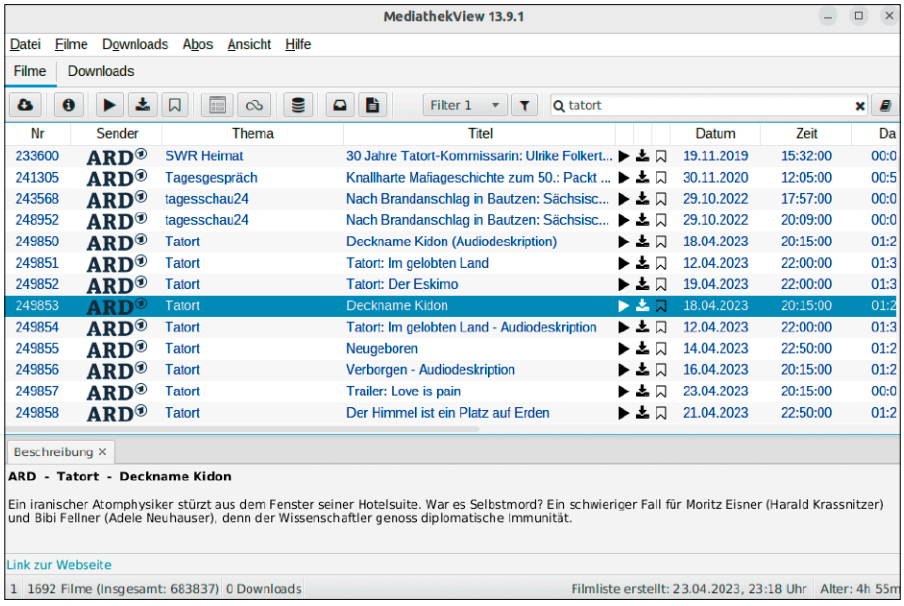
Unter „Videos“ taucht ein neuer Eintrag auf, vor den Sie ein Häkchen setzen. Klicken Sie auf „Download marked items“. Tartube speichert die Dateien im eingestellten Arbeitsverzeichnis, bei Playlists in Unterverzeichnissen.

Die Registerkarte „Videos“ zeigt alle Downloads inklusive Vorschaubildern und Beschreibungen an. Per Klick auf „Player“ lässt sich eine Datei im Standardplayer öffnen. Über „Edit → System preferences“ lassen sich unter „Options“ Downloadparameter festlegen oder neu erstellen. Die Einstellungen für „general“ gelten für den Bereich „Videos“ („Videos tab“). Per Klick auf „Use in Classic Mode tab“ kann man einen Optionssatz als Standard für den „Classic Mode“ erklären. Nach einem Klick auf „Edit“ lässt sich eine Vorgabe anpassen. Sie können beispielsweise unter „Formats“ das bevorzugte Videoformat einstellen oder unter „Convert“ die Umwandlung in ein anderes Format für Video- und Audiodateien. Im „Classic Mode“ kann man über die Schaltfläche auf der rechten Seite ein Menü öffnen, in dem „Set download options“ direkt zur Optionsauswahl führt. Im Fenster wird allerdings nicht angezeigt, welche Einstellungen gerade aktiviert sind.

4. Downloads mit Mediathekview

Inhalte aus den Mediatheken der öffentlich-rechtlichen Sender kann das Tool Mediathekview herunterladen (*https://mediathekview.de*). Im Downloadbereich finden Sie ein DEB-Installationspaket für Debian, Ubuntu oder Linux Mint und ein RPM-Paket für Red Hat, Open Suse oder verwandte System. Mediathekview benötigt eine Java-Laufzeitumgebung, die in den Downloads bereits enthalten ist und nicht getrennt installiert werden muss. Ein Appimage wird ebenfalls angeboten. Wenn Sie dieses ausführbar machen, lässt es sich direkt starten.

Mediathekview benötigt den VLC Player und ffmpeg zum Abspielen beziehungsweise Aufzeichnen. Richten Sie beide Programme vor dem ersten Start von Mediathekview ein. Die Appimage-Version arbeitet derzeit nicht mit einer eventuell vorhandenen Snap-Installation von VLC zusammen,



Alle Sendungen im Blick: Mediathekview ermöglicht eine bequeme Suche im Angebot der öffentlich-rechtlichen Mediatheken. Man kann sich die Inhalte ansehen und herunterladen.

auch wenn der Pfad in den Einstellungen unter „Set bearbeiten“ mit „/snap/bin/vlc“ korrekt konfiguriert ist. Bei der DEB-Installation dagegen kann man auch die Snap-Version verwenden. Im Terminal installieren Sie beide Pakete mit

```
sudo apt install vlc ffmpeg
```

Bei ersten Start fragt Mediathekview nach dem Standort. Sie geben beispielsweise „DE – Deutschland“ an und klicken auf „Mit Standardeinstellungen starten“. Das Programm lädt automatisch die aktuelle Filmdatenbank herunter. Danach tippen Sie einen Suchbegriff in das Eingabefeld auf der rechten Seite des Fensters ein, um den gewünschten Inhalt zu finden. Bei jedem Titel sehen Sie in der Zeile Symbole für „Film abspielen“ und „Film aufzeichnen“. Downloads landen standardmäßig unter „MediathekView“ im Home-Verzeichnis.

5. Bildschirmaufnahmen mit OBS Studio

Mit OBS Studio (*https://obsproject.com*) lässt sich der Bildschirm- oder Fensterinhalt zusammen mit der Audioausgabe aufzeichnen. Man kann damit alles mitschneiden, was auf dem Bildschirm zu sehen und aus dem Lautsprecher zu hören ist. Ein eventueller Kopierschutz ist daher nicht wirksam. Allerdings kann die Aufnahme nur in Echtzeit erfolgen, sie dauert also so lange wie der Film. In dieser Zeit kann man den Rechner nicht verwenden, Störungen durch Pop-ups oder Meldungen sollte man vermeiden, weil diese sonst ebenfalls im Video landen.

Sie können nur die Qualität beziehungsweise Auflösung aufzeichnen, mit der das Video auf dem Monitor dargestellt wird. Hohe Auflösungen erfordern einiges an CPU-Leistung, die ein aktueller Rechner jedoch bieten sollte. Andernfalls kommt es zu Rucklern und Aussetzern.

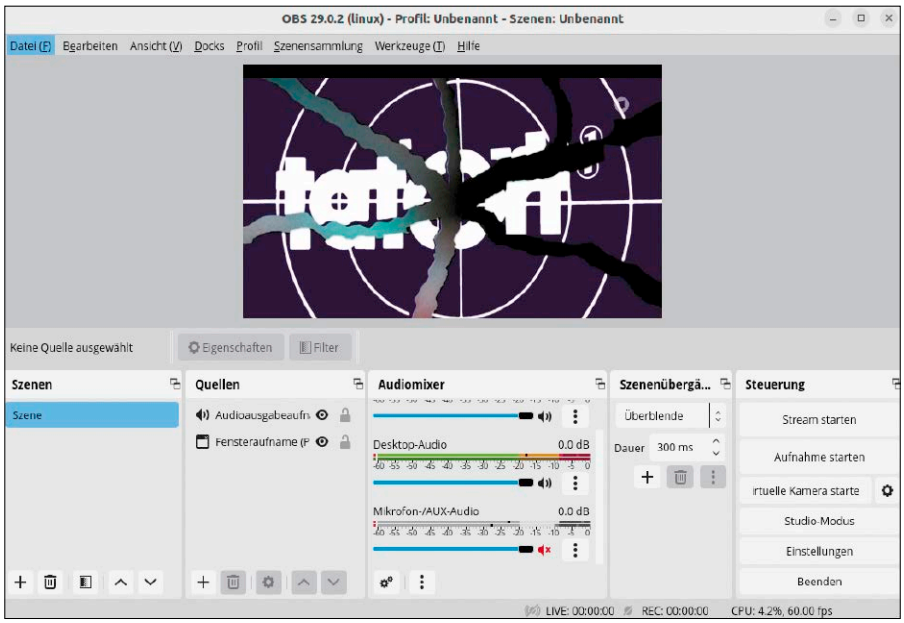
OBS Studio lässt sich als Flatpak mit

```
flatpak install flathub com.
  obsproject.Studio
```

installieren. Alternativ erfolgt die Einrichtung im Terminal über ein PPA (drei Zeilen):

```
sudo add-apt-repository
  ppa:obsproject/obs-studio
sudo apt update
sudo apt install ffmpeg obs-studio
```

Beim ersten Start wählen Sie die Option „Für das Aufnehmen optimieren, Streamen ist zweitrangig“. Bei den anderen Einstellungen belassen Sie die Vorgaben.



OBS Studio zeichnet alles auf, was der Monitor zeigt. Somit lassen sich beliebige Inhalte aller Onlineanbieter speichern, was allerdings nur in Echtzeit erfolgen kann.

OBS konfigurieren: Gehen Sie auf „Datei → Einstellungen“ und dann auf „Ausgabe“. Unter „Aufnahme“ geben Sie hinter „Aufnahmepfad“ ein Zielverzeichnis an, beispielsweise „Videos“ in Ihrem Home-Verzeichnis. „Aufnahmequalität“ und „Aufnahmeformat“ lassen Sie unverändert, außer es sind besondere Einstellungen für einen bestimmten Zweck erforderlich. Unter „Kodierer“ können Sie „Hardware (NVENC, H264)“ wählen, wenn ein Nvidia-Grafikchip im PC steckt und Sie den proprietären Nvida-Treiber installiert haben. Das sorgt für eine geringere CPU-Belastung.

Wechseln Sie dann zu „Video“ und stellen Sie dort die gewünschte Bildschirmauflösung ein. Sie können die Standardauflösung des Desktops verwenden oder eine geringere Auflösung wählen.

In der Rubrik „Hotkeys“ klicken Sie in das Feld hinter „Aufnahme starten“ und drücken die gewünschte Tastenkombination, beispielsweise Alt-F11. Für „Aufnahme beenden“ legen Sie dieselbe Tastenkombination fest.

Aufnahmen vorbereiten und starten: Wenn links unten unter „Szenen“ noch kein Eintrag vorhanden ist, klicken Sie auf die „+“-Schaltfläche und dann auf „OK“. Klicken Sie unter „Quellen“ auf die „+“-Schaltfläche, wählen Sie „Fensteraufnahme (PipeWire)“ und bestätigen Sie mit „Okay“. Es öffnet sich das Fenster „Bildschirmfreigabe“, in dem Sie das Fenster des Browsers wählen und auf „Freigeben“ klicken. Bestätigen Sie mit „Okay“. Alternativ können Sie „Fensteraufnahme (Xcomposite)“ verwenden. Probieren Sie beide Optionen aus und verwenden Sie dann diejenige, die auf Ihrem Rechner die besten Ergebnisse liefert. Fügen Sie „Audioausgabeaufnahme (PulseAudio“) zu den „Quellen“ hinzu und wählen Sie hinter „Gerät“ den Eintrag „Eingebautes Tongerät Analog Stereo“. Die genauen Bezeichnungen können abweichen, je nachdem, welche Hardware OBS erkannt hat.

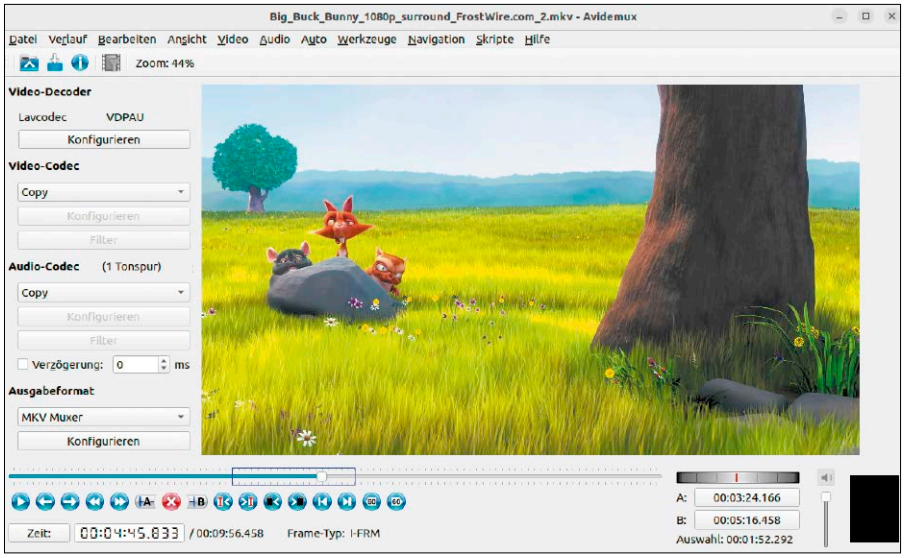
Sollte ein Mikrofon mit dem Rechner verbunden sein, klicken Sie unter „Mikrofon-/Aux-Audio“ auf das Lautsprechersymbol. Damit schalten Sie das Mikrofon stumm und vermeiden störende Nebengeräusche. Öffnen Sie im Browser die Seite mit dem gewünschten Video und stellen Sie die maximale Lautstärke ein. Danach starten Sie die Aufnahme in OBS über die zuvor festgelegte Tastenkombination. Wechseln Sie zum Browser, aktivieren Sie die Vollbildansicht und spielen Sie das Video ab. Ist das Video beendet, wechseln Sie wieder zu OBS und drücken die Tastenkombination erneut, um die Aufzeichnung zu beenden.

Bei dieser Methode lässt es sich nicht vermeiden, dass Einblendungen im Browserfenster wie Fortschrittsbalken und Bedienelemente am Anfang und Ende mit aufgezeichnet werden. Die unerwünschte Teile kann man später mit einem Videoeditor entfernen (siehe Seite 52).

Medien bearbeiten & konvertieren

Nicht immer liegen Audio- und Videodateien im gewünschten Format vor oder man möchte den Inhalt bearbeiten. Für Linux stehen Tools bereit, mit denen sich alle Aufgaben schnell und komfortabel erledigen lassen.

VON THORSTEN EGGELING



Avidemux: Das Programm ist einfach zu bedienen und eignet sich für den einfachen Videoschnitt. Über die Codeceinstellungen lässt sich bei Bedarf auch ein anderes Zielformat festlegen.

Audio- und Videodateien gibt es in unterschiedlichen Formaten. Für Musik sind beispielsweise MP3 (komprimiert) und Flac (verlustfrei komprimiert) verbreitet. Videodateien in den Formaten MKV und MP4 sind Container, in denen Video- und Audiostreams stecken. Die Streams können mit unterschiedlichen Verfahren komprimiert (encodiert) sein und – je nach Qualität – höhere oder niedrigere Auflösungen und Bitraten bieten. Der Unterschied zwischen den beiden Containern: MKV eignet sich für die Wiedergabe am PC, für das heimische Netzwerk und für eigene Streamingserver (siehe ab Seite 56). MP4 lässt sich auch über Webseiten streamen.

Die Umwandlung in ein anderes Format ist meist gewünscht, wenn ein bestimmtes Abspielgerät eine Datei nicht wiedergeben kann oder wenn man bei sehr großen Dateien Platz sparen möchte. Wer Videos bearbeiten will, etwa unerwünschte Passagen ausschneiden, kann das mit und ohne Umwandlung der Datei erledigen. Wir stellen einige Linux-Werkzeuge für die grafische Oberfläche vor, die Video- und Audiodateien bearbeiten und konvertieren. Im nachfolgenden Artikel ab Seite 54 zeigen wir, wie sich Dateien im Terminal oder per Script umwandeln lassen.

Avidemux: Videos schneiden/konvertieren

Mit Avidemux (*https://avidemux.sourceforge.net*) schneiden Sie Videodateien, speichern Audio- und Videostreams oder wandeln Dateien in andere Formate um. Mit dem Tool bearbeiten Sie auch Videos, die Sie mit OBS Studio (siehe ab Seite 48) aufgezeichnet haben, um unerwünschte Inhalte auf den Aufnahmen zu entfernen. Im Downloadbereich lässt sich Avidemux im Appimage-Format herunterladen. Nutzer von Ubuntu und Linux Mint können auch ein PPA verwenden.

Für die Installation aus dem PPA verwenden Sie im Terminal die folgenden drei Kommandos:

```
sudo add-apt-repository
  ppa:xtradeb/apps
sudo apt update
sudo apt install avidemux-qt
  avidemux-plugins-common avidemux-
  plugins-qt
```

Alternativ gibt es auch noch ein Flatpak-Paket:

```
sudo flatpak install flathub org.
  avidemux.Avidemux
```

Nach dem Start von Avidemux, gehen Sie auf „Datei → Öffnen“ und wählen die gewünschte Videodatei aus. Über die Bedienelemente am unteren Fensterrand spielen Sie das Video ab oder navigieren an eine bestimmte Position. Verwenden Sie die Pfeilschaltflächen für eine genaue Positionierung. Per Klick auf die „A“-Schaltfläche setzen Sie eine Anfangsmarkierung und über die „B“ eine Endmarkierung. Markieren Sie damit den Bereich, den Sie entfernen wollen, und gehen Sie im Menü auf „Bearbeiten → Löschen“. Sollte sich unerwünschtes Material nur vor und hinter dem Film befinden, setzen Sie die Markierungen an Anfang und Ende des Bereichs, der erhalten bleiben soll. Avidemux speichert nur den Bereich, der markiert ist.

Stellen Sie unter „Audio-Codec“ und „Video-Codec“ jeweils „Copy“ ein. Unter „Ausgabeformat“ wählen Sie „MKV Muxer“ oder „MP4 Muxer“. Mit Klick auf die Schaltfläche „Video speichern“ erstellen Sie eine neue

Videodatei ohne die überflüssigen Szenen. Avidemux arbeitet im Copymodus sehr schnell, weil das Tool die Streams nur in die Containerdatei kopieren muss.

Wenn Sie die Aufnahmen verkleinern wollen oder ein anderes Format benötigen, ist eine Neukodierung erforderlich. Die können Sie mit Avidemux erreichen, indem Sie unter den Video- und Audiocodecs das gewünschte Format wählen. Nach einem Klick auf „Konfigurieren" stellen Sie die Optionen für die Neucodierung ein. Avidemux bietet Beschleunigung über den Grafikchip, sofern Hardware und Treiber diese Funktion bereitstellen. Die Umwandlung lässt sich damit in der Tat deutlich beschleunigen. Wird eine Unterstützung erkannt, zeigt das Tool bei der Codecwahl beispielsweise „Nvidia H264" oder „Intel H264" an.

Videos mit Handbrake konvertieren

Handbrake (*https://handbrake.fr*) ist ein Videokonverter für die Zielformate MP4, MKV und Webm. Als Videoencoder stehen beispielsweise H.264 und H.265 zur Auswahl – sofern verfügbar auch mit Hardwarebeschleunigung. Handbrake lässt sich als Flatpak installieren:

```
sudo flatpak install flathub fr.
  handbrake.ghb
```

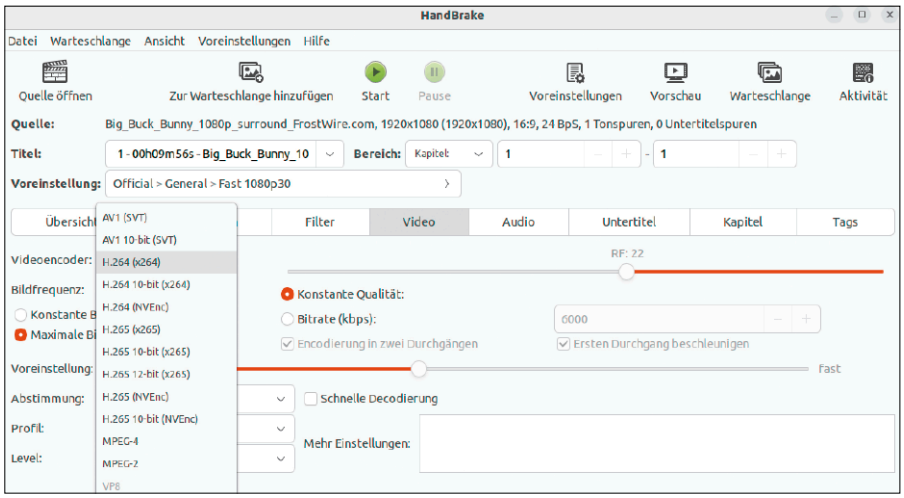
Die Hardwarebeschleunigung erfordert bei Intel GPUs ein zusätzliches Plug-in:

```
sudo flatpak install fr.handbrake.
  ghb.Plugin.IntelMediaSDK
```

In Handbrake wählen Sie nach einem Klick auf „Quelle öffnen" die gewünschte Videodatei. Klicken Sie auf „Voreinstellungen" und wählen Sie ein Zielformat. Über Schaltflächen wie „Dimensionen", „Video" oder „Audio" erreichen Sie die detaillierten Einstellungen. Unter „Video" können Sie beispielsweise den Videoencoder wechseln. Im unteren Bereich des Fensters tippen Sie den Dateinamen für die Zieldatei ein, hinter „In:" wählen Sie den Ordner. Klicken Sie auf „Start", um mit der Umwandlung zu beginnen.

Videos im Editor bearbeiten

Wer Videos schneiden, neu zusammensetzen oder mit Überblendungen versehen will, verwendet Videoeditoren wie Openshot (*www.openshot.org*) oder Shotcut (*https://shotcut.org*). Beide stehen als Appimage-Container zum Download bereit und gelten als einsteigerfreundlich. Der grundsätzliche



Der Videokonverter Handbrake erleichtert die Konfiguration über mitgelieferte Profile. Deren Einstellungen lassen sich individuell anpassen, wobei man die Wahl zwischen mehreren Codecs hat.

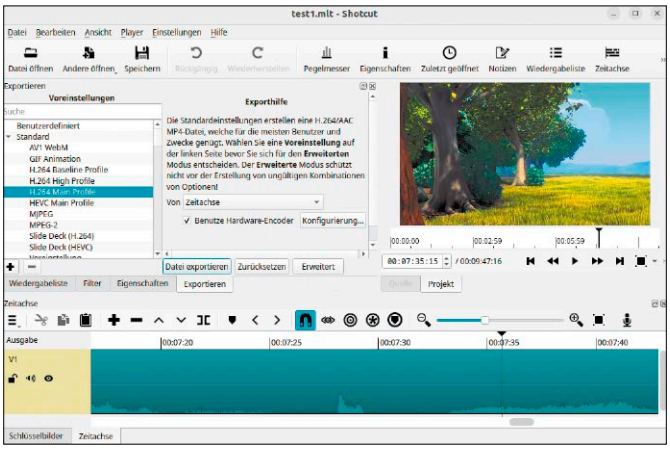
Ablauf ist bei beiden Programmen ähnlich: Zuerst fügt man Elemente wie Video- und Audiodateien oder Bilder der Wiedergabeliste beziehungsweise den Projektdateien hinzu. Danach werden die Elemente auf eine oder mehrere Zeitleisten gezogen und angeordnet. Nicht benötigte Bereiche kann man trennen und ausschneiden. Übergänge lassen sich erzeugen, indem man nebeneinander auf der Zeitleiste liegende Clips etwas übereinander zieht. In den Eigenschaften der Überblendung lässt sich einstellen, wie diese aussehen soll.

Zum Abschluss wird das Projekt als Videodatei exportiert. Openshot und Shotcut bieten mehrere Profile für unterschiedliche Container und Codecs. Hardwarebeschleunigung wird ebenfalls unterstützt.

Audio-CDs rippen & Audio konvertieren

Die Musik auf Audio-CDs ist bereits digitalisiert: Unter Linux sehen Sie im Ordner der CD WAV-Dateien wie „Track 1.wav" und „Track 2.wav", die Sie einfach über den Dateimanager kopieren. Für eine Musiksammlung sollten Sie den Dateien jedoch sprechende Namen geben und auch Metainformationen wie „Titel" „Album" und „Interpret" unterbringen. Ein Programm für diesen Zweck ist Asunder, das Sie bei Ubuntu und Linux Mint über den Paketmanager einrichten. Installieren Sie zusätzlich das Paket „lame", wenn Sie MP3-Dateien erstellen möchten.

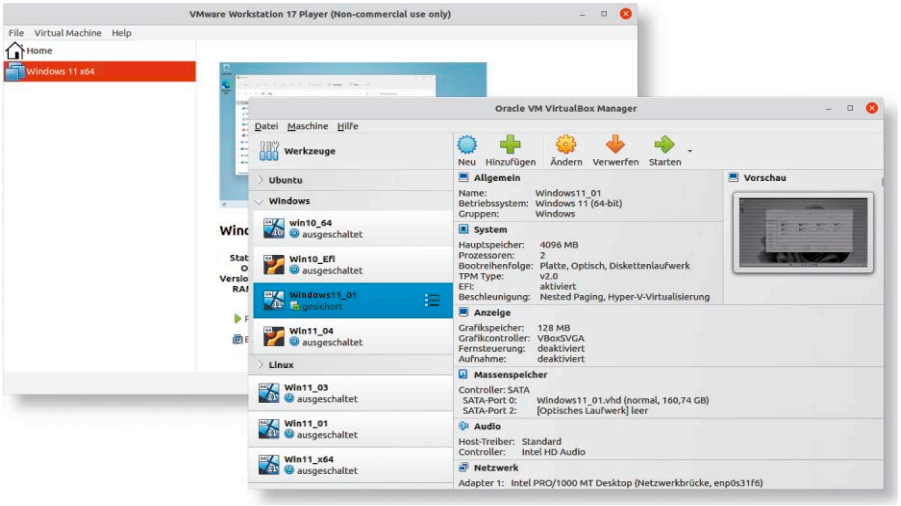
Für die Umwandlung von Audiodateien in ein anderes Format nutzen Sie den Soundconverter. Auch dieses Tool lässt sich als gleichnamiges Paket über den Paketmanager der Distribution beziehen. Klicken Sie im Programm auf das Zahnradsymbol und stellen Sie das gewünschte Zielformat ein. Fügen Sie nach einem Klick auf eines der zugehörigen Icons in der Symbolleiste einzelne Dateien oder Ordner hinzu und klicken Sie auf „Umwandeln". ■



Der Videoeditor Shotcut eignet sich auch für Einsteiger. Er bietet mehrere Zeitleisten sowie Überblendungen und Effekte. Für den Videoexport sind sinnvolle Profile vorgegeben.

Virtualbox gegen Vmware Player

Für Linux-Nutzer stehen mehrere Virtualisierungslösungen zur Verfügung. Wir vergleichen die Funktionen von Virtualbox und Vmware Workstation Player und geben eine Einschätzung der Leistungsfähigkeit.



Virtualbox und Vmware Player im Vergleich: Beide Virtualisierer lassen sich ähnlich bedienen und konfigurieren, Virtualbox bietet jedoch deutlich mehr Funktionen.

VON THORSTEN EGGELING

Virtualbox (*www.virtualbox.org*) steht unter einer Open-Source-Lizenz und ist damit kostenlos verfügbar. Vmware Workstation Player (*www.vmware.com*) ist nur bei privater Nutzung kostenlos. Beim Einsatz im Unternehmen sind circa 150 Euro fällig, außerdem gibt es eine funktionsreduzierte Version von Vmware Workstation Pro ab etwa 200 Euro. Mit beiden Produkten lassen sich virtuelle Maschinen (VMs) unter Linux erstellen und darin Windows- oder Linux-Systeme installieren und starten. Vmware Workstation Player bietet jedoch im Vergleich mit Virtualbox nur die wichtigsten Basisfunktionen.

Installation und erste Schritte

Download, Installation und Ersteinrichtung von Virtualbox beschreiben wir ab Seite 36. Für die Installation von Vmware Workstation Player gehen Sie auf *www.vmware.com/go/downloadplayer-de*, wählen die aktuelle Version 17.0 und klicken auf „Zu den Downloads“. Hinter „VMware Workstation 17.0.0 Player for Linux 64-bit“ klicken Sie auf „Jetzt herunterladen“. Starten Sie ein Terminal, wechseln Sie in das Downloadverzeichnis und starten Sie die heruntergeladene Datei beispielsweise mit

```
sudo sh Vmware-Player-Full-17.0.0
  -20800274.x86_64.bundle
```

Folgen Sie den Anweisungen des Installationsassistenten.

Neue VM erstellen: Beim Vmware Workstation Player sind nur wenige Eingaben erforderlich. Nach Klick auf „Create a New Virtual Machine“ fragt ein Assistent die nötigen Informationen ab. Man gibt eine ISO-Datei für die Linux- oder Windows-Installation an; der Player erkennt das System dann meist automatisch und setzt die passenden Optionen. Bei Windows 11 fordert der Assistent ein Passwort für die Verschlüsselung an, was für die TPM-Unterstützung erforderlich ist.

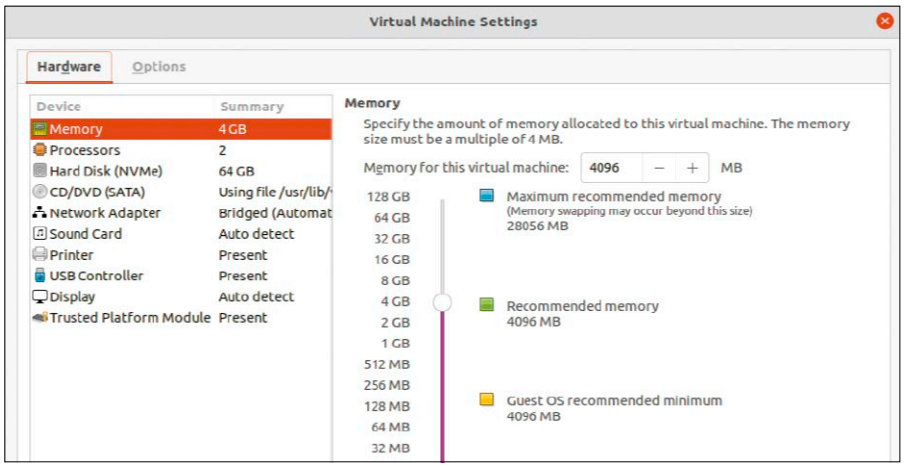
Bei Virtualbox ist der Ablauf ähnlich, der Assistent fragt jedoch mehr Einstellungen ab. Beim Erstellen einer neuen virtuellen Maschine können Sie beispielsweise auch die Größe des Hauptspeichers für das Gastsystem festlegen. Außerdem kann man den Typ der virtuellen Festplatte wählen und die unbeaufsichtigte Installation aktivieren (siehe Artikel ab Seite 34). Beides fehlt beim Player, weil er nur einen Typ virtueller Festplatten bietet und standardmäßig keine unbeaufsichtigte Installation unterstützt.

Leistung verbessern: Wie Virtualbox bietet auch Vmware Tools und Treiber für die Optimierung des Gastsystems an. Die Vmware-Tools verbessern die Grafikleistung und sind für den Datenaustausch über die Zwischenablage sowie für den direkten Zugriff auf Ordner des Hostsystems („Shared Folders“) erforderlich. Bei Gastsystemen wie Ubuntu oder Linux Mint ist keine zusätzliche Installation erforderlich, weil die Pakete „open-vm-tools“ und „open-vm-tools-desktop“ bereits vorinstalliert sind. Andernfalls hängt man das Medium mit den Vmware-Tools über „Virtual Machine → Install VMware Tools“ ein und führt die Installation durch.

Konfiguration von VMs

Bei Bedarf kann man bei Vmware Workstation Player die Einstellungen über „Virtual Machine → Virtual Machine Settings“ anpassen. Es sind ähnliche Grundeinstellungen wie bei Virtualbox verfügbar, beispielsweise für den im Gastsystem verfügbare Haupt-

speicher und die Anzahl der Prozessoren. Es fällt auf, das sich bei Vmware deutlich höhere Werte einstellen lassen: Für den Hauptspeicher bis zu 128 GB und bis zu 32 Prozessoren. Bei 128 GB Hauptspeicher für den Gast und realen 32 GB im Host-PC würde Vmware ständig Speicher auf die Festplatte auslagern müssen, was eine starke Verlangsamung bewirkt. Bei den Prozessorkernen kann man ohnehin nur so viele einstellen, wie das Hostsystem bietet. Mehr als zwei CPUs sind für Standardsoftware nicht erforderlich und bewirken auch keine Beschleunigung. Ein Vorteil gegenüber Virtualbox ergibt sich daher nicht.



VM im Player konfigurieren: Die Software bietet in den Einstellungen alle nötigen Optionen – aber auch nicht mehr. Die Vorgaben für das Gastsystem kann man in der Regel übernehmen.

Probleme bei der Konfiguration des Players

Die beim Player im Vergleich zu Vmware Workstation Pro reduzierten Optionen führen manchmal zu irreführenden Informationen. Ein Beispiel: Bei einem Host-PC mit 32 GB RAM und einer Auslagerungsdatei von nur zwei GB erscheint eine Fehlmeldung. Man soll die Auslagerungsdatei vergrößern oder in den „Preferences“ die Einstellung für den reservierten Speicher ändern. Die genannte Einstellung gibt es jedoch beim Player nicht. Das Problem lässt sich beheben, indem man in die Datei „/etc/vmware/config“ die Zeile

```
prefvmx.minVmMemPct = "100"
```

einträgt. Diese Lösung findet man erst nach intensiver Internetrecherche.

Ähnlich verhält es sich mit anderen fehlenden Einstellungen, obwohl der Player die Funktionen unterstützt, beispielsweise für Secure Boot oder Uefi-Firmware. Auch wenn nicht jeder Nutzer diese Einstellungen benötigt, ist der Weg über die Konfigurationsdateien umständlich – und das nur, weil Vmware den Player künstlich beschränkt hat. Bei Virtualbox sind alle relevanten Einstellungen über die grafische Oberfläche erreichbar.

Leistungsvergleich und Fazit

Die Ausführungsgeschwindigkeit ist in beiden Virtualisierern vergleichbar. Vmware Workstation Player liefert in einigen Bereichen etwas mehr Grafikleistung, etwa bei der 3D-Unterstützung. Die spielt nur bei Anwendungen eine Rolle, die Hardwarebeschleunigung über den Grafikchip nutzen, etwa bei Spielen. Dabei hilft auch, dass sich der virtuelle Grafikadapter mit acht GB RAM konfigurieren lässt. Der verfügbare Gastspeicher muss dafür 16 GB oder größer sein. Anspruchsvollere Spiele laufen aber auch mit diesen Einstellungen eher schlecht.

Als Vorteil von Vmware Workstation Player kann man die übersichtliche Konfiguration anführen – was aber für anspruchsvollere Nutzer zugleich der Nachteil ist. Sicherungspunkte, Klonen und Export von VMs oder der gleichzeitige Start mehrerer virtueller Maschinen fehlen (siehe Tabelle).

Es gibt wenig Grund, den Player statt Virtualbox zu verwenden. Einen weiteren Aspekt wollen wir nicht verschweigen: Vmware liefert hochpreisige Software für Unternehmen und hat einen hohen Qualitätsanspruch. Davon profitiert auch der Player. Bei Virtualbox arbeitet wahrscheinlich ein eher kleines Team an der Weiterentwicklung der Software. Mit häufigen Updates werden kleinere und größere Probleme zwar beseitigt, Nutzer müssen aber immer wieder mit ärgerlichen Fehlern rechnen. Allerdings sind in der Vergangenheit keine Probleme aufgetreten, die die Nutzung von Virtualbox verhindert oder ein Gastsystem zerstört hätten. ■

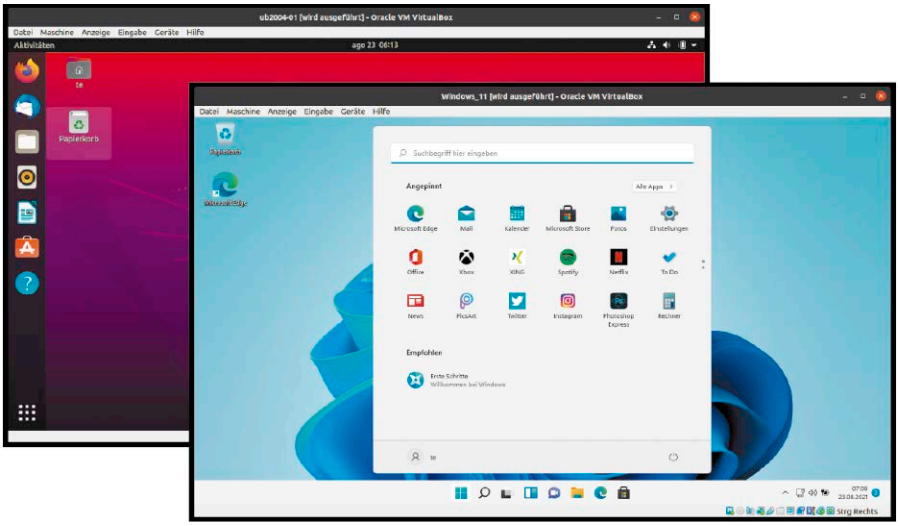
VIRTUALBOX VS. VMWARE PLAYER

	Oracle Virtualbox 7	Vmware Workstation Player 17
Hersteller-Website	*www.virtualbox.com*	*www.vmware.com*
Preis	kostenlos, größtenteils Open Source	ab 150 Euro, private Nutzung kostenlos
Funktionen	**Oracle Virtualbox 7**	**Vmware Workstation Player 17**
Anzahl der CPUs (maximal)	8	32
Drag & Drop (Host/Gast)	ja (teilweise)	ja
Fernzugriff (VNC)	ja	ja
Gemeinsame Ordner	ja	ja
Gemeinsame Zwischenablage	ja	ja
Maximaler Grafikspeicher	128 MB	8 GB
Maximaler Hauptspeicher	wie Host	128 GB
Mehrere Monitore	ja	ja
Mehrere VMs parallel	ja	nein
Open GL/DirectX	ja/ja	ja/ja
TPM/Secure Boot	ja/ja	ja/nein
USB 2.0/3.0 im Gastsystem	ja/ja	ja/ja
VM importieren/exportieren	ja/ja	ja/nein
VM-Klonfunktion	ja	nein
VM-Schnappschüsse	ja	nein
Vollbild/nahtloser Modus	ja/ja	ja/nein

Virtualisierung mit Virtualbox

Die vorausgehenden Seiten sollten zeigen, dass Virtualbox aus guten Gründen der beliebteste und funktionsreichste Virtualisierer unter Linux wie Windows ist. Wie Sie die Software praktisch nutzen, erklärt dieser Grundlagenbeitrag.

VON HERMANN APFELBÖCK



Oracle Virtualbox kann alles – und viel mehr, als dieser knappe Beitrag zeigen kann. Hier geht es nur um die Grundlagen – die Installation der Software, die Einrichtungsschritte für virtuelle Maschinen (VMs) und die allerwichtigsten Optimierungsmöglichkeiten.

1. Installation: Vollständig mit Erweiterungspaket

Die aktuelle Version (7.0.4) von Virtualbox erhalten Sie für alle Betriebssysteme unter *www.virtualbox.org/wiki/Downloads*. Zu den Varianten für die unterschiedlichen Linux-Distributionen führt dort der Link „Linux distributions“. Den Download installieren Sie dann nach Rechtsklick mit dem Paketmanager der Distribution, unter Windows durch Doppelklick des EXE-Programms. Anders als die Linux-Varianten bietet der Windows-Installer eine Selektion von Komponenten, wobei aber außer der Python-Unterstützung alle Optionen zu empfehlen sind.

Exkurs: Virtualbox ist selbstverständlich auch in den Paketquellen der Distributionen erhältlich. Dies aber in älteren Versionen 6.x, sodass der Vorteil einer automatischen Aktualisierung in diesem Fall keiner ist: Die Updates erstrecken sich nämlich nur auf die veraltete Hauptversionsnummer „6“. Eine weitere Installationsoption unter Linux wäre es noch, die Oracle-Paketquelle einzubinden und auf diesem Weg Updates für Version 7 zu erhalten. Dies führen wir hier nicht näher aus (siehe *www.virtualbox.org/wiki/Linux_Downloads*), da die Heft-DVD dafür eine Komplettlösung anbietet. Das dort vertretene Ubuntu 22.04.1 hat ein vorinstalliertes Virtualbox 7, das sich via Systemaktualisierung aktuell hält.

Erweiterungspaket: Auf der allgemeinen Downloadseite erscheint auch das „Oracle VM VirtualBox Extension Pack“. Dieses darf aus lizenzrechtlichen Gründen nicht mit dem freien Virtualbox ausgeliefert werden, ist aber für private Nutzung frei und kostenlos. Nach dem Download dieses Erweiterungspakets starten Sie Virtualbox und gehen im Virtualbox Manager auf „Werkzeuge“. Im mittleren Hauptfenster klicken Sie dann auf die Schaltfläche „Installieren“ und navigieren zum Download. Da der Dialog nur Dateien mit der Extension „.vbox-extpack“ anzeigt, ist die Auswahl einfach und eindeutig. Nach einem Warnhinweis startet die Installation. Das Erweiterungspaket ist zwar optional, aber für häufige Virtualbox-Nutzung uneingeschränkt zu empfehlen. Das frühere Hauptmotiv der USB-Unterstützung entfällt zwar, nachdem diese bereits im Basisprogramm vorliegt, aber das Erweiterungspaket bietet mit RDP-Fernsteuerung für Windows-VMs, Netboot und AES-Festplattenverschlüsselung nach wie vor nützliche Ergänzungen.

Gruppenzuweisung: Eine letzte Aktion vervollständigt die Installation unter Linux (unter Windows unnötig): Fügen Sie die Systembenutzer, die Virtualbox verwenden sollen, zur Gruppe „vboxusers“ hinzu:

```
sudo adduser [User] vboxusers
```

„[User]“ ersetzen Sie durch den Kontonamen des Benutzers. Wiederholen Sie den Befehl für alle gewünschten Konten. Melden Sie sich dann bei Linux ab und wieder an oder starten Sie das System neu. Diese vollständige Installation mit Erweiterung und Gruppenzuweisung ist für eine spora-

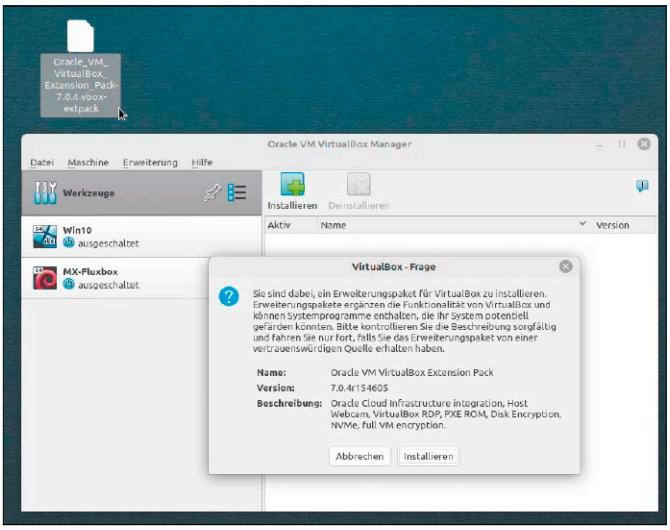
dische Nutzung von Virtualbox nicht zwingend, erspart aber eventuelle spätere Irritationen – insbesondere beim Versuch, USB-Geräte in einer VM zu nutzen.

2. Allgemeine Einstellungen

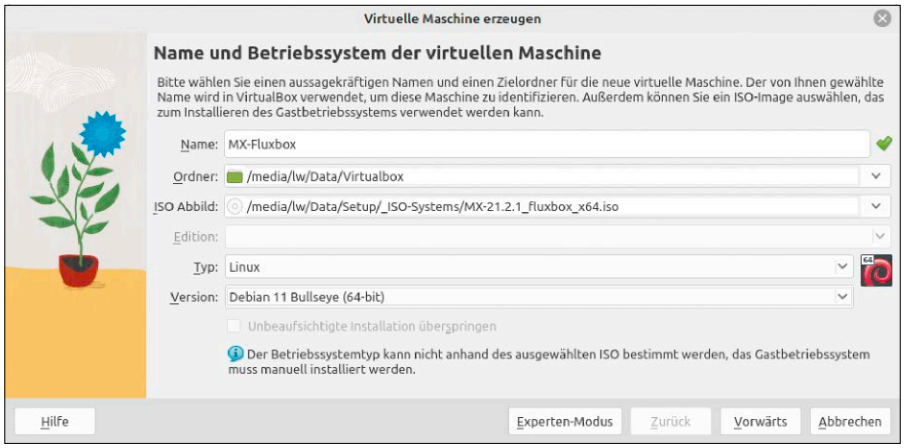
Der Start von Virtualbox am Desktop öffnet den „Oracle VM VirtualBox Manager" – zunächst nur mit dem Eintrag „Werkzeuge". Über eine grundsätzliche Einstellung können Sie vorab entscheiden, dies aber bei Bedarf auch später umstellen: Unter „Datei → Einstellungen → Allgemein" ist der Pfad vorgegeben, wo Virtualbox seine Dateien ablegen wird. Da dies viel Kapazität fordern wird, ist hier eventuell von vornherein ein Ort jenseits von „/home" besser geeignet.
Unter „Datei → Einstellungen → Eingabe → Virtuelle Maschine" lohnt sich in jedem Fall eine Durchsicht der Standard-Hotkeys. Den „Host"-Key mit Kombinationen wie Host-C, Host-L, Host-F, Host-Pos1 werden Sie ständig benötigen, um die VM-Darstellung (Vollbild; Skaliert, Fenster) zu ändern oder das VM-Fenstermenü zu aktivieren (Host-Pos1). Voreingestellter Host-Key ist die rechte Strg-Taste. Alle Hotkeys sind individuell einstellbar, auch der Host-Key.

3. Eine virtuelle Maschine einrichten

Mit der Schaltfläche „Neu" oder „Maschine → Neu" erstellen Sie eine VM. Den „Namen" vergeben Sie beliebig. Als „Ordner" ist voreingestellt, was unter „Datei → Einstellungen → Allgemein" als Standard gilt. Wichtig ist das „ISO Abbild", mit dem die Installation des neuen Systems erfolgt. Navigieren Sie hier über „Ändern" zum Installationsmedium des Systems. Dabei handelt es sich über die typischen Live- und Installer-Downloads für Linux-Distributionen oder um das Installations-ISO einer Windows-Version. Sobald dieses Medium eingetragen ist, erkennt Virtualbox automatisch „Typ" und „Version" dieses Systems. Falls nicht, wählen Sie „Typ" und „Version" manuell. Für Linux sind viele, aber nicht alle Distributionen aufgeführt. Nehmen Sie den Eintrag, der dem System am nächsten kommt, etwa „Ubuntu (64-bit)" für ein Linux Mint oder „Arch Linux (64 Bit)" für ein Endeavour-OS.
Wenngleich der Assistent die Hardwareeinstellungen von dieser Auswahl abhängig macht, ist diese Aktion – sofern überhaupt nötig – nicht kritisch, denn alle Voreinstellungen lassen sich durch manuelle Änderungen anpassen. Sie sollten aber für beste Kontrolle stets die Option „Unbeaufsichtigte Installation überspringen" anklicken.
Mit „Vorwärts" geht es zur RAM-Ausstattung und CPU-Vergabe für die VM. Vier GB und zwei CPU-Kerne sind für die meisten VMs ausreichend. Zum Teil genügt weniger. Die Einstellung hängt nicht zuletzt von der Hardware des Hostsystems ab und von der Frage, ob Virtualbox eventuell künftig sogar mehr als eine VM gleichzeitig mit Ressourcen versorgen soll. Kritisch sind auch diese Vorgaben nicht, da sie sich später – bei ausgeschalteter VM – jederzeit anpassen lassen.
Nach „Vorwärts" kommt der Punkt „Virtuelle Festplatte" mit drei Optionen. Im einfachsten Fall brauchen Sie überhaupt keine Festplatte („Keine Festplatte hinzufügen"), dann nämlich, wenn die VM nur ein Linux-Livesystem starten soll. Dann genügt das bereits vorher eingestellte ISO-Image. Soll das System hingegen ordentlich installiert werden, wählen Sie die oberste Option „Jetzt eine virtuelle Festplatte erstellen". Die Kapazität wählen Sie umso großzügiger, je länger die VM voraussichtlich laufen soll (Updates, Installationen). 30 bis 50 GB sind für Linux-Systeme realistisch, 50 bis 100 GB für Windows.
Wer sich hier nicht sicher ist, sollte die Option „Volle Größe erzeugen" immer inaktiv belassen (Standard) und damit eine dynamische virtuelle Festplatte erzeugen. Das hat zwei Vorteile – und einen Nachteil:
• Eine dynamische virtuelle Festplatte (VDI-Datei) fordert nur den aktuell nötigen Platz und wächst bis zum angegebenen Maximum. Sie belegt also eventuell nur 10 GB, obwohl 50 GB eingestellt sind.
• Eine dynamische VDI lässt sich später ohne Aufwand erweitern. Unter „Werkzeuge → Medien → Festplatten" gibt es einen Schieberegler wie bei der Ersteinrichtung.



Erweiterungspaket für Virtualbox: Das Zusatzpaket ist optional, bietet aber unter anderem den Zugriff auf USB 2.0/3.0. Am besten integrieren Sie es sofort nach der Virtualbox-Installation.



Anlegen einer neuen VM: Das „ISO-Abbild" mit dem Installationsmedium des gewünschten Systems ist in Virtualbox 7 eine erste und wichtigste Entscheidung.

Anlegen der Festplatte: Dynamische Festplatten belegen anfänglich wenig Platz, lassen sich später leicht vergrößern, sind aber langsamer als Laufwerke mit statischer Größe („Volle Größe“).

• Eine statische VDI („Volle Größe erzeugen“) ist im späteren Betrieb schneller.

Nach Abschluss des Schrittes „Virtuelle Festplatte“ und „Vorwärts“ ist die Definition der VM beendet und der grafische Assistent zeigt die Zusammenfassung.

Hinweis: Auf die dritte Option „vorhandene virtuelle Festplatte“ gehen wir später ein (Punkt 9).

4. Anpassungen der virtuellen Maschine

Die VM-Einrichtung via Virtualbox-Assistent führt in aller Regel zu einer sofort lauffähigen VM, lässt aber interessante Optionen außen vor. Es lohnt sich praktisch immer, vor dem ersten Start auf das Angebot „Ändern“ zu klicken und alle Optionen durchzugehen. Die Mehrzahl dieser Optionen setzt entweder das allgemeine Erweiterungspaket (Punkt 1) oder die Gasterweiterungen (Punkt 6) voraus:

Nicht optional, sondern unentbehrlich ist im Punkt „Anzeige“ ein hoher Wert für „Grafikspeicher“, am besten immer „128 MB“. Bei manchen Linux-Gastsystemen wählt Virtualbox den Wert so unterdimensioniert, dass die grafische Oberfläche nicht startet. Aktivieren Sie an dieser Stelle außerdem die Option „3D-Beschleunigung aktivieren“.

Unter „Allgemein → Erweitert“ können Sie durch die „Gemeinsame Zwischenablage“ und „bidirektional“ Inhalte zwischen Host- und Gastsystem über die Zwischenablage austauschen. Dies lohnt sich ebenfalls für „Drag’n’Drop“, um Dateien vom Dateimanager des Hostsystems in den Dateimanager des Gastsystems zu ziehen. Unter „USB“ sollte nicht nur der USB-Controller aktiviert sein, sondern auch die richtige USB-Version. Diese Angabe orientiert sich am Hostsystem und am USB-Port, wo Sie eventuelle USB-Datenträger voraussichtlich nutzen wollen.

5. Installation des virtuellen Systems

Nach dem Start der VM bootet diese über das virtuelle DVD-Laufwerk das Installationsmedium. Eventuell erwarten Sie von dieser VM gar nicht mehr als den Start eines typischen Linux-Livesystems und eine Installation entfällt somit. Wo dies zutrifft, sollte eine solche VM ausdrücklich „Live“ im Namen tragen (etwa „Knoppix-Live“), um es in der Virtualbox-Liste von installierten VMs zu unterscheiden.

In der Regel wird die VM aber eine virtuelle Festplatte enthalten, auf welche Sie nun das System ordentlich installieren. Der Vorgang unterscheidet sich in keiner Weise von einer normalen physischen Installation. Er ist allenfalls einfacher, weil nur eine (virtuelle) Festplatte vorhanden ist. Nach Abschluss der Installation und Herunterfahren der VM sollten Sie – wie nach jeder Installation – das Installations-ISO aus der VM-Konfiguration nehmen. Dies erledigen Sie über „Ändern“ im Virtualbox Manager. Entfernen Sie unter „Massenspeicher“ aber nicht das komplette DVD-Laufwerk, sondern nur das eingehängte ISO-Image. Das geht mit der Klickbox ganz rechts neben „Optisches Laufwerk“ und der Option „Entfernt das virtuelle Medium…“.

Das virtuelle DVD-Laufwerk selbst kann später noch anderweitig nützlich sein, insbesondere aber für die Installation der Gasterweiterungen.

6. Gasterweiterungen in die VM installieren

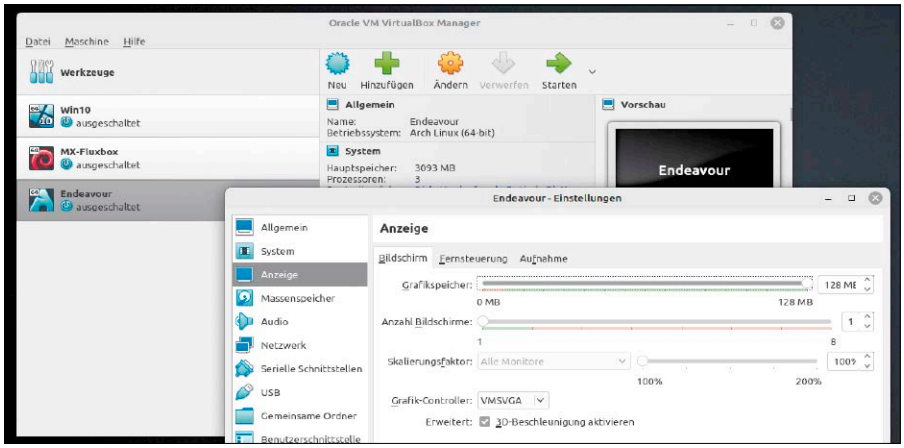
Im Unterschied zum allgemeinen Virtualbox-Erweiterungspaket werden die Gasterweiterungen in die jeweilige VM installiert. Gasterweiterungen sind optional, aber mindestens für häufiger genutzte VMs zu empfehlen. Sie enthalten Treiber für die Maus und den virtuellen Grafikadapter, verbessern damit Bildschirmauflösung, Skalierung, Mausverhalten und erlauben direkte Ordnerfreigaben zwischen Hostsystem und Gast-VM.

Die Gasterweiterungen lädt Virtualbox in das virtuelle DVD-Laufwerk einer laufenden VM, wenn Sie auf das VM-Fenstermenü „Geräte → Gasterweiterungen einlegen“ klicken. Falls die Menüleiste im Vollbild oder im skalierten Anzeigemodus nicht zugänglich ist, verwenden Sie den Hotkey Host-Pos1 (also standardmäßig Strg-Rechts-Pos1).

Das Installationspaket erscheint dann im DVD-Laufwerk der VM und in einer Windows-VM genügt dann der Doppelklick auf „VBoxWindowsAdditions.exe“. Unter Linux müssen Sie eventuell mit dem Terminal zum Pfad des DVD-Ordners navigieren und dann mit

```
sudo ./VboxLinuxAdditions.run
```

die Installation starten.



„Ändern“ der VM nach absolviertem Assistenten: Mindestens der Punkt „Anzeige“ verdient fast immer eine Korrektur beim „Grafikspeicher“.

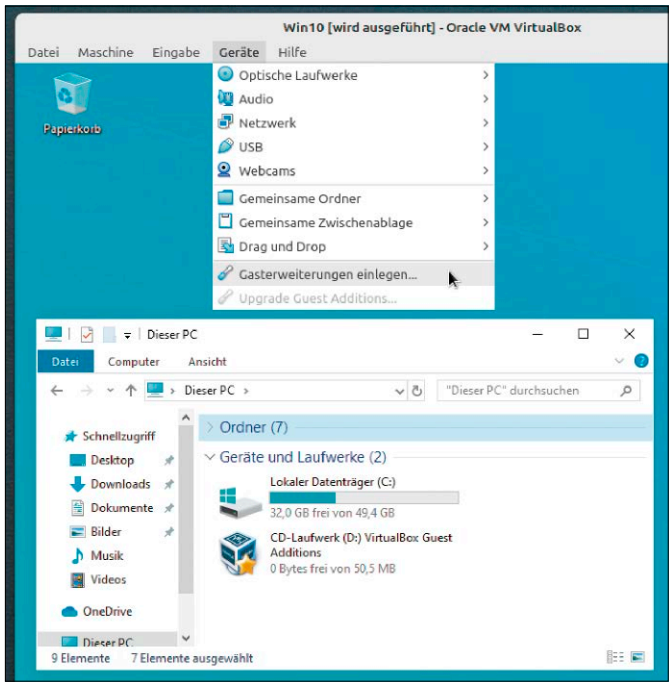
7. VM im Netzwerk: Netzwerkbrücke statt NAT

Standardmäßig gilt für VMs wie bei allen Virtualisierern der „NAT“-Modus im Netzwerk: Dabei dient Virtualbox selbst als virtueller Router und weist der VM eine zufällige IP-Adresse zu. Damit kommt die VM ins Internet, bleibt aber im lokalen Heimnetz isoliert. Es ist der VM zwar möglich, sich über die IP-Adressen des Heimnetzes mit Samba- oder SSH-Server zu verbinden, umgekehrt ist aber keine Verbindung zur VM möglich (SSH, Samba, VNC, RDP, Apache …). Wenn eine VM einen Dienst im Heimnetz anbieten soll, ist eine andere Einstellung erforderlich. Möglichkeiten gibt es mehrere, aber die einfachste erfordert nur einen einzigen Klick und sollte in den meisten Fällen genügen. Gehen Sie bei einer eingerichteten VM nach „Ändern“ auf das „Netzwerk“. Hier finden Sie unter „Netzwerk → Angeschlossen an“ eine Reihe weiterer Optionen. Mit „Netzwerkbrücke“ verbindet sich eine VM direkt mit dem Heimnetz. Die VM erhält also vom Heimrouter via DHCP eine lokale IP-Adresse genau wie ein physischer Rechner. Das macht die VM zum gleichberechtigten Mitglied des lokalen Netzes und sie kann dann von jedem anderen Gerät erreicht werden. Die Umstellung von „NAT“ zu „Netzwerkbrücke“ kann im Virtualbox Manager jederzeit und auch für eine aktuell laufende VM erfolgen.

8. Virtuelle Maschinen umziehen

Bei längerer Benutzung von Virtualbox summieren sich schnell einige VMs, die mit großen virtuellen Festplatten die Kapazität der Systempartition überfordern. Wenn alternative Datenträger zur Verfügung stehen, dann ist der Umzug von VMs kein Problem: Sie klicken einfach im Virtualbox Manager mit rechter Maustaste auf die betreffende VM und wählen dann „Verschieben“. Die Option ist nur aktiv, wenn die VM aktuell ausgeschaltet ist. Danach müssen Sie nur noch zum gewünschten neuen Zielordner navigieren. Virtualbox verschiebt dabei den Ordner mit dem Namen der VM inklusive Konfigurationsdatei (.vbox) und virtueller Festplatte (.vdi).

Wenn Sie ab einem bestimmten Zeitpunkt aus Platzgründen alle neu hinzukommenden VMs an einer anderen Stelle ablegen wollen, dann ändern Sie im Virtualbox Manager mit „Datei → Einstellungen → Allgemein“ den voreingestellten Standardpfad für die VMs. Die VMs aus dem bisherigen Standardpfad funktionieren weiterhin.



Optionale Gasterweiterungen (hier für Windows-VM): Über das Menü „Geräte“ lädt Virtualbox das Paket in das virtuelle DVD-Laufwerk. Von hier wird es dann in die VM installiert.

9. Virtuelle Festplatten von Vmware

Virtualbox kann die virtuellen Festplatten des Vmware Player (*.vmdk) direkt und ohne Konvertierung nutzen. Beim Erstellen einer VM wählen Sie beim Punkt „Virtuelle Festplatte“ die Option „Eine vorhandene virtuelle Festplatte verwenden“ und navigieren dann zur VMDK-Datei. Klicken Sie auf die erste, unbezifferte und kleinste dieser Dateien. Das ist der Verwaltungszeiger auf eventuell zahlreiche Inhaltsdateien einer dynamischen Festplatte. Die restliche Einrichtung der VM verläuft unverändert.

10. Virtualbox via Terminal

Virtualbox ist lückenlos – ohne grafischen Virtualbox Manager – über Terminalbefehle zu bedienen. Ein Motiv dafür werden Desktopnutzer angesichts der komfortablen Oberfläche zunächst nicht sehen. Im Netzwerk und mit SSH-Verbindung zum Hostsystem kann diese Option aber nützlich werden.

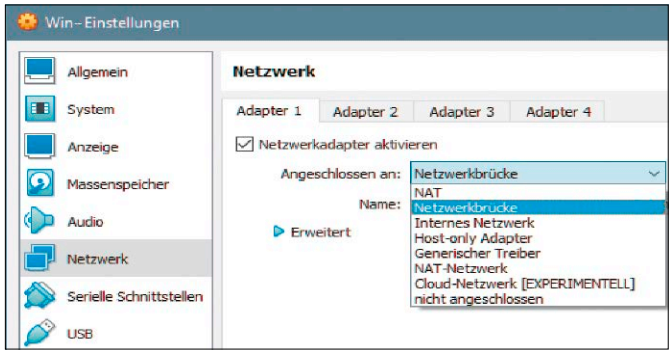
Dann ist nämlich nach SSH-Anmeldung am Hostsystem eine VM etwa mit

```
vboxmanage startvm "Cent-OS"
```

übers Netzwerk zu starten. Die auf dem Host vorhandenen VMs und deren genaue Namen kann der Befehl *vboxmanage list vms* ermitteln. Mit

```
vboxmanage controlvm "Cent-OS"
  poweroff
```

ist eine VM per SSH-Befehl auch wieder zu beenden. Für grafische VM-Desktops ist solche Fernbedienung kaum relevant, wohl aber für VMs, die im Netzwerk eine Serverfunktion erfüllen. Und auf dem lokalen Hostsystem kann die Terminalmethode nützlich sein, um eine VM per Autostart automatisch zu laden. ■

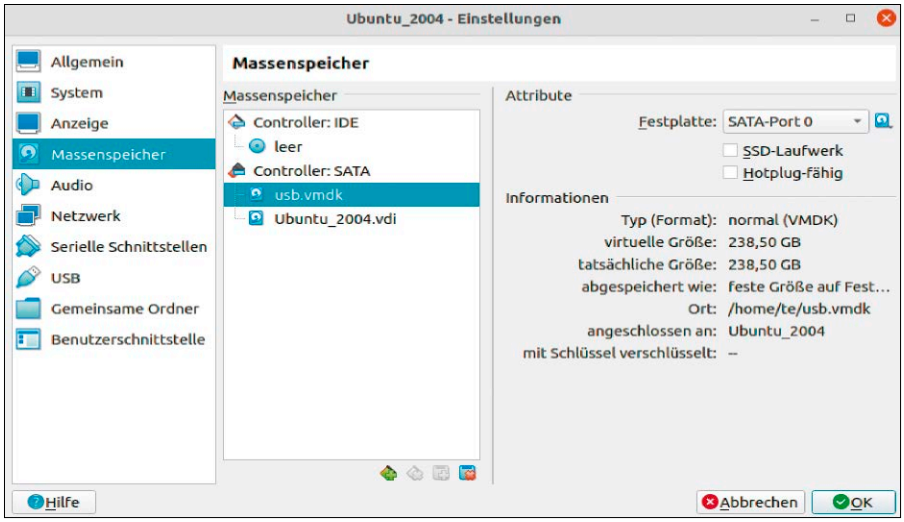


Wichtige Netzwerkeinstellung: Wenn die VM wie ein gleichberechtigter Rechner im lokalen Netz arbeiten soll (etwa als Server), hilft die Umstellung von „NAT“ auf „Netzwerkbrücke“.

Profitipps für Virtualbox

Ein Zweit-PC in Virtualbox funktioniert fast wie ein „echter“ Computer. Aber eben nur fast. Unsere Tipps helfen dabei, einige der Einschränkungen zu umgehen.

VON THORSTEN EGGELING



USB-Stick im Bios-Modus booten: Der Start des Systems gelingt über eine VMDK-Datei am „SATA-Port 0“. Deren Inhalt verweist direkt auf den USB-Stick am Host-PC.

Virtuelle Maschinen (VMs) arbeiten mit virtueller Hardware – und die hat nichts mit dem zu tun, was tatsächlich in Ihrem PC steckt. Eine Ausnahme sind einige USB-Geräte, beispielsweise USB-Laufwerke, von denen man mit den richtigen Einstellungen sogar booten kann. Auch im Netzwerk verhält sich eine VM mit Standardkonfiguration nicht wie andere PCs, was sich aber ebenfalls ändern lässt. Für den direkten Datenaustausch zwischen Host und Gast bietet Virtualbox alternativ spezielle Funktionen an.

System vom USB-Stick booten

In VMs mit aktiviertem Uefi binden Sie ein USB-Gerät über die Einstellungen ein. Gehen Sie dort auf „USB“ und wählen Sie den USB-Stick über die Schaltfläche mit dem grünen Plussymbol aus. Die Option „USB-3.0-Controller (xHCI)“ muss aktiviert sein, wenn der Stick mit einem USB-3.0-Port verbunden ist. Starten Sie die VM und setzen Sie den USB-Stick in der Bootreihenfolge an die erste Stelle, entsprechend der Beschreibung im nächsten Tipp. Danach lässt sich das System vom USB-Stick im Uefi-Modus booten.

Bios-Modus: Der USB-Stick muss als physisches Laufwerk in die VM eingebunden werden. Dafür sind erhöhte Zugriffsrechte erforderlich, die Sie als Mitglied der Gruppe „disk“ erhalten:

```
sudo usermod -a G disk [User]
```

Den Platzhalter „[User]“ ersetzen Sie durch Ihren Benutzernamen. Melden Sie sich bei Linux ab und wieder an. Ermitteln Sie den Gerätepfad des Sticks im Terminal:

```
lsblk -p
```

Wenn in der Ausgabe beispielsweise „/dev/sdf“ für den USB-Stick auftaucht, hängen Sie das Gerät mit

```
sudo umount /dev/sdf?
```

aus. Danach verwenden Sie diesen Befehl (eine Zeile):

```
vboxmanage createmedium disk
  --filename ~/usb.vmdk
  --format=VMDK --variant RawDisk
  --property RawDrive=/dev/sdf
```

In den Einstellungen einer virtuellen Maschine gehen Sie auf „Massenspeicher“, klicken auf „Controller SATA“ und dann auf das Icon ganz rechts daneben („Festplatte hinzufügen“). Wählen Sie „usb.vmdk“ und klicken Sie auf „Auswählen“. Legen Sie die Reihenfolge hinter „Festplatte“ fest. „usb.vmdk“ muss mit „SATA-Port 0“ verbunden sein, die Systemfestplatte mit dem nächsten freien Port. Wenn Sie den virtuellen PC starten, bootet er vom USB-Laufwerk. Wird der Stick vom PC entfernt, müssen Sie „usb.vmdk“ wieder aus der Konfiguration löschen. Das System startet sonst nicht.

Bios/Uefi-Firmwaresetup aufrufen

Eine neu erstellte VM bootet von der ISO-Installationsdatei und das System lässt sich dann auf der bisher leeren virtuellen Festplatte installieren. Da im Uefi-Modus die nun bootfähige Festplatte in der Bootreihenfolge an erste Stelle steht, ist es nicht mehr möglich, ein System aus der ISO-Datei zu booten, etwa für eine Windows-Reparatur.

Die Bootreihenfolge lässt sich aber in der Uefi-Firmware der VM ändern. Dazu klickt man beim Start der VM möglichst schnell in das Fenster und drückt mehrfach die Esc-Taste. Der richtige Zeitpunkt ist allerdings schwer abzupassen – einfacher geht der Start in die Uefi-Firmware im Windows-Gastsystem mit

```
shutdown -r -fw -t 0
```

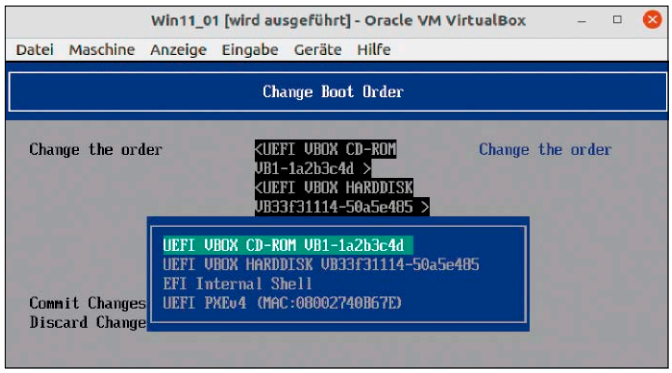
in einer Eingabeaufforderung mit Administratorrecht. Bei Linux-Systemen kommt

```
sudo systemctl reboot --firmware-
  setup
```

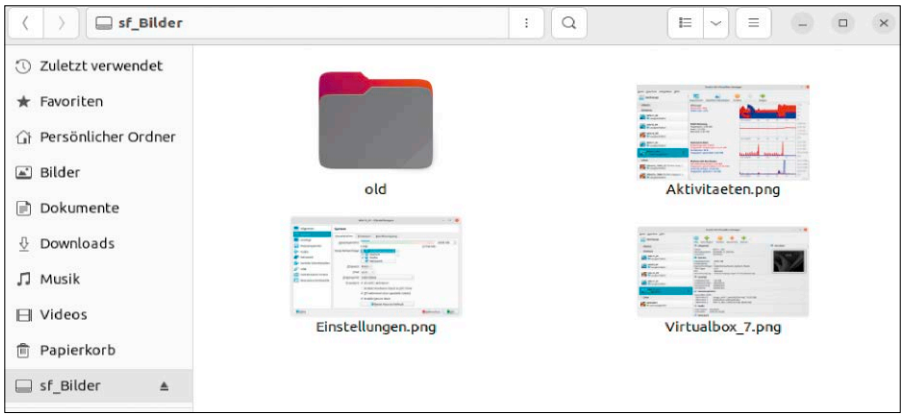
zum Einsatz.

Im Firmwaresetup navigiert man über „Boot Maintenance Manager“ zu „Boot Options → Change Boot Order“ und drückt die Eingabetaste. Mit den Tasten „+“ und „-“ lässt sich die Reihenfolge ändern und „UEFI VBOX CD-ROM“ an die erste Position schieben. Will man auch vom USB-Stick booten, setzt man diesen an die zweite Stelle. Bestätigen Sie mit der Eingabetaste und danach mit „Commit Changes and Exit“. Mit zweimal Esc gelangen Sie zurück ins Hauptmenü, in dem Sie „Continue“ wählen. Die VM bootet jetzt von der konfigurierten ISO-Datei.

Bios-Modus: Die Bootreihenfolge lässt sich in den Einstellungen einer VM unter „System“ festlegen. Standardmäßig befindet sich das virtuelle CD/DVD-Laufwerk in der Reihenfolge vor der Festplatte, was sich auch nicht automatisch ändert. USB-Laufwerke werden in den Einstellungen nicht berücksichtigt (siehe vorheriger Tipp). Beim Start einer VM kann man das Bootgerät über die Taste F12 temporär wählen.



Uefi-Bootreihenfolge: Von welchem Laufwerk eine VM bootet, stellen Sie im Firmwaresetup ein. Es lässt sich mit der Esc-Taste beim Start der virtuellen Maschine aufrufen.



Zugriff auf den Host-PC: „Gemeinsame Ordner“ sind eine Alternative zu Netzwerkfreigaben. Unter Linux – im Beispiel „sf_Bilder“ – ist der Ordner direkt im Dateimanager zu sehen.

Datenaustausch zwischen VM und Host

Standardmäßig konfiguriert Virtualbox den Netzwerkadapter für „NAT“. Die VM kann mit dieser Einstellung die Internetverbindung nutzen, erhält aber keinen Zugriff auf das lokale Netzwerk. Das lässt sich ändern, indem man den Netzwerkadapter als „Netzwerkbrücke“ konfiguriert. Schadsoftware in der VM kann dann allerdings ungeschützte Dateifreigaben infizieren. Die Verwendung der Alternative „Gemeinsamer Ordner“ gilt als sicherer, weil nur genau dieser Ordner betroffen sein kann. Voraussetzung dafür sind die installierten Gasterweiterungen (siehe Artikel ab Seite 36).

Gehen Sie im Fenster der laufenden VM auf „Geräte → Gemeinsame Ordner → Gemeinsame Ordner“. Über die „+“-Schaltfläche bestimmen Sie einen Ordner auf dem Host-PC für den Datenaustausch. Setzen Sie ein Häkchen vor „Automatisch einbinden“. Damit ein Nutzer auf den gemeinsamen Ordner zugreifen darf, fügen Sie ihn im Gastsystem zur Gruppe „vboxsf“ hinzu:

```
sudo usermod -aG vboxsf [User]
```

„[User]“ ersetzen Sie durch den gewünschten Benutzernamen. Starten Sie das Gastsystem neu. Den gemeinsamen Ordner finden Sie unter Linux im Navigationsbereich des Dateimanagers mit dem Präfix „sf_“. Unter Windows erreichen Sie den Ordner im Windows-Explorer über „Netzwerk“ und „Vboxsrv“.

Virtualbox bietet über „Maschine → Dateimanager“ im Fenster einer VM eine weitere Methode für den Datenaustausch. Geben Sie rechts unten Benutzernamen und Passwort für die Anmeldung im Gastsystem ein und klicken Sie auf „Sitzung öffnen“. Die Dateisysteme von Host- und Gast-PC werden nebeneinander angezeigt. Über die Schaltflächen in der Mitte lassen sich markierte Elemente übertragen.

Virtuelle Maschinen automatisch starten

Der Autostart ist bei VMs wünschenswert, in denen Serverdienste laufen. Die Dienste stehen dann im Netzwerk zur Verfügung, ohne dass der Benutzer eingreifen oder sich anmelden muss. Einen Systemd-Dienst mit dem Namen „vboxautostart-service“ richtet Virtualbox bei der Installation ein. Zur Konfiguration tragen Sie in die Datei „/etc/default/virtualbox“ diese zwei Zeilen ein:

```
VBOXAUTOSTART_DB=/etc/vbox
VBOXAUTOSTART_CONFIG=/etc/vbox/
  vboxauto.conf
```

Erstellen Sie die Datei „/etc/vbox/vboxauto.conf“ mit diesem Inhalt (zwei Zeilen):

```
default_policy = deny
[User] = {allow = true}
```

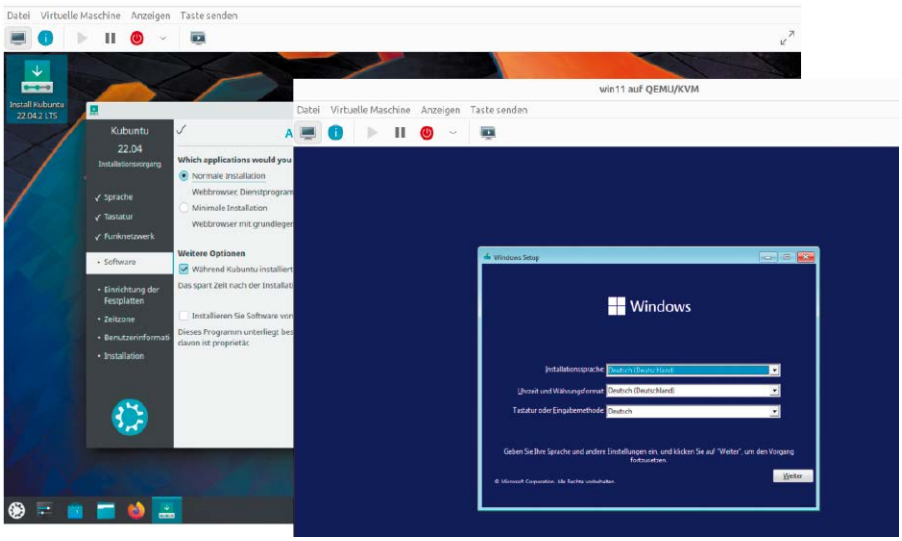
Den Platzhalter „[User]“ ersetzen Sie durch Ihren Benutzernamen. Danach führen Sie die folgenden vier Befehle aus:

```
sudo chgrp vboxusers /etc/vbox
sudo chmod 1775 /etc/vbox
VBoxManage setproperty
  autostartdbpath /etc/vbox
VBoxManage modifyvm "[VM]"
  --autostart-enabled on
  --autostop-type savestate
```

Für den Platzhalter „[VM]“ setzen Sie den Namen der virtuellen Maschine ein, die automatisch starten soll. Der Netzwerkadapter der VM muss als „Netzwerkbrücke“ konfiguriert sein, damit Serverdienste im lokalen Netzwerk erreichbar sind. Starten Sie Linux neu. Die virtuelle Maschine startet dann automatisch und deren Serverdienste sind im Netz verfügbar. ■

Virtualisierung mit KVM

Die Kernel-based Virtual Machine (KVM) bietet unter Linux eine leistungsfähige Virtualisierungslösung. Die Einrichtung einer Windows-VM ist komplexer als etwa bei Virtualbox, aber dennoch lohnend.



VON THORSTEN EGGELING

Virtualisierungslösungen benötigen Verwaltungssoftware sowie Kernel-Module für den Zugriff auf die Hardware. Unter Linux ist mit der Kernel-based Virtual Machine (KVM) die Grundlage bereits vorhanden, zusätzliche Software lässt sich über die Standard-Paketquellen installieren. KVM-Virtualisierung bietet eine sehr gute Leistung für Linux- und Windows-Gastsysteme. Im Vergleich mit anderen Virtualisierungslösungen wie Virtualbox oder Vmware Workstation ist KVM mindestens gleichwertig, teilweise überlegen. Die zugehörigen Verwaltungswerkzeuge sind allerdings nicht immer so intuitiv bedienbar, wie es Virtualbox-Nutzer vielleicht gewohnt sind, außerdem gilt es, einige Mängel zu umgehen. Unsere Tipps helfen bei der erfolgreichen Einrichtung virtueller Maschinen und deren Konfiguration.

Voraussetzungen für KVM-Virtualisierung

Für KVM muss die CPU die Virtualisierungserweiterungen von Intel (Intel VT-x) oder AMD (AMD-V) unterstützen. Die Technik ist bereits seit 2006 in allen Prozessoren zu finden, manchmal aber in der Firmware nicht aktiviert. Genauen Aufschluss über die Fähigkeiten der CPU liefert unter Linux folgender Befehl in einem Terminal:

```
egrep -c '(svm|vmx)' /proc/cpuinfo
```

Der Befehl filtert die Ausgabe von „/proc/cpuinfo“ nach den Begriffen „svm“ (AMD) oder „vmx“ (Intel). Ist das Ergebnis größer „0“, dann unterstützt der Prozessor diese Virtualisierungsfunktionen. Die Zeile

```
cat /proc/cpuinfo
```

gibt die komplette Liste aller CPU-Eigenschaften aus. „vmx“ ist pro CPU-Kern jeweils hinter „flags“ und „vmx flags“ zu sehen.

Ist das Ergebnis „0“, sehen Sie im Bios/Firmwaresetup nach, ob sich AMD-V oder Intel-VT („vt-x“, „Intel Virtualization Technologie“) dort aktivieren lässt. Manchmal gibt es auch Optionen für „AMD-Vi“ beziehungsweise bei Intel „Vt-d“. Wenn vorhanden, aktivieren Sie diese ebenfalls. Dahinter verbirgt sich die I/O-Virtualisierung („Input/Output“), über die sich der Datenaustausch mit Netzwerkadaptern, Grafikchips und Festplattencontrollern beschleunigen lässt.

Weitere Voraussetzungen: Ein Zweitsystem in einer virtuellen Maschine benötigt RAM und Prozessorzeit. Je nach Konfiguration sind zwischen zwei und acht GB erforderlich. Der Rechner sollte daher über genügend RAM verfügen, eine schnelle Multicore-CPU ist ebenfalls wünschenswert. Virtuelle Maschinen laufen zwar auch mit schlechterer Hardwareausstattung, dann allerdings oft nicht mit befriedigender Geschwindigkeit.

```
te@Z77X:~
fpu_exception   : yes
cpuid level     : 22
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge m
ca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscal
l nx pdpe1gb rdtscp lm constant_tsc art arch_perfmon pebs bts rep_good n
opl xtopology nonstop_tsc cpuid aperfmperf pni pclmulqdq dtes64 monitor
ds_cpl vmx smx est tm2 ssse3 sdbg fma cx16 xtpr pdcm pcid sse4_1 sse4_2
x2apic movbe popcnt tsc_deadline_timer aes xsave avx f16c rdrand lahf_lm
 abm 3dnowprefetch cpuid_fault invpcid_single pti ssbd ibrs ibpb stibp t
pr_shadow vnmi flexpriority ept vpid ept_ad fsgsbase tsc_adjust bmi1 avx
2 smep bmi2 erms invpcid mpx rdseed adx smap clflushopt intel_pt xsaveop
t xsavec xgetbv1 xsaves dtherm ida arat pln pts hwp hwp_notify hwp_act_w
indow hwp_epp md_clear flush_l1d arch_capabilities
vmx flags       : vnmi preemption_timer invvpid ept_x_only ept_ad ept_1g
b flexpriority tsc_offset vtpr mtf vapic ept vpid unrestricted_guest ple
```

CPU-Funktionen prüfen: „cat /proc/cpuinfo“ zeigt mit „vmx“ im Terminal an, ob der Prozessor die Hardwareunterstützung für Virtualisierung bereits unterstützt.

Unterstützung aktivieren: Im Firmwaresetup muss bei Intel-CPUs „Intel Virtualization Technologie“ (oder ähnlich) aktiviert sein, damit die KVM-Virtualisierung funktioniert.

Software für KVM installieren

Die Infrastruktur der KVM-Virtualisierung besteht aus mehreren Programmen und Bibliotheken. Für die Installation unter Ubuntu 22.04 oder Linux Mint 21.x genügt im Terminal die Zeile

```
sudo apt install virt-manager
```

Die zusätzlich erforderlichen Pakete werden automatisch installiert. Das Programm Virtual Machine Manager (VMM) aus dem Paket „virt-manager“ stellt die Benutzeroberfläche zum Erstellen und Verwalten von virtuellen Maschinen bereit. In einem deutschsprachigen Ubuntu oder Linux Mint findet man ihn unter der Bezeichnung „Virtuelle Maschinenverwaltung“.

Um die KVM-Virtualisierung verwenden zu können, müssen Benutzerkonten zur Gruppe „libvirt“ gehören. Der aktuell angemeldete Benutzer wird automatisch zur Gruppe hinzugefügt. Weitere Benutzer fügen Sie mit

```
sudo usermod -aG libvirt [User]
```

hinzu. Setzen Sie den Benutzernamen für den Platzhalter „[User]“ ein. Starten Sie Linux neu, damit die Änderungen in der Konfiguration wirksam werden.

Vorbereitungen für eine Windows-Installation

Für die Windows-Installation als Gastsystem in einer virtuellen Maschine (VM) benötigen Sie die ISO-Datei des Installationsmediums. Sie können Windows 10 (*https://bit.ly/w10is*) oder 11 (*https://bit.ly/w11is*) herunterladen. Wenn Sie Windows nur ausprobieren möchten, spielen Version und Edition keine Rolle. Ein Produktschlüssel ist für die Installation nicht erforderlich, ohne Aktivierung lassen sich allerdings einige Einstellungen nicht anpassen, beispielsweise unter „Personalisierung“. Wer die Windows-VM dauerhaft nutzen möchte, muss für die VM einen eigenen Produktschlüssel erwerben.

Eine Alternative ist die Installation von Windows 10 Enterprise (*https://bit.ly/w10ent*), das sich 90 Tage lang ohne Einschränkungen ausprobieren lässt. Windows 11 Enterprise ist für Tests nicht geeignet, weil für die Installation eine registrierte E-Mail-Adresse nötig ist, die zur Nutzung berechtigt.

Zurzeit zeigt die Windows-10-Installation (alle Versionen) in der VM einen gravierenden Fehler. Der Treiber für den Netzwerkadapter wird nicht geladen (Chipsatz „pc-q35-6.2“, Libvirt 8.0.0.1). Der Zugriff auf das Internet ist somit nicht möglich und damit auch keine Windows-Updates. Das Problem betrifft nur die deutschsprachige Ausgabe. Wer Windows 10 benötigt, lädt daher besser die englischsprachige Version herunter und richtet nach der Installation „Deutsch“ in den „Einstellungen“ unter „Zeit und Sprache → Sprache“ ein. Die Ursache des Problems ist bisher nicht bekannt.

Windows 11 ist von dem Problem nicht betroffen und lässt sich ohne Auffälligkeiten installieren. Da die KVM-Virtualisierung einen emulierten TPM-Chip, Uefi und Secure Boot unterstützt, sind alle Hardwarevoraussetzungen für Windows 11 erfüllt.

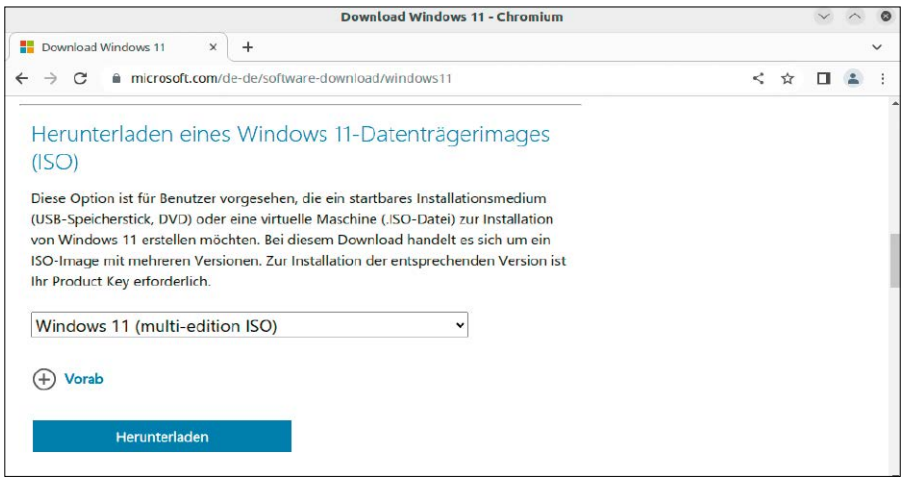
Es gibt aber einen Nachteil: Bei aktiviertem Uefi kann man keine Schnappschüsse als schnelle Sicherung des Systems erstellen. Wer diese praktische Funktion verwenden will, muss Windows 11 im Bios-Modus einrichten. Das funktioniert jedoch standardmäßig nicht und Windows 11 verweigert die Installation. Das Problem lässt sich mit einem angepassten Setupmedium beheben, mit dem sich auch eine automatische Installation durchführen lässt. Unter *https://bit.ly/W11BPA* finden Sie ein Bash-Script, das eine ISO-Datei mit der nötigen Antwortdatei erstellt. Laden Sie die drei Dateien aus dem Ordner „Linux“ herunter. Installieren Sie dann weitere nötige Pakete:

```
sudo apt install p7zip-full
  genisoimage
```

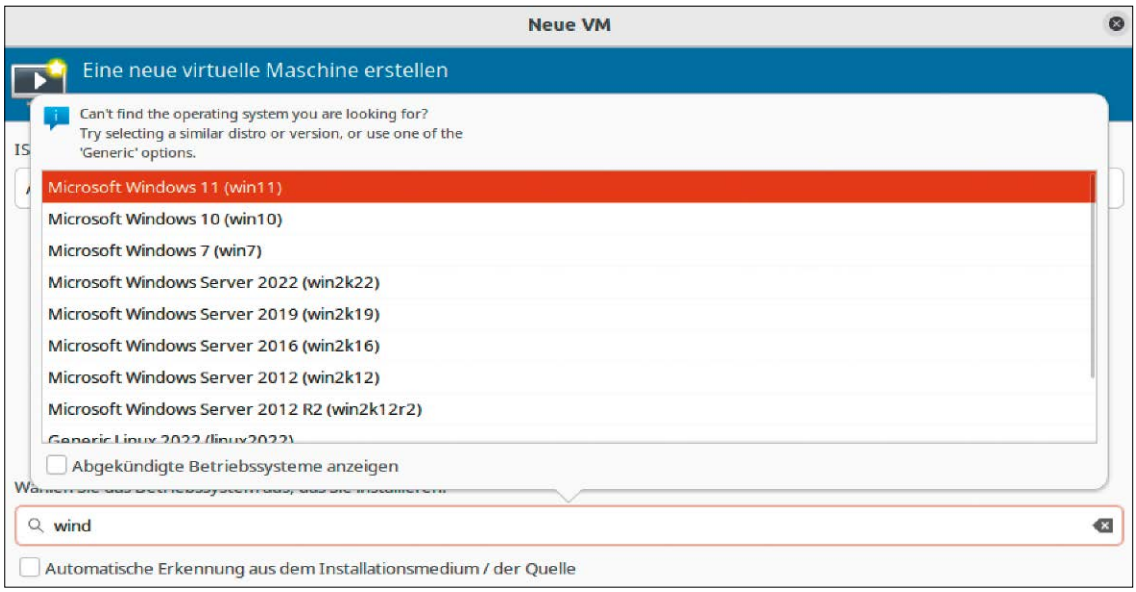
Öffnen Sie die Datei „unattend_x64.xml“ in einem Editor und passen Sie den Benutzernamen an (siehe Kommentare in der Datei). Die XML-Datei enthält außerdem Anweisungen, mit denen sich alle Hardwarebeschränkungen von Windows 11 umgehen lassen. Starten Sie dann das Script im Downloadordner:

```
sh mk_Win11_bypass.sh [ISO-Datei]
```

Für den Platzhalter setzen Sie Pfad und Na-



Windows herunterladen: Windows 10 und 11 bietet Microsoft als ISO-Datei zum kostenlosen Download an. Ohne Produktschlüssel ist die Nutzung nur begrenzte Zeit erlaubt.



Neue VM erstellen: Die korrekte Systemauswahl zu Beginn der Einrichtung ist wichtig, damit Virtual Machine Manager geeignete Standardwerte in die Konfiguration einträgt.

men zur ISO-Datei mit dem Windows-Installationsmedium ein. Das Script erstellt die Datei „Windows_11_bypass.iso“. Bei der Installation fragt Windows nach Sprache, Edition und Zielfestplatte. Der Rest der Installation läuft automatisch ab, wobei ein lokales Benutzerkonto ohne Passwort erstellt wird. Beim ersten Neustart werden Sie aufgefordert, ein Passwort zu vergeben.

Windows in einer VM installieren

Wir beschreiben die Konfiguration am Beispiel einer virtuellen Maschine, in der Windows 11 Pro laufen soll.

Schritt 1: Starten Sie die virtuelle Maschinenverwaltung und klicken Sie auf die Schaltfläche oben links, um eine neue virtuelle Maschine zu erstellen. Im Assistenten wählen Sie die Option „Lokales Installationsmedium (ISO-Abbild oder CDROM)“ und klicken auf „Weiter“.

Schritt 2: Klicken Sie auf „Durchsuchen“, dann auf „Lokal durchsuchen“ und wählen Sie die ISO-Datei des Installationsmediums. Unter „Wählen Sie das Betriebssystem aus, das Sie installieren“ sollte automatisch „Microsoft Windows 11“ erscheinen. Wenn nicht, entfernen Sie das Häkchen vor „Automatische Erkennung aus dem Installationsmedium / der Quelle“, tippen „Windows“ in das Eingabefeld ein und wählen „Microsoft Windows 11“.

Schritt 3: Nach einem Klick auf „Weiter“ folgen Sie den weiteren Anweisungen des Assistenten. Die Voreinstellungen können Sie in der Regel übernehmen. Beim Speicherplatz für das Festplattenabbild sollten Sie jedoch einen höheren Wert eingeben. Der Platz wird nicht sofort belegt, sondern erst, wenn er von Windows tatsächlich benötigt wird. Geben Sie hinter „Name:“ eine aussagekräftige Bezeichnung für die neue VM ein. Diese darf keine Leerzeichen enthalten. Setzen Sie ein Häkchen vor „Konfiguration bearbeiten vor der Installation“ und klicken Sie auf „Fertig.“

Schritt 4: Sie können jetzt fast alle Einstellungen, die der Assistent eingetragen hat, prüfen und ändern. Grundsätzlich lässt sich Windows 11 mit diesen Optionen installieren und verwenden. Unter „Übersicht“ sollten Sie hinter „Firmware“ den Eintrag „BIOS“ wählen, damit sich Schnappschüsse erstellen lassen. Die Voraussetzung dafür ist ein angepasstes Installationsmedium (siehe vorheriger Abschnitt).

Für den Festplattenadapter kommt standardmäßig ein Hardwareemulator zum Einsatz. Dadurch sind im Gastsystem zwar keine zusätzlichen Treiber erforderlich, aber die Leistung ist auch nicht optimal. Stellen Sie deshalb bei „SATA Festplatte 1“ hinter „Festplattenbus“ den Wert „VirtIO“ ein und klicken Sie auf „Apply“. Diese Einstellung lässt sich nach der Installation nicht mehr ändern.

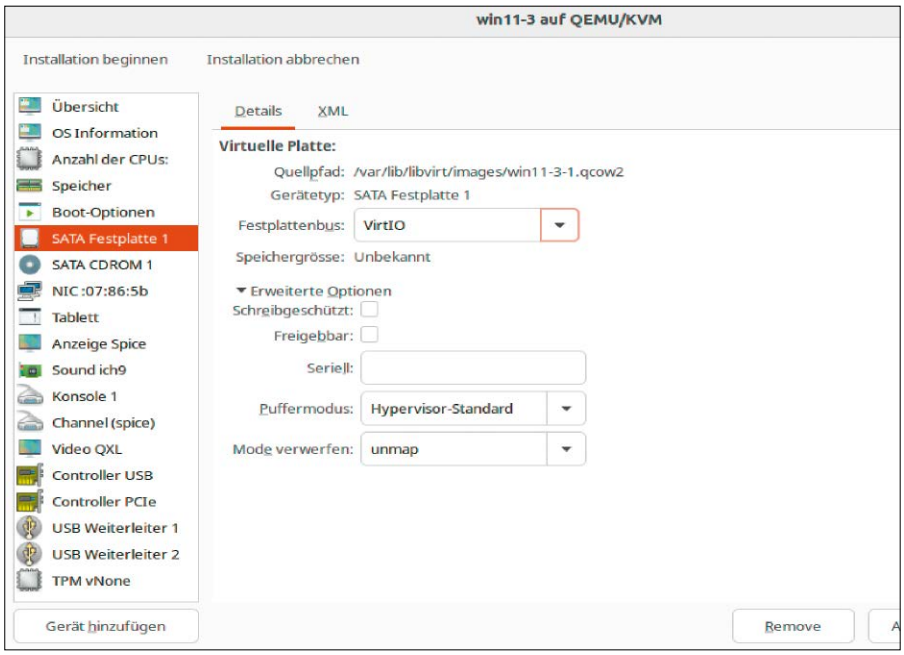
Schritt 5: Laden Sie die Windows-Treiber von *https://bit.ly/VrtoWin* per Klick auf „Stable virtio-win ISO“ herunter. Wechseln Sie dann zurück zur Konfiguration der virtuellen Maschine, klicken Sie links unten auf „Gerät hinzufügen“ und dann auf „Speicher“. Wählen Sie hinter „Gerätetyp“ den Eintrag „CDROM-Gerät“. Dann klicken Sie auf „Verwalten“ und auf „Lokal durchsuchen“. Hier geben Sie die heruntergeladene ISO-Datei an, klicken auf „Öffnen“ und dann auf „Fertig“.

Schritt 6: Mit „Installation beginnen“ öffnet sich das Fenster des virtuellen PCs, in das Sie mit der Maus klicken. Sobald die Meldung „Press any key to boot from CD or DVD“ erscheint, drücken Sie möglichst schnell eine beliebige Taste.

Wenn Sie den Zeitpunkt verpassen, lösen Sie den Mauszeiger, in dem Sie die linke Strg- und Alt-Taste gleichzeitig drücken. Gehen Sie auf „Virtuelle Maschine → Herunterfahren → Ausschalten erzwingen“ und danach auf „Anzeigen → Details“. Unter „Boot-Optionen“ setzen Sie ein Häkchen vor „SATA CDROM 1“, verschieben den Eintrag mit der Pfeiltaste an die erste Position und klicken auf „Apply“. Gehen Sie auf „Anzeigen → Konsole“ und schalten Sie die virtuelle Maschine über die Play-Taste wieder ein. Sie haben dann erneut die Gelegenheit, eine Taste zu drücken und von der ISO-Datei zu booten. Da die Bootreihenfolge erhalten bleibt, müssen Sie diese Einstellung nicht mehr ändern.

Schritt 7: Folgen Sie den Anweisungen des Windows-Installationsassistenten. Im Dialog „Installationsart“ klicken Sie auf „Benutzerdefiniert: nur Windows installieren (für fortgeschrittene Benutzer)“. Ein Zieldatenträger wird nicht angeboten, weil die dafür nötigen Treiber fehlen. Klicken Sie auf „Treiber laden“ und dann auf „OK“.

Wählen Sie den passenden Treiber, für Windows 11 die Zeile „Red Hat VirtIO SCSI con-



Leistung optimieren: Die virtuelle Festplatte sollte mit dem Bustyp „VirtIO“ konfiguriert sein. Windows benötigt dafür einen Treiber, den man in das Installationssystem einbindet.

troller (E:\amd64\w11\viostor.inf)“ und klicken Sie auf „Weiter“. Klicken Sie auf „Weiter“, um die nächste Phase der Installation einzuleiten.

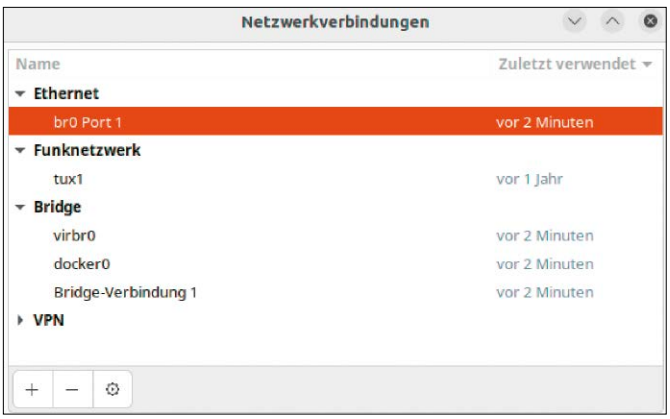
Schritt 8: Nach Anschluss der Installation öffnen Sie im Windows-Explorer das DVD-Laufwerk mit den Windows-Treibern (meist „E:“). Nach der Installation von „virtio-win-gt-x64.msi“ sowie „virtio-win-guest-tools-exe“ fahren Sie Windows herunter. In den Einstellungen der virtuellen Maschine („Anzeigen → Details“) ändern Sie beim Netzwerkadapter (Bezeichnung „NIC:31:c7:0e“ oder ähnlich) das Gerätemodell auf „virtio“. Das Laufwerk „SATA CDROM 2“ mit den Treibern löschen Sie über den Kontextmenüpunkt „Gerät entfernen“.

Linux in einer VM installieren

Für eine Linux-VM folgen Sie den Schritten 1 bis 3 der Windows-Anleitung, danach wählen Sie gleich „Installation beginnen“. Die automatische Erkennung des Betriebssystems funktioniert beispielsweise bei Fedora und Ubuntu, nicht jedoch bei Ubuntu-Varianten wie Kubuntu oder Linux Mint. Entfernen Sie das Häkchen vor „Automatische Erkennung aus dem Installationsmedium / der Quelle“ und verwenden Sie die Suche für die Auswahl der Distribution. Bei Linux Mint 21.1 oder Kubuntu 22.04 beispielsweise verwenden Sie den Eintrag „Ubuntu 22.04 LTS“. In den Einstellungen der VM müssen Sie nichts ändern. Zusätzliche Treiber sind nicht erforderlich und Festplatte sowie Netzwerkadapter sind für Linux bereits optimal konfiguriert.

Datenaustausch mit dem Hostsystem

Die Zwischenablage verwenden Host- und Gastsystem gemeinsam. Text und Bilder lassen sich in beide Richtungen ohne besondere Konfiguration per Strg-C und Strg-V übertragen. Das Netzwerk der virtuellen Maschinen ist standardmäßig als NAT mit eigenem IP-Bereich konfiguriert. Somit sind der Internetzugang und Freigaben im lokalen Netzwerk möglich. Der Host-PC kann eine Verbindung zur IP-Adresse des Gast-PCs aufbauen, etwa für SSH oder einen Webserver.



Netzwerkbrücke: Damit Geräte im lokalen Netzwerk auf das System in der VM zugreifen können, muss man eine „Bridge“ für den Netzwerk-Manager erstellen.

VMs sehen sich untereinander nicht und auch über andere Rechner im lokalen Netzwerk ist keine Verbindung möglich. Wenn Sie das ändern möchten, richten Sie eine Netzwerkbrücke ein. Das funktioniert problemlos mit allen Ethernet-Adaptern, mit WLAN-Adaptern jedoch oft nicht.

Falls noch nicht vorhanden, installieren Sie die nötige Software mit

```
sudo apt install bridge-utils
```

und starten unter Ubuntu oder Linux Mint im Terminal

```
nm-connection-editor
```

Klicken Sie auf die „+“-Schaltfläche, wählen Sie „Bridge“ und klicken Sie auf „Erstellen“. Hinter „Name der Schnittstelle“ tragen Sie *br0* ein. Klicken Sie auf „Hinzufügen“, wählen Sie „Ethernet“ und klicken Sie auf „Erstellen“. Hinter „Geräte“ wählen Sie den Ethernet-Adapter, klicken auf „Speichern“ und dann noch einmal auf „Speichern“. Entfernen Sie „Ethernet-Verbindung 1“ per Klick auf die „-“-Schaltfläche.

In einem anderen Terminal starten Sie den Netzwerk-Manager neu:

```
sudo systemctl restart
  NetworkManager
```

Manchmal ist es nötig, Linux neu zu starten, damit die Einstellungen wirksam werden. Kontrollieren Sie die Konfiguration im Terminal mit

```
ip a
```

„br0“ sollte jetzt eine IP-Adresse aus dem Adressbereich Ihres Router erhalten haben. Rufen Sie die Konfiguration der virtuellen Maschine auf und wählen Sie beim Netzwerkadapter hinter „Netzwerkquelle“ den Eintrag „Bridge device“. Hinter „Gerätename“ tragen Sie „br0“ ein und klicken auf „Apply“. Starten Sie das System in der VM neu. Es erhält nun per DHCP eine IP-Adresse vom Router und ist damit mit jedem Gerät im lokalen Netz erreichbar. ■

Fertige virtuelle VMs

Virtuelle Maschinen muss man nicht zwingend in Virtualbox konfigurieren, danach manuell installieren und mit Software und Diensten ausstatten. Windows, zahlreiche Linux-Desktops und viele Linux-Server gibt es komplett vorkonfiguriert zum Download.

VON HERMANN APFELBÖCK

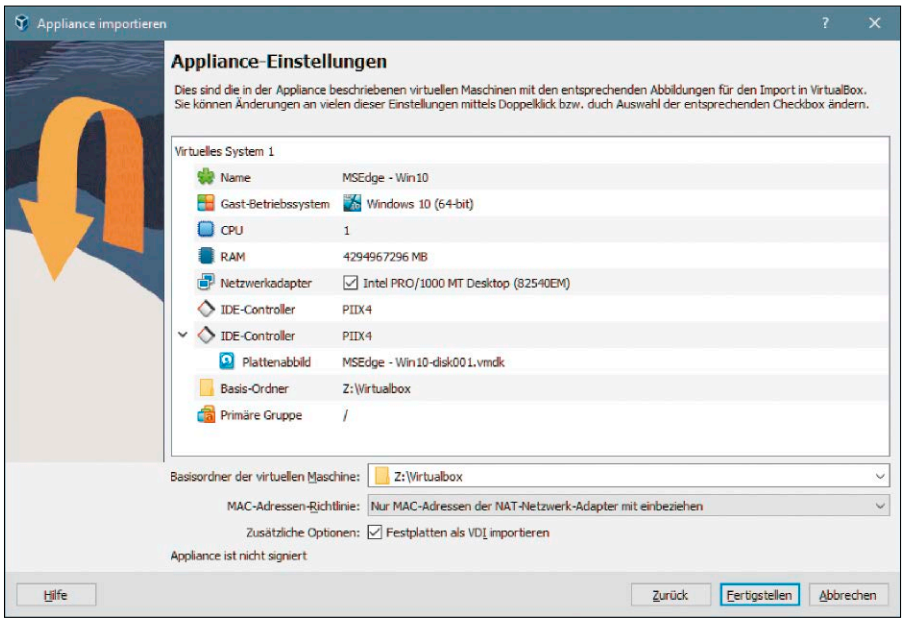
Für komplett ausgestattete VMs (Appliances) gibt es etliche und ergiebige Anlaufstellen im Internet. Im Prinzip ersparen Sie sich damit die Hardwareeinrichtung in Virtualbox, die anschließende Installation des Systems und eventuell die Konfiguration eines komplexen Serverdienstes. Ob und wo sich das wirklich lohnt, hängt vom Verwendungszweck und vom Nutzer-Know-how ab.

OVA-Format: Eingepackte PCs

Die standardisierte Hardware virtueller Maschinen macht es möglich, komplette Systeme einzupacken (Appliance) und diese auf jedem anderen Rechner via Virtualisierer zu starten. Als Virtualbox-Nutzer werden Sie theoretisch selbst mühelos zum Appliance-Entwickler, indem Sie eine sorgfältig konfigurierte VM mit dem Menü „Datei → Appliance exportieren“ als Appliance sichern und weitergeben können. Das Resultat der Aktion ist eine OVA-Datei (Open Virtual Appliance), im Prinzip ein gepacktes TAR-Archiv.

Vmware kennt die Methode analog und verwendet dabei das Format OVF (Open Virtualization Format). Dieses kann Virtualbox ebenso wie sein natives OVA-Format mit „Datei → Appliance importieren“ importieren.

Virtuelle Appliances werden aber nicht immer im OVA-Format angeboten: Die Seite *www.osboxes.org* liefert zum Beispiel grundsätzlich nur die virtuelle Festplatte aus, also VDI-Dateien für Virtualbox. Was ist der Unterschied zu OVA? Virtuelle Maschinen für Virtualbox bestehen im Wesentlichen nur aus dem VDI-Festplattenabbild und einer kleinen XML-Konfigurationsdatei mit der Endung „.vbox“. Folglich genügt eigentlich die virtuelle Festplatte, denn die Konfiguration für ein System ist mit dem Virtualbox Manager in drei Minuten erstellt. Das OVA-Paket hat daher gegenüber einem puren VDI-Abbild nur den kleinen Vorteil, die Konfiguration mitzuliefern, und als zweiten Vorteil eine reduzierte Downloadgröße dank Komprimierung.



Einfacher Import: Eine komplette VM im OVA-Format enthält das Festplattenabbild plus Konfiguration des virtuellen PCs. Letztere können Sie bei Bedarf anpassen.

Schlüsselfertige Desktop-VMs

Die schon genannte Site *www.osboxes.org* bietet nur die Festplattenabbilder. Klicken Sie dort auf „VM Images“ und wählen Sie das benötigte Format – VDI für das hier bevorzugte Virtualbox. Die zahlreichen virtuellen Festplatten sind standardmäßig 7z-gepackt. Unter Windows muss daher der Packer 7-Zip vorliegen (*www.7-zip.de*), unter Linux ist 7z-Unterstützung in der Regel Standard und im Bedarfsfall mit

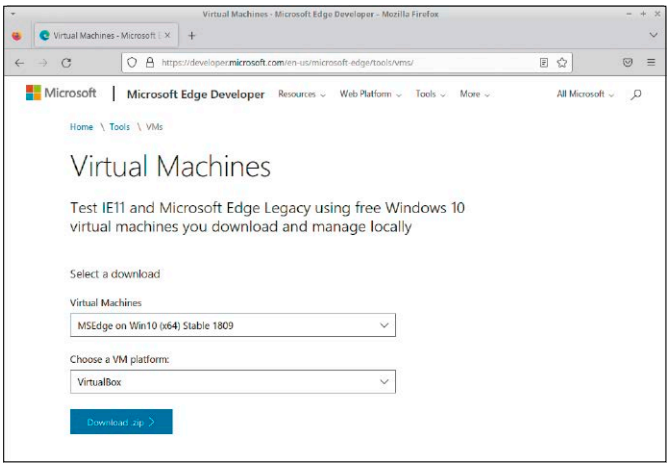
```
sudo apt install p7zip p7zip-full
```

schnell nachgerüstet. Die VDI-Images lassen sich dann einbinden, indem Sie in Virtualbox eine neue virtuelle Maschine erstellen und bei der Festplattenkonfiguration „Eine vorhandene virtuelle Festplattendatei verwenden“. Dazu klicken Sie auf das Ordnersymbol und navigieren zur heruntergeladenen VDI-Datei (der Pfad ist im Prinzip beliebig, aber für bessere Übersicht empfiehlt sich ein Sammelordner für solche VDIs). Nach Auswahl und „Hinzufügen“ ist die VM schon startklar.

Bei den Osboxes-Images handelt es sich überwiegend um Linux-Desktops (von „Android x86“ bis „Zorin OS“), die Sie anschließend beliebig anpassen können. Ganz ohne Pflegeaufwand sind sie dennoch nicht: Wenn Ihnen das voreingestelle Standardkonto – meist „osboxes“ mit Kennwort „osboxes.org“ – nicht zusagt, müssen Sie ein neues Konto einrichten. Oberfläche, Tasta-

tur, Zeitzone sind grundsätzlich US-amerikanisch, was in den Regions- und Spracheinstellungen des jeweiligen Systems geändert werden muss.

Weitere Eigenheiten einer Appliance sind nie auszuschließen. Der Download einer fertigen Desktop-Appliance garantiert zwar den besonders schnellen Einsatz, bleibt aber eher eine Empfehlung für die unkomplizierte Wegwerf-VM. Zudem bietet *www.osboxes.org* nicht durchgehend aktuelle Versionen, sondern zum Teil auch ältere Systeme. Wer eine Desktop-VM für den nachhaltigen Dauerbetrieb einrichten will, nimmt vielleicht doch besser die Mühe der Installation mit dem Originalsystem in Kauf.



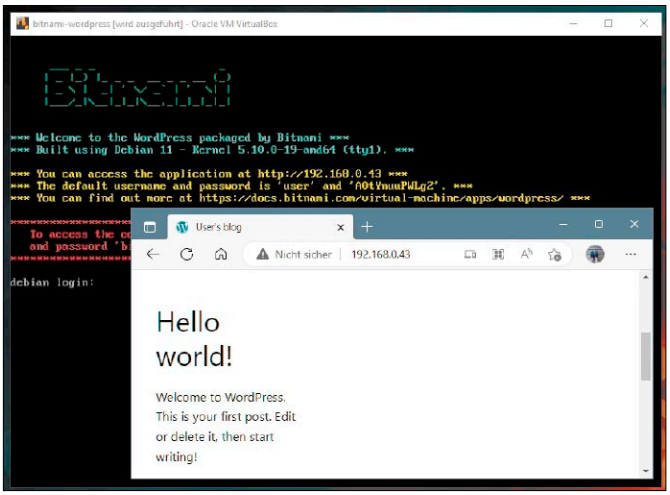
Die kostenlosen Windows-VMs von Microsoft sind primär für Webentwickler gedacht, enthalten aber ein vollständiges Windows für jeden Einsatzzweck.

Windows-Appliance von Microsoft

Microsoft bietet virtuelle Windows-Maschinen unter *https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/* kostenlos zum Download an. Das Angebot richtet sich an Entwickler, die Webseiten mit Edge testen wollen. Es handelt sich aber um komplette Windows-Systeme, die 90 Tage ohne Einschränkung laufen. Das verfügbare Windows 10 („MsEdge on Win10 (x64) Stable 1809“) hat eine Downloadgröße von 6,7 GB. Unter „Select platform“ stellen Sie „Virtualbox“ ein. Den gezippten Download entpacken Sie, öffnen die OVA-Datei per Doppelklick in Virtualbox oder wählen dort „Datei → Importieren“.

Microsoft gibt auf der Website den Tipp, vor dem ersten Start einen Schnappschuss der VM zu erstellen. Stellen Sie diesen vor Ablauf der 90 Tage wieder her, dann lässt sich die Windows-Appliance weitere 90 Tage nutzen. Dieser Hinweis und weitere Tipps zum Verlängern der Laufzeit erscheinen auch beim ersten Start der VM unübersehbar als Wallpaper. Für Linux-Anwender, die Windows vorübergehend für spezielle Software benötigen, ist die Appliance die eindeutig einfachere Alternative gegenüber der Installation des Windows-10-Enterprise-ISOs.

Ohne Nachbearbeitung geht es aber nicht: Das Wallpaper mit den Tipps wird früher oder später lästig. Eventuell wollen Sie auch das Standardkonto „IEUser“ mit Passwort „Passw0rd!“ ändern. Und auch die englischsprachige Oberfläche sowie die Zeitzone müssen über die „Einstellungen“ (Win-I) und „Time & Language → Region“ erst auf Deutsch und europäische Zeitzone gesetzt werden.



Typische Server-Appliance: Diese Wordpress-Instanz auf Debian-Basis von *www.bitnami.com* erspart die Webserver-Konfiguration und ist sofort im lokalen Netzwerk einsatzbereit.

Server-Appliances von Bitnami, Turnkey & Co.

Auf Serversysteme spezialisiert sind die Sites *www.bitnami.com* und *www.turnkeylinux.org*. Hier erhalten Sie – überwiegend in OVA-Format – CMS-Systeme wie Drupal, Typo3, Joomla und Wordpress sowie eine Vielzahl von Shop- und Entwicklungssystemen. Die VMs sind mit allem ausgestattet, was zum Betrieb notwendig ist, und ersparen Installation und Konfiguration von Apache/Nginx, My SQL und PHP. Das ist für alle, erst recht für unerfahrene Nutzer ein unschätzbarer Gewinn. Natürlich sind auch die Netzwerkeinstellungen der VM gleich so gesetzt („Netzwerkbrücke“), dass Serveranwendungen sofort funktionieren.

Eher an Entwickler und Firmen richtet sich das Appliance-Angebot von Vmware (*https://marketplace.vmware.com/vsx*). Das Portal bietet vorkonfigurierte Spezialsysteme. Nicht alle virtuelle PCs sind hier frei verfügbar, einige erfordern eine Registrierung oder eine Gebühr. Eine einmal optimierte VM als OVA-Paket oder als VDI-Image weiterzugeben, ist denkbar einfach. Daher lohnt sich die Suche nach einem solchen Angebot auch bei vielen Einzelprojekten, wie folgende, eher zufällig gewählte Beispiele abschließend zeigen sollen:

Only Office: Im Downloadbereich *www.onlyoffice.com/de/download-docs.aspx* lässt sich nach einem Klick auf „Community“ die „Univention-Anwendung“ wahlweise mit Nextcloud oder Owncloud als VM herunterladen und in Virtualbox importieren.

Whonix: Das anonymisierende Surfsystem ist in der Zielsetzung mit dem Livesystem Tails vergleichbar, hat aber als Virtualbox-Appliance einen anderen Ansatz mit zwei parallelen VMs. Die OVA-Appliance mit circa 2,2 GB gibt es unter *www.whonix.org/wiki/VirtualBox/XFCE*. Nach dem Import in Virtualbox erscheinen zwei neue VMs, wovon Sie immer erst das Gateway, danach die Workstation starten. Das Konstrukt erscheint aufwendig, läuft aber auf jedem durchschnittlichen Rechner mühelos. ■

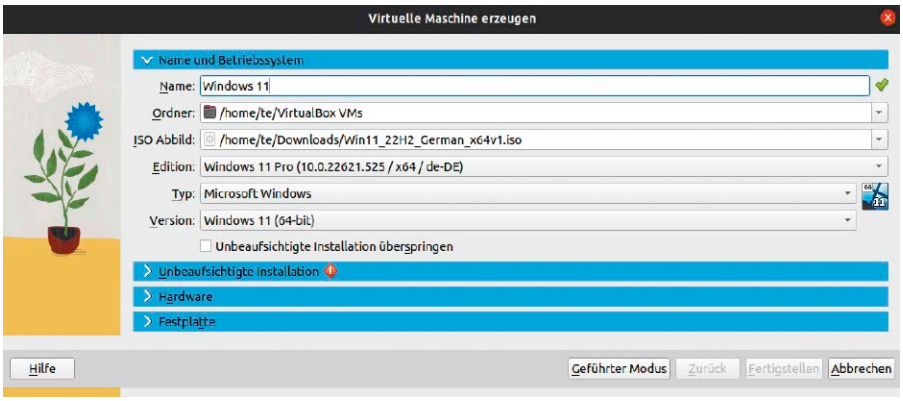
Linux hilft Windows

Nützliche Tools können unter Linux beim Umgang mit Windows-Installationen helfen. Man kann Windows vollautomatisch in einer virtuellen Maschine installieren oder ein vorhandenes Windows virtuell weiterverwenden.

VON THORSTEN EGGELING

Eine alternative Methode kann die Windows-Installation in Virtualbox beschleunigen. Das Setup kann unter Linux komplett automatisch und ohne Benutzereingaben erfolgen. Außerdem lässt sich ein bereits installiertes Windows auf eine virtuelle Festplatte übertragen und dann in Virtualbox weiterverwenden. Die Beschreibungen beziehen sich auf Ubuntu 20.04, 22.04, Linux Mint 20.x und 21. Bei anderen Distributionen weichen die Bezeichnungen der nötigen Zusatzpakete meist ab.

Service: Befehlszeilen und Beispieldateien für diesen Artikel können Sie über *https://m6u.de/depwin* abrufen. Darüber hinaus empfehlen wir die vorherige Lektüre der vorangehenden Virtualbox-Beiträge.



Windows in Virtualbox: Über den Assistenten ist die Windows-Installation schnell gelungen. Noch schneller und vollautomatisch lässt sich die Aufgabe per Script erledigen.

1. Virtuelle Festplatten und WIM-Dateien

Virtualisierungssoftware verwendet für die Installation von Systemen virtuelle Festplatten. Dabei handelt es sich um Dateien, die ein Festplattenabbild enthalten und sich wie eine physikalisch vorhandene Festplatte oder SSD nutzen lassen. Virtualbox verwendet standardmäßig VDI-Dateien (Oracle Virtual Disk Image), kann aber auch Microsofts VHD-Abbilder nutzen (Microsoft Virtual Hard Disk Format).

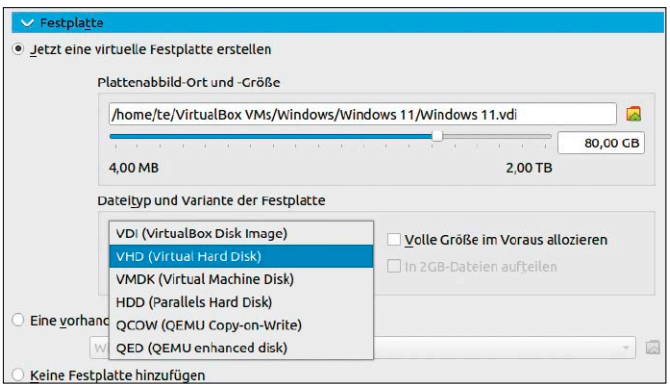
VHD und die Weiterentwicklung VHDX sind die Standardformate bei Microsofts Virtualisierungssoftware Hyper-V. Außerdem kann man seit Windows 7 aus einer VHD-Datei booten (Native Boot). Laut Microsoft soll man jüngeres VHDX bei Windows 10 und höher für Native Boot verwenden, bisher konnten wir aber bei Windows 10 und 11 keine Probleme mit dem VHD-Format feststellen. Virtualbox unterstützt das VHDX-Format zurzeit nicht, weshalb man beim Vorgänger bleiben muss, wenn man den PC auch direkt von der virtuellen Festplatte booten möchte. Wie sich eine VHD-Datei in den Windows-Bootmanager integrieren lässt, können Sie unter *https://m6u.de/depwin* nachlesen.

WIM (Windows Imaging Format) ist ein weiteres Abbildformat von Microsoft. WIM-Dateien sind komprimierte Archive eines Dateisystems, ähnlich wie ZIP-Dateien. Es können mehrere Dateisysteme enthalten sein, die sehr effizient gespeichert werden. Identische Dateien sind nur einmal enthalten. WIM-Dateien lassen sich für Windows-Backups nutzen, kommen aber vor allem bei der Windows-Installation zum Einsatz („install.wim“).

Das Windows-Setupprogramm bereitet die Partitionen sowie die Bootumgebung vor und extrahiert den Inhalt der Datei „install.wim“ auf das Ziellaufwerk. Auf das Windows-Setupprogramm ist man dabei nicht angewiesen. Eine WIM-Datei lässt sich auch unter Linux auf eine virtuelle oder physikalische Festplatte entpacken.

Für Windows 11 ergibt sich nebenbei der Vorteil, dass dann keine Hardwareprüfung erfolgt und sich das System also auch auf offiziell nicht unterstützter Hardware einrichten lässt.

Die Hardwarevoraussetzungen (siehe *https://bit.ly/Win11SP*) gelten ansonsten auch für virtuelle Maschinen.



Virtuelle Festplatte: Standardmäßig verwendet Virtualbox VDI-Dateien. VHD-Dateien lassen sich aber ohne Nachteile ebenfalls nutzen und eignen sich auch für Native Boot.

2. Linux-Tool für die Nutzung von WIM-Dateien

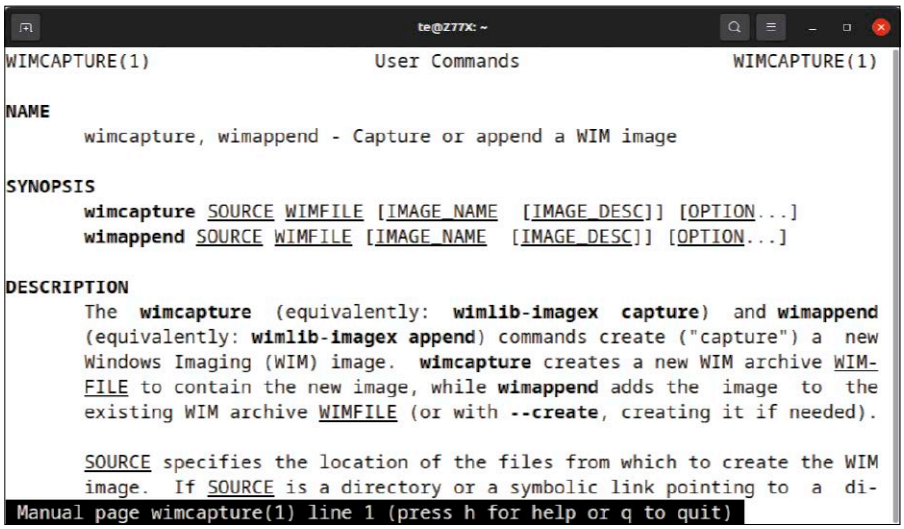
Unter Windows dient das Tool Dism zur Verwaltung von WIM-Dateien. Das Linux-Gegenstück dazu heißt wimlib-imagex (*https://wimlib.net*). Zu Installation verwenden Sie im Terminal die Zeile

```
sudo apt install wimtools
```

wimlib-imagex enthält Kommandos wie „apply" (entpacken), „capture" (archivieren) und „mount", womit sich eine WIM-Datei in das Dateisystem einhängen lässt. Um die Benutzung zu vereinfachen, gibt es einige Hardlinks auf wimlib-imagex, etwa wimapply, wimcapture und wimmount, über die sich die Kommandos direkt ausführen lassen. Der Aufruf ohne weitere Optionen liefert eine Kurzübersicht der möglichen Parameter. Mit beispielsweise

```
man wimcapture
```

erhalten Sie ausführliche Informationen mit Beispielen zur Verwendung.



Weitere Informationen: In den Manpages der einzelnen Wimlib-Tools finden Sie eine Übersicht der erforderlichen Parameter und Optionen sowie Beispiele zur Anwendung.

3. Windows in einer VHD-Datei installieren

Das Tool wimapply reicht aus, um Windows in eine VHD-Datei für eine virtuelle Maschine zu installieren. Die virtuelle Festplatte muss allerdings erstellt, partitioniert und formatiert werden. Danach lassen sich das Windows-System und die Windows-Bootumgebung einrichten. Wir gehen außerdem davon aus, dass Virtualbox bereits installiert ist. Das Virtualbox-Tool Vboxmanage für die Kommandozeile ermöglicht es, virtuelle Festplatten und virtuellen Maschinen automatisch zu erstellen.

Wir haben alle nötigen Befehlszeilen im Script „create_vhd_64.sh" für Windows 10 oder 11 (64 Bit) zusammengefasst (*https://m6u.de/depwin*). Wer Windows 10 in 32 Bit installieren möchte, verwendet „create_vhd_32.sh". Beide Scripts sind weitgehend identisch. Laden Sie das Paket unter „Releases" herunter und entpacken Sie es in Ihr Home-Verzeichnis, beispielsweise nach „deploy-windows".

Vorbereitungen: Bevor Sie die Scripts nutzen können, müssen Sie einige Zusatzpakete einrichten:

```
sudo apt install wimtools build-
  essential git libparted-dev
  python3-pip genisoimage libwin-
  hivex-perl qemu-utils pkg-config
  p7zip-full gettext
```

Sie benötigen das Tool ms-sys (*https://ms-sys.sourceforge.net*), mit dem sich ein Bootrecord für Windows erstellen lässt. Laden Sie die tar.gz-Datei herunter, entpacken Sie diese und führen Sie im Zielverzeichnis die Kommandos

```
make
sudo make install
```

aus. Die Hauptarbeit erledigt dann das Python-Script „setup_win10.py", das von *https://codeberg.org/regnarg/deploy-win10-from-linux* stammt. Es benötigt zusätzliche Python-Module, die Sie mit

```
pip3 install clize construct
  pyparted --user
```

installieren.

Nutzer der älteren Versionen Ubuntu 20.04 oder Linux Mint 20.x lassen pyparted weg und installieren diese Version:

```
pip3 install pyparted==3.11.7
  --user
```

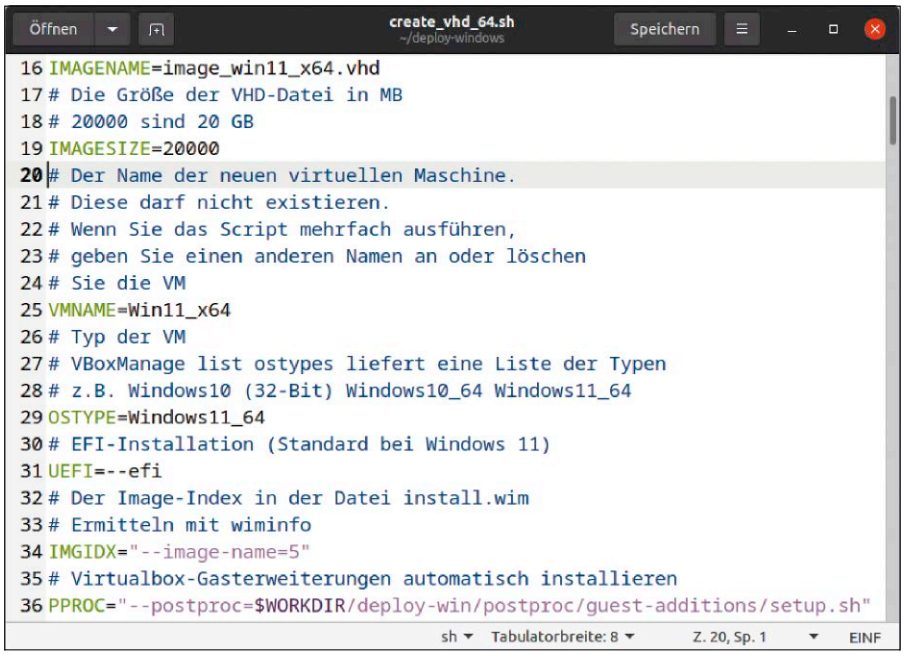
Laden Sie die ISO-Datei des Windows-Installationsmediums über *https://bit.ly/w10is* (Windows 10) oder *https://bit.ly/w11is* (Windows 11) herunter. Kopieren Sie die ISO-Datei in den Ordner „deploy-windows".

Script konfigurieren: Öffnen Sie „create_vhd_64.sh" oder „create_vhd_32.sh" in einem Texteditor und bearbeiten Sie den Abschnitt unter „Konfiguration". Hinter „ISOPATH=" tragen Sie die Bezeichnung der heruntergeladenen ISO-Datei ein. „IMAGESIZE=" legt die Größe der VHD-Datei fest. Hinter „NICDEVICE=" tragen Sie den Namen des Netzwerkadapters ein, den Sie im Terminal mit *ip a* ermitteln. Die Variable „PPROC" enthält den Pfad zu einem Script für die automatische Einrichtung der Virtualbox-Gasterweiterungen. Hinter „UNATT=" steht der Pfad zu einer XML-Datei für die

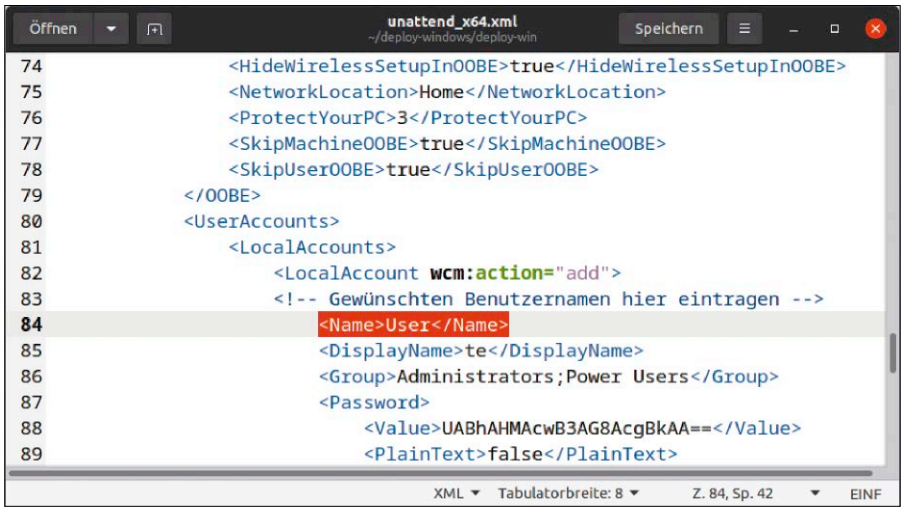
DIE KONFIGURATION DES WINDOWS-BOOTMANAGERS

Die Datei „BCD" enthält eine Datenbank mit Konfigurationsdaten für den Windows-Start. Es sind beispielsweise Informationen über das Startlaufwerk und der Pfad zum Startladeprogramm enthalten. Die Datei liegt auf der EFI-Partition im Order „EFI/Microsoft/Boot". Linux kann die BCD-Datenbank bislang nicht neu erstellen. Man kann aber die Datei vom Installationsdatenträger verwenden und bearbeiten. BCD verwendet das gleiche Speicherformat wie die Windows-Registry, weshalb die Datei sich mit Registrytools für Linux anpassen lässt. Eine Dokumentation der Optionen können Sie unter *https://m6u.de/WBCD* finden.

Über *https://m6u.de/depwin* können Sie ein Script und eine Reg-Datei aus dem Ordner „BCDs" herunterladen, die demonstrieren, wie sich eine universelle BCD-Datei für die Windows-Installation erstellen lässt. Für die Tipps dieses Artikel benötigen Sie das nicht, weil eine bereits vorbereitete BCD-Datei im Ordner „deploy-win" liegt.



Script anpassen: Das Script enthält einen Konfigurationsabschnitt, in dem Sie unter anderem die Größe der VHD-Datei und den Namen der virtuelle Maschine festlegen.



Automatische Windows-Installation: Die Datei „unattend_x64.xml“ dient der Windows-Konfiguration. Tragen Sie den gewünschten Benutzernamen für das lokale Konto ein.

automatische Windows-Installation ohne Benutzereingaben. Passen Sie die Datei für Ihre Installation an, die Kommentare geben dabei Hilfestellung.

Script starten: Führen Sie das Script im Terminal im Verzeichnis „deploy-windows“ etwa mittels

```
./create_vhd_64.sh
```

und Standardrechten aus. Das Script fordert das Passwort für höhere Rechte an. Anschließend können Sie die neue VM in Virtualbox starten. Wenn Sie das Script für eine weitere Installation verwenden wollen, müssen Sie in der Konfiguration andere Namen für die VHD-Datei und die virtuelle Maschine eintragen.

Bitte beachten Sie: Wenn Sie die VHD-Datei auch für Native Boot (siehe Punkt 1) verwenden möchten, sind Sicherungspunkte außerhalb der VM wirkungslos. Für eine Sicherung kopieren Sie einfach die VHD-Datei.

4. Weitere Anwendungen für wimlib-imagex

Die Wimlib-Installation enthält das Script „mkwinpeimg“, mit dem sich ein angepasstes Windows-PE erstellen lässt. Dabei handelt es sich um ein Mini-Windows für Wartungs- und Reparaturarbeiten, das auf der Datei „boot.wim“ basiert. Standardmäßig bietet Windows-PE keinen Netzwerkzugriff und nur wenige Programme. Mit unserem Beispiel-Script „mk-pe.sh“ aus dem Ordner „winpe“ (*https://m6u.de/depwin*) lässt sich das ändern. Es enthält einen Programmstarter, über den Sie Dateimanager und ein Tool für die Netzwerkkonfiguration starten können. Der Starter lässt sich mit portablen Apps erweitern. Beachten Sie, das sich in einem 64-Bit-PE ausschließlich 64-Bit-Programme ausführen lassen. Das Script erstellt eine ISO-Datei für DVDs, für einen USB-Stick kopieren Sie einfach den Inhalt des Ordners „winpe“ auf ein FAT32-Laufwerk.

„Install.wim“ anpassen: Ein weiteres Beispiel-Script liegt im Ordner „Win11-Bypass“. Es zeigt, wie sich die Windows-ISO-Datei mit 7z entpacken und die enthaltene „Install.wim“ mit wimmountrw in das Dateisystem einhängen lässt. Anschließend wird der Inhalt der Datei „bypass.reg“ mit hivexregedit (Paket „libwin-hivex-perl“) in die Registry importiert, die Einbindung mit wimunmount gelöst und die neue ISO-Datei „Windows_11_bypass.iso“ mit genisoimage erstellt. Die jetzt enthaltenen Registry-Werte ermöglichen die Neuinstallation von Windows 11 auch auf offiziell nicht unterstützter Hardware.

Festplatte statt VHD: Für die Windows-Installation auf einer zweiten Festplatte im PC, einem USB-Stick oder einem USB-Laufwerk ist nur eine Befehlszeile nötig. Starten Sie im Ordner „deploy-windows/deploy-win“

```
sudo -E ./setup_win10.py --efi
 --iso=[Windows-11-ISO] --disk=/
 dev/sd[X] --image-name=5
```

Setzen Sie für den Platzhalter den Pfad und Namen der ISO-Datei ein und hinter „--disk=“ den Gerätepfad zum Ziellaufwerk. Es muss neu partitioniert werden, alle enthalten Dateien gehen verloren.

5. Windows-Backup mit wimcapture

Wer Windows auf dem gleichen PC installiert hat, kann mit wimcapture ein Backup erstellen.

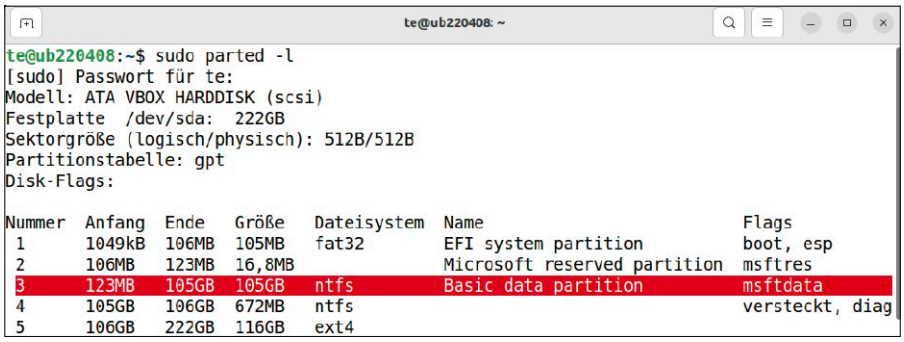
Vorbereitungen: Damit das Backup fehlerfrei gelingt, muss sich das Windows-Dateisystem in einem konsistenten Zustand befinden. Dazu muss Windows ordnungsgemäß beendet worden sein und darf sich

nicht im Ruhezustand befinden. Bei Windows 10/11 verwenden Sie dazu immer „Neu starten“ (nie „Herunterfahren“), bevor Sie ein Linux-System starten.

Im Terminal verschaffen Sie sich mit

```
sudo parted -l
```

einen Überblick über Festplatten und Partitionen. Windows 10 oder 11 sind standardmäßig im Uefi-Modus auf einer GPT-Partition installiert. Parted zeigt hinter „Festplatte“ die Laufwerksbezeichnung an, darunter steht die nummerierte Liste der Partitionen. Die Windows-Partition identifizieren Sie anhand der Größe und der Bezeichnung „Basic data partition“. Das ergibt dann beispielsweise „/dev/sda3“.



Partitionen ermitteln: Der Befehl „sudo parted -l“ zeigt die Partitionen auf der Festplatte an. Nummer „3“ auf „/dev/sda“ ergibt hier den Partitionspfad „/dev/sda3“.

Backup erstellen: Für das Backup verwenden Sie den Befehl wimcapture. Sollte die Windows-Partition gemountet sein, lösen Sie die Laufwerkseinbindung. Im Terminal führen Sie folgenden Befehl aus:

```
sudo wimcapture /dev/sda3 /Backup/
  Win.wim "" "2023-01-01"
```

Ersetzen Sie die Pfadangaben durch die für Ihr System erforderlichen Werte. „/dev/sda3“ ist bei unserem Beispiel die Windows-Partition und „/Backup/Win.wim“ ist das Backupziel. Danach folgen zwei Anführungszeichen für eine leere Bezeichnung sowie ein Datum als Beschreibung, anhand dessen Sie später unterschiedliche Backups auseinanderhalten können.

Inkrementelle WIM-Backups sind besonders platzsparend, weil nur die Änderungen zur ersten Sicherung in der Datei landen. Dafür verwenden Sie die Befehlszeile

```
sudo wimappend /dev/sda3 /Backup/
  Win.wim "" "2023-02-01"
```

Quelle und Ziel sind die gleichen wie bei wimcapture. Das Tool wimappend legt bei jedem Aufruf ein neues Image in der WIM-Datei an, das eine vollständige Wiederherstellung ermöglicht.

Die EFI-Partition ist mit dem Dateisystem FAT32 formatiert. Bei einer Standardinstallation von Linux und Windows auf einer Festplatte gibt es nur eine EFI-Partition, die beide Systeme gemeinsam nutzen. Folgender Befehl

```
sudo tar cvjf efi.tar.bz2 /boot/efi
```

sichert die EFI-Partition.

6. Restore mit wimapply durchführen

Zum Zurücksichern eines Backups verwenden Sie wimapply. Das Tool erwartet als Ziel eine leere Partition. Persönliche Dateien, die sich seit dem letzten Backup geändert haben, müssen Sie vor der Wiederherstellung extra sichern. Oder Sie erstellen zur Sicherheit mit wimcapture ein neues, vollständiges Backup. Sollte die Windows-Partition gemountet sein, lösen Sie die Laufwerkseinbindung. Formatieren Sie zunächst die Windows-Partition (Beispiel):

```
sudo mkfs.ntfs -f /dev/sda3
```

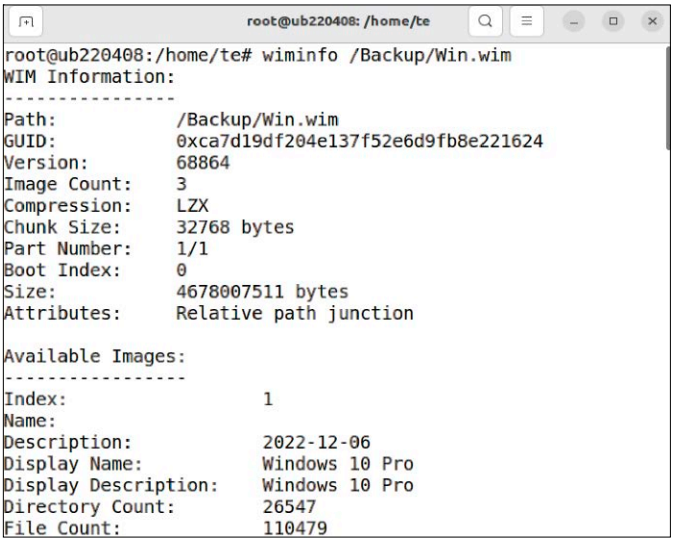
Prüfen Sie die Partitionsangabe genau, damit Sie nicht versehentlich die falsche Partition formatieren. Danach führen Sie folgenden Befehl aus:

```
sudo wimapply /Backup/Win.wim 1 /
  dev/sda3
```

Ersetzen Sie den Pfad zur WIM-Datei und die Gerätebezeichnung durch die für Ihr System gültigen Werte. Die „1“ steht für eine Indexnummer. Sind mehrere Abbilder enthalten, geben Sie die höchste Nummer für das aktuellste Backup an. Die Indexnummern und Beschreibungen lassen sich mittels des Befehls

```
wiminfo /Backup/Win.wim
```

ermitteln.



Index ermitteln: Der Befehl wiminfo liefert die Eigenschaften einer WIM-Datei. Sie erfahren dabei, wie viele Abbilder in der Datei stecken („Image Count“).

Restore auf neue Hardware: Nach Austausch der Festplatte oder für den Umzug auf einen neuen PC verwenden Sie ebenfalls wimapply. Auf einer leeren Festplatte fehlen jedoch die Bootpartition und die Konfiguration. Installieren Sie daher Windows zuerst wie in Punkt 4 beschrieben auf der neuen Festplatte, formatieren Sie die Systempartition neu und entpacken Sie die Sicherung mit wimapply.

Auf der EFI-Partition überschreiben Sie die Dateien mit jenen aus dem Backup (siehe Punkt 5).

Restore in einer VM: Das WIM-Backup lässt sich auch als VHD-Datei wiederherstellen und damit in einer VM nutzen. Als Basis verwenden Sie eine Installation wie in Punkt 3 beschrieben. Das Script „create_vhd_from_Backup.sh“ (*https://m6u.de/depwin*) hängt die Windows-Partition in der VHD-Datei in das Dateisystem ein, formatiert die Partition neu und entpackt das Backup mit wimapply. Passen Sie die Dateinamen und Pfade im Script an, bevor Sie es einsetzen. ■

KI-Nutzung im Alltag

Künstliche Intelligenz kann bei der Suche nach Informationen und beim Erstellen von Texten helfen. Die bisher genutzten Suchmaschinen haben zwar noch nicht ausgedient, werden sich aber durch KI stark verändern.

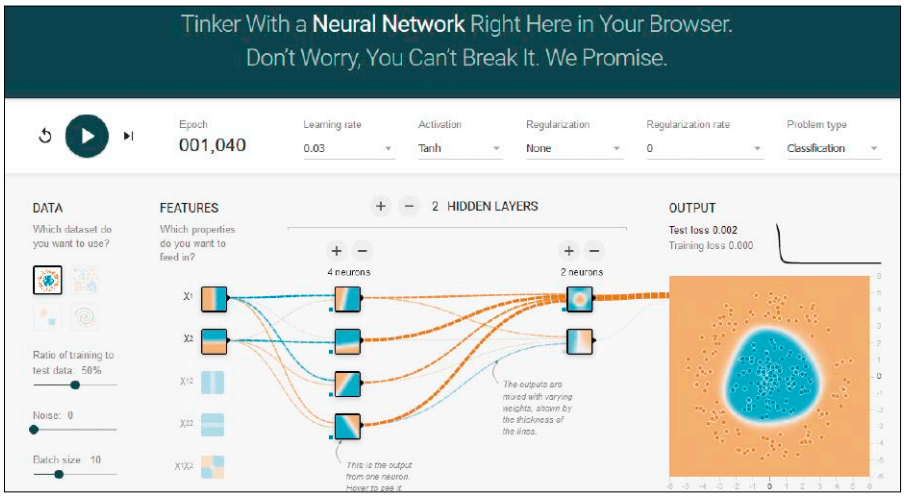
VON THORSTEN EGGELING

Dank Internet lassen sich sehr schnell mehr Informationen abrufen als je zuvor in der Menschheitsgeschichte. Zu fast jedem Thema gibt es Wikipedia-Artikel, Blogbeiträge oder journalistische Texte. Bei der Suche helfen Dienste wie Google oder Bing, die ständig Webseiten katalogisieren und über einen Suchindex auffindbar machen. Besonders relevante, verlässliche oder häufig aufgerufenen Inhalte erscheinen im Suchergebnis an den ersten Positionen. Man ruft eine oder mehrere der angebotenen Webseiten auf und findet dann (hoffentlich) das Gesuchte.

Der Einsatz von künstlicher Intelligenz (KI) für die Beschaffung von Informationen funktioniert völlig anders. Man sollte sich eine KI eher als einen Experten vorstellen, den man zu einem bestimmten Thema befragt. Die Datengrundlage besteht wie bei herkömmlichen Suchmaschinen aus den Inhalten von Webseiten und digitalisierten Druckwerken, aus denen die KI eine Antwort generiert. Die Möglichkeiten gehen jedoch weit über die Fähigkeiten von Suchmaschinen hinaus. Es lassen sich beispielsweise Konzepte für Präsentation, Blogbeiträge oder Briefe erstellen – bei Bedarf in mehreren Sprachen. Für die Formulierung von Suchanfragen und zur Einordnung der Ergebnisse ist es hilfreich, die Funktionsweise einer KI in Grundzügen zu verstehen.

Wie eine KI-Suche funktioniert

KIs verwenden künstliche neuronale Netzwerke. Gruppen von Neuronen sind in mehreren Schichten angeordnet und jedes einzelne Neuron führt Berechnungen durch, die es an die nächste Schicht weitergibt. Zu Beginn ist das Ergebnis zufällig, die KI kann die jeweiligen Werte aber nach und nach unterschiedlich gewichten, bis das gewünschte Ergebnis erzielt wird.



KI ausprobieren: *https://playground.tensorflow.org* vermittelt einen Eindruck von der Arbeitsweise. Mit zusätzlichen Neuronen lässt sich das Ergebnis bei komplexen Mustern verbessern.

Die Funktionsweise lässt sich am einfachsten anhand der Bild- und Mustererkennung demonstrieren. Auf *https://playground.tensorflow.org* finden Sie eine interaktive Anwendung, die auf einem Bild Bereiche mit Punkten gleicher Farbe erkennt. Klicken Sie unter „Data" ein Muster an und starten Sie die Berechnung per Klick auf die „Play"-Schaltfläche. Unter „Output" erscheint das Ergebnis, in dem Bereiche mit gleichfarbigen Punkten mit einem blauen oder orangen Hintergrund erscheinen. Ein dunklerer Hintergrund symbolisiert eine eher sichere Erkennung, ein hellerer deutet auf eine höhere Fehlerquote hin.

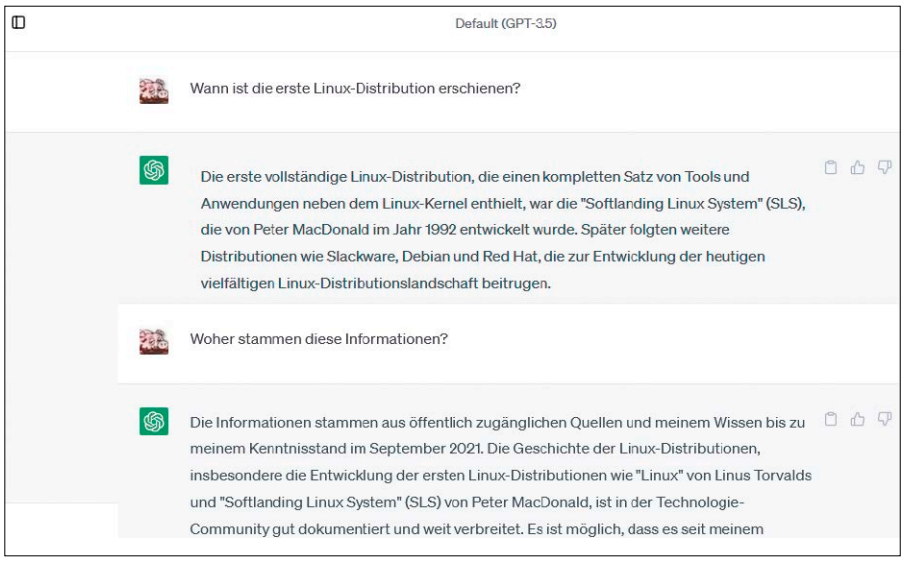
Bei den symmetrischen Mustern liefert das neuronalen Netzwerk schnell ein akzeptables Ergebnis. Die Farbverläufe der einzelnen Neuronen zeigen, wie das Programm vorgeht, die Dicke der Verbindungslinien symbolisiert die Gewichtung. Bei der spiralförmigen Anordnung ist die Unterscheidung schwieriger und zunächst nicht befriedigend. Erst wenn man weitere Neuronen und/oder Schichten hinzufügt, verbessert sich die Leistung.

Texte generieren: Beim Verständnis menschlicher Sprache ist die Situation komplizierter. Zuerst müssen die Sätze in einzelne Wörter oder Wortstämme zerlegt und in Relation zueinander gesetzt werden. Die Neuronen der KI können mit Wörtern jedoch nichts anfangen und arbeiten wie bei der Bilderkennung intern mit Zahlenwerten. Das Ergebnis ist ein Large Language Model (LLM), das Voraussagen über das nächste erwartbare Wort trifft. Man kann sich das ähnlich wie bei einem Lückentext vorstellen, in dem ein fehlendes Wort ergänzt werden soll. Damit die KI eine Frage richtig beantworten kann, muss sie das Vorkommen eines Wortes in einem bestimmten Kontext als wahrscheinlich oder unwahrscheinlich bewerten und dann anhand der verfügbaren Daten eine Antwort ausgeben. Da hier neue Texte anhand der Trainingsdaten erzeugt werden, nennt sich die Technik Generative Pretrained Transformers (GPT).

Suchmaschinen, KI-Chats und Quellenangaben

Suchmaschinen katalogisieren frei zugängliche Internetinhalte. Wenn Sie einem Link im Suchergebnis folgen, entscheiden Sie selbst, ob Sie den Informationen auf einer Website vertrauen oder nicht. Reine KI-Textgeneratoren wie Chat-GPT liefern eine meist gut formulierte Antwort auf Ihre Anfrage. Aus welchen Quellen sich die KI bedient hat, erfährt man in der Regel nicht. Die Frage danach führt nur zu allgemeinen Aussagen wie „Die Informationen stammen aus öffentlich zugänglichen Quellen und meinem Wissen bis zu meinem Kenntnisstand im September 2021“. Die Chat-GPT-Entwickler scheinen Fragen nach den Quellen bewusst zu verhindern, was vielleicht auch etwas mit dem Urheberrecht zu tun hat (siehe Kasten „Rechtliche Fragen“). Auch wenn Chat-GPT keinen direkten Zugriff auf aktuelle Daten aus dem Internet hat, kennt die KI durchaus relevante Webseiten. Eine Frage wie „Wo im Internet finde ich Informationen zur Ubuntu-Konfiguration?“ wird daher korrekt mit einer Liste nützlicher Informationsquellen beantwortet.

Bei Fragen im Bezug auf Software mag eine genaue Quellenangabe nicht besonders wichtig sein. Schließlich kann jeder selbst schnell ausprobieren, ob die angebotene Lösung funktioniert. In anderen Bereichen würde man die Quelle gerne erfahren, etwa um die Verlässlichkeit einzuschätzen. Bestehen Zweifel, sollte man die Fakten über eine Internetsuche prüfen und dabei mehrere Quellen berücksichtigen.



Keine Quellen: Chat-GPT offenbart nicht, woher eine Information genau stammt. Meist erhält man nur allgemeine Hinweise, nach denen man dann selbst im Internet suchen muss.

Index-Suche und KI kombinieren

Die Sprachmodelle GPT 3.5 und 4.0 liefern die Basis für die meisten KI-Dienste im Internet. Einigen bieten daneben eine herkömmliche Websuche an. Man erhält eine konkrete Antwort auf eine Frage und zusätzlich Links zu Webseiten für die weitergehende Recherche.

Bei **You.com** erzeugt die KI einen Antworttext, zeigt aber auch Links zu relevanten Webseiten. Am unteren Rand sind außerdem Schaltflächen mit alternativen Formulierungen für die Suchanfrage untergebracht.

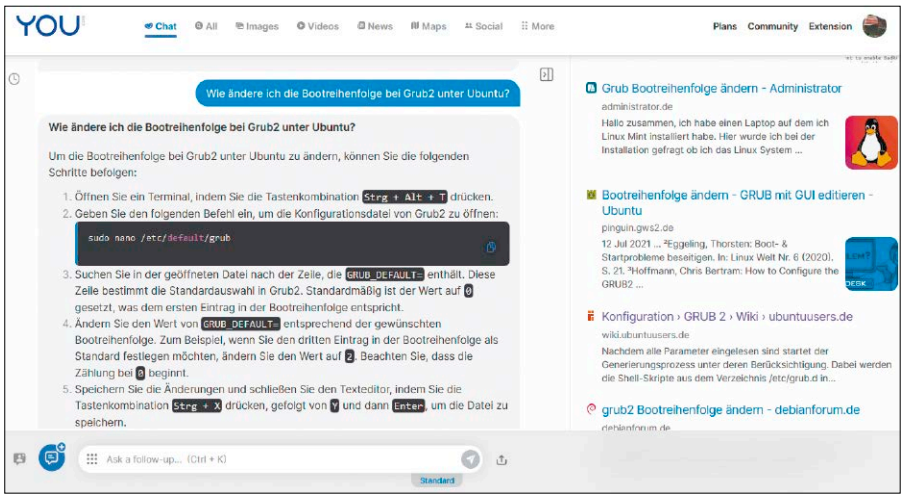
Perplexity zeigt nummerierte Verweise auf Webseiten, die Ziffern tauchen im Antworttext als Quellenbeleg in der jeweiligen Zeile auf. Unter „Related“ werden ähnliche Fragen zum Thema angeboten. Ein Klick darauf startet die Suchanfrage.

Kagi funktioniert ähnlich, zeigt aber zuerst nur das Ergebnis der Suche im Internet. Nach einem Klick auf „Quick Answer“ erscheint die Antwort der KI. Der Dienst verwendet einen eigenen Suchindex und eine selbst entwickelte KI. Im Antworttext werden die Quellen mit Fußnoten angegeben.

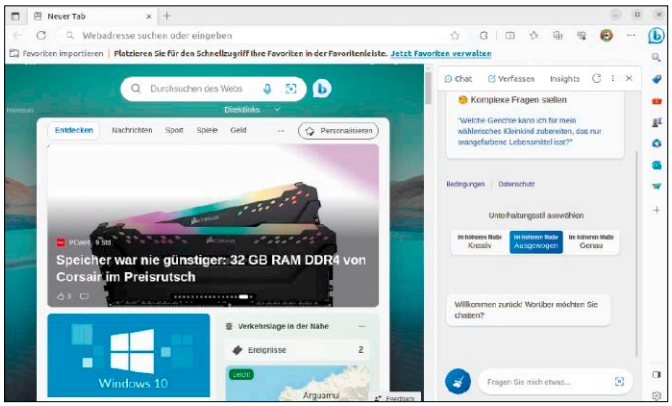
Microsoft hat die KI-Suche in den Browser Edge integriert, den man für Linux über *https://www.microsoft.com/de-de/edge/download* als DEB- oder RPM-Paket herunterladen kann. Für die Nutzung ist ein Mi-

DIE WICHTIGSTEN KI-SUCHMASCHINEN

Name	Beschreibung	Anmeldung erforderlich	Preis	Internet	Sprache Oberfläche/ Ein- und Ausgabe
Andi	klassische Webrecherche mit zusätzlichem Chatbot	nein	kostenlos	*https://andisearch.com*	Englisch/Deutsch
Chat-GPT 3.5	frei zugänglicher KI-Chatbot	nein	kostenlos	*https://chat.openai.com*	Deutsch
Chat-GPT 4.0	verbessertes, aber kostenpflichtigtes Chat-GPT	ja	20 Dollar pro Monat	*https://chat.openai.com*	Deutsch
Friday	KI mit eigenem Sprachmodell, kann mit Chat-GPT bisher nicht mithalten	ja	kostenlos	*https://friday.page*	Englisch/Deutsch
Google Bard	der KI-Chat von Google, zur Zeit noch in der experimentelle Phase	ja	kostenlos	*https://bard.google.com*	Deutsch
Kagi	liefert Webergebnisse und per Klick auf „Quick Answer“ KI-Texte	ja	kostenlos bis 100 Fragen	*https://kagi.com*	Englisch
Microsoft Bing Chat (nur in Edge)	KI-gestützte Suche (GPT-4) und Websuche mit Bing	ja	kostenlos	*www.bing.com/chat*	Deutsch
Perplexity AI	der Dienst nutzt GPT-3.5 und Bing	nein	kostenlos	*www.perplexity.ai*	Englisch/Deutsch
Phind	KI-Suche mit Schwerpunkt Programmierung. Ohne Anmeldung 10 Fragen pro Tag, mit Anmeldung 100	nein	kostenlos	*www.phind.com*	Englisch/Deutsch
You.com	verwendet GPT4 und Diffusion XL	nein	kostenlos	*https://you.com*	Englisch/Deutsch



Kombinierte Suche: You.com liefert meist umfassende Antworten und zeigt die Quellen als Links zu weiterführenden Informationen im rechten Bereich des Fensters an.



Integrierte KI: Microsoft hat den KI-Chat in den Browser Edge integriert. Der lässt sich auch unter Linux installieren, Bing-Chat erfordert aber die Anmeldung mit einem Microsoft-Konto.

crosoft-Konto erforderlich. Der Aufruf erfolgt über das Bing-Chat-Icon rechts oben. Die Antwort ist knapp gehalten, enthält aber meistens die wesentlichen Punkte. Die Quellen zeigt Bing-Chat ähnlich wie Kagi mit Fußnoten an.

Phind produziert per KI meist ausreichend ausführliche Antworttexte und nennt Quellen, die zusätzlich auch unter der Antwort angezeigt werden.

Andi versteht sich als Suchassistent und liefert als Antwort meist eine knappe Zusammenfassung. Im rechten Teil des Fensters erscheinen Webseiten, auf denen die Infos gefunden wurden. Per Klick auf „Visit“ lässt sich die Seite in einem neuen Tab öffnen und mit „Read“ wird der Inhalt in einem Pop-up-Fenster dargestellt. Wer eine Zusammenfassung des Inhalts wünscht, klickt auf „Summarize“, „Explain“ fasst nur die für die Frage relevanten Daten zusammen.

Bard ist die Antwort von Google auf Chat-GPT. Der Dienst befindet sich in einer frühen Entwicklungsphase und arbeitet bisher noch nicht so zuverlässig wie Chat-GPT. Quellen nennt Bard nicht. Der Klick auf „Mit Google suchen“ blendet relevante Links ein, über die sich eine Google-Suche anstoßen lässt.

Friday befindet sich ebenfalls am Anfang der Entwicklung und die Ergebnisse sind zur Zeit oft noch nicht befriedigend. Die Bedienung erfolgt ähnlich wie bei Chat-GPT, indem man die Frage oder Aufgabe in die Eingabezeile tippt. Gibt man „/“ (ohne Anführungszeichen) ein, erscheint ein Menü, das bei der Formulierung der Anfragen hilft. Wählen Sie beispielsweise „Generate Essay Outline“, geben Sie das Thema sowie die gewünschte Anzahl der Wörter ein und unter „Items to emphasize?“ Stichwörter zu den gewünschten Schwerpunkten. Als Ergebnis zeigt Friday die Gliederung eines Essays. Über „Research a Topic“ gibt Friday auch einen Text mit Quellenangaben aus.

Ohne Nutzung des Menüs kann man die Ausgabe durch eine Freitexteingabe beeinflussen, beispielsweise mit „Research [Thema]“ oder „Essay Gliederung mit 500 Wörtern zu [Thema]“.

Hinweis: Die meisten KI-Dienste verwenden eine englischsprachige Oberfläche. Deutschsprachige Eingaben werden intern ins Englische übersetzt, die Antworten erscheinen aber ebenfalls auf Deutsch.

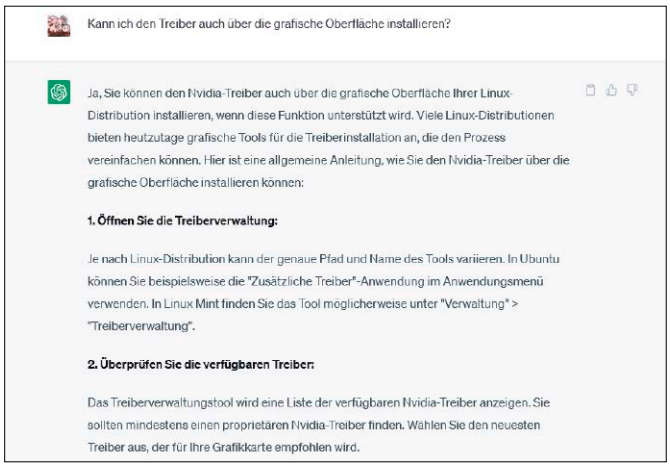
Chat-GPT als Textgenerator nutzen

Chat-GPT 3.5 und 4.0 arbeitet mit einem festen Datensatz, der derzeit bis September 2021 reicht. Neue Informationen kommen momentan nicht hinzu. Die Unterschiede der beiden Sprachmodelle: GPT-3 wurde mit 175 Milliarden Parametern trainiert, GPT-4 mit 100 Billionen Parametern, wodurch sich die Leistung verbessert. Außerdem kann GPT-4 längere Texte bei der Eingabe verarbeiten, was die Möglichkeiten erweitert. Aufgrund des zeitlich begrenzten Datenbestands eignet sich Chat-GPT nicht für die Suche nach aktuellen Informationen. Diese Einschränkung kennen die zuvor genannten KI-Dienste nicht, weil sie bei Bedarf aktuelle Inhalte aus dem Internet einbeziehen.

Die Stärken von Chat-GPT liegen auch in anderen Bereichen. Die Leistung hat viele Nutzer von Anfang überrascht, weil die erzeugten Texte auch auf Deutsch gut lesbar und grammatikalisch weitestgehend korrekt sind. Ein paar eingestreute Floskeln wie „Diese Frage beantworte ich gerne“ oder „Entschuldigen Sie diesen Fehler“ lassen die Antworten menschlich erscheinen. Dabei handelt es sich allerdings um Tricks der Entwickler, denn Chat-GPT kann die Frage nicht wie ein Mensch verstehen und besitzt auch keine Emotionen. Trotzdem mag man kaum glauben, dass die Ergebnisse nur auf Wortanalysen, mathematischen und statistischen Voraussagen sowie Training durch Feedback beruhen.

Chat-GPT kann Texte zu fast beliebigen Themen verfassen oder als Ideengeber dienen. Geben Sie beispielsweise „Erstelle einen Blogbeitrag zum Thema ‚Nvidia Grafikkarte unter Linux optimal einrichten‘ mit 1500 Zeichen“ ein. Der verfasste Artikel ist für einfache Ansprüche ausreichend, geht aber kaum in Details. Mit „Bitte weitere Informationen zur Treiberinstallation“ veranlasst man Chat-GPT, die nötigen Schritte für die Installation über die Paketverwaltung im Terminal auszugeben. Auf die Alternative, das Treiberpaket direkt bei Nvidia herun-

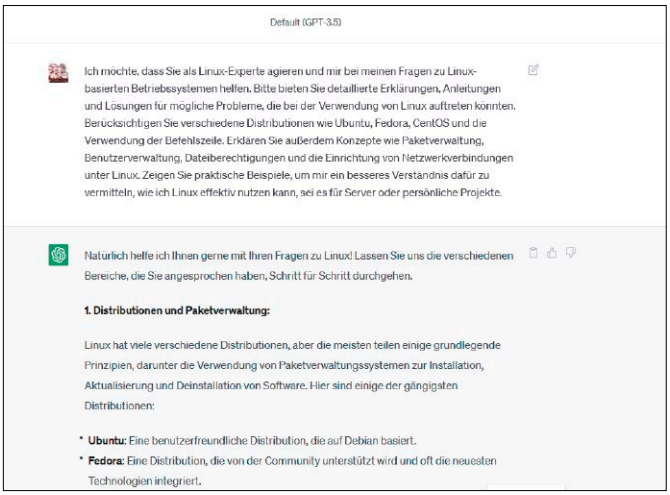
terzuladen, wird ebenfalls hingewiesen. Weitere Alternativen erhält man nach „Kann ich den Treiber auch über die grafische Oberfläche installieren?“, wobei Chat-GPT für Ubuntu-Gnome-Nutzer korrekt empfiehlt „Zusätzliche Treiber“ über „Aktivitäten“ aufzurufen.
Beim Chatverlauf wird der vorherige Kontext stets berücksichtigt. „Nvidia“ kam nur in der ersten Frage vor, dennoch bezieht Chat-GPT auch die nachfolgenden Antworten auf dieses Thema.



Fragen und Nachfragen: Sollte eine Antwort nicht gleich das gewünschte Ergebnis enthalten, kann man Chat-GPT mit einer Detailfrage auf den richtigen Weg führen.

Chat-GPT über den Prompt steuern

Die Eingabezeile bei Chat-GPT heißt Prompt und man kann darüber das Verhalten der KI beeinflussen sowie die Ergebnisse verbessern. Die Möglichkeiten sind derartig zahlreich, dass man sich beim „Prompt Engineering“ am besten von der KI helfen lässt:
„Ich möchte, dass Sie als ChatGPT-Prompt-Generator arbeiten. Ich werde ein Thema senden, Sie müssen einen ChatGPT-Prompt basierend auf dem Inhalt des Themas generieren, der Prompt sollte mit ‚Ich möchte, dass Sie als‘ beginnen, und erraten, was ich tun könnte, und den Prompt entsprechend erweitern. Beschreiben Sie den Inhalt, um ihn für mich nützlich zu machen.“
Chat-GPT fragt dann nach dem Thema, für das Sie einen Prompt erstellen möchten. Geben Sie beispielsweise „Linux-Experte“ ein und kopieren Sie die Antwort. Klicken Sie auf „New Chat“ und fügen Sie die Antwort in den Prompt ein. Da Chat-GPT sich für den Prompt bei unserem Test vor allem auf „detaillierte Erklärungen, Anleitungen und Lösungen für mögliche Probleme, die bei der Verwendung von Linux auftreten könnten“ konzentriert hat, haben wir eine strukturierte Anleitung mit den Punkten Paketverwaltung, Benutzerverwaltung und Dateiberechtigungen erhalten. Sehen Sie einen generierten Prompt als Vorschlag, den Sie jeweils für den gewünschten Schwerpunkt anpassen.



Chat-GPT einstimmen: Den angezeigten Prompt hat die KI zum Bereich „Linux-Experte“ automatisch erzeugt. Die Antwort enthält alle angeforderten Infos und praktische Beispiele.

Tipp: Auf *https://github.com/f/awesome-chatgpt-prompts* finden Sie einige Beispiele für Prompts, die Chat-GPT in unterschiedliche Rollen schlüpfen lassen. ■

RECHTLICHE FRAGEN ZUR VERWENDUNG VON KI-TEXTEN

Einen mit Chat-GPT oder anderen KI-Diensten erstellten Blogbeitrag kann man als eigenes Werk der KI auffassen.
Er besteht zwar aus Inhalten, die irgendwo im Internet zu finden sind, ist aber nicht mit diesen identisch. Zudem erzeugt jede Anfrage einen neuen Text, der sich teilweise deutlich vom vorherigen unterscheidet. Fragt man Chat-GPT selbst nach dem Urheberrecht, bekommt man diese vage Antwort: „Ja, du solltest das Urheberrecht beachten, wenn du Texte verwendest, die mit ChatGPT oder einem ähnlichen KI-Modell generiert wurden. Obwohl die generierten Texte von einer KI erstellt wurden, liegt das Urheberrecht für den erstellten Inhalt in der Regel immer noch beim Urheber, der die ursprünglichen Texte für das Modell erstellt hat, und in einigen Fällen auch bei OpenAI als Entwickler des Modells.“ Um Problemen vorzubeugen, sollte man daher Chat-GPT nur als Ideengeber verwenden und keine KI-generierten Texte als eigenes Werk ausgeben.

Rechtliche Konsequenzen drohen allerdings eher Open AI. Die New York Times und andere Verlage kritisieren die Verwendung ihrer Inhalte als Trainingsdaten für Chat-GPT. Zur Zeit ist unklar, ob Open AI die weitere Nutzung erlaubt wird. Schließlich entgehen den Verlagen Einnahmen, wenn zwar die Inhalte genutzt, aber immer weniger Links von Suchmaschinen zu den redaktionellen Inhalten angeklickt werden. Sollten zahlreiche Inhaltsanbieter die Nutzung ihrer Daten verweigern, würde das die Qualität von Chat-GPT deutlich verschlechtern.

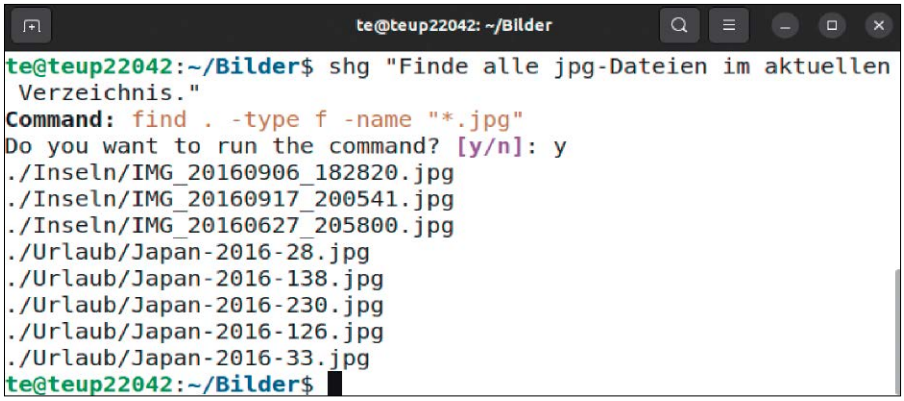
KI-Hilfen für das Terminal

Künstliche Intelligenz kann Fragen zu fast allen Themen beantworten und kennt sich durchaus auch mit Linux aus. Das können Sie ganz gezielt nutzen, um sich Befehlszeilen für das Terminal erzeugen zu lassen.

VON THORSTEN EGGELING

Das Terminal ist mit nützlichen Tools und Funktionen auch unter einem Desktop-Linux kaum entbehrlich. Aber es ist nicht einfach, immer das richtige Werkzeug und die korrekten Optionen für eine Aufgabe zu finden.

Eine KI liefert meist passgenaue Lösungen für ein Problem und kann seine Wahl auch brauchbar erklären. Man muss nur möglichst konkret und präzise fragen. Terminalprogramme mit KI-Anbindung erleichtern die Nutzung. Aber Vorsicht: KIs arbeiten nicht fehlerfrei und man sollte den Vorschlag genau prüfen, bevor man einen tendenziell destruktiven Befehl im Terminal ausführt.



Hilfe für Terminalbefehle: Shell-Genie erzeugt gemäß der gestellten Anfrage eine Befehlszeile, die man nach vorheriger Prüfung auch gleich nutzen kann.

Shell-Genie: Befehlszeilen erstellen

Shell-Genie ist ein Python-Tool, das ein kostenloses KI-Modell des Entwicklers nutzt. Es kann nicht garantiert werden, dass der Zugriff jederzeit möglich ist. Alternativ lässt sich Chat-GPT einbinden. Einen API-Schlüssel dafür erhält man nach der Anmeldung über *https://openai.com/api* und Aufladung des Kontos mit einem Betrag von beispielsweise 20 Dollar. Abgerechnet wird nach dem Umfang der gestellten Suchanfragen (siehe *https://openai.com/pricing*).

Installation: Richten Sie unter Ubuntu oder Linux Mint im Terminal die erforderlichen Pakete mit

```
sudo apt install python3-pip
 python3-venv
```

ein und erstellen Sie dann mit

```
python3 -m venv ~/shell-genie
```

eine virtuelle Python-Umgebung, die Sie mittels

```
source ~/shell-genie/bin/activate
```

aktivieren. Shell-Genie wird dann über

```
pip3 install shell-genie
```

eingerichtet. Laden Sie dann die versteckte Datei „.bashrc“ (im Dateimanager mit Strg-H einblenden) im Home-Verzeichnis in einen Texteditor. Dort fügen Sie die folgenden zwei Zeilen am Ende an:

```
export PATH="$HOME/shell-genie/
 bin/:$PATH"
alias shg="$HOME/shell-genie/bin/
 shell-genie ask"
```

Mit

```
source ~/.bashrc
```

wird die geänderte Datei neu eingelesen und danach starten Sie die Initialisierung des Tools mit

```
shell-genie init
```

Der Einrichtungsassistent fragt nach dem KI-Modell. Wenn Sie einen API-Schlüssel besitzen, verwenden Sie „openai-gpt-3.5-turbo“ und geben dann den Schlüssel ein. Andernfalls nutzen Sie „free-genie“. Folgen Sie den weiteren Anweisungen des Assistenten.

Shell-Genie verwenden: Sie können das Tool über den Aliasnamen „shg“ im Terminal mit dem Kommando

```
shg "[Anfrage]"
```

starten. Für den Platzhalter „[Anfrage]“ setzen Sie für einen ersten Test

```
"Finde alle JPG-Dateien im
 aktuellen Verzeichnis."
```

ein. Die brauchbare Antwort lautet

```
find . -type f -name "*.jpg"
```

Bestätigen Sie mit „y“ gefolgt von der Eingabetaste, um den Befehl auszuführen.

Shell-GPT: Antworten von Chat-GPT erhalten

Shell-GPT (*https://github.com/TheR1D/shell_gpt*) funktioniert ähnlich wie Shell-Genie, benötigt aber in jedem Fall einen API-Schlüssel von Open AI. Die Installation des Python-Tools erfolgt wie für Shell-Genie beschrieben. Sie erstellen eine virtuelle Python-Umgebung mit der Bezeichnung

„shell-gpt“ (siehe oben) und installieren dann das Werkzeug:

```
pip3 install shell-gpt
```

Nehmen Sie auch hier für den bequemen Start den Installationsordner in die Datei „ bashrc“ auf (wie oben).

Shell-GPT verwenden: Beim ersten Start geben Sie den API-Schlüssel für Chat-GPT an. Der Aufruf mit

```
sgpt --help
```

zeigt die verfügbaren Optionen. Einen einfachen Test wie

```
sgpt -s "Aktualisiere mein System"
```

wird Shell-GPT so beantworten:

```
sudo apt update && sudo apt upgrade
  -y
```

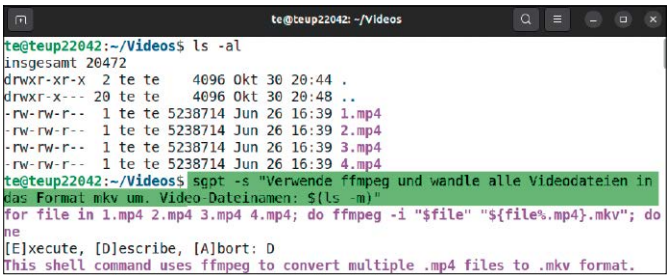
Taste „E“ und Eingabetaste starten den Befehl, Taste „D“ gibt eine Beschreibung aus. Beachten Sie, dass Shell-GPT die Version des Linux-Systems und der verwendeten Shell berücksichtigt. Je nach System kann die Antwort daher unterschiedliche Befehle ausgeben.

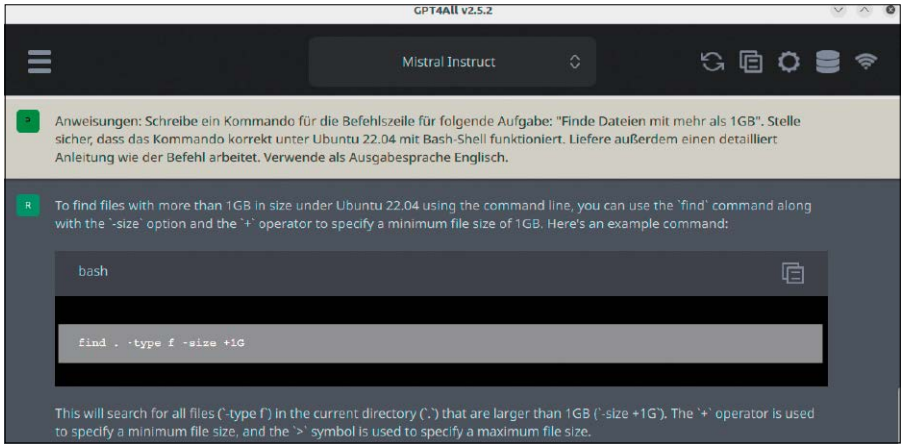
Komplexere Befehlszeilen lassen sich gezielt für bestimmte Dateitypen erstellen. Als Beispiel dient das Verzeichnis „~/Videos“, in dem die Dateien „1.mp4“ bis „4.mp4“ liegen. Die Dateien sollen mit Ffmpeg in das MKV-Dateiformat umgewandelt werden. Die passende Anfrage fällt mit

```
sgpt -s "Verwende ffmpeg und wandle
  alle Videodateien in das Format mkv
  um. Video-Dateinamen: $(ls -m)"
```

in diesem Fall etwas komplizierter aus.

Mehrere Dateien verarbeiten: Shell-GPT versteht Variablen wie „$(ls -m)“ (kommaseparierte Dateiliste) und erstellt eine dazu passende Befehlszeile.





Lokales Modell: Gpt4all arbeitet offline mit einem heruntergeladenen KI-Modell. Die Anfragen müssen ausführlich und präzise sein, damit das Ergebnis zum Linux-System passt.

Tgpt: Befehlszeilen und Bilder erzeugen

Tgpt (*https://github.com/aandrew-me/tgpt*) erlaubt die Nutzung von Chat GPT 3.5 im Terminal und generiert Befehle sowie Bilder. Ein API-Schlüssel ist nicht erforderlich.

Installation: Installieren Sie zuerst Curl, falls noch nicht vorhanden:

```
sudo apt install curl
```

Danach führen Sie diese Befehl aus:

```
curl -sSL https://raw.
  githubusercontent.com/aandrew-
  me/tgpt/main/install | bash -s /
  usr/local/bin
```

Tgpt verwenden: Eine Übersicht mit den Optionen erhalten Sie mit

```
tgpt --help
```

und eine Anfrage formulieren Sie mit

```
tgpt -s "Aktualisiere mein System"
```

Den Start der Befehlszeile bestätigen Sie hier mit Taste Y gefolgt von der Eingabetaste. Mit dem Beispiel

```
tgpt -img "Erstelle Bilder von
  Pinguinen"
```

erstellt Tgpt im aktuellen Verzeichnis einen Ordner mit dem Namen der Anfrage. Darin sind neun Bilder im Webp-Format gespeichert. Der Bildbetrachter von Linux Mint kann die Dateien anzeigen, Ubuntu-Nutzer müssen die Unterstützung mit

```
sudo apt install webp-pixbuf-loader
```

erst installieren. Ein Bildbearbeitungsprogramm wie Gimp kann die Dateien ebenfalls öffnen und auch konvertieren.

Gpt4all: KI mit eigenem Modell verwenden

Gpt4all erwähnen wir hier außerhalb der Konkurrenz. Das Tool verwendet eine grafische Oberfläche und eignet sich für allgemeine KI-Anfragen. Gpt4all generiert auch Befehlszeilen, die man dann kopieren und im Terminal einfügen kann. Gpt4all bietet kostenlose KI-Modelle zum Download an. Ein API-Schlüssel ist nicht erforderlich und man kann das Programm auch ohne Internetverbindung nutzen.

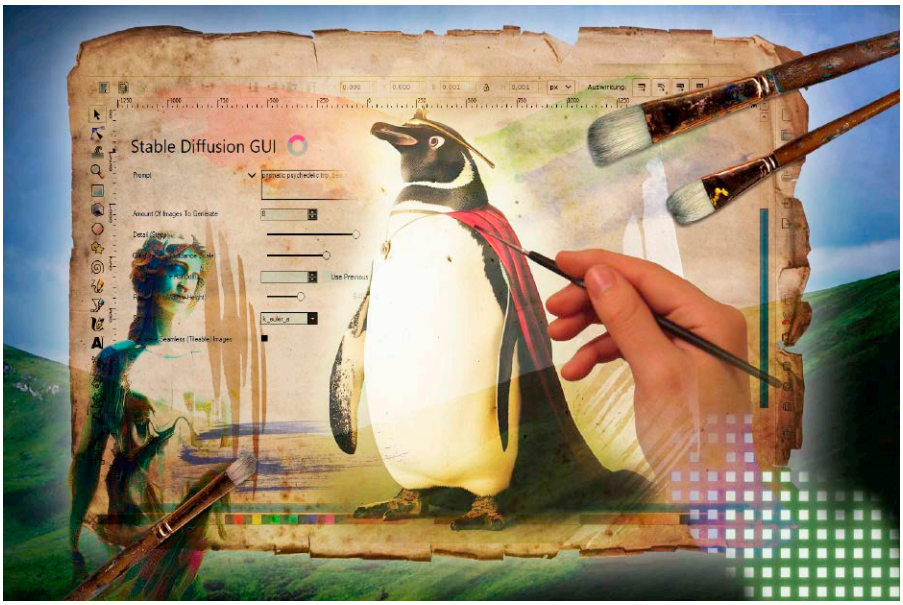
Installation: Unter *https://gpt4all.io* nach gibt es nach einem Klick auf „Ubuntu Installer“ eine „run“-Datei zum Download. Machen Sie diese im Dateimanager ausführbar: Wählen Sie im Kontextmenü „Eigenschaften“ und unter „Zugriffsrechte“ setzen Sie ein Häkchen vor „Datei als Programm ausführen“ (Linux Mint: „Der Datei erlauben sie als Programm auszuführen“).

Erstellen Sie den Ordner „Desktop“ im Home-Verzeichnis, wenn er nicht vorhanden ist. Der Gpt4all-Installer möchte eine Verknüpfung in diesem Ordner erstellen, der auf deutschsprachigem Linux allerdings „Schreibtisch“ heißt. Starten Sie die „run“-Datei per Doppelklick und folgen Sie den Anweisungen. Danach kopieren Sie die „desktop“-Datei von „Desktop“ nach „Schreibtisch“ und starten das Programm über das Desktopicon, das Sie unter Ubuntu über einen rechten Mausklick und „Start erlauben“ ausführbar machen. Bei Linux Mint ist das nicht erforderlich.

Gpt4all verwenden: Beim ersten Start klicken Sie beim Modell „Mistral Instruct“ auf „Download“ (3,8 GB). Ist dieser abgeschlossen, starten Sie Gtp4all neu. Die verfügbaren Modelle unterscheiden sich in Umfang, Geschwindigkeit und Fähigkeiten. Da Gpt4all nichts von Ihrem Betriebssystem weiß, müssen Sie eine Anfrage ausführlicher formulieren (siehe Abbildung). Fordern Sie stets Englisch als Ausgabesprache, sonst übersetzt die KI Shell-Befehle fehlerhaft ins Deutsche (!). ■

KI-Bildgeneratoren

Bildgeneratoren laden zum Experimentieren ein wie kaum ein anderes KI-Thema. Text-zu-Bild-Generatoren gibt es nicht nur mit vorgegebenen Einschränkungen zu Auflösung und Motiven im Web, sondern auch für einen eigenen leistungsstarken PC.

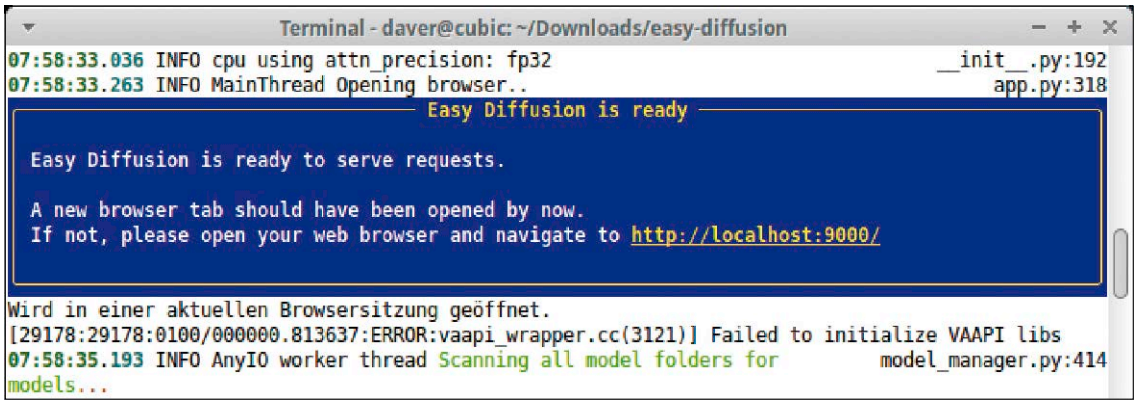


VON DAVID WOLSKI

Es ist kaum zu übersehen, wie viel Aufmerksamkeit allein KI-Bildgeneratoren in den letzten Monaten auf sich gezogen haben. Mit gutem Grund, denn sie demonstrieren die Fortschritte von Deep-Learning-Modellen auf anschauliche und spielerische Weise. Von chaotischen, per neuronalen Netzen erzeugten Zufallsbildern, die Google schon 2015 mit Deep Dream (*https://deepdreamgenerator.com*) einer breiten Öffentlichkeit zugänglich machte, ging die Reise nun zu fast fotorealistischen Abbildungen der Generatoren Dall-E 2 (Open AI), Midjourney (Midjian) oder Dreamstudio (Stable Diffusion). Diese sind die Früchte jahrelanger Entwicklungsarbeiten seit den 60er-Jahren, als das Thema der künstlichen Intelligenz an Universitäten und Forschungsinstituten wie dem MIT erstmals größere Budgets für KI-Forschung erhielt. Die KI-Forschung blieb lange wegen zu kleiner Modelle bei der theoretischen Grundlagenforschung. Der geringe kommerzielle Erfolg von KI außerhalb weniger Nischen zog die Investitionen aus diesem Forschungsbereich in den 80er-Jahren vorerst ab. Weiter ging es erst Ende der 90er, dann aber gleich mit einer KI-Revolution, welche die heutige Entwicklung antreibt: Aus der Verbindung von verbesserten Algorithmen, viel größeren Datensets und wachsender Rechenleistung entstand die KI-Disziplin „Deep Learning" – mehrschichtiges maschinelles Lernen. Dieser Überbegriff beschreibt Techniken, in welchen Computersysteme selbständig Korrelationen und Kausalzusammenhänge aus analysierten Daten ableiten.

Stable Diffusion: Freie Modelle und freie KI

Bis zu zehn Milliarden Rechenoperationen durchläuft ein einziger Datensatz in einem komplexen Deep-Learning-Modell. Die ersten Einsatzfelder fanden sich der biologischen Forschung zum Verhalten von Molekülen und dann in der automatischen Bild- und Audiokorrektur. Denn diese KI-Modelle sind inzwischen sehr gut darin, selbst Inhalte zu generieren, bestehende Muster zu imitieren, weiterzuspinnen und vorherzusagen. Die generative KI nutzt diese Konzepte, um neue Bilder aus Textbeschreibungen oder Vorlagen zu erstellen. Generatoren gibt es mittlerweile nicht nur in der Cloud, sondern auch für den eigenen PC. Vorausgesetzt, dieser bietet genügend Leistung.
Dieser Beitrag stellt zwei Bildgeneratoren vor, welche die freie Software Stable Diffusion nutzen, die an der LMU München von der Forschungsgruppe Compvis mit einigen externen Partnern und der Firma Stabilty AI entwickelt wird. Nicht nur die KI steht unter einer vergleichsweise freizügigen Lizenz, sondern auch die verfügbaren Trainingsdaten: Die gemeinnützige Stiftung LAION (Large-Scale Artificial Intelligence Open Network) hat 2022 eine freie Datenbank mit 5,85 Millionen Bildern und deren Beschreibungen veröffentlicht, mit der Stable Diffusion trainiert ist. Die Datenbank steht unter einer Creative-Commons-Lizenz und enthält die selbst Bilder nicht, jedoch die Beschreibungen und die Links zu den öffentlich aufrufbaren Bildmaterialien im Web.
Das Team hinter Stable Diffusion veröffentlichte den Quellcode der KI-Software zur Bildgenerierung schon 2022 zunächst als Betaversion einem kleineren Forscherkreis, um zwischenzeitlich eine freie Lizenz zu formulieren. Unter den Bedingungen der Lizenz Open Rail steht Stable Diffusion seit August 2022 allen Interessierten offen. Schnell inspirierte der verfügbare Python-Quellcode unabhängige Entwickler, eine lokal installierbare Version für den eigenen Rechner ganz ohne Cloud herauszugeben. Die Motivation dahinter ist die größere Freiheit bei der Generierung von Bildern sowie bei den Motiven selbst. Denn eine



Installation von Easy Diffusion 3.0: Dieser KI-Bildgenerator bietet Linux-Anwendern den einfachsten Einstieg. Der Installer richtet alle notwendigen Komponenten ein.

selbst installierte Version von Stable Diffusion liefert für geduldige Anwender weit mehr Parameter zum Experimentieren. Die mit Stable Diffusion generierten Bilder sind für die meisten privaten und sogar kommerziellen Zwecke frei verwendbar. Es gibt einige detaillierte Einschränkungen in der Nutzung, auf welche der Kasten „Stable Diffusion: Lizenzbedingungen“ eingeht. Anders als in den Cloudinstanzen tragen die Anwender selbst die Verantwortung im Eigenbetrieb von Stable Diffusion.

Was Stable Diffusion kann und wie es sich im Vergleich zu den kommerziellen Mitstreitern schlägt, zeigt ein (englischsprachiges) Onlinedemo unter *https://huggingface.co/spaces/stabilityai/stable-diffusion*, das in der Cloud läuft und recht flott Bilder in geringer Auflösung aus einem eingeschränkten Repertoire produziert. Auf dem eigenen PC gelingt dies ohne diese Einschränkungen und dieser Beitrag zeigt drei Programme als Front-End für Stable Diffusion unter Linux, jeweils mit eigenen Vorteilen und Stärken. Alle haben gemein, dass die Hardwarevoraussetzungen hoch angesetzt sind: Eine aktuelle Grafikkarte (Nvidia oder AMD) mit acht GB VRAM sollte ein Linux-PC für generative KI mitbringen, außerdem mindestens 16 GB Arbeitsspeicher. Diese Voraussetzungen erfüllen nur gut ausgerüstete Gamingboliden.

Easy Diffusion 3.0: Gelungener Einstieg

Stable Diffusion verlangt nach Python und etlichen Python-Modulen. Damit tun sich Linux-Anwender leicht, denn hier fügen sich die benötigten Komponenten gut ein. Eine Installationshilfe als Script liefert dazu das Projekt Easy Diffusion 3.0 (*https://easydiffusion.github.io*), das sehr schnell einsatzbereit ist.

Die Fähigkeiten und die Modelldaten entsprechen dabei jenen von Stable Diffusion 2.1. Eine Besonderheit von Easy Diffusion ist, dass die hohen Hardwareanforderungen kein K.-o.-Kriterium sind, denn es arbeitet notfalls auch mit schnellen CPUs und viel RAM und eignet sich so für erste Versuche. Hohe Auflösungen und eine hohe Detaildichte sind ohne leistungsfähige GPU aber nicht möglich. Die Projektdateien verlangen auf dem System rund 8,8 GB Platz. Es setzt ein Linux-System mit Desktop voraus, obwohl die Oberfläche über einen lokalen Webbrowser zugänglich ist. Zur Installation verlangt Easy Diffusion das Tool Curl, welches in Debian und Ubuntu mit *sudo apt install curl* schnell nachinstalliert ist. Um Python kümmert sich dann das Installations-Script. Dieses liegt auf *https://github.com/easydiffusion/easydiffusion/releases* als „Easy-Diffusion-Linux.zip“. Nach dem Entpacken startet im neu angelegten Verzeichnis der Terminalaufruf

```
./start.sh
```

die weitere Einrichtung, die auch bei flotter Internetverbindung einige wenige Minuten dauert. Nach dem Abschluss startet die Oberfläche von Easy Diffusion in einer automatisch gestarteten Browserinstanz auf der Adresse *http://localhost:9000*.

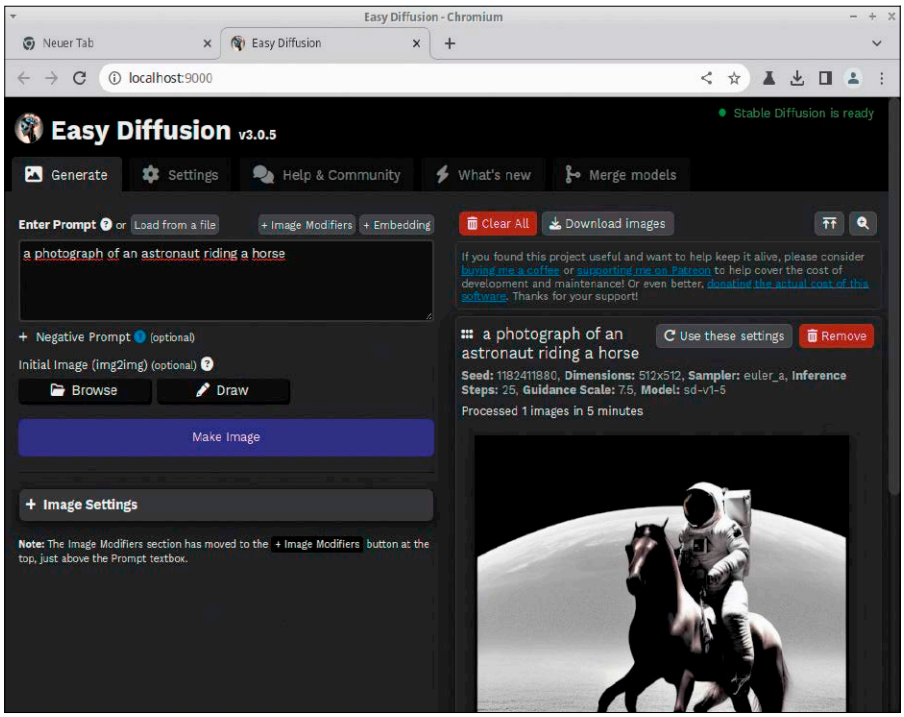
Easy Diffusion bleibt bei den angezeigten Funktionen und Parametern vergleichsweise übersichtlich. Zur KI-Bildgenerierung dient das größere Eingabefeld im Abschnitt „Enter Prompt“, in welche die deutsch- oder englischsprachige Bildbeschreibung kommt. Damit definieren Sie das Motiv, das die KI erzeugen soll. Darunter gibt es das ausklappbare Feld „Negative Prompt“, das Stile, Motivdetails oder Farben aufnimmt, die im Bild explizit nicht vorkommen sollen. Darunter kann mit „Initial Image“ die Textbeschreibung auch mit einem Beispielbild unterlegt werden, um der KI die gewünschte Richtung vorzugeben.

Wichtig und mit den stärksten Auswirkungen auf die zu erwartende Berechnungszeit ist unter „Image Settings“ die Angabe von „Image Size“, welche zunächst mit der mageren Auflösung von 512 × 512 Pixeln arbeitet. Während eine Grafikkarte wie die Nvidia Geforce RTX 4070 diese Größe in wenigen Sekunden berechnet, verlangen hohe Auflösungen schon mal einige Minu-

BESSERE BILDER: TIPPS ZUR SYNTAX

Wer mit Easy Diffusion 3.0 und Automatic1111 AI experimentiert, erkennt schnell: Auf die sorgfältige und nicht zu knappe Bildbeschreibung kommt es an. Damit die Ergebnisse den Erwartungen entsprechen, müssen die Bilder im sogenannten „Prompt“ recht genau und treffend beschrieben werden – in Deutsch oder meist besser in Englisch. Denn mit Englisch kann Stable Diffusion auf einen größeren Satz von Modelldaten zugreifen.

Zu schnellen Erfolgserlebnissen kann die Angabe eines bestimmten Bildstils als zusätzliche Beschreibung verhelfen, so etwa die Eigenschaft „photorealistic“, um fotografieähnliche Resultate zu erhalten. Es können auch Künstlernamen genannt werden. Für unser Aufmacherbild ergänzten wir beispielsweise „painting, in the style of Botticelli“, um einen Pinguin im Stil der Renaissancemalerei zu erhalten.



Der einsteigerfreundliche KI-Bildgenerator hält die Einstellungen schön übersichtlich. Hier gibt es auch die Option, ein bestehendes Bild als Vorlage anzugeben.

ten Geduld. Ohne dezidierte GPU dauert auch die Berechnung der kleineren Auflösungen allein per Core-i7-CPU einige Minuten. Die maximale Bilddimension beträgt 2048 × 2048 Pixel und für solche Größen sind selbst mit leistungsfähiger GPU mehrere Stunden Geduld nötig.

Easy Diffusion erstellt zunächst nur ein Bild nach einem Klick auf „Make Image“ und zeigt links im Feld den Fortschritt an. Um der KI gleich mehrere Ansätze zu gewähren, die oft mit deutlichen Unterschieden ausfallen, dient das Feld „Image Settings → Number of Images“. Im Register „Settings“ gibt es weitere Detaileinstellungen, unter anderem den Filter „Block NSFW images“, welcher anstößiges Bildmaterial über das geladene Modell blockiert.

Automatic1111: Zugriff per LAN

Als anspruchsvolle Bedienoberfläche für Stable Diffusion aus dem Netzwerk ist Automatic1111 gemacht. Die Hardwareanforderungen sind hoch und eine Nvidia-Grafikkarte oder eine AMD-Karte muss vorhanden sein, denn allein mit CPUs arbeitet Automatic1111 generell nicht. Der Vorteil der Oberfläche von Automatic1111: Der Rechenknecht selbst kann sich in einem anderen Raum befinden, zum Zugriff reicht jeder kleine Clientrechner. Der Hostrechner kann aber auch bei einem Cloudunternehmen stehen, um auf diese Weise leistungsfähige Hardware nach Bedarf für wenige Euro anzumieten und nach Nutzungszeit zu bezahlen.

Auch dieser KI-Bildgenerator ist kein pures Front-End, sondern ein Komplettpaket. Er liegt als geradliniger Installer vor, welcher auf dem Linux-Host viele Schritte abnimmt. Wer eine Nvidia-Grafikkarte mit proprietären Treibern hat, kann sofort mit der Installation loslegen: In Debian/Ubuntu holt der Befehl

```
sudo apt install wget git python3
  python3-venv libgl1 libglib2.0-0
```

die Abhängigkeiten und

```
wget -q https://raw.
  githubusercontent.com/
  AUTOMATIC1111/stable-diffusion-
  webui/master/webui.sh
```

lädt das Installations-Script herunter, dass dann mit

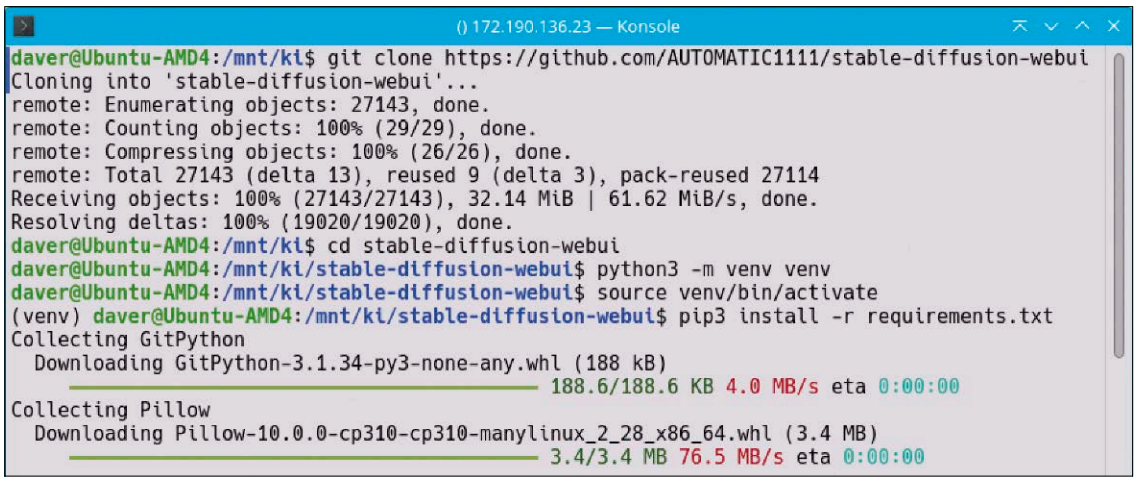
```
bash webui.sh
```

gestartet wird. Das Script fragt gegen Ende auch gleich nach, ob es ein Modell herunterladen soll. Der Installationsprozess ist dann noch länger beschäftigt, denn der Download umfasst 3,5 GB, die sich danach auf rund 12 GB entpacken.

AMD-Grafikkarten: Wer Grafikhardware von AMD einsetzt, muss noch einige Zwischenschritte einlegen, denn Automatic1111 verlangt dann zusätzlich das mächtige KI-Rahmenwerk ROCm von AMD. In Ubuntu 22.04 LTS holt zunächst der Befehl

```
sudo apt install git python3-pip
  python3-venv python3-dev
  libstdc++-12-dev
```

die vorausgesetzten Pakete auf das System. Danach holt



Vorbereitungen für AMD-Grafikkarten: Automatic1111 setzt das Framework ROCm von AMD voraus, das zunächst manuell installiert werden muss.

```
wget https://repo.radeon.com/
  amdgpu-install/5.6/ubuntu/jammy/
  amdgpu-install_5.6.50600-1_all.
  deb
```

das ROCm-Framework von AMD ab und die drei Kommandos

```
sudo dpkg --add-architecture i386
sudo dpkg -i amdgpu-
  install_5.6.50600-1_all.deb
sudo amdgpu-install
  --usecase=graphics,rocm
```

installieren es. Das Rahmenwerk ist sehr umfangreich und verlangt auf der Systempartition rund 16 GB. Mit

```
sudo usermod -aG video $USER
sudo usermod -aG render $USER
```

ist es notwendig, den Benutzer zu zwei neuen Gruppen hinzuzufügen, und danach muss ein Neustart des System erfolgen. Mit

```
git clone https://github.com/
  AUTOMATIC1111/stable-diffusion-
  webui
```

holen Sie dann das Installations-Script für Automatic1111 und

```
cd stable-diffusion-webui
python3 -m venv venv
source venv/bin/activate
```

bereitet die Python-Umgebung vor. Das Kommando

```
pip3 install -r requirements.txt
```

installiert die weiteren Python-Module und

```
pip3 uninstall torch torchvision
pip3 install --pre torch
  torchvision torchaudio --index-
  url https://download.pytorch.org/
  whl/nightly/rocm5.6
```

ersetzt ein Modul mit einer speziell angepassten Variante für AMDs ROCm-Rahmenwerk. Im nächsten Schritt holt

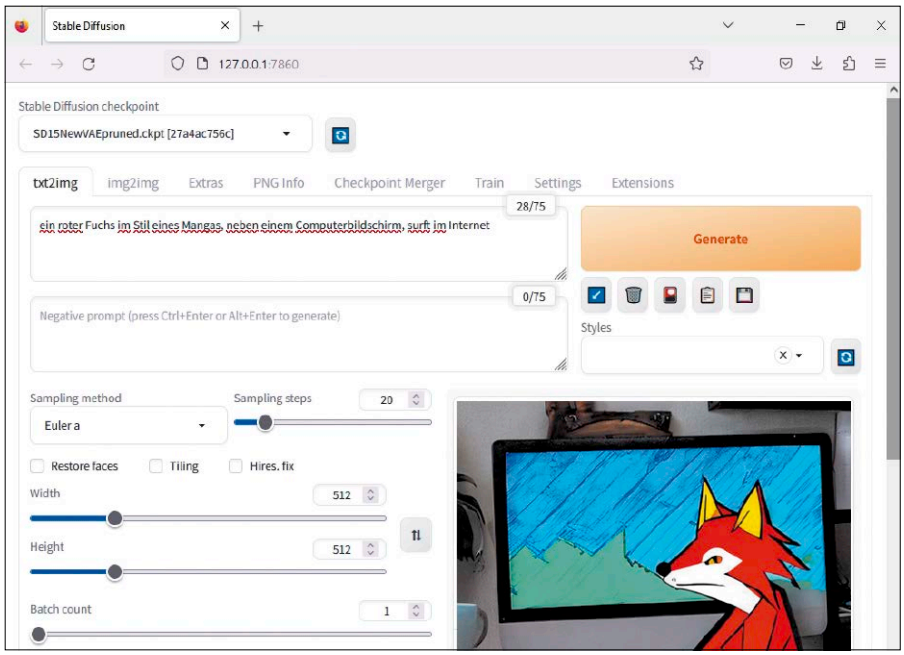
```
wget -O launch.sh https://tinyurl.
  com/27awnm4f
```

das modifizierte Start-Script „launch.sh“ in das aktuelle Verzeichnis. Nach einem Öffnen mit einem Texteditor muss dort die letzte Zeile, welche mit „python3 launch.py“ beginnt, am Ende noch mit den Startparametern „--skip-torch-cuda-test --precision full --no-half“ für AMD-Karten ergänzt werden. Im letzten Schritt ruft

```
bash launch.sh
```

das Script auf, um die Installation abzuschließen. Die Weboberfläche wird nach dem Download der Modelle automatisch gestartet. Auf dem gleichen PC, der Automatic1111 ausführt, öffnet dann in einem (beliebigen) Browser die URL

```
http://0.0.0.0:7860
```



Viele Optionen für Fortgeschrittene: Wer mehr Optionen zur Feinabstimmung wünscht, findet diese bei Automatic1111, um beispielsweise den Bildstil mit der „Sampling method“ zu beeinflussen.

die Oberfläche. Auf einem anderen Rechner im Netz dient stattdessen die Adresse „http://[IP-Adresse]:7860“ zum Aufruf, wobei der Platzhalter „[IP-Adresse]“ der IPv4-Nummer des Hosts entspricht. Port 7860 muss zudem in einer eventuell laufenden Firewall wie UFW oder Firewalld als eingehender Port erlaubt sein.

Die Weboberfläche zeigt oben links das verwendete Modell im Feld „Stable Diffusion Checkpoint“ an. Das Feld „txt2img“ darunter nimmt die Beschreibung auf (Deutsch oder Englisch), wie das Resultat aussehen soll. Ein Klick auf „Generate“ beginnt mit der Berechnung. Zur Verbesserung der Resultate kann der Schieberegler „CFG Scale“ vorgeben, wie nah sich die KI an die Bildbeschreibung halten soll. Je genauer und ausführlicher diese ist, desto höher kann dieser Wert ausfallen. Mit den „Sampling Steps“ ist die Präzision der Berechnung von Bilddetails einstellbar und die Vorgabe von 25 ist ein Kompromiss zwischen Rechenzeit und Darstellungsqualität. Auf leistungsfähigen Grafikkarten verbessern höhere Werte die Qualität. Diese Detaileinstellungen machen Automatic1111 zu einem Bildgenerator für experimentierfreudige Anwender, erhöhen aber im Vergleich zu Easy Diffusion die Rechenzeit noch erheblich. ■

STABLE DIFFUSION: LIZENZBEDINGUNGEN

Die von Stable Diffusion erzeugten Grafiken sind in Hinblick auf die Lizenz vielseitig einsetzbar. Die Trainingsdaten hinter Stable Diffusion und die KI-Software selbst erlauben die Nutzung der Ergebnisse nicht nur für private Zwecke. Auch eine kommerzielle Verwertung ist nach der verwendeten Lizenz „Creative ML Open RAIL-M“ (*https://huggingface.co/spaces/CompVis/stable-diffusion-license*) völlig in Ordnung. Es handelt sich aber um keine traditionelle freie Lizenz im Sinne von Open-Source-Software, denn es gibt durchaus Einschränkungen. Nicht erlaubt ist laut dem Lizenztext der Einsatz zum Verstoß gegen örtliches geltendes Recht. Auch die Erstellung von Falschinformationen, mit dem Ziel andere zu schaden, ist nicht erlaubt, genauso wenig die Erstellung diskriminierender ober beleidigender Inhalte. Auch medizinische Beratung, Strafverfolgung durch Profiling und juristische Beratungen gehören zu den verbotenen Einsatzfeldern für die Grafiken, welche die hier vorgestellten Programme mit Stable Diffusion erzeugen.

Bildbearbeitung mit KI

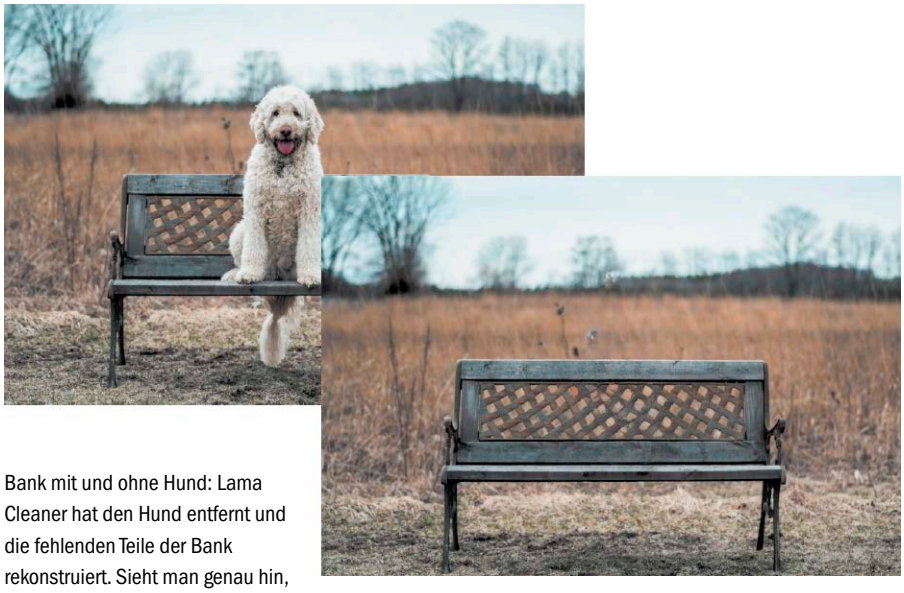
Einige Aufgaben bei der Bildbearbeitung sind besonders zeitintensiv. Es sind oft etliche Arbeitsschritte nötig, etwa um störende Elemente zu entfernen oder Objekte freizustellen. Per KI lässt sich das deutlich beschleunigen.

VON THORSTEN EGGELING

Das Tool Lama Cleaner (*https://github.com/Sanster/lama-cleaner*) kann dank künstlicher Intelligenz bei der Bildbearbeitung helfen. Es ist ein Spezialist für Inpainting, wobei Bilder so bearbeitet werden, dass der Betrachter die Änderungen nicht erkennt. Sie können beispielsweise unerwünschte Objekte aus Bildern löschen – der Hintergrund wird passend rekonstruiert.

Lama Cleaner ist keine einfache Ein-Klick-Lösung. Aufgrund der Komplexität der Aufgabe muss man geeignete Bilder oder Bildausschnitte wählen und sich für ein passendes KI-Modell entscheiden. Nicht immer sind die Ergebnisse wie gewünscht, Verbesserungen erfordern mehrere Anpassungen und Versuche. Hat man die optimalen Einstellungen gefunden, liefert Lama Cleaner erstaunliche Ergebnisse.

Tipp: Wer Lama Cleaner erst einmal ausprobieren möchte, findet eine Onlineversion unter *https://huggingface.co/spaces/Sanster/Lama-Cleaner-lama*.



© Quelle: https://unsplash.com/@overture_creations

Bank mit und ohne Hund: Lama Cleaner hat den Hund entfernt und die fehlenden Teile der Bank rekonstruiert. Sieht man genau hin, gibt es einige Unregelmäßigkeiten, die aber kaum auffallen.

Lama Cleaner installieren

Für eine optimale Geschwindigkeit benötigt Lama Cleaner einen Nvidia-Grafikchip (GPU) mit passendem Treiber. Falls noch nicht geschehen, installieren Sie den Treiber unter Ubuntu (Gnome) über „Aktivitäten“ und einer Suche nach „Zusätzliche Treiber“.

Bei Linux Mint führt der Weg über das Menü „Systemverwaltung → Treiberverwaltung“. Eine schnelle Grafikkarte mit möglichst viel RAM verbessert die Leistung. Wenn der Speicher nicht ausreicht, können Sie nur mit kleinen Bildern arbeiten. Das Gleiche gilt, wenn Lama Cleaner nur die CPU verwendet, was außerdem deutlich langsamer ist.

Wir empfehlen, das Python-Tool Lama Cleaner nur für den aktuell angemeldeten Benutzer zu installieren. Dadurch lassen sich Konflikte mit vorhandenen Python-Bibliotheken vermeiden. Zur Vorbereitung führen Sie die folgenden zwei Terminalbefehle aus:

```
mkdir ~/.local/bin
source ~/.profile
```

Damit nehmen Sie „.local/bin“ in die Variable „$PATH“ auf, was Fehlermeldungen bei der Installation vermeidet. Die nötigen Programme kann dann der Package Installer for Python (pip) einrichten. Installieren Sie das Tool unter Ubuntu/Linux Mint mit

```
sudo apt install python3-pip
```

Lama Cleaner lässt sich jetzt mit den zwei Befehlen

```
pip install --user
  torch==1.13.1+cu117 --extra-
  index-url https://download.
  pytorch.org/whl/cu117
pip install --user lama-cleaner
```

installieren. Wenn Sie keine Nvidia-GPU nutzen, lassen Sie die erste Zeile weg. Starten Sie dann das Programm:

```
lama-cleaner --model=lama
  --device=cuda --port=8080
```

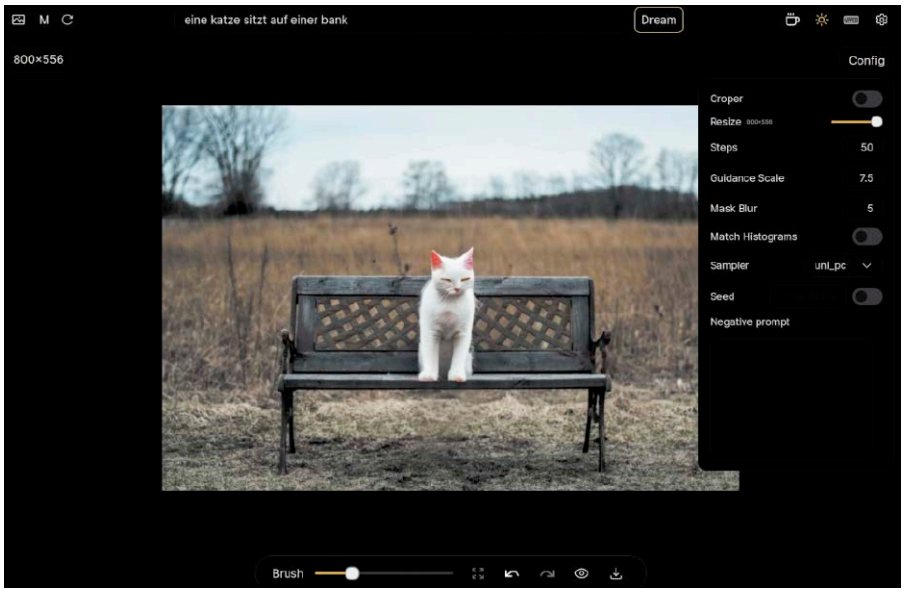
Ohne Nvidia-Grafik ersetzen Sie „cuda“ durch „cpu“. Beim ersten Start lädt Lama Cleaner das angegebene KI-Model „lama“ herunter, was einige Zeit dauern kann.

Objekte mit Lama Cleaner entfernen

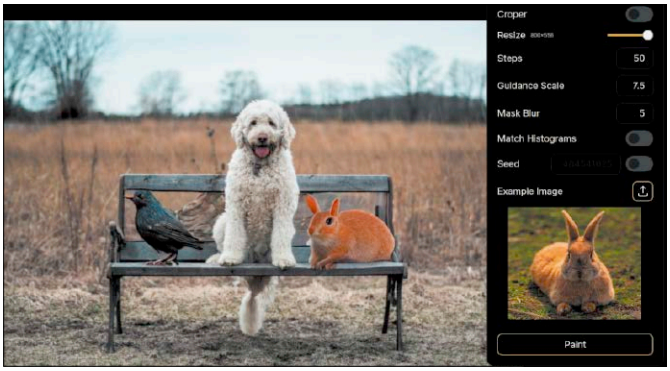
Öffnen Sie im Webbrowser die URL *http://localhost:8080*. Die Oberfläche ist sehr übersichtlich. Fahren Sie mit der Maus in die Mitte des Fensters und klicken Sie in das gelbe Feld. Es öffnet sich der Dialog „File upload“ und damit wählen Sie eine Bilddatei aus. Der Mauszeiger über dem Bild besteht aus einem gelben Kreis, dessen Größe sich mit dem Regler hinter „Brush“ anpassen lässt.

Halten Sie den linken Mauszeiger gedrückt und zeichnen Sie eine gelbe Fläche über den Bereich, den Sie entfernen möchten. Der muss nicht exakt sein, sollte das Objekt aber ungefähr abdecken. Wenn Sie den Mauszeiger loslassen, wird das Objekt entfernt und der Hintergrund ergänzt. Sollte Lama Cleaner nicht alles komplett entfernen, wiederholen Sie den Vorgang für die betroffenen Bereiche. Das erste Bild dieses Beitrags zeigt links einen Hund auf einer Bank, im rechten Bild hat Lama Cleaner den Hund entfernt. Sieht man genau hin, kann man in der Mitte kleine Unregelmäßigkeiten in der Banklehne erkennen. Die könnten jedoch auch natürlichen Ursprungs sein und fallen kaum auf.

Beim Test mit diesem Bild haben wir den kompletten Hund inklusive Schwanz und einem Teil der Sitzbank in einem Stück markiert. Lama Cleaner hat automatisch erkannt, dass die Sitzbank nicht zum Hund gehört, und auch diesen Teil rekonstruiert. Was hier nur Sekunden dauert, würde bei der manuellen Nachbearbeitung mit dem Kopierpinsel einer Bildverarbeitung längere Zeit beanspruchen.



Objekte ersetzen: Das Model Stable Diffusion baut Elemente gemäß Textbeschreibung in ein Bild ein. Diese spezielle KI-Katze wurde allerdings noch nie in der Natur beobachtet.



Elemente einbauen: Der KI-Hase ist seinem Vorbild nicht ganz ebenbürtig. Durch Auswahl anderer Optionen oder Bilder lässt sich das Ergebnis meist noch verbessern.

Objekte in einem Bild ersetzen

Nun soll eine Katze auf der Bank sitzen? Dafür benötigen Sie das KI-Modell Stable Diffusion. Dabei handelt es sich um eine KI, die aus einer Textbeschreibung ein Bild generieren kann. Lama Cleaner unterstützt vier Modelle, die sich bei der Qualität, den Bildgrößen der Trainingsdaten und bei der Geschwindigkeit unterscheiden. Die Entwickler haben jedoch nicht dokumentiert, für welche Bilder oder Zwecke sich ein bestimmtes Modell besser eignet. Man muss es daher ausprobieren.

Sollte Lama Cleaner laufen, beenden Sie den Prozess im Terminal mit Strg-C. Starten Sie das Programm neu:

```
lama-cleaner --model=sd2
  --device=cuda –port=8080
```

Ersetzen Sie „sd2“ durch den Namen des gewünschten Modells (siehe *https://lama-cleaner-docs.vercel.app/models/stable_diffusion*). Alternativ lässt sich das Modell auch in den Einstellungen (Zahnradsymbol) wechseln, wonach der Download bei Bedarf angestoßen wird.

Laden Sie ein Bild und markieren Sie den gewünschten Bereich, wie im vorherigen Abschnitt beschrieben. In die Eingabezeile ab oberen Fensterrand geben Sie eine Beschreibung für das neue Objekt ein und klicken auf „Dream“. Wir haben es mit „Eine Katze sitzt auf einer Bank“ probiert, um den Hund gegen eine Katze auszutauschen. Anweisungen in deutscher Sprache sind möglich, Englisch führt aber meist zu besseren Ergebnissen.

Bei Tieren wie Menschen ist oft die Gesichtspartie verzerrt. Unternehmen Sie mehrere Versuche, bis Lama Cleaner ein akzeptables Resultat erzeugt.

Elemente zum Bild hinzufügen

Beim Start mit „--model paint_by_example“ fügen Sie ein Modell hinzu, das aus einem Referenzbild einen ähnlichen Inhalt erzeugt. Laden Sie das Originalbild und wählen Sie nach einem Klick auf die Schaltfläche hinter „Example Image“ das Referenzbild. Markieren Sie den Bereich, in den Sie das Element einfügen möchten, und klicken Sie auf „Paint“. Bei unserem Test haben wir zum Hund einen Hasen und einen Vogel gesellt. In der Abbildung sehen Sie, dass Lama Cleaner nicht einfach das Bild des Hasen eingebaut, sondern ihn passend zur Bank ausgerichtet hat. Haltung und Aussehen des Hasen wirken aber etwas unnatürlich. Mit unbelebten Objekten funktioniert das deutlich besser.

Hintergrund eines Bildes entfernen

Der Hintergrund lässt ich über das Plug-in Remove Background entfernen, das Sie mit

```
pip install --user rembg
```

installieren. Starten Sie Lama Cleaner mit der zusätzlichen Option

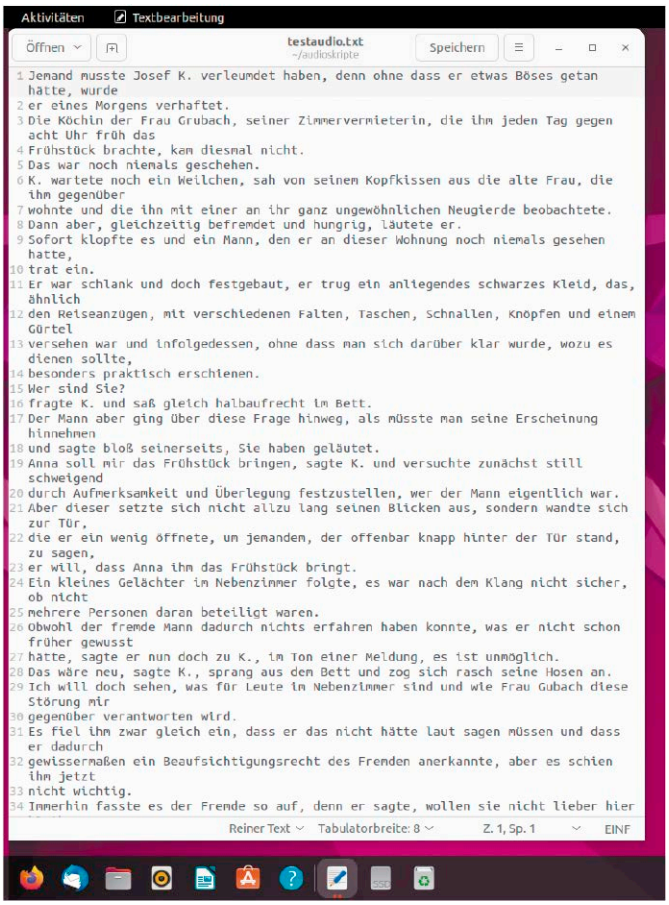
```
--enable-remove-bg
```

neu und laden Sie ein Bild. Klicken Sie auf die neue Schaltfläche auf der linken Seite und dann auf „RemoveBG“. Falls Lama Cleaner zunächst nicht alles entfernt, wiederholen Sie den Vorgang. ■

Whisper wandelt Sprache zu Text

Einen schnellen Rechner vorausgesetzt, wandeln Sie mit dem KI-Programm Whisper die Sprache von Audio- und Filmdateien in geschriebenen Text um. Wir zeigen Ihnen, wie das funktioniert.

VON STEPHAN LAMPRECHT



Toller „Prozess“: Was Whisper hier aus einem Hörbuch als Text extrahiert hat, ist praktisch fehlerlos.

Das Programm Whisper stammt vom Startup Open AI, das mit GPT-3 für Furore sorgt. Die Anwendung ist Open Source und nutzt Python, lässt sich somit auf verschiedenen Plattformen einsetzen. Mit Whisper können Sie Sprache aus Audio- oder Videodateien extrahieren und in verschiedenen Textformaten ausgeben lassen.

Hardware und Software

Wie bei vielen KI-Anwendungen hängen Leistung und Geschwindigkeit auch bei Whisper von der Grafikkarte ab. Damit Sie Ihren Rechner nicht für Stunden lahmlegen, ist es ratsam, die ersten Versuche mit kleinen Dateien zu unternehmen. So können Sie für spätere Projekte besser abschätzen, wie lange Sie für die Spracherkennung benötigen. Auf unserem nicht mehr ganz taufrischen Allroundsystem dauerte die Verarbeitung von einer Filmminute immerhin vier Minuten.

Whisper und Abhängigkeiten installieren: Die meisten Linux-Distributionen installieren Python standardmäßig. Sie benötigen aber noch zwei zusätzliche Anwendungen, die Sie mit

```
sudo apt install ffmpeg git
```

installieren. Wenn Sie sich schon einmal mit Python beschäftigt haben, wissen Sie, dass verschiedene Projekte völlig unterschiedliche Module und Komponenten benötigen. Teilweise widersprechen sich diese auch. Deswegen sollte Whisper besser in einer eigenen Umgebung laufen. Das ist schnell eingerichtet. Sollte eine der Voraussetzungen nicht vorhanden sein, informiert Sie die Paketverwaltung der Distribution darüber. Legen Sie in Ihrem Home-Verzeichnis einen Ordner an, in dem Whisper installiert werden soll. In unserem Beispiel wurde der Ordner „audioskripte“ genannt. Wechseln Sie in einem Terminal in dieses Verzeichnis. Mit

```
python3 -m venv whisperenv
```

legen Sie in diesem Ordner nun eine virtuelle Python-Umgebung unter Ubuntu an und mittels des Befehls

```
source whisperenv/bin/activate
```

aktivieren Sie diese Umgebung. Der große Vorteil: Alles, was Sie jetzt installieren, landet in dieser Umgebung und kommt nicht mit anderen Python-Projekten in Konflikt. Die Eingabeaufforderung zeigt Ihnen auch bereits, dass Sie sich in einer solchen Umgebung befinden. Wenn Sie diese wieder verlassen wollen, um Python anderweitig zu nutzen, verlassen Sie die Umgebung mit „deactivate“. Mittels der Modulverwaltung von Python installieren Sie jetzt Whisper:

```
pip3 install git+https://github.
  com/openai/whisper.git
```

Die eingerichtete Python-Umgebung ist nur im Terminal aktiv – starten Sie das System also neu, muss die Umgebung wieder aktiviert werden.

Ersten Text transkribieren

Damit haben Sie alle Vorbereitungen abgeschlossen und können an die erste Transkription gehen. Legen Sie die Datei, die Sie bearbeiten wollen, in dem Ordner ab, in dem Sie auch die Umgebung von Whisper eingerichtet haben. Mit

```
whisper [Datei]
```

starten Sie die Bearbeitung. Whisper lädt dann zunächst ein Sprachmodell herunter, versucht in den ersten 30 Sekunden die Sprache zu ermitteln und beginnt dann seine Arbeit. Den Fortschritt können Sie im Terminal verfolgen. Ist die Erkennung beendet, liegen anschließend fünf verschiedene Dateien vor: In der TXT-Datei befindet sich der reine Text. Die Dateien TSV, SRT und VTT enthalten zusätzliche Zeitmarken. Beide Formate sind unter Filmexperten bekannt, da sie als Untertitelformate in Schnittprogrammen oder auf Plattformen wie Youtube genutzt werden können. Die JSON-Datei ist das Protokoll der Bearbeitung. Darin ist nicht allein der erkannte Text gespeichert, sondern zusätzliche Informationen zum Erkennungsvorgang.

In diesem Testlauf wurde ein bekannter literarischer Text verwendet. Wie nicht anders zu erwarten war, zeigte Whisper hier keinerlei Schwächen. Doch auch bei einer Datei, die die ersten beiden vorgelesenen Seiten einer Bedienungsanleitung eines Geschirrspülers enthielt, war die Erkennungsrate beim Modell „medium“ schon sehr gut. Letztlich hängt das Ergebnis natürlich auch vom Ausgangsmaterial ab. Bei einem Podcast oder Interview, bei dem es geordnet zugeht, sich die Sprecher also abwechseln und es eine gute Aufnahmequalität gibt, ist der Aufwand für die Nachbearbeitung gering. Bei einer Filmsequenz mit verschiedenen Stimmen, Differenzen in der Lautstärke und Nebengeräuschen werden Sie stärker nachbessern müssen.

Sprachmodell ändern und Erkennung steuern

Wenn Sie Whisper, wie in unserem Beispiel, ohne Argumente gestartet haben, nutzt die Anwendung ein einfacheres Sprachmodell. Dafür ist es, in Abhängigkeit Ihrer Internetverbindung, auch recht schnell heruntergeladen. Auch die Verarbeitung selbst ist recht zügig. Für durchschnittlich anspruchsvolle Texte in deutscher Sprache sollten Sie das Modell „medium“ verwenden. Hier gilt allerdings auch: Je größer das Sprachmodell, umso mehr Platz belegt es auf der Festplatte und umso länger dauert die Erkennung. Die Sprachmodelle legt Whisper im versteckten Verzeichnis „./cache“ im Home-Ordner ab. Wenn Sie die Anwendung später wieder deinstallieren, sollten Sie zusätzlich diesen Ordner manuell leeren.

Ein bestimmtes Sprachmodell fordern Sie mit dem Parameter „--model'[name]'“. Zur Verfügung stehen die Modelle tiny, base, small, medium, large, large-v2. Für „large“ und „large-v2“ brauchen Sie sehr viel Zeit oder einen sehr schnellen Grafikchip mit wenigstens 10 GB VRAM. Mit dem optionalen Schalter „--model_dir“, der eine Pfadangabe erwartet, definieren Sie auf Wunsch ein abweichendes Verzeichnis für die Speicherung der Sprachmodelle. Das kann nützlich sein, wenn Sie von anderen Instanzen auf die Dateien zugreifen wollen.

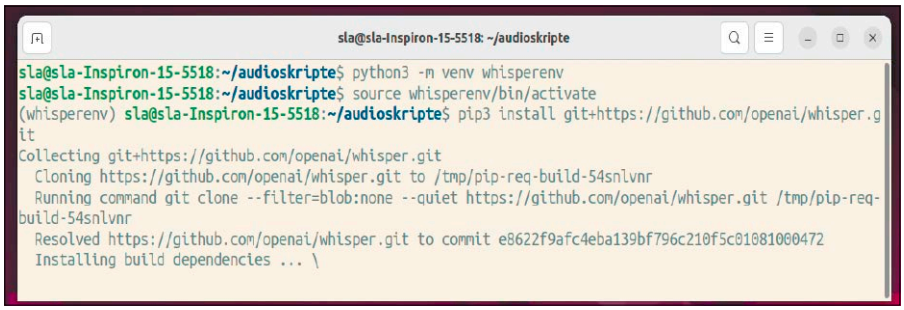
Zudem können Sie der Anwendung die Arbeit erleichtern, wenn Sie vorab die verwendete Sprache als Parameter übergeben. Das übernimmt der Schalter

```
--language 'de'
```

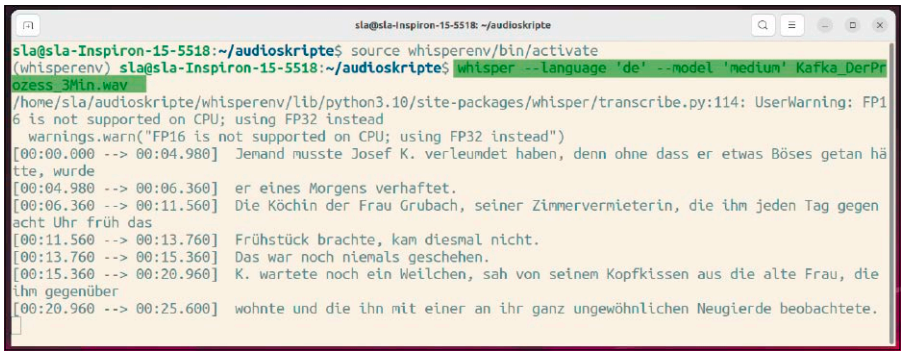
Geht es Ihnen bei der Spracherkennung in erster Linie um die Verschriftlichung eines gesprochenen Textes wie eines Vortrags oder eines Gesprächs, dann benötigen Sie die Untertiteldateien nicht. Mit „--output_format“ legen Sie bei Bedarf das gewünschte Zielformat oder Zielformate fest. In angesprochenen Fall dürfte „txt“ ausreichen.

Wenn Sie Whisper häufiger einsetzen, ist es sinnvoll, sich die Funktionsaufrufe und Parameter in einem Alias oder kleinen Script zu speichern, um Tipparbeit zu sparen. Wenn Sie sich mit dem Schalter „--help“ alle Argumente und Schalter ansehen, die Whisper versteht, finden Sie dort auch die Option, einen erkannten Text gleich automatisch zu übersetzen. Im direkten Vergleich mit Deepl oder auch Libretranslate sind Whisper-Übersetzungen allerdings hölzern. Die Leser werden Sinn und Kernaussagen vermutlich verstehen, aber es empfiehlt sich, einen erkannten Text separat von einem Spezialwerkzeug übersetzen zu lassen.

Whisper liefert jedenfalls ab dem Sprachmodell „Medium“ hervorragende Erkennungsraten. Mit seinen größeren Modellen müssen Sie selbst bei Satzzeichen kaum noch nachbearbeiten. ■



Wenn Sie für Whisper eine eigene Python-Umgebung einrichten, vermeiden Sie Konflikte mit anderen Python-Projekten. Die Installation selbst erfolgt durch Downloads von Github.



Beim Whisper-Start können Sie ein bestimmtes Sprachmodell fordern und festlegen, dass Sie lediglich den Text oder ein anderes Format benötigen.

Wireguard-VPN: Schnell und sicher

Per VPN lassen sich Daten sicher durchs Internet transportieren und man kann aus der Ferne auf die Geräte im heimischen Netzwerk zugreifen. Mit Wireguard lässt sich ein VPN besonders komfortabel einrichten.

VON THORSTEN EGGELING

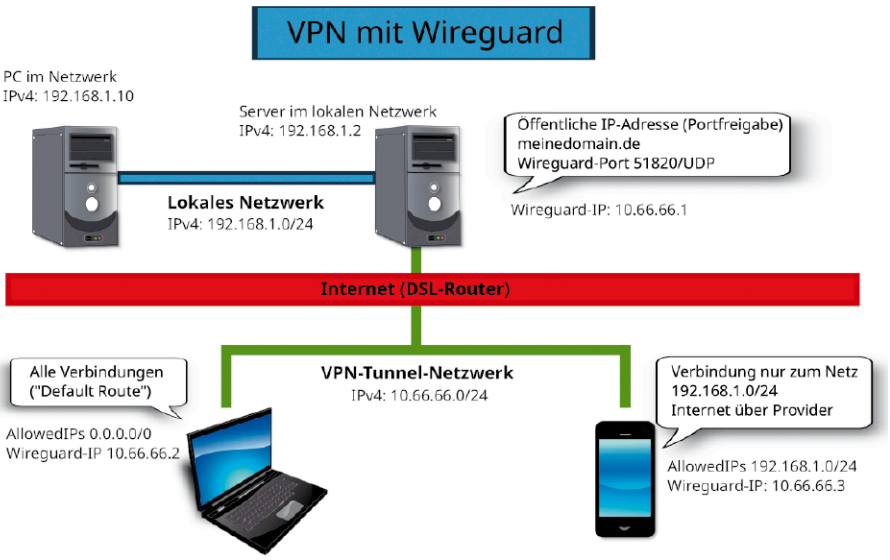
Wireguard ist eine VPN-Software (Virtual Private Network), die schnellen Aufbau der Verbindung und effiziente Datenübertragung bietet. Per VPN lassen sich zwei Netzwerke miteinander verbinden. Die Technik kann man für den sicheren Zugriff auf das heimische Netzwerk verwenden, beispielsweise um am Urlaubsort Smarthome-Geräte zu steuern oder auf Netzwerkressourcen zuzugreifen. Außerdem lässt sich der komplette Internetverkehr über das VPN leiten: Gleich an welchem Ort der Welt sieht es dann so aus, als ob Sie zu Hause vor dem Gerät sitzen. Streamingdienste oder Mediatheken, die im Ausland gesperrt sind („Geoblocking"), arbeiten ohne Einschränkungen. In fremden WLANs sorgt VPN für Sicherheit, weil der gesamte Datenverkehr verschlüsselt wird.

Wir beschreiben, wie sich Wireguard als Server einrichten lässt und wie die Clientkonfiguration dafür aussieht. Wir beschreiben nur die Konfiguration für IPv4, wofür eine öffentliche IPv4-Adresse vom Provider erforderlich ist. Information zur IPv6-Konfiguration finden Sie über *http://bit.ly/3ELasWq*.

Wer eine Fritzbox mit Fritz-OS ab Version 7.50 besitzt, kann direkt zu Punkt 5 springen und Wireguard im Router aktivieren.

1. Wireguard installieren

Wir gehen bei unserem Konfigurationsbeispiel davon aus, dass in Ihrem Netzwerk ein Linux-PC mit Ubuntu 22.04 oder Linux Mint 21 läuft, der auch als VPN-Server dienen soll. Clients, also Geräte, die sich per VPN mit Ihrem Netzwerk verbinden sollen, können unter Linux oder Windows (*www.wireguard.com/install*) laufen. Die Clientsoftware ist außerdem für Android (*http://bit.ly/3ZvbeyN*) und iOS (*http://bit.ly/41vjzEp*) verfügbar.



So funktioniert Wireguard: Die Clients erhalten Wireguard-IPs für die Kommunikation über den VPN-Tunnel. „AllowedIPs" regelt den Zugriff auf das Heimnetzwerk oder Internet.

Die Installation gelingt am schnellsten über ein Script (*https://github.com/angristan/wireguard-install*), das Sie herunterladen und starten. Führen Sie im Terminal die folgenden drei Befehle aus:

```
curl -O https://raw.
 githubusercontent.com/angristan/
 wireguard-install/master/
 wireguard-install.sh
chmod +x wireguard-install.sh
sudo ./wireguard-install.sh
```

Sollte das Tool curl nicht vorhanden sein, installieren Sie es über das gleichnamige Paket. Das Script fragt die Optionen der Konfiguration nacheinander ab. In der Regel müssen Sie nur mit Eingabetaste bestätigen. Ein Beispiel sehen Sie in der Abbildung auf der nächsten Seite, Erklärungen lesen Sie im nächsten Punkt. Kontrollieren Sie in einem zweiten Terminal mit

```
ip a
```

die IP-Adresse sowie die Bezeichnung des Netzwerkadapters und passen Sie gegebenenfalls an, was das Script automatisch erkannt hat. Bei „Server Wireguard port" haben wir den Wert „51820" eingetragen, weil dies der Standardport ist.

Das Script richtet im letzten Schritt die erforderlichen Zusatzpakete ein. Die Serverkonfiguration wird unter „/etc/wireguard/wg0.conf" gespeichert.

Danach geht es mit der Konfiguration des ersten Clients weiter. Vergeben Sie eine ID, beispielsweise „01", und bestätigen Sie die Optionen jeweils mit der Eingabetaste. Die Konfigurationsdatei für Linux oder Windows

liegt in Ihrem Home-Verzeichnis, beispielsweise mit dem Namen „wg0-client-01.conf“. Die Länge des Dateinamens (ohne Extension) darf maximal 15 Zeichen betragen. Sonst akzeptiert Wireguard die Datei nicht.

Um weitere Clients zu konfigurieren, starten Sie das Script erneut. Tippen Sie „1“ („Add a new user“) ein und bestätigen Sie mit der Eingabetaste. Die IP-Adressen werden automatisch erzeugt, Sie können die Werte einfach übernehmen.

Router konfigurieren und dynamische DNS: Wenn Ihr Internetanbieter keine feste IP-Adresse liefert, verwenden Sie einen Anbieter für dynamische IP-Adressen. Kostenlos sind beispielsweise *https://freedns.afraid.org* oder *www.noip.com*. Fritzbox-Nutzer können *https://myfritz.net* nutzen. Im Router muss außerdem eine Weiterleitungsregel („Port forwarding“) für den Port „51820“ auf den Server-PC eingerichtet sein (siehe *www.pcwelt.de/1086581*).

2. Konfiguration für den Server

Die Datei „/etc/wireguard/wg0.conf“ enthält den Abschnitt „[Interface]“ mit der Konfiguration des Wireguard-Servers. Hinter „Address“ steht die interne IP-Adresse für das VPN „10.66.66.1/24“. In diesem Adressraum findet die Kommunikation mit den Clients statt. „ListenPort“ legt den Port fest, auf dem Wireguard eingehende Verbindungen erwartet. „PrivateKey“ ist der Sicherheitsschlüssel des Servers, mit dem sich prüfen lässt, ob ein Client zum Verbindungsaufbau berechtigt ist. Danach folgen mehrere Zeilen mit „PostUp“ und „PostDown“, die über iptables-Regeln die Durchleitung der Pakete zwischen dem Wireguard-Interface („wg0“) und dem Netzwerkadapter festlegen.

Im Abschnitt „[Peer]“ wird der Server mit den Clients bekannt gemacht. Hinter „PublicKey“ steht der öffentliche Schlüssel des Clients, der für den Verbindungsaufbau nötig ist. „PresharedKey“ ist ein zusätzliches Sicherheitsmerkmal und beim Server und Client identisch. „AllowedIPs“ enthält die IP-Adressen im Wireguard-Tunnel, die der Client verwenden darf, beispielsweise „10.66.66.2/32“. In eigenen „[Peer]“-Abschnitten für weitere Clients wird die Adresse hochgezählt, etwa „10.66.66.3/32“, „10.66.66.4/32“ und so weiter.

Alle IP-Adressen müssen bei Wireguard im CIDR-Format (Classless Inter-Domain Routing) angegeben werden. Einen Umrechner finden Sie unter *www.ipaddressguide.com/cidr*. „/32“ ergibt nur genau die IP „10.66.66.2“. „10.66.66.1/24“ unter „[Interface]“ umfasst den gesamten Bereich von „10.66.66.0“ bis „10.66.66.255“.

Wireguard-Server einrichten: Das Script „wireguard-install.sh“ installiert die nötigen Softwarepakete und fragt die Einstellungen ab. In der Regel können Sie die Vorgaben übernehmen.

```
te@UB5: ~/Downloads
te@UB5:~$ cd Downloads/
te@UB5:~/Downloads$ sudo ./wireguard-install.sh
Welcome to the WireGuard installer!
The git repository is available at: https://github.com/angristan/wireguard-insta
ll

I need to ask you a few questions before starting the setup.
You can keep the default options and just press enter if you are ok with them.

IPv4 or IPv6 public address: 192.168.1.48
Public interface: enp0s3
WireGuard interface name: wg0
Server WireGuard IPv4: 10.66.66.1
Server WireGuard IPv6: fd42:42:42::1
Server WireGuard port [1-65535]: 51820
First DNS resolver to use for the clients: 8.8.8.8
Second DNS resolver to use for the clients (optional): 8.8.4.4
```

```
wg0.conf (/etc/wireguard)
Datei  Bearbeiten  Ansicht  Suchen  Werkzeuge  Dokumente  Hilfe
Erhöhte Berechtigungen
wg0.conf
[Interface]
Address = 10.66.66.1/24,fd42:42:42::1/64
ListenPort = 51820
PrivateKey = 0LjcJDkmctnBQlO0HbaL1lqBuAJPUt5jfrGltqG8sEs=
PostUp = iptables -I INPUT -p udp --dport 51820 -j ACCEPT
PostUp = iptables -I FORWARD -i enp0s3 -o wg0 -j ACCEPT
PostUp = iptables -I FORWARD -i wg0 -j ACCEPT
PostUp = iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
PostUp = ip6tables -I FORWARD -i wg0 -j ACCEPT
PostUp = ip6tables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
PostDown = iptables -D INPUT -p udp --dport 51820 -j ACCEPT
PostDown = iptables -D FORWARD -i enp0s3 -o wg0 -j ACCEPT
PostDown = iptables -D FORWARD -i wg0 -j ACCEPT
PostDown = iptables -t nat -D POSTROUTING -o enp0s3 -j MASQUERADE
PostDown = ip6tables -D FORWARD -i wg0 -j ACCEPT
PostDown = ip6tables -t nat -D POSTROUTING -o enp0s3 -j MASQUERADE

### Client 01
[Peer]
PublicKey = z61bs0j9RKSVSwPnUgn0gSkjJUzg510o+Bhjfn5roz4=
PresharedKey = VHcPa/+R/AAwOeTTsY43qr2WAxuH8iEGbv7VSBnZsYw=
AllowedIPs = 10.66.66.2/32,fd42:42:42::2/128
Einfacher Text  Leerzeichen: 4  Z. 28, Sp. 45  EINF
```

Serverkonfiguration: Die Konfigurationsdatei enthält die Werte für Server und Clients. Die Befehle hinter „PostUp“ und „PostDown“ sorgen für die Weiterleitung der Datenpakete.

3. Konfiguration für den Client

Die Datei „wg0-client-01.conf“ sieht ähnlich aus wie die Konfigurationsdatei beim Server. Unter „[Interface]“ stehen der „PrivateKey“ des Clients und die IP-Adresse. Hinter „DNS“ hat das Script öffentliche DNS-Server von Cloudflare eingetragen. Sie können auch andere IPs verwenden, beispielsweise den öffentlichen DNS-Server „8.8.8.8“ von Google. Oder Sie tragen die DNS-Server des Internetproviders ein, den der Wireguard-Server verwendet.

Im Abschnitt „[Peer]“ steht der „PublicKey“ des Clients und der mit dem Server gemeinsam genutzte „PresharedKey“. Hinter „AllowedIPs“ sind die IP-Bereiche konfiguriert, die durch den Wireguard-Tunnel befördert werden. Bei „0.0.0.0/0“ läuft der gesamte Internetverkehr über das VPN. Steht hier „192.168.1.0/24“, dann kann der Client nur auf Geräte im lokalen Netzwerk des Servers zugreifen, alle anderen Zugriffe laufen über die aktuelle Internetverbindung des Clients. Der Adressbereich muss zum Netzwerk passen, beispielsweise „192.168.178.0/24“ bei der Standardkonfiguration einer Fritzbox.

Die Adresse hinter „Endpoint“ verweist auf die IP-Adresse und Port des Servers im lokalen Netzwerk. Das funktioniert so nicht, weil der Server unter dieser IP über das Internet nicht erreichbar ist. Tragen Sie für einen ersten Test die öffentliche IP des Routers ein, die Sie beispielsweise über *www.whatsmyip.org* herausfinden. Oder Sie konfigurieren gleich einen Anbieter für dynamisches DNS.

Aktivieren Sie im Router außerdem die Portweiterleitung auf die interne IP und den Port des Wireguard-Servers.

Für das Smartphone erzeugen Sie mit

```
qrencode -o conf.png < ~/wg0-
  client-01.conf
```

einen passenden QR-Code.

Grafischer Helfer: Wireguird kann VPN-Verbindungen aufbauen und beenden, wofür root-Recht erforderlich ist. Außerdem lässt sich die Konfiguration bearbeiten.

4. Client für Wireguard einrichten

Auf einem anderen PC, der als Client dienen soll, installieren Sie im Terminal die nötige Software mit

```
sudo apt install wireguard
 resolvconf
```

Kopieren Sie die angepasste Datei „wg0-client-01.conf“ vom Server in den Ordner „/etc/wireguard“ (als root) und ändern Sie die Zugriffsrechte (drei Zeilen):

```
sudo chown root:root /etc/
 wireguard/wg0-client-01.conf
sudo chmod 644 /etc/wireguard/wg0-
 client-01.conf
sudo chmod 755 /etc/wireguard
```

Starten Sie die Verbindung:

```
sudo wg-quick up /etc/wireguard/
 wg0-client-01.conf
```

Der Aufbau der Verbindung lässt sich mit

```
sudo wg show
```

prüfen. Hinter „transfer:“ sehen Sie, viel viele Daten übertragen und empfangen wurden. Beenden Sie die VPN-Verbindung folgendermaßen:

```
wg-quick down /etc/wireguard/wg0-
 client-01.conf
```

Für einen ausführlichen Test müssen Sie die Verbindung in einem anderen Netzwerk aufbauen. *www.whatsmyip.org* meldet ohne VPN die öffentliche IP des aktuellen Netzwerks und mit aktiviertem VPN die IP des Heimnetzwerks.

Für tägliche Nutzung ist eine grafische Oberfläche zur Steuerung von Wireguard wünschenswert. Der Netzwerkmanager ab Ubuntu 20.04 unterstützt Wireguard nur unvollständig, denn Wireguard-Verbindungen lassen sich nur über einen Umweg aktivieren und deaktivieren. Die Konfigurationsdatei importieren Sie im Terminal mit

```
nmcli connection import type
 wireguard file /etc/wireguard/
 wg0-client-01.conf
```

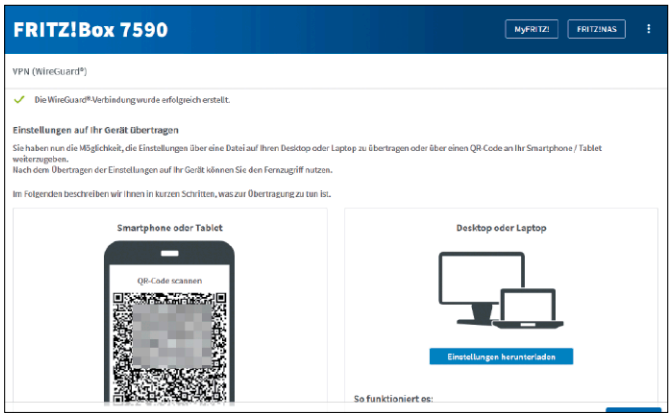
Die Verbindung wird damit sofort aktiviert. Mit dem Befehl

```
nm-connection-editor
```

können Sie die Konfiguration bearbeiten. Unter „Allgemein“ entfernen Sie das Häkchen vor „Automatisch mit Priorität verbinden“. Mit Hilfe von

```
nmtui-connect
```

lässt sich die VPN-Verbindung über eine einfache grafische Oberfläche manuell beenden oder starten.



Wireguard mit der Fritzbox: Die Serverkonfiguration ist mit wenigen Mausklicks erledigt. Die Clientkonfiguration laden Sie herunter und kopieren die Datei nach „/etc/wireg“.

Wireguird (*https://github.com/UnnoTed/wireguird*) bietet sich als Alternative an. Unter „Releases“ wird ein DEB-Paket für die Installation angeboten. Das Tool berücksichtigt vorhandene Konfigurationen unter „/etc/wireguard“, über „Add Tunnel“ lassen sich Konfigurationsdateien importieren.

Nutzer von Linux Mint können auch ein Leistenapplet verwenden. Klicken Sie die Leiste am unteren Rand des Bildschirms mit der rechten Maustaste an und gehen Sie auf „Applets“. Klicken Sie auf „Herunterladen“, suchen Sie nach „Wireguard“ und klicken Sie auf die Schaltfläche am rechten Rand der Zeile. Wechseln Sie zu „Verwalten“ und klicken Sie auf die „+“-Schaltflächen. Nach einem Klick auf das neue Leisten-Applet lässt sich die Wireguard-Verbindung aktivieren.

Wireguird und das Mint-Applet fordern bei jeder Aktion administrative Rechte, die Sie mit Ihrem Passwort bestätigen müssen. Die Netzwerkmanager-Tools kommen auch ohne erhöhte Rechte aus.

5. Fritzbox als Wireguard-Server

Fritz-OS unterstützt Wireguard ab Version 7.50. Falls noch nicht vorhanden, richten Sie über die Fritzbox-Oberfläche unter „Internet → MyFritz!-Konto“ zuerst ein Myfritz-Konto ein. Alternativ stellen Sie unter „Internet → Freigaben → DynDNS“ einen anderen Anbieter ein.

Gehen Sie auf den Punkt „Internet → Freigaben → VPN (WireGuard)“. Hier klicken Sie auf „Verbindung hinzufügen“, belassen Sie die Option „Vereinfachte Einrichtung“ und klicken auf „Weiter“. Geben Sie der neuen Konfiguration eine aussagekräftige Bezeichnung, beispielsweise „Notebook“, und klicken Sie auf „Fertigstellen“.

Danach sehen Sie einen QR-Code für Smartphones oder Tablets, nach einem Klick auf „Einstellungen herunterladen“ speichern Sie die Konfigurationsdatei für PCs. Speichern Sie die Einstellungen sofort, denn später lässt sich diese Seite nicht mehr aufrufen. Verwenden Sie die Konfigurationsdatei auf dem Client-PC wie in Punkt 4 beschrieben.

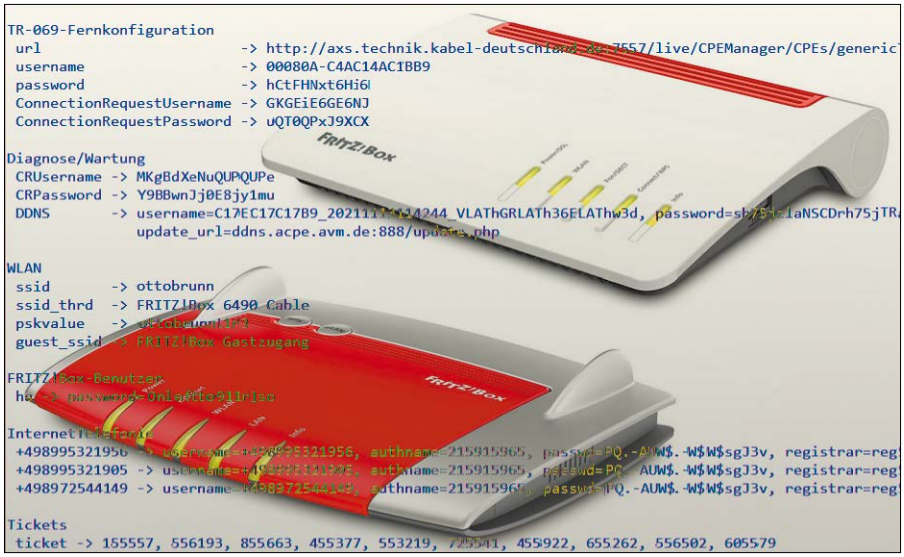
Die Fritzbox konfiguriert „AllowedIPs = 192.168.178.0/24,0.0.0.0/0“ was den Zugang zum Fritzbox-Netzwerk ermöglicht und den gesamten Internetverkehr über das VPN leitet.

Wenn Sie nur das Heimnetzwerk benötigen, lassen Sie „0.0.0.0/0“ weg. ■

Fritzbox per Kommandozeile

Wie lautet gleich wieder das Kennwort für das Gast-WLAN? Mit wem hat meine Frau gestern so lange telefoniert? Router wie die Fritzbox verwalten so viele Infos, geben sie aber nur her, wenn man sich durch die Konfigurationsoberfläche klickt. Oder?

VON HERMANN APFELBÖCK



Definition und Umfang

Die Fritzbox-Tools sind eine umfangreiche Sammlung von PHP-Scripts, die über Terminalbefehle ausgelöst werden. Je nach Befehl kann man Informationen aus der Fritzbox auslesen, Konfigurationsbackups anlegen und wieder zurückschreiben und viele Einzelfunktionen von außen starten, so etwa Smarthome-Aktoren von AVM oder die LED-Anzeige der Fritzbox.

Um Missverständnissen vorzubeugen: Die Fritzbox-Tools können – mit einigen wenigen Ausnahmen – nicht mehr als das, was ein zutrittsberechtigter Fritzbox-Nutzer im Normalfall auf der Konfigurationsoberfläche erledigt. Ihre Reichweite ist sogar begrenzter als die Fritzbox-Oberfläche, weil AVM nicht alle Funktionen für PHP-Scripting offenlegt (so offenbar der gesamte Bereich WLAN/Funknetz). Der entscheidende Vorteil der Fritzbox-Tools ist es, dass Informationen wie die öffentliche IP-Adresse, die aktuelle Anrufliste oder der Onlinezähler mit einem vorbereiteten Terminalbefehl in zwei Sekunden ausgelesen sind. Und mehr noch: Als Terminalbefehl lassen sich solche Aktionen auch automatisch erledigen, etwa als Cronjob oder Autostart auf einem beliebigen Linux-System im Netzwerk.

Einfache Installation auf Debian/Ubuntu

Die Fritzbox-Tools laufen im Prinzip auf jedem Betriebssystem. Weil aber PHP installiert sein muss, ist die Einrichtung auf Linux am einfachsten. Auf jedem updategepflegten Linux wird eine PHP-Version 7.x für die Konsole („cli“) nämlich bereits vorliegen. Außerdem gibt es mindestens eine interessante Funktion der Tools, die Open SSL benötigt – und auch dies ist Standard unter Linux. Für Debian/Ubuntu-basierte Distributionen genügt daher der Download des winzigen DEB-Pakets „fb-tools.deb“ von *www.mengelke.de/Projekte/FritzBox-Tools* (nur 90 KB) und die Installation per Doppelklick oder im Terminal:

```
sudo dpkg -i fb-tools.deb
```

Für Linux-affine Windows-Nutzer ist genau derselbe Weg zu empfehlen, sofern sie ein Debian oder Ubuntu im „Windows Subsystem für Linux“ (WSL) verwenden. Dies ist wesentlich einfacher, als der Anleitung für die Installation unter Windows zu folgen.

Erste Umschau: Auf den typischen Hilfeschalter „-h“

```
fb_tools -h
```

meldet die Toolsammlung die verfügbaren Hauptbefehle (Modes). Einige dieser Befehle besitzen wieder diverse Unterbefehle (Funktionen), wovon Sie sich mit

```
fb_tools konfig -h
fb_tools smarthome -h
```

überzeugen können.

Es gibt nun einige einfache Modes (ohne Unterbefehle), die ohne jede Benutzerauthentifizierung sofort Antworten liefern:

```
fb_tools boxinfo
fb_tools systemstatus
```

Damit erhalten Sie die Basisdaten über Modell, Hardwarerevision, Provider, Laufzeit, Neustarts. Ebenfalls selbsterklärend ist die Abfrage der öffentlichen IP-Adresse:

```
fb_tools getip
```

Bei anderen Modes wie „traffic, anrufliste, led, konfig, smarthome“ werden Sie hingegen keinen Erfolg haben. Das Tool meldet dann „Anmeldung fehlgeschlagen, SID.lua ist ungültig“. Das bedeutet, dass Sie sich für diese Modes und Funktionen an der Fritzbox anmelden müssen.

Anmeldung und Fritzbox-Einstellung

Alle wirklich interessanten Funktionen setzen eine Anmeldung voraus.

Die verläuft aber denkbar einfach innerhalb des Kommandos:

```
fb_tools Geh3im@fritz.box
 anrufliste
```

Dies genügt, falls der Router nur durch ein allgemeines Passwort geschützt ist. Wenn Sie in der Fritzbox Benutzerkonten angelegt haben, benötigen Sie folgende Syntax

```
fb_tools sepp:Geh3im@fritz.box
 anrufliste
```

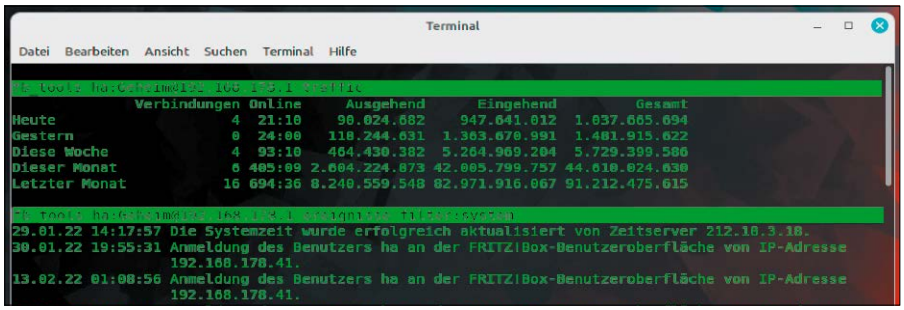
mit der Abfolge „[Konto:Kennwort@Gerät]“. Und noch ein akademisches Detail: Wer sich in mehreren Netzen befindet, muss den angesprochenen Router statt mit „fritz.box“ genau adressieren (was aber auch sonst nie schadet):

```
fb_tools sepp:Geh3im@192.168.178.1
 anrufliste
```

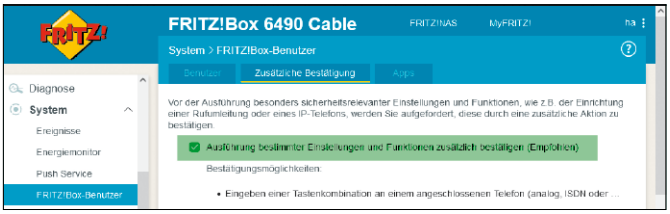
Mit dieser Syntax und somit korrekter Anmeldung sind aber auf jüngeren Fritzboxen immer noch nicht sämtliche Funktionen realisierbar. Die Lösung dafür liegt in der Fritzbox-Konfiguration unter „System → Fritz!Box-Benutzer → Zusätzliche Bestätigung → Ausführung bestimmter Einstellungen und Funktionen zusätzlich bestätigen“. Die Option ist standardmäßig aktiviert und verhindert einige Kommandos der Fritzbox-Tools.

Es ist Ermessensfrage, ob man dies dauerhaft abschalten will. Zumindest vorübergehend ist das nötig, um einen der interessantesten Befehle abzusetzen:

```
fb_tools sepp:Geh3im@192.168.178.1
 konfig export-decrypt
```



Fritzbox-Abfragen: Der Einblick in das Systemprotokoll und die Trafficstatistik („Online-Zähler“) gehört zu einfacheren Kommandos der Fritzbox-Tools.



Etliche Funktionen sind trotz korrekter Anmeldung mit den Fritzbox-Tools nicht erreichbar. Verursacher ist diese Einstellung in der Fritzbox-Konfiguration.

Dieses Kommando liest im Klartext sämtliche Verbindungsdaten aus, unter anderem Provider-Zugangsdaten, WLAN-Passwörter, Telefoniepasswörter, Internet- und Myfritz-Onlinezugangsdaten. Diese Daten sind in dieser Form und Vollständigkeit weder über die Fritzbox-Oberfläche noch in der (verschlüsselten) Konfigurationssicherung erreichbar.

Weitere Beispiele

Mit dem Mode „konfig“ können Sie interaktiv oder automatisiert Konfgurationssicherungen des Routers ausführen:

```
fb_tools sepp:Geh3im@192.168.178.1
 konfig export fritz.export
```

Mit „konfig import“ lässt sich eine Sicherung später wieder zurückspeichern.

Der einfache Mode „traffic“ hat keine Unterfunktionen und spuckt nach

```
fb_tools [...] traffic
```

die Zusammenfassung aus, die in der Konfigurationsoberfläche unter „Internet →Online-Monitor → Online-Zähler“ zu finden ist.

Der Mode „Ereignisse“ bietet das Systemprotokoll („System → Ereignisse“) und hat dabei genau dieselben optionalen Filter wie die Oberfläche:

```
fb_tools [...] ereignisse
 filter:system
```

Einfache, aber mindestens im zweiten Fall interessante Aktionen lösen folgende Kommandos aus:

```
fb_tools [...] led off
fb_tools [...] reconnect
```

Die LED-Leuchten lassen sich mit „on“ jederzeit wieder aktivieren. Das unkomplizierte „reconnect“ darf als weiteres Highlight der Toolsammlung gelten, weil die Fritzbox-Oberfläche diese Option unter „Internet → Online-Monitor → Neu verbinden“ gut versteckt. Dass ein „reconnect“ die Fritzbox tatsächlich in Sekunden neu verbindet, können Sie anschließend dem Systemprotokoll entnehmen (unter „System → Ereignisse“ oder mit dem „ereignisse“-Kommando der fb_tools).

Besonders ergiebig ist der Mode „SmartHome“, der mit

```
fb_tools sepp:Geh3im@192.168.178.1
 smarthome list
```

alle Smarthome-Komponenten („Aktoren“) mit AIN-Kennziffer anzeigt (AIN=Aktor Identifikationsnummer). Einschränkend ist zu bemerken, dass solche Steuerung eine homogene und ausschließliche Nutzung von AVM-Produkten voraussetzt. Da der Verfasser solche Funksteckdosen und Sensoren nicht nutzt, vertrauen wir an dieser Stelle auf Aussagen des Toolentwicklers und von Kommentaren im Web.

Auf Basis der mit „smarthome list“ ermittelten Gerätekennungen lässt sich die betreffende Hardware dann detailliert steuern: Ein AVM-Thermostat mit der AIN „18“ kann dann etwa mit folgendem Befehl

```
fb_tools [...] smarthome set 18 20
```

auf exakt 20 Grad gesetzt werden oder mit

```
fb_tools [...] smarthome set 18 spar
```

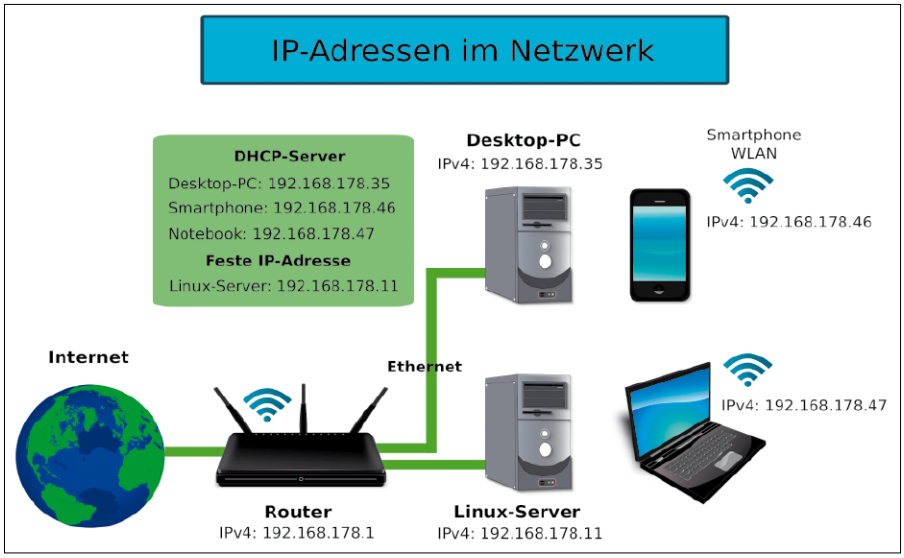
auf eine in der Fritzbox (unter „Smart Home → Geräteverwaltung“) hinterlegte Spartemperatur. ■

IP-Adressen und Gerätenamen

Für die Fehlersuche im Netzwerk, aber auch für die Serverkonfiguration sind Grundkenntnisse der Netzwerkfunktionen hilfreich. Der Artikel bietet die wichtigsten Grundlagen rund um IP-Adressen und Namensauflösung.

VON THORSTEN EGGELING

Im heimischen Netzwerk geschieht das Meiste automatisch. WLAN-Verbindung herstellen oder Ethernet-Kabel anschließen und fertig. Die Infrastruktur, mit dem DSL-Router oder Kabelmodem im Zentrum, ermöglicht die Verbindung aller Geräte zum Internet. Die Situation ändert sich, wenn man Serverdienste im Netzwerk betreiben möchte, etwa Freigaben für den Transfer von Dateien, Webserver, SSH-Server oder Multimedia-Server. Im optimalen Fall kann man den Aufwand gering halten, wenn alle Geräte immer über ihre Namen oder IP-Adressen erreichbar sind. Das funktioniert jedoch oft nicht zuverlässig, weshalb man sich dann mit den IP-Adressen befassen muss. Was Sie dazu wissen müssen und wie sich ein Linux-Server sinnvoll und funktionssicher konfigurieren lässt, erfahren Sie in diesem Artikel.



Netzwerkstruktur: IP-Adressen vergibt im Heimnetzwerk der DHCP-Server im Router automatisch und dynamisch. Für Server sollte man jedoch eine feste IP festlegen.

1. IPv4-Adressen im lokalen Netzwerk

Jedes Gerät im Netzwerk benötigt eine eindeutige IP-Adresse. In der Regel werden zwei zugewiesen: Eine IPv4- und eine IPv6-Adresse. Da es weltweit nicht genügend IPv4-Adressen gibt (etwa 4,3 Milliarden), bekommt nur der Router eine öffentliche IPv4-Adresse, bei einigen Internetanbietern sogar nur eine öffentliche IPv6-Adresse. Zum Schutz der Privatsphäre weisen die Provider dem Router regelmäßig eine neue IPv4-Adresse zu. Mit welcher öffentlichen IP man gerade im Internet erscheint, lässt sich beispielsweise auf *https://ipv6-test.com* prüfen.

Die für den Nutzer wesentlich wichtigeren lokalen IP-Adressen werden standardmäßig vom Heimrouter verteilt – per DHCP (Dynamic Host Configuration Protocol, siehe Punkt 4). Die für private Netzwerke verfügbaren Adressen sind in RFC 1918 (Request For Comment, *https://datatracker.ietf.org/doc/html/rfc1918*) festgelegt. Typisch sind beispielsweise 192.168.178.1 oder 192.168.0.1. Die letzte Ziffer im Bereich von 1 bis 254 steht – ähnlich wie eine Hausnummer – für das jeweilige Gerät. Die ersten drei Zifferngruppen repräsentieren das gesamte Netzwerk und müssen bei allen heimischen Netzwerkgeräten identisch sein. Sonst ist keine Verbindung möglich, weder zum DSL-Router noch zu anderen Geräten im Netzwerk. Mit einer „1“ am Ende ist in der Regel der DSL-Router konfiguriert, 192.168.178.35 erhält dann zum Beispiel der Desktop-PC, 192.168.178.47 das Notebook.

Die genannten lokalen IP-Nummern sind nur im lokalen Netzwerk gültig und lassen sich nicht im Internet nutzen. Es ist Aufgabe des Routers, die Internetanfragen einzelner Geräte über NAT (Network Address Translation) umzusetzen und mit der öffentlichen IP zu versenden. Die Antworten aus dem öffentlichen Netz werden dann wieder an die richtige lokale IP-Adresse geschickt.

2. Besonderheiten bei IPv6-Adressen

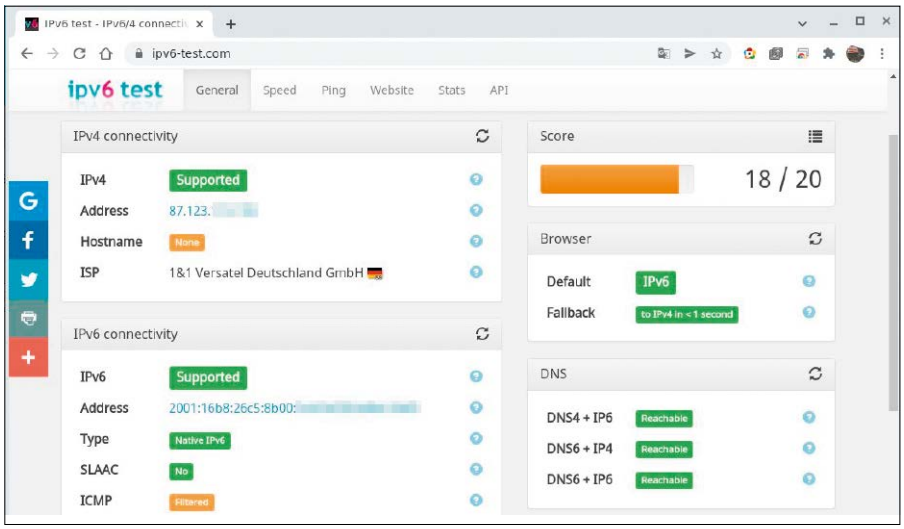
Diese Adressen sind komplizierter aufgebaut, dafür sind davon genügend für (zur Zeit) jedes einzelne Gerät auf der Welt vorhanden (340 Sextillionen, 2 hoch 128). Die

ersten vier durch Doppelpunkt getrennten Blöcke kennzeichnen das Präfix und die Subnetz-ID, die der Router den Geräten vorgibt. Dieser Teil der Adresse ändert sich per Zuweisung durch den Internetanbieter regelmäßig. Die letzten vier Böcke enthalten die Interface-ID, die jeder Rechner selbst generiert. Die resultierende IPv6-Adresse sieht dann beispielsweise so aus:

```
2001:16a9:2731:3100:b7cd:640:6d01
 :c9a2
```

Wenn zwischen zwei Doppelpunkten nichts steht, bedeutet das „0“. Führende Nullen werden ebenfalls weggelassen.

Jedes Gerät verwendet die eigene IPv6-Adresse als öffentliche IP im Internet. Damit keine eindeutige Identifizierung möglich ist, erzeugen die Betriebssysteme regelmäßig eine zufällige Interface-ID (IPv6 Privacy Extensions). Im lokalen Netzwerk spielt das auch für Server keine Rolle, da die IPv4-Adressen ausreichen, um alle Geräte im Netzwerk zu erreichen. Anders sieht es aus, wenn man auf den Server über das Internet von außen auch über IPv6 zugreifen will (siehe Punkt 7).



Wie ist meine öffentliche IP? Auf *https://ipv6-test.com* kann man die WAN-IPv4 des Routers ermitteln und die IPv6-Fähigkeiten prüfen. Die IPv6-Adresse gehört zum Rechner.

3. Das eigene Netzwerk analysieren

Für die Netzwerkkonfiguration ist unter Ubuntu und Linux Mint der Network-Manager zuständig. Bei Ubuntu gehen Sie in den „Einstellungen“ auf „Netzwerk“ oder „WLAN“, Nutzer von Linux Mint gehen im Startmenü auf „Einstellungen → Netzwerk“ und dann auf „WLAN“ oder „Kabelgebunden“. Über die Schaltfläche mit dem Zahnradsymbol gelangt man jeweils zu den Netzwerkeinstellungen.

Die Übersichtseite unter „Informationen“ (Linux Mint: „Details“) liefert die wichtigsten Infos. Angezeigt werden die Verbindungsgeschwindigkeit sowie die IPv4- und IPv6-Adresse. Beide müssen aus dem IP-Bereich des Routers (siehe Punkt 4) stammen, damit eine Verbindung möglich ist. Wenn die IPv6-Adresse mit „fe80“ beginnt, handelt es sich um eine Link-Lokale-Adresse. In diesem Fall hat der Rechner keine IPv6-Adresse erhalten, weil die Funktion im Router abgeschaltet ist oder der Provider kein IPv6 bietet. Die IP hinter „Vorgabestrecke“ (Gateway) ist mit der des Routers identisch, hinter „DNS“ steht ebenfalls die Router-IP oder die IP eines DNS-Servers (Domain Name System) im Internet.

NETZWERKKONFIGURATION BEI UBUNTU SERVER

Ubuntu Server verwendet eine andere Konfiguration als die Desktopversion. Statt dem Network-Manager kommt Netplan zum Einsatz. Die zentrale Konfigurationsdatei ist „/etc/netplan/00-installer-config.yaml“. Standardmäßig ist darin nur DHCP für IPv4 aktiviert. Ändern Sie die Konfiguration entsprechend der Abbildung. Achten Sie auf die exakten Einrückungen der Blöcke mit Leerzeichen. Im Editor nano können Sie sich die Leerzeichen über Alt-P als Punkt anzeigen lassen.

Unsere Beispielkonfiguration stellt die feste IPv4-Adresse „192.168.178.10“ für die Netzwerkschnittstelle „enp0s3“ ein und legt als Gateway sowie Nameserver die Fritzbox fest. Passen Sie die Werte für Ihr Netzwerk an. IPv6 wird über DHCP konfiguriert. Wenden Sie die geänderte Konfiguration mit

```
sudo netplan try --timeout 90
```

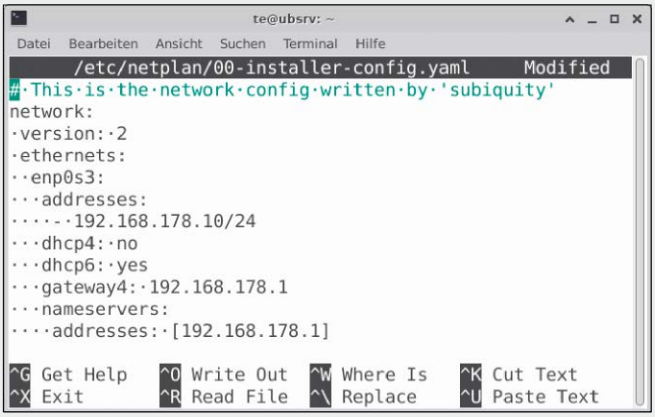
an und prüfen Sie die korrekte Funktion. Nach 90 Sekunden werden die vorherigen Einstellungen wiederhergestellt. Über

```
sudo netplan apply
```

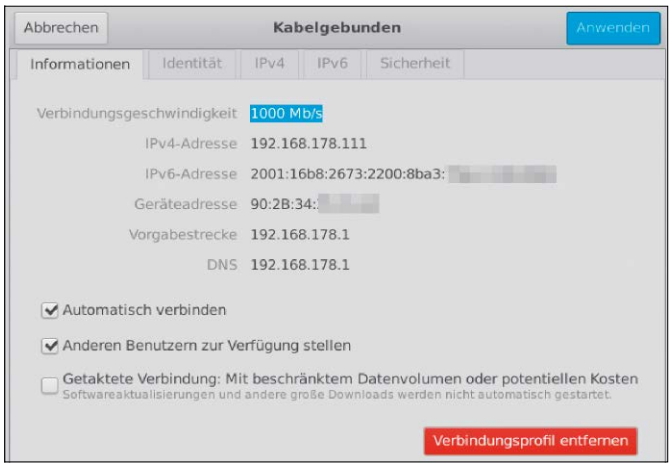
lässt sich die Konfiguration dauerhaft anwenden. Ubuntu Server verwendet keine Privacy Extensions, die IPv6-Adresse bleibt somit gleich. Wer eine zufällige Interface-ID benötigt, ergänzt die Zeile

```
ipv6-privacy: true
```

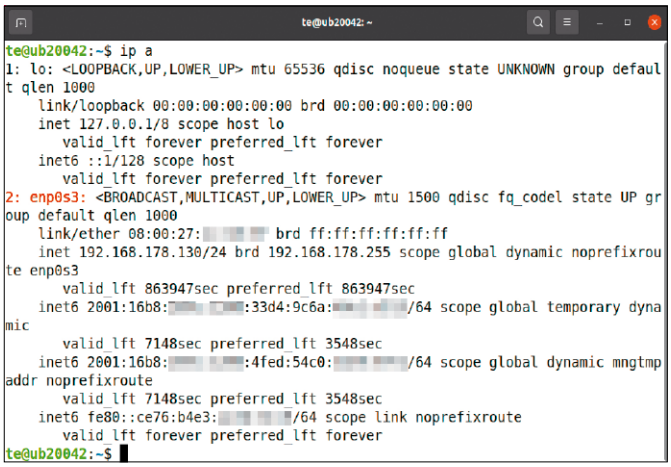
direkt unter „dhcp6: yes“.



Serverkonfiguration: In der Netplan-Konfigurationsdatei „00-installer-config.yaml“ legt man bei Ubuntu Server eine statische IPv4-Adresse fest. Achten Sie auf die korrekten Einrückungen.



Aktuelle Konfiguration prüfen: Die Infoseite der Netzwerkeinstellungen zeigt die wichtigsten Daten, unter anderem die IPv4- und IPv6-Adresse, die Vorgabestrecke (Gateway) und den DNS-Server.



Adaptercheck im Terminal: Der Befehl „ip a“ gibt Informationen zu allen Netzwerkadaptern aus. Hinter „inet“ steht die IPv4-Adresse, hinter „inet6“ erfährt man die IPv6-Adressen.

Tools für das Terminal: Der Network-Manager lässt sich auch über die Kommandozeile abfragen. Der Befehl

```
nmcli
```

ohne weitere Parameter liefert einen Teil der zuvor erwähnten Informationen der grafischen Oberfläche und gibt zusätzlich den Gerätenamen aus, beispielsweise „enp0s3“ für eine Ethernet-Verbindung. Mit

```
nmcli device show [Gerätename]
```

ermitteln Sie alle verfügbaren Informationen inklusive der DNS-Server. Wer nur wissen möchte, welche Adressen zu den Netzwerkadaptern gehören, verwendet den folgenden Befehl:

```
ip a
```

Es werden Gerätenamen und mehrere IPv6-Adressen angezeigt, von denen aber nur die erste für die Internetverbindung genutzt wird.

4. DHCP-Server prüfen und konfigurieren

Alles, was ein Gerät über das Netzwerk wissen muss, erfährt es vom Router über DHCP (Dynamic Host Configuration Protocol). Beim Systemstart sendet jedes Gerät (DHCP-Client) eine Rundsendenachricht in das Netzwerk und der DHCP-Server (Router) antwortet mit den erforderlichen Daten. Die Identifikation eines Clients erfolgt anhand der weltweit eindeutigen Geräteadresse des Netzwerkadapters (MAC, Media Access Control). Dem Client kann daher beim nächsten Start die gleiche IP zugewiesen werden. Die Adresse bleibt jedoch nur für einen im Router festgelegten Zeitraum reserviert. War ein Gerät über diesen Zeitraum inaktiv, wird beim Start eine neue IPv4 vergeben.

Wie der DHCP-Server konfiguriert ist, erfahren Sie in der Benutzeroberfläche des Routers. Sie erreichen diese im Webbrowser über seine IP-Adresse, bei einer Fritzbox auch über *http://fritz.box*. Wo die Einstellungen genau zu finden sind, entnehmen Sie der Dokumentation zum Router. Bei einer Fritzbox beispielsweise sind die DHCP-Einstellungen unter „Heimnetz → Netzwerk“ nach Klicks auf „Netzwerkeinstellungen“ und „IPv4-Einstellungen“ zu sehen. Klicken Sie links unten auf „Ansicht: Standard“, um zur erweiterten Ansicht zu wechseln. Sonst sind nicht alle Optionen sichtbar.

Vor „DHCP-Server aktivieren“ ist ein Häkchen gesetzt, darunter lässt sich der Adressbereich festlegen. Der Standard ist 192.168.178.20 bis 192.168.178.200. Die Bereiche 192.168.178.2 bis 192.168.178.19 sowie 192.168.178.201 bis 192.168.178.254 können daher für eigene statische IP-Adressen verwendet werden (siehe Punkt 6). Hinter „Gültigkeit“ lässt sich angeben, wie lange eine IP-Adresse reserviert bleibt. Für ein Heimnetz sind die voreingestellten zehn Tage in Ordnung. Wer allerdings ein öffentliches Internetcafé betreibt, sollte auf „1“ reduzieren. Denn wenn alle verfügbaren IP-Adressen reserviert sind, können keine weiteren vergeben werden.

Unter „Gastnetz“ gibt es Einstellungen für einen weiteren DHCP-Server im Netzwerk „192.168.179.1“. Hier lässt sich nur die Gültigkeit einstellen. Das Gastnetz ist erst aktiv, nachdem es unter „WLAN → Gastzugang“ aktiviert wurde.

IPv6-Netzwerk: Klicken Sie unter „Netzwerkeinstellungen“ auf „IPv6-Einstellungen“. Sie sollten alle Einstellungen beim Standard belassen, um Probleme zu vermeiden. Die Fritzbox weist den Clients über den DHCPv6-Server nur die DNS-Server zu. Die weitere Konfiguration wird dem jeweiligen Betriebssystem überlassen.

5. Von Nummern und Namen

IP-Adressen kann man sich nur schlecht merken, weshalb sich im Internet und im lokalen Netzwerk Geräte auch über den Namen ansprechen lassen. Im Internet sind dafür DNS-Server zuständig, die zu URLs wie „www.google.de“ die passende IP-Adresse liefern. Welcher DNS-Server per DHCP übermittelt wurde, erfährt man im Terminal über

```
resolvectl dns
```

Im Heimnetz ist die Situation komplizierter. Ubuntu und Linux Mint verwenden Avahi für die Bekanntgabe von Gerätenamen und Netzwerkressourcen. Mac-OS, Smart-TVs und Drucker verwenden kompatible Protokolle (Apple Bonjour, mDNS, DNS-SD). Avahi sorgt dafür, dass im Ubuntu-Dateimanager unter „Andere Orte“ (Linux Mint: „Netzwerk“) Linux-Samba-Freigaben auftauchen. Drucker im Netzwerk werden ebenfalls automatisch gefunden.

Wer sehen möchte, was sich alles über Avahi meldet, verwendet im Terminal

```
avahi-browse -art
```

Ein Tool für die grafische Oberfläche ist avahi-discover, das sich über das gleichnamige Paket nachinstallieren lässt. Avahi verwendet für Geräte beziehungsweise

Dienste die Domain „.local“. Die Verbindung zu einem Linux-PC lässt sich beispielsweise mit

```
ping [Rechnername].local
```

testen. Der Befehl liefert die IP-Adresse von „[Rechnername]“ zurück.

Die Rolle des Routers: Eine Anfrage beim Router kann auch für die Namensauflösung dienen. Was möglich ist, hängt allerdings vom Routermodell ab. Die Fritzbox verwendet „fritz.box“ für lokale Domainnamen. Somit ist jeder Rechner statt mit der IP-Adresse so erreichbar:

```
ping [Rechnername].fritz.box
```

Wenn man nur „[Rechnername]“ verwendet, hängt die Fritzbox das Suffix automatisch an. Das funktioniert in jede Richtung mit Linux- und Windows-PCs sowie den meisten anderen Geräten.

Andere Router bieten diesen Komfort oft nicht, weil sie nur die DNS-Server des Providers per DHCP übermitteln, aber keine Namensauflösung für das lokale Netzwerk bieten. Das hat zur Folge, dass man von Windows 10/11 aus mit einer ping-Abfrage Linux-Rechner über ihren Namen und auch mit angehängtem „.local“ findet, unter Linux aber keine Windows-Rechner. Wer die Verbindung mit ping unter Linux prüfen möchte, muss daher die IP des Windows-PCs ermitteln und verwenden.

In der Praxis hat das jedoch kaum Auswirkungen. Im Linux-Dateimanager kann man in der Adressleiste (Strg-L) über

```
smb://[Rechnername]
```

auf Windows-Freigaben zugreifen. Die Namensauflösung erfolgt in diesem Fall über Samba-Funktionen, wofür weder Router noch andere Nameserver-Funktionen erforderlich sind. Das kann man auch im Terminal mit

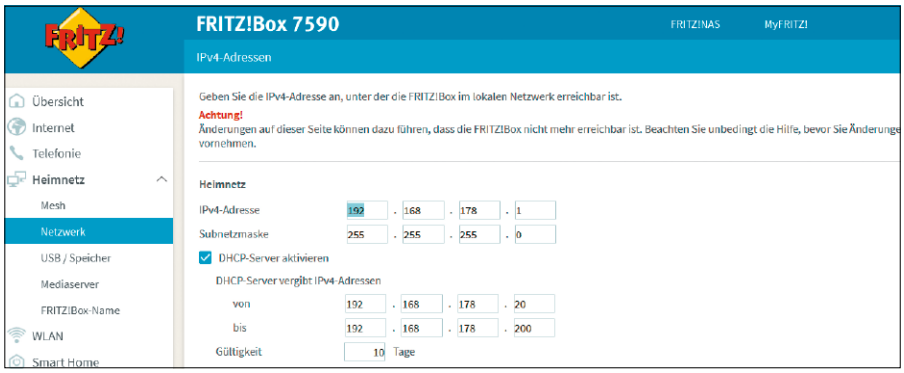
```
nmblookup [Rechnername]
```

nutzen, um sich die IP-Adresse ausgeben zu lassen.

6. Feste IPv4-Adresse einstellen

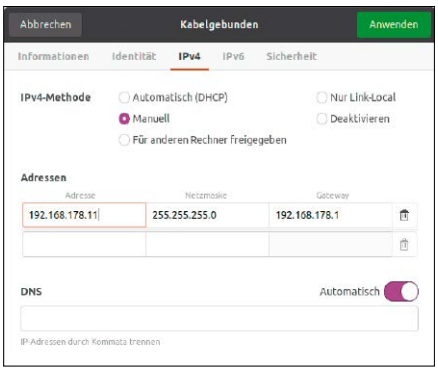
Einige Serverdienste lassen sich nur mit einer IP-Adresse und nicht mit dem Namen des Rechners konfigurieren. Ein Linux-Server sollte daher zuverlässig immer die gleiche IPv4 erhalten, was den Zugriff unabhängig von der Namensauflösung und auch über das Internet gewährleistet, wenn im Router Portfreigaben konfiguriert sind.

Bei einer Fritzbox gehen Sie auf „Heimnetz → Netzwerk“. Klicken Sie unter „Netzwerkverbindungen“ beim gewünschten Rechner auf das Icon mit dem Stiftsymbol. Setzen Sie ein Häkchen vor „Diesem Netzwerkgerät immer die gleiche IPv4-Adresse zuweisen“ und bestätigen Sie mit „OK“. Wenn man über „Internet → Freigaben“ Portfreigaben für den Zugriff aus dem Internet einrichtet, wird die feste IP automatisch aktiviert.



DHCP-Einstellungen: Der Bereich, aus dem ein Router IPv4-Adressen vergibt, lässt sich ändern. Meist stehen aber standardmäßig genügend IP-Nummern zur freien Verfügung.

Falls ein Router keine entsprechende Funktion bietet, nutzen Sie die Linux-Einstellungen. Öffnen Sie die Netzwerkkonfiguration (siehe Punkt 3) und dort auf „IPv4“. Wählen Sie die Option „Manuell“ (Linux Mint: „Manuell“ hinter „Adressen“) und tragen Sie eine IP-Adresse ein, die der Router nicht über DHCP vergibt (siehe Punkt 4). Hinter „Gateway“ gehört die IP des Routers und bei „Netzwerkmaske“ tragen Sie „255.255.255.0“ ein, was für IP-Adressen aus den üblichen Bereichen 192.168.X.X richtig ist. Nach einem Klick auf „Anwenden“ starten Sie Linux neu.



IPv4-Adresse festlegen: In der Netzwerkkonfiguration von Ubuntu oder Linux Mint lässt sich DHCP abschalten und man kann die Adressen manuell eingeben.

7. Statische IPv6-Adresse festlegen

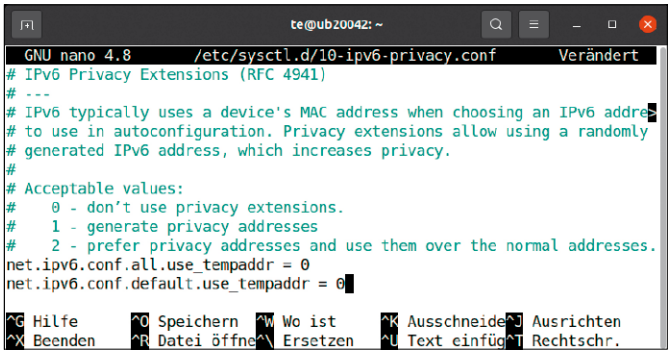
Eine feste IPv6-Adresse ist nur erforderlich, wenn ein Serverdienst auch oder nur über dieses Protokoll von außen aus dem Internet erreichbar sein soll. Öffnen Sie die Konfigurationsdatei im Terminal:

```
sudo nano /etc/
  sysctl.d/10-ipv6-privacy.conf
```

Ändern Sie die Werte hinter „net.ipv6.conf.all.use_tempaddr=“ und „net.ipv6.conf.default.use_tempaddr=“ jeweils auf „0“ und speichern Sie die Datei. Starten Sie Linux neu. Ermitteln Sie dann die neue Adresse:

```
ip a
```

Wenn Sie bei der Fritzbox eine Portfreigabe einrichten, tragen Sie die letzten vier Blöcke hinter „IPv6 Interface-ID“ ein. Fritzbox verwendet sonst eine der vorherigen IPv6-Adressen, weil der Router nichts von der geänderten Konfiguration erfährt. ■

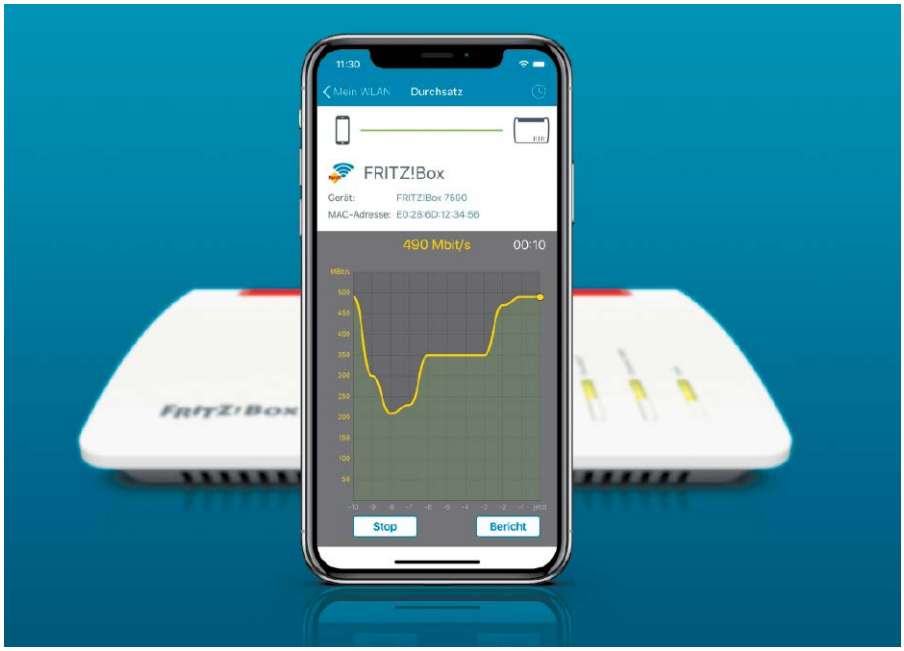


Unveränderliche Adresse: Wenn man die Privacy Extensions in der Datei „10-ipv6-privacy.conf“ abschaltet, bleibt die IPv6 gleich. Im Internet ist der PC dann allerdings identifizierbar.

Optimales WLAN

Heimische Funknetze haben zwei Problemfelder: Das eine ist die Sicherheit gegenüber unerwünschten Gästen, das zweite eine befriedigende Leistung und Reichweite an allen Standorten, wo mobile Geräte zum Einsatz kommen.

VON HERMANN APFELBÖCK



Die Leistung moderner WLAN-Router wird immer besser, aber wachsende Ansprüche beim Downloaddurchsatz (Streaming) und räumlichen Situationen mit Etagen, Balkon, Garten machen die Optimierung unzulänglicher WLAN-Abdeckung weiterhin zum Dauerthema. Und dass nicht jeder Nachbar ins Funknetz kommt, dort Bandbreite abzweigt und in persönlichen Daten spazieren geht, bleibt ebenfalls ein Muss der optimalen WLAN-Konfiguration.

WLAN-Sicherheit: Die entscheidenden Regeln

Obligatorisches Kennwort: Das WLAN-Kennwort – in der Fritzbox unter „WLAN → Sicherheit → Verschlüsselung" – muss Ihr lokales Netzwerk zuverlässig vor Fremden schützen: Eine Mindestlänge und Komplexität ist kein Problem, weil sich alle Mobilgeräte das Kennwort dauerhaft merken. Im Router aktivieren Sie dies je nach Modell mit den Optionen „WPA2 + WPA3" oder „WPA2 (CCMP)". Auch älteres „WPA/WPA2" bietet noch ausreichende Sicherheit, wenn das Passwort komplex genug ist. Denn mit geduldigen Wörterbuch-Angriffen auf das WLAN-Passwort muss man immer rechnen, etwa von gelangweilten Nachbarn, die nichts Besseres zu tun haben, als Ihr Netzwerk zu entern.

Obligatorisches Gastnetz (mit Isolation): Es ist immer unangenehm, Besuchern das primäre Funknetzkennwort mitteilen zu müssen. Ein Gast-WLAN, das getrennt vom sonstigen WLAN arbeitet, erspart solche Bedenken. Moderne Router und Access Points bieten einen „Gastzugang" mit „Wireless Isolation", „Client Isolation", „AP Isolation" oder ähnlich lautend. In der Fritzbox finden Sie die Option unter „WLAN → Gastzugang → Gastzugang aktiv". Das Gast-WLAN erhält eine eigene SSID-Kennung und ein eigenes Passwort. Es erlaubt keinen Zugriff auf das lokale Netzwerk und dessen Freigaben (Client Isolation). Wenn Sie die zusätzliche Option „Internetanwendungen beschränken: Nur Surfen und Mailen erlaubt" aktivieren, dann werden zusätzlich alle Ports geschlossen, die für Downloads über FTP oder Bittorrent zuständig sind.

Die weitere Option „Die mit dem Gastzugang verbundenen WLAN-Geräte dürfen untereinander kommunizieren" lockert die restriktive Konfiguration ein wenig: Die im Gast-WLAN angemeldeten Geräte dürfen dann zumindest untereinander Daten austauschen – Smartphones per Wi-Fi-Direct oder Notebooks über Freigaben.

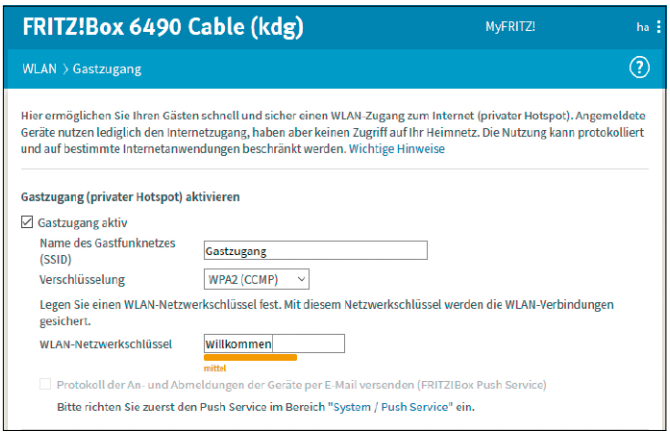
Optionale MAC-Filterung: WLAN-Router sind im Normalfall so eingestellt, dass sich jedes Gerät am Funknetz anmelden darf, sofern der Benutzer das WLAN-Kennwort richtig eingibt. Das ist bequem, aber nicht sicher. In der Fritzbox finden Sie die Einstellung unter „WLAN → Sicherheit" ganz unten in der Option „Alle neuen WLAN-Geräte zulassen". Wenn Sie hingegen das Funknetz auf „die bekannten WLAN-Geräte beschränken", werden neue Clients (mit noch nicht gespeicherter MAC-Adresse) generell abgewiesen. Alle bekannten und bereits gespeicherten Geräte sehen Sie in der Liste darüber einschließlich ihrer MAC-Adresse. Geräte, die Sie hier mit dem roten Kreuz entfernen, kommen dann ebenfalls nicht mehr in Ihr WLAN.

Dieser Schutz ist nicht ganz bequem: Jedes hinzukommende Gerät im Haushalt oder jedes Besuchergerät muss explizit mit seiner MAC-Adresse neu aufgenommen werden („WLAN-Gerät hinzufügen").

Es empfiehlt sich, vor dem Aktivieren dieser Option alle benötigten Geräte anzumelden, sodass deren MAC-Adressen in

der Liste der bekannten Geräte bereits aufgeführt sind.

Optionale SSID-Unterdrückung: Der Funknetzname (SSID) muss nicht öffentlich für alle Nachbarn sichtbar sein. In der Fritzbox lässt sich diese Öffentlichkeit über „WLAN → Name des WLAN-Funknetzes sichtbar" abschalten. Danach muss beim Zutritt zusätzlich zum WLAN-Kennwort auch die SSID explizit eingegeben werden. Wi-Fi-Scanner zeigen den Netznamen zwar auch an, wenn er unterdrückt wird, aber technische Laien in Ihrer Nachbarschaft werden Ihr Netzwerk nicht mehr sehen.



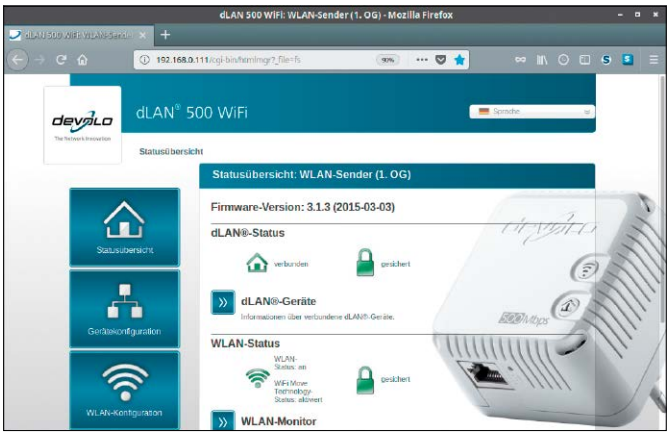
Vorkonfigurierter Gastzugang für Besucher: Sie müssen das primäre WLAN-Kennwort nicht preisgeben und halten Besucher vom lokalen Netzwerk fern (Client Isolation).

WLAN-Leistung: Die Ausbauoptionen

WLAN-Test: Bei Zweifeln über WLAN-Reichweiten und Signalstärken gibt es objektive Testmöglichkeiten. Bequem und werbefrei ist die Android- und iOS-App „Fritz!App WLAN", mit der Sie mit dem Mobilgerät die kritischen Bereiche abgehen. Über „Verbinden" können Sie das Funknetz wechseln, falls Ihr Heimnetz mehrere Sender hat, und unter „Mein WLAN" gibt es die Option „WLAN messen". Was die App als „Mbit/s" mindestens melden sollte, hängt natürlich vom Bedarf vor Ort ab. Mit 10 MBit/s lässt sich surfen, für HD-Streaming sollte es Richtung 30 bis 50 MBit/s gehen, für große Downloads möglichst nahe an die Bandbreite, die der Internetzugang generell bietet.

Allgemeine Optimierungsmaßnahmen: Ratschläge, die Position des Routers zu ändern, scheitern praktisch immer an den Gegebenheiten. Da Router an den Splitter (DSL) oder an die Multimediadose (Kabel) gebunden sind, sind nur minimale Ortsänderungen möglich, die nur Minimales bewirken. Gleiches gilt für die Ausrichtung von Antennen am Router oder am Endgerät, sofern überhaupt vorhanden.

WLAN-Repeater: Repeater sind Signalverstärker der WLAN-Basisstation. Sie sollten dort angesteckt oder aufgestellt werden, wo das Signal der Basisstation noch einigermaßen zu empfangen ist. Die Mitte zwischen Basisstation und den Endgeräten ist ein oft genannter Pauschaltipp, ein Platz nahe am Endgerät kann aber durchaus bessere Resultate liefern. Optimal ist das Verfahren generell nicht, da jedes Datenpaket zweimal gesendet (vom Router und vom Repeater) und zweimal empfangen werden muss (vom Repeater und vom Endgerät). Trotzdem kann ein Repeater den Datendurchsatz verdoppeln. Die unterschiedlichen Preise zwischen 20 und 120 Euro rechtfertigen sich durch theoretische Sendeleistungen von 300 bis 1700 MBit/s, durch Dualband-Fähigkeit (2,4 und 5 GHz) und Funktionen wie zusätzliche Ethernet-Anschlüsse. Da Repeater in unserer Sicht immer eine Notlösung bleiben, sind hochpreisige Repeater aber selten sinnvoll.



Powerline-Adapter (Basisadapter am Router vorausgesetzt) liefern das WLAN an jeder Steckdose an jeden Ort. Eine Kombination mit einem extra Access Point ist oft noch leistungsstärker.

Powerline/DLAN-Wi-Fi-Adapter: Powerline ist eine Ethernet-Vernetzung, die für die Hauptdistanz die Stromleitung nutzt, die kurzen Restwege übernehmen dann wieder Ethernet-Kabel. Der Basisadapter ist via Ethernet direkt mit dem Router verbunden, weitere Adapter kommen dorthin, wo die Netzwerkverbindung benötigt wird. Für die angeschlossenen Endgeräte spielt die Powerline-Brücke keine Rolle: Für Linux, Windows oder Mac-OS handelt es sich um eine Ethernet-Verbindung.

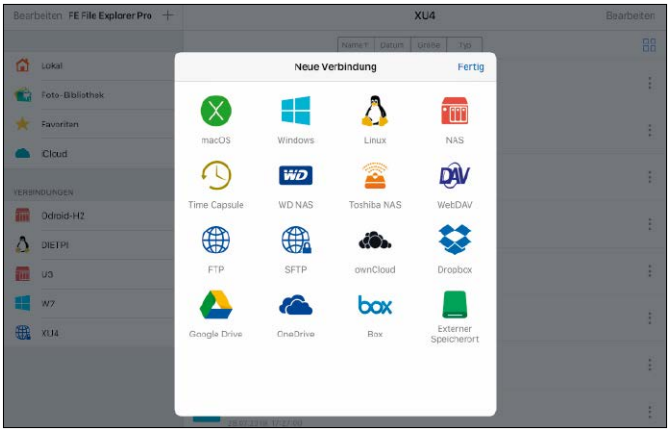
Powerline-Adapter können aber auch das Funknetz ausbauen, indem der entfernte Adapter (bei den Endgeräten) per Wi-Fi weiterfunkt. Ein Starterkit des Markführers Devolo mit Basisadapter und Wi-Fi-Adapter (plus Ethernet-Buchsen) ist für etwa 90 Euro erhältlich. Der Fritzbox-Hersteller AVM bietet ähnliche Powerline-Sets mit Wi-Fi-Sender ab 110 Euro. Wenn bereits eine Powerline-Basis vorliegt, gibt es auch einzelne Wi-Fi-Erweiterungsadapter ab etwa 50 Euro. Im Prinzip sind solche Lösungen nichts anderes als Access Points mit vergleichbaren Funktionen (Gastnetz, Kindersicherung, Zeitschaltung).

Access Point: Wenn das Router-Funknetz einen wichtigen Raum nicht abdeckt, dort aber Ethernet vorliegt, verwenden Sie an diesem Standort vorzugweise einen WLAN-Access-Point. In den meisten Haushalten dürfte eine Ethernet-Verkabelung in jede Ecke eher unwahrscheinlich sein, aber es kann ja auch ein Powerline-Adapter aushelfen. Eine solche Kombination von Powerline und Access Point scheint unnötig, weil die oben beschriebenen Powerline/DLAN-Wi-Fi-Adapter scheinbar dasselbe bieten und dabei ein Gerät einsparen. Wer optimale Funkleistung möchte, ist aber mit einem Access Point wie etwa D-Link DAP-1665 noch ein Stück schneller unterwegs – auch in Verbindung mit einer Powerline-Brücke. ■

Mobilgeräte im Heimnetz

Smartphones und Tablets mit Android und iOS sind in jeder Beziehung vollwertige Teilnehmer im heimischen Heimnetz. Hier soll es ausschließlich um deren Client-Rolle gehen, also um den Dateizugriff (Backup) auf Netzfreigaben und um Medienwiedergabe.

VON HERMANN APFELBÖCK



FE File Explorer ist eine Empfehlung für alle Android- und Apple-Mobilgeräte. Der Dateimanager für Samba, SSH, FTP und Cloud garantiert vor allem eine komfortable Medienwiedergabe.

Angesichts zahlreicher Cloud-Apps, die Google, Apple und Hersteller auf den Geräten als Standard und oft sogar als Pflichtsoftware mitliefern, bleiben die Fähigkeiten für den lokalen Netzwerkzugriff erbärmlich – nämlich gleich null. Wer von seinem „Heimserver" (Raspberry, Router, Windows-Freigabe?) Medien nutzen oder Daten wie Smartphone-Fotos dort sichern will, ist voll und ganz auf die Angebote in den App Stores von Google und Apple angewiesen. Dort wiederum gibt es exzellente Apps, aber leider auch grottenschlechte, außerdem Werbeschleudern und datenschutztechnische Minenfelder.

Die handverlesenen nachfolgenden Empfehlungen sollten für mehr als 90 Prozent typischer Alltagsbedürfnisse ausreichen. Zweifeln Sie nicht, dass Ihr Smartphone oder Tablet darüber hinaus jede plausible bis exotische Spezialaufgabe im Netzwerk erfüllen könnte: Remote-Steuerung für TV, Mediencenter oder VLC, Remotedesktop für Windows- oder Linux-PCs, Überwachungskamera mit Webserver, Samba-Server – das sind nur einige Beispiele und Anregungen.

FE File Explorer: Dateimanager für iOS und Android

Für Android- wie iOS-Geräte ist der FE File Explorer eine klare Empfehlung: Schnell, funktionsreich und attraktiv taugt der englischsprachige Dateimanager für den Zugriff auf Netzwerkressourcen aller Art. Neben Samba- und Windows-Freigaben hat er FTP, SFTP (SSH), Webdav und außerdem noch diverse Clouddienste im Portfolio (Google Drive, Onedrive, Dropbox, Owncloud). Die kostenlose Version ist allerdings arg beschränkt, insofern sie nur eine einzige eingerichtete Serverquelle erlaubt und – noch limitierender – nur wenige Audio- und Videoformate unterstützt. Die Bezahlversion spielt nach unserer Erfahrung alle gängigen Audio- und Videoformate. Die knapp fünf Euro für die unlimitierte Pro-Version sind daher gut angelegt.

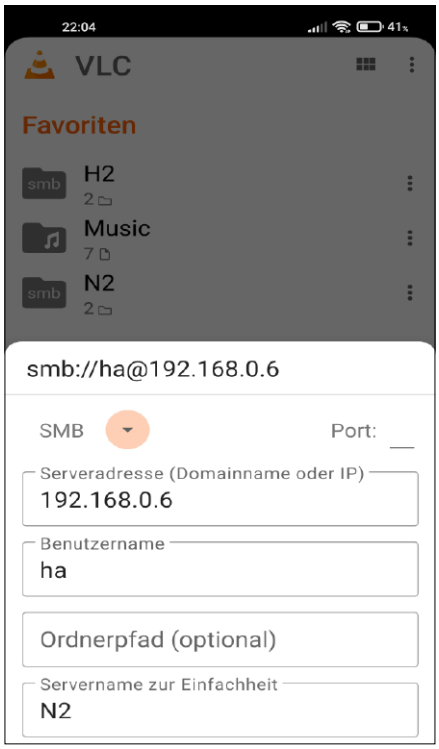
Mit der „+"-Schaltfläche rechts unten ist eine neue Verbindung schnell eingerichtet und dauerhaft gespeichert. Für lokale Netzressourcen ist nach Auswahl des Servertyps, also etwa „Windows", „Linux" oder „SFTP", die lokale IP-Adresse die wichtigste Angabe, das optionale Speichern von „User" und „Password" vereinfacht den Zugriff.

In der Funktion als klassischer Dateimanager ist das Tool intuitiv, da es bei markierten Objekten das Allerwichtigste („Copy", „Move", „Delete") unten direkt anzeigt. Ansonsten stehen weitere Dateiaktionen im Drei-Punkte-Menü bereit. Trotzdem kann der FE File Explorer dem später genannten Total Commander als Dateimanager nicht das Wasser reichen. Seine Vorzüge liegen eindeutig in der Medienwiedergabe.

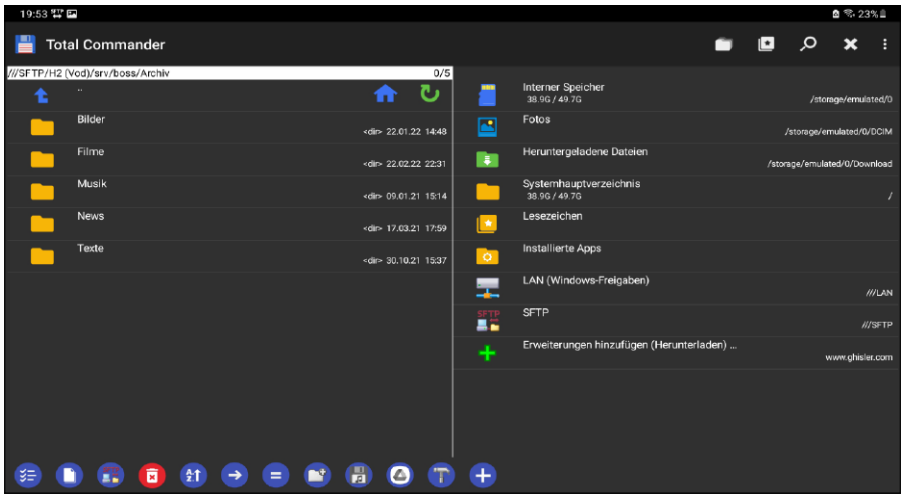
Allzweckwaffe VLC

Am Tablet und Smartphone steht meistens die Wiedergabe von Medien im Vordergrund, während aktive Dateimanager-Aktionen oft sekundär bleiben. Das ist zu rechtfertigen, wenn gelegentliche Sicherungen auf anderem Weg erfolgen, etwa direkt per USB. Für die reine Medienwiedergabe kann man, wie so oft, auf den VLC-Medienplayer zurückgreifen. Der ist nicht nur eine Universalwaffe hinsichtlich aller Audio- und Videoformate, sondern auch beim Netzwerkzugriff. Die Bedienung unter iOS und Android ist nicht ganz einheitlich, aber ans Ziel kommt man in beiden Varianten:

Bei Android führt unten das Angebot „Dateien" und dort die Schaltfläche „+" zu einem Konfigurationsdialog, der unter anderen die lokalen Netzprotokolle „SMB" und „SFTP" anbietet. Damit kommen Sie mit dem VLC auf jeden Samba- oder SSH-Server.



Allzweckwaffe für Medienwiedergabe: Geht es ausschließlich um Film- und Musikwiedergabe vom Heimserver, dann genügt der VLC-Mediaplayer.



Total Commander mit LAN- und SFTP-Plug-in: Als Dateimanager ist die Android-App unschlagbar. Die Medienwiedergabe delegiert er an VLC & Co., wobei er Audio auch selbst übernehmen kann.

Die Angabe der IP-Adresse und des Benutzerkontos sind vorab einzugeben, das Passwort wird bei erster Nutzung abgefragt und kann dann dauerhaft gespeichert werden. Bei iOS ist unten das Angebot „Netzwerk" einschlägig. Eventuell bereits automatisch angezeigte Netzrechner können die Aktion vereinfachen. Der logische Weg ist aber „Verbinden → SMB" mit dann folgenden Einträgen für „Server" (IP-Adresse), „Benutzer", „Passwort" und Arbeitsgruppe (oft „Workgroup", falls nicht manuell umgestellt). Das Protokoll SFTP bietet die iOS-Variante nicht an, dafür aber zusätzlich die Verbindung zu Plex-Servern.

Total Commander: Nur Android

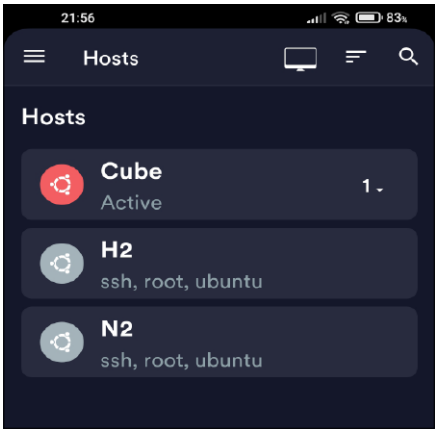
Für den Zugriff auf lokale Samba- und SSH/SFTP-Netzfreigaben, ferner auch auf FTP-Server und Cloudspeicher (Google, Onedrive) gibt es – allerdings nur für Android – eine App, die alles kann: den Total Commander. Die kostenlose App ist für Android-Tablets eine uneingeschränkte Empfehlung. Auf schmalen Smartphones ist immer nur ein Verzeichnispanel von zweien sichtbar und nur (ältere) Nutzer, die mit Zwei-Fenster-Managern sozialisiert wurden, kommen damit problemlos klar. Ungeachtet der altmodischen Bedienung hat das anpassungsfähige Tool mit den letzten Versionen optisch deutlich gewonnen und bietet inzwischen auch eine hervorragende interne Audiowiedergabe. Das Abspielen von Videos delegiert der Commander an den Player Ihrer Wahl.

Für seine Netzwerkfähigkeiten benötigt der Total Commander winzige Plug-ins, die Sie im Google Store über die Suche „Total Commander Plugin" finden. Einschlägig für das lokale Netzwerk sind das LAN-Plug-in für Samba-Freigaben und das SFTP-Plug-in für SSH-Server. Ob Sie zusätzlich FTP, Webdav, Google Drive, Onedrive für Internetquellen benötigen, ist Ermessenssache.

Installierte Plug-ins erscheinen im Hauptverzeichnis des Total Commander. Egal, welches Plug-in Sie verwenden, funktioniert das Einrichten einer Ressource weitgehend analog. Mit „Neuer Server" oder „Neuer Verbindung" richten Sie den Zugriff ein: Zunächst vergeben Sie einen Namen, darunter die Server- und Authentifizierungsdaten. Beim LAN-Plug-in für das lokale Netz sollten Sie die IP-Adresse gegenüber dem Servernamen bevorzugen, sofern der Datenserver eine feste IP verwendet.

Mobilgeräte als SSH-Client

Smartphones und Tablets sind nicht unbedingt erste Wahl für die SSH-Fernwartung. Der Bildschirm ist selbst auf Tablets relativ beschränkt, weil die virtuelle Tastatur für Terminaleingaben zumeist eingeblendet bleiben muss. Ein schneller Eingriff in eine Konfigurationsdatei, eine Taskübersicht mit „htop", ein Shutdown oder das Abholen einer wichtigen Datei ist aber auch mit Mobilgeräten machbar – und das mit Sofakomfort. Bester Kandidat für Android wie iOS ist die englischsprachige App Termius. Unter „Host" legen Sie mit dem Pluszeichen einen Eintrag an („New host"). Im Prinzip genügt der Eintrag der IP-Adresse, falls der Server den Standardport 22 nutzt. Man kann bei geringen Sicherheitsansprüchen im lokalen Netz auch gleich das Benutzerkonto und das Kennwort hinterlegen. Allgemeine Einstellungen zu Schriftgröße und Farben werden unter den „Settings" eingetragen, die für alle Hosts gelten. Um Einstellungen an einem bereits eingetragenen Server („Host") zu ändern, hilft längeres Drücken des Hosteintrags, was den Host markiert und in der kleinen Symbolleiste den Editierstift einblendet. Für bereits eingetragene Rechner genügt dann ein Fingertipp, um die SSH-Verbindung zu starten. ■



SSH-Client für Android und iOS: Das englischsprachige Termius verwaltet beliebig viele SSH-Server.

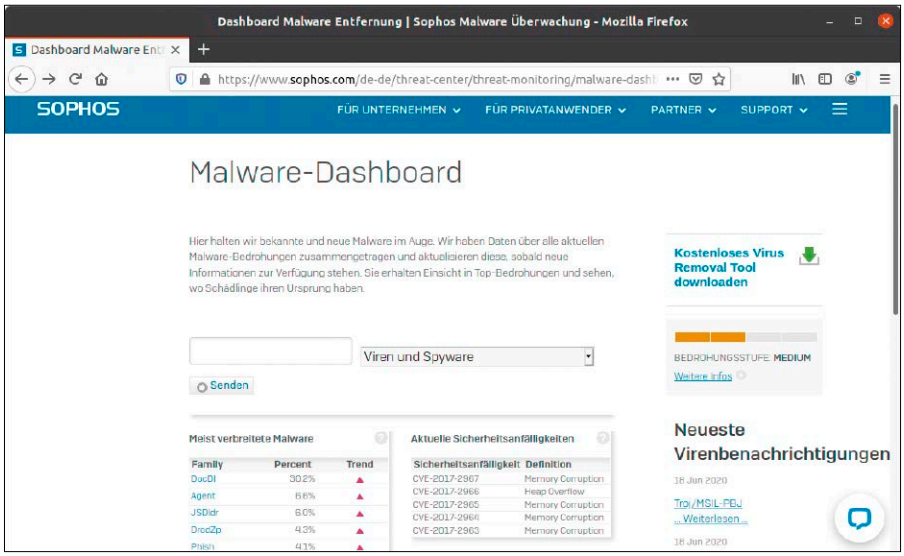
Virensicher im eigenen Netzwerk

Linux ist kaum von Viren, Würmern und Trojanern betroffen. Ein Linux-PC im eigenen Netzwerk kann jedoch dazu beitragen, den Schutz von beteiligten Windows-Rechnern zu verbessern.

VON THORSTEN EGGELING

Jeden Tag entdecken die Virenlabore mehrere hunderttausend neue Viren und andere Schadsoftware. Die werden meist automatisch generiert und immer leicht verändert, damit Antivirensoftware sie nicht so leicht aufspüren kann. Ziel sind vor allem Windows-Rechner. Die sind zwar aus technischer Perspektive prinzipiell nicht viel unsicherer als Linux, aber das Nutzerverhalten ist dort ein anderes. Vor allem ist Windows für Angreifer lohnender, weil das System weitverbreitet ist. Wer in einem gemischten Netzwerk arbeitet, also mit Linux- und Windows-Rechnern, kann für etwas Entspannung sorgen. Dateifreigaben für Windows lassen sich unter Linux mit einem eigenen Virenscanner überwachen. Das sorgt für mehr Sicherheit, sollte die Schutzsoftware unter Windows aufgrund einer Infektion ausfallen.

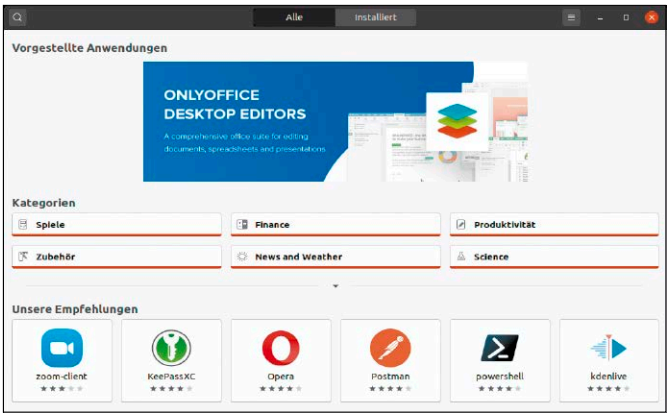
Eine besondere Bedrohung, die auch Netzwerkfreigaben betrifft, stellen Verschlüsselungs-Trojaner dar. Vor dem Verlust wichtiger Dateien kann jedoch ein regelmäßiges Backup auf einen Linux-PC schützen.



Permanente Bedrohungen: Die Hersteller von Antivirensoftware informieren über aktuelle Bedrohungen und Sicherheitslücken. Davon sind meist nur Windows-Systeme betroffen.

Drohende Gefahren für Ihre Rechner

Es gibt im Wesentlichen nur zwei Angriffsszenarien auf Computer. Die größte Bedrohung geht vom Benutzer aus, der vor dem Bildschirm sitzt. Wer Software aus fragwürdiger Quelle ohne Prüfung installiert oder Programme aus E-Mail-Anhängen startet, holt sich am schnellsten Schadsoftware auf den Rechner. Das gilt im Prinzip für Windows und Linux gleichermaßen. Allerdings verwenden Linux-Anwender für die Softwareinstallation überwiegend die Paketquellen der jeweiligen Distribution. Dass darüber Viren auf den Rechner gelangen, ist so gut wie ausgeschlossen. Dateien aus E-Mail-Anhängen sind unter Linux standardmäßig nicht startfähig. Nur wenn der Benutzer selbst eine Datei als „ausführbar" kennzeichnet, lässt sie sich starten. Auch PDF-Dateien oder Makros in Office-Doku-



Sichere Software: Linux-Nutzer laden neue Programme nicht irgendwo aus dem Internet, sondern in der Regel über gut geschützte Paketquellen, die frei von Schadsoftware sind.

menten können Sicherheitslücken ausnutzen oder Schadsoftware mitbringen. Dagegen hilft nur, die Software stets aktuell zu halten und in den Sicherheitseinstellungen der Office-Software die Ausführung von Makros zu verbieten oder nur auf Nachfrage zu erlauben. Das ist jedoch die Standardeinstellung.

Das andere Szenario kommt ohne Mithilfe des Nutzers aus: Angriffe aus das Internet oder dem lokalen Netzwerk, etwa von einem infizierten Rechner aus, können Sicherheitslücken im Betriebssystem nutzen, um Schadsoftware zu verbreiten.

Reine Desktop- oder Büro-PCs sind davon in der Regel kaum betroffen, denn standardmäßig laufen dort keine Dienste, die von außen erreichbar sind (siehe Kasten „Schutz von Linux-Servern"). Daher gibt es auch keine Angriffsfläche. Das gilt für Linux wie Windows.

Sichere Netzwerkfreigaben unter Linux

Gewähren Sie nur die Zugriffsrechte, die wirklich erforderlich sind. Wenn Windows-Rechner keinen Schreibzugriff auf Netzwerkfreigaben besitzen, kann auch kein Schaden angerichtet werden. Wird der Linux-PC beispielsweise nur als Speicher für Backups genutzt, ist das problemlos möglich (siehe unten „Regelmäßige Backups erstellen"). Anders sieht es aus, wenn Freigaben zum Datenaustausch zwischen den Rechnern im lokalen Netzwerk dienen sollen. Dafür muss der Schreibzugriff möglich sein.

Wenn noch nicht geschehen, richten Sie auf Ihrem Linux-Rechner den Freigabedienst Samba in einem Terminal ein:

```
sudo apt install samba
```

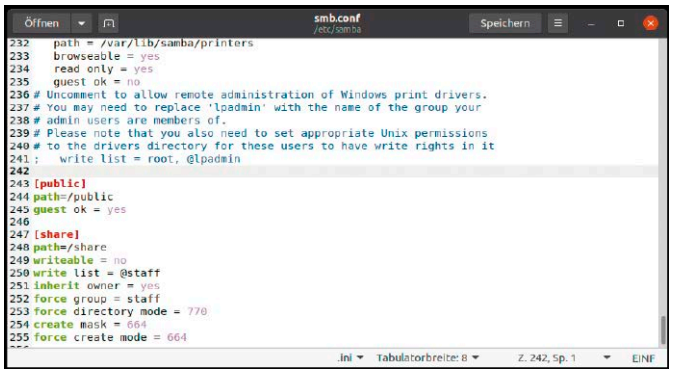
Bearbeiten Sie die Konfigurationsdatei mit einem Editor Ihrer Wahl:

```
sudo nano /etc/samba/smb.conf
```

Ändern Sie die Bezeichnung hinter „workgroup=" auf die Arbeitsgruppe, die Sie in Ihrem Netzwerk verwenden. Der Standard ist „WORKGROUP". Eine schreibgeschützte und ohne Anmeldung (Gastzugang) erreichbare Freigabe erzeugen Sie mit diesen Zeilen:

```
[public]
path=/public
guest ok = yes
```

Die Angabe hinter „path=" gibt den Pfad zu einem Ordner im Dateisystem an, den Sie als Speicherplatz im Netzwerk verwenden wollen. „guest ok = yes" ermöglicht den Zugriff für alle Windows- und Linux-Rechner ohne Benutzernamen und Passwort.



Freigaben (auch) für Windows: In der zentralen Konfigurationsdatei „smb.conf" legen Sie fest, welche Ordner Sie freigeben möchten und wer Schreib- oder nur Lesezugriff hat.

Die restriktivere Konfiguration für einen Ordner mit Schreibzugriff kann folgendermaßen aussehen:

```
[share]
path=/share
writeable = no
write list = @staff
inherit owner = yes
force group = staff
force directory mode = 770
create mask = 664
force create mode = 664
```

Hier erhalten nur Mitglieder der Gruppe „staff" den vollen Schreibzugriff. Neue und geänderte Dateien sowie Ordner versieht Samba mit passenden Zugriffsrechten. Damit das funktioniert, müssen einige Voraussetzungen erfüllt sein.

1. Benutzer müssen über ein Konto auf dem Linux-Rechner verfügen. Erstellen Sie neue Benutzer beispielsweise unter Ubuntu 20.04 in den „Einstellungen" unter „Benutzer".

2. Jeder Benutzer benötigt ein Samba-Passwort, das Sie mit

```
sudo smbpasswd -a [User]
```

festlegen. Für den Platzhalter „[User]" setzen Sie den jeweiligen Benutzernamen ein.

3. Die Benutzer müssen in unserem Beispiel zur Gruppe „staff" gehören, die bei Ubuntu standardmäßig vorhanden ist. Fügen Sie Benutzer mit

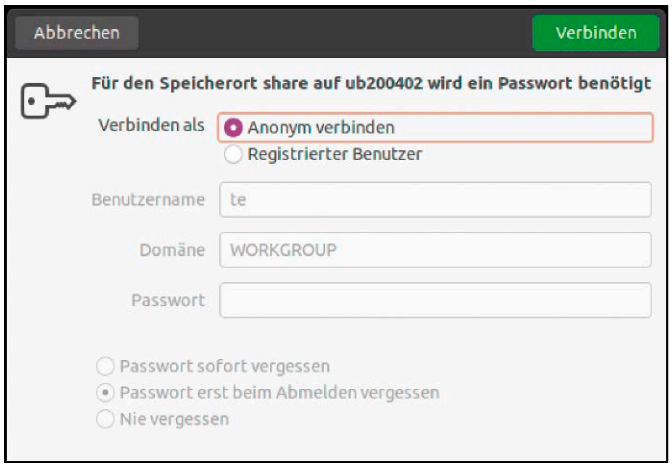
```
sudo usermod -a -G staff [User]
```

SCHUTZ VON LINUX-SERVERN

Sobald auf einem Rechner Serverdienste laufen, steigt die Gefahr. Besonders betroffen sind Webserver oder Fernsteuerungssoftware. Von außen ist ein Server durch die Routerfirewall geschützt beziehungsweise gar nicht ansprechbar. Angriffe aus dem lokalen Netzwerk sind jedoch möglich. Ist der Dienst auch über das Internet erreichbar, steigt das Risiko nochmal deutlich. Dafür muss man jedoch selbst eine Portfreigabe im Router einrichten. In diesem Fall muss der Server sehr sicher konfiguriert sein – stets aktuelle Software, sichere Passwörter, Zwei-Faktor-Authentifizierung, Basis-Angriffsschutz mit fail2ban (siehe *www.pcwelt.de/2321862*). Soll nur eine begrenzte Personenzahl auf den Server zugreifen, empfiehlt sich der Einsatz von VPN (*www.pcwelt.de/2448309*).

Öffentlich erreichbare Server sollten ab und zu auf Rootkits untersucht werden. Ein Rootkit eröffnet dem Angreifer die Option, sich auf dem kompromittierten System anzumelden, Netzwerkverkehr zu überwachen oder Programme zu starten.

Chkrootkit hilft beim Aufspüren von Rootkits. Es ist in den Paketquellen aller Distributionen zu finden und wird im Terminal mit root-Recht gestartet („sudo chkrootkit"), um das System zu untersuchen. Um sicher zu sein, dass das eigene System und damit das Programm chkrootkit nicht seinerseits kompromittiert ist, ist es ratsam, chkrootkit von einem unabhängigen Livesystem zu verwenden. Möglicherweise hat der Angreifer sein Rootkit gegenüber der Software getarnt, deswegen kann es nicht schaden, eine zweite Meinung etwa mit dem Programm rkhunter einzuholen. Auch dieses Tool ist in allen Distributionen über die Paketquellen beziehbar.



Beim Server anmelden: Beim Zugriff auf einen Server über den Dateimanager haben Sie die Wahl zwischen einer anonymen Verbindung als Gast oder mit Benutzernamen und Passwort.

zur Gruppe hinzu. Sie können auch eine andere Gruppe verwenden oder mit „sudo groupadd“ eine neue Gruppe erstellen.

4. Der freigegebene Ordner, in unserem Beispiel „/share“, muss der gewählten Gruppe gehören. Legen Sie die Berechtigungen im Dateisystem mit

```
sudo chown -R root:staff /share
```

fest.

Wenn Benutzernamen und Passwörter auf den Client-PCs mit denen auf dem Server übereinstimmen, erfolgt der Zugang ohne die Abfrage von Anmeldeinformationen. Sollte das aus Sicherheitsgründen unerwünscht sein, legen Sie andere Benutzernamen und/oder Passwörter fest. Linux und Windows fragen dann nach den Anmeldeinformationen. Wenn Sie diese nicht speichern, erfolgt nach einem Neustart des Systems keine automatische Anmeldung. Die Freigabe ist dann zumindest nicht permanent für Schadsoftware erreichbar.

Hinweise: Wenn es einen Benutzer mit dem gleichen Namen auf dem Linux-Server gibt, aber mit einem abweichenden Passwort, fragt Windows nach Benutzernamen und Passwort. Soll nur die Verbindung zur Gastfreigabe erfolgen, tippen Sie als Benutzernamen beispielsweise „gast“ ein und lassen das Passwort leer. Für Samba spielt der Name des Gastbenutzers übrigens keine Rolle. Es werden alle unbekannten Benutzernamen als „bad user“ behandelt und damit als Gäste. Wenn es den Benutzer auf dem Linux-Server nicht gibt, versucht Windows eine automatische Anmeldung als Benutzer „Gast“ und Samba gewährt den Zugriff auf Gastfreigaben.

Unter Linux erscheint in jedem Fall ein Dialog, in dem Sie die Option „Anonym verbinden“ (Gast) wählen oder „Registrierter Benutzer“ und dann Benutzernamen und Passwort eintippen. Sollte im Ubuntu-Dateimanager der Zugriff auf Freigaben über „Andere Orte → Windows Netzwerk“ nicht klappen, drücken Sie Strg-L und tippen die Adresse der Samba-Freigabe in der folgenden Form

```
smb://[Server]/[Freigabe]
```

direkt ein.

Virenscanner I: Sophos Antivirus

Sophos bietet eine kostenlose Antivirenlösung für Linux an. Technischen Support gibt es aber nur bei der Bezahlversion. Für den Download über *https://m6u.de/sopho* müssen Sie sich registrieren. Das Programm lässt sich ausschließlich über die Kommandozeile steuern, eine grafische Oberfläche gibt es nicht. Entpacken Sie die heruntergeladene Datei, öffnen Sie ein Terminal und wechseln Sie in das Verzeichnis der Software. Dort starten Sie mit

```
sudo ./install.sh
```

die Einrichtung. Folgen Sie den Anweisungen des Assistenten. Übernehmen Sie alle Vorgaben per Druck auf die Eingabetaste, außer bei der Frage „Do you wish to install the Free (f) or Supported (s) version of SAV for Linux?“. Hier tippen Sie „f“ ein und bestätigen mit Eingabetaste. Nach der Installation starten Sie

```
sudo /opt/sophos-av/bin/savupdate
```

zum Update der Virensignaturen. Das müssen Sie später nicht manuell wiederholen, weil Sophos Antivirus automatisch alle 60 Minuten nach Updates sucht. Danach können Sie mit

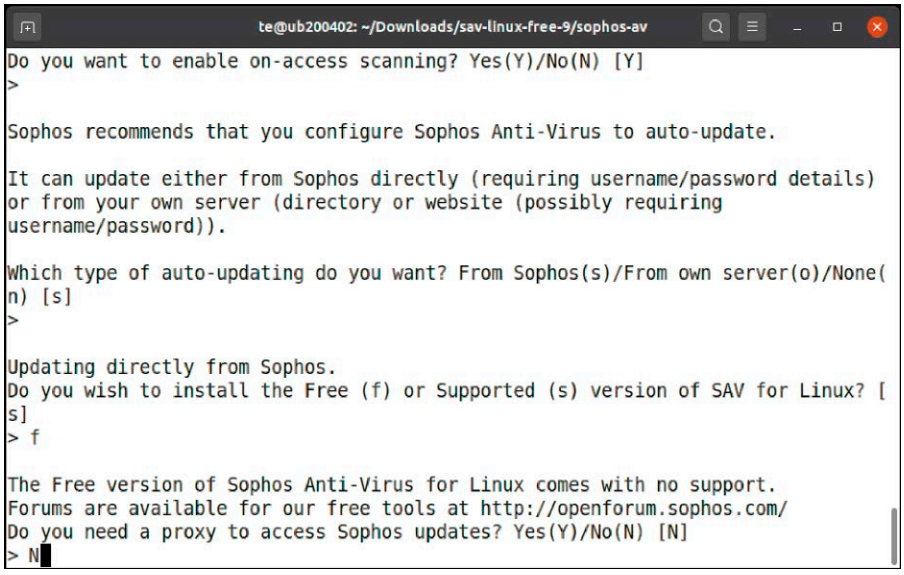
```
sudo /opt/sophos-av/bin/savscan /
```

das gesamte System auf Schadsoftware untersuchen. Standardmäßig ist die On-Access-Überprüfung aktiv. Sophos Anti-Virus prüft alle Dateioperationen, also jede Datei, die neu hinzukommt oder kopiert wird. Sollte Schadsoftware enthalten sein, wird die Datei blockiert, aber nicht gelöscht oder verschoben. Auch Windows-Nutzer, die eine infizierte Datei von einer Netzwerkfreigabe öffnen wollen, erhalten darauf keinen Zugriff. Mit

```
sudo /opt/sophos-av/bin/savlog
```

lassen Sie sich die Protokolle ausgeben.

Man sollte in regelmäßigen Abständen nach Schadsoftware suchen, betroffene Dateien verschieben, dann genauer untersuchen und gegebenenfalls löschen. Verwenden Sie die folgende Befehlszeile, wenn



Sophos Anti-Virus einrichten: Die Installation der Schutzsoftware erfolgt im Terminal. Ein Assistent fragt die Parameter ab, die Sie zum Großteil einfach mit der Eingabetaste bestätigen.

Sie nur den Ordner „/share“ prüfen und infizierte Dateien nach „/infected“ verschieben wollen:

```
sudo /opt/sophos-av/bin/savscan
  -nc -move=/infected /share
```

Die Option „-nc“ unterdrückt eventuelle Rückfragen. Informationen zu weiteren Optionen liefern

```
man savscan
```

sowie die Konfigurationsanleitung (*https://m6u.de/cgeng*) und die Startupanleitung (*https://m6u.de/sgeng*) für Linux.

Automatischer Scan: Laden Sie die Konfigurationsdatei des Crondienstes mit

```
sudo crontab -e
```

und tragen Sie dort diesen Auftrag ein (Beispiel):

```
0 1 * * * /opt/sophos-av/bin/savscan
  -nc -move=/infected /share >> /
  var/log/savscan.log
```

Dies würde den Virenscanner jede Nacht um 1:00 Uhr starten.

Virenscanner II: Eset Nod32 Antivirus

Von Eset gibt es einen Virenscanner für Linux, der auch eine grafische Oberfläche bietet. Über *www.eset.com/de/home/antivirus-linux* lässt sich eine kostenlose Version herunterladen, die Sie 30 Tage lang testen können. Für den Download ist eine Registrierung erforderlich. Die Vollversion kostet ab 29,95 Euro pro Jahr. Damit sich das Programm installieren lässt, müssen Sie unter Ubuntu oder Linux Mint ein zusätzliches Paket installieren:

```
sudo apt install libc6:i386
```

Danach verwenden Sie im Downloadverzeichnis diese beiden Befehle:

```
chmod 774 eset_nod32av_64bit_de.
  linux
sudo ./eset_nod32av_64bit_de.linux
```

Ein Assistent führt Sie durch die Installation. Zum Abschluss startet das Programm automatisch und aktualisiert selbständig die Virensignaturen. Über „Computer prüfen → Standardprüfung“ führen Sie einen ersten Virenscan auf allen lokalen Laufwerken durch.

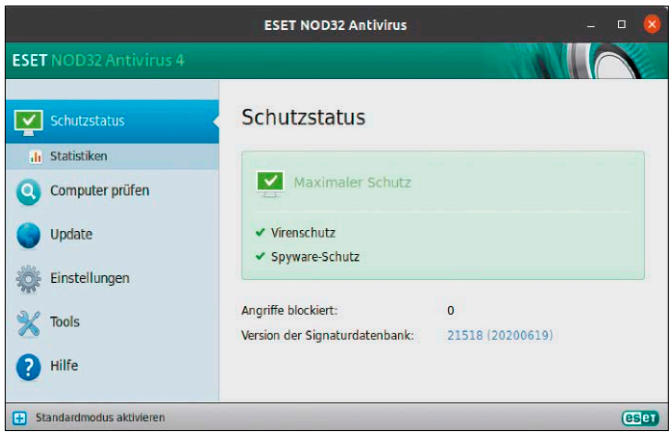
Eset Nod32 Antivirus schützt den Rechner mit dem Echtzeit-Dateischutz. Neue Dateien werden automatisch geprüft, auch in den im Netzwerk freigegebenen Ordnern. Wird eine Bedrohung erkannt, versucht das Programm, die Datei zu säubern. Wenn das nicht gelingt, landet die Datei in Quarantäne. Klicken Sie links unten im Fenster auf „Erweiterten Modus aktivieren“. Damit blenden Sie zusätzliche Optionen ein. Gehen Sie auf „Tools → Log-Dateien“. Hier sehen Sie Meldungen zu den erkannten Bedrohungen. Unter „Tools → Quarantäne“ finden Sie eine Liste mit Dateien, die in Quarantäne verschoben wurden. Sollten Sie Vireninfektionen als Irrtum verifizieren, lassen sich solche Dateien wiederherstellen. Mit

```
sudo /opt/eset/esets/sbin/esets_
  scan [Pfad]
```

starten Sie einen Virenscan auf der Kommandozeile.

Das ist nützlich, wenn Sie per SSH mit dem Server verbunden sind und gezielt bestimmte Ordner untersuchen wollen. Wenn die Echtzeitprüfung aktiv ist, sollte das jedoch in der Regel nicht nötig sein.

Tipp: Laden Sie über *http://2016.eicar.org/85-0-Download.html* eine Testdatei herunter, beispielsweise „eicar.com“. Sobald Sie die Datei speichern, sollte jeder Virenscanner Alarm schlagen. Wenn nicht, prüfen Sie die Konfiguration.



Eset Nod32 Antivirus: Dieser Virenscanner bietet eine grafische Oberfläche, die Sie aber nur selten bemühen müssen. Die Echtzeitprüfung beseitigt Schadsoftware automatisch.

Regelmäßige Backups erstellen

Backups auf Freigaben, für die standardmäßig der Schreibzugriff erlaubt ist, sind keine gute Idee. Backups sollten möglichst auf Laufwerken gespeichert werden, die nicht ständig mit dem Windows-PC verbunden. Die Gefahr, dass Backups unter die Kontrolle von Schadsoftware geraten, lässt sich nur reduzieren, wenn Dateien von Windows-Rechnern auf anderem Wege gesichert werden.

Ein empfehlenswertes Tool zum Sichern persönlicher Dateien ist Duplicati (*www.duplicati.com*). Die Software läuft unter Windows, Linux und Mac-OS. Konfiguration und Bedienung erfolgen über eine Weboberfläche im Browser.

Als Backupziel unterstützt das Programm lokale Ordner und Laufwerke, aber auch Onlinespeicher wie Google Drive oder Dropbox. Zum Datenschutz lassen sich die Backups verschlüsseln.

Im lokalen Netzwerk mit einem Linux-Server empfiehlt sich die Sicherung mit Duplicati über SFTP (SSH). Unter Linux muss dazu das Paket „openssh-server“ installiert sein und unter Windows Duplicati. Standardmäßig hat Windows über SSH keinen Zugriff auf den Linux-Server. Die Backups können somit auch nicht durch Schadsoftware kompromittiert werden. ■

Backuptool: Duplicati beherrscht auch die Datensicherung über SFTP (SSH). Windows hat auf den Backupordner keinen Zugriff, weshalb eventuelle Schadsoftware nichts ausrichten kann.

IPTV-Server für das Heimnetzwerk

Im Heimnetz lassen sich mehrere Geräte mit Fernsehprogrammen versorgen. Ein TV-Server stellt dafür die Streams bereit und ermöglicht auch den Mitschnitt von Sendungen.

Fernsehen mit Kodi: Die Mediacentersoftware Kodi bringt auch TV-Kanäle auf den Bildschirm. Dafür ist aber ein eigener IPTV-Server im Netzwerk erforderlich.

VON THORSTEN EGGELING

Die Programme der Fernsehsender können auf unterschiedlichen Wegen auf Ihre Geräte gelangen. Die klassische Methode sind Tuner in Fernsehern oder TV-Receivern, die per Koaxialkabel von einer Satellitenschüssel, einer Antenne oder einem Kabelnetzanbieter versorgt werden. Eine Alternative oder Ergänzung ist Streaming über das Internet. Smart-TVs bieten über Apps beispielsweise Zugriff auf die Mediatheken der öffentlich-rechtlichen Sender und auf kommerzielle Streamingdienste. Ein eigenes Multimedia-Netzwerk können Sie sich aber auch selbst aufbauen. Unterschiedliche Empfangswege wie Fernsehen über Satellit, Antenne oder Internet lassen sich unter einer einheitlichen Oberfläche zusammenfassen und mit weiteren Streamingangeboten kombinieren. Über WLAN oder Ethernet-Kabel verteilen Sie das Angebot an alle Geräte im heimischen Netzwerk.

1. Fernsehen über Kabel, Satellit, Antenne und Internet

Beim Fernsehempfang kommt es auf den Wohnort und die verfügbare Infrastruktur an. In Ballungsräumen ist meist TV über das Kabelnetz (DVB-C/C2) verfügbar. Die zusätzliche „2“ bei diesem und auch den anderen DVB-Standards (Digital Video Broadcasting) weist auf eine weiterentwickelte Technik mit verbesserter Qualität und meist auch höherer Auflösung hin. Aktuelle Geräte unterstützen sowohl das ältere DVD-C als auch DVB-C2. Sie müssen für die Bereitstellung ein Nutzungsentgelt zahlen – auch für sonst frei empfangbare Sender. Wie hoch es ist, hängt von Wohnort und Anbieter ab.

DVB-S beziehungsweise DVB-S2 sind überall verbreitet, wo die Montage einer Satellitenschüssel kein Problem ist. Das Signal erhalten Sie für die frei empfangbaren Sender kostenlos per Satellit, was in Europa über die Astra-Satellitenflotte so gut wie flächendeckend möglich ist. Privatsender gibt es manchmal nur in SD-Qualität gratis, die öffentlich-rechtlichen Sender auch in HD.

Das als Überall-Fernsehen beworbene DVB-T (seit April 2017 DVB-T2) kommt über die Antenne, bietet aber nur ein eingeschränktes Programmangebot. Die öffentlich-rechtlichen Sender gibt es kostenlos. Privatsender sind verschlüsselt und nur nach Abschluss eines Abos zu empfangen (siehe *www.pcwelt.de/2158822*).

Für alle genannten DVB-Techniken benötigen Sie einen Tuner im Fernseher oder ein externes Gerät. Für den PC gibt es Steckkarten oder USB-DVB-Sticks.

TV aus dem Internet: Die meisten öffentlich-rechtlichen Sender streamen das Liveprogramm kostenlos ins Internet. Allerdings wird der Livestream unterbrochen, wenn die Internetlizenz für den Inhalt fehlt, was bei fast allen fremdproduzierten Filmen der Fall ist. International ist die Menge der Streaminganbieter fast unüberschaubar. Eine Google-Suche etwa nach „iptv playlist“ führt Sie zu zahlreichen Adresslisten. Einiges davon ist allerdings wohl halblegal, beispielsweise Server, die aktuelle

Satelliten-TV: Für Astra reicht meist schon eine kleine SAT-Schüssel, wenn Sie freien Blick auf den Satelliten haben. Die wichtigsten deutschsprachigen Sender können Sie kostenlos sehen.

DVB-T2: Terrestrisches Fernsehen kann man über Antenne auch unterwegs auf dem Smartphone nutzen. Der TV-Empfang ist jedoch noch nicht in allen Regionen möglich.

IPTV-Server: Der Telestar Digibit R1 verfügt über vier DVB-S2-Tuner und kann daher gleichzeitig vier Geräte über das Netzwerk mit TV-Programmen versorgen.

Sportereignisse übertragen und dafür wahrscheinlich keine Lizenzen besitzen.

2. Hardware für den eigenen TV-Streamingserver

Für den TV-Empfang am PC benötigen Sie eine TV-Steckkarte oder einen TV-Stick mit dem passenden Tuner. Oft gibt es Kombinationen von DVB-C2/DVB-T2 oder Geräte, die nur DVB-S/S2 empfangen können. Für einen TV-Server sind die Geräte für den PC allerdings kaum empfehlenswert. Nicht jedes Modell lässt sich unter Linux problemlos in Betrieb nehmen. Außerdem steigen CPU-Belastung und Leistungsaufnahme. Wer es trotzdem probieren möchte, findet auf *https://linuxtv.org* Informationen zur den unterstützten Geräten und Hinweise zur Installation.

Besser geeignet sind Netzwerk-TV-Tuner (IPTV-Server), die als unabhängige Geräte DVB im Netzwerk bereitstellen. Die Vorteile: Sie benötigen keinen Treiber, da der Datenaustausch über standardisierte Netzwerkprotokolle erfolgt. Der Betrieb ist auch unabhängig vom PC möglich, etwa mit einer App auf dem Smartphone. Es lassen sich so viele Clients versorgen, wie DVB-Tuner im Gerät stecken.

Bei IPTV-Servern für DVB-S gibt es ein breites Angebot. Eine Übersicht finden Sie auf *www.satip.info*. Es gibt Geräte, die eher für die Montage auf dem Dachboden in der Nähe der Satellitenschüssel gedacht sind, beispielsweise Telestar Digibit Twin mit zwei Tunern (etwa 110 Euro, *https://telestar.de*). Telestar Digibit R1 (etwa 180 Euro, vier Tuner) und Digital Devices Octopus NET V2 S2/2 (etwa 299 Euro, zwei Tuner) sind von der Bauweise her für die Wohnung geeignet. Wo immer Sie die Geräte auch unterbringen, in jedem Fall benötigen Sie ein eigenes Koaxialkabel für jeden DVB-S2-Tuner, das von der Satellitenschüssel zum IPTV-Server führt. Bei DVB-C2 reicht ein einzelnes Koaxialkabel. Die Verteilung kann über einen einfachen Zweigeräteadapter erfolgen. Die Ausgänge im Octopus Net dienen zur Versorgung nachgeschalteter Geräte wie Fernseher oder Set-Top-Box. Für DVB-T2 genügt in Ballungsräumen eine Zimmerantenne mit oder ohne Antennenverstärker. Ist der Sender zu weit entfernt, benötigen Sie eine Dachantenne. Informationen zu den Empfangsgebieten erhalten Sie auf *www.dvb-t2hd.de/empfangscheck*.

Die Verbindung zum Netzwerk erfolgt über ein Ethernet-Kabel. Alternativ sind auch Power-LAN-Adapter oder Ethernet/WLAN-Adapter möglich. Beachten Sie, dass das Netzwerk bei gleichzeitigem Zugriff auf zwei Tunern ungefähr 16 Megabit/s (SD) oder 32 Megabit/s (HD) stabil transportieren muss. Das ist für Fast-Ethernet (100 MBit/s) kein Problem und erst recht nicht für das mittlerweile verbreitete Gigabit-Ethernet (1000 MBit/s). Bei Power-LAN und vor allem bei WLAN kann es unter ungünstigen Bedingungen jedoch knapp werden. Die Folge sind Bildausfälle oder der IPTV-Server ist nicht mehr erreichbar. Sorgen Sie daher für eine optimale WLAN-Abdeckung und Geschwindigkeit.

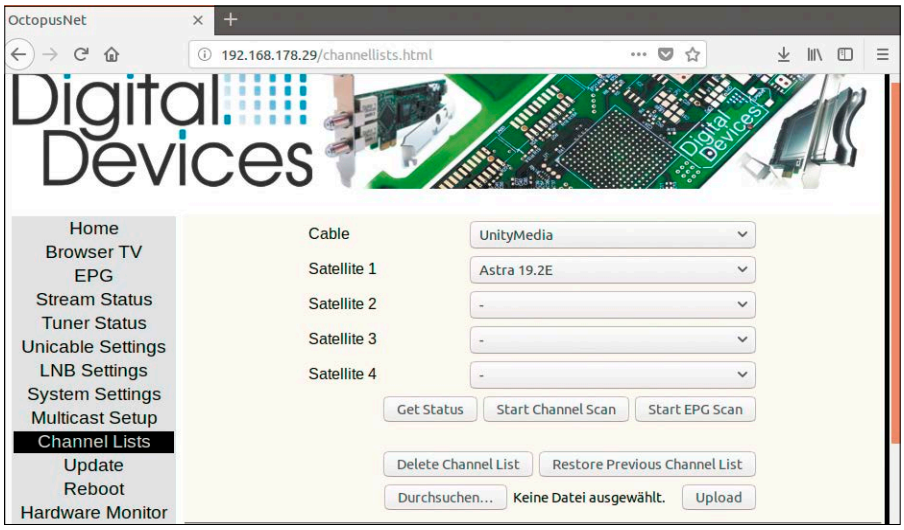
3. IPTV-Server konfigurieren und testen

Nach Inbetriebnahme des Gerätes rufen Sie dessen Weboberfläche mit „http://[IP-Adresse]“ auf. Den Wert für „[IP-Adresse]“ bekommen Sie sie über die Weboberfläche Ihres DSL-Routers oder Kabelmodems heraus, die Sie im Browser beispielsweise über „http://192.168.0.1“ oder

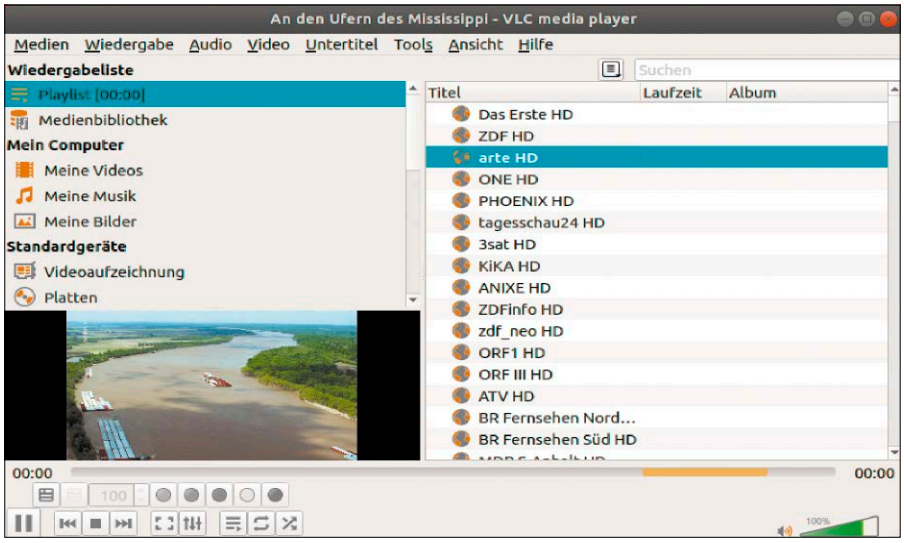
STREAMINGCLIENTS FÜR PC, TV-GERÄT UND SMARTPHONE

Kodi (*https://kodi.tv*) ist eine gut bedienbare Multimedia-Oberfläche mit vielen Funktionen. Sie finden die Software über die Paketverwaltung der meisten Linux-Distributionen und für Android bei Google Play. Für den Raspberry Pi empfiehlt sich die für das Gerät optimierte Distribution Libre Elec, die Kodi enthält. Eine Installationsanleitung finden Sie unter *www.pcwelt.de/2301815*.

Für Tvheadend benötigt Kodi ein Add-on, das Sie unter Linux über das Paket „kodi-pvr-hts“ installieren. Auf dem Raspberry Pi oder unter Android installieren Sie das Add-on „Tvheadend HTSP Client“. In die Konfiguration des Add-ons tragen Sie die IP-Adresse des Tvheadend-Servers ein. Geben Sie Benutzernamen und Passwort des bei Tvheadend angelegten Benutzers an oder lassen Sie die Felder leer, wenn Sie den anonymen Zugriff erlaubt haben (Benutzer „*“). Im Hauptmenü starten Sie die Fernsehwiedergabe über „TV“, indem Sie nach einem Klick auf „Kanäle“ oder „Guide“ zum gewünschten Kanal navigieren. Laufende Sendungen nehmen Sie mit der „Aufnehmen“-Schaltfläche auf. Über den „Guide“ lassen sich Aufzeichnungen auch planen, um sie später in Kodi anzusehen.



IPTV-Server konfigurieren: Die Einstellungen für das Gerät nehmen Sie über die Weboberfläche vor. Sie lassen nach Kanälen suchen, die dann als m3u-Kanalliste abrufbar sind.



VLC als TV-Empfänger: Öffnen Sie die m3u-Kanalliste in VLC. Über die Wiedergabeliste wählen Sie den gewünschten Kanal aus und ein Vorschauvideo erscheint im Fenster.

„http://192.168.178.1" (Fritzbox) erreichen. Suchen Sie in den Einstellungen den DHCP-Server. In diesem Bereich finden Sie meist auch die DHCP-Client-Liste. Bei einer Fritzbox finden Sie die Liste unter „Heimnetz → Heimnetzübersicht".

Die Einrichtung eines IPTV-Servers läuft im Prinzip immer gleich ab. Sie erzeugen auf dem Gerät eine Kanalliste, die dann später die Clients über die IP-Adresse und die verfügbaren Tuner und Kanäle informiert.

Bei einem Octopus Net beispielsweise gehen Sie in der Weboberfläche auf „Channel List", wählen hinter „Cable" (DVB-C) oder „Satellite 1" bis „Satellite 4" (DVB-S) den gewünschten Anbieter aus und klicken auf „Start Channel Scan". Nach Abschluss des Scans laden Sie die m3u-Datei über den Link hinter „Channel List:" herunter. Da es sich um einfache Textdateien handelt, können Sie die m3u-Dateien in einem Editor öffnen und bearbeiten. Entfernen Sie Zeilen mit Sendern, die Sie nicht benötigen, und passen Sie bei Bedarf die Senderbezeichnungen an. Am besten erstellen Sie eine neue m3u-Datei, in die Sie die Zeilen für alle gewünschten SD-, HD- und Radiosender kopieren.

IPTV-Server ausprobieren: Die m3u-Datei öffnen Sie beispielsweise im VLC Mediaplayer. Gehen Sie auf „Ansicht → Wiedergabeliste". In der Liste sehen Sie alle Einträge der Playliste, der Kanal lässt sich per Doppelklick wechseln.

4. Streamingserver Tvheadend installieren

In Ihrem Netzwerk läuft jetzt zwar schon ein IPTV-Server, dem aber ein paar wichtige Funktionen fehlen. Wenn Sie TV-Sendungen auch aufzeichnen wollen und erfahren möchten, was gerade im Fernsehen läuft, benötigen Sie weitere Software.

Tvheadend (*https://tvheadend.org*) ist ein Streamingserver für Linux, der alle verbreiteten DVB-Standards unterstützt. Die Konfiguration erfolgt über eine Weboberfläche im Browser.

Tvheadend läuft unter den meisten Linux-Distributionen, ist aber in der Regel nicht in den Standard-Repositorien enthalten. Wer keinen stromhungrigen PC für den Server verwenden möchte, installiert Tvheadend auf einem Raspberry Pi. Die Installation verläuft bei Raspbian und Ubuntu ähnlich.

Raspberry Pi (Raspbian): Wir gehen davon aus, dass Sie auf dem Raspberry Pi das aktuelle Raspbian Stretch installiert haben (*www.raspberrypi.org/downloads/raspbian*). Führen Sie im Terminal die folgenden fünf Befehle aus:

```
sudo apt install dirmngr apt-
  transport-https
sudo apt-key adv --keyserver hkp://
  keyserver.ubuntu.com:80 --recv-
  keys 379CE192D401AB61
sudo echo "deb https://dl.bintray.
  com/mpmc/deb raspbianstretch
  stable-4.2" | sudo tee -a /etc/apt/
  sources.list
sudo apt update
sudo apt install tvheadend
```

Sie werden aufgefordert, Benutzername und Passwort für den Administrator festzulegen. Diese Daten gelten nur für die Erstinstallation.

Ubuntu 18.04: Bei Ubuntu verwenden Sie diese fünf Befehlszeilen:

```
sudo apt-get install dirmngr
wget -qO- https://doozer.io/keys/
  tvheadend/tvheadend/pgp | sudo
  apt-key add -
sudo echo "deb http://apt.
  tvheadend.org/unstable bionic
  main" | sudo tee -a /etc/apt/
  sources.list.d/tvheadend.list
sudo apt update
sudo apt install tvheadend
```

Geben Sie den Benutzernamen und das Passwort des administrativen Benutzers ein, wenn Sie dazu aufgefordert werden.

5. Tvheadend konfigurieren

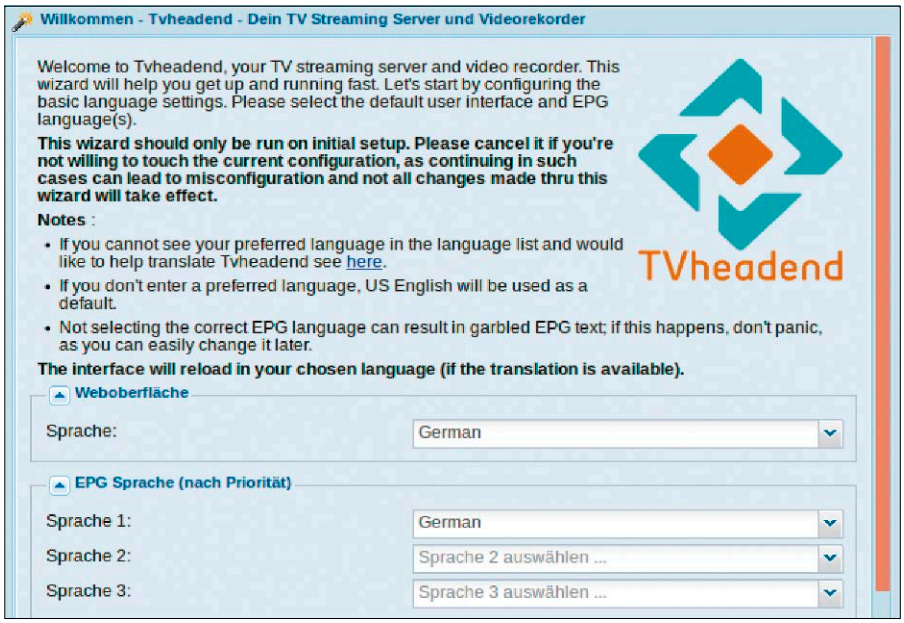
Öffnen Sie im Browser die Adresse „http://[ip-adresse]:9981“. Den Platzhalter „[ip-adresse]“ ersetzen Sie durch die IP-Nummer Ihres Raspberry Pi oder Ubuntu-PCs. Melden Sie sich bei Tvheadend an. Ein Assistent führt durch die nötigen Schritte. Zuerst stellen Sie die Sprache ein und legen dann Benutzernamen und Passwörter für den administrativen Benutzer und einen Standardbenutzer fest. Beim Standardbenutzer verwenden Sie für beides jeweils „*“ (ohne Anführungszeichen), wenn keine Anmeldung erforderlich sein soll. Klicken Sie auf „Save & Next“.

Im Fenster „Netzwerkeinstellungen“ wählen Sie bei „Netzwerk 1“ den Eintrag „IPTV Automatisches Netzwerk“ aus der Liste und klicken auf „Speichern & Weiter“. Tippen Sie die URL ein, über die sich die m3u-Liste vom IPTV-Server herunterladen lässt (siehe Punkt 3), und klicken Sie auf „Speichern & Weiter“. Danach scannt Tvheadhend die verfügbaren Kanäle. Sollte das Programm nichts finden, kann es wahrscheinlich die Liste nicht vom Server abholen. In diesem Fall kopieren Sie die in Punkt 3 heruntergeladene m3u-Datei nach „/home/hts“, beispielsweise unter dem Namen „channels.m3u“. Blättern Sie im Tvheadend-Assistenten zurück und tippen Sie als „URL“

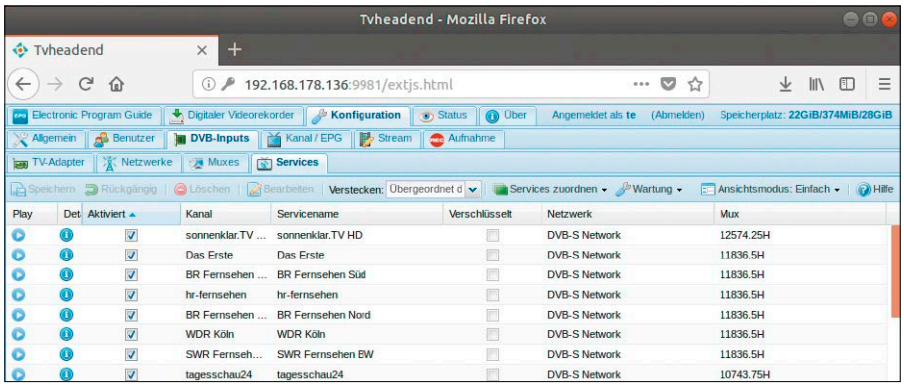
```
file:///home/hts/channels.m3u
```

ein. Wenn Sie jetzt erneut auf „Speichern & Weiter“ klicken, sollte es funktionieren. Sie sehen dann eine Fortschrittsanzeige, die bei DVB-S2 mehrere Hundert Muxes finden sollte. Klicken Sie auf „Speichern & Weiter“, wenn der Vorgang abgeschlossen ist. Im Fenster „Service Mapping“ setzen Sie keine Häkchen, sondern klicken nur auf „Speichern & Weiter“ und danach auf „Fertigstellen“.

Gehen Sie auf „Konfiguration → DVB-Inputs → Services“. Klicken Sie auf „Services zuordnen → Alle Services zuordnen“. Entfernen Sie das Häkchen hinter „Verschlüsselte Services einschließen“ und setzen Sie eines hinter „Verfügbarkeit testen“. Klicken Sie auf „Services zuordnen“. Die Prüfung dauert eine Weile. Danach gehen Sie auf „Konfiguration → Kanal/EPG“. Entfernen Sie die Häkchen in der Spalte „Aktiviert“ bei allen Sendern, die Sie nicht sehen wollen, und klicken Sie auf „Speichern“. In die Spalte „Nummer“ lässt sich nach einem Doppelklick eine Ziffer eintragen und damit die Sortierung der Sender ändern.



Ersteinrichtung: Tvheadend startet mit einem Assistenten, der Sie bei der Konfiguration unterstützt. Es sind nur wenige Schritte nötig, die Kanalsuche dauert jedoch einige Zeit.



Kanalvielfalt: Über DVB-C2 und DVB-S2 empfangen Sie Hunderte von Sendern. Verschlüsselte Angebote lassen sich herausfiltern, für mehr Übersicht sollten Sie die Kanalliste bearbeiten.

6. TV-Streams aus dem Internet einbinden

Streamingangebote aus dem Internet lassen sich ähnlich in Tvheadend einbinden wie die m3u-Liste eines lokalen IPTV-Servers. Eine Übersicht mit Anbietern wie 3sat, Das Erste und ZDF finden Sie über *www.pcwelt.de/IPTV*.

Gehen Sie in der Tvheadend-Weboberfläche auf „Konfiguration → DVB-Inputs → Netzwerke“. Klicken Sie auf „Hinzufügen“, wählen Sie „IPTV Netzwerk“ und tippen Sie eine Bezeichnung ein, beispielsweise „IPTV-Sender“. Klicken Sie auf „Anlegen“. Wechseln Sie dann zur Registerkarte „Muxes“, und klicken Sie auf „Hinzufügen“. Wählen Sie das eben angelegte Netzwerk „IPTV-Sender“. Tragen Sie in das Feld hinter „URL:“ eine Adresse ein, beispielsweise

```
https://zdf1314-lh.akamaihd.
  net/i/de14_v1@392878/master.m3u8
```

für das ZDF („hohe Qualität“, 1280 x 720). Bei den Feldern „Mux-Name:“ und „Servicename:“ tippen Sie jeweils eine aussagekräftige Bezeichnung ein, etwa „ZDF-IPTV“. Klicken Sie auf „Anlegen“. Wechseln Sie auf die Registerkarte „Services“, suchen Sie dort den eben hinzugefügten Servicenamen und klicken Sie ihn an. Gehen Sie auf „Ausgewählte zuordnen → Gewählte Services zuordnen“.

Wechseln Sie danach auf „Kanal /EPG → Kanäle“. Der neue Sender ist hier zu sehen und Sie können ihm in der Spalte „Nummer“ eine Kanalnummer zuweisen. Der externe IPTV-Server erscheint bei den Clients genauso wie die Kanäle des eigenen IPTV-Servers. ■

Multiboot mit Linux & Windows

Alle aktuellen Linux-Distributionen unterstützen die Installation mehrerer Systeme auf einem PC. Die Verfahren sind – abhängig von der Hardware – jedoch unterschiedlich.

Von **Thorsten Eggeling**

© vege - Fotolia.com

Auf einem PC lassen sich beliebig viele Betriebssysteme einrichten, solange der Platz auf der Festplatte dafür ausreicht. Es sind etliche Varianten möglich. Sie können mehrere Linux-Systeme installieren und daneben noch diverse Windows-Versionen. Danach wählen Sie das System, das gerade am besten für eine bestimmte Aufgabe geeignet ist, etwa ein Linux zum sicheren Surfen und Arbeiten und ein Windows für Spiele oder die Steuererklärung.

1. Vorbereitungen für Multiboot

Bevor Sie loslegen, erstellen Sie ein Backup wenigstens der persönlichen Dateien und Einstellungen. Legen Sie sich außerdem passende Rettungs- und Wiederherstellungs-Tools bereit. Auf der Heft-DVD finden Sie mehrere Linux-Distributionen und Reparatur-Systeme. Wie Sie die Linux-Bootumgebung bei Bedarf reparieren, beschreiben wir auf Seite 38 und 44. Das ist auch immer dann nötig, wenn Sie Windows nach Linux installieren.

Windows-Nutzer benötigen eine Windows-Installations-DVD oder einen bootfähigen USB-Stick mit einem Reparatur-System. Unter Windows 8 und 10 legen Sie ein Wiederherstellungslaufwerk an, indem Sie Win-R drücken, *recoverydrive.exe* eintippen, auf „OK“ klicken und dann den Anweisungen des Assistenten folgen.

Optimal ist die Installation zusätzlicher Betriebssysteme auf einer zweiten Festplatte im PC. Die Installationen lassen sich so besser getrennt halten. Ein zweites oder drittes Linux-System lässt sich auch auf einem USB-Laufwerk einrichten (→ Punkt 5).

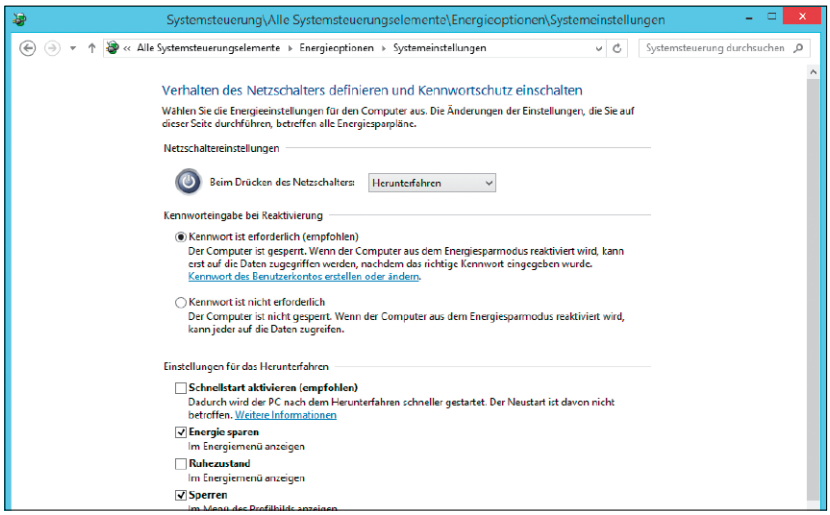
Platz schaffen: Sollte sich nur eine Partition auf Ihrer Festplatte befinden, aber noch genügend Platz frei sein, lassen sich Partitionen verkleinern und dann weitere Partitionen erstellen. Linux-Distributionen wie Ubuntu (mehrere Varianten auf Heft-DVD) bieten das bei der Installation im Setup-Pro-

CSM aktivieren: Auf Uefi-PCs installieren Sie auch Linux um Uefi-Modus. Für den Biosmodus muss eine Option wie „Uefi and Legacy“ aktiviert sein.

gramm an. Ist auf dem PC bisher nur Windows installiert, verkleinern Sie die Partition am besten in Windows über die Datenträgerverwaltung („diskmgmt.msc“). Klicken Sie mit der rechten Maustaste auf die gewünschte Partition, und wählen Sie im Menü „Volume verkleinern“. Alternativ verwenden Sie Parted Magic (bootfähig auf Heft-DVD).

Bios und Uefi: Neuere PCs und Notebooks besitzen eine Uefi-Firmware (Unified Extensible Firmware Interface), und Windows 8 und 10 sind immer im Uefi-Modus auf einer GPT-Partition vorinstalliert (GUID Partition Table). Sollen mehrere Systeme auf die gleiche Festplatte, müssen Sie alle im Uefi-Modus installieren. Auf einer zweiten Festplatte können Sie auch eine herkömmliche MBR-Partition verwenden (Master Boot Record).

Damit die Installation reibungslos abläuft, müssen Sie einige Einstellungen im Bios/Firmware-Setup des PCs ändern. Ins Setup kommen Sie direkt nach Einschalten des PCs meist über Tasten wie Entf, Esc oder F2. Bei neueren Uefi-PCs mit vorinstalliertem Windows 8 oder 10 klicken Sie im Anmeldebildschirm rechts unten auf das Ausschaltknopf-Symbol, halten die Shift-Taste gedrückt und klicken auf „Neu starten“. Es erscheint ein Menü, in dem Sie auf „Problembehandlung → Erweiterte Optionen → Uefi-Firmwareeinstellung“ gehen und dann auf „Neu starten“ klicken.



Hybrider Standby-Modus: Deaktivieren Sie bei Windows 8 den Schnellstart. Sie haben sonst von Linux aus keinen Zugriff darauf, oder das Dateisystem wird beschädigt.

Im Bios-Setup müssen Sie die Bios-Emulation „CSM Support“ (Compatibility Support Module) „Uefi with CSM“ oder „Legacy Boot“ aktivieren, damit sich Systeme auch im Bios-Modus starten und installieren lassen (→ Punkt 2). Wenn Sie nur im Uefi-Modus installieren möchten (→ Punkt 3), darf die Option auch auf „Uefi Only“ oder ähnlich gesetzt sein. Schalten Sie außerdem „Secure Boot“ ab, das in Multiboot-Umgebungen oft Probleme bereitet. Deaktivieren Sie außerdem Optionen wie „Fastboot“, sonst funktioniert die USB-Tastatur wahrscheinlich nicht, wenn Sie von einer DVD booten. Bei der Gelegenheit können Sie auch gleich die Bootreihenfolge so einstellen, dass der PC primär von DVD oder USB-Stick bootet.

Systeme entfernen und Bootumgebung wiederherstellen

Sie wollen Linux entfernen und die Windows-Bootumgebung auf den Originalzustand zurücksetzen? Wenn Sie Linux samt Grub auf eigener Festplatte installiert haben, können Sie diese bei einem Bios-System einfach neu formatieren. Befinden sich Windows und Linux dagegen auf der gleichen Festplatte, oder der Bootmanager liegt auf der Windows-Systemplatte, booten Sie den PC von der Windows-Installations-DVD. Sobald das Fenster „Windows-Setup“ erscheint, drücken Sie die Tastenkombination Shift-F10 und führen folgenden Befehl aus:

```
bootrec /fixmbr
```

Damit entfernen Sie Grub, und Windows startet dann wieder direkt. Unter Windows löschen Sie über die Datenträgerverwaltung die Linux-Partition.

Bei einem Uefi-System liegen die Startdateien in der EFI-Partition. Löschen Sie vom noch installierten Linux-System aus unter „/boot/efi“ das Verzeichnis der jeweiligen Distribution, beispielsweise „ubuntu“.

Lassen Sie sich dann mit

```
sudo efibootmgr
```

die Booteinträge im NVRAM der PC-Firmware anzeigen. Sie finden hier Einträge wie „Boot0000* ubuntu“, die Sie mit *sudo efibootmgr -b 0000 -B* entfernen. Wahrscheinlich gibt es mehrere Einträge, die sich auf das zu löschende System beziehen, die Sie alle entfernen. Anschließend setzen Sie die Bootreihenfolge mit einem Befehl wie

```
sudo efibootmgr -o 0002,0000,0003,0004
```

Die laufenden Nummern tragen Sie gemäß der Ausgabe von efibootmgr in der gewünschten Reihenfolge ein. Der Eintrag für Windows steht an erster Stelle.

Sie wollen die Windows-Installation entfernen? Formatieren Sie mit Gparted die Windows-Partition etwa mit dem Dateisystem Ext4. Bei einem Uefi-System löschen Sie unter „/boot/efi“ die Ordner „Boot“ und „Microsoft“. Mit efibootmgr entfernen Sie dann wie oben beschrieben alle Einträge, die sich auf Windows beziehen, und ändern die Bootreihenfolge so, das Linux zuerst startet. Starten Sie in einem Terminalfenster *sudo update-grub*, um Windows aus dem Bootmenü zu entfernen.

Linux neben Windows 8 oder 10: Schalten Sie unter diesen Windows-Versionen den hybriden Standby-Modus ab. Ist dieser aktiv, verweigern neuere Linux-Systeme den Zugriff auf die Windows-Partition, während ältere bei Schreibzugriffen eventuell das Windows-Dateisystem beschädigen. Dazu entfernen Sie unter „Systemsteuerung → Energieoptionen → Auswählen, was beim Drücken des Netzschalters geschieht“ das Häkchen vor „Schnellstart aktivieren (empfohlen)“ und klicken auf „Änderungen speichern“. Sollte die Option ausgegraut sein, klicken Sie auf „Einige Einstellungen sind momentan nicht verfügbar“.

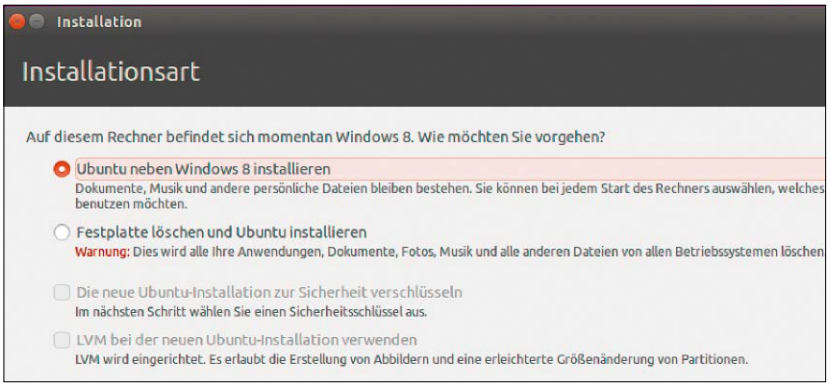
2. Linux neben Windows im Bios-Modus

Windows benötigt mindestens eine Partition auf der Festplatte, Linux standardmäßig zwei: eine für das System und eine für die Swap-Partition. Für die Parallelinstallation von Linux ist eine zweite Festplatte optimal.

Installationsmedium: Auf Heft-DVD finden Sie bootfähige Versionen mehrerer Ubuntu-Systeme. Diese unterscheiden sich vor allem durch die Desktop-Umgebung. Wir verwenden für diesen Artikel Ubuntu 15.04, die Installation verläuft jedoch bei allen Ubuntu-Varianten ähnlich.

Installation im Bios-Modus: Booten Sie den PC von Heft-DVD oder einem mit Unetbootin erstellten Installations-Stick. Eventuell müssen Sie die Bootreihenfolge im Bios-Setup (→ Punkt 1) umstellen oder das Bootmenü des Bios aufrufen. Wählen Sie das gewünschte Linux über die DVD-Oberfläche aus, für unser Beispiel Ubuntu 15.04.

Auf dem Ubuntu-Desktop starten Sie das Setup mit dem Link „Ubuntu 15.04 installieren“. Wählen Sie als Sprache „Deutsch“ aus und klicken Sie auf „Weiter“. Setzen Sie Häkchen vor „Aktualisierungen während der Installation herunterladen“ und „Software von Drittanbietern installieren“ (für MP3-Unterstützung), und klicken Sie auf „Weiter“. Danach gibt es folgende Möglichkeiten:



Installationsart: Der Setup-Assistent bietet „Ubuntu neben Windows 8 installieren“ an, wenn er eine Windows-Installation auf der Festplatte findet.

1. Windows belegt die komplette Festplatte: Wählen Sie im Fenster „Installationsart“ die Option „Ubuntu neben Windows 8 installieren“. Nach einem Klick auf „Weiter“ zeigt Ihnen das Setup-Programm die vorgeschlagene Partitionsaufteilung. Ziehen Sie mit der Maus die Linie zwischen den Partitionen an eine andere Position, um die Aufteilung zu verändern. Klicken Sie auf „Jetzt installieren“.

2. Im PC steckt nur eine Festplatte, und darauf gibt es eine freie Partition: Wählen Sie „Ubuntu neben Windows 8 installieren“ und klicken Sie auf „Jetzt installieren“. Es erscheint eine Übersicht mit den Partitionen, die das Setup-Programm neu anlegen und formatieren wird. Prüfen Sie diese Angaben, damit nicht versehentlich die falschen Partitionen gelöscht werden. Bestätigen Sie mit „Weiter“.

3. Es gibt eine zweite leere Festplatte: Das Fenster „Installationsart“ bietet die Option „Festplatte löschen und Ubuntu installieren“. Nach einen Klick auf „Weiter“ wählen Sie die zweite Festplatte aus und klicken auf „Jetzt installieren“. Auch hier prüfen Sie die Auswahl sorgfältig, damit die Windows-Partition nicht gelöscht wird – es sei denn, Sie wollen Windows durch Linux ersetzen.

4. Benutzerdefiniert installieren: Den Bootloader erstellt das Setup-Programm bei allen zuvor beschriebenen Optionen in jedem Fall auf die Bootfestplatte. Das ist komfortabel und an sich kein Problem, erschwert aber die spätere Deinstallation. Deshalb ist es besser, den PC vorübergehend nur mit der neuen leeren Festplatte zu starten. Eine Alternative ist, im Setup-Assistenten „Etwas Anders“ zu wählen und dann die Linux-Partitionen manuell anzulegen, sinngemäß wie unter → Punkt 4 beschrieben.

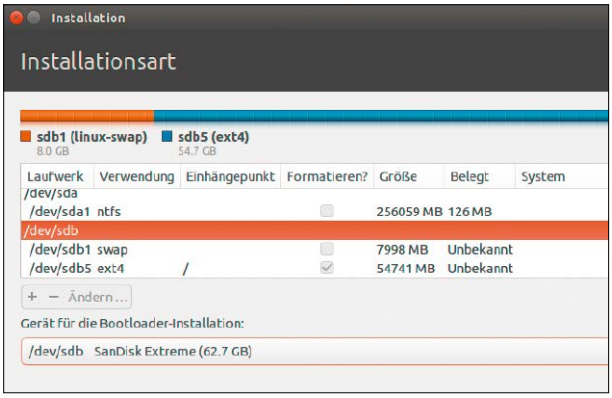
Bei „Gerät für die Bootloader-Installation“ geben Sie die Festplatte an, auf der Sie Linux installieren wollen. Wer häufig mit anderen Systemen experimentiert, kann auch einen USB-Stick als Ziellaufwerk angeben.

Starten Sie den PC nach Abschluss der Installation neu. Es begrüßt Sie der Bootmanager Grub, über den Sie Linux oder Windows starten. Wenn sich der Bootloader auf einer zweiten Festplatte oder dem USB-Stick befindet, booten Sie den PC von diesem Gerät.

3. Linux und Windows im Uefi-Modus

Alle bootfähigen Systeme auf Heft-DVD sind dort auch als ISO-Images enthalten (unter „/Image-Dateien“). Schreiben Sie die Datei des gewünschten 64-Bit-Systems von der Heft-DVD mit Unetbootin (auf Heft-DVD) einen bootfähigen USB-Stick, oder brennen Sie aus dem ISO eine Installations-DVD. Rufen Sie kurz nach dem Start das Bootmenü der Firmware auf. Wählen Sie den Eintrag mit vorangestelltem „Uefi“. Anders als bei der Bios-Installation sehen Sie ein Grub-2-Bootmenü, in dem Sie „Try Ubuntu without installing“ wählen. Per Doppelklick auf „In-

Ubuntu erkennt Windows auch im Uefi-Modus. Bei der Parallelinstallation entsteht ein neuer Eintrag im Bootmenü der Firmware.



Ubuntu mobil: Für die Installation auf USB partitionieren Sie manuell. Ganz wichtig ist, dass der Bootloader auf dem Stick landet.

stall Ubuntu 15.04“ starten Sie das Setup-Programm. Wählen Sie die Sprache, und klicken Sie auf „Weiter“. Setzen Sie Häkchen vor „Aktualisierungen während der Installation herunterladen“ und „Software von Drittanbietern installieren“, und klicken Sie auf „Weiter“.

Im Fenster „Installationsart“ zeigt der Setup-Assistent ähnliche Optionen wie bei der Bios-Installation. „Ubuntu neben Windows Boot Manager installieren“ wählen Sie für die Installation auf der gleichen Festplatte. Sollte keine freie Partition vorhanden sein, haben Sie Gelegenheit, die Windows-Partition zu verkleinern. Klicken Sie die Option „Festplatte löschen und Ubuntu installieren“ an, wenn Sie Linux auf einer zweiten Festplatte installieren oder Windows durch Linux ersetzen möchten. Nach Abschluss der Installation starten Sie den PC neu. Über das Grub-Bootmenü wählen Sie zwischen Linux und Windows.

4. Mehrere Linux-Systeme auf einem PC

Es würde den Rahmen dieses Artikels sprengen, auf alle möglichen Parallelinstallationen von Linux-Systemen einzugehen. In der Regel gilt: Gleichartige Systeme lassen sich meist problemlos nebeneinander einrichten – so etwa alle Distributionen, die auf Ubuntu/Debian basieren (Ubuntu, Linux Mint, Lubuntu, Xubuntu). Die jeweiligen Setup-Programme erkennen die bereits vorhandene Distribution und bieten eine Parallelinstallation mit Optionen an, wie in → Punkt 2 für Windows beschrieben.

Distributionen wie Open Suse, Fedora oder Debian entdecken eine Ubuntu-Installation nicht, und Ubuntu findet keine Fremdsysteme. Die jeweiligen Setup-Tools bieten dann standardmäßig nur an, die Festplatte zu formatieren und eine Neuinstallation durchzuführen. Wählen Sie in diesem Fall eine leere Partition aus, die Sie möglichst zuvor im bereits installierten System erstellt haben. Wenn das Setup eine entsprechende Option bietet, wählen Sie als Ziel für den Bootloader die Root-Partition („\“) aus, also das Ziel-Laufwerk der neuen Installation.

Oft lässt sich die Einrichtung des Bootloaders auch verhindern. Bei der Installation etwa von Ubuntu nach Open Suse öffnen Sie im Ubuntu-Installationssystem ein Terminal und geben dort folgenden Befehl ein:

```
ubiquity -b
```

Installieren Sie das System dann in einer freien Partition oder auf einer zweiten Festplatte. Durch den Schalter „-b“ unterbleibt die Installation des Bootloaders. Verwenden Sie dann in Open Suse folgenden Terminalbefehl:

```
sudo update-bootloader --refresh
```

Damit binden Sie Ubuntu in das Open-Suse-Bootmenü ein. War zuerst Ubuntu auf der Festplatte, veranlassen Sie Grub, mit *update-grub* nach neuen Installationen zu suchen. Die genannten Befehle zur Aktualisierung der Grub-Konfiguration funktionieren bei Bios- wie bei Uefi-Systemen. Es ist außerdem möglich, den Bootloader auf USB-Stick, das System aber auf der Festplatte einzurichten, sinngemäß wie in → Punkt 5 beschrieben.

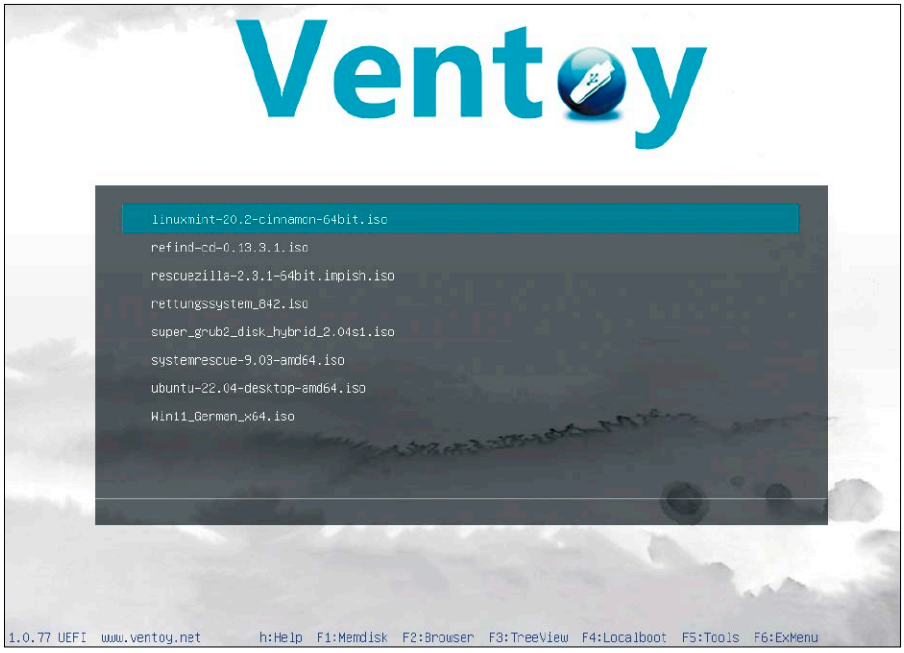
5. Linux auf einem USB-Gerät einrichten

Für die Installation auf einem USB-Gerät booten Sie Ubuntu von DVD oder einem USB-Stick wie unter → Punkt 2 beschrieben. Wählen Sie im Fenster „Installationsart“ die Option „Etwas Anderes“. In der Regel wird sich auf einer USB-Festplatte oder einem USB-Stick nur eine Partition befinden. Löschen Sie diese über die Schaltfläche „-“. Alle darauf befindlichen Daten gehen verloren. Erstellen Sie über die Schaltfläche „+“ eine kleine Partition für die Auslagerungsdatei („Swap“). Als Faustregel gilt: Der Swap-Speicher sollte etwa 20 bis 30 Prozent größer sein als der Hauptspeicher (RAM). Auf die gleiche Weise legen Sie eine große Partition für das Linux-System an. Hier wählen Sie hinter „Einbindungspunkt“ den Eintrag „/“ aus der Liste. Unter „Gerät für die Bootloader-Installation“ wählen Sie das USB-Gerät aus, meist ist das „/dev/sdb“. Kontrollieren Sie diese Angabe genau. Wenn Sie den Bootloader auf die Festplatte schreiben, startet das System von der Festplatte ohne angeschlossenes USB-Gerät nicht mehr. Klicken Sie zum Abschluss auf „Jetzt installieren“, und folgen Sie den weiteren Anweisungen des Setup-Programms. ●

Werkzeuge für Linux auf USB

Linux läuft sowohl als Livesystem als auch normal installiert auf USB-Datenträgern. Beide Varianten erlauben auch das Multiboot von mehreren Systemen. Vor allem das Bündeln von Livesystemen auf einen einzigen Stick gelingt mit den passenden Tools spielend.

VON HERMANN APFELBÖCK



Dieser Beitrag erklärt die empfehlenswerten technischen Werkzeuge, um Linux-ISO-Abbilder startklar auf USB befördern. Diese automatisierten Tools erlauben auch unerfahrenen Nutzern, mobile Livesysteme, individuell angepasste Zweitsysteme oder ganze Sammlungen von Reparaturtools und Installationsmedien zu bauen. Die reguläre Installation eines oder mehrerer Linux-Systeme auf USB-Stick ist aufwendiger. Hier ist der Lohn ein updatefähiges, beliebig erweiterbares Linux auf dem mobilen Datenträger.

Werkzeuge für Einzelsysteme

Rohkopierer befördern den Inhalt der ISO-Abbilder beginnend mit dem MBR- und der Uefi-Bootumgebung bis zum letzten Bit bitgenau auf den USB-Stick. Wenn die ISO-Datei diese beiden Bootumgebungen mitbringt (hybrid), wird das so kopierte Livesystem überall starten. Terminal-Klassiker unter Linux ist dd mit seiner einfachen Syntax mit Inputfile (if) und Outputfile (of):

```
sudo dd if=ubuntu.iso of=/dev/sdc
```

Genau dasselbe machen simple Tools wie Win 32 Disk Imager (für Windows) oder USB Imager (für Linux/Windows/Mac-OS, auf Heft-DVD), ebenso auch der überschätzte Etcher (für Linux/Windows/Mac-OS). Auf dem Stick befindet sich dann neben der Bootumgebung für MBR und Uefi eine große, schreibgeschützte ISO-9660-Partition, die den kompletten Datenträger belegt, selbst wenn das kopierte ISO-Abbild nur einen Bruchteil benötigen würde. Jede anderweitige Nutzung des Sticks – für Daten oder weitere Systeme – scheidet daher aus. Der Stick erhält genau ein Livesystem zur Installation einer Linux-Distribution oder zur sonstigen Nutzung.

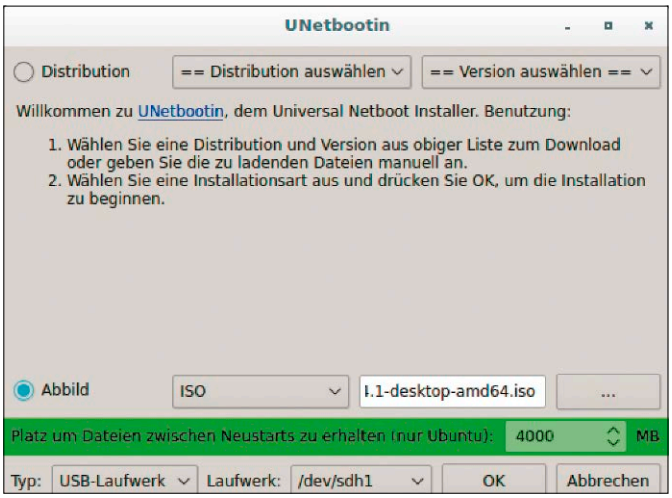
Das Tool Unetbootin (für Linux, Windows und Mac-OS, auf Heft-DVD, Download *https://unetbootin.github.io*) war ehemals ein Hilfsprogramm, um ISO-Abbilder ohne hybride MBR- und Uefi-Bootumgebung überall bootfähig zu machen. Dazu legt Unetbootin eine eigene Bootumgebung an und die eigentlichen Daten des Livesystems landen auf einer FAT32-Partition, die den gesamten restlichen Platz des USB-Sticks einnimmt. Der Stick muss vor dem Unetbootin-Einsatz mit FAT32 formatiert werden. Bei größeren Sticks funktioniert das nur unter Linux, weil Windows für Sticks jenseits von 32 GB nur NTFS oder exFAT anbietet.

Da inzwischen fast alle Linux-ISO-Abbilder hybrid booten können, scheint Unetbootin überflüssig. Aber das trifft nicht zu: Anders als bei Rohkopierern wie dd ist der nicht belegte Platz auf der FAT32-Partition beliebig für Daten nutzbar. Zwar ist Multiboot bei Unetbootin-Sticks ausgeschlossen, aber eine multifunktionale Nutzung des Sticks als System- und Datenmedium ist möglich (für Dateigrößen bis vier GB).

Hinzu kommt bei Unetbootin der Vorzug eines optionalen Persistenzspeichers für alle Ubuntu-basierten Livesysteme. Beim Kopieren solcher Systeme erscheint im Pro-

grammfenster automatisch die Option „Platz um Dateien zwischen Neustarts zu erhalten“. Ein Wert wie „2000“ oder „4000“ MB ermöglicht es, im späteren Livesystem Programme zu installieren oder das System individuell einzurichten.

Unetbootin muss – wie alle Imagetools – mit root/sudo-Recht oder unter Windows als „Administrator“ gestartet werden. Generell gibt es bei Unetbootin zwei Methoden, um ISO-Images zu kopieren – entweder mit der Option „Abbild“, falls die ISO-Datei bereits lokal vorliegt, oder mit der Option „Distribution auswählen“, die das gewählte Abbild erst aus dem Internet holt. Bei der Auswahl des Laufwerks ist Sorgfalt und absolute Gewissheit erforderlich, weil der Datenträger komplett überschrieben wird.



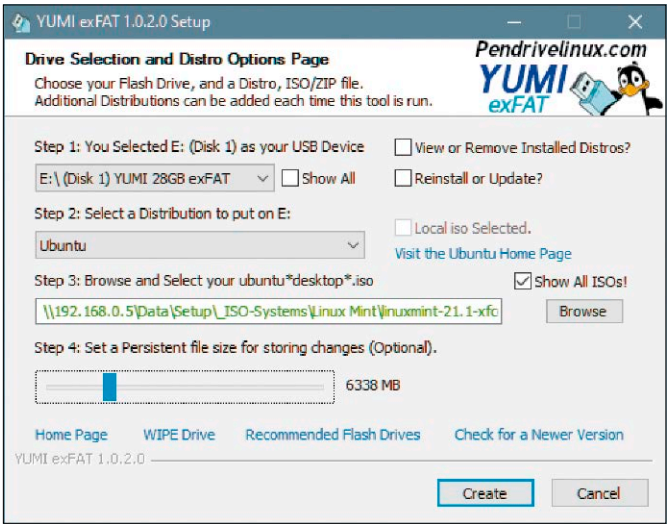
Nutzen Sie in Unetbootin, Yumi und Ventoy das Angebot der Persistenz. Dann kann das (Ubuntu-)Livesystem Einstellungen speichern und zusätzliche Software installieren.

Yumi: Multiboot-Stick

Yumi (Your Universal Multiboot Installer) gibt es nur noch für Windows. Die Linux-Variante wird nicht mehr weiter gepflegt. Wählen Sie auf der Downloadseite *www.pendrivelinux.com/yumi-multiboot-usb-creator* die Variante „YUMI exFAT“ (die Varianten „YUMI Legacy“ und „YUMI UEFI“ werden zwar noch angeboten, aber seit zwei Jahren nicht mehr gepflegt). Yumi benötigt unter Windows keine Installation – einfach herunterladen, die ausführbare Datei starten und loslegen. Das englischsprachige Tool kann mehrere Linux-Systeme auf exFAT-formatierte USB-Sticks befördern und die Livesysteme beim Booten in einem Auswahlmenü anbieten. Großer Vorzug von Yumi ist die Tatsache, dass das Tool für jedes Ubuntu-basierte System sehr bequem Persistenzspeicher einrichten kann und dabei sehr einfach in der Benutzung ist – quasi ein Unetbootin mit Wiederholschleife für Multiboot.

Die wenigen Schritte sind ähnlich wie bei Unetbootin: Sie wählen mit „Step 1“ das gewünschte Ziellaufwerk, mit „Step 2“ die Distribution und im letzten Schritt „Step 3“ das ISO-Image der gewünschten Linux-Distribution. Bei der Auswahl der ISO-Datei zeigt Yumi nur Dateiobjekte an, die zur Distribution passen, die Sie vorher in „Step 2“ gewählt haben (es sei denn Sie aktivieren die Option „Show all ISOs“).

Dies ist deswegen notwendig, weil Yumi zwar sehr viele, aber nicht alle Linux-Systeme booten kann. Wählen Sie daher in „Step 2“ immer präzise aus, damit Yumi die passende Bootumgebung einrichtet. Systeme, die hier nicht aufgelistet sind, können Sie unter Angabe eines technisch verwandten Systems ohne Gewähr kopieren. Yumi kann auch ISO-Images aus dem Internet laden. Dazu wählen Sie mit „Step 2“ die Distribution und aktivieren dann das Kästchen „Download Link“.



Yumi im Installermodus: Das Windows-Tool hat längst nicht die Möglichkeiten von Ventoy, ist aber sehr einfach zu bedienen und bietet Persistenz über einen simplen Schieberegler.

Bei allen Ubuntu-basierten Systemen erscheint nach „Step 3“ ein zusätzlicher „Step 4“, mit dem Sie dem System einen persistenten Speicher und damit begrenzte Anpassungsfähigkeit spendieren können.

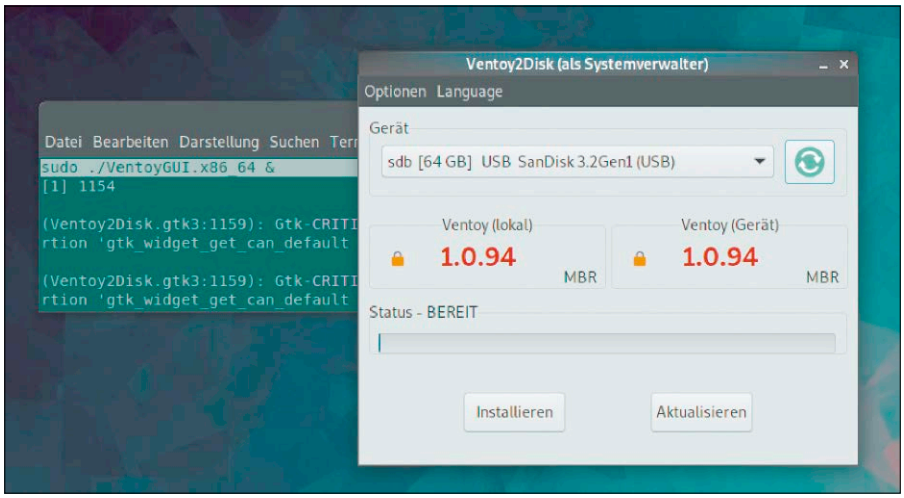
Nach absolvierter Kopie fragt Yumi jedes Mal automatisch nach: „Would you like to

PERSISTENZSPEICHER FÜR LIVESYSTEME

Zusätzlicher „Persistenz“-Speicher macht die an sich eingefrorenen Linux-Livesysteme deutlich flexibler. Damit werden Konfigurationsänderungen, Updates, Softwareeinstellungen und sogar größere Installationen dauerhaft gespeichert. Dieser flexible Speicherplatz wird außerhalb des eigentlichen Systems in einer großen Datei (oder Partition) angelegt und beim Start in das System eingebunden. Notwendige Voraussetzung ist dafür ein beschreibbares Dateisystem, wie es die hier beschriebenen Tools Unetbootin, Yumi und Ventoy anlegen. Es gibt außerdem typische Livedistributionen wie Puppy Linux oder Knoppix, die diese Möglichkeit selbst mitbringen. Mit Rohkopierern wie dd geschriebene Livesysteme können keine Persistenz anbieten.

add more ISOs...". Mit „Ja" oder „Yes" können Sie dann nach demselben Strickmuster weitere Systeme aufnehmen, solange der Platz reicht. Beim Booten des Datenträgers erscheint der Yumi-Bootloader: Der bietet unter „Linux Distributions" die eingerichteten Systeme auf USB. Nach 30 Sekunden Wartezeit ohne Auswahl bootet standardmäßig das festinstallierte System der ersten Festplatte.

Yumi kann auf einem früher erstellten Multiboot-Stick nachträglich Systeme hinzufügen oder entfernen. Beim Erweitern gehen Sie einfach so vor wie oben beschrieben. Sie erhalten dabei zwar keinen Hinweis auf die bereits vorhandenen Systeme, aber diese bleiben unangetastet. Für das Löschen aktivieren Sie die Option „View or Remove Installed Distros".



Ventoy-Initialisierung: Einmal „Installieren" geklickt, ist die Hauptsache schon erledigt. Die gewünschten ISO-Abbilder kopieren Sie danach einfach auf die Ventoy-Datenpartition des Sticks.

Ventoy: ISO-Abbilder auf Stick

Ventoy ist das technisch eleganteste, funktionsreichste, im Detail aber etwas kompliziertere Multiboot-Werkzeug. Die folgenden zwei Abschnitte beschreiben nur die fundamentalen Optionen dieses Boot-Kosmos. Für alltägliches Live-Multiboot muss man einen USB-Stick nur einmal mit Ventoy initialisieren und benötigt die Software danach für diesen Stick nicht mehr. Alles Weitere funktioniert auf einfacher Dateiebene durch Kopieren und Löschen auf dem Stick. Ventoy geht nämlich einen anderen Weg als andere Imagetools und nutzt die Fähigkeit des Grub-Bootmanagers, ISO-Dateien direkt zu starten. Man kopiert einfach die ISO-Dateien der gewünschten Livesysteme auf den USB-Stick, alles Weitere erledigt Ventoy automatisch im Hintergrund. Es findet die ISO-Dateien, baut sie in die Grub-Konfiguration ein und erstellt oder aktualisiert das Auswahlmenü, über das sich die Livesysteme booten lassen. Das funktioniert mit praktisch allen bekannten Linux-Distributionen plus Windows.

Ventoy gibt es für Linux und Windows (außerdem noch als unabhängiges ISO-Livesystem). Für Linux wählen Sie unter *https://github.com/ventoy/Ventoy/releases* das Archiv „ventoy-1.0.94-linux.tar.gz", für Windows das entsprechende ZIP-Archiv. Nach dem Entpacken in ein beliebiges Verzeichnis starten Sie dort mit

```
sudo ./VentoyGUI.x86_64
```

das Ventoy-Hauptprogramm (unter Windows das Programm „Ventoy2Disk.exe"). Der Dialog ist einfach und die optionale Umstellung über „Language" auf Deutsch kaum nötig. Unter „Gerät" wählen Sie den gewünschten USB-Stick aus und klicken auf „Installieren". Das ist dann schon die gesamte Aktion: Der Stick wird neu formatiert und alle enthaltenen Daten gehen verloren. Dabei entsteht eine kleine 32-MB-Partition mit Grub und den Bootloader-Dateien für Uefi-Boot, außerdem sorgt ein MBR dafür, dass der Stick auch im Bios-Modus bootet. Den gesamten Rest des Datenträgers übernimmt die zweite, große Partition mit dem Dateisystem exFAT. Mit diesem Microsoft-Dateisystem können alle aktuellen Linux-Distributionen umgehen und sie zeigen sofort nach der Aktion die Datenpartition als Gerät „Ventoy" im Dateimanager: Dorthin kopieren Sie nun einfach die gewünschten ISO-Dateien.

Beim Booten eines Rechners mit dem Ventoy-Stick werden Sie in einem Menü sämtliche vorher kopierten Abbilder vorfinden – in einfacher alphabetischer Reihenfolge der Dateinamen. Wer dies möchte, kann typische ISO-Namen wie „q4os-5.2-x64-tde.r1.iso" schon beim ersten Kopieren oder nachträglich lesbarer umbenennen – etwa „Q4-OS.5.2.iso". Die Erweiterung „.iso" muss bleiben und Versionsnummern sind sinnvoll, um veraltete Versionen leicht zu erkennen (und bei Bedarf auszutauschen). Natürlich kann die exFAT-Partition zusätzlich Ordner und Benutzerdaten aller Art enthalten. Alles, was nicht die Endung „.iso" trägt, ignoriert das Ventoy-Menü.

Bei Uefi-Boot und aktiviertem „Secure Boot" wird beim ersten Start der Hinweis „Access denied" erscheinen, den Sie zunächst mit „OK" übergehen und dann mit „Enroll key from disk" und einem Neustart korrigieren.

Ventoy-Livesysteme mit Persistenz

Die Flexibilität durch Persistenzspeicher (für Ubuntus) unterstützt Ventoy großzügiger als Yumi oder Unetbootin, jedoch ist es hier mit einem einfachen Schieberegler nicht getan. Das Prozedere ist komplizierter und setzt voraus, dass Sie an einem PC mit der Ventoy-Software und mit eingelegtem Ventoy-Stick arbeiten:

1. Erstellen Sie im Terminal und im Verzeichnis der Ventoy-Software (nicht im Stick) mit

```
sudo sh ./CreatePersistentImg.sh
  -s 2048
```

die Persistenzdatei. Wenn Sie keine Größe angeben („-s" für „size") entsteht eine Datei „persistence.dat" mit einem GB. Verschieben Sie die Datei dann in die exFAT-Partition des „Ventoy"-Sticks, wo auch die ISO-Dateien liegen.

Wichtiger Hinweis: Der Standardname „persistence.dat" darf geändert werden, etwa zu „Xubuntu_Persistence.dat", wenn die Persistenzdatei einem Xubuntu zugeordnet werden soll. Das ist deswegen wichtig, weil Sie vielleicht für mehrere Systeme des Sticks eine Persistenzdatei einrichten möchten (theoretisch ist es sogar möglich, einem System mehrere Persistenzdateien zuzuweisen).

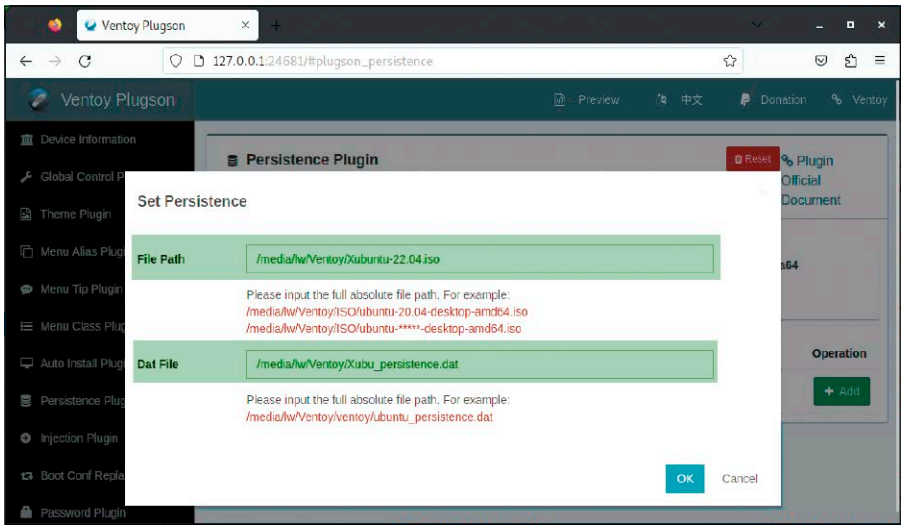
2. Zurück im Verzeichnis der Ventoy-Software starten Sie folgendes Ventoy-Script im Terminal:

```
sudo sh ./VentoyPlugson.sh /dev/
  sd[X]
```

„[X]“ ersetzen Sie durch den Buchstaben, über den der Ventoy-Stick erreichbar ist – etwa „/dev/sdc“. Das Script startet eine Weboberfläche und zeigt dessen Adresse *http://127.0.0.1:24681*, die Sie im Browser des lokalen Systems aufrufen.

3. Gehen Sie dort in der linken Navigationsspalte auf „Persistence Plugin“. Mit „+ Add“ verknüpfen Sie nun die Persistenzdatei mit dem passenden ISO, indem Sie für beide den kompletten Pfad in die vorgesehenen Felder eintragen (siehe Abbildung).

4. Beim späteren Start des Livesystems kommt dann noch eine Option hinzu: Sie können das System ab sofort wahlweise mit oder ohne Persistenzdatei laden.



Ventoy ermöglicht Persistenz für mehrere Systeme, sogar mehrere Persistenzspeicher für ein System. Die Einrichtung erfordert aber etwas Handarbeit.

USB-Multiboot: Ordentlich installiert

Persistenz macht Livesysteme zwar deutlich flexibler, aber Livesysteme bleiben sie dennoch. Ein Multiboot-Stick mit Live-Linux bleibt daher immer ein pragmatischer Werkzeugkasten oder eine Installersammlung. Für individuell eingerichtete Desktopsysteme ist echte Installation auf USB-Stick die bessere Alternative. So genutzte Systeme sind updatefähig, beliebig erweiterbar und verwenden das eingerichtete Benutzerkonto.

Der genutzte USB-Datenträger muss entsprechend groß sein – 128 GB aufwärts sollten für zwei bis vier kleinere Systeme ausreichen.

Bei Uefi-Partitionsstil schreiben Linux-Installer die Bootinformation grundsätzlich in die bereits bestehende EFI-Partition, selbst wenn der Benutzer bei der Installation ein anderes Ziel angibt. Konfliktfrei funktioniert das Ganze daher nur, wenn der Installer die interne(n) Festplatte(n) erst gar nicht sieht (vorübergehend abklemmen) oder wenn für den Stick der alte MBR-Partitionsstil gewählt wird. Da auch moderne Rechnerfirmware den alten MBR-Stil (via CSM – Compatibility Support Module) immer noch erlaubt, halten wir diese Methode für die einfachste. Das Wichtigste bei der Installation im alten MBR-Partitionsstil:

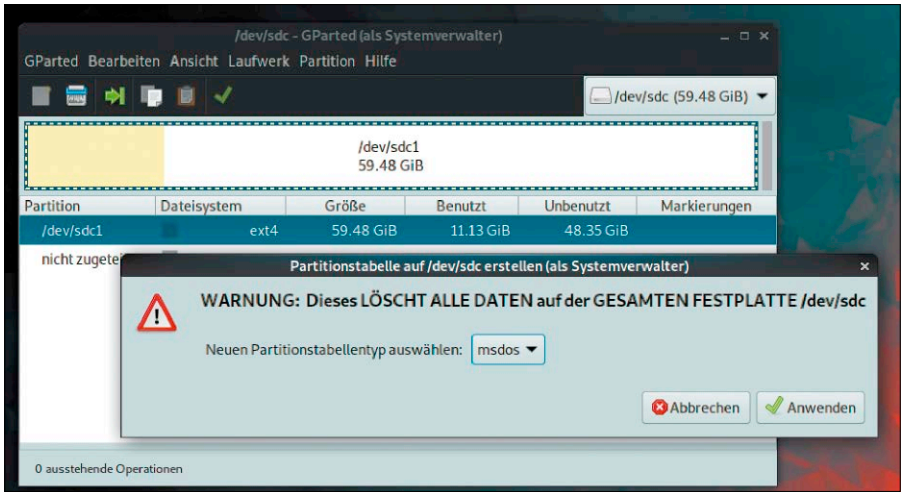
1. Das Installationsmedium der Linux-Distribution muss im Bios-Modus gebootet werden. Bei der Auswahl im Firmware-Bootmenü muss daher der Eintrag ohne „UEFI“ gewählt werden. Bei USB-Medien wird oft ein eindeutiger Gerätename angezeigt (zum Beispiel „Sandisk Ultra…“), zum Teil aber auch nur „USB“. Bei zwei Einträgen „USB“ und „UEFI: USB“ wäre daher der erste der richtige.

2. Bei der Installation des ersten Linux-Systems auf dem USB-Datenträger muss der Stick ausdrücklich mit neuer MBR-Partitionstabelle überschrieben werden. Dies bietet im Prinzip jeder Linux-Installer an, etwa Ubuntus Ubiquity mit der manuellen Installationsart („Etwas anderes“) und der Option „Neue Partitionstabelle“. Sie können das aber auch vorab mit dem bewährten und übersichtlicheren Gparted erledigen („Laufwerk → Partitionstabelle erstellen → msdos“) und danach auch gleich über „Partition → Neu“ die gewünschten Partitionsgrößen für die zwei, drei geplanten Systeme erstellen – allesamt als „primäre“ Partitionen mit Dateisystem Ext4.

3. Ist der Stick wie beschrieben mit Gparted vorbereitet, müssen Sie bei den nachfolgenden Installationen den Distributionen (deren root-Verzeichnis „/“) nur noch die bereits vorhandenen Partitionen zuweisen (etwa „/dev/sdc1“, „/dev/sdc2“). Als Bootloader-Gerät ist jeweils der Stick anzugeben (etwa „/dev/sdc“).

4. Viele Systeme werden auf die moderne Methode der GPT-Partitionierung hinweisen oder diese sogar fordern, was Sie aber einfach ignorieren können.

5. Sowohl die Installationsmedien zum Einrichten des Sticks als auch später der fertige Multiboot-Stick müssen im Bios-Modus gebootet werden. ■

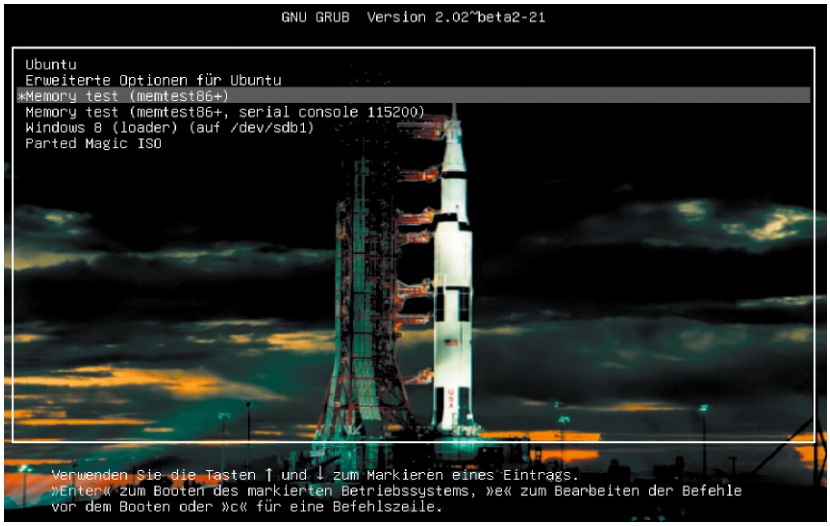


Reguläre USB-Installationen: Wer sich in Linux-Installern verirrt, kann den Stick vorab mit Gparted vorbereiten – hier mit MBR-Partitionsstil.

Booten mit Grub 2

Der Bootloader Grub 2 sorgt für den Start von Linux und anderen Systemen. Wie Sie Grub 2 anpassen und bei Problemen reparieren, lesen Sie in diesem Artikel.

Von **Thorsten Eggeling**



Hübscher booten: Lesen Sie am Ende dieses Beitrags, wie Sie das Grub-Bootmenü optisch anpassen. Priorität hat beim Booten aber das Wichtigste – dass es funktioniert.

Der Grand Unified Bootloader 2 ist bei fast allen Linux-Distributionen Standard. Der Bootloader ist das erste Programm, das ein PC nach dem Einschalten ausführt. Er ermöglicht über ein Menü die Wahl zwischen mehreren Betriebssystemen. Ist nur Linux installiert, lädt er den Kernel, der dann das Betriebssystem initialisiert. Bei einer Multiboot-Konfiguration leitet Grub die Anforderung beispielsweise an den Windows-Bootloader weiter.

Grub 2 muss mit einer Vielzahl unterschiedlicher Konfigurationen zurechtkommen. Aktuelle PCs booten standardmäßig von einer Partition im GPT-Format und verwenden Uefi-Firmware. Bei älteren PCs gibt es ein Bios und MBR-Partitionen. Linux kann auf Partitionen mit den Dateisystemen Ext2 bis Ext4 oder BTRFS installiert sein. Und dann gilt es auch noch, Soft- und Hardware-Raid und LVM zu berücksichtigen.

Wie Sie mögliche Fehler beheben und Grub 2 individuell anpassen, erfahren Sie in diesem Artikel. Wir beziehen uns auf Ubuntu 15.04. Die Anleitungen funktionieren genau so oder ganz ähnlich auch bei anderen Distributionen.

1. So funktioniert Grub 2

Bei herkömmlichem Bios werden bei der Linux-Installation 512 Bytes des Grub-2-Bootloaders („boot.img“) in den MBR (Master Boot Record) der ersten Festplatte geschrieben. Damit findet der Bootloader den ersten Sektor der Datei „/boot/grub/core.img“ und führt den enthaltenen Code aus. Dieser lädt Module, die für den Zugriff auf das Dateisystem nötig sind, und zeigt das Bootmenü an.

Ist Linux im Uefi-Modus installiert, liegt der Bootloader in der EFI-Partition, die in das Dateisystem unter „/boot/efi“ eingebunden ist. Für jedes System gibt es ein eigenes Verzeichnis – etwa „/boot/efi/EFI/ubuntu“. Die Bootloader-Dateien „grubx64.efi. shim x64.efi“ und „MokManager.efi“ sind in einer Secure-Boot-Umgebung nötig. „grub.cfg“ enthält einen Verweis auf die Konfigurationsdatei „/boot/grub/grub.cfg“, die Definitionen für das Bootmenü enthält.

Die Konfiguration von Grub 2 erfolgt automatisch über die Scripts unter „/etc/grub.d“. Das wichtigste Script „10_linux“ sucht unter „/boot“ nach Linux-Kerneln („vmlinuz-*“) und Ramdisk-Dateien („initrd.img-*“) und erstellt die Einträge für das Bootmenü. „30_os-prober“ ist für die Suche nach Betriebssystemen wie Mac-OS und Windows zuständig. „30_uefi_firmware“ bindet Dateien von der EFI-Partition ins Menü ein. Die Scripts werden bei jedem Upgrade auf einen neuen Kernel automatisch ausgeführt.

Standards setzen: Variablen in der Datei „/etc/default/grub“ steuern das Verhalten von Grub 2. Sie können etwa einen höheren Wert hinter „GRUB_TIMEOUT=“ eintragen, um die Wartezeit zu verlängern, bevor das Standardsystem bootet. Die Angaben hinter „GRUB_CMDLINE_LINUX_DEFAULT“ werden als Kernel-Parameter an den Standardeintrag angehängt. Bei Ubuntu steht hier „quiet splash“. Wenn Sie beide Parameter entfernen, sehen Sie beim Booten zur Diagnose von Fehlern die Textausgaben des Systems auf dem Bildschirm.

Nach Änderungen aktualisieren Sie die Konfiguration mit diesem Terminal-Befehl:

```
sudo update-grub
```

Das Script führt der Reihe nach alle Scripts in „/etc/grub.d“ aus, ermittelt dabei alle Betriebssysteme und erstellt die Datei „/boot/grub/grub.cfg“. Dabei werden auch Systeme berücksichtigt, die Sie auf einem USB-Laufwerk einge-

richtet haben. Wenn Sie das nicht wünschen, entfernen Sie die USB-Datenträger vorher.

2. Grub 2 reparieren

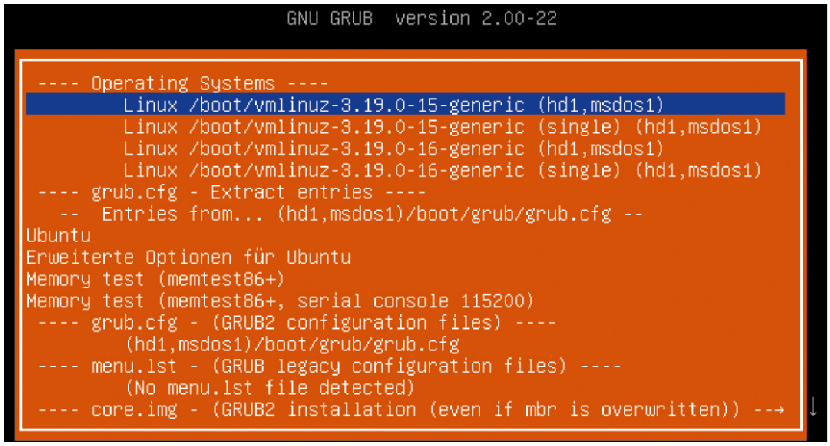
Wenn Grub 2 Fehler meldet, sich das System aber noch booten lässt, installieren Sie Grub 2 neu. Bei einem Bios-System verwenden Sie die folgenden Befehlszeilen:

```
sudo grub-install /dev/sdx
sudo update-grub
```

Statt „x“ tragen Sie die Bezeichnung für die Bootfestplatte ein. Bei nur einer Festplatte verwenden Sie „sda“. Ist beispielsweise Linux auf „/dev/sdb“ und Windows auf „/dev/sda“ installiert, können Sie auch die Linux-Festplatte als Ziel angeben. Setzen Sie im Bios in der Liste der Bootgeräte die Linux-Festplatte an die erste Stelle. Über das Grub-Bootmenü starten Sie dann Linux oder Windows. Der Vorteil: Wenn Sie Windows neu installieren, bleibt der Grub-Bootloader auf der Linux-Festplatte erhalten.

Rettungssystem für Grub 2: Wenn der Rechner nicht mehr startet, etwa weil der Bootloader von einer Windows-Installation überschrieben wurde, verwenden Sie Super Grub 2 Disk. Sie finden das System für Bios-Installationen bootfähig auf der Heft-DVD unter „Extras und Tools“. Starten Sie dort „Super Grub Disk 2“ und dann „Everything“. Sie sehen eine Liste der installierten Systeme beziehungsweise Kernel-Versionen. Versuchen Sie, den gewünschten Eintrag zu starten. Sollte das nicht funktionieren, starten Sie Super Grub 2 Disk erneut und probieren die anderen Optionen. Danach befinden Sie sich im installierten System, in dem Sie wie gewohnt arbeiten können. Verwenden Sie die oben erwähnten zwei Befehlszeilen, um die Grub-Konfiguration zu aktualisieren und Grub im MBR neu zu installieren.

Uefi-Systeme unterstützt Super Grub 2 Disk erst ab der Version 2.02s3, die es zeitlich nicht mehr auf die Heft-DVD geschafft hat. Laden Sie sich die ISO-Datei über *www.supergrubdisk.org* herunter, und schreiben Sie das



Booten im Notfall: Super Grub 2 Disk sucht nach Installationen auf der Festplatte und zeigt sie in einem Menü an. Der Linux-Start funktioniert auch bei defekter Grub-Umgebung.

Image auf einen USB-Stick:

```
sudo dd if=super_grub2_disk_
  hybrid_2.02s3.iso of=/dev/sdx
```

„x“ ersetzen Sie durch die Gerätekennung des Sticks. Alle darauf befindlichen Dateien gehen verloren. Booten Sie dann den PC vom USB-Stick, und gehen Sie im Menü auf „Detect and show boot methods“. Wählen Sie das gewünschte System zum Start aus. Im installierten System reparieren Sie dann Grub 2 und die EFI-Dateien:

```
sudo grub-install
```

Ein Ziel-Laufwerk geben Sie nicht an. Das Script findet das Verzeichnis „/boot/efi“ automatisch.

Live-DVD verwenden: Wie Sie den PC im Notfall von einer Linux-Installations-DVD booten, ist ab Seite 38 erklärt. Um Grub neu zu installieren, binden Sie die Dateisysteme mit folgenden Zeilen ein:

```
sudo mount -o bind /dev /System/
  dev
sudo mount -o bind /sys /System/
  sys
sudo mount -t proc /proc /System/
  proc
```

„System“ ersetzen Sie durch den Einbindepunkt des installierten Ubuntu unter „/media/ubuntu/“. Bei einem Uefi-System mounten Sie zusätzlich die EFI-Partition mit

```
sudo mount /dev/sdxy /System/boot/
  efi
```

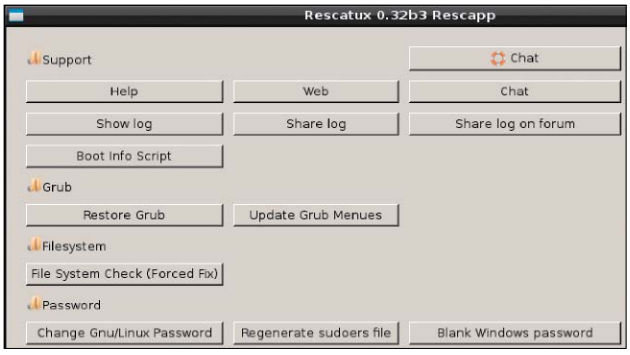
Ersetzen Sie „xy“ durch den Pfad zur EFI-Partition. Wenn Sie diesen nicht kennen, verwenden Sie *sudo parted -l*.

ISO-Dateien über Grub 2 starten

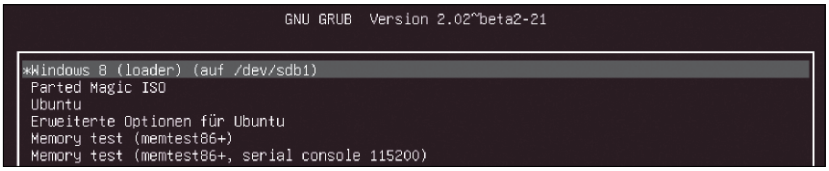
Grub 2 kann Systeme direkt aus ISO-Dateien booten. Das ist praktisch für schreibgeschützte Zweit- oder Notfallsysteme. Für Parted Magic erstellen Sie in die Datei „/boot/grub/custom.cfg“ mit folgendem Inhalt (sechs Zeilen):

```
menuentry "Parted Magic ISO" {
set isofile="/boot/pma
  gic_2015-03-06.iso"
loopback loop (hd0,msdos1)$isofile
linux (loop)/pmagic/bzImage iso_
  filename=$isofile edd=on
  vga=normal keymap=de-latin1 de_DE
  vmalloc=512MiB
initrd (loop)/pmagic/initrd.img
  (loop)/pmagic/fu.img (loop)/pma
  gic/m32.img
}
```

„pmagic_2015-03-06.iso“ kopieren Sie aus dem Ordner „Image-Dateien“ der Heft-DVD nach „/boot“. „hd0,msdos1“ entspricht „/dev/sda1“. Die richtige Angabe für Ihr System ermitteln Sie aus den anderen Menüeinträgen in der Datei „/boot/grub/grub.cfg“. Die Kernel-Parameter hinter „linux (loop)“ lauten für jedes System anders. Beispiele finden Sie in der Datei „boot/grub/grub.cfg“ auf der Heft-DVD.



Linux-Reparatur: Rescatux zeigt einen einfachen Script-Starter für mehrere spezielle Tools. Damit stellen Sie eine defekte Grub-Installation wieder her.



Bootmenü: Die Reihenfolge der Menüeinträge ergibt sich aus der Script-Nummerierung. Durch Umbenennen können Sie Windows an die erste Stelle setzen.

Das Tool zeigt die Liste aller Partitionen. Führen Sie die folgenden vier Befehlszeilen aus:

```
sudo chroot /System
grub-install /dev/sdx
update-grub
exit
```

„System“ steht wieder für den Einbindepunkt der Ubuntu-Partition, für „x“ setzen Sie den Pfad zum Boot-Laufwerk ein. Bei einem Uefi-System lassen Sie „/dev/sdx“ weg.

Reparatur mit Notfallsystem: Rescatux (auf Heft-DVD) macht defekte und überschriebene Bootloader wieder flott, eignet sich jedoch nur für Bios-Systeme, da es nicht im Uefi-Modus booten kann. Nach dem Start rufen Sie die gewünschte Aktion im Tool Rescapp auf. Hier gibt es etwa „Restore Grub“ und „Update Grub Menüs“. Das Tool „Boot Repair“ repariert die Grub-Bootumgebung mit einem Mausklick.

3. Bootmenü für Grub 2 anpassen

Die in Punkt 1 erwähnten Scripts unter „/etc/grub.d“ und die Konfigurationsdatei „/boot/grub/grub.cfg“ sollten Sie nicht bearbeiten. Sie werden beim nächsten Grub-Update wahrscheinlich durch neue Versionen ersetzt, wobei Ihre Änderungen verlorengehen. Wer trotzdem Änderungen durchführen möchte, sollte immer Sicherungskopien anlegen. Der vorgesehene Weg zu eigenen Menüpunkten führt über die Datei „/etc/grub.d/40_custom“. Oder Sie verwenden „41_custom“ zusammen mit „/boot/grub/custom.cfg“. Ein Beispiel: Bei einer Parallelinstallation von Linux und Windows 7 taucht im Bootmenü auch „Windows 7 Recovery Environment“ auf. Damit starten Sie die Windows-Wiederherstellungsumgebung des PC-Herstellers, die ohne Rückfrage mit der Rekonstruktion des ursprünglichen Windows beginnt und die Linux-Installation entfernt. Um den problematischen Menüeintrag zu beseitigen, kopieren Sie aus „/boot/grub/grub.cfg“ den Block, der mit „menuentry ‚Windows 7 (loader)“ beginnt und mit „}“ endet, in die neue Datei „/boot/grub/custom.cfg“. Danach ergänzen Sie in „/etc/default/grub“ diese Zeile:

```
GRUB_DISABLE_OS_PROBER=true
```

Mit *update-grub* generieren Sie die Konfigurationsdatei „/boot/grub/grub.cfg“ neu. Das Script „30_os_prober“ erzeugt jetzt keine Menüeinträge für Windows mehr. Stattdessen kommt der Menüeintrag für Windows aus „/boot/grub/custom.cfg“ zum Einsatz.

Menüreihenfolge ändern: Die Datei „/etc/default/grub“ legt über „GRUB_DEFAULT“ fest, welches System automatisch bootet. Der Wert „0“ bedeutet, dass das System startet, zu dem der erste Eintrag im Bootmenü gehört. Ändern Sie diesen Wert auf die Position des gewünschten Systems im Bootmenü, um ein anderes Standardsystem festzulegen. Alternativ ändern Sie die Reihenfolge, indem Sie die Scripts neu nummerieren. Haben Sie wie oben beschrieben eine „custom.cfg“ mit dem Menüeintrag für Windows erstellt, verwenden Sie diese zwei Zeilen:

```
sudo mv 41_custom 07_custom
sudo update-grub
```

Windows landet dann im Menü an der ersten Position und wird standardmäßig gestartet, wenn „GRUB_DEFAULT=0“ gesetzt ist.

4. Grub 2 optisch anpassen

Das Grub-Startmenü lässt sich aufhübschen: Installieren Sie die Pakete „grub2-splashimages“ und „grub2-themes-ubuntu-mate“. In der Datei „/etc/default/grub“ ergänzen Sie dann diese zwei Zeilen:

```
GRUB_GFXMODE=800x600
GRUB_BACKGROUND=/usr/share/images/
 grub/Apollo_17_The_Last_Moon_
 Shot_Edit1.tga
```

In „/etc/grub.d/40_custom“ hängen Sie folgende vier Zeilen an:

```
set color_normal="white/black"
set color_highlight="black/black"
set menu_color_normal="white/
 black"
set menu_color_highlight="white/
 dark-gray"
```

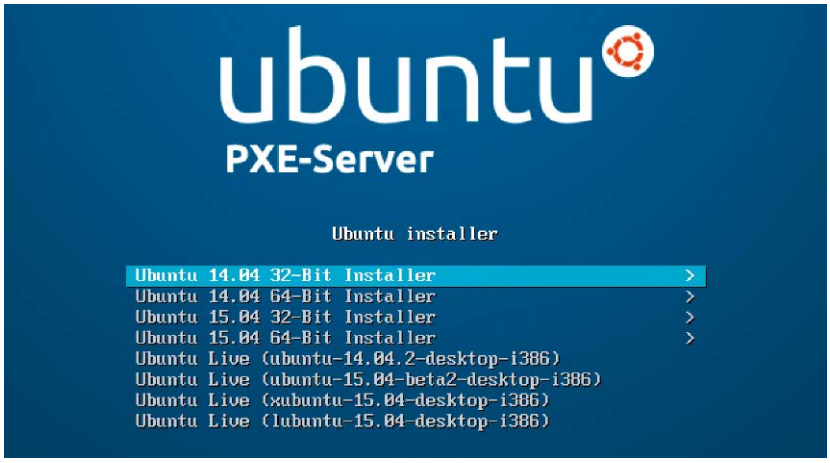
Aktualisieren Sie die Konfiguration mit *update-grub*, und starten Sie das System neu. Das Ergebnis sehen Sie in der ersten Abbildung dieses Beitrags. Eine Liste der Variablen und Farben finden Sie im Grub-Manual (*http://pcwe.lt/C7XXHl*). Komplexere Anpassungen sind über Grub-Themes möglich. Machen Sie die eben durchgeführten Änderungen rückgängig, und tragen Sie in „/etc/default/grub“ folgende Zeile ein:

```
GRUB_THEME=/boot/grub/themes/
 ubuntu-mate/theme.txt
```

Nach *update-grub* und einem Neustart sehen Sie das Ubuntu-Mate-Theme für Grub. Die Dateien des Themes liegen im angegebenen Pfad, die Konfiguration erfolgt über die Datei „theme.txt“. ●

Booten übers Netz (PXE)

Ein Linux-System muss nicht auf der lokalen Festplatte liegen. Es lässt sich auch über das Netzwerk installieren oder starten und zentral administrieren.



Von Thorsten Eggeling

PXE steht für Preboot Execution Environment und ist eine Funktion, die in der Firmware des Netzwerkadapters oder der Hauptplatine steckt. Darüber lassen sich Systeme booten, die auf einem Netzwerklaufwerk liegen. Typisches Einsatzgebiet ist die regelmäßige Neuinstallation auf Rechnern in Schulungsräumen. Es ist außerdem möglich, ein komplettes System über das Netzwerk zu laden und PCs ohne eigene Festplatte zu betreiben.

1. Voraussetzungen für PXE

Das Bios beziehungsweise die Netzwerkkarte müssen PXE unterstützen. Rufen Sie das Bios-Setup auf, indem Sie kurz nach dem Einschalten des PCs die Entf-Taste, Esc oder F2 drücken. Die Konfiguration für PXE finden Sie meist unter „Onboard Devices Configuration“, „Boot“ oder „BIOS Features“. Aktivieren Sie zuerst Optionen wie „LAN PXE Boot Option ROM“ und „Ipv4 PXE Support“. Wenn der PC im Uefi-Modus bootet, aktivieren Sie die Bios-Emulation CSM (Compatibility Support Module), die Sie unter Bezeichnungen wie „CSM Support“, „UEFI with CSM“ oder „UEFI and Legacy“ finden.

PXE ist zwar auch über Uefi möglich, jedoch nicht mit der von uns in diesem Artikel vorgeschlagenen Konfiguration. Speichern Sie die Änderungen, und rufen Sie das Bios-Setup erneut auf. Setzen Sie den Netzwerkadapter an die erste Stelle in der Liste der Bootgeräte. Bei vielen PCs lässt sich auch ein Bootmenü über Tasten wie Esc, F9, oder F12 aufrufen. Dann können Sie manuell zwischen dem Start von der Festplatte oder über das Netzwerk wählen.

Bios-Setup: Aktivieren Sie im Bios eine Option wie „Lan PXE Boot Option ROM“, und konfigurieren Sie den Netzwerkadapter als erstes Bootgerät.

Als System für die Installation und das Booten übers Netzwerk verwenden wir Ubuntu 14.04 LTS und Ubuntu 15.04. Wir gehen davon aus, dass sich in Ihrem Netzwerk bereits ein PC befindet, der unter Ubuntu ab Version 14.04 läuft und den Sie als PXE-Server verwenden wollen. Andere Systeme sind möglich, dazu müssten Sie aber das in diesem Artikel verwendete Bash-Script anpassen.

2. Server für PXE konfigurieren

Ein Client-PC findet den PXE-Server im Netzwerk über eine DHCP-Anfrage (Dynamic Host Configuration Protocol). Für DHCP ist im Normalfall der DSL-Router zuständig. Da es nur einen DHCP-Server im Netz geben darf, kommt dnsmasq als Proxy-DHCP-Server zum Einsatz. dnsmasq lässt sich so konfigurieren, dass DHCP-Anfragen an den Router weitergeleitet, aber PXE-Anfragen verarbeitet werden. dnsmasq kann einzelne Dateien ausliefern, die für die Netzwerkinstallation von Ubuntu erforderlich sind (Punkt 3). Sorgen Sie im Router dafür, dass sich die IP-

Nummer des Servers nicht ändert. Bei einer Fritzbox rufen Sie die Konfigurationsseite auf und gehen auf „Heimnetz → Netzwerk“. Sie erhalten die Liste Ihrer Netzwerkgeräte. Klicken Sie bei der IP-Adresse Ihres Linux-Servers auf „Bearbeiten“, und aktivieren Sie „Diesem Netzwerkgerät immer die gleiche IPv4-Adresse zuweisen.“

Installation per Script: Damit Sie die Befehle für die Installation nicht eintippen müssen, haben wir ein Installationspaket vorbereitet. Laden Sie es über *http://pcwe.lt/pxeboot* herunter, und entpacken Sie die tar.gz-Datei in Ihr Home-Verzeichnis, etwa in den Ordner „pxe“. Schalten Sie das Script mit diesen Zeilen ausführbar:

```
cd ~/pxe
chmod 755 pxe_install.sh
```

„pxe_install.sh“ legt Konfigurationsdateien nur im eigenen Verzeichnis ab. Nachdem Sie ein System erstellt haben (siehe die Punkte 3 bis 5), rufen Sie folgende Befehlszeile auf, um die Dateien an die richtige Position zu kopieren:

```
sudo pxe_install.sh copy
```

Sollten im Zielverzeichnis bereits Dateien gleichen Namens vorhanden sein, tippen Sie in der Regel „z“ ein, um die Dateien zusammenzuführen. Bereits vorhandene Zeilen werden nicht erneut eingefügt. Oder Sie drücken die Enter-Taste und kopieren die Dateien aus dem Verzeichnis „pxe/etc“ beziehungsweise deren Inhalt manuell. Damit ist sichergestellt, dass Dateien unter „/etc“ nicht unbeabsichtigt ersetzt werden. „pxe_install.sh“ ermittelt automatisch, ob die nötigen Programmpakete für eine bestimmte Aufgabe noch nicht vorhanden sind und bietet Ihnen, wenn nötig, deren Installation an.

3. Ubuntu über das Netzwerk installieren

Für Ubuntu gibt es fertig vorbereitete Netzwerk-Installer. Dabei handelt es sich um kleine Pakete mit der Größe von etwa 25 MB, der Rest der Dateien wird über das Internet nachgeladen. Öffnen Sie „pxe_install.sh in“ einem Editor. Am Anfang finden Sie einen kommentierten Ausschnitt für die

Feste IP-Adresse: Der PXE-Server muss immer über die gleiche IP-Nummer erreichbar sein. Eine feste IP-Adresse lässt sich in allen DSL-Routern konfigurieren.

Konfiguration. Tragen Sie hinter „dhcprange“ den IP-Bereich für Ihr Netzwerk ein. Wenn Sie diesen nicht kennen, informiert *ifconfig* auf der Kommandozeile: Die IP-Nummer Ihres PCs steht hinter „inet Adresse“. Lautet diese etwa „192.168.0.27“, gehört in das Script „192.168.0.0“. Die letzte Zahl wird also durch „0“ ersetzt. Ändern Sie bei Bedarf die Pfadangabe hinter „tftpdir“. In diesem Verzeichnis landen die Dateien, die sich später über das Netzwerk booten lassen, sowie die Konfigurationen.

Hinter „netbootnamelist“ stehen die Bezeichnungen der Distributionen für das Menü und bei „netbooturllist“ die Download-Adressen. Das Script ist für Ubuntu 14.04 und 15.04 vorkonfiguriert (32 und 64 Bit).

Speichern Sie die Datei, und führen Sie folgenden Befehl aus:

```
sudo ./pxe_install.sh netinst
```

Das Script lädt die Dateien herunter und entpackt sie nach „tmp/installer“ im Installationsverzeichnis. Für jede Distribution gibt es ein eigenes fortlaufend nummeriertes Verzeichnis. Kontrollieren Sie den Inhalt der Datei „~/pxe/etc/dnsmasq.conf“. Diese enthält alle Angaben, die für einen erfolgreichen Start nötig sind. Die Werte für das Netzwerk, Pfade und Menüeinträge sollten denen entsprechen, die Sie im Script konfiguriert haben. Mit

```
sudo ./pxe_install.sh copy
```

kopiert das Script „tmp/installer“ nach „/var/lib/tftpboot“ sowie „dnsmasq.conf“ nach „/etc“ und startet dnsmasq neu.

Installation über das Netzwerk: Sie müssen jetzt nur noch den Client-PC über PXE booten. Er findet dann den Linux-Server per DHCP automatisch und zeigt das Menü für die Installation an. Wählen Sie „Netzwerk-Installer“ und dann das gewünschte System. Der Netzwerk-Installer von Ubuntu unterscheidet sich deutlich von dem auf der Standard-Ubuntu-DVD. Es zeigt nur eine einfache grafische Oberfläche, die sich per Tastatur bedienen lässt. Der Vorteil: Sie haben die Wahl zwischen mehreren Installationstypen, beispielsweise „Kubuntu desktop“ oder „Ubuntu desktop“.

Bandbreite sparen mit Apt-Cacher-ng

Wenn Sie die Netzwerk-Installer häufiger verwenden, empfiehlt sich die Installation von Apt-Cacher-ng auf dem Server. Eine Installationsanleitung finden Sie unter *http://goo.gl/v54T0H*. Im Netzwerk-Installer wählen Sie für den Spiegel-Server „Deutschland“ und tippen danach unter „HTTP-Proxy-Daten“ Adresse und Port des Apt-Cacher-ng-Servers ein, etwa „http://192.168.0.12:3142“. Beim erneuten Abruf eines Pakets wird dieses dann aus dem Cache im eigenen Netzwerk geladen und nicht über das Internet. Apt-Cacher-ng ist auch bei der Bereitstellung bootfähiger Systeme über das Netz nützlich (→ Punkt 5). Passen Sie im Script „pxe_install.sh“ den Abschnitt „Apt-Cacher-ng verwenden“ für Ihr Netzwerk an.

Software-Auswahl: Die Ubuntu-Netzwerkinstallation ermöglicht – anders als die DVD – eine Auswahl zwischen unterschiedlichen Software-Sammlungen.

4. Ubuntu über ISO-Dateien installieren

Alternativ zum Netzwerk-Installer lassen sich auch ISO-Dateien über das Netzwerk booten. Das entspricht dann in etwa der Installation von DVD. Bereiten Sie dazu „pxe_install.sh“ vor wie in Punkt 2 beschrieben. Passen Sie zusätzlich die Variablen unter „Konfiguration für bootinst und addiso“ an. Starten Sie dann diesen Befehl:

```
sudo ./pxe_install.sh addiso Da
  tei.iso
```

Für „Datei.iso“ setzen Sie den kompletten Pfad zur ISO-Datei ein. Das Script erstellt die Dateien für die Bootumgebung unter „tmp/installer/“ und die Konfigurationsdateien für dnsmasq sowie den NFS-Server unter config. Das Live System aus der ISO-Datei findet seinen Platz unter „/netboot“. Mit folgender Zeile kopieren Sie die Dateien nach „/var/lib/tftpboot“ und „/etc“:

```
sudo ./pxe_install.sh copy
```

Sie können das Script auch mehrmals mit verschiedenen ISO-Dateien aufrufen und zusammen mit den Netzwerk-Installern verwenden (Punkt 3).

Wenn der Ordner „tmp/installer/“ bereits vorhanden ist, integriert das Script die zugehörigen Menüeinträge automatisch.

5. Ubuntu über das Netzwerk starten

Öffnen Sie „pxe_install.sh“ (*http://pcwe.lt/pxeboot*) in einem Editor, und passen Sie die IP-Adressen und Pfade unterhalb von „Konfiguration für bootinst und addiso“ an. Die Angabe hinter „ubuntu=“ bestimmt die Ubuntu-Version. „trusty“ steht für Ubuntu 14.04 TLS und „vivid“ für 15.04 LTS. Darunter folgt mit „arch=“ die Architektur: „i386“ (32 Bit) oder „amd64“ (64 Bit). Hinter „desktop=“ tragen Sie ein, welche Oberfläche Sie verwenden wollen, etwa „xubuntu-desktop“ für ein System mit Xfxe4. Das Script enthält im Kommentar weitere Beispiele. Hinter „username=“ tragen Sie den gewünschten Benutzernamen für das neue System ein.

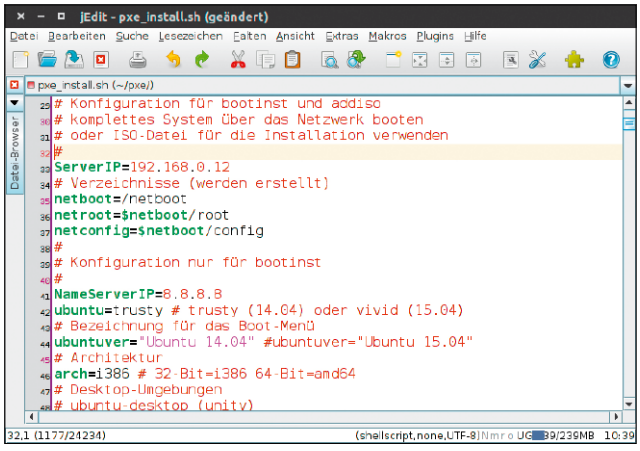
Wie das System später arbeitet, legen Sie mit „UseAufs=1“ fest. Das Script erstellt dann zwei NFS-Freigaben. Eine ist schreibgeschützt und nimmt das Ubuntu-System auf, die andere enthält die Konfiguration für die Clients. Jeder PC erhält einen eigenen Ordner mit der eindeutigen ID seines Netzwerkadapters als Bezeichnung (MAC-Adresse). Hier landen dann neue Dateien beispielsweise aus dem Home-Verzeichnis. Änderungen im Basissystem sind vom Client aus nicht möglich. Diese erfolgen bei Bedarf auf dem PXE-Server mit *sudo ./pxe_install.sh softinst*. Wenn Sie das nicht wünschen, tragen Sie hinter „UseAufs=“ eine „0“ ein. Dann dürfen Sie das System aber immer nur auf einem Rechner starten. Sonst gibt es wegen der gleichlautenden Host-Namen und gleichzeitiger Schreibzugriffe Konflikte. Starten Sie das Bash-Script mit der Zeile

```
sudo ./pxe_install.sh bootinst
```

Das System wird unter „/netboot/root/“ erstellt. Sie werden bei der Installation nach dem Ziel für Grub2 gefragt. Wählen Sie hier nichts aus, bestätigen Sie mit „OK“ und danach mit „Yes“. Sie müssen außerdem eine Zeitzone einstellen und das Passwort für den im Script konfigurierten Benutzer vergeben. Mit folgender Zeile kopieren Sie abschließend die Konfigurationsdateien nach „/etc“:

```
sudo ./pxe_install.sh copy
```

Starten Sie das System über das Netzwerk auf einem Client-PC, und fahren Sie es wieder herunter. Kopieren Sie die Dateien „hostname“ und „hosts“ von „pxe/config“ nach „/netboot/config/MAC/etc“. „MAC“ ersetzen Sie durch die MAC-Adresse des jeweiligen Clients. Ändern Sie in den Dateien jeweils „IhrHostNameHier“ auf den gewünschten Rechnernamen. Wenn Sie „UseAufs=0“ verwendet haben, kopieren Sie beide Dateien beispielsweise nach „/netboot/root/trusty/etc“. ●

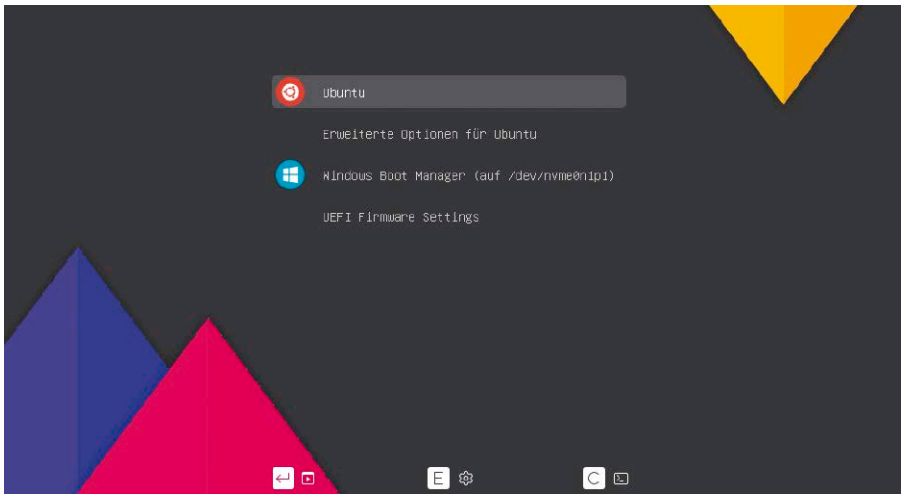


Script konfigurieren: Das Script enthält am Anfang einen Abschnitt für die Konfiguration. Ändern Sie die IP-Adressen entsprechend Ihrer Netzwerkkonfiguration.

Booten mit und ohne Grub

Der Bootloader Grub 2 sorgt für den Start von Linux und anderen Systemen. Wie Sie Grub 2 anpassen oder auch ganz ohne Grub auskommen, lesen Sie in diesem Artikel.

VON THORSTEN EGGELING



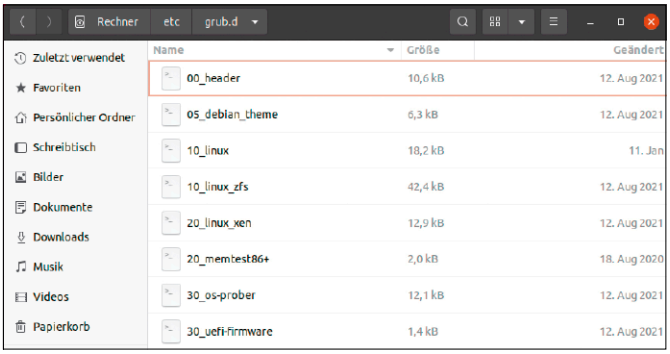
Grub in Farbe: Das meist schlichte Grub-Bootmenü lässt sich mit einem Hintergrundbild und grafischen Symbolen aufwerten. Andere Schriftarten sind ebenfalls möglich.

Grub 2 ist der Standard-Bootloader bei fast allen Linux-Distributionen. Ist nur ein Linux-System auf dem Rechner installiert, bekommen Sie Grub nicht zu Gesicht. Bei mehreren Linux-Installationen oder einer Parallelinstallation mit Windows ermöglicht Grub die Auswahl des gewünschten Systems über ein Bootmenü. In diesem Fall ist es hilfreich, die Grundlagen der Grub-Konfiguration zu kennen. Mit eigenen Anpassungen lässt sich beispielsweise die Bootreihenfolge ändern oder Grub optisch anders gestalten. Wer möchte, kann auch ganz auf Grub verzichten. Auf Uefi-PCs lässt sich Linux direkt starten, was die Konfiguration erleichtert und den Start beschleunigt.

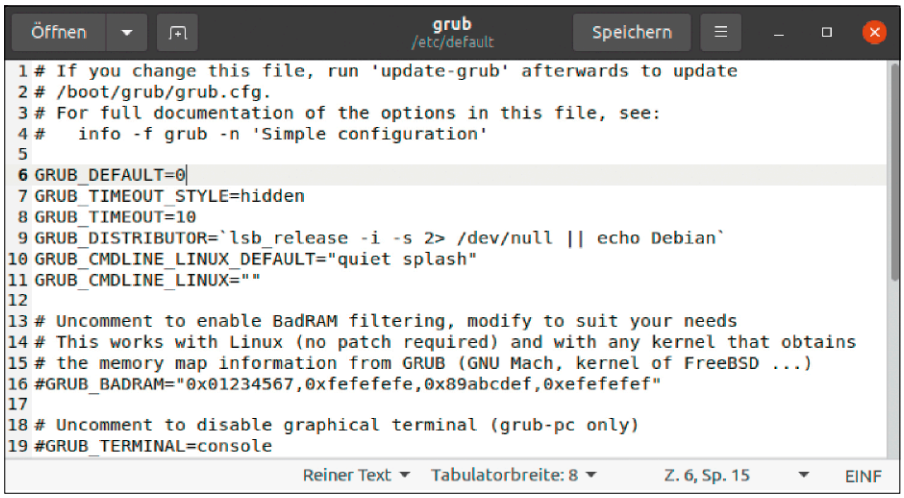
Die Grub-Basiskonfiguration

Grub wird bei der Linux-Installation automatisch eingerichtet. Auf einem Rechner mit Uefi-Firmware werden die Dateien des Bootloaders auf die EFI-Partition kopiert („/boot/efi“). Für jedes Betriebssystem gibt es ein eigenes Verzeichnis, das dann etwa bei Ubuntu „/boot/efi/EFI/ubuntu“ heißt. Die Bootloader-Datei ist „grubx64.efi“. „shimx64.efi“ und „MokManager.efi“ sind in einer Secure-Boot-Umgebung nötig. „grub.cfg“ enthält einen Verweis auf die Konfigurationsdatei „/boot/grub/grub.cfg“, die Definitionen für das Bootmenü enthält. Wurde Linux auf einem Bios-PC oder im CSM-Modus (Compatibility Support Module) installiert, belegt der Grub-Startcode 512 Bytes im MBR (Master Boot Record) der Startfestplatte. Das Bios führt beim Start des PCs den Code aus dem MBR aus (Stufe 1), der einen Verweis auf den ersten Sektor der Festplatte enthält. Hier beginnt die Stufe 1.5 des Grub-Starts, die Zugriff auf das Dateisystem hat, weitere Dateien für Stufe 2 laden kann und zuletzt das Bootmenü anzeigt.

Die Grub-Konfiguration, inklusive der Einträge für das Bootmenü, ist in der Datei „/boot/grub/grub.cfg“ gespeichert. Sie wird über die Scripts aus dem Ordner „/etc/grub.d“ automatisch erstellt. Das wichtigste Script ist „10_linux“. Es sucht im Verzeichnis „/boot“ nach Linux-Kerneln („vmlinuz-*“) sowie Ramdisk-Dateien („initrd.img-*“) und erstellt die Einträge für das Bootmenü. „30_os-prober“ ist für die Suche nach anderen Betriebssystemen wie Mac-OS und Windows verantwortlich. „30_uefi_firmware“ bindet Dateien von der EFI-Partition ins Menü ein. Die Scripts werden bei jedem Upgrade des Kernels automatisch ausgeführt und erstellen eine neue „/boot/grub/grub.cfg“.



Grub-Konfiguration: Die Grub-Konfigurationsdatei „/boot/grub/grub.cfg“ wird automatisch mit einigen Scripts erzeugt. Eigene Anpassungen lassen sich aber auch vornehmen.



Bootmenü anpassen: Die Datei „/etc/default/grub“ enthält Variablen. Sie können beispielsweise festlegen, wie lange das Bootmenü vor einem automatischen Start angezeigt wird.

Das Bootmenü von Grub 2 anpassen

Die Datei „/etc/default/grub“ enthält Variablen, die von den Scripts in „/etc/grub.d“ ausgewertet werden. Der Wert hinter „GRUB_TIMEOUT=“ bestimmt, wie lange das Menü angezeigt wird, bevor das Standardsystem bootet. Setzt man ihn auf „-1“, erfolgt kein automatischer Start und man startet das gewünschte System manuell mit der Eingabetaste.

„GRUB_TIMEOUT_STYLE=“ ist standardmäßig auf „hidden“ festgelegt. Das Bootmenü wird dadurch nicht angezeigt. Weitere mögliche Werte sind „menu“, wodurch das Grub-Menü immer angezeigt wird, oder „countdown“, was die Zeit bis zum automatischen Start herunterzählt. Sind mehrere Systeme installiert, wird die Variable ignoriert und das Menü immer angezeigt.

Die Angaben hinter „GRUB_CMDLINE_LINUX_DEFAULT=“ werden als Kernel-Parameter angehängt. Bei Ubuntu steht hier „quiet splash“. Wenn Sie beide Parameter entfernen, sehen Sie beim Booten zur Diagnose von Fehlern die Textausgaben des Systems auf dem Bildschirm.

Nach Änderungen aktualisieren Sie die Konfiguration im Terminal:

```
sudo update-grub
```

Das Script führt der Reihe nach alle Scripts in „/etc/grub.d“ aus, ermittelt dabei die Betriebssysteme auf den Festplatten und erstellt die Datei „/boot/grub/grub.cfg“ neu. Dabei werden auch Systeme berücksichtigt, die auf anderen Laufwerken installiert sind. Bei USB-Laufwerken führt das zu Problemen, wenn diese später nicht mehr angeschlossen sind. Grub zeigt dann einen Fehler und es lässt sich kein System mehr starten. In der Regel entfernen Sie besser USB-Geräte, auf denen Linux installiert ist, bevor Sie „update-grub“ verwenden.

Anpassung der Grub-Script-Dateien

Die Scripts unter „/etc/grub.d“ und die Konfigurationsdatei „/boot/grub/grub.cfg“ sollten Sie nicht bearbeiten. Die Dateien werden beim nächsten Grub-Update durch neue Versionen ersetzt, womit manuelle Änderungen verloren gehen. Wer trotzdem Änderungen eintragen möchte, sollte daher immer Sicherungskopien anlegen.

Für eigene Anpassungen ist die Datei „/etc/grub.d/40_custom“ vorgesehen. Oder Sie verwenden „41_custom“ zusammen mit „/boot/grub/custom.cfg“. Dafür ein Beispiel: Bei einer Parallelinstallation von Linux und Windows 10/11 kann im Bootmenü auch „Windows Recovery Environment“ auftauchen. Dies startet die Windows-Wiederherstellungsumgebung des PC-Herstellers – wenn vorhanden. Diese beginnt meist sofort und ohne Rückfrage mit der Rekonstruktion des ursprünglichen Windows und entfernt die Linux-Installation. Damit Sie diese Option nicht versehentlich starten, sollten Sie den Menüeintrag entfernen. Kopieren Sie aus „/boot/grub/grub.cfg“ den Block, der mit

```
menuentry "Windows Boot Manger"
```

beginnt und mit „}“ endet, in die neue Datei „/boot/grub/custom.cfg“ (auf Bios-PC etwa: „menuentry Windows 10 (auf /dev/sda1)“). In „/etc/default/grub“ ergänzen Sie diese Zeile:

```
GRUB_DISABLE_OS_PROBER=true
```

Danach führen Sie

```
sudo update-grub
```

aus. Das Script „30_os_prober“ erzeugt jetzt keine Menüeinträge für Windows mehr. Stattdessen kommt der Menüeintrag für Windows aus „/boot/grub/custom.cfg“ zum Einsatz.

Menüreihenfolge ändern: In der Datei „/etc/default/grub“ legen Sie über „GRUB_DEFAULT“ fest, welches System automatisch bootet. Der Wert „0“ bedeutet, dass das System startet, zu dem der erste Eintrag im

ALTERNATIVER BOOTLOADER REFIND

Die Firmware der meisten PCs bietet ein Bootmenü, über das man eine Startfestplatte oder einen Uefi-Booteintrag wählen kann. Bei Bedarf kann man damit etwa den Windows-Bootloader direkt ohne Umweg über Grub starten. Das Firmware-Bootmenü lässt sich meist über Tasten wie Esc, F8 oder F12 aufrufen. Besonders komfortabel ist das nicht, besser geht es mit dem alternativen Refind Bootmanager (*www.rodsbooks.com/refind*), der sich aber nur für Uefi-PCs bei abgeschaltetem Secure Boot eignet. Das Tool findet automatisch EFI-Bootdateien und Linux-Kernel auf der Festplatte und präsentiert die Booteinträge in einem ansprechenden grafischen Menü.

Refind ist in den Standard-Paketquellen von Ubuntu 20.04 und Linux Mint 20 enthalten und mit

```
sudo apt install refind
```

zu installieren. Über das Refind-Bootmenü können Sie Grub starten, indem Sie mit den Pfeiltasten „Boot EFI/ubuntu/grubx64.efi from EFI System Partition“ wählen und danach das gewünschte System im Grub-Bootmenü. Oder Sie entscheiden sich für einen Eintrag wie „boot/vmlinuz-5.13.0-39-generic“, womit sich der Kernel direkt unter Umgehung von Grub starten lässt.

Bootmenü gehört. Ändern Sie diesen Wert auf die Position des gewünschten Systems im Bootmenü, um ein anderes Standardsystem festzulegen. Alternativ ändern Sie die Reihenfolge, indem Sie die Scripts neu nummerieren. Haben Sie beispielsweise – wie oben beschrieben – eine „custom.cfg“ mit dem Menüeintrag für Windows erstellt, dann verwenden Sie diese Zeile:

```
sudo mv 41_custom 07_custom
```

Danach starten Sie wieder „sudo update-grub“. Windows landet dann im Menü an der ersten Position und wird bei „GRUB_DEFAULT=0“ standardmäßig gestartet.

Grub 2 mit Themes aufwerten

Wem das Grub-Bootmenü zu langweilig ist, kann den Bildschirm selbst gestalten oder vorgefertigte Themes verwenden. Das geht am einfachsten mit dem Tool Grub-Customizer, das sich unter Ubuntu 20.04 oder Linux Mint 20 im Terminal mit

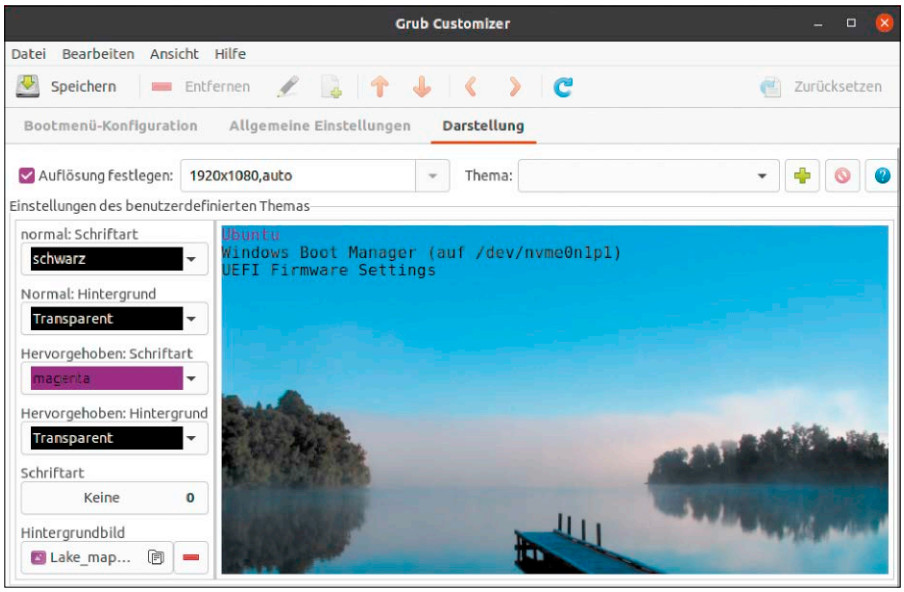
```
sudo apt install grub-customizer
```

installieren lässt. In den Standard-Repositorien gibt es außerdem die Pakete „grub2-themes-ubuntu-mate“ und „grub2-themes-ubuntustudio“ mit den Grub-Themen von Ubuntu Mate und Ubuntu-Studio. Das Paket „grub2-splashimages“ enthält einige Hintergrundbilder.

Im Grub-Customizer kann man auf der Registerkarte „Bootmenü-Konfiguration“ die Einträge im Bootmenü bearbeiten und auf der Registerkarte „Allgemeine Einstellungen“ den Standard-Booteintrag sowie die Zeit bis zum automatischen Start festlegen. Unter „Darstellung“ bestimmen Sie Schriftart, Farben und Hintergrundbild. Das Hintergrundbild muss eine PNG-Datei sein und die exakte Größe haben, wie hinter „Auflösung festlegen“ angegeben ist. Mit „Themes“ kann man eines der installierten Themen wählen. Weitere Grub-Themes gibt es unter *www.gnome-look.org/browse?cat=109*. Die Downloads enthalten meist eigene Installations-Scripts, eine Anleitung dafür ist im Beschreibungstext enthalten.

Linux ohne Grub starten

Auf Uefi-PCs ist Grub nicht zwingend erforderlich. Der Linux-Kernel kann selbst Code enthalten, der sich direkt von der Uefi-Firmware ausführen lässt. Unter Umgehung von Grub startet das System schneller. Der Kernel-Bootloader mit dem Namen „Efi Stub“ ist in den meisten aktuellen Linux-Kerneln enthalten. Das lässt sich



Grub-Customizer: Das grafische Tool kann die Einträge im Grub-Bootmenü konfigurieren. Außerdem lassen sich ein Hintergrundbild und Schriftfarben festlegen.

prüfen, indem man die Datei „/boot/config-[Kernel-Version]“ in einem Texteditor öffnet. Den Platzhalter ersetzen Sie durch die Versionsnummer des genutzten Kernels. Ist in der Datei die Option „CONFIG_EFI_STUB=y“ zu finden, ist der EFI-Bootloader im Kernel vorhanden und Sie können ihn direkt starten. Eine Alternative zur nachfolgend beschriebenen Konfiguration ist Refind (siehe Kasten „Alternativer Bootloader Refind“).

Schritt 1: Der Kernel und die dazugehörige Ramdisk-Datei müssen im Ordner des Systems unter „/boot/efi/EFI“ liegen. Auf der Seite *https://wiki.debian.org/EFIStub* finden Sie unter „Copy the files“ eine Anleitung, wie Sie Scripts erstellen, mit denen die Dateien bei einem Kernel-Update automatisch kopiert werden. Sie müssen die Pfade für Ihr System anpassen. Bei Ubuntu beispielsweise liegen Kernel und Ramdisk im Ordner „/boot“, der EFI-Ordner ist „/boot/efi/EFI/ubuntu“. Führen Sie die Scripts manuell aus, um die Dateien für die erste Verwendung zu kopieren.

Schritt 2: Mit dem Befehl

```
lsblk
```

finden Sie den Gerätepfad der Systempartition („/“) heraus, beispielsweise „/dev/sdb2“.

Schritt 3: Verschaffen Sie sich im Terminal mittels

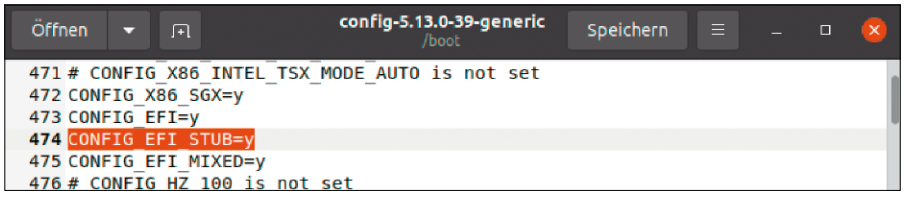
```
sudo -i
```

administrative Rechte und erstellen Sie dann den Uefi-Booteintrag mit

```
export UUID=$(blkid -s UUID -o value
 /dev/[sdXY])
efibootmgr -c -g -L "Ubuntu Efi" -l
 '\EFI\ubuntu\vmlinuz' -u
 "root=UUID=$UUID rw quiet
 rootfstype=ext4 add_efi_memmap
 initrd=\\EFI\\ubuntu\\initrd.
 img" -verbose
```

Den Platzhalter „[sdXY]“ ersetzen Sie durch die Bezeichnung, die Sie in Schritt 2 ermittelt haben. Passen Sie außerdem die Pfade für Ihr System an. Beachten Sie die exakte Verwendung der doppelten und einfachen Anführungszeichen sowie die Verwendung von „\“ und „\\“.

Das Codebeispiel finden Sie auch auf der Seite *https://wiki.debian.org/EFIStub*. ■

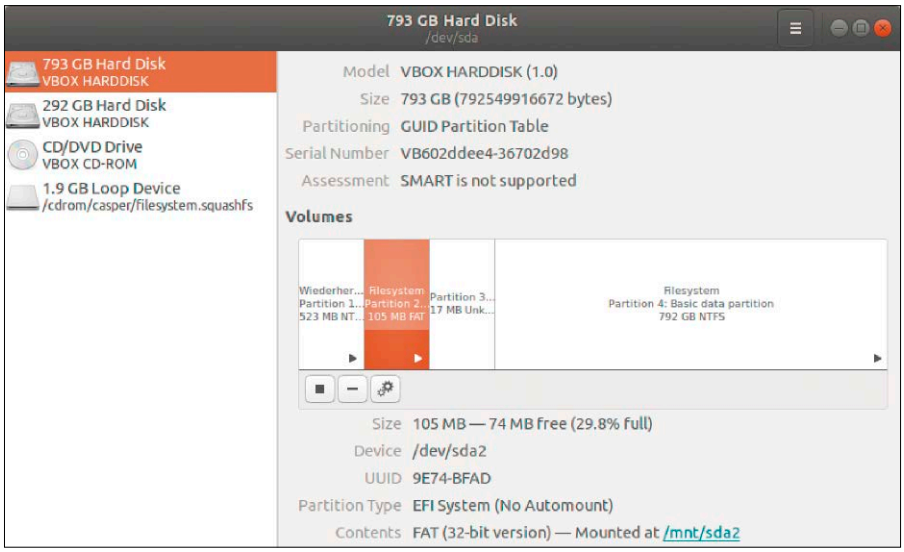


Kernel untersuchen: Wenn der Linux-Kernel mit der Option „CONFIG_EFI_STUB=y“ erstellt wurde, lässt er sich auch über die Uefi-Firmware und ohne Grub starten.

Linux-Umzug auf Uefi

Das bisherige Linux läuft auf einem Bios-PC, soll aber auf einem neuen PC im Uefi-Modus booten. Durch eine Grub-Neuinstallation lässt sich ein solcher Umzug schnell bewältigen.

VON THORSTEN EGGELING



Windows neben Linux: Windows 8.1/10 ist immer im Uefi-Modus installiert. Es gibt eine EFI-Partition, die sich aber auch für ein Linux nutzen lässt, das bisher im Bios-Modus bootet.

Die Uefi-Firmware ist flexibel und ermöglicht über ein Kompatibilitätsmodul auch den Systemstart im herkömmlichen Bios/MBR-Modus. Befinden sich zwei Festplatten im PC, kann man von einer im Uefi-Modus und von der anderen im Bios-Modus booten. Bei nur einer Festplatte muss man sich für eine der Methoden entscheiden. Soll ein im Bios-Modus installiertes Linux von einem alten auf einen neuen Computer umziehen und dort im Uefi-Modus booten, sind einige Umbauten erforderlich.

Service: Alle Befehlszeilen aus diesem Artikel lassen sich über *www.pcwelt.de/ubuefi* im Browser abrufen.

Voraussetzung und Vorbereitungen

Je nach Situation auf Ihrem PC gibt es mehrere mögliche Szenarien:

- Auf dem neuen PC ist Windows installiert. Sie wollen oder können nur eine Festplatte verwenden. Linux muss von der alten auf die neue Festplatte umziehen und für den Uefi-Modus angepasst werden.
- Sie bauen die alte Festplatte mit dem Bios/MBR-Linux als weitere Festplatte in den PC ein. Linux sowie Windows sollen sich über Grub im Uefi-Modus starten lassen.
- Sie haben einen neuen PC ohne Betriebssystem gekauft. Das bisherige Linux soll auf die neue Festplatte umziehen und im Uefi-Modus starten. Eventuell soll später auch Windows installiert werden.

In der Regel wird auf dem neuen PC Windows im Uefi-Modus installiert sein. Kontrollieren Sie im Bios/Firmware-Setup, welche Bootoptionen eingestellt sind.

In der Regel sollte in einem Menü wie „Boot“ oder „Boot Order“ als Option beispielsweise „Uefi“ oder „Uefi only“ eingestellt sein. „Uefi and Legacy“ oder „CSM“ sind auch möglich und sorgen dafür, dass der PC sowohl im Uefi- als auch im Bios-Modus booten kann.

Deaktivieren Sie außerdem Secure Boot. Die Einstellung finden Sie meist unter einem Menü wie „Bios Features“, „Security“ oder ähnlich. Die Funktion soll die Bootumgebung vor Schadsoftware schützen, indem sie nur digital signierte Software erlaubt. Linux-Distributionen wie Ubuntu stellen zwar einen signierten Kernel zur Verfügung, zusätzliche Treiber, etwa für Grafikchips von Nvidia, sind jedoch nicht signiert und lassen sich bei aktiviertem Secure Boot nicht laden.

Livesystem bereitlegen: Alle beschriebenen Arbeiten müssen über ein Zweitsystem erfolgen. Sie können Ubuntu 19.04 von der Heft-DVD verwenden, das Sie für den Uefi-Modus auf einen USB-Stick kopieren (mit dd unter Linux oder Win 32 Disk Imager unter Windows).

Linux mit Uefi neben Windows einrichten

Verbinden Sie die Festplatte mit dem alten Linux-System mit dem neuen PC. Sollte kein freier SATA-Anschluss vorhanden sein, verwenden Sie einen SATA/USB-Adapter. Starten Sie das Linux-Livesystem im Uefi-Modus. Er ist am englischsprachigen Grub-Menu auf schwarzem Untergrund zu erkennen. Das Uefi-Livesystem startet mit einer englischsprachigen Tastaturbelegung. Wenn Sie auf die deutsche Belegung umstellen möchten, drücken Sie die Taste E. Gehen Sie auf die Zeile, die mit „linux“ beginnt, und tragen Sie hinter „splash“ gefolgt von einem Leerzeichen diese Werte ein:

```
console-setup/layoutcode?=de
```

Auch im Grub-Editor gilt das englischsprachige Tastaturlayout (siehe Kasten). Drücken Sie die F10-Taste, um das Livesystem zu starten.

Schritt 1: Ist bereits Windows installiert, müssen Sie zuerst Platz für Linux schaffen. Dazu starten Sie Gparted, verkleinern die Windows-Partition und erstellen eine Ext4-Partition für Linux (siehe *www.pcwelt.de/764369*).

Schritt 2: Öffnen Sie ein Terminalfenster und verschaffen Sie sich mit

```
sudo -i
```

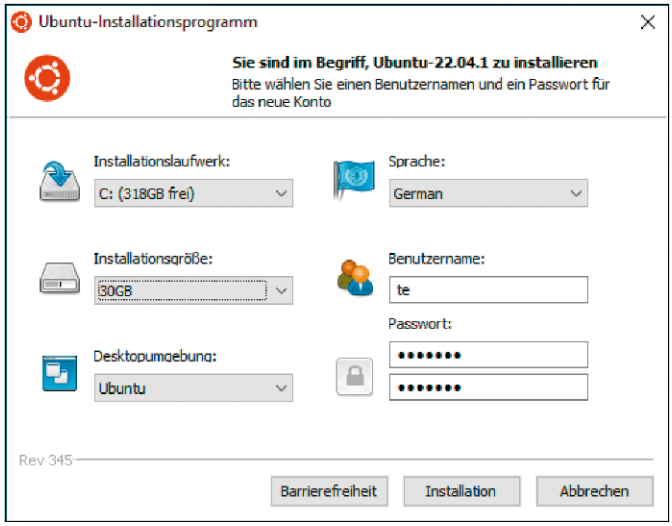
Ubuntu-Installation mit Wubiuefi

Für Linux ist standardmäßig eine eigene Partition auf der Festplatte nötig. Wenn Windows-Nutzer die bestehende Partitionierung nicht ändern möchten, können sie die Linux-Installation auch alternativ mit Hilfe von Wubiuefi durchführen.

VON THORSTEN EGGELING

Dieser und die folgenden Artikel in diesem Special beschreiben eher ungewöhnliche Linux-Installationsmethoden. Den Anfang macht Wubiuefi, mit dem sich Ubuntu von Windows aus installieren lässt. Linux benötigt dabei keine eigene Partition oder Festplatte und wird in einer Containerdatei auf der Windows-NTFS-Partition eingerichtet. Das Verfahren ist für Benutzer interessant, die möglichst wenig an der Windows-Konfiguration ändern und Linux vielleicht nur gelegentlich verwenden wollen.

Die parallele Installation von Linux und Windows auf einem PC stellt allerdings auch sonst keine besondere Herausforderung dar. Bei einer Standardinstallation erkennt das Setuptool ein bereits installiertes Windows und bietet die Einrichtung von Linux neben Windows an. Anleitungen dafür sind im E-Book dieser LinuxWelt auf der Heft-DVD zu finden.



Ubuntu-Installation vorbereiten: Wubiuefi richtet die Linux-Umgebung auf der Windows-NTFS-Partition ein. Der Systemstart erfolgt über einen Uefi-Eintrag oder den Windows-Bootmanager.

Wie Wubiuefi funktioniert

Mit Wubiuefi (*https://github.com/hakuna-m/wubiuefi*) lässt sich Ubuntu mit einem Setupprogramm von Windows 10/11 einrichten. Anders als der Name vermuten lässt, eignet sich das Tool nicht nur für die Installation auf Uefi-PCs, sondern auch für Systeme, die im herkömmlichen Bios-Modus starten.

Wubiuefi lädt die ISO-Datei des Ubuntu-Installationsmediums herunter und erstellt die erforderlichen Dateien im Ordner „C:\Ubuntu“. Die bei Redaktionsschluss aktuelle Version Wubi for Ubuntu 22.04.1 (rev. 345) richtet Ubuntu 22.04.01 ein. Sie haben dabei die Wahl zwischen allen offiziellen Flavours, also Ubuntu mit Gnome, Kubuntu (KDE), Xubuntu (XFCE), Lubuntu (LXQT), Ubuntu Budgie sowie Ubuntu Mate. Wubiuefi installiert Ubuntu in der Containerdatei „C:\ubuntu\disks\root.disk“, die mit dem Dateisystem Ext4 formatiert ist. Deshalb ist keine eigene Systempartition erforderlich. Linux kann das System standardmäßig nicht aus Containerdateien starten. Dafür sind einige Anpassungen im Bootloader und im Installationssystem durch Wubiuefi erforderlich. Deshalb müssen die Entwickler das Tool eigens für jede Ubuntu-Version überarbeiten.

Nachteile von Wubiuefi: Bei der Installation muss man vorab eine fixe Größe der Containerdatei festlegen. Maximal sind 512 GB möglich, minimal sechs GB. Die Containerdatei auf einem NTFS-Laufwerk reduziert die Systemleistung bei Festplattenzugriffen. Das ist jedoch kaum zu bemerken, vor allem, wenn die Datei auf einer schnellen SSD liegt.

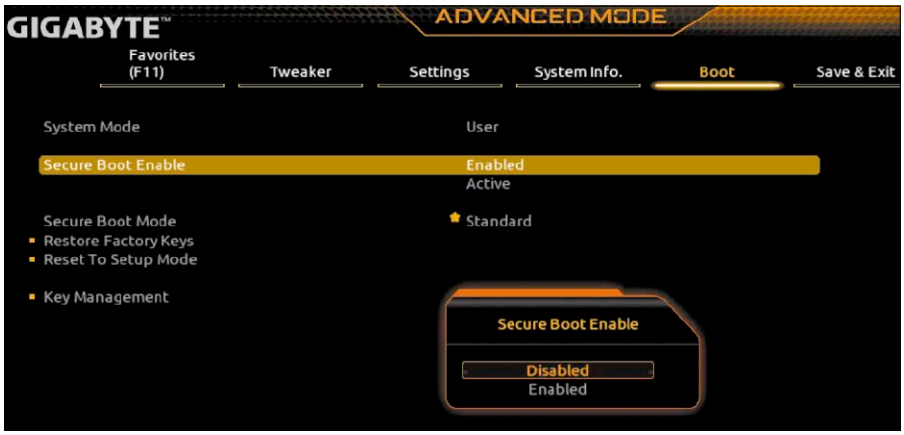
Besonderheiten bei PCs mit Uefi-Firmware

Windows 10 oder 11 sind standardmäßig im Uefi-Modus installiert. Ob das auch auf Ihrem PC der Fall ist, lässt sich unter Windows prüfen. Drücken Sie die Tastenkombination Win-R, tippen Sie *msinfo32* ein und bestätigen Sie mit „OK“. Hinter „BIOS-Modus“ steht „Vorgängerversion“, wenn keine Uefi-Firmware verwendet wird. Andernfalls lautet die Angabe „UEFI“. Hinter „Sicherer Startzustand“ (Secure Boot) finden Sie dann in der Regel den Eintrag „An“.

Vor der Linux-Installation über Wubiuefi müssen Sie ferner Secure Boot deaktivieren, weil das Tool einen modifizierten Bootloader verwendet, dessen digitale Signatur der Uefi-Firmware nicht bekannt ist. Später können Sie die Signatur des Entwicklers in

die Firmware importieren und Secure Boot wieder aktivieren.

Rufen Sie das Firmwaresetup kurz nach dem Einschalten des PCs über eine Taste wie Esc, Entf, F2, F8 oder F10 auf (nicht standardisiert). Unter Windows 10 oder 11 gelangen Sie aber auch so in das Firmwaresetup: Klicken Sie im Windows-Anmeldebildschirm rechts unten die „Ein/Aus"-Schaltfläche oder im laufenden System auf die Schaltfläche „Ein/Aus" im Startmenü. Halten Sie dann die Umschalt-Taste gedrückt und klicken Sie im Menü der Schaltfläche auf „Neu starten". Gehen Sie jetzt auf „Problembehandlung → Erweiterte Optionen → UEFI-Firmwareeinstellungen" und klicken Sie auf „Neu starten". Die Einstellungen für Secure Boot finden Sie meist unter einem Menü wie „Bios Features", „Security", „Boot" oder ähnlich. Setzen Sie die Option auf „Disabled".



Firmwaresetup: Vor der Ubuntu-Installation schalten Sie Secure Boot ab. Später importieren Sie die digitale Signatur und können die Funktion wieder aktivieren.

Linux mit Wubiuefi installieren

Laden Sie das Tool über *https://github.com/hakuna-m/wubiuefi/releases* herunter und starten Sie das Programm wubi22041r345.exe (Stand Februar 2023). Wählen Sie das Ziellaufwerk unter „Installationslaufwerk" und geben Sie unter „Installationsgröße" die gewünschte Größe der Containerdatei an. Unter „Desktopumgebung" wählen Sie die gewünschte Ubuntu-Edition, beispielsweise „Ubuntu" für das Standard-Desktopsystem mit Gnome. Den Benutzernamen übernimmt Wubiuefi von Windows, Sie können aber auch einen anderen eintragen. Legen Sie ein Passwort fest und klicken Sie auf „Installation". Das Tool lädt die ISO-Datei herunter und richtet die Dateien für Linux ein. Für einen schnelleren Download können Sie die ISO-Datei „ubuntu-22.04.1-desktop-amd64.iso" auch manuell von *https://ubuntu.com* herunterladen und im Verzeichnis von Wubiuefi ablegen.

Nach Abschluss der Ersteinrichtung starten Sie Windows neu. Der PC sollte jetzt automatisch den Uefi-Eintrag des Linux-Systems starten. Wenn nicht, gehen Sie ins Firmwaresetup und setzen „Ubuntu" an die erste Stelle in der Bootreihenfolge. Bei Rechnern mit herkömmlichem Bios erfolgt die Auswahl von „Ubuntu" über den Windows-Bootmanager.

Beim ersten Start wird das Ubuntu-Livesystem aufgerufen und die Installation eingeleitet. Bei Ubuntu 22.04 erscheint das Fenster „Aktualisierungen und andere Software", in dem man zwischen „Normale Installation" und „Minimale Installation" (nur Webbrowser und einige Dienstprogramme) wählen kann. Setzen Sie ein Häkchen vor „Installieren Sie Software von Drittanbietern für Grafik- und Wi-Fi-Hardware und zusätzliche Medienformate", wodurch Ubuntu beispielsweise Treiber für Nvidia-Grafikchips und WLAN-Adapter einrichtet. Nach einem Klick auf „Weiter" läuft der Rest automatisch ab. Danach erfolgt ein Neustart.

Vereinfachtes Setup: In der zweiten Phase der Installation startet das Ubuntu-Livesystem. Die Konfiguration zeigt nur ein Fenster, das Weitere geschieht automatisch.

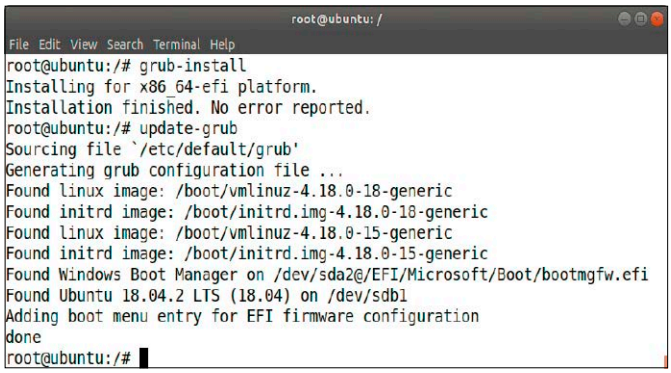
Secure Boot wieder aktivieren

Aus der Dokumentation des Entwicklers unter *https://github.com/hakuna-m/wubiuefi/wiki* ist zu schließen, dass beim ersten Start nach einer Installation bei aktiviertem Secure Boot automatisch die MOK-Verwaltung (Machine Owner Keys) aufgerufen werden sollte. Darüber ist es möglich, den Signaturschlüssel des Entwicklers zu importieren und den Bootloader damit als sicher einzustufen. Auf unseren Testrechnern hat das nicht funktioniert und wir haben Secure Boot daher für die Installation deaktiviert.

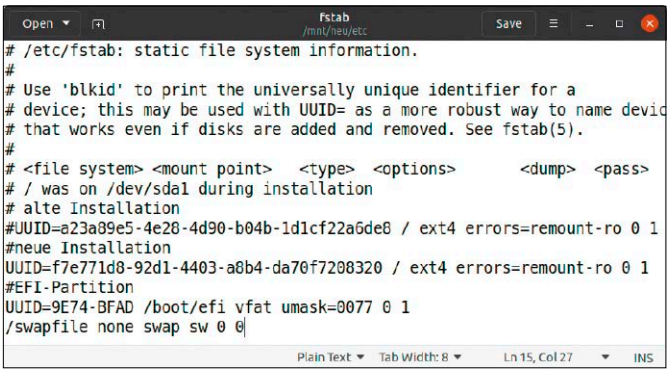
Um den Schlüssel nachträglich zu importieren, starten Sie Ubuntu und führen Sie im Terminal diesen Befehl aus:

```
sudo mokutil --import /boot/efi/
  EFI/ubuntu/wubildr/hakunamatata_
  wubi.cer
```

Geben Sie ein Passwort ein, das keine Sonderzeichen enthält, beispielsweise „12345678". Danach starten Sie neu. Beim Aufruf von Ubuntu erscheint jetzt die MOK-Verwaltung, die Sie über eine beliebige Taste aktivieren. Gehen Sie auf „Enroll MOK", „Continue" und „Yes". Tippen Sie das vorher vergebene Passwort ein, dann bestätigen Sie mit der Eingabetaste und gehen auf „Reboot". Danach rufen Sie das Firmwaresetup auf und schalten Secure Boot ein. Ubuntu startet jetzt auch mit aktiviertem Secure Boot.



Grub aktualisieren: Nach dem Linux-Umzug wird Grub mit dem Kommando *update-grub* neu eingerichtet. Die Scripts finden die Linux- und Windows-Installationen und erzeugen das Bootmenü.



Partitionen einbinden: In der Datei „/etc/fstab“ ändern Sie die UUID-Kennung für die neue Linux-Partition und binden dann die EFI-Partition in das Dateisystem unter „/boot/efi“ ein.

die root-Rechte. Mit

```
blkid
```

ermitteln Sie, welche Partitionen vorhanden sind. „/dev/sda5“ ist beispielsweise die neue Ext4-Partition, „/dev/sda2“ ist die EFI-Partition und über „/dev/sdb1“ ist die Bios-Installation auf der zweiten Festplatte zu erreichen. Führen Sie diese drei Befehle aus:

```
mkdir /mnt/neu /mnt/alt
mount /dev/sda5 /mnt/neu
mount /dev/sdb1 /mnt/alt
```

Passen Sie die Laufwerkspfade für Ihr System entsprechend an.

Schritt 3: Kopieren Sie das alte System auf die neue Festplatte. Beachten Sie den Schrägstrich „/“ jeweils am Ende der Pfade:

```
rsync --stats --progress --numeric-
  ids -axAhHSP /mnt/alt/ /mnt/neu/
```

Schritt 4: Binden Sie die EFI-Partition ein, die Windows erstellt hat:

```
mkdir /mnt/neu/boot/efi
mount /dev/sda2 /mnt/neu/boot/efi
```

Schritt 5: Führen Sie die folgenden zwei Befehlszeilen aus:

```
for dir in /dev /dev/pts /proc /sys /
  run; do sudo mount --bind $dir /
  mnt/neu/$dir; done
chroot /mnt/neu /bin/bash
```

Damit binden Sie einige Pfade des laufenden Livesystems ein und starten eine chroot-Umgebung. Sie arbeiten darin, als ob Sie den Rechner mit diesem System gestartet hätten.

Schritt 6: Entfernen Sie die installierten Grub-Pakete:

```
apt-get purge grub-common grub-pc
  os-prober
```

Danach installieren Sie Grub für den Uefi-Modus:

```
apt-get install grub-common grub-
  efi-amd64 os-prober
grub-install
update-grub
exit
```

„update-grub“ gibt alle gefundenen Betriebssysteme aus, neben Ubuntu auch das installierte Windows. Mit „exit“ in der letzten Zeile verlassen Sie die chroot-Umgebung.

Schritt 7: Sie müssen jetzt nur noch die Einbindung der Partitionen anpassen:

```
gedit /mnt/neu/etc/fstab
```

Hinter „UUID=“ ersetzen Sie die ID der vorherigen Partition durch die neue, die Sie über blkid ermitteln. Ergänzen Sie darunter die Einbindung der EFI-Partition. Ein Beispiel sehen Sie in der Abbildung. Starten Sie den PC neu. Es begrüßt Sie das Grub-Menü, in dem Sie zwischen Linux und Windows wählen können.

Leere Festplatte oder alte weiterverwenden

Soll Linux neben Windows von der alten Festplatte gestartet oder auf eine bisher leere Festplatte transportiert werden, sind die Schritte ähnlich wie zuvor beschrieben. Im ersten Fall starten Sie bei Schritt 2 und lassen Schritt 3 aus. Binden Sie die Linux-Partition als „/mnt/neu“ ein und folgen Sie den Schritten 4 bis 6. In Schritt 7 müssen Sie nur die Zeile für die EFI-Partition ergänzen, da die bisherige UUID sich nicht ändert.

Soll Linux auf ein neues, bisher leeres Laufwerk umziehen, ist es unterm Strich am einfachsten, das gleiche System im Uefi-Modus neu zu installieren. Danach löschen Sie über ein Livesystem die Dateien der Neuinstallation, kopieren mit rsync (Schritt 3) das bisherige System auf die neue Partition und folgen dann den weiteren Schritten, um die Installation anzupassen. Windows lässt sich später auf einer freien Partition oder zweiten Festplatte installieren. Danach müssen Sie wahrscheinlich Grub reparieren. Gehen Sie dabei sinngemäß so vor wie in den Schritten 2 und 4 bis 6 beschrieben. ■

ENGLISCHE TASTATURBELEGUNG FÜR GRUB UND LIVESYSTEME

Zeichen	Auf deutscher Tastatur
=	Umschalt-` (Links neben der Rücktaste)
?	Umschalt-Minus (neben Umschalt rechts)
/ (Slash)	Minus-Taste (neben Umschalt rechts)
- (Bindestrich/Minus)	ß
/ (Slash)	– (neben Umschalt rechts)
\ (Backslash) und | (Pipe)	# und Umschalt-#
: (Doppelpunkt)	Umschalt-ö
_ (Unterstrich)	Umschalt-ß
" und ' (doppelte/einfache Anf.-Zeichen)	ä und Umschalt-ä
z und y	y und z

Hardware & Treiber für Linux

Gängige Linux-Distributionen bringen Treiber für fast jede Hardware mit. Sollte ein Gerät nicht vollständig unterstützt werden oder gar nicht funktionieren, gibt es auch dafür Lösungen.

VON THORSTEN EGGELING

Computerhardware wird vor allem für den Windows-Markt produziert. Vom Gerätehersteller können Linux-Nutzer kaum Unterstützung erwarten und zusätzliche Treiber für Linux gibt es in der Regel nicht als Setup-Paket. Es ist daher ratsam, sich bereits vor dem Kauf neuer Hardware über die Linux-Tauglichkeit zu informieren. Auf älteren PCs oder Notebooks lässt sich Linux meist ohne besondere Auffälligkeiten installieren. Aber auch hier kann es in Ausnahmefällen vorkommen, dass der Bildschirm schwarz bleibt, einzelne Funktionen unter Linux nicht bereitstehen oder neuere Hardware am USB-Anschluss nicht erkannt wird. Einige Probleme lassen sich durch Konfigurationsänderungen oder durch Wechsel der Linux-Distribution beheben. Am Anfang steht jedoch die Untersuchung der Hardware. Die kann ergeben, dass sich das Gerät mit einem neueren Kernel oder einem zusätzlichen Treiber nutzen lässt.

Hardwaremacken umgehen

PC-Hardware folgt keinen eindeutigen Standards. Für die Hersteller ist nur eins wichtig: Windows muss anstandslos laufen. Der eine oder andere Fehler in der Firmware oder auf der Hauptplatine wird dann bei Bedarf über einen Treiber repariert, den es für Linux aber nicht gibt. Besonders Notebooks, die auf Microsoft Windows zugeschnitten sind, bereiten mit ihren zahlreichen Bios-Versionen, abweichenden ACPI-Stromsparfunktionen und Chipsatzvarianten häufiger Ärger. Mal bleibt der Bildschirm dunkel, mal geht nach den ersten Bootmeldungen nichts mehr weiter. Bei der Linux-Neuinstallation helfen dann oft spezielle Kernel-Parameter weiter.

Wenn Sie Ubuntu 22.04 oder Linux Mint 21 vom Installationsmedium booten, begrüßt Sie das Grub-Bootmenü. Mit dem ersten Eintrag „Try or Install Ubuntu“ beziehungsweise „Start Linux Mint 21 Cinnamon 64-Bit“ startet das System mit den Standardeinstellungen.

Sollte der Bildschirm schwarz bleiben oder unlesbar sein, kann der zweite Menüeintrag „Ubuntu (safe graphics)“ oder „Start Linux Mint 21 Cinnamon 64-Bit (compatibility mode)“ weiterhelfen. Dabei werden Optionen an den Kernel übergeben, die die Hardwaresteuerung beeinflussen. Jedes Linux-System bietet eine Reihe von Kernel-Optionen – in der Dokumentation oft auch als Bootparameter oder Cheatcodes bezeichnet.

Über das Grub-Bootmenü lassen sich zusätzliche Optionen angeben. Dazu drückt man nach der Markierung eines Bootеintrags die Taste E und erhält dann einen Mini-Texteditor für den jeweiligen Eintrag gezeigt. Die Navigation im Textfeld erfolgt mit den Cursortasten. Grundsätzlich müssen Kernel-Parameter in die Zeile eingetragen werden, die mit „linux“ beginnt, aber vor „--“. Nach der Änderung startet die Taste F10 den Bootеintrag mit den neuen Einstellungen.

Bitte beachten Sie, dass im Grub-Editor eine englischsprachige Tastaturbelegung gilt. Bleibt der Bildschirm nach einem zunächst erfolgreichen Start dunkel, so liegt dies meist an nicht ausreichend unterstützten Grafikchips. Folgende Optionen können in diesem Fall weiterhelfen.

xforcevesa: Bei der Angabe dieser Option nutzt der Kernel für die Anzeige der grafischen Oberfläche nur den Vesa-Modus. Dieser Modus läuft auf den meisten Grafikchips, ohne jedoch deren spezielle Merkmale wie Hardwarebeschleunigung und Fähigkeiten zu nutzen.

nomodeset: Aktuelle Linux-Kernel können den Bildschirmmodus auf eigene Faust wechseln und schalten schon während des Bootvorgangs in einen grafischen Modus. Dies funktioniert nicht bei allen Grafikchips – so haben einige Modelle von Nvidia Probleme damit. Mit „nomodeset" verzichtet der Kernel auf den Wechsel in den Grafikmodus und bleibt bei purem Text. Ubuntu und Linux Mint verwenden diese Option bei Auswahl des zweiten Menüeintrags.

Auf einigen Notebooks verhindern inkompatible Stromsparfunktionen im ACPI (Advanced Configuration and Power Interface) den Linux-Start. Linux Mint verwendet beim Menüeintrag „Start Linux Mint 21 Cinnamon 64-Bit (compatibility mode)" einige der nachfolgend genannten Optionen.

acpi=off oder **noacpi** zwingt Linux dazu, ACPI komplett zu ignorieren und damit ohne Stromsparfunktionen und Leistungsmanagement für CPU und GPU zu starten. Auch Hyperthreading und die Lüfterregelung sind abgeschaltet.

acpi=ht: Mit dieser Option beachtet der Linux-Kernel gerade mal so viele ACPI-Fähigkeiten der Hardware, dass Hyperthreading der CPU funktioniert. Andere Stromsparfunktionen bleiben dagegen deaktiviert.

acpi=strict weist die ACPI-Unterstützung des Kernels an, nur ACPI-Merkmale der vorhandenen Hardware zu beachten, die exakt dem Standard folgen. Auf problematischen Notebooks ist diese Option immer einen Versuch wert.

acpi_osi=linux umgeht die Abfrage des Linux-Kernels, ob das ACPI eines Rechners kompatibel ist. Sinnvoll ist dieser Parameter, wenn einige Stromsparfunktionen nicht verfügbar sind oder die Drehzahlsteuerung der Lüfter nicht funktioniert.

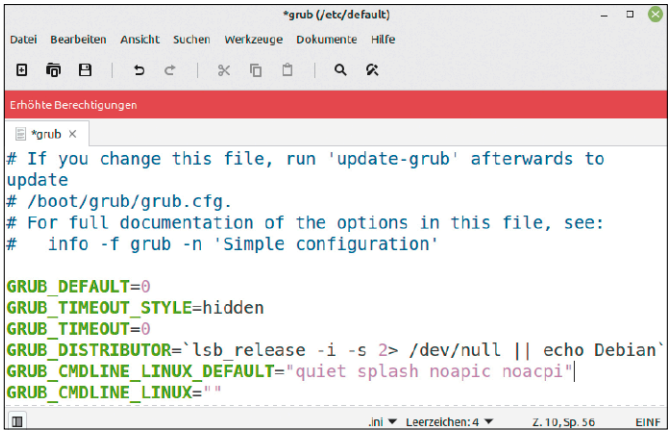
Eine weitere Komponente nennt sich „Local APIC" und nimmt die Interrupt-Anforderungen auf jedem Prozessorkern entgegen. Der Parameter „nolapic" löst vielfältige Probleme mit heiklen Bios-Versionen, reduziert aber in jedem Fall die Zahl der vorhandenen CPU-Kerne auf einen. Geeignet ist dies nur als erste Hilfe, bis ein Bios-Update oder eine neue Kernel-Version echte Abhilfe schafft.

noapic: Verhindert, dass APIC für die Auflösung von Hardwarekonflikten auf Interrupt-Ebene verwendet wird. Der Parameter hilft auf Systemen mit einem unverträglichen Bios und inkompatiblen ACPI-Funktionen weiter. Eine häufig erfolgreiche Kombination bei besonders widerspenstigen Notebooks ist diese:

```
acpi=off noapic nolapic
```

Kernel-Optionen: Hardwareprobleme lassen sich im Grub-Bootmenü teilweise mit zusätzlichen Optionen umgehen. Linux Mint bietet einige standardmäßig an.

Kernel konfigurieren: Damit Ubuntu oder Linux Mint Kernel-Optionen bei jedem Start verwenden, müssen diese in die Datei „/etc/default/grub" eingetragen werden.



iommu=soft: Die „Input-Output Memory Management Unit" (IOMMU) ist ein Merkmal einiger Hauptplatinen und erlaubt Peripheriegeräten den direkten Speicherzugriff. Dies funktioniert zusammen mit Linux nicht immer, was zum Ausfall von USB-Ports oder Netzwerkchip führt. Dieser Parameter aktiviert zusammen mit abgeschaltetem IOMMU im Bios/Uefi, ein softwaremäßiges IOMMU.

Für Ubuntu und Co. liefert die englischsprachige Hilfeseite *https://help.ubuntu.com/community/BootOptions* eine Übersicht geläufiger Bootparameter. Die komplette Liste der Parameter mit Beschreibung für Entwickler bietet die offizielle Kernel-Dokumentation unter *https://www.kernel.org/doc/html/latest/admin-guide/kernel-parameters.html*.

Nach der Linux-Installation: Für ein installiertes System lassen sich die gewünschten Kernel-Optionen via Bootloader genauso angeben wie im Live- und Installationssystem.

Damit eine Änderung permanent gilt, ist die Bearbeitung einer Konfigurationsdatei mit sudo-Recht nötig:

```
sudo -H gedit /etc/default/grub
```

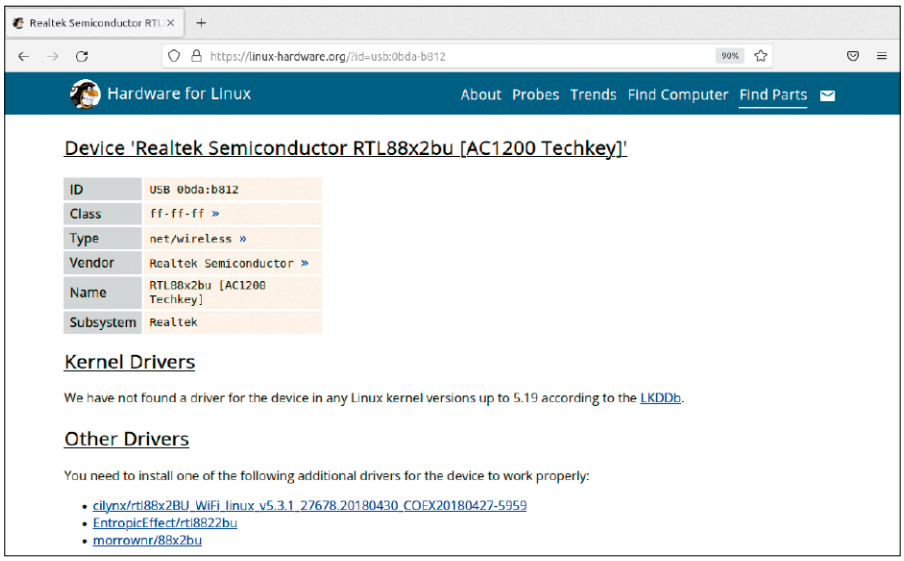
Die Zeile

```
GRUB_CMDLINE_
  LINUX="[parameter1]=[wert1]
  [parameter2]=[wert2]"
```

definiert die manuell hinzugefügten Angaben. Stehen hier schon Optionen, so ergänzen Sie zusätzlich nötigen nach einem Leerzeichen in dieser Zeile. Nach Änderung und Sicherung der Konfigurationsdatei ist die Änderung aber noch nicht wirksam, denn erst muss noch der Bootloader mit diesem Terminalbefehl aktualisiert werden:

```
sudo update-grub
```

Erst danach startet das Linux-System standardmäßig mit den hinzugefügten Kernel-Optionen.



Kein Treiber: Hardware Infos findet man bei *https://linux-hardware.org*. Für das Gerät mit der ID „0bda:b812“ ist bis einschließlich Version 5.19 kein Kernel-Modul vorhanden.

Hardware untersuchen und Infos finden

Jedes interne und externe Gerät besitzt eine eindeutige ID, die über den Herstellerund das Gerät informiert. Diese IDs lassen sich im Terminal mit den folgenden drei Befehlszeilen auslesen und in einer Datei speichern:

```
sudo lshw -numeric -html > lshw.html
sudo lspci -nn > lspci.txt
sudo lsusb -v > lsusb.txt
```

In der Datei „lshw.html“ finden Sie allgemeine Informationen zum PC, etwa den Typ der Hauptplatine, die Firmwareversion und den Prozessortyp. „lspci.txt“ zeigt Informationen über per PCI (Peripheral Component Interconnect) angebundene Komponenten, beispielsweise Soundchips („Audio device“), Grafikkarten („VGA compatible controller“) und Netzwerkchips („Ethernet controller“). In der Datei „lsusb.txt“ sehen Sie, welche Geräte mit den USB-Ports verbunden sind.

Ein Beispiel: Mit lsusb finden Sie die ID „0bda:b812“. Der erste Teil „0bda“ verweist auf den Hersteller „Realtek Semiconductor Corp.“ (siehe USB ID Repository: *https://usb-ids.gowdy.us/read/UD*), der zweite Teil „b812“ kennzeichnet das Gerät. Eine Internetsuche nach der kompletten ID liefert einige Ergebnisse, darunter auch *https://linux-hardware.org/?id=usb:0bda-b812*. Hier erfährt man, dass bis einschließlich Kernel 5.19 kein Treiber für diesen WLAN-Stick mit dem Chipsatz „RTL88x2bu“ verfügbar ist. In der Liste unter „Status“ sind einige Analysen zu finden, die Nutzer an *https://linux-hardware.org* gesendet haben. Bei den meisten steht „failed“ – das Gerät ließ sich also nicht in Betrieb nehmen. Die ersten Einträge mit „works“ weisen darauf hin, dass ein Treiber von *https://github.com/morrownr/88x2bu* für diese Hardware erforderlich ist.

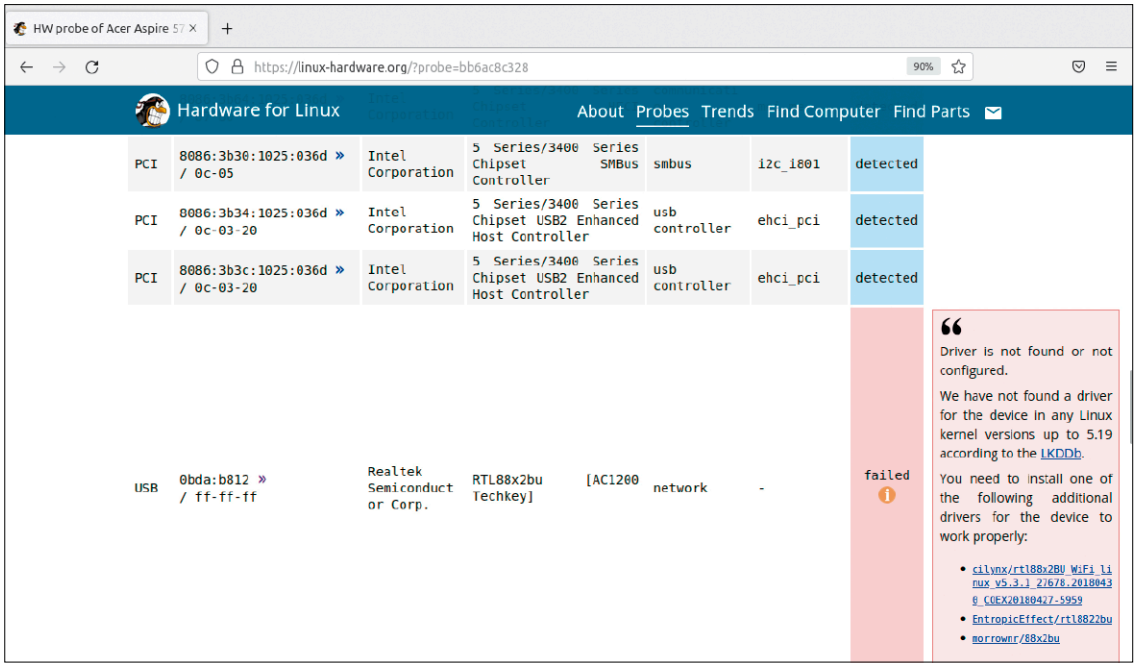
Analysedaten einsenden: Statt nach der Geräte-ID zu suchen, kann man die Daten seines PCs selbst anonym bei *https://linux-hardware.org* hochladen und dort prüfen lassen. Nutzer von Ubuntu oder Linux Mint installieren das nötige Tool im Terminal:

```
sudo apt install hw-probe
```

und starten es so:

```
sudo -E hw-probe -all -upload
```

Sie erhalten eine URL, die Sie im Browser aufrufen. In der Übersicht unter „Devices“ sind dann alle Geräte aufgelistet. Steht in der Spalte „Status“ der Eintrag „works“ oder „detected“, sollte das Gerät funktionieren. Ausrufungszeichen deuten jeweils darauf hin, dass es bei einzelnen Benutzern Probleme gab. Ein Klick darauf führt zu weiteren Informationen. Beim Status „failed“ wurde kein Treiber gefunden, geladen oder konfiguriert. Sofern vorhanden, führt ein Kasten



Problemlösung: Nach Einsendung der Hardwareanalyse zeigt *https://linux-hardware.org* an, welches Gerät nicht funktioniert und was dagegen zu tun ist.

rechts daneben zur Lösung. Weiter unten auf der Seite unter „Logs“ kann man sich per Klick etwa auf „Hwinfo“, „Lspci“ oder „Lsusb“ die Ausgaben der jeweiligen Tools anzeigen lassen.

Neue Kernel oder Treiber

Die Infos von *https://linux-hardware.org* können ergeben, dass ein neuerer Kernel die Hardware unterstützt. Welchen Kernel Ihr System aktuell nutzt, finden Sie im Terminal mit dem Befehl

```
uname -a
```

heraus. Ubuntu 22.04 und Linux Mint 21 verwenden zur Zeit die Kernel-Version 5.15. Wer einen neueren Kernel benötigt, muss ihn selbst erstellen. Eine Anleitung für Ubuntu und Linux Mint finden Sie über *https://m6u.de/BMUK*. Alternativ kann man zu einer Distribution wechseln, die deutliche aktuellere Updates bietet („Rolling Release“). Manjaro Linux beispielsweise ist aktuell schon bei Kernel 6.0.2 (*https://manjaro.org*).

Treiber kompilieren: Wenn der Quellcode verfügbar ist, kann man den Treiber selbst erstellen. Dabei gibt es zwei Herausforderungen: Der Quellcode muss zum laufenden Kernel passen und die nötigen Schritte können sich je nach Treiber unterscheiden. Lesen Sie daher immer die zugehörigen Anleitungen sorgfältig durch. Exemplarisch liefern wir eine kurze Anleitung für den oben genannten WLAN-Stick mit dem Chipsatz „RTL88x2bu“.

Schritt 1: Öffnen Sie ein Terminal und installieren Sie einige zusätzliche Pakete:

```
sudo apt install git build-
  essential dkms linux-headers-
  $(uname -r)
```

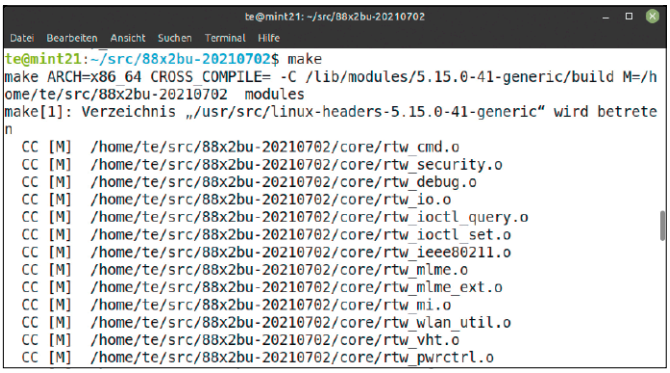
Schritt 2: Gehen Sie auf *https://github.com/morrownr/88x2bu-20210702* und klicken Sie auf „Code“. Kopieren Sie die URL unter „HTTPS“. Dann erstellen Sie ein Arbeitsverzeichnis und laden den Quelltext des Treibers herunter (vier Zeilen):

```
mkdir -p ~/src
cd ~/src
git clone [URL]
cd 88x2bu-20210702
```

Statt „[URL]“ fügen Sie die zuvor kopierte Adresse ein. Passen Sie die Pfadangabe hinter „cd“ entsprechen der Treiberversion an.

Schritt 3: Führen Sie die folgenden drei Befehle aus:

```
make clean
make
sudo insmod 88x2bu.ko
```



Treiber kompilieren: Nach dem Download des Treiber-Quellcodes genügt in der Regel der Befehl „make“, der ein neues Modul für den laufenden Kernel erstellt.

Damit wird der Treiber aus dem aktuellen Ordner „~/src/88x2bu-20210702“ geladen. Mittels

```
dmesg
```

lassen Sie sich die letzten Kernel-Meldungen ausgeben, die über den erfolgreich geladenen Treiber informieren oder Fehlermeldungen anzeigen. Für die meisten Treiber folgt abschließend dieser Befehl:

```
sudo make install
```

Damit wird der Treiber in einen Ordner unterhalb von „/lib/modules/[Kernel-Version]“ kopiert und ab dem nächsten Linux-Start automatisch geladen. Bei unserem Beispieltreiber ist das nicht erforderlich, weil ein Script die Aufgabe übernimmt (siehe Schritt 4).

Die WLAN-Hardware funktioniert jetzt und Verbindungen lassen sich wie gewohnt über den Netzwerkmanager herstellen.

Wenn allerdings Secure Boot aktiviert ist, erzeugt der Befehl insmod eine Fehlermeldung: Der Treiber wird nicht geladen, weil er nicht digital signiert ist. Sie müssen dann entweder Secure Boot im Firmwaresetup deaktivieren oder den Treiber signieren (siehe *https://m6u.de/KNMD*).

Schritt 4: Der Treiber von *https://github.com/morrownr/88x2bu-20210702* lässt sich komfortabel per Script einrichten:

```
sudo ./install-driver.sh
```

Sie werden gefragt, ob Sie die Konfigurationsdatei „/etc/modprobe.d/88x2bu.conf“ mit den Treiberoptionen bearbeiten möchten. In der Regel ist das nicht nötig, Erklärungen zu den Optionen sind in der Konfigurationsdatei enthalten. Wenn Sie Linux jetzt neu starten, wird der neue Treiber automatisch geladen und die WLAN-Hardware lässt sich nutzen. ■

LINUX UND NEUE HARDWARE

Vor der Anschaffung neuer Hardware sollte man sich immer über die Linux-Kompatibilität informieren. Bei Notebooks oder PCs können Händler nur selten Auskunft geben, außer sie sind auf Linux-Hardware spezialisiert. Hersteller von WLAN- oder TV-Sticks geben manchmal Linux in der Liste der unterstützten Betriebssysteme an. Dann kann es sein, dass sich das Gerät mit gängigen und aktuellen Linux-Distributionen direkt in Betrieb nehmen lässt. Oft ist die Linux-Unterstützung jedoch nur theoretisch vorhanden. Konkret: Es funktioniert eventuell nur mit einer bestimmten Distribution oder Kernel-Version. Oder es ist nur Sourcecode verfügbar, aus dem man den Treiber selbst kompilieren muss.

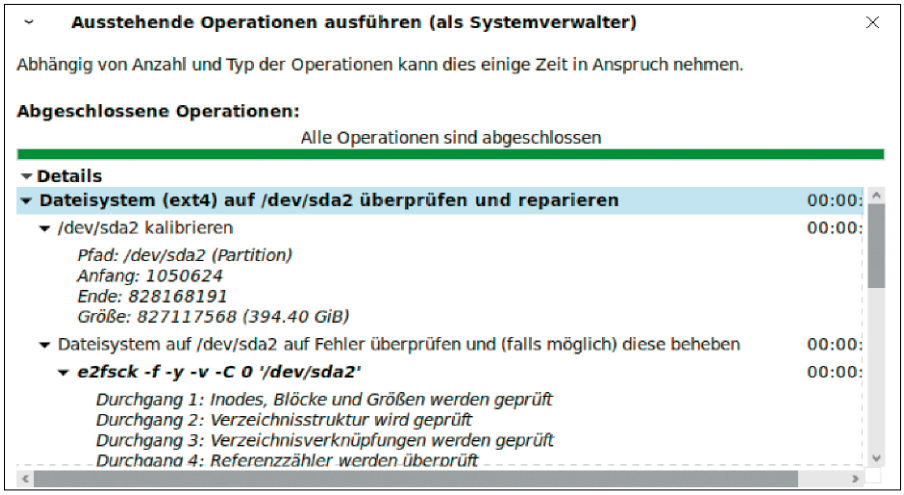
Lesen Sie daher die Rezensionen und Bewertungen anderer Käufer und suchen Sie im Internet nach den Erfahrungen von Linux-Nutzern. Basiskomponenten wie SATA-Adapter, Onboard-Ethernet und Grafikchips bereiten selten Probleme. Oft sind es auch nur Kleinigkeiten, die nicht funktionieren – lästig ist das trotzdem. Bei Notebooks beispielsweise reagieren manchmal die Tasten für die Bildschirmhelligkeit oder Lautstärke nicht, das Touchpad lässt sich nicht nutzen oder der Akku wird unter Linux zu schnell leer. Die Lösungen, die man im Internet findet, sind so vielfältig wie die Hardwarekomponenten. Im besten Fall ist nur eine kleine Änderung in der Konfiguration nötig oder ein Firmwareupdate. Wenn ein Gerät unter Linux aber als Problemkandidat bekannt ist, sollte man Abstand nehmen.

Linux-Bootprobleme beseitigen

Wenn Linux nicht mehr bootet, kann eine defekte Festplatte oder ein korruptes Dateisystem die Ursache sein. Meist ist aber nur die Bootumgebung beschädigt, was sich dann relativ leicht reparieren lässt.

VON THORSTEN EGGELING

Es kann durch Updates, ein Systemupgrade oder durch eine Windows-Installation verursacht werden: Linux bootet nicht mehr. Symptome sind, dass der Bildschirm nach dem Einschalten des PCs schwarz bleibt oder eine Fehlermeldung des Bootmanagers Grub erscheint. Dieser Zustand ist von Problemen mit der Desktopumgebung zu unterscheiden (siehe Artikel ab Seite 36). Auch dabei kann zwar der Monitor schwarz bleiben, doch zeigt die Laufwerks-LED nach dem Start über eine längere Zeit deutliche Aktivitäten, was auf ein arbeitendes System schließen lässt.



Dateisystem prüfen: Defekte im Dateisystem können den Linux-Start verhindern. Analyse und Reparatur lassen sich in einem Rettungssystem mit Gparted durchführen.

1. Hardware untersuchen und Daten retten

Als Erstes prüfen Sie, ob die Festplatte oder SSD noch ansprechbar ist. Dazu rufen Sie das Firmwaresetup auf, was meist über Tasten wie Esc, F2 oder Entf kurz nach dem Einschalten des PCs gelingt. Oft sehen Sie die verfügbaren Laufwerke bereits auf der Übersichtsseite oder in einem Menü wie „Boot“. Das Linux-Laufwerk beziehungsweise das Laufwerk mit dem Bootmanager muss in der Bootreihenfolge an der ersten Stelle stehen. Bei einem Uefi-PC ist das bei Ubuntu und Linux Mint ein Eintrag, der mit „ubuntu“ beginnt. Sollte das Linux-Laufwerk nicht dabei sein, prüfen Sie im PC die Verbindung mit dem Datenkabel und die Stromversorgung.

Für weitere Untersuchungen booten Sie den PC mit dem LinuxWelt-Rettungssystem von der LinuxWelt-DVD. Aus der ISO-Datei im Ordner „Image-Dateien“ können Sie auch einen USB-Stick erstellen. Verwenden Sie dafür Unetbootin (auf der LinuxWelt-DVD). Zusätzliche Infos zu bootfähigen USB-Sticks finden Sie unter *www.pcwelt.de/2089747*.

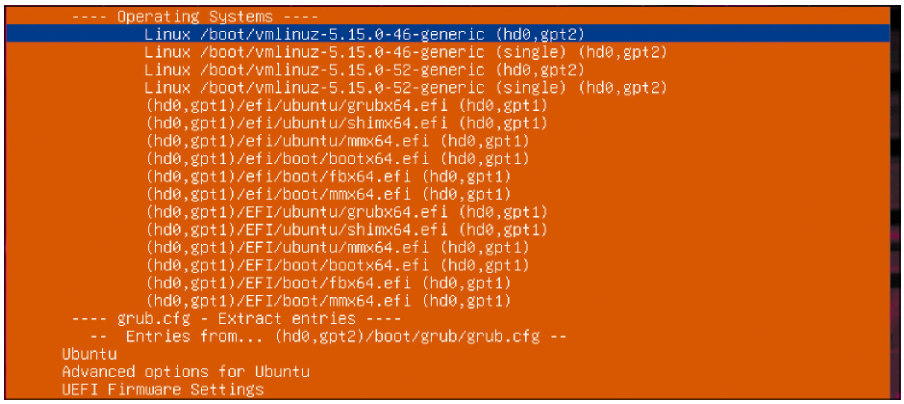
Starten Sie im Rettungssystem den Dateimanager per Doppelklick auf das Icon „Rechner“ auf dem Desktop. Unter „Geräte“ lässt sich die Linux-Partition mit einem Mausklick einhängen. Sie können dann Dateien aus Ihrem Home-Verzeichnis auf einen externen Datenträger sichern (siehe auch den Artikel ab Seite 34). Das ist sinnvoll, wenn das System aufgrund zeitweiser Ausfälle oder wegen Defekten im Dateisystem nicht bootet.

Starten Sie das Tool Gparted über das Menü und „Systemwerkzeuge“ oder über das Icon in der Taskleiste. Wählen Sie das Linux-Laufwerk rechts oben aus und klicken Sie die Linux-Partition mit der rechten Maustaste an. Wählen Sie im Menü „Aushängen“, wenn Sie die Partition zuvor über den Dateimanager eingebunden haben. Danach wählen Sie „Überprüfen“ und bestätigen die Aktion über „Bearbeiten → Alle Operationen ausführen“. Wenn das Dateisystem repariert werden konnte, sollte Linux wieder starten. Andernfalls ist wahrscheinlich die Bootumgebung defekt und muss repariert werden.

2. Linux über Zweit-Grub starten

Super Grub Disk 2 (*www.supergrubdisk.org*) lässt sich von der LinuxWelt-DVD über den Menüpunkt „Extras und Tools“ booten. Für einen USB-Stick laden Sie die ISO-Datei vom Hersteller herunter. Achten Sie darauf, dass der PC bei einem Uefi-System über den Booteintrag mit dem vorangestellten „Uefi“ bootet. Gehen Sie im Menü auf „Detect and show boot methods“. Super Grub

Disk 2 sucht nach bootfähigen Systemen und zeigt diese an. Es genügt, den gewünschten Eintrag unter „Operating Systems“ zu wählen, beispielsweise „Linux /boot/vmlinuz-5.15.0-41-generic (hd0, gpt2)“. Grub lädt den Kernel direkt und startet das System. Das funktioniert auf Bios- und Uefi-Systemen. Im erfolgreich gestarteten Linux reparieren Sie anschließend die Bootumgebung (siehe Punkt 3).



Booten im Notfall: Wenn zumindest der Linux-Kernel auf der Festplatte zu finden ist, lässt sich Linux über ein Rettungsmedium mit Super Grub Disk 2 starten.

3. Grub-Bootumgebung wiederherstellen

Starten Sie das System über Super Grub Disk 2 (siehe Punkt 2) und öffnen Sie ein Terminalfenster. Bei einer Uefi-Installation ermitteln Sie zuerst, ob die Uefi-Partition vorhanden und in das Dateisystem eingebunden ist. Der Befehl

```
mount | grep boot
```

sollte beispielsweise „/dev/sda1 on /boot/efi type vfat“ ausgeben. Im Ordner „/boot/efi/EFI/ubuntu“ liegen die Bootloader-Dateien mit der Dateinamenserweiterung „.efi“. Wenn das nicht der Fall ist, ermitteln Sie mittels

```
sudo parted -l
```

(kleines „L“) die Partitionen. Eine FAT32-Partiton, meist mit der Bezeichnung „EFI System Partition“, hat beispielsweise die Nummer „1“ („dev/sda1“). Binden Sie die EFI-Partition mit

```
sudo mount /dev/sda1 /boot/efi
```

ein. Danach verwenden Sie die folgenden Befehle:

```
sudo grub-install --recheck
sudo update-grub
```

Kontrollieren Sie in der Datei „/etc/fstab“, ob die Partitionen korrekt eingebunden werden. Vergleichen Sie ferner die Werte hinter „UUID=“ (Laufwerkskennung) mit der Ausgabe von

```
blkid
```

und korrigieren Sie bei Bedarf die Angaben in der Datei „/etc/fstab“.

Bios-System: Standardmäßig wird der Bootloader auf dem Systemlaufwerk installiert, sofern Sie bei der Installation nichts anderes gewählt haben. Bei einer Neuinstallation richten Ubuntu 22.04 und Linux Mint 21 das Laufwerk im GPT-Stil ein. Der Befehl

```
sudo parted -l
```

zeigt dann eine „EFI System Partition“. Die spielt jedoch im Moment keine Rolle und ist für den Fall gedacht, dass Sie die Festplatte später in einem neuen PC mit Uefi-Firmware verwenden wollen. Grub ist auf der Bios-Boot-Partition installiert, bei der in der Spalte „Flags“ der Wert „bios_grub“ steht. Das Installationslaufwerk lässt sich mit

```
mount | grep "on / type"
```

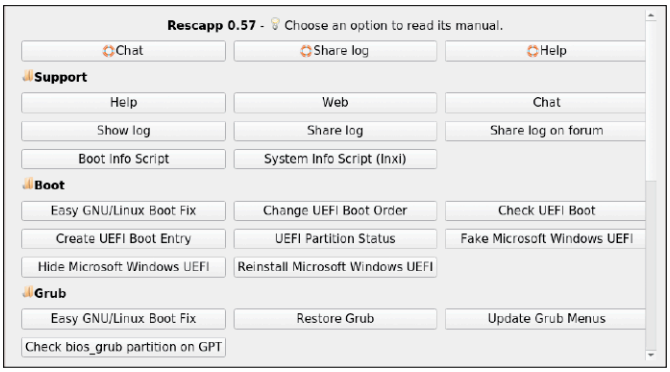
ermitteln. Wenn „sda“ in der Ausgabe auftaucht, ist Linux auf der ersten Festplatte installiert, bei „sdb“ auf der zweiten. Sie können auch die zweite Festplatte als Ziel der Grub-Installation angeben, müssen dann aber die Bootreihenfolge im Firmwaresetup entsprechend anpassen.

Für die erneute Grub-Installation verwenden Sie diese beiden Befehle:

```
sudo grub-install --recheck /dev/sdx
sudo update-grub
```

Für „sdx“ tragen Sie die Bezeichnung für die Boot-Festplatte ein, beispielsweise „/dev/sda“.

Wichtig: Geben Sie nur den Gerätenamen ohne Partitionsnummer an.



Reparaturen durchführen: Mit Rescatux lassen sich die meisten Probleme mit der Bootumgebung beheben. In der Regel führt „Easy GNU/Linux Boot Fix“ zum Erfolg.

4. Grub-Reparatur über ein Rettungssystem

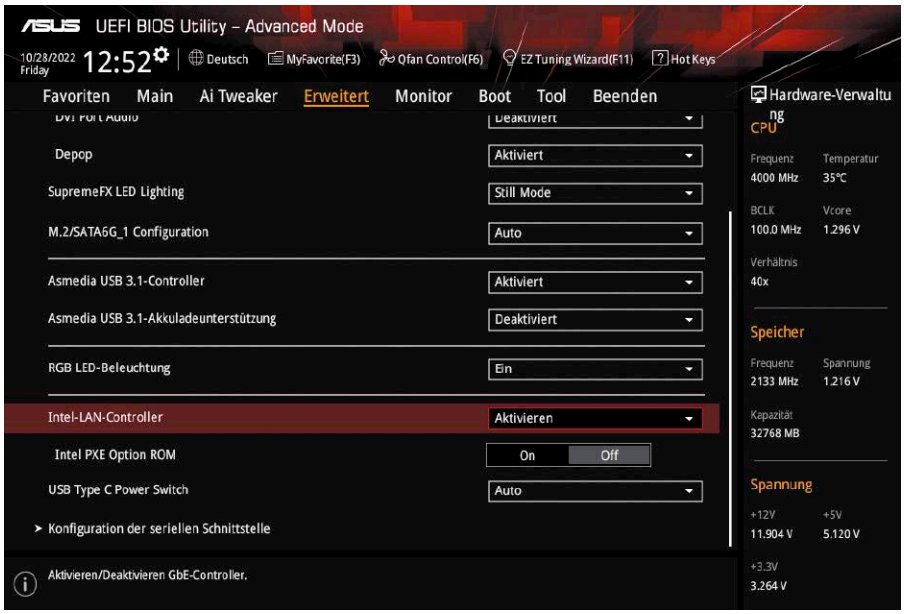
Rescatux (*www.supergrubdisk.org/rescatux*) bietet Werkzeuge für die grafische Oberfläche, mit denen sich Linux reparieren lässt. Sie finden das System auch in der ISO-Datei der Extra-DVD zu diesem Heft (siehe Seite 13). Booten Sie den PC mit Rescatux. Im Fenster „Rescatux-Startup-Wizard“ klicken Sie auf „Yes“, womit Sie die Standardeinstellungen wählen. Danach klicken Sie auf „Start Rescapp“.

Per Klick auf „Menu“ gelangen Sie zu einem Fenster mit Schaltflächen für die eigentlichen Funktionen. „Easy GNU/Linux Boot Fix → Run“ ermöglicht die Reparatur des Grub-2-Bootloaders. Das Tool durchsucht alle Laufwerke nach Partitionen und bietet diese zur Auswahl an. Hier wählt man jene Partition aus, die das Linux-System beherbergt, beispielsweise „sda2 Linux_Mint_21_Vanessa“. Nach einem Klick auf „OK“ fragt das Tool nach der Zielfestplatte für Grub. In der Regel wählen Sie „sda“, außer Sie haben Bootloader- und Systemlaufwerk auf getrennten Festplatten eingerichtet. Klicken Sie auf „OK“. Jetzt lässt sich bei Bedarf die Uefi-Bootreihenfolge anpassen. Setzen Sie den Eintrag „ubuntu“ an die erste Stelle. Nach einem Klick auf „OK“ wird die Reparatur durchgeführt. Beenden Sie Rescatux und starten Sie dann das installierte Linux-System. ■

Netzwerkfehlern auf der Spur

Wenn das Netzwerk nicht wie gewohnt funktioniert, liegt eine fehlerhafte Konfiguration vor oder die Hardware ist defekt. Linux bietet einige Tools, mit denen sich das Netzwerk analysieren lässt.

VON THORSTEN EGGELING



Firmwareeinstellungen: Onboard-Netzwerkadapter lassen sich im Setup deaktivieren, was auch mal versehentlich geschehen kann. Dann kann die Hardware von Linux nicht erkannt werden.

Netzwerkausfälle sind schwer zu diagnostizieren, weil dafür mehrere Komponenten die Ursache sein können. Für diesen Artikel gehen wir davon aus, dass der DSL-Router eine Internetverbindung hergestellt hat, dass WLAN oder die Ethernet-Verbindung sowie weitere beteiligte Geräte wie WLAN-Access-Point, Switch oder Repeater funktionieren. Die Grundvoraussetzungen lassen sich am einfachsten mit einem zweiten PC, Notebook, Tablet oder Smartphone prüfen. Sind externe Fehlerquellen ausgeschlossen, kann das Problem nur beim betroffenen PC oder seinem Betriebssystem liegen.

Netzwerkkonfiguration im Terminal prüfen

Ermitteln Sie zuerst die IP-Adresse des DSL-Routers oder Kabelmodems. Als Standard wird oft 192.168.0.1 oder 192.168.1.1 verwendet, bei einer Fritzbox 192.168.178.1. Sehen Sie im Handbuch oder auf der Unterseite des Routers nach. Sie können auch ein Gerät mit funktionierender Netzwerkverbindung verwenden und die nachfolgenden Befehle hier ausführen. In einem Terminal finden Sie die IP-Adresse des PCs mit dem Befehl

```
ip a
```

heraus. Unter „1:“ steht hinter „inet“ immer die IP-Adresse „127.0.0.1“ des Loopback-Adapters („lo“), der internen Aufgaben dient. Danach folgen unter „1:“, „2:“, und so weiter die Angaben für Ethernet und WLAN-Adapter. Lautet die IP-Adresse in einem Fritzbox-Netzwerk beispielsweise „192.168.178.175“ (Adressbereich „192.168.178.2“ bis „192.168.178.254“), dann hat das Gerät eine korrekte IP-Adresse per DHCP (Dynamic Host Configuration Protocol) vom Router erhalten. Steht hinter „inet“ eine IP aus einem anderen Bereich oder gar keine Adresse, kann keine Verbindung zum Netzwerk aufgebaut werden. Mit

```
route -n
```

führen Sie einen weiteren Test durch. In der Spalte „Router“ muss die IP-Nummer des Routers stehen, beispielsweise „192.168.178.1“ bei einer Fritzbox.

Dabei gibt es eine Ausnahme: Wenn die Verbindung über einen zweiten Router oder einen WLAN-Access-Point aufgebaut wird, können diese für ein eigenes Netzwerk konfiguriert sein. Die Geräte leiten den Datenverkehr dann von einem zum anderen Netzwerk. In diesem Fall prüfen Sie, ob Access Point oder Router eine Verbindung zum DSL-Router herstellen können. Um diese Fehlerquelle auszuschließen, verbinden Sie das Ethernet-Kabel oder WLAN direkt mit dem DSL-Router.

Ist der Netzwerkadapter aktiv? Wenn außer „lo“ kein Netzwerkadapter und damit auch keine Konfiguration angezeigt wird, ist der Adapter vielleicht nur abgeschaltet. Bei Notebooks lassen sich Ethernet- und WLAN-Adapter meist über eine Tastenkombination deaktivieren (Flugmodus) und auch wieder aktivieren. Kontrollieren Sie auch im Firmwaresetup des Rechners, ob der Netzwerkadapter aktiviert ist.

PCs verfügen meist über Kontroll-LEDs, die den Status anzeigen. Bleiben diese trotz funktionstüchtigem Ethernet-Kabel dunkel, kann der Netzwerkadapter defekt sein.

Erreichbarkeit von Geräten testen

Der nächste Test prüft, ob ein Gerät im lokalen Netz auf Anfragen antwortet. Der Befehl

```
ping -c 5 192.168.178.1
```

unternimmt fünf Versuche, eine Fritzbox zu erreichen. Ersetzen Sie die IP-Adresse durch die Ihres Routers und probieren Sie auch andere Adressen im Netzwerk aus. Bei der Ausgabe „Destination Host Unreachable“ ist die Zieladresse nicht erreichbar, andernfalls erhalten Sie eine Antwort mit der benötigten Antwortzeit in Millisekunden. Ein positives Ergebnis sollte zumindest beim Router immer erscheinen, wenn „ip a“ zuvor eine korrekte Konfiguration ausgegeben hat. Einzelne Geräte können jedoch die Ping-Anfragen blockieren.

DNS-Server für das Web: Mit einer Befehlszeile wie

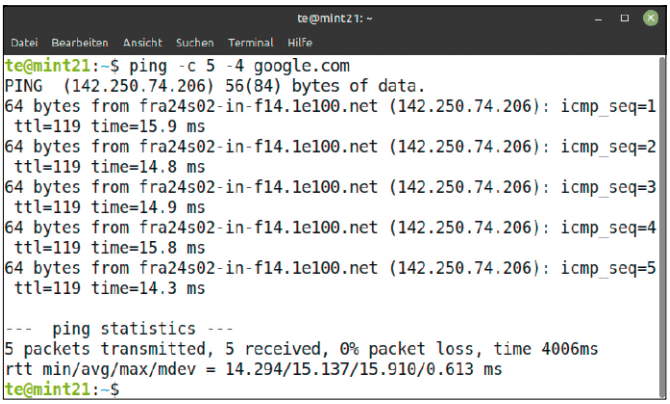
```
ping -c 5 -4 google.com
```

prüfen Sie die Namensauflösung über den DNS-Server. Der Rückgabewert enthält die IPv4-Adresse. Wenn nicht, ist der DNS-Server gerade nicht erreichbar oder falsch konfiguriert. Im Webbrowser lassen sich dann ebenfalls keine Seiten mehr über den Domainnamen aufrufen. Für einen Test der Namensauflösung für IPv6 ersetzen Sie „-4“ durch „-6“. Mit dem Befehl

```
resolvectl status
```

lässt sich prüfen, welcher DNS-Server konfiguriert ist. Wenn Sie selbst nichts anderes eingestellt haben (siehe nächster Punkt), erhält ein PC die Adresse des DNS-Servers per DHCP vom DSL-Router. Ist dieser nicht erreichbar, würde allerdings die Namensauflösung bei keinem Gerät im Netzwerk funktionieren.

Erreichbarkeit testen: Rechner im lokalen Netzwerk und im Internet liefern auf eine Ping-Anfrage eine Rückmeldung, wenn sie aktiv sind und die Netzwerkverbindung vorhanden ist.



Konfiguration prüfen: Die Übersichtsseite der Einstellungen zeigt die wichtigsten Werte an. Unter „IPv4“ und „IPv6“ sollte in der Regel alles auf „Automatisch“ stehen.

Fehlersuche über die grafische Oberfläche

Für das Netzwerk ist bei Linux meist der Netzwerkmanager zuständig. Ubuntu-Nutzer finden die Konfiguration in den „Einstellungen“ unter „Netzwerk“ oder „WLAN“, Nutzer von Linux Mint gehen im Menü auf „Einstellungen → Netzwerk“. Bei den genutzten Verbindungen muss der zugehörige Schalter aktiviert sein. Per Klick auf das Zahnradsymbol gelangt man unter beiden Systemen und bei jeder Verbindungsart zur Konfiguration. Auf der Übersichtsseite „Informationen“ (Linux Mint: „Details“) werden die wichtigsten Werte wie IPv4-Adresse, Vorgabestrecke (Gateway) und DNS-Server angezeigt. Für das WLAN werden Signalstärke und Verbindungsgeschwindigkeit angezeigt. Bei schlechten Werten reduzieren Sie den Abstand zum WLAN-Router oder finden einen besseren Standort für den Router.

Standardmäßig ist unter „IPv4“ alles auf „Automatisch“ eingestellt. Dadurch erhält der Rechner alle Werte automatisch vom DHCP-Server im Router. Das sollte auch so bleiben, außer man benötigt eine feste IP-Adresse für einen Server. Bei Auswahl der Option „Manuell“ kann man eine eigene IP-Adresse eintragen, die dann aber im Netzwerk nicht anderweitig vergeben sein darf und zum IP-Adressbereich des Routers passen muss.

Unter „IPv6“ gibt es die gleichen Optionen und auch hier sollte überall „Automatisch“ aktiviert sein. Für die Verbindung zu anderen Rechnern im lokalen Netzwerk spielt IPv6 keine Rolle. Beim Aufruf von Adressen im Internet kann aber IPv6 zum Einsatz kommen, wenn DSL-Router und Internetanbieter das unterstützen. Da bisher alle Server im Internet auch eine IPv4-Adresse besitzen, ist die Technik (noch) nicht zwingend erforderlich.

Firewall prüfen: Bei Ubuntu und Linux Mint ist die Firewallsoftware ufw („Uncomplicated Firewall“) installiert, aber standardmäßig nicht aktiviert. Wenn ufw eingeschaltet ist, blockiert die Firewall alle eingehenden Verbindungen, wodurch sich Serverdienste wie SSH nicht erreichen lassen. Bei Linux Mint ist das Konfigurationstool Gufw vorinstalliert („Einstellungen → Firewall-Konfiguration“). Ubuntu-Nutzer installieren es im Terminal so:

```
sudo apt install gufw
```

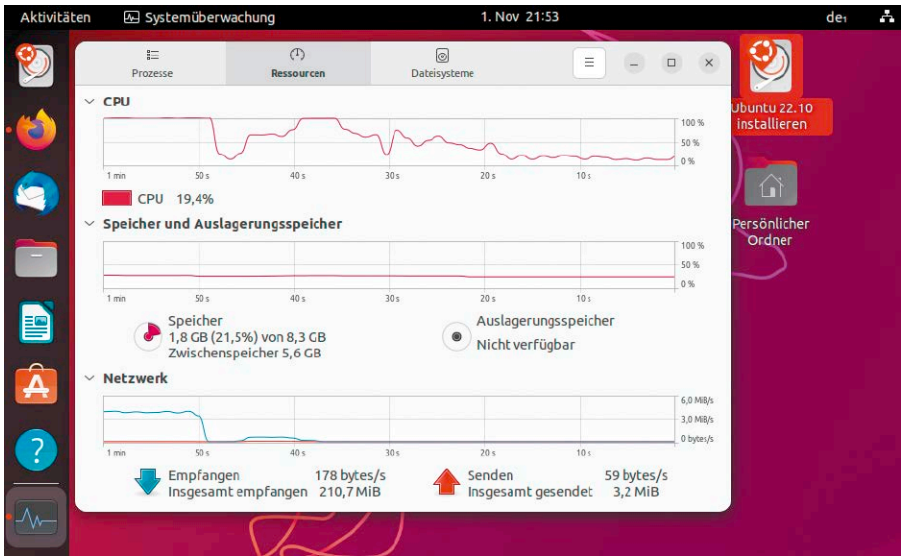
Sollte die Firewall aktiviert sein, stellen Sie den Schalter hinter „Status“ auf „Aus“ und prüfen die Netzwerkfunktionen. In der Regel kann die Firewall deaktiviert bleiben, außer Sie benötigen eine spezielle Konfiguration für einzelne Serverdienste im lokalen Netzwerk.

Durch die Firewall im DSL-Router sind direkte Zugriffe über das Internet auf den PC ohnehin blockiert. Wenn Sie gezielt Portfreigaben eingerichtet haben, müssen Sie eine zweite Firewall auf dem PC dafür ebenfalls konfigurieren – das erhöht die Sicherheit nicht und bedeutet nur unnötigen Konfigurationsaufwand. ■

Wenn der Desktop streikt

Probleme mit der grafischen Oberfläche werden meist durch eine defekte Konfiguration oder fehlerhafte Treiber verursacht. Analyse und Reparatur sind etwas aufwendig, aber nicht wirklich kompliziert.

VON THORSTEN EGGELING



Test im Livesystem: Das Ubuntu-Installationsmedium verwendet nur Standardtreiber. Wenn es über einen längeren Zeitraum stabil läuft, sind Hardwaredefekte unwahrscheinlich.

Die grafische Oberfläche von Linux-Systemen läuft nur einwandfrei, wenn alle Komponenten mitspielen. Auf der Hardwareseite ist der Treiber für den Grafikchip dafür zuständig, dass überhaupt etwas auf dem Bildschirm erscheint. Bei der Software steuert der Displayserver (Xorg oder Wayland) den Monitor an, der Windowmanager zeichnet die Programmfenster und Desktopumgebungen wie Gnome, Cinnamon oder KDE liefern wesentliche Bestandteile wie Menüs, Systemleisten und Fensterelemente. Alles muss zusammenpassen und für alles gibt es Konfigurationsdateien – Raum genug für ausreichend Fehlerquellen. In der Praxis läuft der Linux-Desktop dennoch meist sehr stabil. Wie sich einige grundsätzliche Probleme untersuchen und beheben lassen, ist Gegenstand dieses Artikels.

Desktopprobleme untersuchen

Wenn bei der Linux-Neuinstallation Grafikprobleme auftauchen, helfen meist Kernel-Optionen weiter (siehe ab Seite 24). Bei einem System, das bereits einige Zeit ohne Auffälligkeiten lief, gehören Hardwaredefekte oder defekte Konfigurationsdateien zum Kreis der Verdächtigen. Es kann beispielsweise sein, dass der Desktop gar nicht mehr erscheint, nach einiger Zeit komplett einfriert oder sich nur zögerlich mit der Maus bedienen lässt. Um den Fehler einzugrenzen, booten Sie den PC mit einem beliebigen Livesystem. Auf der Heft-DVD dieser LinuxWelt finden Sie etwa Ubuntu 22.10. Starten Sie den Webbrowser, arbeiten Sie mit Libre Office, spielen Sie Videos ab und lassen Sie das Livesystem eine Zeitlang laufen. Wenn der Desktop auch hier einfriert oder Fehler zeigt, kann die Hardware das Problem sein. Prüfen Sie die Lüfter, installieren Sie ein Firmwareupdate oder lassen Sie den Hersteller oder Verkäufer das Gerät testen.

Fehler nach der Anmeldung: Ein anderer Fehlertyp liegt vor, wenn die grafische Oberfläche mit dem Anmeldebildschirm erscheint, die Anmeldung jedoch nicht zur gewohnten Oberfläche führt. Man landet entweder wieder bei der Anmeldung, der Desktop ist leer oder nicht benutzbar. Bei derartigen Symptomen ist wahrscheinlich die Konfiguration defekt. Legen Sie testweise einen neuen Benutzer an, da dieser mit einer frischen Konfiguration startet. Treten hier keine Fehler auf, muss es an einer der Konfigurationsdateien liegen. Wenn Sie es vorziehen, verwenden Sie einfach das neue Benutzerkonto weiter und kopieren persönliche Dateien vom alten in das neue Home-Verzeichnis.

Benutzerprofil umbenennen: Wer sich genauer mit dem Problem beschäftigen möchte, geht einen anderen Weg. Beenden Sie alle Programme und wechseln Sie zu einer virtuellen Textkonsole. Bei Linux Mint 21 verwenden Sie die Tastenkombination Strg-Alt-F1, bei Ubuntu 20.04 oder 22.04 drücken Sie Strg-Alt-F3. Melden Sie sich in der Konsole an. Bei Linux Mint stoppen Sie dann den Displaymanager (Anmeldebildschirm) mit

```
sudo service lightdm stop
```

und Ubuntu-Nutzer verwenden dazu diesen Befehl:

```
sudo service gdm3 stop
```

Benennen Sie Ihr Home-Verzeichnis um, erstellen Sie ein neues Home-Verzeichnis

und setzen Sie die Zugriffsrechte:

```
sudo mv /home/[user] /home/[user].bak
sudo mkdir /home/[user]
sudo chown [user]:[user] /home/[user]
```

Den Platzhalter „[user]“ ersetzen Sie jeweils durch die Bezeichnung Ihres Benutzerkontos. Danach starten Sie den Displaymanager mit

```
sudo service lightdm start
```

oder so:

```
sudo service gdm3 start
```

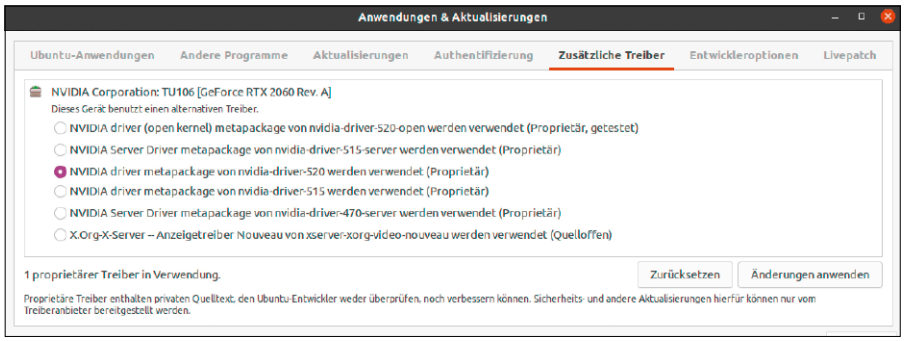
Melden Sie sich an und testen Sie die Funktionen des Systems. Wenn keine Probleme mehr auftauchen, liegt der Fehler in einer der Konfigurationsdateien. Damit beginnt der mühsame Teil der Analyse. Sie kopieren einzelne Ordner oder Unterordner nach und nach aus der Sicherungskopie („/home/[user].bak“) in das Home-Verzeichnis, melden sich ab und wieder an und warten auf mögliche Fehler. Beachten Sie, dass Konfigurationsverzeichnisse und -dateien mit einem Punkt beginnen und erst sichtbar werden, wenn Sie im Dateimanager die Tastenkombination Strg-H drücken.

Wenn der Fehler wieder auftritt, machen Sie die letzte Kopieraktion rückgängig. Danach kopieren oder verschieben Sie alle anderen Verzeichnisse und Dateien – außer den fehlerhaften – aus „/home/[user].bak“ nach „/home/[user]“.

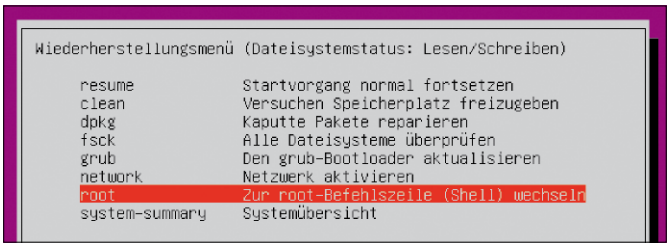
Probleme mit Treibern beheben

Nach der Installation verwenden Ubuntu und Linux Mint den Open-Source-Standardtreiber für den jeweiligen Grafikchip. Dessen Leistung ist für typische Desktopaufgaben ausreichend. Für anspruchsvollere Aufgaben installieren Sie optimierte Treiber für Grafikadapter von Nvidia oder AMD. Ubuntu-Nutzer suchen über „Aktivitäten“ nach „Treiber“ und klicken auf „Zusätzliche Treiber“. Bei Linux Mint führt der Weg über das Menü „Systemverwaltung → Treiberverwaltung“.

Treiberauswahl: Wenn ein Treiber verfügbar ist, werden meist mehrere Optionen angezeigt. Bisher galt die Regel, dass der Nvidia-Treiber mit der höchsten Versionsnummer und dem Zusatz „Proprietär, getestet“ die beste Wahl ist. Bei Treibern mit dem Zusatz „open kernel“ gilt das aber zur Zeit nicht. Unter *https://github.com/NVIDIA/open-gpu-kernel-modules* ist der Hinweis zu finden, dass bei Geforce-Modellen nur



Bessere Treiber? Die proprietären Treiber bieten zwar mehr Leistung, sind aber auch eine Fehlerquelle. Bei Problemen aktivieren Sie zumindest vorübergehend den Standardtreiber.



Notfallstart: Wenn die grafische Oberfläche nicht startet, booten Sie in das Wiederherstellungssystem. In der „root-Befehlszeile“ lassen sich defekte Treiber deinstallieren.

„Alpha-Qualität“ zu erwarten ist, der Treiber also mehr als unfertig ist. Im Moment ist daher ein Treiber ohne den Zusatz „open kernel“ zu empfehlen.

Zurück zum Standardtreiber

Bei Problemen mit dem proprietären Treiber stellen Sie den Standard „X.Org-X-Server“ wieder her. Sollte das über „Zusätzliche Treiber“ nicht möglich sein, weil der Desktop schwarz bliebt, starten Sie das System im Recoverymodus. Wenn bei Ihrer Installation das Grub-Bootmenü nicht automatisch erscheint, halten Sie bei Start des PCs die Umschalt-Taste gedrückt. Im Bootmenü gehen Sie dann auf den Eintrag mit dem Zusatz „Advanced options“ und danach auf den ersten Eintrag, der „(recovery mode)“ enthält. Im Menü wählen Sie „network“ und bestätigen mit „Ja“. Danach wählen Sie „root“ und drücken die Eingabetaste. Entfernen Sie den proprietären Nvidia-Treiber

```
sudo apt purge nvidia*
```

oder den AMD/ATI-Treiber:

```
sudo apt purge fglrx*
```

Fehlt der proprietäre Treiber, verwendet Linux wieder den Standardtreiber. Mit *reboot* verlassen Sie das Rettungssystem und starten Linux neu.

Die grafische Oberfläche sollte jetzt wieder nutzbar sein. ■

ZUSATZOPTIONEN FÜR NVIDIA-TREIBER

Bei der Installation neuer Nvidia-Treiber auf einem Desktopsystem vermeiden Sie besser Treiber mit dem Zusatz „Server“. Diesem Paket fehlen einige Tools für Desktopnutzer, beispielsweise nvidia-settings. Damit kann man sich Infos zum Grafikchip anzeigen lassen und auf Notebooks unter „PRIME profiles“ Stromsparfunktionen aktivieren: Standard ist „NVIDIA On-Demand“, womit der Nvidia-Chip nur bei Bedarf aktiviert wird. „NVIDIA (Performance Mode)“ schaltet den Chip dauerhaft ein, was den Akku schnell leert. „Intel (Power Saving Mode)“ belastet den Akku am wenigsten. Bei einigen Treiberversionen ist diese Option aber ausgegraut und daher nicht wählbar. Verwenden Sie dann im Terminal diesen Befehl:

```
sudo prime-select intel
```

Mit der Zeile

```
sudo prime-select on-demand
```

aktivieren Sie wieder den Standardmodus.

Dateisysteme unter Linux

Bei Dateisystemen gibt es keinen Stillstand. Im Hinblick auf ihre immense Verantwortung geschehen aber alle Fortschritte zäh, konservativ und abseits der öffentlichen Wahrnehmung. Ubuntus aktuelle Parteinahme für ZFS sorgt für frische Diskussion.

VON HERMANN APFELBÖCK

Seit vielen Jahren gilt das Dateisystem Ext4 als Standard auf dem Linux-Desktop, zumeist auch auf Servern. Eindeutige Plädoyers für andere Dateisysteme wie etwa beim NAS-System Freenas für ZFS blieben lange Zeit rar – am Desktop sowieso. Jetzt tut sich aber einiges: 2017 schlug sich Open Suse Leap auf die Seite von BTRFS, ebenso und ganz aktuell Fedora 33. Viel diskutiert ist Ubuntus ZFS-Option für die Installation am Desktop. Wir nehmen dies zum Anlass für einen Heftschwerpunkt zum Thema „Dateisysteme". Dieser erste Beitrag soll die Bedeutung und Funktionsweise von Dateisystemen skizzieren, die wichtigsten kurz charakterisieren und die erweiterten Fähigkeiten von Dateisystemen diskutieren. Dies führt dann zwanglos zu Fragen, für welche Szenarien sich welche Dateisysteme am besten eignen und ob der Linux-Desktop tatsächlich eine Abkehr vom bisherigen Ext4-Standard benötigt. Die nachfolgenden vier Artikel führen dann in den praktischen PC-Alltag und zeigen Basiskonfiguration und Tuningtipps für die Linux-Dateisysteme Ext4, ZFS, BTRFS und für Windows-Alternativen für den Datenaustausch.

1. Dateisysteme: Die sichtbare Spitze

Am Linux-Desktop zeigen sich Dateisysteme nur an zwei Stellen deutlich: bei der (manuellen) Installation und in der Laufwerksverwaltung. Die Installation bietet die Formatierung mit Ext2/3/4, XFS, JFS, BTRFS, eventuell ZFS, die Laufwerksverwaltung hat in der Regel zusätzlich NTFS und FAT32, exFAT im Angebot. Inaktive (ausgegraute) Linux-Dateisysteme lassen sich durch Nachinstallationen passender Pakete aktivieren.

Die Aktion, ein Laufwerk oder einen Teil dessen (Partition) mit einem Dateisystem zu versehen, nennt sich bekanntlich „Formatieren". Optionales Partitionieren (Aufteilen) eines Laufwerks ist einer Formatierung vorgeschaltet. Dort und in der daraus resultierenden Partitionstabelle geht es darum, ein Laufwerk aus organisatorischen Gründen in mehrere Bereiche aufzuteilen (Partitionen). Sobald eine Partition anschließend durch ein Dateisystem formatiert wird, erhält die Partition in der Partitionstabelle eine knappe Kennziffer, um welches Dateisystem es sich handelt.

Die sichtbare Spitze des Eisbergs „Dateisystem" wird wesentlich größer, sobald die zugehörigen Terminaltools zum Einsatz kommen. Erst diese zeigen die Komplexität und die Tatsache, dass ein Formatieren mit grafischen Werkzeugen für zahlreiche Parameter einfach bewährte Kompromisswerte setzt. Ein besonders wichtiger Parameter ist die Block- oder Clustergröße, die standardmäßig 512 Bytes, heute meist vier KB beträgt.

Wichtig und sichtbar für den Anwender sind ferner Standardverzeichnisse eines Dateisystems. Diese sind allerdings bloße Namen, Konvention und Tradition und vom eigentlichen Handwerk des Dateisystems Lichtjahre entfernt.

2. Dateisystem-Pflicht: Die Übersetzungsleistung

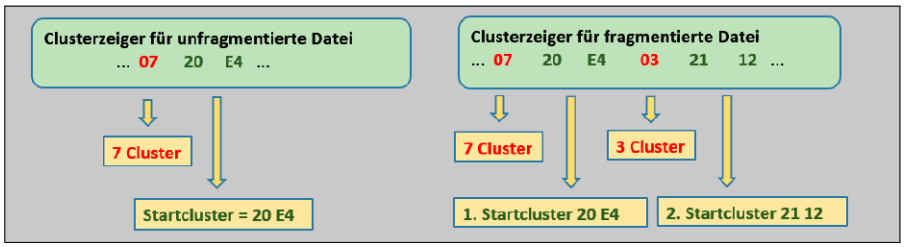
Dateisysteme kennen Pflicht und Kür (dazu später). Unabdingbare Pflicht für jedes Dateisystem ist es, angeforderte Dateien zu finden und bereitzustellen. Die Tatsache, dass sich Dateien über hierarchische Pfade, über Namen, Extensionen oder Datumsangaben aufrufen oder filtern lassen, erfordert erheblichen Verwaltungsaufwand. Der Controller der Hardware (Festplatte, SSD) kann jede Einheit (Sektor, Block) in Milli- oder Mikrosekunden ansteuern. Aber er braucht die exakte Kennziffer der gewünschten Einheit: Ordner und Dateinamen sind ihm so fremd wie der Dateibegriff

insgesamt. Wenn ein Laufwerk die Bits aus etlichen angeforderten Blöcken ausliefert, weiß es weder, dass es sich um eine zusammengehörige Datei handelt, noch weniger, dass diese sich in einem bestimmten Ordner befindet und einen Namen besitzt. Nebenbei: Auch die Einteilung in Partitionen ist der Hardware unbekannt. Das ist alles Aufgabe des Dateisystems.

Das Dateisystem errichtet ab Formatierung eine Dateitabelle. Jede Datei erhält dort einen Eintrag mit Metadaten wie Dateiname, Erstelldatum, Rechtemaske. Format und Umfang dieser Einträge bestimmen die maximalen Datei- und Pfadnamen, maximale Dateigrößen und die Tauglichkeit für Multiuser-Systeme mit Rechteverwaltung. Entscheidend zum Auffinden der Dateiinhalte ist der Verweis auf die Zuordnungseinheiten – Cluster oder Blöcke (Cluster ist der klarere Begriff für eine Dateisystemeinheit, weil „Block" auch hardwaretechnisch die kleinste Datenträgereinheit meint). Um die Übersetzungsarbeit für die Hardware zu vereinfachen, entsprechen diese Cluster genau oder als einfaches Vielfaches der Block- oder Sektorgröße des Datenträgers – oft vier KB, sofern der Nutzer bei der Formatierung keine andere Wahl trifft. Als Clusterzeiger in der Dateitabelle dient dann eine schlichte Ziffer für den Startcluster der Datei, ferner eine weitere Ziffer für die Anzahl der Folgecluster (da eine Datei in der Regel mehrere oder viele Cluster beansprucht).

Nehmen wir an, Sie klicken im Dateimanager auf eine Datei „Rechnung_034-2020.odt". Woher weiß das Dateisystem, dass es den Inhalt dieser Datei etwa aus den Clustern 12 057, 12 058 und 12 116 zu laden hat? Und woher weiß das System, welche Dateinamen es anzeigen soll, wenn Sie im Home-Verzeichnis auf „Dokumente" klicken? Anhand der kompletten Pfadangabe beginnt die Suche immer auf der obersten Ebene der Dateitabelle. Dort findet sich der Eintrag für den ersten Ordnernamen der Pfadangabe, in dessen Inhalt geht die Suche dann weiter zum nächsten Unterordner gemäß Pfadangabe bis hinunter zur gesuchten Datei.

Noch sind wir beim Eintrag der Datei in der Dateitabelle – nicht bei der Datei selbst: Wo diese liegt, zeigen nun aber die Clusterverweise. Startcluster und Anzahl der Cluster können nun an die Hardware weitergegeben werden. Wenn die Datei unfragmentiert ist, also der komplette Inhalt in einer zusammenhängenden Clusterfolge abgelegt ist, genügt es, den Startcluster anzuspringen und ab dort die angegebene Anzahl von Cluster einzulesen. Bei fragmentierten Dateien folgt in der Dateitabelle ein weiterer Eintrag mit dem nächsten Startcluster und der Clusteranzahl.



Teil eines Eintrags in der Dateisystemtabelle (schematisch): Das System muss Dateiinhalte aus Clustern einsammeln. Die Dateitabelle nennt nur die Anzahl der Cluster und die Kennziffer des Startclusters.

3. Dateisystem-Kür: Erweiterte Eigenschaften

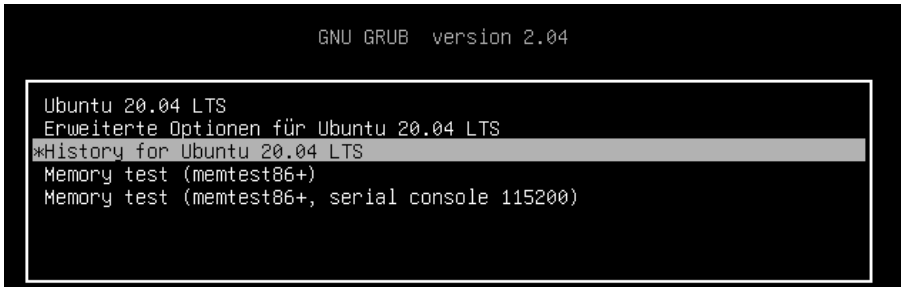
Die angesprochene Kernaufgabe erledigt jedes Dateisystem. Die Limits für Pfadlänge, Dateigröße und Datenträgergröße sind zum Teil pragmatisch (Pfadlänge bei NTFS, Größen bei F2FS oder Ext2/3), ohne aber bei Desktopsystemen an ernsthafte praktische Grenzen zu stoßen. Lediglich das alte FAT32 hat mit einer maximalen Dateigröße von nur vier GB ein Limit, das in den PC-Alltag hineinwirkt.

Was Dateisysteme neben der Pflicht der Dateibereitstellung zusätzlich leisten sollen, wird durchaus kontrovers interpretiert. Die einzelnen Eigenschaften (siehe Tabelle) lassen sich in folgende Hauptaspekte gliedern:

1. Optimierte Leistung: Während einfache Dateisysteme Schreibaktionen sofort und undifferenziert einfach in die nächstmöglichen freien Cluster schreiben, gibt es eine Reihe von intelligenteren Methoden, um erstens die Zugriffe zu beschleunigen und zweitens die Fragmentierung zusammenhängender Dateien zu verringern. **Allocate-on-Flush** verzögert den Schreibvorgang, um den kompletten Platzbedarf einer Datei abzuwarten und dann zusammenhängend zu speichern (unfragmentiert). **Extents** verschlanken die Dateisystemtabelle, indem sie bei vermehrten Metadaten selbige in normale Datencluster auslagern. Permanentes Dateisystem-**Caching** verwendet nur ZFS mit entsprechenden RAM-Ansprüchen.

Sparse-Dateien sind eine intelligente Antwort auf Dateien ohne Inhalt: Das Dateisystem erkennt die „Leere" und belegt keine Cluster, selbst wenn die Metadaten eine formale Dateigrößen im MB- oder GB-Bereich definieren. **Trim-Support** ist eine Spezialität für SSDs, um die Hardware über gelöschte und somit freigewordene Blöcke zu informieren. Eine eher marginale Eigenschaft ist **Execute-in-Place**, das Programmausführung direkt vom Datenträger erlaubt (ohne Kopie in den Arbeitsspeicher), aber nur für sehr speziellen Programmecode in Betracht kommt.

2. Optimierte Sicherheit: Das verbreitete **Journaling** ist sowohl eine Sicherheitsfunktion als auch eine Leistungsoptimierung: Das Journal protokolliert entweder nur die Metadaten in der Dateitabelle oder sämtliche Änderungen an Dateiinhalten (Full Journaling). Nach Absturz, Hard Reset oder Stromausfall muss das Dateisystem dann nicht komplett geprüft werden, sondern sieht im Journal alle Dateiänderungen, die



Dateisystemfunktionen treten selten wie hier ins sichtbare Licht: ZFS-Snapshots erscheinen neuerdings als „History" im Grub-Menü von Ubuntu (falls ZFS als Dateisystem arbeitet).

nicht ordentlich abgeschlossen wurden. Einige wenige Dateisysteme führen obendrein gesonderte **Change-Logs** und schreiben **Checksummen** in die Metadaten. **Copy-on-Write (CoW)** bedeutet, dass geänderte Blöcke nicht an Ort und Stelle überschrieben, sondern zunächst in freie Cluster kopiert werden. Die dadurch entstehende Redundanz ist Voraussetzung für **Snapshot**-Sicherung (nur BTRFS und ZFS).

3. Erweiterte Metadaten: Alle elaborierteren Dateisysteme notieren als Metadaten deutlich mehr als die unbedingt erforderlichen Pfade, Namen und Clusterverweise. Besitz, Dateirechte, mehrere Zeitstempel und Streams als formal unstrukturierte Metadaten sind fast überall Standard. Streams eignen sich als interne Infos für Software, aber auch als Kommentarfunktion.

4. Erweiterte Funktionen: Besondere Attraktivität für Anwender haben native Zusatzfunktionen des Dateisystems wie **Verschlüsselung** und **Kompression**. Hier kann das ansonsten pragmatische NTFS gegenüber den Linux-Standards klar punkten. **Snapshots** zur Systemsicherung bieten andererseits nur die Linux-Dateisysteme BTRFS und ZFS. Diese gehen aber noch einen ganzen Schritt weiter, indem sie einen eigenen **Volume-Manager** zur Laufwerksverwaltung integrieren. Funktional bedeutet das, dass Größenänderungen des Dateisystems online wie offline und mit Anschluss zusätzlicher Laufwerke möglich sind.

4. Dateisysteme und ihre Performance

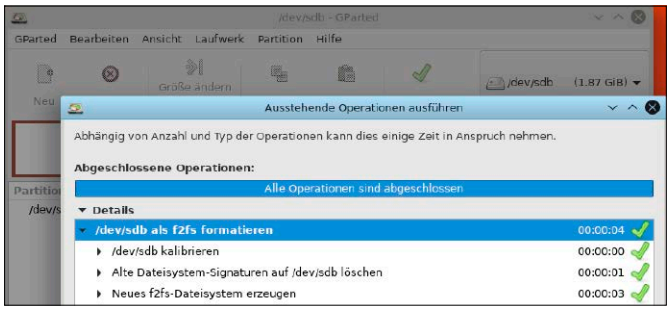
Zur Leistung von Dateisystemen gibt es zahlreiche Messungen, die sich aber nicht gegenseitig bestätigen. Zuverlässiges Testen der Dateisystemleistung ist heikel, weil sehr viele Faktoren mitspielen. Die Größe der Dateien ist relevant, weil Dateisysteme ihre jeweiligen Vorzüge besitzen. Noch wichtiger ist die Clustergröße, denn jedes Dateisystem ist umso schneller, je weniger Einzelblöcke es zusammensuchen muss. Ein gerechter Vergleich müsste überall dieselbe Clustergröße verwenden – soweit dies einstellbar ist. Dies wiederum kann zu Ungerechtigkeiten führen, wenn Dateisysteme intern auf ihre Standardgrößen hin optimiert sind. Für einen gerechten Vergleich müssten ferner alle Daten unfragmentiert vorliegen. Spezielle Funktionen wie Kompression müsste man von vornherein ausschalten, eventuell auch das Aufzeichnen von speziellen Metadaten – soweit dies überhaupt vorgesehen ist.

Angesichts dieser Situation ist ein objektiver Vergleichstest eine akademische Herausforderung, die wir an dieser Stelle radikal und vereinfachend abkürzen: Generell darf man von einfachen Dateisystemen wie Ext2 oder FAT32, die sich weder mit Journaling, Fehlerprüfung noch mit luxuriösen Metadaten abgeben müssen, höheren Durchsatz erwarten. Gerade auf nicht sys-

DIE WICHTIGSTEN DATEISYSTEME

	Ext4	Ext3	Ext2	BTRFS	ZFS	XFS	JFS	F2FS
Dateinamenlänge	255	255	255	255	255	255	255	255
Pfadnamenlänge	kein Limit	kein Limit	kein Limit	kein Limit	kein Limit	kein Limit	kein Limit	kein Limit
Dateigröße	16 TB	2 TB	2 TB	16 EB	16 EB	8 EB	4 PB	ca. 4 TB
Dateisystemgröße	1 EB	32 TB	32 TB	16 EB	2^128	8 EB	32 PB	16 TB
Anzahl Dateien	2^32	k. A.	k. A.	2^64	2^128	k. A.	kein Limit	2^63
Dateibesitz	ja	ja	ja	ja	ja	ja	ja	ja
Dateirechte	ja	ja	ja	ja	ja	ja	ja	ja
Zeitstempel	3	2	2	3	4	2	3	3
Streams	ja	ja	ja	ja	ja	ja	ja	ja
Checksumme	teilweise	nein	nein	ja	ja	z. T.	nein	nein
Hardlinks	ja	ja	ja	ja	ja	ja	ja	ja
Softlinks	ja	ja	ja	ja	ja	ja	ja	ja
Journaling (Full)	ja	ja	nein	nein	ja	ja	nein	ja
Journaling (Metadaten)	ja	ja	nein	nein	nein	ja	ja	nein
Änderungslogs	nein	nein	nein	k.A.	nein	ja	nein	nein
Execute in place	ja	ja	ja	k.A.	nein	k. A.	k. A.	nein
Copy-on-Write	nein	nein	nein	ja	ja	z. T.	k. A.	ja
Snapshots	nein	nein	nein	ja	ja	nein	nein	nein
Verschlüsselung	experimentell	nein	nein	nein	ja	nein	nein	experimentell
Komprimierung	nein	nein	nein	ja	ja	experimentell	nein	ja
Quota (Kontingente)	ja	ja	ja	ja	ja	ja	ja	ja
Permanenter Cache	nein	nein	nein	nein	ja	nein	nein	nein
LVM, Raid	nein	nein	nein	ja	ja	nein	nein	nein
Vergrößern/Verkleinern	ja	ja	nur offline	ja	nur online	nur Vergrößern	nur online	Offline-Vergrößern
Geräteanschluss	nein	nein	nein	ja	ja	ja	nein	nein
Sparse-Dateien	ja	ja	ja	ja	ja	ja	ja	ja
Extents	ja	nein	nein	ja	nein	ja	ja	z. T.
Allocate-on-Flush	ja	nein	nein	ja	ja	ja	nein	ja
Trimsupport	ja	ja	ja	ja	nur FreeBSD	ja	ja	ja

temrelevanten Laufwerken mit Benutzerdaten ist älteres Ext2 oft die beste und schnellste Alternative, exFAT auch nicht immer verkehrt. F2FS bietet sich für USB-Sticks an. Elaborierte Dateisysteme können den zusätzlichen Verwaltungsaufwand durch optimierte Schreibverfahren und präventive Maßnahmen gegen die Fragmentierung nur teilweise kompensieren.



Nachgerüstete Spezialdateisysteme: Wenn die meist kleinen Pakete für Dateisysteme nachinstalliert sind (hier „f2fs-tools"), sind sie auch in grafischen Werkzeugen wie Gparted aktiv.

5. Relevante Dateisysteme

Wie viele Dateisysteme braucht Linux? Die Betriebssystemkonkurrenz leistet sich längst nicht den Luxus so zahlreicher Entwicklungen. Der langjährige Windows-Standard **NTFS** ist bislang ausreichend und hat Komfortfunktionen an Bord, Ähnliches gilt für **APFS** unter Mac-OS sowie das einfachere **HFS+**. Für wachsende Serveransprüche arbeitet Microsoft an **ReFS**, das zwar astronomische Kapazitäten verwaltet, aber noch viele unter NTFS selbstverständliche Attribute vermissen lässt. Für das einfache Austauschformat **FAT32** hat Microsoft beizeiten den Nachfolger **exFAT** nachgelegt, um drängende Größenlimits zu überwinden.

Unter Linux tummeln sich zahlreiche prominente, exotische und spezialisierte Dateisysteme. Die Übersichtstabelle beschränkt sich auf jene, die am Linux-Desktop sichtbar in Erscheinung treten (etwa in der Laufwerksverwaltung). Da Ext4, BTRFS und ZFS nachfolgend eigene Beiträge erhalten, beschränken wir uns an dieser Stelle auf eine Kurzcharakteristik der verbleibenden Dateisysteme Ext3, Ext2, JFS, XFS und F2FS:

Ext3 und Ext2: Der wichtigste Unterschied dieser Ext-Versionen ist das mit Ext3 eingeführte Journal. Wo diese Sicherheitsfunktion keine Rolle spielt, ist Ext2 die einfachere und schlankere Wahl. Anders ausgedrückt: Wenn Journaling-Sicherheit gefragt ist (Systempartition), nimmt man besser gleich Ext4, wo nicht, genügt auch Ext2.

XFS: Das Journaling-Dateisystem wurde ursprünglich für Serveraufgaben geschaffen. Die ehemals gelobten Geschwindigkeitsvorteile beim Umgang mit sehr großen Dateien und beim Mehrfachzugriff auf Daten dürften mittlerweile weitgehend egalisiert sein. Ein spürbarer Unterschied zu Ext4 besteht heute nicht mehr. Messbar mag XFS aber immer noch vorne liegen, da etwa Open Suse die Home-Partition standardmäßig mit XFS formatiert.

JFS: Das „Journaling File System" ist so alt (1990 von IBM), dass es die damals noch revolutionäre Journal-Funktion zur Namensgebung verwendete. JFS ist heute eigentlich JFS2 und hat keine herausragenden Eigenschaften, aber auch keine nennenswerten Schwächen.

F2FS: Das „Flash-Friendly File System" von Samsung ist ein Spezialist für Flashspeicher – also für SD-Karten, SSDs und eMMC. Die begrenzte Lebensdauer von rund 10 000 Schreibzugriffen pro Speicherzelle legt es dort nahe, die Dateiinhalte turnusmäßig so umzuverteilen, dass alle Bereiche des Datenträgers in etwa gleichmäßig beansprucht werden. Für solches „Wear-Leveling" sorgt die Hardware im Prinzip selbständig. F2FS entlastet diese Aufgabe aber dadurch, dass es die Daten für Schreibvorgänge strukturiert und zwischen Daten mit tendenziell kurzer (Benutzerdaten) und langer Lebensdauer (Dateitabelle, Betriebssystem) unterscheidet. F2FS ist in der Regel nicht vorinstalliert, kann aber mit dem Paket „f2fs-tools" leicht nachgerüstet werden. ■

	NTFS	FAT32	exFAT	HFS+	APFS
	255	255	255	255	255
	255	255	255	kein Limit	kein Limit
	16 EB	4 GB	16 EB	ca. 8 EB	8 EB
	16 EB	16 TB	64 ZB	ca. 8 EB	k. A.
	2^32	k. A.	k. A.	2^32	2^63
	ja	nein	nein	ja	ja
	ja	nein	nein	ja	ja
	3	2	2	4	4
	ja	nein	nein	ja	ja
	nein	nein	nein	nein	z. T.
	ja	nein	nein	ja	ja
	ja	nein	nein	ja	ja
	nein	nein	nein	nein	k. A.
	ja	z. T.	z. T.	ja	k. A.
	ja	nein	nein	ja	k. A.
	nein	nein	nein	k. A.	k. A.
	k. A.	nein	nein	k. A.	ja
	nein	nein	nein	nein	ja
	ja	nein	nein	optional	ja
	ja	nein	nein	ja	ja
	ja	nein	nein	ja	ja
	nein	nein	nein	nein	nein
	nein	nein	nein	nein	nein
	ja	nur offline	nein	nein	k. A.
	nein	nein	nein	nein	k. A.
	ja	nein	nein	nein	ja
	ja	nein	z. T.	ja	ja
	nein	nein	nein	ja	ja
	ja	ja	ja	ja	ja

Die Tabelle zeigt die wichtigsten Dateisysteme für Linux, Windows und Mac-OS. Es handelt sich um Auswahl und Extrakt (inklusive Korrekturen) der Tabellensammlung von *http://en.wikipedia.org/wiki/Comparison_of_file_systems*.

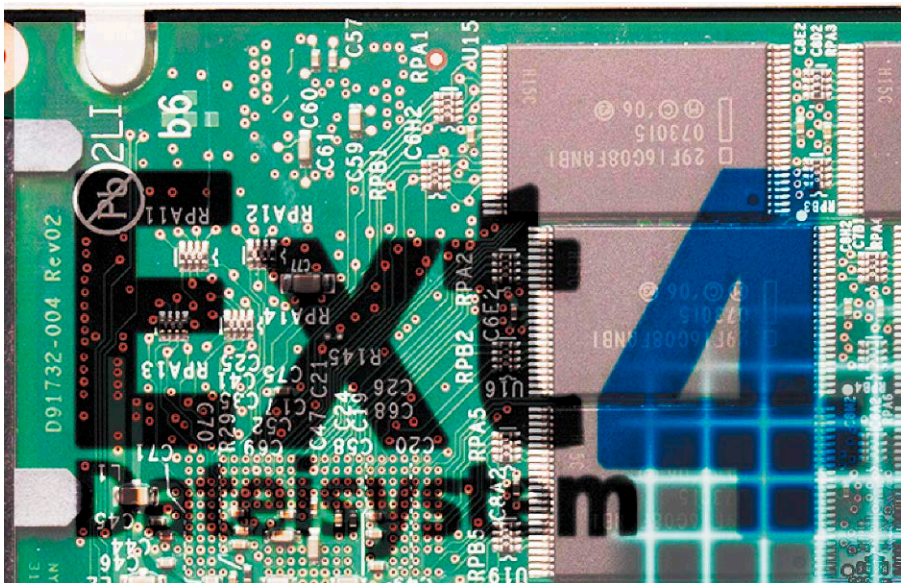
Die Größenangaben GB, TB, PB, EB sind wie folgt aufzulösen:
1 GB (Gigabyte) = 1024 MB (Megabyte)
1 TB (Terabyte) = 1024 GB
1 PB (Petabyte) = 1024 TB
1 EB (Exabyte) = 1024 PB

Eine „Legende" zu den allermeisten Eigenschaften (linke Spalte) liefert Punkt 3 des Haupttextes.

Der Linux-Standard Ext4

Das robuste Ext4 ist in den meisten Linux-Distributionen der Standard bei der Installation und bei der Formatierung externer Laufwerke. Die Voreinstellungen garantieren Datensicherheit, Ext4-Tools ermöglichen optionales Tuning und Dateiverschlüsselung.

VON HERMANN APFELBÖCK



Die Entwicklung von Ext („Extended Filesystem“) reicht über die Vorgänger 3 und 2 letztlich zurück bis ins Jahr 1993. Änderungen bei Ext folgten ganz konservativ den gewachsenen Standardanforderungen (etwa Journaling-Sicherheit) oder technischen Notwendigkeiten (etwa Kapazitätslimits), experimentelle Extras standen offenbar nie zur Diskussion.

Version Ext4 hat mit seinen aktuellen Spezifikationen keine drohenden Limits hinsichtlich Gerätegrößen, Dateigrößen oder mangelnder Metadaten. Es darf seit mehr als zehn Jahren als Quasistandard auf allen Desktop- und Serverdistributionen gelten, wo ein grundsolides Dateisystem gewünscht ist – genau das: nicht weniger, nicht mehr.

Integration und Werkzeuge

Die kleine Ewigkeit als Linux-Standard hatte wenige Konsequenzen am grafischen Desktop. Zwar ist eine händische Formatierung mittels

```
sudo mkfs.ext4 […]
```

nur in Sonderfällen nötig, weil Installer und Laufwerksverwaltungen Ext4 integrieren. Nennenswert darüber hinaus geht die Desktopintegration aber nicht. Auch für Ext4 sind Interna nur über Terminalwerkzeuge zu erledigen. Alle Ext4-Tools sind im Standardpaket „e2fsprogs“ enthalten und mit dem Kommando

```
dpkg -L e2fsprogs
```

leicht zu ermitteln. Neben den fundamentalen Programmen mke2fs oder gleichbedeutend mkfs.ext4 (Formatieren) und e2fsck oder gleichbedeutend fsck.ext4 (Integritäts-Check) gibt es eine ganze Reihe weiterer Werkzeuge: badblocks, debugfs, dumpe2fs, e2image, e2scrub, e2undo sind allesamt forensische Tools, die im Alltag keine große Rolle spielen und typische PC-Anwender überfordern dürften. e2freefrag, e4defrag, filefrag liefern Infos zur Fragmentierung oder leisten aktive Defragmentierung (e4defrag). E4defrag kann mit Schalter „-v“ auf Einzeldateien, Verzeichnisse und Partitionen angewandt werden.

Resize2fs ist das Low-Level-Tool für Größenänderungen von Partitionen. In der Regel wird man hierfür am Desktop bevorzugt zum grafischen Gparted greifen. Für die beiden verbleibenden und interessantesten Ext-Tools – tune2fs und e4crypt – folgen konkrete Einsatzbeispiele.

Laufwerksoptionen mit tune2fs steuern

Das Werkzeug tune2fs steuert viele Dateisystemeigenschaften wie die zu schreibenden Metadaten, die Absicherung durch das Journaling oder die Häufigkeit von Integritäts-Checks. Selbst auf der Systempartition sind nicht immer Standards erforderlich, auf externen Datenträgern noch weniger. Klar ist dennoch: Folgende Eingriffe verringern die Robustheit des Dateisystems und bleiben eine Ermessensfrage.

Ext4-Journaling abschalten: Auf externen Laufwerken mit (oft nur redundanten) Benutzerdaten ist die Absicherung durch das Journalprotokoll selten notwendig. Ohne Journaling entfallen viele Schreibaktionen, was den Datendurchsatz beschleunigt. Oft wäre dort die Wahl des journalfreien Vor-

gängers Ext2 von vornherein die bessere Wahl, aber auch auf Ext4 lässt sich Journaling deaktivieren (hier für „sde1“):

```
sudo umount /dev/sde1
sudo tune2fs -O ^has_journal /dev/
  sde1
```

„tune2fs -O“ (Buchstabe „O“) entfernt Dateisystemattribute mit „^“, während „+“ solche hinzufügen kann. Die aktuellen Eigenschaften ermitteln Sie so:

```
sudo tune2fs -l /dev/sde1
```

Die Ausgabe wird nach obiger Aktion neben „Filesystem features“ das Attribut „has_journal“ nicht mehr anzeigen.

Ext4-Checks reduzieren: Folgender tune2fs-Befehl

```
sudo tune2fs -i60 -c100 /dev/sda
```

reduziert die Datenträger-Checks: Die langwierige Prozedur wird dann nur noch alle 60 Tage („-i60“) oder nach hundert Neustarts („-c100“) erfolgen – je nachdem, welches Ereignis früher erfüllt ist.

Reservierten root-Speicher reduzieren: Ext4 reserviert auf jeder Partition Speicherplatz für das root-Konto. Falls ein System durch eine vollgeschriebene Systempartition lahmgelegt wird, kann sich noch root anmelden. Der reservierte Platz beträgt immerhin fünf Prozent der Gesamtkapazität und lässt sich gefahrlos verringern:

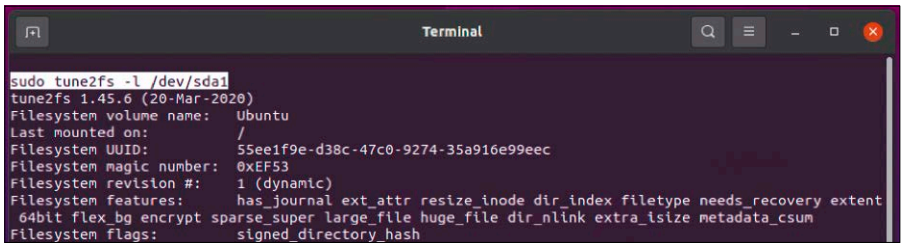
```
sudo tune2fs -m 1 /dev/sda1
```

Dies reduziert die Anzahl der root-Reserve auf Partition „/dev/sda1“ auf ein Prozent. Ganz ausschalten („-m 0“) sollten Sie die Reserve aber nicht.

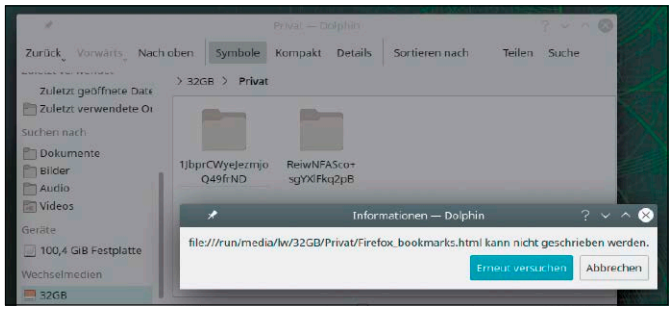
Ext4-Metadaten reduzieren: Ext4-formatierte Partitionen speichern bei jeder Datei mehrere Zeitangaben. Erstelldatum und Änderungsdatum werden immer eingetragen („ctime“ und „mtime“: Creation und Modification). Optional ist hingegen das Erfassen des letzten Dateizugriffs („atime“: Access). Diese Information ist nur dann relevant, wenn Sie mit „find -atime“ nach Zugriffszeiten von Dateiobjekten suchen. Wenn Sie das nie tun, kann die Festplattenaktivität reduziert werden. Hier hilft ausnahmsweise nicht tune2fs, sondern nur ein Eingriff in die Datei „/etc/fstab“:

```
UUID=[…]  /  ext4  noatime  0  2
```

Wenn in der Optionen-Spalte bereits Einträge stehen, setzen Sie „,noatime“ an deren Ende (mit Trennkomma). Der Vollständigkeit halber: Es gibt auch noch die Option „nodiratime“, die bei Verzeichnissen darauf verzichtet, die Zugriffszeit zu vermerken. Wenn Sie die Aktivität der Festplatte reduzieren möchten, ist „noatime“ die weitreichendere Maßnahme.



Eigenschaften eines Ext4-Dateisystems: „tune2fs -l“ zeigt alle statischen und dynamischen Attribute einer Ext4-Partition. Die „Filesystem features“ sind konfigurierbar.



Verschlüsselter Ordner auf USB-Stick: Ohne Passwort kann ein fremdes System den Ordner nicht benutzen. Auch die Dateinamen sind codiert. Andere Ordner des Datenträgers bleiben zugänglich.

Verschlüsselung mit Ext4

Ext4 hat durch Google transparente Verschlüsselung erhalten, die Google im Hinblick auf Android-Geräte entwickelt hat. Die Leistung der Ext4-Verschlüsselung ist mit Cryptsetup/Luks vergleichbar oder sogar besser, außerdem fordert Ext4-Verschlüsselung keine Neuformatierung. Trotzdem muss man diese Option unter Linux noch deutlich kritisch beurteilen – nach dem Motto: Es funktioniert im Prinzip. Die nachfolgend beschriebene Aktion beschränkt sich auf das einfache, aber realistische Szenario, dass das Verzeichnis eines USB-Datenträgers nur auf genau einem PC gelesen werden darf.

Da eine engere Desktop- oder Dateimanager-Integration fehlt, müssen im Terminal die beiden Tools tune2fs und e4crypt zusammenarbeiten. Folgendes Kommando

```
sudo tune2fs -O +encrypt /dev/sdc1
```

aktiviert zunächst die Verschlüsselung für Partition „/dev/sdc1“ (auf bereits vorhandene Daten hat diese Aktion keine Auswirkung). Danach benötigt die Verschlüsselung einen Ext4-Schlüssel:

```
e4crypt add_key
```

Das Passwort wird nur einmal abgefragt und hat keine Komplexitätsanforderungen. Dieser Schlüssel wird im Schlüsselbund des gerade angemeldeten Benutzers gespeichert. Der Befehl

```
keyctl show
```

gibt Einblick in den Schlüsselbund (eventuell muss dafür das kleine Paket „keyutils“ nachinstalliert werden) und zeigt den neuen Ext4-Schlüssel als „logon: ext4:…“. Die nach „ext4:“ folgende Hexadezimal-ID brauchen Sie zur Verschlüsselung des Verzeichnisses (Beispiel):

```
e4crypt set_policy [Hex-ID] /media/
  lw/Privat
```

Ab sofort werden alle neuen Dateien im Verzeichnis „Privat“ automatisch auf Dateisystemebene verschlüsselt gespeichert und transparent wieder entschlüsselt. Das funktioniert, solange der Ext4-Schlüssel im Schlüsselbund gespeichert ist, also bis zur nächsten Anmeldung am System. Ohne Schlüssel bleibt der Datenträger zwar insgesamt lesbar, aber der Ordner „Privat“ zeigt nur Zeichensalat – auch bei den Dateinamen. Für erneuten Zugriff auf die Daten genügt nach dem Einhängen des Ext4-Datenträgers die erneute Eingabe dieses Befehls:

```
e4crypt add_key
```

Das Tool fragt das Passwort ab und lädt bei korrekter Eingabe den Ext4-Schlüssel in den Schlüsselbund. Das Verzeichnis und die enthaltenen Dateien sind dann sofort wieder lesbar.

Das Systemkonto, das diese Aktion ausführt, spielt keine Rolle. Wer auf dem betreffenden Rechner das Kennwort weiß, hat Zugriff auf das verschlüsselte Verzeichnis des Ext4-Datenträgers. ■

Das Dateisystem ZFS

Das ursprünglich für Sun Solaris entwickelte ZFS gilt als „last word in filesystems“. Es geht über die engere Definition eines „Dateisystems“ weit hinaus, kennt keine Limits, besitzt alle Funktionen und Metadaten und integriert einen Volume Manager.

VON HERMANN APFELBÖCK

Eine gerechte Bewertung von ZFS ist nicht einfach: Metadaten, Besitzrecht, ACLs, Streams, Zeitstempel, Checksummen, Hardlinks, Softlinks, Quotas, Journaling, Caching? Alles drin – und viel mehr: Das Dateisystem hat nach heutigem Ermessen keine Größen- oder Mengenbegrenzungen. Dazu arbeitet es als Volume Manager zum Zusammenlegen von Festplattenpools, verkleinert/vergrößert den Pool online durch Hot-Plug oder Entnahme von Datenträgern. Der integrierte Raid-Z-Controller ermöglicht ausfallsichere Mehrfachspeicherung. Automatische und manuelle Snapshots sorgen für Systemsicherheit (neben der automatischen Fehlerkorrektur und Journaling). Datenkomprimierung, Verschlüsselung und Netzfreigaben erledigt ZFS noch nebenbei. ZFS im Desktopanflug (Ubuntu)? Kaum je zuvor ist auf dem PC-Desktop etwas so krass Überdimensioniertes gelandet wie dieses Dateisystem. Das ist kein SUV oder Pick-up, der nicht in die Garage passt: Hier landet ein Chinook-Transporthubschrauber im Schrebergarten. „Viel zu groß“ ist aber nur das eine Problem, fast noch gewichtiger ist die Tatsache, dass für dieses Flugobjekt kein Führerschein A bis D ausreicht. Wer die Pilotenausbildung machen will, muss ein Semester einplanen.

ZFS: Werkzeuge und Grundlagen

ZFS ist nicht im Linux-Kernel integriert, weil Linus Torvalds dies – auch, aber nicht nur – aus lizenzrechtlichen Bedenken ablehnt. Die einzige Linux-Distribution, die optionale ZFS-Unterstützung direkt mitbringt, ist Ubuntu 20.04/20.10, sofern diese Option bei der Ubuntu-Installation gewählt wurde. Überall sonst – und auch unter Ubuntu ohne ZFS-Installation – lässt sich das ZFS-Dateisystem mit diesen beiden Paketen

```
sudo apt install zfsutils-linux
  zfs-fuse
```

nachrüsten. Eine Integration in grafische Werkzeuge ist dadurch aber nicht gegeben, ZFS erfordert grundsätzlich Terminalarbeit. Die in den genannten Paketen enthaltenen Terminalprogramme sind mit zfs, zpool und zfs-fuse überschaubar, hinzu kommen noch die eher peripheren Tools zdb (Debugger) und zstreamdump (Output-Filter für „zfs send“). Die geringe Toolanzahl kann aber nicht lange darüber hinwegtäuschen, wie komplex ZFS ist: Die Manpages für die beiden Werkzeuge zfs und zpool könnten mit etwas Kommentierung dieses Magazin füllen.

ZFS fordert eine großzügige Cacheverwaltung, deren RAM-Verbrauch von der Festplattenkapazität abhängt: Einige Hundert MB gehen verwaltungstechnisch grundsätzlich weg, ferner pro TB Plattenkapazität etwa ein GB RAM. Ein Desktoprechner mit einer Vier-TB-Platte muss also etwa vier GB RAM für ZFS abzweigen. Außerdem laufen für ZFS mindestens vier Systemdienste, der wichtigste heißt „zfs-zed“.

Wer sich bei einer Ubuntu-Installation für ZFS entscheidet, erlebt dies erst einmal als unkomfortable Zunahme an Komplexität: Laufwerkstools wie Gparted oder Gnome-Disks zeigen die rpool-Partitionen von ZFS zwar an, können sie aber nicht bearbeiten. Terminaltools wie mount, lsblk oder df werden durch die komplexe ZFS-Partitionierung durchweg unübersichtlicher.

Für produktive Nutzung sind „zfs“ und „zpool“ zuständig. Ersteres verantwortet die Eigenschaften des Dateisystems, zweiteres ist für die Verwaltung der Datenträger zuständig, die bei ZFS immer als „Pool“ organisiert sind, selbst wenn nur ein Datenträger vorliegt. Der Befehl

```
zpool list
```

zeigt die aktuellen ZFS-Datenträger des Pools an, Basisbefehle wie „zpool create“ oder „zpool add“ formatieren Datenträger mit ZFS oder fügen sie einem bestehendem Pool hinzu. Einem Pool untergeordnet sind ZFS-Datasets, die keineswegs einem kompletten Datenträger entsprechen müssen. In Datasets werden Standardpfade und Snapshots als je einzelnes Dateisystem verwaltet, wie folgender zfs-Befehl zeigt:

```
zfs list
```

Er bringt die Mountübersicht und informiert über den Belegungszustand. Eine

detaillierte Anzeige der ZFS-Eigenschaften pro Dataset oder Verzeichnispfad liefert dann folgender Befehl:

```
zsf get all /
```

Die hier angezeigte umfangreiche Liste der ZFS-Eigenschaften können Sie auch einzeln abfragen. So ist etwa eine Eigenschaft wie „compressratio“ mit

```
zfs get compressratio
```

global über den gesamten Pool zu ermitteln. Sicher gewöhnungsbedürftig sind dabei die ZFS-Pfadangaben wie „rpool/USERDATA/lw_0am7f7“ mit ID. Dass dies (in unserem Fall) mit „/home/lw“ zu übersetzen ist, zeigt der bereits genannte Befehl „zfs list“.

Beispiel 1: ZFS-Snapshots

Wer Ubuntu mit ZFS installiert hat, sieht bei jeder Installation im Terminal Infos wie folgende (Beispiel):

```
Anforderung zur Speicherung des
  aktuellen Systemzustands
Erfolgreich als "autozsys okpszm"
  gespeichert
```

ZFS ist also unter Ubuntu soweit integriert, dass bei jeder Installation standardmäßig ein Snapshot entsteht. Dies gilt für Installationen aus den normalen Paketquellen im Terminal wie im grafischen Softwarecenter. „zfs“ kann alle Snapshots auflisten:

```
zfs list -t snapshot [-o
  name,creation -s creation]
```

Was in eckiger Klammer steht, ist nicht zwingend, reduziert aber auf Snapshotnamen und Erstelldatum und sortiert („-s“) nach dem Erstelldatum – neueste zuletzt. Snapshotnamen bestehen aus dem ZFS-Pfad, gefolgt von einem „@“ und dem Namen des Snapshots. Eine Bezeichnung wie

```
rpool/USERDATA/lw_0am7f7@
  autozsys_w6sj7d
```

zeigt einen automatischen Snapshot („autozsys_...“) im Home-Verzeichnis „/home/lw „(„rpool/USERDATA/lw_0am7f7“). Periodisch landen Snapshots auch im Grub-Menü. Damit kann der Systembenutzer über das Bootmenü zu einem früheren Systemzustand zurückkehren. Wird der Systemstart mit Umschalt-Taste (Bios-Boot) oder Esc (Uefi-Boot) unterbrochen, dann zeigt Grub den zusätzlichen Eintrag „History for Ubuntu...“ und darunter dann die einzelnen Sicherungen (Beispiel):

```
Revert to 24.12.2020 @ 16:22
```

Mit dem Befehl

```
sudo zfs snapshot create [...]
```

lassen sich Snapshots manuell erstellen – allerdings erwartet ZFS dabei die Pfadangabe gemäß seiner rpool-Verzeichnisstruktur:

```
sudo zfs snapshot rpool/USERDATA/
  lw_0am7f7@24.12.2020
```

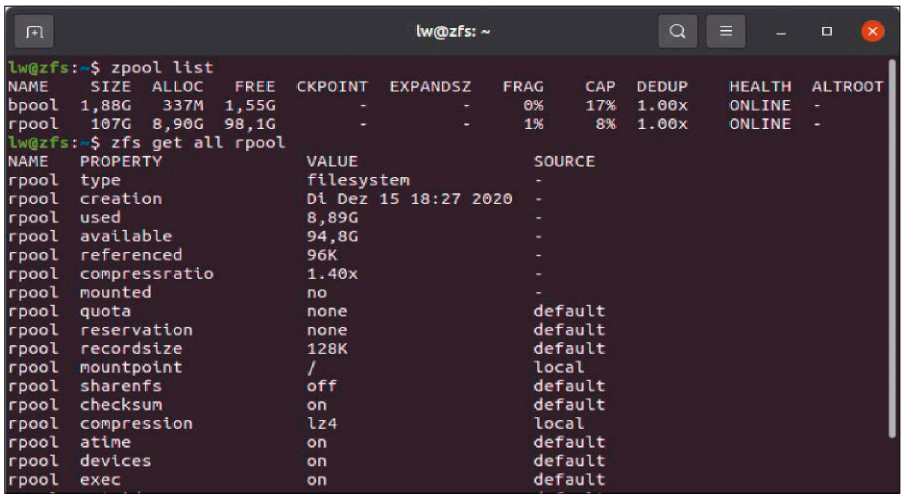
Das ist eine Sicherung des Home-Verzeichnisses (von „/home/lw“), die später mit

```
sudo zfs rollback rpool/USERDATA/
  lw_0am7f7@24.12.2020
```

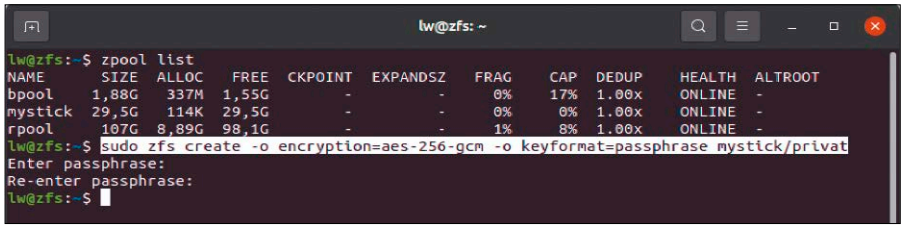
wiederhergestellt werden kann. Der Parameter „destroy“

```
sudo zfs destroy rpool/USERDATA/
  lw_0am7f7@24.12.2020
```

löscht nicht mehr benötigte Snapshots.



Da steckt was drin: ZFS-Objekte zeigen eine opulente – im Bild stark verkürzte – Liste von Eigenschaften, die zum Teil statisch, zum Teil dynamisch, zum Teil vom Benutzer konfigurierbar sind.



Einfach ist anders: Hier wird ein Verzeichnis auf einem USB-Stick als verschlüsselter Bereich definiert.

Beispiel 2: ZFS-Komprimierung

Mit seiner internen Komprimierung kann ZFS erheblich Platz sparen. Bei einer Ubuntu-Installation mit ZFS ist je nach Format der Benutzerdateien ein Platzgewinn von bis zu 50 Prozent zu erzielen. Die Komprimierung kann auch ad hoc für externe Datenträger genutzt werden. Im folgenden Beispiel bearbeiten wir einen USB-Stick („/dev/sde“):

```
sudo zpool create -f stick32 /dev/
  sde
```

Dies bedeutet eine ZFS-Formatierung, die alle bisherigen Daten löscht. Danach liefert der Befehl

```
sudo zfs get all stick32
```

die Menge aller ZFS-Attribute und zeigt, dass die Eigenschaft „compression“ aktuell auf „off“ steht. Das ändert dieser Befehl:

```
sudo zfs set compression=lz4
  stick32
```

Die erneute Abfrage der Eigenschaften zeigt nun bei „compression“ den Wert „lz4“. Das war’s schon. Der USB-Stick ist unter „/stick32“ im Dateisystem eingehängt und kann nun genutzt werden, nachdem der Benutzer mit

```
sudo chown -cR sepp:sepp /stick32
```

den Besitz übernommen hat.

Beispiel 3: ZFS-Verschlüsselung

Um einen verschlüsselten Bereich zu erstellen, beginnt man mit einem neuen Pool unter Angabe eines Namens und der Gerätekennung (hier: „/dev/sde“):

```
sudo zpool create mystick /dev/sde
```

Auf dem neuen Datenpool „mystick“ entsteht nun mit Namen „privat“ der verschlüsselte Bereich.

Nach folgendem Befehl

```
sudo zfs create -o encryption=aes-
  256-gcm -o keyformat=passphrase
  mystick/privat
```

wird zweimal das Passwort abgefragt. ■

Das Dateisystem BTRFS

BTRFS hat als der etwas kleinere ZFS-Konkurrent das Potenzial für den künftigen Linux-Standard am Desktop. Es bietet fundamentale Vereinfachungen für die Datenträgeradministration ohne die überdimensionierten Maße eines ZFS.

VON HERMANN APFELBÖCK

BTRFS (B-Tree-Filesystem, „Butter FS“, „Better FS“) gibt es seit 2007, ist seit 2009 im Linux-Kernel und gilt seit 2014 als stabil. BTRFS hat viele Gemeinsamkeiten mit ZFS und gilt als dessen kleineres Linux-Pendant, das besser auf die Leistung und die Anforderungen am Linux-Desktop abgestimmt ist und keine zusätzlichen RAM-Ressourcen fordert. Dennoch bleiben die BTRFS-Spezialitäten vorerst „nur“ optional interessant und für ein typisches Desktopsystem sicher nicht zwingend. Bemerkenswert ist die interne Datenkomprimierung, während Datenverschlüsselung (im Unterschied zu ZFS) weiterhin fehlt. Als Formatierungsoption für interne wie externe Laufwerke hat BTRFS überall in den grafischen Werkzeugen wie Installern oder Laufwerksverwaltungen Einzug gefunden. Überwiegend findet der Umgang mit BTRFS aber im Terminal mit den Programmen statt, die das in der Regel vorinstallierte Paket „btrfs-progs“ (früher „btrfs-tools“) mitbringt. Das wichtigste dieser Tools nennt sich schlicht „btrfs“ und bringt eine Menge an Unterfunktionen mit. Dieser Beitrag hat nur Platz für die interessantesten Fähigkeiten von BTRFS.

BTRFS-Snapshots

BTRFS bietet Snapshots (Systemsicherungspunkte), um – mit einem einzigen Befehl – den aktuellen Partitionszustand zu sichern. Während grafische BTRFS-Tools, die über die grundlegende Formatierung (etwa mit Gnome-Disks) hinausgehen, den meisten Distributionen fehlen, hat Open Suse die Integration ein Stück verbessert. Das Konfigurationszentrum Yast2 bringt mit der Komponente Yast2-Snapper die wichtige Snapshot-Verwaltung in grafischer Darstellung. Dort genügt ein Klick auf „Erzeugen“ für einen manuellen Schnappschuss und „Löschen“ für das Entfernen des markierten Eintrags. Der Punkt „Änderungen anzeigen“ führt zu einem Detailbericht für den markierten Schnappschuss, der gezieltes Zurückschreiben einzelner Dateien ermöglicht – eine kleinteilige Arbeit, die zumindest für Systemdateien gute Kenntnisse voraussetzt.

Bedauerlich ist, dass der Yast2-Snapper kein komplettes Rollback zu einem früheren Zustand auslösen kann. Hierfür bietet Open Suse in erster Linie sein Bootmenü mit Auswahl der Snapshots. Im laufenden System gibt es für diesen Zweck auch noch das Terminaltool Snapper:

```
sudo snapper list
```

Dies zeigt zunächst sämtliche Snapshots mit Kennzahl. Dort suchen Sie den geeigneten Snapshot anhand des Datums und geben dann diesen Befehl

```
sudo snapper rollback [x]
```

mit der zugehörigen Kennziffer ein. Danach starten Sie das System neu. Beim Rollback geschieht grundlegend anderes als beim Wiederherstellen einzelner Dateien im Yast-Modul: Hier hängt Snapper den kompletten Snapshot an die ursprüngliche Stelle ins Dateisystem ein und ersetzt dabei die bisherigen Daten.

Insgesamt erscheint die Snapshotintegration in Open Suse prinzipiell verdienstvoll, aber für Desktopnutzer unzureichend. Wer sich mit BTRFS-Snapshots genauer befassen will, kommt trotz Yast2-Snapper und Konsolen-Snapper am zugrunde liegenden Basisprogrammen btrfs nicht vorbei (Beispiel):

```
sudo btrfs subvolume snapshot /home
  /home/snapshot.2021.01.01
```

Die Quelle – hier „/home“ – ist kein beliebig wählbarer Pfad, sondern muss ein existierendes BTRFS-Subvolume sein, welche wiederum der Befehl

```
sudo btrfs subvolume list /
```

liefern kann.

Snapshots sind auch bei größeren Laufwerken blitzschnell erledigt, da es sich vorläufig nur um einen Zeiger auf identische Dateiobjekte handelt. Erst bei Änderungen muss BTRFS die Originalversion für den Snapshot gesondert speichern. Der Snapshot wird dauerhaft den Originalzustand anzeigen und diesen erhalten, egal was im Originalordner geschieht. Ein „Rollback“, wie es Snapper nennt, gibt es eigentlich nicht: Vielmehr wird das bisherige Original ausgehängt und der Snapshot eingehängt.

BTRFS-Komprimierung auf SSD

BTRFS bietet für komplette Datenträger transparente (Hintergrund-)Komprimierung aller gespeicherten Dateien. Auf SSDs mit wenig Kapazität kann eine Linux-Installation mit BTRFS Platz sparen und obendrein den Datendurchsdatz erhöhen. Preis ist eine höhere Prozessorlast, was aber bei aktuellen CPUs kaum auffallen sollte. Wenn Linux mit BTRFS installiert wurde (was inzwischen auch Ubuntu & Co. anbieten), lässt sich die optionale Komprimierung für das root-Dateisystem in der Datei „/etc/fstab“ einrichten. Nach

```
sudo nano /etc/fstab
```

werden Sie eine gut gefüllte Datei mit diversen Subvolumes vorfinden. Für das root-Verzeichnis „/“ wird als Dateisystem „btrfs“ und in der Optionenspalte lediglich „defaults“ anzutreffen sein. Für die zusätzliche Komprimierung ergänzen Sie die Option „compress“:

```
UUID=[Partitions-ID]  /  btrfs
  defaults,compress  0  0
```

Theoretisch kann Analoges auch für „subvol=/@/home“ und weitere Subvolumes erfolgen.

BTRFS-Komprimierung auf USB

Wer Bedenken vor der Formatierung und Komprimierung eines Systemdatenträgers hat, kann BTRFS immerhin für externe Laufwerke in Erwägung ziehen. Neben dem standardmäßig vorgesehenen

```
sudo mkfs.btrfs /dev/sd[x]
```

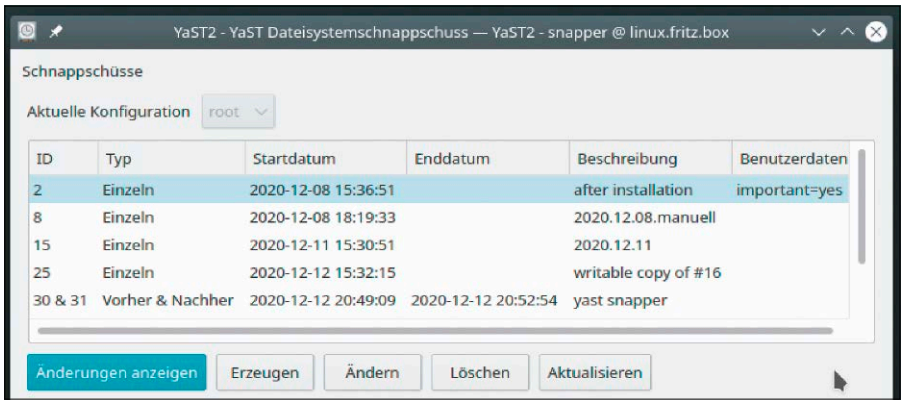
bieten auch die Gnome- und KDE-Laufwerkstools BTRFS-Formatierung. Falls die optionale Kompression gewünscht ist, sollte sie baldmöglichst nach der Formatierung aktiviert werden, da sie erst ab diesemZeitpunkt wirkt (vorher vorhandene Daten bleiben unberücksichtigt). Dies geschieht am Mountpunkt des eingehängten Laufwerks (hier „[...]/btrfs-stick“):

```
sudo btrfs property set /media/
  sepp/btrfs-stick compression zstd
```

Das Attribut bleibt dann permanent gesetzt, auch nach Aushängen und erneutem Einhängen. Davon und von den aktuellen Eigenschaften eines BTRFS-Dateisystems können Sie sich mit

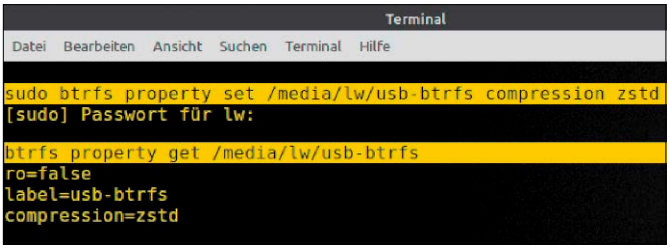
```
btrfs property get /media/sepp/
  btrfs-stick
```

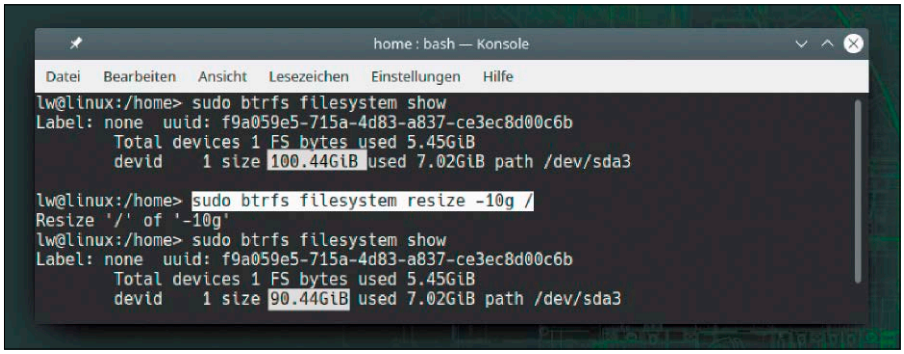
jederzeit überzeugen. BTRFS-Kompression kann gerade bei langsamen USB-Laufwerken und Speicherkarten den Datendurchsatz deutlich verbessern.



Snapshotverwaltung: Open Suse kann mit dem Yast2-Snapper ein grafisches BTRFS-Werkzeug anbieten. Ansonsten bleibt BTRFS-Verwaltung ein Terminaljob.

BTRFS bietet native, transparente Komprimierung. Um die Funktion für externe Datenträger dauerhaft zu aktivieren, genügt das Setzen einer „Property“ für den Mountpunkt.





Größenänderung mit BTRFS: Diese Aktion kostet keine Sekunde. Für den Befehl muss man nur den Mountpunkt kennen, nicht den oder die verwendeten Datenträger.

BTRFS: Weitere Praxisbeispiele

Konvertierung: Das Tool btrfs-convert (im Paket „btrfs-progs“ enthalten) kann von einem Livesystem aus das Ext4-Dateisystem eines bereits installierten Linux zu BTRFS konvertieren. Wir raten ab – nicht aus empirischer Erfahrung, sondern aufgrund prinzipieller Vorsicht vor Eingriffen dieser Dimension.

Datenträger zusammenlegen: Folgender Befehl legt zwei (ausgehängte) Datenträger zu einem logischen Volume zusammen:

```
sudo mkfs.btrfs /dev/sdc /dev/sdd
```

Achtung – das ist eine Formatierung und eventuelle Daten auf den Laufwerken gehen verloren. Um diesen neuen Speicherplatz einzuhängen, benötigen Sie ein leeres Verzeichnis und einen Mountbefehl:

```
sudo mount /dev/sdc ~/Sticks
```

Es spielt keine Rolle, welche der beiden Gerätekennungen Sie verwenden. Sie können später auch noch weitere Datenträger hinzufügen:

```
sudo btrfs device add /dev/sdf ~/
  Sticks/
```

Das gilt analog auch für das root-Dateisystem („/“), falls dort der Speicherplatz knapp werden sollte:

```
sudo btrfs device add /dev/sdf /
```

Größenänderungen: Wie schnell BTRFS Größenänderungen auf einem Volume oder einem Verbund erledigt, zeigt der folgende Befehl:

```
sudo btrfs filesystem resize -10g /
```

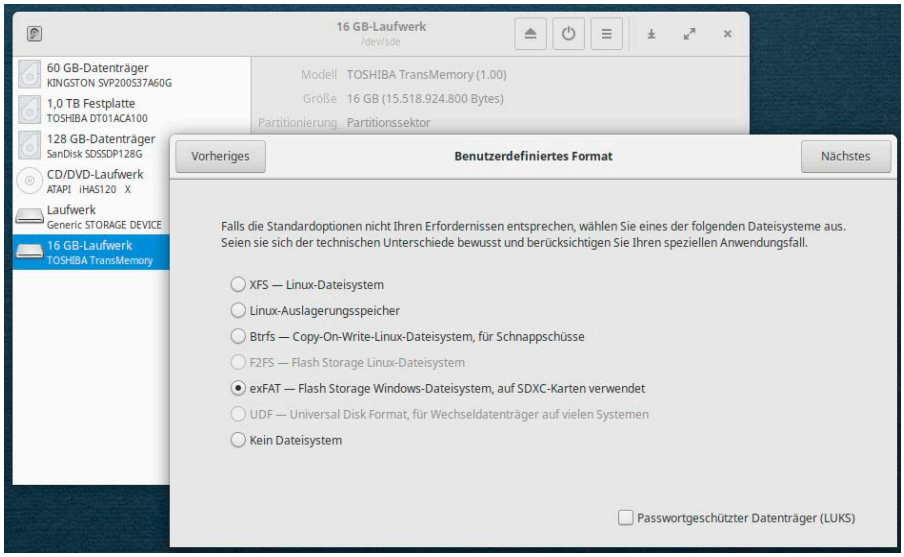
Das verkleinert das root-Dateisystem sofort um zehn GB. ■

Windows-Dateisysteme unter Linux

Für eine Linux-Installation stehen die Windows-Dateisysteme NTFS, FAT32 und exFAT nicht zur Diskussion. Ganz anders sieht es bei externen Datenträgern aus, die unter verschiedenen Betriebssystemen und Geräten genutzt werden sollen.

VON HERMANN APFELBÖCK

Selbst kompromisslose Linux-Anwender sind gut beraten, auf das verbreitete Windows Rücksicht zu nehmen. USB-Sticks oder USB-Festplatten sind unter Windows schlicht nicht verwendbar, wenn die Datenträger mit einem Linux-Dateisystem formatiert sind (Ext, XFS, BTRFS, ZFS …). Die Windows-Reaktion „Sie müssen den Datenträger formatieren…“ ist borniert bis arrogant, weil Microsoft zweifellos in der Lage wäre, zumindest ein Ext4 einzubinden. Aber diese Weigerung ist seit Jahren Status quo und wird sich auch nicht zeitnah ändern. Daher ist es fast unausweichlich, für mobile Laufwerke (eventuell auch in weiteren Situationen) auf ein Microsoft-Dateisystem auszuweichen.



exFAT unter Linux: Das Microsoft-Dateisystem (ohne Dateirechte) überwindet das Vier-GB-Limit von FAT32 für einzelne Dateien und ist auf modernen Linux-Desktops weitgehend Standard.

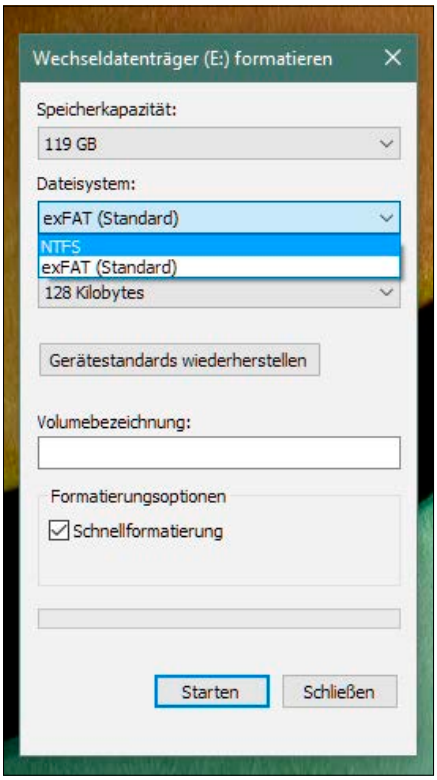
FAT32: Limitiert, aber unkompliziert

Das alte FAT32 (seit 1996) hat gegenüber moderneren Nachfolgern nur einen großen Pluspunkt – es ist wirklich unter jedem PC-System (alte und neue Linux-, Windows-, Mac-OS-Versionen) lesbar und beschreibbar. Unterhaltungselektronik wie Smart-TVs, Hi-Fi-Receiver oder Auto-Soundsysteme werden am USB-Port in jedem Fall einen FAT32-Datenträger einlesen. Sämtliche PC-Betriebssysteme können Datenträger auch selbst mit FAT32 formatieren. Da FAT32 außer zwei Zeitstempeln keine Metadaten und keine Dateirechte anbietet, eignet es sich ausschließlich als Datencontainer insbesondere für USB-Sticks. Das Größenlimit für den Datenträger von 32 GB unter Windows ist künstlich (siehe unten).

Vier-GB-Datei-Limit: Entscheidender ist das FAT32-Limit für eine einzelne Datei von vier GB. IMG- und ISO-Dateien überschreiten diese Größe häufig ebenso wie hochauflösende Filmdateien. Während Windows das Größenproblem im Falle des Falles sofort meldet, kopiert Linux bis zum Erreichen der Grenze und bricht erst dann mit einer Fehlermeldung ab. Für USB-Medien, die keine riesigen Imagedateien oder Filmdateien aufnehmen müssen, reicht FAT32 aber völlig aus.

32-GB-Datenträger-Limit: Bei USB-Sticks, -Festplatten, SD-Karten größer als 32 GB unterschlägt Windows beim Formatieren die Option „FAT32“ und schlägt nur „NTFS“ und „exFAT“ vor, als wäre dies bei Datenträgern dieser Größe technisch nicht anders möglich. Das müssen Sie nicht akzeptieren, wenn ein Linux im Haus ist. FAT32 kann problemlos auch große Datenträger verwalten, indem es einfach die Blockgröße entsprechend hochskaliert. Verwenden Sie etwa Gnome-Disks oder den KDE-Partitionmanager zum Formatieren. FAT32 erscheint dort in der Regel einfach als „FAT“, zum Teil auch erläutert als „Kompatibel mit allen Systemen…“.

USB-Medien mit Livesystemen/Multiboot-Livesystemen: Im Unterschied zu installiertem Linux laufen Linux-Livesysteme sehr wohl auf auch auf FAT32. In den meisten Fällen ist hier FAT32 sogar notwendig oder empfohlen. Tools wie Unetbootin (*http://unetbootin.github.io/*) zum Erstellen von Livesystemen oder Tools wie Yumi (*www.pendrivelinux.com/yumi-multiboot-usb-creator*) zum Einrichten von Multiboot-Live-



Künstliches FAT32-Limit: Ab 32 GB Kapazität bietet Windows nur noch „NTFS“ oder „exFAT“. Linux kann auch große USB-Datenträger mit FAT32 formatieren.

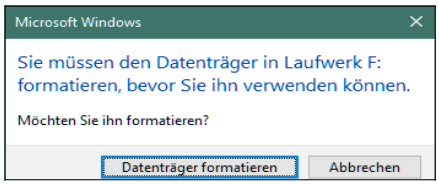
systemen setzen eine FAT32-Formatierung schlicht voraus.

exFAT: „Großer“ Datenaustausch

exFAT ist ähnlich simpel wie FAT32 und besitzt keine Metadaten für Rechte. Entscheidender Unterschied zu FAT32 ist die unlimitierte Größe für Einzeldateien. Wer ISO/IMG-Images und Filme zwischen Linux und Windows austauschen will, kann mit exFAT auf USB- und SD-Datenträgern wenig falsch machen.

Nachdem der Dateisystemtreiber Einzug in den Linux-Kernel gefunden hat, ist exFAT unter Linux größtenteils ohne Nachhilfe nutzbar. Auch grafische Werkzeuge wie Gnome-Disks („Partition formatieren → Andere → exFAT“) bieten inzwischen direkte exFAT-Unterstützung und Dateimanager laden entsprechende Datenträger automatisch. Ausnahme: Der Partitionierer Gparted hat exFAT zwar in seiner Dateisystemliste, will aber bislang nicht mit exFAT formatieren (inaktiv).

SDHX-Karten: Der jüngere SDHX-Standard bei SD-Karten, der sehr große Kapazitäten erlaubt, empfiehlt grundsätzlich eine Formatierung mit exFAT.



Arrogante Reaktion auf Ext, XFS, BTRFS & Co.: Datenträger mit Linux-Dateisystemen will Windows nicht lesen, sondern formatieren (vernichten).

Exorbitante Blockgröße: Während sich normale Blockgrößen (Cluster) bei Dateisystemen im KB-Bereich bewegen, kann die maximale Blockgröße bei exFAT theoretisch bis zu 32 MB betragen! Aus diesem Grund kann das relativ einfache Dateisystem praktisch beliebig große Datenträger adressieren. Empirisch lassen sich unter Linux aber offenbar „nur“ maximal Vier-MB-Blöcke einrichten, und dies auch nur im Terminal:

```
sudo mkfs.exfat -s 8192 /dev/sd[x]
  [n]
```

Die von vier MB völlig abweichende Zahl „8192“ ergibt sich aus der Vervielfachung der kleinsten Einheit „1“, die 512-Byte-Cluster erstellt. Wenn von vornherein klar ist, dass ein Laufwerk ausschließlich sehr große Dateien aufnehmen wird, dann ist eine derart extreme Formatierung durchaus sinnvoll und beschleunigt alle Dateivorgänge. Für kleine Dateien bedeutet das hingegen pure Platzverschwendung. Dies gilt im Prinzip für alle Dateisysteme, ist aber bei dem ungewöhnlichen exFAT eine besondere Erwähnung wert.

Nachinstallation: Wo exFAT unter Linux tatsächlich noch fehlen sollte, ist es mit

```
sudo apt install exfat-fuse exfat-
  utils
```

schnell nachgerüstet (im Beispiel für Debian/Ubuntu & Co.).

NTFS: Auf USB kontraproduktiv

Sofern nicht dumme Geräte der Unterhaltungselektronik berücksichtigt werden müssen, scheint NTFS auf den ersten Blick die beste Wahl für Austauschdatenträger. Das trifft aber nur bedingt zu. Externe USB-Datenträger mit NTFS-Formatierung rangieren unter Linux im Prinzip als rechteloses FAT-Dateisystem: Wenn Linux-Standardbenutzer – Systemverwalter sowieso – externe Geräte ein- und aushängen, erhalten sie auf NTFS-Partitionen (wie auf FAT32 oder exFAT) vollen Lese- und Schreibzugriff. Das sollte zunächst auf einem Austauschdatenträger nicht stören, kann aber erheblich stören, wenn von Windows-Seite spezielle NTFS-Eigenschaften aktiviert wurden. Dateien, für die etwa unter Windows Komprimierung oder Verschlüsselung angefordert wurde, werden unter Linux nicht ankommen. Andererseits wird Linux eingestellte NTFS-Benutzerrechte ignorieren.

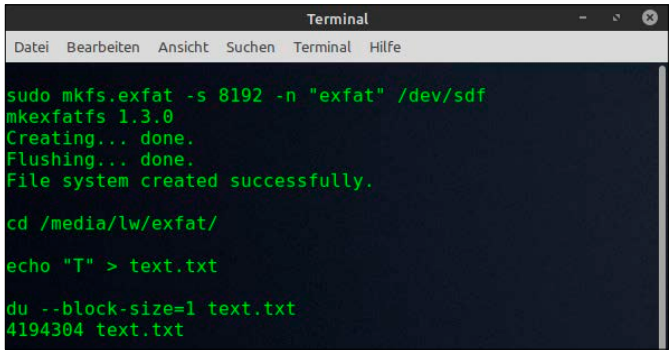
Mit anderen Worten: NTFS ist als Austauschformat solange in Ordnung, als seine eigentlichen Fähigkeiten nicht genutzt werden und es nur als unkompliziertes Containerformat dient. Dann kann man aber gleich zum simplen FAT32 oder exFAT greifen.

FAT32/exFAT und Samba-Freigaben

Datenträger mit rechtelosen Dateisystemen per Samba freizugeben, ist ein absoluter Komfort-Tipp für faule Heimadministratoren. Dateirechte fallen komplett weg und es zählen nur noch die Netzwerkrechte, die in der Samba-Konfigurationsdatei („/etc/samba/smb.conf“) mit wenigen Zeilen definiert sind:

```
[exfat]
path = /media/sepp/toshiba
write list = sepp
browseable = yes
```

Wer sich als „sepp“ ausweisen kann (Benutzer- und Samba-Konto sind natürlich Voraussetzung), kann auf dieser (exFAT-) Freigabe mit vorhandenen und neu erstellten Dateien machen, was er will. ■



Extrem: exFAT kann Vier-MB-Blöcke (Cluster) einrichten, was dann für jede winzige Datei vier MB Speicher kostet, aber bei durchgehend riesigen Dateien den Zugriff beschleunigt.

Der Terminal-Guide: Kategorienübersicht

DATEIEN (1)	
Befehl	**Kurzbeschreibung**
cat / head / tail	Textviewer
chmod	Rechte zeigen / ändern
chown	Besitzer zeigen / ändern
cp	Dateien kopieren
file	genauen Dateityp ermitteln
find	Suche nach allen Dateiattributen
ln	Dateien / Ordner: Soft- und Hardlinks anlegen
locate	Indexsuche nach Dateinamen
ls	Dateien auflisten
mv	Dateien verschieben / umbenennen
rm	Dateien und Ordner löschen
mc	→ siehe Terminalergänzungen
rdfind	→ siehe Terminalergänzungen

SYSTEM (3)	
Befehl	**Kurzbeschreibung**
→ /etc/*_ver* /etc/*-rel*	Infos zu Distribution, Version
→ /var/log	Logdateien syslog, auth.log, dpkg.log
hostname	Servername oder Computername
lsb_release	Kurzinfo zur Distribution
inxi	Infotool → siehe Terminalergänzungen
shutdown / reboot	System beenden und Neustart
systemd-analyze	Bootanalyse
sysctl	Kernel-Parameter steuern
→ /etc/sysctl.conf	Kernel-Parameter (Konfigurationsdatei)
uname	Kurzinfo zu System und Kernel
grub-install / update-grub	Bootmanagerkonfiguration reparieren
uptime	Systemlaufzeit ermitteln
which	Pfad von Programmen ermitteln
whereis	Pfad von Programmen ermitteln
Systemdienste	
service	Dienste-Info und Steuerung (veraltet)
systemctl	Dienste-Info und Steuerung (systemd)

ORDNER (2)	
Befehl	**Kurzbeschreibung**
cd	Navigation
du	Info zur Verzeichnisbelegung
mkdir	Ordner erstellen
ncdu	→ siehe Terminalergänzungen
rmdir	Ordner löschen (nur leere)
tree	Ordnerhierarchie und Dateien auflisten
Backup und Archive	
rsync	Backups & Synchronisierung
tar	Packer & Archivierer

SOFTWARE (4)	
Befehl	**Kurzbeschreibung**
→ /etc/apt/sources.list	Paketquellen für (apt) unter Debian & Co.
apt (yum, pacman)	Verwaltung, Installationen, Aktualisierung
dpkg (rpm)	Softwareverwaltung und Installation
dpkg-query	Softwareinfos, Inventuren und Paketdetails
make	Kompilieren von Quellcode
man	Befehlsbeschreibungen und Schalter

HARDWARE (5)	
Befehl	**Kurzbeschreibung**
→ /proc/cpuinfo	Infodatei (dynamisch) zur CPU
→ /proc/meminfo	Infodatei (dynamisch) zum RAM
dmesg	Kernel-Protokoll („Driver Message“)
dmidecode	Infos zur Hardware
free	Speicherbelegung
hwinfo	Infos zur Hardware
lscpu	Infos zur CPU
lshw	alle Hardwareinfos
lsmod	Kernel-Module anzeigen
lspci	Info zu PCI-Geräten
lsusb	Info zu USB-Geräten
sysbench	CPU-, RAM-, Datenträgertest
hardinfo	Infotool (grafisch), nicht Standard
inxi	→ siehe Terminalergänzungen

Die nach Themen geordnete Übersicht über die wichtigsten Terminalprogramme ist selbsterklärend. Konkrete Beispiele zu allen Werkzeugen bringt die unmittelbar nachfolgende Sammlung auf insgesamt zehn Seiten.

VON HERMANN APFELBÖCK

LAUFWERKE (6)	
Befehl	**Kurzbeschreibung**
→ /etc/fstab	statische Mountanweisungen
blkid	Infos zu Datenträger inkl. UUID
dd	Binärkopierer für Datenträger und Dateien
df	Info zur Datenträgerbelegung
fdisk / cfdisk	Partitionierung
gdisk / cgdisk	Partitionierung
hdparm	Steuerung der Laufwerksparameter
lsblk	Infos zu Datenträger inkl. UUID
mkfs	Datenträger formatieren
mount	Datenträger einhängen
parted	Partitionierung

PROZESSE / TASKS (8)	
Befehl	**Kurzbeschreibung**
Autostarts	Programmstarts bei Desktopanmeldung
crontab	Cronjobs einsehen und erstellen
disown	Terminal als Parentprozess lösen
htop	Infos zu Tasks und Tasksteuerung
iotop	Infos zur Festplattenaktivität
killall	Tasks über Namensangabe beenden
lsof	Dateien: offene auflisten
pkill	Tasks über Namensangabe beenden
ps	Infos zu Tasks und Tasksteuerung
top	Infos zu Tasks und Tasksteuerung
Systemdienste → SYSTEM (3)	

TERMINAL-INTERNA (10)	
Befehl	**Kurzbeschreibung**
→ ~/.bashrc	Standard-Start-Script der Shell
alias	Befehlsabkürzungen
apropos	Befehlssuche
bind	Tastenkombinationen erstellen
cdpath	erweiterte Ordnernavigation
history	Befehlsverlauf
PS1	Variable für Bash-Prompt
shopt	Shell-Optionen setzen
whatis	Befehlsbeschreibung

TERMINALERGÄNZUNGEN (11)	
Befehl	**Kurzbeschreibung**
htop	Infos zu Tasks und Tasksteuerung
inxi	Infos zu System, Hardware, Software, Netz
mc	Terminaldateimanager
ncdu	Info zur Ordnerbelegung und Löschtool
powertop	Infos & Tuning zum Stromverbrauch
rdfind	Dateidubletten suchen, löschen, verlinken

BENUTZERKONTEN (7)	
Befehl	**Kurzbeschreibung**
adduser	Systemkonto anlegen
deluser	Systemkonto löschen
id	Gruppenzugehörigkeiten und UID
passwd	Kennwort für Systemkonto anlegen
smbpasswd	Samba-Benutzer anlegen / löschen
sudo	Wechsel des Kontos (meist zu root)
sudoedit	Wechsel des Kontos (meist zu root)
useradd (→ adduser)	Systemkonto anlegen
userdel (→ deluser)	Systemkonto löschen
usermod	Systemkonto ändern
visudo	Verwaltung des sudo-Rechtes

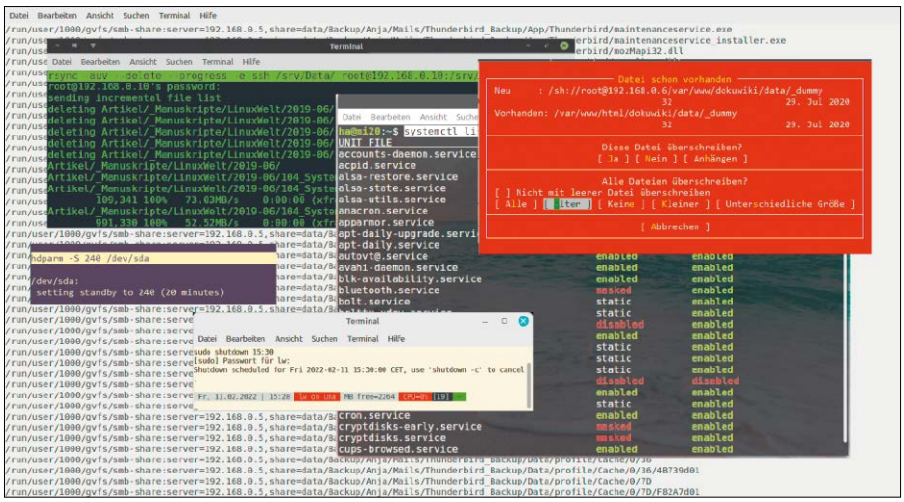
NETZWERK / WEB (9)	
Befehl	**Kurzbeschreibung**
ifconfig	Infos (veraltet, aktuell: ip)
ip	Infos zu Adapter und IP
net	Infos u. Freigaben auf Userebene
nmap	Portanalyse im LAN und WAN
ping	Erreichbarkeit eines Rechners testen
scp	Dateien kopieren auf SSH-Server
sftp	Dateien kopieren auf SSH-Server
smbpasswd	Samba-Benutzer anlegen / löschen
→/etc/samba/smb.conf	Samba-Konfiguration
ssh	SSH-Fernzugriff (Client)
ssh-copy-id	SSH-Fernzugriff (Client)
ssh-keygen	SSH-Fernzugriff (Client)
SSH-Serverkomponente	SSH-Fernzugriff (Server)
Web & Webserver	
→/etc/apache2/	Apache-Konfiguration
curl	Download & Upload
wget	Download
whois	Siterecherche

STRINGS / FILTER (12)	
Befehl	**Kurzbeschreibung**
awk	Outputfilter (Spaltenauswahl u.a.)
column	Spaltenanordnung durch Tabulatoren
grep	Textfilter, Textsuche
sed	Streameditor: Stringverarbeitung
sort	Sortieren des Terminaloutputs

DESKTOP (13)	
Befehl	**Kurzbeschreibung**
startx	Start der grafischen Oberfläche
xdotool	steuert Maus- und Fensteraktionen
xkill	beendet grafische Programmfenster
xprop	Infos zu grafischen Programmen
xrandr	Monitorauflösung und Frequenz

Der Terminal-Guide: Die Beispielsammlung

Die nachfolgenden Terminalbeispiele berücksichtigen alle Kommandos, die in der voranstehenden Kategorienübersicht genannt wurden. Beachten Sie, dass für komplexe Programme typische Beispiele genannt werden, aber keinesfalls eine vollständige Aufstellung aller Optionen.



VON HERMANN APFELBÖCK

1. Dateien

cat & Co: Zur Ausgabe von Text- und Konfigurationsdateien auf dem Terminal steht mit cat, less, more, head, tail eine ganze Reihe von Alternativen bereit. Für den interaktiven Einsatz wird das einfache cat meistens genügen:

```
cat /etc/fstab
```

head und tail beschränken sich auf die Ausgabe der ersten oder der letzten zehn Zeilen, auf Wunsch auch mit genauer Zeilenangabe (hier 20):

```
tail -n 20 /var/log/syslog
```

more und **less** erlauben seitenweises Blättern, was dann aber auch ein Editor wie nano oder mcedit übernehmen kann.

chmod & chown sind unverzichtbar zur Rechteänderung und Besitzübernahme von Dateien auf Linux-Dateisystemen (und optional auf NTFS). chown erledigt mit Schalter „-R“ rekursiv den Dateibesitz (Benutzer:Gruppe):

```
chown -R ha:ha /srv/renkforce
```

Den Dateibesitz vorausgesetzt, ändert chmod die Dateirechte – mit „-R“ rekursiv:

```
chmod -R 777 ~/Dokumente
```

Das Oktalrecht „7“ erlaubt alles für alle (Stelle 1: Benutzerkonto, Stelle 2: Gruppe, Stelle 3: alle anderen). Rekursives chown unterscheidet nicht zwischen Dateien und Ordnern, was zu Problemen führen kann. Dies kann die Zuhilfenahme von → **find** (Punkt 1) erfordern.

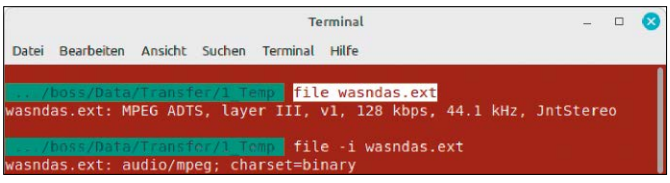
cp kopiert Dateien und aktualisiert („-u“) auch rekursiv („-r“) ganze Verzeichnisse.

```
cp mein.pdf ~/Schreibtisch
cp -ru /mnt/transfer/* ~/transfer/
```

file ermittelt den Dateityp und die genauen inhaltlichen Dateieigenschaften:

```
file bild.png
ls > liste.txt && file -f liste.txt
```

file ist nützlich, wenn Name und Extension irreführend sind. file macht eine Headeranalyse und lässt sich nicht von Namen täuschen. Weniger präzise ist **mimetype** mit Schalter „-M“.



find ist Herr über alle Dateiattribute (Name, Alter, Größe, Rechte) und sucht, filtert, löscht, bearbeitet Dateien rekursiv. Wichtige Schalter sind -iname, -type, -delete, -exec. Folgender Befehl listet alle Dateien im Home-Verzeichnis, die jünger sind als drei Tage:

```
find $HOME -mtime -3
```

Das nächste Beispiel zeigt alle JPG-Bilder, die höchstens fünf, mindestens vier Jahre alt sind:

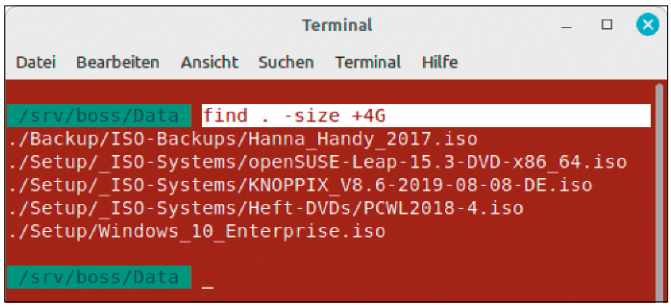
```
find $HOME -mtime -1800 -mtime +1400 -iname *.jpg
```

und

```
find . -size +800M -size -2G
```

liefert alle Dateien mit einer Größe zwischen 800 MB und 2 GB. Bei typischen Rechteänderungen, die zwischen Dateien („-type f“) und Ordnern („-type d“) unterscheiden sollen, hilft find ebenfalls aus.

```
find . -type f -exec chmod 664 {} \;
find . -type d -exec chmod 775 {} \;
```



ln erstellt Softlinks (Schalter „-s“) für Dateien und Ordner sowie Hardlinks für Dateien.

```
ln -s /media/sepp/ISOs/ ~/Schreibtisch/ISOs
```

locate bietet turboschnelle Dateinamenssuche. Das Paket „mlocate“ (!) enthält neben dem Suchkommando locate das Indexierungstool updatedb, das in regelmäßigen Abständen gestartet werden muss. Suchkommandos wie

```
locate -A -i heisenberg einstein
```

liefern sofort alle passenden Dateien mit Pfad.

ls listet und filtert Dateien und Verzeichnisse nach vielen Kriterien und beherrscht auch rekursive Listen:

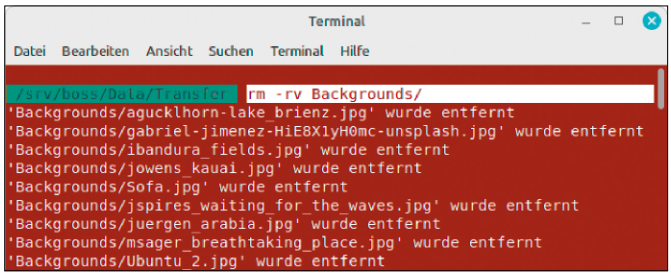
```
ls *.odt
ls -R /media/Archiv/
```

mv benennt Dateien im gleichen Ordner um oder verschiebt sie in einen anderen Ordner:

```
mv datei.txt datei.old
mv /mnt/transfer/text.txt ~/.text.txt
```

rm löscht einzelne Dateien, Dateimuster innerhalb eines Ordners, aber auch ganze Verzeichnisse samt Inhalt:

```
rm test.txt
rm /home/sepp/*.jpg
rm -r /home/sepp/kram
```



2. Ordner

cd wechselt in das angegebene Verzeichnis. Bei fehlender (also relativer) Pfadangabe

```
cd Bilder
```

muss sich der Ordner „Bilder“ im aktuellen Ordner befinden. Absolute Pfadangaben funktionieren immer:

```
cd /media/data/Bilder
```

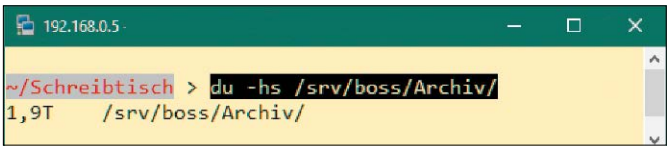
„cd“ ohne Angabe geht immer ins Home, „cd ..“ ins nächsthöhere Verzeichnis (siehe auch → Punkt 11, cdpath).

du ermittelt den Speicherplatz von angegebenen Verzeichnissen oder des aktuellen Ordners (ohne Parameter):

```
du /home/sepp/pictures
```

Eine einfache Gesamtsumme liefert diese Variante:

```
du -hs /home/sepp
```



mkdir erstellt neue, leere Verzeichnisse – mit relativer oder absoluter Pfadangabe:

```
mkdir test
mkdir /home/sepp/test
```

rmdir löscht ausschließlich leere Verzeichnisse – mit relativer oder absoluter Pfadangabe:

```
rmdir /media/data/Bilder
```

Zum Löschen mit Inhalt, siehe rm (Punkt 1).

tree ist kein Muss, aber eine oft bevorzugte ls-Alternative bei der Auflistung von Dateien:

```
tree /home
tree -fas /home
```

Der zweite Befehl zeigt die Ordnerstruktur hierarchisch. „-f“ liefert die vollen Pfade, „-a“ steht für alle (auch versteckte), und „-s“ zeigt die Dateigrößen.

rsync kopiert, aktualisiert („-u“), spiegelt („--delete“) Verzeichnisse rekursiv („-a“) im lokalen Dateisystem und im Netzwerk:

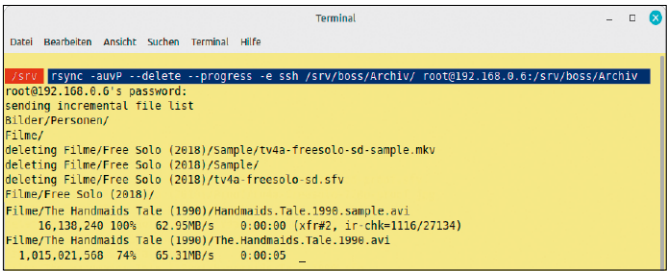
```
rsync -au /home/sepp/ /media/USB/backup
```

Schalter „-dry-run“ (kurz „-n“) dient als Simulation und Vorabtest:

```
rsync -au --delete --dry-run /home/sepp/ /media/sepp/
 USB/backup
```

Besonderes Highlight im Netzwerk ist die direkte Unterstützung von SSH:

```
rsync -au --delete -e "ssh -p 22" /srv/archiv/
 root@192.168.178.10:/srv/boss/Archiv
```



tar komprimiert Ordner und Dateien:

```
tar -czf 2022_02_12 /home/sepp/
```

„-c“ steht für create, „-z“ für platzsparende gzip-Komprimierung, „-f“ sorgt für rekursiven Umfang.

Der Name des Archivs folgt nach den Schaltern, am Ende der Pfad der Quelldateien. Schalter „-x“

```
tar -xf 2022_02_12
```

entpackt Tar-Archive.

3. System

Infos zur Distribution sind je nach Distribution an unterschiedlichen Stellen zu finden. Eine zuverlässige Quelle unter jedem Linux sind die Dateien „/etc/*_ver*“ und „/etc/*-rel*“. Der Befehl

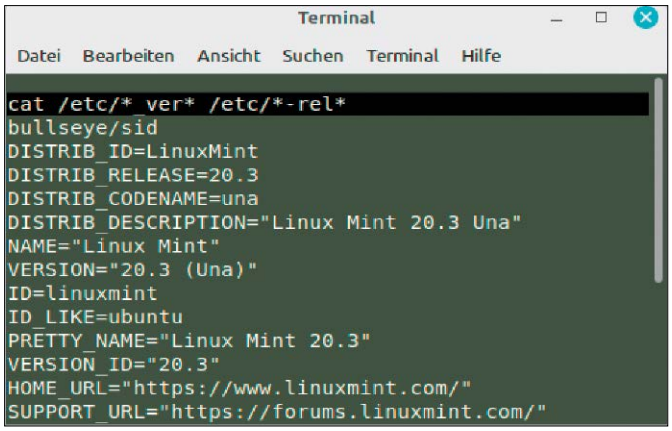
```
cat /etc/*_ver* /etc/*-rel*
```

sollte auf jedem System ausführlichere Infos liefern als die mageren Alternativen

```
lsb_release -a
```

und

```
uname -a
```



/var/log ist der Ablageort für diverse Log- und Protokolldateien (syslog, auth.log, dpkg, Apache, Samba). syslog ist das Systemlogbuch, auth.log protokolliert alle Systemanmeldungen, dpkp.log vermerkt alle manuellen (De-)Installationen. Unter „/var/log/samba“ erscheint jedes zugreifende Netzgerät mit Hostnamen oder lokaler IP-Adresse.

hostname liefert Servername oder Computername des Systems, mit Schalter „-d“

```
hostname -d
```

den Namen der DNS-Domain, im Heimnetz jenen des Routers.

shutdown und **reboot** benötigen root-Recht und schalten das System sofort oder nach definierter Frist (Sekunden) ab oder lösen einen Neustart aus. reboot ist eigentlich überflüssig und durch

```
shutdown -r
```

zu ersetzen.

Der Befehl

```
shutdown now
```

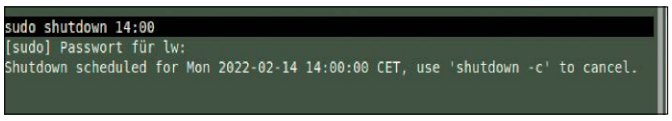
fährt das System sofort herunter, während

```
shutdown 22:00
```

einen bestimmten Zeitpunkt definiert. Interaktiv und flexibel ist

```
shutdown +30
```

mit einer angegebenen Minutenfrist.



systemd-analyze ist eines der vielen Tools des Init-Daemons systemd. Es protokolliert detailliert den Bootprozess und kann die Ursache von Bootverzögerungen entlarven. Eine knappe Zeitmessung bietet

```
systemd-analyze
```

Die Befehle

```
systemd-analyze blame
systemd-analyze dump
```

bringen in unterschiedlicher Darstellung die millisekundengenaue Abfolge des Systemstarts.

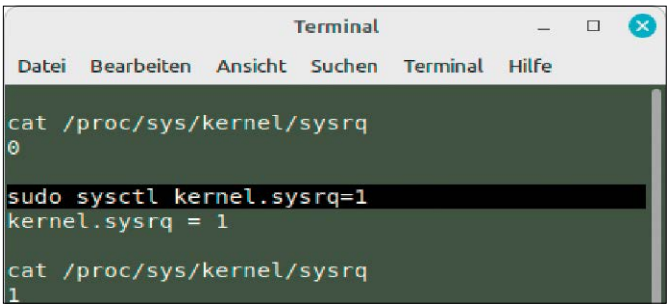
sysctl steuert viele Kernelparameter. Der Befehl

```
sysctl -a
```

listet die zahlreichen Optionen, die sysctl (interaktiv) oder die Systemdatei „/etc/sysctl.conf“ (permanent) manipulieren kann. Die nachfolgenden Beispiele aktivieren die Sysrq-Hotkeys (Notfallhotkeys wie Alt-Druck-B) und ändern das Swap-Verhalten:

```
sysctl kernel.sysrq=1
sysctl vm.swappiness=90
```

Das gilt nur für die Sitzung. Dauerhaft muss die Änderung in die Datei „/etc/sysctl.conf“ eingetragen werden.



grub-install ist der typische Reparaturbefehl nach Bootproblemen und schreibt die Grub-Bootumgebung neu. Dabei muss das Zielgerät für die Grub-Umgebung angegeben werden:

```
grub-install --recheck /dev/sda
update-grub
```

Die Kennung „/dev/sda“, also die erste interne Festplatte, ist ein Beispiel und muss gegebenenfalls angepasst werden.

which ermittelt den Systempfad eines Programms. Dieser wird etwa für Croneinträge, Autostarts oder Desktopverknüpfungen benötigt.

```
which poweroff
```

Das ähnliche whereis

```
whereis poweroff
```

liefert neben dem Systempfad des Programms eventuelle weitere zu Bibliotheken oder Manpages.

service informiert über aktive und inaktive Systemdienste und bietet deren Steuerung. service ist auf systemd-Distributionen im Prinzip obsolet und durch das mächtigere systemctl ersetzt, aber aus Kompatibilitätsgründen weiterhin vertreten. Der Befehl

```
service --status-all
```

bietet eine Übersicht. Für einen bestimmten Dienst gibt es folgende Aktionen (Info, Abschalten, Neustart):

```
service apache2 status
service apache2 stop
service apache2 restart
```

systemctl ist das wichtigste Kommandozeilenwerkzeug von systemd. Es informiert über aktive und inaktive Systemdienste und bietet deren Steuerung. Ohne Optionen listet

```
systemctl
```

einfach alle geladenen Units auf. Folgender Befehl filtert die Systemdienste:

```
systemctl list-unit-files --type service
```

systemctl kann Dienste abschalten, starten, dauerhaft deaktivieren und wieder reaktivieren:

```
systemctl stop apache2
systemctl start apache2
systemctl disable apache2
systemctl enable apache2
```

```
systemctl list-units --type=service
  UNIT                                LOAD   ACTIVE SUB     DESCRIPTION
  accounts-daemon.service             loaded active running Accounts Service
  acpid.service                       loaded active running ACPI event daemon
  alsa-restore.service                loaded active exited  Save/Restore Sound Card St
  apparmor.service                    loaded active exited  Load AppArmor profiles
  avahi-daemon.service                loaded active running Avahi mDNS/DNS-SD Stack
  blk-availability.service            loaded active exited  Availability of block devi
  clean-mount-point@media-lw-GRUBE.service loaded active exited  Clean the /media/lw/GRUBE
  colord.service                      loaded active running Manage, Install and Genera
  console-setup.service               loaded active exited  Set console font and keyma
  cron.service                        loaded active running Regular background program
  cups-browsed.service                loaded active running Make remote CUPS printers
  cups.service                        loaded active running CUPS Scheduler
  dbus.service                        loaded active running D-Bus System Message Bus
```

4. Software

apt (pacman / yum): Terminal-Paketmanager aktualisieren das System inklusive der kompletten Software, (de-)installieren Software und entfernen überflüssige gewordene Pakete.

```
apt update && apt upgrade
apt install vlc
apt remove vlc
apt autoremove
```

Die Beispiele gelten für die verbreiteten Debian/Ubuntu-Systeme mit DEB-Softwarepaketen. In Arch-Distributionen (Manjaro, Endeavour) und RPM-basierten Systeme (Fedora, Cent-OS) heißen die analogen Paketmanager pacman und yum mit gleicher Reichweite:

```
pacman -Syu
yum check-update && yum update
```

Dies entspricht *apt update && apt* upgrade unter Debian & Co.

dpkg installiert Software und ist die Basis des Paketmanagers apt in Debian-basierten Distributionen. Folgender Befehl installiert ein heruntergeladenes, lokal vorliegendes DEB-Paket:

```
dpkg -i meinbrowser.deb
```

Schalter „-i“ ist die Kurzform für „--install“. Weitere dpkg-Optionen sind meist nicht erforderlich, weil diese über apt gesteuert werden können.

dpkg-query ist das Info-Tool zu dpkg. Eine Komplettübersicht zur installierten Software liefert

```
dpkg-query -l
```

und sehr detailliert:

```
dpkg-query -s
```

Nützlich ist ferner, mit

```
dpkg-query -L mc
```

den Umfang eines Pakets zu ermitteln, da Linux-Pakete oft eine ganze Anzahl von Komponenten enthalten.

```
dpkg-query -L mc
/.
/etc
/etc/mc
/etc/mc/edit.indent.rc
/etc/mc/filehighlight.ini
/etc/mc/mc.default.keymap
/etc/mc/mc.emacs.keymap
/etc/mc/mc.ext
/etc/mc/mc.menu
/etc/mc/mcedit.menu
```

make kompiliert Quellcode zu lauffähigen Programmen. Falls es keine anderslautenden Anweisungen gibt, ist im Verzeichnis des heruntergeladenen Quellcodes folgender Dreischritt typisch:

```
./configure
make
make install
```

man zeigt die komplette Hilfeseite (Manpage) des angegebenen Programms. Auch grafische Programme haben Manpages.

```
man rsync
man --html rsync
```

Leertaste blättert seitenweise, Cursor zeilenweise, Taste Q schließt die Manpage. Bei weniger komplexen Tools genügt statt „man“ auch die Abfrage „[befehl] --help“.

5. Hardware

Infotools zur Hardware wie **lscpu** (CPU-Info), **free** (RAM-Info), **lspci** (PCI-Info) **lsusb** (USB-Info) bringen größtenteils nur die Infos in lesbare Form, die jedes Linux im Loop-Ordner „/proc/“ etwa als „/proc/cpuinfo“ und „/proc/meminfo“ ablegt und dynamisch aktualisiert. Die Rohdaten an dieser Stelle sind nämlich größtenteils unkomfortabel lesbar und zu umfangreich. Hervorragende Info-Datensammler sind **inxi** (siehe Punkt 11) und das grafische Tool **hardinfo**.

```
free -m
               gesamt       belegt        frei    gemeinsam     Zwischen   verfügbar
Speicher:        7921         1228         5380          34         1312         6383
Auslager:        2047            0         2047
```

dmesg zeigt das detaillierte Kernel-Protokoll vom Systemstart bis jetzt. Es ist eine der wichtigsten Quellen zur Ursachenforschung bei Boot-, Hardware- und Systemproblemen:

```
dmesg -T
```

Schalter -T macht die Zeitangaben besser lesbar und

```
dmesg -T --level=emerg,alert,crit,err,warn
```

filtert mit Levelangaben harmlose Infomeldungen weg. Bei reproduzierbaren Problemen löscht

```
dmesg -c
```

alle bisherigen Meldungen, um dann nach einer problematischen Aktion erneut dmesg zu befragen.

dmidecode liefert genaue Hardwareinfos. Zum Filtern mit „--type“ gibt es wahlweise Schlüsselwörter oder exakte Kennziffern. Mögliche Schlüsselwörter sind „bios“, „system“, „baseboard“, „chassis“, „processor“, „memory“, „cache“, „connector“, „slot“ – also etwa:

```
dmidecode --type bios
dmidecode --type memory
```

Die 42 Ziffernschlüssel für exakte Einzelinfos sind der Manpage zu entnehmen.

```
sudo dmidecode --type 16
# dmidecode 3.2
Getting SMBIOS data from sysfs.
SMBIOS 2.7 present.

Handle 0x0007, DMI type 16, 23 bytes
Physical Memory Array
        Location: System Board Or Motherboard
        Use: System Memory
        Error Correction Type: None
        Maximum Capacity: 32 GB
        Error Information Handle: Not Provided
        Number Of Devices: 4
```

hwinfo ist meistens nicht Standard, aber über den gleichnamigen Paketnamen überall schnell nachinstalliert. Hwinfo kann **lscpu, lsusb, lspci** und **lshw** ersetzen:

```
hwinfo --short
```

verschafft einen guten Überblick über CPU, Grafikkarte, Festplatten, Netzwerkadapter und Festplattencontroller. Eine Vielzahl von (kombinierbaren) Schlüsselwörtern kann die Recherche eingrenzen:

```
hwinfo --disk --partition
```

Insgesamt 50 verfügbaren Kategorien zeigt das Tool nach *hwinfo -help* an.

lshw ist erstaunlicherweise bei den meisten Distributionen Standard. Brauchbar ist

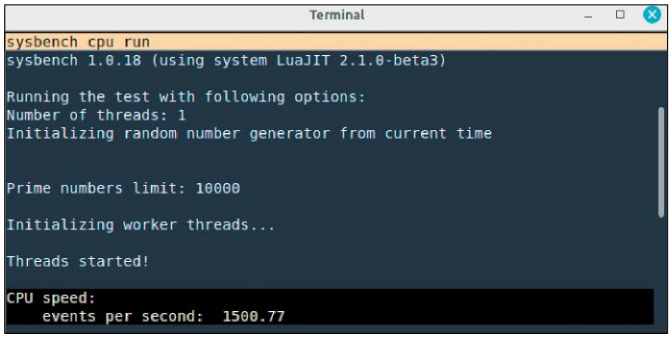
```
lshw –short
```

mit einer knappen Übersicht zu CPU, RAM, Netzadapter, Laufwerke. Ansonsten ist hwinfo das bessere Werkzeug.

sysbench ist ein einfacher Benchmark im Terminal für CPU, RAM und Datenträger, der einen Leistungsvergleich verschiedener Rechner und Komponenten erlaubt:

```
sysbench cpu run
sysbench memory run
```

Die Option für Datenträger („fileio“) ist umständlich und bleibt hier ohne Beispiel.



6. Laufwerke

Die Konfigurationsdatei **„/etc/fstab“** bleibt für Linux-Nutzer eine zentrale Anlaufstelle für statische Laufwerkseinbindungen, wenngleich Installer mindestens die Systempartition eintragen und grafische Werkzeuge wie Gnome-Disks auch nachträgliche Einhängepunkte in die fstab übernehmen können. Eine typische Mountzeile sieht wie folgt aus:

```
#Kennung  Mountordner   FS    Optionen  Dump  Pass
UUID=[…]  /srv/bigboss  ext4  defaults  0     0
```

„Dump“ ist historisch und immer „0“, „Pass“ gibt an, ob Dateisystemprüfungen erfolgen sollen. Statt der UUID (→ Punkt 6: lsblk, blkid) ist auch, aber weniger eindeutig „Label=“ oder die Device-Kennung „/dev/sd[x][y]“ möglich. Der Umfang der Optionen in Spalte 4 ist umfangreich und auch in grafischen Tools nur in Teilmenge berücksichtigt (→ mount).

blkid → lsblk

dd ist ein Binärkopierer für Laufwerksabbilder:

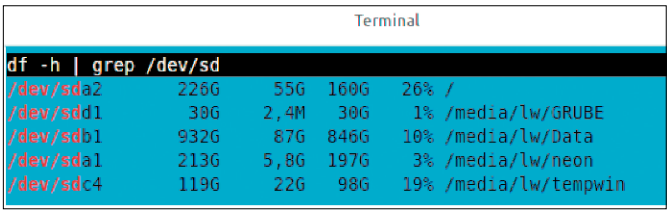
```
dd if=datei.iso of=/dev/sdf bs=4M status=progress
```

„if“ definiert die Quelle (input file), „of“ das Ziel (output file). Mit „bs“ (blocksize) lässt sich der Durchsatz beschleunigen und „status=progress“) sorgt für eine Statusmeldung. dd schreibt auch – umgekehrt – Abbildsicherungen von Datenträgern:

```
dd if=/dev/sda1 of=/srv/data/raspbian.img
```

df ermittelt den belegten und freien Platz von Partitionen und Festplatten und liefert einen knappen und schnellen Überblick:

```
df
df -h | grep /dev/sd
```



fdisk / gdisk dienen zur Partitionierung auf der Kommandozeile (siehe auch → parted). Nachdem das ältere fdisk inzwischen auch den GPT-Partitionsstil und somit auch Datenträger jenseits der Zwei-TB-Kapazität beherrscht, ist gdisk eigentlich überflüssig, wird aber für GPT-Partitionsstil nach wie vor empfohlen. Folgender Befehl

```
fdisk -l /dev/sdc
```

liefert Informationen zum angegebenen Datenträger. Der Befehl

```
fdisk /dev/sdc
```

startet die Aktion, die über definierte Buchstabeneingabe verläuft („m“ für Hilfe, „n“ für neue Partition etc.). fdisk und gdisk sind unbequem, aber logisch und warnen vor destruktiven Aktionen. Wer es etwas bequemer haben will, kann die funktionsidentischen Tools **cfdisk** und **cgdisk** nutzen. Hier gibt es eine menügesteuerte Bedienung über Tabulator- und Navigationstasten.

hdparm steuert das hardwaretechnische Verhalten der Laufwerke wie etwa den Time-out für den Ruhezustand und kann Laufwerke ein- und ausschalten. Schalter „-C“

```
hdparm -C /dev/sda
```

frägt den Status eines Laufwerks ab (aktiv?). Folgender Befehl

```
hdparm -y /dev/sda
```

versetzt das Laufwerk in den Stand-by-Modus und Schalter „-S“

```
hdparm -S 60 /dev/sda
```

setzt den Timer für den Ruhezustand (Zahl in Sekunden mal 5, hier 60*5 = 5 Minuten).

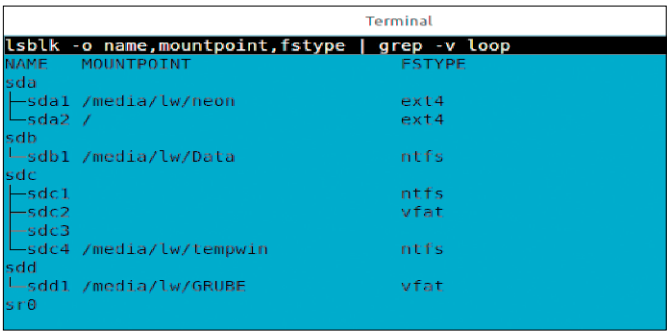
lsblk zeigt angeschlossene Datenträger mit Mountpunkt. Folgender Befehl

```
lsblk -f
```

zeigt auch die eindeutigen UUID-Kennungen. Mit Schalter „-o“ sind sehr detaillierte Recherchen möglich:

```
lsblk -o name,fstype,uuid,size,owner,type,mountpoint
 ,label,model
```

Das ähnliche → **blkid** wird dadurch weitgehend überflüssig.



mkfs formatiert den angegebenen Datenträger mit dem gewünschten Dateisystem („Make Filesystem“). Das Dateisystem wird nach „mkfs.“ angegeben, der Datenträger als letzter Parameter.

```
mkfs.ext4 -L Daten /dev/sdc1
mkfs.ntfs --quick -L Daten /dev/sdc1
```

Je nach gewähltem Dateisystem unterstützt mkfs diverse weitere Optionen.

mount zeigt im Dateisystem eingehängte Medien und lädt aktiv Datenträger in den gewünschten Mountpunkt (Ordner). Folgender Befehl

```
mount | grep /dev/sd
```

zeigt alle eingehängten SATA-Laufwerke. Das Kommando

```
mount /dev/sda1 /media/sepp/usb_2TB
```

hängt „sda1“ im angegebenen Mountordner ein. Der einfache Befehl

```
mount -a
```

arbeitet alle Anweisungen der Datei → „/etc/fstab“ ab, während

```
mount -o loop Datei.iso /mnt/iso
```

eine ISO-Datei einhängt. Mount kennt nach Schalter „-o“ annähernd 30 Optionen, die interaktiv oder in der Datei „/etc/fstab“ angegeben werden können. „defaults“ ist eine Sammeloption, mit der man im Zweifel nicht viel verkehrt macht.

parted ist ein Script-fähiges Partitionierungsprogramm und Basis für den grafischen Klassiker Gparted. Das Tool ist mächtig, aber in der Bedienung noch unbequemer als → fdisk/gdisk.

```
parted -l
```

zeigt eine kompetente Laufwerksübersicht. Den interaktiven Modus startet

```
parted
```

oder direkt *parted /dev/sda*. Dort gibt es den Befehl „print“ für diverse Informationen und „select“ für die Laufwerksauswahl. Die wichtigsten Bearbeitungsbefehle sind mklabel, mkpart, resizepart.

7. Benutzerkonten

adduser richtet ein neues Systemkonto inklusive Home-Verzeichnis ein:

```
adduser sepp
```

Dabei wird automatisch ein Systemkennwort abgefragt. adduser ist ein Wrapper für das eigentliche Kernprogramm **useradd.** Funktional sind die Tools identisch, adduser ist etwas einfacher.

deluser löscht ein bestehendes Systemkonto. Soll auch das zugehörige Home-Verzeichnis gelöscht werden, muss das explizit angegeben werden:

```
deluser sepp
deluser sepp --remove-home
```

deluser ist ein Wrapper für das eigentliche Kernprogramm **userdel**. Funktional sind die Tools identisch, deluser ist etwas einfacher.

id ist ein kleines Infotool, das Gruppenzugehörigkeiten und UID-Kennungen von Systemkonten

```
id
id sepp
```

knapp und trocken ausliefert.

passwd ohne weiteren Angabe

```
passwd
```

ändert das eigene Systemkennwort, bei Angabe eines anderen Kontos (sudo-Recht vorausgesetzt)

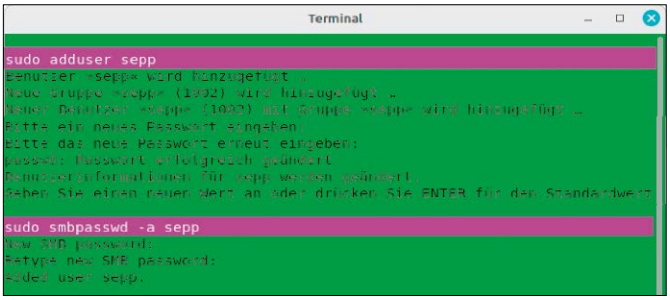
```
passwd sepp
```

auch das Kennwort eines anderen Benutzers.

smbpasswd fügt auf einem Samba-Serversystem neue Samba-Benutzer hinzu („-a“), löscht diese („-x“), aktiviert („-e“) und deaktiviert sie („-d“):

```
smbpasswd -a sepp
smbpasswd -x sepp
```

Samba-Konten sind unabhängig vom Systemkonto, können aber der Einfachheit halber dasselbe Passwort verwenden.



sudo (sudoedit zum Editieren) wechselt den Benutzerkontext – meist zu root mit uneingeschränkten Rechten (für root ist keine Kontoangabe nötig):

```
sudo apt install filezilla
sudoedit /etc/ssh/sshd_config
```

Die Liste aller sudo-berechtigten Konten liegt in der Datei „/etc/sudoers“ (→ visudo).

usermod bearbeitet bestehende Benutzerkonten. Folgende Beispiele zeigen die Aufnahme in eine weitere Gruppe (-aG), eine Kontonamensänderung (-l) und das Sperren eines Kontos (-L):

```
usermod -aG sudo sepp
usermod -l sepp anton
usermod -L sepp
```

visudo ist der empfohlene, weil fehlertolerante Spezialeditor für die Konfigurationsdatei „/etc/sudoers“. Eine typische Zeile, die dem Benutzer „sepp“ uneingeschränktes sudo-Recht einräumt, lautet wie folgt:

```
sepp ALL=(ALL:ALL) ALL
```

8. Prozesse / Tasks

Autostarts bei der Desktopanmeldung sind nützlich, um wichtige Systemsoftware wie Audio oder Aktualisierungsbenachrichtigung bereitzustellen. Alle Autostarts für den aktuellen Benutzer werden als „.desktop“-Dateien unter

```
~/.config/autostart
```

gespeichert. Die globalen Autostarts liegen hier:

```
/etc/xdg/autostart/
```

Es handelt sich um Textdateien, die mit jedem Editor bearbeitet werden können, wobei der Programmaufruf in der Zeile „Exec=“ definiert ist. Die meisten Distributionen bieten ein grafisches Tool, um die Autostarts zu verwalten („Startprogramme“).

crontab zeigt (*crontab -l*) oder editiert (*crontab -e*) die Datei des Systemdienstes Cron, der für zeitgesteuerte Tasks zuständig ist:

```
crontab –e
```

Wenn kein Konto angegeben ist, handelt sich um die Crontab des aktuellen Benutzers. Der Befehl

```
sudo crontab -e
```

öffnet folglich die Crontab des root-Kontos. Crontab-Einträge benötigen fünf Zeitangaben (Minute, Stunde, Tag, Monat, Wochentag)

mit Leerzeichen getrennt und danach den Programmbefehl. Ein tägliches Backup um 18:00 Uhr, tägliches Abschalten des Systems um 22:00 Uhr kann dann so aussehen (benötigt root-Crontab für den Befehl shutdown):

```
0  18  *  *  *  /usr/bin/rsync -av /home/sepp/ /svr/
 backup/sepp
0  22  *  *  *  /usr/sbin/shutdown now
```

```
 GNU nano 4.8          /tmp/crontab.P1iUOX/crontab          Verändert
#Min  Std  Tag  Monat  WoTa  command
30    1    *    *       *    /usr/sbin/rtcwake -m off -s 19800
0     9    *    *       *    /usr/bin/updatedb
# 1:30 Uhr PC ausschalten, aufwecken 5,5 Stunden spaeter (7:00 Uhr)
# 9:00 Uhr Locate-Datenbank auffrischen
```

disown löst ein im Terminal gestartetes Programm vom Elternprozess (Terminal). Das ist nur am grafischen Desktop relevant, um zu verhindern, dass mit dem Schließen des Terminals auch das Programm beendet wird. Außerdem kann das Terminal dann für weitere Kommandos verwendet werden.

```
gedit ~/.bashrc & disown
```

Geht es nur um die Verwendbarkeit des Terminals für weitere Eingaben, dann genügt dies:

```
gedit ~/.bashrc &
```

htop liefert auf der Konsole einen präzisen Überblick über alle laufenden Prozesse und macht Tools wie **top, iotop** oder **dstat** in vielen Fällen überflüssig, siehe → Punkt 11: **htop**.

iotop zeigt Infos zur Festplattenaktivität. Dabei zeigt es die dafür verantwortlichen Tasks und unterscheidet Lese- und Schreib-Operationen. Um von vornherein nur die aktiven Prozesse zu filtern, eignet sich der Schalter „--only“:

```
iotop --only
```

killall und **pkill** beenden Tasks über die Angabe des Programmnamens. Das ist nicht selbstverständlich, da Task-Killer wie das Lowlevel-Tool kill die exakte PID (Process ID) benötigen. killall erfordert den vollständigen Programmnamen

```
killall firefox
```

und pkill ist sogar mit einem Teilstring des Programmnamens zufrieden (Vorsicht!):

```
pkill fire
```

Interaktiv arbeitet man in der Regel mit top und htop einfacher: top ermöglicht nach Eingabe „k“ den Abschuss eines Programms. Bei htop hilft beim markierten Prozess F9, um dann zwischen „SIGTERM“ und härterem „SIGKILL“ (und weiteren Optionen) zu wählen.

lsof zeigt alle aktuell geöffneten Dateien („list open files“)

```
lsof
```

oder jene eines bestimmten Pfads

```
lsof /media/
```

oder alle von einem bestimmten Prozess geöffneten Dateien:

```
lsof -c nginx
```

Anlässe für lsof sind Zugriffsprobleme oder Shutdown-Bremsen.

```
lsof -c smbd | grep /srv/
smbd      2639   ha  cwd       /srv/boss/Archiv
smbd      2639   ha    8r      /srv/boss/Archiv/Texte/Literatur/Neuzeit/Camus, Albert
smbd      2639   ha   14rR     /srv/boss/Archiv/Texte/Literatur/Neuzeit/Camus, Albert/Albert Camus
smbd      2639   ha   43r      /srv/boss/Data/Transfer/Favoriten/Autotext.exe
smbd      2639   ha   44rR     /srv/boss/Archiv/Texte/Literatur/Neuzeit/Camus, Albert/Albert Camus
smbd      2639   ha   45r      /srv/boss/Data/Transfer/Favoriten/Favoriten.exe
smbd      2639   ha   46r      /srv/boss/Data
smbd      2639   ha   51r      /srv/boss/Archiv/Texte/Literatur/Neuzeit
smbd      2639   ha   52r      /srv/boss/Archiv/Texte/Literatur/Neuzeit/Camus, Albert
smbd      2639   ha   54rR     /srv/boss/Archiv/Texte/Literatur/Neuzeit/Camus, Albert/Albert Camus
smbd      2639   ha   55r      /srv/boss/Archiv
```

ps ist ein Lowlevel-Tool zur Prozessanalyse und ermittelt die PID von Tasks, um sie wiederum mit **kill** beenden zu können. Im interaktiven Alltag wird sich der Anwender eher an ein Tool wie **htop** oder **top** halten.

```
ps -A
```

zeigt alle laufenden Prozesse. Bei der Suche nach einem bestimmten Programmnamen hilft

```
ps -A | grep apache2
```

oder die kleine Ergänzung pgrep, die genau dasselbe macht:

```
pgrep apache2
```

top ist ein Prozessmanager wie das (bessere) → htop. Es verliert neben htop aber seine Berechtigung nicht ganz: Sein Vorzug ist die Weitergabe der Prozessinfos an eine Datei:

```
top -b -d 10.0 > top.txt
```

Der Schalter „-b“ sorgt für den Batchmodus, der die eigene Anzeige von top abschaltet. Die Prozessliste wird hier alle zehn Sekunden („-d“ für „delay“) an die Ausgabedatei geschickt.

9. Netzwerk / Web

ifconfig ohne weitere Angaben zeigt Netzadapter, IPv4/IPv6-Adresse, MAC-Adresse, Download- und Uploadmenge. Es kann aber auch Adapter abschalten

```
ifconfig eth0 down
```

oder eine neue IP-Adresse beziehen:

```
ifconfig eth0 192.168.1.25
```

Das nach wie vor vorhandene Tool ist aber im Prinzip obsolet und vollständig durch das neuere **ip** ersetzt.

ip ermittelt Netzwerk- und Adapterinfos und ersetzt zunehmend ifconfig. Der Befehl

```
ip address
```

ermittelt die aktuelle IP Adresse (Kürzungen wie „ip a“ genügen, sofern sie eindeutig bleiben).

```
ip link
```

zeigt die Netzwerkadapter mit MAC-Adresse und folgendes Beispiel

```
ip link set enp3s0 down
```

schaltet den Adapter enp3s0 ab.

net ist – wie die Eingabe ohne Parameter belegt – eine umfangreiche Sammlung von Befehlen zur Netzwerk- und Samba-Administration in Analogie zum Windows-Tool net. Folgende Beispiele beschränken sich auf einen einzigen Unterbefehl „net usershare“:

```
net usershare list
```

zeigt die aktuellen Samba-Freigaben auf Benutzerebene (im Unterschied zu administrativen Freigaben via „/etc/samba/smb.conf“). Der Befehl

```
net usershare add musik ~/Musik sepp:F
```

gibt den Ordner „Musik“ mit vollen Rechten für den Samba-Nutzer „sepp“ frei. Der Samba-Server muss wie bei administrativen Freigaben installiert sein und laufen.

nmap leistet eine Komplettübersicht der lokalen LAN-Adressen, Dienste und Ports sowie Analyse von öffentlichen WAN-Adressen. Folgender Befehl

```
nmap -sP 192.168.178.*
```

schickt Ping-Anfragen an alle 255 Adressen des Adressraum. Das schnelle Scan-Ping (Schalter „-sP“) zeigt alle laufenden Netzgeräte. Ohne „-sP“ macht nmap zeitaufwendige Portscans mit Hostnamen, IP-Adresse, MAC-Adresse und allen offenen Ports (standardmäßig begrenzt auf 1–1000).

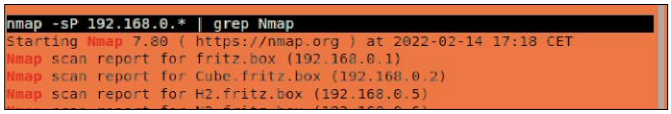
```
nmap 192.168.178.10
```

Ein voller Portscan aller Ports ist mit

```
nmap -p0-65535 192.168.178.10
```

zu erzwingen. Für ermittelte offene Ports – im folgenden Beispiel „22" - kann nmap dann auch den verantwortlichen Dienst ermitteln („-sV" steht für „service version"):

```
nmap -sV -Pn -p22 178.23.136.15
```



ping informiert, ob eine Internetsite oder ein lokaler Rechner online und erreichbar ist:

```
ping wikipedia.de
ping 192.168.1.1
```

scp / sftp sind zwei Alternativen für den Datenaustausch mit OpenSSH-Servern. scp ist ein einfaches Kopiertool wie cp und eignet sich für die schnelle Kopie einzelner Dateien.

```
scp datei.txt sepp@192.168.178.10:~/
```

Dies kopiert eine Datei aus dem aktuellen Verzeichnis in das Home des Benutzers „sepp" am SSH-Server. Abweichende Ports um Massentransport sind ebenfalls vorgesehen:

```
scp -P 2222 ~/Bilder/*.* root@192.168.178.10:/srv/
  transfer
```

sftp orientiert sich an FTP und hat einen größeren Befehlsumfang als nur das Kopieren. Nach

```
sftp root@192.168.178.10
```

zeigt das Kommando *help* eine Übersicht der Kommandos. Befehle wie ls und cd oder auch die automatische Ergänzung mit der Tab-Taste arbeiten wie im Terminal gewohnt. Das Kopieren erfolgt mit get (Download) und put (Upload).

smbpasswd erstellt neue Samba-Konten („-a"), löscht („-x"), aktiviert („-e") und deaktiviert bestehende („-d"):

```
smbpasswd -a sepp
smbpasswd -x sepp
```

Samba-Konten sind unabhängig vom Systemkonto, dürfen aber der Einfachheit halber dasselbe Passwort verwenden.

/etc/samba/smb.conf ist die einzige Konfigurationsdatei des Samba-Servers. Manuelles Bearbeiten ist nach wie vor alternativlos, aber relativ einfach. Um Home-Verzeichnisse per Samba freizugeben, genügt es, in der Zeile

```
; [homes]
```

das Semikolon zu entfernen. Eine allgemeine Freigabe für ein beliebiges Verzeichnis lässt sich über drei Zeilen am Ende der Datei „smb.conf" realisieren:

```
[data]
path = /srv/data
writeable = yes
```

Das Beispiel gibt das Verzeichnis „/srv/data" unter der Bezeichnung „data" frei. Für den Zugriff ist auf dem Server ein System- sowie ein Samba-Konto erforderlich.

ssh ist der Befehl für den Fernzugriff auf andere Linux-Rechner im Netzwerk. Im Prinzip genügt

```
ssh 192.168.0.10
```

oder auch:

```
ssh raspberry
```

Anmeldekonto und gegebenenfalls abweichender Port („-p") sowie grafisches X11-Forwarding („-X") können mitangegeben werden:

```
ssh -X -p 2222 root@192.168.0.10
```

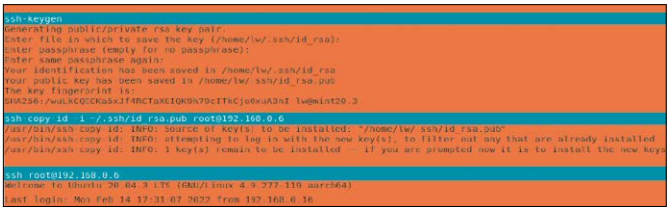
ssh-keygen und **ssh-copy-id** sind optionale Hilfstools für den SSH-Fernzugriff (am Client), um sich die Eingabe des Anmeldekennworts zu sparen. Der Befehl

```
ssh-keygen
```

erstellt auf dem Clientsystem einen Zugangsschlüssel. Der Befehl

```
ssh-copy-id -i ~/.ssh/id_rsa.pub sepp@192.168.178.20
```

kopiert den Schlüssel zum Server.



SSH-Server: Während der SSH-Client auf jedem Linux Standard ist, muss auf dem entfernten Rechner die Serverkomponente installiert sein und laufen (openssh-server). Dies ist auf Desktopsystemen nicht Standard. Der Server ist ab Installation aktiv. Die Serverkonfiguration unter **/etc/ssh/sshd_conf** ist nur manuell zu verändern. Typische Optionen sind mit

```
Port 2222
PermitRootLogin no
AllowUsers sepp
LoginGraceTime 8
```

Portänderungen (sicherer), Zulassen des root-Log-ins (unsicherer), Einschränken der Zugriffskonten (sicherer), Verkürzen der Anmeldefrist (sicherer).

Webserver Apache und seine Konfiguration (→ /etc/apache2/) sind mit einigen Befehlsbeispielen hier nicht darzustellen. Die typische Konfigurationsdatei

```
/etc/apache2/sites-available/000-default.conf
```

muss in jedem Fall manuell bearbeitet werden, wobei als „DocumentRoot" der Ordner der jeweiligen Webanwendung anzugeben ist. Über Änderungen muss der laufende Apache stets mit

```
systemctl reload apache2
```

informiert werden, also über einen Neustart.

curl beherrscht Downloads und Uploads von und auf Webserver. Für den Download genügt

```
curl --remote-name https://seite.de/datei.txt
```

und für den Fall eines nicht öffentlichen Bereichs (FTP, geschütztes HTTPS) diese Variante:

```
curl --remote-name https://seite.de/datei.txt --user
  sepp:passw0rt
```

Ähnliches gilt für den Upload:

```
curl --upload-file datei.txt --user sepp:passw0rt
  https://seite.de/
```

wget ist gegenüber **curl** das einfachere Werkzeug, sofern es ausschließlich um den Download geht. Dieser Befehl holt eine einzelne Datei

```
wget http://seite.de/Datei.txt
```

und der folgende von einem passwortgeschütztem Website-Bereich:

```
wget -q --user=sepp --password=0815 http://seite.de/
  datei.pdf
```

Ein Massendownload bis hinunter zur sechsten Verzeichnisebene („-l6“) erledigt dieser Befehl:

```
wget -r -l6 http://seite.de
```

whois liefert Domaininfos über Hosting, Besitzer, Adresse, Telefon.

```
whois -I pcwelt.de
```

Der tatsächliche Umfang ist allerdings abhängig von der Domainkonfiguration und somit der Freizügigkeit des Domainbetreibers. Um die Verbindungspunkte zu einem Server darzustellen, ist

```
traceroute pcwelt.de
```

eine nützliche Ergänzung.

10. Terminal-Interna

~/.bashrc im Home jedes Kontos ist das Start-Script jeder Bash-Shell, egal ob im grafischen Terminal oder in der Textkonsole. Wenn Alias-Kürzel, Variablen, Shell-Optionen dauerhaft gelten sollen, ist ein Eintrag in diese Datei erforderlich. Ort und Reihenfolge spielen bei diesen einfachen Einträgen keine Rolle.

alias reduziert längere und öfter benötigte Befehle auf eine bequeme Kurzform:

```
alias ini='nano ~/.bashrc'
alias sync='rsync -auvP --delete -e "ssh -p 22" /srv/
 Data/ root@192.168.178.6:/srv/Data'
```

apropos bietet eine Programmsuche für eine grobe thematische Eingrenzung zum gewünschten Thema oder Befehl:

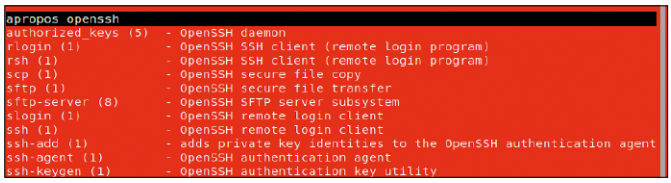
```
apropos openssh
```

apropos ist nur ein Hilfsbefehl, der die Manpages durchsucht. Der Befehl

```
man -k openssh
```

ist funktionsidentisch, jedoch erlaubt apropos auch Kombinationen:

```
apropos --and file rename
```



bind steuert die Tastenbelegung im Terminal und etabliert eigene Hotkeys:

```
bind '"\C-L":kill-whole-line'
bind '"\ed":"& disown"'
bind '"\e1":"nano ~/.bashrc\n"'
```

„\C-“ ist der Code für die Strg-Taste, „\e“ für die Alt-Taste und „\n“ ist der Code für die Eingabetaste.

CDPATH ist eine Bash-Variable für schnelles Springen in wichtige Verzeichnisse. In ihr lassen sich – durch Doppelpunkt getrennt – mehrere Ordnerpfade speichern, um von beliebiger Stelle mit *cd [Verzeichnis]* in ein Unterverzeichnis eines der gespeicherten Ordner zu wechseln:

```
CDPATH='.:~:/srv/archiv/:/srv/data/:/var/www/
 html/:/media/lw/musik/'
```

Das aktuelle Verzeichnis („.“) sollte immer am Beginn stehen.

history zeigt die letzten 500 (Standard)-Terminalbefehle mit Numerierung. „![Nummer]“ startet den betreffenden Befehl. Die Befehlssuche mit Cursor-oben und Strg-R basiert ebenfalls auf der Historyliste.

PS1 ist die Bash-Variable für den Eingabeprompt, der beliebige Informationen transportieren kann, dabei aber altertümliche Escape-Codes verwendet, die hier nicht erläutert werden können:

```
PS1="[$LOGNAME] \w > "
PS1="\u@\h [\w] > "
PS1="\033[43;30m\]\d, \A \[\033[41;37m\] \u on \H \
 [\033[47;30m\] \w \[\033[0m\]\n"
```

shopt steht für „shell options“ und steuert einige kleine, aber nützliche Verhaltensweisen der Historyfunktion und der Verzeichnisnavigation. Der Befehl

```
shopt
```

zeigt alle Optionen. Die nützliche Anweisung („-s“ für „set“)

```
shopt -s autocd
```

sorgt dafür, dass eine (korrekte) Pfadangabe für den Verzeichniswechsel genügt. „cd“ wird dann unnötig.

whatis ist das Gegenstück zu apropos: Es liefert für einen angegebenen Befehl wie

```
whatis firefox
```

die Kurzbeschreibung aus den Manpages. Während apropos Programme für eine bestimmte Aufgabe sucht, zeigt whatis ganz knapp, was ein bestimmtes Programm kann:

11. Terminalergänzungen

htop ist Pflicht auf jedem SSH-administrierten System. Der Taskmanager für das Terminal bietet einen präzisen Überblick über alle Prozesse, erlaubt den gezielten Abschuss einzelner Tasks (F9) und kann die Prozesspriorität steuern (F7/F8). Taste F4 aktiviert einen Textfilter, Taste F6 ändert die Sortierung nach CPU-Anteil, Speicher oder Festplattenzugriff.

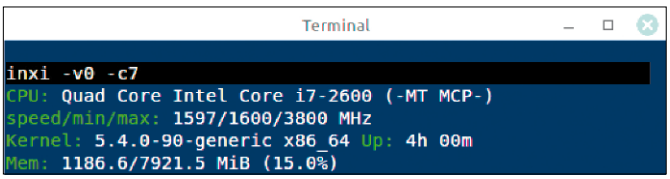
inxi ist für praktisch jedes Linux-System eine Empfehlung. Es liefert schnell und kompakt unzählige Infos über Hardware, Laufwerke, Netzwerk, System, Distribution. Während

```
inxi -v8
```

mit maximaler Gesprächigkeit („-v8“) die allermeisten Infos auswirft, ist auch gezielte Recherche mit annähernd hundert Schaltern möglich:

```
inxi -i
```

liefert nur die Netzwerkinfos. Am einfachsten ist der Einsatz der Verbose-Level „-v0“ bis „-v8“.



mc startet den „Midnight Commander“, einen Terminaldateimanager, der auch auf Desktopsystemen vertreten sein sollte. Das Tool erledigt alle Belange der Ordnernavigation und Dateibearbeitung inklusive SSH („Shell-Verbindung“). Selbst rsync-ähnlicher Datenabgleich ist möglich, wenn man den Konflikt-Dialog nach F5 (Kopieren) zu lesen weiß: Die Option „Älter“ ist der Updatemodus, der fehlende und neuere Dateien kopiert, „Keine“ kopiert nur die bislang fehlenden Dateien.

ncdu sortiert Verzeichnisse standardmäßig nach der enthaltenen Datenmenge und bietet eine bequemere Festplattenanalyse als das Standardwerkzeug **du** (Punkt 2). ncdu wechselt wie ein Datei-

manager zwischen den Verzeichnissen und kann auch aktiv löschen (Taste „d“). Wichtig ist mit

```
ncdu /home
```

die Angabe des passenden Startverzeichnisses, weil ncdu – einmal gestartet – in keine höhere Verzeichnisebene wechselt.

powertop liefert detaillierte Infos zum Stromverbrauch aller Komponenten und dient als Tuningtool. Zur Analyse genügt

```
powertop
```

und zum aktiven Umsetzen der Tuningoptionen dieser Befehl:

```
powertop --auto-tune
```

Dies gilt aber nur für die aktuelle Sitzung.

rdfind findet und beseitigt Dateidubletten. Ein Analyselauf ohne Aktion sieht so aus:

```
rdfind /home/
```

Automatisches Löschen aller Dubletten mit

```
rdfind -deleteduplicates true /home/
```

ist riskant, kann aber durch Softlinks aller Dubletten

```
rdfind -makesymlinks true /home/sepp
```

abgefedert werden.

12. Strings / Filter

awk filtert, verarbeitet, verrechnet Übergabetexte nach Suchstrings und Spalten aus Befehlen und Textdateien. Folgender Befehl filtert zunächst Zeile 2 von „free -m“ und dort die vierte Spalte:

```
free -m |awk 'NR==2' |awk '{print $4}'
```

Folgende Variante verfeinert das Ganze zu einer gut lesbaren Ausgabe des aktuell freien Speichers:

```
free -m | awk '/Speicher:/ {print "Frei: " int($2-$3) " MB
  [von "$2 " MB]"}'
```

Das nächste Beispiel entfernt die Zeilennummern aus der Bash-History und **sort** sortiert die verbleibenden Kommandos:

```
history | awk '{print $2}' | sort
```

```
free -m | awk '/Speicher:/ {print "Frei: " int($2-$3) " MB [von "$2"]"}'
Frei: 6616 MB [von 7921]
```

column ordnet den Terminal-Output deutlich übersichtlicher durch Spaltenanordnung mit Tabulatoren:

```
mount | column -t
```

In manchen Fällen ist es zweckmäßig, einen ganz bestimmten Separator (hier den Doppelpunkt) durch Tabulatoren zu ersetzen:

```
cat /etc/passwd | column -s: -t
```

grep ist der verbreitetste Ausgabefilter. grep filtert den Inhalt von Textdateien oder die Ausgabe eines anderen Befehls nach dem gesuchten String:

```
cat /proc/cpuinfo | grep "MemFree"
cat /var/log/auth.log | grep "failed"
```

Grep eignet sich aber auch für die schnelle Textsuche in vielen Dateien, sofern diese einfaches Reintextformat besitzen („-i“ ignoriert Groß-/Kleinschreibung, „-r“ arbeitet rekursiv):

```
grep -ir "heisenberg" /home/sepp/*.txt
```

sed ersetzt alle Zeichenfolgen in einer oder vielen Datei(en) durch einen neuen String, löscht Zeilen oder fügt neue ein. Während der Befehl

```
sed "s/LinixWelt/LinuxWelt/g" *.html
```

alle Änderung nur im Terminal anzeigt, erledigt Schalter „-i“ oder „--in-place“ tatsächlich:

```
sed -i "s/LinixWelt/LinuxWelt/g" *.html
```

Der Schreibfehler „LinixWelt“ wird überall korrigiert. Effizient, aber auch riskant sind Löschkommandos mit „d“:

```
sed -i '/bind /d' ~/.bashrc
```

Jede Zeile mit dem String „bind“ wird entfernt.

sort sortiert die Ausgabe anderer Befehle alphabetisch (Standard)

```
find /media/Archiv/Filme/ | sort
```

oder numerisch (-n)

```
du -aS | sort -n
```

oder auch nach der bestimmten Spalte (-k):

```
history | sort -k2
```

13. Desktop

startx startet – etwa nach Reparaturen – die grafische Oberfläche aus der virtuellen Textkonsole:

xdotool eignet sich für Systembastler und steuert Maus- und Fensteraktionen. Folgender Befehl

```
xdotool key "super+d"
```

simuliert den Hotkey Windows-D, um den Desktop anzuzeigen, und

```
xdotool mousemove 0 0;xdotool click 1
```

befördert den Mauszeiger in die linke obere Ecke und löst dort einen Mausklick aus. Die Befehlskombination

```
TMP=$(xdotool selectwindow);xdotool windowkill $TMP
```

wartet auf den Klick auf ein Programmfenster. Der Befehl „selectwindow“ ermittelt das Fenster-Handle und beendet den Task.

xkill beendet grafische Programme, deren Fenster nicht mehr reagieren. Nach

```
xkill
```

verwandelt sich der Mauszeiger in ein Kreuz, das ein angeklicktes Fenster gewaltsam beendet. Die rechte Maustaste beendet xkill ohne Aktion.

xprop (ähnlich **xwininfo**) ermittelt Programmnamen und Eigenschaften grafischer Programme. Nach der Eingabe

```
xprop
```

im Terminal verwandelt sich der Mauszeiger in ein Kreuz. Nach Klick auf das gewünschte Fenster erscheinen im Terminal die Infos, insbesondere der zugehörige Programmname.

```
xprop | grep "(STRING)"
WM_WINDOW_ROLE(STRING) = "browser"
WM_LOCALE_NAME(STRING) = "de_DE.UTF-8"
WM_CLIENT_MACHINE(STRING) = "mint20.3"
WM_CLASS(STRING) = "Navigator", "Firefox"
```

xrandr ist das Basistool für die Monitoreinstellungen am grafischen Desktop. Im Normalfall bietet der Desktop eine grafische Alternative in Systemeinstellungen. Im Prinzip kann aber auch xrandr Auflösung und Wiederholfrequenz festlegen.

```
xrandr
```

zeigt die angeschlossenen Monitore, mögliche Auflösungen und maximale Frequenz. Der Befehl

```
xrandr -s 1920x1080
```

legt die Auflösung für einen Monitor fest und der Befehl

```
xrandr --output DVI-0 --mode 1280x1024
```

für einen bestimmten Monitor. Der Befehl

```
xrandr --output HDMI-0 -off
```

schaltet einen bestimmten Monitor ab. ■

Linux-Systemordner

Mit der typischen Linux-Ordnerstruktur startet der systematische Tabellenteil dieses Magazins. Die Übersichtstabellen beantworten kompakt die wichtigsten Fragen rund um Linux-Technik, Linux-Probleme und Distributionen.

LINUX IN TABELLEN

Thema / Inhalt	Beschreibung	Seite
Dateisystemstruktur	die wichtigsten Ordner im Linux-Dateisystem	40
System- und Hardwareinfos	System-, Hardware- und Prozessinformationen abfragen	42
System- und Konfigurationsdateien	die wichtigsten Konfigurations- und Protokolldateien	44
Terminal-Essentials	unentbehrliche Terminalbefehle	46
Netzwerk & Internet	Befehle und Tools für lokales Netz und Internet	48
Linux-Dienste	Standarddienste unter Linux	49
Hotkeys: allgemeine Systemstandards	unentbehrliche Tastenkombinationen	50
Hotkeys: Desktop & Dateimanager	Werkzeuge und Konfiguration für die Fernwartung	51
Distributionsüberblick	prominente Distributionen für jeden Einsatzzweck	52

VON HERMANN APFELBÖCK

Die nachfolgenden Tabellen bieten fundamentale Linux-Infos in komprimierter Form. Diese Tabellen sind primär nicht als Lesestoff konzipiert, sondern als Anlaufstelle für Fragen aller Art. Es gibt hier technische Grundlagen zur Dateisystemstruktur oder zu fundamentalen Konfigurationsdateien. Ferner zeigen Beispielkommandos die wichtigsten Terminalbefehle für Dateibearbeitung, Informationsbeschaffung und Netzwerkkontrolle. Nicht zuletzt erhalten Sie eine charakterisierende Übersicht über die wichtigsten Linux-Distributionen.

Die Linux-Verzeichnisstruktur: Insbesondere für Windows-Umsteiger bedeutet die Ordnerorganisation unter Linux eine große Umstellung. Statt Laufwerksbuchstaben für physikalische Datenträger auf oberster Ebene liegen bei einer Standard-Linux-Installation alle Daten unter dem root- oder Wurzelverzeichnis „/“. Es bedeutet für die Nutzung und Verwaltung von Linux-Systemen eine große Hilfe, wenn Sie eine klare Kenntnis darüber haben, was in Verzeichnissen „/etc“, „/media“ oder „/usr“ zu erwarten ist und wie sich das Home-Verzeichnis genauer untergliedert. Diese Kenntnis ist dann eine erfreulich nachhaltige: Die Dateisystemstruktur gilt im Prinzip seit Jahrzehnten unverändert für alle Distributionen. ■

DIE LINUX-VERZEICHNISSTRUKTUR

Pfad	Beschreibung
/	Wurzelverzeichnis, bei vielen Dateimanagern als „Rechner“ bezeichnet
/boot	systemkritischer Ordner mit den zum Booten notwendigen Dateien: Kernel, Bootmanager und Ramdisk „initramrd“ mit Treiberausstattung
/boot/grub	systemkritischer Ordner mit den Konfigurationsdaten für den Grub-Bootmanager; optionale Eingriffe in die Datei grub.cfg nur für erfahrene Benutzer
/bin	systemkritischer Ordner mit den zentralen ausführbaren Programmen, die für den Systembetrieb notwendig sind (etwa bash, chmod, login, lsblk, mount …); s. a. /sbin und /usr/bin
/cdrom	alter Mountordner für den Inhalt optischer Laufwerke, eigentlich obsolet (ähnlich das inzwischen seltene /floppy)
/dev	Systemverzeichnis für Gerätedateien: Alle erkannten Geräte sind hier konsequent als Datei abgebildet
/etc	zentrales Verzeichnis für alle systemweiten Konfigurationsdateien, zum Teil als Einzeldateien im Hauptverzeichnis /etc wie etwa sudoers (sudo-Rechte), fstab (Laufwerke), mime-types (Dateitypen), shadow (Konten und Kennwörter), zum größeren Teil in Extra-Verzeichnissen – prominente Beispiele: /etc/apache2 für die Konfiguration des Apache-Webservers /etc/apt/ mit der Liste der angemeldeten Paketquellen (sources.list und /etc/apt/sources.list.d) /etc/samba mit der Konfiguration des Samba-Servers und der Windows-Freigaben (smb.conf) /etc/ssh mit der Konfiguration von Open SSH als Client (ssh_config) und Server (sshd_config) /etc/X11 für Konfigurationen der grafischen Oberfläche
/home	Sammelordner für alle sämtliche Benutzerkonten (mit Ausnahme von root)

DIE LINUX-VERZEICHNISSTRUKTUR (FORTSETZUNG)

Pfad	Beschreibung
/home/[user]/	Home-Verzeichnis eines Benutzers mit typischen Unterordnern für Benutzerdaten („Dokumente“, „Bilder“ etc.); /home/[user] ist neben den temporären Mountordnern /media/[user] und /run/user/[Konto-ID] das einzige Verzeichnis mit allen Rechten für den Benutzer inklusive Besitzrecht
/home/[user]/.cache	benutzerbezogener Zwischenspeicher hauptsächlich für Schriften, Bildminiaturen und Systemicons
/home/[user]/.config	wichtiger versteckter Sammelordner für benutzerspezifische Softwareeinstellungen (Desktop-einstellungen, Sprache, Autostart, Webbrowser, Mail, Mime-Dateitypen, Software aller Art)
/home/[user]/.local	weiterer Sammelordner für Desktop-Benutzereinstellungen, die Priorität über allgemeine Einstellungen erhalten, zum Beispiel eigene oder geänderte Verknüpfungen (.desktop-Dateien) unter ../.local/share/applications
/lost+found	enthält nach Dateisystemprüfungen mit fsck gerettete Dateifragmente (in der Regel nur für Forensiker verwertbar)
/media	Mountordner für Wechseldatenträger wie USB- oder DVD-Laufwerke, wird beim Automount grafischer Oberflächen nach Anschluss von Medien in der Regel als Mountpunkt genutzt (macht /cdrom und /floppy obsolet). Die Inhalte werden dabei unter /media/[user]/[Laufwerk] mit allen Rechten für den aktuellen Benutzer geladen.
/mnt	optionaler Ordner für temporäres und statisches Mounten externer Datenträger wie USB- oder DVD-Laufwerke (wird vom Automount auf heutigen Systemen nicht mehr genutzt, siehe /media)
/lib **/lib64**	systemkritische Ordner mit unentbehrlichen Systembibliotheken (32 und 64 Bit). Weitere lib-Ordner mit Systembibliotheken (etwa /usr/lib, /var/lib) sind für Anwendungssoftware notwendig, aber nicht systemkritisch
/opt	optionaler Sammelordner für nachträglich installierte Anwendungsprogramme, die nicht zum Standardrepertoire einer Linux-Distribution gehören
/proc **/sys**	Sammelordner für dynamisch abgefragte System- und Hardwaredaten aller Art, insbesondere zu CPU, RAM, Kernel, Datenträger und Prozesse; /proc ist Informationsquelle für viele Systemtools, etwa für CPU- oder RAM-Abfragen (Beispiel-Quelldateien: cpuinfo, meminfo, modules, mounts, partitions, uptime)
/tmp	Sammelordner für temporär benötigte Dateien bei der Softwareausführung und bei installationen – das einzige Verzeichnis, auf das alle Systemkonten uneingeschränkten Schreibzugriff haben
/root	Home-Verzeichnis des Pseudo-Kontos root; falls root aktiviert und genutzt wird, entstehen dieselben Unterverzeichnisse für Benutzerdaten und Konfigationsdaten wie bei /home/[user]
/run	dynamische Informationsablage für alle Programme (tmpfs-Ordner während der Systemlaufzeit)
/run/user/[user-id]/gvfs/	Mountordner für automatisch eingehängte Netzressourcen unter Gnome-artigen Desktops (Gnome, Budgie, Cinnamon, XFCE)
/usr	kein „User“- oder „Benutzer“-Ordner, sondern der umfangreiche Sammelordner für die nicht-systemnahe Anwendungssoftware („User System Resources“), also die am Desktop meistgenutzen Programme
/usr/bin	enthält die meiste Anwendungssoftware für die grafische Oberfläche (vgl. /bin und /sbin)
/usr/lib	bevorratet die zugehörigen Systembibliotheken für nicht-systemnahe Anwendungssoftware
/usr/local	ergänzender Softwareordner: ausführbare Programme unter /usr/local/bin haben Vorrang gegenüber dem Pfad /usr/bin
/usr/share/applications	Sammelordner für Programmstarter, die in Menüs oder am Desktop angezeigt werden
/sbin	systemkritischer Ordner mit zentralen ausführbaren Programmen für die Systemverwaltung, die nur mit root-Recht laufen (etwa fdisk, fsck, hdparm, mkfs, parted …); s. a. /bin und /usr/bin
/srv	gemäß FSH-Standard (Filesystem Hierarchy) der Standard-Mountordner für Datenträger auf Serversystemen, wobei manche Serversysteme nach wie vor /mnt oder /media verwenden
/var/log	Sammelordner für Systemprotokolle
/var/spool	Verzeichnis für abzuarbeitende Warteschlangen, in erster Linie Druckaufträge
/var/www/html	Standardordner für Apache- oder Nginx-Webdienste
Virtuelle Ordner *	**Beschreibung**
computer:///	nützliche Übersicht über alle physischen Datenträger sowie der aktuell eingehängten Netzwerkfreigaben
applications:///	Übersicht der installierten (Gnome-)Programme
burn:///	Dateien, die für das Brennen auf CD/DVD vorgemerkt sind
fonts://	Übersicht über die installierten Schriften
preferences:///	Systemeinstellungen – gleichbedeutend mit dem Aufruf gnome-control-center
trash:///	Papierkorb – gleichbedeutend mit Klick auf „Papierkorb“ im Dateimanager

*Diese virtuellen Ordner beherrschen viele, aber nicht alle Linux-Dateimanager, manche nur eine Untermenge davon.

System- und Konfigurationsdateien

Linux ist ein System, das durch zahlreiche Konfigurationsdateien im Textformat, selten im Binärformat gesteuert wird. Die folgende Liste nennt die wichtigsten Kandidaten.

Systemkonfiguration	Beschreibung
/etc/crontab **/var/spool/cron/crontabs/[user]**	globale Konfigurationsdatei für zeitgesteuerte Crontasks (benötigt keine Anpassung) benutzerspezifische Dateien für Cron. **Achtung**: auch für root (!) Crontab-Format: Minute Stunde Tag Monat WoTag Befehl Beispiel: `0 22 * * * /usr/sbin/rtcwake -m off -s 36000` (täglicher Shutdown um 22:00 Uhr und geplanter Neustart, volle Pfadangaben (!) in crontab)
/etc/fstab	Filesystemtabelle: beim Systemstart automatisch zu ladende Datenträger mit UUID, Mountpunkt, Dateisystem und Optionen Typischer Eintrag: `UUID=8eff8a09-dbb6 /media/data ext4 defaults 0 0`
/etc/group	Liste der Benutzergruppen
/etc/hdparm.conf	optionale Einstellungen für Datenträger, z. B. „spindown“-Anweisungen bei Inaktivität
/etc/hostname	Hostname des Linux-Systems
/etc/hosts	enthält Domainnamen, die nicht vom DNS-Server übersetzt werden sollen, mit direkter IP-Angabe. Zwecke: direkter Start ohne DNS-Vermittlung oder Verbot von Domains
/etc/passwd	Liste aller internen und explizit eingerichteten Benutzerkonten
/etc/rc.local	globale Autostarts beim Systemstart (vor der Useranmeldung): nur Terminalbefehle möglich
/etc/shadow	Passwortdatei aller Systemkonten; reine Textdatei, aber die Passwörter sind verschlüsselt
/etc/sudoers	Benutzerliste für alle sudo-berechtigten Konten. Standardeditor ist visudo. Typischer Eintrag: `[Kontoname] ALL=(ALL:ALL) ALL`
/etc/sysctl.conf	Einstellungen für den Linux-Kernel, z. B. Swapping-Verhalten (vm.swappiness), Magic-Key-Notfalltasten (kernel.sysrq), Netzwerkparameter (net.ipv4.*). Anpassungen nur für Profis.
/etc/apt/sources.list **/etc/apt/sources.list.d/*.list**	Hauptpaketquellen für das Paketverwaltungssystem apt unter Debian/Ubuntu/Mint PPAs und externe Paketquellen unter Debian/Ubuntu/Mint
/etc/default/grub	Standardvorgaben für den Bootmanager Grub2
/etc/network/interfaces	klassische Netzwerkkonfiguration eines Netzwerk-PCs etwa über die Einträge „auto eth0“ und „iface eth0 inet dhcp“. Auf grafischen Systemen übernimmt der Network-Manager diese Aufgabe. Die Konfigurationsdatei wird dann ignoriert
/etc/xdg/autostart/*.desktop	alle hier versammelten Dateien werden bei der Benutzeranmeldung gestartet
/usr/share/applications/*.desktop **/home/[user]/.local/share/applications**	systemweite Programmverknüpfungen für Desktop und Startmenü benutzerspezifische Programmverknüpfungen mit Priorität
Netz- und Webdienste	**Beschreibung**
/etc/apache2/apache2.conf	Hauptkonfigurationsdatei des Apache-Webservers
/etc/apache2/sites-available/000-default.conf	Konfigurationsdatei für aktive Apache-Dienste: fundamentale Einträge sind „<VirtualHost *:[Portangabe]>“ und „DocumentRoot [Pfadangabe]“
/etc/hosts.allow	bestimmten Rechnern (Hostname oder IP-Nummer) die hier definierten Dienste erlauben; standardmäßig leer (nur Kommentierung und Syntaxbeispiel)
/etc/hosts.deny	bestimmten Rechnern (Hostname oder IP-Nummer) die hier definierten Dienste verbieten; standardmäßig leer (nur Kommentierung und Syntaxbeispiel)
/etc/nginx/nginx.conf	Hauptkonfigurationsdatei des Nginx-Webservers
/etc/nginx/sites-available/default	Konfigurationsdatei für aktive Nginx-Dienste: fundamentale Einträge sind „server listen:[Portangabe]“ und „location [Pfadangabe]“
/etc/openvpn/server.conf	Hauptkonfigurationsdatei des Open-VPN-Servers
/etc/php/[x.x]/apache2/php.ini	PHP-Konfiguration unter Apache2

Netz- und Webdienste (Fortsetzung)	Beschreibung
/etc/samba/smb.conf	Samba-Konfigurationsdatei mit Freigabedefinitionen unter „Share Definitions“. Wichtigste Angaben „[Freigabename]“ in eckigen Klammern, „path=“ mit vollständiger Pfadangabe, „valid users=“ mit Kontonamen, „guest ok=“ mit „yes“ oder „no“
/etc/ssh/ssh_config	Konfiguration des Open-SSH-Clients, benötigt in der Regel keine Änderungen
/etc/ssh/sshd_config	Konfiguration des Open-SSH-Servers, u. a. Portangabe „Port xx“ und diverse Sicherheitseinstellungen wie „PermitRootLogin yes“ (root-Zugang erlauben) und „PasswordAuthentication yes“ (Zugang via Passwort erlauben)
/home/[user]/.ssh/rc	benutzerspezifisches Run-Command-Script: automatische Befehle, die beim Aufruf einer SSH-Sitzung vom Server abgearbeitet werden, wenn sich [user] anmeldet
Bash-Shell	**Beschreibung**
/etc/inputrc	globale Eingabestandards für das Terminal (Tastendefinitionen Pos1, Ende, Bild_auf/ab etc.)
/etc/bash.bashrc	globales Start-Script der Bash-Shell für Aliases, Functions, Variablen, die systemweit gelten
/etc/profile	globales Start-Script der Bash-Shell als Log-in-Shell: wird nur bei einer Shell-Neuanmeldung ausgeführt – also bei Anmeldung per SSH oder virtueller Konsole (Strg-Alt-F1)
/etc/skel/.bashrc	.bashrc und weitere Dateien unter /etc/skel bestimmen die Grundausstattung („skeleton“) für die Bash-Shell, wenn ein neues Benutzerkonto eingerichtet wird
/home/[user]/.bash_history	benutzerspezifisches Kommandoprotokoll der Bash-Shell, standardmäßig die 500 letzten Shell-Eingaben. Der tatsächliche Umfang wird durch die Variable „$HISTFILESIZE“ bestimmt
/home/[user]/.bash_login	optionales benutzerspezifisches Start-Script
/home/[user]/.bash_logout	optionales benutzerspezifisches End-Script beim Beenden jeder Bash-Shell
/home/[user]/.bash_profile	optionales benutzerspezifisches Start-Script
/home/[user]/.bashrc	benutzerspezifisches Start-Script der Bash-Shell für Aliases, Functions, Variablen
/home/[user]/.inputrc	benutzerspezifische Eingabestandards für das Terminal (Tastendefinitionen Pos1, Ende, Bild_auf/ab etc.); Achtung: Diese Datei dominiert über die globale /etc/inputrc
/home/[user]/.profile	benutzerspezifisches Start-Script der Bash-Shell als Log-in-Shell: wird nur bei nach Neuanmeldung ausgeführt – also etwa bei SSH oder virtueller Konsole (Strg-Alt-F1)
Diverse Software	**Beschreibung**
/etc/[Software]/[Datei(en)]	globale Konfigurationseinstellungen für „[Software]“ unter /etc/
/home/[user]/.[Datei]	benutzerspezifische Konfigurationsdatei direkt im Home-Verzeichnis, etwa „.conkyrc“
/home/[user]/.[Software]	benutzerspezifische Konfiguration größerer Anwendungssoftware wie etwa /home/[user]/.mozilla, /home/[user]/.thunderbird oder /home/[user]/.ssh
/home/[user]/.config/[Software]	Sammelordner für benutzerspezifische Konfigurationsdateien, etwa /home/[user]/.config/vlc/, /home/[user]/.config/mc/ oder die Desktop-Konfigurationszentrale /home/[user]/.config/dconf/user (binär und nur mit dem Dconf-Editor zu bearbeiten)
Protokolle	**Beschreibung**
/var/log/	Sammelordner für diverse Log- und Protokolldateien (Systemlog, Samba, Apt, Apache, FTP), Zusammenfassungen zum Teil über grafische Tools wie etwa gnome-logs erreichbar
/var/log/apache2/access.log	Protokoll aller Zugriffe auf Webserver-Dienste inklusive Zugriffs-IP, Zugriffsziel, Browser
/var/log/auth.log	chronologisches Protokoll aller Anmeldeversuche sowohl an der grafischen Shell als auch via SSH oder an der Webserver-Konfigurationsoberfläche
/var/log/dmesg	chronologisches Protokoll des Kernels mit allen jüngeren Hardwareereignissen; ältere Ereignisse bewahrt das Protokoll /var/log/kern.log
/var/log/dpkg.log	chronologisches Protokoll aller Updates und Installationen
/var/log/faillog	Protokoll gescheiterter Anmeldungen: Die Binärdatei muss mit `faillog -a` gelesen werden, die Spalte „Failures“ zeigt die Anzahl der Fehlversuche beim jeweiligen Konto
/var/log/nginx/access.log	chronogisches Protokoll aller Zugriffe auf Webserver-Dienste inklusive Zugriffs-IP-Adresse Zugriffsziel und Webbrowser
/var/log/samba	alle zugreifenden Netzwerkrechner mit IP-Adresse oder mit Hostnamen als Einzelprotokoll, sofern in /etc/samba/smb.conf mindestens „log level=1“
/var/log/syslog	chronologisches Protokoll aller Systemereignisse: Netzwerk, Dienste, Cronjobs, Festplatten

Systemdienste unter Linux

Dienste sind kleine Tasks, die permanent auf bestimmte Ereignisse warten oder diese aktiv abfragen. Die Anzahl solcher Dienste ist stark abhängig von Distribution und Konfiguration. Die folgende, naturgemäß unvollständige Liste orientiert sich an einem Standard-Ubuntu.

Dienstname	Beschreibung
acpid	stellt fundamentale ACPI-Funktionen bereit (Ausschalten, Ruhezustände, Helligkeitssteuerung)
alsa | alsa-utils	notwendig zur Soundausgabe, bietet Treiber für Soundchips
anacron	zeitgesteuerte Tasks, die bei Bedarf nachgeholt werden (wichtig bei oft inaktiven PCs/Notebooks)
apache2 | nginx | ligthtpd	aktiver Webserver
apparmor	erweitertes Sicherheitskonzept zur Kontrolle von Anwendungen (Mandatory Access Control)
apport	Fehlerberichterstattung nach Abstürzen bei Ubuntu-Systemen
avahi-daemon	vereinfachte Kommunikation im lokalen Netzwerk (gemäß Apples Zeroconf), findet und verbindet Rechner ohne Hilfe eines DNS-Servers
bluetooth	ermöglicht die Erkennung und das Pairing von Bluetooth-Geräten
brltty	ermöglicht die Terminalbedienung mit Braille-Blindenschrift (Braille-Display vorausgesetzt)
cron	zeitgesteuerte Tasks (via crontab)
cups	freies Drucksystem (Common Unix Printing System)
cups-browsed	auf Apple-Airprint spezialisierter Suchdienst für Drucker
dbus	unentbehrlicher „Desktop-Bus“ für die interne Kommunikation von Programmen (z. B. Meldung an Dateimanager über angeschlossenes USB-Gerät)
geoclue	meldet die geografische Lokalisierung an Programme, die den Standort des Systems benötigen
grub-common	meldet erfolgreichen Systemstart an Grub (Grub-Startmenü erscheint nur, wenn die Meldung fehlt)
hddtemp	Sensoren- und Temperaturmessung für das Systemprotokoll
irqbalance	Interruptsteuerung für bessere Lastverteilung zwischen den CPU-Kernen
kerneloops	meldet Fehler des Linux-Kernel an die Kernel-Entwickler
modemmanager	bietet Zugriff auf mobile Breitbandverbindungen (2G/3G/4G)
networking	bietet Zugriff auf Ethernet- und Wi-Fi-Verbindungen
network-manager	grafische Erweiterung für die Netzwerkverwaltung
lvm2	Unterstützung für LVM-Partitionierung (Logical Volume Manager), z. B. bei Partitionsverschlüsselung
nmdb	Hilfsdienst für den Samba-Server zur Namensauflösung von Netzwerkrechnern
ntp	synchronisiert die Systemzeit mit der eines Zeitservers im Internet
openvpn	erlaubt die Client- und Serverrolle für verschlüsselte VPN-Verbindungen (Virtual Private Network)
plymouth	sorgt für Startanimation bei Ubuntu-Systemen
procps	übernimmt die Kernel-Parameter aus der Datei /etc/sysctl.conf in die aktuelle Sitzung
rsync	rsync-Trigger für Backups und Synchronisierung über das Netzwerk
rsyslog	verantwortlich für die Systemprotokollierung
saned	bietet die Schnittstelle zu angeschlossenen Scannern mit optionaler Scannerfreigabe im Netz
smbd	aktiver Samba-Server für Windows-Freigaben (nur die Serverrolle benötigt einen Dienst)
ssh	aktiver Open-SSH-Server für Fernzugriff (nur die Serverrolle benötigt einen Dienst)
udev	unentbehrlicher Verwaltungsdienst für angeschlossene Datenträger und Automount
ufw	aktiviertes Firewall-Front-End für iptables (die Firewall selbst kann aber dennoch inaktiv ein)
x11-common	Hilfsprogramm für die grafische Oberfläche (X11), das einige Standardverzeichnisse anlegt

Hotkeys für System und Terminal

Die Übersicht beschreibt substanzielle und weitgehend standardisierte Tastenkombinationen. Manche Linux-Funktion ist nur über diesen Hotkey erreichbar.

Grub-Bootloader	Beschreibung
Umschalt (oder Esc)	veranlasst den Grub-Bootloader, das Bootmenü anzuzeigen, auch wenn kein Multiboot vorliegt; ermöglicht die Anzeige „Erweiterte Optionen“ mit Reparaturfunktionen
Taste e (kleines „e“)	Editierbefehl im Grub-Bootmenü: ermöglicht zusätzliche Kernel-Parameter in der mit „linux“ beginnenden Zeile (bei Bootproblemen)
Strg-X	startet das System mit den Kernel-Parametern, die im Editiermodus geändert wurden
F6 (und weitere F-Tasten)	nicht standardisiert: Distributionen wie Ubuntu, Open Suse bieten beim Start die wichtigsten Kernel-Notfallparameter (noacpi, nomodeset) per Funktionstasten
Magic Keys (Sys-RQ-Kernel-Hotkeys)	**Beschreibung**
Voraussetzung für Kernel-Hotkeys	Auf den meisten Systemen sind Sys-RQ-Hotkeys zumindest teilweise aktiviert. Verantwortlich ist der Eintrag „kernelsysrq=[xx]“ in der Datei /etc/sysctl.conf. Die umfangreichste Einstellung ist „kernelsysrq=1“.
Alt-Druck-E	beendet möglichst alle Prozesse inklusive X-Server, ausgenommen den Init-Prozess
Alt-Druck-I	beendet möglichst alle Prozesse inklusive Init-Prozess
Alt-Druck-L	beendet hängende Prozesse mit härterem „Kill“-Aufruf (statt weicherem „Terminate“)
Alt-Druck-S	schreibt alle Daten aus dem Festplattencache physisch auf den Datenträger
Alt-Druck-U	hängt alle gemounteten Dateisysteme aus und schreibgeschützt wieder ein
Alt-Druck-B	löst einen Neustart aus (Ultima Ratio, aber besser als Abschalten des Rechners)
Virtuelle Konsolen	**Beschreibung**
Strg-Alt-F1 (bis F6)	startet die virtuelle Konsole („tty[1-6]“) oder wechselt zu dieser, sofern diese bereits läuft
Strg-Alt-F7	bei den meisten Distributionen die virtuelle Konsole mit der grafischen Oberfläche (seltener Strg-Alt-F6 oder Strg-Alt-F2)
Strg-Alt-Cursor_links | rechts	Wechsel zur vorherigen oder nächsten virtuellen Konsole (nicht überall möglich)
Terminal- (Bash-)Hotkeys	**Beschreibung**
Strg-C	bricht das aktuell aktive Terminalprogramm oder Script ab
Strg-D	beendet das Terminal (wie der Befehl „exit“)
Strg-L	leert den Textinhalt des Terminals (wie der Befehl „clear“)
Strg-U	löscht die aktuelle Befehlszeile von der Cursorposition bis zum Zeilenanfang
Strg-K	löscht die aktuelle Befehlszeile von der Cursorposition bis zum Zeilenende
Strg-R **Eingabetaste** **Alt-Eingabetaste (evtl. Strg-Eingabetaste)**	startet Suchmodus in der Bash-History: nach Tippen etwa von „apt“ Anzeige des letzten apt-Befehls, mit Strg-R zum nächsten passenden History-Eintrag etc. im Suchmodus gefundenen und aktuell angezeigten Befehl sofort ausführen im Suchmodus gefundenen und aktuell angezeigten Befehl zum Editieren auf den Prompt
Strg-S	stoppt die Textausgabe eines Terminalbefehls – nützlich, um die durchlaufende Anzeige an bestimmter Stelle genauer zu kontrollieren
Strg-Q	setzt die nach Strg-S gestoppte Textausgabe wieder fort
Strg-Z	setzt einen Terminaltask (etwa nano oder htop) in den Hintergrund und gibt damit den Prompt für Eingaben frei, mit „fg“ zurück zum Hintergrundprogramm
Tab	Autovervollständigung eines Datei- oder Pfadnamens, von dem nur die ersten Buchstaben eingegeben sind
Strg-Umschalt-C | Strg-Umschalt-V	Kopieren/Einfügen in/aus Zwischenablage (das übliche Strg-C und Strg-V funktioniert nicht)

Hotkeys: Desktop & Dateimanager

Die zahlreichen Linux-Desktops und Dateimanager haben ihre je eigenen Fähigkeiten. Die hier versammelten Standards gelten jedoch für die allermeisten Kandidaten.

Desktop-Hotkeys	Beschreibung
Super	Super (Windows-Taste) zeigt das Hauptmenü des Desktops, (unter Gnome die „Aktivitäten“, die Gnome-Programmübersicht benötigt den speziellen Hotkey Super-A)
Super-D (auch Strg-Alt-D)	minimiert alle Fenster und zeigt den Desktop, erneutes Super-D restauriert die Fenster wieder
Super-L	sperrt die Sitzung und zeigt Anmeldedialog
F11	schalltet Fenster in den Vollbildmodus und zurück (Browser, Dateimanager, Terminal, Editoren ...)
Alt-Tab	Taskswitcher der laufenden Tasks, um zwischen den geöffneten Programmen zu wechseln
Alt-F2	startet den „Ausführen“-Dialog (oder den „Anwendungsfinder“)
Alt-F4	schließt das aktuelle Programmfenster
Alt-F7	verschiebt aktuelles Programmfenster (wichtig bei geringer Auflösung oder fehlender Titelleiste), alternativ funktioniert auch Alt-Taste und direktes Verschieben mit der Maus
Alt-F9	minimiert das aktuelle Programmfenster
Alt-F10	maximiert das aktuelle Programmfenster
Strg-+ | Strg–	vergrößert | verkleinert die Skalierung in vielen Programmen (Browser, Terminal, Dateimanager ...)
Strg-A	markiert den kompletten Text des aktuellen Fensters (funktioniert in den meisten Programmen)
Strg-C | V | X	Kopieren, Einfügen, Ausschneiden von markierten Inhalten (via Zwischenablage)
Strg-Z	macht die letzte Aktion rückgängig, auch Dateiaktionen wie Löschen und Umbenennen
Strg-Alt-Entf	startet das System neu (funktioniert nicht bei allen Desktops, z. T. nur Abmelden wie Super-L)
Strg-Alt-Rücktaste	beendet auf vielen Desktops die grafische Oberfläche (X-Server) und führt zum Anmeldebildschirm
Strg-Alt-T	startet ein Terminalfenster
Strg-Umschalt-Z	macht eine mit Strg-Z ausgelöste Rückgängig-Aktion ihrerseits rückgängig
Druck	speichert Screenshot vom kompletten Desktop unter „~/Bilder“ (nicht bei allen Desktops)
Alt-Druck	speichert Screenshot vom aktuellen Programmfenster unter „~/Bilder“ (nicht bei allen Desktops)
Strg-Alt-Cursor_links | rechts	wechselt zwischen den Desktoparbeitsflächen (auf einigen Desktops Strg-Alt-Cursor_auf | ab)
Strg-Alt-Umschalt-Cursor_links | rechts	verschiebt das aktuelle Fenster zur nächsten Arbeitsfläche (auch Strg-Alt-Umschalt-Cursor_auf | ab)
Dateimanager-Hotkeys	**Beschreibung**
Strg-1|2|3	Ansichtsmodus wechseln (Listen-, Symbolansicht)
Strg-D	aktuellen Ordner als Lesezeichen anlegen
Strg-H	versteckte Dateiobjekte ein- oder ausblenden (Gnome-Dateimanager)
Alt-.	versteckte Dateiobjekte ein- oder ausblenden (KDE-Dateimanager und Midnight Commander)
Strg-L	Dateimanager-Adressleiste zum editierbaren Eingabefeld umschalten
Strg-M	Verknüpfung zum markierten Objekt anlegen
Strg-N	neues Dateimanager-Fenster öffnen
Strg-Umschalt-N	neues Verzeichnis erstellen
F2	markiertes Dateiobjekt umbenennen
F3	Zwei-Fenster-Modus aktivieren und deaktivieren
F9	linke Navigationsleiste ein- oder ausblenden
Strg und mehrere Mausklicks	selektives Markieren einer beliebigen Anzahl von Dateiobjekten
Umschalt und zwei Mausklicks	Markieren einer zusammenhängenden Gruppe von Dateiobjekten