LINUX WELT XXL

NEU: 2 DVDs für Umsteiger & Profis



LINUX WELT XXL

SONDERHEFT XXL
2/2022 Mai – Juli € 12,90
Schweiz sfr 25,80 · Österreich, Benelux € 14,40

NEU!

196 Seiten!

Linux statt Windows

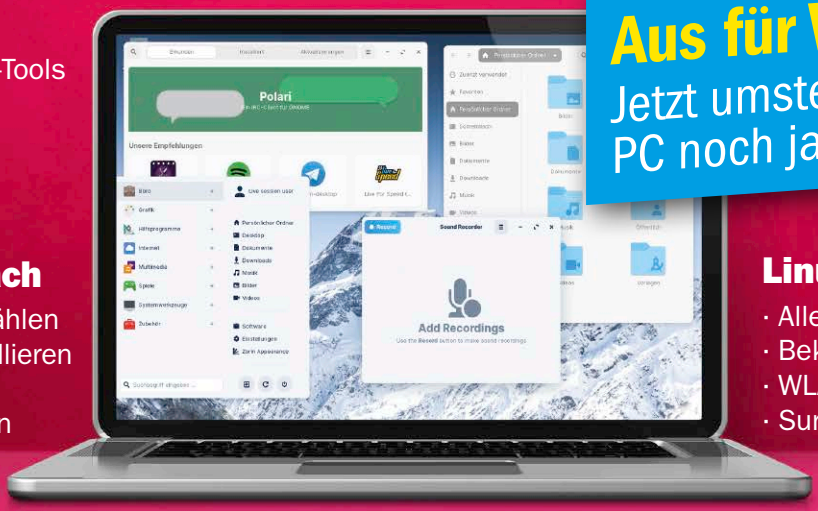
Das große Umsteiger-Handbuch 2022

Linux ist besser

- Gratis-System und Gratis-Tools
- Auch für ältere Rechner
- Besserer Datenschutz
- Höhere Sicherheit
- Kostenlose Updates

Umstieg ganz einfach

- Das beste System auswählen
- Parallel zu Windows installieren
- Software einrichten
- Alles individuell anpassen



Aus für Windows 10?
Jetzt umsteigen und Ihren PC noch jahrelang nutzen!

Linux wie Windows

- Alle Daten weiter nutzen
- Bekannte Tools einsetzen
- WLAN einfach verbinden
- Surfen wie gewohnt

NEU: 2 DVDs!

DVD im Heft

Linux Umsteiger-DVD 2022

Die einfachsten Systeme

1. Linux Mint Edge
2. Elementary OS
3. KDE Neon User Edition
4. LinuxWelt-Rettungssystem



E-Book 1
70 Linux-Systeme im Überblick

E-Book 2
Auf 300 Seiten: LinuxWelt Digital XXL

Extra Download-DVD

Linux Profi-DVD 2022

Linux ohne Grenzen

1. Knoppix 9.1
2. Clonezilla 2.8.1
3. Manjaro Nix Architect 21.2
4. Slax 11.2
5. MX Workbench 21
6. Gparted Live 1.3.1

Die besten Linux-Tools

Auf DVD: Diese Programme braucht Ihr Rechner für Office, Netzwerk, Tuning, Dateimanagement u.v.m.

Mit 1-Klick-Installer auf Heft-DVD

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

PC-WELT

Sonderheft-Abo

Für alle Sonderausgaben der PC-WELT



Sie entscheiden, welche Ausgabe Sie lesen möchten!

Die Vorteile des PC-WELT Sonderheft-Abos:

- ✓ **Bei jedem Heft 1€ sparen** und Lieferung frei Haus
- ✓ **Keine Mindestabnahme** und der Service kann jederzeit beendet werden
- ✓ **Wir informieren Sie per E-Mail** über das nächste Sonderheft

Jetzt bestellen unter
www.pcwelt.de/sonderheftabo oder per Telefon: 0931/4170-177 oder ganz einfach:

1. Formular ausfüllen **2. Foto machen** **3. Foto an idg-techmedia@datam-services.de**

Ja, ich bestelle das PC-WELT Sonderheft-Abo.

Wir informieren Sie per E-Mail über das nächste Sonderheft der PC-WELT. Sie entscheiden, ob Sie die Ausgabe lesen möchten. Falls nicht, genügt ein Klick. Sie sparen bei jedem Heft 1,- Euro gegenüber dem Kiosk-Preis. Sie erhalten die Lieferung versandkostenfrei. Sie haben keine Mindestabnahme und können den Service jederzeit beenden.

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

○ Ich bezahle bequem per Bankeinzug. ○ Ich erwarte Ihre Rechnung.

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PWSJO14130

PC-WELT aus dem Haus IDG Tech Media GmbH, Georg-Brauchle-Ring 23, 80992 München, Registergericht München, HRB 99110, Geschäftsführer: Jonas Triebel.
Die Kundenbetreuung erfolgt durch den PC-WELT Kundenservice, DataM-Services GmbH, Postfach 9161, 97091 Würzburg

Jetzt umsteigen! Auf Linux!

Sie können den Umstieg auf Linux ganz in Ruhe angehen. Auf unserer Heft-DVD finden Sie das beliebte System Linux Mint als sogenanntes Livesystem. Das booten Sie voll funktionsfähig von der Heft-DVD und probieren es gefahrlos aus. Änderungen am PC finden nicht statt. Wenn Sie danach die DVD entnehmen und den Rechner neu starten, ist alles wie vorher.

Vorteile von Linux: Das freie Betriebssystem Linux ist kostenlos, sicher und stabil. Es läuft auf nahezu jedem Rechner und lässt sich individuell anpassen. Eine große Community im Internet hilft gerne bei Fragen, und die meisten Systeme lassen sich vor der Installation als Livesystem testen. Hardware-Beschränkungen wie bei Windows 11 gibt es nicht. Es spricht also alles für einen Linux-Umstieg.

Ratgeber im Heft: In dieser Ausgabe finden Sie alle nötigen Informationen für einen einfachen Wechsel auf Linux – einschließlich der Infos, welche der vielen Linux-Systeme sich für Umsteiger besonders gut eignen und wie Sie Linux und Windows auch parallel nutzen können.

Herzlichst, Ihr

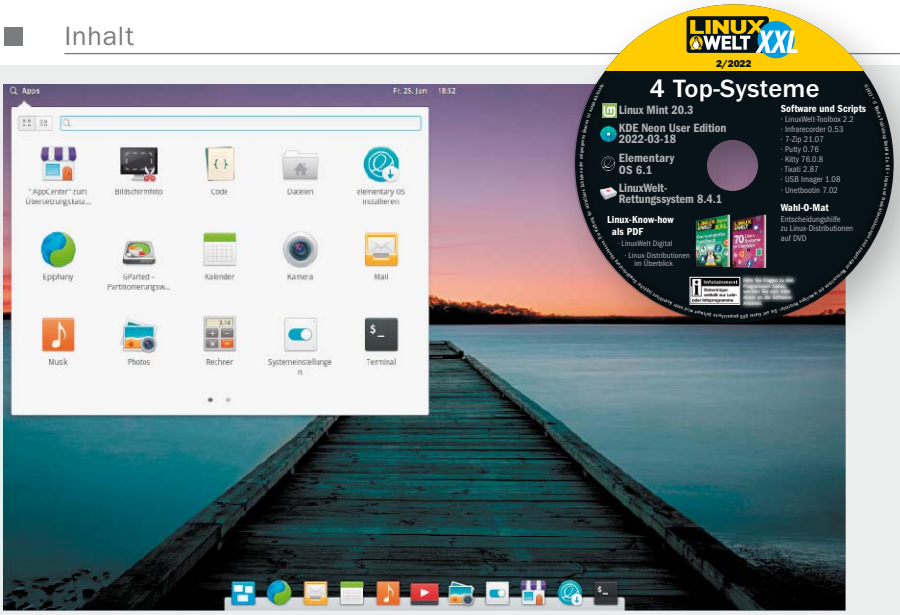


Arne Arnold
Redakteur
aarnold@it-media.de

MINI-ABO LINUXWELT: EIN HALBES JAHR GEBALLTES LINUX-KNOW-HOW!

Wenn Ihnen die LinuxWelt gefällt, können Sie sich das Heft für sechs Monate per Mini-Abo einfach ins Haus schicken lassen. Sie sparen damit satte 33 Prozent und erhalten noch einen Gutschein dazu.
Gratis-Versand: Mit dem Mini-Abo der LinuxWelt bekommen Sie drei Ausgaben der LinuxWelt ohne Versandkosten direkt nach Hause geliefert. In der Regel treffen sie noch vor dem offiziellen Verkaufsstart bei Ihnen ein.
Digitaler Zugriff: Als Ergänzung zum Mini-Abo der gedruckten Hefte bekommen Sie Ihre Ausgaben auch digital auf Ihr Mobilgerät.
33 Prozent sparen plus Gutschein: Mit dem Mini-Abo zahlen Sie nur 18 statt 25,50 Euro. Und zusätzlich erhalten Sie eine Geldprämie oder einen Gutschein über 10 Euro!
Alle Infos: Das Mini-Abo können Sie ganz einfach über *www.pcwelt.de/linux* bestellen. Nach drei Ausgaben verlängert sich das Abo automatisch um ein Jahr (sechs Ausgaben LinuxWelt für zurzeit 53,50 Euro).
Wenn Sie kein Abo möchten, kündigen Sie einfach vor Erhalt der dritten Ausgabe.





Linux: Einfach umsteigen

Für viele Rechner tickt die Uhr. Rigorose Hardwareansprüche von Windows 11 verhindern das Upgrade von Windows 10 und schieben Millionen PCs aufs Abstellgleis. Gut, dass es Linux gibt!

S. 16



Linux wie Windows

So halten Sie Ihr System aktuell und lösen alle Probleme.

S. 46



Linux ist besser

Gegenüber Windows 11 liegt Linux klar in Führung.

S. 14

Im Heft / Auf DVD

6 Hallo Linux, Adieu Windows
Das sind die Vor- und Nachteile von Linux und die besten Tipps zur Wahl des richtigen Desktops auch für ältere Hardware

8 Die Heft-DVD: 4 Top-Distributionen
Zu den vier Linux-Systemen auf der Heft-DVD finden Sie hier ausführliche Informationen und Tipps und Tricks für den Alltag

12 Extra: Download-DVD für den USB-Stick oder die DVD
Auf die Download-DVD haben wir sechs Spezialsysteme für Profis und Fortgeschrittene gepackt



Für Ein- und Umsteiger

14 Linux statt Windows 11
Virtualisierung, Parallelbetrieb, Ersatz: Sie entscheiden über den harten oder sanften Umstieg

16 Linux für Umsteiger
Was Windows-Umsteiger am dringendsten brauchen und welche Distributionen dies erfüllen

18 Linux-Desktops versus Windows 11
Warum Linux-Desktops der Oberfläche von Windows 11 überlegen sind

20 Linux-Desktops: Schick & funktional
Gnome, KDE, XFCE, Cinnamon & Co: Der Ratgeber zeigt die Vor- und Nachteile der Linux-Desktops

26 Linux-Desktops: Tipps & Tools
Tools und Konfigurationstricks optimieren Gnome und KDE Plasma

32 Dualboot und Virtualisierung
Windows soll bleiben? Dualboot ist besonders einfach, Windows-Virtualisierung komfortabler

36 Virtualisierung mit Virtualbox & Vmware
Grundlagen & Tipps: So verbessern Sie Leistung, Sicherheit und Datenaustausch virtueller Systeme

42 Umzug von Daten & Software
Benutzerdateien erhalten: Worauf Sie beim harten Umstieg auf Linux achten müssen

46 Systemtipps für Umsteiger
Diese Linux-Eigenschaften sollte jeder Windows-Umsteiger kennen

48 Installationen & Upgrades bei Mint
Solo, Multiboot & Upgrade: Der Mint-Installer beherrscht noch mehr als diese Standards

52 Linux Mint 20.3
Wir stellen die Neuheiten gegenüber dem Vorgänger vor

56 Linux vs. Windows 11: Hardwarevoraussetzungen
Flexibles Linux: Kompromissloses Windows 11 überlässt Linux ganze Rechnergenerationen

58 Notebooks für Linux
Der Ratgeber zeigt, worauf Linux-Anwender beim Erwerb eines neuen Notebooks achten müssen

Standards

3 Editorial
194 Impressum

Sicherheit für Ihre Daten

120 Datenschutz für Mobilgeräte
Notebooks und USB-Medien verschlüsseln: So wählen und nutzen Sie das optimale Werkzeug

124 Sichere Netzfreigaben
Wie Sie Freigaben in typischen Heimnetzszenarien dosieren

127 Daten in der Cloud
Wie sich Cloud und Datenschutz vereinbaren lassen

130 Open PGP in Thunderbird
Seit Version 78 vereinfacht Thunderbird den Datenschutz

132 Mails sichern und umziehen
Backups und Umzüge für den Mailaustausch: So sichern Sie Mails manuell oder automatisch

135 Eigene Internetdienste
Dyn DNS und Netzwerksicherheit: So überwinden Sie Zugriffshürden und weisen unerbetene Gäste ab

Netzwerk optimieren

138 Neu: Fritz-OS 7.5
Neben Wireguard-VPN kommen zahlreiche Verbesserungen

140 Fritzbox per Kommandozeile
So erreichen Sie fast alle Fritzbox-Funktionen im Terminal

142 Alte Router – neue Rollen
Nicht mehr genutzte DSL-Router anderweitig einsetzen

146 IP-Adressen & Gerätenamen
IPv4-/IPv6-Adressierung müssen Heim-Admins kennen

150 Optimales WLAN
Sichere und schnelle Basis für optimales Funknetz legen

152 Linux-Server fürs Heimnetz
SSH, VNC, Samba, UPnP, Apache

154 Android & iOS: Austausch
So kommen Tablets & Smartphones auf Medien- und Datenserver

Hardware

156 Worauf Sie achten müssen
Das sind die Kriterien für optimale Hardwareunterstützung

160 Datenträger für Linux
Was Sie über SATA, SATA-SSDs und NVMe-SSDs wissen sollten

162 Server, Mini-PCs, Platinen
Der Ratgeber hilft Ihnen, die passende Geräteklasse zu wählen

166 Drucker & Peripherie
Welche Leistung welche USB-Standards wirklich bringen

168 Monitore & Grafikkarten
Was Linux-Nutzer über Grafikchips wissen müssen

172 Externe Geräte an USB
So beheben Sie aufgetretene Fehlfunktionen

174 Firmware & Treiber
So bringen Sie nicht erkannte Hardware zum Laufen

176 Mit Linux recyceln
Linux-Systeme machen alte Rechner wieder flott

178 Akkulaufzeiten optimieren
So halten Notebookakkus länger

180 Besonderheiten bei Festplatten und SSDs
Diese Maßnahmen sorgen für Speed und längere Lebensdauer

182 Mobilgeräte entrümpeln
So schaffen Sie Platz auf Smartphones und Tablets

184 Aufgeräumte Elektronik
Einfache Maßnahmen und preisgünstige Hilfen schaffen Ordnung

186 Fernzugriff und Datenserver
SSH erlaubt neben Terminal-fernwartung auch Datenaustausch

190 Datenserver mit Samba
So konfigurieren Sie Samba und passen bei Bedarf Dateirechte an

Systempflege für Ihr Linux

62 Linux als Dauerläufer
Ubuntu und andere Langzeitsysteme: Nachhaltigkeit beginnt mit der geeigneten Distribution

64 Update- und Upgrade-Guide
Regelmäßige Updates sind Pflicht

68 Rolling Releases
Der Radarcheck zeigt Vor- & Nachteile wichtiger Rolling-Distributionen

72 Systemoptimierung für Linux Mint
So nutzen Sie die Systemzentralen und die Mint-Tools optimal

76 Desktoptuning (Cinnamon)
Hier finden Sie alle Optionen der Oberflächenanpassung

80 Speedtipps für Linux Mint
Systemnahe Leistungstipps: So beschleunigen Sie Updates, Datenträger und Bootzeiten

82 Releases & Kernel-Updates
Distributionen liefern Point Releases, aber auch manuelle Kernel-Updates sind möglich

84 Reparatur- & Spezialsysteme
Pannenhilfe: Diese Spezialisten sind im Notfall alternativlos

88 Separate Home-Partition
Rückversicherung: Unabhängige Home-Verzeichnisse garantieren schmerzfreie Neuinstallationen

90 Mehr Platz auf Datenträgern
Schaffen Sie Platz durch Deinstallation und Löschen

94 Auslagern & Komprimieren
So verlegen Sie Home, VMs, Software und Benutzerdaten

96 Netz & Web: Eine Inventur
Wie Sie Speicher- und Softwaredienste im Netz zentralisieren

Die LinuxWelt-Toolbox

98 Die LinuxWelt-Toolbox
Softwarezentrale der Redaktion: So nutzen Sie die Toolbox

100 Tools für Ubuntu & Mint
Diese Tools sollten auf keinem Desktop fehlen

104 Netzwerk & Internet
Samba, Apache, Fernwartung: So erweitern Sie das Netzwerk mit zusätzlichen Funktionen

108 Multimedia
Wer mehr als pure Wiedergabe benötigt, findet in der Toolbox bewährte Ergänzungen

110 Büroanwendungen
Wo Libre Office nicht ausreicht: Die besten Alternativen

112 Raspberry & Co.
Die besten Systeme, Server- und Streamingprogramme für Mini-PCs

114 Linux-Automatisierung
Autostart, Cron, Scripting: Diese Werkzeuge automatisieren wiederkehrende Standardaufgaben

116 Service- und Livesysteme
Reparatur – Surfen – Sicherheit: Für spezielle Aufgaben lohnt sich der Einsatz externer Livesysteme

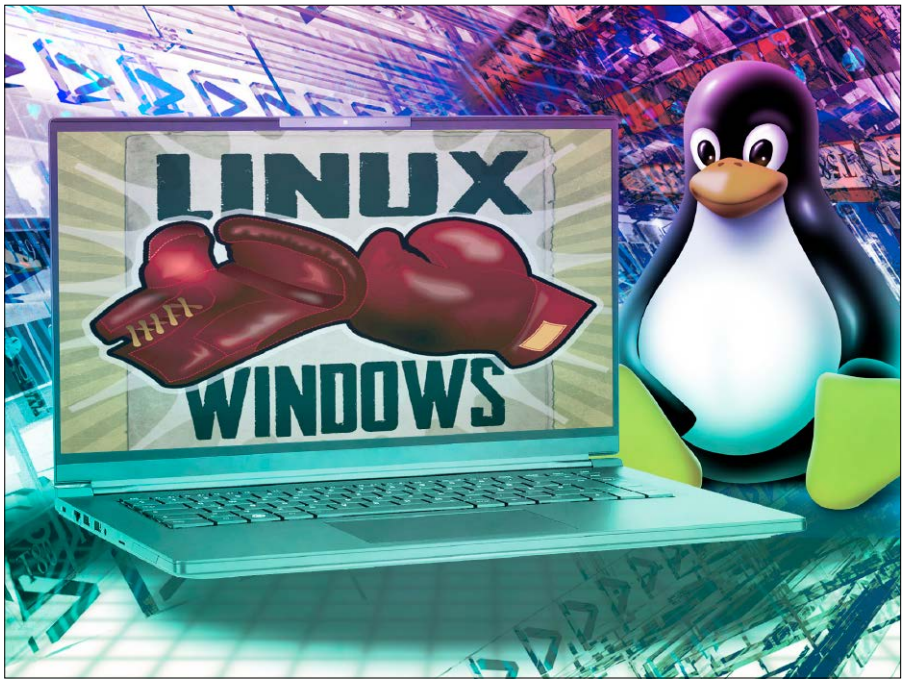
118 Hardwareinfos und -Checks
Was Betriebssysteme nicht preisgeben, ermitteln die hier empfohlenen Werkzeuge



Hallo Linux, Adieu Windows



Die DVD dieses Sonderhefts stellt einige sorgfältig ausgewählte Linux-Distributionen als Alternative zu Windows 10 und 11 vor. Darüber hinaus ist die Heft-DVD eine Quelle an Dokumentation und Hilfestellungen für den gelungenen Umstieg.



VON DAVID WOLSKI

Das war keineswegs von Microsoft geplant und in der Entwicklungsphase von Windows 11 nicht absehbar: Windows 11 kam mit seinen extrem hohen Hardwareanforderungen zur Unzeit – denn Inflation und Lieferschwierigkeiten lassen die Preise für die benötigte Hardware empfindlich in die Höhe schnellen. Unabhängig davon, ob Windows 11 gelungen erscheint oder nicht, interessieren sich viele Anwender wie nach jeder neuen Windows-Ausgabe ernsthaft für Linux als Alternative. Denn es wird nicht für jede Hardware ein nahtloser Umstieg auf Windows 11 in Frage kommen oder gewünscht sein, wenn die Performance dabei sogar bei durchaus noch leistungsfähigen Rechnern auf der Strecke bleibt.

Linux hält Hardware fit

Argumente für Linux und dafür, sich jetzt mit einem Umstieg zu befassen, gibt es also genügend. Aber dieser muss nicht überstürzt sein, denn es bleibt noch Zeit: Windows 10 wird nicht gleich auf das Abstellgleis geschoben. Bis 2025 wird es weiterhin Systemupdates geben. Und abhängig von der Adaptionsrate von Windows 11 bis dahin eventuell auch nochmal außerplanmäßige Flicken für besonders krasse Sicherheitslücken – diese treten bei allen Systemen bisweilen auf, auch bei Linux. Die Aktualisierung von Linux-Systemen ist üblicherweise bei den großen, etablierten und gut gepflegten Linux-Distributionen keine hohe Hürde mehr.

Bei Windows 10 ist ein Sprung auf Windows 11 auf der gleichen Hardware nicht so einfach möglich oder sogar von Microsoft gar nicht vorgesehen, wenn eine Voraussetzung wie TPM-2.0-Chip nicht erfüllt ist. Dann gehören Windows-PCs, die eigentlich noch passabel laufen könnten, zum Alteisen. Und nicht nur das – sie werden zum Sicherheitsproblem. Denn wenn Microsoft die Sicherheitspatches für Windows 10 irgendwann 2025 einstellt, so ist das System voraussichtlich schnell von neu entdeckten Sicherheitslücken in dann schon alten Windows 10 bedroht. Es ist damit zu rechnen, dass Windows 10 dann zum bevorzugten Ziel von Angriffen und Cyberkriminellen wird, so wie zuvor schon Windows XP und dann Windows 7.

Ähnlichkeiten und Unterschiede

Es wäre verkehrt, eine Linux-Distribution als nahtlosen Ersatz für eine Windows-Installation anzupreisen. Denn Linux ist ein Unix-System, vom Aufbau her grundsätzlich von Windows 10/11 verschieden, das auf Windows NT beruht, welches wiederum seine Wurzeln im Betriebssystem VMX von Digital Equipment hat. Linux ist generell modularer, in der Verwendung und Administration sehr unterschiedlich zu Windows.

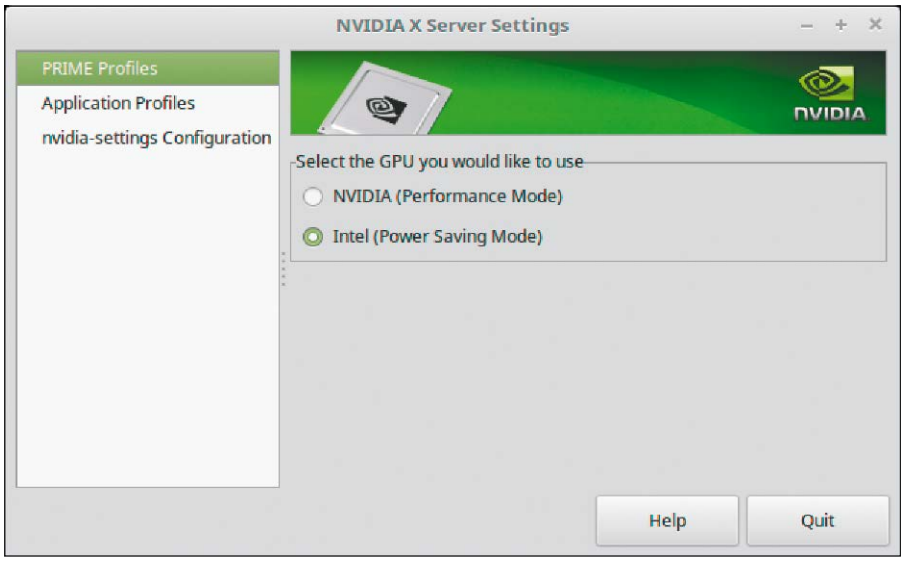
Auch entwickeln sich Linux-Distributionen zwischen Hauptversionsnummern in großen Schritten weiter, sowohl im Betriebssystemunterbau, mit neueren Kernels und vorinstallierten Tools, verfügbaren Softwarepaketen und auf dem Desktop. Das kann einschüchternd wirken.

Dagegen bleibt Windows seinen Anwendungsprinzipien treu. Es geht um Konsistenz, nicht um revolutionäre Änderungen. Was für wenig Überraschungen sorgt, ist aber mal Grund zur Enttäuschung: So sind die die technischen Neuerungen im Unterbau von Windows 11 sehr überschaubar – im direkten Vergleich zu Windows 10 hat sich nicht viel geändert. Aufräumarbeiten und das neue (optionale) Linux-Subsystem WSL2 fallen auf.

Bezüglich der vorhandenen Hardware gibt es beim Umzug von Windows auf Linux kaum Einschränkungen. Wo bislang ein Windows 10 lief, ist generell jede Linux-Distribution geeignet. Die übliche Hardware von Intel und AMD wird von aktuellen Linux-Systemen klaglos unterstützt, denn die tonangebenden Hardwarehersteller und IT-Größen sind mit Entwicklern am Fortschritt und an der Richtung des Linux-Kernels beteiligt. Treiber für Chipsets, neue CPUs und für Standardkomponenten fließen deshalb immer zeitig in den Kernel mit ein. Probleme gibt es eventuell noch bei besonders neuen und wenig verbreiteten Netzwerkchips der Standards 802.11ac (WIFI6) und 802.11ax sowie bei exotischen Notebooks. Bei der Entscheidung und Tests, ob eine Linux-Distribution für den Zielrechner geeignet ist, hilft die Machart der üblichen Linux-Varianten, wie sie auch auf Heft-DVD vertreten sind. Denn es handelt sich um Livesysteme, die erst einmal auch nur zum Desktop booten, der autark ohne Installation zuerst mal zeigt, ob es für die vorhandene Hardware propere Unterstützung gibt.

Das richtige Linux wählen

Wer dennoch ein möglichst flottes und dabei schlichtes Linux-System oder auch einen richtig alten Computer der letzten zehn Jahre wiederbeleben will, kann dies mit der Wahl des passenden Desktops angehen. Denn Linux gibt es auch in besonders ressourcenschonenden Darreichungsformen, beispielsweise mit den Arbeitsumgebungen XFCE, LXQT oder gar dem schlichten LXDE, die jeweils nur wenige hundert MB an Speicher verlangen. Das ermöglicht es, ein voll ausgestattetes Linux-System auch auf Ein-Platinen-Computern wie dem Raspberry Pi auszuführen. Je genügsamer eine Arbeitsumgebung, desto deutlicher fallen in der Bedienung des Desktop auch die Unterschiede zu Windows aus.



Linux-Distributionen stellen ein komplettes System bereit: Für spezielle Chips, etwa eine Nvidia-GPU, ist jedoch die nachträgliche Installation weiterer Linux-Treiber nötig.



Gelungener Umstieg: Die übliche PC-Hardware und Notebooks, hier ein Modell mit Intel-CPU ohne exotische Chipsätze, läuft mit einem aktuellen Linux-System genauso problemlos wie unter Windows 10/11.

Ein Umstieg erfordert aber auch das Lernen anderer Methoden zur Einrichtung und Pflege des Systems, wobei moderne Linux-Distributionen an Komfort wenig vermissen lassen. Die installierbaren Distributionen auf Heft-DVD sind deshalb nach diesen Gesichtspunkern ausgewählt: Einfache Installation, ansprechender Desktop, gute Dokumentation durch eine solide Ubuntu-Basis und schließlich ein breites Angebot an leicht installierbarer Software über bequeme Paketmanager. ■

E-BOOKS ALS PDF: EXTRA VIEL LINUXWELT

Auf der Heft-DVD finden Sie ein E-Book vom März 2022, das die wichtigsten Grundlagenartikel aus der LinuxWelt in einer PDF-Datei bündelt. Hier erfahren Sie Wesentliches über Linux, Administration, die Grundlagen des Betriebssystems und zu Open-Source-Programmen. In mehreren Rubriken wie Hardware, System, Sicherheit, Software, Netzwerk und anderen sind die nach wie vor aktuellen Artikel nach Thema gegliedert. Das PDF-Dokument lässt sich unter Linux, Windows und Mac-OS X lesen. Alles was Sie brauchen, ist ein PDF-Reader wie Evince (Gnome), Okular (KDE) oder Google Chrome/Chromium oder Firefox ab Version 78. Aufgefrischt und mit neueren Artikeln ergänzt sind die Rubriken Grundlagen, Distributionen, Software, Netzwerk und ein passendes Special aus der letzten Ausgabe zum Thema „Umstieg von Windows auf Linux“ ist ebenfalls dabei. In einem zweiten PDF findet sich außerdem der Artikel „Linux-Distributionen im Überblick“ auf 22 Seiten aus der Linux-Welt 5/2021.

Die Systeme auf DVD

Die Heft-DVD präsentiert aktuelle Linux-Systeme, die auf dem Desktop punkten und eine Alternative für Windows sein können. Außerdem gibt es eine neue Version des Rettungs- und Livesystems der LinuxWelt. Alles läuft direkt von DVD.



VON DAVID WOLSKI

Linux im XXL-Format: Auf der beiliegenden DVD geht zum einen um komfortable und gut aufgestellte Desktopsysteme, aber auch ein universelles Livesystem ist dabei, das die LinuxWelt-Redaktion speziell für dieses Heft wieder aktualisiert hat. Alle diese Linux-Varianten sind Livesysteme und booten von DVD beziehungsweise von einem selbst erstellten USB-Stick. Sie tasten ein anderes, schon installiertes Betriebssystem auf einem Computer erst mal nicht an. Dies ist mittlerweile die übliche und bequeme Methode von Entwicklern dieser mit tonangebenden Linux-Distributionen, Desktop, Verwendungsweise und Vorzüge in der Bedienung zu zeigen. Nur wenn das System ansprechend erscheint, geht es dann an die Installation per komfortablen Installationsprogramm. Und das Livesystem der LinuxWelt ist sowieso universell, denn die enthaltenen Tools sind sowohl für Windows- und Linux-Anwender in vielen Szenarien nützlich und von Haus aus für den Livebetrieb ausgelegt.

Der Weg zum laufenden System ist stets kurz: Um eine der Linux-Varianten von der DVD zu starten, legen Sie den Datenträger in das optische Laufwerk und starten den Rechner neu. Booten Sie dabei nicht von der Festplatte, sondern von der DVD. Dazu rufen Sie entweder beim Start per Tastendruck das Bootmenü der Firmware oder des Bios auf, was meist mit der Taste F8 oder F12 gelingt. Oder Sie ändern die Bootreihenfolge im Bios. Welche Taste Sie drücken müssen, verraten die Meldungen am Bildschirm. Die DVD startet nur im Bios-Modus und die Option „CSM/Legacy-Modus“ muss dazu in den Uefi-Einstellungen moderner PCs und Notebooks aktiviert sein. Der Uefi-Boot und Secure Boot werden von der Heft-DVD nicht unterstützt. Ein übersichtliches Multibootmenü stellt alle startfähigen Linux-Systeme zur Auswahl und hat für alle Einträge jeweils noch Untermenüs für die wichtige Startoptionen in petto. Wenn das Notebook oder der PC kein optisches Laufwerk hat, so ist ein bootfähiger USB-Stick in greifbarer Nähe: Aus der DVD lässt sich mit den mitgelieferten Tools auch ein startbarer USB-Datenträger erzeugen, unter Windows, Linux und Mac-OS. Und sollte gar kein Rechner mit optischem Laufwerk zur Verfügung stehen, so gibt das Image unserer DVD auch als Download über Bittorrent. Das ist ein Thema des nächsten Artikels, denn hier geht es zunächst um die Systeme auf Heft-DVD.

Linux Mint 20.3 Edge

Die neue Version des populären Desktop-Linux-Systems basiert noch einmal auf Ubuntu 20.04, genauer auf Ubuntu 20.04.4 vom Februar 2022. Der Zusatz „Edge“ bezieht sich auf den neuen Kernel 5.13, der hier enthalten ist. Neu ist auch eine neue Ausgabe des Cinnamon-Desktops, der mit großzügigeren Titelleisten und abgerundeten Fensterkanten auf hochauflösenden HiDP-Monitoren freundlicher wirken will. Eine neue Funktion in Cinnamon ist eine Kalenderintegration in die Zeit- und Datumsanzeige. Der Kalender arbeitet zunächst mit dem Gnome Calendar zusammen, kann aber auch mit dem Google-Kalender des eigenen Google-Kontos und sogar mit Thunderbird abgeglichen werden. Bei aktivierten Stromsparfunktionen fährt Cinnamon das System bei längerer Inaktivität erst in den Stand-by-Modus und dann später erst in den Ruhezustand herunter. Für häufig besuchte Webseiten und Clouddienste im Browser lassen sich Programmverknüpfungen anlegen, die sich ähnlich wie native Programme verhalten. Flatpaks tauchen auch im Softwaremanager auf und lassen sich dort einfach installieren. Flatpaks bringen ihre eigene Systemumgebung



Frische Minze: Linux Mint 20.3 Edge erneuert Kernel- und Softwareversionen, bleibt bei seiner Systembasis aber Ubuntu 20.04 treu.

mit und laufen isoliert von Systembibliotheken, um eventuelle Konflikte zu vermeiden. Das hat den Vorteil, dass mit Linux Mint 20.3 nun jetzt auch neuere Gnome-Programme installiert werden können, die mit den älteren Bibliotheken des Cinnamon-Desktops nicht kompatibel wären. Snaps von Ubuntu werden in Linux Mint nicht unterstützt.

Wieder enthalten sind die X-Apps von Mint. Dies sind nicht mehr nur Mint-Abspaltungen bekannter Linux-Programme mit neuem Namen, sondern auch Eigenentwicklungen. So hat der Videoplayer Hypnotix zum Abspielen von (freien) TV-Streams aus dem Internet ein Update erhalten und zeigt nun Länderflaggen zu den Angeboten an. Das Programm Thingy zeigt die zuletzt verwendeten Dokumente in einem Dateibrowser an. Die Notizblockanwendung Sticky Notes für den Desktop hat eine Suchfunktion erhalten. Von diesen Entwicklungen abgesehen, entspricht Linux Mint 20 weitgehend dem Stand von Ubuntu 20.04 und bringt Libre Office 6.4 mit, aber auch den neuesten Firefox. Linux Mint 20.3 Edge liegt als leicht installierbares Livesystem vor. Das Installationsprogramm entspricht jenem von Ubuntu 20.04.3, bietet aber keine Option zur Verwendung des Dateisystems ZFS an, zumal dies sowieso eher für Server und Storagesysteme interessant ist. Wer Linux Mint 20.3 schon installiert hat, muss das System nicht neu installieren, weil es sich um einen Point Release handelt.

Website: *https://www.linuxmint.com/edition.php?id=296*

Dokumentation: *https://linuxmint.com/rel_elsie.php*

Elementary OS 6.1

Es gibt gewiss keinen Mangel an Arbeitsoberflächen für Linux-Systeme. Was Elementary OS aber schon immer, seit den ersten Ausgaben, anders macht, ist die Bündelung von Desktop und zugehörigen

EXTRAS UND TOOLS AUF DVD

Zum Starten liegengebliebener Linux- und Windows-Systeme, zur Fehleranalyse, zum sicheren Löschen von Festplatten bietet das Multibootmenü der DVD in der Rubrik „Extras und Tools“ eine Reihe an kleineren Livesystemen und startfähigen Werkzeugen an.

Netboot.xyz 2.0.57: Dieses bootfähige Tool ist selbst keine Linux-Distribution, sondern ein Bootprogramm, das eine große Auswahl von Linux-Systemen per Menü anbietet, von Github in den Arbeitsspeicher herunterlädt und startet. Netboot.xyz basiert auf iPXE und arbeitet auf regulärer PC-Hardware mit Ethernet-Verbindung ins Internet.

Shred-OS 2021.08.2: Aufgefrischt: Dieses winzige Livesystem startet ein Menü im Textmodus, um Daten auf magnetischen Datenträgern endgültig zu überschreiben. Auch Wiederherstellungstools können dann nichts mehr rekonstruieren. Auf Festplatten arbeitet Shred-OS sehr zuverlässig. Für Flashmedien (USB-Sticks, SSDs, NVMEs) ist das Tool allerdings nicht geeignet. Shred-OS startet im Uefi- sowie Bios-Modus.

Super Grub Disk 2.04: Das startfähige Tool liefert eine Boothilfe für Linux-Systeme, bei welchen der Bootloader vom Typ Grub 2 nicht mehr intakt ist oder von Windows überschrieben wurde. Es läuft im Bios- sowie Uefi-Modus.

Hardware Detection Tool 0.5.2: Einen Überblick zur kompletten Hardware eines Systems bietet das startfähige Hardware Detection Tool, auch wenn noch kein Betriebssystem installiert ist. In einem englischsprachigen Menü zeigt HDT Kategorien wie PCI, RAM, Prozessor und Bios an. Das Programm läuft nur im Bios-Modus.

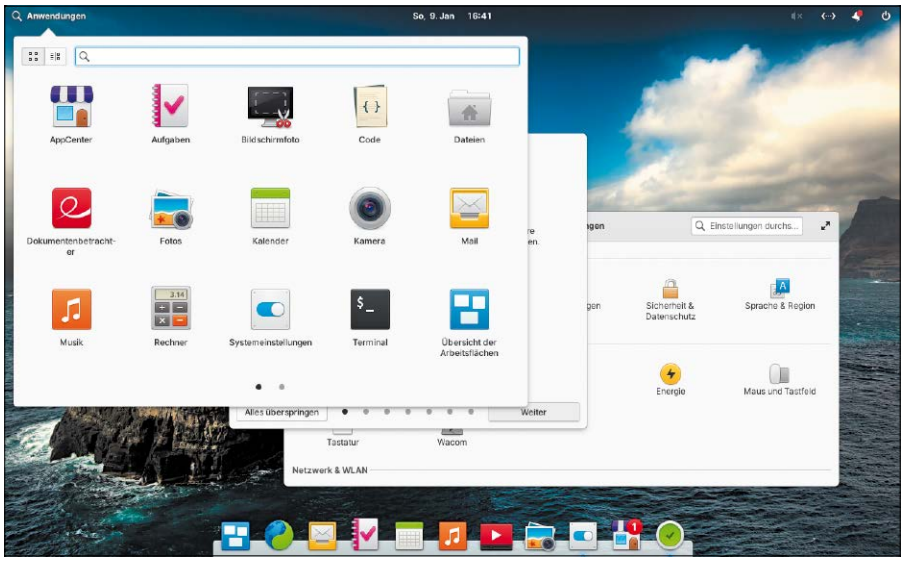
Memtest 86+ 5.31b: Das Testprogramm für den Arbeitsspeicher zeigt sich im Multibootmenü bei einem Start der DVD im Bios-Modus. Memtest 86+ 5.31b testet auch neue DDR4-Module auf Fehler, unterstützt aktuelle 64-Bit-CPUs sowie alle verbreiteten Speichertypen der x86-Architektur. Es beginnt sofort nach dem Start mit den Tests, die jederzeit unterbrochen werden können.

Plop Bootmanager 6: Der Plop Bootmanager verfügt über einen einen eigenen Treiber für USB-Geräte und CD/DVD-ROM-Laufwerke. So kann dieser Bootmanager von diesen Laufwerken booten, auch wenn es das Bios des PCs nicht unterstützt. Das Tool startet nur im Bios-Modus.

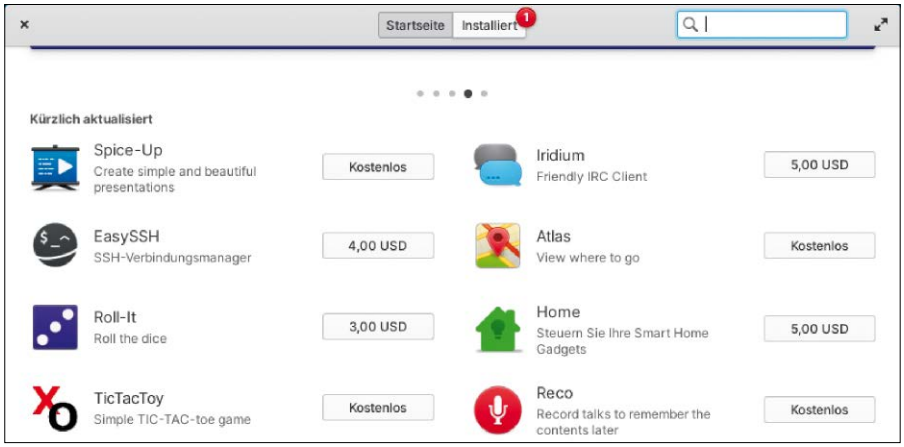
Plop Kexec 1.6: Dies ist eine spezialisierte Variante des Plop Bootmanagers, die auch im Uefi-Modus funktioniert und zum Boot von Linux-Systemen auf USB-Sticks dient, wenn diese nicht als als bootfähig erkannt werden. Dieses Werkzeug zeigt zunächst nur eine Statusanzeige im Textmodus an. Sobald jetzt ein USB-Datenträger mit einem bootfähigen Linux-System angeschlossen wird, erkennt Plop Kexec dessen Bootmenü und zeigt die Einträge in seinem eigenen Menü an.



Die bootfähigen Extras und Tools auf der Heft-DVD: Nur im Bios-Modus stehen alle Werkzeuge zur Verfügung, bei einem Boot unter Uefi nur jene, die diesen Modus unterstützen.



Ein Hauch von Mac-OS: Elementary OS steht auf den Schultern von Ubuntu 20.04 LTS und Gnome, geht auf dem Desktop und mit seinen vorinstallierten Anwendungen aber ganz eigene Wege.



Eine Spezialität in Elementary OS: Der App Store ist jetzt wieder besser gefüllt. Bei einem Klick auf einen Eintrag gibt es ausführliche Informationen zum Paket.

Anwendungen, die einen Hauch von Mac-OS auf Linux-Rechner bringen. Diese Unternehmung gelingt nicht nur durch die Lust an der Sache, sondern auch durch das Konzept von Elementary OS, einen eigenen App Store zu pflegen. Dort gibt es nicht nur Open-Source-Programme aus den üblichen Ubuntu-Repositorys und PPAs (Extra-Paketquellen von Entwicklern), sondern eine gepflegte Liste an Anwendungen, die auch mal Geld kosten können. Das ist allerdings keine Voraussetzung, denn auch die üblichen Paketquellen Ubuntus liefern in Elementary OS die üblichen Programme frei Haus, zumal als Betriebssystembasis ein Ubuntu 20.04.3 arbeitet. Ambitioniert wie immer lieferte das kleine, sehr engagierte Entwicklerteam eine neue Version des eigenen, in Vala programmierten Desktops „Pantheon“ mit dunklem Thema und anpassungsfähigen farblichen Akzentuierungen und Multitouch-Gesten zur Bedienung auf neuen Laptops. Kalender und Dateimanager bekamen neue Features für Poweruser und ein Firmwareupdater wurde von Gnome übernommen. Die tiefgreifende Neuerung war aber die Aufnahme von Flatpaks in den eigenen App Store, um zusätzliche Anwendungen samt Bibliotheken in Containern bereitzustellen. Auch der App Store ist jetzt mit über 90 Programmen sowie Flatpaks gut gefüllt. In der Kommandozeile steht, wie auf jedem Ubuntu, sowieso auch apt bereit und holt Software aus den Paketquellen von Ubuntu 20.04 LTS – also zuweilen auch ältere Versionen.

Elementary OS hat den Ubuntu-Installer stark als Abspaltung umgebaut und den Ablauf der Installation geändert. Das Livesystem startet zunächst mit der Auswahl der Sprache und dem Textmodus, welcher einem Livesystem entspricht, oder der Installation. Der Installationsvorgang ist vereinfacht und fragt nicht nicht zuerst nach Details wie gewünschten Benutzernamen, Passwort und Hostname. Diese Abfrage erfolgt erst nach dem ersten Boot nach der Einrichtung auf dem Datenträger.

Website: *https://elementary.io/de*

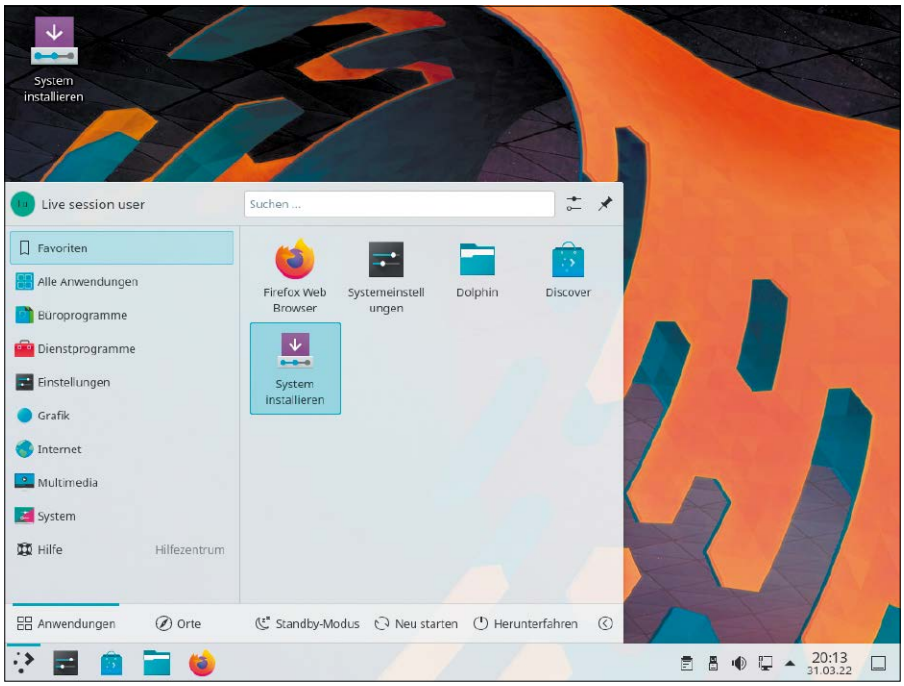
Dokumentation:
https://elementary.io/de/support

KDE Neon User Edition

KDE Plasma ist einer der perfekten Desktops für fortgeschrittene Anwender, die gut mit einem opulenten Funktionsumfang zurechtkommen und die Arbeitsumgebung gerne bis ins Detail selbst konfigurieren. KDE Neon ist das laufend aktualisierte Vorzeigesystem für KDE Plasma, zumal zu dieser Distribution auch einige KDE-Entwickler und ehemalige Kubuntu-Köpfe gehören. In der vorliegenden Ausgabe nutzt KDE Neon als Unterbau noch Ubuntu 20.04, liefert aber einen frischen Desktop. Und mit diesen Eigenschaften hat sich die KDE Neon heute, sechs Jahre nach seiner Ersterscheinung, seinen festen Platz unter den gut gepflegten inoffiziellen Ubuntu-Varianten erobert und wurde noch vor Kubuntu zur wichtigsten KDE-Distribution.

Auf Heft-DVD liegt die stabile User Edition dieser Distribution als alltagstaugliches Desktopsystem. Diese Mixtur aus stabiler Ubuntu-Basis bietet einige Vorteile gegenüber anderen Distributionen, denn KDE Plasma 5 entwickelt sich auch immer noch schnell weiter. Eine Distribution wie Kubuntu oder Open Suse Leap kann dabei nicht immer Schritt halten. In der vorliegenden Ausgabe der KDE Neon User Edition mit Langzeitsupport ist KDE Plasma 5.24 enthalten. Die KDE-Komponenten werden auch in der vorliegenden User Edition teilweise als Rolling Release gepflegt – das heißt, KDE-Komponenten bekommen laufende Updates, während der Ubuntu-Kern bei den erprobten Programmversionen der letzten LTS-Ausgabe bleibt. Mit KDE Plasma 5.24 tut diese Desktopumgebung einen Riesenschritt auf den neuen Displayserver Wayland zu, der in den kommenden KDE-Versionen zum Standard werden soll.

Der Installer ist eine KDE-Version von Calamares, der auch in Kubuntu und Lubuntu



Bereitet sich auf Wayland vor: In KDE 5.24, welches in der KDE Neon User Edition als Desktop enthalten ist, funktioniert der neue Unterbau der grafischen Oberfläche schon fast problemlos.

die Einrichtung auf Festplatte übernimmt. Das installierbare Livesystem enthält deutsche Sprachpakete und bietet die gesamte Oberfläche auch in Deutsch an. Vorinstalliert werden neben KDE-Programmen nur Firefox und VLC. Für die weitere Ausstattung gibt es den grafischen Paketmanager Plasma Discover und zur Installation stehen alle Programmpakete aus den Quellen Ubuntus 20.04 bereit.

Website: *https://neon.kde.org*

Dokumentation: h*ttps://neon.kde.org/faq*

LinuxWelt-Rettungssystem 8.4.1

Das LinuxWelt-Rettungssystem 8.4.1 tritt mit dem Anspruch an, ein möglichst unkompliziertes und dabei kompaktes Livesystem mit aktuellen Werkzeugen, Partitionierer und Browser von DVD zu starten. In dieser Ausgabe stehen deshalb auch Gparted 1.3.1, die Kommandozeilentools Testdisk, Photorec und Ext4magic zur Wiederherstellung gelöschter Dateien im Mittelpunkt sowie das Datenträger-Imaging-Programm Clonezilla und der Verschlüsseler Veracrypt 1.24. Als Browser liegen Firefox 98.0.2, Chrome 100, und Opera 74 vor. Der schlanke Mate-Desktop, Browser und der Partitionierer Gparted liegen in deutscher Sprache vor. Kleinere, aber wichtige Tools in der Shell wie der Portscanner Nmap und das Rettungstool ddrescue zum Erstellen von Datenträgerabbildern ergänzen das neue System. Es gibt zwei Eigenentwicklungen der LinuxWelt-Redaktion im Livesystem, unter „Anwendungen → Systemwerkzeuge“ zum sicheren Löschen von SSDs („SATA Secure Erase“) sowie für NVMEs („NVME Secure Erase“).

Auch wenn sich diese Tools und die Kommandozeilenprogramme testdisk, photorec, ext4magic als auch ddrescue an fortgeschrittene Anwender richten, so ist die Oberfläche des Livesystems einladend und einfach gehalten. Nach dem Start des Mate-Desktops wartet der übliche Network-Manager rechts oben darauf, eine WLAN-Verbindung aufzubauen. Zu den grafischen Programmen finden sich in der oberen Leiste des Mate-Desktops Verknüpfungen für den bequemen Zugriff auf die wichtigsten Programme. Es sind NTFS-Treiber mit an Bord und der Dateimanager kann Windows-Partitionen damit direkt öffnen. Der Kernel ist auf Version 5.16.10 gehievt.

Das Rettungssystem kann dank Mate auf dem Desktop recht genügsam mit Ressourcen haushalten. Es läuft bereits auf einer 64-Bit-CPU der letzten 15 Jahre und einem GB RAM anständig. Ab mehr als zwei GB Arbeitsspeicher, also auf halbwegs aktuellen Rechnern, kann das Livesystem im Multibootmenü komplett in den Speicher geladen werden und läuft dann extrem flott.

Das Livesystem liefert unter „Anwendungen → Systemwerkzeuge → Bootfähigen USB-Stick erstellen“ ein Programm mit, um das Livesystem auf einem USB-Stick oder einem Wechselmedium bootfähig einzurichten. ■



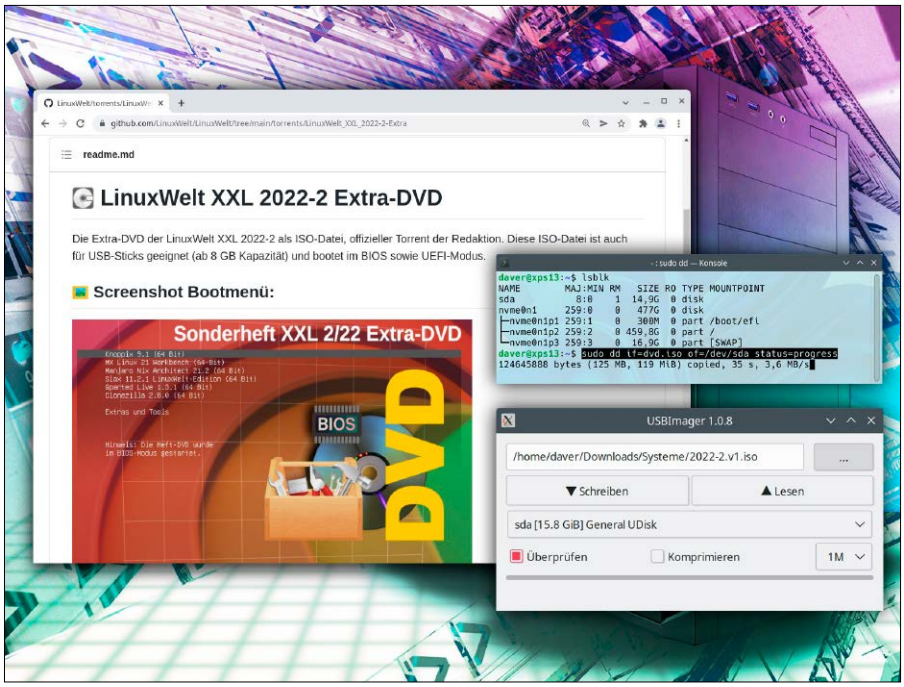
Aufgefrischt: Das LinuxWelt-Rettungssystem basiert jetzt auf der Slackware-Variante Aporteus und ist mit vielen nützlichen Tools und mit neuen Browsern auf der Heft-DVD vertreten.

Download-DVD für USB-Sticks



Zusätzlich zur Heft-DVD gibt es eine Download-DVD, die nicht dem Heft beiliegt, sondern als Bittorrent-Download vorliegt (4,7 GB). Diese Extra-Scheibe versammelt Spezialsysteme und Linux-Distributionen für fortgeschrittene Anwender und interessierte Nutzer.

VON DAVID WOLSKI



Die letzte Ausgabe des XXL-Sonderhefts präsentierte schon eine Heft-DVD, die sich nach einer Umwandlung zurück in ein ISO-Image auch auf einen USB-Stick übertragen lässt, um einen Rechner davon zu booten. Möglich macht dies der Bootloader 2.06, der für unsere Multibootumgebung sorgt und in dieser Ausgabe ein wichtiges Update erhalten hat, um Unverträglichkeiten mit Bios- und Uefi-Systemen zu beheben. Nützlich ist dies nicht nur bei PCs ohne optisches Laufwerk – die Systeme booten von USB auch bedeutend schneller. Die Übertragung klappt auch wieder mit dieser Heft-DVD.

Auslesen und Übertragen

In Linux und Mac-OS eignet sich zum Auslesen der DVD und zum Schreiben des Images auf USB-Sticks einfach das vorinstallierte Kommandozeilentool dd. Um aus der eingelegten Heft-DVD im Laufwerk „/dev/sr0“ die rund 8,5 GB große Imagedatei „dvd.iso“ im aktuellen Verzeichnis zu erzeugen, dient folgende Befehlszeile, die eine Fortschrittsanzeige präsentiert:

```
sudo dd if=/dev/sr0 of=dvd.iso
  status=progress
```

Windows: Auf Heft-DVD findet sich zum Auslesen unter Windows das Open-Source-Programm Infrarecorder 0.53 (Download unter *http://infrarecorder.org*, 4–5 MB, englischsprachig).

Nach dem Start auf der Oberfläche auf „Actions → Copy Disc → to a Disc Image“ und nach der Eingabe des gewünschten Dateinamens der Imagedatei und einem Klick auf „OK“ geht es los. Dieser Vorgang dauert einige Minuten. Auf dem Zieldatenträger verlangt die Datei etwa 8,2 GB an Speicherplatz.

Dieses Image ist für gewöhnliche DVD-Rs sowie für USB-Sticks ab acht GB geeignet und kann beispielsweise mit dem USB Imager 1.08 (auf Heft-DVD, Download aller Versionen unter *https://gitlab.com/bztsrc/usbimager*) unter Windows, Linux und Mac-OS auf das Zielmedium übertragen werden. Der vorbereitete USB-Stick bootet jetzt zuverlässiger im Bios- sowie Uefi-Modus und zeigt wie die Heft-DVD ein Multibootmenü mit allen Booteinträgen für die folgenden sechs Livesysteme an.

Die Download-DVD

Nicht nur die reguläre Heft-DVD gibt es auch jetzt wieder zum Download (siehe gleichnamiger Kasten) per Bittorrent. Auf die gleiche Weise stellen wir ein zusätzliches Image bereit, das einige Livesysteme in einer komfortablen Multibootumgebung zusammenfasst.

Knoppix 9.1: Dieses Livesystem ist ein echter Klassiker, erscheint seit über 20 Jahren und liegt hier in der deutschsprachigen Variante in CD-Größe vor. Auf 700 MB versammelt Knoppix den Chromium-Browser, grafische Dateimanager, Dokumentenbetrachter und grundlegende Linux-Tools unter einer schlanken LXDE-Oberfläche.

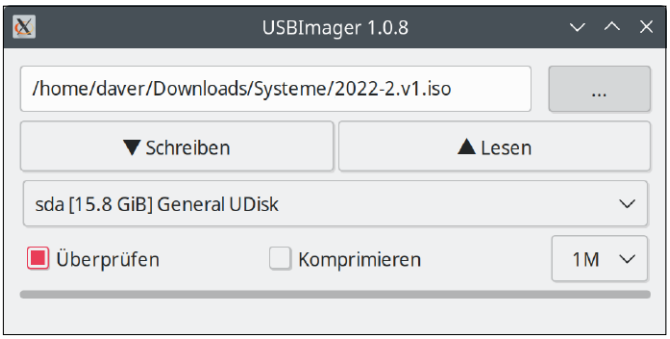
Manjaro Nix Architect 21.2: Das installierbare Livesystem im Textmodus erlaubt eine weit detailliertere Konfiguration eines Zielsystems mit Manjaro Linux, einem Arch-Linux-Derivat für Fortgeschrittene. Aber keine Sorge, der mitgelieferte Installer entspricht nicht der puristischen manuellen Installation im Stil eines Arch Linux. Denn der englischsprachige Installationsprozess fragt über seine Textmenüs Schritt für Schritt die notwendigen Einstellungen ab. Auch hat Manjaro Architect eine Vielzahl installierbarer Desktops zur Auswahl.

Clonezilla 2.8.1: Das Backuptool für ganze Festplatten oder auch nur einzelne Partitionen schreibt Abbilder in komprimierte Imagedateien, die es entweder lokal auf einer anderen Festplatte speichert oder auf einem USB-Medium und sogar per SSH oder Samba auf einem Server im Netzwerk. Es erkennt alle verbreiteten Dateisysteme aus dem Umfeld von Windows und Linux. Die Backupimages kann Clonezilla gepackt als Dateien speichern und zu einem Umzug eine Festplatte 1:1 klonen.

Slax 11.2.1: Ein ansehnliches Minisystem zum Surfen mit den Browsern Firefox ESR und Chromium bringt das schlanke und flotte Livesystem Slax auf den Desktop. Es fühlt sich auch auf richtig alten Rechnern noch wohl, bootet blitzschnell und zeigt eine schlichte, ansprechende, englischsprachige Oberfläche. Zunächst ist auch noch das US-Tastaturlayout aktiv, was ein Rechtsklick auf den Denktophintergrund im Menü „Keyboard Layout → German“ nach ändert.



Sammlung nützlicher Livesysteme: Die Extra-DVD bringt in einem Image, das auch für USB-Sticks geeignet ist, diese sechs weiteren Systeme unter und liegt auf Github als Bittorrent-Download vor.



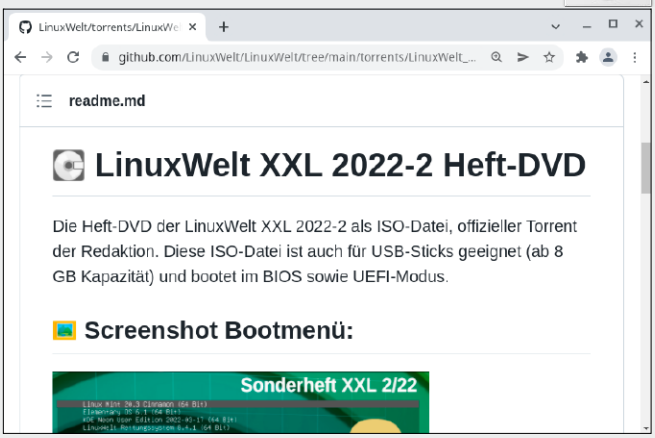
Der USB Imager: Dieses Open-Source-Programm (verfügbar für Linux, Windows und Mac-OS) ist ein grafisches Tool zur Übertragung von Imagedateien auf USB-Sticks und Speicherkarten.

Gparted Live 1.3.1: Der mächtige Partitionierer Gparted darf auf keiner bootbaren Toolsammlung fehlen und ist auch in anderen Livesystemen enthalten. Dies ist aber die offizielle Ausgabe der Gparted-Entwickler in einem kompakten System.

MX 21 Workbench: Hier präsentiert sich ein universeller Werkzeugkasten in einem Livesystem mit übersichtlicher Präsentation aller Tools gleich nach dem Start. Unter anderem finden sich hier Festplattentools wie Photorec und Testdisk. Auch der leicht in jeder Sitzung aktualisierbare Virenscanner Clam TK ist mit von der Partie. ■

DOWNLOAD: DVDS ALS IMAGEDATEIEN

Der Umfang der Download-DVD ist mit 4,7 GB zu groß, um das Image einfach als Download anzubieten. Besser ist dazu das Protokoll Bittorrent geeignet, das die Netzwerklast auf mehrere unserer Server verteilt. Die Torrent-Datei und einen Magnet-Link mit einer unkorrumpierbaren Checksumme hat die LinuxWelt-Redaktion erstellt und auf der eigenen Github-Seite unter *https://github.com/LinuxWelt/LinuxWelt/tree/main/torrents* hinterlegt. Mittlerweile liegen dort auch die Heft-DVDs aus der LinuxWelt zurück bis zur Ausgabe 1/2022 jeweils als Image mit aktualisiertem Bootloader, der die Kompatibilität zu Firmwares im Bios- und Uefi-Modus verbessert hat. Der Klick auf einen der Einträge auf unserer Github-Seite führt dort zur einer kurzen Dokumentation und Downloadanleitung. Unter Windows eignet sich zum Download eines der ISO-Images das Freewareprogramm Tixati 2.87 (2.86 (Freeware, Download unter *https://www.tixati.com/download*, 16 MB, auf Heft-DVD, englischsprachig) und in Linux die meist schon vorinstallierten Bittorrent-Clients Transmission (Gnome) oder Ktorrent (KDE).



Die Bittorrent-Downloads der LinuxWelt bei Github: Auf unserer Seite finden Sie zu den Heft-DVDs und zur Extra-DVD des Sonderhefts jeweils die benötigten Bittorrent-Dateien und Magnet-Links.

Linux statt Windows 11: Umzugsstrategien

Für viele Rechner tickt die Uhr. Rigorose Hardwareansprüche von Windows 11 verhindern das Upgrade von Windows 10 und schieben Millionen brauchbarer bis sehr guter PCs und Notebooks auf das Abstellgleis. Gut, dass es Linux gibt!



VON HERMANN APFELBÖCK

Es ist ärgerlich bis skandalös, auf welcher Hardware Windows 11 Installation oder Upgrade verweigert. Selbst fast neuwertige und gut ausgestattete PCs und Notebooks sind betroffen, auf denen aktuell – das technisch kaum unterscheidliche – Windows 10 bestens läuft. Dabei klingen die Forderungen erst mal ganz moderat: Dualcore-CPU mit mindestens einem GHz, vier GB RAM, Secure-Boot-Uefi und TPM 2.0. Wer es aber nach Installation der „PC-Integritätsprüfung" genauer wissen will, wird feststellen, dass auch i7-Quadcore-CPUs mit 2,6 GHz durch die Prüfung fallen – siehe Abbildung. Natürlich kursieren inzwischen Registryeinträge (mehr falsche als richtige), die eine Prüfung einzelner oder aller Kriterien unter den Tisch fallen lassen. Aber ob man das wirklich will? Zumal Microsoft derzeit vage bleibt, ob es dauerhaft Updates für ein Windows 11 ausliefern will, das auf diese Weise quasi „unautorisiert" installiert wurde.

Immerhin bleibt Zeit

Wenn Sie aktuell ein Windows 10 auf einem vom Nachfolger nicht unterstützten Rechner nutzen, dann ist es Zeit für strategische Überlegungen. Eile besteht nicht, denn Windows 10 wird noch bis 2025 mit Updates versorgt. Aber wenn jüngere Hardware voraussichtlich weit über 2025 hinaus ordentliche Leistung bringen wird, sollten Sie sich ab sofort mit Umstiegsstrategien auseinandersetzen. Sobald Microsoft die Sicherheitsupdates für Windows 10 einstellt, ist das System durch Sicherheitslücken bedroht. Daher ist damit zu rechnen, dass Windows 10 ab 2025 zum bevorzugten Ziel von Hackern wird. Das von Microsoft festgelegte Ende der Nutzungsdauer bedeutet aber nicht das Ende der Nutzbarkeit. Sie können das System samt Software weiter produktiv nutzen, allerdings ohne Verbindung zum Internet. Auf nachträgliche Softwareinstallationen sollte dann verzichtet werden und muss, falls unvermeidlich, aus vertrauenswürdigen Quellen stammen.

Harte und sanfte Umzugsstrategien

Linux statt Windows? Linux neben Windows? Sollen Sie das alte Windows komplett ersetzen oder parallel am Leben lassen? Auf den folgenden Seiten geht es um die Auswahl der richtigen Linux-Distribution, dann um die Optionen eines Dualboot-Betriebs oder einer virtuellen Maschine, um Softwarependants unter Linux und natürlich auch um den Erhalt aller Benutzerdaten. Wie radikal oder behutsam Sie den Windows-Einsatz beenden oder reduzieren, hängt vor allem davon ab, welche Software Sie unbedingt brauchen und welche Softwareformate Ihr System bearbeiten muss.

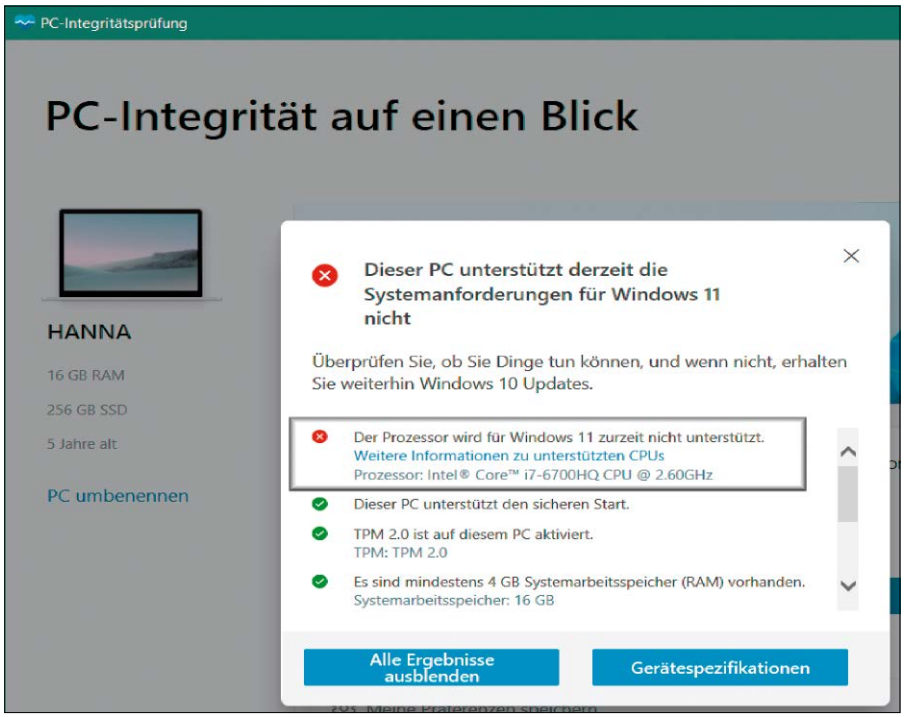
A. Windows komplett durch Linux ersetzen: Diese Variante ist die einfachste. Sie kommt für jedes Gerät in Betracht, wo weder aktuell noch künftig Softwareprodukte wie Microsoft Office, Adobe Photoshop, Adobe Indesign, Autocad sowie diverse Windows-only-Spiele laufen sollen. Diese Liste ist sicher durch Exoten erweiterbar, aber in der Masse ist es Microsoft- und Adobe-Software plus Gaming, was die Nutzer zu Windows zwingt. Dass alle allgemeinen Aufgaben (Internet, Mail, Audio, Video, Foto, Office-Austauschformate) Linux ausgezeichnet erledigt, ist ab Seite 42 detailliert erklärt. Vor einem solchen Umstieg auf Linux müssen alle Benutzerdaten unter Windows auf einen externen Datenträger gesichert werden, um sie später unter Linux wieder ins System zu kopieren.

B. Linux und Windows im Dualboot: Eine Parallelinstallation neben Windows wird bei allen empfohlenen Linux-Distributionen beim Setup direkt angeboten und ist technisch einfach, wenn man ein paar Regeln beim Booten beachtet. Diese Variante ist vor allem dort zu empfehlen, wo Win-

dows weiterhin die volle System- und Grafikleistung erhalten soll, also insbesondere für installierte Spiele. Für häufige Office- und Publishingarbeiten kann die Notwendigkeit, stets das System zu wechseln, lästig werden. Dualboot setzt außerdem voraus, dass für zwei Systeme ausreichend SSD- oder Festplattenspeicherplatz zur Verfügung steht. Und noch ein Hinweis: Wenn das Windows abgelaufen ist, müssen Sie im Windows-System den oder die Netzwerkadapter abschalten („Systemsteuerung → Netzwerk → Netzwerkverbindungen“).

C. Windows als virtuelle Maschine unter Linux: Ein bestehendes Windows-10-System kann komplett in eine virtuelle Maschine umgewandelt werden und als solche unter Linux laufen (siehe ab Seite 36). Das bietet gegenüber Dualboot erhebliche Komfortvorteile. Außerdem ist es möglich, ein künftig abgelaufenes virtuelles Windows über den Router für das Internet zu sperren (etwa in der Fritzbox unter „Internet → Filter“), ohne das Hostsystem zu beschränken. Auch eine virtuelle Maschine erfordert natürlich ordentlich Speicherplatz, tendenziell aber weniger als eine Dualboot-Lösung. Allerdings kommt Virtualisierung nur für leistungsfähige Hardware in Betracht. Ab acht GB RAM und Vierkern-CPU sind produktives Office & Co. in einer Windows-VM eine ideale Lösung, Spiele hingegen eher nicht.

D. Linux und Windows im Netzwerk-Team: Dank Netzwerk muss nicht mehr jedes System als Solist und Universalmaschine mit allen Programmen und Daten arbeiten. Ein Windows 10 oder 11 in der Pro-Version (nicht Home!) bietet den Remotedesktop-Serverdienst – siehe „Remote“ unter „Einstellungen“ (Strg-I). Damit holt sich jedes Linux bei Bedarf ein Windows mit einem Word oder Photoshop auf den Bildschirm. Das einschlägige Clientprogramm Remmina ist bei vielen Distributionen standardmäßig an Bord. Die Nachteile dieses Rechner-Teamworks sind in einem Homeoffice durchaus tolerierbar: Der Windows-Rechner muss immer laufen und bei Bedarf von einem lokalen Nutzer auf Zuruf freigegeben werden. Für gute Leistung und Optik ist Ethernet oder Powerline zu empfehlen, WLAN eher nicht. ■



Ein Top-Notebook – aber nicht gut genug für Windows 11: Warum Windows 11 auf solcher Hardware nicht laufen will, entbehrt jeder Ressourcen-Logik.

IST WINDOWS 11 EIN PFLICHTUPGRADE?

Einige Sätze zu Windows 11 können wir uns in der LinuxWelt nicht verkneifen. In der „Windows-Welt“ wird wortreich diskutiert, wie leistungsstark, nützlich, innovativ Windows 11 zu beurteilen sei. Ob also, falls die Hardware ausnahmsweise mitmacht, das Upgrade von Windows 10 ratsam ist. Nach unserer Einschätzung ist das einzige ernsthafte Upgrademotiv, dass das System dann wieder jahrelang Sicherheitsupdates erhält. Hübsche Fensteroptik und Schriften sowie manche optimierte Benutzerführung wird erkauft durch Reduktion und Minimalismus. Wer vorher in einer vertikalen Windows-10-Taskleiste alle Möglichkeiten benutzerspezifischer Systemleisten genutzt hat, steht auf dem Desktop nach dem Upgrade auf Windows 11 vor einem Neuanfang. Allein die Tatsache, dass auf heutigen 16:9-Monitoren keine vertikale Anordnung der Leiste möglich ist, ist unzeitgemäß und kontraproduktiv. Dass fundamentale Explorer-Optionen wie „Senden an“ in einen Unterdialog gewandert sind, ist ebenso unverständlich.

Und sonst? Technisch bietet Windows 11 definitiv nichts Neues. Oder doch? Ja – Nutzer der Home-Version werden jetzt zu einem Online-Systemkonto gezwungen, damit Microsoft jede Systemanmeldung mitprotokollieren kann. Diese Tatsache ist (neben Remotedesktop-Server und Bitlocker) ein ernstes Motiv für die Wahl der teureren Pro-Edition.

Die Rückkehr der Desktop-Widgets soll wohl dafür sorgen, dass Microsofts Edge-Browser fleißig genutzt wird, selbst wenn der Nutzer eigentlich einen anderen Browser verwendet: Besser gleich abschalten! Wenn dann noch kleinere Hakeleien dazukommen wie in unserem Fall fehlender HDMI-Sound (irgendwann wird wohl ein Treiberupdate ankommen und helfen), dann bedauert man, sich das Rollback zu Windows 10 durch vorschnelles Tabula Rasa mit der Datenträgerbereinigung verbaut zu haben.

Nein! Windows 11 ist kein Pflichtupgrade. Es ist ein lauter Weckruf, sich mit Linux-Alternativen zu befassen.

Linux für Umsteiger

Ein Linux für Windows-Umsteiger sollte unkompliziert und attraktiv sein und möglichst lange ohne Neuinstallation auskommen. Zusätzliche Windows-Analogien am Desktop und im Dateimanager können für rasche Heimatgefühle sorgen.

VON HERMANN APFELBÖCK

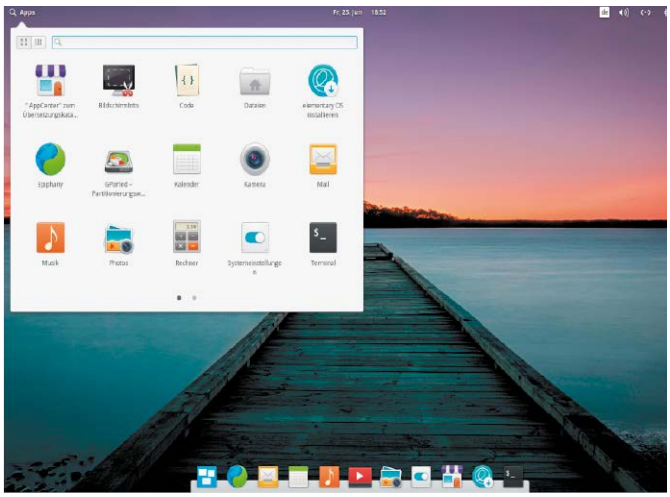
Die Top-10-Liste auf der nächsten Seite filtert aus den zahlreichen Linux-Varianten eine Auswahl, die sich für Windows-Umsteiger besonders eignet. Auf knappem Raum müssen wir uns auf grundsätzliche Regeln für die Distributionssuche und eine kurze Begründung unserer Top-Liste beschränken.

Kriterien für die Systemwahl

Hardwaretechnisch gibt es beim Umzug keinerlei Einschränkungen. Wo bislang ein Windows 10 läuft, ist im Prinzip jedes Linux geeignet. Wer dennoch Ressourcen sparen will, kann dies mit der Desktopwahl steuern: Unter den in der Tabelle aufgeführten Desktops ist XFCE der sparsamste, Pantheon, Cinnamon und KDE liegen im Mittelfeld, Budgie und Gnome sind am anspruchsvollsten.

Grafischer Installationsassistent: Acht der Top-10-Distributionen in der Tabelle verwenden als Setupprogramm den Ubuntu-Installer oder Calamares. Solus-OS und Manjaro haben eigene, aber Calamares ähnliche Installer. Alle diese Installer bieten einfache und klare Benutzerführung, und zwar auch für kompliziertere Szenarien wie Dualboot, die Partitionsänderungen erfordern.

Nachhaltige Dauerläufer: Windows-Umsteiger sollten sich keinesfalls auf Exoten einlassen, deren Nachhaltigkeit ungewiss ist. In unserer Liste dominieren Debian/Ubuntu-Distributionen mit Langzeitsupport, die es auch in zehn Jahren noch geben wird und die jahrelange Systemaktualisierung gewährleisten. Konservative Stabilität ist nicht zuletzt auch ein Grund, warum die hervorragenden Distributionen Solus und Manjaro am Ende der Liste stehen (Rolling Releases).



Elementary OS: Die hübsche Ubuntu-Variante mit Pantheon-Desktop ist so simpel und reduziert wie möglich – einfach für Umsteiger, aber nichts für Bastler.

Grafische Systemzentralen: Powershell und Kommandozeile gelten unter Windows als Profiwerkzeug. Normale Windows-Nutzer erwarten eine komplette grafische Nutzung für Softwareinstallation, Systemkonfiguration, Datenträgerverwaltung und Desktopanpassung. Alle Top-10-Systeme leisten dies annähernd, aber es gibt nur wenige Distributionen, die diesen Anspruch praktisch nahtlos erfüllen – zu allererst Linux Mint und Kubuntu. Die Kubuntu-KDE-Umgebung beansprucht hier mit ihren Konfigurationszentralen und Systemtools den unbestrittenen Platz eins, ist aber aus anderen Gründen nicht durchgehend umsteigerkompatibel.

Desktopstandards: Bei der Suche nach der besten Umsteigeroberfläche bleiben nur wenige objektive Kriterien, die wahrscheinlich alle Windows-Umsteiger als selbstverständlich erachten:

• Steuerzentrale à la „Systemsteuerung“ oder „Einstellungen“: Eine Art „Systemsteuerung“ gibt es überall, allerdings mit unterschiedlichem Umfang – umfassend bei Kubuntu und Linux Mint, brauchbar, aber etwas unübersichtlich bei allen Gnome- und Budgie Distributionen, deutlich ausgedünnt bei XFCE-Distributionen und bei Elementary OS.

• Durchsuchbares und kategorisiertes Startmenü: Die Startmenüs fallen sehr unterschiedlich aus – hübsch, aber minimalistisch bei Elementary OS, relativ simpel auch bei den Distributionen mit XFCE und Budgie. Ein Eingabefeld zur manuellen Programmsuche ist aber überall vertreten. Die Vollbild-Übersicht ohne Kategorisierung von Ubuntu (Gnome) ist schick, aber gewöhnungsbedürftig und unübersichtlich. Am funktionsreichsten sind die Kandidaten unter Mint und Kubuntu.

• Kombinierte Task- und Favoritenleiste: Für Favoritenstarter und Taskübersicht gehen Elementary, Ubuntu Budgie und Solus einen pragmatischen Weg, indem sie einfach ein schickes externes Tool einbauen (Plank-Dock). Der angepasste Gnome-Desktop von Ubuntu kann sich mit seinem Favoritendock ebenfalls sehen lassen. Mint gibt sich mit einem eigenen Leistenmodul erfolgreich Mühe, die Funktionalität der Windows-Taskleiste praktisch identisch nachzubauen. In allen anderen Distributionen ist für diese Funktionalität entweder etwas Bastelarbeit in der Systemleiste er-

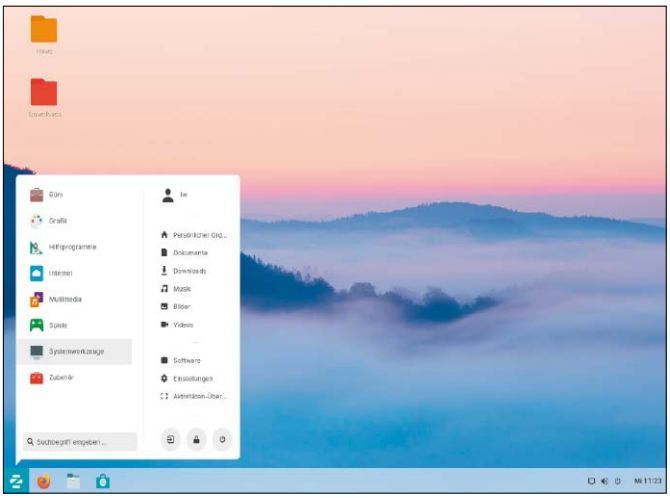
forderlich oder einfach die Installation der Plank-Docks.

• Desktop mit Ordnerfunktionalität: Dass der zentrale, stets zugängliche Ordner „Desktop“ als Ablage für Dateien und Programmstarter dienen kann, ist für Windows-Nutzer seit 25 Jahren Standard. Linux-Desktops wie Gnome, Budgie und Pantheon verzichten absichtlich auf diese Funktion, wobei aber Ubuntu mit seinem angepassten Gnome dies wieder ermöglicht.

• Dateimanager mit Navigationsspalte und Kontextmenüs: Weitgehend Windows-Explorer-analog zeigen und verhalten sich der XFCE- sowie KDE-Dateimanager. Bei anderen Desktopumgebungen ist vor allem Drag & Drop nicht überall Windows-konform. Die Umgewöhnung zu Menübefehlen oder Hotkeys ist aber nicht schwierig, zumal diese identisch mit Windows sind.

Softwarecenter: Windows-Nutzer erwarten zur Ergänzung von System- und Anwendungssoftware eine grafische Zentrale und dort ein umfassendes Angebot. Ersteres ist überall vorhanden, aber mit unterschiedlichem Bedienkomfort – am besten bei Mint, Ubuntu, Kubuntu. Alle Ubuntu-basierten Systeme bieten Zigtausende von Programmen, ebenso Manjaro. Nur Solus-OS muss sich mit seinem kleinen Repository bislang auf Softwareprominenz beschränken.

Desktopanpassungen: Ubuntu (Gnome) und Elementary (Pantheon) wollen vereinfachen und sind relativ hermetisch (nach dem Motto: „Akzeptier' mich, schön wie ich bin“). Solus und Ubuntu Budgie (mit Budgie-Desktop) bieten mehr Spielraum, dies aber nicht intuitiv und objektbezogen, sondern über eigene Konfigurationstools, die man sich erst aneignen muss. Eindeutig einladender für Benutzereingriffe sind die Distributionen mit XFCE – und dies größtenteils intuitiver und logischer als Mint und Kubuntu. Die letztgenannten Distributionen sind am Desktop vorbildlich flexibel (Kubuntu-KDE bis ins Detail), können dabei aber Umsteiger gelegentlich auch überfordern.



Zorin-OS fokussiert auf Windows-Umsteiger und macht aus Gnome eine klassische Oberfläche.

Kommentar zur Rangliste

Naheliegende Kandidaten als Windows-Ersatz sind zwei inoffizielle Ubuntu-Varianten, nämlich **Linux Mint** und **Zorin-OS**. Die machen es sich zur Aufgabe, mit der Cinnamon-Oberfläche (Mint) beziehungsweise mit einem modifizierten und wieder „klassisch“ gezähmten Gnome (Zorin) viele Windows-Funktionen nachzubilden. Es bereitet aber auch keine ganz große Mühe, sich an das deutlich andere, aber einfache Konzept von **Ubuntu** (Gnome) zu gewöhnen. **Elementary** ist ein Kandidat für Anwender, die ihre Programme auf einem ästhetischen und aufgeräumten Desktop nutzen wollen – aber nicht viel mehr.

Die Distributionen **Xubuntu, Voyager** und **Manjaro** bieten mit dem Klassiker XFCE eine reaktionsschnelle, logische und anpassungsfähige Oberfläche. Insbesondere Voyager Live demonstriert zum Teil fast übertrieben, was das konservative XFCE an Optik und Themen hergibt.

Kubuntu scheint auf den ersten Blick absolut Windows-like. Doch ist der KDE-Desktop mit seinen kleingliedrigen Anpassungsoptionen doch eher ein Fall für Desktopbastler. Unter der Haube kocht KDE mit den KIO-Slaves (KDE-Input/Output) sein eigenes Süppchen, das noch nicht alle Zutaten im Griff hat: Die aktuelle Unfähigkeit, von ungemounteten Windows/Samba-Freigaben Filme zu streamen, kostet Kubuntu in unserer Tabelle mindestens zwei Ränge.

Ubuntu Budgie und das schnelle **Solus-OS** liefern einen klaren, ästhetischen, Windows-analogen Desktop. Die Oberfläche ist weniger hermetisch als bei Ubuntu oder Elementary, braucht aber für Anpassungen etwas Gewöhnung. ■

TOP 10: LINUX-DISTRIBUTIONEN FÜR UMSTEIGER

Rang	Distribution	aktuell	Desktop*	Systembasis	Webseite	ISO (MB)	Beschreibung
1	Linux Mint	20.3	Cinnamon	Debian/Ubuntu	*www.linuxmint.com*	2100	attraktiver, intuitiver Cinnamon-Desktop mit vielen Windows-Analogien
2	Xubuntu	20.04**	XFCE	Debian/Ubuntu	*https://xubuntu.org*	1600	konservativer, aber intuitiver und anpassungsfähiger XFCE-Desktop
3	Zorin-OS (Core)	16	Gnome	Debian/Ubuntu	*https://zorinos.com*	2700	stark angepasster Gnome mit vielen Windows-Analogien, „Core“ kostenlos
4	Elementary OS	6.0	Pantheon	Debian/Ubuntu	*https://elementary.io/de*	2400	„Mac“-Desktop: schick, einfach, aber reduziert (keine Desktopablage)
5	Ubuntu	22.04**	Gnome	Debian/Ubuntu	*www.ubuntu.com*	2700	Ubuntu-Originalversion mit angepasstem Gnome (Dock, Desktopablage)
6	Kubuntu	22.04**	KDE	Debian/Ubuntu	*www.kubuntu.org*	2300	funktionsreiche, detailverliebte und komplexe Oberfläche KDE Plasma
7	Voyager Live	22.04**	XFCE	Debian/Ubuntu	*https://voyagerlive.org/*	2900	ausgereizter XFCE-Desktop mit schicken Details und Systemergänzungen
8	Ubuntu Budgie	22.04**	Budgie	Debian/Ubuntu	*https://ubuntubudgie.org*	2011	attraktiver Desktop mit eigenwilliger Konfiguration, keine Desktopablage
9	Solus-OS	4.3	Budgie	unabhängig	*https://getsol.us/home*	1900	schnelles System mit Budgie-Desktop (s. o.), Rolling Release***
10	Manjaro	21.1	XFCE	Arch	*https://manjaro.org*	2900	schnelles Arch mit Installer, Softwarezentrale, XFCE, Rolling Release***

*Standardoberfläche der Distribution ** Version 22.04 soll im April 2022 erscheinen ***erhält laufend Funktionsupdates (daher stets aktuell, aber weniger stabil)

Desktops: Linux vs. Windows 11

Ein Vergleich der Desktops von Windows 11 mit typischen Linux-Desktops ist durchaus angebracht. Schließlich können die Linux-Desktops das, was Windows bietet, schon lange. Zumindest dann, wenn Sie die richtigen Erweiterungstools nutzen.

VON THORSTEN EGGELING

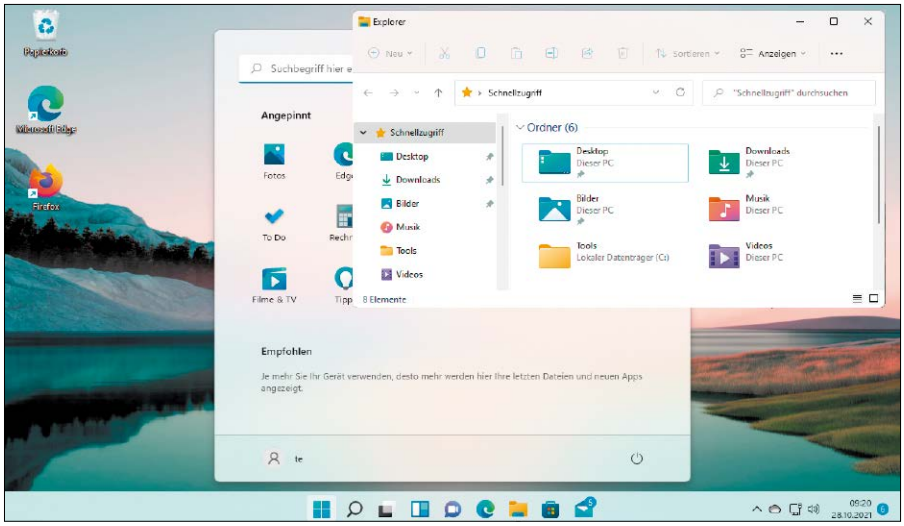
Eigentlich sollte Windows 10 das letzte und einzige Microsoft-Betriebssystem für den Desktop sein. Doch dann kam 2021 doch die Ankündigung, dass es ein Windows 11 geben wird. Ein Upgrade für das weltweit am häufigsten genutzte Desktop-Betriebssystem sorgt in jedem Fall für Aufmerksamkeit – erst recht, wenn es sich auf vielen älteren PCs nicht installieren lässt (siehe Seite 56).

Die technischen Neuerungen im Windows-Unterbau sind überschaubar. Im Vergleich zu Windows 10 hat sich nicht viel geändert. Dafür befinden sich jetzt Startmenü und Taskleiste in der Mitte unten am Bildschirm, Fenster zeigen abgerundete Ecken, die „Einstellungen“ sind etwas übersichtlicher geworden. Linux-Nutzern wird bei Windows 11 einiges bekannt vorkommen – Ähnlichkeiten mit KDE Plasma sind nicht zu verleugnen. Bei Windows 11 fehlen jedoch in vielen Bereichen Anpassungsmöglichkeiten, die Linux-Nutzer seit langem gewohnt sind.

Konzepte grafischer Oberflächen

Grafische Benutzeroberflächen für Computer gibt es seit den 1970er-Jahren. Am Grundkonzept hat sich seither wenig geändert: mit der Maus anklickbare Icons, Anwendungen in skalierbaren Fenstern. Platz für Innovationen ist aber dennoch genügend vorhanden. Elemente wie Finder und Dock bei Mac-OS oder das Startmenü von Windows 95 haben über Jahre die Gestaltung grafischer Oberflächen beeinflusst. Das iPhone hat 2007 der Entwicklung noch einmal neue Impulse gegeben: Vollbild statt Fenster und Finger statt Maus. Dazu kommen die Anzeige von Nachrichten auf dem Sperrbildschirm und die Sprachsteuerung. Microsoft hat das dazu verleitet, Desktopnutzern mit Windows 8 eine ähnliche Benutzeroberfläche aufzuzwingen – ein Flop, wie man inzwischen weiß. Mit Windows 10 ging es dann wieder eher in Richtung klassische Bedienung und in Windows 11 hat Microsoft den Desktop erneut leicht renoviert.

Auch wenn Microsoft bei Designentscheidungen schon häufiger danebenlag, kann man die Gründe dafür teilweise nachvollziehen. Im Vergleich mit Linux-Desktops ist jedoch bei Windows 11 kaum Neues zu finden. Der entscheidende Unterschied: Linux-Nutzern bleibt die Wahl zwischen unterschiedlichen Desktopumgebungen, die zudem meist fast beliebig anpassbar sind.



Windows 11: Die neue gestaltete Oberfläche zeigt frische Farben, teiltransparente Fenster mit abgerundeten Ecken und eine Taskleiste mit abgespeckten Startmenü in der Mitte.

Windows: Startmenü und Taskleiste

Startmenü und Taskleiste in der Mitte des unteren Bildschirmrands kann man als nett gemeinten Vorschlag Microsofts verstehen. Unter Umständen lassen sich damit Mauswege verkürzen, weil die meisten Anwender eher in der Mitte des Bildschirms arbeiten. Ob das in der Praxis eine besonders große Zeitersparnis darstellt, sei dahingestellt. Zudem reduziert sich der Vorteil, wenn zahlreiche Icons in der Taskleiste angepinnt oder viele Programme gestartet sind. Die Startmenüschaltfläche verschiebt sich dann immer weiter nach links. Wer möchte, kann die Taskleiste über die Einstellungen links anordnen. Andere Positionen sind nicht möglich.

Das Startmenü hat Microsoft deutlich entschlackt. Es zeigt einige angepinnte Pro-

gramme, die Position lässt sich per Drag & Drop ändern. Die Live-Kacheln von Windows 10 fehlen. Per Klick auf „Alle Apps“ ruft man eine alphabetisch sortierte Liste aller Programme auf.

Windows 11 gruppiert die Icons in der Taskleiste, wenn mehrere Fenster einer Anwendung geöffnet sind. Um zum gewünschten Fenster zu gelangen, fährt man mit dem Mauszeiger über das Icon und klickt auf die Fenstervorschau. Das ist auch bei Windows 10 so. Die Gruppierung lässt sich hier jedoch abschalten oder nur aktivieren, wenn die Taskleiste voll ist.

Linux: Starter und Leisten

Wie Anwendungsstarter und Taskleiste aussehen, hängt von der Distribution beziehungsweise Desktopumgebung ab. Ubuntu beispielsweise verfolgt einen stark reduzierten Ansatz. Für den Starter und die Icons der laufenden Anwendungen gibt es nur eine gemeinsame Leiste. Wer mehr Einstellungen wünscht, wird bei Linux Mint Cinnamon oder Kubuntu (KDE) fündig. Die Systeme zeigen frei konfigurierbare Leisten, deren Position und Bestandteile man nach Belieben anpassen kann. Es stehen unterschiedlich gestaltete Widgets für Menüs, Programmstarter oder Fensterlisten zur Verfügung. Die bei Windows 11 genannten Einschränkungen sind Kubuntu, Lubuntu, Xubuntu oder Linux Mint weitestgehend unbekannt.

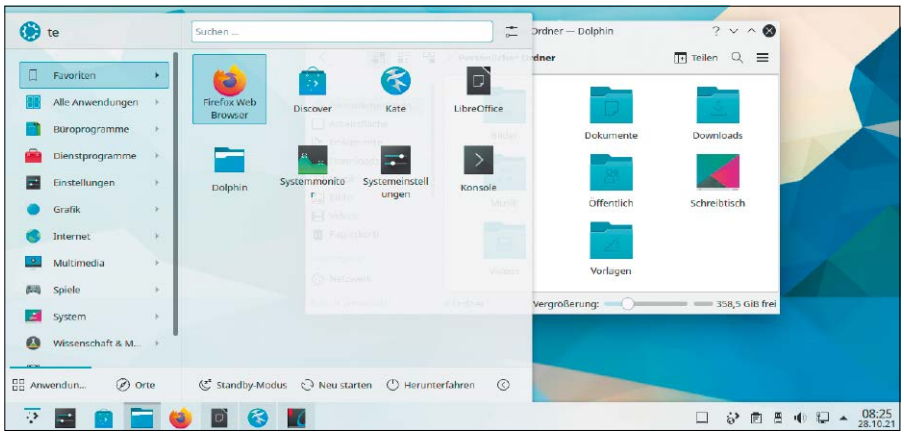
Die Funktionalität des Desktops

An der Desktoparbeitsfläche hat sich in Windows 11 nicht viel geändert. Hier lassen sich Ordner, Dateien oder Verknüpfungen ablegen, auch per Drag & Drop vom Windows-Explorer aus. Verwendet man die rechte Maustaste, öffnet sich ein Menü und fragt nach der gewünschten Aktion.

Linux: Auch beim Desktop verfolgt Ubuntu (mit Gnome) seine eigene, sehr reduzierte Strategie. Auf dem Desktop lassen sich Ordner, aber keine Dateien oder Verknüpfungen erstellen. Der Cinnamon- oder KDE Desktop ist dagegen voll funktionsfähig und bietet die gleichen Möglichkeiten wie Windows 11.

Konfiguration und Einstellungen

Seit Windows 8 arbeitet Microsoft am Umbau der Systemeinstellungen. Bei jedem Upgrade wandern mehr Funktionen von der alten Systemsteuerung in die neuen



Kubuntu 21.10 mit KDE Plasma 5.23: Es scheint fast so, als habe Microsoft bei KDE mitgewirkt. Optisch sind sich Windows 11 und der aktuelle KDE-Desktop sehr ähnlich.



Kontrollleiste bearbeiten: KDE kann die Elemente in der Leiste beliebig anordnen. Mit einem Abstandshalter lässt sich das Menü auch in der Mitte unterbringen.

„Einstellungen“. Für die Benutzer erschwert das die Orientierung, weil eine Option oft nicht mehr am gewohnten Ort zu finden ist. Die „Einstellungen“ in Windows 11 sind jedoch gut gelungen. Hauptkategorien wie „System“ oder „Personalisierung“ bleiben als Navigation auf der linken Seite des Fensters immer sichtbar. Die Unterkategorien sind im rechten Teil des Fensters zu sehen, von wo aus man in weitere Unterpunkte gelangt. Der aktuelle Pfad wird oben im Fenster angezeigt. Man sieht daher jederzeit, wo man sich gerade befindet, und blättert per Klick auf einen Teil des Pfades zum vorherigen Punkt zurück.

Linux: Die „Einstellungen“ bei Ubuntu 20.04 (Gnome-Desktop) müssen den Vergleich mit Windows 11 nicht scheuen. Navigation und Aufbau sind ähnlich. Es gibt aber deutlich weniger Optionen, was die Übersichtlichkeit erhöht, aber die Anpassungsmöglichkeiten reduziert. Das KDE-Kontrollzentrum (Kubuntu) ist ähnlich aufgebaut, bietet aber mehr Einstellungen und Unterkategorien. Man muss daher häufiger blättern. Maximal ist nur eine Unterebene vorhanden, sodass man mit einem Mausklick zu den Hauptkategorien zurückgelangt. Linux Mint mit Cinnamon ist schlechter aufgestellt. Die einzelnen Optionen erreicht man eher umständlich über das Menü „Einstellungen“. Eine Komplettübersicht erhält man in den nicht sehr übersichtlichen „Systemeinstellungen“. ■



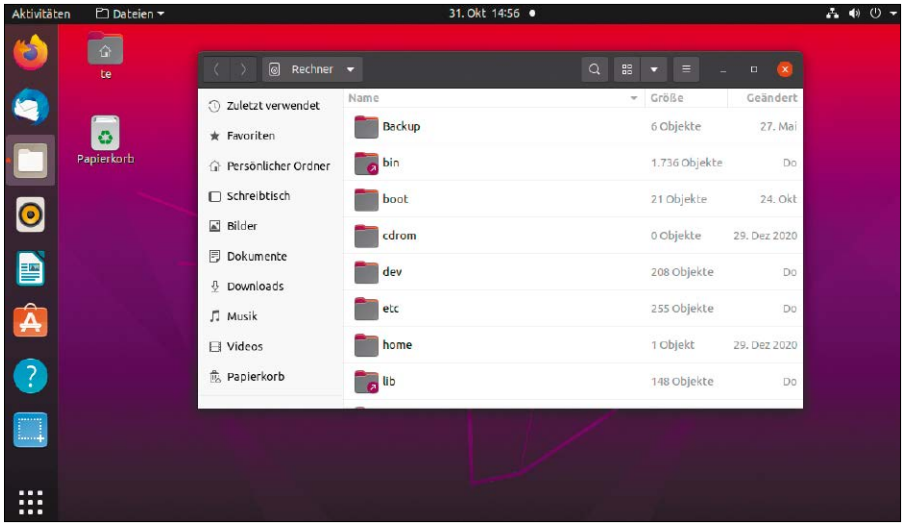
KDE-Systemeinstellungen: Kubuntu punktet bei den Einstellungen. Die sind ähnlich gut organisiert wie bei Windows 11 und der Desktop lässt sich hervorragend anpassen.

Funktionale und hübsche Desktops

Linux-Nutzer können sich den Desktop aussuchen, der funktional zu ihnen passt und der ihnen optisch gefällt. Dabei ist man nicht auf ein bestimmtes Linux-System festgelegt. Die meisten Distributionen bieten mehrere Desktops an.

VON THORSTEN EGGELING

Nutzer haben unterschiedliche Ansprüche an die Bedienoberfläche. Auf der einen Seite stehen Anwender, die kaum mehr als ein Terminal erwarten. Andere legen besonderen Wert auf die Ästhetik: Einheitliche Farben, klare Linien und präzise Schriften sind ihnen wichtig. Zwischen den beiden Extremen bewegen sich Anwender, die ohnehin nur den Browser oder Mediaplayer öffnen und denen System und Desktop herzlich egal sind. Linux hat für alle genannten Benutzergruppen etwas zu bieten. Es ist am einfachsten, gleich die Distribution zu installieren, die den individuellen Ansprüchen am ehesten entspricht. Die zugehörigen Livesysteme bieten einen ersten Eindruck von Aussehen und Bedienung.



Ubuntu 20.04: Das Ubuntu-System mit Gnome-Desktop ist weder besonders schön noch anpassungsfähig. Aber es ist sehr übersichtlich und einfach zu bedienen.

Desktopumgebungen wie Gnome, KDE oder XFCE stammen aus eigenständigen Projekten und sind daher nicht an eine spezielle Distribution gebunden. Konfiguration und Paketmanagement unterscheiden sich je nach Linux-Distribution teilweise jedoch gravierend. Die Distributoren fügen eigene Tools hinzu und setzen jeweils andere Akzente auf dem Desktop.

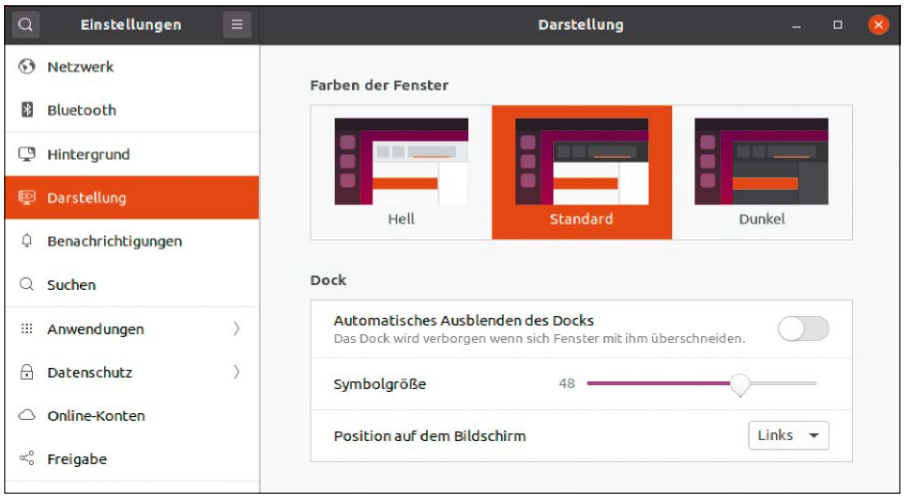
Gnome: Weniger ist manchmal weniger

Die Gnome-Entwickler verfolgen eine ganz eigene Philosophie. Ein naturbelassenes Gnome (*www.gnome.org*) bietet wenig von dem, was etwa Linux-Mint- oder Windows-Nutzer gewohnt sind. Ein klassisches Startmenü oder eine Taskleiste gibt es nicht und der Desktop kann weder Ordner noch Verknüpfungen aufnehmen. Stattdessen zeigt sich im aktuellen Gnome 41 nach der Anmeldung oder nach einem Klick auf „Aktivitäten“ eine horizontale Leiste (Gnome Dash) mit einigen Programmstartern. Laufende Anwendungen signalisiert das Dash mit einem Punkt. Das Icon ganz rechts führt zu einer Übersicht mit allen installierten Programmen, die sich über das Kontextmenü in die Favoriten aufnehmen lassen.

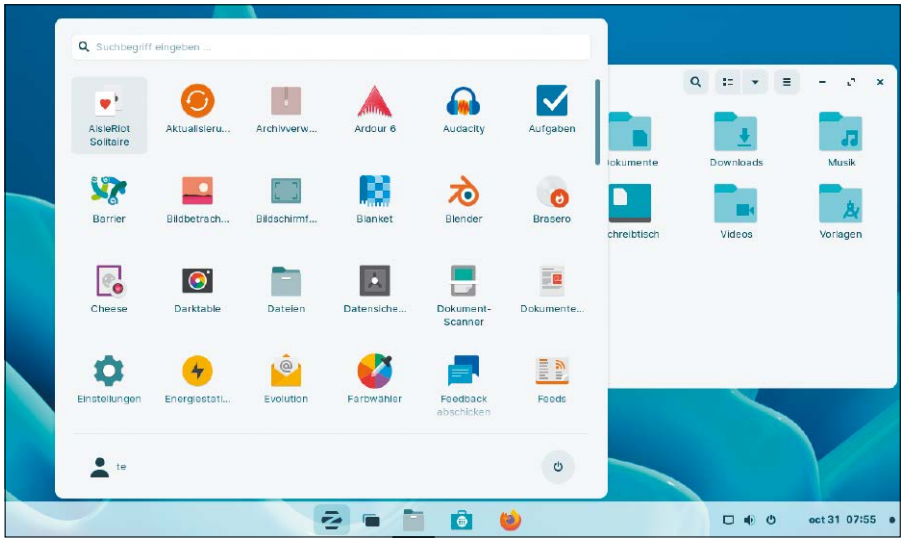
Die Ansicht über „Aktivitäten“ zeigt auch die virtuellen Arbeitsflächen. Standardmäßig gibt es davon zwei. Verschiebt man ein Programmfenster auf die letzte Arbeitsfläche, fügt Gnome automatisch eine weitere hinzu. Gnome lässt sich am besten mit einem Touchpad oder der Tastatur bedienen. Mit einer Zwei-Finger-Geste kann man beispielsweise zwischen den Arbeitsflächen wechseln. Die Super-Taste (Windows-Taste) ruft „Aktivitäten“ auf, Alt-Esc wechselt zwischen Fenstern und Alt-Leertaste zeigt das Fenstermenü. Minimieren- und Maximieren-Schaltflächen gibt es bei Gnome-Fenstern nicht. Man kann Super-H verwenden, um Fenster zu verbergen, über den Taskwechsler Alt-Tab lässt es sich später wieder hervorholen.

Design und Leistung: Gnome bezeichnet sich selbst als „einfach, schön und elegant“. Das mag in einzelnen Bereichen stimmen, insgesamt wirkt der Gnome-Desktop jedoch eher altbacken. Beschriftungen sind teilweise zu groß und grob, Schaltflächen in 3D-Darstellung gelten als nicht besonders modern, die Standardicons etwa im Dateimanager sind eher langweilig. Der Verzicht auf übermäßige Effekte bei Desktop und Fenstern trägt allerdings kaum Verbesserung der Leistung bei. Gnome fühlt sich weder besonders schnell noch langsam an.

Einstellungen: Die Gnome-Einstellungen sind übersichtlich und funktional. Für das Erscheinungsbild des Desktops gibt es keine Optionen, vom Hintergrundbild einmal abgesehen. Neu in Gnome 41 ist die Kategorie „Multitasking“. Es gibt beispielsweise eine Option, über die sich die aktiven Bildschirmkanten abschalten lassen. Ist die Funktion aktiv, füllt ein Fenster die Hälfte des Bildschirms aus, wenn es an den linken oder rechten Rand gezogen wird. Zieht man es an den oberen Rand, wird es auf Vollbild vergrößert.
Gnome lässt sich individuell anpassen, aber dafür sind zusätzliche Werkzeuge erforderlich. Beispiele finden Sie ab Seite 26.
Standardsoftware: Zu Gnome gehören einige Anwendungen, die alle im einheitlichen Design erscheinen. Dazu gehören beispielsweise der Texteditor Gedit, der Mediaplayer Videos und der Musikplayer Rhythmbox. Die Paketverwaltung mit dem Namen „Software“ gehört ebenfalls zu Gnome und ist mit leichten Änderungen in den meisten Distributionen zu finden, die auf Gnome basieren.
Distributionen: Ein weitestgehend unverändertes Gnome installieren Fedora, Debian und Open Suse. Ubuntu verwendet ebenfalls Gnome, zeigt aber den Programmstarter Ubuntu-Dock dauerhaft links auf dem Bildschirm.
Zorin-OS basiert auf Ubuntu und verwendet Gnome als Desktop. Davon ist allerdings nicht viel zu sehen. Das System zeigt eine Taskleiste und ein klassisches Startmenü. Die Auswahl des Desktopthemas und geeigneter Schriftarten verleihen Zorin ein sehr klares und ästhetisches Design. Die kostenlose Core-Version bietet nicht alle Einstellungen. Wer mehr möchte, muss Zorin-OS Pro kaufen (39 Dollar). Dort sind auch Desktoplayouts im Stil von Windows 11 und Mac-OS enthalten.



Gnome-Einstellungen: Die ansonsten komfortable Systemzentrale hat bei Ubuntu/Gnome unter „Darstellung“ nicht viel zu bieten. Gerade einmal drei Themes stehen zur Auswahl.



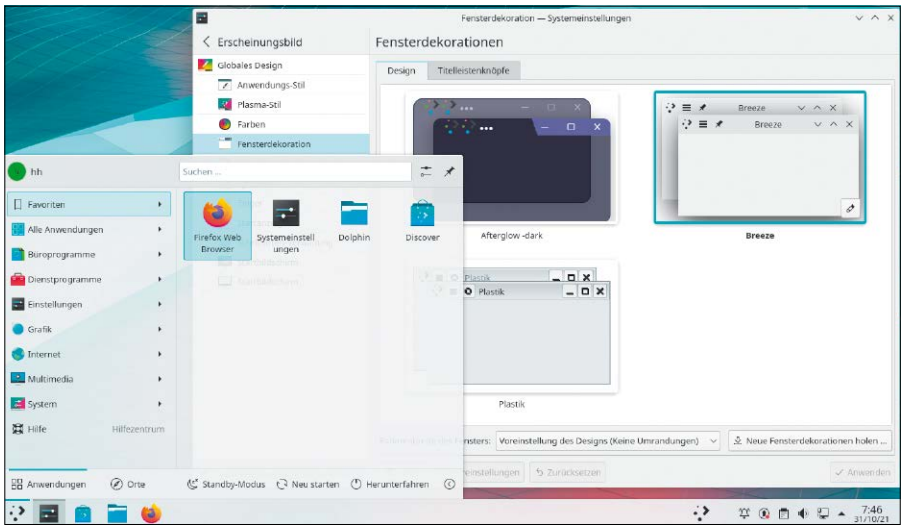
Zorin-OS (Pro): Zorin basiert auf Ubuntu, bringt aber eigene Anpassungen mit. Die Pro-Edition enthält zusätzliche Desktoplayouts mit Designs im Stil von Mac-OS oder Windows 11.

KDE: Schick und gut anpassbar

Die intensive und schnell fortschreitende Entwicklung hat bei KDE (*https://kde.org*) in der letzten Zeit zu zahlreichen Verbesserungen geführt. In diesem Artikel beziehen wir uns auf neuere KDE-Versionen. Kubuntu 21.10 und KDE Neon installieren aktuell KDE Plasma 5.23. Bei älteren Versionen sind nicht alle beschriebenen Funktionen zu finden.
KDE zeigt ein klassisches Startmenü und eine Taskleiste. Das Startmenü („Anwendungs-Starter“) zeigt zuoberst Favoriten für den Schnellzugriff an. Unter „Alle Anwendungen“ erscheint eine alphabetisch sortierte Liste der installierten Anwendungen. Der Rest des Menüs zeigt Programmkategorien wie „Büro“ und „Internet“.
Der rechte Mausklick kann teilweise zur schnelleren Navigation dienen. Bei „Systemeinstellungen“ beispielsweise sind im Menü die zuletzt aufgerufenen Einstellungen zu sehen, bei Firefox „Ein neues Fenster öffnen“ und „Ein neues privates Fenster öffnen“.
Am unteren Rand sind Schaltflächen für „Standby-Modus“, „Neu Starten“ und „Herunterfahren“ untergebracht. Rechts davon gibt es ein Icon, das zu „Sperren“, „Abmelden“ und „Benutzer wechseln“ führt. Die beiden Bereiche können ihre Plätze tauschen, wenn man das eine oder andere häufiger benötigt. Dazu klickt man auf das Icon ganz rechts oben, um die Einstellungen des Anwendungsstarters aufzurufen, und aktiviert unter „Primäre Aktionen“ die Option „Sitzungs-Aktionen“.
Die Taskleiste heißt bei KDE „Fensterleiste nur mit Symbolen“. Sie dient als Programmstarter und zeigt laufende Programme an. Über einen rechten Mausklick und den Menüpunkt „Fensterleiste mit Symbolen einrichten“ lässt sich die Leiste anpassen.
Design und Leistung: KDE bietet eine klare Optik mit scharfer Schriftdarstellung und meist mit modernen, flachen Schaltflächen. Die Gestaltung der KDE-Anwendungen ist zum größten Teil einheitlich. Die KDE-Ent-



Elemente in den Leisten: Startmenü und Taskleiste sind bei KDE Miniprogramme, die sich beliebig anordnen lassen. Man kann auch zusätzliche Elemente hinzufügen oder nach Alternativen suchen.



KDE Neon: Diese Distribution der KDE-Entwickler auf Ubuntu-Basis enthält stets die aktuelle KDE-Version aus dem offiziellen stabilen Zweig.

wickler scheinen eine Vorliebe dafür zu haben, jede denkbare Option in ein Programm einzubauen. Das führt in einigen Anwendungen zu überladenen Menüs mit Unter- und Unter-Unter-Menüs, die kaum noch auf den Bildschirm passen. Besonders übersichtlich ist das nicht, lädt aber zum Experimentieren ein. Die Geschwindigkeit des Systems scheint das nicht zu beeinträchtigen. KDE ist nach wie vor kein Leichtgewicht unter den Desktopumgebungen, aber auf jedem aktuellen Rechner angenehm und schnell zu bedienen.

Einstellungen: KDE besitzt eine Zentrale für die Systemeinstellungen, die der von Gnome ähnelt. Wer den Desktop individuell konfigurieren möchte, wird hier seine Freude haben. Die Basiseinstellungen sind unter „Erscheinungsbild" zu finden. Hier lässt sich ein „Anwendungs-Stil" auswählen, weitere sind über „Neue globale Designs holen" abrufbar. Die Details sind beispielsweise unter „Plasma-Stil", „Farben" und „Fensterdekoration" einstellbar. Wem die vorgegebenen Stile nicht genügen, kann zusätzliche herunterladen.

Zurück in der Hauptübersicht sind unter „Arbeitsbereich" weitere Einstellungen für den Desktop zu finden. Die betreffen vor allem das Verhalten der Arbeitsbereiche und der Fenster.

Standardsoftware: Zu den KDE-Anwendungen gehören der Dateimanager Dolphin und der Texteditor Kate. Dazu kommt die Programmverwaltung Discover, über die man auch die zahlreichen Plasma-Erweiterungen abrufen kann. Systemaktuali-

WEITERE SPANNENDE DESKTOPUMGEBUNGEN

Gnome, KDE, XFCE oder Cinnamon sind die bevorzugten Desktopoberflächen vieler Linux-Nutzer. Daneben gibt es weniger bekannte Software, die entweder Ähnliches bietet oder ganz andere Wege einschlägt. Zu nennen ist beispielsweise der **Mate-Desktop** (*https://mate-desktop.org*), der eine Art Mischung von Gnome und Cinnamon darstellt. Durch den offiziellen Ubuntu-Ableger hat er eine gewisse Verbreitung gefunden.

Auf Ubuntu-Basis läuft außerdem Elementary OS, dessen Entwickler den eigenen **Pantheon-Desktop** verantworten. Das System orientiert sich bei der Desktopgestaltung eher an Mac-OS als an Windows. Elementary OS ist ästhetisch ansprechend, bei der Bedienung aber gewöhnungsbedürftig. Es gibt keine Menüleiste, die Steuerung erfolgt ausschließlich über die Symbolleiste oder das Kontextmenü. 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.

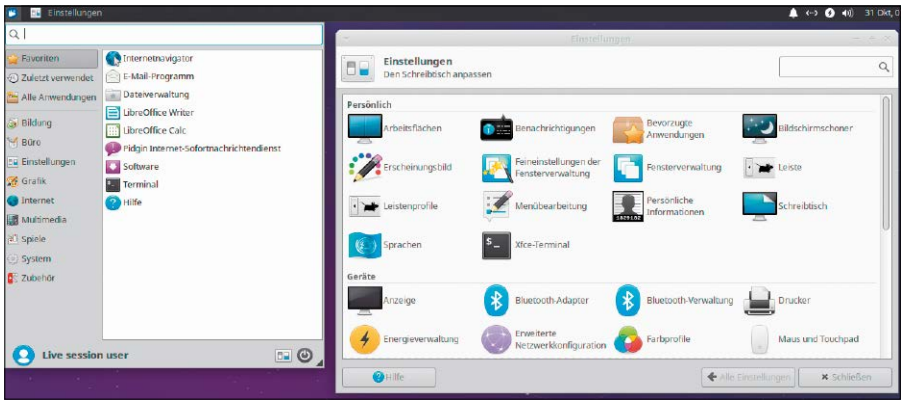
In einer ähnlichen Liga spielt der **Budgie-Desktop** (Ubuntu Budgie, Solus-OS), der sich ebenfalls an Mac-OS orientiert.

Wieder eher konservativ ist der **Moksha-Desktop**, der in Bodhi Linux zu finden ist. Startmenü und Taskleiste gehören zu seinem Repertoire. Individuelle Anpassungen sind möglich, aber kompliziert. Dafür ist das System auf Geschwindigkeit getrimmt. Obwohl es auf Ubuntu basiert, startet und reagiert es außerordentlich schnell.

Bunsenlabs ist eine eher ungewöhnliche Linux-Distribution, die den Fenstermanager **Openbox** und dessen Fähigkeiten nutzt. Es gibt eine Menü-Schaltfläche und eine Taskleiste. Das Kontextmenü des ansonsten funktionslosen Desktops öffnet ebenfalls das Hauptmenü. Die schlichte, aber ästhetische Oberfläche ist in Grenzen anpassungsfähig. Das Wichtigste findet sich unter „Preferences → Openbox → WM Preferences" sowie „Preferences → Appearance". Bunsenlabs gehört zu den besonders schnellen und anspruchslosen Linux-Systemen.

sierungen lassen sich über Discover ebenfalls installieren.

Distributionen: Alle größeren Distributionen bieten Ausgaben mit KDE-Desktop. Kubuntu 20.04 (ab April 2022 in Version 22.04) ist als LTS-Version mit KDE Plasma 5.18 nicht ganz auf dem neuesten Stand. In dieser Version wurde beispielsweise der Anwendungsstarter noch nicht überarbeitet. Kubuntu 21.10 enthält KDE Plasma 5.22 und damit bereits etliche Neuerungen. Wer ein besonders aktuelles KDE möchte, greift zu KDE Neon. Das System basiert auf Ubuntu 20.04, enthält aber immer die neueste KDE-Version. Fedora installiert ebenfalls relativ neue KDE-Versionen und Open Suse Tumbleweed ist als Rolling Release ohnehin immer auf dem neuesten Stand.



XFCE-Desktop: Die Desktopumgebung ist funktional und schnell, genügt aber nicht allen ästhetischen Ansprüchen. Die „Einstellungen“ sind im Vergleich zu Gnome eher unübersichtlich.

XFCE: Leichtgewicht für Individualisten

Auch XFCE (*www.xfce.org*) gehört zu den älteren Desktopumgebungen, die Entwicklung verläuft aber eher langsam. Nach mehr als vier Jahren Pause erschien im August 2019 die Version 4.14, im Dezember 2020 wurde das kleine Update 4.16 nachgereicht. Häufige Updates alleine sind jedoch auch kein Qualitätsmerkmal. XFCE hat auf jeden Fall eine treue Fangemeinde, weil die Desktopumgebung sparsam mit Ressourcen umgeht und trotzdem gut anpassbar ist.

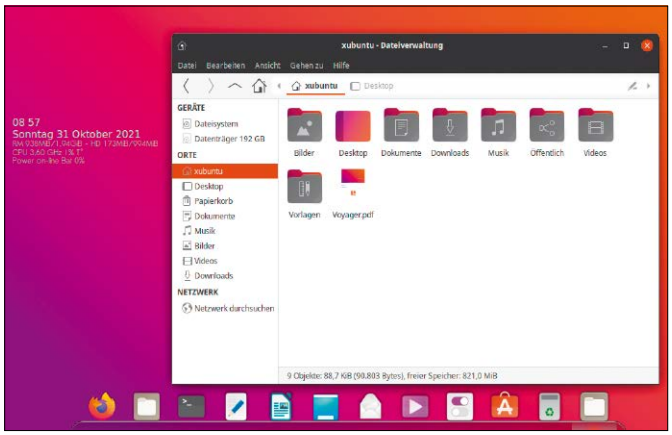
Xubuntu positioniert eine klassische Taskleiste am oberen Bildschirmrand. Das Startmenü mit Suchfunktion zeigt „Favoriten“, „Zuletzt verwendet“ und „Alle Anwendungen“. Darunter sind Kategorien wie „Büro“ und „Internet“ zu finden. Für den schnellen Start kann man Programme aus dem Menü über das Kontextmenü in die Favoriten aufnehmen. Im rechten Bereich sind die Uhr und der Lautstärkeregler sowie Statusbenachrichtigungen zu Netzwerk und Updates untergebracht. Fedora mit XFCE ist ähnlich konfiguriert, zeigt aber ein einfacheres Startmenü ohne Suchfunktion.

Bei XFCE bestehen die Leisten wie bei KDE aus einzelnen Elementen. Ein rechter Mausklick auf einen freien Bereich in der Leiste führt zum Menü „Leiste → Leisteneinstellungen“. Auf der Registerkarte „Anzeige“ lässt sich festlegen, ob die Leiste waagerecht oder senkrecht ausgerichtet sein soll. Wer die Leiste am unteren Bildschirmrand sehen möchte, entfernt das Häkchen vor „Leiste sperren“. Klicken Sie dann ganz links auf die Leiste und ziehen Sie sie nach

PROMINENTE LINUX-DESKTOPSYSTEME

Distribution	aktuell	Webseite	Download (MB)	Basis	Beschreibung
Bodhi Linux	6.0.0	*www.bodhilinux.com*	850	Ubuntu	besonders schlankes und schnelles System mit Moksha-Desktop
Bunsenlabs	Lithium	*www.bunsenlabs.org*	1200	Debian	sehr reduzierte und schnelle Distribution mit Openbox vor allem für Altgeräte
Debian	11	*www.debian.org*	340–3700	–	konservative Basis vieler Desktopdistributionen mit Gnome, KDE u. a.
Elementary OS	6.0	*https://elementary.io/de/*	2500	Ubuntu	inoffizielles Ubuntu-Derivat mit eigenem Pantheon-Desktop
Fedora Spins	34	*https://spins.fedoraproject.org*	1600–2000	Red Hat	Fedora-Ableger mit KDE, XFCE, LXQT, Mate oder Cinnamon
Fedora Workstation	34	*https://getfedora.org/de*	1900	Red Hat	innovativer, aber kurzlebiger Gnome-Desktop-Ableger von Red Hat Enterprise
KDE Neon	5.23.2	*https://neon.kde.org/download*	1800	Ubuntu	inoffizielles Ubuntu-Derivat mit besonders aktuellem KDE-Desktop
Kubuntu	22.04*	*www.kubuntu.org*	3100	Ubuntu	offizielles Ubuntu-Derivat mit KDE Plasma
Linux Mint	20.3	*www.linuxmint.com*	2100	Ubuntu	inoffizielles Ubuntu-Derivat mit eigenem Cinnamon-Desktop
Lubuntu	22.04*	*https://lubuntu.me*	1800	Ubuntu	offizielles Ubuntu-Derivat mit LXQT
Manjaro	21.1	*https://manjaro.org*	3000	Arch	schnelles Arch mit Installer und Softwarezentrale; Rolling Release
Netrunner	21.01	*www.netrunner.com*	2600	Debian	umfangreiche Standardsoftware auf aktuellem KDE-Desktop
Open Suse	Tumbleweed	*https://get.opensuse.org*	4500	Suse Linux	Rolling Release mit umfangreicher und aktueller Desktopuswahl
Solus-OS	4.3	*https://getsol.us/home*	1900	–	unabhängiges Linux mit eigenem Budgie-Desktop; Rolling Release
Ubuntu	22.04*	*www.ubuntu.com*	2700	Debian	Ubuntu-Originalversion von Canonical mit angepasstem Gnome
Ubuntu Budgie	22.04*	*https://ubuntubudgie.org*	2800	Ubuntu	offizielles Ubuntu-Derivat mit Budgie-Desktop
Ubuntu Mate	22.04*	*https://ubuntu-mate.org*	3000	Ubuntu	offizielles Ubuntu-Derivat mit Mate-Desktop
Voyager	20.04.2	*https://voyagerlive.org/*	2000	Ubuntu	inoffizielles Ubuntu-Derivat mit angepasstem XFCE oder Gnome
Xubuntu	22.04*	*https://xubuntu.org*	1800	Ubuntu	offizielles Ubuntu-Derivat mit XFCE-Desktop
Zorin-OS (Core)	16	*https://zorinos.com*	2800	Ubuntu	inoffizielles Ubuntu-Derivat mit stark angepasstem Gnome-Desktop

* Version 22.04 soll im April 2022 erscheinen



XFCE mal anders: Voyager zeigt einen angenehm gestalteten XFCE-Desktop auf Basis von Xubuntu. Durch das Dock am unteren Bildschirmrand soll das System Mac-OS ähneln.

unten. Danach können Sie das Häkchen wieder setzen.

Auf der Registerkarte „Objekte“ sind die enthaltenen Elemente aufgelistet, die Position lässt sich über die Pfeil-Schaltfächen ändern. Über die „+“-Schaltfläche fügen Sie neue Elemente hinzu. Die können Sie auch mit der Maus direkt vom Dialog auf die gewünschte Stelle in der Leiste ziehen.

Jedes Element besitzt eigene Einstellungen, die sich über die Schaltfläche mit dem Zahnradsymbol aufrufen lassen. Das geht auch direkt in der Leiste über den Kontextmenüpunkt „Einstellungen“. Bei Xubuntu sehen Sie an der ersten Position das „Whisker-Menü“, welches sich auch bei Fedora nachträglich aktivieren lässt. Welche Einträge das Menü an welcher Stelle zeigt, lässt sich detailliert in den Einstellungen festlegen. Auf der Registerkarte „Suchbefehle“ erfährt man, welche Kürzel im Suchfeld des Menüs gelten. „!w“ beispielsweise leitet eine Suche in der Wikipedia ein. Sie können neue Suchbefehle festlegen und vorhandene ändern.

Design und Leistung: Xubuntu ist nicht unbedingt ein Hingucker. Als Grafikbibliothek dient GTK 2, der Vorgänger des im aktuellen Gnome verwendeten GTK 3. Die grafischen Elemente und Schriftarten wirken daher nicht besonders elegant, unterscheiden sich aber auch nicht wesentlich vom Gnome-Desktop. XFCE benötigt wenig Hauptspeicher und liegt beim Ressourcenbedarf im unteren Bereich. Die Desktopumgebung ist daher immer eine Empfehlung für weniger leistungsstarke Hardware.

Einstellungen: Die „Einstellungen“ erreichen Sie bei Xubuntu schnell über das Icon am unteren Rand des Startmenüs. Relevante Bereiche für die Desktopgestaltung sind „Erscheinungsbild“, „Schreibtisch“ und „Feineinstellungen der Fensterverwaltung“. Über „Fensterverwaltung“ lässt sich der Fensterstil festlegen. Wählen Sie „Greybird-acessibility“ für einen etwas größeren Fensterrahmen, der sich leichter mit der Maus anfassen lässt.

Standardsoftware: Zum XFCE-Desktop gehören beispielsweise der Dateimanager Thunar, der Mediaplayer Parole und der Texteditor Mousepad. Diese recht einfachen Programme können mit ihren Pendants in Gnome oder KDE nicht ganz mithalten. Wem der Funktionsumfang nicht ausreicht, kann aber einfach das gewünschte Programm einer anderen Desktopumgebung installieren.

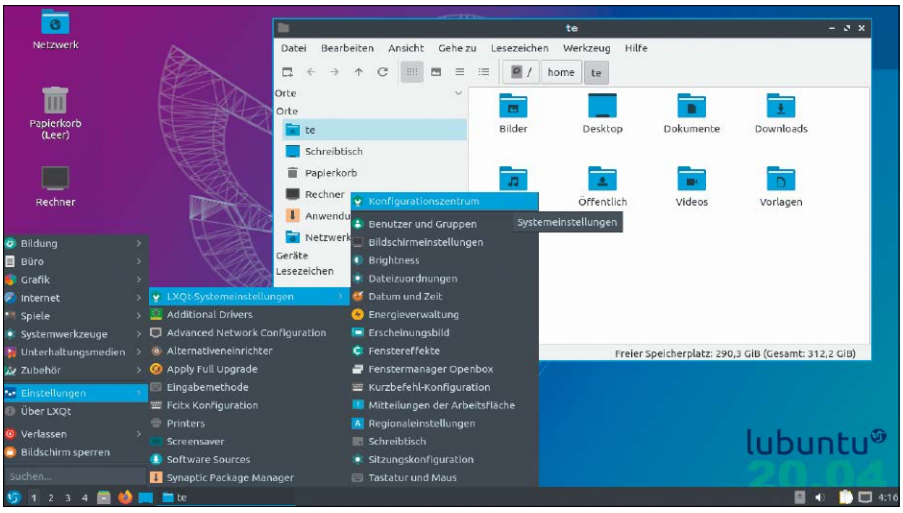
Distributionen: Xubuntu 20.04 LTS ist als offizielle Ubuntu-Variante wahrscheinlich die beste Wahl für ein System mit XFCE-Desktop. XFCE gibt es ohne besondere Anpassungen auch bei Fedora oder Open Suse. Die schicke Distribution Voyager demonstriert, was mit XFCE möglich ist. Die Distribution basiert auf Xubuntu oder Debian und hat den Desktop im Mac-OS-Design gestaltet. Prägendes Merkmal ist das Dock am unteren Bildschirmrand. Das typische XFCE-Panel ist ebenfalls vorhanden, daneben weitere Leisten für spezielle Funktionen. Das System wird mit mehreren Desktopstilen und Hintergrundbildern ausgeliefert, über die sich Gestaltung und Farbgebung anpassen lassen.

LXQT: Leicht und schnell

Das „L“ in LXQT steht für leichtgewichtig („Lightweight X11 Desktop Environment“, *https://lxqt-project.org*). Das Ziel der Entwickler ist ein besonders schlanker Desktop, der sich auch auf leistungsschwacher Hardware gut verwenden lässt. „QT“ weist auf das verwendete GUI-Toolkit Qt hin, das auch KDE verwendet.

LXQT bleibt beim bewährten Konzept. Eine Leiste am unteren Bildschirmrand mit einem einfachen Startmenü, Schnellstarter, Taskleiste und Symbole etwa für Netzwerk und Lautstärkeregelung. Die Leiste lässt sich konfigurieren. Wie bei KDE und XFCE sind Menü und Anwendungsstarter einzelne Elemente, die sich beliebig verschieben lassen. Die Leiste lässt sich ebenfalls an allen Bildschirmrändern andocken. Bei Bedarf können weitere Leisten mit unterschiedlichen Bedienelementen erstellt werden.

Design und Leistung: In puncto Ästhetik ist LXQT zwischen KDE und XFCE angesiedelt. Bedienelemente und Fenster sind ansprechend gestaltet, die Farbgebung ist angenehm. Wirklich modern sieht die Oberfläche aber nicht aus. Dafür ist der Ressour-



LXQT-Desktopumgebung: Lubuntu zeigt ein einfaches Startmenü mit klassischen Funktionen. Die Darstellung ähnelt teilweise KDE, ohne dessen feine Zeichnungen zu erreichen.

cenbedarf nicht besonders hoch und die Desktopoberfläche lässt sich flüssig bedienen. Einige Benutzer mag es stören, dass bei LXQT in einigen Bereichen die deutschen Übersetzungen fehlen und daher Teile der Einstellungen nur in englischer Sprache erscheinen.

Einstellungen: Über das Menü und „Einstellungen → LXQt-Systemeinstellungen“ lässt sich das „Konfigurationszentrum“ aufrufen, das beispielsweise zu „Bildschirmeinstellungen“ oder „Datum und Zeit“ führt. Man kann die einzelnen Optionen auch direkt unter „LXQt-Systemeinstellungen“ ansteuern. Über „Erscheinungsbild“ kann man den „Widget Style“ wählen. Die Vorgabe ist „Breeze“. Wählt man „Windows“, versprüht der Desktop den spröden Charme der 90er-Jahre (Windows 95). Bei „Icon Theme“ und „LXQt Theme“ gibt es einige wenige Themes zur Auswahl. Die Darstellung lässt sich im „Konfigurationszentrum“ auch über „Fenstermanager Openbox“ beeinflussen, wo es mehr Themes zur Auswahl gibt.

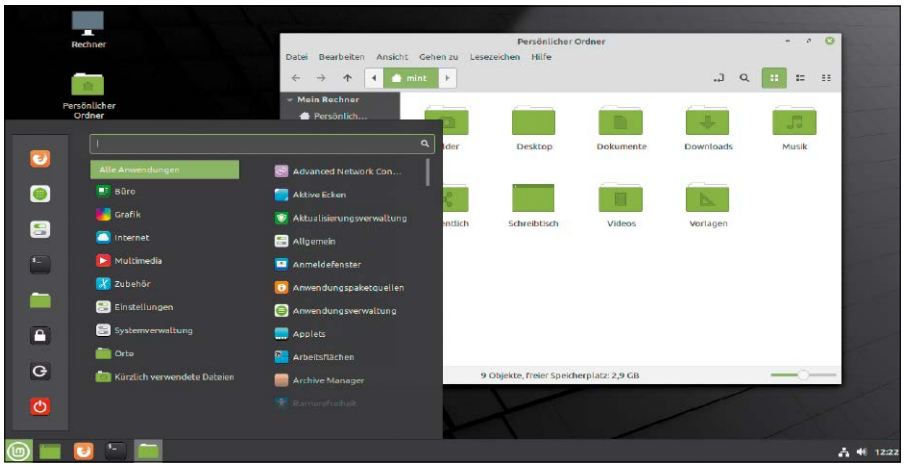
Standardsoftware: Zu LXQT gehören der Dateimanager Pcmanfm-Qt, der Bildbetrachter Lximage-Qt und das Qterminal. Besondere Überraschungen hat die Software nicht zu bieten. Sie integriert sich jedoch gut in die Desktopoberfläche und liefert die wichtigsten Funktionen.

Distributionen: LXQT-Editionen gibt es beispielsweise von Ubuntu (Lubuntu) und Fedora. Die Desktopumgebung lässt sich außerdem bei Debian, Open Suse und Manjaro installieren.

Cinnamon: Der robuste Klassiker

Cinnamon (*https://github.com/linuxmint/cinnamon*) orientiert sich an klassischen Desktops wie Gnome 2, Windows XP und Windows 7. Es gibt ein Startmenü mit Suchfunktion, das Kategorien wie „Büro“, „Grafik“ und „Multimedia“ zeigt. Es genügt, mit der Maus über die Kategorien zu fahren, der Inhalt zeigt sich dann in der rechten Hälfte des Fensters. Ganz links gibt es einige Schaltflächen, die zu den „Favoriten“-Programmen führen. Die Reihenfolge lässt sich ändern, man kann Programme hinzufügen oder entfernen.

Die Leiste am unteren Bildschirmrand dient als Taskleiste und zeigt laufende Programme als Icon an. Per rechtem Mausklick und „An der Leiste anheften“ lässt sich ein Programm dauerhaft in der Leiste unterbringen, die damit auch als Schnellstarter dient. Die Elemente der Leiste sind „Applets“, die sich beliebig verschieben oder löschen lassen. Cinnamon bietet standardmäßig nur wenige Applets an, weitere kann man jedoch herunterladen (siehe ab Seite 26).



Linux-Mint: Die Cinnamon-Desktopumgebung kommt bei der Bedienung ehemaligen Windows-Nutzern entgegen. Die Oberfläche ist gut anpassbar, Leisten lassen sich beliebig bearbeiten.

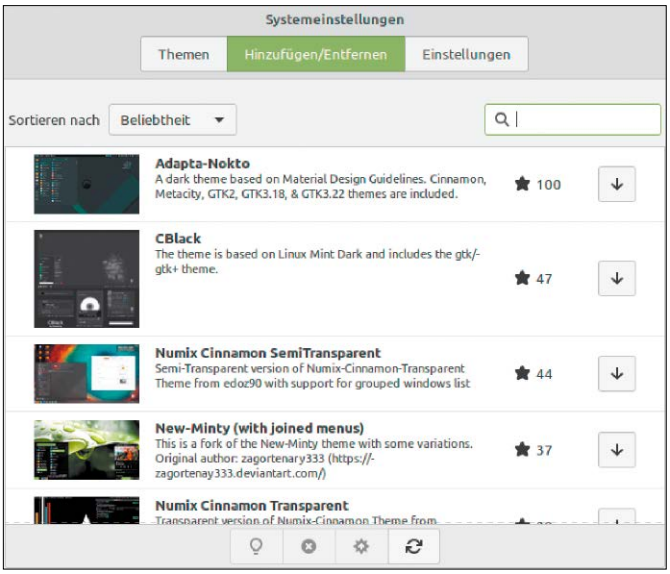
Der Desktop lässt sich standardmäßig als Dateiablage nutzen. Sie können Ordner, Dokumente oder Programmverknüpfungen darauf ablegen.

Design und Leistung: Die Cinnamon-Oberfläche ist zwar schlicht, aufgrund einer gelungenen Farbgebung und präzisen Schriftdarstellungen aber angenehm anzusehen. Cinnamon ist bei den Systemressourcen nicht besonders anspruchsvoll und läuft daher auch auf älterer Hardware. Für Geräte mit weniger als vier GB RAM und schwachem Grafikchip ist aber eher XFCE zu empfehlen.

Einstellungen: Alle Optionen sind bequem über die „Systemeinstellungen“ erreichbar. Themen und Hintergrundbilder für die Arbeitsfläche sind mit wenigen Mausklicks geändert. Zusätzliche Themen lassen sich auf der Registerkarte „Hinzufügen/Entfernen“ herunterladen.

Standardsoftware: Zu Cinnamon gehören Programme wie der Texteditor Xed, der Bildbetrachter Xviewer und der Dokumentbetrachter Xreader. Alle basieren auf bekannten Open-Source-Anwendungen, wurden von den Entwicklern aber angepasst, um sich besser in Cinnamon zu integrieren.

Distributionen: Cinnamon ist eine Eigenentwicklung des Linux-Mint-Teams. Die Desktopumgebung lässt sich auch in anderen Systemen installieren, beispielsweise Ubuntu oder Fedora. Der Desktop ist vor allem bei Windows-Umsteigern beliebt. ■



Desktopthemen: Linux Mint wird mit zahlreichen Stilen ausgeliefert. Wenn nichts Passendes dabei ist, lassen sich weiter Designs herunterladen.

Desktoptipps für Gnome & KDE

Gnome bietet kaum Einstellungen, KDE dafür sehr viele. Trotzdem lassen sich beide Desktopumgebungen sehr gut anpassen. Bei Gnome benötigt man dafür jedoch einige Tools, während man bei KDE nur die richtige Option finden muss.

VON THORSTEN EGGELING

Hinter Gnome und KDE stehen unterschiedliche Bedienkonzepte der Entwickler. Gnome soll möglichst übersichtlich und reduziert sein, KDE spricht eher Individualisten an. Viele Benutzer bevorzugen Gnome trotzdem, wünschen sich aber an der einen oder anderen Stelle etwas mehr Komfort und Einfluss. Das sehen auch andere so, weshalb es für Gnome etliche Erweiterungen gibt, mit denen sich die Oberfläche anpassen lässt. Die muss man jedoch erst finden und einrichten. KDE bietet dagegen schon von Haus aus zahlreiche Möglichkeiten, die man aber erst entdecken muss. Bei beidem hilft dieser Artikel.



Der Standard-Gnome-Desktop: Gnome schneidet optisch insgesamt nicht schlecht ab, jedoch ist die Anwendungsübersicht mit großen Icons für Desktop-PCs kaum geeignet.

Gnome-Desktop erweitern

Gnome unterstützt Schnittstellen, über die sich der Desktop ausbauen lässt. Einzelne Bestandteile kann man ersetzen, beispielsweise das Menü. Das Panel lässt sich mit zusätzlichen Icons und Funktionen ausstatten. Wir haben die Tipps und Anleitungen unter Ubuntu 20.04 LTS ausprobiert. Bei anderen Systemen mit Gnome können eventuell abweichende Schritte nötig sein.

Gnome für Erweiterungen vorbereiten: Mehrere Gnome-Shell-Erweiterungen lassen sich über die Ubuntu-Standard-Paketquellen installieren. Wer weitere oder neuere benötigt, verwendet das offizielle Verzeichnis *https://extensions.gnome.org* im Webbrowser. Dafür sind Vorbereitungen erforderlich.

Schritt 1: Installieren Sie über *https://m6u.de/GNSH* die Firefox-Erweiterung Gnome Shell Integration. Wenn Sie Google Chrome nutzen, finden Sie für den Browser eine passende Erweiterung im Chrome Web Store über *https://m6u.de/GNCH* (siehe auch Kasten „Gnome-Erweiterungen in Ubuntu 21.10“).

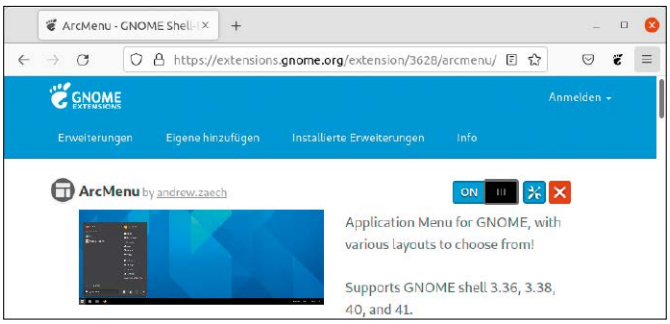
Schritt 2: In einem Terminal (Strg-Alt-T) installiert man ein zusätzliches Paket:

```
sudo apt install chrome-gnome-shell
```

Schritt 3: Zur Verwaltung der Erweiterungen und für einige weitere Einstellungen empfiehlt sich das weitere Tool Gnome Tweaks. Es lässt sich im Terminal mit

```
sudo apt install gnome-tweaks
```

installieren. Deutschsprachiges Ubuntu zeigt das Tool bei einer Suche nach „Tweaks“ oder „Optimierunge“n über „Aktivitäten“ als „Optimierungen“ an. Zusammen mit Gnome Tweaks wird unter Ubuntu



Erweiterungen für Gnome einrichten: Im Browser kann man über *https://extensions.gnome.org* neue Erweiterungen direkt aktivieren und auch konfigurieren.

20.04 automatisch das Paket „gnome-shell-extension-prefs“ eingerichtet. Dabei handelt es sich um ein neueres Tool zur Verwaltung und Konfiguration. Sie finden es über eine Suche nach Erweiterungen.

Hinweis: Die Gnome-Erweiterungen müssen zur verwendeten Gnome-Shell passen. Bei der Installation über *https://extensions.gnome.org* wird die Version automatisch ermittelt. Ist die Erweiterung dafür noch nicht verfügbar, wird der Hinweis „Incompatible“ angezeigt. Welche Gnome-Version installiert ist, kann dieser Terminalbefehl ermitteln:

```
gnome-shell --version
```

Bei Ubuntu 20.04 LTS handelt es sich zur Zeit um Version 3.36.9.

Gnome: Schwebendes Dock für Ubuntu

Die Erweiterung Floating Dock ermöglicht ein frei platzierbares Dock auf dem Gnome-Desktop. Es lässt sich nicht nur beliebig verschieben, sondern auch horizontal oder vertikal positionieren und ausblenden. Zur Installation gehen Sie auf *https://extensions.gnome.org/extension/2542*, setzen den Schalter rechts oben auf „On“ und klicken auf „Installieren“. Floating Dock wird sofort mit einem blauen, verschiebbaren Icon mit drei weißen Punkten sichtbar. Ein Klick darauf öffnet das Dock. Nach einem rechten Mausklick auf das Icon erscheinen einige Symbole. Über die Pfeile lässt sich die Ausrichtung ändern. Außerdem gibt es Icons für Abmelden, Sperren, Ausschalten und Bereitschaft.

Gnome: Ubuntu Dock ersetzen

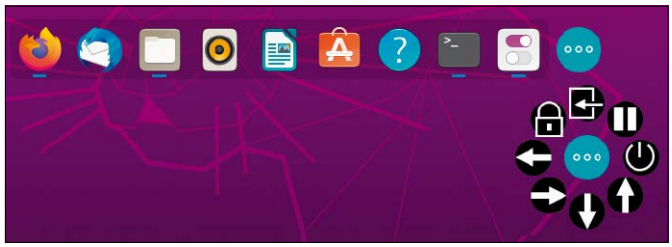
Ubuntu 20.04 verwendet standardmäßig die Gnome-Erweiterung Ubuntu Dock für die Favoritenleiste am linken Rand des Bildschirms. Dabei handelt es sich um eine modifizierte Version von Dash to Dock. Das Original ist aber eigentlich besser und funktionsreicher. Zur Installation gehen Sie auf *https://extensions.gnome.org/extension/307*, setzen den Schalter rechts oben auf „On“ und klicken auf „Installieren“. Die neue Leiste wird sofort aktiviert, was an den etwas größeren Abständen der Icons zu erkennen ist.

Öffnen Sie „Optimierungen“ und gehen Sie auf „Erweiterungen“. Oder Sie starten „Erweiterungen“, was die gleichen Optionen bietet. Klicken Sie auf das Zahnradsymbol bei „Dash to dock“. Auf der ersten Registerkarte „Position und Größe“ lässt sich die Position des Docks auf dem Bildschirm festlegen. Alle vier Seiten sind möglich.

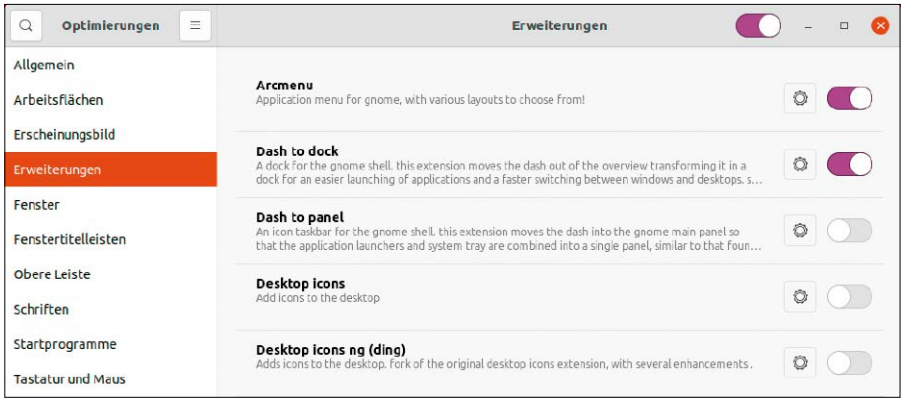
Es lässt sich außerdem einstellen, ob das Dock automatisch ausgeblendet werden soll. Bei der Option ist eine Schaltfläche mit Zahnradsymbol zu finden, das zu weiteren Einstellungen führt. Standardmäßig ist „Fester ausweichen“ aktiviert. Das Dock wird dann nur ausgeblendet, wenn kein Fenster es überdeckt. Ist die Option deaktiviert, lässt sich das Dock einblenden, indem man mit dem Mauszeiger schnell an die Bildschirmkante fährt.

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. Das entspricht der Funktion der Taskleiste in Windows.



Floating Dock: Diese Dock-Variante lässt sich auf dem Bildschirm beliebig verschieben. Das Kontextmenü bietet einen Schnellzugriff beispielsweise auf Ausschalt-Optionen.



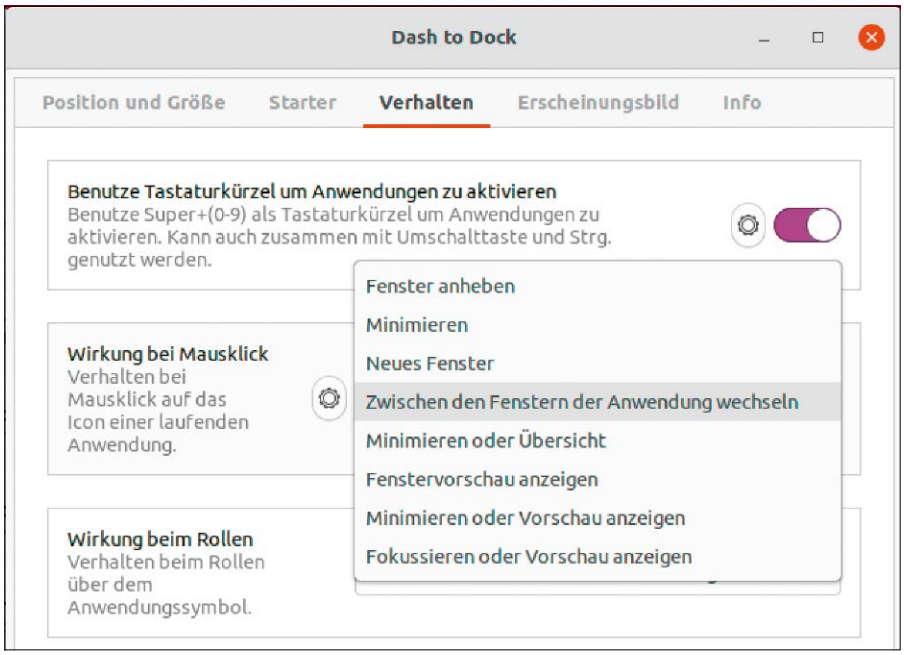
Gnome-Tweak-Tool: Unter „Erweiterungen“ sind die installierten Gnome-Tools aufgeführt. Sie lassen sich hier aktivieren und über die Schaltfläche mit dem Zahnradsymbol konfigurieren.

GNOME-ERWEITERUNGEN IN UBUNTU 21.10

Bei Ubuntu 21.10 gibt es einige Änderungen, die die Installation von Gnome-Erweiterungen erschweren. Zur Zeit lässt sich die Erweiterung Gnome Shell Integration in Firefox nicht nutzen. Eine Abhilfe ist es, zuerst die Snap-Version von Firefox entfernen und diesen als DEB-Paket zu installieren:

```
sudo snap remove firefox
sudo apt install firefox firefox-locale-de
```

Alternativ dazu kann man auch Google Chrome (*https://www.google.de/chrome*) und die dazugehörige Erweiterung installieren (*https://m6u.de/GNCH*). Der Chromium-Browser wäre theoretisch auch möglich. Der liegt aber ausschließlich als Snap-Paket vor und auch hier funktioniert Gnome Shell Integration nicht. Über das Gnome-Tweak-Tool lassen sich Erweiterungen nicht mehr verwalten. Dafür dient jetzt ausschließlich das Systemtool „Erweiterungen“. Ab April 2022 erscheint Ubuntu 22.04. Noch ist unklar, ob die Probleme damit Geschichte sind.



Dash to Dock: Bei dieser Erweiterung können Sie einstellen, was der Mausklick auf ein Dock-Icon bewirkt. Standard ist „Zwischen den Fenstern der Anwendungen wechseln".

Ubuntu Dock entfernen: Es ist möglich, Dash to Dock und Ubuntu Dock parallel zu installieren. Das Ubuntu Dock lässt sich allerdings nicht vollständig deaktivieren, läuft im Hintergrund weiter und benötigt RAM. Außerdem wird es im Hintergrund manchmal sichtbar, etwa wenn man auf „Aktivitäten" klickt. Wen das stört, der kann das Ubuntu Dock im Terminal mit

```
sudo apt remove gnome-shell-
  extension-ubuntu-dock
```

beseitigen. Dabei werden auch die Pakete „ubuntu-desktop" und „ubuntu-desktop-minimal" deinstalliert. Das hat keine weiteren Auswirkungen, außer bei einem Systemupgrade auf die nächste Ubuntu-Version. Sobald dieses ansteht, sollten Sie die entfernten Pakete mit

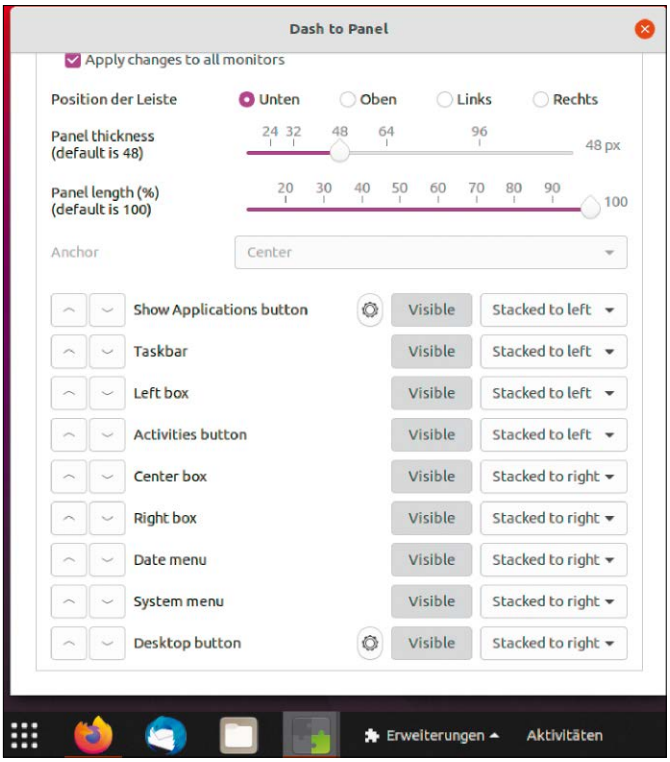
```
sudo apt install gnome-shell-
  extension-ubuntu-dock ubuntu-
  desktop ubuntu-desktop-minimal
```

wieder nachinstallieren.

Gnome: Panelleiste statt Dock verwenden

Eine eher traditionelle Taskleiste lässt sich mit der Erweiterung Dash to Panel nachbilden, die das Favoritendock mit dem Hauptpanel zusammenführt. Gehen Sie auf *https://extensions.gnome.org/extension/1160* und aktivieren Sie die Erweiterung. Die Leiste erscheint sofort am unteren Bildschirmrand.

Ganz links ist das Icon „Anwendungen anzeigen" zu sehen, das als Startmenü dient und zur Anwendungsübersicht und zur Suche führt. Ein rechter Mausklick darauf blendet ein Menü für die schnelle Navigation ein, beispielsweise zu „Energieoptionen" und „Festplattenverwaltung" sowie zu „Extensions" und „Erweiterungseinstellungen".



Dash to Panel: Die Reihenfolge der Elemente auf der Leiste kann geändert werden. Damit lässt sich vermeiden, dass Größenänderungen des Menüs die Taskbar verschieben.

Auf „Anwendungen anzeigen" folgen die Favoriten-Icons aus dem Dock. Laufende Programme erscheinen hier ebenfalls mit ihren Icons und die aktiven Programme sind mit einem farbigen Strich an der Unterseite des Icons markiert.

Dash to Panel lässt sich auf dem gleichen Weg konfigurieren wie zuvor bei Dash to Dock beschrieben. Es lässt sich die Position der Leiste, deren Höhe und Länge festlegen. Auf der Registerkarte „Verhalten" kann man die Option „Anwendungsmenü-Schaltfläche anzeigen" aktivieren. Damit wird das Menü der jeweils aktiven Anwendung angezeigt, das sonst bei Gnome standardmäßig im Panel untergebracht ist. Bei Gnome enthält dieses allerdings nicht viele Menüpunkte. Meist ist nur „Neues Fenster" oder Ähnliches enthalten. Wenn Sie das Anwendungsmenü einblenden, sollten Sie auf der Registerkarte „Position" die Reihenfolge der Elemente anpassen. Ansonsten verschiebt sich die Leiste ständig, wenn das Menü seine Breite ändert. Bewegen Sie „Taskbar" mit der Pfeil-Schaltfläche über „Left Box". Das Anwendungsmenü wird dann weiter rechts untergebracht und seine Größe wirkt sich nicht mehr auf die Taskbar aus.

Auf der Registerkarte „Aktion" bietet Dash to Panel Einstellungen für „Klickaktion". Standard ist die Option „Fenster durch-

wechseln + minimieren“. Ein Klick auf das Icon holt ein minimiertes Fenster in den Vordergrund, ein erneuter Klick minimiert es wieder. Sind mehrere Fenster einer Anwendung geöffnet, wechselt jeder Klick zum nächsten Fenster. Beim letzten angekommen, wird es minimiert. Stellt man „Fenster umschalten“ ein, werden einzelne oder alle Fenster einer Anwendung bei jedem Klick minimiert oder wiederhergestellt. Fährt man mit der Maus über eine Icongruppe, sieht man in jedem Fall eine Vorschau und kann per Klick zum gewünschten Fenster wechseln.

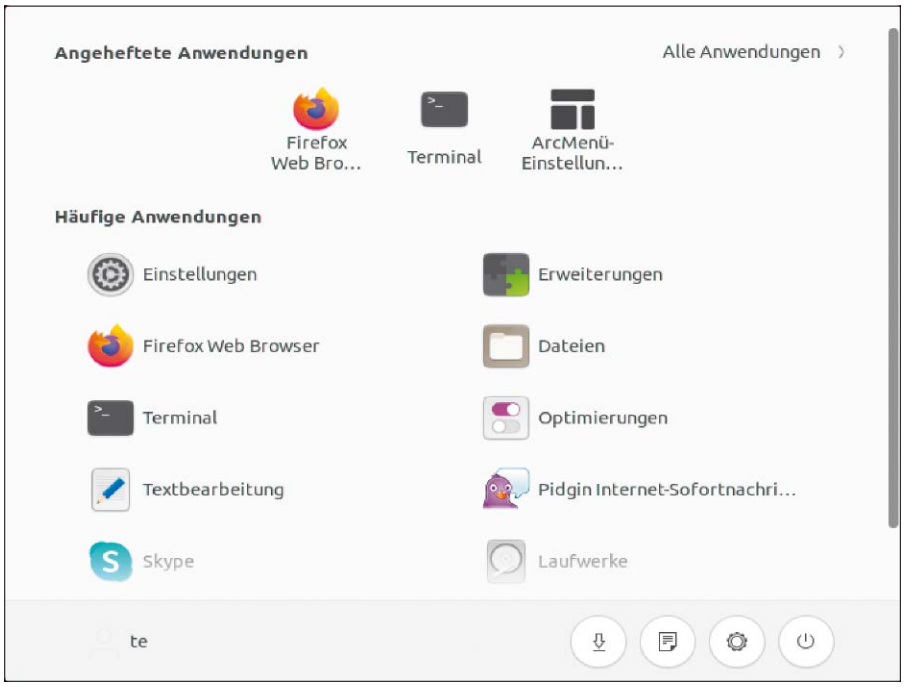
Gnome: Startmenü nachrüsten

Die Auswahl eines Programmstarters oder die Suche über „Aktivitäten“ ist sicher für viele Benutzer ausreichend. Bei Bedarf lässt sich aber auch ein klassisches Startmenü einbauen. Dafür installieren Sie Arc Menu über *https://extensions.gnome.org/extension/3628*. Bei einer Standardinstallation ersetzt Arc Menu das bisherige „Aktivitäten“, die sich aber weiterhin über die Super-Taste (Windows-Taste) aufrufen lassen. Das Menü zeigt die angehefteten Anwendungen und auf der rechten Seite gelangt man beispielsweise schnell zu „Persönlicher Ordner“ oder zu „Downloads“. Schaltflächen für Neustart oder Ausschalten sowie ein Suchfeld sind ebenfalls vorhanden. Ein Klick auf „Alle Programme“ führt zu einer Übersicht der installierten Anwendung in einer Kategorienansicht. Für die Konfiguration klickt man im Menü auf „ArcMenü-Einstellungen“. Der Dialog ist – wie bei den anderen Erweiterungen auch – ebenfalls über Gnome Tweaks oder Erweiterungen ansteuerbar. Unter „Menü-Layout“ stehen zahlreiche Ansichten zur Verfügung. Gehen Sie auf „Modern-Menü-Layouts“ und wählen Sie „Windows“ für ein Menü im Windows-10-Stil. Hinter „Elf“ verbirgt sich ein Design ähnlich dem von Windows 11.

Das Gno-Menü ist ein weiteres, angenehm gestaltetes Menü für Gnome. Es zeigt ein Layout in einem ähnlichen Stil wie Windows 10. Zusätzlich baut die Erweiterung die Schaltflächen „View“ („Aktivitäten“) und „Apps“ („Anwendungen anzeigen“) in das Panel ein. Die Installation über *https://extensions.gnome.org/extension/608* funktioniert derzeit nur bis Gnome Shell 3.34 und somit nicht unter Ubuntu 20.04. Eine angepasste Version für Gnome 3.36, 3.38 und 40 kann man unter *https://giacomoblog.info/blog/gnomenu-revisited* herunterladen. Für die Installation verwenden Sie diese Befehlszeile

```
gnome-extensions install gnomenu@
  panacier.gmail.com.zip
```

im Terminal, und dies im Download-Verzeichnis.



Arc Menu: Dieses Menü ist Windows 10 nachempfunden und lässt sich als Gnome-Erweiterung einfach in die Panelleiste integrieren. Das Menü bietet verschiedene Layouts.

Gnome: Anzeige der Tray-Icons verbessern

Bei Ubuntu ist die Gnome-Erweiterung Ubuntu Appindicators bereits vorinstalliert. Anwendungen können daher Icons etwa für Benachrichtigungen im Panel anzeigen. Das funktioniert jedoch nicht mit einigen älteren Programmen, außerdem lässt sich die Darstellung nicht verändern.

Eine Alternative ist die Erweiterung Tray Icons Reloaded, die Sie über *https://extensions.gnome.org/extension/2890* installieren. Über „Erweiterungen“ oder Gnome Tweaks deaktivieren Sie anschließend Ubuntu Appindicators und aktivieren stattdessen Tray Icons Reloaded. In den Einstellungen der Erweiterung lassen sich beispielsweise die Größe der Icons, Kontrast und Helligkeit anpassen.

Gnome: Icons auf dem Desktop

Gnome zeigt standardmäßig keine Icons auf dem Desktop. Bei Ubuntu sind immerhin die Icons für „Persönlicher Ordner“ und „Papierkorb“ zu sehen. Dafür sorgt die bereits vorinstallierte Gnome-Erweiterung Desktop Icons. Auch dafür gibt es einen leicht verbesserten Ersatz. Installieren Sie Desktop Icons NG über *https://extensions.gnome.org/extension/2087*. Über „Erweiterungen“ deaktivieren Sie die bisherige Erweiterung und aktivieren stattdessen Desktop Icons NG.

Die Konfiguration erreichen Sie per rechtem Mausklick auf einen freien Bereich des Desktops und „Einstellungen“. Sie können festlegen, ob Sie den persönlichen Ordner oder den Papierkorb auf dem Desktop unterbringen wollen. Das konnte aber auch schon die Ubuntu-Erweiterung. Bei Desktop Icons NG lässt sich aber zusätzlich die Anzeige externer Laufwerke und von Netzwerklaufwerken aktivieren oder deaktivieren.

Gnome: Verknüpfungen auf dem Desktop

Über das Kontextmenü des Gnome-Desktops oder per Drag & Drop vom Dateimanager aus ist es nicht möglich, Starter-Verknüpfungen zu Programmen oder Ordnern auf dem Desktop abzulegen. Mit einem Trick geht es aber doch. Für Programmverknüpfungen gehen Sie so vor:

Schritt 1: Öffnen Sie den Dateimanager und gehen Sie in den Ordner „/usr/share/



Mehr Funktionen für den Desktop: Auch auf dem Gnome-Desktop lassen sich Verknüpfungen erstellen. Man muss allerdings die „.desktop"-Datei manuell kopieren und deren Start erlauben.

applications". Suchen Sie die gewünschte Anwendung, beispielsweise Firefox („firefox.desktop").

Schritt 2: Kopieren Sie die Datei in den Ordner „Schreibtisch" in Ihrem Home-Verzeichnis. Direktes Kopieren auf den Desktop ist nicht möglich.

Schritt 3: Klicken Sie die Datei mit der rechten Maustaste an, wählen Sie „Eigenschaften" und gehen Sie auf „Zugriffsrechte". Setzen Sie ein Häkchen vor „Datei als Programm ausführen".

Schritt 4: Klicken Sie die „.desktop"-Datei auf dem Desktop mit der rechten Maustaste an und wählen Sie „Start erlauben".

Wenn Sie eine Verknüpfung zu einem Ordner erstellen möchten, öffnen Sie ein Terminal. Folgender Befehl

```
ln -s ~/Downloads/ ~/Schreibtisch/
```

genügt, um am Desktop eine Verknüpfung zum Ordner „Downloads" in Ihrem Home-Verzeichnis anzulegen.

KDE individuell konfigurieren

KDE Plasma ermöglicht von Haus aus und ohne zusätzliche Tools zahlreiche Anpassungen. Die gewünschten Elemente oder Designs lassen sich über die grafische Oberfläche einrichten. Was fehlt, kann man bequem herunterladen und mit wenigen Mausklicks installieren. Die Tipps und Anleitungen haben wir unter Kubuntu 20.04 ausprobiert. Bei neueren Versionen können die Beschriftungen und Menüpunkte abweichen.

KDE: Leisten hinzufügen und bearbeiten

KDE Plasma 5 liefert in allen Linux-Distributionen einen traditionellen Desktop mit einem horizontalen Panel am unteren Bildschirmrand. Darin enthalten sind das Anwendungsmenü, die Taskleiste und der Infobereich beispielsweise mit Uhr und Lautstärkeregler. Vor allem bei eher breiten als hohen Notebookdisplays ist das nicht optimal. Hier ist eine zusätzliche seitliche Leiste beispielsweise als Favoritenstarter für häufig benötigte Anwendungen sinnvoll. Das schafft dann auch Platz auf der horizontalen Leiste für die laufenden Programme, die man dann nicht mehr gruppieren muss. In KDE ist der kleine Umbau ohne Erweiterungen möglich.

Schritt 1: Klicken Sie mit der rechten Maustaste auf die vorhandene Leiste am unteren Bildschirmrand und gehen Sie auf „Kontrollleiste bearbeiten". Fahren Sie mit dem Mauszeiger über die Leiste. Sie sehen dann die Bezeichnungen der unterschiedlichen Elemente. Bei „Fensterleiste" klicken Sie auf „Entfernen". Klicken Sie auf die Schaltfläche „Bildschirmkante", halten Sie die Maustaste gedrückt und ziehen Sie die Leiste an den linken Bildschirmrand. Dann klicken Sie auf das Symbol „Schließen" (rotes Kreuz) oder einfach auf einen freien Bereich des Desktops, um die Bearbeitung zu beenden.

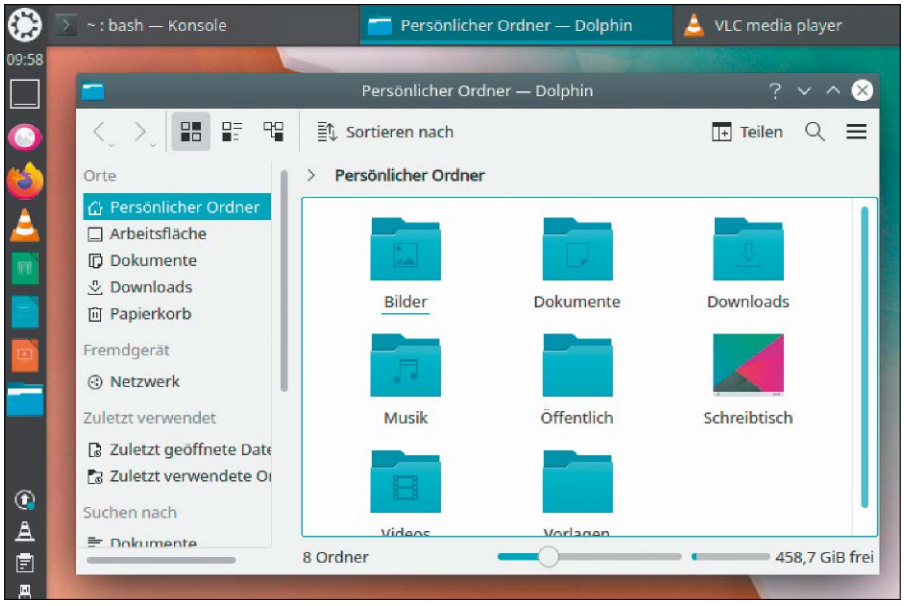
Schritt 2: Jetzt kommt die zweite Leiste nach einem Rechtsklick auf den Desktophintergrund und „Kontrollleiste hinzufügen → Leere Kontrollleiste" hinzu. Die neue Leiste erscheint unten auf dem Bildschirm. Nach einem rechten Mausklick darauf wählen Sie „Kontrollleiste bearbeiten", klicken auf „Bildschirmkante" und ziehen die Leiste an den oberen Rand.

Schritt 3: Sie befinden sich weiter im Bearbeitungsmodus und klicken auf die „+"-Schaltfläche („Miniprogramme hinzufügen"). Per Doppelklick fügen Sie „Fensterleiste" zur horizontalen Leiste hinzu.

Schritt 4: Die horizontale und die vertikale Leiste überlappen sich in der linken Ecke. Um das zu ändern, klicken Sie – weiterhin im Bearbeitungsmodus der horizontalen Leiste – auf den rechten Anfasser im grauen Bereich.

Reduzieren Sie die Länge um die Breite der vertikalen Leiste. Ein Klick auf das Regler-Symbol rechts unter der Leiste öffnet das Menü „Ausrichtung der Kontrollleiste". Klicken Sie auf „Rechts". Damit entsteht auf der linken Seite der gewünschte Abstand zur vertikalen Leiste. Beenden Sie den Bearbeitungsmodus.

Schritt 5: Öffnen Sie das Anwendungsmenü, suchen Sie häufig genutzte Anwendungen und klicken Sie jeweils im Kontextmenü auf „Zu Kontrollleiste hinzufügen (Miniprogramm)".



Mehr Leisten: Vor allem bei breiten Displays lohnt sich eine zusätzliche vertikale Leiste. Diese kann zum Beispiel die Icons für die Favoritenprogramme aufnehmen.



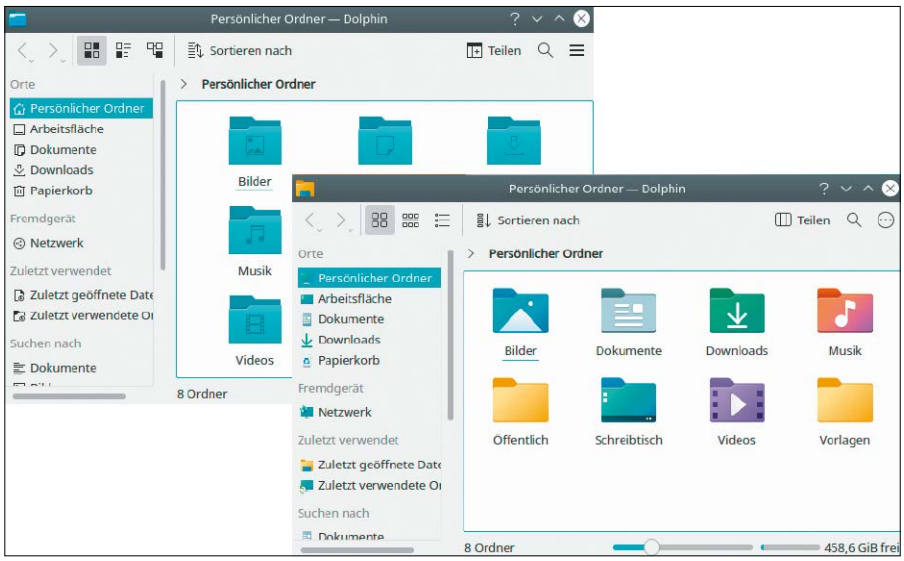
Menü für die Menüs: Der Kontextmenüpunkt „Alternative anzeigen“ liefert eine Liste der verfügbaren Miniprogramme. Darüber lässt sich schnell zu einem anderen Menü wechseln.

Schritt 6: Gehen Sie bei der vertikalen Leiste im Kontextmenü auf „Kontrollleiste bearbeiten“. Fügen Sie einen Abstandshalter zwischen dem Systemabschnitt und den Anwendungsstartern hinzu. Der Systemabschnitt wird damit nach unten verschoben.

KDE: Das Menü austauschen

Das Anwendungsmenü von KDE 5.16 in Ubuntu 20.04 ist mit seiner Kategorienansicht und den Favoriten-Icons zwar funktional, wirkt aber nicht mehr besonders modern. Über einen rechten Mausklick und „Alternativen anzeigen“ lässt sich das Menü ändern. Zur Auswahl stehen das großformatige Menü „Anwendungs-Starter“ und die „Anwendungsübersicht“ für eine Vollbilddarstellung.

Noch mehr Auswahl gibt es über einen rechten Mausklick und „Miniprogramme hinzufügen“. Gehen Sie auf „Neue Miniprogramme herunterladen“ und installieren Sie beispielsweise „Menu 11“ im Windows-11-Stil oder „Tiled Menu“ im Stil von Windows 10. Gehen Sie erneut auf „Miniprogramme hinzufügen“ und wählen Sie das gewünschte Menü per Doppelklick aus. Im Bearbeitungsmodus schieben Sie es dann an die gewünschte Position und entfernen dann das bisherige Menü.



Abwechslungsreiche Icons: Ein neues Icon-Paket ist in KDE schnell installiert. Der KDE-Standard im Dateimanager ist links zu sehen, rechts hingegen ein Set mit Windows-11-Icons.

KDE: Neue Icons

Die Icons sind bei KDE Plasma standardmäßig recht ansehnlich. Wer möchte, kann aber auch andere Icon-Sammlungen installieren. Dazu geht man in den Systemeinstellungen auf „Symbole“. Hier kann man dann eines der vorinstallierten Pakete wählen und per Klick auf „Anwenden“ aktivieren. Eine größere Auswahl weiterer Icon-Sets erhält man nach einem Klick auf „Neue Symbole herunterladen“. Beim gewünschten Angebot, beispielsweise „Win11 Icon Theme“ genügt dann ein Klick auf „Installieren“. Zurück in den Systemeinstellungen lässt sich die neue Icon-Sammlung aktivieren. ■

DESKTOPUMGEBUNG WECHSELN

Linux-Nutzer sind nicht auf eine Desktopumgebung festgelegt. Sie können sogar mehrere Desktopumgebungen nebeneinander installieren und dann die gewünschte Arbeitsfläche im Anmeldebildschirm auswählen. Das funktioniert unter Ubuntu und Linux Mint. Bei der Installation einer kompletten Desktopumgebung werden allerdings zahlreiche Pakete heruntergeladen und beim ersten Start legt jede Variante eigene Konfigurationsdateien an oder ändert bestehende Einstellungen. Der Eingriff in das System ist relativ umfangreich und nicht immer vollständig rückgängig zu machen. Eine erwartbare Nebenwirkung ist beispielsweise, dass Theme-Elemente der einen Desktopumgebung auch in einer anderen auftauchen. Es ist daher grundsätzlich die bessere Wahl, gleich eine Distribution mit der bevorzugten Desktopumgebung zu installieren.

Wer trotzdem einen weiteren Desktop installieren möchte, sollte in jedem Fall – wie vor allen größeren Änderungen am System – ein Backup der Dateien im Home-Verzeichnis oder besser des gesamten Systems erstellen.

Am einfachsten ist die Installation der Meta-Pakete. Damit wird aus einem Ubuntu mit Gnome-Desktop beispielsweise ein Kubuntu oder Xubuntu. Die Meta-Pakete heißen „kubuntu-desktop“ (KDE), „xubuntu-desktop“ (XFCE), „lubuntu-desktop“ (LXQT) und „cinnamon“ (Cinnamon-Desktop). Die Installation erfolgt einfach im Terminal mit

```
sudo apt install [Metapaketname]
```

Danach müssen meistens noch einige Sprachpakete eingerichtet werden, was in den „Einstellungen“ über „Region und Sprache → Installierte Sprachen verwalten“ erfolgen kann.

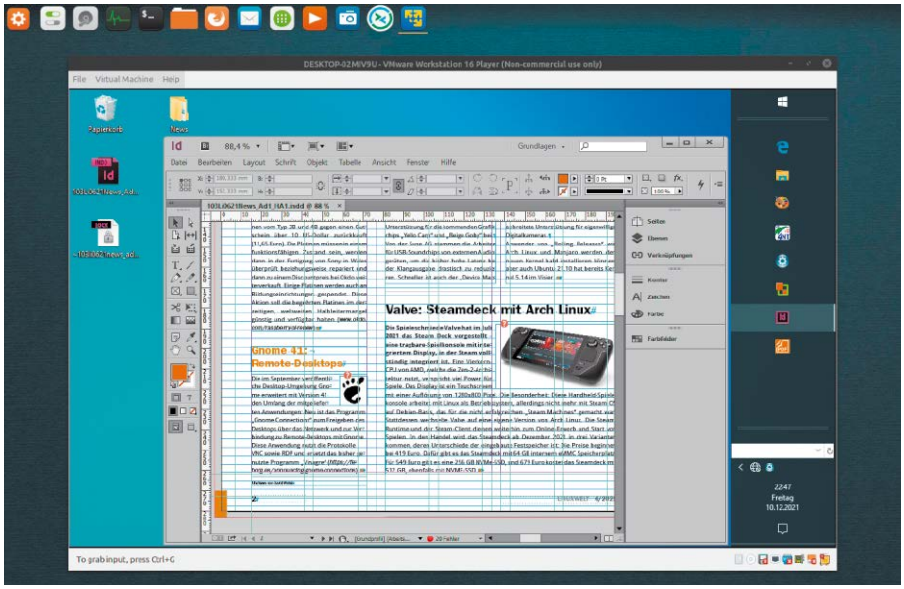
Dualboot und Virtualisierung

Die Scheu, ein Windows komplett über Bord zu werfen, ist nachvollziehbar und absolut berechtigt, wenn Linux unentbehrliche Windows-Software nicht adäquat ersetzen kann. Es bieten sich zwei Lösungen an – vorübergehend oder auch dauerhaft.

VON HERMANN APFELBÖCK

Die Hardware nach Bedarf mit Linux oder Windows zu booten, ist eine bewährte Möglichkeit, Windows und Software (inklusive Lizenzen) zu erhalten und sich andererseits im Nutzeralltag zunehmend an Linux zu halten. Technisch ist Dualboot eine relativ anspruchslose Lösung, die lediglich ausreichend Speicherplatz auf dem Systemdatenträger erfordert.

Die Umwandlung eines bestehenden Windows in eine virtuelle Maschine (VM) und der Betrieb als VM unter Linux sind anspruchsvoller. Die Einrichtung erfordert mehr Planung und Sorgfalt und der Betrieb ist nur auf leistungsfähiger Hardware zu empfehlen. Ein Bolide muss es nicht sein: Acht GB RAM, leistungsfähige Zwei- oder Vierkern-CPU und – fast am wichtigsten – eine ausreichend große SSD (für Linux plus virtuelle VM-Festplatte) garantieren den flotten Betrieb beider Systeme. Dies vorausgesetzt, ist Virtualisierung die komfortablere Lösung, weil die Windows-Programme jederzeit unter Linux bereitstehen.



Windows-VM – hier unter Linux Mint: Das ist der eindeutig bequemste Weg, um Windows-Programme unter Linux zu nutzen.

1. Vorbereitungen unter Windows

Für Dualboot und mehr noch für Virtualisierung ist es dringend zu empfehlen, das Windows-System gründlich (!) zu entschlacken. Bei Dualboot schaffen Sie dadurch mehr Platz für Linux. Gleiches gilt auch beim virtuellen Windows, sofern dessen virtueller Datenträger später von der Linux-Partition starten soll. Ein schlankeres Windows lässt sich aber auch wesentlich (!) schneller in eine VM umwandeln. Löschen und deinstallieren Sie über „Systemsteuerung → Programme & Features“ alles, was Sie nicht benötigen. Suchen Sie in der Systemsteuerung nach „Systemschutz“ und minimieren Sie dessen Speicherplatzbelegung. Nutzen Sie ferner die Datenträgerbereinigung (cleanmgr.exe) mit der Option „Systemdateien bereinigen“ und mit allen darunter verfügbaren Optionen, um sämtliche überflüssige Dateien zu löschen. Benutzerdateien, die Sie später unter Windows nicht brauchen, verschieben Sie am besten auf einen externen Datenträger, um sie später auf das Linux-System zu übertragen. Abschließend klicken Sie die Systemfestplatte im Explorer mit rechter Maustaste an, um diese über „Eigenschaften → Tools → Optimieren“ zu defragmentieren.

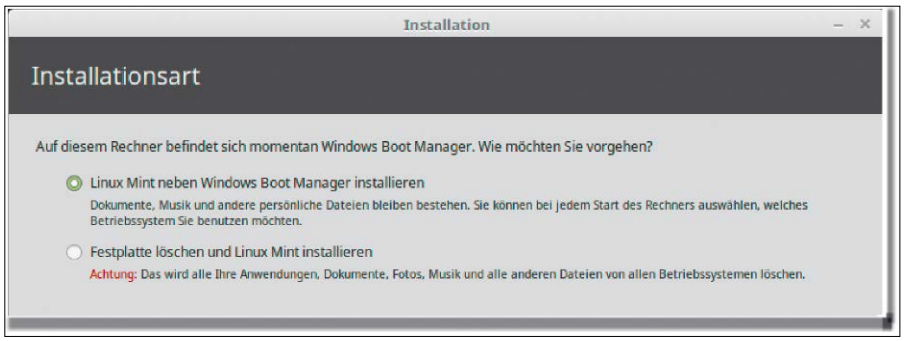
2a. Dualboot mit Windows: Nur im Uefi-Modus

Alle Linux-Installer erkennen und respektieren vorhandenes Windows. Etwas knifflig ist jedoch die Unterscheidung zwischen Bios- und Uefi-Partitionsstil (Bios/MBR versus Uefi/GPT). Die Parallelinstallation kann nur gelingen, wenn das Linux-Livesystem in jenem Modus gestartet wird, in dem Windows installiert ist. Andernfalls kann der Linux-Installer das vorhandene System nicht erkennen und wird dieses, sofern der Benutzer das Problem nicht bemerkt, bei der Ubuntu-Installation überschreiben. Auf allen PCs mit Windows 10 herrscht der moderne Uefi-Modus mit GPT-Partitionsstil. Paralleles Linux muss also ebenfalls im Uefi/GPT-Modus installiert werden. Für die

Installation neben Windows 10 gelten folgende Regeln:
Wenn Sie das gewünschte ISO-Abbild auf USB-Stick kopiert haben (mit dd, Gnome-Disks, Etcher oder auch dem Win 32 Disk Imager unter Windows), müssen Sie den Zielrechner über das Bios-Bootmenü damit starten. Das Bootmenü ist durch frühzeitiges Drücken der Taste F2, F8, F12 oder Esc zu erreichen. Dort erscheinen dann alle Laufwerke zweimal – einmal mit, einmal ohne den Vorsatz „UEFI". Für Parallelinstallation neben Windows wählen Sie den „UEFI"-Eintrag. Der eindeutige Hinweis, dass Sie im richtigen Modus sind, erscheint später im Linux-Installer, sofern er das existierende System anzeigt und etwa „Ubuntu neben [XXX] installieren" (oder „Parallel installieren") anbietet. Ist dies nicht der Fall, obwohl ein Windows vorliegt, dann brechen Sie ab und booten erneut, aber im Uefi-Modus!
Auch die Heft-DVD der LinuxWelt bootet (und installiert) wahlweise im Bios- oder Uefi-Modus. Dieser Hinweis gilt für den Fall, dass Sie Linux Mint oder Elementary OS von der aktuellen DVD neben Windows installieren möchten.
„Secure Boot": Diese Uefi-Funktion sollte im Bios deaktiviert werden. Sie verbietet das Booten nicht signierter Systeme, was den Start von Schadsoftware verhindern soll. Ubuntu-Distributionen besitzen zwar eine Signatur, allerdings nur nach einer Standardinstallation. Sobald im späteren Betrieb unsignierte Treiber hinzukommen (insbesondere für die Grafikkarte), verhindert Secure Boot den Systemstart.

2b. Dualboot: Die Installation

Nach dem Start des Rechners über das Installationsmedium finden Sie am Desktop einen Link, der das Setup anstößt – etwa mit dem Namen „Ubuntu 20.04 installieren". Die Ubuntu-Familie verwendet zwei verschiedene Installer (die meisten „Ubiquity", einige den bunteren „Calamares"). Nach der Sprachauswahl erscheint der Dialog „Installationsart" (Calamares: „Partitionen"): Was dieses Fenster anbietet, hängt von der Situation ab.
A. Gibt es nur eine interne Festplatte, die derzeit von Windows belegt ist, sehen Sie die Option „Ubuntu neben Windows Boot Manager installieren" (Calamares: „Parallel dazu installieren"). Nach einem Klick auf „Weiter" schlägt der Assistent eine neue Aufteilung der Partitionen vor, indem er die Windows-Partition verkleinert und Platz für Ubuntu schafft. Die Partitionsgröße lässt sich ändern, indem Sie die Aufteilungsmarkierung mit der Maus verschieben. Auf eher kleinen SSDs sollten Sie gut überlegen, wieviel Sie Windows als Zweitsystem noch einräumen wollen, jedoch müssen etliche Gigabyte für Updates bleiben.



Dualboot-Installation: Die Windows-Partition wurde erkannt und das Setup bietet die Wahl zwischen einer Dualboot- und einer radikalen Soloinstallation.

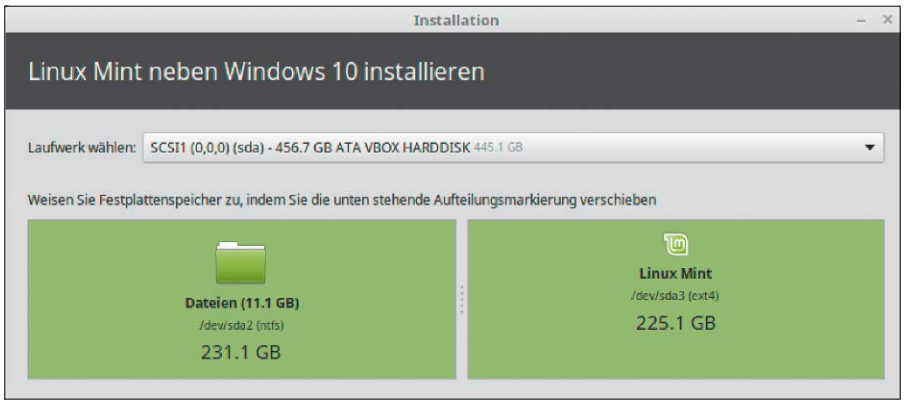
B. Ist neben dem installierten Windows eine freie Partition vorhanden, erkennt der Installer das automatisch. Auch in diesem Fall wählen Sie die Option „Ubuntu neben Windows Boot Manager installieren" (Calamares: „Parallel installieren").
C. Sind bereits zwei oder mehr Systeme vorhanden, dann führt das Angebot, „Ubuntu neben [XXX]" zu installieren, zu einer weiteren Aufteilung und Partitionierung wie unter Variante A. Auf diese Möglichkeit gehen wir hier aber nicht näher ein, da es nicht dem typischen Dualboot-Szenario bisheriger Windows-Nutzer entspricht.
Hinweis: Natürlich zeigt der Installer-Dialog in jedem Fall auch die Option „Festplatte löschen und Linux installieren". Dies wäre der radikale Schritt, um sich von Windows endgültig zu verabschieden.

3a. Virtualisierung: Vmware-Converter

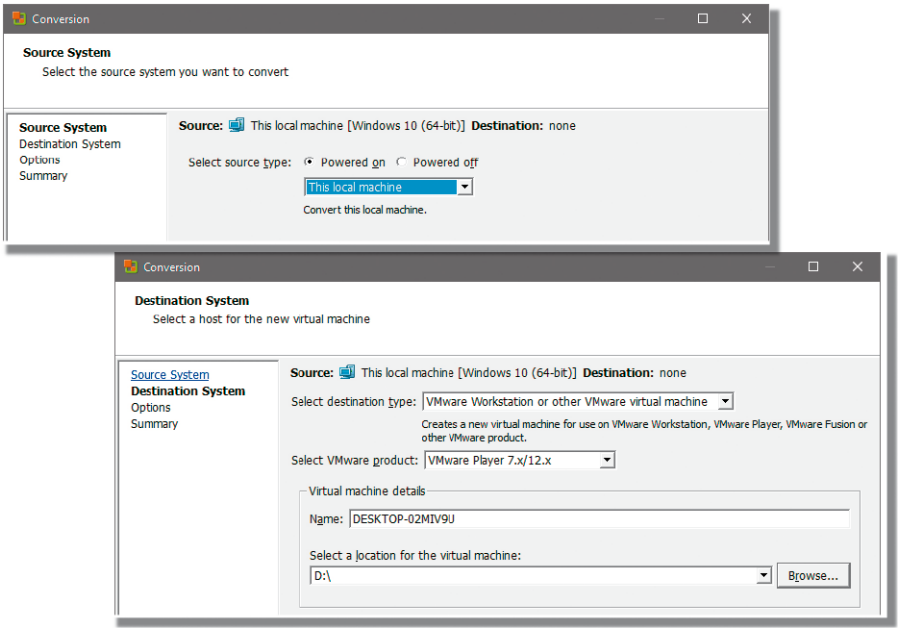
Die nachfolgend beschriebene Methode, aus dem laufenden Windows eine identische Windows-VM zu erstellen, ist sicher nicht die einzig mögliche, aber – mit Abstand – die komfortabelste. Was Sie dazu primär benötigen, ist der Vmware Vcenter Converter Standalone. Diese beeindruckende englischsprachige Software erhalten Sie auf *www.vmware.com/de/products/converter.html* in Version 6.2 von 2017. Laden und installieren Sie die Datei (171 MB) auf dem Windows-10-System, das Sie in eine VM überführen möchten. Versichern Sie sich vor der Nutzung noch einmal, dass Sie gemäß Punkt 1 die Windows-Partition optimal gesäubert haben.
Den installierten Vmware-Converter starten Sie dann nach Rechtsklick unbedingt mit der Option „Als Administrator ausführen", weil Sie andernfalls das laufende System nicht kopieren können. Verwenden Sie im

SOFTWARE MIT „CLOUD"-LIZENZ

Bei Produktivsuiten wie Office 365 oder Adobe Creative Cloud gibt es oft Zweifel, ob diese auch „offline" zu nutzen sind. Die Frage stellt sich lautstark bei einem abgelaufenem Windows (Multiboot oder VM), das aus dem Internet genommen werden muss. Technisch handelt es sich um lokal installierte Desktopsoftware: Word, Excel, Photoshop oder Indesign arbeiten also auch offline uneingeschränkt. Der Unterschied zum klassischen Softwarepaket ist die Abo-Lizenz, die regelmäßig online verifiziert wird. Wer online ist, bekommt davon nichts mit. Ist das System offline, gibt es eine typische Frist von einem Monat, bis diese Kontrolle erfolgen muss – was die Programme rechtzeitig anmahnen. Dann genügt es, im Windows-System den Netzwerkadapter zu aktivieren und die Software zu starten. Die kurze Verbindung zu Microsoft oder Adobe ist auch bei abgelaufenem Windows sicherheitstechnisch vertretbar.



Dualboot optimieren: Der Linux-Installer verkleinert automatisch die bestehende Partition (links), um eine zweite für Linux (rechts) zu schaffen. Mit der Maus korrigieren Sie die Partitionsgrößen.



Laufendes Windows in eine VM umwandeln: Der Vmware Vcenter Converter erledigt das gut geführt und verweist interaktiv auf Konflikte und Konfigurationsfehler.

ersten Dialog das Angebot „Powered on“ und „Convert machine“, im Folgedialog die Option „This local machine“. Nach „Next“ stellen Sie oben um auf „Vmware Workstation or other VWmware virtual machine“. Neben „Select Vmware product“ wählen Sie den für private Nutzung kostenlosen „Vmware Player 7.x/12.x“ (es sei denn, Sie besitzen eine bessere kostenpflichtige Vmware-Software). Der Vmware Player dient später als Virtualisierungssoftware unter Linux.

Darunter vergeben Sie einen Namen für die virtuelle Maschine – am einfachsten den voreingestellten Hostnamen. Im nächsten Feld bestimmen Sie unter „Select a location...“ den Pfad, wo Sie die virtuelle Festplatte der VM ablegen. Es obliegt Ihrer Planung, ob dies bereits der endgültige Ort sein soll. Es ist nämlich später kein ernstes Problem, das komplette virtuelle Windows an einen anderen Ort zu kopieren. Bei einer einzigen lokalen und mehr als halb gefüllten Festplatte müssen Sie mindestens vorläufig ein externes Laufwerk (USB) wählen, weil hier für die virtuelle Platte nicht genügend Platz ist.

Nach „Next“ geht es ans Eingemachte: Unter „Data to copy“ aktivieren Sie bei nur einer internen Festplatte alle Einträge (nicht nur „C:“, sondern auch die bootrelevanten Partitionen „\\?\Volume...“). Für die Größe der Systempartition „C:“ können Sie ein Maximum vorgeben, das allerdings größer sein muss als die aktuelle Belegung. Eventuelle weitere Festplatten sollten Sie unbedingt deaktivieren.

Unter „Devices“ müssen Sie die „Memory“-Einstellung bearbeiten. Zum Beispiel sind bei physikalischen acht GB für die VM vier GB eine vernünftige Größe. Auf der Registerkarte „Other“ vergeben Sie für die „Cores“ am besten ebenfalls die Hälfte der verfügbaren für die VM. Diese Anpassungen sind wichtig, weil die VM sonst das physische Maximum erhielte. Alles Weitere ist nicht substanziell: Sinnvoll ist es, unter „Advanced“ die Option „Install Vmware Tools“ zu aktivieren.

Mit „Finish“ starten Sie die Konvertierung, die je nach Umfang und Datenträger mindestens eine Stunde dauert. Ein Ende mit Fehlermeldung „Failed“ ist nicht selten, wird aber nach unserer Erfahrung trotzdem eine funktionierende VM hinterlassen. Diese besteht nur aus einer großen VMDK-Datei mit der virtuellen Festplatte und der kleineren VMX-Konfigurationsdatei.

3b. Virtualisierung: VM unter Linux

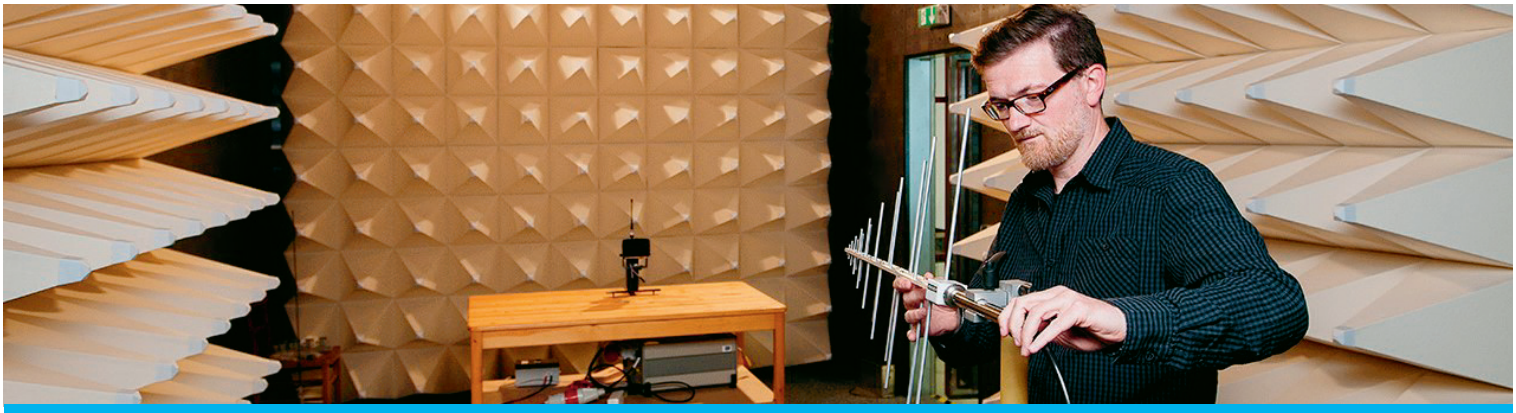
Für den Start der Windows-VM im späteren Linux benötigen Sie den Vmware Player. Den gibt es unter *www.vmware.com/de/products/workstation-player.html*. Mit

```
sudo chmod +x VMware-Player-Full-[…].bundle
sudo ./VMware-Player-Full-[…].bundle
```

installieren Sie die Software. Diese startet die Windows-VM einfach nach Doppelklick auf die VMX-Datei. Beachten Sie, dass zunächst die Windows-Bootumgebung repariert werden muss. Dies bietet die Windows-VM beim ersten Start via „Problembehandlung“ und „Starthilfe“ automatisch an und erledigt es erfolgreich. Beachten Sie ferner, dass die VM erst nach dem zweiten und dritten Start und erst, nachdem die „Vmware Tools“ installiert sind („File → Manage“ im Vmware Player), richtig flüssig läuft.

Ein leidiges Thema ist dann nur noch die Aktualisierung: Wir hatten bei unseren Windows-Konvertierungen Fälle, wo die Windows-VM sofort aktiviert war. Ist das nicht der Fall, sollte die Aktivierung in der Systemsteuerung über „Einstellungen → Update & Sicherheit → Aktivierung“ mit Produktschlüsseln der Vollversion wie mit OEM-Schlüsseln funktionieren. Wenn dies fehlschlägt, nutzen Sie die telefonische Aktivierung bei Microsoft. Die Windows-VM ist uneingeschränkt lizenzberechtigt, wenn Sie das originale Windows durch Linux ersetzt haben. ■

FEIG



SOFTWAREENTWICKLER EMBEDDED LINUX (M/W/D)

FEIG ELECTRONIC ist ein innovatives, inhabergeführtes, mittelständisches Unternehmen und zählt seit über 50 Jahren zu den führenden Herstellern von mikroelektronischen Produkten in den Bereichen Payment, RFID, Verkehrssensorik und Steuerungselektronik. Bei uns können Sie Entwicklung erleben.

Zur Verstärkung unseres Fachbereiches „IDENTIFICATION und PAYMENT“ suchen wir für unsere Firmensitze in Weilburg oder in Bad Hersfeld zum nächstmöglichen Zeitpunkt „Softwareentwickler embedded Linux“ (m/w/d). Gemeinsam mit Ihnen wird geklärt, wo Sie Ihre Fähigkeiten am besten entfalten können. Auch Bewerbungen von Berufsanfängern und Absolventen nehmen wir gerne entgegen.

Was Sie für uns tun können

- Entwicklung und Pflege von Treibern und Komponenten für ein embedded Linux System
- Aufbau und Pflege von Board Support Packages
- Test und Analyse der Systeme auf der Zielhardware
- Analyse von Kundenproblemen
- Entwicklung von automatisierten Testfällen zur Qualitätssicherung
- Inbetriebnahme von Hardware

Was Sie dafür mitbringen sollten

- Abgeschlossenes Studium der Elektrotechnik/ Informatik/Technischen Informatik oder eine vergleichbare Qualifikation
- Fundierte Kenntnisse in C
- Erfahrung in der Programmierung industrieller Mikrokontroller wünschenswert
- Idealerweise Kenntnisse in sym./asym. Verschlüsselungsverfahren
- Idealerweise Erfahrung in der Linux Kernel-Programmierung
- Gute Englisch- und Deutschkenntnisse in Wort und Schrift
- Teamorientiertes und selbstständiges Arbeiten

Was wir Ihnen bieten

Bei FEIG erwartet Sie eine innovative Unternehmenskultur mit kurzen Entscheidungswegen, großem Gestaltungsfreiraum und familiärer Atmosphäre in einem Kreis von Kollegen, die füreinander einstehen. Bei uns werden Sie nach Ihren individuellen Fähigkeiten eingesetzt und Ihre persönliche Weiterentwicklung und Karriere liegen uns am Herzen. Erleben Sie sichere Arbeitsplätze und attraktive Arbeitsbedingungen in einem permanent wachsenden, erfolgreichen Unternehmen, bei dem es Spaß macht, mitzuarbeiten.

Wir freuen uns auf Ihre Bewerbung!

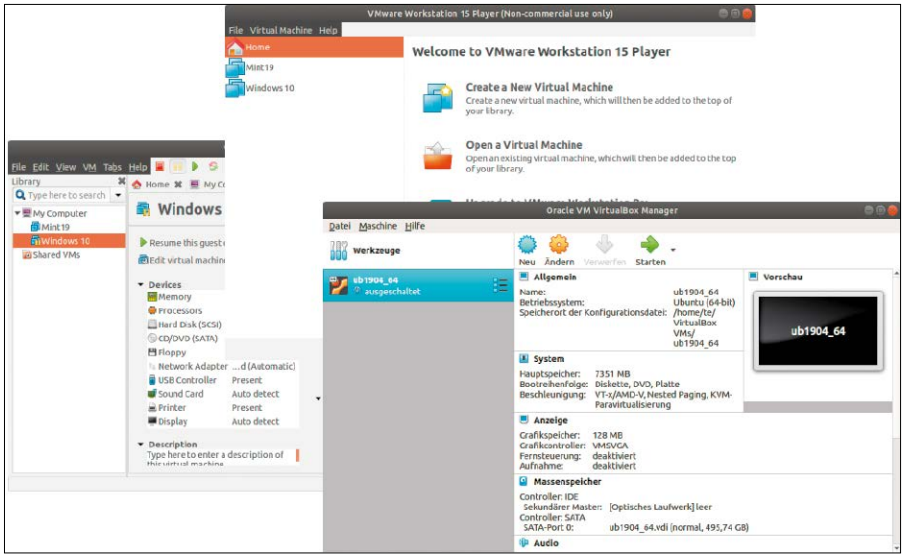
Bitte schicken Sie Ihre vollständigen Bewerbungsunterlagen inkl. Gehaltsvorstellung und nächstmöglichem Eintrittsdatum bevorzugt per E-Mail an **karriere@feig.de** an unsere Personalreferentin Ellen Schäfer.
Weitere Informationen finden Sie unter **www.feig.de/karriere**

FEIG ELECTRONIC GmbH, D-35781 Weilburg, E-Mail: karriere@feig.de, www.feig.de

Virtualisierung mit Virtualbox & Vmware

Virtualisierung ist die einfachste Methode, ein anderes Betriebssystem ohne Reboot zu starten. Unter Linux lassen sich dann Windows-Programme bequem nutzen oder andere Linux-Systeme ausprobieren.

VON THORSTEN EGGELING



Virtualisierer: Virtualbox, Vmware Workstation Player und Vmware Workstation Pro sind Programme für einen virtuellen Zweit-PC, in dem Sie Windows oder Linux starten.

Virtualisierungssoftware bietet vielfältige Möglichkeiten. Sie können fast beliebige Windows-Anwendungen unter Linux verwenden, neue Betriebssysteme ausprobieren, Software gefahrlos testen oder ein sicheres Zweitsystem für das Onlinebanking einrichten. Gegenüber einem auf der Festplatte installierten Betriebssystem bietet Virtualisierung einige Vorteile, denn der aktuelle Zustand einer virtuellen Maschine lässt sich jederzeit sichern. Sie können nach einem Neustart Ihre Arbeit da fortsetzen, wo Sie aufgehört haben. Außerdem ist es möglich, das Betriebssystem schnell auf einen vorherigen Sicherungspunkt zurückzusetzen. Virtuelle Maschinen lassen sich klonen und einfach auf einen anderen PC transportieren.

Es gibt jedoch auch Nachteile: In einer virtuellen Maschine steht dem System nicht die volle Leistung der Hardware zur Verfügung. Die Geschwindigkeit ist daher etwas geringer. Vor allem Spiele, die eine schnelle Grafikkarte benötigen, funktionieren daher gar nicht oder nur unbefriedigend. Für Linux stehen mehrere Virtualisierer zur Verfügung. In diesem Artikel geben wir Tipps zu Virtualbox und Vmware. Tipps zur Open-Source-Software Qemu gibt es übrigens unter *www.pcwelt.de/2444004*.

1. So funktioniert Virtualisierung

Für den Zugriff auf die Hardware ist der Kernel zuständig. Der Programmcode der Treiber ist entweder fest einkompiliert oder wird über Module bei Bedarf geladen. Die Treiber stellen Schnittstellen bereit, über die Programme die Hardware nutzen können. Der Kernel sorgt für die Zuteilung von Systemressourcen wie Rechenzeit und Hauptspeicher. Grundsätzlich kann immer nur ein Treiber exklusiven Zugriff auf die Hardware erhalten und daher nur ein Betriebssystem auf dem PC laufen.

Virtualisierungssoftware verwendet einen Virtual Machine Monitor (VMM), auch Hypervisor genannt, der – wie jede andere Anwendung auch – die Hardware über den Kernel des installierten Betriebssystems nutzt. Der Hypervisor emuliert Hardwarekomponenten per Software, beispielsweise SATA-Controller, Netzwerkadapter und Grafikkarten. Wenn im virtualisierten System („Gastsystem“) ein Zugriff beispielsweise auf das Netzwerk erfolgt, läuft dieser über einen virtuellen Netzwerkadapter und dann über einen Treiber des installierten Systems („Hostsystem“) zum physikalisch vorhanden Netzwerkadapter. Das Gastsystem sieht nicht die physische Hardware, sondern nur die virtuellen Komponenten.

2. Sicherheit in virtuellen Maschinen

Auch Virtualisierungssoftware kann Fehler enthalten, die den Ausbruch von Schadsoftware aus einer virtuellen Maschine ermöglichen. In der Vergangenheit gab es dafür einige Beispiele, wenn auch nur unter Laborbedingungen (siehe *www.pcwelt.de/199 6967*). Die größte Gefahr geht von virtuellen Maschinen aus, die auf das lokale Netzwerk zugreifen dürfen. Einige Schadprogramme suchen nach Netzwerk-

freigaben und infizieren dann die gefundenen Dateien.
Etliche Schadprogramme erkennen eine virtuelle Umgebung und stellen dann ihre Funktion ein. Das soll Virenexperten erschweren, die Funktionen zu untersuchen. Aus diesem Grund können Sie sich auch nicht darauf verlassen, dass eine Software, die Sie in einem virtualisierten Betriebssystem ausprobieren, keinen Schaden anrichten kann.
Für jeden PC – ob virtuell oder nicht – gelten die gleichen Regeln: Halten Sie die Software aktuell und installieren Sie zeitnah alle verfügbaren Updates für das Betriebssystem. Bei Windows-Gästen kann ein Virenscanner die Sicherheit verbessern. Windows 8.1 und 10 bringen mit Windows Defender bereits eine Sicherheitslösung mit, die ausreichend Schutz bietet (siehe *www.pcwelt.de/2142242*).

3. Virtuelle Maschinen per Hardware beschleunigen

CPUs bieten seit etwa 2006 Paravirtualisierung mit Hardwareunterstützung. Die Leistung der virtualisierten Systeme wird dadurch deutlich verbessert. AMD nennt die Technik „AMD Virtualization" (AMD-V), Bei Intel heißt die Erweiterung „Virtualization Technology", „Intel VT" oder „Intel VT-x". Auskunft über die Fähigkeiten der CPU gibt folgender Terminalbefehl:

```
egrep -c '(svm|vmx)' /proc/cpuinfo
```

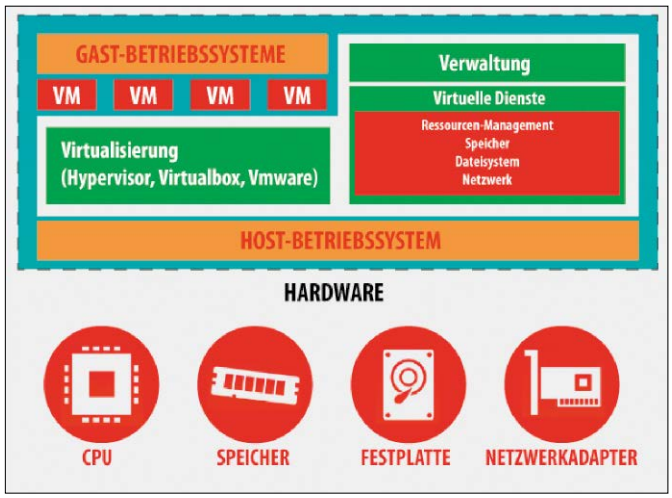
Ist in der Ausgabe ein Wert größer „0" zu sehen, dann unterstützt der Prozessor Virtualisierungsfunktionen. Bei einem Intel Core i7 beispielsweise lautet das Ergebnis „8", weil alle acht Prozessorkerne Intel-VT unterstützen. Mit

```
cat /proc/cpuinfo
```

können Sie sich auch die komplette Liste der CPU-Eigenschaften anzeigen lassen. Die Werte „vmx" beziehungsweise „svm" tauchen hinter „flags:" auf. Erscheint in der Ausgabe von cpuinfo „0", sehen Sie im Bios/Firmware-Setup nach, ob sich AMD-V oder Intel-VT („vt-x" oder „Intel Virtualization Technologie") dort aktivieren lässt.

4. Virtualbox unter Linux installieren

Virtualbox ist in den Standard-Paketquellen etwa von Ubuntu und Linux Mint enthalten. Es handelt sich zur Zeit um die ältere Version 5.2. Es ist jedoch empfehlenswert, stets die neueste Version zu verwenden. Der



System im System: Die Basis der Virtualisierung bildet ein Hypervisor, der Aufrufe zwischen den virtuellen Maschinen und dem Host-Betriebssystem umsetzt und Hardware emuliert.

```
te@ub1804: ~/src/virt-manager-2.1.0
Datei  Bearbeiten  Ansicht  Suchen  Terminal  Hilfe
model name      : Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz
stepping        : 9
microcode       : 0xb4
cpu MHz         : 805.757
cache size      : 8192 KB
physical id     : 0
siblings        : 8
core id         : 1
cpu cores       : 4
apicid          : 2
initial apicid  : 2
fpu             : yes
fpu_exception   : yes
cpuid level     : 22
wp              : yes
flags           : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov
pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe syscall nx pdpe1gb rdt
scp lm constant_tsc art arch_perfmon pebs bts rep_good nopl xtopology nonstop_ts
c cpuid aperfmperf tsc_known_freq pni pclmulqdq dtes64 monitor ds_cpl vmx smx es
t tm2 ssse3 sdbg fma cx16 xtpr pdcm pcid sse4_1 sse4_2 x2apic movbe popcnt tsc_d
eadline_timer aes xsave avx f16c rdrand lahf_lm abm 3dnowprefetch cpuid_fault in
vpcid_single pti ssbd ibrs ibpb stibp tpr_shadow vnmi flexpriority ept vpid ept
```

Hardwareunterstützung: „cat /proc/cpuinfo" gibt Infos zum Prozessor aus. Erscheint bei einer Intel-CPU „vmx", lässt sich Intel-VTx zur Beschleunigung von virtuellen Maschinen nutzen.

Hersteller Oracle beseitigt regelmäßig Fehler in der Software und verbessert die Unterstützung für aktuelle Gast-Betriebssysteme. Binden Sie daher die Downloadquelle von Virtualbox in die Paketverwaltung ein. Sie erhalten dann automatisch Updates, sobald diese verfügbar sind. Bei Ubuntu oder Linux Mint öffnen Sie ein Terminal und führen diese beiden Befehle aus:

```
wget -q https://www.virtualbox.
 org/download/oracle_vbox_2016.
 asc -O- | sudo apt-key add -
wget -q https://www.virtualbox.
 org/download/oracle_vbox.asc -O-
 | sudo apt-key add -
```

Damit importieren Sie den Oracle-Schlüssel in die Liste der vertrauenswürdigen Softwareanbieter. Danach starten Sie diese drei Kommandos:

```
sudo sh -c "echo deb http://
 download.virtualbox.org/
 virtualbox/debian bionic contrib
 > /etc/apt/sources.list.d/
 virtualbox.list"
sudo apt update
sudo apt-get install dkms
 virtualbox-6.0
```

Ersetzen Sie „bionic" (Ubuntu 18.04/Linux Mint 19) bei Bedarf durch den Codenamen der gewünschten Distribution (etwa „disco" für Ubuntu 19.04).
Fügen Sie dann alle Benutzer, die Virtualbox verwenden sollen, zur Gruppe „vboxusers" hinzu:

```
sudo adduser [User] vboxusers
```

Ersetzen Sie den Platzhalter „[User]" durch den Log-in-Namen des gewünschten Benutzers. Melden Sie sich bei Linux ab und wieder an oder starten Sie das System neu. Beim ersten Start bietet Virtualbox automa-



Erweiterungen für Virtualbox: Das Virtualbox-Zusatzpaket sollten Sie auf jeden Fall installieren. Es enthält Software, über die sich USB-Geräte in virtuelle Maschinen einbinden lassen.

tisch Download und Installation des Oracle VM Virtualbox Extension Packs an. Wenn nicht, laden Sie das Paket über *www.virtualbox.org/wiki/Downloads* manuell herunter und installieren es. Damit ergänzen Sie nützliche Funktionen, beispielsweise bessere Unterstützung von USB-Geräten.

5. Installationsmedien besorgen

Für virtuelle Maschinen verwenden Sie die gleichen Installationsmedien wie bei einer herkömmlichen Installation. Eine DVD müssen Sie nicht brennen, die ISO-Datei genügt. ISO-Dateien für die Linux-Installation finden Sie regelmäßig auf der LinuxWelt-Heft-DVD oder Sie laden die gewünschte Datei beim Anbieter herunter. Wenn Sie keine Windows-Installallations-DVD besitzen, erhalten Sie die ISO-Datei über *www.pcwelt.de/win10iso*. Die Webseite bietet beim Aufruf mit einem Browser unter Linux den ISO-Download an.

Windows muss auch in einer virtuellen Maschine mit einem eigenen Produktschlüssel aktiviert werden. Sie können das System jedoch auch ohne Aktivierung eine Zeitlang nutzen. Es gibt aber einige Einschränkungen. In den „Einstellungen" sind beispielsweise die Optionen unter „Personalisierung" deaktiviert. Microsoft stellt die Enterprise-Version von Windows 10 kostenlos für einen 90-Tage-Test zur Verfügung (*www.pcwelt.de/k2mNT9*). Hier gibt es keine Funktionsbeschränkungen. Windows 10 Enterprise bietet in etwa das Gleiche wie Windows 10 Pro. Wer unter Linux eine bestimmte Windows-Anwendung nur für kurze Zeit benötigt, sollte zu dieser Enterprise-Edition greifen.

6. Gast-Betriebssysteme in Virtualbox installieren

Die Einrichtung eines Betriebssystems in Virtualbox unterscheidet sich kaum von der Installation auf realer Hardware. Nach dem Start von Virtualbox gehen Sie im Menü auf „Maschine → Neu". Ein Assistent führt Sie durch die Einrichtung des virtuellen PCs.

Schritt 1: Vergeben Sie hinter „Name:" eine aussagekräftige Bezeichnung, beispielsweise „Windows 10 Pro 64 Bit" oder „Linux Mint 19 64 Bit". Hinter „Typ" wählen Sie „Microsoft Windows" beziehungsweise „Linux" und hinter „Version" das gewünschte System, beispielsweise „Windows 10" oder „Linux". Bei Version stellen Sie „Windows 10 (64 Bit)" oder „Ubuntu (64 Bit)" ein, je nach der Variante, die Sie installieren wollen.

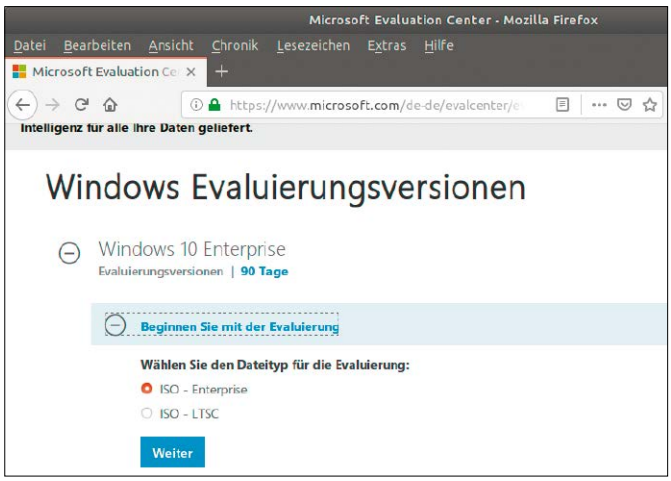
Schritt 2: Im nächsten Schritt stellen Sie den in der virtuellen Maschine verfügbaren Hauptspeicher ein. Für Windows 10 mit 64 Bit schlägt Virtualbox 2048 MB RAM vor, für Linux 1024 MB. In der Regel ist das ausreichend und mehr RAM bringt kaum mehr Geschwindigkeit.

Schritt 3: Im Dialog „Platte" belassen Sie die Option „Festplatte erzeugen" und klicken auf „Erzeugen". Als Dateityp wählen Sie „VDI (Virtual Box Disk Image)". Nach einem Klick auf „Weiter" wählen Sie „dynamisch alloziert", wenn die Datei der virtuellen Festplatte dynamisch bis zur maximal angegebenen Größe wachsen soll. Die Erstellung geht dann schneller und belegt erst einmal weniger Platz auf der physischen Festplatte. Bei „feste Größe" wird der Platz hingegen komplett belegt und die Erzeugung dauert länger. Dafür läuft das System in der virtuellen Maschine etwas schneller.

Nach einem Klick auf „Weiter" geben Sie die Größe der virtuellen Festplatte an. Wie groß diese sein sollte, hängt von der geplanten Nutzung ab. Für Windows oder Linux mit ein paar Anwendungen und Updates genügen 50 bis 100 GB. Um Reserven zu haben, kann es aber auch deutlich mehr sein, je nach Kapazität Ihrer Festplatte. Nachträglich lassen sich virtuelle Festplatten nur mit erheblichem Aufwand vergrößern. Sie können aber jederzeit schnell weitere Festplatten „einbauen" und als Datenspeicher oder für Anwendungen nutzen. Klicken Sie zum Abschluss auf „Erzeugen".

Schritt 4: Sie sehen jetzt wieder das Hauptfenster von Virtualbox mit einer Übersicht der Konfiguration. Klicken Sie in der Symbolleiste auf „Ändern" und gehen Sie auf „Massenspeicher". Klicken Sie auf das CD/DVD-Symbol („leer") und dann rechts im Fenster auf das CD-Icon mit dem Pfeil. Navigieren Sie über „Datei für virtuelles CD/DVD-Medium auswählen..." zur ISO-Datei des Systems, das Sie installieren wollen.

Unter „Netzwerk" können Sie die Konfiguration des Netzwerkadapters ändern. Standardmäßig ist hinter „Angeschlossen an" die Option „NAT" eingestellt. Die virtuelle Maschine hat dann Internetzugriff, sieht



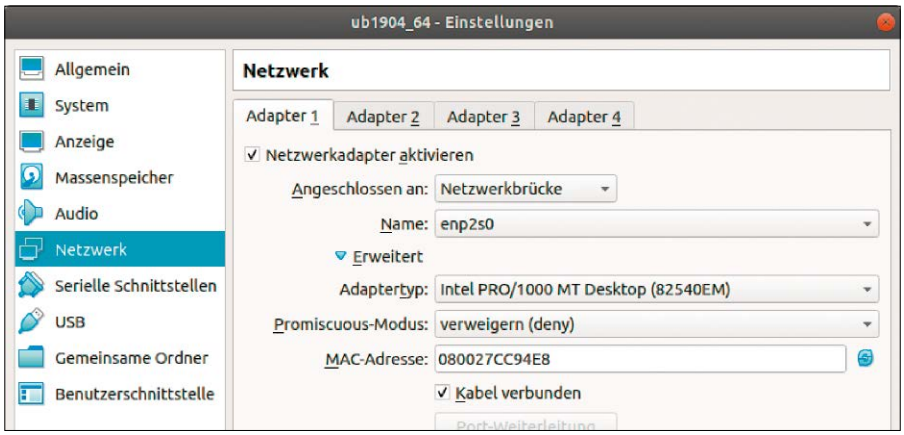
Windows ausprobieren: Für gelegentliche Windows-Nutzer eignet sich die Enterprise-Edition, die Sie 90 Tage lang verwenden können. Die ISO-Datei gibt es gratis bei Microsoft.

aber nichts vom lokalen Netzwerk. Um das zu ändern, stellen Sie „Netzwerkbrücke“ ein. Bedenken Sie dabei aber die möglichen Risiken, wie in Punkt 2 beschrieben. Klicken Sie auf „OK“, um die Einstellungen zu speichern.

Schritt 5: Klicken Sie auf „Starten“. Im Fenster erscheint nach kurzer Zeit der Bildschirm des Windows- oder Linux-Setups. Folgen Sie den Anweisungen des jeweiligen Assistenten. Die zweite Phase des Windows-10-Setups beginnt mit dem Bildschirm „Willkommen“ und führt dann zu „Zuerst die Region. Ist sie richtig?“. Das ist der richtige Zeitpunkt, um ein erstes Backup über „Maschine → Sicherungspunkt erstellen“ anzulegen. Wenn der Testzeitraum von Windows 10 Enterprise abgelaufen ist, stellen Sie diesen ersten Sicherungspunkt wieder her und beginnen mit einem frischen System, das Sie erneut 90 Tage lang ausprobieren können. Die gewünschten Anwendungen müssen Sie allerdings neu installieren. Bei Linux-Gästen sollten Sie einen ersten Sicherungspunkt nach der Erstkonfiguration und Installation aller Updates anlegen.

Eine virtuelle Maschine müssen Sie nach der Verwendung nicht herunterfahren. Schließen Sie einfach das Fenster und aktivieren Sie die Option „den Zustand der virtuellen Maschine speichern“. Per Klick auf „Starten“ setzen Sie später Ihre Arbeit an der Stelle fort, an der Sie aufgehört haben.

Hinweis: Der Mauszeiger ist – ohne Gasterweiterungen (siehe Punkt 7) – im Fenster gefangen. Sie bekommen ihn wieder frei, indem Sie die Strg-Taste rechts auf der Tastatur drücken („Host-Taste“).

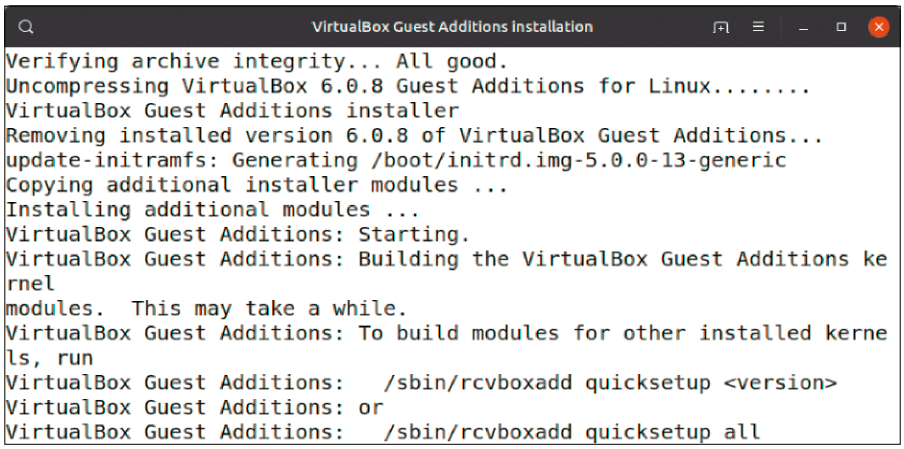


Mit und ohne lokales LAN: Stellen Sie „Netzwerkbrücke“ für den Zugriff auf das Heimnetz ein. Sicherer ist die Voreinstellung „NAT“, wenn die VM nur Internetzugriff haben soll.

7. Virtualbox-Gasterweiterungen installieren

Für optimale Leistung und einige Komfortfunktionen ist zusätzliche Software erforderlich. Dafür müssen im Gastsystem einige Kernel-Module kompiliert werden. Damit das funktioniert, installieren Sie in einem Ubuntu-18.04-Gastsystem folgende Pakete in einem Terminalfenster:

```
sudo apt install gcc make perl dkms
```



Gastsystem optimieren: Die Gasterweiterungen enthalten Kernel-Module, die erst kompiliert werden müssen. Nach der Installation lassen sich zusätzliche Funktionen nutzen.

VIRTUALISIERUNGSSOFTWARE FÜR LINUX

	KVM/Qemu	Oracle Virtualbox 6	Vmware Workstation 15 Player	Vmware Workstation 15 Pro
Internet	*www.linux-kvm.org, www.qemu.org*	*www.virtualbox.com*	*www.vmware.com*	*www.vmware.com*
Preis	kostenlos (Open Source)	kostenlos (z. T. Open Source)	ab 166 Euro (für Privatanwender kostenlos)	ab 275 Euro
Funktionen				
3D-Beschleunigung	nein	ja	ja	ja
Appliance Export/Import (OVA)	ja/ja (mit Zusatztools)	ja/ja	nein/ja	ja/ja
Gemeinsame Ordner	ja (mit Zusatztools)	ja	ja	ja
Gemeinsame Zwischenablage	ja (mit Zusatztools)	ja	ja	ja
Mehrere VMs parallel	ja	ja	nein	ja
USB 2.0/3.0 im Gastsystem	ja/ja	ja/ja	ja/ja	ja/ja
VM-Klonfunktion	ja	ja	nein	ja
VM-Schnappschüsse	ja	ja	nein	ja

Gehen Sie im Fenster der laufenden virtuellen Maschine auf „Geräte → Gasterweiterungen einlegen“. Es erscheint ein Fenster, in dem Sie auf „Ausführen“ klicken und mit dem root-Passwort bestätigen. Ein Script erstellt die nötigen Kernel-Module automatisch. Kommt Windows als Gast-Betriebssystem zum Einsatz, starten Sie „VBoxWindowsAdditions.exe“ vom Medium mit den Gasterweiterungen und folgen den Anweisungen des Assistenten.

8. Erweiterte Funktionen

Nach der Installation der Gasterweiterungen und Neustart des Gastsystems gibt es neue Funktionen: Wenn Sie die Größe des Virtualbox-Fensters ändern, passt sich die Bildschirmauflösung entsprechend an. Der Mauszeiger löst sich jetzt automatisch, wenn Sie ihn aus dem Fenster ziehen.

Unter „Geräte → Gemeinsame Zwischenablage“ und „Geräte → Drag und Drop“ aktivieren Sie jeweils „bidirektional“. Über die Zwischenablage lassen sich dann Texte oder Bilder zwischen Gast- und Hostsystem austauschen. Drag & Drop funktioniert nicht immer, bei unseren Tests beispielsweise nur mit Windows-Gastsystemen.

Zur komfortablen Datenübertragung zwischen Host und Gast empfehlen wir einen gemeinsamen Ordner. Dazu gehen Sie im Fenster der virtuellen Maschine auf „Geräte → Gemeinsame Ordner → Gemeinsame Ordner“. Über die „+“-Schaltfläche bestimmen Sie einen Ordner für den Datenaustausch auf dem Hostsystem. Setzen Sie Häkchen vor „Automatisch einbinden“ und „Permanent erzeugen“. Damit ein Nutzer im Gastsystem den gemeinsamen Ordner nutzen kann, fügen Sie ihn unter Ubuntu mit folgender Befehlszeile zur Gruppe „vboxsf“ hinzu:

```
sudo adduser [User] vboxsf
```

„[User]“ ersetzen Sie durch den Benutzernamen des gewünschten Benutzers. Starten Sie das Gastsystem neu. Den gemeinsamen Ordner finden Sie unter Linux im Navigationsbereich des Dateimanagers beziehungsweise im Verzeichnis „/media“ mit dem Prefix „sf_“. Ist Windows installiert, erreichen Sie den Ordner im Windows-Explorer über „Netzwerk“ und „Vboxsrv“.

9. USB-Geräte in ein Gastsystem einbinden

USB-Geräte wie Drucker, Scanner oder Sticks lassen sich jederzeit in ein Gastsystem einbinden, stehen währenddessen aber auf dem Hostsystem nicht mehr zur Verfügung. Die USB-Unterstützung aktivieren Sie in der Konfiguration einer virtuellen Maschine nach einem Klick auf „USB“. Setzen Sie ein Häkchen vor „USB-Controller aktivieren“. Darunter wählen Sie die gewünschte Option für USB 1.1, 2.0 oder 3.0, je nachdem, an welchen Port das USB-Gerät angeschlossen ist. Starten Sie den virtuellen PC, gehen Sie auf „Geräte → USB“ und setzen Sie ein Häkchen vor das USB-Gerät, das Sie einbinden möchten.

Manchmal funktioniert die Einbindung nicht, weil der Host das Gerät blockiert. Das lässt sich beheben, indem Sie die USB-Einstellungen der virtuellen Maschine ändern. Sie sehen Sie hier den Bereich „Filter für USB-Geräte“. Über die Schaltfläche mit dem „+“-Symbol wählen Sie das gewünschte Gerät aus. Verbinden Sie das USB-Gerät erst nach den Start der virtuellen Maschine mit dem PC. Das Hostsystem lädt dann den zugehörigen Treiber nicht und die Einbindung in das Gastsystem gelingt zuverlässig.



Datenaustausch: Über gemeinsame Ordner erhalten Sie im Gastsystem Zugriff auf ausgewählte Ordner des Hosts. Darüber lassen sich Dateien und Downloads hin und her kopieren.

10. Von USB-Laufwerken booten

Virtualbox kann von einem USB-Laufwerk booten, etwa um ein darauf installiertes Linux-System zu starten. Das klappt jedoch nur über einen Umweg. Ermitteln Sie im Terminalfenster zuerst mit dem Befehl mount, über welchen Laufwerkspfad sich das Gerät ansprechen lässt, beispielsweise „/dev/sdi“. Mit den folgenden drei Befehlen ermitteln Sie die Hersteller- und Produkt-ID sowie die Seriennummer:

```
udevadm info -a -n /dev/sdi | grep
  idVendor
udevadm info -a -n /dev/sdi | grep
  idProduct
udevadm info -a -n /dev/sdi | grep
  serial
```

Notieren Sie sich jeweils die erste Zeile der Ausgabe.

Mit der Zeile

```
sudo gedit /etc/udev/
  rules.d/50-usbdrive.rules
```

erstellen Sie eine Udev-Regel mit diesem Inhalt:

```
SUBSYSTEMS=="usb",
  ATTRS{idVendor}=="0781",
  ATTRS{idProduct}=="5588", ATTRS{
  serial}=="00000000000000000000",
  GROUP="users", MODE="0666"
```

Ersetzen Sie die Angaben im Beispiel durch die zuvor mit udevadm ermittelten Werte. Lesen Sie die Udev-Regeln neu ein:

```
sudo udevadm control --reload
```

Trennen Sie das USB-Laufwerk vom PC und verbinden Sie es erneut. Durch die geänderten Regeln haben Sie jetzt Lese- und Schreibzugriff auf den USB-Gerätepfad. Mit

```
VBoxManage internalcommands
  createrawvmdk -filename ~/
  usbdrive.vmdk -rawdisk /dev/sdi
```

erzeugen Sie eine „vmdk“-Datei, die auf den physischen Datenträger verweist.

Klicken Sie nun in der Konfiguration einer virtuellen Maschine auf „Massenspeicher“ und gehen Sie auf „Controller: SATA“. Im Kontextmenü klicken Sie auf „Festplatte hinzufügen“ und dann auf „Vorhandene Festplatte auswählen“. Über „Hinzufügen“ geben Sie die „vmdk“-Datei an.

Starten Sie die virtuelle Maschine, klicken Sie mit der Maus in das Fenster, drücken Sie die F12-Taste und dann „2“, um von der zweiten Festplatte (dem USB-Stick) zu booten. Für den Druck F12 bleibt nur wenig Zeit, bevor das System startet. Bei Bedarf verzögern Sie den Start mit

```
VBoxManage modifyvm [VM-NAME]
  --bioslogodisplaytime 10000
```

um 10 Sekunden. Den Platzhalter „[VM-NAME]“ ersetzen Sie durch die Bezeichnung der virtuellen Maschine.

11. Vmware Workstation (Player) nutzen

Das ausführlich erklärte Virtualbox ist unsere klare Empfehlung: Der für private Nutzung kostenlose Vmware Workstation Player bietet deutlich weniger Funktionen als Virtualbox (siehe Tabelle) und auch nicht mehr Geschwindigkeit. Die Vollversion Vmware Workstation leistet Ähnliches wie Virtualbox, kostet aber etwa 275 Euro.

Wer Vmware trotzdem installieren möchte, öffnet im Browser die Adresse *https://my.vmware.com/de/web/vmware/downloads*. Auf der Seite finden Sie Links zum Download von Vmware Workstation Player (kostenlos) und Vmware Workstation Pro (Testzeitraum 30 Tage). Die Installation läuft bei beiden ähnlich ab.

Da auch Vmware einige Kernel-Module kompilieren muss, installieren Sie zuerst die Entwicklertools:

```
sudo apt install make gcc
```

Die heruntergeladene Setupdatei starten Sie in einem Terminalfenster:

```
sudo bash VMware-
  Player-15.1.0-13591040.x86_64.
  bundle
```

Ein Assistent führt Sie durch die Installation. Die Installationen von Gastsystemen erfolgt nach Klick auf „Create a New Virtual Machine“ ähnlich wie in Punkt 6 für Virtualbox beschrieben. Abweichend davon werden Sie gleich zu Beginn aufgefordert, eine ISO-Datei des Setupmediums anzugeben. Vmware versucht dann einen „Easy Install“, bei dem Sie etwa Benutzernamen und Passwort und bei Windows auch den Produktschlüssel vorab festlegen können. Das ist jedoch nicht hilfreich, wenn Sie das System etwa von einer Linux-Live-DVD nur ausprobieren möchten.

Außerdem funktioniert „Easy Install“ beispielsweise bei Windows 10 Enterprise nicht zuverlässig. Wählen Sie daher besser die Option „I will install the operating system later“, klicken Sie nach Abschluss des Assistenten auf „Edit virtual machine setting“ und legen Sie unter „CD/DVD“ das ISO-Abbild fest.

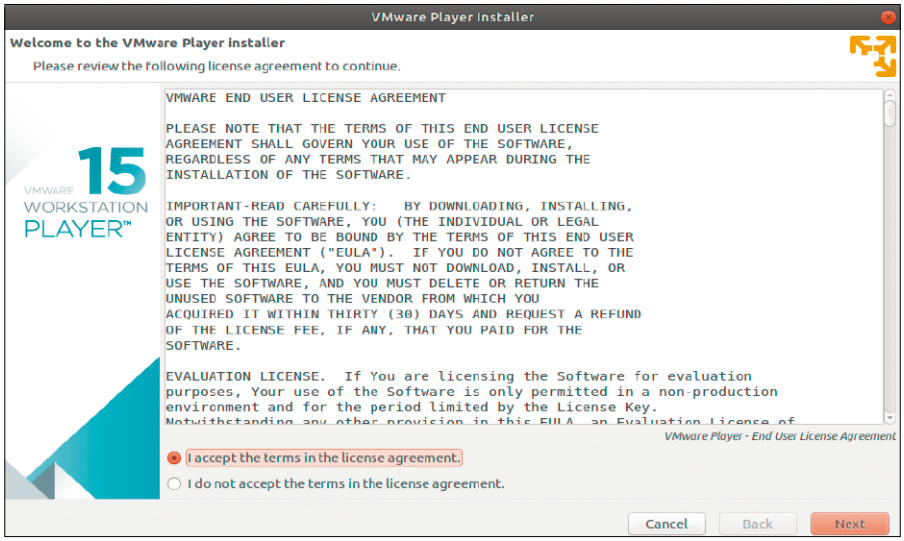
Per Klick auf „Power On“ starten Sie die virtuelle Maschine und führen die Installation des Gastsystems durch. Zur Optimierung installieren Sie in einem Windows-Gastsystem die Vmware-Tools über das Menü „Virtual Machine → Install VMware Tools“. Das geht zwar auch unter Linux, Vmware empfiehlt jedoch, die Open-Source-Variante der Tools über

```
sudo apt install open-vm-tools
  open-vm-tools-desktop
```

einzurichten. ■



System vom USB-Laufwerk starten: Die „vmdk“-Datei enthält Verweise zum physischen USB-Datenträger, den Virtualbox als Bootgerät in die virtuelle Maschine einbindet.



Vmware Workstation Player: Vmware bietet ein komfortables Setuptool, über das die Installation schnell geschehen ist. Bei privater Nutzung ist der Player kostenlos.

VIRTUALBOX: KLONEN UND EXPORTIEREN

Was bei einem System auf der Festplatte ein erheblicher Aufwand ist, gelingt bei virtuellen Maschinen mit wenigen Mausklicks. Wählen Sie im Kontextmenü einer virtuellen Maschine „Klonen“, um eine Kopie zu erstellen. Handelt es sich um ein aktiviertes Windows, setzen Sie ein Häkchen vor „Hardware-UUIDs behalten“. Der Klon ist dann ebenfalls aktiviert, Sie dürfen Original und Kopie aber nie gleichzeitig starten. Klone können nur den aktuellen Systemzustand enthalten, bei Bedarf aber auch die bisherigen Sicherungspunkte.

Über „Datei → Appliance exportieren“ lassen sich ebenfalls Kopien erstellen. Der Export erfolgt im „Open Virtualisation Fomat“ als OVA-Datei, die sich in Virtualbox – auch auf einem anderen Linux- oder Windows-PC – importieren lässt. Andere Virtualisierer wie etwa Vmware Workstation Player und Vmware Workstation Pro können diese Dateien ebenfalls importieren.

Umzug von Daten und Software

Der Umstieg auf ein Linux-System fällt leicht. Doch was ist mit den bisherigen Daten und Medien? Dieser Beitrag erklärt, wie Sie den Umzug vorbereiten, welche Software sorgenfrei funktioniert und wo Hindernisse auftreten können.

VON HERMANN APFELBÖCK



Hier geht es um die Konsequenzen eines kompletten Systemumzugs auf Linux. Während Dualboot und Virtualisierung stets den Rückgriff auf Windows und Windows-Software erlauben, sind Sie bei einem reinen Linux-System künftig ausschließlich auf Linux-Software angewiesen. Bei privater Nutzung gibt es keine Einschränkungen: Multimedia, Office, Mail, Archiv – für alles gibt es gute und zum Teil auch unter Windows populäre Software. Homeoffice in Zusammenarbeit mit Word- und Excel-Nutzern ist in den allermeisten Fällen und mit etwas Toleranz ebenfalls problemlos.

Sicherung der Benutzerdaten

Oberste Pflicht vor einem Überschreiben der Windows-Partition durch Linux ist die Sicherung aller Benutzerdateien. Am einfachsten geschieht dies auf einen externen USB-Datenträger. Einen pauschalen Königsweg gibt es dabei nicht: Externe Klonsoftware wie Rescuezilla (*https://rescuezilla.com/*) sichert zwar lückenlos, aber zu 95 Prozent Windows-Systemballast, den Sie nicht mehr brauchen.

Ob eine Sicherung des gesamten Benutzerordners „\Users\" oder eines Benutzerkontos „\Users\[Name]\" genügt, hängt nicht zuletzt davon ab, ob der Windows-Benutzer seine Daten in den vorgesehenen Ordnern wie „Dokumente", „Bilder" abgelegt hat oder außerhalb des Benutzer-Homes. Wir bringen daher nur zwei Beispiele als Anregung:

Wer sehr genau weiß, welche Dateitypen gesichert werden müssen, kann sich mit einer stark gefilterten und ballastfreien Lösung in der Eingabeaufforderung oder in Powershell begnügen (im Beispiel ist C: die Windows-Partition, E: das Backuplaufwerk):

```
xcopy /kreisch c:\*.xls? e:\
xcopy /kreisch c:\*.doc? e:\
xcopy /kreisch c:\*.mp3 e:\
...
```

Eine umfassendere Sicherung der Benutzerdateien, die dennoch den kompletten Windows-Ballast wegfiltert, erzielen Sie mit Robocopy (Beispiel):

```
robocopy c:\ e:\ /MIR /XD "Windows"
  "Program Files*" "$*" "Boot"
  "ProgramData" "Microsoft*"
  "Config.msi" "MSOCache" "Intel"
  "PerfLogs" "Cache*" "Packages"
  /XJD /W:0 /R:0
```

Orientieren Sie sich am Hauptverzeichnis, um die größten unnötigen Ordner nach „/XD" (Exclude Directory) von der Sicherung auszuschließen. Das funktioniert nur lückenlos, wenn Sie sich im Explorer auch die versteckten Ordner anzeigen lassen („Ansicht → Ausgeblendete Elemente"). Lassen Sie sich Zeit für die Filterregeln und kontrollieren Sie zunächst mit zusätzlichem Schalter „/L" die Auswirkung:

```
robocopy c:\ e:\ /MIR /XD "Windows"
  "Program Files*" […] /XJD /W:0 /R:0
  /L
```

Wenn Robocopy mit „/L" immer noch zu viel Ballast meldet, fügen Sie weitere Exclude-Angaben hinzu. Erst sobald Sie mit der „/XD"-Filterliste zufrieden sind, lassen Sie Schalter „/L" weg und starten damit die tatsächliche Sicherung. Für den Backupdatenträger gelten keine besonderen Einschränkungen, weil Linux NTFS, FAT32 wie exFAT unterstützt – mit einer Ausnahme:

Verschlüsselung! Gesicherte Benutzerdateien nützen Ihnen später nichts, wenn sie mit einer Methode verschlüsselt wurden, die Linux nicht beherrscht. Windows Pro erlaubt die NTFS-native EFS-Verschlüsselung von Ordnern und Dateien. Wenn Sie

auf FAT32, exFAT oder ins Netzwerk sichern, geht diese Verschlüsselung automatisch verloren und die Dateien sind unter Linux nutzbar. Wenn Sie jedoch auf einen NTFS-formatieren Datenträger sichern, sollten Sie mit

```
cipher /n /u
```

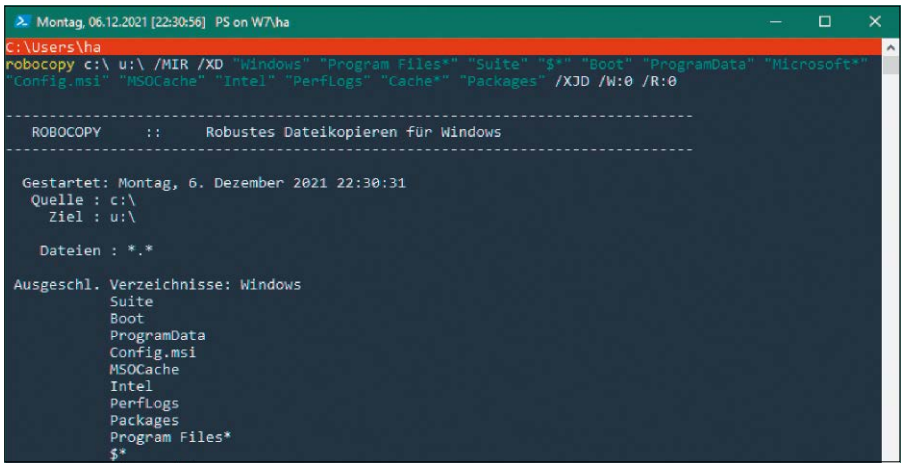
nach EFS-verschlüsselten Dateien fahnden und die Verschlüsselung über „Eigenschaften → Erweitert" entfernen. Analoges gilt für auch für andere Verschlüsselungsmethoden, die unter Linux nicht unterstützt werden: Nutzen Sie die Verschlüsselungsoption unter Microsoft Office? Haben Sie Winrar-Archive mit Passwort angelegt? Und es gibt diverse weitere Windows-Tools, die nicht plattformübergreifend verschlüsseln. Positive Ausnahmen sind 7-Zip und Veracrypt.

Sicherung von Einstellungen

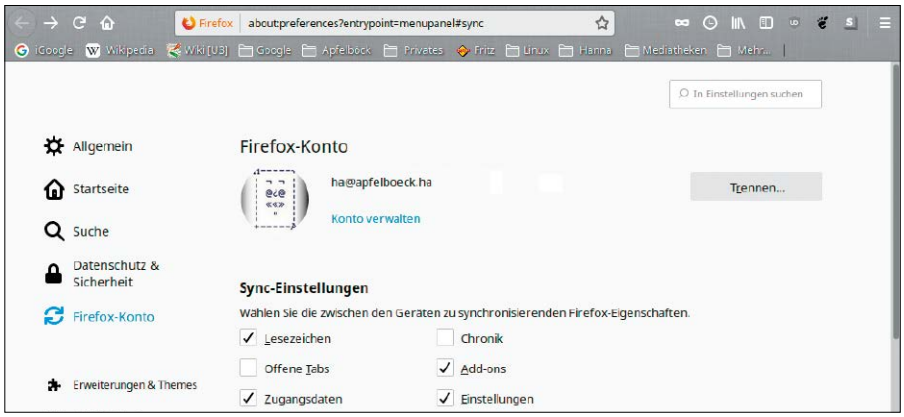
Zahlreiche plattformunabhängige Programme laufen sowohl unter Windows wie Linux und nutzen hier wie dort dieselben Konfigurationsdateien. Dieses Thema ist aber für die Masse von Software an dieser Stelle nicht abzuarbeiten. Eine Sicherung des Benutzerordners unter Windows oder die oben beschriebene Robocopy-Sicherung, die den „\Users"-Pfad einbezieht, sollte aber alle wesentlichen Einstellungen berücksichtigen. Trotzdem bleibt dann immer noch die Aufgabe, beispielsweise eine Datei „sitemanager.xml" mit den FTP-Zugangsdaten für Filezilla unter Linux wieder an die richtige Stelle zu kopieren.

Das Beispiel soll mahnen, auf Software mit Zugangsdaten und Kennwörtern besonders sensibel zu achten: Es ist kein großes Problem, einen Medienplayer neu einzurichten, egal ob dieser an sich plattformübergreifend wäre oder nicht. Wenn Sie aber Anmeldedaten samt Ihrer Windows-Software über Bord werfen, entstehen ernste Probleme. Ob Sie diese Daten direkt per Konfigurationssicherung übernehmen können oder notfalls extern notieren müssen, hängt von der Software ab.

Webbrowser: Erfreulicherweise ist die wichtigste Software mit Authentifizierungsdaten mühelos von Windows nach Linux zu übertragen, nämlich Webbrowser und Mailclient. Beim Browser brauchen Sie nicht einmal eine lokale Sicherung, sofern Sie die überall angebotene Cloudsynchronisierung verwenden (Chrome, Firefox, Edge, Opera, Vivaldi – alle plattformunabhängig).



Sicherung der Benutzerdaten unter Windows: Das Problem ist es, alles Wichtige zu kopieren und andererseits den Windows-Ballast auszuschließen. Robocopy kann's am besten.



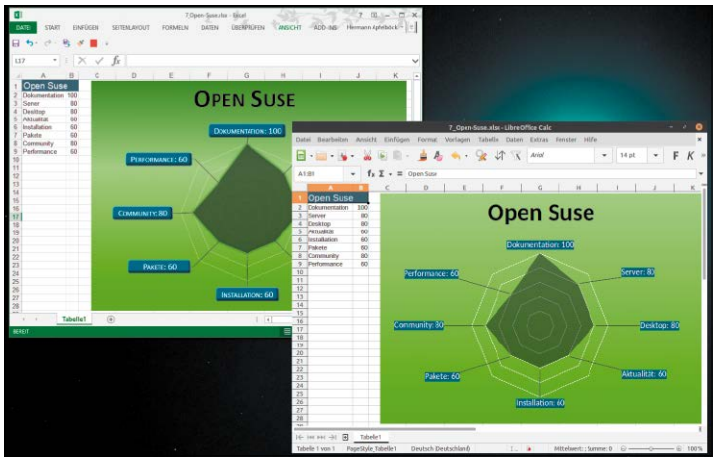
Leichte Übung Browserumzug: Die Synchronisierung in Chrome und Firefox sorgt für plattformübergreifende Vereinheitlichung. Den Umfang bestimmen Sie selbst (hier unter Firefox).

In Chrome/Chromium brauchen Sie nur ein Google-Konto. Über „Einstellungen" und „Google und ich" können Sie die Synchronisierung aktivieren und über deren Umfang bestimmen. Alles zu synchronisieren ist am bequemsten, wichtig sind aber nur Lesezeichen und Passwörter. Ist dies auf einem beliebigen Windows- oder Linux-Rechner erfolgt, dann erhält jeder Chrome/Chromium, den Sie später auf einem anderen System installieren, dieselben Lesezeichen und Kennwörter – sobald Sie auch dort die Synchronisierung aktivieren.

Firefox bietet die Synchronisierung unter „Einstellungen → Synchronisation". Auch hier benötigen Sie ein Konto auf dem Mozilla-Server. Ist dieses eingerichtet, können Sie die Synchronisierung im gewünschten Umfang starten. Jeder weitere Firefox auf einem neuen System erhält bei aktivierter Synchronisierung dieselben Einstellungen.

Mail und Thunderbird: Wer seine Mails im Browser liest und schreibt (Webmailer), muss sich generell nicht umstellen. Nicht viel anders liegt der Fall, wenn Sie zwar ein lokales Mailprogramm, aber das IMAP-Protokoll verwenden. Dann liegen alle Mails auf dem Server und es genügt unter Windows wie Linux das Einrichten des IMAP-Kontos im Mailprogramm.

Besonders einfach gestaltet sich ein Umzug oder Parallelbetrieb, wenn Sie unter Windows das Mailprogramm Thunderbird nutzen. Thunderbird trennt zwischen Programm- und Benutzerdaten. Letztere befinden sich unter Windows im Ordner „%appdata%\Thunderbird\Profiles\[xxxxxxxx].default", wobei das achtstellige „xxxxxxxx" für eine zufällig generierte Zeichenkombination steht. Wenn Sie alle Daten dieses Ordners kopieren und unter Linux im Pfad „~/.thunderbird/[xxxxxxxx].default/" einfügen, können Sie sofort wie gewohnt mit allen Mails und Einstellungen weiterarbeiten. Vor der Aktion muss Thunderbird unter Linux installiert werden und einmal gestar-



Weitreichende, aber nicht vollständige Kompatibilität: Bei einigen speziellen Funktionen und Formatierungen muss Libre Office nachbearbeiten oder passen.

tet sein, damit der Ordner „~/.thunderbird/[xxxxxxxx].default/“ existiert. Löschen Sie dort vor der Kopieraktion alle Dateien, die Thunderbird automatisch erstellt hat.

Outlook und Thunderbird: Thunderbird kann auch aushelfen, um alle Maildaten unter Windows aus Microsoft Outlook zu importieren. Diese Option bietet das Mailprogramm beim Setup automatisch an. Danach transportieren Sie das Thunderbird-Profil – wie oben beschrieben – nach Linux.

Software unter Linux

Für alle ab Seite 46 empfohlenen Desktopdistributionen gilt: Ab Installation sind Sie mit der vorinstallierten Software für alle wesentlichen Aufgaben gerüstet – und mehr noch: Die von Windows gesicherten Benutzerdaten sind allesamt lesbar, abspielbar und weiterzubearbeiten. Ausnahmen gibt es allerdings: Manche proprietäre Formate wie Indesign sind unter Linux nicht unterstützt.

Musikformate wie MP3, WMA, FLAC, AAC, WAV oder OGG spielen alle Standardplayer. Stets zu empfehlen ist der multifunktionale VLC, der alle gängigen Musikformate abspielt. Eigentliche Kernkompetenz des VLC sind aber Videos und Filme jeden Formats. Pixelgrafiken wie JPG oder PNG sind generell problemlos. Vorinstallierte Viewer wie Eog (Eye of Gnome) oder Shotwell kennen alle gängigen Formate und genügen für Thumbnailübersicht und Diashow. Anspruchsvolle Bildbearbeitung leistet Gimp, das alle Bildformate beherrscht. Lediglich bei proprietären Formaten von Photoshop, Illustrator, Corel Draw ist gelegentlich mit Fehlern zu rechnen.

Das meist vorinstallierte Libre Office lädt und bearbeitet alle Dateien, die mit Microsoft Office erstellt wurden (mit Ausnahme von Access-Datenbanken). Hundertprozentige Kompatibilität ist aber nicht erreichbar. Word, Excel und Powerpoint bieten etliche Formate, mathematische Funktionen, Diagrammtypen oder Übergangseffekte, die Libre Office nicht kennt. Bei der Weiterbearbeitung müssen Sie daher gegebenenfalls nachbessern. Geben Sie Dateien am besten im älteren DOC- oder XLS-Format an Windows-Nutzer weiter (nicht DOCX, XLSX). Word & Co. verstehen aber auch die nativen Open-Document-Formate von Libre Office (ODT, ODS).

Noch bessere Kompatibilität zu Microsoft Office bietet Softmaker Office (*www.softmaker.de*). Die Standardversion kostet 69,95, Softmaker Professional 2021 mit Duden Korrektor und weiteren Ergänzungen 99,95 Euro. ■

WINE & PLAYONLINUX

Das ambitionierte Wine (*www.winehq.org*) ist ein Nachbau der Windows-API mit dem Ziel, Windows-Software unter Linux zu ermöglichen. Die Erfolge, die Wine vorweisen kann, fallen qualitativ sehr unterschiedlich aus: Dass eine konkret benötigte Version einer Windows-Software einen störungsfreien „Platinum“- oder „Gold“-Status erreicht, bleibt aber ein Glücksfall. Nüchtern bewertet ist Wine eine Dauerbaustelle, die man Windows-Umsteigern nicht als Standardwerkzeug oder gar Allheilmittel empfehlen kann. Trotzdem kann sich die gezielte Recherche in der Wine-Datenbank (*https://appdb.winehq.org/*) lohnen. Denn falls hier ein für Sie wichtiges Programm unter „Gold“ oder „Platinum“ erscheint, dann ist Wine die einfachere Lösung gegenüber Dualboot oder Virtualisierung.

Das zusätzliche Werkzeug Playonlinux (*www.playonlinux.com*) ist nur ein Organisationstool für Wine. Aber es vereinfacht Installationen von Software und bietet eine Verwaltung für mehrere Wine-Versionen. Playonlinux ist über

```
sudo apt install playonlinux
```

zu installieren und bringt dabei automatisch ein aktuelles Wine mit. Wenn ein Programm eine andere Wine-Version bevorzugt, erledigt Playonlinux dessen Einrichtung bei der Installation mit. Das Tool erstellt im Pfad „~/.PlayOnLinux/wineprefix“ jeweils eine eigene virtuelle Windows-Partition für jedes installierte Programm. Der Aufwand ist beträchtlich und sollte nicht für jedes marginale Windows-Tool erfolgen.

Wenn Sie Playonlinux starten, klicken Sie zunächst auf „Installieren“. Das Installationsmenü zeigt Windows-Programme und Spiele, für die es bewährte Installations-Scripts gibt. Mit der Auswahl und „Installieren“ dieser Softwarevorgaben sind Sie auf der sicheren Seite. Ist die gewünschte Software in den Vorgaben nicht enthalten, können Sie folgenden Weg versuchen: Im Installationsmenü klicken Sie unten auf „Installiere ein Programm, das nicht aufgelistet ist“. Damit startet die manuelle Installation, bei der Sie die Option „Installiere ein Programm in einem neuen virtuellen Laufwerk“ anklicken und für die neue Umgebung einen Namen vergeben. Den nächsten Dialog überspringen Sie mit „Weiter“, sofern Sie mit den Optionen nichts anfangen können. Nun entsteht eine generische Windows-Umgebung unter „~/.PlayOnLinux/wineprefix /[Name]“, in die Sie im nächsten Schritt das Windows-Programm installieren. Ob die Software dann ohne spezielle Anpassung funktioniert, ist ein Experiment mit ungewissem Ausgang.

Digital Life

Windows 11
Diagnose, Wartung, Rettung



Jetzt am Kiosk!

Für nur
5,90 €

71 Tools und Vollversionen gratis!

Bestellen unter
www.pcwelt.de/windows oder per Telefon: 0931/4170-177 oder ganz einfach:

1. Formular ausfüllen **2. Foto machen** **3. Foto an idg-techmedia@datam-services.de**

Ja, ich bestelle das Digital Life Schritt für Schritt Booklet 2/22 Windows 11 für nur 5,90 €.

Zzgl. Versandkosten (innerhalb Deutschland 2,50€, außerhalb 3,50€)

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

○ Ich bezahle bequem per Bankeinzug. ○ Ich erwarte Ihre Rechnung.

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

DigitalLife erscheint im Verlag IT Media Publishing GmbH & Co. KG, Gotthardstraße 42, 80686 München, Registergericht München, HRA 104234, Geschäftsführer: Sebastian Hirsch.
Die Kundenbetreuung erfolgt durch den PC-WELT Kundenservice, DataM-Services GmbH, Postfach 9161, 97091 Würzburg

Systemtipps für Umsteiger

Nach der Wahl der richtigen Linux-Distribution ist die Installation einfach und der Desktop umsteigerfreundlich. Trotzdem ist Linux anders und kein Quasi-Windows. Dieser Beitrag erklärt wichtige Unterschiede im Benutzeralltag.

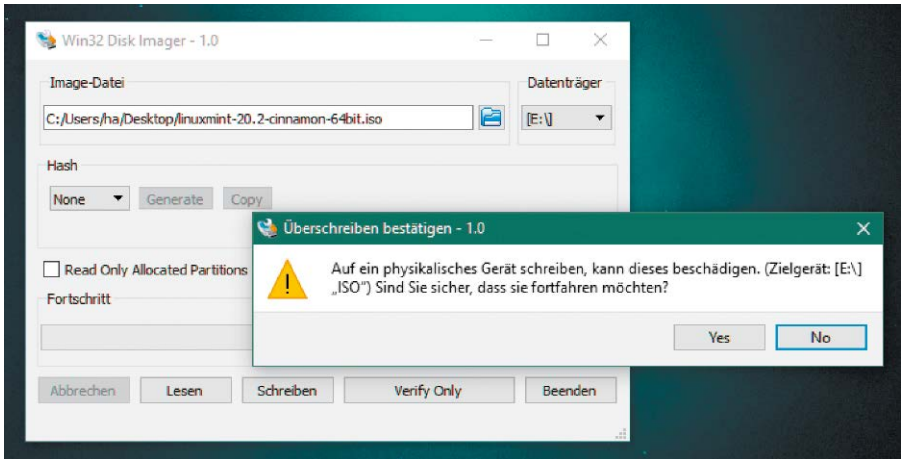
VON HERMANN APFELBÖCK

Die folgenden zwei Seiten machen aus Windows-Nutzern keine Linux-Gurus. Aber sie benennen typische Umsteigerprobleme und zeigen knapp und praxisnah, wie Sie sich am schnellsten auf Linux-Verhältnisse umstellen.

Handarbeit mit ISO-Abbildern

Die Live- und Installationsabbilder von Linux-Distributionen müssen bootfähig auf USB kopiert werden. Diese Prozedur ist Windows-Nutzern nicht selbstverständlich. Das einfachste Werkzeug, um dies unter Windows zu erledigen, ist der Win 32 Disk Imager (auf Heft-DVD). Hier genügt es, das Zielgerät („Device“) und die Quelldatei („Image File“) anzugeben. Lassen Sie sich alle Dateien anzeigen („*.*“), weil das Tool sonst nur IMG-Abbilder anbietet. Die Schaltfläche „Schreiben“ startet den Kopiervorgang. Unter Linux kann im Prinzip jedes Laufwerkstool (Gnome-Disks, KDE-Partitionmanager) ISO-Dateien bootfähig auf USB befördern.

Für bereits fortgeschrittene Ansprüche, aber nur für Ubuntu-basierte Systeme eignet sich Unetbootin (auf Heft-DVD). Hier nutzen Sie die Option „Abbild“ und navigieren dann zur gewünschten ISO-Datei. Danach wählen Sie neben „Typ“ die Option „USB-Laufwerk“, und neben „Laufwerk“ geben Sie den Laufwerksbuchstaben des USB-Sticks an. Der Vorteil von Unetbootin ist die zusätzliche Persistenzoption („Platz um Dateien zwischen Neustart zu erhalten“): Dies macht die an sich unveränderlichen Livesysteme ein Stück anpassungsfähig. Geht es nur um das Ausprobieren oder die Installation einer Distribution, ist diese Technik überflüssig.



Um ein Linux zu installieren, benötigt man dessen ISO-Abbild bootfähig auf USB-Stick. Der simple Win 32 Disk Imager erledigt diesen Kopierjob unter Windows.

Navigation im Dateisystem

Der Gang zur obersten Ebene im Dateimanager ist für Umsteiger irritierend: Statt der angeschlossenen Datenträger erscheint die Ordnerstruktur des Linux-Systems. Datenträger wie USB-Laufwerke sind im Prinzip an beliebiger Stelle eingehängt (meist unter „/media“ oder „/mnt“). Das ist aber nur eine Frage der Gewöhnung: Nutzen Sie in der Seitenleiste des Dateimanagers die Rubrik „Geräte“. Diese zeigt alle Datenträger. Das Mounten erfolgt durch Mausklick auf das „Gerät“. Der Mountpunkt im Dateisystem muss Sie dabei gar nicht interessieren.

Was Windows unter „Eigene Dateien“ speichert, finden Sie in Linux unter „/home“ (in der Seitenleiste des Dateimanagers meist als „Persönlicher Ordner“ angezeigt). Wie unter Windows haben Sie hier alle Rechte. Alle Benutzerdateien und Downloads sowie die Konfigurationseinstellungen von Software landen dort. Letztere sind standardmäßig versteckt, lassen sich aber bei den meisten Dateimanagern mit Strg-H einblenden.

Die Laufwerksbezeichnungen „/dev/sd[x][n]“

Laufwerke eindeutig zu bestimmen, ist fundamental bei der Installation oder beim Schreiben von ISO-Abbildern. Unter Windows dienen aufsteigende Buchstaben als Kennung. Linux ist eigentlich klarer, jedoch komplizierter: Eine Kennung wie „/dev/sda1“ beginnt mit „/dev/“ für „Device“, „sd“ kennzeichnet die Schnittstelle „Sata Device“ (seltener „sc“ für SCSI-Device, „m“ für Raid). Wichtig wird es danach: „a“ bedeutet die erste interne Festplatte, „b“ die zweite oder bereits das erste USB-Laufwerk. Die nach-

folgende Zahl ist die Partitionskennung. Die Kennungen sind mit grafischen Werkzeugen wie „Laufwerke“ (gnome-disks) oder im Terminal mit *lsblk -f* zu ermitteln.

„sudo“ und Administratorrechte

Die Verhältnisse zwischen Benutzer- und Administratorkonto unter Linux und Windows sind ähnlich, aber der Wechsel vom Benutzer- zum root-Recht folgt anderen Regeln. Möglich ist dieser Wechsel bei Windows wie Linux nur Systemkonten, die zur Gruppe der Administratoren gehören (der Erstbenutzer, den Sie bei der Installation einrichten, gehört immer dazu).
Während Windows nur das „Ja“ bei der Abfrage der „Benutzerkontensteuerung“ verlangt, fordert Linux die Eingabe des Systemkennworts. Diese Abfrage erscheint bei allen systemnahen Aktionen (Installation, Paketquellen, Aktualisierung). Im Terminal kann dem Befehl „sudo“ vorangestellt werden, um dem Befehl root-Recht zu verleihen.
Im Dateimanager sind Schreibaktionen wie „Ordner anlegen“ oder „Löschen“ inaktiv, wenn man sich jenseits von „/home“ oder „/media“ aufhält. Linux Mint bietet daher das Kontextmenü „Als Systemverwalter öffnen“, um im Dateimanager uneingeschränkt zu arbeiten. Wenn ein Dateimanager diese Option nicht besitzt, können Sie ihn im Terminal mit (Beispiel)

```
sudo nautilus
```

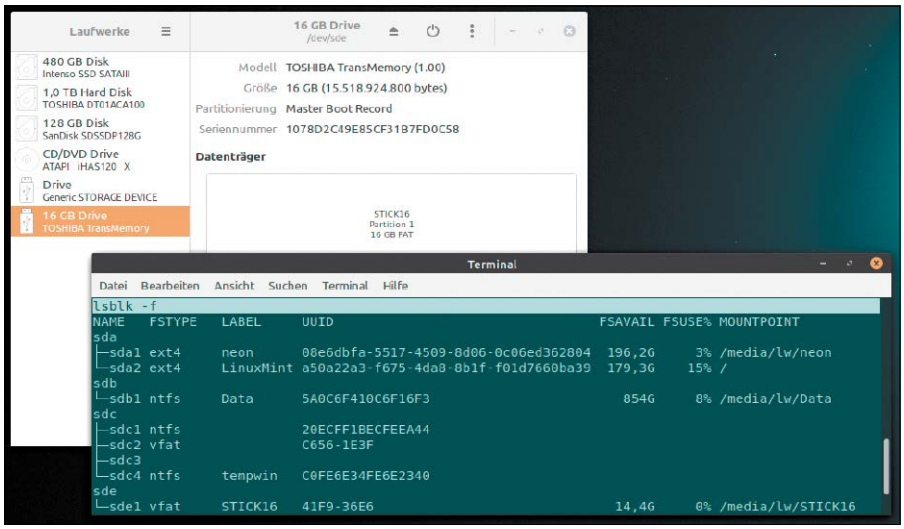
starten, um root-Recht zu erzwingen.

Achtung auf Groß-Kleinschreibung

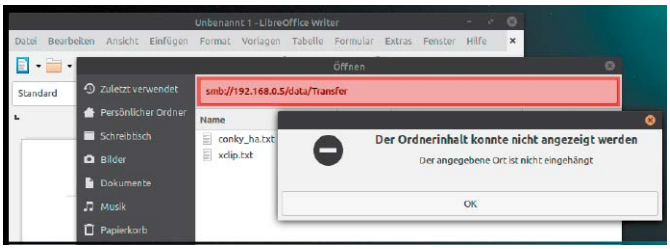
Terminalbenutzer stolpern früher oder später über das Problem, dass Linux konsequent casesensitiv arbeitet. Unter Windows spielt die Schreibung keine Rolle. „DIR“ ist dasselbe wie „dir“. Unter Linux ist genaue Schreibung zwingend: Den Befehl „Lsblk“ gibt es nicht und ein Schalter „-X“ bedeutet etwas anderes als „-x“. Wenn Sie im Home-Verzeichnis „ls d*“ abfragen, erhalten Sie kein Ergebnis, weil „Dokumente“ und „Downloads“ mit Großbuchstaben beginnen.

Netzprotokolle und Anwendungssoftware

Linux-Dateimanager beherrschen die Netzwerkprotokolle Samba (smb://), FTP (ftp://), SSH (sftp://) und Webdav (webdav://). Adressen wie „smb://raspberry“ oder „smb://192.168.178.10“ können Sie daher direkt in die Adresszeile des Dateimanagers eingeben. Für Einsteiger irritierend ist die Tatsache, dass ein solcher Netzwerkpfad zwar im Dateimanager ans Ziel führt, im Terminal oder einer Software jedoch scheitert. Einfacher Grund ist, dass diese Programme die Protokolle nicht beherrschen: Sie erwarten, dass Netzressourcen in das lokale Dateisystem eingehängt wurden, und arbeiten nur über den Mountpunkt. Daher die Regel – erst im Dateimanager mounten, danach in der Software nutzen!



Keine Zweifel bei Laufwerkskennungen: Sowohl grafische Werkzeuge wie Terminaltools bieten ausreichend Infos, um einen Datenträger eindeutig zu identifizieren.



Libre Office kann die Netzfreigabe nicht direkt nutzen. Die meisten Anwendungen setzen voraus, dass Netzlaufwerke vorher mit dem Dateimanager ins Dateisystem geladen werden.

Die lokalen Dateirechte

Dateirechte sind unter Windows wie Linux kompliziert. Einsteiger können nichts Klügeres machen, als Rechteänderungen zu vermeiden. Dabei helfen Desktopsysteme mit Dateimanagern, die Datenträger und Netzfreigaben automatisch so ins Dateisystem mounten, dass keine Konflikte entstehen. Dennoch muss man wissen, wie sich Dateirechte umstellen lassen.
Um zunächst den Besitz von Dateien zu übernehmen, ist das Terminal den grafischen Dateimanagern („Eigenschaften → Zugriffsrechte“) überlegen. Der Befehl chown („change ownership“) arbeitet mit Schalter „-R“ rekursiv über ganze Ordnerebenen (Beispiel):

```
sudo chown -R sepp:sepp /home/sepp
```

Nachfolgende Rechteänderungen (die den Besitz voraussetzen) sind auch im grafischen Dateimanager mit „Eigenschaften → Zugriffsrechte“ gut zu erledigen. Unter Ubuntu kann die Schaltfläche „Zugriffsrechte der enthaltenen Dateien ändern“ die Rechte setzen – für „Besitzer“, „Gruppe“ und „Andere“. Bei Linux Mint funktioniert die Rechtevergabe ähnlich. Das Fenster „Eigenschaften → Zugriffsrechte“ sieht nur etwas anders aus. Es gibt die drei Rubriken „Eigentümer“, „Gruppe“ und „Andere“, bei der letzten fehlt allerdings die Beschriftung. Hinter „Ordnerzugriff“ stellen Sie wie bei Ubuntu die Zugriffsrechte ein. Die Einstellungen gelten für alle Unterordner, wenn Sie auf „Zugriffsrechte auf enthaltene Dateien übertragen“ klicken.
Eine weitere Rechteänderung, die jeder Linux-Nutzer kennen muss, betrifft das „Ausführen“-Bit für Scripts und Binärdateien, das sich über „Eigenschaften → Zugriffsrechte“ oder mit

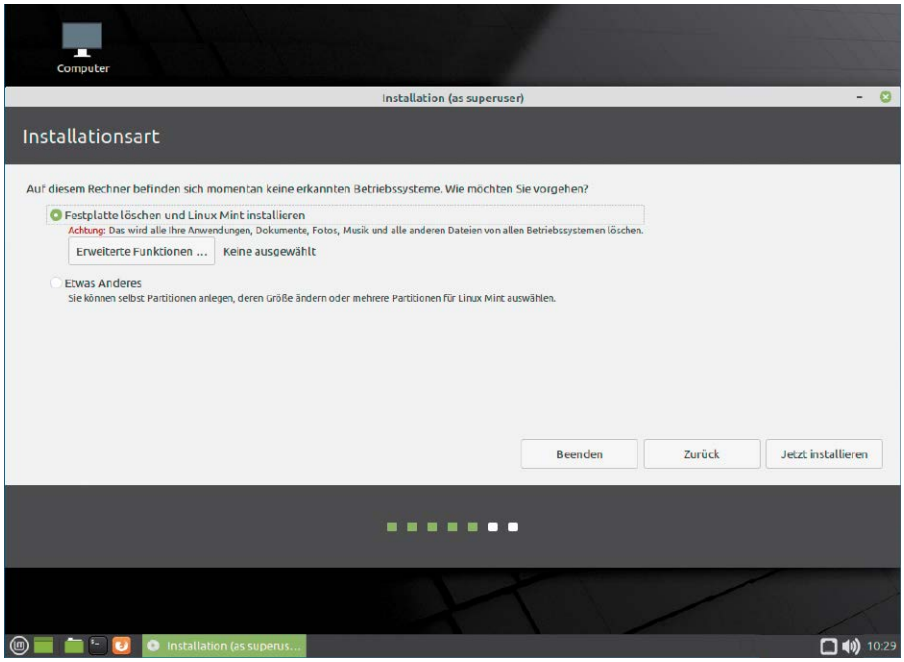
```
chmod +x [Datei]
```

setzen lässt. ■

Installationen und Upgrades bei Mint

Linux Mint 20 bringt Verbesserungen bei der Aktualisierungsverwaltung, beim Dateimanager und Warpinator, ferner Feinschliff am Cinnamon-Desktop. Hier gibt es die besten Tipps zur System- und Desktopoptimierung des jüngsten Mint.

VON HERMANN APFELBÖCK



Einfache Soloinstallation: Zum Einrichten als alleiniges System wählen Sie „Festplatte löschen“. Linux Mint übernimmt damit die komplette erste (und oft einzige) interne Festplatte.

Dieser Artikel bespricht sowohl die automatisierten Installeroptionen als auch die wichtigsten manuellen Partitionierungsmethoden eines Mint-Setups. Die Heft-DVD bietet, Linux Mint 20.3 „Edge“ mit Cinnamon-Desktop zum Ausprobieren und Installieren. Die Edge-Variante ist eine offizielle Mint-Edition, die sich nur im jüngeren Kernel von der Standardedition unterscheidet (Kernel 5.4) und somit besonders aktuelle Hardwaretreiber mitbringt.

Das Upgrade auf Version 20.3

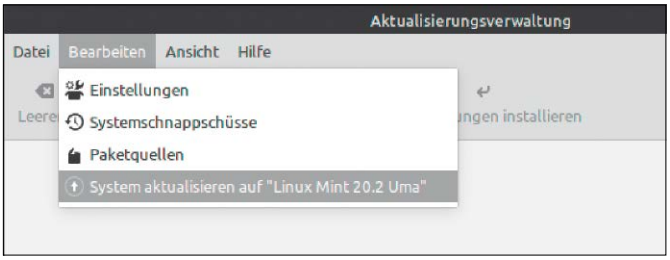
Wer bereits ein Linux Mint 20, 20.1 oder 20.2 laufen hat, braucht natürlich kein Installationsmedium, sondern kann das System per Upgrade aktualisieren.

Mint-Upgrades auf die nächsthöhere Version, aktuell also von 20.x auf 20.3, erfolgen via Internet über die Aktualisierungsverwaltung. Gehen Sie dort auf „Auffrischen“ und installieren Sie alle verfügbaren Updates. Wenn dann im Hauptfenster eine neuere Version der Aktualisierungsverwaltung (mintupdate) angeboten wird, installieren Sie diese mit der Schaltfläche „Die Aktualisierung anwenden“. Nach diesem Vorgang startet die Aktualisierungsverwaltung mit der aktuellsten Version neu und zeigt im Menü „Bearbeiten“ die zusätzliche Option „System aktualisieren auf Linux Mint 20.3 Una“. Damit lösen Sie das Upgrade aus.

Manche Mint-Nutzer, insbesondere auch LinuxWelt-Leser, haben eventuell die Betaversion 20.2 auf dem Rechner. Ein Upgrade auf das finale 20.2 ist hier nicht erforderlich. Hier genügt aber standardmäßiges „Auffrischen“ und „Aktualisierungen installieren“ in der Aktualisierungsverwaltung oder alternativ

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

im Terminal, um die Beta auf den endgültigen Stand zu bringen.



Upgrade der Vorgängerversionen 20.x: Der Vorgang wird über diese Option der „Aktualisierungsverwaltung“ angestoßen.

Livesystem und Soloinstallation

Für eine Neuinstallation verwenden Sie als LinuxWelt-Leser am einfachsten die Heft-DVD mit Linux Mint 20.3 Edge. Die ISO-Abbilder aller Mint-Editionen erhalten Sie auf der Seite *https://linuxmint.com/download.*

php, die auf deutsche und internationale Quellen verweist („Download mirrors“). Die Auswahl der Quelle spielt keine Rolle für die Sprachlokalisierung. Das etwa zwei GB große ISO-Image schreiben Sie nach dem Download mit einem Werkzeug wie Etcher, Win 32 Disk Imager (unter Windows), Gnome-Disks oder dd auf einen USB-Stick und booten dann damit Ihr Zielgerät.

Ob Heft-DVD oder Kopie auf USB – es handelt sich in jedem Fall um ein Livesystem, das auch das Ausprobieren der jeweiligen Edition ermöglicht. Die Installation startet dann der Desktoplink „Install Linux Mint“, wobei alle Mint-Editionen den identischen Ubuntu-Installer verwenden. Die folgenden Anleitungen gelten daher uneingeschränkt für alle Editionen und voraussichtlich auch für künftige Mint-Versionen.

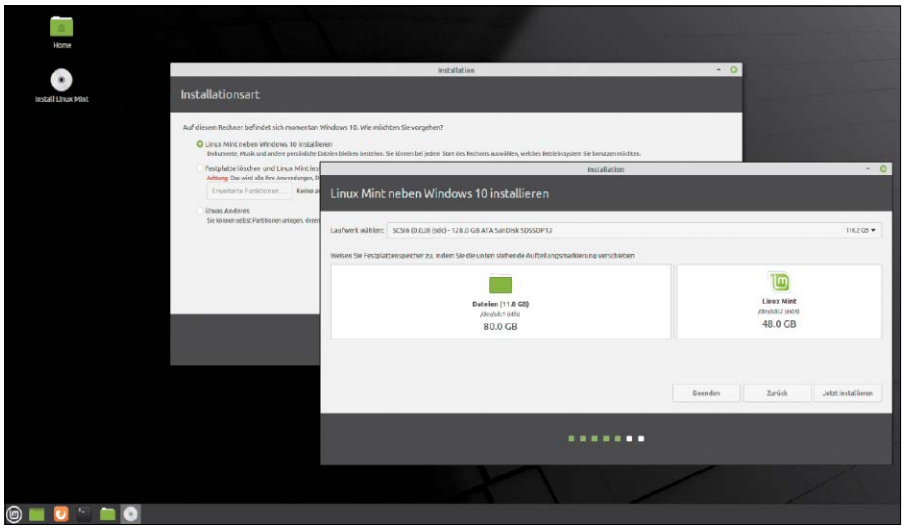
Für eine Installation als alleiniges System spielt es eigentlich keine Rolle, ob das Mint-Livesystem im Bios- oder im Uefi-Modus bootet. Jedoch werden Festplatten immer größer, und bei einer internen Zielfestplatte mit mehr als zwei TB ist auch für eine Soloinstallation der modernere Uefi/GPT-Bootmodus erforderlich. Mit Uefi-Boot sind Sie in jedem Fall auf der sicheren Seite: Verwenden Sie daher zum Booten das Bootmenü des Bios (F2, F8, F12, Esc-Taste) und wählen dort jenen Eintrag des Bootgeräts, der mit „Uefi“ gekennzeichnet ist. Der zweite Eintrag ohne „Uefi“ bootet im Bios-Modus.

Im Livesystem starten Sie die Installation mit der Desktopverknüpfung. Zuerst wählen Sie die Sprache „Deutsch“ und deutsche Tastatur aus. Im nächsten Schritt erscheint der entscheidende Dialog „Installationsart“ mit zwei möglichen Szenarien:

1. Wenn die primäre Festplatte des Rechners kein System enthält, lautet die oberste und vormarkierte Option „Festplatte löschen und Linux Mint installieren“.

2. Hat der Installer auf der primären Festplatte ein System gefunden, dann erscheint als oberste und markierte Option „Linux Mint neben [...] installieren“ und erst als zweite Option „Festplatte löschen [...]“.

Wenn Sie Linux Mint als alleiniges System verwenden wollen und ein eventuell bestehendes System nicht mehr brauchen, wählen Sie in beiden Situationen die Option „Festplatte löschen“. Dabei wird die Festplatte formatiert, der Datenbestand (und ein eventuelles System) gelöscht und das neue System eingerichtet. Danach müssen Sie nur noch im Fenster „Wer sind Sie?“ die Angaben für das erste Benutzerkonto eintragen. Dieses Konto erhält automatisch den Status eines Systemverwalters.



Parallelinstallation: Der Installer erkennt bestehende Systeme und partitioniert bei Bedarf neu. Mit der Maus verändern Sie die Partitionsgrößen nach Bedarf.

Multiboot-Installationen

Bei Multiboot-Installationen ist die Unterscheidung zwischen Bios/MBR- und Uefi/GPT-Partitionsstil entscheidend. Die Parallelinstallation kann nur gelingen, wenn das Mint-Livesystem in jenem Modus gestartet wird, in dem das bereits vorhandene System installiert wurde. Andernfalls wird der Installer das vorhandene System nicht erkennen und – sofern der Benutzer das Problem nicht bemerkt – bei der Neuinstallation überschreiben.

Auf PCs mit Windows 10 herrscht der Uefi-Modus mit GPT-Partitionsstil. Weitere Systeme müssen auf die gleiche Weise eingerichtet werden. Den aktuellen Partitionsstil des existierenden Systems können einschlägige Tools ermitteln – unter Windows die „Datenträgerverwaltung“, unter Linux Mint das Standardwerkzeug Gnome-Disks. GPT erscheint hier als „gpt“, der MBR-Modus als „msdos“.

Um beim Rechnerstart den richtigen Modus zu wählen, benötigen Sie das Bootmenü des Uefi-Bios. Wie bereits beschrieben, ist das Bootmenü ist durch frühzeitiges Drücken der Taste F2, F8, F12 oder Esc zu erreichen. Dort erscheinen die vorhandenen Laufwerke zwei Mal – mit und ohne den Vorsatz „UEFI“. Für Uefi-Parallelinstallation wählen Sie den „UEFI“-Eintrag.

Nach dem Start des Mint-Livesystems erhalten Sie dann im Installer weitere Bestätigung für den richtigen Modus, sofern unter „Installationsart“ das bereits vorhandene System genannt sowie die Option „Linux Mint neben [XXX] installieren“ angeboten wird.

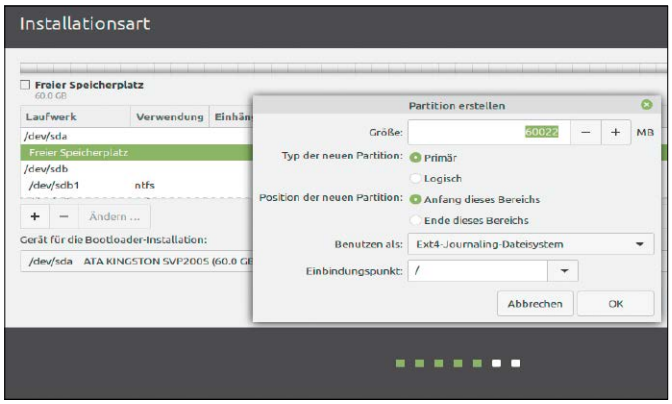
Was das Fenster „Installationsart“ genau anbietet, hängt von der Situation ab. Wir gehen hier von einer Parallelinstallation neben Windows aus, jedoch gelten diese Infos auch für ein Linux-System im Uefi-Modus:

A. Gibt es nur eine interne Festplatte, die derzeit von Windows belegt ist, dann sehen Sie die Option „Linux Mint neben Windows Boot Manager installieren“. Nach einem Klick auf „Weiter“ schlägt der Assistent eine neue Aufteilung der Partitionen vor, indem er die Windows-Partition verkleinert und Platz für Linux Mint schafft. Die Neupartitionierung ist notwendig, weil jedes System eine eigene Partition benötigt. Die Partitionsgrößen justieren Sie mit der Aufteilungsmarkierung und der Maus. Beachten Sie, dass Windows mehr Platz benötigt als Linux Mint.

B. Ist neben einem installierten Windows (oder Linux) eine freie Partition oder Festplatte vorhanden, dann erkennt der Installer das automatisch. Auch in diesem Fall wählen Sie die Option „Linux Mint neben Windows Boot Manager installieren“. Eine Neupartitionierung und Größenanpassung entfällt dabei.

Vorhandenes System ersetzen

Eine technisch einfachere Multiboot-Installation ergibt sich auf einem Rechner, der zwei oder mehrere Systeme enthält und



System ersetzen: Um ein bestehendes System durch Mint zu ersetzen, müssen Sie die Partition löschen und den „freien Speicherplatz“ mit Ext4 ausstatten. Einhängepunkt ist „/“.

auf dem nun eines der bestehenden Systeme durch Linux Mint ersetzt werden soll. Auch hier ist es entscheidend, das Livesystem im richtigen Modus (Bios/Uefi) zu booten, damit der Installer die Partitionsverhältnisse richtig analysiert. Ein Boot im falschen Modus erkennen Sie daran, dass der Installer keine installierten Systeme meldet, obwohl welche vorliegen.

Um ein bestehendes System durch Mint zu ersetzen, wählen Sie dann im Fenster „Installationsart“ den untersten Punkt „Etwas Anderes“. Dort löschen Sie in der Laufwerksliste mit der Schaltfläche „-“ die Partition des obsoleten Systems und erstellen im „Freien Speicherplatz“ mit der „+“-Schaltfläche eine neue Ext4-Partition mit dem Mountpunkt „/“. Unter „Gerät für die Bootloader-Installation“ übernehmen Sie die voreingestellte primäre Festplatte „/dev/sda“.

Linux Mint auf USB installieren

Der Installer schlägt als Ziel stets die erste interne Festplatte „/dev/sda“ vor. Für die Installation auf ein USB-Gerät müssen Sie die richtige Zielpartition manuell festlegen. Daher wählen Sie im Fenster „Installationsart“ die Option „Etwas Anderes“. In der Partitionsübersicht klicken Sie zunächst auf die Schaltfläche „-“, um vorhandene Partitionen auf dem USB-Datenträger zu entfernen. Dabei muss absolute Gewissheit über den richtigen Datenträger bestehen. Erstellen Sie dann auf dem „freien Speicherplatz“ mit der „+“-Schaltfläche eine neue, primäre Partition mit dem kompletten Speicherplatz und dem Dateisystem Ext4. Hinter „Einbindungspunkt“ wählen Sie den Eintrag „/“ aus der Liste. Unter „Gerät für die Bootloader-Installation“ wählen Sie dasselbe USB-Laufwerk aus, auf dem Sie installieren - etwa „/dev/sdb“. Es ist wichtig, auch den Bootloader auf USB zu schreiben, andernfalls startet das System nur auf dem Rechner, mit dem Sie installiert haben.

Separate Home-Partition

Weder der Ubuntu/Mint-Installer noch andere Installer haben die nützliche Option eines unabhängigen Home-Verzeichnisses als automatisierten Standard. Wer sein „Home“ auf eigener Partition einrichten will, muss im Dialog „Installationsart“ die Option „Etwas Anderes“ ansteuern – und somit die manuelle Partitionierung. Zunächst wählen Sie das Laufwerk, auf dem Sie das System installieren möchten. Dort legen Sie mit der „+“-Schaltfläche erst die „EFI-System-Partition“ an, für die etwa 100 MB ausreichen. Danach folgt im freien Speicherplatz die Systempartition mit dem Dateisystem Ext4 und dem „Einbindungspunkt“ „/“. Als Nächstes erstellen Sie auf dem weiteren Datenträger die Home-Partition mit dem Einbindungspunkt „/home“ und dem Dateisystem Ext4 oder XFS. Für alles Weitere und den nötigen Eintrag in die „/etc/fstab“ sorgt der Installer. Im so instal-

VERSCHLÜSSELUNGSVARIANTEN

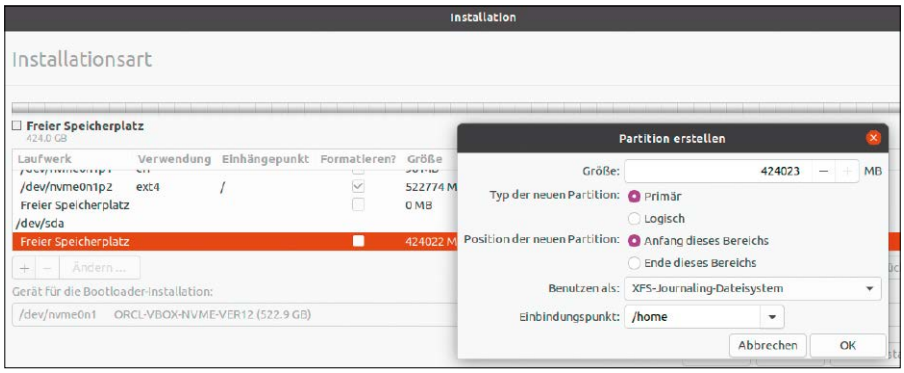
Der Mint-Installer bietet zwei Methoden an, um vertrauliche Daten zu verschlüsseln. Insbesondere auf mobilen Notebooks sollte eine dieser Methoden gewählt werden, damit die Benutzerdaten bei Verlust oder Fremdzugriff unlesbar geschützt bleiben.

Partitionsverschlüsselung (Cryptsetup): Cryptsetup-verschlüsselte Systeme bieten den sichersten und schnellsten Datenschutz unter Linux. Der Datenträger lässt nach Ausbau oder beim Booten durch Fremdsysteme keinen Einblick in die Daten zu, denn Cryptsetup leistet eine Komplettverschlüsselung der Systempartition. Lediglich die kleine Bootpartition „/boot“ mit binären Bootdaten bleibt unverschlüsselt. Cryptsetup-Verschlüsselung ist nur bei der Installation möglich – nicht nachträglich. Beachten Sie ferner, dass Sie für Cryptsetup dem Installer stets die gesamte primäre Festplatte überlassen müssen. Eine kompliziertere Kombination von Cryptsetup mit Multiboot oder mit manuellen Partitionsaufteilungen ist nicht vorgesehen. Die Festplatte muss folglich leer sein oder darf nur noch Daten enthalten, die Sie nicht mehr benötigen.

Für Cryptsetup wählen Sie unter „Installationsart“ die Option „Festplatte löschen und Linux Mint installieren“. Über „Erweiterte Funktionen“ kommen Sie zum Unterfenster „LVM...verwenden“. Der Logical Volume Manager (LVM) ist notwendig, um neben der Bootpartition die Cryptsetup-formatierte Partition und die virtuelle LVM-Partition zu organisieren, die bei korrekter Kennworteingabe unverschlüsselt ins Dateisystem geladen wird. Ist der Punkt LVM aktiviert, können Sie jetzt die entscheidende Option einschalten: „Die neue Linux-Mint-Installation zur Sicherheit verschlüsseln“. Nach „OK“ und „Jetzt installieren“ folgt noch die Abfrage des Sicherheitsschlüssels. Dieses Kennwort sollte eine gewisse Mindestkomplexität haben, aber für tägliche Eingabe zumutbar sein. Denn jedes Mal, wenn Sie später das System booten, erscheint zunächst die Abfrage „Please unlock disk [...]“.

Home-Verschlüsselung (Ecrypt FS): Das Mint-Team übernimmt den Ubuntu-Installer Ubiquity seit Jahren nicht original. Dass Mint etwa auf das überdimensionierte ZFS-Dateisystem verzichtet, ist für ein Desktopsystem nachvollziehbar und lobenswert. Ein weiterer auffälliger Unterschied zu Ubuntu ist die nach wie vor verfügbare Option „Meine persönlichen Daten verschlüsseln“ beim Anlegen des Erstbenutzerkontos (im Fens-

lierten System zeigen sich zunächst keine Unterschiede zu einer Standardinstallation. Die Vorteile einer Home-Partition auf einem unabhängigen Datenträger werden erst evident, wenn Sie bei einer künftigen Neuinstallation sofort wieder alle vertrauten Daten und Softwareeinstellungen vorfinden. Dazu müssen Sie nur bei der manuellen Partitionierung („Etwas Anderes“) den Home-Datenträger ansteuern und das dort genutzte Dateisystem und als Einbindepunkt „/home“ wählen. Wichtig ist, das Häkchen vor „Partition formatieren“ nicht zu verwenden, um die Daten zu erhalten.



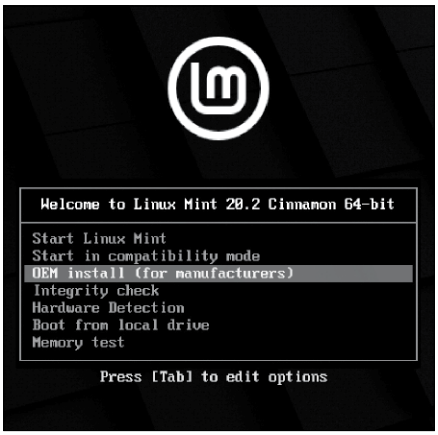
Bei der Installation lässt sich eine eigene Partition für die Home-Verzeichnisse konfigurieren. Diese lässt sich bei späterer Neuinstallation in das nächste System einbinden.

Die „OEM“-Installationsvariante

Beim Start des Mint-Livesystems erscheint beim Booten die Option „OEM install...“. Diese Option eignet sich für die Systemeinrichtung für Freunde, Familienmitglieder oder Arbeitskollegen. Dabei konfigurieren Sie das System vorab mit dem temporären Konto „oem“. Der künftige Nutzer kann später unabhängig über sein eigenes Konto entscheiden (Name, Kennwort).

Das Setup unterscheidet sich zunächst kaum von einer normalen Installation. Ein wichtiger Unterschied ergibt sich beim Anlegen des Erstbenutzers („Wer sind Sie?). Dieser ist unveränderbar als „oem“ vorgegeben. Ein Passwort für dieses temporäre Konto muss dennoch vergeben werden.

Der erste Start des so installierten Systems geht ohne Anmeldung zum Desktop. Dort ist nun Gelegenheit, mit dem temporären Konto „oem“ das System zu optimieren. Sinnvoll sind nur systemweite Aktionen (Aktualisierung, Softwareausstattung, Netzwerkeinstellungen). Danach kann der Desktoplink „Vorbereitung zur Auslieferung“ geklickt und der Rechner dem Endbenutzer übergeben werden. Diesem wird nach dem Start der bekannte Installerdialog „Wer sind Sie?“ angeboten, um den Erstbenutzer anzulegen. Danach laufen noch etliche Installationsergänzungen. Der Benutzer wird System, Software, Netzwerk so vorfinden, wie Sie es mit dem temporären „oem“-Konto optimiert haben. ■

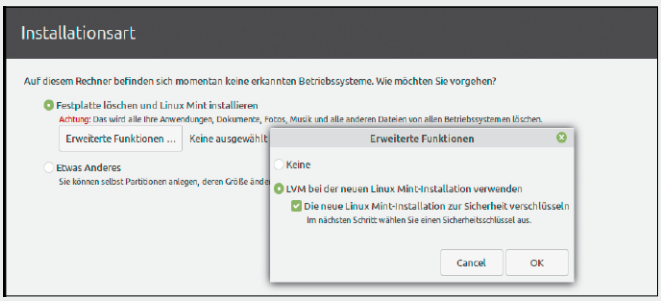


Nicht nur für Händler interessant: Die OEM-Installation ermöglicht eine optimierte Systemeinrichtung für Kollegen oder Freunde.

ter „Wer sind Sie?“). Diese Home-Verschlüsselung mit Ecrypt FS schützt alle Dateien unter „/home/[user]“. Diese liegen verschlüsselt unter „/home/.ecryptfs/[user]/.Private“ und werden unter „/home/[user]“ unverschlüsselt eingehängt, sobald sich der Benutzer anmeldet.

Ubuntu hat diese Verschlüsselungsmethode schon 2018 ersatzlos gestrichen. Die Gründe sind nicht von der Hand zu weisen: Kritiker wiesen darauf hin, dass Ecrypt FS Schwächen besitzt, da temporäre Benutzerdateien auch außerhalb von „Home“ entstehen, die dann nicht verschlüsselt werden. Gravierender noch sind Leistungseinbußen bei großen Dateimengen. Um diese Einbußen zu minimieren, verzichtet Ecrypt FS auf das Aushängen des Home-Ordners beim Abmelden. Dies ist eine weitere Designschwäche und ein theoretisches Datenschutzproblem auf Multiuser-Systemen.

Empfehlung: Die technisch einfache Home-Verschlüsselung kommt in Betracht, wenn das Benutzer-Home keine riesigen Datenmengen aufnehmen wird. Sie ist transparent (Entschlüsselung durch Anmeldung) und komfortabel, mit allen sonstigen Installeroptionen kombinierbar und lässt sich nach der Installation auch für andere Systemkonten aktivieren (in Mate/XFCE unter „Benutzer und Gruppen“, unter Cinnamon nur im Terminal). Cryptsetup ist schneller, umfassender und ohne theoretische Schwächen. Nachteile sind die allfällige Passworteingabe beim Start und die komplexere LVM-Partitionierung, die nur bei der Installation erfolgen kann und dabei immer den kompletten Datenträger übernimmt.

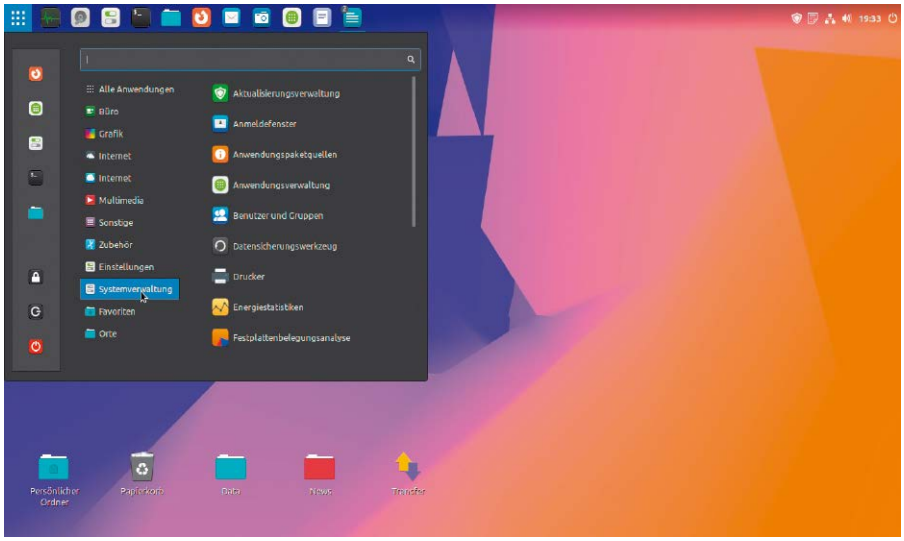


Cryptsetup-Datenträgerverschlüsselung: Dieser Daten- und Systemschutz ist in Linux Mint einfach einzurichten, falls das neue System die komplette primäre Festplatte übernehmen darf.

Linux Mint 20.3

Linux Mint 20.3 erneuert seine Systembasis, indem es seinen Unterbau auf das dritte Point Release 20.04.3 LTS seines Ubuntu-Vorbilds umstellt. Wir stellen die Neuheiten in Version Linux Mint 20.3 gegenüber dem Vorgänger vor.

VON HERMANN APFELBÖCK



Das beliebte Desktopsystem Linux Mint erhielt Anfang 2022 sein Update auf Version 20.3. Mint basiert auf Ubuntu LTS. Das dritte Point Release von Ubuntu LTS, nämlich 20.04.03, war schon Ende August 2021 erschienen, doch Mint benötigte einige Zeit, um den neuen Unterbau zu übernehmen. Mint 20.3 wird, wie sein Unterbau, bis 2025 mit Updates unterstützt. Das jüngste Mint „Una" garniert somit Systemaktualisierung mit zahlreichen, aber durchgehend bescheidenen Änderungen.

Cinnamon-Edition auf Heft-DVD: Linux-Welt-Leser, welche die Hauptedition mit Cinnamon neu installieren möchten, sparen sich den 2,1-GB-Download, weil das Live- und Installationsmedium von Linux Mint 20.3 Edge von der Heft-DVD startet.

Upgrades von 20.x: Wenn Sie bereits ein Linux Mint 20.x installiert haben, brauchen Sie natürlich kein Installationsmedium. Für die Aktualisierung auf Version 20.3 gibt es ein Onlineupgrade. Das genaue Prozedere war bei Redaktionsschluss Anfang Januar noch offen.

Nach bisherigen Erfahrungen gibt es entweder die komfortable Option über „Aktualisierungsverwaltung" oder den manuellen Weg über ein nachinstalliertes Tool:

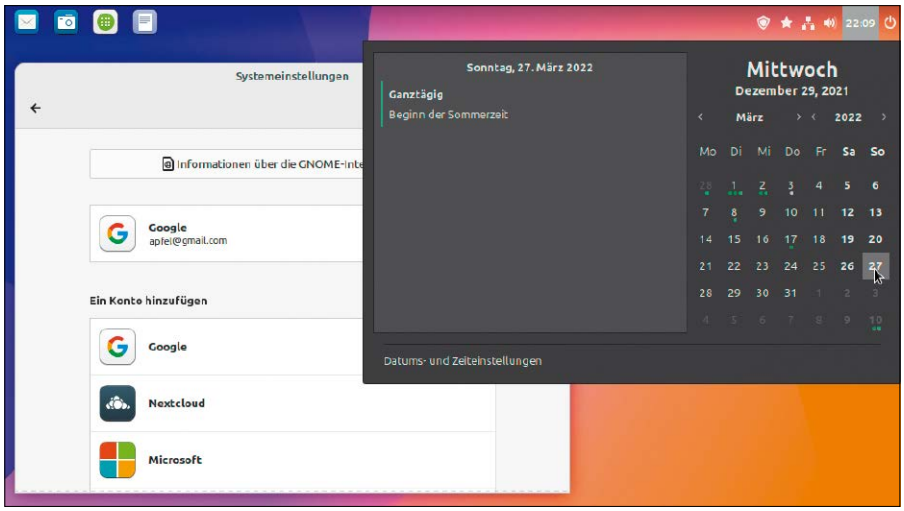
```
sudo apt install mintupgrade
mintupgrade download
mintupgrade upgrade
```

Welchen Weg das Mint-Team im aktuellen Fall vorsieht, erfahren Sie im Zweifel auf *https://blog.linuxmint.com/*.

Die drei Mint-Editionen

Wie immer lässt es sich Linux Mint nicht nehmen, drei Desktops anzubieten. Dabei ist aber die Hauptedition mit Cinnamon ohne Zweifel das Aushängeschild von Linux Mint, dessen wichtigste Eigenentwicklung und das Hauptmotiv der Nutzer, sich für Linux Mint zu entscheiden. Auch die Ansprüche an die Hardware unterscheiden sich mittlerweile so gering, dass die beiden zusätzlichen Editionen neben Cinnamon fast überflüssig erscheinen. Mit vier GB RAM und einer Dualcore-CPU lässt sich jede Mint-Edition flüssig bedienen. Der RAM-Bedarf aller drei Systeme liegt nach der Anmeldung bei etwa 600 MB.

Linux Mint 20.3 XFCE bleibt dennoch das sparsamste Mint, weil die Anforderungen dieses Desktops auch an CPU und Grafikchip aufgrund sparsamer Grafikeffekte



Synchronisierte externe Kalender: Das kleine Leistenapplet („Kalender"), das bei vielen Nutzern nur als Zeitansage dient, kann unter anderem den Google-Kalender integrieren.

sehr gering sind. Der konservative XFCE-Desktop ist unter Linux Mint durch frische Iconsets deutlich modernisiert.

Linux Mint 20.3 Mate hat im Mint-Umfeld zwischen Cinnamon und XFCE einen schweren Stand: Wer das möglichst sparsamste Linux Mint sucht, greift besser zu XFCE. Wer andererseits das attraktivste Linux Mint nutzen will, erhält mit Cinnamon den besten Mint-Desktop.

Linux Mint 20.3 Cinnamon ist die mit Abstand dominierende Hauptvariante. Die Cinnamon-Oberfläche orientiert sich an vielen Windows-Standards und ist eine der wenigen Linux-Desktops, die im Benutzeralltag eine vollständig grafische Bedienung erlauben. Linux Mint fokussiert auf Umsteiger und Einsteiger, hat aber auch Linux-Freaks auf seiner Seite. Die nachfolgende Vorstellung bezieht sich in erster Linie auf die Cinnamon-Hauptedition.



Namenskonflikt beim Kopieren: Der Dateimanager Nemo erspart die manuelle Eingabe eines anderen Namens durch die neue Option „Verdoppeln".

Version 20.3: Was ist neu?

Version 20.3 erneuert Kernel- und Softwareversionen. Wer jedoch den Vorgänger 20.2 („Uma") konsequent aktualisiert hat, wird dort ebenfalls schon Kernel 5.4.0, Firefox 95 oder Thunderbird 78.14 vorfinden. Und wer Wert auf ein aktuelles Libre Office legt, wird dieses eher über das externe PPA beziehen, als sich mit der hier vorinstallierten und nicht mehr taufrischen Version 6.4.7.2 zu begnügen. In der Softwareaktualität lag der Fokus des konservativen Ubuntu-Derivats aber noch nie. Ziel von Mint ist ein einsteiger- und umsteigerfreundlicher Desktop mit durchgehend grafischer Bedienung und umfassender Softwareausstattung. So wurde auch dieses Mal vor allem an Zubehörprogrammen und an den Cinnamon-Komponenten gefeilt. Alle nachfolgenden Neuerungen gelten für die Cinnamon-Hauptedition. Nicht alle, aber fast alle Verbesserungen bei den X-Apps übernehmen aber auch die Mate- und XFCE-Edition. Auch die geänderte Themenoptik für Fenster und Titel ist zum Großteil auch in die anderen Editionen eingeflossen.

Cinnamon: Der Mint-Desktop ist bei Version 5.2.5 angekommen. Die meisten Neuerungen im Vergleich zur Vorgängerversion 5.0.7 zeigt die Oberfläche aber nur unterm Mikroskop.

Das Cinnamon-Hauptmenü ist das standardmäßige Menüapplet für die Cinnamon-Systemleiste und zeigt jetzt Icons für sämtliche angebotenen Programme. Eine neue Einstellungsoption in dem seit jeher detailliert konfigurierbaren Hauptmenü bietet unter „Verhalten" einen Verzögerungsmechanismus bei der Mausbewegung über das Menüsymbol.

Die „Gruppierte Fensterliste" (Grouped-Window-List) ist ein weiteres komplexes Applet der Systemleiste. Es entspricht als Kombination von Taskverwaltung und Favoritenstarter ziemlich exakt der Windows-Taskleiste inklusive der dauerhaften Pin-Option (als Favorit), der Gruppierung von Tasks (etwa mehrerer Browsertabs oder Dateimanager-Fenster) und der Vorschaubilder für geöffnete Fenster. Der detaillierte (und reichlich komplizierte) Einstellungsdialog dieses Applets ist unverändert, aber die Darstellung für gruppierte Anwendungen mit geöffneten Unterfenstern wurde verbessert.

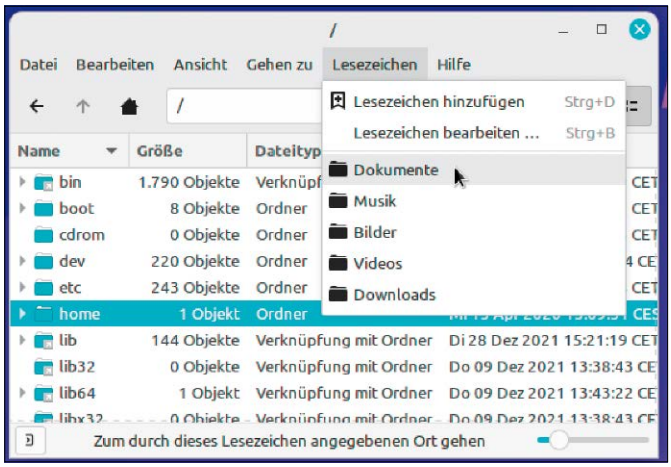
Der Cinnamon-Kalender dient in der Systemleiste oft nur zur Anzeige der Uhrzeit, leistet aber wesentlich mehr als etwa nur eine schnelle Monatsübersicht. Das Applet ist jetzt in der Lage, mehrere Onlinekalender zu synchronisieren und mit verschiedenen Farbmarkierungen anzuzeigen. Besonders einfach ist die Integration des Google-Kalenders, indem man unter „Systemeinstellungen → Internetkonten" das Google-Konto am System anmeldet. Zur Anmeldung an Evolution-Server mit Kalenderdaten kann Thunderbird mit einem Add-on aushelfen.

Weiteres Applet-Tuning: Der optionale „Arbeitsflächenwechsler" **(Workspace Switcher)** erhält eine zusätzliche Einstellungsoption, um das Scrollen mit dem Mausrad durch die virtuellen Desktops komplett abzuschalten. Dies kommt Nutzern entgegen, die ausschließlich mit gezieltem Mausklick zum gewünschten Desktop wechseln wollen. Beim Standardapplet „Meldungen" **(Notifications)** gibt es die neue, aber definitiv marginale Option, die Anzahl ausstehender Systemmeldungen zu unterdrücken. Ebenfalls marginal ist das Tuning für das optionale Leistenapplet „Fensterliste" **(Window List):** Dessen Einstellungsdialog zeigt nun die Option, die Fensternamen auszublenden. Dies führt dann zu einer Nur-Symbol-Darstellung ähnlich der „Gruppierten Fensterliste", die den meisten Nutzern sowieso als alleinige Taskverwaltung ausreichen wird.

Nvidia-Support: Programmverknüpfungen auf Linux-Desktops sind bekanntlich Text-

MEHR INFOS ZU LINUX MINT

Projektseite (mit Downloadadressen)
https://linuxmint.com/
Offizieller Blog mit News
http://blog.linuxmint.com/
Softwaredatenbank für Linux Mint
https://community.linuxmint.com/software/browse
Hardwaredatenbank für Linux Mint
https://community.linuxmint.com/hardware/search
Forum für technische Fragen (dt.)
www.linuxmintusers.de
Forum für technische Fragen (engl.)
https://forums.linuxmint.com



Themenfarbe und Akzentfarbe: Beachten Sie die dezente Akzentfarbe im Menü des Dateimanagers im Vergleich zur Themenfarbe (markiertes Objekt und „Schließen"-Button).

dateien mit der Endung „.desktop" und einer verbindlichen Anweisungsstruktur. In der Nachfolge von Gnome erweitert nun auch Cinnamon diese Starter um die Option „PrefersNonDefaultGPU". Diese dient auf Notebooks mit hybriden Intel-Nvidia-Grafiklösungen dazu, für das jeweilige Programm die leistungsstärkere Nvidia-Grafik zu verwenden.

Dateimanager Nemo: Der Dateimanager von Cinnamon zeigt jetzt beim Kopieren und Einfügen gleichnamiger Dateien im Dialog „Dateikonflikt" die zusätzliche Option „Verdoppeln". Schon vorher gab es das Angebot, einen anderen Namen zu wählen, was aber stets einen manuellen Eingriff des Benutzers forderte. Beim „Verdoppeln" erledigt der Dateimanager die Namensänderung automatisch, indem er den Zusatz „(Kopie)" anfügt.

Als weitere Kleinigkeit bei Nemo bleibt der Inhalt der Zwischenablage erhalten, wenn Nemo beendet wird. Vorher kopierte Dateinamen können folglich als Text in Terminals oder Scripts eingefügt werden. Kaum alltagsrelevant sind zusätzliche Beschreibungstags für Mediendaten „m4a" und „mp4" sowie die Möglichkeit, für Nemo-Kontexterweiterungen (nemo-actions) Pfadangaben im „UriScheme"-Format zu verwenden (*file:///...*).

Fensteranimationen: Die Effekte wurden überarbeitet und vereinfacht. Dies führt zu einem deutlich reduziertem Dialog unter „Systemeinstellungen → Effekte", der jetzt auf das frühere Register „Anpassen" komplett verzichtet. Pauschale Anpassungen sind auf der verbleibenden Registerkarte immer noch möglich, ohne aber noch so kleinteilige Details wie Effektdauer in Millisekunden und Effektkurven anzubieten.

Fensterthemen und Farben

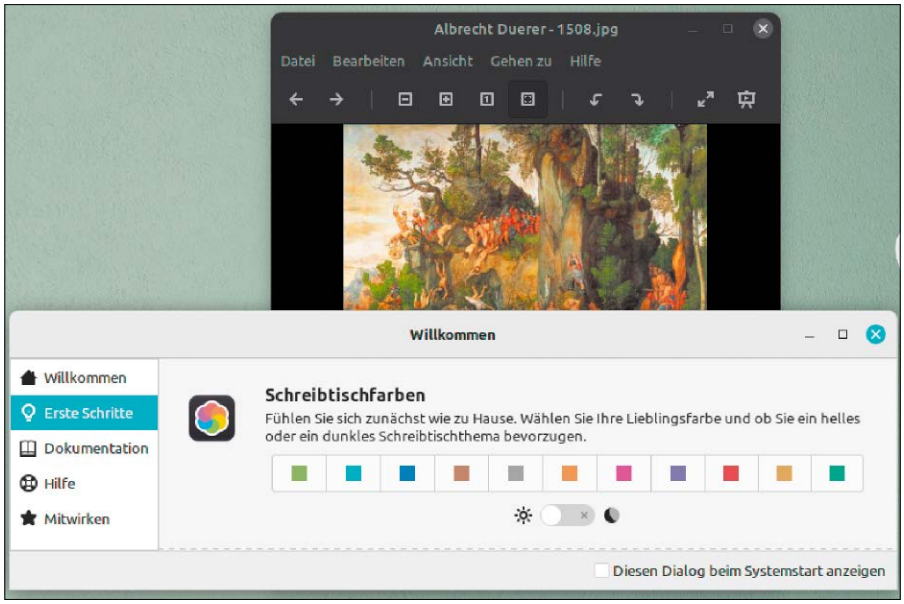
Linux Mint 20.3 bringt für alle drei Desktops eine überarbeitete Fensteroptik. Die Titelleiste wird etwas höher und somit die wichtigen Fenstercontrols (Schließen, Minimieren) größer und griffiger. Wie Windows 11 zeigen alle Programmfenster gerundete Ecken, hier allerdings nur oben beim Fenstertitel. Das Resultat insgesamt ist nicht spektakulär, aber optisch wie funktional überzeugend. Als unscheinbarer, aber feinsinniger Optikschliff kommen noch Akzentfarben für Anwendungsmenüs hinzu, die den aktiven Menüpunkt mit dezenter Schattierung hervorheben, anstatt wie bisher die relativ aufdringliche Themenfarbe („Mint-Y-Aqua" et cetera) zu verwenden. Allerdings versteht Linux Mint derartige Themenänderungen immer als offenes Angebot. Sobald der Nutzer unter „Systemeinstellungen → Themen" von den Mint-Y-Standards abweicht, erscheint wieder die gewohnte kleinere Titelleiste ohne gerundete Ecken. Dafür genügt es schon, beim Element „Steuerung" auf ein älteres Mint-X-Thema zu wechseln. Natürlich gibt es Dutzende weitere und ältere Mint-Themen online („Hinzufügen/Entfernen"), die den neuen Themenstil der Version 20.3 ebenfalls aufheben.

Und mehr noch: Das Mint-Team selbst verweist auf das extra zurückgelegte Paket „Mint-Y-Legacy" für konservative Nutzer, das nach

```
sudo apt install mint-themes-legacy
```

wieder komplett die Optik der Vorgängerversionen zurückholt. Diese „Legacy"-Komponenten erscheinen dann wieder unter „Systemeinstellungen → Themen".

Dunkler Modus für etliche Apps: Schon seit einigen Mint-Versionen gibt es einen systemweiten dunklen Modus für alle Programmfenster – am einfachsten einzustellen im Willkommen-Dialog, differenzierter unter „Systemeinstellungen → Themen". Wem es mit dieser globalen Einstellung zu finster zugeht, kann jetzt systemweit beim hellen Modus bleiben, aber für bestimmtes Zubehör die dunkle Darstellung wählen. Für die Medienwiedergabe **Celluloid** gilt dies schon länger. **Hypnotix,** eine Mint-Eigenentwicklung und Sammlung von nahezu 3000 freien IP-TV-Kanälen, wurde überarbeitet und zeigt im Dialog „Einstellungen"



Dunkle Apps trotz hellem Systemthema: Immer mehr Zubehörprogramme (hier Bildbetrachter Xviewer) bieten einen Dunkelmodus unabhängig vom globalen Thema.

die Option „Dunklen Modus bevorzugen“. Der Bildbetrachter **Xviewer** ist jetzt standardmäßig dunkel, unabhängig vom Systemthema, lässt sich aber über „Bearbeiten → Einstellungen → Module“ weiterhin hell schalten. Analoges gilt für die Bildverwaltung **Pix** mit ihrer zusätzlichen Option „Bearbeiten → Einstellungen → Allgemein“.

Weiteres Zubehörtuning

Hypnotix, der umfangreiche, aber relativ chaotische Akkumulator für TV-Sender, erhält jetzt eine Suchfunktion. Dasselbe gilt für die überarbeiteten **Sticky Notes.** Diese Desktopnotizen zeigen zudem ein neues Control, um den markierten Text umstandslos zu formatieren. Die aufklappende Drop-down-Liste bietet verschiedene Textgrößen sowie Auszeichnungen wie „Fett“ oder „Kursiv“.

Der (PDF-)Dokumentenbetrachter **Xreader** und der Texteditor **Xed** bringen platzsparende Optionen, um die Menüleiste auszublenden. Zum bedarfsweisen Einblenden dient die dafür typische Alt-Taste. Der Xreader verzichtet zudem auf seine Funktionsleiste, sobald mit F11 (oder „Ansicht → Vollbild“) die Vollbildanzeige aktiviert wird. Der Texteditor wiederum nutzt den neuen Hotkey Strg-Tab, um schnell zwischen mehreren Texten in Tabs zu wechseln.

Das verdienstvolle Tool **Webapps** ist eine Mint-Eigenentwicklung und hat die Aufgabe, Internetsites wie lokale installierte Desktopprogramme darzustellen – ohne Adressleiste und Navigationsbuttons, dafür aber integriert ins Hauptmenü oder in die Systemleiste. Das Zubehör zeigt in seinem Verwaltungsdialog nun den jeweils genutzten Browser an. Das ist praktisch, wenn mehrere Browser im System und für die Webapps genutzt werden.

Thingy („Bibliothek“) ist eine ganz neue Eigenentwicklung. Allerdings ist das Zubehör nicht viel mehr als ein kleines Verwaltungstool für zuletzt genutzte Dokumente. Auch die Reichweite des neuen Tools ist nicht beeindruckend, da es bislang nur Office-Dokumente und PDFs erfasst – übrigens ausschließlich lokal geöffnete (nicht übers Netz). Nach dem Start des Tools wählt man zunächst den Dokumenttyp, also etwa „Dokumentenbetrachter“, wenn man jüngst genutzte PDFs suchen will. Diese zeigt Thingy dann im Hauptfenster an und startet bei Doppelklick den zugehörigen Viewer/Editor (Xreader, Writer, Calc et cetera).

Kritisches Fazit

Sie werden zustimmen: Auch in Version 20.3 darf man dem Mint-Team um Clem Lefebvre Liebe zum Detail und klare Fokussierung auf Desktopnutzer attestieren. Was dieses Team dann im Einzelnen für verbesserungswürdig und ausbaufähig erachtet, führt aber – objektiv betrachtet – allzu oft in marginale Nebensächlichkeiten. Der Ausbau von Desktopnotizen ist ein Anachronismus, X-Apps wie Xed (Editor) oder Xreader (PDF-Viewer) tun schon längst, was sie tun sollen oder tun müssen. Ressourceninvestitionen in Eigenentwicklungen wie Thingy, Hypnotix oder Warpinator bleiben fragwürdig: das neue Thingy ist nicht mehr als eine „Zuletzt verwendet“-Liste für Office und PDF, Hypnotix nur eine aufgehübschte Liste der „Free IPTV“-Liste (*https://github.com/Free-IPTV/Countries*) und der technisch wie bedientechnisch tadellose Warpinator hat schlicht das Problem, dass der Datenaustausch im lokalen Netz nicht auf Linux Mint gewartet hat.

Das Highlight der neuesten Mint-Version ist tatsächlich nicht im Funktionalen zu suchen, sondern bei der Optik. Vergrößerte und abgerundete Titelleisten und unaufdringliche Akzentfarben in Programmmenüs machen die Oberfläche eleganter und präziser.

Anders als etwa einem Ubuntu oder Windows 11 fehlt Linux Mint hier aber der diktatorische Mut, diese Optik einfach verbindlich zu setzen. Der komplizierte „Themen“-Dialog ist zwar basisdemokratisch, aber in seiner Komplexität eine Herausforderung – erst recht, wenn man sich zusätzlich einige Community-Themen oder die „Legacy“-Themen des Vorgängers nachinstalliert hat.



Desktopnotizen: Die Sticky Notes erhalten ein zusätzliches Menü zur schnellen Formatierung.

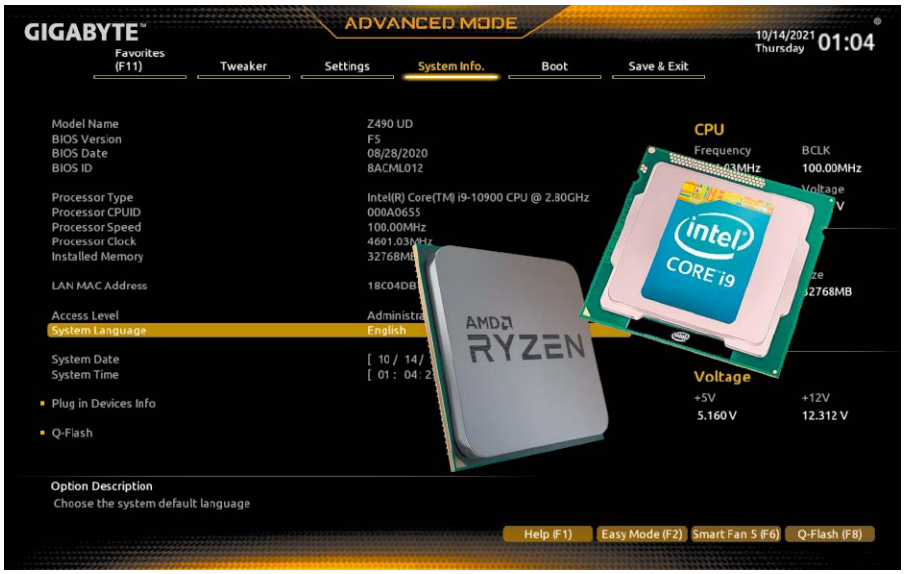
Bei diversen, komplexeren Desktopkomponenten steht es ähnlich: Das Mint-Konzept, alles anzubieten, aber möglichst nichts vorzuschreiben, führt zu Konfigurationsdialogen, die sowohl für den Entwickler wie für den Endbenutzer anstrengend werden. Für Leistenapplets wie Hauptmenü oder „Gruppierte Fensterliste“ wäre dringend Simplifizierung angesagt. Immerhin bei den Desktopeffekten hat Version 20.3 einen ersten Schritt in die richtige Richtung getan. ■



Thingy: Das neue Zubehör („Bibliothek“) versammelt die zuletzt genutzten PDF- und Office-Dokumente – hier waren es offenbar einige LinuxWelten.

Hardware für Linux und Windows

Die folgenden beiden Artikel bieten Informationen für die Kaufentscheidung und Tipps für den problemlosen Hardwarebetrieb unter Linux. Zum Einstieg geht es um Windows (11). Warum? Weil Hardware vor allem für Windows konstruiert wird.



VON THORSTEN EGGELING

Am 5. Oktober 2021 hat Microsoft Windows 11 veröffentlicht. Für Linux-Nutzer oder zukünftige Umsteiger lohnt sich ein Blick auf die gegenüber Windows 10 geänderten Ansprüche an die Hardware. PCs und Notebooks mit Baujahr 2017 und älter erfüllen die Hardwarevoraussetzungen für Windows 11 in der Regel nicht und müssen daher offiziell bei Windows 10 bleiben, das immerhin noch bis zum 14. Oktober 2025 mit Updates versorgt wird. Danach muss man die Geräte ausmustern oder auf Linux umsteigen – was natürlich auch schon jetzt möglich ist.

Microsoft argumentiert, dass nur die jetzt angehobenen Hardwarevoraussetzungen Stabilität, Sicherheit und Leistung des Systems gewährleisten. Auf welche Bereiche sich das auswirkt, erklärt das Unternehmen jedoch nicht ausführlich. Es wird bisher auch nicht technisch begründet, warum ein bestimmter Prozessor unterstützt wird, ein etwas älteres, offenbar baugleiches und nur niedriger getaktetes Modell jedoch nicht.

In diesem Beitrag beleuchten wir, was neuere Hardware für Windows 11 zu bieten hat und was das für Linux-Nutzer bedeutet.

Die CPU-Unterstützung bei Linux

Linux stellt an die Hardware keine besonderen Ansprüche. Das System lässt sich auch auf Geräten installieren, die zehn Jahre und älter sind (siehe ab Seite 176). Auf aktuellen PCs und Notebooks macht Linux aber mehr Spaß. Multicore-CPUs von AMD oder Intel, SSDs und ausreichend RAM ermöglichen schnelle Startzeiten und flüssiges Arbeiten.

Davon profitieren auch Standardanwendungen wie Office-Pakete und Browser. Wer den Computer für Spiele oder Videoschnitt verwendet oder Virtualisierungssoftware einsetzt, benötigt dafür einen aktuelleren und leistungsstarken Rechner. Intel-CPUs der Core-i-Serie (Core i3, i5, i7, i9 ab etwa 2010) oder vergleichbare AMD-CPUs (AMD Ryzen 3, 5, 7, 9) bieten auf jeden Fall ausreichend Leistung. Die Softwareentwicklung kann bei Linux oft nicht mit den Neuerungen bei der Hardware mithalten. Besonders neue Geräte liefern nicht immer die optimale Leistung, weil die erforderlichen Anpassungen noch nicht in die Kernel- und Treiberentwicklung eingeflossen sind. Eine Linux-Installation ist trotzdem möglich und meist ist die reduzierte Leistung nur messbar und kaum spürbar. Man kann aber generell davon ausgehen, dass ein neuerer Kernel beziehungsweise das nächste Update der Linux-Distribution die Leistung verbessern.

Die CPU-Unterstützung bei Windows

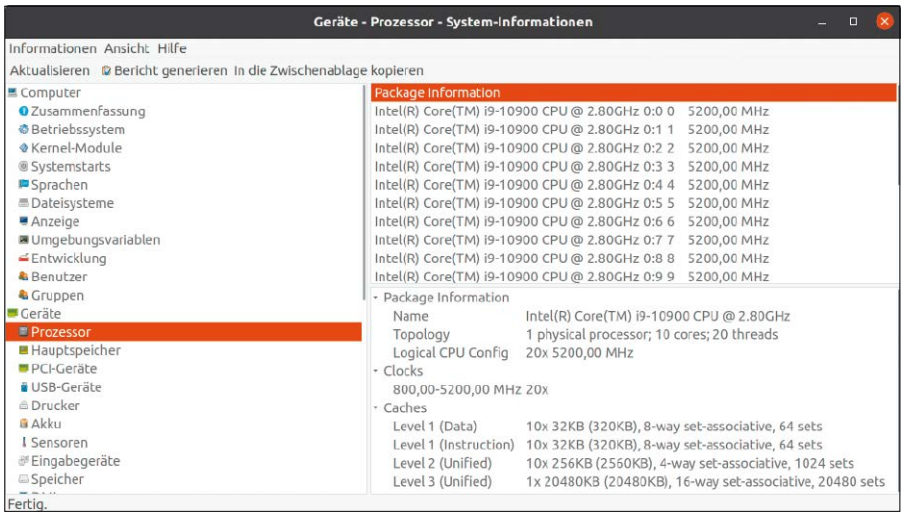
Bis einschließlich Version 10 verhält sich Windows nicht grundsätzlich anders als Linux. Es lässt sich auch auf Geräten mit relativ alten CPUs installieren, 32-Bit-Prozessoren werden ebenfalls unterstützt. Aber auch hier gilt: Auf Geräten mit lahmer CPU, wenig RAM und langsamer Festplatte läuft Windows nicht wirklich flüssig.

Windows 11 basiert auf Windows 10 und läuft daher zufriedenstellend auf der gleichen Hardware. Das Setupprogramm verweigert bei einer zu alten CPU jedoch die Installation. Die Beschränkung auf neuere Prozessoren dürfte für viele Windows-Nutzer ein Problem darstellen. Noch 2020 wurden Geräte mit CPUs verkauft, die Windows

11 nicht mehr akzeptiert.
Nach Aussage von Microsoft dient die CPU-Beschränkung der Systemsicherheit. Aktuelle CPUs kennen Funktionen, über die sich beispielsweise Speicherbereiche vor unberechtigtem Zugriff schützen lassen. Microsoft nennt das Virtualization Based Security (VBS). Die Hypervisor-Enforced Code-integrität (HVCI) nutzt VBS, um Kernel-Modustreiber und Binärdateien vor dem Start zu prüfen, und lehnt unsignierte Treiber ab. Ältere Prozessoren beherrschen diese Techniken meist auch, allerdings laut Microsoft nur mit ungenügender Leistung. Damit das System nicht zu stark ausgebremst wird, hat Microsoft daher diese CPUs auf die schwarze Liste gesetzt. Eine Übersicht mit den unterstützten CPUs finden Sie über *www.pcwelt.de/Nyg_D5* (Intel) und w*ww.pcwelt.de/OhqwZY* (AMD).
Hinweis: Upgrade oder Neuinstallation auf Windows 11 sind auf eigene Gefahr auch auf nicht unterstützter Hardware möglich. Informationen dazu finden Sie unter *www.pcwelt.de/2616501* (Neuinstallation) und *www.pcwelt.de/2616877* (Upgrade).

TPM und Secure Boot

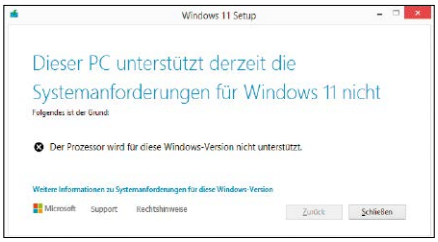
Das Trusted Platform Module (TPM) stellt die Systemintegrität sicher und dient zur Erstellung sicherer, hardwarebasierter Kryptografieschlüssel, etwa zur Laufwerksverschlüsselung. Bei vielen vor 2015 gebauten Computern ist TPM noch nicht vorhanden. Das spielt aber keine Rolle, weil dann auch die CPU für Windows 11 zu alt sein dürfte.
TPM 2.0 ist in der Regel auf Hauptplatinen mit Intel-Chipsätzen ab Serie 100 und Intel X299 zu finden. Bei AMD ab Serie 300 sowie AMD X399 und TRX40. Im Firmwaresetup ist TPM oft deaktiviert (siehe ab Seite 174). Secure Boot muss für die Installation von Windows 11 ebenfalls aktiviert sein. Alle verbreiteten Linux-Distributionen können mit Secure Boot umgehen (siehe ab Seite 174). TPM spielt bei Linux standardmäßig keine Rolle, wird vom Kernel aber unterstützt. Man kann die Technik beispielsweise für die Laufwerksverschlüsselung oder SSH-Schlüssel verwenden. Die Linux-Entwickler sind beim Einsatz von TPM zurückhaltend, weil es dem Open-Source-Gedanken widerspricht. Schließlich weiß niemand genau, wie TPM intern funktioniert und ob die Hersteller keine Hintertür für Geheimdienste eingebaut haben.



Mehr als genug Leistung: Intel-i9-CPUs beispielsweise der zehnten Generation bieten zehn Cores und 20 Threads oder mehr. Das ist auch für anspruchsvolle Anwendungen ausreichend.

Ist Linux weniger sicher?

Microsoft legt bei Windows 11 mit VBS, HVCI, TPM und Secure Boot viel Wert auf Sicherheit. Das ist verständlich, weil das meistverbreitete Betriebssystem beliebtestes Ziel von Angriffen ist. Da die Funktionen auf die Unterstützung durch die Hardware angewiesen sind, bleiben ältere Geräte außen vor. Nutzer von Windows 10 müssen sich jetzt natürlich fragen, ob ihr System vergleichsweise unsicher ist.
Linux ist alleine schon aufgrund der geringen Verbreitung auf Desktopsystemen weniger bedroht. Infektionen mit Viren und Trojanern sind jedoch ebenfalls möglich. Davor schützen aber mehrere Mechanismen: Heruntergeladene Dateien oder Anhänge von E-Mails sind standardmäßig nicht ausführbar. Selbst ein versehentlicher Klick darauf bewirkt gar nichts. Software und Kernel sowie Treiber stammen aus besonders geschützten Repositorien,



Zu alt für Windows 11: Selbst bei relativ schnellen Prozessoren, die nur wenige Jahre alt sind, verweigert Windows 11 die Installation. Die Beschränkung lässt sich jedoch umgehen.

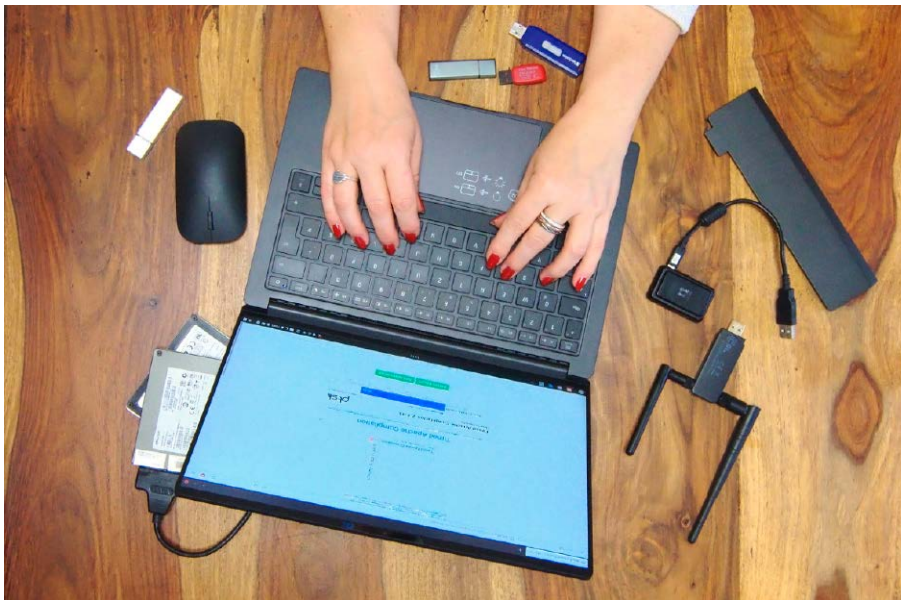
Schadsoftware kann darüber nicht auf den Rechner gelangen. Zusätzliche Treiber oder Software erstellen erfahrene Anwender selbst aus dem Quellcode. Theoretisch könnte Schadsoftware enthalten sein, was aber durch die Community schnell entdeckt werden würde. Das Gleiche gilt für Software aus alternativen Quellen, etwa *https://launchpad.net*. ■

EMPFOHLENE HARDWAREVORAUSSETZUNGEN

	Ubuntu 20.04	MX Linux 19.4 (XFCE)	Windows 10	Windows 11
CPU-Taktfrequenz	2 GHz	1,5 GHz	1 GHz	1 GHz, zwei Kerne
CPU-Architektur	64 Bit	32/64 Bit	32/64 Bit	64 Bit
Platz auf der Festplatte	25 GB	20 GB	16/32 GB	64 GB
Hauptspeicher (RAM)	4 GB	2 GB	1–2 GB	4 GB
Bildschirmauflösung	1024 × 768	1024 × 768	800 × 600	1280 × 720 (720p)
Grafik	3D-Beschleunigung und 256 MB RAM	3D-Beschleunigung	ab DirectX 9, WDDM 1.0 Treiber	ab DirectX 12, WDDM 2.0 Treiber
Sonstiges	–	–	–	Uefi, Secure Boot, TPM, Internet bei der Home-Edition

Notebooks für Linux

Hardware unterliegt stetem Wandel und Hersteller folgen bei der Treiberentwicklung meist den Vorgaben für Microsoft Windows. Der folgende Leitfaden zeigt, worauf Linux-Anwender schon beim Erwerb eines Notebooks achten sollten.

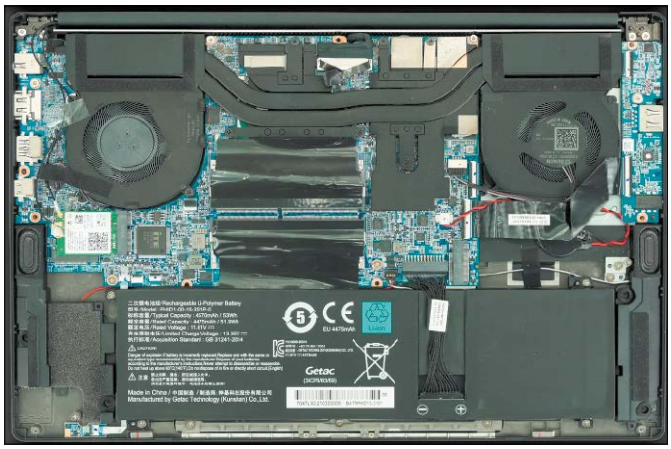


VON DAVID WOLSKI

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
```

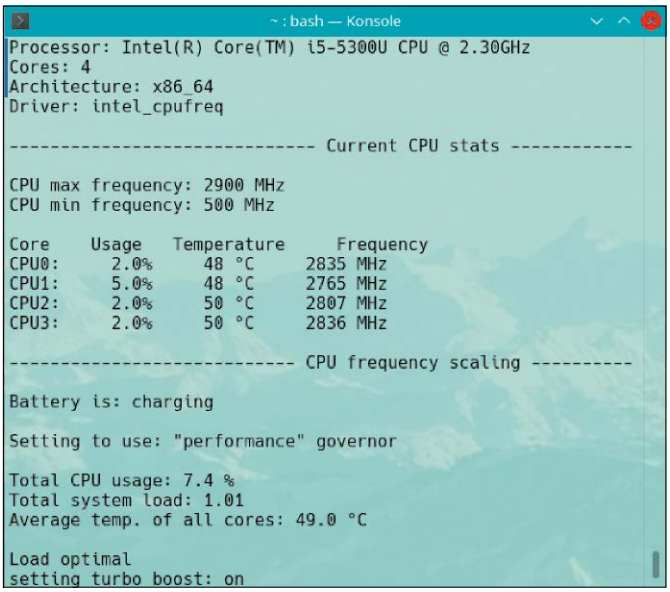
installieren das Tool. Allerdings muss nun noch der Systemd-Dienst mit dem separaten Befehl

```
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

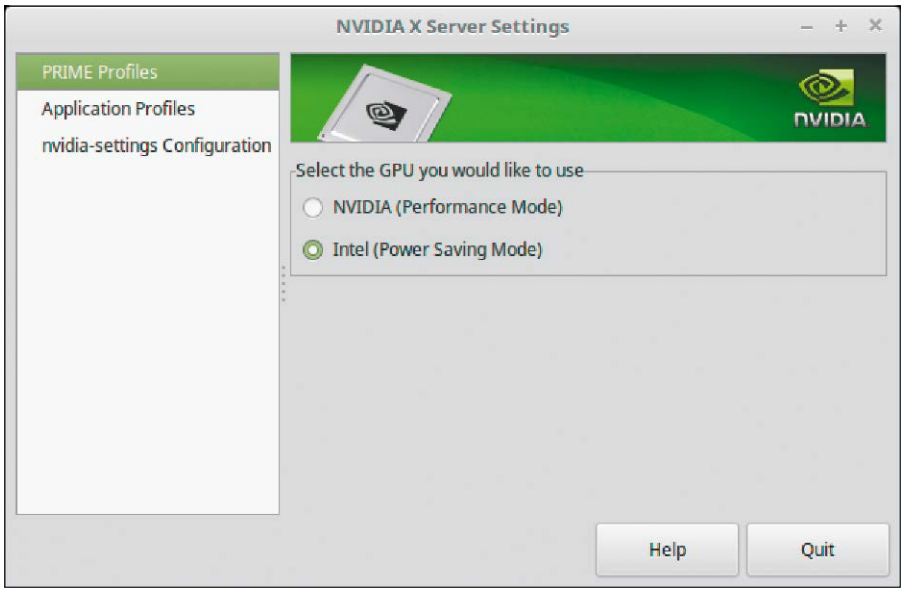
GEBRAUCHTMARKT: LEASINGRÜCKLÄUFER UND ALTGERÄTE

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.



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: 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.

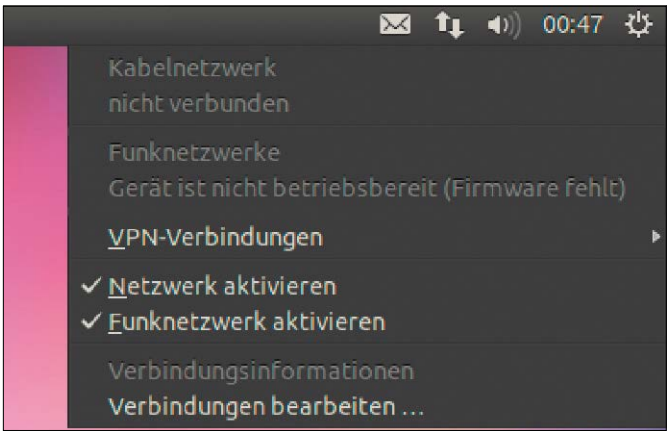
Leider machen es einige wenige Ausreißer nötig, bei der Suche nach geeigneten Notebooks auf die genaue Typenbezeichnung des WLAN-Chips achten und dann im Inter-



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 [702]).

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
```

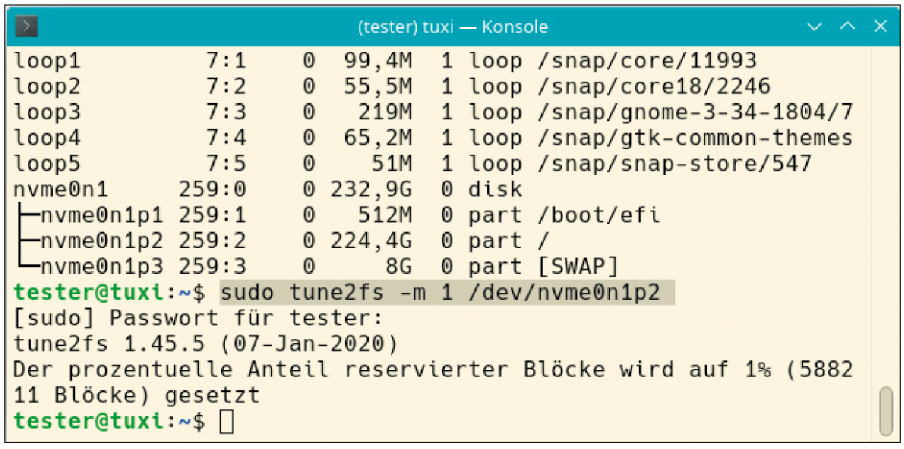
reduziert die Anzahl der reservierten Blöcke auf der Partition „/dev/nvme0n1p2“ auf ein Prozent.

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. ■

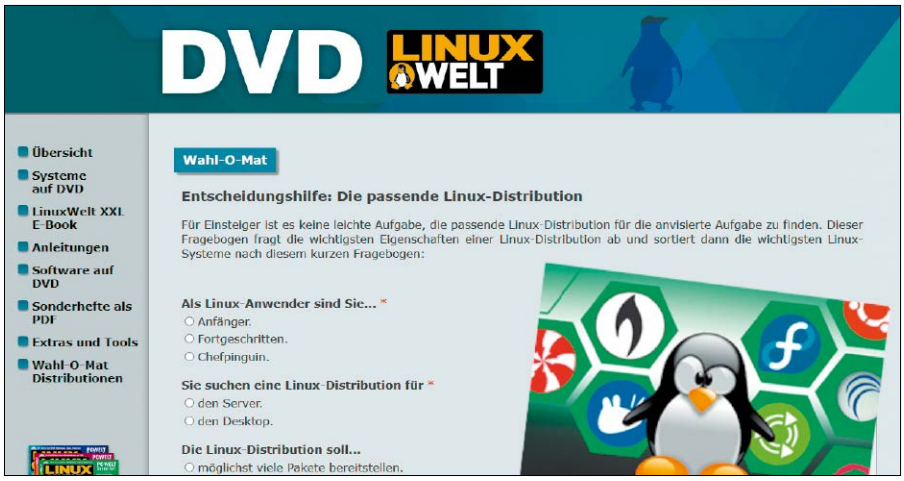


Wertvollen Platz sparen: Bei Ext4 werden fünf Prozent der Blöcke für root für den Notfall reserviert. Das kann das Tool tune2fs gefahrlos auf ein Prozent reduzieren.

Linux als Dauerläufer

In der Regel müssen Linux-Nutzer sich nur alle drei oder fünf Jahre um ein Upgrade der Distribution kümmern. Wer möchte, kann aber zwischenzeitlich trotzdem neuere Software installieren.

VON THORSTEN EGGELING



Distributionsauswahl: Den Wahl-O-Mat rufen Sie über die HTML-Oberfläche der Heft-DVD auf. Beantworten Sie die Fragen und lesen Sie die Informationen, die zu den Kriterien passen.

Die Auswahl einer geeigneten Linux-Distribution hängt vom Einsatzzweck ab. Auf einem produktiv eingesetzten Arbeitsrechner oder Server wird man ein stabiles und bewährtes System bevorzugen. Das Upgrade auf die nächste Version werden die meisten Nutzer dann vermeiden oder möglichst lange hinausschieben. Schließlich bedeutet jedes Upgrade eine längere Arbeitsunterbrechung – und möglicherweise funktioniert danach nicht mehr alles wie vorher.

Auf der anderen Seite des Spektrums stehen Nutzer, die meist technisch interessiert sind und die neuesten Versionen von Betriebssystem und Anwendungen bevorzugen. Für diesen Personenkreis gibt es Distributionen mit kürzerer Laufzeit und einer höheren Updatefrequenz. Wer es noch aktueller möchte, greift zu einem Rolling Release und hält damit das System fortlaufend auf dem aktuellen Stand (siehe Artikel ab Seite 68).

Der Fokus der nachfolgenden Artikel liegt jedoch auf der möglichst langen Nutzung einer Linux-Installation. Das gelingt mit geringem Aufwand, wenn man ein paar Regeln beachtet.

Linux-Distributionen für jeden Zweck

Die Standardeditionen von Ubuntu und Linux Mint bieten fünf Jahre Laufzeit und sind mit LTS gekennzeichnet (Long Term Support). Eine neue LTS-Version erscheint alle zwei Jahre (Ubuntu 18.04, 20.04, 22.04). Man kann dann ein Upgrade durchführen oder damit noch drei Jahre warten. Bei Bedarf lässt sich der Supportzeitraum für Ubuntu kostenpflichtig sogar auf bis zu zehn Jahre verlängern (*https://ubuntu.com/advantage*).

Wer ein System mit neueren Tools und Anwendungen bevorzugt, erhält es bei Ubuntu zweimal im Jahr (20.10, 21,04, 21.10), die Versorgung mit Updates erfolgt neun Monate lang. MX Linux beispielsweise basiert auf Debian, von dem es etwa alle zwei Jahre eine neue Ausgabe gibt. Das MX-Linux-Team stellt jedoch einmal im Jahr ein Upgrade mit neuer Software bereit. Manjaro ist ein Rolling Release, das fortwährend aktualisiert wird.

Die Distributionsvielfalt verstellt ein wenig den Blick dafür, dass die Basis oft identisch ist. Meist liefert Ubuntu den Unterbau, das wiederum mit Debian verwandt ist. Fedora basiert auf Red Hat Linux und Manjaro auf Arch Linux. Nur Open Suse ist eine unabhängige Entwicklung, die eng mit den kommerziellen Produkten Suse Linux Enterprise Desktop und Suse Linux Enterprise Server verbunden ist.

Bei der Entscheidung für eine bestimmte Distribution spielen mehrere Aspekte eine Rolle:

- der Nutzer ist Anfänger, erfahrener Anwender oder Profi
- die Distribution soll sich für einen Server oder Desktop eignen
- es werden eine breite Softwareauswahl oder nur gut getestete Paket gewünscht
- die Software soll entweder möglichst aktuell oder eher stabil sein

Bei der Auswahl der passenden Distribution hilft Ihnen unser Wahl-O-Mat, der sich über die HTML-Oberfläche der LinuxWelt-DVD im Browser aufrufen lässt.

Distributionen für Desktop oder Server

Es gibt zwar spezielle Serverdistributionen, jedoch ist die Basis der Server- und Desktopeditionen weitestgehend identisch. Unterschiede gibt es meist bei der Installation und der Vorauswahl der Software. Eine Desktopumgebung ist bei Servern oft entbehrlich, dafür möchte man dort aber Webserver, Datenbanken und E-Mail-Server bereits bei der Installation einrichten.

Das Installationsmedium beispielsweise von Debian 10 (*https://www.debian.org*) trägt dem Rechnung. Über das Installationstool wird zuerst ein Grundsystem eingerichtet, danach können Sie die gewünschten Pakete installieren – bei Bedarf mit Desktopumgebung oder ohne.

Bei Ubuntu Server (*https://ubuntu.com/download/server*) werden nur ein Grundsystem und der Open-SSH-Server einge-

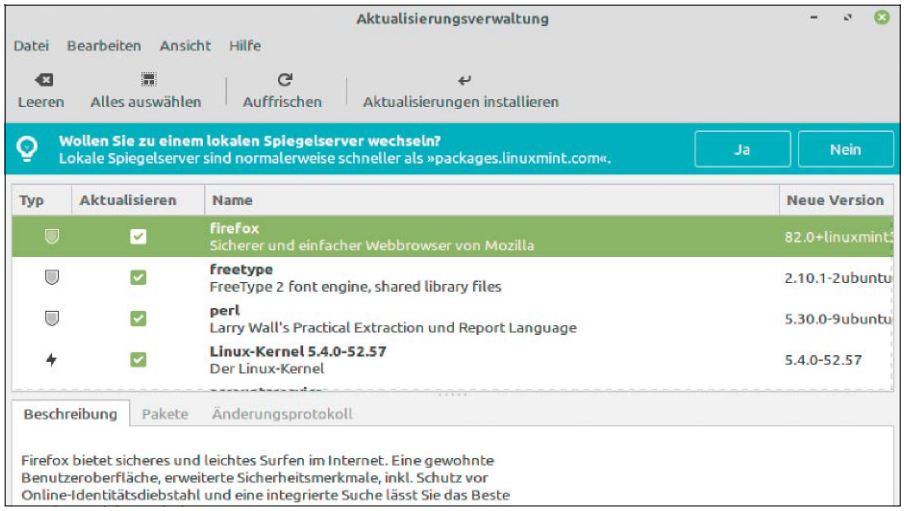
richtet. Bei der Installation können Sie zusätzliche Snap-Pakete für die Serverrolle installieren und alles andere dann später im Terminal über apt.

Bei der Installation von Ubuntu Desktop und vielen anderen Desktopdistributionen werden Sie nicht nach einer Softwareauswahl gefragt. Das Installationstool richtet automatisch alle Pakete ein, die für einen Arbeitsrechner sinnvoll sind. Sie können später aber alle Pakete installieren, die auch für Ubuntu Server verfügbar sind.

Die meisten Rechenzentren, bei denen Sie root-Server oder virtuelle Server mieten können, bieten Debian 10 oder Ubuntu 20.04 LTS für die Installation an. Manchmal befindet sich auch Cent-OS 7 im Angebot, das bis Mai 2029 mit Updates versorgt wird. Etwas teurere Webhosting-Pakete für Geschäftskunden enthalten beispielsweise Lizenzen für Red Hat Enterprise Linux oder Suse Linux Enterprise Server, die zehn Jahre Support erhalten.



Server oder Desktop: Für Debian gibt es nur ein Installationsmedium. Softwarepakete lassen sich aber vorab auswählen – bei einem Server lassen Sie die Desktoppakete einfach weg.



System aktualisieren: Die regelmäßigen Updates schließen vor allem Sicherheitslücken. Für wenige wichtige Anwendungen wie Firefox gibt es aber auch neue Versionen.

Updates und Upgrades

Solange ein System vom Distributor offiziell unterstützt wird, gibt es Sicherheitsupdates und oft auch Updates für einige ausgewählte Programme. Ubuntu/Mint-Nutzer erhalten beispielsweise neue Versionen von Firefox und Thunderbird. Kernel-Upgrades gibt es ebenfalls in unregelmäßigen Abständen (siehe Artikel ab Seite 82). Ist das Lebensende einer Distribution erreicht, liegen die Updates noch eine Zeit lang auf den Downloadservern. Es kommen aber wahrscheinlich keine neuen Updates hinzu, was ein Sicherheitsrisiko darstellen kann.

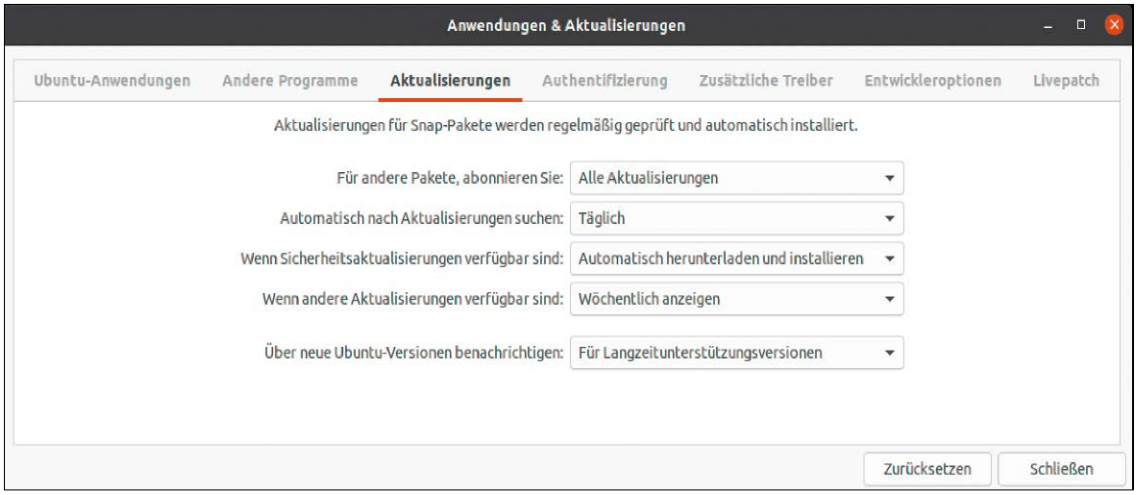
Ob man das System ohne Aktualisierungen einfach weiterbetreiben und sich das Upgrade sparen sollte, hängt vom Einsatzbereich ab. Wenn ein Linux-Server im Heimnetzwerk tatsächlich nur für den Datenaustausch etwa über Samba-Freigaben dient und aus dem Internet nicht erreichbar ist, kann das Upgrade auch ignoriert werden. Theoretisch besteht immer die Gefahr, dass ein Rechner über Sicherheitslücken im Kernel oder Fehler in der Serversoftware angegriffen wird. Die Gefahr geht dann aber eher von anderen Rechnern im Netzwerk aus, die von Schadsoftware betroffen sind. Für einige Geräte, beispielsweise ein älteres NAS, gibt es nach einiger Zeit auch keine Updates mehr. Privatanwender werden das Gerät trotzdem nicht gleich entsorgen wollen. Ganz anders sieht es bei Servern aus, die über das Internet erreichbar sind. Darauf muss immer ein aktuelles System inklusive aller verfügbaren Updates installiert sein. ■

NEUE SOFTWARE FÜR ÄLTERE SYSTEME

Software altert rasch: Fünf Jahre Laufzeit von LTS-Versionen sind für die Softwareentwicklung eine lange Zeitspanne. Allerdings benötigt nicht jeder unbedingt die neueste Version von Libre Office oder Gimp. Wenn doch, lassen sich aktuellere Programme über das Tool Ubuntu Software in einem Snap-Container installieren. Unter Linux Mint leisten die „Anwendungsverwaltung“ und Flatpak-Pakete Ähnliches. Aktuellere Software für Ubuntu und Linux Mint lässt sich aber oft auch über externe PPAs installieren (Personal Package Archive). Eine Internetsuche nach der gewünschten Software zusammen mit dem Schlüsselwort „ppa“ führt schnell zum passenden Angebot, das meist bei *https://launchpad.net* gehostet ist. Eine Beschreibung, wie sich das PPA einbinden und die Software installieren lässt, finden Sie auf der jeweiligen Webseite.

System und Software aktualisieren

Eine Linux-Installation kann man über einen langen Zeitraum nutzen. Regelmäßige Updates sind aus Sicherheitsgründen Pflicht und alle paar Jahre bringt man das System per Upgrade auf den neuesten Funktionsstand.



Grundeinstellungen: Ubuntu erledigt Download und Installation von Updates automatisch. Wer Kontrolle und manuelle Updates bevorzugt, kann die automatischen Updates auch abschalten.

VON THORSTEN EGGELING

Einer der größten Vorteile von Linux-Systemen ist die komfortable Updatefunktion. Die aktualisiert nämlich nicht nur das Betriebssystem, sondern auch die installierte Software. Das gilt für alle Programme, die über die Paketverwaltung beziehungsweise die konfigurierten Paketquellen eingerichtet wurden. Aktualisierungen lassen sich wahlweise automatisch beziehen oder auch manuell einleiten. Beides hat Vor- und Nachteile. Das gilt auch für Upgrades, also den Umstieg auf die nächste Version des Betriebssystems. Vor Updates und vor allem vor den umfangreichen Upgrades sollte man einige Sicherheitsmaßnahmen ergreifen, damit das System bei Fehlern nicht unbenutzbar wird. Wie immer vor größeren Änderungen, ist ein Backup anzuraten (siehe Punkt 6).

1. Automatische Updates für Ubuntu

Ubuntu 20.04 ist standardmäßig so eingerichtet, dass Sicherheitsupdates automatisch heruntergeladen und installiert werden. Vorsichtige Nutzer werden jedoch eher ein manuelles Update konfigurieren. Außerdem kann es wünschenswert sein, Updatedownloads zu reduzieren oder abzuschalten, beispielsweise wenn man viel mit dem Notebook unterwegs ist und deshalb keine schnelle Internetverbindung zur Verfügung steht.

Für die Konfiguration suchen Sie über die „Aktivitäten“ nach „Anwendungen“ und rufen „Anwendungen & Aktualisierungen“ auf. Dort gehen Sie auf die Registerkarte „Aktualisierungen“. Die erste Einstellung ist etwas seltsam mit „Für andere Pakete, abonnieren Sie:“ beschriftet. Standard ist hier „Alle Aktualisierungen“. Sie können die Updates aber auch auf „Sicherheits- und Empfehlungsaktualisierungen“ oder auf „Nur Sicherheitsaktualisierungen“ einschränken.

Ferner legen Sie hier fest, wie oft Ubuntu nach Aktualisierungen suchen soll. Stellen Sie „Niemals“ ein, wenn Sie den Download der Paketlisten und damit das automatische Update abschalten wollen. Hinter „Wenn Sicherheitsaktualisierungen verfügbar sind“ ist „Automatisch herunterladen und installieren“ eingestellt. Wählen Sie „Sofort anzeigen“, wenn Ubuntu mit dem Fenster „Aktualisierungsverwaltung“ über Updates nur informieren soll. Sie können Sie dann jederzeit auf „Jetzt installieren“ klicken oder das Update mit „Später erinnern“ vorerst verschieben.

Hinter „Über neue Ubuntu-Versionen benachrichtigen“ ist bei Ubuntu 20.04 LTS standardmäßig „Für Langzeitunterstützungsversionen“ eingestellt. Die nächste LTS-Version ist planmäßig im April 2022

verfügbar (22.04 LTS), die Benachrichtigung erfolgt meist drei Monate nach diesem Termin. Sie können dann ein Upgrade durchführen oder damit bis zum April 2025 warten. Wenn Sie keine Benachrichtigung über die Nachfolgeversion wünschen, stellen Sie „Niemals“ ein.

2. Updatekonfiguration bei Linux Mint 20

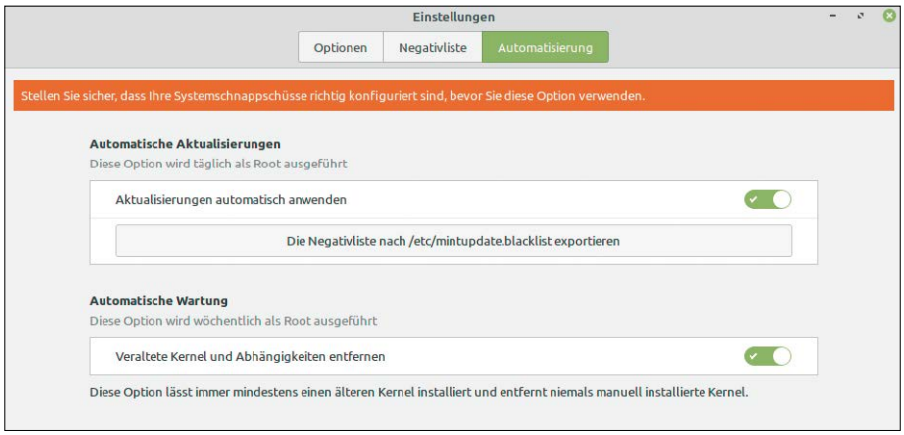
Bei Linux Mint 20 Cinnamon ist die Updateverwaltung vorsichtiger konfiguriert. Automatische Aktualisierungen sind standardmäßig deaktiviert. Sie werden über ein Icon rechts unten in der Leiste am unteren Bildschirmrand informiert, sobald Updates verfügbar sind. Klicken Sie das Icon an. Es öffnet sich das Fenster „Aktualisierungsverwaltung“, in dem Sie nur auf „Aktualisierungen installieren“ klicken.

Die Konfiguration der Aktualisierungsverwaltung lässt sich über den Menüpunkt „Bearbeiten → Einstellungen“ ändern. Wechseln Sie auf die Registerkarte „Automatisierung“. Linux Mint empfiehlt in einem farblich hervorgehobenen Hinweis, dass Sie Systemschnappschüsse konfigurieren sollen, bevor Sie das automatische Update aktivieren. Mehr dazu lesen Sie in Punkt 6. Wenn das erledigt ist, aktivieren Sie – wenn gewünscht – „Aktualisierungen automatisch anwenden“. Außerdem können Sie „Veraltete Kernel und Abhängigkeiten entfernen“ einschalten. Linux Mint löscht dann alle älteren Kernel bis auf den direkten Vorgänger des aktuellen. Sollten Problem mit einem neuen Kernel auftreten, lässt sich über das Grub-Bootmenü der funktionstüchtige Vorgänger wählen und der problematische Kernel danach deinstallieren.

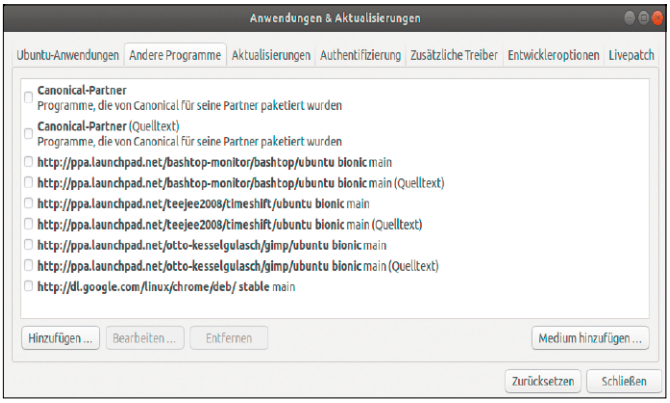
Auf der Registerkarte „Optionen“ legen Sie fest, wie oft Linux Mint die Paketliste auffrischen soll. Der Standard steht bei zehn Minuten nach dem Systemstart und danach alle zwei Stunden. Der Download der Paketliste lässt sich auch deaktivieren, wodurch dann auch keine automatischen Updates mehr erfolgen.

3. Pakete von Drittanbietern entfernen

Wer nur die Standard-Paketquellen verwendet, kann diesen Abschnitt überspringen. Sollte aber Software aus anderen Quellen installiert sein, sollten Sie vor einem großen Systemupgrade auf die nächsthöhere Version der Distribution zusätzliche Maßnahmen ergreifen. Probleme können nämlich auftreten, wenn ein PPA oder eine andere externe Paketquelle nicht nur eine bestimmte Software, sondern dabei auch Updates für Systembibliotheken installiert. Es ist nicht sichergestellt, dass das Systemupgrade die gleiche oder eine höhere Version nebst zugehörigen Abhängigkeiten installieren kann. Wird die passende Bibliothek nicht gefunden, bricht das Systemupgrade ab.



Linux Mint: Die automatische Aktualisierung ist standardmäßig deaktiviert. Bevor Sie die Funktion nutzen, sollten Sie Systemschnappschüsse mit Timeshift konfigurieren.



Zusätzliche Paketquellen: Ubuntu deaktiviert Fremdquellen vor dem Upgrade. Danach können Sie die Häkchen wieder setzen und bei Bedarf den Namen der Distribution anpassen.

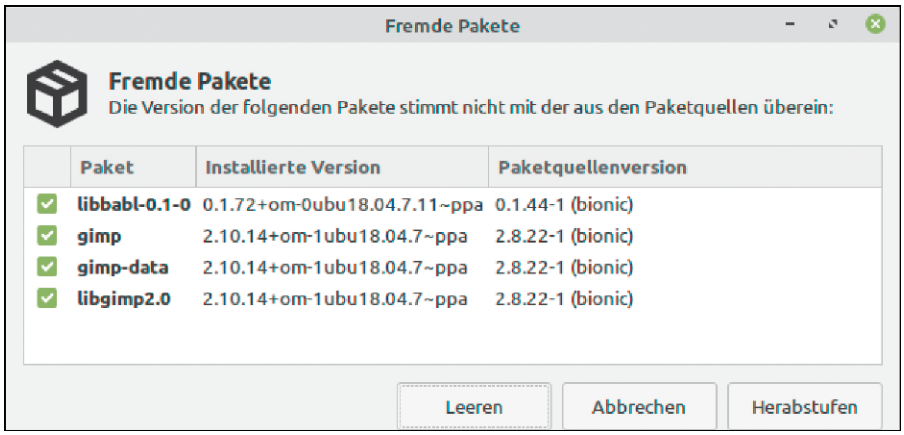
UPDATES EINZELNER PAKETE VERBIETEN

Manchmal sind bestimmte Paketupdates unerwünscht, etwa dann, wenn man selbst eine eigene Version mit anderen Optionen eingerichtet hat oder weil eine neue Version Probleme bereitet. Unter Linux Mint lassen sich Updateausnahmen in den Einstellungen der „Aktualisierungsverwaltung“ auf der Registerkarte „Negativliste“ konfigurieren. Über die „+“-Schaltfläche legen Sie Pakete und Versionen fest, die nicht aktualisiert werden sollen. Alternativ können Sie im Fenster „Aktualisierungsverwaltung“ über das Kontextmenü eines Pakets das Update genau dieser Paketversion oder auch aller zukünftigen Versionen unterbinden. Damit die Negativliste auch beim automatischen Update berücksichtigt wird, wechseln Sie auf die Registerkarte „Automatisierung“ und klicken auf „Die Negativliste nach /etc/mintupdate.blacklist exportieren“.

Ubuntu-Nutzer verwenden im Terminal diesen Befehl:

```
sudo apt-mark hold [Paketname]
```

Dies verhindert, dass „[Paketname]“ aktualisiert, automatisch installiert oder entfernt wird. Verwenden Sie „unhold“ statt „hold“, um eine Sperre wieder aufzuheben.



Vor dem Upgrade: Linux Mint bietet an, aktuellere Versionen aus fremden Quellen durch die älteren Versionen aus den Standard-Paketquellen zu ersetzen.

Ubuntu deaktiviert beim Upgrade automatisch alle zusätzlich eingebundenen PPAs und andere fremde Repositorien. Wenn Sie auf Software aus diesen Quellen angewiesen sind, prüfen Sie vor dem Upgrade, ob die Pakete auch für die neue Ubuntu-Version verfügbar sind. Nach dem Upgrade lassen sich die Quellen über „Anwendungen & Aktualisierungen“ auf der Registerkarte „Andere Programme“ wieder aktivieren. Bei einigen müssen Sie wahrscheinlich den Namen der Distribution anpassen. Ändern Sie beispielsweise „bionic“ auf „focal“, wenn Sie von Ubuntu 18.04 zu 20.04 wechseln.

Bei Ubuntu bleiben die Fremdpakete jedoch erhalten, auch wenn die Quellen deaktiviert sind. Die Entwickler verlassen sich darauf, dass das schon irgendwie gut gehen wird. In vielen Fällen wird das so sein, in einigen aber nicht. Wer auf der sicheren Seite sein will, folgt dem Vorbild Linux Mint. Installieren Sie dazu ein zusätzliches Tool:

```
sudo apt install ppp-purge
```

Mit der Befehlszeile

```
sudo ppa-purge [ppa-Name]
```

lässt sich eine externe Paketquelle deaktivieren und das Programm wird auf die Version aus den Standard-Paketquellen zurückgesetzt. Ist es dort nicht verfügbar, wird es deinstalliert. Ersetzen Sie den Platzhalter „[ppa-Name]“ durch die tatsächliche Bezeichnung des PPAs, die typischerweise mit „ppa:“ beginnt.

Linux Mint: Für ein Upgrade müssen bei Linux Mint Drittanbieterquellen zwingend deaktiviert sein und Software aus diesen Quellen muss entfernt werden. Das Risiko eines Fehlschlags beim Upgrade wird dadurch minimiert. Wenn Software aus zusätzlichen Quellen installiert ist, gehen Sie im Menü auf „Systemverwaltung → Anwendungspaketquellen“ und dann auf „PPAs“. Entfernen Sie alle Häkchen in der Spalte „Aktiviert“. Klicken Sie auf „OK“, um den apt-Zwischenspeicher zu aktualisieren. Unter „Zusätzliche Paketquellen“ gehen Sie entsprechend vor. Gehen Sie auf „Wartung“ und klicken Sie auf „Fremde Pakete herabstufen“. Wählen Sie alle Pakete aus und klicken Sie auf „Herabstufen“. Danach klicken Sie auf „Fremde Pakete entfernen“, wählen alles aus und klicken auf „Entfernen“.

4. Das Systemupgrade bei Ubuntu

Direkt vor einem Upgrade sollte man Sicherheitshalber ein Backup des gesamten Systems erstellen oder wenigstens das der persönlichen Dateien (siehe Punkt 6).

Installieren Sie außerdem alle verfügbaren Updates (siehe dazu auch den Beitrag ab Seite 68).

Sobald Ubuntu eine neue Systemversion meldet, genügt ein Klick auf „System jetzt aktualisieren“. Es kann immer nur auf die nächsthöhere Version aktualisiert werden, beispielsweise von Ubuntu 18.04 auf 20.04 (LTS-Versionen). Folgen Sie einfach den Anweisungen des Assistenten. Der Kernel und alle Softwarepakete werden dann auf den neuesten Stand gebracht. Wenn keine Upgradeinfo erscheint oder wenn Sie das Upgrade frühzeitig manuell durchführen wollen, verwenden Sie diese Befehlszeile im Terminal:

```
sudo update-manager -c
```

Das Upgrade lässt sich dann folgendermaßen auch ohne grafische Oberfläche im Terminal durchführen:

```
sudo do-release-upgrade -d
```

In der Regel gelingt das Upgrade problemlos. Es gibt jedoch einige Hürden, mit denen Sie rechnen müssen. Für die neue Linux-Version stehen unter Umständen nicht alle Softwarepakete zur Verfügung, die Sie bisher installiert hatten. Der Upgradeassistent informiert Sie über die nicht mehr unterstützten Pakete. Meist handelt es sich nur um einige veraltete Systembibliotheken, die ohnehin kein aktuelles Programm mehr verwendet. Sie sollten aber die Liste prüfen und im Internet nach Alternativen suchen, wenn Sie die genannte Software tatsächlich benötigen.

5. Das Systemupgrade bei Linux Mint

Installieren Sie alle verfügbaren Updates und erstellen Sie ein Backup (siehe Punkt 6). Damit sich Linux Mint auf die neueste Version (21 kommt im Sommer) aktualisieren lässt, muss das letzte Point Release 20.3 installiert sein.

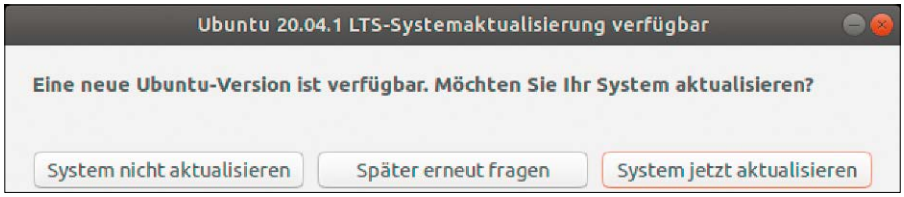
Upgradebereitschaft prüfen: Öffnen Sie ein Terminal und führen Sie die folgenden drei Befehle aus:

```
sudo apt update
sudo apt upgrade
sudo apt install mintupgrade
```

Das Tool mintupgrade erledigt ein Upgrade zur nächsthöheren Version – demnächst von Linux Mint 20.3 auf 21. Starten Sie das Tool ohne vorangestelltes „sudo“. Höhere Rechte werden bei Bedarf angefordert:

```
mintupgrade check
```

Bestätigen Sie die Prüfung mit Y-Taste und Eingabetaste. Sollte bisher keine Sicherung mit Timeshift („Systemschnappschüsse“)



Upgrade einleiten: Kurze Zeit nach Erscheinen einer neuen Version wird deren Installation angeboten. Sie können das Angebot sofort annehmen oder das Upgrade verschieben.

konfiguriert sein (Punkt 6), erhalten Sie eine Fehlermeldung und der Vorgang bricht ab. Wurde eine Sicherung mit einem anderen Tool durchgeführt, können Sie dem System mit

```
echo "{}" | sudo tee /etc/timeshift.
 json
```

eine Timeshift-Sicherung vorgaukeln. Löschen Sie die Datei „timeshift.json“ später wieder, falls Sie Timeshift später verwenden möchten.

Mit der Option „check“ weisen Sie mintupdate an, die Paketquellen temporär für das neue System zu ändern und die Installation zu simulieren. Ansonsten wird nichts am System geändert. Unter „Die folgenden Pakete werden ENTFERNT“ gibt das Tool aus, welche Pakete von Linux Mint 20 nicht mehr unterstützt werden. In der Regel handelt es sich um veraltete Systembibliotheken, die ohnehin nicht mehr verwendet wird. Wenn etwas Auffälliges dabei ist oder benötigte Software, suchen Sie im Internet, ob die Software vom neuen System unterstützt wird. Die abschließende Meldung „Command ‚check‘ completed successfully“ signalisiert, dass Sie mit dem Upgrade fortfahren können. Andernfalls folgen Sie der Anweisung in der Fehlermeldung.

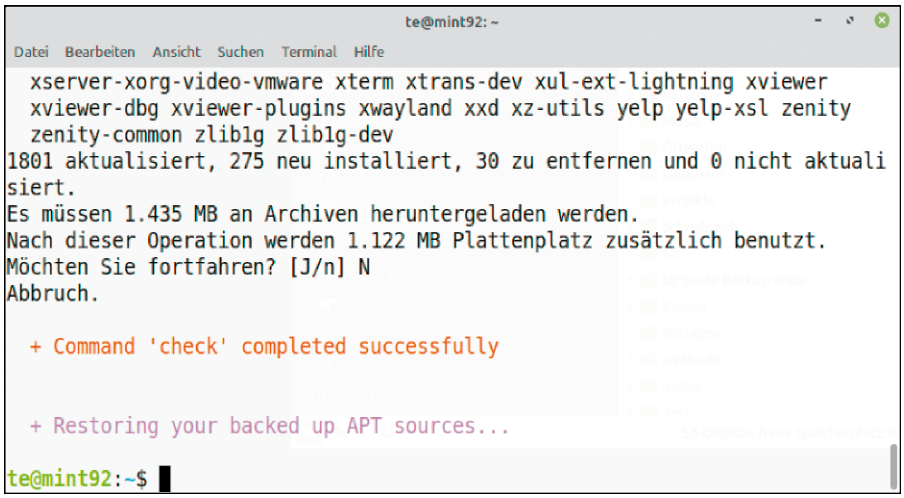
Upgrade durchführen: Im nächsten Schritt laden Sie mit

```
mintupgrade download
```

die Upgradedateien herunter, am installierten System ändert sich aber dadurch noch nichts. Erst das Kommando

```
mintupgrade upgrade
```

führt die Installation durch, was dann nicht mehr umkehrbar ist.



Upgradecheck unter Mint: Mit dem Tool mintupgrade prüfen Sie, ob das System für die Aktualisierung bereit ist. Wenn keine Fehler angezeigt werden, führen Sie das Upgrade durch.

6. Backups vor Updates oder Upgrades

Bei einem Arbeitsrechner genügt oft die Sicherung der persönlichen Dateien. Das Betriebssystem lässt sich nach einem Totalausfall oder einem Festplattendefekt oft schneller durch Neuinstallation als durch Rücksichern von Komplettbackups wiederherstellen. Sollten auf dem Rechner jedoch Serverdienste laufen oder sehr viel Software installiert sein, empfiehlt sich eine komplette Sicherung des Systems und zusätzlich ein komplettes Backup der Home-Verzeichnisse.

Ubuntu: Sie können das Programm „Datensicherungen“ verwenden, das für die automatische Sicherung des eigenen Home-Verzeichnisses konfiguriert ist. Unter „Zu ignorierende Ordner“ lassen sich Ordner einstellen, die nicht im Backup landen sollen. Über „Speicherort“ geben Sie den Zielordner an. Dieser kann auf einem Netzwerklaufwerk, einer lokalen Festplatte oder einem Cloudserver liegen.

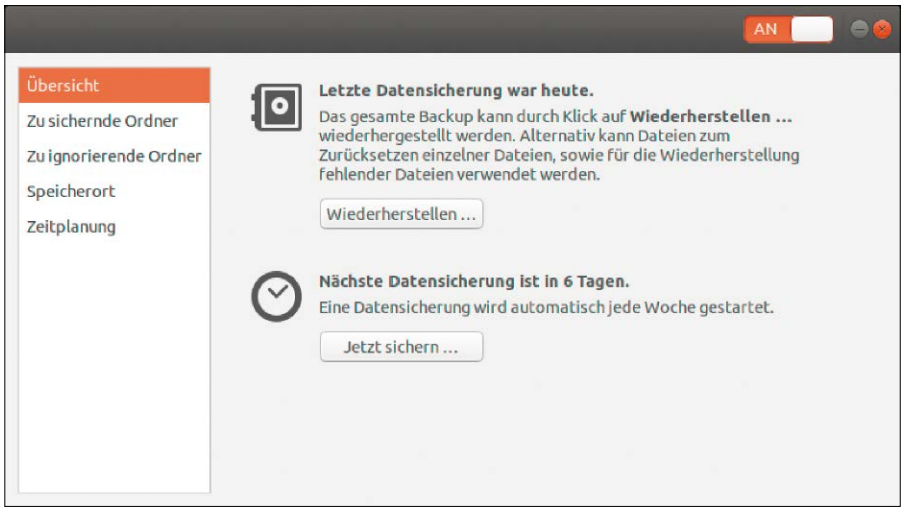
Für Komplettbackups empfiehlt sich ein Tool wie Timeshift. Ubuntu-Nutzer installieren es im Terminal mit diesen Befehlen:

```
sudo add-apt-repository -y
 ppa:teejee2008/timeshift
sudo apt update
sudo apt install timeshift
```

Nach dem Start führt Sie ein Assistent durch die Konfiguration. Belassen Sie die Option „rsync“ und klicken Sie auf „Weiter“. Im nächsten Schritt geben Sie das Ziellaufwerk an. Am besten eignet sich eine zweite oder externe Festplatte, die mit einem Linux-Dateisystem formatiert sein muss, etwa Ext4. Netzwerklaufwerke werden nicht unterstützt. Im letzten Schritt definieren Sie einen Zeitplan und die Menge der Systempunkte.

Wiederherstellen: Die Backups bestehen aus unkomprimierten Ordnern und Dateien unter „/timeshift/snapshots“. Einzelne Dateiobjekte oder der komplette frühere Zustand lassen sich daher mit jedem Livesystem rekonstruieren, falls das primäre System nicht mehr funktioniert.

Linux Mint: Wer nur die persönlichen Daten sichern will, geht im Menü auf „Systemverwaltung → Datensicherungswerkzeug“ und klickt auf „Jetzt sichern“. Folgen Sie den Anweisungen des Assistenten. Timeshift zur Systemsicherung ist bei Linux Mint standardmäßig installiert. ■



Persönliche Dateien sichern: Das Tool „Datensicherungen“ ermöglicht unter Ubuntu ein automatisches Backup der Dateien aus dem Home-Verzeichnis nach Zeitplan.

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

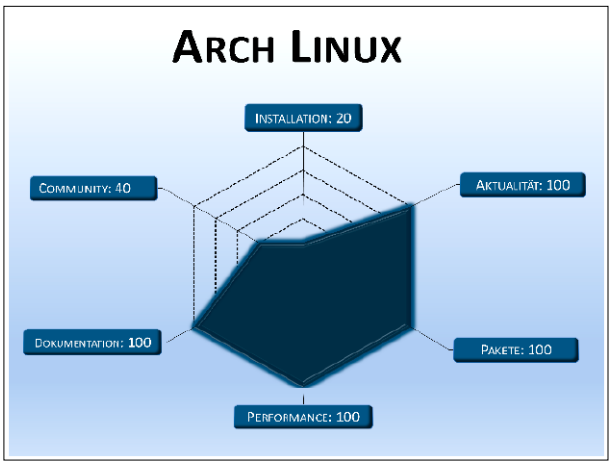
Gut geeignet sind Rolling Releases für anspruchsvolle Desktopsysteme, denn die gelegentliche Mühe sporadischer Korrekturen wird durch ein besonders aktuelles System belohnt. Es ist aber nicht jedes Rolling Release für den Einsatz auf einem Arbeitsrechner geeignet. So ist die Entwicklerversion Ubuntus 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.

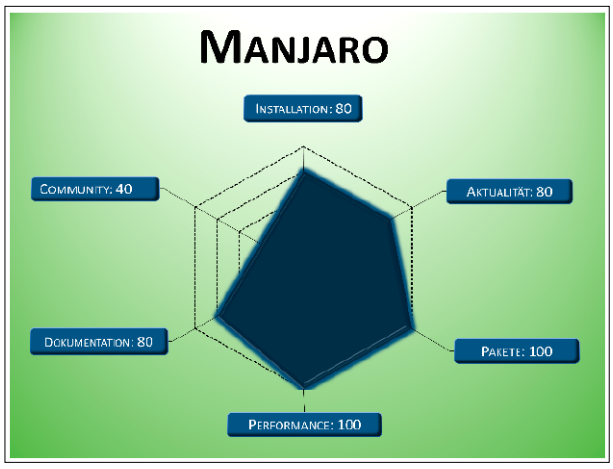
Alle Bestandteile in den offiziellen Repositorys sind deshalb stets sehr aktuell, wenn auch auf das Kernsystem begrenzt. Zahlreiche weitere Pakete liefern inoffizielle AURs („Arch User Repositories“), die es über ein ausgefeiltes Buildsystem erlauben, aus dem Quellcode von Programmen fertige Pakete zu 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.

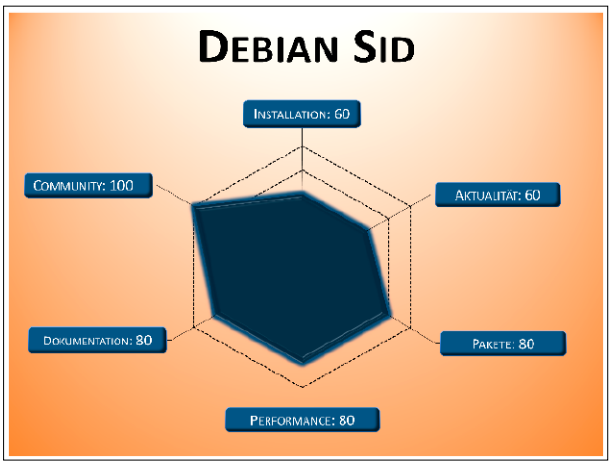
Zwar handelt es sich bei Manjaro im prinzipiellen Aufbau und beim Paketsystem um einen Abkömmling von Arch Linux, allerdings geht die kleine Distribution inzwischen doch viele eigene Wege, sodass sie nicht mehr mit Arch gleichzusetzen ist. Die Unterschiede beginnen damit, dass Manjaro nicht aus den gleichen 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



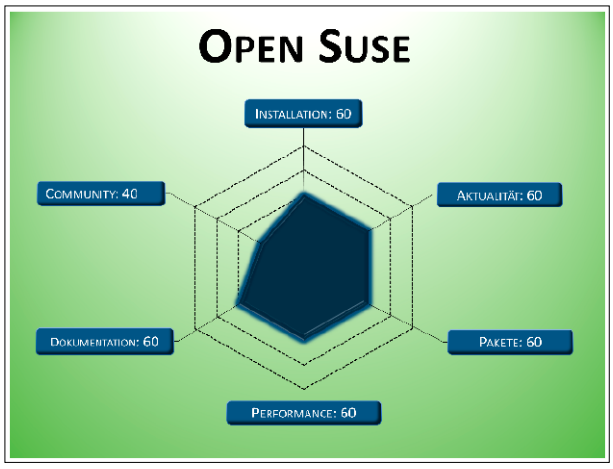
Der Weg eines Pakets zu einer neuen Debian-Ausgabe verläuft von den Zweigen „Experimental“ zu „Unstable“ und dann „Testing“. In „Unstable“ liegt Debian als Rolling Release vor und hat von den Debian-Machern den Codenamen „Sid“ bekommen, der sich wie alle Namen im Debian-Universum auf einen Charakter 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

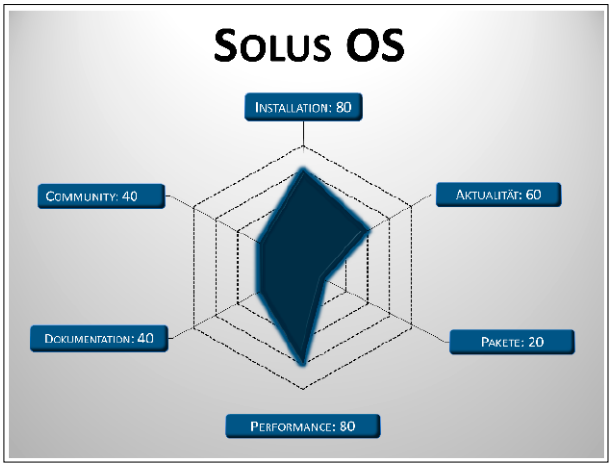


„Tumbleweeds“ sind Steppenläufer, die der Wind mal hierhin, mal dorthin weht. So wie die umherwehenden Wüstensträucher ist Open Suse Tumbleweed stets in Bewegung, da hier die neuesten, nicht immer ausgiebig getesteten Programmpakete ankommen. Eigentlich hat Open Suse nicht den Ruf, ein System mit den 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



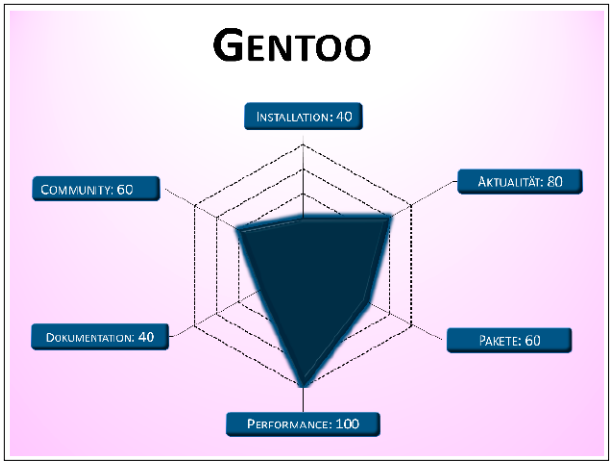
Bescheidener Neuanfang: Solus-OS trat ursprünglich dazu an, eine große Nummer auf dem Linux-Desktop zu werden. Der ehemalige Hauptentwickler ersann dazu den Desktop Budgie als Gnome-Abspaltung und ließ etliche Optimierungen für die typische Arbeitslast grafischer Anwendungen in den verwendeten Linux-Kernel 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 Mint 20: Systemoptimierung

Linux Mint 20.3 ist schnell eingerichtet und bietet eine umfassende grafische Bedienung. Doch hier – wie bei jedem System – gibt es Optionen, sich die Wartung und Pflege zu vereinfachen und wichtige Komponenten noch effizienter zu nutzen.

VON HERMANN APFELBÖCK

Dieser Artikel macht einen Rundgang durch die wichtigsten Mint-Systemtools und die systemnahen Mint-Zubehörprogramme. Aufgabe ist es, die zahlreichen Optionen zur Systemoptimierung zu erklären, zum anderen aber auch Defizite aufzuzeigen, die sich mit Know-how und cleveren Anpassungen kompensieren lassen. Danach nutzen Sie Linux Mint noch souveräner und effizienter.

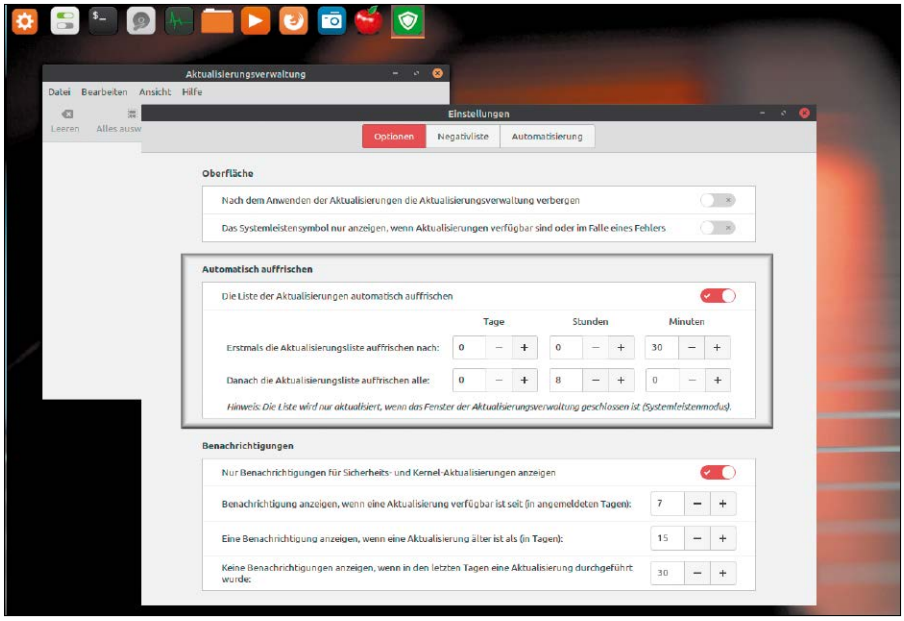
Optionen der Aktualisierungsverwaltung

Das Systemtool „Aktualisierungsverwaltung" (Mintupdate) hält das System und die komplette Software auf dem aktuellen Stand. Einmal über „Bearbeiten → Einstellungen" komfortabel konfiguriert, müssen Sie sich danach in dieser Hinsicht um nichts mehr kümmern.

Automatisierung: Beginnen Sie im Register „Automatisierung", weil es hier für ein Desktopsystem eine sehr einfache Empfehlung gibt: Aktivieren Sie alle vier Optionen, um das System automatisch zu aktualisieren, alte Kernel automatisch zu löschen und ferner auch Cinnamon-Spices (nur Cinnamon-Edition) und Flatpaks auf dem Stand zu halten. Die beiden letztgenannten Optionen sind an dieser Stelle neu. Damit übernimmt jetzt die „Aktualisierungsverwaltung" zwei zusätzliche Jobs, die bisher manuell über

```
flatpak update
cinnamon-spice-updater --update-
  all
```

oder mit entsprechenden Autostarts erledigt werden mussten.



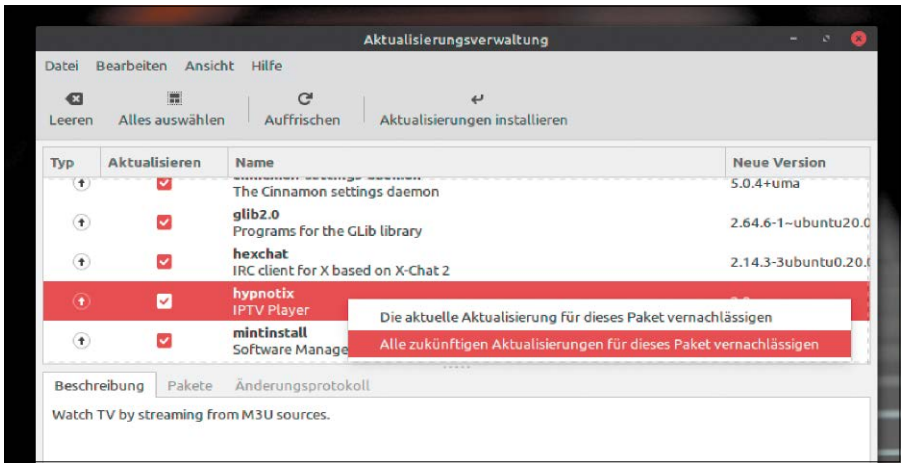
Einmal sauber eingestellt, künftig weitgehend automatisch: Die Mint-Aktualisierungsverwaltung belohnt eine genaue Durchsicht aller Updateoptionen.

Negativliste: Das Register „Negativliste" wird in besonderen Fällen wichtig, wenn eine Software auf keinen Fall aktualisiert werden soll. Die Gründe können bekannte Inkompatibilitäten der neueren Version sein, aber auch Umstellungen technischer oder bedientechnischer Art, die der Anwender einfach nicht wünscht. Das Mediencenter Kodi war zuletzt ein prominenter Kandidat für eine Updatesperre. Nach Klick auf das „+"-Symbol tragen Sie einfach den Paketnamen ein. Eine bequeme Alternative zum manuellen Eintrag in die Negativliste bietet die Updateliste nach der Aktion „Auffrischen". Wenn Sie die Liste der angezeigten Software durchgehen und ein angezeigtes Update dauerhaft verhindern möchten, klicken Sie es rechts an und erhalten die Option „Alle zukünftigen Aktualisierungen [...] vernachlässigen". Auch dies führt zu einem Eintrag in der „Negativliste".

Achtung: Die automatische Aktualisierung (siehe Register „Automatisierung") ignoriert die Negativliste. Dies ändern Sie dadurch, dass Sie unter „Automatisierung" auf diesen Schalter klicken: „Die Negativliste nach /etc/mintupdate.blacklist exportieren". Wenn Sie die Negativliste später ändern, müssen Sie erneut an diesen Klick denken.

Optionen: Im Register „Optionen" ist der Abschnitt „Automatisch auffrischen" der wichtigste. Aktivieren Sie diese Option, damit das System am Spiegelserver (siehe nächsten Punkt) automatisch nachsieht, ob

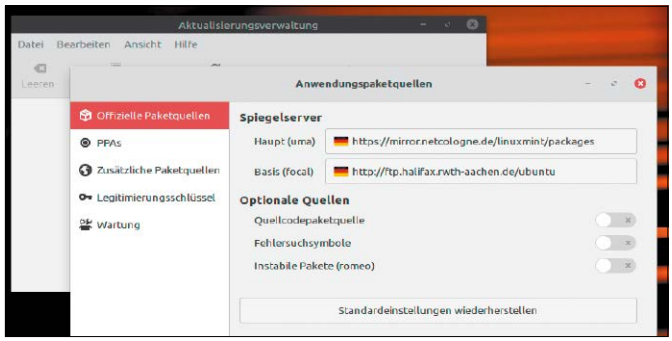
neue Updates bereitstehen. Eher unkritisch sind die Zeitintervalle: Der Punkt „Erstmals auffrischen“ bezieht sich auf den Systemstart. Setzen Sie die Voreinstellung „10“ Minuten deutlich nach hinten, wenn Sie nach Start das System üblicherweise erst mal intensiv nutzen. Ein weiterer Updatecheck ist dann sicher nicht alle zwei Stunden erforderlich (Voreinstellung) und kann so erhöht werden („Tage“), dass er für normale Sitzungen komplett entfällt.
Die weiteren Abschnitte „Oberfläche“ und „Benachrichtigungen“ sind eigentlich marginal. Wenn Sie möglichst unbehelligt bleiben wollen, aktivieren Sie alle verfügbaren Optionen und setzen unter „Benachrichtigungen“ die Tageswerte deutlich höher.



Aufnahme in die „Negativliste“: Damit können Sie bestimmte Software dauerhaft einfrieren und ihr alle Updates verbieten.

Paketquellen und schnelle Spiegelserver

Das Systemtool „Anwendungspaketquellen“ (mintsources) zeigt und verwaltet alle zentralen Server für Software- und Updatebezug. Von einer möglichst schnellen Verbindung zu diesen Servern profitieren Sie eventuell täglich – abhängig davon, wie oft Sie Software installieren und wie die Updateintervalle in der „Aktualisierungsverwaltung“ (mintupdate) eingestellt sind. Daher lohnt sich in den „Anwendungspaketquellen“ das Einstellen schneller lokaler Spiegelserver, dies umso mehr, wenn Sie ein Highspeed-Internet nutzen. Spiegelserver bieten nur die Software aus den „Offiziellen Paketquellen“, dies sind aber die mit Abstand wichtigsten und umfangreichsten: Der Server für „Haupt (uma)“ liefert alle Updates für Mint-eigene Komponenten, der noch wichtigere Server für „Basis (focal“) die Updates und Software der Ubuntu-Paketquellen. Beim Klick auf die voreingestellten Server startet automatisch ein Geschwindigkeitstest, der die schnellsten Server nach oben sortiert. Schnelle lokale Spiegelserver – zumeist von Universitäten – sind ein Win-Win-Angebot. Der Nutzer erhält seine Software und Updates schneller, die primären Mint- und Ubuntu-Server werden entlastet und somit indirekt auch ignorante Nutzer belohnt, die sich um diese Einstellung nicht kümmern.
Hinweis: Wie beschrieben, berücksichtigt die jüngste Mint-Aktualisierungsverwaltung auch Software von PPAs, „Zusätzlichen Paketquellen“ (etwa Google Chrome) und Flatpaks. Von lokalen Spiegelservern können diese aber nicht profitieren.



Das ist Ihr heißer Draht zu frischer Software: Deutsche Spiegelserver nützen Ihnen und den Distributionsanbietern (Mint und Ubuntu) gleichermaßen.

Die Systemschnappschüsse (Timeshift)

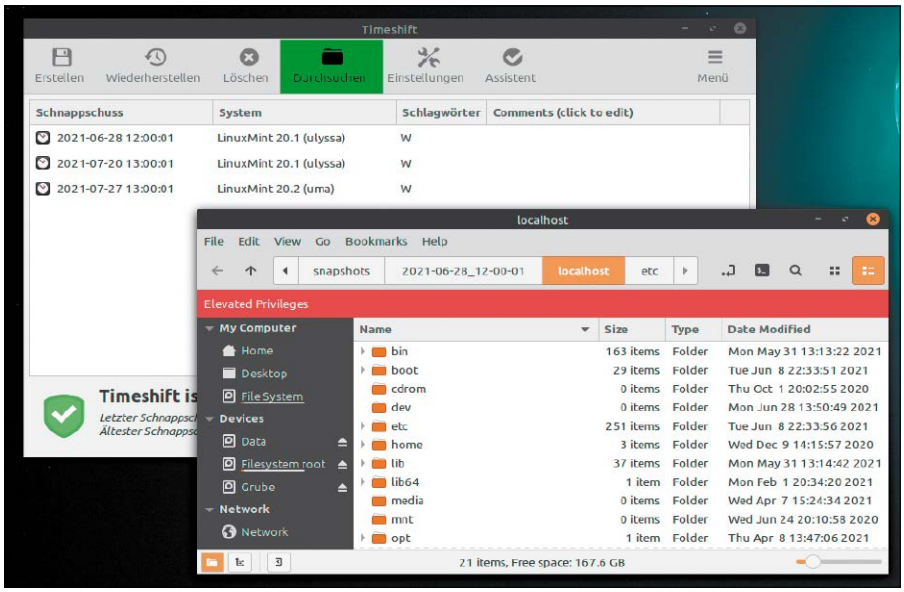
Linux Mint besteht auf „Systemschnappschüsse“ mit Timeshift und fordert deren Einrichtung schon beim „Willkommen“-Dialog nach dem ersten Systemstart. Sie sind gut beraten, dies zu akzeptieren und im Optimalfall bei der Einrichtung und beim „Schnappschussort“ (Zieldatenträger der Sicherung) einen unabhängigen zweiten Datenträger anzugeben. Falls dies nicht möglich ist, akzeptieren Sie das Standardziel „/timeshift“ im Wurzelverzeichnis. Beim Zeitplan („Schnappschussebenen“) sollten wöchentliche Sicherung und drei bis fünf aufbewahrte Sicherungspunkte genügen.
Wiederherstellen: Am bequemsten ist die Wiederherstellung mit Timeshift selbst: Das Tool zeigt in seiner Liste der Momentaufnahmen alle Punkte nach Alter geordnet. „Wiederherstellen“ schreibt einen markierten Punkt zurück. Die Wiederherstellung ist aber notfalls (und wichtig) auch im Terminal möglich, folglich in der virtuellen Konsole (Strg-Alt-F1), falls die Oberfläche streikt. Die einfachste Methode, einen Snapshot wiederherzustellen, ist dieser Befehl:

```
sudo timeshift --restore
```

Dann zeigt Timeshift die Liste aller verfügbaren Snapshots an und der gewünschte kann mit der angegebenen Kennziffer ausgewählt werden.
Ferner sollten Sie wissen, dass das von Timeshift genutzte Tool Rsync die Backupsätze einfach als unkomprimierte Ordner und Dateien ablegt. Daher können Sie gezielt einzelne Dateiobjekte suchen und zurückkopieren – am bequemsten in Timeshift mit „Durchsuchen“. Dieses Wissen ist aber auch wichtig für den „Worst Case“: Die Schnappschüsse liegen im Backupdatenträger unter „/timeshift/snapshots“. Somit lässt sich ein früherer Systemzustand mit jedem Livesystem notfalls manuell rekonstruieren.

Benutzerkonten mit Verschlüsselung

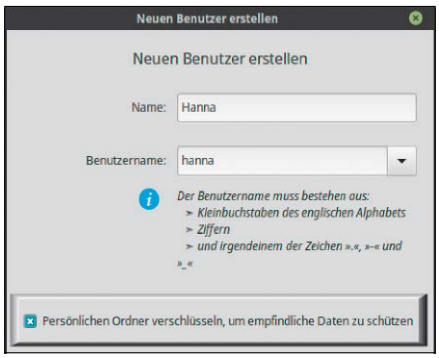
Eventuell genügt das bei der Installation eingerichtete Systemkonto dauerhaft. Es hat sudo-Recht und somit den Status „Systemverwalter“: Dennoch sollten Sie wissen, wie Sie Konten verwalten und einrichten. Unter „Systemeinstellungen → Benutzer



Wiederherstellen mit Timeshift: Wer nur bestimmte Daten benötigt, verwendet statt „Wiederherstellen“ die Option „Durchsuchen“. Hier sind alle Dateiobjekte einzeln erreichbar.

und Gruppen“ können Sie Benutzerkonten einsehen, Kennwörter und Kontotyp ändern sowie neue Konten anlegen, wobei Konten vom Typ „Systemverwalter“ automatisch sudo-Recht erhalten.

Neue Konten können Sie wahlweise mit oder ohne Home-Verschlüsselung einrichten (Ecrypt FS, siehe dazu auch „Installationen und Upgrades“ ab Seite 48). Das ist ein interessanter Aspekt für den Fall, dass Sie die Home-Verschlüsselung bei der Installation für Ihr eigenes Konto für unnötig erachtet hatten. Die Mate- und XFCE-Edition bieten in der Benutzerverwaltung die Option „Persönlichen Ordner verschlüsseln...“ an, wenn Sie ein neues Konto einrichten. Cinnamon lässt diese Option allerdings vermissen. Hier hilft dieser alternative Terminalbefehl:



Neuen Benutzer mit verschlüsseltem Home einrichten: Was Mate und XFCE hier anbieten, lässt ausgerechnet Cinnamon vermissen. Dort muss ein Terminalbefehl aushelfen.

```
sudo adduser --encrypt-home
  [Kontoname]
```

Anschließend legen Sie das Passwort fest und bestätigen dann alle Abfragen mit Eingabetaste.

Dateimanager Nemo: Neue Funktionen

Neue Inhaltssuche: Mit Version 5.0.3 des aktuellen Mint-Systems erhält Nemo eine nützliche Ergänzung: Nach Klick auf das Lupensymbol erscheint jetzt eine zweizeilige Abfrage. Die erste Zeile ist der bekannte Filter nach Dateinamen und kann auf das aktuelle Verzeichnis begrenzt oder rekursiv auf alle Unterordner bezogen werden. Die zweite Zeile ermöglicht die neue Inhaltssuche. Dabei verarbeitet Nemo neben purem Text alle verbreiteten Formate wie Office- oder PDF-Dokumente. Diese Funktion ist – auf überschaubare Datenmengen angesetzt – ebenso flott wie praktisch.

Dateiobjekte „anheften“ und „favorisieren“: Bekanntlich kann Nemo jedes Dateiobjekt nach Rechtsklick und „Zu Favoriten hinzufügen“ in eine Favoritenliste aufnehmen. Die Favoriten sind dann in der Navigationsspalte unter „Favoriten“ jederzeit erreichbar, auf Wunsch auch in einem zusätzlichen Leistenapplet. Unter „Bearbeiten → Einstellungen → Ansichten“ gibt es neuerdings die zusätzliche Option „Favoriten vor anderen Dateien sortieren“. Falls aktiv, werden die favorisierten Dateiobjekte zusätzlich in der Ordnerliste nach oben sortiert. Das ist verwirrend, weil es ja noch die weitere Option „Anheften“ gibt, die Dateiobjekte ebenfalls nach oben sortiert.

Aber gewiss: Es kann Dateiobjekte geben, die man durch „Anheften“ nur in ihrem Verzeichnis nach oben sortieren will, während Favoriten global im ganzen Dateisystem gelten und nun auf Wunsch auch noch im eigenen Verzeichnis die erste Stelle erhalten.

Dateimanager Nemo als Integrator

Nemo und Bulky: Das nagelneue Renametool Bulky ist unter „Zubehör → Dateiumbenennung“ zu finden. Es ermöglicht für alle markierten Dateien (Bulky arbeitet nicht rekursiv) Zeichenersetzungen, Einfügen von Text an bestimmter Position, Löschen von Zeichen an bestimmter Position und Änderungen von Groß- und Kleinschreibung. Zur Kontrolle werden die geänderten Namen in der linken Spalte angezeigt, erst der Klick auf „Umbenennen“ löst die Aktion aus. Unverständlich bleibt, warum das Tool nicht als Kontextmenü in den Dateimanager Nemo integriert wurde. Das ist nämlich dank der modularen „Nemo-Actions“ eine leichte Übung. Eine zusätzliche Datei „bulky.nemo_action“ unter „/usr/share/nemo/actions“ mit diesem Fünfzeiler (siehe auch Abbildung oben rechts)

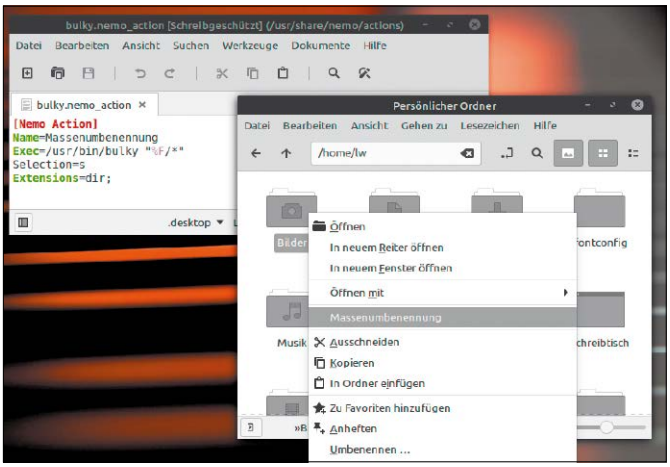
```
[Nemo Action]
Name=Massenumbenennung
Exec=/usr/bin/bulky "%F/*"
Selection=s
Extensions=dir;
```

übergibt alle Dateien eines markierten Ordners via Nemo an das Tool Bulky. Der Name des zusätzlichen Kontextmenüs ist frei wählbar – in unserem Beispiel „Massenumbenennung“. Das Anlegen der Action-Datei unter „/usr/...“ erfordert root-Recht.

Nemo und Google Drive: Der Dateimanager kann die Daten auf Google Drive direkt unter „Netzwerk“ anbieten. Unter „Systemeinstellungen → Internetkonten“ machen Sie Cinnamon (Mate und XFCE bieten diesen Punkt nicht) mit Ihren Webkonten bekannt. Nach einer Anmeldung bei Google wird Nemo mit dem Webdienst verknüpft. Das funktioniert analog auch mit Nextcloud-Servern, allerdings nicht mit Microsoft Onedrive oder Dropbox, wobei Dropbox jedoch unter *www.dropbox.com/install* seinen eigenen Linux-Client anbietet.

Nemo und Mintstick: Die kleine Mint-Eigenentwicklung Mintstick hat keinerlei Fä-

higkeiten, die über das mächtige Gnome-Disks („Laufwerke“) hinausführen. Es erscheint zwar im Menü unter „Zubehör“ sogar in doppelter Funktion als „USB-Abbilderstellung“ und als „USB-Stick-Formatierer“, erhält aber seine Rechtfertigung alleine durch die Integration in den Dateimanager: Nach Rechtsklick auf eine ISO- oder IMG-Datei erscheint das Kontextmenü „Startfähigen USB-Stick erstellen“. Der Pfad zum Abbild ist damit schon links eingetragen und nach Auswahl des Ziellaufwerks rechts sowie Klick auf „Schreiben“ beginnt die Übertragung. Einfacher geht’s nicht!



Rename-Tool Bulky in den Dateimanager integrieren: Dank der unkomplizierten Action-Scripts für Nemo ist das keine große Aufgabe.

Warpinator: Auch für Android und Ubuntu

Für private Heimnetze, die ohne Serverfreigaben auskommen, ist das relativ junge Mint-Tool Warpinator eine einfache Alternative des Datenaustauschs. Ursprünglich wurde der Warpinator per Autostart standardmäßig geladen, in Version 20.2 nicht mehr. Ein erster Tipp, falls Sie das Tool permanent brauchen, ist daher der Autostart in den „Einstellungen“ des Tools („Automatisch starten“). Ebenda als „Speicherort für empfangene Dateien“ bietet sich auf Desktoprechnern der „Schreibtisch“ an, da Sie die Dateien von dort am bequemsten an die endgültige Stelle übertragen. Ob der Datenaustausch am Zielgerät jeweils explizit genehmigt werden soll, ist Ermessenssache.

Die eigentliche Aktion ist einfach: Der Warpinator sucht nach seinesgleichen im Netzwerk und zeigt alle Geräte mit laufendem Warpinator an. Man klickt einfach auf das Zielgerät, das die Dateien erhalten soll, und zieht dann mit der Maus die gewünschten Dateien aus dem Dateimanager Nemo in das Warpinator-Fenster. Beachten Sie diesen einfacheren Weg über Nemo: Die Dateiauswahl im Tool selbst ist über „Dateien senden“ natürlich auch möglich, aber viel umständlicher. Den Warpinator gibt es inzwischen auch als Android-App im Google Play Store. Auf anderen Linux-Distributionen lässt sich der Warpinator als Flatpak installieren, dabei fordert das an sich kleine Tool aber ein GB beim Download sowie erheblichen Plattenplatz.

Mintbackup auf externes Laufwerk

Die Mint-Eigenentwicklung „Datensicherungswerkzeug“ sichert die Benutzerdateien im Home-Verzeichnis. Das Tool bietet beim Start nur die Optionen „Wiederherstellen“ und „Jetzt sichern“ und ist nicht mehr als ein klickfreundliches grafisches Tar-Front-End. Beim Sichern kopiert es einfach unter „/home/[konto]“ alle Benutzerordner und Dateien mit Pfad, Zeitstempel und Rechte in ein Tar-Archiv. Wenn Sie auch versteckte Ordner wie „~/.config“ oder „~/.thunderbird“ einbeziehen wollen, müssen Sie dies beim Schritt „Verzeichnisse einschließen“ explizit anfordern. Dies bleibt dann auch für künftige Sicherungen erhalten. Beim späteren „Wiederherstellen“ müssen Sie sich über Navigationsfeld nur zum Pfad des Tar-Archivs durchklicken und mit „Öffnen“ und „Vor“ den Vorgang auslösen. Da auch der Standard-Archivmanager (File-Roller) das Tar-Format beherrscht, können Sie aber auch einzelne Dateien aus dem Backup ziehen.

Das Tool hat nur rudimentäre Einstellungsoptionen in der Dconf-Zentrale (com.linuxmint.backup). Ärgerlich ist vor allem, dass das Standardziel der Sicherung unter „~/Dokumente/Sicherungen“ hier nicht erscheint und folglich nicht dauerhaft zu ändern ist. Wenn Sie auf einen externen Datenträger sichern möchten, müssen Sie das jedes Mal explizit angeben. Einzige Abhilfe ist es, das Verzeichnis „~/Dokumente/Sicherungen“ zu löschen und eine Umleitung über einen Symlink anzulegen (Beispiel):

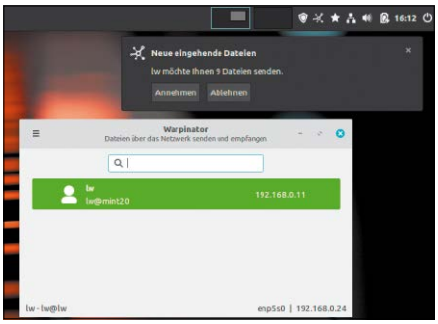
```
ln -s /media/lw/Data/Sicherungen ~/
  Dokumente/Sicherungen
```

Das setzt aber voraus, dass der externe Datenträger unter dem angegebenen Pfad standardmäßig zur Verfügung steht.

Editor Xed mit Komfortfunktionen

Xed („Zubehör → Textbearbeitung“) ist einer der besten Zubehöreditoren und in seinem Umfang oft unterschätzt. Eine der nützlichsten, aber nicht standardmäßig aktiven Funktionen ist die „Wortvervollständigung“, die Sie unter „Bearbeiten → Erweiterungen“ aktivieren sollten. Xed orientiert sich dabei (Case-sensitiv) an den Wörtern aller derzeit geöffneten Dateien. Ab welcher Buchstabenmenge die Vorschläge angezeigt werden sollen, ist einstellbar. Für Scripts ist „2“ oder „3“ zu empfehlen. Unabhängig von diesem Automatismus lässt sich die Vorschlagliste auch jederzeit mit Strg-Leertaste erzwingen. Wenn Sie keinen der Vorschläge mit Eingabetaste übernehmen wollen, blendet die Rücktaste die Vorschlagliste wieder aus.

Xed hebt Schlüsselwörter durch unterschiedliche Farben hervor, wenn er die Script-Sprache automatisch erkennt. Falls nicht, hilft ein Klick auf das Auswahlfeld unten in der Statusleiste oder das Menü „Ansicht → Hervorhebungsmodus“. Unter „Bearbeiten → Einstellungen“ gibt es außerdem eine Auswahl von Farbthemen und wichtige Optionen wie Zeilennummern, Schriftgröße und automatische Backups. ■



Warpinator: Das Sharingtool ist schneller als Samba und sicher konfigurierbar. Es eignet sich mindestens für eine Nebenrolle im privaten Netz oder für Arbeitsgruppen im Büro.

Desktoptuning Cinnamon

Linux Mint definiert sich maßgeblich über die Cinnamon-Oberfläche, die mit der aktuellen Version wieder neuen Feinschliff erhält. Cinnamon ist klassisch, aufgeräumt und anpassungsfähig, zudem umsteigerfreundlich mit vielen Windows-Analogien.

VON HERMANN APFELBÖCK

In der Annahme, dass Cinnamon für die meisten Nutzer das eindeutige Hauptmotiv für die Wahl von Linux Mint ist, fokussieren wir uns beim Thema „Desktoptuning" ganz auf Cinnamon. Die Mint-Editionen mit Mate und XFCE bleiben außen vor.

RAM-Limit und Reparaturoptionen

Nach etlichen behobenen Cinnamon-Speicherlecks gibt es jetzt eine neue, prophylaktische Speicherüberwachung des Desktops. Unter „Systemeinstellungen → Allgemein" erscheint der Punkt „Speichergrenze". Hier können Sie Cinnamon ein Limit vorgeben. Voreingestellt sind „2048", minimal zulässig sind „1024" MB – und dies sollte völlig ausreichen. Der Verbrauch wird laut Voreinstellung alle 300 Sekunden überprüft. Bei Überschreiten des Limits erfolgt ein Zwangsneustart von Cinnamon, alle sonstigen Programme laufen weiter.

Weitere manuelle Problemlöser bietet Cinnamon schon länger und dies in mehreren Abstufungen:

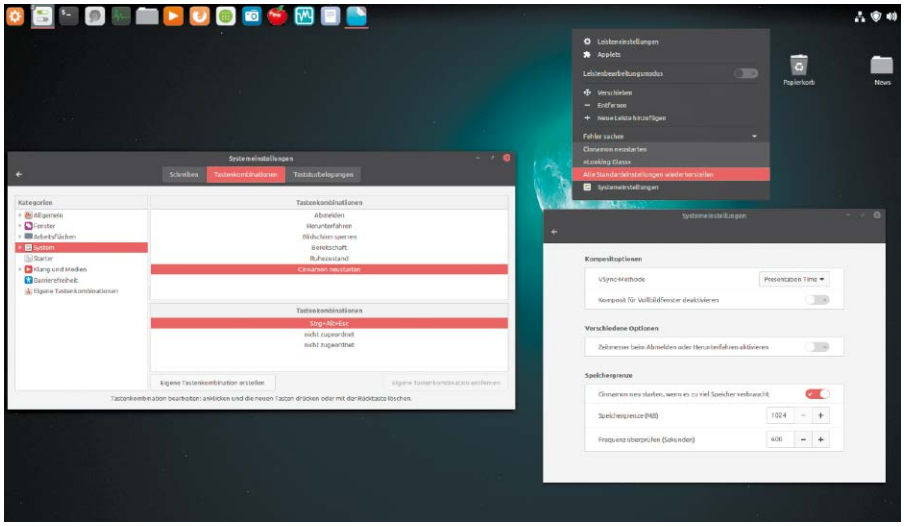
• Der Hotkey Strg-Alt-Esc startet die Oberfläche neu. Technisch identisch hierzu ist der Rechtsklick auf der Systemleiste und die Option „Fehler suchen → Cinnamon neustarten".

• Der Hotkey Strg-Alt-Rücktaste ist die härtere Variante, die nicht nur den Desktop, sondern die komplette Sitzung beendet und zum Anmeldebildschirm zurückführt.

• Weitere Troubleshooting-Optionen bietet das Tool cinnamon-looking-glass. Es lässt sich durch Rechtsklick auf die Systemleiste und „Fehler suchen → Looking Glass" starten oder im Terminal über *cinnamon-looking-glass*. Hier gibt es unter der Schaltfläche „Actions" (ganz rechts) die zusätzliche Möglichkeit, die Cinnamon-Konfiguration auf den Standard zurückzusetzen („Reset Cinnamon Settings").

• Falls ein Reset der Cinnamon-Einstellungen auf grafischer Ebene nicht mehr möglich ist, kann dies auch folgender Terminalbefehl erledigen:

```
dconf reset -f /org/cinnamon/
```



Eingebaute Problemlöser: Bei Cinnamon-Problemen helfen die Hotkeys Strg-Alt-Esc und Strg-Alt-Rücktaste und Kontextoptionen der Systemleiste. Außerdem gibt es ein neues Speicherlimit.

Wichtige Cinnamon-Einstellungen

Cinnamon bietet zahlreiche Anpassungsmöglichkeiten über die „Systemeinstellungen". Die Desktoperweiterungen, die sogenannten „Cinnamon-Spices" („Desklets", „Erweiterungen", „Applets") werden nachfolgend erklärt. Hier geht es zunächst um die lohnendsten Standardanpassungen:

„Themen" bestimmen das Aussehen entscheidend. Der Unterpunkt „Schreibtisch" legt 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 „Fensterrahmens" für die Titelleisten aller Programmfenster empfehlen wir „Mint-Y-Dark", damit die Titelleisten einen klaren Kontrast zum restlichen Fenster erhalten. Wenn Sie allerdings beim Punkt „Steuerung" eine dunkle Optik wählen, empfiehlt sich umgekehrt ein heller Fensterrahmen. Unter „Themen" die optimale Kombination von Fensterrahmen, Symbolen, Steuerung (Programmoptik) und Schreibtisch (Menü und Leiste) zu finden, ist nicht ganz einfach und mit Experimentieren verbunden. Anfänger und pragmati-

sche Anwender können sich die Aufgabe mit dem „Willkommen“-Assistent (mintwelcome) vereinfachen. Der bietet im ersten Punkt „Schreibtischfarben“ eine simple pauschale Farb- und Themenwahl – inklusive Schalter für helle oder dunkle Anwendungsoptik.

Unter „**Fenster → Titelleiste**“ bestimmen Sie Aussehen und Verhalten der Titelleiste genauer: Die Kontrollelemente (Minimieren, Schließen, Maximieren) können ebenso individuell eingestellt werden wie das Verhalten beim Doppelklick oder Rechtsklick auf der Titelleiste. So kann etwa das Mausrad auf der Titelleiste das Fenster in Stufen transparent schalten („Deckkraft anpassen“).

„Schreibtisch“ ist insofern wichtig, weil Cinnamon hier die Auswahl der Standardsymbole am Desktop anbietet („Papierkorb“, „Netzwerk“, „Eingehängte Datenträger“). Unabhängig von dieser Feineinstellung kann die Drop-down-Liste rechts oben mit „Keine Schreibtischsymbole“ alle Icons am Desktop auch komplett abschalten.

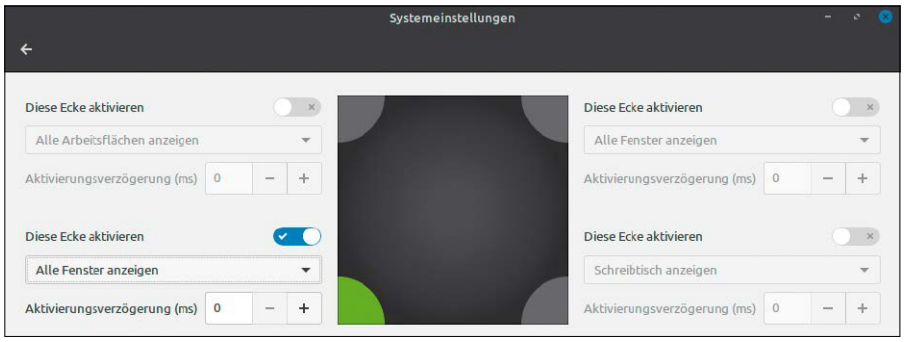
Hintergrundbild: Den Desktophintergrund ändern Sie über „Systemeinstellungen → Hintergrundbilder“, noch einfacher durch Rechtsklick am Desktop und „Hintergrund [...] ändern“. Abgesehen von den mitgelieferten Bildern können Sie mit dem kleinen Plus-Symbol (unten links) einen eigenen Bilderordner eintragen. Die Hintergrundbilder älterer Mint-Versionen sind ebenfalls noch verfügbar. So lädt etwa der Befehl

```
sudo apt install mint-backgrounds-ul*
```

alle Hintergründe der Vorgängerversionen (Ulyssa, Ulyana). Diese werden ordentlich unter „Systemeinstellungen → Hintergrundbilder“ einsortiert.

„Aktive Ecken“ lösen durch Mausbewegung in eine Bildschirmecke eine Desktopaktion oder ein Programm aus. Dosiert an einer oder zwei Ecken genutzt, ist das nützlich. 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“), dann können unten zwei aktive Ecken scharf –›gestellt werden. Als Aktionen bieten „Aktive Ecken“ typische Fensteraktionen wie „Alle Fenster anzeigen“, aber auch die individuelle Option „Einen Befehl ausführen“, den Sie darunter manuell eintragen – etwa „gnome-terminal“.



Mausgeste mit Wirkung: Eine oder zwei „Aktive Ecken“ sind prädestiniert für wichtige Fensteraktionen. Die Ecke sollte keine anderen wichtigen Klickziele enthalten.

Bildschirm und Schriften skalieren

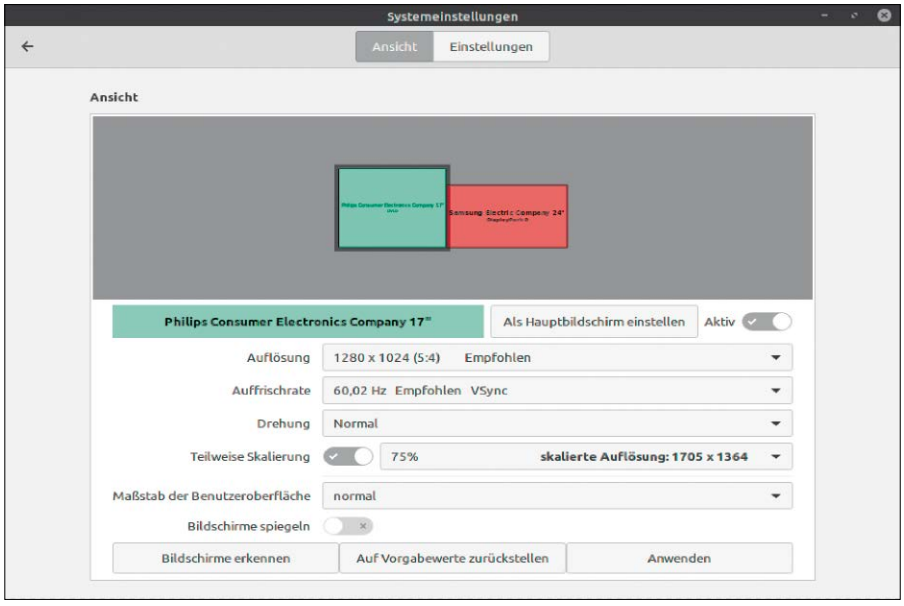
Cinnamon kann die Bildschirmdarstellung optimal anpassen. Unter „Systemeinstellungen → Bildschirm“ gibt es den Punkt „Teilweise Skalierung“, um den Monitor unabhängig von der nativen Auflösung von 75 bis 200 Prozent zu skalieren (in 25-Prozent-Schritten).

Die Option muss aber erst im Register „Einstellungen“ aktiviert werden und ist dort noch als „experimentell“ bewertet. Falls der Monitor nicht mitmacht, bleibt das Feld „Teilweise Skalierung“ einfach inaktiv. Wo fraktionale Skalierung funktioniert, arbeitet sie auch im Multimonitorbetrieb – und dies unabhängig für jeden Monitor.

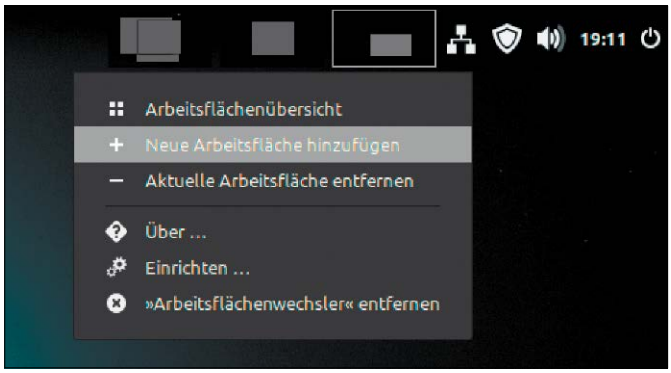
Eine weitere Option der Darstellungsoptimierung ist der „Skalierungsfaktor der Schrift“ unter „Einstellungen → Schriften“. Ein Verändern des Standardwert „1.0“ auf „0,9“ oder „1,1“ beeinflusst Darstellung und Lesbarkeit der Desktopelemente wesentlich. In Kombination mit der fraktionalen Monitorskalierung sollte Cinnamon optimale Lösungen für jede Hardware und für jeden Nutzer bieten.

Arbeiten mit virtuellen Arbeitsflächen

Virtuelle Arbeitsflächen sind umso nützlicher, je kleiner der Bildschirm ausfällt. Das Handling ist unter Cinnamon vorbildlich. Als Standardhotkeys dienen Strg-Alt-Cursor rechts/links zum Wechsel und Strg-Alt-Cursor-oben zur Übersicht. Die zusätzlich ge-



Die fraktionale Monitorskalierung (mit „teilweise“ unglücklich übersetzt) ist noch relativ neu und in den Systemeinstellungen als „experimentell“ eingestuft.



Virtuelle Desktops: Die gewünschte Anzahl richten Sie im optionalen Leistenapplet „Arbeitsflächenumschalter“ oder in der Arbeitsflächenübersicht ein (Strg-Alt-Cursor-oben).

drückte Umschalt-Taste verschiebt das aktuelle Programmfenster auf die nächste Arbeitsfläche. Jeder Desktopwechsel wird durch einen dezenten Systemklang und eine kurze Anzeige von „Arbeitsfläche [n]“ signalisiert. Zusätzlich gibt es das optionale Applet „Arbeitsflächenwechsler“, das per Klick auf eines der vier kleinen Fenster in der Systemleiste zur betreffenden Arbeitsfläche wechselt. Mit etwas Vorbereitung geht alles auch komplett mit der Maus: Wenn Sie in den Systemeinstellungen eine „Aktive Ecke“ scharf schalten und dieser die Aktion „Alle Arbeitsflächen anzeigen“ zuweisen, erhalten Sie mit dieser Mausaktion immer alle virtuellen Desktops. Anwendungsfenster lassen sich per Drag & Drop auf andere Desktops verschieben.

Die Anzahl der virtuellen Desktops können Sie in der Arbeitsflächenübersicht (Strg-Alt-Cursor-oben) veringern oder erhöhen – durch Schließen eines Desktops (rotes „X“) 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 („Neue Arbeitsfläche hinzufügen“ beziehungsweise „Aktuelle Arbeitsfläche entfernen“).

Spices (1): Desklets sind out!

Cinnamon kennt keine Einschränkungen, den Desktop als Dateiablage, Programmstarter oder Infofläche zu nutzen. Das ist gut, die Spices-Kategorie „Desklets“ allerdings nicht mehr zeitgemäß. Die brauchbarsten Desklets „Digitaler Bilderrahmen“ für eine kleine Diashow und das „Uhr-Desklet“ hat Mint standardmäßig an Bord. Sie müssen in den „Systemeinstellungen“ nur aktiviert und konfiguriert werden (Rechtsklick und „Einrichten“). Als direktester Weg führt auch der Rechtsklick am Desktop und „Desklets hinzufügen“ an dieses Ziel. Unter den nachladbaren Desklets werden Sie aber kaum ein Exemplar finden, das sich nicht effizienter als Leistenapplet oder als Hotkey realisieren ließe.

Spices (2): Interessante „Erweiterungen“

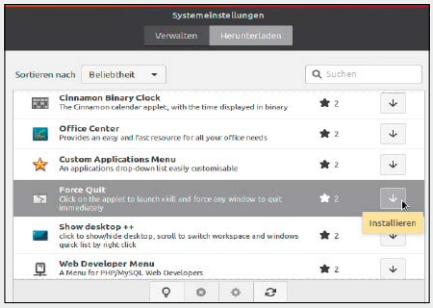
Die Spices-Kategorie unter „Einstellungen → Erweiterungen“ bietet hauptsächlich optische Ergänzungen wie „Desktop Cube“ oder „Opacify Windows“. Unterm Strich sind „Erweiterungen“ marginal, aber es gibt Ausnahmen. Folgende Erweiterungen sind ohne Einschränkung zu empfehlen:

„Transparent Panels“ ist unter den Erweiterungen auf Platz eins der Beliebtheitssortierung und längst überfällig für eine Integration in Cinnamon. Die monofunktionale Erweiterung tut nicht mehr, als der Name sagt: Sie macht die Systemleiste(n) transparent – auf Wunsch mit Schattenwurf, um die Leiste optisch ein wenig vom Hintergrundbild abzuheben.

Die Erweiterung **„Smart Panel“** ist komplizierter und erlaubt Komfortklicks für die primäre Cinnamon-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. Die Option „Run 1st

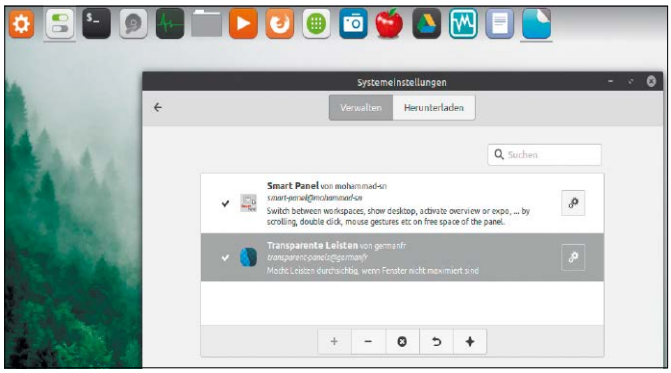
SPICES: EXTERNE CINNAMON-GEWÜRZE

Cinnamon kann durch Spices („Gewürze“) verändert und erweitert werden. Die Sammelstelle lautet *https://cinnamon-spices.linuxmint.com*. Im Prinzip können Sie alle Spices dort beziehen und in jene Ordner entpacken, wie es die Webseite beschreibt. Der einfachere Weg führt aber über die „Systemeinstellungen“. Die Spices unterteilen sich in vier Kategorien – „Themen“ (Optik), „Applets“ (für die Systemleiste), „Desklets“ (Desktopgadgets) und „Erweiterungen“. Ihr Wert reicht von unentbehrlich über nützlich bis marginal. Wenn Sie in den Systemeinstellungen einen der Unterpunkte „Applets“, „Desklets“, „Erweiterungen“ wählen, zeigt das Register „Verwalten“ die auf dem System vorhandenen Spices, die Sie unten mit Plus- oder Minus-Taste aktivieren oder abschalten könnten. Spices, die nicht zum Systemstandard gehören, lassen sich durch das Löschsymbol auch ganz entfernen. Das Zahnradsymbol neben vielen Spices bietet weitere Feineinstellungen.



Spices nachladen: Ob Theme, Applet, Desklet oder Erweiterung – Sie gehen auf das Register „Herunterladen“, holen das Desktoptool ab und aktivieren es dann unter „Verwalten“.

Weitere Spices aus dem Web beziehen Sie über das Register „Herunterladen“ (für „Themen“ das Register „Hinzufügen/Entfernen“). Sobald Sie ein Modul durch Klick auf das Pfeil-Symbol geladen haben, erscheint es in der Liste unter „Verwalten“ und kann dann aktiviert werden.



Durchsichtige Systemleiste(n): Für diesen Effekt benötigt Cinnamon die Erweiterung „Transparent Panels“.

Custom Command“ wird dann jenes Programm starten, das unter „Custom Commands“ eingetragen ist.

Spices (3): Die Applets der Systemleiste

Das Angebot der Systemleiste wird durch modulare Applets geregelt, die sich anpassen, erweitern und reduzieren lassen. Selbst das Hauptmenü ist ein Applet, das sich auch abschalten lässt. Einige Grundeinstellungen gibt es beim Rechtsklick auf die Leiste über die Option „Leisteneinstellungen“. Die derzeit aktiven und sonstigen verfügbaren Applets verwalten Sie am besten in der Übersicht „Systemeinstellungen → Applets“. Positionell verschieben lassen sich die Applets aber nur, wenn Sie nach Rechtsklick auf die Leiste den „Leistenbearbeitungsmodus“ aktivieren.

Applets ein- und ausschalten: Nach Rechtsklick auf eine freie Stelle in der Leiste erhalten Sie die Option „Applets zur Leiste hinzufügen“ (das entspricht dem Gang zu „Systemeinstellungen → Applets“). Die aktiven Applets zeigen ein Häkchen. Mit der Minus-Schaltfläche schalten Sie das Element ab, mit der Plus-Schaltfläche ein.

Applet-Konfiguration: Die allermeisten Applets bieten eine eigene kleine Konfiguration („Einrichten“ oder „Einstellungen“). So lohnen etwa das Hauptmenü- oder das Klangapplet in jedem Fall einen Besuch des Einrichtungsdialogs.

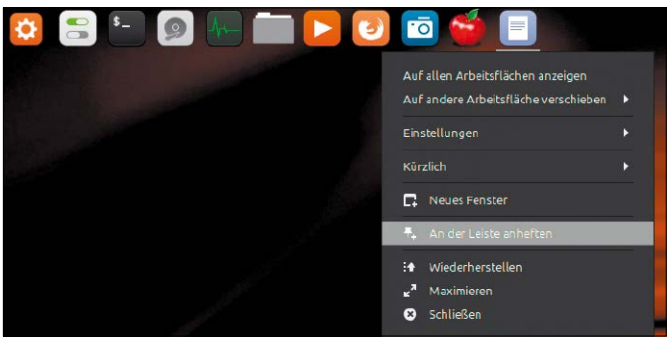
Applet-Empfehlungen: Unentbehrlich sind die Applets „Menü“ und eine „Fensterliste“ – vorzugsweise die „Gruppierte Fensterliste“. Typischerweise sollten auch „Klang“, „Netzwerkverwaltung“, „Kalender“ und „Meldungen“ nicht fehlen. Alles Weitere ist geräteabhängig, nutzungsspezifisch oder optional: Applets wie „Places“ oder „Places Center“ erlauben den Sofortzugriff auf lokale Datenträger und Netzwerkfreigaben. Am umfassendsten ist „Places Center“, das erst mit „Herunterladen“ nachinstalliert werden muss.

Das Applet „Gruppierte Fensterliste“: Dieses Leistenapplet 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 (ohne „Leistenbearbeitungsmodus“) einfach mit der Maus ändern.

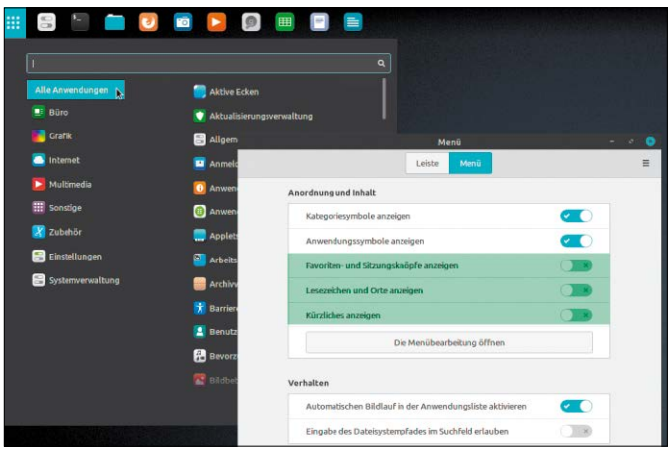
Das Applet bietet nach Rechtsklick und „Einstellungen → Einrichten“ zahlreiche Optionen auf vier Registerkarten. Hier geht es zum einen darum, wie gestartete Programme in der Fensterliste repräsentiert werden sollen (nur Icon? Name?), um die Gruppierung zusammengehöriger Fenster (etwa beim Dateimanager), zum anderen um die Darstellung von statischen Programmfavoriten. Durch Mouse-over kann man Vorschaubilder in einstellbarer Größe und Anordnung einblenden.

Das Menü-Applet: Das Startmenü zeigt eine nach Kategorien sortierte Programmübersicht, ein Instant-Search-Feld zur Suche, Programmfavoriten („Favoriten“) und Schalter zum Abschalten oder Abmelden. Aber das Cinnamon-Startmenü kann komplett umgebaut werden, auch Favoriten oder Shutdown-Schalter sind optional. Nach Rechtsklick auf das Menüsymbol und „Einrichten“ gibt es eine Reihe von Basiseinstellungen, welche Elemente das Menü anzeigen soll.

So lässt sich die Option „Favoriten und Beendenoptionen anzeigen“ abschalten, um das Menü zu verkleinern. Neben „Symbol“ und „Text“ können Sie den Menünamen („Menü“) und das Symbol des Menüs nach Belieben ändern. ■



„Gruppierte Fensterliste“: Das Leistenapplet ist komplex (siehe „Einstellungen“), das dauerhafte Anheften (oder wieder entfernen) von Programmen aber ganz bequem via Kontextmenü.



Abgespecktes Menü: Wenn andere Applets die Rolle übernehmen, kann das Hauptmenü Angebote wie „Favoriten“ oder die Beenden-Optionen ausblenden.

Speedtipps für Linux Mint

Wie bei jedem Betriebssystem gibt es auch bei Linux Mint Optionen, die das System beschleunigen und die Benutzung effizienter machen. In diesem Artikel geht es um systemnahe Leistungstipps.

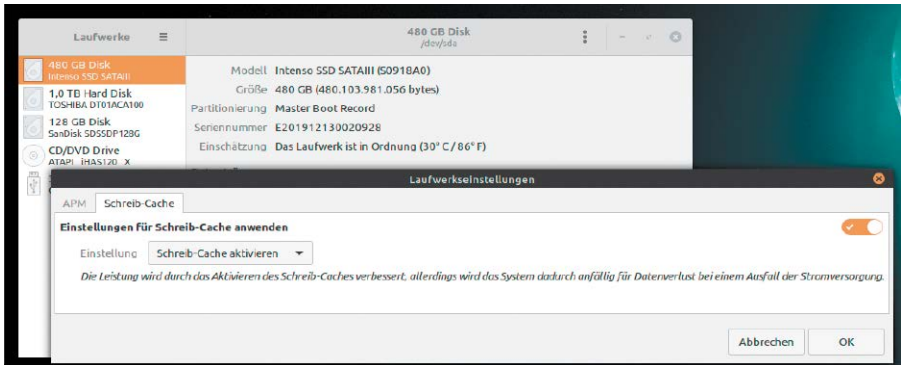
VON HERMANN APFELBÖCK

Wenn Linux Mint auf einigermaßen aktuelle Hardware trifft, ist die Distribution bereits nach der Standardinstallation überzeugend schnell. Mit den nachfolgenden Tipps gewinnen Sie aber noch ein Stück Leistung hinzu. Dabei bleiben Mint-spezifische Speedtipps allerdings rar: Die wirksamsten Maßnahmen gelten allgemein für Ubuntu- oder sogar für alle Linux-Systeme.

Allgemeines Mint-Tuning

Auf die Vorzüge schneller Update- und Softwaredownloads dank optimaler Spiegelserver haben wir an früherer Stelle hingewiesen. Eine weitere Standardpflicht ist der Gang in die „Systemeinstellungen“ und zur „Treiberverwaltung“. Für Grafikkarten und WLAN-Chips bieten nämlich die mitgelieferten Open-Source-Treiber nicht die optimale Leistung. Wenn Sie den Punkt „Treiberverwaltung“ starten, beginnt automatisch eine Treibersuche. Wird ein passender Treiber gefunden, können Sie diesen nachinstallieren. Die Durchsicht der Datenträger unter „Laufwerke“ (Gnome-Disks) kann einen erheblichen Mangel offenbaren: Klicken Sie jedes Laufwerk an und kontrollieren Sie über das „Punkte“-Menü und den Eintrag „Laufwerkseinstellungen“, ob der „Schreib-Cache“ aktiviert ist.

Eine grundsätzliche Überlegung gilt der Wahl der kleineren XFCE- oder Mate-Edition. Ein Boost ist davon aber nicht zu erwarten: Beim Booten erzielen XFCE wie Mate nur einen marginalen Vorsprung von ein bis zwei Sekunden. Das sollte niemanden vom attraktiveren Cinnamon abhalten.



Schneller Schreibcache: Diese wichtige Leistungsoption aktivieren Sie mit Gnome-Disks („Laufwerke“) je Datenträger mit einem Mausklick.

Ebenfalls gleichauf liegen XFCE und Mate beim RAM-Bedarf (etwa 580 MB) gegenüber etwa 730 MB bei Cinnamon – auch dies ist wohl kein ernstes Argument gegen Cinnamon.

Marginal bleibt der unausrottbare Tipp für Cinnamon, unter „Systemeinstellungen → Effekte“ die Effekte abzuschalten. Das mag etwas Ressourcen einsparen, aber nicht den Desktop nennenswert beschleunigen, da alle voreingestellten Effekte in 100 bis 200 Millisekunden ablaufen. Gefühlt machen solche Fenstereffekte beim Minimieren oder Wiederherstellen den Desktop sogar flüssiger. Manuelle Experimente unter „Systemeinstellungen → Effekte → Anpassen“ mit erhöhter Effektdauer können die Fensteraktionen aber tatsächlich bremsen, falls Sie mit Werten jenseits von 400, 500 Millisekunden hantieren.

Softwarebeschleunigung durch Preload

Preload beschleunigt den Start von Software, die Sie häufig verwenden oder sogar per Autostart laden. Der Dienst protokolliert die Programmfavoriten und lädt deren Standardkomponenten vorab in den Speicher. Preload ist vor allem ein Kandidat für mechanische Festplatten, wo mindestens 15 und bis zu 50 Prozent Startbeschleunigung der Programmfavoriten zu erreichen sind. Preload ist mit

```
sudo apt install preload
```

schnell nachinstalliert und dann sofort aktiv (siehe *systemctl --type=service*).

Swapping ausschalten oder anpassen

Swapping, das Auslagern länger ungenutzter Speicherseiten vom RAM auf Festplatte, ist ein Relikt der 90er-Jahre, als RAM notorisch knapp war. Bei heutigen acht oder 16 GB zeigt die Beobachtung der Swapaktivität im Taskmanager praktisch durchgehend, dass kein Swapping stattfindet. Folglich können Sie die Swapdatei dort abschalten. Die Terminalbefehle

```
sudo swapoff /swapfile
sudo rm /swapfile
```

beenden die Auslagerung und löschen die Auslagerungsdatei. Zuletzt deaktivieren Sie in der Datei „/etc/fstab“ die Zeile

```
/swapfile [...]
```

durch ein Kommentarzeichen „#“.

Für den seltenen Fall, dass der Taskmanager aktives Swapping meldet, sollten Sie dem Kernel das Swapping erlauben – aber auch dann gibt es Optimierungschancen. Wie aktiv der Kernel auslagert, steuert der Parameter „Swappiness“, dessen aktuellen Wert Sie mit

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

ermitteln (Standard ist „60“). Je höher der Wert (von „0“ bis „100“), desto aggressiver schreibt der Kernel in die Swapdatei. Die Anpassung lohnt sich aber nur in extremen Hardwaresituationen: Viel RAM bei langsamer Festplatte legen es nahe, Swapping zu reduzieren – etwa auf „10“. Bei wenig RAM und schneller SSD empfiehlt sich ein hoher Wert wie „90“:

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

Dauerhaft gilt der Swappiness-Wert erst, wenn Sie die Datei „/etc/sysctl.conf“ bearbeiten:

```
sudo nano /etc/sysctl.conf
```

Vermutlich fehlt der Eintrag „vm.swappiness“ noch – dann fügen Sie folgende Zeile einfach am Ende hinzu:

```
vm.swappiness=90
```

Tipp für Systembastler: Der Befehl *sysctl -a* listet Kernelparameter auf, die man mit dem Tool sysctl oder in der Systemdatei „/etc/sysctl.conf“ manipulieren kann. Das Anpassen des Swappiness-Werts ist ein Beispiel für die allgemeine Vorgehensweise.

Festplattenaktivitäten auf Ext4

Das Standarddateisystem Ext4 bietet für Festplatten viele Optionen über den Befehl tune2fs, die zum Teil mit eingehängten, oft nur mit ausgehängten Datenträgern funktionieren. Eine Übersicht für eine Festplatte erhalten Sie mit diesem Befehl:

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

Folgendes Beispiel reduziert die Datenträgerchecks:

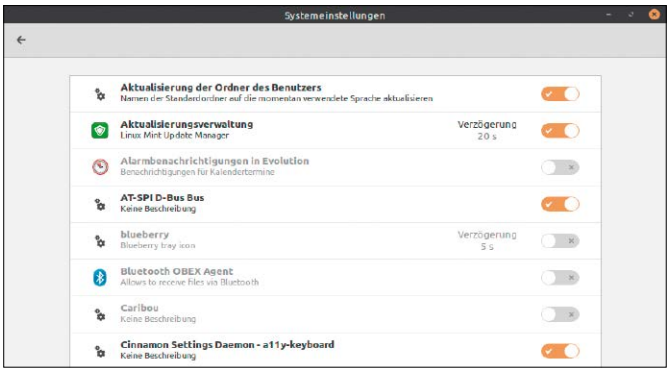
```
sudo tune2fs -i60 -c100 /dev/sda
```

Ein Festplattencheck wird dann nur noch alle 60 Tage („-i60“) oder nach 100 Reboots („-c100“) erfolgen – je nachdem, welches Ereignis früher eintritt.

Ein weiteres Beispiel ist das Abschalten der Journalingfunktion. Journaling dient zur Wiederherstellung von Dateien nach Abstürzen und ist auf der Systempartition



Festplattenchecks reduzieren: Das Tool tune2fs kann mit zahlreichen Optionen die Schreib- und Kontrollaktivitäten von Ext4-Datenträgern beeinflussen.



Alle Autostarts: „Startprogramme“ zeigt die ganze Menge der Komponenten erst an, wenn die Anweisung „NoDisplay“ in den Konfigurationsdateien abgeschaltet haben.

wünschenswert. Auf USB oder reinen Datenpartitionen verursacht diese Funktion nur unnötigen Schreibaufwand:

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

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

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

in der Zeile „Filesystem features“ überzeugen können. Umgekehrt lässt sich das Journaling so wieder aktivieren:

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

Autostarts ausmisten

Desktops wie Cinnamon laden zahlreiche Programme bei der Anmeldung. Das Abschalten solcher Autostarts über das Tool „Startprogramme“ spart Speicher und beschleunigt den Desktopstart. Wer rigoros ausmisten will, muss aber wissen, dass „Startprogramme“ viele systemnahe Komponenten ausblendet. Dafür sorgt die Anweisungszeile „NoDisplay=true“ in der jeweiligen Desktopdatei. Mit

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

schalten Sie die Anweisung in allen Startern ab. Damit werden unter „Startprogramme“ alle Autostarts sichtbar und können deaktiviert werden. Theoretisch können Sie außer D-Bus, X-Settings-Plug-in, Automount und den Sicherheitsdienst alles abschalten. Aber es ist Ermessensfrage, worauf Sie tatsächlich verzichten können: Ohne „Pulseaudio“ ist nur ein Audiostrom möglich, ohne Erinnerungen der „Aktualisierungsverwaltung“ müssen Sie selbst an die Updates denken.

Systemdienste abschalten

Jedes Linux lädt Dienste, die längst nicht jeder benötigt. Das Abschalten von Diensten ist aber eine Wissenschaft für sich – mit unkalkulierbaren Folgen, wenn der Benutzer nicht kompetent ist. Einblick in die aktiven Dienste erhalten Sie im Terminal:

```
systemctl --type=service
```

Systemdienste sind keine Bremsen. Das können Sie mit

```
systemd-analyze blame
```

kontrollieren, der die Ladezeiten absteigend (längste bis kürzeste) auflistet. Trotzdem können Sie unnötige Dienste abschalten (Beispiel):

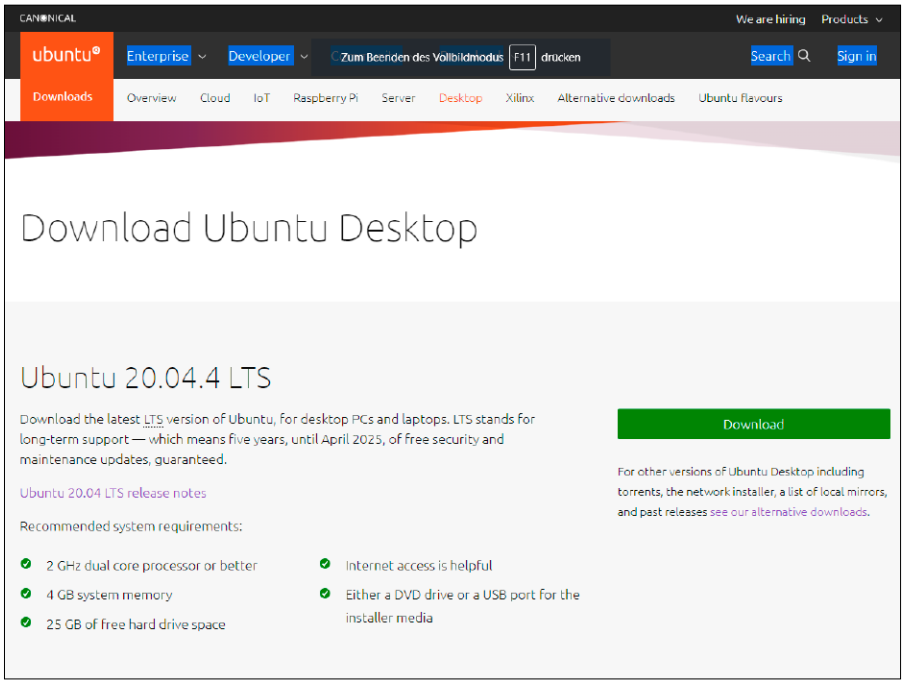
```
sudo systemctl stop avahi-daemon.
  service
sudo systemctl disable avahi-
  daemon.service
```

Diese Befehle stoppen den angegebenen Netzwerkdienst und deaktivieren ihn dauerhaft. Mit den Parametern „enable“ und „start“ wäre er wieder zu aktivieren. ■

Point Releases und neue Kernel

Mit einem möglichst aktuellen Installationsmedium vermeiden Sie bei einer Neuinstallation umfangreiche Updates. Zumindest der Linux-Kernel lässt sich aber auch bei einem installierten System außerhalb der Reihe aktualisieren.

VON THORSTEN EGGELING



Neueste Version: Wer die Desktopausgabe von Ubuntu herunterlädt, erhält Version 20.04.1. Die ist etwas aktueller als die erste Version vom April 2020, enthält aber noch keinen neuen Kernel.

Die langlebigen LTS-Versionen von Ubuntu und Linux Mint versprechen einen sorglosen Betrieb über mehrere Jahre. Wer allerdings eine LTS-Distribution ein oder zwei Jahre nach dem ursprünglichen Erscheinungsdatum neu installiert, muss zahlreiche Updates herunterladen, bevor er das System sicher nutzen kann. Um das zu vermeiden, stellen die Distributoren in unregelmäßigen Abständen aktualisierte Installationsmedien bereit. Die Bezeichnung enthält eine zusätzliche Nummer nach der Hauptversion. Aus Ubuntu 20.04 wird dann beispielsweise Ubuntu 20.04.1, auch erstes „Point Release“ genannt. Um nicht mehrere Versionen pflegen zu müssen, wird auch bei bestehenden Installation die Versionsnummer durch die standardmäßigen Updates angehoben. Es gibt allerdings bei einigen Komponenten Unterschiede zwischen Neuinstallation und Update.

1. Point Releases und neue Kernel für Ubuntu

Mit jedem neuen Linux-Kernel wird die Hardwareunterstützung ausgebaut oder verbessert. Bei einer funktionierenden Linux-Installation auf unveränderter Hardware gibt es keinen ernsthaften Grund, auf einen neuen Kernel umzusteigen. Anders sieht es aus, wenn neue Hardware dazukommt, die vom bisherigen Kernel nicht oder nur unzureichend unterstützt wird. Manchmal ist auch für neue Software ein neuerer Kernel Voraussetzung, wenn diese ein bestimmtes Kernel-Modul erfordert oder erstellen will.

Damit Nutzer nicht auf die nächste Hauptversion der Distribution warten müssen, installiert ein Point Release von Ubuntu-Desktop automatisch einen neueren Kernel als in der ursprünglichen Version.

Teilweise gibt es zusätzlich aktuellere Versionen des X-Servers und einiger Grafikbibliotheken, wenn das im Zusammenspiel mit dem neuen Kernel nötig ist. Die Entwickler bezeichnen das als LTS Enablement Stack-Support oder HWE (Hardware Enablement).

Wer auf seinem Rechner im April 2020 Ubuntu 20.04 LTS installiert hat, ist inzwischen durch Updates bei Version 20.04.02 LTS angelangt. Der Kernel trägt die Versionsnummer 4.13. Ein Anhängsel wie „-122“ oder ähnlich deutet auf einige Sicherheitsupdates hin. Welche Kernel-Version das System aktuell verwendet, finden Sie im Terminal mit

```
uname -a
```

heraus. Mit

```
lsb_release -a
```

ermitteln Sie die genaue Version des Betriebssystems.

2. Point Releases und Kernel für Linux Mint

Auch die Entwickler von Linux Mint geben Point Releases heraus. Linux Mint 19 beispielsweise basiert auf Ubuntu 18.04. danach folgten Linux Mint 19.1, 19.2 und 19.3.

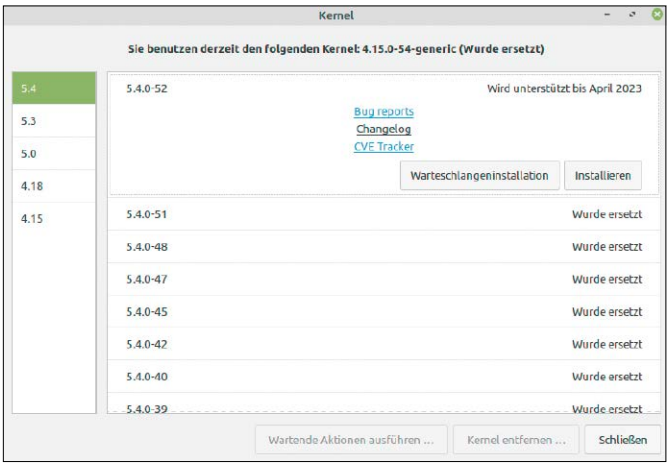
Datum der Veröffentlichung und Versionsnummer stimmen nicht mit Ubuntu überein. Anders als bei Ubuntu ändern die regulären Updates nichts an der Versionsnummer vor dem Punkt. Der Kernel wird über *sudo apt upgrade* ebenfalls nicht automatisch aktualisiert.

War ursprünglich beispielsweise Linux Mint 20.2 installiert, bleibt es dabei. Das wird auch dadurch deutlich, dass die Point Releases eigene Codenamen tragen: Ulyana, Ulyssa, Uma, Una. Aus Sicht der Mint-Entwickler scheinen auch Zwischenversionen den Status einer neuen Ausgabe der Distribution zu besitzen.

Wer auf ein Point Release updaten möchte, muss das manuell einleiten. Dazu geht man über das Menü auf „Systemverwaltung → Aktualisierungsverwaltung“ und dann auf „Bearbeiten“. Im Menü erscheint beispielsweise „System aktualisieren auf ‚Linux Mint 20.3 Una‘“. Diese Aktualisierung wird auch Voraussetzung für das erwartete Upgrade auf Linux Mint 21 sein.



Point Release für Linux Mint: Die Installation neuer Versionen erfolgt nicht automatisch, lässt sich aber über die „Aktualisierungsverwaltung“ manuell anstoßen.



Kernel für Linux Mint: Neue Kernel bietet das System in einem eigenen Fenster zur Installation an, weist aber darauf hin, dass Probleme mit zusätzlichen Treibern auftreten können.

3. Kernel bei Ubuntu aktualisieren

Wird eine Hardware vom installierten Kernel nicht unterstützt, kann man eine neuere Kernel-Version ausprobieren. Die Installation ist in der Regel unproblematisch, weil das System bei Fehlfunktionen jederzeit wieder mit dem älteren Kernel booten kann. Zur Installation des HWE-Kernels starten Sie bei Ubuntu 18.04 im Terminal

```
sudo apt-get install --install-
  recommends linux-generic-
  hwe-18.04 xserver-xorg-hwe-18.04
```

Der Kernel des letzten Point Release entspricht dem der nächsten LTS-Version. Die Kernel von Ubuntu 18.04.05 und 20.04 waren daher im April 2020 identisch (5.4.0-52). Mit weiteren Point Releases für Ubuntu 20.04 können Sie auch bei dieser Version den Kernel aktualisieren. Ersetzen Sie dafür in der Befehlszeile „18.04“ jeweils durch „20.04“.

Ubuntu bietet eine weitere Option, um auf einen noch aktuelleren Kernel zu wechseln. Das Paket „linux-generic-hwe-20.04-edge“ bietet eine Vorschau auf den kommenden HWE-Kernel. Bei sehr neuem Kernel ist zu beachten, dass zusätzliche Treiber beispielsweise von Nvidia oder Virtualbox die Version unterstützen müssen. Ansonsten schlägt das Kompilieren fehl und die Hardware lässt sich nicht nutzen. Bei Problemen ruft man das Grub-Bootmenü auf. Sollte es nicht automatisch erscheinen, halten Sie die Umschalt-Taste nach dem Einschalten des PCs gedrückt. Im Menü gehen Sie auf „Erweiterte Optionen für Ubuntu“ und wählen einen älteren Kernel. Danach deinstallieren Sie die neuere Version.

4. Neue Kernel für Linux Mint

Linux Mint bietet etwas mehr Klarheit im Kernel-Wirrwarr. Aktuelle Kernel-Updates zeigt die „Aktualisierungsverwaltung“ an. Wer neuere Kernel benötigt, geht auf „Ansicht → Linux-Kernel“. Man erhält zuerst eine Warnung, dass ein neuer Kernel zu Problemen führen kann.

Eine Anleitung, wie sich das Problem über das Grub-Bootmenü beheben lässt (siehe Punkt 3), ist ebenfalls enthalten. Nach einem Klick auf „Fortsetzen“ erscheint ein Fenster, über das sich der gewünschte Kernel auswählen lässt.

Bei jedem Eintrag gibt es Links zu „Bug reports“ und „Changelog“, die über Fehler und Neuerungen informieren. ■

EXPERIMENTELLE KERNEL INSTALLIEREN

Traditionell kompiliert man experimentelle Kernel selbst, was aber sehr zeitaufwendig ist. Einfacher geht es über Downloads von *https://kernel.ubuntu.com/~kernel-ppa/mainline*. Bei Redaktionsschluss waren hier Kernel bis Version 5.17 als DEB-Pakete zu finden. Für ein 64-Bit-System laden Sie unter „amd64“ alle Pakete herunter, die „generic“ enthalten, und die Datei mit der Endung „all.deb“. Im Terminal erfolgt die Installation im Downloadverzeichnis per

```
sudo dpkg -i *.deb
```

Bitte beachten Sie, dass bei sehr neuem Kernel die Wahrscheinlichkeit geringer ist, dass sich damit zusätzliche Treiber kompilieren lassen.

Für mehr Komfort kann man über *https://github.com/teejee2008/ukuu/releases* das DEB-Paket für das Tool Ukuu herunterladen und installieren. Es ermöglicht die einfache Installation und Deinstallation der Kernel von *https://kernel.ubuntu.com* in Ubuntu und Linux Mint.

Reparatur- und Spezialsysteme

Der wichtigste Unterschied zwischen Allzweck-Livesystemen und Spezialsystemen ist die Auswahl der angebotenen Software. Spezialsysteme liefern eng fokussierte Werkzeuge oder konzentrieren sich sogar auf eine einzige Aufgabe.

VON HERMANN APFELBÖCK

Die meisten Linux-Desktops kommen als Livesysteme und können auf die Festplatte eines havarierten Linux, Windows oder Mac-OS zugreifen. Das erlaubt mit jedem Live-Ubuntu die Rettung von Dateien durch Kopie auf unabhängige Laufwerke, das Editieren fehlerhafter Konfigurationsdateien oder das Verkleinern der Systempartition mit Gparted. Da Livesysteme zudem eine temporäre Installation zusätzlicher Programme erlauben, wird im Prinzip jedes Livesystem zum Reparatursystem. Dennoch ist der Wert der nachfolgend vorgestellten Spezialsysteme unbestritten: Einige dieser Experten machen ihren Job einfach unschlagbar gut, andere haben ihren Wert als kompetente Toolsammlung, die viel manuelle Arbeit erspart.



Zweitsystem und Reparatursystem in einem: Das LinuxWelt-Rettungssystem hat Spezialtools zur Datenrettung an Bord, taugt aber auch als mobiles Surfsystem.

LinuxWelt-Rettungssystem: Linux für Linux

Das neue Notfall- und Rettungssystem (64 Bit) der LinuxWelt-Redaktion basiert auf Porteus und genügt im Prinzip auch als allgemeines Surf- und Zweitsystem. Der Mate-Desktop, Browser und die meisten Programme liegen in deutscher Sprache vor. Der Standardbenutzer „guest" hat das Passwort „guest". Dieses wird etwa zur Rückkehr vom Bildschirmschoner zum Desktop abgefragt. Das root-Passwort lautet „toor". Im Fokus stehen aber Datenrettungstools wie Testdisk, Photorec und Ext4magic zur Wiederherstellung gelöschter Dateien, der Partitionierer Gparted, der Verschlüsseler Veracrypt und das Klonprogramm Clonezilla. Kleinere Tools wie der Portscanner Nmap und das Rettungstool ddrescue zum Erstellen von Datenträgerabbildern ergänzen das System. Auf Basis der enthaltenen NTFS-Treiber kann der Dateimanager auch Windows-Partitionen bearbeiten.

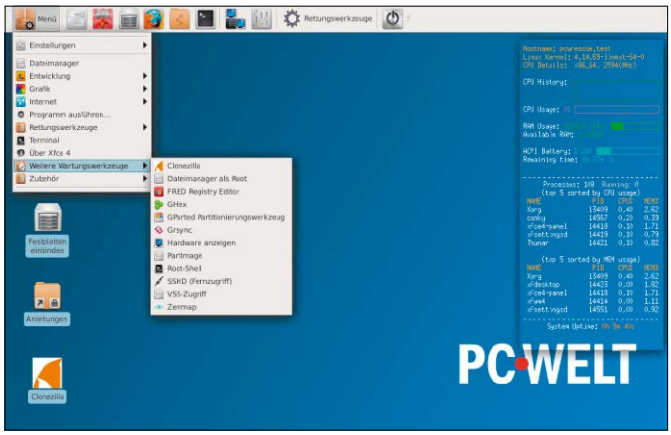
Bei regelmäßiger Nutzung des Systems empfiehlt sich eine Übertragung auf USB-Stick mit FAT32-Dateisystem. Mit einer einfachen Kopie des ISO-Images (dd, Gnome-Disks, Win 32 Disk Imager) ist es hier aber nicht getan, weil die Bootumgebung nicht hybrid ist, sondern nur auf CD/DVD bootet. Der Weg führt im Livesystem selbst unter „Anwendungen → Systemwerkzeuge → Bootfähigen USB-Stick erstellen" zum passenden Programm, das aber nach unserer Erfahrung unzuverlässig ist. Besser ist der manuelle Weg: Jedes Linux kann im Dateimanager das ISO-Abbild mounten („Bereitstellen"). Dann kopieren Sie einfach den kompletten Inhalt des ISO-Abbilds (Ordner „boot", „porteus" et cetera) auf den USB-Stick. Um das System bootfähig zu machen, navigieren Sie mit dem Terminal in den Ordner „/boot" (auf dem neuen USB-Stick) und starten mit root-Recht

```
sudo bash Porteus-Installer-for-
  Linux.com
```

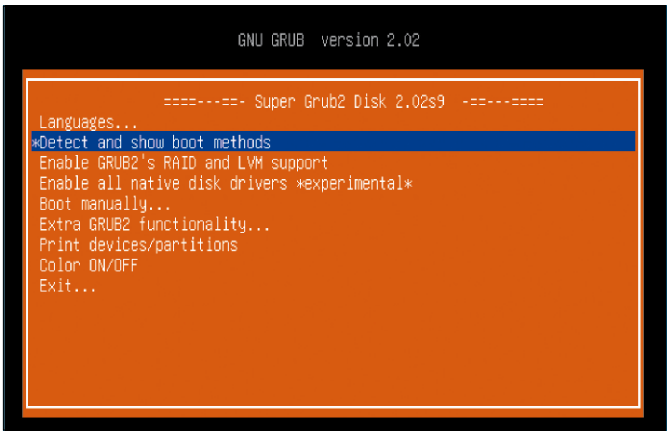
das erforderliche Tool.

PC-WELT-Rettungs-DVD: Linux für Windows

Die PC-WELT-Rettungs-DVD ist ein Livesystem mit speziellen Tools für defektes Windows, kann aber auch als Linux-Helfer eingesetzt werden. Der Browser Firefox sowie Clonezilla und Gparted sorgen für vielseitige Einsatzoptionen. Unter „Rettungswerkzeuge" finden sich dann speziellere Tools, mit denen Sie das Windows-Passwort löschen, Partitionen („Partition retten") oder gelöschte Dateien („QPhotorec") wiederherstellen oder nach Schadsoftware („ClamAV") suchen können. Das Menü „Weitere



Hilfe für Windows: Die PC-Welt-Rettungs-DVD ist auf Windows-Pannen spezialisiert. Sie kann Festplatten klonen, nach Viren suchen und das Kennwort zurücksetzen.



Ist der Bootloader Grub2 defekt oder falsch konfiguriert, booten Sie den PC mit Super Grub2 Disk. Das Tool findet alle Systeme und startet das gewünschte.

Wartungswerkzeuge → Fred Registry Editor" startet einen Registry-Editor, der Werte in der Registry des installierten Windows-Systems ändern kann.

Das Rettungssystem ist am besten auf einem USB-Stick aufgehoben und startet dort deutlich schneller als von DVD. Der Stick lässt sich aus dem laufenden Livesystem erstellen. Dazu gehen Sie im „Menü" auf „Zubehör → Installation auf USB-Laufwerk", wählen das Ziellaufwerk, setzen optional ein Häkchen vor „Verschlüsseltes /home erstellen" und ändern dahinter bei Bedarf die Größe. Danach klicken Sie auf „Installation starten". Sie werden dann beim ersten Start des Systems aufgefordert, ein Passwort für das sicher verschlüsselte Verzeichnis zu vergeben. Wichtige Konfigurationsdaten wie der WLAN-Schlüssel oder in Firefox gespeicherte Passwörter bleiben dann auch nach einem Neustart erhalten.

HDT: Unabhängige Hardware-Inventur

Das Tool HDT (Hardware Detection Tool) verschafft einen umfassenden Überblick zur Hardware eines Computers, auf dem kein funktionierendes Betriebssystem installiert ist. HDT ist aber auch dann vorzuziehen, wenn Sie mit einem Betriebssystem nicht ausreichend vertraut sind, um sich die erforderlichen Hardware-Informationen zu beschaffen.

HDT zeigt alle Informationen zu CPU, Hauptplatine, PCI-Karten, RAM-Speicher, DMI-Geräte, Soundchip, Festplatten und VESA-Fähigkeiten der Grafikkarte. Mit dem Eintrag „Reboot" verlassen Sie das Tool und starten den Rechner neu.

HDT liegt auf jeder LinuxWelt-DVD und startet über „Extras und Tools → Hardware Detection Tool (HDT)" – vorzugsweise im „Menu Mode".

Super Grub2 Disk: Der Notstarter

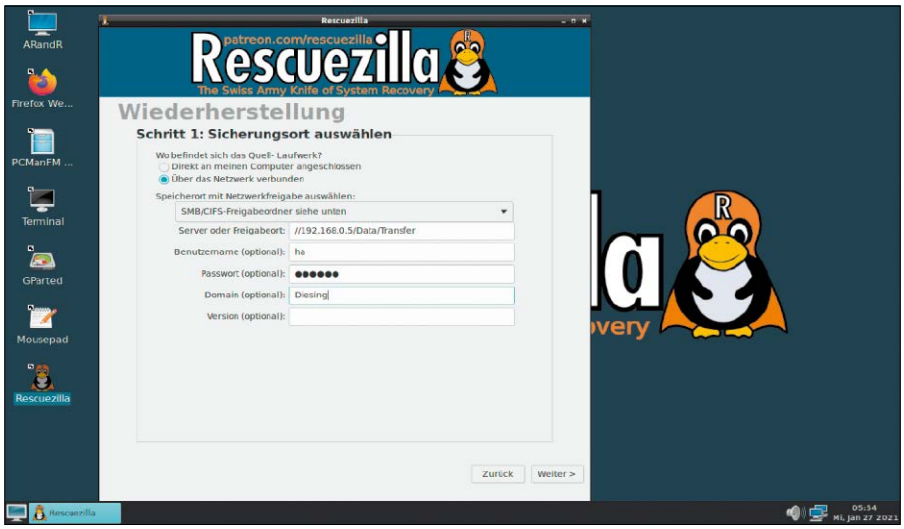
Die Super Grub2 Disk ist ein unentbehrlicher Boothelfer. Für Bootprobleme mit Grub sind meistens fehlerhafte Partitionierungen bei der Installation oder die typische Grub-Entsorgung durch Windows-Installationen verantwortlich. Super Grub2 Disk durchforstet mit der Option „Detect and show boot methods" alle Datenträger nach Linux-Systemen, zeigt danach deren Liste (falls mehrere) und startet das ausgewählte System. Die Reparatur der Grub-Umgebung findet dann typischerweise mit

```
sudo grub-install --recheck /dev/
  sda
sudo update-grub
```

im wiederbelebten System statt. Das bootfähige Super Grub2 Disk hat nur etwa 20 MB Größe und lohnt gewiss keinen eigenen USB-Stick: Das Tool startet standardmäßig von der Heft-DVD unter „Extras und Tools".

LIVESYSTEME: SERVICE & REPARATUR

Name	Aktuell	Webadresse	Download (MB)	Beschreibung
Clonezilla Live	2.7.2	*http://clonezilla.org*	300	Servicesystem zum Klonen von Festplatten/Partitionen
Clu Linux Live	6.0	*https://sourceforge.net/projects/clu-linux-live*	420	Rettungssystem ohne Desktop: Datenrettung via SSH/Samba
Gparted Live	1.3.0	*https://gparted.org/download.php*	390	Livesystem zum Partitionierer Gparted (auf Heft-DVD)
HDT (Hardware Detection Tool)	0.5.2	*www.serverelements.com/?target=Hardware_Detection_Tool*	1	minimales Servicesystem zur Hardwareanalyse (auf Heft-DVD)
Kali Linux	2021.2	*www.kali.org*	3600	Sicherheitssystem mit großem Toolumfang
Kaspersky Rescue Disk	18	*https://support.kaspersky.com/viruses/krd18*	550	Livesystem mit Kaspersky-Virenscanner
LinuxWelt-Rettungssystem	8.1	*www.pcwelt.de/lw-rettungssystem*	700	Rettungssystem für Linux
PC-WELT-Rettungs-DVD	6.4.1	*https://www.pcwelt.de/3890747*	1200	Notfallsystem für Windows-Nutzer mit AV-Scanner
Rescatux	0.73	*https://www.supergrubdisk.org/rescatux/*	700	Reparaturen für den Bootloader Grub 2
Rescuezilla	2.2	*https://rescuezilla.com/*	900	Servicesystem zum Klonen von Festplatten/Partitionen
Super Grub2 Disk	2.04s1	*https://www.supergrubdisk.org/*	20	Notstarter bei defektem Bootloader Grub2 (auf Heft-DVD)
System Rescue CD	8.0.3	*www.system-rescue-cd.org*	710	Rettungssystem mit großer Toolsammlung



Wer damit nicht klont, ist selbst schuld: Rescuezilla macht eine heikle Mission zum lässigen Spaziergang.

Rescatux: Grub-Reparaturen

Rescatux ist ein eng spezialisiertes Rettungssystem, um kaputte und überschriebene Grub-Bootloader von installierten Linux-Systemen wieder flottzumachen. Bei einem Schönheitswettbewerb für Live- und Reparatursysteme hätte Rescatux vermutlich den letzten Platz sicher, aber diese optischen Mängel macht es durch seinen Nutzwert wett. Rescatux stellt defekte Grub-Bootloader wieder her, wenn diese beispielsweise von einer parallelen Windows-Installation überschrieben wurden. Nach dem Booten von Rescatux startet die englischsprachige Reparaturanwendung Rescapp automatisch. Im Menüpunkt „Grub (+)" kann die Reparaturoption „Restore Grub" einen neuen Grub-Bootloader schreiben und dabei alle automatisch erkannten Betriebssysteme (Linux und Windows) in ein neues Bootmenü einbinden. Die Funktion „Update Grub Menus" greift zur Restaurierung der Bootmenüs auf die Konfigurationsdateien des installierten Linux-Systems zurück.

Speziell für Ubuntu-Systeme ist unter „Expert Tools" zudem das Werkzeug „Boot-Repair" vorhanden, das den Bootloader eines Ubuntu-Systems wiederherstellen kann. Im Bootmenü des Hilfssystems steht eine Version für 64 Bit und für 32 Bit zur Auswahl. Diese muss passend zum defekten System ausgewählt werden.

Rescuezilla: Klonen bequem

Zum Klonen von Systempartitionen sind unabhängige Livesysteme wie Rescuezilla (oder Clonezilla) zwingend erforderlich, weil das Kopieren im laufenden System technisch scheitern würde. Rescuezilla ist der Nachfolger des eingestellten Redo Backup. Das ISO-Abbild 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, das auch eine Basisausstattung als Zweitsystem mitbringt (Browser, Gparted). Im Zentrum steht aber das Tool Rescuezilla, das die Imagesicherung und Wiederherstellung mit wenigen Schaltflächen einfach macht. Im Prinzip gibt es nur „Backup" und „Wiederherstellung".

Backup: „Schritt 1" ist die Auswahl des physikalischen Quell-Datenträgers, dessen Partitionen gesichert werden sollen. „Schritt 2" erlaubt die Auswahl der gewünschten Partitionen auf diesem Datenträger – am einfachsten alle angezeigten Partitionen (Standard). In „Schritt 3" markieren Sie das Backupziel. Dabei zeigt die Standardoption „Direkt an meinen Computer angeschlossen" die internen Laufwerke sowie USB-Medien, aber auch Samba-Freigaben sind als Ziel möglich. „Schritt 4" sollten Sie bei der Vorgabe belassen, „Schritt 5" ist lediglich ein aussagekräftiger Sicherungsname.

Wiederherstellung: Hier fragt „Schritt 1" zunächst das Laufwerk ab, wo sich die Sicherung befindet. Wird das Laufwerk korrekt gewählt, zeigt „Schritt 2" die dort vorhandene(n) Imagesicherung(en), und in „Schritt 3" geht es zum Zieldatenträger. Hier dürfen keine Zweifel bestehen, weil Rescuezilla dieses Laufwerk komplett überschreiben wird.

Clonezilla: Der Klon-Meister

Der Downloadbereich *https://clonezilla.org/downloads.php* bietet mehrere Clonezilla-Varianten. Wir empfehlen „alternative stable", die auf Ubuntu basiert. Das Livesystem kann mit den üblichen Mitteln (dd, Gnome-Disks, Etcher, Win 32 Disk Imager) bootfähig auf USB-Stick kopiert werden. Anders als Rescuezilla hat das Livesystem Clonezilla keinen Desktop, sondern fokussiert sich ausschließlich auf seinen Spezialjob. Der im Vergleich zu Rescuezilla relativ unkomfortable Spezialist wird in textbasierten Menüs mit Cursor-, Tabulatortasten und Eingabetaste bedient. Immerhin können Sie nach der ersten Option „Clonezilla live" im Folgefenster „de-DE.UTF" wählen, um Menü und Erklärungen weitestgehend in deutscher Sprache zu erhalten. Im Folgefenster sollten Sie außerdem das Tastaturlayout auf „German" setzen.

Gibt es Gründe, das spröde Clonezilla dem komfortablen Rescuezilla vorzuziehen? Ja, in der Tat: Clonezilla sichert nämlich nicht nur lokal und auf Samba-Freigaben, sondern auch auf SFTP, NFS, oder Webdav. Außerdem können die Sicherungsimages komprimiert und verschlüsselt werden. Diese Eigenschaften machen Clonezilla zum unbestrittenen Klon-Experten für besondere Aufgaben. Überall dort, wo nur ein Systemzustand von Linux oder Windows gesichert werden soll, genügt aber Rescuezilla vollauf.

Clu Linux: Gar nicht so exotisch

Warum sollte man freiwillig ein Live- und Rettungssystem ohne grafischen Desktop benutzen? Clu Linux gibt darauf eine recht clevere Antwort, indem es die Reparaturen ins Netzwerk verlegt. Und das kann dann komfortabler sein als die Datenrettung am lokalen System. Beim Start sind vier Fragen zu beantworten, erstens nach dem (root-) Kennwort, ferner ob alle lokalen Laufwerke gemountet und ob Samba- und SSH-Server aktiviert werden sollen. Diese Entscheidungen sind alles andere als grundlos, denn wenn Sie allem zustimmen, sind sämtliche Laufwerke des darunterliegenden Rechners automatisch im Samba/Windows-Netz und außerdem via SSH/SFTP freigegeben (mit dem angegebenen root-Kennwort und über die IP-Adresse). Clu Linux hat zwar alle typischen Terminalprogramme vorrätig, nicht zuletzt den Midnight Commander, aber die Datenrettung läuft dann viel bequemer mit grafischen Dateimanagern

über Samba oder SSH im Netz. Clu Linux bootet nur von CD/DVD.

Kali Linux: Sicherheits-Checks

Livesysteme, die als Werkzeugkiste zum Thema Sicherheit dienen, sind eine Klasse für sich. Neben **Backbox Linux, Parrot-OS** und dem mittlerweile eingestellten **DEFT** nennen wir hier den renommierten Vertreter **Kali Linux**. Er liefert auf Debian-Basis eine riesige Sammlung spezialisierter Tools. Mit seiner sorgfältigen Zusammenstellung und der ausführlichen Dokumentation unter *https://docs.kali.org* setzt sich Kali Linux von ähnlichen Systemen ab. Der Einstieg in das Thema (Un-)Sicherheit wird damit etwas einfacher, trotzdem ist Kali alles andere als ein Einsteigersystem, sondern vielmehr ein Spezialsystem für Sicherheitsexperten.

Das Livesystem (Variante „Live Boot" unter *www.kali.org/get-kali*) startet in seiner Standardausgabe einen aktuellen englischsprachigen XFCE-Desktop. Falls eine Anmeldung nötig wird, gelingt diese als Benutzer „kali" mit Passwort „kali". Das üppige Menü gliedert die zahlreichen Tools unter Kategorien wie „01 – Information Gatherung" oder „06 – Wireless Attacks". Normale Programme stehen ganz unten als „Usual Applications".

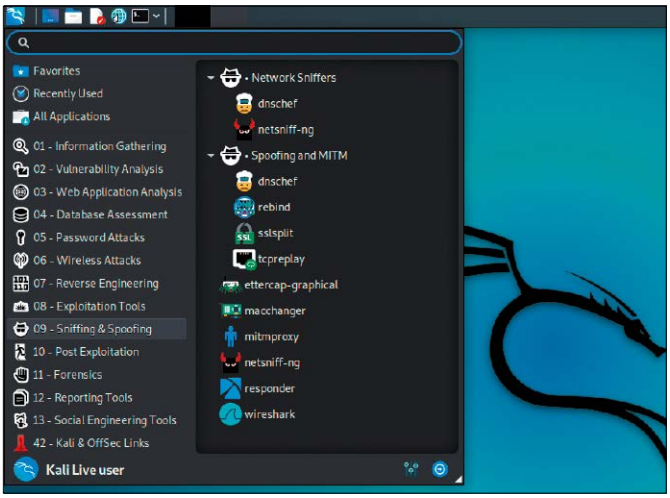
Gparted Live: Unabhängiger Partitionierer

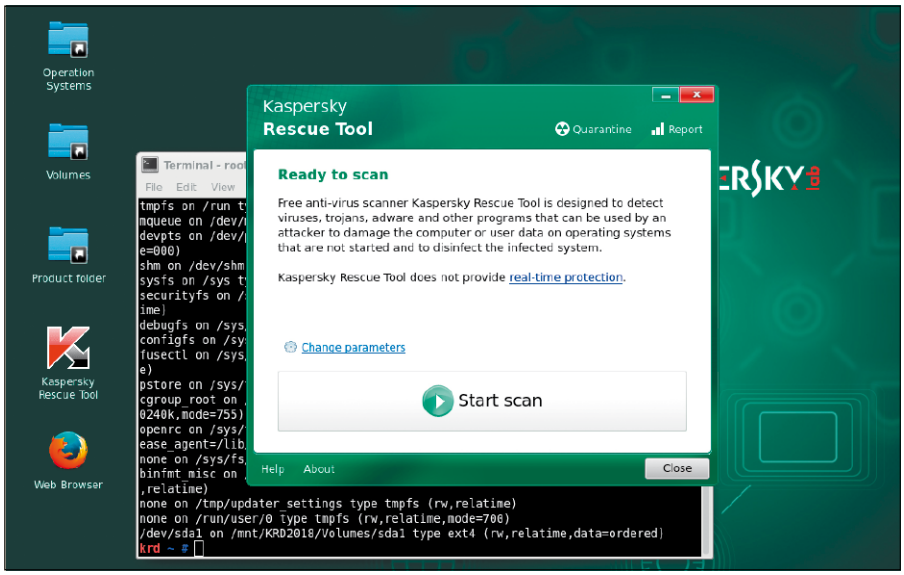
Dias Livesystem der Gparted-Entwickler eignet sich auch für Windows-Anwender. Gparted Live enthält stets den Partitionierer Gparted in der neuesten Version – und nicht viel mehr. Der Klassiker eignet sich bestens zur Neupartitionierung, Partitionsänderung und Formatierung und unterstützt dabei eine grandiose Anzahl von Dateisystemen und Partitionstabellen aus dem Umfeld von Linux, Unix, Apple und Windows. Im Prinzip ist Gparted alles andere als rar und befindet sich im Repertoire vieler Livesysteme wie etwa auch im Linux-Welt-Rettungssystem. In Gparted Live liegt es aber stets in aktueller Version vor und lädt gleich nach dem Start.

System Rescue CD: Reparatur-Klassiker

System Rescue CD bringt alles mit, was fortgeschrittene Anwender benötigen, um Daten von einem defekten Computer zu kratzen oder liegengebliebene Linux-Systeme flottzumachen. Das System ist äußerst anspruchslos und läuft auch auf alter Hardware. Automatisch als root angemeldet arbeiten Sie auf einem englischsprachigen Desktop, jedoch ist immerhin das deutsche Tastaturlayout voreingestellt. Das Gentoo-basierte Linux mit XFCE-Oberfläche bietet in einem gut sortieren Startmenü vorrangig Kommandozeilenprogramme. Zum Umfang gehören aber auch Photorec und Testdisk zur Datenrettung, der „Hardware Lister" zur Rechnerinspektion, der Partitionierer Gparted, Text- und Hex-Editoren sowie der Browser. Für die Arbeit mit Dateien gibt es einen klassischen Zwei-Fenster-Dateimanager.

Werkzeuge für Sicherheitsprofis: Kali Linux ist eine Sammlung und Startrampe für zahlreiche Spezialprogramme, die Systemschwächen und Sicherheitslücken entlarven.





Live-Virenscanner: Linux-basierte, unabhängige gestartete Scanner wie hier Kaspersky Rescue Disk richten sich hauptsächlich an Windows-Anwender.

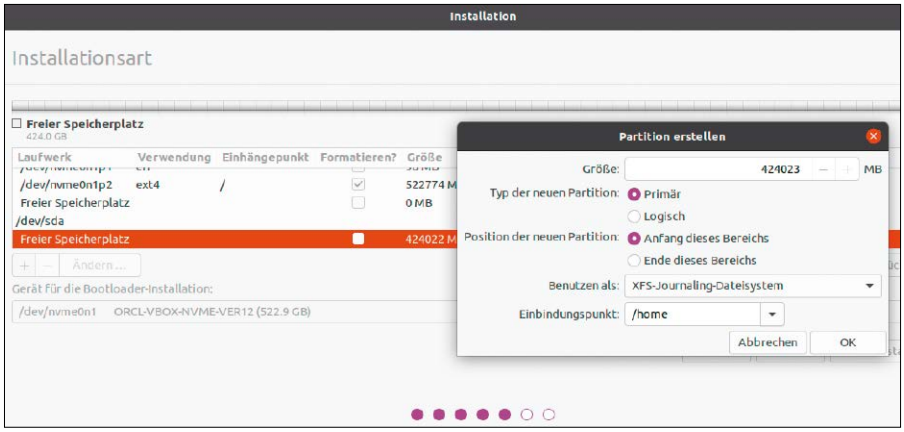
Live-Virenscanner: Ein Windows-Service

Eine weitere Kategorie Linux-basierter Notfallsysteme sind bootfähige Virenscanner, die es von praktisch allen namhaften AV-Softwarehäusern gibt. Linux-Systeme benötigen derartige Checks so gut wie nie, umso mehr aber Windows-Systeme. Linux spielt auf solchen Scanner-Livesystemen die dienende Rolle und soll einen Scannerbetrieb ermöglichen, der unabhängig vom eventuell kompromittierten Windows läuft. Ohne Linux wären solche Livesysteme von Kaspersky, Avira & Co. nicht machbar. Die **Kaspersky Rescue Disk**, die hier nur als Stellvertreterin ihrer Klasse genannt wird, zeigt einen Desktop mit älterem KDE und hängt die vorhandenen Partitionen automatisch ein. Ohne Internet geht aber gar nichts, denn allen Livesystemen dieser Art ist gemein, dass der Virenscanner zunächst online seine Virensignaturen aktualisieren muss. ■

Langlebiges Home-Verzeichnis

Partitionen lassen sich auch anders aufteilen, als das Setuptool bei der Installation standardmäßig vorschlägt. Insbesondere bietet eine separate Home-Partition Vorteile für nachhaltige Nutzerdaten trotz Neuinstallation.

VON THORSTEN EGGELING



Separates Home: Bei einer Neuinstallation lässt sich eine eigene Partition für die Home-Verzeichnisse konfigurieren. Die lässt sich dann bei späterer Neuinstallation wieder einbinden.

Bei der Linux-Installation gibt es viele mögliche Varianten. Distributionen wie Open Suse bieten beim „Geführten Setup" eine separate Home-Partition an. Ubuntu und Linux Mint gehen eher den konservativen Weg. Das gesamte System und auch die Home-Verzeichnisse werden standardmäßig gemeinsam auf einer Ext4-Partitition installiert. Die Trennung von System und Home-Verzeichnissen ist aber ebenfalls möglich und bietet Vorteile für die Datensicherheit und bei einer Neuinstallation des Systems.

Vorteile einer separaten Home-Partition

In aktuellen PCs stecken oft eine SSD mit relativ wenig Speicherplatz und eine deutlich größere Festplatte. Bei solcher Konfiguration ist es sinnvoll, das Home-Verzeichnis auf eine eigene Partition auszulagern. Die SSD gelangt dann wohl kaum an die Grenze ihrer Kapazität und die Festplatte bietet Platz auch für umfangreiche Datensammlungen. Das System startet von der SSD trotzdem sehr schnell und die Festplatte wirkt kaum als Bremse.

Bei allen PCs und Notebooks, auch mit nur einem Laufwerk, bietet die separate Home-Partition ebenfalls Vorteile. Bei einer Neuinstallation des Systems lässt sich die Partition einbinden, die Dateien darin bleiben erhalten und die Konfiguration von Programmen wie Thunderbird und Firefox sowie der Desktopumgebung steht sofort wieder zur Verfügung. Das funktioniert in der Regel auch, wenn man eine neuere oder sogar andere Distribution installiert. Die Desktopeinstellungen werden jedoch nur bei gleicher Desktopumgebung übernommen.

Ein Backup des Home-Verzeichnisses sollten Sie regelmäßig erstellen und bei Bedarf getrennt davon auch des gesamten Systems (siehe Artikel ab Seite 64). Eine eigene Home-Partition bietet dabei keinen Vorteil. Anders sieht es aus, wenn die vielleicht ältere Festplatte Fehler meldet und wahrscheinlich bald ausfällt. Sie können die Home-Partition oder deren Inhalt einfach auf eine neue Festplatte kopieren und diese in das Dateisystem einhängen (Infos unter *www.pcwelt.de/210432*).

Home-Partition bei der Neuinstallation

Wir gehen davon aus, dass Sie Ubuntu 20.04 neu auf einem Computer mit einem oder zwei unbenutzten Laufwerken installieren möchten. Bei Linux Mint läuft es entsprechend ab, andere Distributionen bieten ähnliche, aber meist abweichend bezeichnete Optionen.

Schritt 1: Booten Sie den Computer vom Installationsmedium und rufen Sie das Ubuntu Setuptool auf. Folgen Sie den Anweisungen des Assistenten. Im Dialog „Installationsart" wählen Sie die Option „Etwas Anderes" für die manuelle Partitionierung.

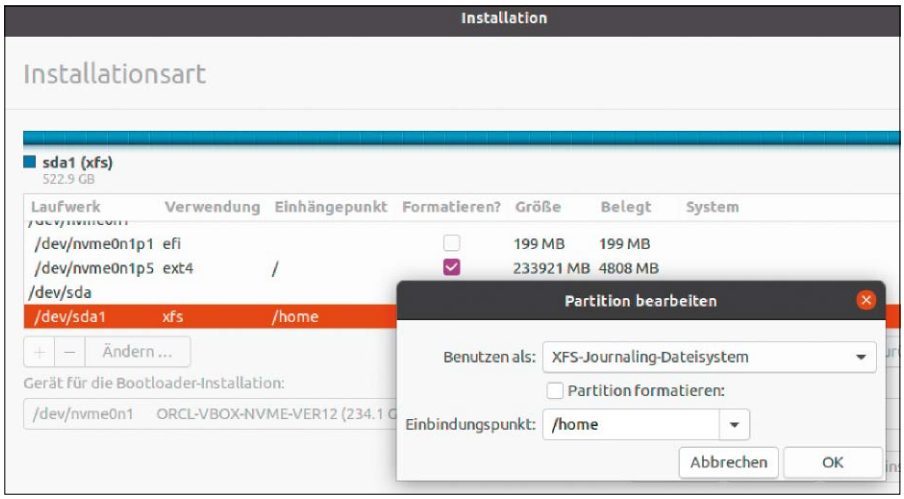
Schritt 2: Wählen Sie das Laufwerk, auf dem Sie das Betriebssystem installieren möchten. Sollten sich darauf Partitionen befinden, löschen Sie diese über die „-"-Schaltfläche. Oder Sie klicken auf „Neue Partitionstabelle", um alles auf einmal zu löschen. Alle bisherigen Daten auf der Festplatte gehen dabei verloren.

Schritt 3a: Wenn nur eine Festplatte zur Verfügung steht, klicken Sie auf „Freier Speicherplatz" und legen darin über die „+"-Schaltfläche neue Partitionen an. Bei einem Uefi-PC beginnen Sie mit einer „EFI-System-Partition", für die 100 MB ausrei-

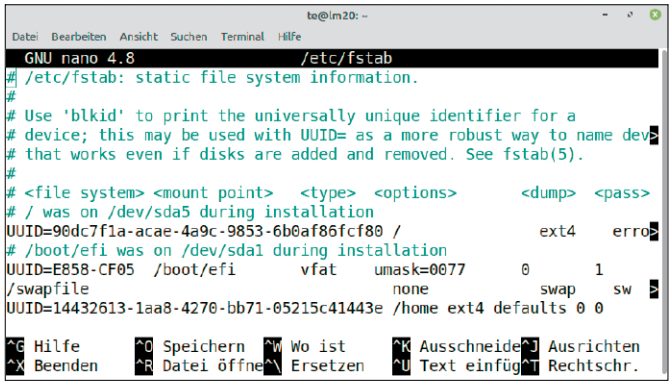
chen. Danach folgt die Systempartition mit dem Dateisystem Ext4. Die Größe hängt vom Laufwerk ab. 50 GB sollten für einen Arbeitsrechner ausreichen. Wählen Sie hinter „Einbindungspunkt“ den Eintrag „/“.
Als Nächstes erstellen Sie die Home-Partition mit dem Einbindungspunkt „/home“ und dem Dateisystem Ext4. Alternativ können Sie auch XFS verwenden, was teilweise zu einer besseren Leistung führen kann. Deutlich spürbar ist das aber in der Regel nicht. Das Home-Verzeichnis kann den verbleibenden Platz auf der Festplatte füllen oder Sie lassen noch etwas Raum für eine Swappartition mit der Größe des eingebauten RAM. Auf einer SSD und mit genügend Hauptspeicher ist das nicht zwingend erforderlich.
Schritt 3b: Bei zwei Laufwerken gehen Sie wie in Schritt 3a vor, erstellen aber die Home-Partition mit dem Einbindepunkt „/home“ auf der anderen Festplatte beziehungsweise SSD.
Schritt 4: Klicken Sie auf „Jetzt installieren“, prüfen Sie die Partitionierung und klicken Sie auf „Weiter“. Danach absolvieren Sie die weiteren Schritte des Assistenten und starten abschließend das neu installierte Ubuntu.

Neuinstallation mit vorhandener Home-Partition

Sollte eine Neuinstallation nötig oder gewünscht sein, verwenden Sie unter „Installationsart“ wieder „Etwas Anderes“. Klicken Sie die Systempartition an und dann auf „Ändern“. Wählen Sie hinter „Benutzen als:“ den Eintrag „Ext4-Journaling-Dateisystem“, als Einbindepunkt geben Sie „/“ an und setzen ein Häkchen vor „Partition formatieren“. Sie können auf die Formatierung auch verzichten. Dann wird eine Art Reparaturinstallation durchgeführt, bei der aber Verzeichnisse wie „/etc“, „/usr“ und „/var“ gelöscht werden. Zusätzliche Software müssen Sie danach neu installieren. Bei einem defekten System ist diese Methode der Reparatur jedoch einen Versuch wert. Erstellen Sie aber vorher ein Backup.
Bei der Home-Partition wählen Sie das zuvor genutzte Dateisystem und als Einbindepunkt „/home“. Das Häkchen vor „Partition formatieren“ darf nicht gesetzt sein. Nach einem Klick auf „Jetzt installieren“ prüfen Sie genau, dass die Home-Partition tatsächlich nicht neu formatiert wird. Klicken Sie auf „Weiter“ und fahren Sie mit der Installation fort.



Ohne Datenverlust: Achten Sie darauf, dass bei einer Neuinstallation kein Häkchen vor „Partition formatieren“ gesetzt ist, damit die Dateien auf der Home-Partition erhalten bleiben.



Home-Partition einbinden: In der Datei „/etc/fstab“ geben Sie an, welche UUID und welches Dateisystem die neue Partition besitzt und wo diese eingehängt werden soll („/home“).

Home-Partition nachträglich einbinden

Bei einer schon bestehenden Installation lässt sich das Home-Verzeichnis jederzeit auf eine eigene Partition auslagern. Über ein Tool wie Gparted (*sudo apt install gparted)* verkleinern Sie vorhandene Partitionen, um Platz dafür zu schaffen, oder Sie erstellen eine neue Home-Partition auf einer zweiten Festplatte.
Schritt 1: Ermitteln Sie zunächst im Terminal mit dem Befehl

```
blkid
```

die UUIDs der Partitionen.
Schritt 2: Öffnen Sie die Konfigurationsdatei für die Einbindung der Partitionen in einem Editor:

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

Fügen Sie folgende Zeile an:

```
UUID=[ID] /home ext4 defaults 0 0
```

Den Platzhalter „[ID]“ ersetzen Sie durch die zuvor ermittelte UUID der neuen Home-Partition. Setzen Sie „xfs“ statt „ext4“ ein, falls Sie XFS bei der Formatierung verwendet haben.
Schritt 3: Schließen Sie alle Anwendungen und beenden Sie die grafische Oberfläche. Ubuntu-Nutzer (20.04) verwenden dann

```
sudo service gdm3 stop
```

und Benutzer von Linux Mint 20 den folgenden Befehl:

```
sudo service lightdm stop
```

Drücken Sie Alt-F2, um eine Textkonsole einzublenden, bei der Sie sich anmelden.
Schritt 4: Benennen Sie „/home“ um und legen Sie ein neues Verzeichnis an:

```
sudo mv /home /home.bak
sudo mkdir /home
```

Schritt 5: Binden Sie die neue Home-Partition ein und kopieren Sie alle Dateien:

```
sudo mount -a
sudo rsync -aXS /home.bak/ /home/
```

Achten Sie auf die abschließenden Slash-Zeichen („/“). Starten Sie Linux mit

```
sudo reboot
```

neu. Das System verwendet jetzt die neue Partition für das Home-Verzeichnis. Die alten Dateien in „/home.bak“ können Sie danach löschen oder als Sicherungskopie aufbewahren. ■

Mehr Platz auf Datenträgern

Einen „Elektronik-Frühjahrsputz“ kann man zu jedem Zeitpunkt im Jahr starten. Hier beschäftigen wir uns mit den Datenträgern: So schaffen Sie Platz und Ordnung auf internen und externen Festplatten, auf SSD/NVMe und Micro-SD-Karten.



VON HERMANN APFELBÖCK

Das große Aufräumen: Dieser Ratgeber nimmt sich mehr vor als das Entsorgen von temporären Daten, Browsercache und überflüssiger Software. Jenseits typischer Tools wie Bleachbit geht es hier nicht nur um Platzgewinn auf SSDs und Festplatten, sondern auch um aufgeräumte Netzwerke, Durchblick bei Onlinekonten, Ausmisten und Säubern der Hardware. Einmal im Jahr ist es Zeit, Platinenrechner und Ausbau-PCs staubfrei zu fegen und Kabelsalat nachhaltig zu entwirren. Nicht zuletzt nehmen wir auch vermüllte Android-Smartphones und Tablets ins Visier.

Den Start aber machen die Datenträger: Wer Linux- und Windows-Systeme auf knapp bemessenen SSDs, ferner Platinenrechner wie den Raspberry Pi auf kleinen Micro-SD-Karten betreibt, hat selten Platz zu verschenken und sollte die Daten von Betriebssystem und Programmen gut organisieren. Gelegentliche Aufräumarbeiten lohnen sich allemal, bei kleineren Datenträgern wie etwa SD-Karten auch öfter. Aber es soll es nicht nur um den Platzgewinn gehen: Wer mehrere Geräte im Homeoffice betreibt, gewinnt nach Inventur und Re-Organisation wieder den Durchblick über die Daten und verringert Entropie und unnötige Redundanz.

Inventar der Software

Was ist installiert? Benötigt das System diese Ausstattung tatsächlich? An dieser Stelle haben wir vorerst nur das lokale System im Auge. Beachten Sie in diesem Zusammenhang auch den weiteren Beitrag (ab Seite 94), der das Verteilen von Software im Netzwerk diskutiert.

Ein lückenloser Überblick über installierte Software ist unter Linux nicht ganz einfach, weil verschiedene Installationsquellen verschiedene Tools erfordern. Wem ein grober Überblick genügt, kann sich bei Desktopdistributionen an das grafische Softwarecenter halten. So zeigt die Anwendungsverwaltung von Linux Mint über das kleine Balkenmenü die Option „Installierte Anwendungen zeigen“ und in den meisten Ubuntu-Edition bietet Gnome-Software analog das Register „Installiert“. In den dort angezeigten Katalogen können Sie überflüssige Software per Mausklick entfernen. Die Mint-Zentrale zeigt, installiert und deinstalliert auch Flatpak-Pakete, die Ubuntu-Zentrale auch Snap-Software. Wer es detailliert haben will, muss differenzieren: Mit dem Tool apt installierte Pakete – unter Debian/Ubuntu/Mint meist das Wichtigste – zeigt folgender Befehl:

```
apt list --installed
```

Installierte Snap-Pakete zeigt dieser Befehl

```
snap list
```

und Flatpak-Pakete folgender:

```
flatpak list
```

Die jeweiligen Deinstallationsbefehle lauten dann so:

```
sudo apt remove [Name]
sudo snap remove [Name]
sudo flatpak uninstall [Name]
```

Als „[Name]“ ist hier jeweils anzugeben, was vorher mit dem „list“-Befehl ermittelt wurde.

Bei apt-Deinstallationen auf Debian/Ubuntu/Mint sollte am Ende solcher Aufräumarbeiten immer

```
sudo apt autoremove
```

folgen. Dies beseitigt nämlich nach der Softwarereinigung die abhängigen und nicht mehr benötigten Pakete – und erst das sorgt in der Regel für signifikanten Platzgewinn. Bestätigen Sie eine allzu opulente Liste von abhängigen Paketen aber nicht kritiklos, da manche Deinstallation

den kompletten Desktop mitziehen kann. Wer die bestmögliche Kontrolle behalten will, lässt am besten nach jedem „apt remove“ ein „apt autoremove“ folgen. Dann bleibt die Liste abhängiger Pakete klein und kontrollierbar.

Kriterien für die Deinstallation von Software

Für oder gegen das Ausmisten von Software gibt es mehrere Kriterien:

1. Jede Software, die Sie offenbar seit Monaten nicht benutzt haben, ist ein Kandidat zur Deinstallation.

2. Software, deren Funktion Sie nicht kennen, sollten Sie nicht ungeprüft deinstallieren. Hier empfiehlt sich mindestens ein vorheriger Start, um sich von der Funktion zu überzeugen. Ist dies nicht aussagekräftig, weil kein grafisches Fenster lädt oder das Terminal keinen Output zeigt, nehmen Sie lieber Abstand.

3. Manche Software gilt bei vielen Distributionen als Standard, obwohl deren Funktion vielerorts durch Webdienste (via Browser) ersetzt werden könnte. Einen dicken Mailclient brauchen zum Beispiel nur Nutzer mit mehreren Mailkonten und auch die eigentlich nur, wenn sie Nachrichten zwischen verschiedenen Konten verschieben möchten. Im Übrigen genügt Webmail mit dem Browser. Auch Office-Pakete sind nicht auf jedem System nötig, insbesondere wenn ein Google- oder Microsoft-Konto genutzt wird.

4. Software in Snap-Paketen – und mehr noch in Flatpaks – fordert erheblichen Plattenplatz. Die Deinstallation dieser Containerformate und deren Ersatz durch das klassische Binärpaket aus den Paketquellen spart daher erhebliche Kapazitäten. Dafür muss man dann aber in der Regel eine ältere Version der Software in Kauf nehmen.



Softwareinventur: Die grafischen Softwarezentralen unter Ubuntu/Mint bieten eine Option, um installierte Programme aufzulisten und bei Bedarf per Mausklick zu deinstallieren.

Konfigurationsdateien der Software

Eine Deinstallation von Software beseitigt nicht die Konfiguration und eventuelle Benutzerdaten, die von dieser Software angelegt wurden. Diese benutzerbezogenen Reste liegen im Home-Verzeichnis im versteckten Ordner „./config“ oder auch direkt im Home-Ordner in versteckten Verzeichnissen, deren Name auf die verantwortliche Software verweist – etwa „.thunderbird“. Strg-H im Dateimanager (unter KDE: Alt-Punkt) blendet die Objekte ein. Überwiegend handelt es sich um Konfigurationsbrösel, deren Löschen kaum Platzgewinn verspricht, aber doch für bessere Übersicht und schnellere Navigation sorgt. Es gibt aber Ausnahmen: Ergiebig ist das Löschen überflüssiger Bild- und Multimediadaten (etwa nach Deinstallation von Kodi, Shotwell) sowie der Indizes von

DATENTRÄGERBELEGUNG ANALYSIEREN

Am Anfang steht die Inventur: Wie viel Platz ist auf den Partitionen frei? Welche Verzeichnisse belegen wie viel Speicher? Unter Ubuntu und Linux Mint finden Sie das Tool Baobab als „Festplattenbelegungsanalyse“ oder „Festplattenbelegung analysieren“ im Hauptmenü. Es zeigt nach dem Start eine Übersicht der Datenträger. Hier sind die Gesamtkapazität und der aktuelle Füllstand ersichtlich. Nach Klick auf dem Pfeil ganz rechts startet Baobab eine Ordneranalyse, die es als Kreis- oder Kacheldiagramm visualisiert. KDE kann mit einem ähnlichen Visualisierungstool Filelight aufwarten.

Auf allen Systemen – mit oder ohne grafischen Desktop – gibt der Befehl *df -h* im Terminal schnelle Auskunft zur Belegung der Laufwerke. Mit einem Grep-Filter

```
df -h - | grep /dev/sd
```

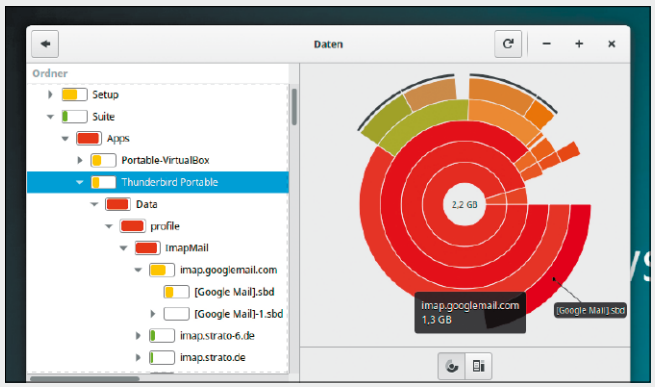
können Sie temporäre Dateisysteme zur besseren Übersicht ausblenden. Vor allem die Prozentzahl („Verw%“) bietet gute Orientierung zum Handlungsbedarf. Nach Verzeichnissen und Dateien schlüsselt der Befehl

```
du | sort -h
```

den Platzbedarf auf. Dies ergibt eine aufsteigend sortierte Liste mit den umfangreichsten Verzeichnissen am Ende. Statt der bytegenauen Aufstellung kürzt

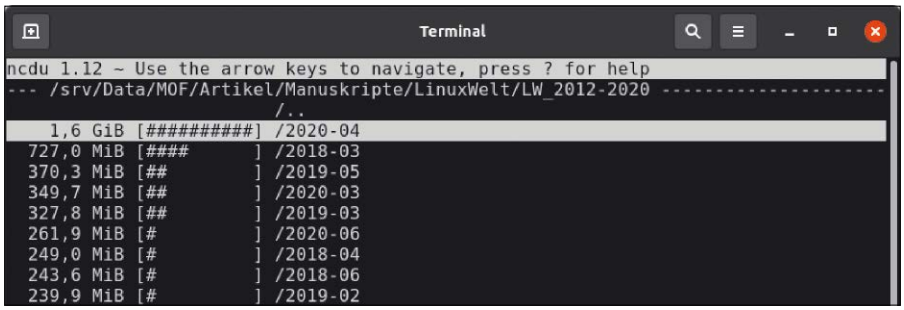
```
du -h | sort -h
```

die Werte lesbarer mit Megabyte-, Gigabyte- und Terabyte-Angaben ab. Der Befehl berücksichtigt sämtliche Unterordner und sollte in dem Verzeichnis gestartet werden, wo Sie den Platzbedarf messen wollen.



Festplattenbelegung: Das Tool Baobab visualisiert den Plattenplatz von Ordnern durch entsprechend große Segmente im Kreisdiagramm.

Suchprogrammen (Recoll, Baloo). Deinstallierte Browser und Mailprogramme hinterlassen ebenfalls große Datenhalden im Benutzerordner. Normalerweise können Sie die betreffenden Ordner ohne Bedenken löschen. Bei Mailprogrammen betrifft dies allerdings auch die Nachrichten. Wer diese sichern möchte (bei IMAP-Konten, die alles am Server erhalten, nicht zwingend erforderlich), kann einen Ordner wie „~/.thunderbird“ auf einen externen Datenträger verschieben.



Entdeckungen mit Ncdu: 1,6 GB, 700 MB für ein paar Texte? Das Tool Ncdu ist eine große Hilfe dabei, unnötige Datenhalden zu finden und interaktiv zu entsorgen.

Dateien manuell löschen

Eine große Hilfe für manuelles Löschen ist Ncdu (mit identischem Paketnamen). Denn das Terminalprogramm sortiert die Verzeichnisse standardmäßig nach der enthaltenen Datenmenge, wechselt wie ein Dateimanager zwischen den Verzeichnissen und kann selbst aktiv löschen. Die einzig wichtige Bedienregel ist die Auswahl des Startverzeichnisses. Ist Ncdu nämlich einmal gestartet, wird es in keine höhere Verzeichnisebene wechseln. Wenn Sie das komplette Dateisystem durchforsten wollen, sollten Sie das Tool mit

```
ncdu /
```

starten. Ncdu sortiert automatisch nach Ordnergrößen, kann aber mit Taste „n“ auch nach Namen sortieren, mit „s“ wieder nach der Größe („size“). Das Tastenkommando „d“ („delete“) ist der Löschbefehl für markierte Dateiobjekte.

Massenvernichtung: Um ganze Dateigruppen rationell anhand eines Namensmusters oder einer Extension rekursiv zu löschen, ist find das beste Werkzeug. Es bringt seinen eigenen Löschschalter „-delete“ mit:

```
find ~ -type f -iname "*.pdf"
  -delete
```

Dies löscht im gesamten Home-Verzeichnis („~“) alle PDF-Dateien. Die Angabe „-type -f“ (Files) sorgt dafür, dass der Befehl nur Dateien, keine Ordner berücksichtigt.

Das Löschen von Verzeichnissen bestimmten Namens erfordert einen Umweg:

```
find ~ -type d -iname "ORI" -exec rm
  -r {} \;
```

Das Beispiel nimmt an, dass es Backupordner namens „ORI“ gibt, die komplett gelöscht werden dürfen. „type -d“ („Directories“) sorgt dafür, dass der Befehl nur Ordner berücksichtigt.

Backupsäuberungen mit Rsync

Hygienisches Löschen von obsoleten Daten auf der einen Seite, Doppelt- und Dreifach-Redundanz auf unabhängiger Hardware auf der anderen Seite sind kein Widerspruch – im Gegenteil: Wer wichtige Benutzerarchive größeren Umfangs regelmäßig sichert, ärgert sich über die Zeit- und Platzverschwendung durch überflüssige Daten doppelt und dreifach. Daher ist es sinnvoll, periodisch den Quelldatenträger manuell auszumisten und den Rest dann Rsync mit

LÖSCHEN UND REDUZIEREN VON SYSTEMDATEN

Apt-Cache: Die Paketverwaltung von Debian/Ubuntu/Mint sammelt die heruntergeladenen Pakete bei Installation und Aktualisierung unter „/var/cache/apt/archives“. Dieses Verzeichnis dient als Cache, wenn ein Update einmal abbricht. Den apt-Cache leeren Sie mit

```
sudo apt-get clean
```

am besten regelmäßig. Auch das Tool Bleachbit bietet eine entsprechende Option. Die Maßnahme kann mehrere GB freischaufeln.

Obsolete Pakete: Der Aufräumbefehl

```
sudo apt autoremove
```

entfernt ältere Kernel-Versionen und abhängige Softwarepakete, die nach der Deinstallation von Software obsolet wurden.

Reserve für root minimieren: Das Standarddateisystem Ext4 reserviert auf jeder Partition einen Speicherbereich für das Konto „root“.

Dieser Platz steht für Daten nicht zur Verfügung. Das soll gewährleisten, dass sich root auch auf voller Systempartition noch anmelden kann. Standardmäßig liegt der reservierte Platz bei fünf Prozent, da sind bei einer 120-GB-SSD immerhin sechs GB. Die Reserve können Sie gefahrlos verringern. Das gelingt mit dem Programm tune2fs, das einige Eigenschaften vonExt2/3/4-Dateisystemen nachträglich und ohne Datenverlust anpassen kann: Der als root oder mit sudo ausgeführte Befehl

```
tune2fs -m 2 /dev/sda1
```

verringert die Anzahl der reservierten Blöcke der Partition „/dev/sda1“ auf zwei Prozent. Der Platzgewinn ist natürlich umso größer, je größer die Datenträgerkapazität.

Auslagerungsdatei verkleinern: Ubuntu und Linux Mint verwenden eine Auslagerungsdatei, deren Ort und Größe Sie über

```
swapon -s
```

in Erfahrung bringen. Vier oder acht GB sind je nach Größe leicht zu gewinnen, indem Sie die Auslagerung abschalten und dann die Datei verkleinern:

```
sudo swapoff -a
sudo fallocate -l 4G [Pfad/Name]
sudo mkswap [Pfad/Name]
sudo swapon [Pfad/Name]
```

Wenn Sie als „[Pfad/Name]“ den Ort des bisherigen Swapfiles beibehalten, sind keine weiteren Maßnahmen in der Datei „/etc/fstab“ erforderlich.

Schalter „--delete“ zu überlassen – der löscht dann auch im Ziel die obsoleten Daten (Beispiel).

```
rsync -auvP --delete --progress /
  srv/Data/ /media/sepp/usb0/Data
```

Das erste nach den Schaltern angegebene Verzeichnis ist der Quellordner mit abschließendem Slash („/“), das zweite das Backupziel. Testen Sie umfangreiche Sicherungen immer erst mit dem zusätzlichen Schalter „--dry-run“

```
rsync -auvP --delete --dry-run
  --progress […]
```

und legen Sie den Befehl dann als Alias ab. Aber Achtung! Erfahrungsgemäß sind die Rollen von Quelle und Ziel nicht immer eindeutig: Wenn eine USB-Festplatte (oder ein Samba/SFTP-Server), die als Backupziel dient, gelegentlich auch neue und wichtige Daten von anderer Stelle als von der eigentlichen „Quelle“ erhält, dann gerät „rsync --delete“ zur Massenvernichtungswaffe. Wo Unsicherheit besteht, bewährt sich folgende Methode. Erst drehen Sie die Quelle und Ziel um

```
rsync -auvP --progress [Backup]/
  [Quelle]
```

und sichern alles Neue zur „Quelle“. Danach löschen Sie dort alles Unnötige und sichern danach mit „rsync --delete“ wieder zurück zum Backup-Datenträger.

Die Suche nach Dateidubletten

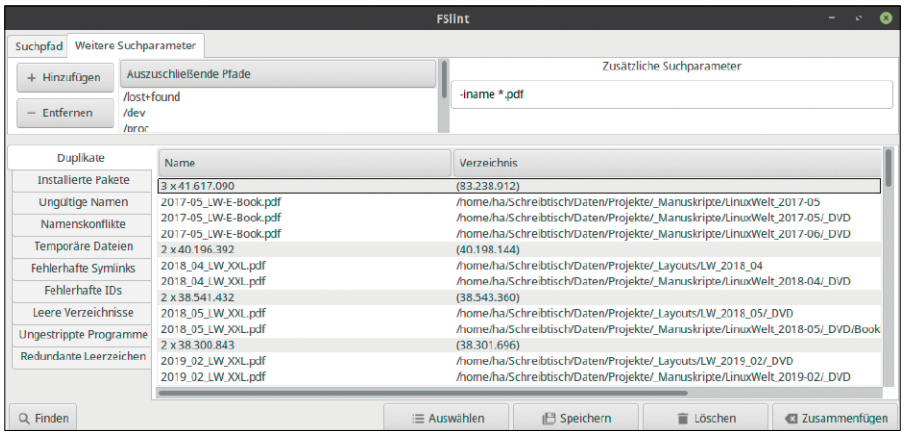
Effiziente Dublettensuche ist nicht trivial und sollte mehr als namensgleiche Dateien erkennen. Das Tool fdupes vergleicht Dateigrößen und geht bei Größenübereinstimmung in die Byteanalyse mit MD5-Prüfsummen. Das Paket „fdupes“ finden Sie überall in den Standard-Paketquellen. Folgender Aufruf ausgehend vom aktuellen Verzeichnis („.“)

```
fdupes -r -S -n -d .
```

macht eine rekursive Suche in allen Unterverzeichnissen („-r“) mit Angabe der Dateigrößen („-S“), Überspringen leerer Dateien („-n“) und interaktivem Löschmodus („-d“). Die Analyse kann je nach Datenanzahl und Dateigrößen einige Zeit beanspruchen. Danach markieren Sie bei aktiviertem Löschmodus („-d“) jene Dublettendatei per angezeigter Kennziffer, **die Sie behalten wollen.** Die andere beziehungsweise alle anderen Dateien werden gelöscht. Der interaktive Löschmodus erfordert Konzentration und Sorgfalt. Wo viele Dubletten zu erwarten sind, die irrelevant sind, ist es effizienter, das Ergebnis mit

```
fdupes -r -S -n . > dups.txt
```

ohne den interaktiven Modus in eine Liste zu schreiben und nach Durchsicht dieser Liste die lohnenden Löschaktionen im Dateimanager zu erledigen.



Suche nach Dateidubletten mit fslint: Dieses Werkzeug ist eine Empfehlung für den Desktop. Im Terminal leistet das Tool fdupes ganze Arbeit.

Grafisches fslint: Am Desktop bietet das Werkzeug fslint mehr Komfort als fdupes. Fslint liegt mit gleichnamigem Paketnamen in den Paketquellen der meisten Distributionen. Sie finden es nach der Installation im Startmenü als „Fslint Janitor“ oder starten es mit *fslint-gui* im Terminal. Das Programm durchsucht standardmäßig alle Unterordner der einstellbaren Startordner. Für zusätzliche Filter können Sie selbst sorgen, indem Sie unter „Weitere Suchparameter → Zusätzliche Suchparameter“ einen find-Schalter wie „-iname *.mp3“ eintragen. In der Ergebnisliste nach erfolgter Analyse markieren Sie die überflüssigen Dubletten und klicken auf „Löschen“.

Löschen mit Bleachbit

Das in den meisten Standard-Paketquellen erhältliche Bleachbit hat jede erdenkliche großräumige bis marginal-kosmetische Löschaktion im Repertoire und darf als klassischer Cleaner unter Linux gelten. Die meisten Löschaktionen finden im Home-Verzeichnis statt (Browser, Mail, Office), jedoch kann Bleachbit auch in der Paketverwaltung löschen, wenn es mit „BleachBit (as root)“ oder im Terminal mit *sudo bleachbit* gestartet wird. Bleachbit kann aber noch mehr, als in der grafischen Oberfläche angewählte Optionen abzuarbeiten. Alle Detailfunktionen sind auch als Terminalkommando abrufbar. Der Befehl

```
bleachbit --list-cleaners
```

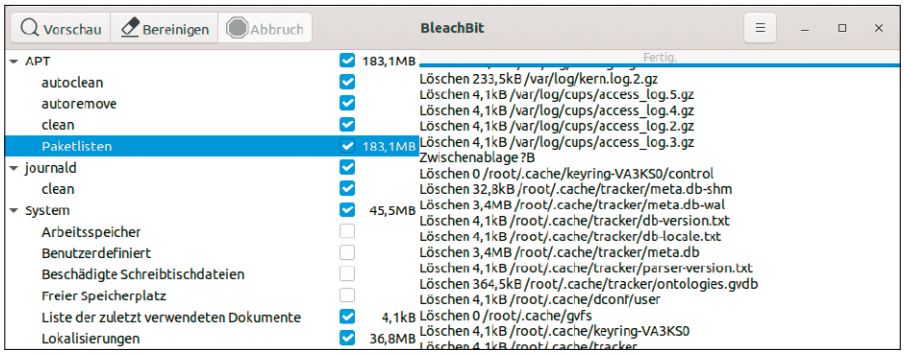
zeigt alle Löschmodule an – annähernd 200, wovon aber die meisten nur Spezialroutinen für einzelne Programme sind (insbesondere für Browser). Jedes einzelne Modul kann mit dem Schalter „--clean“

```
bleachbit --clean system.cache
```

gestartet werden. Bei Löschzielen mit diversen Unterabteilungen (system, apt, firefox, chromium, google_chrome, thunderbird) funktioniert auch diese Variante

```
bleachbit --clean apt.*
```

mit Stellvertreterzeichen. ■



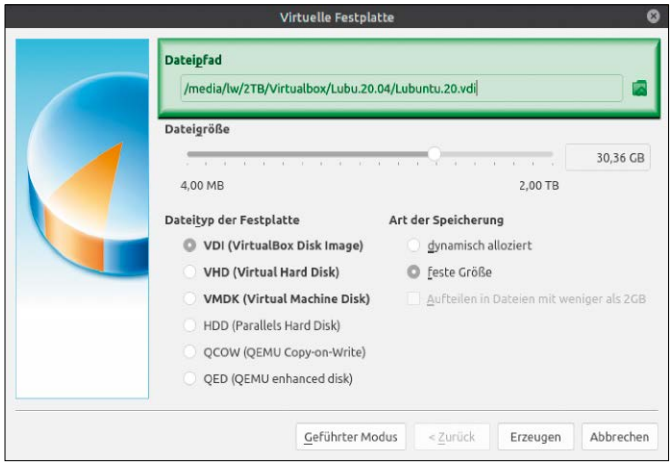
Löschklassiker: Bleachbit informiert vorab detailliert über die Löschmengen und ist ideal zum Aufräumen von Browsercache, Updatecache, verwaisten Paketen und temporären Dateileichen.

Auslagern und Komprimieren

Während Systempartitionen auf Micro-SD-Karten und SSDs gerne an Kapazitätsgrenzen gelangen, sind externe und erschwingliche USB-Festplatten mit 8, 10, 16 TB kaum vollzubekommen. Die Frage liegt nahe: Was kann man auslagern?

VON HERMANN APFELBÖCK

Standardordner wie „Bilder“, „Dokumente“, „Videos“ im Home unter Linux wie Windows sind nett gemeint, aber vielerorts obsolet. Überall, wo heute Datenmassen von Benutzerdateien anfallen, liegen diese meist jenseits der Systempartition auf externen Datenträgern und Home-Servern. Das ist flexibler und skalierbarer als darauf zu hoffen, dass der Platz auf dem Systemdatenträger dauerhaft ausreicht. Dieser Artikel zeigt weitere und besonders lohnende Beispiele für das Auslagern von Daten und Software.



Virtuelle Festplatte auf USB-Laufwerk: Intensivnutzer von Virtualisierungssoftware gewinnen dadurch Hunderte von Gigabyte auf der Systempartition.

Virtuelle Maschinen/Festplatten

Virtuelle Maschinen (sofern ordentlich installiert und nicht nur Livesystem) erfordern viel Platz für die virtuellen Festplatten. Mit zehn bis 20 GB pro System ist selbst bei dynamischer Allozierung zu rechnen und für etliche VMs sind dann schnell 200 GB und mehr verbraten. Standardmäßig wollen Virtualbox oder Vmware diese Festplattendateien („vdi“ oder „vmdk“) immer auf die Systempartition schreiben, aber das können Sie gezielt umlenken. Am einfachsten geht das, indem Sie ein neues virtuelles System wie gewohnt einrichten, dann aber nicht starten, sondern beim neuen Eintrag nach Rechtsklick auf „Settings“ (Vmware) oder „Ändern“ (Virtualbox) gehen. Dort können Sie unter „Hard Disk“ (Vmware) oder „Massenspeicher → Controller. SATA“ (Virtualbox) die bisherige Definition löschen und eine neue Harddisk anlegen, die jetzt auf dem externen Datenträger Ihrer Wahl liegt. Via USB 3.x ist solcher Betrieb virtueller VMs leistungstechnisch mehr als zufriedenstellend.

Die Home-Partition auslagern

Anders als bei System und Software steht bei Benutzerdateien nicht die Leistung, sondern die Kapazität des Laufwerks im Vordergrund. Clevere Anwender richten daher das Benutzer-Home schon bei der Installation auf einem Extra-Datenträger ein. Wo dies nicht der Fall ist und der Platz auf der Systempartition knapp wird, lässt sich das auch nachholen. Ermitteln Sie zunächst mit dem Terminalbefehl

```
blkid
```

die UUID-Kennungen der Partitionen. Das externe Laufwerk (oder eine zweite interne Festplatte) richten Sie dann mit dem Mountpunkt „/home“ in der Datei „/etc/fstab“ ein (zum Editieren ist sudo-Recht erforderlich):

```
UUID=[…] /home ext4 defaults 0 0
```

Eine Formatierung mit Linux-Dateisystem ist für den Home-Datenträger zwingend, im Beispiel ist es das Dateisystem Ext4. Danach schließen Sie alle laufenden Programme und beenden im Terminal zwangsweise die grafische Oberfläche, indem Sie unter Ubuntu den Displaymanager Gdm3

```
sudo service gdm3 stop
```

oder unter Linux Mint 20

```
sudo service lightdm stop
```

Lightdm stoppen. Vom „schwarzen“ Monitor gelangen Sie mit Strg-Alt-F2 zur Textkonsole und melden sich dort an. Dort benennen Sie das bisherige Home um, erstellen einen neuen Home-Ordner, mounten das externe Laufwerk in diesen Mountpunkt und kopieren alle Daten:

```
sudo mv /home /home.bak
sudo mkdir /home
sudo mount -a
sudo rsync -aXS /home.bak/ /home/
```

Achten Sie auf die abschließenden Slash-Zeichen („/“). Starten Sie Linux mit

```
sudo reboot
```

neu. Das System verwendet ab sofort für das Home-Verzeichnis den neuen Datenträ-

ger. Den Ordner „/home.bak“ können Sie löschen und damit viel Platz für die Systempartition schaffen.

Skalierbare Datenarchive

Was für ausgelagerte Home-Verzeichnisse gilt, ist natürlich auch kleinteiliger für anwachsende Datenarchive realisierbar. Wird der Platz irgendwo knapp, laden Sie einen externen Datenträger in das geeignete Verzeichnis und vergrößern damit die Kapazität. Dazu ist nicht mehr erforderlich als die Angabe des Geräts und des Mountpunkts:

```
sudo mount /dev/sdc1 /home/sepp/
  Musik/Jazz
```

Würde der so eingehängte Datenträger auf oberster Ebene die Ordner von Jazzinterpreten enthalten, wäre die Ordnung perfekt. Über die Datei „/etc/fstab“ sorgen Sie dann für automatisches Einhängen des Datenträgers. Dazu brauchen Sie wieder blkid, um UUID-Kennziffer und Dateisystem zu ermitteln, und dann den Eintrag in die fstab:

```
UUID=[…] [Dateisystem] /home/
  sepp/Musik/Jazz auto 0 0
```

Testen Sie das Ergebnis mit diesem Befehl:

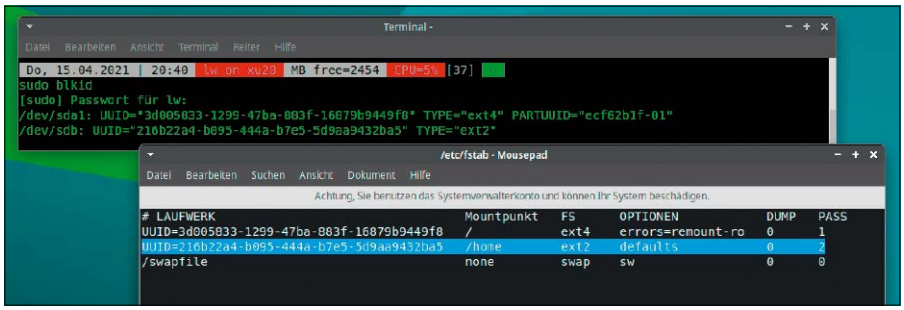
```
sudo mount -a
```

Ist dies in Ordnung, mountet das Laufwerk künftig beim Systemstart automatisch in das gewünschte Verzeichnis.

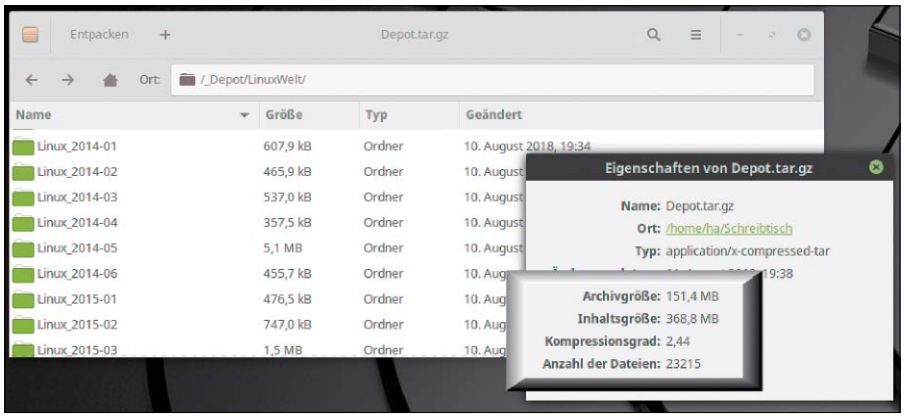
Software auf externen Datenträgern

Mit den zahlreichen portablen Apps unter Windows kann Linux nicht mithalten. Als portable Software gibt es hier nur die Appimages in begrenzter Auswahl. Dieses Containerformat benötigt keine Installation und ist auch auf externen USB-Medien lauffähig (bei Snaps und Flatpaks trifft dies nicht zu). Die Images werden einfach auf den Datenträger der Wahl kopiert und dort ausführbar geschaltet (im Dateimanager oder mit „chmod +x“). Die größte Sammlung solcher Appimages bietet *https://www.appimagehub.com*. Auch die Website *https://www.linux-apps.com* bietet im Listenfeld rechts oben den Filter „AppImage“.

Appimages laufen praktisch voraussetzungslos, haben aber doch eine wichtige Bedingung: Der Datenträger, auf dem die Programme liegen, muss mit einem Dateisystem formatiert sein, das erweiterte Dateiattribute vorsieht – also ein Linux-Dateisystem wie Ext4 oder Windows NTFS. Auf FAT/exFAT-Dateisystemen ist es nicht möglich, das Appimage ausführbar zu schalten.



Ausgelagertes „Home“: Das ist mit die effizienteste Maßnahme, die Systempartition zu entlasten. Ein mobiles „Home“ auf USB oder Micro-SD sorgt obendrein für mobile Benutzerdaten.



Platzgewinn und kaum Komfortverlust: Komprimierte „tar.gz“-Archive sind schnell und mit der Archivverwaltung (file-roller) bequem zu benutzen.

Benutzerdaten zusammenlegen und/oder komprimieren

Das Zusammenlegen von Datenhalden in Packerarchiven oder in ISO-Images bringt mehrere Vorteile:

1. Wenn Hunderte von kleineren Dateien in eine gepackt werden, entfällt der typische „Verschnitt“. Um den Verschnitt anhand eines Extrembeispiels zu erläutern: Eine Datei mit einem Byte benötigt eine komplette Zuordnungseinheit – meistens 4096 Byte, eventuell aber auch das Doppelte und mehr.

2. Wird beim Zusammenlegen zusätzlich komprimiert, spart dies zusätzlichen Platz – sehr viel bei Textdokumenten aller Art (PDF, Office), eher wenig bei Bild- und Videoformaten.

3. Synchronisierungsbackups laufen wesentlich schneller, wenn statt Hunderten nur noch eine Datei befragt werden muss, ob eine identische Version vorliegt.

Es gibt aber auch Nachteile: Die Suche nach einzelnen Dateien oder Dateiinhalten funktioniert ohne aufwendige Hilfsmittel nicht mehr. Auch nachträgliches Bearbeiten von Dateien wird komplizierter oder unmöglich (ISO). Daher eignen sich diese Methoden nur für abgeschlossene Projekte.

ISO-Images erstellen: In einem Werkzeug wie Brasero klicken Sie auf „Daten-Projekt“ und ziehen den gewünschten Ordner in das Brasero-Fenster. Nachdem Brasero die Projektgröße errechnet hat, klicken Sie recht unten auf „Brennen“, vergeben den Namen für die ISO-Datei und klicken auf „Abbild erstellen“.

ISO-Abbilder sind ohne zusätzliche Software mit jedem Betriebssystem unkompliziert zu mounten und (schreibgeschützt) zu benutzen.

Komprimierte Archive erstellen: Hier ist das schnelle tar auf der Kommandozeile erste Wahl. Ein typischer Befehl zum Einpacken beginnt mit einigen Optionen, nennt dann das Zielarchiv und zuletzt den Ordner mit den zu sichernden Daten:

```
tar -czvf depot.tar.gz Depot
```

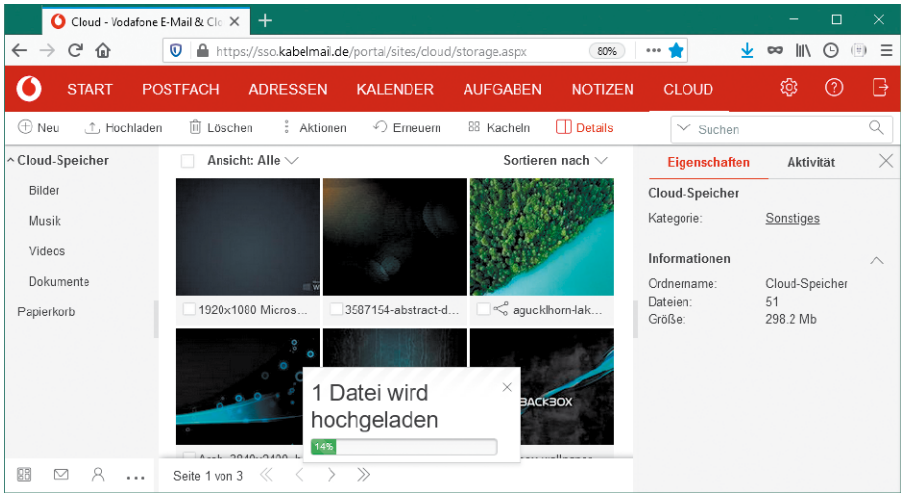
Das Beispiel geht davon aus, dass sich tar im richtigen Verzeichnis befindet und darunter den Ordner „Depot“ findet. Die Nutzung von „tar.gz“-Archiven ist unter Desktop-Linux mit dem Archivmanager (unter Windows mit 7-Zip) praktisch genauso komfortabel wie der Umgang mit unkomprimierten Daten im Dateimanager. Es ist nicht nötig, die Daten auszupacken. ■

Netz & Web: Eine Inventur

Aufräumen im Netz hat zwei Aspekte: Der eine hat die angeschlossenen Rechner im Fokus und analysiert, wie sich diese durch Netzwerkfunktionen entlasten lassen. Der zweite betrifft die Netzwerkdienste selbst: Was brauchen Sie wirklich?

VON HERMANN APFELBÖCK

Selbst in privaten Heimnetzen sammelt sich heute schnell ein kleiner Gerätepark von PCs, Notebooks, Tablets, Platinen. Homeoffice und Homeschooling seit 2020 potenzieren den schon vorher bestehenden Trend. In einem gut organisierten Netzwerk können sich die einzelnen Endgeräte hinsichtlich Benutzerdaten und installierter Software auf das Allerwesentlichste beschränken. Auf der anderen Seite stehen die Fragen, ob jede Aufgabe wirklich eine Extrahardware braucht und welche Webdienste entbehrlich sind.



Es muss nicht immer Google oder Microsoft sein: Die Standardcloud von Internetprovidern ist selten engagiert und inspiriert, aber für ein paar Bildfreigaben oder Sicherungen reicht es allemal.

Aufräumen im Heimnetz und Web

Es soll ja Heimbastler geben, die nicht mehr beantworten können, wie viele Geräte (insbesondere Platinenrechner) in ihrem Netz arbeiten – und mit welcher Aufgabe. Leider ist es Gesetz, dass jede Hardware irgendwann ein Problem hat. Je mehr Geräte und Systeme das Netz bevölkern, desto häufiger ist der Admin mit Fehleranalyse und Problemkorrektur beschäftigt. Diese Tatsache ist so trivial wie ihre Konsequenz: Wer sich von einem Uralt-Notebook trennen kann, das zwar noch läuft (aber keiner weiß, warum), oder von einem Raspberry, der nur das Backup vom Backup erledigt, hat danach oft eine Sorge weniger.

Im Web hat mancher Onlinejunkie längst den Überblick verloren, in welchen Netzwerken, Clouddiensten und Foren er angemeldet ist. Das ist ein weites Feld: In diesem knappen Beitrag muss das pauschale Plädoyer genügen, den Überblick zu behalten und die Komplexität zu verringern.

Konkreter wird es beim Umgang mit Cloudspeichern im Web (Dropbox, Onedrive, Google Drive et cetera), sofern es dort nur um das pure Datenkontingent geht: Bei heutigen Festplatten und Kapazitäten auf USB-Laufwerken oder Samba/Windows-Servern besteht keine Not, Benutzerdaten massenhaft ins Internet zu sichern – womöglich verstreut bei diversen Anbietern. Wer dies tut, weil er standortunabhängigen Zugriff auf die Daten haben will, sollte zumindest die Alternativen sehen:

- Viele Provider wie Telekom, Vodafone, 1&1 haben ein kostenfreies Cloudkontingent inklusive. Man ist als Kunde dieser Provider nicht auf US-Anbieter wie Google, Microsoft oder Dropbox angewiesen. Dasselbe gilt praktisch überall auch für das Mailkonto.
- Wer eine Homepage und damit einen virtuellen oder dedizierten Server bei einem Webhoster betreibt, hat neben seiner öffentlichen Homepage immer auch einen großzügigen Onlinespeicher. Damit kann man sowohl Datensicherung wie auch Datenfreigabe für andere über SSH oder auch über passwortgeschütztes HTTP erledigen.

Softwarefunktionen auslagern

Ein aufgeräumtes Netzwerk kann die einzelnen Geräte entlasten und deren Wartung vereinfachen, indem Software delegiert wird. Neben populärer Cloudsoftware von Google und Microsoft genügen auch lokale Netzmethoden. Linux ist ideal für solche auf mehrere Netzgeräte verteilte Software, aber auch Mac-OS kann uneingeschränkt mitspielen.

Open SSH mit X11: Für die Nutzung entfernter Software genügt ein überall aktivierter Open-SSH-Server. Wenn zum Beispiel ein Virtualisierer oder ein Mailpro-

gramm zum Zweck der Zentralisierung nur auf einem Rechner installiert ist, so startet der Befehl (Beispiel)

```
ssh -X ha@192.168.178.20 virtualbox
```

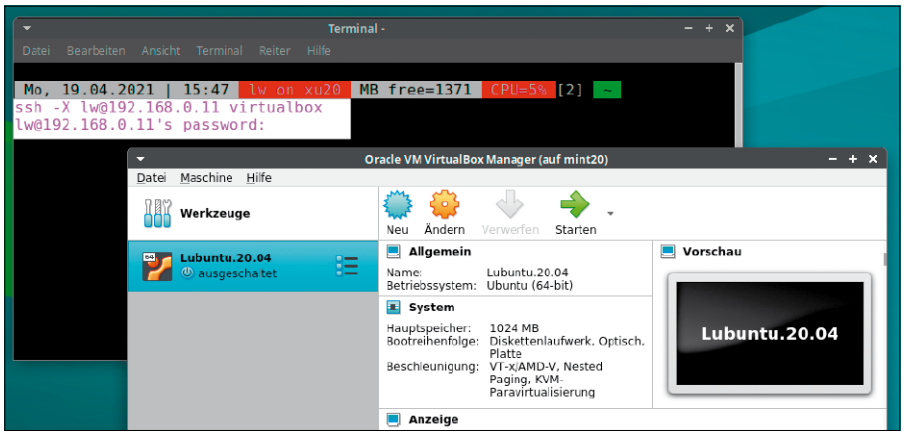
den SSH-Zugriff mit X-Forwarding, das angeschlossene Kommando „virtualbox“ lädt auch gleich das benötigte Programm. Der große Vorteil von X-Forwarding gegenüber VNC und Remotedesktop ist die Tatsache, dass der Rechner (hier jener mit Virtualbox) lokal ganz normal genutzt werden kann. Abgesehen vielleicht von einer geringen Leistungseinbuße, wird der lokale Benutzer wird vom Fernzugriff nicht gestört oder gar ausgesperrt.

Windows steht sowohl als zugreifender Client wie als Server etwas außen vor, obwohl es inzwischen einen Open-SSH-Client wie Server im Angebot hat (siehe „Einstellungen → Apps → Optionale Features“). Als SSH-Server kann es aber nur die Kommandozeile anbieten und als SSH-Client ist das Empfangen grafischer Fenster mit dem zusätzlichen Xming (X-Server für Windows, *www.straightrunning.com*) etwas umständlich und oft optisch unbefriedigend.

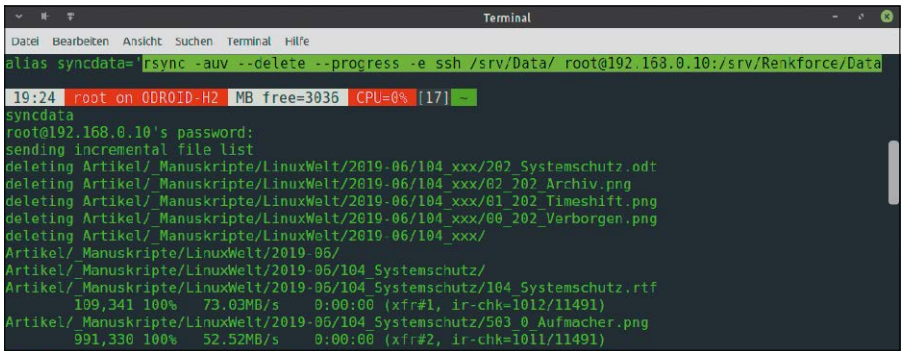
Desktopfreigaben: Sollen auch Windows-Rechner grafische Software von Linux-Maschinen mitbenutzen, ist ein VNC-Zugriff auf den gesamten Linux-Desktop die beste Lösung. Als Serversoftware auf den Linux-Rechnern eignet sich zum Beispiel x11vnc und als Zugriffsclient unter Windows etwa Tight VNC *www.tightvnc.com*). Linux-Rechner können sich mit dem universellen Remmina zu VNC-Servern verbinden.

Wenn Sie umgekehrt an einem Linux-System ein Windows-Programm benötigen, dann empfiehlt sich die Windows-Freigabe via Remotedesktop (Win-Pause und dort „Remoteeinstellungen → Remoteverbindung zulassen“). Aber Achtung: Diese im Heimnetzwerk sehr nützliche Funktion ist nur in der „Pro“-Version von Windows enthalten, nicht in „Home“. Der Zugriff mit Linux erfolgt auch hier über Remmina (RDP-Protokoll), der Zugriff mit einem anderen Windows über das Tool Remotedesktopverbindung („mstsc.exe“). Die Authentifizierungsdaten (lokales Konto des Windows-Systems) können in Remmina wie Mstsc gespeichert und automatisch übergeben werden.

Desktopfreigaben via VNC oder RDP sind elegant, optisch ansprechend und außerdem auch auf Android-Tablets oder iPads (Smartphones sind zu klein) über kostenlose Apps erreichbar.



Softwareaufgaben im Netzwerk verteilen: Nicht jeder Rechner muss jede Software installieren. X11-Forwarding und Desktopfreigaben ermöglichen Programmstarts auf entfernten Systemen.



Synchronisierung inklusive Löschen: Solche Rsync-Jobs mit Löschschalter räumen im Zielordner weg, was an der Quelle nicht vorliegt. Solches Aufräumen ist rational, braucht aber Kontrolle.

Einen Nachteil haben sie aber: Der lokale Nutzer wird durch den Zugriff gestört (VNC) oder ausgesperrt (RDP).

Datenabgleich und Säuberungen

Samba-Server sind auf Linux-PCs und Platinenhardware schnell eingerichtet und entlasten dann als Datenzentralen alle sonstigen Netzwerkrechner. Für das Auslagern oder Synchronisieren von Benutzerdaten ist das Tool Rsync (fast) überall die beste Wahl, da es alle Dateien original überträgt, daher uneingeschränkte Datennutzung ohne weitere Hilfsmittel erlaubt und auch rationale Säuberung beherrscht („--delete“). Rsync kann von jedem Netzrechner Daten beziehen oder dorthin kopieren, wo Open SSH läuft. Samba-Freigaben sind nicht nötig. Ein Beispielaufruf sieht etwa wie folgt aus:

```
rsync -auvP --delete --progress -e
  "ssh -p 22" /srv/Archiv/Musik/
  root@192.168.0.10:/srv/Archiv/
  Musik
```

Zwischen Linux- und Mac-Rechnern gibt es kaum eine pragmatischere Methode, große Datenmengen synchron zu halten. Das relativ umständliche Kommando muss nur einmal getestet und dann als Alias (etwa „syncmusic“) abgekürzt werden. Und es darf – angesichts „--delete“ – keine Zweifel geben, dass der erste Pfad (Quellpfad) den aktuellen Datenbestand enthält.

Windows kann da im Prinzip auch mitspielen, allerdings nicht mit seinem eigenen SSH-Client. Denn Rsync ist eine Client-Server-Lösung und Windows besitzt kein Rsync. Möglich wird SSH plus Rsync unter Windows nur über das optionale Linux-Subsystem.

Das aber dürfte vielen Windows-Nutzern für den Zweck der Datensynchronisierung als Overkill erscheinen. Eine Rsync-adäquate Methode, die auch Überflüssiges löschen kann („/mir“), bietet das Windows-Tool Robocopy:

```
robocopy d:\Archiv\Musik
  \\192.168.0.10\Musik/mir
```

Der entscheidende Unterschied ist hier, dass auf dem Rechner mit der IP-Adresse „192.168.0.10“ eine Samba-Freigabe „Musik“ angelegt sein muss. ■

Die LinuxWelt-Toolbox

Für Linux gibt es zahlreiche Programme, die aber nicht immer ganz einfach zu finden sind. Die LinuxWelt-Toolbox bietet Orientierung und ermöglicht die schnelle Installation der gewünschten Software.

VON THORSTEN EGGELING



Komfortable Installationen: Die LinuxWelt-Toolbox zeigt Programmbeschreibungen und Infolinks. Für die Installation oder den Start der gewünschten Software genügt meist ein Mausklick.

Schon nach einer Linux-Standardinstallation stehen die wichtigsten Programme und Systemtools sofort zur Verfügung. Weitere Software kann man über die Paketverwaltung installieren, außerdem lassen sich zusätzliche Paketquellen für zusätzliche Programme einbinden. Der direkte Download und nachfolgende Installation von Softwarepaketen sind ebenfalls möglich, daneben gibt es aktuellere Programme auch noch in systemunabhängigen Flatpak-, Snap- oder Appimage-Containern. Bei der Fülle des Angebots ist es nicht leicht, den Überblick zu behalten und ein geeignetes Programm für einen bestimmten Zweck zu finden. Hier hilft die LinuxWelt-Toolbox. Sie versammelt Anleitungen für die Installation und Nutzung von Software aus allen wichtigen Bereichen. Über das Tool können Sie installierte Programme aus einer Anleitung heraus direkt starten oder neu installieren.

Das Programm läuft unter Ubuntu ab Version 18.04, Linux Mint ab Version 19, Raspberry-Pi-OS und Debian 10 (Buster). Es lässt sich auch unter Windows 8.1/10 starten, etwa für die Übernahme von Befehlszeilen in ein Linux-Terminalfenster.

Die LinuxWelt-Toolbox installieren

Um alle Funktionen der LinuxWelt-Toolbox verwenden zu können, müssen xterm und apturl installiert sein. Nutzer von Ubuntu oder Linux Mint installieren die Programme im Terminal mit

```
sudo apt update
sudo apt install xterm apturl
```

Unter Debian/Raspberry-Pi-OS installieren Sie nur xterm, apturl steht hier nicht zur Verfügung. Xterm ist für den Start von Programmen und Shell-Scripts erforderlich, apturl dient zur Installation von Programmen über die grafische Oberfläche.

LinuxWelt-Toolbox starten: Entpacken Sie das Tool von der Heft-DVD aus dem Ordner „Software“ in Ihr Home-Verzeichnis. Im Verzeichnis „LinuxWelt-Toolbox“ finden Sie die Datei „lwToolbox_x86_64“ für 64-Bit-Systeme, die Sie über den Dateimanager per Doppelklick starten. Nutzer eines 32-Bit-Systems verwenden „lwToolbox_i386“ und für den Raspberry Pi eignet sich „lwToolbox_arm“. Unter Windows verwenden Sie „lwToolbox_x86_64.exe“ (nur 64 Bit).

Beim ersten Start prüft LinuxWelt-Toolbox, ob die erforderlichen Tools installiert sind. Wenn nicht, werden Sie zur Installation aufgefordert. Außerdem erfolgt eine Aufforderung zum Update der Tools-Datenbank. Klicken Sie auf „Download“, um die Datenbank zu aktualisieren.

Probleme beheben: Unter Linux sollten standardmäßig alle weiteren Voraussetzungen für LinuxWelt-Toolbox installiert sein. Sollte das Tool beim Start oder Updatedownload einen Fehler zeigen, starten Sie ein Terminal und wechseln (mit *cd*) in das Verzeichnis, in das Sie LinuxWelt-Toolbox entpackt haben. Hier starten Sie

```
./check_deps.sh
```

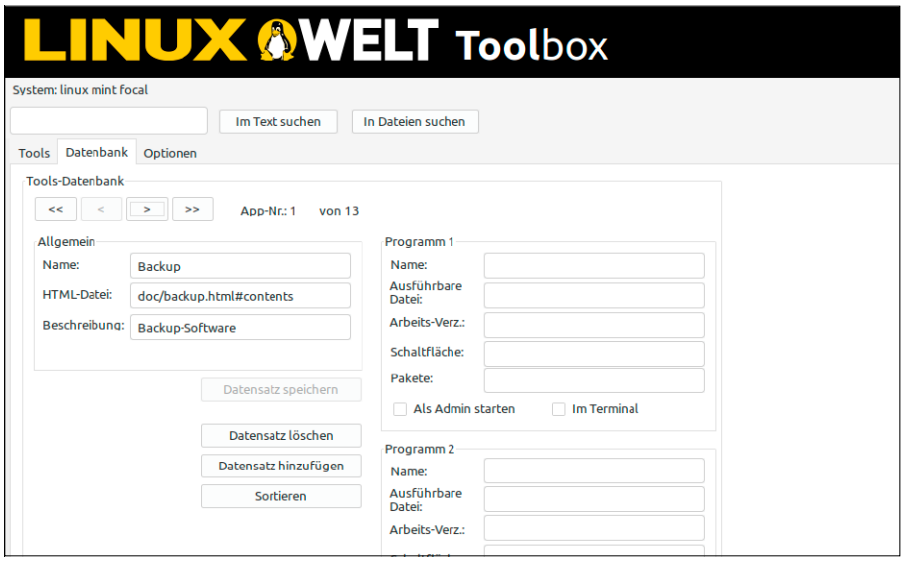
Das Bash-Script prüft, ob alle erforderlichen Bibliotheken sowie xterm und apturl vorhanden sind. Wenn nicht, bestätigen Sie die Installationen jeweils mit „J“ gefolgt von der Eingabetaste.

LinuxWelt-Toolbox konfigurieren

LinuxWelt-Toolbox versucht, das Linux-System automatisch zu erkennen, und zeigt das Ergebnis hinter „System:“ und auf der Registerkarte „Optionen“ an. Die Informationen bezieht die Toolbox aus der Datei „/etc/os-release“. Wichtig ist der Ubuntu-Codename, der für die Einbindung zusätzlicher Paketquellen erforderlich sein kann. Bei Linux Mint 20 und Ubuntu 20.04 lautet der Codename „focal“, bei Linux Mint 19 und Ubuntu 18.04 „bionic“. Welche Codenamen es gibt, erfahren Sie unter *https://wiki.ubuntu.com/Releases*. Sollte die automatische Erkennung nicht funktionieren, tragen Sie den Codenamen selbst auf der Registerkarte „Optionen“ ein und klicken auf „Speichern“.

Hinter „Terminal für Programmstarts“ steht „/usr/bin/gnome-terminal“. Sollte dieses Terminal nicht installiert sein, sucht die LinuxWelt-Toolbox nach „lxterminal“, „lxterm“ oder „xterm“ und trägt den Pfad dazu ein. Sie können aber auch selbst Ihr bevorzugtes Terminalprogramm eintragen.

Die Angabe hinter „Skript für erhöhte Rechte (root):“ verweist auf „Tools/exec_pkexec.sh“. Darüber kann das Passwort des Systemverwalters abgefragt werden, wenn das für einen Programmstart erforderlich ist.



LinuxWelt-Toolbox konfigurieren: Das Programm ist flexibel. Wer möchte, kann die Funktion der Schaltflächen ändern und darüber auch andere Tools installieren oder starten.



Software installieren: Unter Linux Mint und Ubuntu erfolgen Installationen über apturl. Das Tool zeigt eine kurze Beschreibung und fordert nach einem Klick auf „Installieren“ das Passwort an.

Die Datenbank der LinuxWelt-Toolbox

Die LinuxWelt-Toolbox verwendet XML-Dateien aus dem Unterverzeichnis „Tools“ als Datenbank. Über die Registerkarte „Datenbank“ können Sie die Inhalte bei Bedarf ändern und auch eigene Tools hinzufügen. Die Beschreibungstexte stammen aus den HTML-Dateien im Ordner „doc“. Diese lassen sich auch im Webbrowser aufrufen – eine Übersicht liefert die Datei „index.html“. Wenn Sie selbst Anpassungen vorgenommen haben, sichern Sie die Ordner „Tools“ und „doc“ vor einem Update des Tools, damit diese nicht verloren gehen.

Für eine individuell erweiterte Toolsammlung verwenden Sie die Rubrik „Benutzer“. Die Datei „doc/benutzer.html“ ist bereits vorhanden und kann mit eigenen Inhalten gefüllt werden. Basiskenntnisse in HTML sind dabei von Vorteil, Sie können sich aber an den Inhalten der anderen Dateien orientieren. Neue Einträge erstellen Sie auf der Registerkarte „Datenbank“ nach einem Klick auf „Datensatz hinzufügen“. Eine aussagekräftige Bezeichnung hinter „Name:“ ist erforderlich, außerdem der relative Pfad zu einer HTML-Datei („doc/[Dateiname]“). Die Angaben unter „Programm 1“ und „Programm 2“ sind optional. Sind die Felder ausgefüllt, erzeugt LinuxWelt-Toolbox eine oder zwei Schaltflächen, über die sich ein Programm installieren oder starten lässt.

Die LinuxWelt-Toolbox nutzen

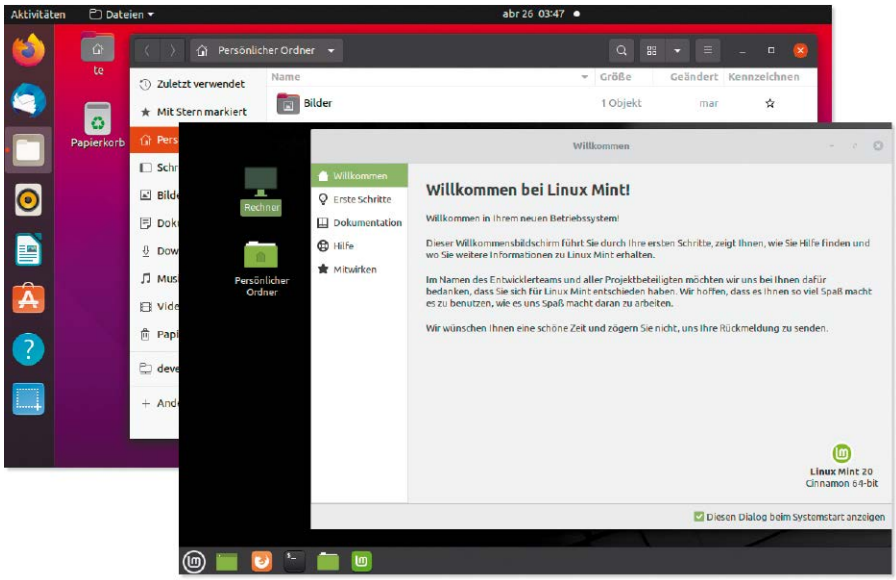
Das Programm zeigt links oben ein Auswahlfeld, über das Sie Kategorien wie „Ubuntu/Mint“, „Netzwerk“ oder „Multimedia“ ansteuern. Die Schaltflächen darunter führen dann zu den jeweiligen Rubriken. In den Beschreibungen gibt es meist Links auf weiterführende Informationen, die sich per Mausklick im Standardbrowser öffnen lassen. Über die blauen Schaltflächen installieren oder starten Sie Programme, die Informationen dafür sind in der Datenbank hinterlegt. Auch im Beschreibungstext gibt es Schaltflächen für den Start oder die Installation. Installationen erfolgen in der Regel über apturl, wobei das Passwort über ein Fenster angefordert wird. Ist apturl nicht vorhanden, kommt xterm zum Einsatz. Es wird eine Befehlszeile mit vorangestelltem „sudo“ übergeben und Sie tippen das Passwort im Terminal ein.

Für die manuelle Installation im Terminal verwenden Sie die angegebenen Befehlszeilen, die Sie über die Schaltfläche „Kopieren“ aus der Anleitung in die Zwischenablage kopieren, dann in einem Terminal mit Shift-Strg-V einfügen und mit der Eingabetaste starten.

Die Schaltflächen für den Start oder die Installation von Anwendungen funktionieren nur unter Linux. Wer LinuxWelt-Toolbox unter Windows verwendet, kann aber auch hier die Befehlszeilen in die Zwischenablage kopieren. In einer Putty-Fernsitzung oder in einem Fenster des Windows Subsystem für Linux (WSL) unter Windows 10 fügen Sie den Inhalt einfach per Klick auf die rechte Maustaste ein. ■

Tools für Ubuntu und Linux Mint

Linux-Systeme bringen standardmäßig eine umfangreiche Softwareausstattung mit. Die LinuxWelt-Toolbox liefert Informationen zu den nützlichsten Tools und hilft bei der Installation von Werkzeugen für spezielle Aufgaben.

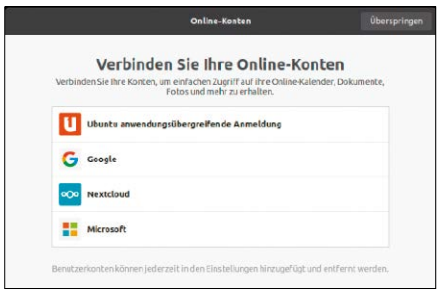


VON THORSTEN EGGELING

Die meisten Open-Source-Programme gibt es für alle Linux-Distributionen und auch für Windows und Mac-OS. Wir beschränken uns in diesem Special – mit Ausnahme der Rubrik „Raspberry Pi" – auf die weitverbreiteten und miteinander verwandten Systeme Ubuntu (Standard mit Gnome-Desktop) und Linux Mint (Cinnamon-Desktop). Einige Beschreibungen können auch für andere Systeme gelten, meist weichen aber beispielsweise die Paketbezeichnungen ab oder ein Tool ist für eine bestimmte Distribution nicht standardmäßig verfügbar. Alles rund um Ubuntu/Mint zu Themen wie Installation, Konfiguration und zusätzlicher Software finden Sie in der gleichnamigen Rubrik der LinuxWelt-Toolbox.

1. Ubuntu/Mint installieren und einrichten

Auch wenn Ubuntu und Linux Mint einen identischen Unterbau verwenden, gibt es doch einige Unterschiede. Die Installation beider Systeme läuft in etwa gleich ab, aufgrund der beiden Desktopumgebungen – Gnome und Cinnamon – kommen aber andere Oberflächen beziehungsweise Tools für die Konfiguration zum Einsatz. Hilfe bei der Erstkonfiguration bietet Linux Mint über den „Willkommensbildschirm", den Linux Mint nach der Anmeldung automatisch lädt, solange Sie das Kästchen rechts unten aktiviert lassen. Sie können ihn aber jederzeit über das Menü und „Systemverwaltung → Willkommensbildschirm" starten. Der Willkommen-Dialog nennt unter „Erste Schritte" die wesentlichen Einrichtungspflichten, die Sie der Reihe nach abarbeiten können. Was dabei zu beachten ist, lesen Sie in der LinuxWelt-Toolbox unter „Linux Mint 20 Praxis".



Ubuntu fragt nach der Neuinstallation einige Informationen ab, beispielsweise zu Onlinekonten.

Ergänzend dazu zeigt „Linux Mint Lösungen", welche Schritte bei der Beseitigung von Systemproblemen helfen.

Auch bei Ubuntu startet nach der Neuinstallation ein Willkommensbildschirm. Der hilft jedoch nur bei der Einrichtung von verknüpften Onlinekonten, der Aktivierung von Ortungsdiensten sowie des Livepatch-Dienstes (Kernel-Updates ohne Neustart). Für alles andere müssen Sie sich durch die umfangreichen „Einstellungen" hangeln. Auf was man bei der Ubuntu-Neuinstallation achten sollte und was für die Konfiguration wichtig ist, lesen Sie unter „Ubuntu-Installation" und „Ubuntu 20.04". „Ubuntu Lösungen" hilft bei der Beseitigung von bekannten Systemproblemen.

2. Desktopumgebungen für Ubuntu und Linux Mint

Bereits bei der Installation einer Linux-Distribution entscheiden Sie sich für eine Desktopoberfläche. Die Auswahl ist größtenteils Sache des Geschmacks oder der Gewohnheiten und auch nicht zwingend an eine bestimmte Linux-Distribution gebun-

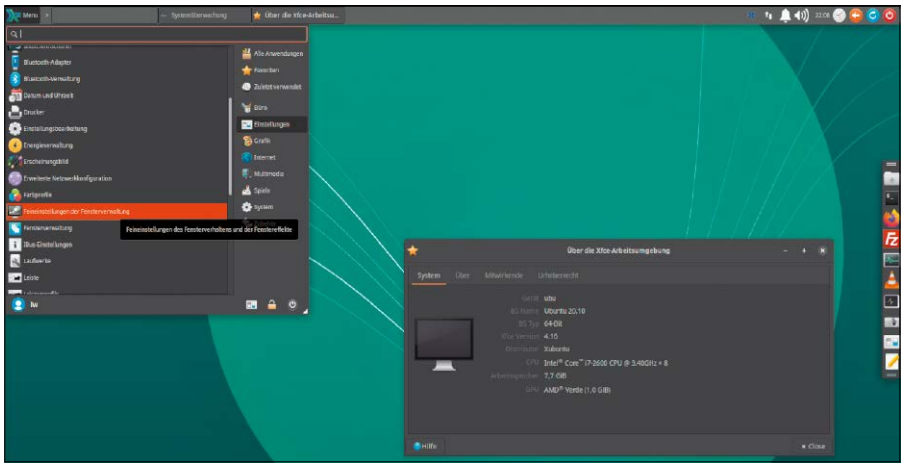
den. Es kann jedoch auch technische Gründe für die Entscheidung geben. Einige Desktopumgebungen und Linux-Systeme eignen sich besser für ältere oder weniger leistungsfähige Rechner. Für halbwegs aktuelle Rechner ist jedoch keine Ubuntu/Mint-Edition eine Herausforderung. Wer eine Desktopumgebung erst einmal testen will, verwendet ein Livesystem oder installiert Linux in einer virtuellen Maschine (siehe Punkt 9). Die Downloadadressen der Distributionen finden Sie in der LinuxWelt-Toolbox unter „Desktops“.

Es ist auch möglich, die Desktopumgebung bei einem bereits installierten System zu wechseln. Die grafische Oberfläche eines Linux-Systems ist eine installierbare Software wie jede andere auch – und somit beliebig austauschbar. Im Prinzip lässt sich jede Desktopumgebung in jeder Distribution installieren, wenn die nötigen Programmpakte zur Verfügung stehen. Der Desktopwechsel gelingt jedoch nicht immer ohne Schwierigkeiten. Manchmal fehlen Pakete, die Konfigurationsdateien sind nicht optimal angepasst oder es gibt unerwünschte Auswirkungen auf die ursprüngliche Desktopumgebung. Ein Upgrade der Distribution kann ebenfalls fehlschlagen, insbesondere wenn eine besonders aktuelle Desktopumgebung nicht aus den Standard-Paketquellen stammt. Wir beschreiben die manuelle Installation in der LinuxWelt-Toolbox unter „Desktops“ dennoch, weil erfahrene Linux-Nutzer die Probleme mit etwas Internetrecherche beheben können. Bei produktiv genutzten PCs raten wir vom Wechsel der Desktopumgebung ab.

3. Tuningtool für den Ubuntu-Desktop

Wichtige zuätzliche Einstellungsoptionen für Gnome bietet das Tool gnome-tweaks („Optimierungen“ auf deutschem System). Da die meisten Gnome-Nutzer das Tool für unentbehrlich halten und notfalls nachinstallieren, bringen einige Gnome-Distributionen das Programm bereits mit – Ubuntu 20.04/21.04 allerdings nicht. Mit gnome-tweaks ist es möglich, Arbeitsflächen, Schriftbild, Fensterverhalten, Fensterschaltflächen und Fensteroptik sowie die Gnome-Erweiterungen genauer zu justieren.

Installation: Eine ausführliche Funktionsbeschreibung und Installationsanleitung liefert die LinuxWelt-Toolbox nach einem Klick auf „Tweak-Tools“.



Desktopalternative: XFCE ist ein relativ flinker Desktop, der sich auch für ältere Hardware eignet. Trotzdem ist die Oberfläche besonders anpassungsfähig.

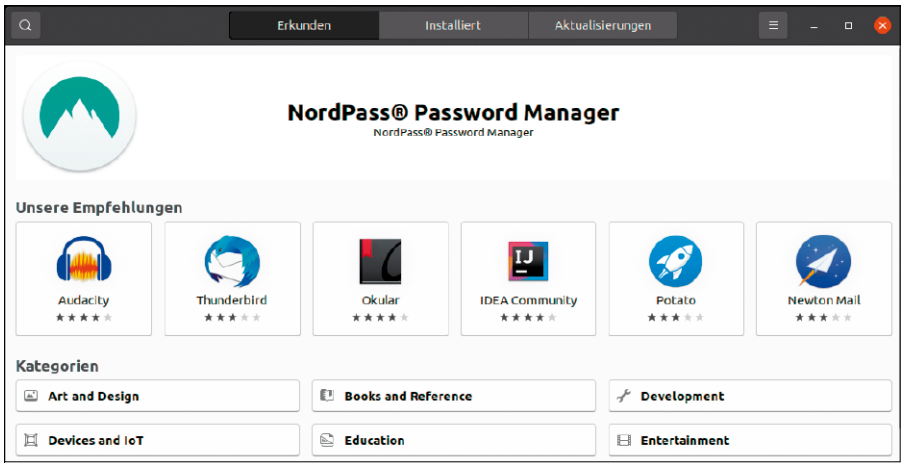
4. Softwarepakete suchen und installieren

Bei Ubuntu ist das Programm „Ubuntu Software“ die erste Anlaufstelle für die Suche nach neuer Software. Es lässt sich über das Icon im Dock oder eine Suche nach Software über „Aktivitäten“ starten. Ubuntu Software zeigt Programmempfehlungen, Sie können nach Software suchen oder in Kategorien wie „Musik und Audio“ oder „Spiele“ stöbern. Benutzer von Linux Mint nutzen die „Systemverwaltung → Anwendungsverwaltung“ für den gleichen Zweck. Fortgeschrittene Linux-Nutzer verwenden meist das Kommandozeilentool apt, mit dem sich jede Software aus den Paketquellen installieren lässt, denn Ubuntu Software bietet nur eine begrenzte Auswahl an. Eine Alternative ist Synaptic, das bei Linux Mint bereits vorinstalliert ist. Es bietet wie apt den Zugang zu allen verfügbaren Softwarepaketen. Sie finden Synaptic bei Linux Mint im Menü „Systemverwaltung → Synaptic-Paketverwaltung“. Das Tool arbeitet schnell und ermöglicht vor allem eine gezieltere Paketauswahl. Meist genügt die Eingabe eines Suchbegriffs in das Eingabefeld unter „Schnellauswahl-Filter“. Oder Sie klicken auf die Schaltfläche „Suche“ und tippen den Suchbegriff ein. Über das Auswahlfeld darunter lässt sich der Bereich beispielsweise auf „Name“ oder „Beschreibung und Name“ eingrenzen. Per Klick auf „Einstellungen → Paket-

WENN DIE SOFTWAREINSTALLATION NICHT FUNKTIONIERT

Es kann jeweils nur ein Tool auf die Paketdatenbank zugreifen. Daher ist es möglich, dass apt im Terminal eine Meldung wie „Konnte keinen exklusiven Zugang zur Sperrdatei /var/lib/dpkg/lock-frontend erhalten.“ ausgibt oder Synaptic mit einer ähnlichen Nachricht keine Software installieren möchte. In diesem Fall läuft wahrscheinlich gerade ein automatisches Update im Hintergrund. Warten Sie einfach, bis der Vorgang abgeschlossen ist, und probieren Sie es dann noch einmal. Manchmal blockiert das automatische Update den Rechner jedoch für eine längere Zeit oder es beendet sich nicht ordnungsgemäß. Starten Sie dann Linux neu. Sollte ein Update tatsächlich noch nicht abgeschlossen sein, werden Sie benachrichtigt, und der Linux-Neustart erfolgt erst nach Beendigung des Updates.

Wer das Problem häufiger hat, sollte bei Ubuntu über „Anwendungen & Aktualisierungen“ unter „Aktualisierung“ den Punkt „Wenn Sicherheitsaktualisierungen verfügbar sind“ auf „Sofort anzeigen“ stellen. Mit diesen Einstellungen muss man allerdings selbst daran denken, das System möglichst täglich mit dem manuellen Aufruf der Aktualisierungsverwaltung auf Updates zu überprüfen. Bei Linux Mint ist die automatische Aktualisierung standardmäßig abgeschaltet.



Softwarezentrale: Ubuntu Software zeigt Softwareempfehlungen und lädt zum Stöbern ein. Die Alternativen apt und Synaptic ermöglichen aber den Zugriff auf jede installierbare Software.

quellen“ gelangen Sie zum Fenster „Anwendungen & Aktualisierungen“. Auf der Registerkarte „Andere Programme“ lässt sich festlegen, welche Repositorien die Paketverwaltung berücksichtigt.

Installation: Wechseln Sie in der LinuxWelt-Toolbox über das Ausklappmenü in die Rubrik „Ubuntu/Mint“. Ubuntu-Nutzer installieren Synaptic per Klick auf die Schaltflächen „Paketverwaltung“ und „Synaptic installieren“.

5. Noch mehr Software dank Containerformaten

Die traditionelle Paketverwaltung unter Linux biete prinzipielle Sicherheitsvorteile gegenüber dem Download aus nicht verifizierten Quellen. Auf der anderen Seite klagen Anwender über mangelnde Flexibilität und Aktualität und Entwickler über den enormen Aufwand, ihr Programm für jede Linux-Distribution und jede Distributionsversion einzeln pflegen zu müssen. Angesichts dieses Dilemmas wurde die einstmals strikte Softwareverteilung unter Linux bereits an mehreren Stellen aufgeweicht: PPAs (Personal Package Archives) geben Entwicklern die Möglichkeit, ihre aktuelle Software außerhalb der Distributionsquellen bereitzustellen. Technisch entsprechen PPAs aber dem klassischen Weg, ein Programm für genau eine Distributionsversion anzubieten. Containerformate gehen einen großen Schritt weiter: Sie bieten distributionsunabhängige Software und müssen daher alles, was ein Programm braucht, selbst mitbringen. Das vereinfacht den Softwarebezug für den Anwender und verringert den Aufwand beim Softwarehersteller. Andererseits entstehen Nachteile durch erheblich größere Downloads, hohen Festplattenbedarf, erhöhte RAM- und CPU-Ansprüche und – zum Teil – wachsende Komplexität.

Snap-Container enthalten vollständige Anwendungen inklusive aller abhängigen Bibliotheken und laufen unabhängig vom restlichen System. Dadurch können Softwareentwickler neueste Programmversionen schneller bereitstellen, weil sie keine Detailanpassungen für einzelne Distributionen und Distributionsversionen leisten müssen.

Die Sandbox-Technik der **Flatpaks** stellt isolierte Container mit allen notwendigen Komponenten bereit. Auch hier ist eine Laufzeitumgebung Voraussetzung, die sich aber in allen Distributionen installieren lässt.

Appimages haben gegenüber den technisch komplexeren Techniken Snap und Flatpak einen entscheidenden Vorteil: Auf dem Zielrechner ist keinerlei Werkzeug erforderlich – keine Laufzeitumgebung (Runtime), kein Paketwerkzeug. Die Images werden einfach heruntergeladen, ausführbar geschaltet und – laufen.



Appimage-Programme: Bei Appimage stecken alle erforderlichen Komponenten in einer einzelnen Datei. Für den Start müssen Sie die Datei nur ausführbar machen.

Installation: Bei Linux Mint ist Flatpak standardmäßig mit dabei, bei Ubuntu Snap. Die jeweils andere Technik lässt sich jedoch bei beiden Systemen nachinstallieren. Was dazu nötig ist, erfahren Sie in der LinuxWelt-Toolbox unter „Portable Tools“. Appimages laufen unter Ubuntu und Linux Mint und benötigen keine Extrasoftware. Downloadadressen einiger bekannter Programme finden Sie ebenfalls unter dem Punkt „Portable Tools“.

6. Tools für die Dateiverwaltung

Dateien kopieren, löschen oder verschieben gehört zu den täglichen Handgriffen. Der Dateimanager ist daher eines der wichtigsten Tools. Bei Linux gibt es mehrere davon. Je nachdem, welche Distribution beziehungsweise Desktopoberfläche installiert ist, zeigt sich standardmäßig Nautilus (Ubuntu Unity), Dolphin (KDE) oder Nemo (Cinnamon/Linux Mint).

Nautilus und Nemo bieten praktische Erweiterungen, etwa um die Größe von mehreren Bildern zu ändern oder Prüfsummen von Dateien zu berechnen. Außerdem lassen sich in beide Dateimanager Scripts einbinden. Über das Kontextmenü können Sie dann etwa Ordner schnell packen oder Audiodateien konvertieren. Für Nemo gibt es eine Erweiterung, über die sich ein Terminalfenster im Dateimanager einblenden lässt, das automatisch in den jeweils geöffneten Ordner wechselt.

Installation: Nautilus, Nemo und Dolphin lassen sich unter allen Ubuntu-Varianten installieren. Die Pakete sind in den Standardrepositorien enthalten. Über die LinuxWelt-Toolbox finden Sie alle relevanten Paketnamen und Funktionen für die schnelle Installation nach einem Klick auf „Dateimanager“.

Weitere Alternativen gibt es in der Rubrik „Zwei-Fenster-Dateimanager“.

7. Eigene Dateien und System sichern

Für die Sicherung der Benutzerdateien ist bei Ubuntu standardmäßig ein Tool installiert, das Sie per Suche im Dash nach „Datensicherungen“ finden. Linux-Mint-Nutzer rufen ein ähnliches Tool über „Systemverwaltung → Datensicherungswerkzeug“ auf.

Für regelmäßige Backups des gesamten Systems empfehlen wir das Tool Timeshift. Es erstellt Momentaufnahmen des Dateisystems, die beim Zurückspielen einen vorherigen Zustand wiederherstellen. Der erste Sicherungspunkt ist immer ein komplettes Backup der Systemverzeichnisse und mit einigen Gigabyte recht groß. Die weiteren Wiederherstellungspunkte sind dann aber deutlich kleiner, da Timeshift nur noch die Unterschiede zum vorherigen Sicherungspunkt speichert.

Installation: Die Installationshinweise zu Timeshift finden Sie über die LinuxWelt-Toolbox nach einem Klick auf die Schaltfläche „Backup“. Bei Linux Mint ist Timeshift standardmäßig installiert.

8. Nützliche Linux-Systemtools

Wie viel Speicher steckt im Rechner? Wo ist die Konfigurationsdatei für den Samba-Server? Wie beende ich ein eingefrorenes Programmfenster? Und wo ist das Mountverzeichnis für das eingehängte Netzlaufwerk? Antworten auf diese und viele weitere Fragen geben wir in einem längeren Beitrag, den Sie in der LinuxWelt-Toolbox per Klick auf „Systemtools in der Praxis“ aufrufen. Dabei kommen prominente grafische Programme unter Ubuntu und Linux Mint zu Wort, aber den größeren Anteil erhalten die typischen Terminalprogramme.

Diese haben nämlich zwei entscheidende Vorteile: Erstens funktionieren sie auf allen Linux-Distributionen, zweitens sind sie alternativlos, wenn ein Server per SSH im Terminal administriert wird. Ein Teil der Tools ist bei Ubuntu oder Linux Mint standardmäßig installiert, wenn nicht, finden Sie in der LinuxWelt-Toolbox eine Installationsanleitung.

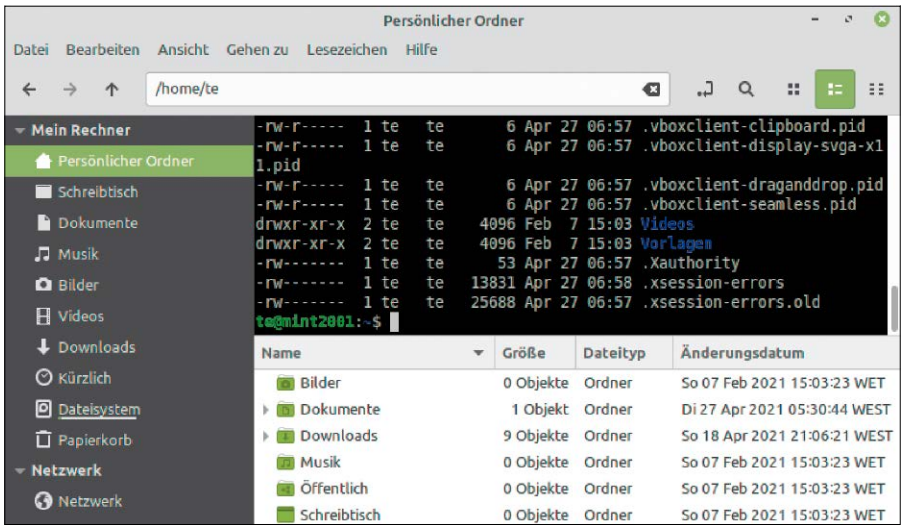
9. Virtualisierung und Windows-Programme

In einer virtuellen Maschine können Sie weitere Betriebssysteme installieren und starten. Alles läuft im Fenster und Sie müssen Linux nicht beenden, wenn Sie beispielsweise schnell ein Windows-Programm benötigen. Als Virtualisierungssoftware ist Virtualbox in den Standard-Paketquellen enthalten. Darüber lässt sich die Open-Source-Variante installieren, die aber meist nicht ganz aktuell ist und einige Funktionen vermissen lässt, beispielsweise die Unterstützung von USB-Geräten. Der Hersteller Oracle (*www.virtualbox.org*) stellt jedoch eigene Linux-Repositorien bereit, über die sich die jeweils aktuelle Version einrichten lässt.

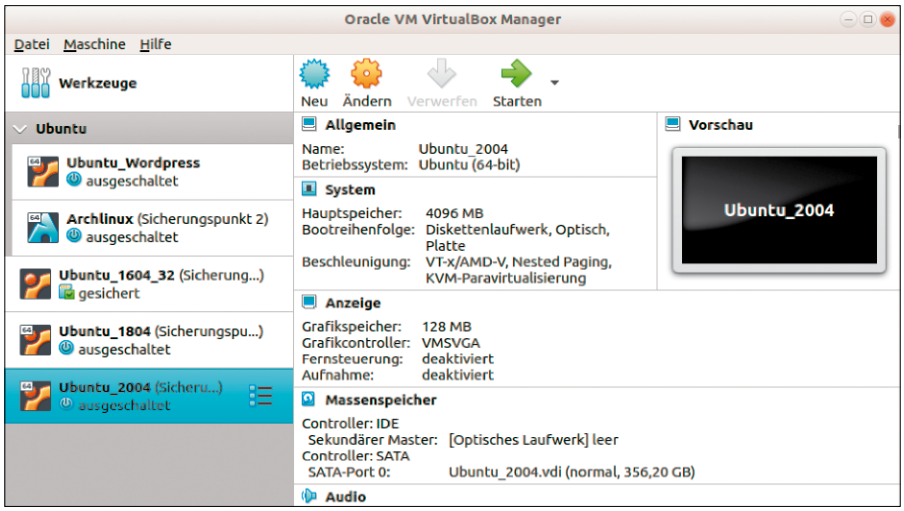
Installation: Klicken Sie in der LinuxWelt-Toolbox auf „Virtualisierung“. Sie finden hier eine Schaltfläche für den Import der Oracle-PGP-Schlüssel, mit dem die Pakete digital signiert sind. Danach klicken Sie auf „Virtualbox installieren“. Die Befehlszeilen für die manuelle Installation sind darunter zu finden.

Alternative: Für den Start von Windows-Programmen unter Linux eignet sich auch Wine, das Windows-Funktionen unter Linux nachbildet. Am einfachsten gelingt die Installation von Windows-Software über Playonlinux. Die Softwareauswahl für Wine ist jedoch begrenzt. Oft funktionieren nur ältere Programmversionen problemlos. Sehen Sie auf *www.playonlinux.com* nach, ob die von Ihnen benötigte Software unterstützt wird.

Installation: Für die Einrichtung von Playonlinux, die automatisch die passende Wine-Version anfordert, klicken Sie in LinuxWelt-Toolbox auf „Virtualisierung“ und dann auf „Playonlinux installieren“. ■



Nemo aufbohren: Die Erweiterung „nemo-terminal“ baut ein Terminalfenster in den Dateimanager ein. Das ist für Anwender nützlich, die häufig auf der Kommandozeile arbeiten.



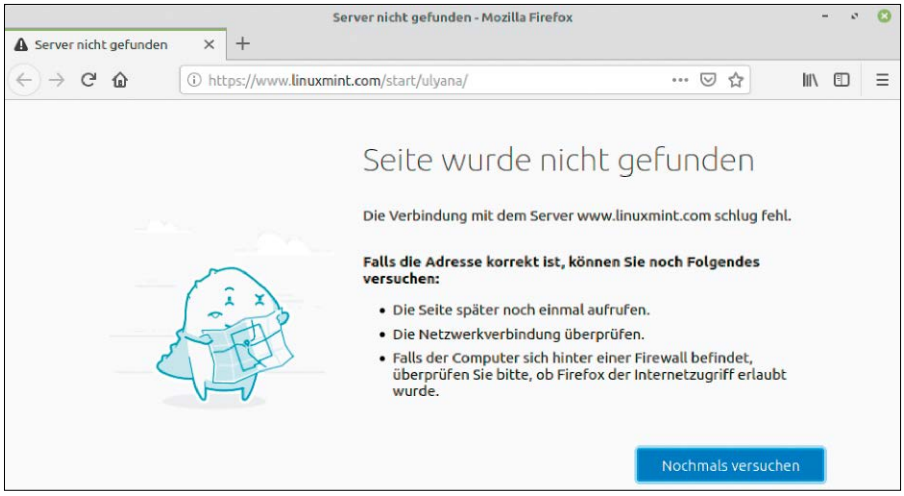
Virtuelle PCs: Mit Virtualbox starten Sie ein zweites Betriebssystem in einem Fenster. Darin können Sie Software bedenkenlos ausprobieren oder neue Betriebssysteme testen.

Software für das Netzwerk & Internet

Netzwerkprobleme lassen sich dank nützlicher Tools unter Linux meist schnell beheben, und auch für Dateifreigaben oder Webserver hat Linux die passende Software zu bieten. Die Konfiguration ist aber nicht immer ohne Tücken.

VON THORSTEN EGGELING

Bei Linux handelt es sich um ein ausgesprochenes Netzwerkbetriebssystem. Nicht ohne Grund laufen die meisten Server im Internet und auch viele Server in Unternehmen und Behörden unter Linux. Private Anwender profitieren ebenfalls: Die Netzwerkkonfiguration von Linux gilt als zuverlässig und sicher. Probleme kann es allerdings bei der Treiberversorgung sehr neuer Ethernet-Netzwerkadapter oder WLAN-Adapter geben. Hinweise und Lösungen dafür finden Sie beispielsweise in der LinuxWelt-Toolbox in der Rubrik „Hardware“. In der Rubrik „Netzwerk“ der LinuxWelt-Toolbox haben wir Ratgeber rund um das Thema gesammelt. Sie erfahren, welche Tools es für die Analyse des Netzwerks gibt und wie sich Serverdienste konfigurieren lassen. Ergänzend behandeln wir die Themen Fernzugriff und Fernwartung sowie Onlinezusammenarbeit.



Ohne Netz: Wenn der Browser keine Webseiten anzeigt, kann die Internetverbindung ausgefallen sein. Oder der Rechner kann keine Verbindung herstellen, wofür es mehrere Ursachen geben kann.

1. Netzwerkprobleme beheben

Am Netzwerk sind mehrere Komponenten beteiligt: Router, Ethernet-Kabel, WLAN, Netzwerkadapter, Treiber für die Adapter, nicht zuletzt der Internetanbieter. Bei der Suche nach Fehlern führt nur eine systematische Herangehensweise zum Ziel. Dabei sollte man einige Fehlerursachen schnell ausschließen und sich Schritt für Schritt der Fehlerquelle nähern. Man kann im Netzwerk die folgenden Problembereiche unterscheiden:

A: Der Internetzugriff funktioniert bei keinem Gerät. Der Browser meldet „Seite wurde nicht gefunden“. Rechner im eigenen Netzwerk sind aber erreichbar, beispielsweise Dateifreigaben. Das Netzwerk funktioniert also grundsätzlich, aber der Internetzugang nicht. Hier liegt eine Störung beim DSL-Anschluss vor oder der Router ist falsch konfiguriert oder defekt.

B: Nur bei einem einzelnen Rechner funktioniert der Internetzugang über den Browser nicht, andere Rechner im Netzwerk sind erreichbar. Hier ist wahrscheinlich der Browser falsch konfiguriert oder eine Einstellung verhindert den Internetzugang.

C: Ein einzelner Rechner hat keinen Internetzugriff, Geräte im lokalen Netzwerk sind dort ebenfalls nicht erreichbar. Der betroffene Rechner hat keine Netzwerkverbindung. Prüfen Sie die Netzwerkkonfiguration und die Funktion des Netzwerkadapters.

D: Kein Rechner kann auf das Internet zugreifen, das lokale Netzwerk ist auch nicht zu erreichen. Das Netzwerk funktioniert hier grundsätzlich nicht. Wahrscheinlich ist der Router defekt oder falsch konfiguriert. Tritt das Problem im WLAN auf, prüfen Sie die WLAN-Konfiguration des Routers.

Am besten nähert man sich dem Fehler abwechselnd von beiden Enden des Netzwerks aus:

1. Ist das Ethernet-Kabel fest mit dem PC verbunden? Ist der WLAN-Adapter im Notebook aktiviert? Einige Geräte besitzen einen Schalter, über den sich WLAN und Bluetooth abschalten lassen. Oft ist das auch über eine Tastenkombination möglich.

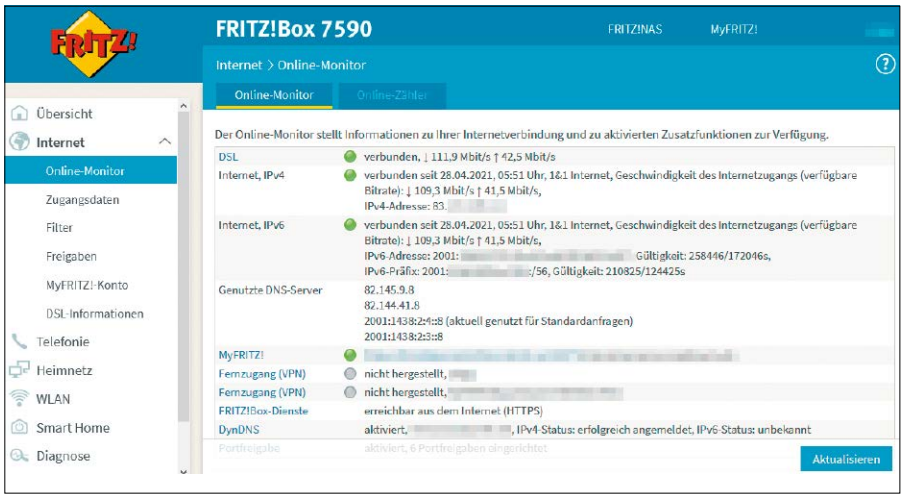
2. Sind das Ethernet-Kabel und DSL-Kabel korrekt mit dem Router verbunden? Leuchten am Router Kontroll-LEDs, die eine Verbindung zum Internetprovider, die Ethernet- und WLAN-Aktivitäten signalisieren?

3. Hat Linux den Netzwerk/WLAN-Adapter erkannt und ist dieser aktiv? Sehen Sie bei Ubuntu in den „Einstellungen“ unter „Netz-

werk“ nach, bei Linux Mint gehen Sie im Menü auf „Einstellungen → Netzwerk“.

4. Ist der Router über seine IP-Adresse erreichbar? Geben Sie im Browser die IP-Adresse des Routers ein, etwa „http://192.168.0.1“ oder „http://192.168.1.1“. Bei einer Fritzbox lautet die Adresse standardmäßig „http://192.168.178.1“, alternativ funktioniert auch „http://fritz.box“. Wenn diese Verbindung nicht funktioniert und die Webseite des DSL-Routers nicht im Browser erscheint, ist der Router falsch konfiguriert oder defekt. Wiederholen Sie den Test mit einem anderen PC oder Notebook und einem anderen Ethernet-Kabel.

Gehen Sie in der LinuxWelt-Toolbox auf „Netzwerk“ und dann auf die Schaltfläche „Netzwerkprobleme“. Im Ratgeber finden Sie Tipps zu den Tools, die Sie für die Untersuchung des Netzwerks verwenden können.



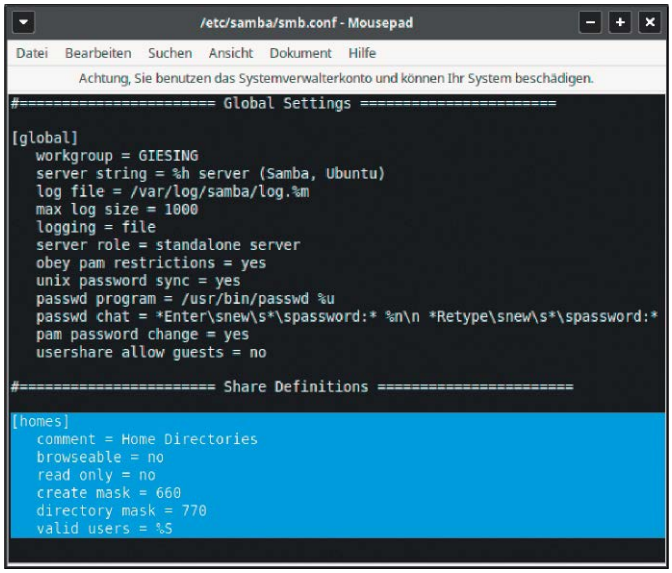
Internetzugriff: Der Router zeigt an, ob eine Internetverbindung besteht. Wenn nicht, ist die Verbindung zum Anbieter unterbrochen oder die Zugangsdaten sind falsch.

2. Datenaustausch mit Samba

Das SMB/CIFS-Protokoll, unter Linux als Samba bekannt, ermöglicht den Dateitransfer zwischen Windows und Unix-basierenden Systemen und den Zugriff auf Netzwerkdrucker. Der Samba-Client ist unter Ubuntu und Linux Mint standardmäßig installiert. Sie können daher über den Dateimanager auf Linux- und Windows-Freigaben zugreifen (siehe Punkt 3). Wenn der Linux-PC als Dateiserver dienen soll, muss man den Samba-Server installieren. Samba verwendet als globale Konfigurationsdatei „/etc/samba/smb.conf“. Darin sind die allgemeinen Einstellungen für den Samba-Server und die Freigaben festgelegt.

Bei der Konfiguration der Freigaben ist zu beachten, welche Nutzer Lese- und Schreibzugriff erhalten sollen und ob dafür auch die passenden Rechte im Linux-Dateisystem gesetzt sind.

Eventuell müssen Sie die Benutzerkonten unter Linux erst erstellen und Passwörter für den Zugriff festlegen. Wie Sie dabei vorgehen müssen und wie die Konfigurationsdatei aussehen muss, erfahren Sie in der LinuxWelt-Toolbox nach einem Klick auf „Samba“.



Dateifreigaben konfigurieren: In die Datei „/etc/smb.conf“ tragen Sie die Basiseinstellungen ein und erlauben allen Nutzerkonten den Zugriff auf das Home-Verzeichnis.

3. Probleme mit Samba-Freigaben beheben

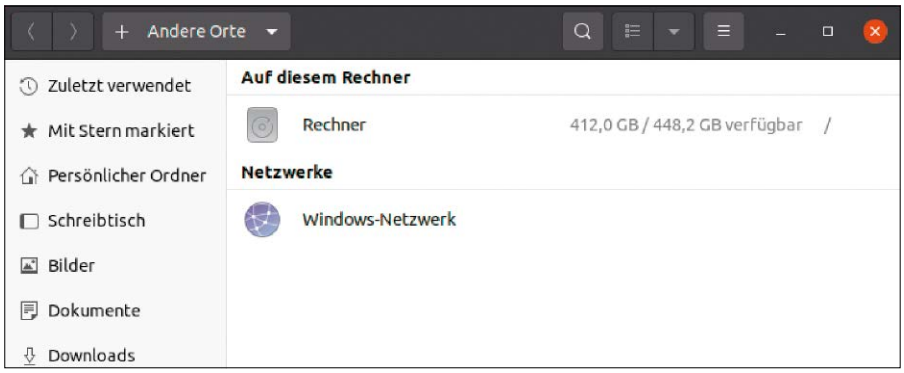
Der Zugriff auf Ordnerfreigaben erfolgt beispielsweise unter Ubuntu 20.04 im Dateimanager Nautilus über „Andere Orte –› Windows-Netzwerk“. Unter Windows gehen Sie im Explorer auf „Netzwerk“. Bei aktuellen Linux-Versionen und Windows 10 funktioniert beides jedoch nicht mehr. Windows 10 und Ubuntu 20.04 zeigen keine Linux-Rechner mit Samba-Freigaben an.

Das bisher Gesagte gilt nur für aktuelle Betriebssysteme mit einer Standardkonfiguration. Bei älteren Samba-Installationen vor Version 4.11 funktioniert der Zugriff über den Dateimanager, ebenso bei Windows 7 und 8.1 sowie vielen älteren NAS-Geräten.

Die Auflistung von Netzwerkfreigaben fand bisher über das Protokoll SMB 1.0 statt. Es ist gut 30 Jahre alt und enthält mehrere

TIPPS & TOOLS FÜR DAS HEIMNETZWERK

Linux ist für das Netzwerk geschaffen und macht als Netzwerkclient wie als Server eine glänzende Figur. In der LinuxWelt-Toolbox finden Sie nach einem Klick auf „Netzwerk-Tools“ einen Beitrag, der Basiswissen und vertiefende Tipps für ein optimiertes Heimnetz liefert. Dabei geht es um das lokale LAN- und WLAN-Netz mit typischen Geräten, Kommunikationsprotokollen, Freigaben und Serververwaltung. Alle genannten Tools wie ping, ip, iwlist, arp oder nmap sind bei Linux meist schon vorinstalliert oder lassen sich aus den Standardrepositorien nachrüsten.



Zugriff auf Samba-Server: Ubuntu zeigt im Dateimanager das „Windows-Netzwerk“ zwar an, die Freigaben werden jedoch nicht aufgelistet. Ursache ist das obsolete SMB-1.0-Protokoll.

Sicherheitslücken. Deshalb ist SMB 1.0 in Windows 10 meist deaktiviert. Ob das tatsächlich der Fall ist, hängt von der Edition und der Netzwerkumgebung ab. Wie Sie das prüfen und SMB 1.0 gegebenenfalls wieder aktivieren, lesen Sie in der Linux-Welt-Toolbox nach einem Klick auf die Schaltfläche „Samba-Probleme beheben“.

Wer SMB 1.0 aus Sicherheitsgründen nicht aktivieren möchte, tippt die Adresse in der folgenden Form

`smb://[Server]/[Freigabe]`

in die Adresszeile (Strg-L) des Linux-Dateimanagers ein. Unter Windows verwenden Sie in der Adresszeile des Windows-Explorers diese Adresse:

`\\[Server]\[Freigabe]`

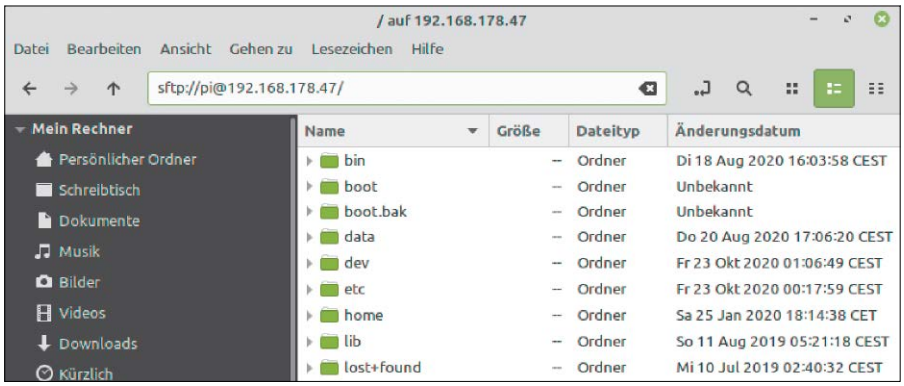
Für etwas mehr Komfort können Sie Linux das Protokoll WS-Discovery beibringen. Damit werden Samba-Server und ihre Freigaben unter Windows sichtbar. Auf den Linux-Dateimanager hat das jedoch keinen Einfluss. Die nötige Software laden Sie über *https://github.com/christgau/wsdd/releases* herunter. Eine Anleitung zur Installation finden Sie in der LinuxWelt-Toolbox unter „Samba-Probleme beheben“.

4. Alternative Methoden für den Datenaustausch

Samba ist zwar weitverbreitet und überall verfügbar, das Protokoll gilt jedoch als nicht besonders schnell. Alternative Protokolle und Dienste versprechen zwar auch nicht mehr Komfort, können aber oft bei der Geschwindigkeit punkten. Der plattformübergreifende Zugriff auf Dateien ist bei den meisten Protokollen ebenfalls möglich.

Der Linux/Unix-Klassiker ist das Network File System (NFS). NFS bietet in etwa die gleichen Funktionen wie Samba, aber keine Benutzerauthentifizierung. Berechtigte Rechner beziehungsweise IP-Adressen oder Netzwerkbereiche werden auf dem Server konfiguriert und erhalten dann Lese- oder Schreibzugriff. Da NFS wie auch Samba für das eigene lokale Netzwerk gedacht sind, stellt das kein besonderes Sicherheitsrisiko dar. Windows 10 unterstützt NFS ab Version 1709, allerdings nur in der Pro-Version.

Weitere Alternativen sind Webdav mit einem Apache-Server sowie SSH/SFTP. Linux-Systeme können damit als Clients standardmäßig umgehen, für Windows benötigen Sie teilweise zusätzliche Software. Wie Sie einen NFS-, Webdav- oder SSH-Server installieren und Freigaben konfigurieren, lesen Sie in der LinuxWelt-Toolbox nach einem Klick auf „Samba-Alternativen“. Hinweise zu Linux als Webdav-Client sowie einer besonders sicheren SFTP-Konfiguration erhalten Sie über „Webdav und SFTP“.



Freigaben über SSH: SSH/SFTP lässt sich im Dateimanager bequem nutzen. Verwenden Sie in der Adresszeile eine URL in der Form „sftp://[User]@[Server-IP]“.

5. Webserver auf dem PC einrichten

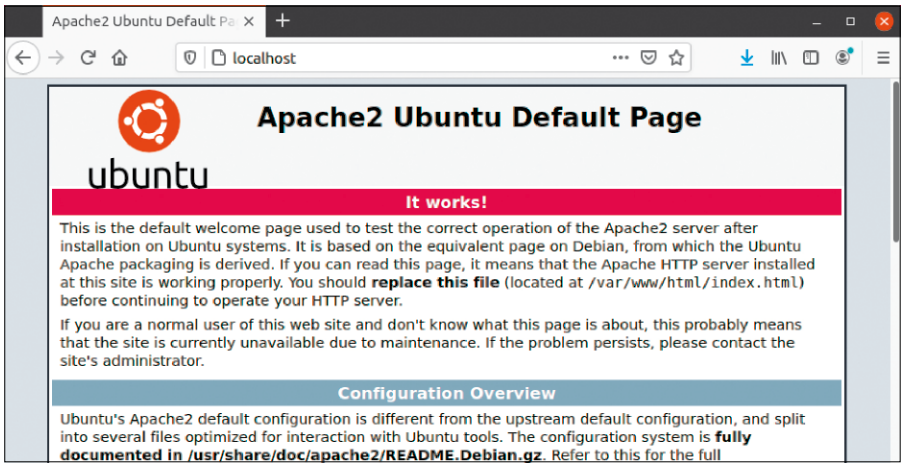
Im eigenen Netzwerk lässt sich ein Webserver für ein Intranetportal nutzen, etwa mit einem Wiki für die Ideensammlung oder mit einem Teamkalender. Sie können außerdem beliebige Webanwendungen wie Wordpress, Joomla oder Magento installieren und die Konfiguration sowie Gestaltung der Weboberfläche ausprobieren.

Der Webserver auf dem eigenen PC kann seine Dienste auch im Internet anbieten. Dazu müssen Sie in Ihrem DSL-Router die Portweiterleitung auf den Server-PC aktivieren. Als Webserver eignen sich Apache und Nginx. Nginx gilt als leistungsfähiger und wird oft für stark frequentierte Websites verwendet, häufig auch in Kombination mit Apache. Im privaten Netzwerk spielt das jedoch keine Rolle. Hier kommt es eher darauf an, wofür man den Webserver einsetzen will und ob es beispielsweise für das gewünschte Content-Management-System (CMS) Anleitungen für die Konfiguration mit Apache und/oder Nginx gibt. In der Linux-Welt-Toolbox liefert „Apache/Nginx Grundlagen“ Informationen zur Installation beider Webserver. Ergänzend dazu lesen Sie unter „Apache/Nginx Lösungen“ Hinweise zur Behebung möglicher Probleme.

6. Online im Team arbeiten

Die Erfahrungen der Jahre 2020 und 2021 haben gezeigt, das sich viele Arbeiten auch zu Hause erledigen lassen. In einigen Berufen spielt es aus technischer Sicht kaum eine Rolle, wo man vor dem Computer sitzt. In der Regel stellen die Arbeitgeber die Infrastruktur für den heimischen Arbeitsplatz bereit, in kleinen Unternehmen oder als Freiberufler muss man selbst tätig werden. Im Internet gibt es zahlreiche Angebote für die Teamarbeit. Der Einstieg ist meist kostenlos möglich. Wer mehr Funktionen benötigt, kann die gewünschten Pakete kostenpflichtig abonnieren.

Bei der Entscheidung für einen bestimmten Anbieter spielen die Ausstattung der



Funktionsprüfung: Nach der Installation des Apache-Webservers rufen Sie auf dem Server-PC die Adresse „http://localhost“ auf. Wenn der Server arbeitet, sehen Sie den Inhalt der Startseite.

Software und die Sicherheit wichtige Rollen: Cloudserver sind Vertrauenssache. Der Betreiber muss sicherstellen, dass die Server ausreichend geschützt sind und Daten nicht in falsche Hände geraten. Ein eigener Server in einem Rechenzentrum verspricht mehr Datenschutz. Immerhin kann man hier selbst entscheiden, welche Software läuft und wie wirksam die Verschlüsselung ist. Allerdings ist man auch selber für die Sicherheit verantwortlich. Diese Aufgabe erfordert Erfahrung und ständige Kontrollen.

Der eigene Server kann auch zu Hause stehen. Diese Option bietet sich vor allem an, wenn die Internetanbindung ausreichend schnell ist, beispielsweise mit 100 MBit/s Download und 50 MBit/s Upload oder mehr. Bei langsameren Verbindungen reagieren Webanwendungen oft zäh und die Nutzung macht keinen Spaß. Für kleine Teams oder gelegentliche Nutzung sind die Einschränkungen aber hinnehmbar. Damit der heimische Server nicht Ziel von Hackerangriffen wird, sind die gleichen Maßnahmen erforderlich wie im Rechenzentrum. Die wichtigsten haben wir in einem Artikel unter *www.pcwelt.de/2091052* zusammengetragen. Am sichersten ist eine VPN-Verbindung zwischen den Netzwerken. Eine Lösung mit Wireguard beschreiben wir in der LinuxWelt-Toolbox unter „VPN“.

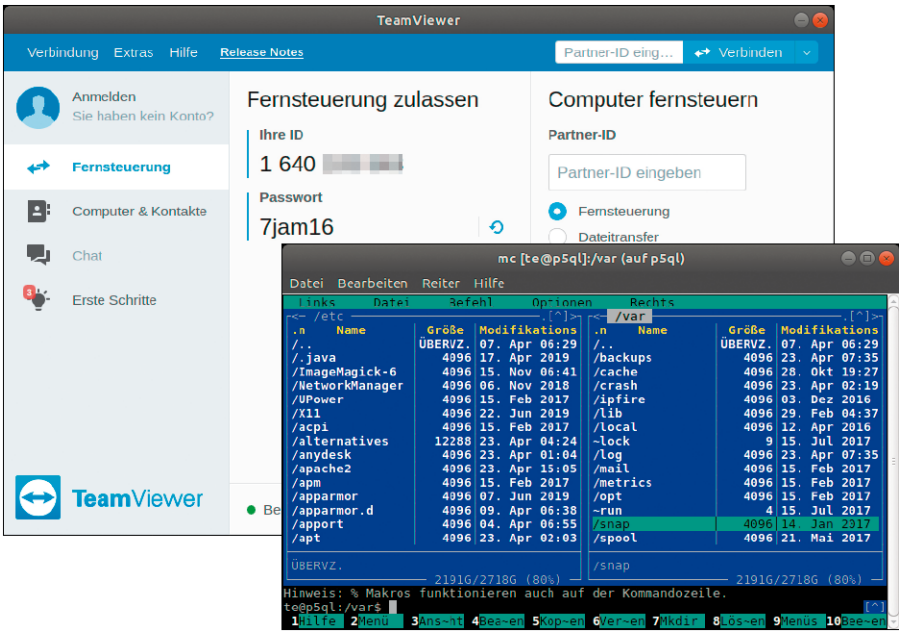
Ein Klick auf die Schaltfläche „Zusammenarbeit“ liefert Informationen zu den gängigen Angeboten von Google und Microsoft. Wer möchte, kann sich auch mit Nextcloud einen eigenen Cloudserver zu Hause oder im Rechenzentrum einrichten. Über die Open-Source-Software lassen sich Dateien auf dem Server ablegen, ähnlich wie bei Google Drive oder Onedrive.

7. Fernzugriff und Fernwartung

Über einen Fernzugang kann man online auf einem anderen PC arbeiten, Dateien kopieren oder anderen Benutzern bei Problemen helfen. Die Software dafür gibt es für Privatanwender gratis. Für viele Wartungsarbeiten unter Linux benötigen Sie keine grafische Benutzeroberfläche und ein Terminalfenster reicht völlig aus. Auf dem PC, den Sie fernsteuern möchten, muss dazu nur der SSH-Server laufen. Das funktioniert erst einmal nur im lokalen Netzwerk, zumindest wenn auf dem Server-PC keine Firewall aktiv ist. Damit der SSH-Server aus dem Internet erreichbar wird, müssen im Router Portfreigaben eingerichtet sein (siehe „Portfreigaben“ in der LinuxWelt-Toolbox). Sicherer ist allerdings eine VPN-Verbindung (siehe „VPN“ in der LinuxWelt-Toolbox).

Ist ein grafischer Desktopzugriff erforderlich, verwenden Sie beispielsweise Teamviewer (*www.teamviewer.com*). Private Nutzer dürfen die Software kostenlos verwenden. Beim gewerblichen Einsatz beginnen die Abopreise bei 27,90 Euro monatlich pro Benutzer. Deutlich günstiger ist die Remote-Access-Lizenz für zurzeit 9,90 Euro pro Monat, die den Fernzugriff für einen Remotemitarbeiter auf bis zu drei Computer oder Server erlaubt. Die genannten Preise werden jährlich abgerechnet.

Bei Teamviewer läuft die Vermittlung der Verbindung über einen Server bei *teamviewer.com*. Deshalb müssen keine Ausnahmen in der Firewall des Rechners und keine Portfreigaben im Router konfiguriert werden. Das ermöglicht die Einrichtung der Software auch technisch weniger versierter Personen. Teamviewer ist für alle gängigen Plattformen verfügbar: Windows, Mac-OS, Linux, Chrome-OS, Android, iOS und den Raspberry Pi. In der LinuxWelt-Toolbox lesen Sie nach einem Klick auf „Fernzugriff“ Informationen zur Installation und Konfiguration von Teamviewer und zur Fernwartung über SSH. ■



Fernzugriff: Mit Teamviewer greifen Sie über das Internet auf den Desktop eines anderen PCs zu. Für die Fernwartung genügt aber auch ein Terminal mit dem Midnight Commander.

Programme für Audio, Video & Fotos

Im Bereich Multimedia hat Linux einiges zu bieten. Sie können zwischen mehreren Mediaplayern wählen sowie Fotos und Videos mit komfortablen Programmen bearbeiten.

VON THORSTEN EGGELING

Ein Argument gegen Linux lautet häufig: Da läuft kein Adobe Photoshop. Das ist unbestritten wahr. Allerdings benötigen auch nicht alle Anwender Photoshop für die Bearbeitung von ein paar Urlaubsfotos. Dafür reichen einfachere Programme aus, die auch unter Linux zur Verfügung stehen. Ein ähnliches Bild zeigt sich bei Videoeditoren. Eine Software mit dem Funktionsumfang von Adobe Premiere gibt es nicht. Dafür stehen unter Linux gleich mehrere Gratisprogramme zur Bearbeitung von Videos zur Verfügung, die einfach zu bedienen sind und für Amateurfilmer ausreichen.

Bei der Wiedergabe von Musik und Filmen müssen Linux-Nutzer auf nichts verzichten. Die Standardplayer unter Ubuntu und Linux Mint spielen alle gängigen Formate ab. Wem der Funktionsumfang nicht ausreicht, der installiert den VLC Media Player oder den Smplayer.

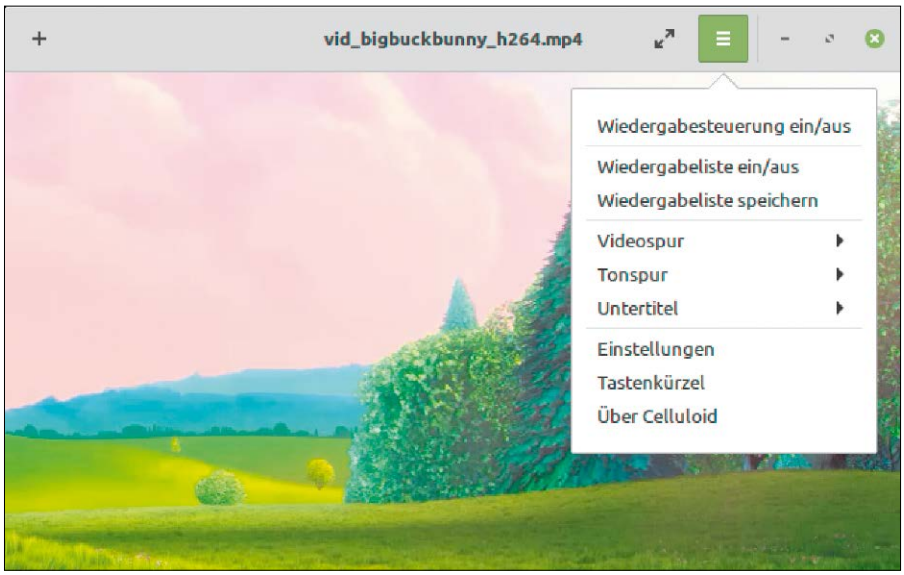
1. Audio- und Video-Abspielsoftware

Je nach Linux-Distribution sind unterschiedliche Programme für die Audio- und Videowiedergabe vorinstalliert. Bei Ubuntu 20.04 heißt das Programm schlicht „Videos“, bei Linux Mint 20 „Celluloid“. Beide Player haben in etwa den gleichen Funktionsumfang und ermöglichen beispielsweise den Wechsel der Tonspur oder die Anzeige von Untertiteln. Wenn ein Player ein bestimmtes Audio- oder Videoformat nicht abspielen kann, fordert er die Installation des nötigen Codecs in der Regel automatisch an. Die Installation aller verfügbaren Codecs kann bei Linux Mint jederzeit über das Menü und „Multimedia → Multimedia-Codecs installieren“ erfolgen. Ubuntu-Nutzer öffnen ein Terminal und führen diese beiden Befehle aus:

```
sudo add-apt-repository multiverse
sudo apt install ubuntu-restricted-extras
```

Alternativen: Mit dem VLC Media Player und dem Smplayer stehen Linux-Nutzern weitere Abspielprogramme zur Verfügung. Beide bringen eigene Codecs mit und spielen daher standardmäßig alle bekannten Formate ab.

In der LinuxWelt-Toolbox finden Sie alle Informationen zu den Playern in der Rubrik „Multimedia“ nach einem Klick auf „Medienplayer“.



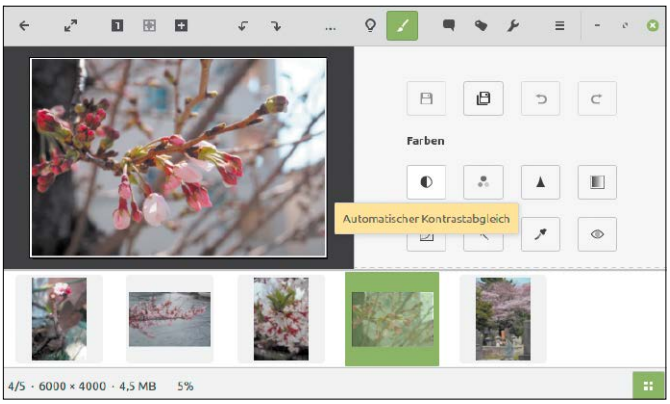
Videos abspielen: Celluloid unter Linux Mint ist ein einfacher Audio- und Videoplayer ohne spezielle Funktionen, der aber seinen Zweck vollauf erfüllt.

2. Fotosammlungen verwalten und Fotos bearbeiten

Einfache Anzeigeprogramme für Bilddateien sind bei Ubuntu 20.04 und Linux Mint 20 standardmäßig installiert. Bei Ubuntu handelt es sich um Eog („Eye of Gnome“), der sich als „Bildbetrachter“ meldet. Linux Mint setzt auf Xnviewer. Beide Programme zeigen Bilder nach einem Doppelklick im Dateimanager, können alle gängigen Bildformate anzeigen und bieten eine Diashow-Funktion.

Linux Mint bringt außerdem das Werkzeug Pix mit, das einfache Bearbeitungsfunktionen wie „Bildgröße ändern“ oder „Format umwandeln“ bietet. Ubuntu enthält dafür Shotwell, das etwas mehr Funktionen hat – Bilder zuschneiden, Farbe und Farbton anpassen oder „Rote-Augen-Effekt“ entfernen. Wem dies nicht ausreicht, installiert Gthumb. Das Tool bietet weitere Bearbeitungsfunktionen und kann Bilddateien auch mit Schlagwörtern und Kommentaren ausstatten.

Der Spezialist für die Organisation von Fotosammlungen heißt Digikam. Damit lassen sich Fotos nach Alben, Tags oder Stichwörtern sortieren und kategorisieren. Mit der automatischen Gesichtserkennung können Sie Fotos von Personen jeweils in eigenen Ordern ablegen. Digikam enthält zahlreiche Tools für die Fotobearbeitung wie die Tonwert- oder Rote-Augen-Korrektur. Auch eine Unterstützung von RAW-Formaten ist vorhanden. Ein Ersatz für Programme wie Darktable und Rawtherapee ist Digikam allerdings nicht (siehe: „HDR-Fotografie“ in der LinuxWelt-Toolbox).
Alle Informationen zur Installation der genannten Tools finden Sie in der LinuxWelt-Toolbox unter „Fotos verwalten“.



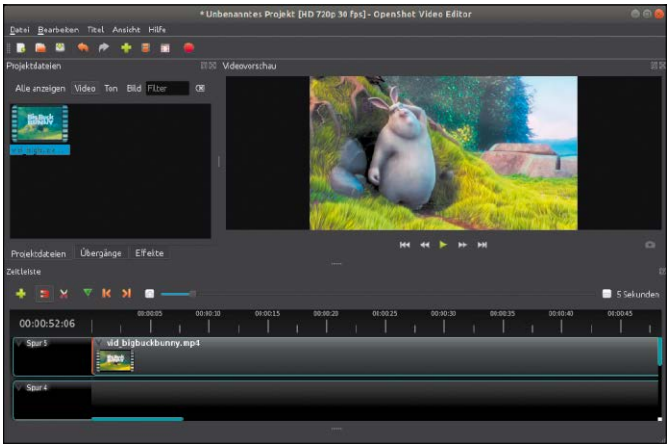
Fotos ansehen und bearbeiten: Gthumb zeigt Bilder und Bildsammlungen an und bietet einfache Bearbeitungsfunktionen für die Verbesserung von Fotos.

3. Bilder mit Gimp bearbeiten

Mit Gimp können Sie ebenfalls Fotos bearbeiten, die Zielgruppe sind aber anspruchsvolle Nutzer, die unter Windows Photoshop einsetzen. Das Programm bietet Malwerkzeuge, Ebenen, Masken, Automatikverbesserung und etliche Filter. Sie können Fotos retuschieren, Bilder freistellen oder verfremden. Wie bei Photoshop erschließen sich die meisten Funktionen nicht auf Anhieb. Bestimmte Effekte sind nur durch eine Kombination von Masken und Ebenen zu erreichen. Für Gimp finden Sie im Internet aber ausreichend Unterstützung. Ein guter Einstieg ist die Dokumentation unter *www.gimp.org/docs*.
Gimp ist in den Standardrepositorien von Ubuntu und Linux Mint enthalten. Neuere Versionen gibt es als Snap-Paket. Zur Installation und für weitere Infos klicken Sie in der LinuxWelt-Toolbox auf „Gimp“.

4. Audio- und Videodateien konvertieren

Wer Audio-CDs besitzt, aber MP3-Dateien bevorzugt, kann die CDs mit Asunder einlesen und in MP3s umwandeln. Liegen Audiodateien bereits in einem anderen Format vor, kann man sie mit Soundconverter umwandeln. Für die Umwandlung von Videos eignet sich Handbrake. Das Programm kann Videodateien fast aller gebräuchlichen Formate öffnen, dann mit einem H.264- oder H.265-Codec neu komprimieren und in einen MP4- oder MKV-Container speichern. Handbrake bietet eine Liste mit Voreinstellungen, etwa „Android 480p30“ oder „Vimeo Youtube HQ 1080p60“ für unterschiedliche Auflösungen und Qualitäten.



Videos bearbeiten: Openshot bietet mehrere Audio-/Videospuren in der Zeitleiste und kann eigene Filmaufnahmen mit Übergängen und Effekten ansehnlich gestalten.

Was Sie für die Installation und Nutzung wissen müssen, erfahren Sie in der LinuxWelt-Toolbox unter „Medien konvertieren“.

5. Videoeditoren für Ubuntu und Linux Mint

Wer Videos nicht nur umwandeln, sondern bearbeiten möchte, kann dafür den auch für Einsteiger verständlichen Videoeditor Openshot verwenden (*www.openshot.org*). Ebenfalls empfehlenswert ist Shotcut (*https://shotcut.org*), mit dem sich ebenfalls einsteigerfreundlich arbeiten lässt.
Weitere Videoeditoren für Linux sind Pitivi, Kdenlive und Cinelerra. Pitivi (*www.pitivi.org*) ähnelt in Bedienung und Funktionsumfang Openshot.
Kdenlive (*https://kdenlive.org*) und Cinelerra (*http://cinelerra.org*) bieten mehr Funktionen, benötigen aber auch mehr Einarbeitungszeit.
Weitere Informationen finden Sie in der LinuxWelt-Toolbox unter „Videoeditoren“. Die Installation erfolgt teilweise aus den Standardrepositorien, neuere Versionen gibt es meist als Appimage-Paket. ■

SCREENCASTS UND LIVESTREAMS

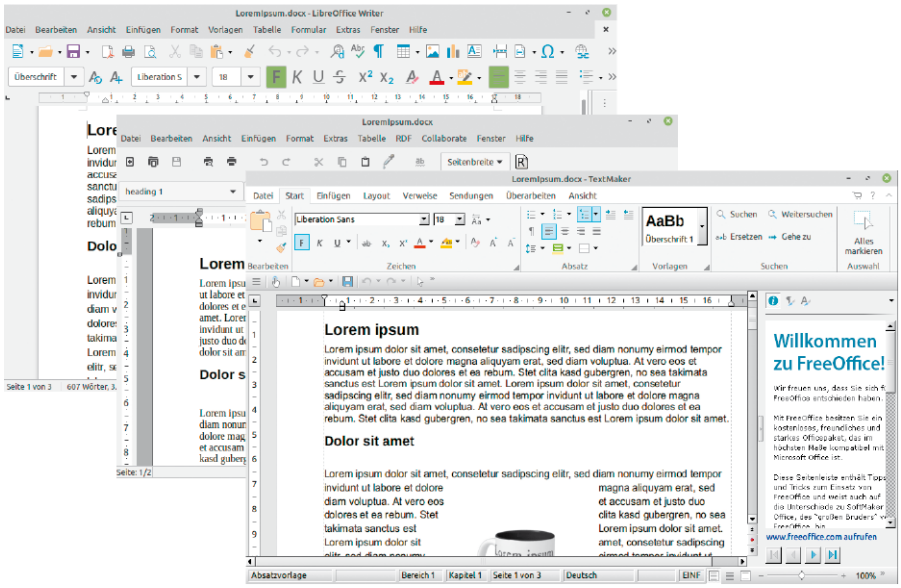
OBS (*https://obsproject.com*) ist eine Screencasting- und Videostreaming-Software. Sie kann den Bildschirminhalt inklusive Audiokommentar oder weiteren Videoquellen encodieren, direkt streamen oder als Video aufzeichnen. Letzteres ist sinnvoll für Videopodcasts, für nachträglich kommentierte Videoaufnahmen oder für Screencasts als Schulung. OBS ist ein komplettes Aufnahmestudio. Der Rechner sollte leistungsstark sein und über ein qualitativ hochwertiges Mikrofon und eine Webcam verfügen. Alle Daten von Audio- und Video-Aufnahmegeräten setzt OBS zu einem Stream in den Formaten H.264/MPEG-4 oder H.265/HEVC zusammen. Wie Sie OBS installieren und nutzen, erfahren Sie in der LinuxWelt-Toolbox nach einem Klick auf „OBS“ oder „Screencasts“.

Büroanwendungen für Linux

Libre Office ist bei Ubuntu und Linux Mint vorinstalliert, Textverarbeitung oder Tabellenkalkulation stehen daher sofort zur Verfügung. Alternative oder zusätzliche Anwendungen können die Produktivität jedoch verbessern.

VON THORSTEN EGGELING

Wer eine Linux-Distribution wie Ubuntu oder Linux Mint installiert, erhält damit zugleich Libre Office als Grundausstattung. Libre Office startet und läuft auf aktuellen Rechnern ausreichend schnell. Trotzdem ist das Büropaket kein Leichtgewicht unter den Anwendungen. Für ältere Rechner eigen sich alternative Office-Anwendungen vielleicht besser. Die meisten in diesem Artikel genannten Programme sind über die Paketverwaltung schnell installiert. Anleitungen und weiterführende Links finden Sie in der LinuxWelt-Toolbox in der Rubrik „Office“.



Freie Wahl: Libre Office Writer, Abiword und Freeoffice Textmaker sind drei Gratis-Textverarbeitungsprogramme für Linux, die für die meisten Aufgaben ausreichen.

1. Office-Pakete für Linux

Der Funktionsumfang von Libre Office (*www.libreoffice.org*) reicht für die meisten privaten Nutzer aus. Anders kann es aussehen, wenn häufig Dokumente bearbeiten muss, die mit Microsoft Office erstellt wurden. Die kann Libre Office zwar öffnen, bei komplexen Dokumenten können aber Formatierungen verloren gehen. Excel-Dateien sind besonders problematisch, weil Libre Office Calc nicht alle Excel-Funktionen kennt. VBA-Makros in Microsoft-Office-Dokumenten unterstützt Libre Office ebenfalls nicht. Wer darauf angewiesen ist, muss Microsoft Office nutzen. Das geht in einer virtuellen Maschine auch unter Linux, sodass man deswegen nicht auf Windows umsteigen muss. Informationen dazu finden Sie in der LinuxWelt-Toolbox in der Rubrik „Ubuntu/Mint“ nach Klick auf „Virtualisierung“.

Wem es auf möglichst originalgetreue Übernahme von Formatierungen aus Microsoft Word ankommt, der sollte Softmaker Office ausprobieren (*www.softmaker.de*). Die Importfilter sind besser als jene von Libre Office. Die Vollversion Softmaker Office Standard kostet 79,95 Euro. Für 99,95 Euro gibt es Softmaker Office Professional, das mit dem Duden-Korrektor eine leistungsfähige Rechtschreibprüfung enthält. Das Office-Paket lässt sich 30 Tage lang kostenlos testen. Sie können auch die Gratisversion Free Office (*www.freeoffice.com*) nutzen, die sich nur in Kleinigkeiten von der Kaufversion unterscheidet (siehe *www.freeoffice.com/de/freeoffice-vergleich*).

Installation: Libre Office ist in der Regel standardmäßig eingerichtet und steht in den Standard-Paketquellen bereit. Wer eine aktuellere Version installieren möchte, verwendet die Anleitung aus der LinuxWelt-Toolbox in der Rubrik „Office“ nach einem Klick auf „Office-Pakete“. Unter „Libre Office 7.1“ finden Sie Infos zur aktuellen Libre-Office-Version.

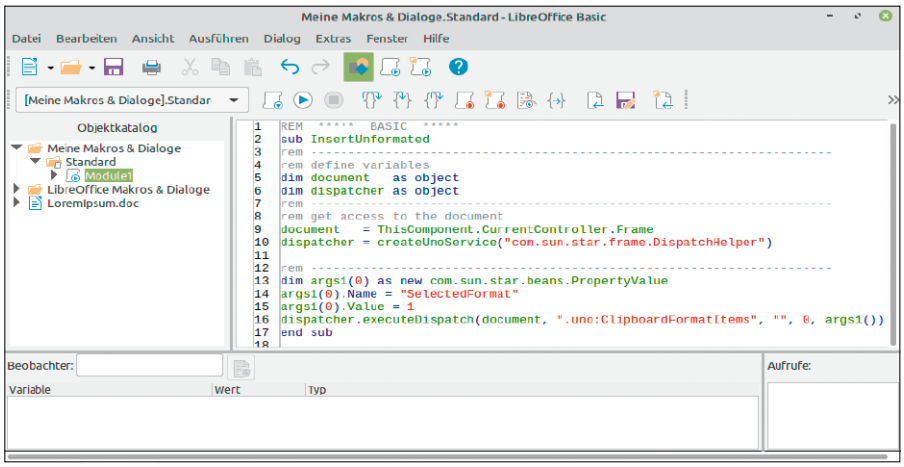
2. Erweiterungen für Libre Office

Über Erweiterungen (*http://extensions.libreoffice.org*) lassen sich in Libre Office neue Funktionen einbauen. Empfehlenswert ist auch die verbesserte Rechtschreib- und Grammatikprüfung Language Tool (*www.languagetool.org*).

Die Installationsanleitung liefern wir Ihnen in der LinuxWelt-Toolbox (Schaltfläche „Office-Pakete“).

Häufig wiederkehrende Arbeitsschritte lassen sich in Libre Office über Basic-Makros

automatisieren. Damit ist es sogar möglich, komplexe Programme mit eigener Oberfläche zu entwickeln. Den Einstieg in die Makroprogrammierung erleichtert der Makrorecorder, mit dem Sie Menüklicks sowie Tastatureingaben aufzeichnen und später wiedergeben. Die Funktion müssen Sie aber erst über „Extras → Optionen → Erweitert“ aktivieren, indem Sie ein Häkchen vor „Makroaufzeichnung ermöglichen“ (eingeschränkt)“ setzen. Der Hinweis „eingeschränkt“ deutet schon darauf hin, dass sich nicht alle Aktionen aufzeichnen lassen. Der Einstieg in die Makrosprache von Libre Office ist nicht einfach. Obwohl es den Makrorecorder und die Programmiersprache bereits in Open Office und dem Vorgänger Star Office gab, fehlt bis heute eine umfassende Dokumentation mit sprechenden Beispielen. Wie Sie den Makrorecorder verwenden, Makros starten und eigene Makros entwickeln können, haben wir in der LinuxWelt-Toolbox unter „Makros für Libre Office“ beschrieben.



Libre Office automatisieren: Häufige benutze Funktionen lassen sich als Makro aufzeichnen. Das Beispiel zeigt den Code, mit dem sich Text unformatiert einfügen lässt.

3. Alternative Office-Programme

Wer nur ab und zu einen Brief schreibt, für den kann auch Abiword ausreichen (*www.abiword.org*). Das Programm benötigt nur wenige Systemressourcen. Die Bedienung ist einfach und orientiert sich an den Standards von Libre Office und Word 2003. Das Gleiche gilt auch für die Tabellenkalkulation Gnumeric (*www.gnumeric.org*). Den Funktionsumfang von Excel erreicht das Programm nicht, dafür gibt es aber ausgefeilte finanzmathematischer Funktionen und ein gut bedienbares Modul, mit dem sich Graphen erzeugen lassen. Broschüren oder Zeitschriften mit komplexen Layouts kann man mit Scribus erstellen (*www.scribus.net*). Das Programm beherrscht professionellen Textsatz und kann Dokumente so für den Druck vorbereiten, dass auch die Farben stimmen (CMYK-Farbseparation).

Installation: Informationen zu den genannten Tools finden Sie in der LinuxWelt-Toolbox über die Schaltfläche „Office-Programme“.

4. Schnelle Suche in Dokumenten

Dateiinhalte finden sie besonders schnell mit Hilfe des Tools Docfetcher (*http://docfetcher.sourceforge.net*). Das Programm bietet eine Volltextsuche in Dateien, die mit Libre Office, Microsoft Office oder Abiword erstellt wurden, sowie in PDFs, Epub-Dateien und einfachen Textdateien jeder Art. Das Tool Recoll (*www.lesbonscomptes.com/recoll*) leistet Ähnliches, bietet aber eine fortgeschrittene Abfragesyntax. Recoll bringt außerdem einen eigenen Webserver mit, mit dessen Hilfe Sie anderen PCs im Netzwerk die Suche im Browserfenster zur Verfügung stellen.

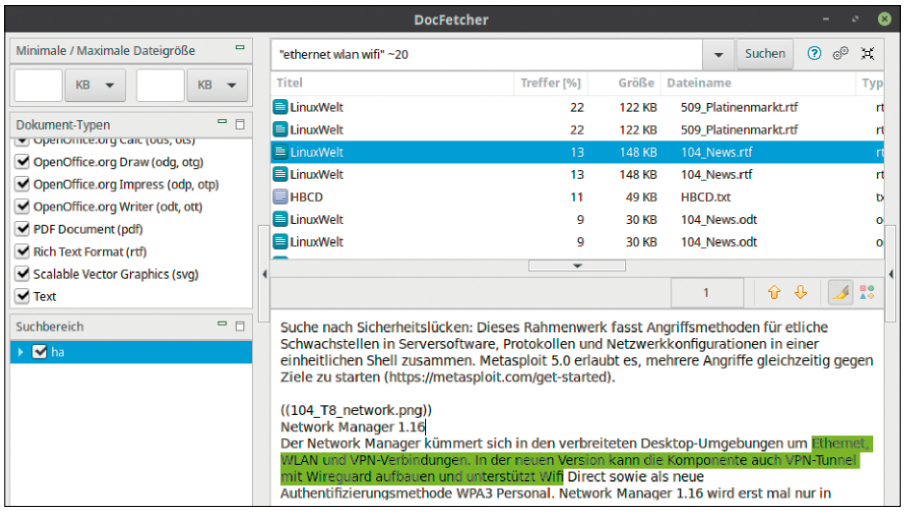
Installation: Docfetcher ist ein portables Tool für alle Betriebssysteme und benötigt eine Java-Runtime (Paket: „default-jre“). Sie müssen es nur herunterladen und entpacken. Recoll lässt sich unter Ubuntu und Linux Mint direkt installieren. Lesen Sie dazu die Anleitung in der LinuxWelt-Toolbox nach einem Klick auf „Desktop-Tools“.

5. PDFs erstellen und bearbeiten

Libre Office oder Softmaker Office konvertieren Dokumente in das universelle PDF-Format. Mit Libre Office Draw können Sie PDFs öffnen und weiterbearbeiten, was aber nur bei einfachen Dokumenten gelingt. Komplexere Formatierungen gehen oft verloren.

PDFs lassen sich auch ohne Probleme aufteilen: Sie können einzelne Seiten extrahieren, hinzufügen, löschen oder drehen. Ein geeignetes Tool dafür ist PDF-Arranger. Mehr Funktionen und eine ansprechende grafische Oberfläche bietet PDF Split and Merge. Damit können Sie Dokumente zusammenfügen und zerteilen, Seiten drehen und umsortieren. Sie können Dokumente per Maus zusammenstellen und sehen dabei stets eine Vorschau des fertigen PDFs.

Installation: Informationen zu den genannten Programmen finden Sie in der LinuxWelt-Toolbox nach einem Klick auf „PDF-Tools“.

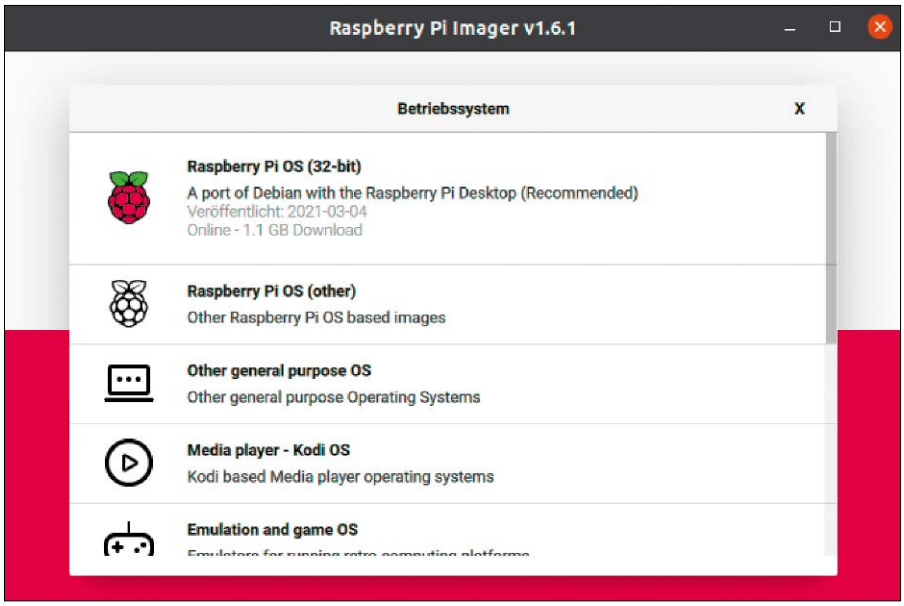


Docfetcher: Die Erstellung des Suchindexes kann einige Zeit dauern. Dafür erfolgt die Suche nach Textinhalten aller Art dann schnell und mit Vorschau auf das Ergebnis.

Software für Mini-PCs

Für den Raspberry Pi stehen mehrere Betriebssysteme zur Verfügung und er eignet sich als sparsamer Server für das Heimnetzwerk. Als Medienabspieler am TV-Gerät lässt er sich ebenfalls nutzen.

VON THORSTEN EGGELING



Betriebssysteme für den Raspberry Pi: Mit dem Tool Raspberry Pi Imager laden Sie das gewünschte System herunter und übertragen es auf eine SD-Karte.

Kleine Ein-Platinen-Rechner wie der Raspberry Pi sind preisgünstig und nehmen wenig Leistung auf. Sie eignen sich daher besonders gut als Dauerläufer für Serverrollen. Man sollte von den kleinen Geräten aber auch nicht zu viel erwarten. Die vergleichsweise geringe Rechenleistung, Festplatten nur am USB-Anschluss und ein schwacher Ethernet-Adapter begrenzen den Datendurchsatz, was sich etwa auf den Einsatz als Dateiserver negativ auswirkt. Für viele Nutzer ist die Geschwindigkeit jedoch ausreichend. Wenn nicht, sollte man sich für einen anderen Mini-PC mit mehr Leistung entscheiden.

Besonders gut eignet sich der Raspberry Pi als geräuschlose und flexible Multimedia-Zentrale am TV-Gerät. Die Leistung reicht selbst für HD-Videos aus. Im optimalen Fall benötigt man neben dem Raspberry Pi keine weitere Hardware, weil sich die Oberfläche des Mediacenters Kodi/Libre Elec mit der TV-Fernbedienung steuern lässt.

Software für den Raspberry Pi

Das aktuelle Spitzenmodell Raspberry Pi 4 B ist mit bis zu acht GB RAM ausgestattet, die CPU läuft mit 1500 MHz. Auf dem Gerät mit der Größe einer Scheckkarte befinden sich zwei USB-3.0-Ports, zwei USB-2.0-Ports, eine Gigabit-Ethernet-Buchse sowie ein WLAN- und Bluetooth-Adapter. Das Betriebssystem wird am PC auf eine SD-Karte kopiert, von der der Raspberry Pi dann bootet. Am einfachsten geht das mit dem Raspberry Pi Imager, den Sie unter *www.raspberrypi.org/software* als DEB-Paket für Ubuntu oder Linux Mint herunterladen und installieren. Den Imager gibt es aber auch für Mac-OS und Windows. Im Tool wählen Sie das gewünschte Betriebssystem aus – Standard ist Raspberry-Pi-OS, das auf Debian basiert. Im Angebot sind außerdem mehrere Ubuntu-Varianten.

Weitere Informationen zu den verfügbaren Systemen finden Sie in der LinuxWelt-Toolbox in der Rubrik „Platinenrechner“ nach einem Klick auf „Systeme“, „Ubuntu für den Raspi“ und „Raspberry Pi 400“.

Raspberry Pi vom USB-Stick booten

Beim Raspberry Pi ist es vorgesehen, das Betriebssystem auf einer SD-Karte unterzubringen. Allerdings gelten SD-Karten im Dauerbetrieb als nicht besonders zuverlässig, woran auch der Kartenleser des Raspberry Pi schuld sein kann. Eine Alternative ist der Start des Betriebssystems von einem USB-Stick. Dafür muss bei älteren Modellen, die vor September 2020 hergestellt wurden, ein Update des Eeprom erfolgen. Welche Schritte dafür nötig sind und was Sie für den erfolgreichen Start des Betriebssystems konfigurieren müssen, erfahren Sie in der LinuxWelt-Toolbox nach einem Klick auf „Booten von USB“.

Serveranwendungen für den Raspberry Pi

Wenn der Raspberry Pi unter Raspbian-OS oder Ubuntu läuft, lassen sich Web- oder Dateiserver wie unter Debian, Ubuntu oder Linux Mint installieren. Die Anleitungen aus der LinuxWelt-Toolbox unter „Netzwerk“ gelten entsprechend. Es geht aber auch einfacher. Nextcloud Pi (*https://ownyourbits.com/nextcloudpi/*) beispielsweise ist ein Sorglospaket für den Raspberry Pi und andere Kleinrechner wie beispielsweise Odroid XU4, Rock64, Banana Pi, sowie für PCs (x86). Es kombiniert das Betriebssystem Raspbian gleich mit einer eingebauten Nextcloud. Das Image schreiben Sie nach dem Entpacken mit den üblichen Mitteln auf eine SD-Karte. Im Prinzip ist die Nextcloud nach Einlegen der SD-Karte in die Platine sofort lauffähig und konfigurationsbereit. Mehr dazu finden Sie unter „Cloudserver (Nextcloud)“ in der LinuxWelt-Toolbox.

Canonical (Ubuntu) stellt unter *https://ubuntu.com/appliance* ebenfalls betriebsbereite Softwarepakete für den Raspberry Pi zur Verfügung. Angeboten werden populäre Serveranwendungen wie Open HAB für das Smart Home, Medienallrounder Plex, Nextcloud für Datei- und Dokumentsharing und Mosquitto, womit Geräte des Internet der Dinge (IoT) Nachrichten austauschen können. Was dabei zu beachten ist, lesen Sie in der LinuxWelt-Toolbox nach einem Klick auf „Appliances (Server)“.

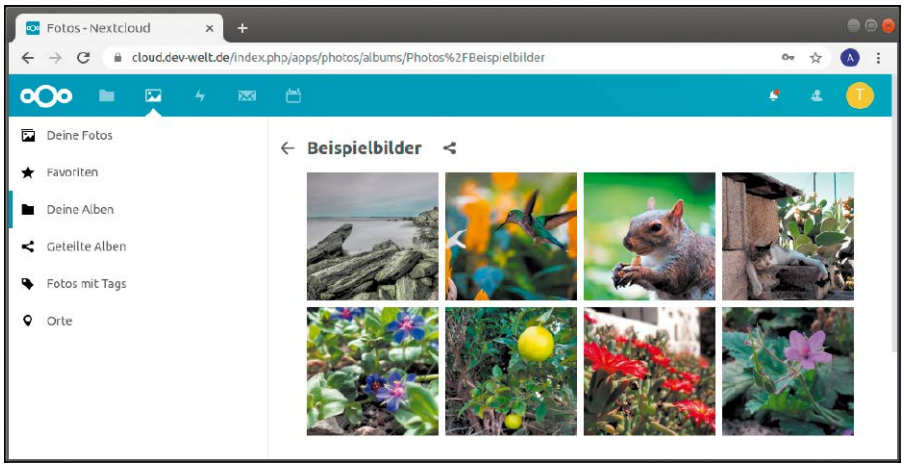
Mini-PC als Mediacenter einsetzen

Libre Elec (*https://libreelec.tv*) ist ein besonders schlankes Linux-System mit dem Multimedia-Center Kodi (*https://kodi.tv*). Video- und Audiodateien kann Kodi von einer USB-Festplatte, einer Netzwerkfreigabe oder aus dem Internet beziehen. Zugleich ist es möglich, die Dateien über Kodi im Netzwerk für andere Geräte freizugeben. Die Steuerung der Oberfläche erfolgt über die Fernbedienung des TV-Geräts, mit einer eigenen Fernbedienung für den Raspberry Pi oder auch mit einer Smartphone-App. Dank Hardwarebeschleunigung durch die GPU ist die Wiedergabe von HD-Videos mit 4K-Auflösung bei 60 Hz möglich.

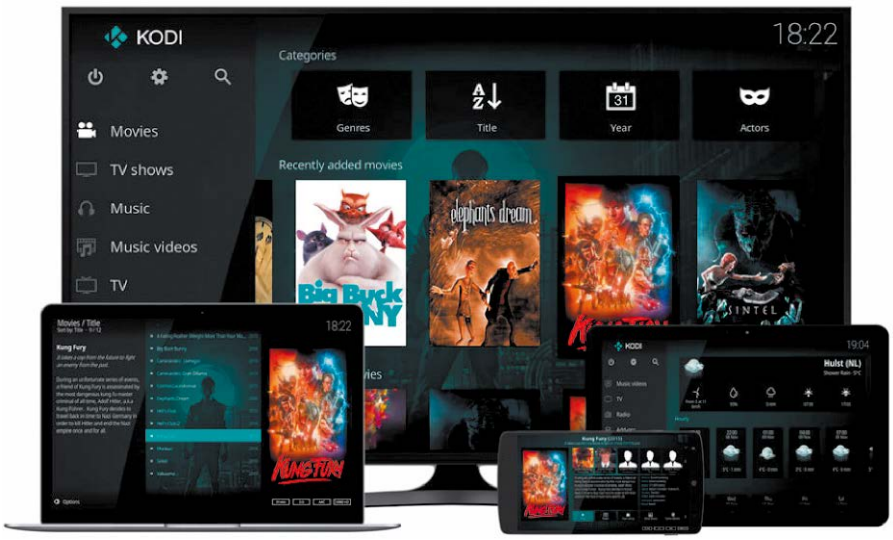
Kodi installieren Sie auf dem Raspberry Pi am schnellsten über das Setuptool Libre Elec USB-SD Creator (*https://libreelec.tv/downloads*), das für Linux, Windows und Mac-OS verfügbar ist. Legen Sie die SD-Karte in den Kartenleser Ihres PCs und starten Sie das Tool. Wählen Sie die Version „Raspberry Pi 2 and 3“ aus und klicken Sie auf „Herunterladen“. Nach dem Download wählen Sie das Laufwerk mit der SD-Karte aus und klicken auf „Schreiben“.

Kodi lässt sich aus den Paketquellen auch direkt unter Raspberry-Pi-OS installieren. Zusammen mit dem Desktop und vielleicht noch weiteren Serverdiensten ist das Gerät dann aber meist voll ausgelastet, was zu stockender Wiedergabe von Videos führt. Daher ist diese Installationsmethode nicht zu empfehlen.

Eine preisgünstige Alternative zum Raspberry Pi ist ein Fire TV Stick von Amazon. Der ist inklusive Alexa-Sprachfernbedienung für 40 Euro erhältlich, die HD-Variante kostet 60 Euro. Der Stick läuft unter Android und die Installation von Kodi ist eigentlich nicht vorgesehen. Mit einem Trick klappt das aber doch und Sie können neben Netflix und Amazon Prime Video auch Kodi als universellen Abspieler auf dem Fire TV Stick starten. Alle Informationen zu Kodi und den möglichen Installationsvarianten lesen Sie in der LinuxWelt-Toolbox nach einem Klick auf „Kodi“. ■



Der eigene Cloudserver: Nextcloud läuft auch auf einem Raspberry Pi. Sie können damit beispielsweise anderen Personen Bildersammlungen über das Internet anbieten.



Medienzentrale: Kodi läuft auf fast jeder Hardware inklusive dem Raspberry Pi. Ein Kodi-Server genügt, um Videos und Musik für alle Geräte im Netzwerk bereitzustellen.

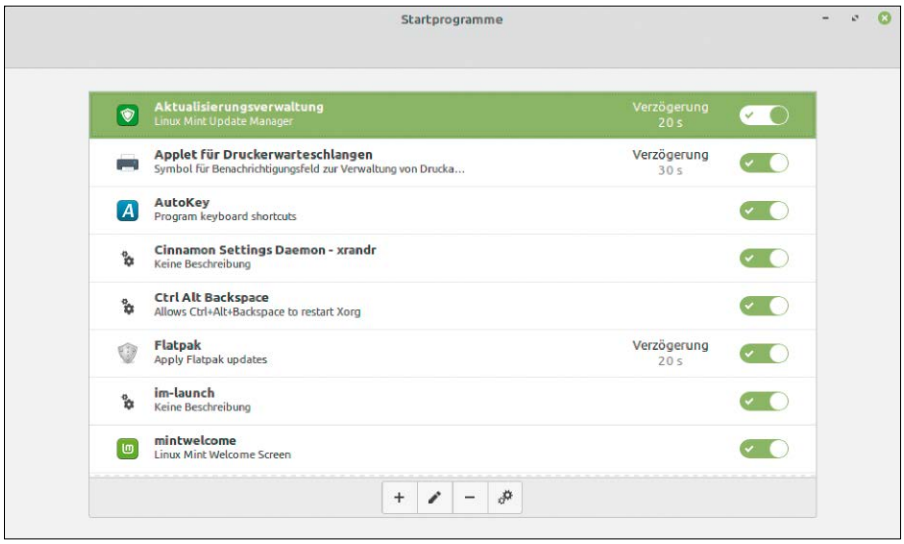
STEUERN UND MESSEN MIT RASPBERRY PI

Auf dem Raspberry Pi sind mehrere Schnittstellen untergebracht, die eine Kommunikation mit der Außenwelt ermöglichen. Eine der wichtigsten ist die frei programmierbare GPIO-Leiste (General Purpose Input/Output). Darüber lassen sich LEDs oder Relais steuern sowie Messwerte von Sensoren abfragen. Mit ein paar zusätzlichen Bauteilen wird dann aus dem Raspberry Pi ein Lehr- und Lerncomputer, der in die Welt der Elektronik und zugleich in die Programmierung einführt. Das eignet sich auch für Kinder und Jugendliche ab etwa 12 Jahren (mit Begleitung durch Erwachsene). Welche Bauteile Sie benötigen und wie der Einstig in die Programmierung klappt, erfahren Sie in der LinuxWelt-Toolbox nach einem Klick auf „Raspberry GPIO“.

Tools für die Linux-Automatisierung

Regelmäßige oder komplizierte Aufgaben können Sie Linux überlassen. Mit Zusatztools und Shell-Scripting lässt sich praktisch jedes Vorhaben automatisieren und somit Zeit und Arbeit sparen.

VON THORSTEN EGGELING



Programme automatisch starten: Soll ein Programm direkt nach der Anmeldung bei Linux zur Verfügung stehen, erstellen Sie dafür einen Eintrag mit „Startprogramme".

Ein Betriebssystem, das Gedanken liest und dann alles Nötige automatisch erledigt, wäre ein Traum – oder vielleicht auch ein Albtraum. So etwas können wir Ihnen aber ohnehin nicht bieten, dafür aber ein paar Hilfen und Arbeitserleichterungen. Um Routinearbeiten beispielsweise müssen Sie sich nicht kümmern, wenn Linux diese automatisch ausführt. Für den Start von Programmen, entweder beim Systemstart oder nach Zeitplan, gibt es mehrere Möglichkeiten. Sollten für eine Aufgabe mehrere Programme erforderlichen sein, lassen diese sich per Bash-Script nacheinander starten, bei Bedarf auch abhängig von bestimmten Bedingungen. Ein Script ist ebenfalls nützlich, wenn mehrere Dateien verarbeitet werden sollen, etwa bei der Konvertierung von Audio- oder Bilddateien. Ein weiterer Aspekt der Automatisierung sind Abkürzungen für häufig verwendete Eingaben. Das können Textbausteine sein, die Sie in einem Editor einfügen wollen, oder kurze Alias-Definitionen für Kommandos im Terminal.

Programme automatisch starten

Der Autostart ist die einfachste Form der Automatisierung. Sie nutzen die Funktion, wenn Sie ein bestimmtes Programm immer benötigen und es nach der Anmeldung sofort zur Verfügung stehen soll. Zur Verwaltung der Autostarts suchen Sie unter Ubuntu über „Aktivitäten" nach „Startprogramme", bei Linux Mint gehen Sie im Menü auf „Einstellungen → Startprogramme". Über „Hinzufügen" beziehungsweise die Plus-Schaltfläche lassen sich Programme in den Autostart aufnehmen. In der Regel genügt hinter „Befehl" der Programmname ohne Pfad. Mint Nutzer können eine Startverzögerung einstellen, damit das System nach der Anmeldung nicht zu sehr blockiert wird.

Programme beim Systemstart ausführen

Eine unkomplizierte und universelle Methode, Programme automatisch beim Start zu aktivieren, bietet der Taskplaner Cron. Dieser unterstützt das Schlüsselwort „@reboot", das den Systemstart als Zeitpunkt der Ausführung festlegt. Im Terminal bearbeiten Sie mit

```
crontab -e
```

die Croneinträge für den aktuell angemeldeten Benutzer. Beim ersten Aufruf werden Sie nach dem gewünschten Editor gefragt. Wählen Sie vorzugsweise den Editor nano und bestätigen Sie mit der Eingabetaste. Die Entscheidung wird in der standardmäßig versteckten Datei „.selected_editor" gespeichert. Wenn Sie den Editor später ändern wollen, starten das Tool *select-editor* und wählen einen anderen Eintrag.

Im aufgerufenen Editor definieren Sie mit „@reboot" am Zeilenbeginn

```
@reboot [/Pfad/Script]
```

und dem nachfolgenden Befehl oder Script einen Autostart-Task. Soll der Start verzögert erfolgen, nutzen Sie eine Befehlszeile wie

```
@reboot sleep 60 && [/Pfad/Script]
```

Die Zeitangabe hinter „sleep" ist in Sekunden anzugeben.

Wenn das Programm mit root-Rechten ausgeführt werden muss, verwenden Sie

```
sudo crontab -e
```

Alle Befehlszeilen sowie weitere Informationen finden Sie in der LinuxWelt-Toolbox in der Rubrik „Automatisierung" nach einem Klick auf „Autostarts und Cronjobs".

Programme nach Zeitplan starten

Die Standardaufgabe von Cron ist der Start von Programmen zu einem bestimmten Zeitpunkt. Crontab-Einträge benötigen fünf Zeitangaben (Minute, Stunde, Tag, Monat, Wochentag) mit Leerzeichen oder Tabulatoren getrennt, danach den Programmbefehl. Ein Backup, das täglich um 22:00 Uhr laufen soll, kann dann so aussehen:

```
0 22 * * * rsync -av /home/sepp/ /
 media/[User]/USB/backup
```

Der Asterisk (*) bedeutet wie üblich „alle“ an der betreffenden Stelle – hier also „an jedem Tag, jedem Monat, jedem Wochentag“.

Wer Cronjobs über die grafische Oberfläche verwalten und erstellen möchte, kann dafür das Tool Zeit verwenden (*https://github.com/loimu/zeit*). Wie Sie das Tool installieren und Cronjobs damit konfigurieren lesen Sie in der LinuxWelt-Toolbox unter „Autostarts und Cronjobs“.

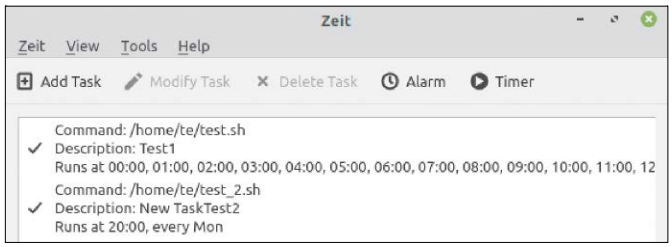
Programme über Systemd ausführen

Vor Ubuntu 18.04 gab es die Datei „/etc/rc.local“ zum automatischen Start von Programmen und Scripts. Seit der vollständigen Umstellung auf Systemd für den Start von Diensten wird dieses Verfahren nicht mehr unterstützt. Man kann es aber über eine Systemd-Servicedatei nachbilden. Welchen Inhalt diese haben muss und was sonst noch zu beachten ist, erfahren Sie in der LinuxWelt-Toolbox nach einem Klick auf „Systemd“. Außerdem finden Sie hier grundlegende Information zu Systemd und Servicedateien.

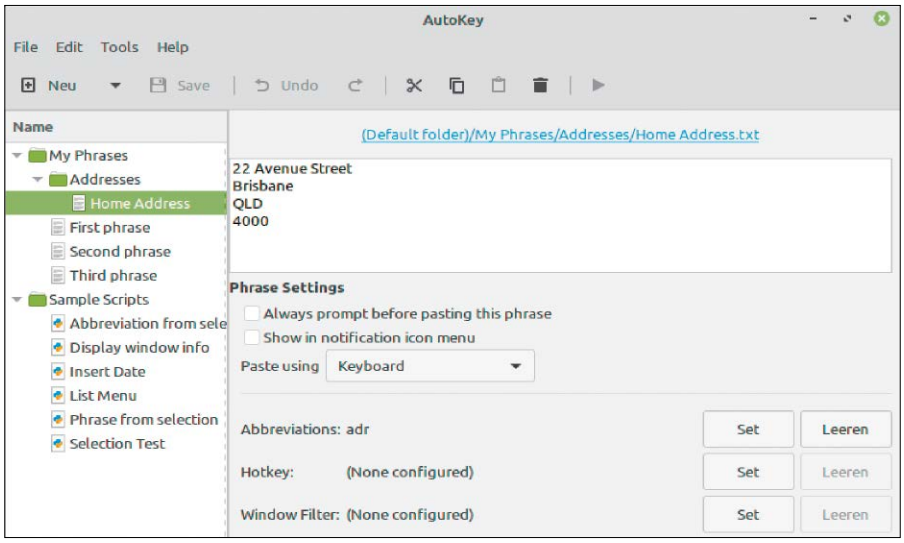
Textbausteine und Scripting mit Autokey

Das englischsprachige Autokey ist ein vielseitiges Tool für systemweite Textbausteine bis hin zu raffinierten Scripts. Sie legen damit Textbausteine an, die Sie über ein Kürzel oder einer Tastenkombination in einen Editor, die Textverarbeitung, das E-Mail-Programm oder das Terminalfenster einfügen. Es lassen sich in Autokey außerdem Scripts erstellen, um komplexere Aufgaben bei der Automatisierung zu erledigen.

Autokey ist in den Paketquellen von Ubuntu 18.04 und 20.5 sowie Linux Mint 19 und 20 enthalten (Paket: „autokey-gtk“). Damit das Programm automatisch startet, gehen Sie auf „Edit → Preferences“ und setzen ein Häkchen vor „Automatically start AutoKey after login“. Wie Sie Autokey nutzen, lesen Sie in der LinuxWelt-Toolbox nach einem Klick auf „Autokey“. Hier finden Sie neben der Installationsanleitung auch Tipps zur Konfiguration und Beispiel-Scripts.



Automatisierte Aufgaben: Mit dem Tool Zeit erstellen Sie Cronjobs für einmalige oder wiederkehrende Aufträge. Das eignet sich beispielsweise für regelmäßige Backups.



Globale Textbausteine: Häufig genutzte Texte und Wörter definieren Sie in Autokey. Über ein Kürzel gefolgt von der Eingabetaste fügen Sie den Text beispielsweise in einem Editorfenster ein.

Terminal- und Bash-Optimierung

Die wichtigste Initialisierungsdatei bei jedem Terminalstart ist die Datei „~/.bashrc“. Enthalten sind standardmäßig einige Funktionen und Variablendefinitionen, die Aussehen und Funktionen des Terminals beeinflussen. In der Datei lassen sich Kurzbefehle konfigurieren, etwa für schnelle die schnelle Ordnernavigation oder um komplexe Befehle zu vereinfachen. Die Zeile

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

beispielsweise bewirkt, dass man mit der Eingabe von d gefolgt von der Eingabetaste zum Verzeichnis „Downloads“ gelangt. Das funktioniert aber erst, wenn man die Konfiguration mit

```
source ~/.bashrc
```

neu einliest oder sich ab- und wieder anmeldet.

Welche nützlichen Definitionen sich sonst noch in der „~/.bashrc“ unterbringen lassen, erfahren Sie nach einem Klick auf „Terminal & Shell-Scripts“. ■

AUTOMATISIEREN MIT BASH-SCRIPTS

Im einfachsten Fall enthält ein Bash-Script nur einen Befehl, der ein anderes Programm startet. Der Bash-Interpreter bietet aber auch eine eigene Script-Sprache, mit fast allem, was man von einer Programmiersprache erwarten kann. Im praktischen Einsatz geht es meist um die Abarbeitung von Dateilisten, etwa wenn ein bestimmter Befehl auf alle Dateien in einem Ordner angewandt werden soll. Oder ein Script wertet den Rückgabewert eines Tools aus, um davon abhängig eine bestimmte Aktion auszuführen. Wer sich für Bash-Scripting interessiert, findet in der LinuxWelt-Toolbox nach einem Klick auf „Bash-Script-Basics“ eine Kurzeinführung und unter „Terminal & Shell-Scripts“ einige praktische Beispiele.

Service- & Mobilsysteme

Linux-Installations-DVDs bieten bereits eine Grundausstattung für einfache Reparaturen. Spezialisierte Rettungssysteme können die Analyse und Wartung defekter Installationen jedoch deutlich erleichtern.

VON THORSTEN EGGELING



LinuxWelt-Rettungssystem: Das System lässt sich von der Heft-DVD booten. Es bietet eine vollwertige Reparatur- und Wartungsumgebung inklusive Gparted und Clonezilla.

Aktuelle Distributionen werden in der Regel als Livesystem ausgeliefert, von dem aus die Installation erfolgt. Man gewinnt so gleichzeitig einen ersten Eindruck vom Aussehen der Oberfläche und der Bedienung einer Distribution. Dieses Livesystem lässt sich später auch für Reparaturen verwenden. Zusätzliche Spezialprogramme kann man dort während der Laufzeit temporär einrichten, sie gehen jedoch bei einem Neustart verloren. Für Reparaturaufgaben eignen sich daher spezialisierte Systeme noch besser, die alle nötigen Tools enthalten.

Die LinuxWelt-Toolbox bietet in der Rubrik „Service/Mobil-Systeme“ eine Übersicht mit den wichtigsten Livesystemen. Sie erfahren, was Sie beim Umgang mit den heruntergeladenen ISO-Dateien und beim Transfer auf einen USB-Stick beachten müssen. Außerdem finden Sie Tipps zur Auswahl eines für bestimmte Zwecke geeigneten Systems, ausführliche Installationsanleitungen und Downloadlinks.

Linux-Live- und Installationssysteme

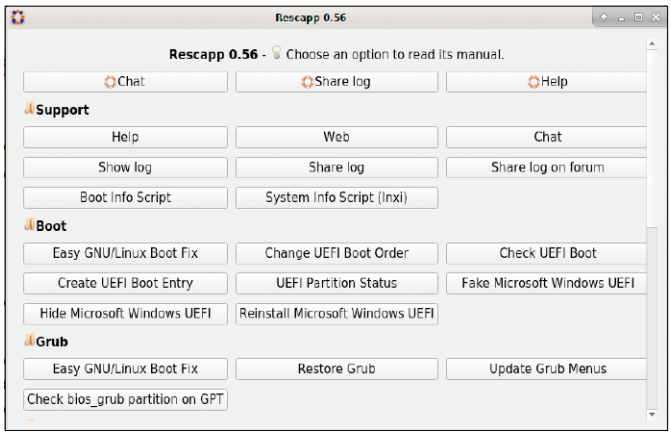
Von der Heft-DVD dieser LinuxWelt lassen sich Linux Mint Edge 20.3, Elementary OS 6.1, KDE Neon User Edition booten und installieren. Vom Livesystem aus lassen sich beispielsweise die Dateien aus Ihrem Home-Verzeichnis sichern oder Sie können die Bootumgebung reparieren. Die Livesysteme sind außerdem so konstruiert, dass sich temporär Reparaturtools oder Analysesoftware nachinstallieren lassen. Das eigentliche System ist jedoch schreibgeschützt. Das ist in den meisten Fällen auch erwünscht, damit das System immer in einem definierten Zustand startet und nicht manipuliert werden kann. Livesysteme eignen sich daher auch gut als sichere Surfumgebung. Auf einem USB-Stick lässt sich die Konfiguration eines Livesystems bei Bedarf auch ändern und speichern (Persistenz), was regelmäßig genutzte Zweit- oder Reparatursysteme deutlich komfortabler macht (siehe „Images und Livesysteme“ in der LinuxWelt-Toolbox).

Linux mit Zweitsystem reparieren

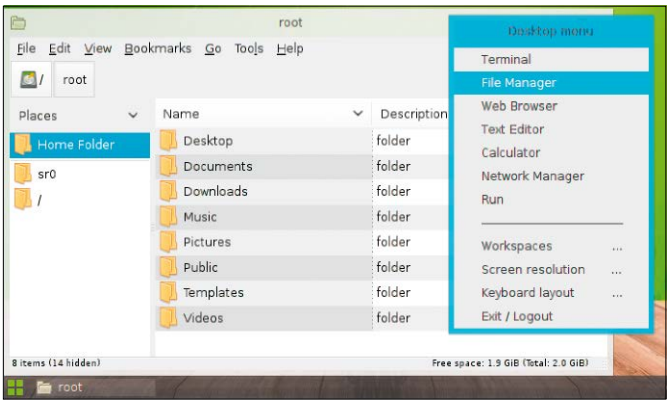
Über ein Livesystem erhalten Sie Zugriff auf die Partitionen eines installierten Betriebssystems. Das lässt sich nutzen, wenn Sie das Passwort vergessen haben, die Konfigurationsdateien bearbeiten oder den Bootmanager reparieren müssen. Das LinuxWelt-Rettungssystem (auf Heft-DVD) von der LinuxWelt-Redaktion startet schnell und ist auf die Wartung von Linux-Installationen spezialisiert. Es enthält unter anderem den Partitionierer Gparted, das Verschlüsselungsprogramm Veracrypt und das Klonprogramm Clonezilla.

Windows-Reparaturen mit Linux-System

Die PC-WELT-Rettungs-DVD (Download: *www.pcwelt.de/1168242*) enthält spezielle Tools für Windows-Systeme. Im System sehen Sie nach einem Klick auf „Rettungswerkzeuge“ Menüeinträge für Tools, mit denen Sie beispielsweise das Windows-Passwort löschen, gelöschte Dateien wiederherstellen („QPhotorec“) oder nach Schadsoftware suchen können („ClamAV“). Mit dem Tool Fred lässt sich die Windows-Registry bearbeiten. Sie können fehlerhaf-



Rescatux ist auf die Reparatur der Bootumgebungen von Linux und Windows spezialisiert. Die Steuerung der Tools erfolgt über die Script-Sammlung Rescapp.



Das kleine Slax startet schnell, bietet aber nur die nötigsten Programme. Es eignet sich für Aufgaben, die nicht mehr als einen Dateimanager, Browser und das Terminal benötigen.

te Einträge korrigieren oder die Konfiguration von Systemdiensten ändern. Firefox, Clonezilla und Gparted sind mit an Bord.

Spezial- und Surfsysteme

Einige Livesysteme erledigen nur eine bestimmte Aufgabe, andere bieten umfangreiche Toolsammlungen.

Informationen zu den genannten Systemen inklusive Downloadlinks finden Sie in der LinuxWelt-Toolbox in der Rubrik „Service/Mobil-Systeme.

Super Grub Disk: Der Grub-Bootmanager kann nach fehlerhafter Partitionierung bei der Installation schon mal an falscher Stelle landen, wonach das System nicht booten will. Das ist aber kein ernstes Problem, wenn Super Grub2 Disk zur Hand ist (auf Heft-DVD). Mit der Option „Detect and show boot methods“ durchforstet das Hilfsprogramm alle Datenträger nach Systemen, zeigt diese an und startet das ausgewählte System. Die eigentliche Reparatur des Bootmanagers erfolgt dann im gestarteten System (siehe „Mobile Reparatursysteme“ in der LinuxWelt-Toolbox).

Rescatux: Das System bietet einen Browser, Dateimanager, Terminal sowie einiges Zubehör und kann damit auch als allgemeines Notfallsystem dienen. Im Zentrum steht aber die grafisch organisierte und somit klickbare Script-Sammlung Rescapp. Während Super Grub Disk installierte Systeme nur sucht und startet, kann Rescatux defekte Grub-Bootloader wiederherstellen.

Gparted Live ist das sehr reduzierte Livesystem der Gparted-Entwickler, welches das Partitionierungsprogramm Gparted, einen Webbrowser und ein Terminal mitbringt. Zwar ist Gparted auch auf den meisten Linux-Systemen vorinstalliert oder über den Paketmanager erhältlich, aber in Notsituationen ist Gparted Live die schnelle Alternative, um Festplatten und Partitionen zu löschen, erstellen, vergrößern und verkleinern. Größenänderungen an der Systemfestplatte sind generell nur über ein unabhängiges Livesystem möglich.

Clonezilla erledigt das Backup und Restore kompletter Datenträger oder Partitionen. Die Images können lokal und auf Netzwerkfreigaben gespeichert werden. Clonezilla beherrscht die meisten verbreiteten Linux- und Windows-Dateisysteme und eignet sich auch für den direkten Umzug von einer alten auf eine neue Festplatte.

Slax gehört zu den wirklich kleinen und schnellen Livesystemen (265 MB): Viel mehr als ein Browser, Dateimanager, Mediaplayer und ein rudimentärer Desktop ist nicht dabei. Über einen Rechtsklick auf den Desktophintergrund aktivieren Sie im Menü „Keyboard Layout → German“ das deutsche Tastaturlayout.

Das **Livesystem Tails** erfüllt nur den einen Zweck: Den unkomplizierten Zugang zum TOR-Netzwerk. Hinter dem Kürzel TOR steht „The Onion Router“ – eine Verkettung anonymisierender Proxyserver. Dieses Proxynetzwerk erlaubt auch in Zeiten von rigoroser Überwachung des Netzwerkverkehrs ein hohes Maß an Anonymität. ■

MEHRERE SYSTEME VOM USB-STICK STARTEN

Linux-Livesysteme lassen sich über Unetbootin bequem auf einem USB-Stick einrichten. In der Regel kann man aber immer nur ein System auf dem Stick unterbringen. Abhilfe schafft das Tool Ventoy (*https://www.ventoy.net*), das eine Sammlung bootfähiger Systeme einrichten kann.

Laden Sie die „tar.gz“-Datei beispielsweise in den Ordner „Downloads“ herunter und entpacken Sie das Archiv. Öffnen Sie ein Terminal und verwenden Sie diese zwei Befehle:

```
cd ~/Downloads/ventoy-1.0.42
sudo sh VentoyWeb.sh
```

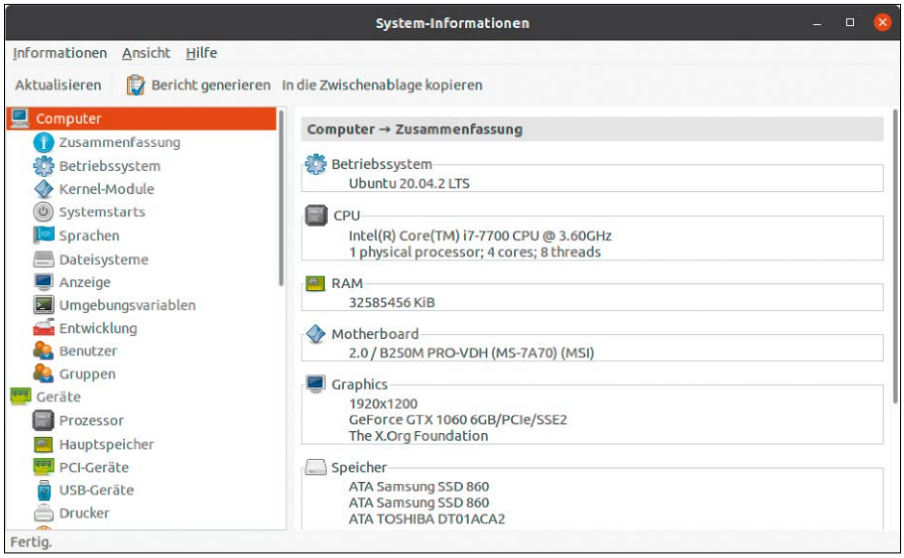
Öffnen Sie die angezeigte URL *http://127.0.0.1:24680* im Webbrowser. Unter „Languages“ können Sie „German (Deutsch)“ als Sprache einstellen. Wählen Sie den USB-Stick aus. Der muss neu formatiert werden, wodurch alle darauf befindlichen Dateien verloren gehen. Klicken Sie auf „Installieren“. Ventoy belegt danach eine kleine Partition mit 32 MB, der Rest wird mit dem Dateisystem exFAT formatiert und steht weiter zur Verfügung. Kopieren Sie einfach die gewünschten ISO-Dateien auf den Stick und booten Sie den PC damit. Ventoy erkennt die ISO-Dateien automatisch und bietet ein Menü für die Auswahl. Weitere Details zur Konfiguration von Ventoy finden Sie in der LinuxWelt-Toolbox in der Rubrik „Service/Mobil-Systeme“ nach einem Klick auf „Images und Livesysteme“.

Hardware: Analyse und Überwachung

Über geeignete Tools lassen sich genauere Informationen zu Hardware herausfinden, etwa wenn ein Gerät unter Linux nicht funktioniert. Empfehlenswert sind außerdem Tools zur Überwachung von Festplatte und CPU.

VON THORSTEN EGGELING

Die meisten Linux-Systeme liefern nur spärliche Informationen zur Hardware im PC. Bei Ubuntu erfahren Sie in den „Einstellungen“ unter „Info“ gerade einmal, welcher Prozessor verbaut ist, wie viel RAM verfügbar ist, wie der Grafikchip heißt und welche Kapazität die Festplatte bietet. Es stehen jedoch einige Tools zur Verfügung, über die Sie genauere Informationen erhalten. Das kann weiterhelfen, etwa wenn ein Gerät nicht automatisch erkannt wird und Sie einen passenden Treiber dafür suchen. Weitere Tools können Sie zur Überwachung der Temperatur von Prozessor und Festplatten einsetzen, um frühzeitig eine unzureichende Kühlung zu erkennen. Weitere Informationen, Dowloadlinks und Installationsanleitungen finden Sie in der LinuxWelt-Toolbox in der Rubrik „Hardware“.



Was steckt im PC? „System Profiler und Benchmark“ liefert eine Übersicht mit den wichtigsten Informationen, beispielsweise zu CPU, Mainboard, RAM und Grafikchip.

Grundlegende Hardwareinfos abrufen

Ein grafisches Übersichtsprogramm für die Hardwarekomponenten lässt sich – wenn noch nicht vorhanden – im Terminal mit

```
sudo apt install hardinfo
```

nachinstallieren. Auf einem deutschsprachigen System nennt sich das Tool „System Profiler und Benchmark“. Unter Linux Mint ist es standardmäßig an Bord (im Menü unter „Systemtools“). Das Tool hat links eine Kategorienspalte und zeigt im rechten Fenster die zugehörigen Werte. Hardinfo ist übersichtlich, klickfreundlich und zeigt wesentliche Informationen etwa auch zum System, zu eingehängten Dateisystemen und zum Netzwerk.

Detaillierte Informationen ermitteln

Jede Hardware besitzt eine eindeutige ID, über die sich Hersteller und Gerätetyp ermitteln lassen. Die Hardware-IDs ermitteln Sie unter Linux im Terminal mit diesen drei Befehlen:

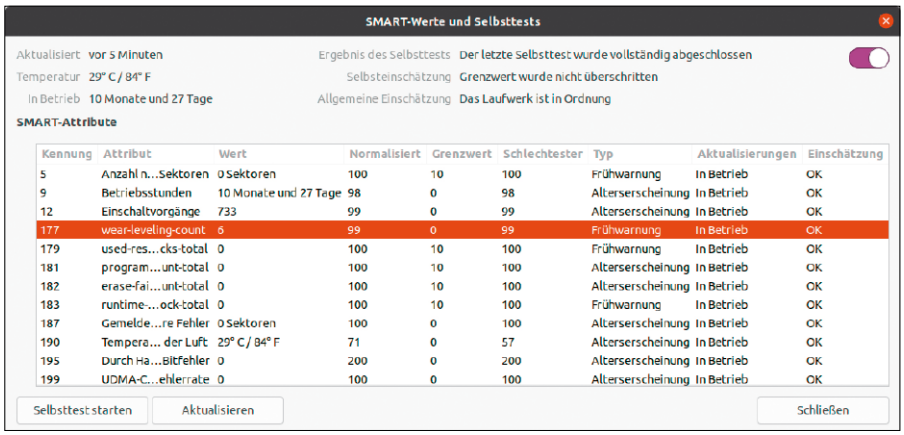
```
sudo lshw -numeric -html > lshw.html
sudo lspci -knn > lspci.txt
sudo lsusb -v > lsusb.txt
```

In der Datei „lshw.html“ finden Sie danach allgemeine Informationen zum PC, zum Typ der Hauptplatine, zur Bios-Version sowie zum 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. 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 Komplettgeräts enthält und die Sie nicht weiter beachten müssen. Wenn Sie jetzt eine Internet-Suchmaschine mit der gefundenen ID in Kombination mit dem Suchbegriff „Linux“ füttern, finden Sie weitergehende Informationen. Im schlimmsten Fall wird das Gerät von Linux gar nicht unterstützt oder erst ab einer bestimmten Kernel-Version oder es sind spezielle Schritte für die Konfiguration nötig. Hilfe bei der Problemlösung finden Sie in der LinuxWelt-Toolbox nach einem Klick auf „Hardware für Linux“.

Festplatten und SSDs

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.

Gnome-Disks zeigt – sofern ein passender Hardwaresensor verfügbar ist – auch die Temperatur von Laufwerken an und gibt Infos zum Zustand. Drücken Sie die Tastenkombination Strg-S, um die SMART-Werte zu 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.



Festplatten und SSDs prüfen: Gnome-Disks („Laufwerke“) zeigt die aktuelle Temperatur eines Laufwerks an. Die SMART-Werte geben Hinweise auf mögliche Fehler.

Hardwareüberwachung mit Sensoren

Der Linux-Kernel bietet Module für die Abfrage von Sensoren, die aber nicht alle automatisch geladen werden. Um den passenden Treiber zu finden, installieren Sie das Paket „lm-sensors“ im Terminal:

```
sudo apt install lm-sensors
```

Danach starten Sie das Tool über

```
sensors
```

Auf den meisten PCs gibt das Tool nur Infos zur Temperatur der Prozessorkerne aus. Dafür ist ein Modul zuständig, das der Kernel standardmäßig lädt. Um weitere Sensoren zu finden, führen Sie die Zeile

```
sudo sensors-detect --auto
```

aus. Die Option „--auto“ sorgt dafür, dass alle Fragen automatisch mit dem vorgegebenen Wert beantwortet werden. Am Ende sehen Sie eine Liste der erforderlichen Kernel-Module. Im optimalen Fall hat sensors-detect den Sensorchip erkannt, beispielsweise „it87“ oder „nct6775“. Sollte nur „cortemp“ (Intel), „k10temp“ oder „k8temp“ (AMD) auftauchen, scrollen Sie im Terminal zum Beginn der Informationen und dann wieder nach unten. Achten Sie auf die Angabe „yes“ am Ende der Zeilen. Bei einem Beispiel-PC mit der Hauptplatine MSI B250M PRO-VDH tauchte hier

```
Trying family 'VIA/Winbond/
  Nuvoton/Fintek'... Yes
Found unknown chip with ID 0xd352
```

auf. sensors-detect hat zwar einen Sensor-Baustein gefunden, den Treiber aber nicht geladen, weil dieser offiziell die Version des Chips nicht unterstützt. In diesem Fall kann es helfen, das Laden des Treibers zu erzwingen, für unser Beispiel etwa mit diesem Befehl:

```
sudo modprobe nct6775 force_
  id=0xd352
```

Das Tool sensors sollte dann deutlich mehr Informationen liefern, wenn der Treiber geladen wurde. Über den Befehl

```
dmesg
```

lassen Sie sich die letzten Kernel-Meldungen ausgeben. Bei Erfolg sehen Sie beispielsweise

```
nct6775: Found NCT6795D or
  compatible chip at 0x4e:0xa20
```

Es gibt allerdings keine Gewähr dafür, dass das bei jeder Hauptplatine ähnlich funktioniert. Die Suche im Internet nach der gemeldeten ID in Verbindung mit „sensors“ liefert meist Ergebnisse mit den Erfahrungen anderer Benutzer.

Treiber beim Systemstart laden: Damit die Sensor-Informationen direkt nach einem Linux-Neustart zur Verfügung stehen, erstellen Sie eine Konfigurationsdatei:

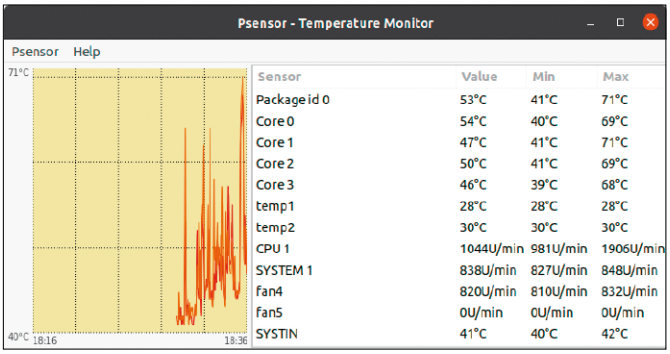
```
sudo gedit /etc/modules-load.d/
  sensoren.conf
```

Tragen Sie die Namen der Treiber jeweils in einer eigenen Zeile ein. „cortemp“, „k10temp“ oder „k8temp“ müssen Sie nicht eintragen, weil der Kernel diese Module automatisch lädt. Wenn zusätzliche Optionen erforderlich sind, erstellen Sie zusätzlich die Datei „/etc/modprobe.d/sensoren.conf“. Hier tragen Sie beispielsweise diese Zeile ein:

```
options nct6775 force_id=0xd352
```

Sobald lm-sensors konfiguriert ist, können Sie psensor für eine grafische Darstellung verwenden. Das Programm lässt sich unter Ubuntu und Linux Mint über das gleichnamige Paket installieren.

Alle Befehlszeilen sowie weiterführende Informationen liefert die LinuxWelt-Toolbox nach einem Klick auf „Sensoren“ in der Rubrik „Hardware“. ■



CPU überwachen: Psensor zeigt die Temperatur des Prozessors und die Umdrehungszahlen der Lüfter an. Wird die CPU zu heiß, sollten Sie die Lüfter prüfen.

Datenschutz für mobile Geräte

Betriebssysteme leisten mit ihrer Benutzeranmeldung keinen ernsthaften Datenschutz. Bei Fremdzugriff gibt jeder Rechner auch ohne Kenntnis der Anmeldedaten alle Festplatteninhalte preis. Dagegen hilft nur eines: Verschlüsselung.

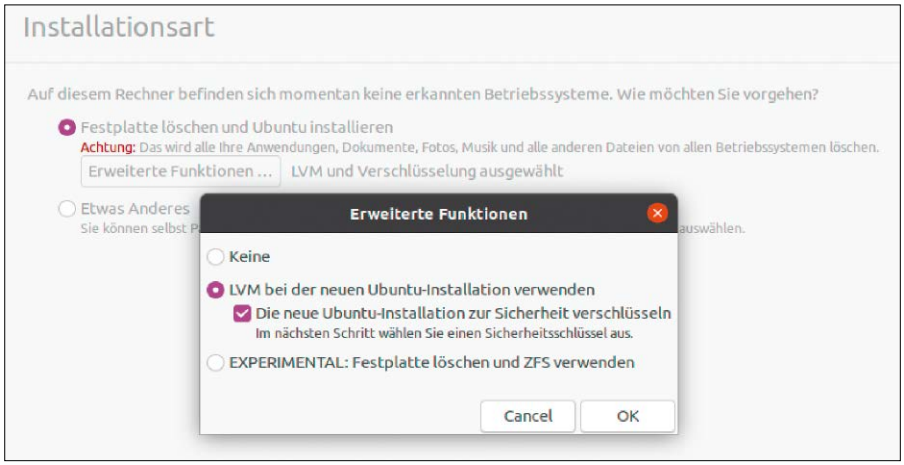
VON HERMANN APFELBÖCK

Besonders gefährdet von Fremdzugriffen sind mobile Rechner wie Notebooks. Es genügt bekanntlich, einen Computer mit einem Fremdsystem zu booten oder – aufwendiger – die ausgebauten Datenträger auf einem anderen Rechner zu nutzen. Noch einfacher ist das Auslesen der Daten bei ungeschützten USB-Datenträgern, die verloren oder vergessen wurden. Eine Distribution, die auf lokalen Datenschutz spezialisiert wäre, gibt es nicht mehr, seit True OS eingestellt wurde – ist aber auch nicht nötig: Die hier bevorzugt genannten Ubuntu-Systeme samt Derivaten bringen mehrere und komfortable Werkzeuge mit, um persönliche Daten sicher zu verschließen. Dieser Beitrag bespricht die wichtigsten:

1. komplette System- und Laufwerksverschlüsselung mit Luks
2. verschlüsseltes (und optional mobiles) Home-Verzeichnis mit Luks
3. verschlüsselte USB-Datenträger mit Luks
4. verschlüsseltes Home-Verzeichnis (einfaches Ecrypt FS)
5. verschlüsselte Container mit plattformunabhängigem Veracrypt

1. Installation mit Partitionsverschlüsselung

Mit Cryptsetup/Luks verschlüsselte Systempartitionen bieten kompromisslosen Schutz für Notebooks. Der Systemdatenträger lässt auch beim Booten durch Fremdsysteme keinen Einblick in die Daten zu. Die Luks-Laufwerksverschlüsselung (Linux Unified Key Setup) chiffriert die komplette Systempartition auf Basis eines frei



Datenträgerverschlüsselung: Diese Option ist in allen Ubuntus einfach einzurichten, sofern das neue System die komplette primäre Festplatte übernehmen darf.

wählbaren Passworts. Ohne Kenntnis dieses Passworts ist bei Fremdzugriff nur das „/boot"-Verzeichnis lesbar, das keinerlei persönlichen Daten enthält.

Luks-Verschlüsselung der Systempartition ist allerdings nur bei der Installation möglich – nicht nachträglich. Die beiden Ubuntu-Installer Ubiquity (Ubuntu, Xubuntu, Budgie, Mate und viele Derivate wie Mint) sowie der Calamares-Installer (Kubuntu, Lubuntu, Manjaro und andere) bieten diese Option per einfachen Klick an. Der entscheidende Dialog im Installationsprogramm lautet „Installationsart" (oder „Partitionen"). Beachten Sie, dass Sie für die Verschlüsselung dem Installer die gesamte primäre Festplatte überlassen müssen. Die Festplatte sollte leer sein oder nur noch Daten enthalten, die Sie nicht mehr benötigen. Eine kompliziertere Kombination von Luks und speziellen Partitionsaufteilungen ist im Installer nicht vorgesehen.

Klicken Sie unter „Installationsart" auf „Festplatte löschen ..." und darunter auf „Erweiterte Funktionen". Aktivieren Sie im Unterfenster den Punkt „LVM [...] verwenden", wonach die entscheidende Option „Die neue [...]-Installation ... verschlüsseln" aktiv wird. Diese wählen Sie aus und bestätigen mit „OK". Der Calamares-Installer kommt für dieselbe Aktion ohne Unterfenster aus und bietet direkt im Hauptdialog die schlichte Option „Verschlüssele System".

Wenn Sie dann auf „Weiter" klicken, folgt die Abfrage des Sicherheitsschlüssels (Kennwort). Das Kennwort sollte eine gewisse Mindestkomplexität haben, aber für tägliche Eingabe zumutbar sein, denn das System startet später nur noch nach der Kennworteingabe. Der Rest der Installation verläuft wie gewohnt.

Bei jedem Boot des System erscheint später stets die englischsprachige Abfrage „Please unlock disk [...]". Dort geben Sie das Kenn-

wort ein, um den Systemstart fortzusetzen. Abgesehen von dieser Kennwortabfrage ist die Systembenutzung vollkommen transparent – Sie arbeiten wie an einem unverschlüsselten System. Nichtsdestotrotz sollte sich jeder Anwender im Klaren sein, dass der für Luks erforderliche LVM (Logical Volume Manager) die Partitionierung komplexer macht und bei Bootproblemen höheren Reparaturaufwand verursacht.

2. Verschlüsseltes und mobiles Home-Verzeichnis

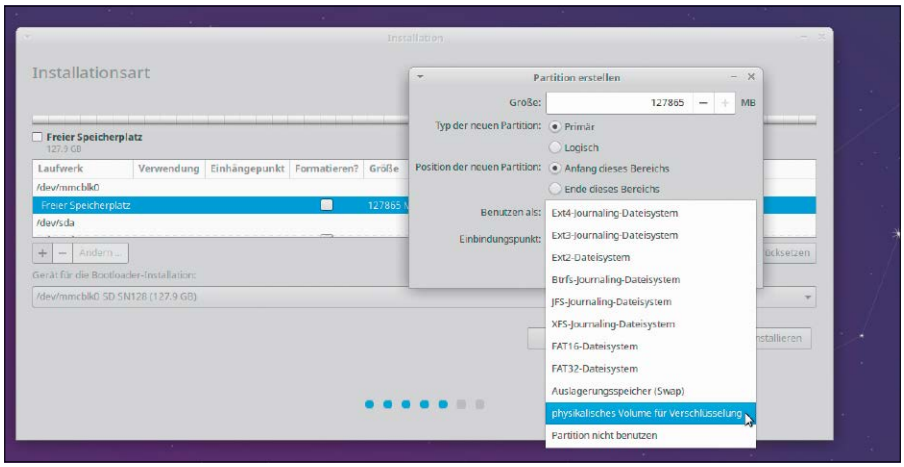
Rein datenschutztechnisch ist die Komplettverschlüsselung der Systempartition eine übertriebene Maßnahme. Eigentlich schützenswert sind in der Regel nur die Benutzerdateien unter „/home“. Dass bei der Luks-Vollverschlüsselung etwa auch globale Konfigurationsdateien unter „/etc“ bei Fremdzugriff unzugänglich sind, mag in manchen Fällen erwünscht sein. Den allermeisten Anwendern aber geht es ausschließlich um die persönlichen Daten.

Eine meist ausreichende Lösung, die obendrein noch interessante Mobilitätsaspekte mitbringt, ist daher ein verschlüsseltes Home auf einem separaten Datenträger. Alle Linux-Distributionen, Ubuntu-Derivate allemal, ermöglichen Home-Verzeichnisse auf separaten Datenträgern – intern oder extern auf USB oder SD, die dann auch Luks-verschlüsselt werden können. Wichtig ist nur, die Möglichkeit schon bei der Neuinstallation zu bedenken, denn nachträgliches Einrichten eines Luks-verschlüsselten Homes ist sehr ambitioniert.

1. Als Voraussetzung sollte neben der internen Festplatte für das System ein weiterer physikalischer Datenträger für das Home vorliegen. Dies kann eine weitere Festplatte, aber auch ein USB-Laufwerk oder eine (schnelle) SD-Karte ein. Die nötige Kapazität des Home-Laufwerks sollten Sie selbst einschätzen, aber 64 bis 256 GB sind eher die Untergrenze.

2. Nach dem Boot des Installationsmediums und Start des Ubuntu-Installers wählen Sie im Dialog „Installationsart“ die Option „Etwas Anderes“ für die manuelle Partitionierung. In Calamares (Kubuntu, Lubuntu) entspricht das der Option „Manuell“.

3. Wählen Sie zunächst das Laufwerk, auf dem Sie das System installieren möchten – in der Regel die erste interne Festplatte „/dev/sda“. Löschen Sie dort alles über die „-“-Schaltfläche. Alle bisherigen Daten auf der Festplatte gehen verloren. Klicken Sie dann auf den einzigen verbliebenen Eintrag „Freier Speicherplatz“ und legen darin über die „+“-Schaltfläche neue Partitionen an.



Verschlüsseltes Home: Der Ubuntu-Installer bietet unter „Dateisysteme“ eine Option für Luks-verschlüsselte Partitionen (hier unter Xubuntu).



Nach der manuellen Partitionierung (hier unter Mint): Der Installer-Hauptdialog zeigt das verschlüsselte „Home“ auf Laufwerk „sdc1“, EFI-Partition und System landen auf Laufwerk „sda“.

4. Bei einem Uefi-PC beginnen Sie zuallererst mit einer Partition vom Dateisystemtyp „EFI-System-Partition“. Dort ist nur eine Größenangabe erforderlich (100 MB reichen, falls nur Linux installiert wird), da weder Einhängepunkt (keiner) noch ein physisches Dateisystem (immer FAT32) abgefragt werden. Falls Sie diese Aktion übersehen, wird Sie ein im Uefi-Modus gebooteter Installer automatisch auf diesen Fehler hinweisen.

5. Den verbleibenden „freien Speicherplatz“ auf der ersten internen Festplatte (meist „/dev/sda“) übergeben Sie im einfachsten Fall mit voller Kapazität, mit dem Dateisystem Ext4 und mit dem Einbindungspunkt „/“ an das Betriebssystem.

6. Auf dem zweiten Datenträger erstellen Sie nun die Home-Partition. Der passende Einbindungspunkt „/home“ wird im Dropdown-Feld angeboten. Das Wichtigste: Als Dateisystem unter „Benutzen als“ wählen Sie die Option „physikalisches Volume für Verschlüsselung“. Danach müssen Sie nur noch ein Kennwort vergeben und dann den Verlauf der Installation abwarten. Im späteren Systemalltag wird das Passwort für das Home-Laufwerk – genau wie bei der Komplettverschlüsselung – vor jeder Systemanmeldung abgefragt.

Hinweis 1: Unter Calamares werden Sie bei Schritt 6 die Optionen „LUKS“ oder „LUKS2“ antreffen, was die Sache schwieriger zu machen scheint. Jedoch muss das Dateisystem gar nicht explizit gewählt werden. Wenn irgendein Linux-Dateisystem wie Ext4 eingestellt ist, dann ist nämlich die selbsterklärende Option „Verschlüsseln“ aktiv und muss nur bestätigt werden. Danach fragt der Dialog das Kennwort ab und wählt automatisch als Dateisystem „LUKS“.

Hinweis 2: Wenn Sie das verschlüsselte Home auf einen mobilen Datenträger legen

(USB, SD), kann dieser unter jedem Linux nach Eingabe des Kennworts (siehe Punkt 3) genutzt werden – nicht als „Home“ zwar, aber als neutrale Datenquelle. Damit können Sie im Handumdrehen auf mehreren Linux-Systemen gleiche Home-Standards setzen.

3. Luks-verschlüsselte USB-Datenträger

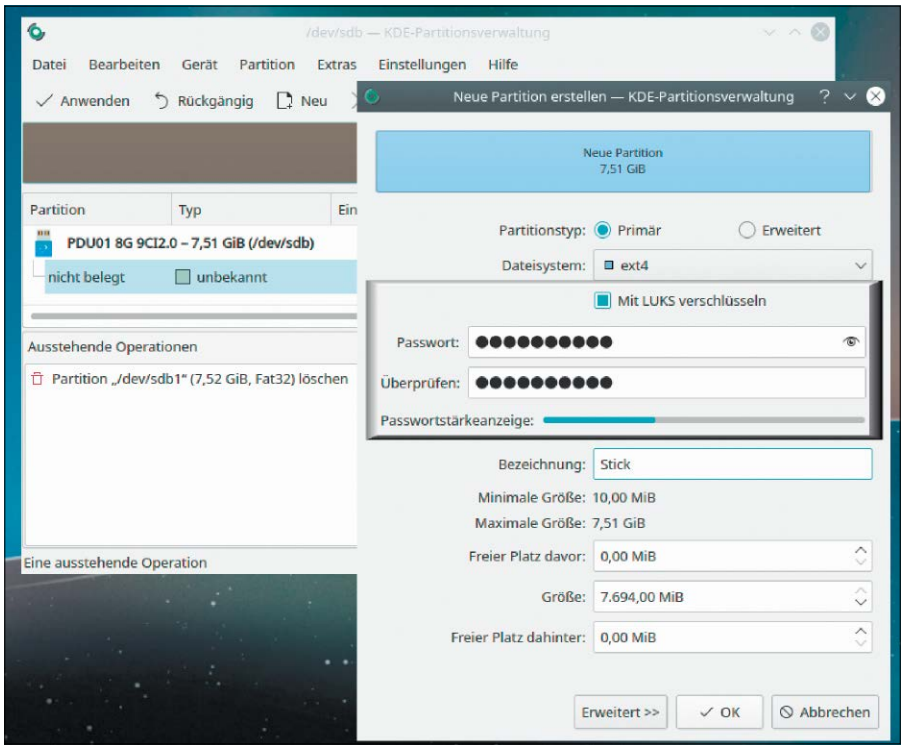
Luks-Verschlüsselung eignet sich nicht nur für System- oder Home-Partitionen. Luks auf USB-Sticks und -Festplatten mit Benutzerdaten ist technisch weniger anspruchsvoll und mit dem Systemtool Gnome-Disks („Laufwerke“) ganz einfach zu realisieren, wie nachfolgend beschrieben. KDE-Systeme (etwa Kubuntu/Lubuntu) mit der KDE-Partitionsverwaltung beherrschen das aber natürlich auch (siehe Abbildung). Beachten Sie, dass bei der Aktion alle Daten auf dem USB-Medium verlorengehen. Wenn Sie die Daten benötigen, müssen Sie diese erst an einen anderen Ort sichern und danach auf den Luks-formatierten Datenträger zurückschreiben.

1. Sie schließen das USB-Laufwerk an und starten das Tool „Laufwerke“. Dort hängen Sie das Laufwerk mit dem viereckigen Symbol links unterhalb der Partitionsanzeige aus und löschen mit der Minus-Schaltfläche eventuell bestehende Partitionen.

2. Klicken Sie dann auf das Zahnradsymbol und dort auf „Partition formatieren“. Im Folgedialog wählen Sie „Andere“ und „Weiter“ und im weiteren Unterdialog dann die Option „Passwortgeschützter Datenträger (Luks)“. Danach geben Sie zweimal das Kennwort ein und klicken auf „Formatieren“. Das war’s schon.

3. Die Alltagsbedienung ist ganz einfach – dafür sorgen alle geläufigen Dateimanager wie Nautilus, Nemo oder Thunar. Wenn Sie das USB-Gerät anschließen, erscheint automatisch der Dialog „Geben Sie eine Passphrase zum Entsperren [...] ein“. Bei manchen Dateimanagern muss das Gerät explizit in der Navigationsspalte angeklickt werden. Nach Eingabe des Kennworts ist das Medium entsperrt, gemountet und normal benutzbar.

Wer optimalen Schutz auch auf einem gelegentlich unbeaufsichtigten System erreichen will, sollte den Datenträger nach aktiver Benutzung stets aushängen – auch dies funktioniert im Dateimanager. Außerdem ist es bei unbeaufsichtigten Rechnern wichtig, auf das Speichern des Kennworts (im „Schlüsselbund“) zu verzichten. Solche Speicherung wird hier wie in anderen Fällen angeboten und kann mit „Passwort sofort vergessen“ abgelehnt werden.



KDE kann’s natürlich auch: Die KDE-Partitionsverwaltung verschlüsselt hier einen USB-Stick mit Luks (der Haupttext beschreibt das Vorgehen mit Gnome-Disks).

4. Home-Verschlüsselung mit Ecrypt FS

Ecrypt FS ist eine gegenüber Luks/Cryptsetup vergleichsweise einfache, dateibasierte Verschlüsselungsmethode, die aufgrund theoretischer (und eher akademischer) Sicherheitsmängel etwas diskreditiert wurde. Nach unserer Ansicht ist diese Methode für private Datenschutzansprüche weiterhin völlig ausreichend. Mit dieser Einschätzung sind wir nicht allein: Der modifizierte Ubuntu-Installer von Linux Mint zeigt beim Anlegen des Erstbenutzers nach wie vor die Option „Meine persönlichen Dateien verschlüsseln“. Dabei handelt es sich um das besagte Ecrypt FS, angewandt auf das komplette Home-Verzeichnis des Erstbenutzers. Bei Fremdzugriff auf den Rechner ist zwar der Großteil des Dateisystems lesbar, nicht aber der Inhalt von „/home/[user]“. Dieser liegt verschlüsselt und mit verschlüsselten Dateinamen unter „/home/.ecryptfs/[user]/.Private“. Die Dateien werden automatisch unverschlüsselt nach „/home/[user]“ geladen, sobald sich der Benutzer am System anmeldet. Insofern ist die Home-Verschlüsselung ebenso transparent wie Luks und sogar etwas einfacher, weil das Entsperren mit der Systemanmeldung zusammenfällt.

Der Ubuntu-Installer hat sich aufgrund der oben angesprochenen Bedenken von Ecrypt FS verabschiedet. In den Ubuntu-Paketquellen ist das Werkzeug aber noch durchaus vertreten und mit

```
sudo apt install ecryptfs-utils
```

schnell nachgerüstet. Danach legt der Terminalbefehl

```
sudo adduser --encrypt-home sepp
```

ein neues Konto mit Home-Verschlüsselung an, wobei das zugehörige neue Systemkennwort zweimal abgefragt wird. Das war’s schon: Der neue Benutzer kann sich anmelden und sein verschlüsseltes „Home“ wird bei der Anmeldung automatisch aus „/home/.ecryptfs/sepp“ unverschlüsselt nach „/home/sepp“ gemountet.

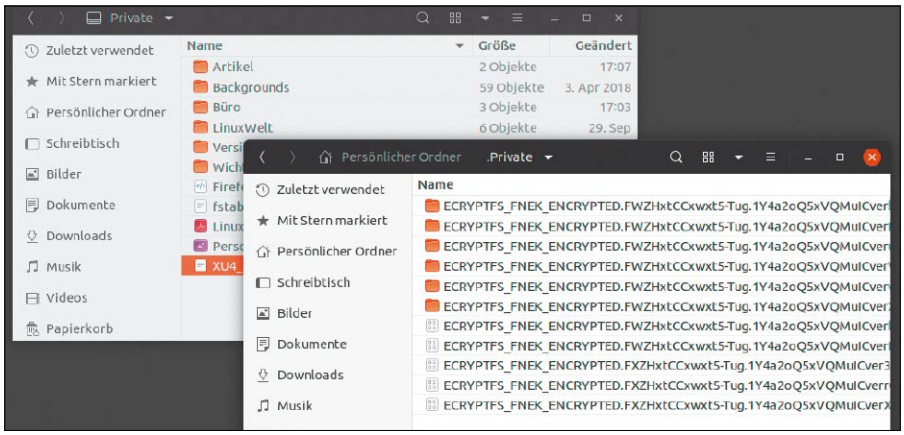
Das Home des Erstbenutzers lässt sich mit dieser Methode nicht mehr umstellen. Jedoch kann Ecrypt FS im Home des Erstbenutzers immerhin nachträglich einen verschlüsselten Ordner „Private“ einrichten:

```
ecryptfs-setup-private
```

Das Kommando fordert zunächst die Eingabe des Systemkennworts („login-passphra-

se"). Danach erwartet das Werkzeug mit der „mount-passphrase" den Schlüssel, mit dem die Daten codiert werden. Die „mount-passphrase" müssen Sie bei der späteren Benutzung niemals interaktiv eingeben und darf daher komplex ausfallen. Nach der nächsten Anmeldung erscheint im Home-Verzeichnis der neue Ordner „~/Private". Alle Dateien darin werden durch die Kontenanmeldung aus dem versteckten Ordner „~/.private" entschlüsselt.

Noch ein Vorteil von Ecrypt FS: Während Luks/Cryptsetup etwas Systemleistung kostet (drei bis zehn Prozent), können wir auch hier auch bei großen Datenmengen keinen Unterschied zu unverschlüsselten Daten feststellen. Ecrypt FS ist für Desktopsysteme und Notebooks oft der angemessene und der einfachste Schutz.



Ecrypt FS funktioniert als Teillösung auch nachträglich: Das Tool richtet unter „/home/[user]" einen Ordner „~/Private" ein, der bei der Systemanmeldung die Daten aus „~/.Private" entschlüsselt.

5. Veracrypt: Verschlüsselte Container auf USB

Solange Linux unter sich bleibt, empfehlen wir eindeutig die bisher beschriebenen Optionen. Sobald aber verschlüsselte Daten auf mobilen USB-Medien mit anderen Betriebssystemen gelesen werden sollen, kommen Luks und Ecrypt FS nicht in Betracht. Eine plattformunabhängige Alternative ist Veracrypt (*www.veracrypt.fr/en/Downloads.html*), das allerdings nicht ganz deren Systemintegration und Transparenz erreicht. Unter Ubuntu & Co. kommt man bequemsten über das PPA

```
sudo add-apt-repository
 ppa:unit193/encryption
sudo apt update
sudo apt install veracrypt
```

an die aktuellste Version.

Vor dem Einsatz der Software sollten Sie sicherstellen, dass Ihr USB-Laufwerk mit NTFS formatiert ist. FAT32 ist nicht geeignet, weil dort eine verschlüsselte Containerdatei nur maximal vier GB fassen könnte. Ein Linux-Dateisystem ist ebenfalls ungeeignet, weil dann Windows nicht zugreifen könnte.

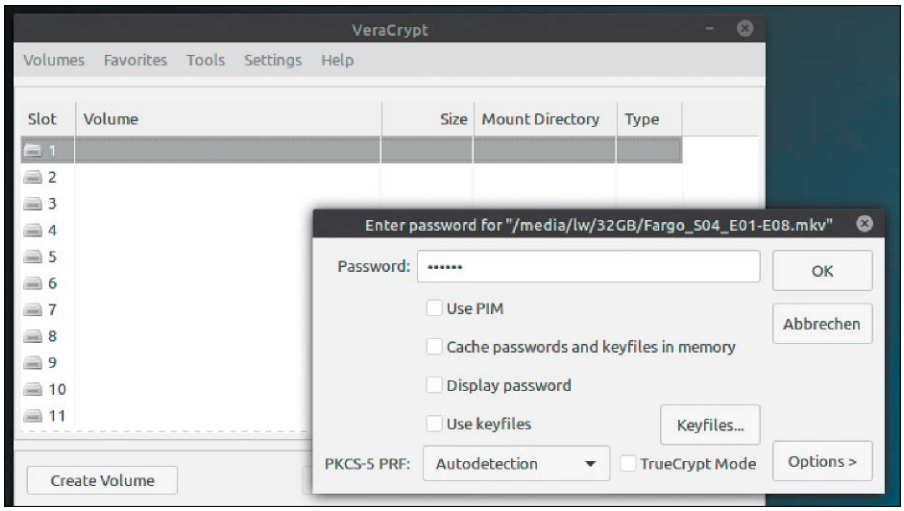
Um eine neue Containerdatei anzulegen, klicken Sie im Hauptfenster auf „Create Volume", dann auf „Create an encrypted file container" und auf „Standard VeraCrypt volume". Hier geben Sie Pfad und Namen einer bisher nicht existierenden Datei auf dem USB-Laufwerk an. Unter „Encryption Options" belassen Sie alles und definieren dann die Größe der Containerdatei. Diese sollte großzügig ausfallen, weil sich die Kapazität nachträglich nicht anpassen lässt (Veracrypt kann zwar beliebig viele Container nutzen, aber das erschwert den Überblick). Danach kommt die Passwortvergabe. Hier gibt es diverse Optionen – am einfachsten ist ein gutes, aber gut memorierbares Passwort.

Bei den nachfolgenden „Format Options" für das innere Dateisystem des Containers wählen Sie wie beim generellen Dateisystem für das Laufwerk erneut das Windows-Dateisystem NTFS. Ein USB-Medium, das Sie unter allen Systemen nutzen möchten, muss nicht nur selbst ein allgemein kompatibles Dateisystem haben, sondern auch der Veracrypt-Container muss mit einem solchen formatiert sein.

Im Allgemeinen machen Sie mit NTFS als Datenträgerformat und internes Containerformat wenig falsch. Zur Schlüsselerstellung auf Basis des Passworts erwartet Veracrypt Mausbewegungen im eigenen Fenster. Schließen Sie den Vorgang am Ende mit „Format" ab. Damit ist der Container einsatzbereit.

Um den Container zu verwenden, navigieren Sie mit „Select File" im Hauptdialog zur Containerdatei. Mit Klick auf „Mount" wird diese im Dateimanager geöffnet. Linux mountet Container standardmäßig (aber nicht zwangsläufig) nach „/media/veracrypt[nummer]", Windows auf freie Laufwerkbuchstaben. Auf diesen Datenträgern lesen und arbeiten Sie wie auf einem normalen Laufwerk. „Dismount" im Hauptdialog entlädt den Container, der somit wieder geschützt ist.

Achtung root-Recht: Beachten Sie, dass Sie beim Mounten von Veracrypt-Containern unter Linux nach dem Systemkennwort (sudo) gefragt werden, das mit dem Containerpasswort nichts zu tun hat. ■



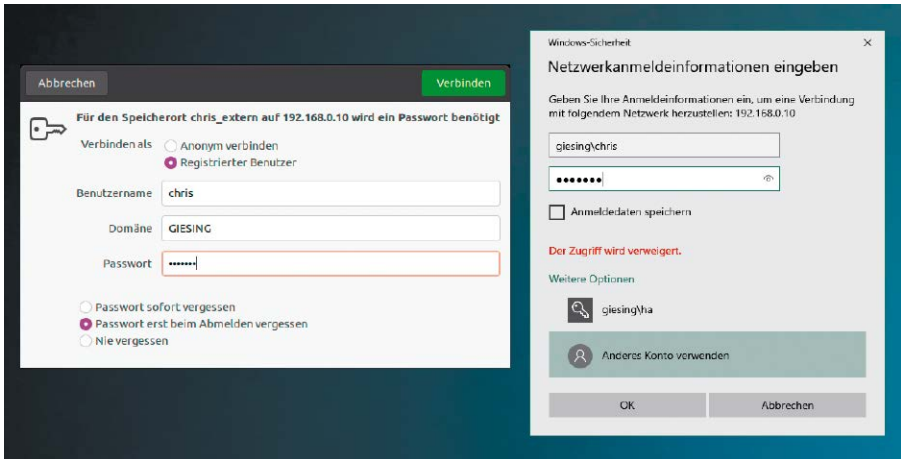
Verschlüsselte Veracrypt-Container: Das externe Werkzeug ist für den Austausch mit Windows-Systemen unverzichtbar, kann aber auch Installationsversäumnisse kompensieren.

(Ziel-)Sichere Netzfreigaben

Bei „Datenschutz & Sicherheit“ denken die meisten an verlorene Datenträger, Hacker im Netz, Aktivitätentracking oder Netzwerkspionage. Darum geht’s hier aber nicht: Thema sind hier zielgenaue Netzfreigaben, die erlauben, was nötig ist, aber nicht mehr.

VON HERMANN APFELBÖCK

Wer im privaten Netz oder einem kleinen Firmennetz für den komfortablen Datenaustausch der Teilnehmer sorgen will, braucht keine jahrelange Admin-Erfahrung. Aber ein klarer Plan kann nicht schaden. Wo genügt sicherer Lesezugriff? Wo ist für wen Schreibrecht erforderlich? Benötigen einige oder alle Teilnehmer geschützte, private Bereiche, die für andere unzugänglich sein sollen? Das ist das Thema der folgenden Seiten: Die User sollen Zugriff auf alles Notwendige erhalten, ohne den Datenbestand der anderen zu kompromittieren oder das System gefährden zu können.



Samba-Anmeldungen: Neben Konto und Passwort wird die „Domäne“ abgefragt – im privaten Umfeld wahlweise der Rechnername oder die Arbeitsgruppe („smb.conf“, Zeile „workgroup=[...]“)

1. Netzfreigaben und Außensicht

Paranoia vor unerwünschten, unbekannten Eindringlingen ist im lokalen Netzwerk nicht angebracht: Samba-, SSH-Freigaben oder vergleichbare lokale Dienste (UPnP/DLNA-Medien, Apache-Server) sind nur vom Teilnehmerkreis innerhalb des lokalen Netzes zu erreichen, nicht von außen über das Internet. Sicher ist es technisch möglich, solche Freigaben für das Internet zu öffnen, aber dies geschieht nicht unabsichtlich, sondern nur durch gezielte manuelle Portweiterleitungen im Router zur IP-Adresse des Servers. Dies ist hier nicht das Thema, und wer sich dies zutraut, muss deutlich höhere Sicherheitsansprüche stellen, komplexe Kennwörter verwenden und fundiertes Know-how zur Serversicherheit mitbringen. Einziges theoretisches Einfallstor – zumindest für einige unmittelbare Nachbarn – wäre ein offenes oder schwach geschütztes WLAN. Ist das WLAN über WPA durch ein komplexes Kennwort abgesichert, dann ist jeder Zugriff von außen ausgeschlossen.

Lokale Serverdienste ohne Portweiterleitungen können sich folglich sicherheitstechnisch ganz auf die Nutzer, Geräte und Betriebssysteme konzentrieren, die sich innerhalb des lokalen Adressraums tummeln. Im Home-Office sind das oft nur einige Familienmitglieder mit etlichen PCs, Notebooks und Smartphones und Tablets.

2. Samba: Die Voraussetzungen

Der Server, der Dateien im Netz freigibt, benötigt dazu die Serverkomponente. Auf vielen Serverdistributionen ist dieser Standard, bei Bedarf mit

```
sudo apt update && sudo apt upgrade
sudo apt install samba samba-common
```

aber auch schnell nachinstalliert. Die Zugriffskomponente, den Samba-Client, bringt jedes Linux, Windows und Mac-OS immer mit (für Tablets und Smartphones gibt es Apps im jeweiligen App Store). Die weiteren Voraussetzungen auf dem Server sind für jeden Benutzer ein Systemkonto (für die Dateirechte auf dem Server selbst) sowie ein Samba-Konto (für die Netzwerkrechte). Wir beschreiben diese Aktionen mit dem Terminal, weil diese Methode auch auf SSH-administrierten Servern und Platinen funktioniert:

1. Die Systemkonten richten Sie so ein:

```
sudo adduser anna
sudo adduser bert
```

Zuerst müssen Sie Ihre sudo-Berechtigung mit Ihrem eigenen Systemkennwort nachweisen. Der Befehl legt dann das Systemkonto an und fordert dafür ein neues Systemkennwort, alle nachfolgenden Abfragen sind optional. Zum Auflisten aller Systemkonten hilft

```
cat /etc/passwd
```

Die Systemkonten stehen am Ende mit IDs ab „1000“ (ID 1000 hat der Erstbenutzer).

2. Nun erhält jeder Nutzer noch sein eigenes Samba-Konto:

```
sudo smbpasswd -a anna
sudo smbpasswd -a bert
```

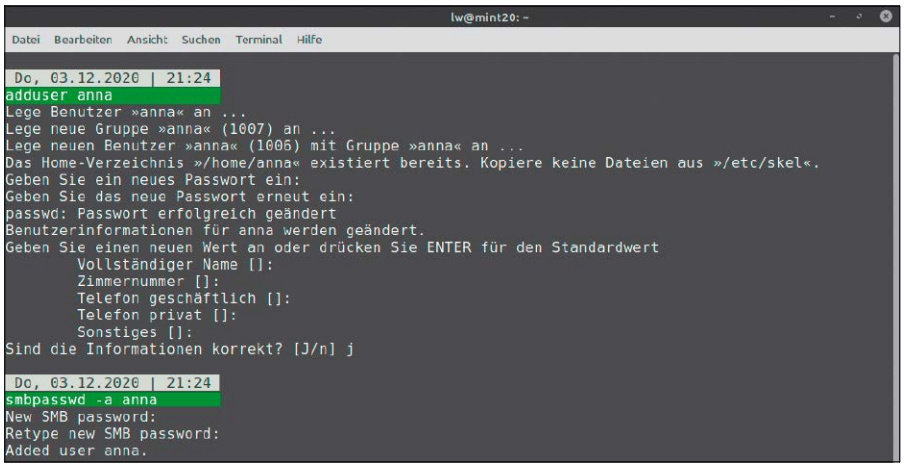
Dieser Befehl legt Samba-Konten neu („-a“ für „add“) an und fordert dafür ein Samba-Kennwort. Zur besseren Übersicht ist es zu empfehlen, dieses Kennwort identisch mit dem Systemkennwort zu wählen (im Prinzip sind die Kennwörter unabhängig). Alle eingerichteten Samba-Konten zeigt folgender Befehl:

```
sudo pdbedit -L
```

3. Die eigentliche Definition der Freigaben erfolgt auf dem Server in der zentralen Samba-Konfigurationsdatei „/etc/samba/smb.conf“ mit root-Recht (sudo). Hier gibt es dann sehr unterschiedliche Strategien, deren einfachste Varianten wir nachfolgend beschreiben. Grundsätzlich ist zu empfehlen, von der Originaldatei und von funktionierenden Versionen dieser Datei jeweils eine Sicherungskopie anzulegen. Die Rückkehr zum letzten Zustand ist dann völlig unkompliziert. Beachten Sie, dass Samba Änderungen der Konfigurationsdatei oder deren Austausch erst realisiert, wenn der Dienst mit

```
sudo service smbd restart
```

neu gestartet wird.



Systemkonto plus Samba-Konto: Dies sind die Grundvoraussetzungen für jeden Samba-Netzwerkzugriff. Die Freigaben selbst regelt dann die Samba-Konfiguration.

3. Samba und die Home-Verzeichnisse

Die Standarddatei „/etc/samba/smb.conf“ bietet eine sehr einfache Freigabevariante, die sich für viele Netzwerke eignet und die Sie nur freischalten müssen. An relativ später Stelle finden Sie hier einen auskommentierten Abschnitt, der mit „;[homes]“ beginnt. Wenn Sie dort alle Semikolon-Kommentarzeichen entfernen („#“-Zeilen sind nur Erläuterungen), gibt der Samba-Server die Home-Verzeichnisse aller Benutzer frei. Die Voraussetzungen gemäß Punkt 2 müssen allerdings vorab erfüllt sein.

Abweichend zur Vorgabe ist der Schreibzugriff in aller Regel notwendig („read only = no“), damit die Benutzer ihre Dateien dort ablegen dürfen. Alle anderen Angaben („browseable = no“ oder „valid users = %S“) sind sinnvoll, weil der Server dann ohne Angabe eines erlaubten Kontos schlicht gar nichts anzeigt: Die Adresse „smb://[IP]“ unter Linux oder „\\[IP]“ unter Windows führt dann einfach zu einem leeren Dateimanagerfenster, während „smb://[IP]/anna“ zur Authentifizierung aufruft (sofern ein Konto „Anna“ vorliegt). Der Abschnitt lautet also insgesamt:

```
[homes]
comment = Homes
browseable = no
read only = no
create mask = 660
directory mask = 770
valid users = %S
```

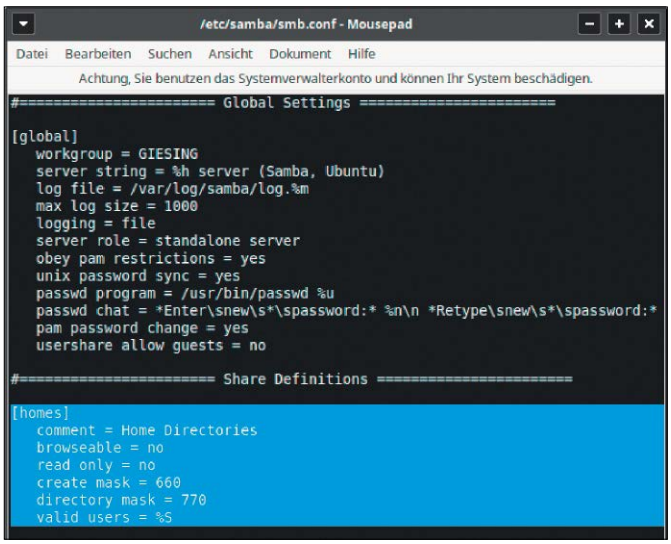
Solche Freigabe der Homes ist ebenso sinnvoll wie einfach, wenn mehrere Familienmitglieder oder Mitarbeiter ihr je eigenes Home-Verzeichnis für Arbeiten und Backups erhalten sollen.

Die Zugriffsrechte von neu erstellten Dateien werden auf „660“ gesetzt, was volles Schreibrecht einräumt. Bei Verzeichnissen sorgt „directory mask = 770“ für Vollzugriff beim Benutzer.

Datenschutztipp für Home-Freigaben: Bei der beschriebenen Freigabemethode haben die diversen Benutzer keinen Zugriff auf das Home der anderen. Der Administrator aber natürlich schon, wenn er den Server mit root-Recht via SSH verwaltet. Wenn Nutzer bestimmte Daten auch vor dem Administrator schützen wollen, müssen sie diese manuell verschlüsseln. Es gibt aber noch einen komfortableren Weg: Wenn das Systemkonto „anna“ mit

```
sudo adduser --encrypt-home anna
```

eingerichtet wurde (siehe dazu vorangehenden Artikel), dann wird dieses Home automatisch verschlüsselt. Die Fernanmeldung per Samba sorgt dann genau wie eine Systemanmeldung für die Entschlüsselung. Auch neu angelegte Daten werden wunschgemäß verarbeitet. Der Administrator wird also bei der Durchsicht dieses Home-Verzeichnisses nur verschlüsselten Dateien vorfinden. Allerdings kann er sich immer noch direkt als „anna“ anmelden, da er in



Ausgemistete Datei „smb.conf“ mit Home-Freigaben: Das ist der absolut einfachste Weg, für mehrere User eine Netzwerkheimat zu schaffen.

der Regel das Kennwort kennt. Im privaten Umfeld könnte man das so lösen, dass der Administrator beim Anlegen des Kontos („adduser…“) dem Benutzer selbst die diskrete Eingabe seines Kennwort erlaubt.

4. Samba-Freigaben für einzelne Konten

Die beschriebenen Home-Freigaben sind sehr praktisch, eignen sich aber nicht überall – jedenfalls nicht als alleiniges Angebot. Wer den Benutzern ein zentrales Datendepot mit Medien und Dokumenten anbieten will, benötigt in jedem Fall eine andere Lösung (siehe Punkt 5). Der Samba-Standard für die Homes hat aber insbesondere auf Platinenservern noch ein anderes, nämlich ein Platzproblem. Das System samt Home-Ordner liegt dort auf relativ kleinen SD-Karten, die eigentlichen Kapazitäten bieten externe USB- oder SATA-Laufwerke. Wo mit solchen Platzproblemen zu rechnen ist, benötigen die User ihre Spielwiese an anderer Stelle. Dies erfordert dann eine gesonderte Freigabe für jeden Benutzer in der Datei „/etc/samba/smb.conf“:

```
[Anna]
path=/srv/Data/Anna
browseable = yes
valid users = anna
write list = anna
create mask = 660
directory mask = 770
```

Hier erhält „Anna“ im genannten Ordner („path“) das volle Schreibrecht („write list“). Die Zugriffsrechte von neu erstellten Dateien werden auf „660“ gesetzt, was „Anna“ ebenfalls Schreibrecht einräumt. Bei Verzeichnissen sorgt „directory mask = 770“ für Vollzugriff beim Benutzer. Da an dieser Stelle außer „Anna“ (und Gruppe „anna“) keiner zugreifen soll, ist die letzte Stelle (für andere Konten) in der Bitmaske auf „0“ gesetzt. Um lokale Rechteprobleme mit bestehenden Dateien (mit root als Besitzer) vorab auszuschließen, erstellt der Administrator am besten nur den Ordner „/srv/Data/Anna“ (wie im Beispiel) ohne weitere Daten und weist dann „Anna“ das Besitzrecht zu:

```
sudo chown -R anna /srv/Data/Anna/
```

Für alles, was „Anna“ dann selbst auf dem Server stellt, gilt sie dann als Besitzer.

5. Samba-Freigaben für alle (1)

Um ein gemeinsames Medien- und Dokumentenarchiv für viele Benutzer bereitzustellen, gibt es zwei verschiedene Methoden: Die etwas einfachere Freigabevariante bezieht sich auf nur ein Konto, das man als Arbeitskonto allen Beteiligten mitteilen könnte – etwa „worker“ oder „family“. Die Benutzer müssen dann nur wissen, dass sie auf diese Freigabe nicht mit dem eigenen Konto, sondern mit diesem Pseudokonto zugreifen müssen. Die Definition in der smb.conf könnte dafür so aussehen:

```
[Data]
path=/srv/Data
writeable = yes
guest ok = no
read only = no
browseable = yes
valid users = worker
write list = worker
create mask = 660
directory mask = 770
```

„worker“ muss natürlich wieder als System- und als Samba-Konto definiert sein (siehe Punkt 2). Damit „worker“ alle bestehenden Daten verwenden darf, müssen wahrscheinlich zunächst die lokalen Datei- und Besitzrechte geändert werden:

```
sudo chown -R root:worker /srv/Data
sudo find /srv/Data -type f -exec
  chmod 664 {} +
sudo find /srv/Data -type d -exec
  chmod 775 {} +
```

Von „worker“ neu erstellte oder geänderte Dateien erhalten laut „smb.conf“ ebenfalls die Rechtemasken 775 und 664.

6. Samba-Freigaben für alle (2)

Eine Samba-Freigabe, die mehrere Konten lesend und schreibend nutzen können, ist ein kleines Stück aufwendiger als der Zugriff mit einem Pseudokonto (Punkt 5). Das Problem besteht – wie generell – nicht bei den Samba-Rechten, sondern bei den lokalen Dateirechten. Auch hier ist es wahrscheinlich wieder notwendig, den Konten erst einmal Dateibesitz und Rechte einzuräumen. Um den Aufwand für mehrere oder viele Konten zu verringern, ist eine zusätzliche Benutzergruppe zu empfehlen. Diese kann etwa „family“ oder „mitarbeiter“ heißen:

```
sudo groupadd family
```

Die Konten sind der neuen Gruppe mit

```
sudo usermod -aG family anna
```

schnell zugewiesen. Nach der Aktion ist mindestens eine Systemabmeldung erforderlich. Danach erhält die Gruppe im Freigabepfad die nötigen Dateirechte:

```
sudo chown -R root:family /srv/Data
sudo find /srv/Data -type f -exec
  chmod 664 {} +
sudo find /srv/Data -type d -exec
  chmod 775 {} +
```

Für die Freigabe selbst in der „smb.conf“ ergibt sich folgende Empfehlung:

```
[data]
path = /srv/Data
writeable = no
write list = @family
inherit owner = yes
force group = family
force directory mode = 775
create mask = 664
force create mode = 664
```

„write list = @family“ gewährt der Gruppe vollen Schreibzugriff. Die weiteren Optionen sorgen dafür, dass neu erstellte Elemente dem Besitzer des darüber liegenden Ordners („inherit owner“) sowie der Gruppe „family“ gehören und Vollzugriff erhalten. ■

SAMBA UND SSH

Der Samba-Zugriff für viele Benutzer bedeutet auch entsprechend viele Systemkonten und jedes Systemkonto ist wiederum prinzipiell SSH-fähig.

Da auf Samba-Servern fast immer auch ein SSH-Server läuft, ist dies selbst für kleine Homeoffice-Server ein triftiger Grund, allzu großzügige „777“-Rechtemasken zu vermeiden. Klar – dem einzelnen User sollte auf seiner Samba-Freigabe alles Nötige erlaubt sein, aber wenn alle Dateirechte auf „777“ gesetzt sind, dann hat auch der nächste User dort vollen Zugang – freilich nicht über Samba, aber eben über SSH! Die Beispiele im Haupttext zeigen daher restriktivere Rechtemasken, die für andere Konten (die dritte Stelle der Rechtemaske) keines oder nur Leserecht vorsehen. Wer es sich einfach machen will, kann großzügiger konfigurieren, sollte dann aber den SSH-Zugriff einschränken. Dazu genügt es, in der Datei „/etc/ssh/sshd_config“ mit

```
AllowUsers ha
```

nur noch den Admin für SSH zuzulassen. Fast ein Muss auf Samba-Servern!

Daten in der Cloud

Wahrscheinlich käme man mit entsprechender Organisation ohne Clouddaten, Synchronisierung, Kollaboration durchs Leben. Einfacher wäre das gewiss nicht. Die richtige Einstellung zur Cloud heißt nicht „Nein“, sondern „Ja“ mit Augenmaß.

VON HERMANN APFELBÖCK



Es ist schon klar: Alle Dateien, die Sie bei einem Cloudanbieter speichern, befinden sich in fremden Händen: Der Cloudanbieter hat darauf Zugriff und – je nach gesetzlicher Situation – gewährt er auch anderen Zugriff, außerhalb Europas (Google, Microsoft, Dropbox) deutlich mehr als in Europa und Deutschland. Das heißt aber nicht, dass der Anwender auf die vielen Komfortfunktionen der Cloud verzichten muss. Mit kritischer Selbstbeschränkung auf das wirklich Notwendige und punktueller Verschlüsselung sensibler Daten kann er von den Vorteilen profitieren, ohne den Datenschutz zu vernachlässigen.

Cloudfunktionen und Alternativen

„Cloud“ ist ein großes Wort: Es meint virtuelle Maschinen, Serverdienste, Software, Datenbanken und Speicherplatz im Web, genau genommen auch Mail (siehe dazu die nachfolgenden Beiträge).

Hier geht es aber ausschließlich um Speicherplatz und Cloudfunktionen, wie er privaten Nutzern von allen Seiten angeboten wird (Google, Microsoft, Hardwarehersteller, Internetprovider, diverse spezialisierte Cloudanbieter wie Dropbox, Box, Spider Oak, Tresorit, Amazon, Strato). Die wichtigsten Motive, solche Angebote zu nutzen, sind folgende:

Globaler Zugriff: Wichtige Daten wie Termine, Kontakte, Kennwörter, Projektdaten sollen – für Sie selbst – von jedem Ort und Gerät zugänglich und aktualisierbar sein.

Datenfreigabe: Sie möchten Dokumente, Bilder, Medien unkompliziert anderen Personen anbieten.

Offsite-Backup: Wichtige Dateien sollen zusätzlich zur lokalen Sicherung auch im Internet liegen, damit sie auch einen eventuellen Elementarschaden zu Hause sicher überleben.

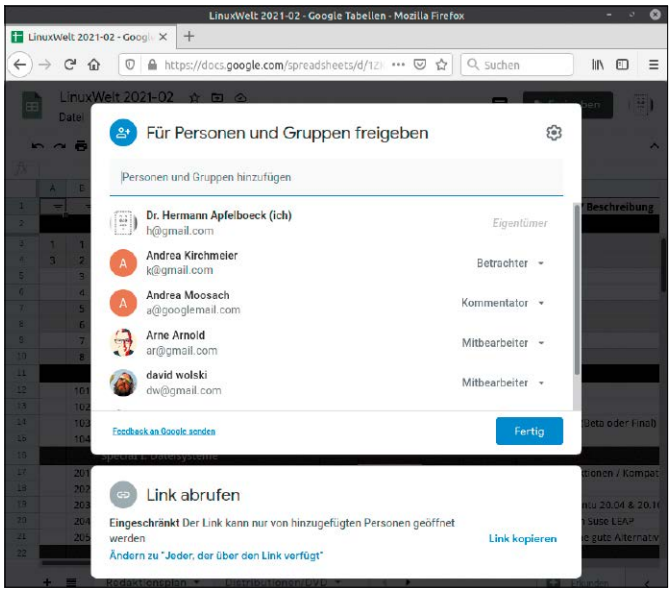
Synchronisierung von Software: Systeme und Programme sollen auf allen Geräten dieselben Voreinstellungen verwenden. Obwohl es auch für Windows und MS Office solche Cloudsynchronisierung gibt, ist letztlich der Webbrowser der einzige wichtige Softwarekandidat. Wer mehrere Rechner benutzt, wird darauf nicht verzichten wollen.

Kollaboration: Texte, Tabellen, Kalenderdaten sollen mit anderen Mitarbeitern gemeinsam genutzt und in Echtzeit bearbeitet werden.

Theoretische Alternativen werden Sie für alles finden, aber schwerlich ohne erheblichen Komfortverlust. Selbst wer sich eine selbst gehostete Lösung wie Nextcloud zutraut, wird bei Funktionalität und Echtzeitkooperation in Tabellen, Editoren und Kalender nicht annähernd den Komfort von Google oder Microsoft erreichen. Und selbst dann, wenn eine Kalenderanwendung auf der eigenen Homepage, eine Nextcloud oder ein Feng Office auf dem Platinenrechner funktional befriedigt, bedeutet dies für normale Anwender große Verantwortung, die leicht kontraproduktiv ausgeht: Fehlerhaft konfigurierte Eigenserver servieren die persönlichen Daten dann zwar nicht an Google & Co., aber an Hacker oder gleich öffentlich ins Web.

Daten und Freigaben in Cloudanwendungen

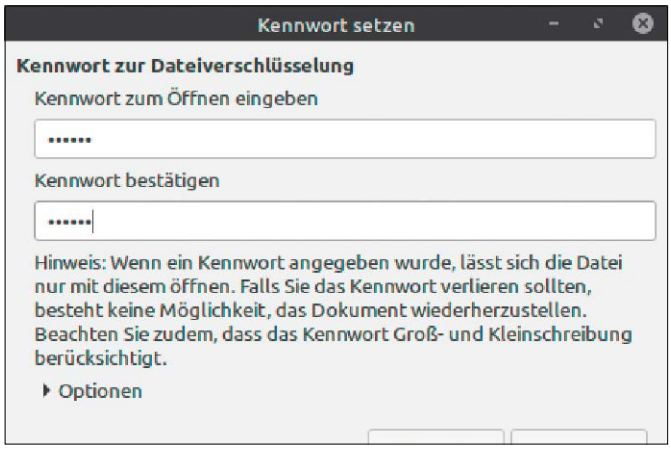
Clouddienste wie Kalender, Notizen, Tabellen et cetera müssen Sie nehmen, wie sie sind. Das heißt, Sie können diese nicht persönlich verschlüsseln. Für den Cloud-Admin sind die Daten ebenso lesbar wie für den Big-Data-Crawler des Anbieters. Einfache Maßnahme angesichts dieser Tatsache ist eine kritische Zurückhaltung mit personenbezogenen Daten: Wenn im Kalender „Arzt Hiebler“ steht statt „Kardiologe Hiebler, Sonnenstr. 17“, dann genügt das für den Nutzer ebenso, ohne Präzises preiszugeben. Grundsätzlich ist davon abzuraten,



Sichere Datenfreigabe in der Cloud: Bei einfacheren Diensten gibt es nur die allgemeine öffentliche Linkfreigabe, hier bei Google (oder bei Microsoft) genaue personenbezogene Freigaben.

Namen, Postadressen, Mailadressen dritter Personen auf einem mehr oder weniger öffentlichen Dokument zu versammeln. Ganz abgesehen vom vielleicht noch tolerierbaren Big-Data-Algorithmus gibt es immer wieder Pannen und Datenlecks – selbst bei Branchengrößen wie Google oder Dropbox. Der zweite Datenschutzaspekt bei Cloudanwendungen betrifft das „Teilen", also die Freigabe von Inhalten. Die Vorgehensweise ist überall einfach und unterm Strich weniger risikobehaftet als etwa bei einer komplexen Eigenlösung mit Nextcloud, Feng Office oder einem Mediawiki. Die offenere Freigabemethode erzeugt einfach einen Zugriffslink, mit dessen Kenntnis (verschickt typischerweise per Mail an die gewünschten Adressaten) jeder Webnutzer auf das Dokument zugreifen kann. Diese Methode ist bei einigen Clouddiensten die einzig mögliche Freigabe. Je nach Dokumentinhalt und Anzahl der Adressaten ist es bei dieser Methode ratsam, den Freigabelink nach kurzer Frist wieder abzuschalten. Denn der Zugriff ist hier in keiner Weise technisch beschränkt, und ein Weblink kann schnell seine Kreise ziehen.

Clouddienste wie Google Drive oder Microsoft Onedrive bieten neben dem pauschalen Freigabelink noch eine sicherere, personenbezogene Freigabe. Bei Google muss der Adressat ein Google-Konto besitzen, das nach „Freigeben" in die Liste der erlaubten Teilnehmer eingetragen wird. Wer Adressaten ohne Google-Konto erreichen will, muss sich für die unsichere allgemeine Freigabe entscheiden. Microsofts Onedrive kennt analog zu Google die gezielte Freigabe für Adressaten mit Microsoft-Konto, hat aber außerdem noch ein dritte Variante: die pauschale Freigabe mit Kennwort. Damit ist auch für Adressaten ohne Microsoft-Konto eine sichere Datenfreigabe möglich.



Dokumente mit Libre Office verschlüsseln (ähnlich MS Office): Diese Methode genügt für einzelne Dateien und geringe Datenmengen.

Benutzerdateien in der Cloud

Bei heutigen Festplatten, riesigen Kapazitäten auf externen USB-Laufwerken und unkomplizierten Linux-Lösungen für zentrale Samba-Server besteht keine ernste Notlage, Benutzerdaten massenhaft ins Internet zu sichern (und dies womöglich noch verstreut bei diversen Anbietern). Wer den Schutz seiner persönlichen Daten ernst nimmt, wird solche Cloudnutzung auf ein Mindestmaß bei einem Anbieter beschränken und außerdem alle dort abgelegten Dateien verschlüsseln, die persönliche Informationen oder Firmeninterna enthalten. Dafür gibt es etliche unkomplizierte Methoden.

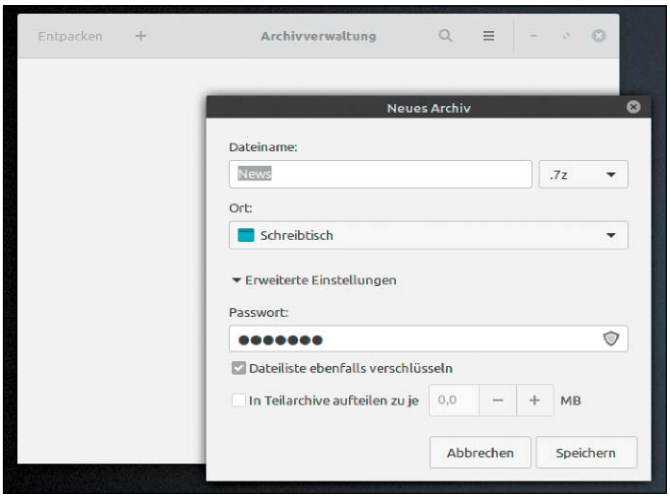
Kennwortschutz in Office: Libre Office und Microsoft Office bieten eine integrierte Verschlüsselung. Diese Methode, Dateien ad hoc einzeln zu verschlüsseln, eignet sich allerdings nur für wenige sensible Texte oder Tabellen, für größere Datenmengen ist sie zu unbequem. Libre Office bietet die Option „Datei → Speichern unter → Mit Kennwort speichern". Das Kennwort muss dann jeweils beim Öffnen eingegeben werden. Dass ein Dokument geschützt ist, ist Libre Office bei der Weiterbearbeitung klar: Es genügt künftig, normal zu speichern. Microsoft Office erledigt denselben Job unter „Datei → Speichern unter → Tools → Allgemeine Optionen". Libre Office kann – bei Kenntnis des Passworts – auch geschützte Microsoft-Dateien öffnen. Umgekehrt ist das nicht der Fall.

7-Zip-Verschlüsselung: Packer wie 7-Zip können zuverlässig verschlüsseln. Diese Methode eignet sich für kleinere und mittlere Datenmengen, denn immerhin sind mehrere Dateien oder auch komplette Ordner problemlos möglich. Wichtig für die Cloud: 7-Zip-Archive lassen sich zwischen Linux und Windows austauschen. Falls 7-Zip noch nicht vorliegt, installieren Sie den Packer unter Ubuntu und Co. mit

```
sudo apt install p7zip-full
```

nach, für Windows gibt es unter *www.7-zip.de/download.html* mehrere Downloadvarianten (der 64-Bit-Exe-Installer dürfte die einfachste Wahl sein). In Zusammenarbeit mit dem File-Roller oder Ark („Archivverwaltung") unter Linux, worunter sich 7-Zip integriert, beziehungsweise dem 7z-Filemanager unter Windows ist Verschlüsseln und Entschlüsseln recht komfortabel: Sie ziehen Datei oder Ordner einfach mit der Maus in das Fenster („Archivverwaltung" oder „7-

Zip"), bestätigen unter Linux, dass damit ein neues Archiv angelegt werden soll, und geben dann das Format „7z" und ferner unter „Erweiterte Einstellungen" das Passwort an. Die Option „Dateiliste ebenfalls verschlüsseln" sorgt dafür, dass das verschlüsselte Archiv auch keine Dateinamen verrät. Beim späteren Doppelklick des Archivs wird automatisch das Kennwort abgefragt und nur bei Kenntnis desselben entpackt. Unter Windows ist der Vorgang im Prinzip analog.



Packer 7-Zip als Sicherheitstool: In der Archivverwaltung muss das Format „.7z" gewählt werden, damit die Verschlüsselungsoptionen angeboten werden.

Onlinebackup mit Veracrypt-Container

Verschlüsselte Veracrypt-Container mit gewisser Größe und vielen darin enthaltenen Dateien sind für interaktives Arbeiten auf Cloud- oder Webservern völlig ungeeignet. Nur um etliche kleine Dateien einzusehen oder zu ändern, müsste man ständig die große Containerdatei downloaden und – meist noch deutlich langsamer – wieder uploaden.

Eine für Veracrypt einschlägige Ausnahme gibt es aber trotzdem – ein Onlinebackup für abgeschlossene größere Projekte. Wenn Sie etwa die Buchhaltung eines abgeschlossenen Jahres zur Sicherheit (etwa vor heimischen Elementarschäden) extern ablegen wollen, bietet ein Veracrypt-Container eine sichere Lösung. Der Download ist nur dann erforderlich, wenn Sie das komplette Backup benötigen.

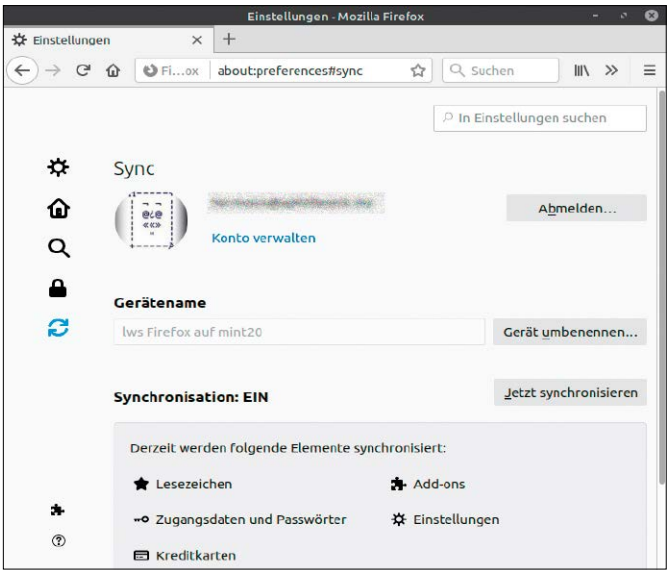
Das Kennwort für solche Backups sollten Sie an sicherer lokaler Stelle speichern oder notieren, um es auch nach Monaten oder Jahren wieder parat zu haben. Derartige verschlüsselte Projektsicherung ist Cloudnutzwert pur für den Anwender, für den Anbieter hingegen eine echte Strafe, der viel Speicherplatz ohne jeden auswertbaren Inhalt kostet. Hinweise zur Installation und praktischen Nutzung von Veracrypt ersparen wir uns an dieser Stelle, weil diese der Artikel „Datenschutz für mobile Geräte" ab Seite 120, Punkt 5, anbietet.

Synchronisierte Browser

Wer mehrere PCs und Notebooks verwendet, wird auf die Browsersynchronisierung nicht verzichten wollen: Ein neu installierter Browser zeigt nach fünf Minuten das gewohnte Gesicht. Browsersynchronisierung ist nur bei Windows und seinem Edge-Browser Bestandteil der allgemeinen Onedrive-Cloud, bei den typischen Linux-Browsern Firefox und Chrome/Chromium muss sie als Extrafunktion im Browser aktiviert werden. Der Umfang der Synchronisierung ist bei allen Browsern ähnlich und außerdem individuell einstellbar. Typischerweise werden Lesezeichen, Verlauf, Passwörter, Designs und Erweiterungen erfasst. Grundsätzlich übertragen die Browser die Synchronisierungsdaten zwar verschlüsselt, speichern sie aber nicht alle verschlüsselt auf dem Server – jedenfalls nicht ohne Aufforderung.

Firefox: Die Synchronisierung benötigt ein kostenloses Konto auf *https://accounts.firefox.com* (via Menü „Bei Firefox anmelden"). Der Umfang der Synchronisierung ist unter „Einstellungen → Sync" im Detail einstellbar. In der Regel wird man aus Komfortgründen auch die Passwörter einbeziehen („Zugangsdaten"). Anders als Chrome/Chromium verschlüsselt Firefox standardmäßig alle Daten, der Zugangsschlüssel verbleibt auf dem Gerät des Benutzers. Die Mozilla Foundation ist grundsätzlich vertrauenswürdig und macht keine Geschäfte mit Benutzerdaten. Weitere Maßnahmen sind nicht nötig.

Chrome/Chromium: Voraussetzung für die Synchronisierung ist ein Google-Konto. Der Umfang der Synchronisierung ist wie bei Firefox konfigurierbar. Anders als beim Firefox werden bei Google aber nur die Kennwörter verschlüsselt. Den Rest kann Google beliebig auswerten. Jedoch bietet der Browser unter „Einstellungen → Google und ich → Synchronisierung und Google-Dienste" den zusätzlichen Punkt „Verschlüsselungsoptionen". Das dabei genutzte Kennwort ist unabhängig vom Google-Kennwort und verschlüsselt alle Daten auf dem Google-Server, der Schlüssel verbleibt auf Ihrem Gerät. ■



Kleine, aber unentbehrliche Cloudfunktion: Webbrowser (hier Firefox) bieten plattformübergreifend identische Lesezeichen und Einstellungen via Synchronisierung.

Open PGP in Thunderbird

Mit Open PGP lassen sich E-Mails verschlüsseln oder signieren. Die dafür nötigen Funktionen sind ab Version 78 standardmäßig in Thunderbird enthalten und lassen sich somit komfortabler denn je nutzen.

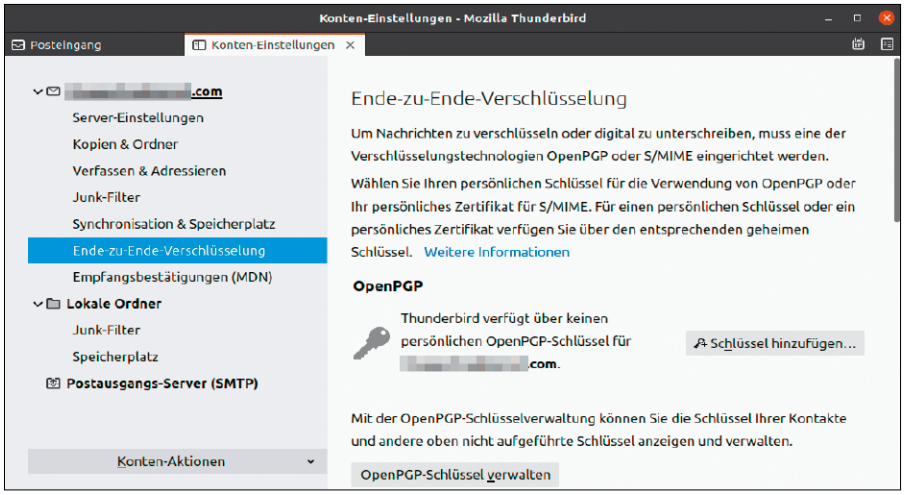
VON THORSTEN EGGELING

Die Kommunikation per E-Mail ist unkompliziert und wird daher immer noch häufig genutzt. Sie benötigen dafür nicht mehr als die E-Mail-Adresse des Empfängers. Dadurch wird jedoch auch der Missbrauch durch Spammer erleichtert. Ferner sollte man zumindest beim Austausch von Nachrichten mit vertraulichen Inhalten auf mehr Sicherheit setzen und die Nachrichten mit PGP (Pretty Good Privacy) verschlüsseln und/oder signieren. Vertrauenswürdige Schlüssel stellen dabei sicher, dass nur der jeweilige Empfänger die Nachrichten entschlüsseln, lesen oder die Echtheit prüfen kann.

PGP, das es bereits seit 1991 gibt, genießt allerdings keine breite Akzeptanz. Die nötigen Tools müssen erst installiert werden, die Konfiguration gilt als zu kompliziert. Zumindest für Thunderbird-Nutzer ab Version 78 könnte sich das ändern. Open PGP ist hier bereits integriert und lässt sich ohne großen Aufwand einsetzen.

Wie Open PGP funktioniert

Das Prinzip von Open PGP ist einfach. Ein Nutzer mit der E-Mail-Adresse „sepp@beispiel.de“ erzeugt selbst ein Schlüsselpaar. Seinen öffentlichen Schlüssel teilt er seinen Kommunikationspartnern mit, die E-Mails an ihn damit verschlüsseln. Der Empfänger, sepp@beispiel.de, kann die Nachrichten dann mit seinem privaten Schlüsseln entschlüsseln. Beim Signieren einer E-Mail erzeugt sepp@beispiel.de eine digitale Unterschrift mit seinem eigenen privaten und öffentlichen Schlüssel. Der Empfänger verwendet den öffentlichen Schlüssel, um die Integrität des Inhalts und den Absender zu prüfen.



E-Mails verschlüsseln und unterschreiben: Ab Version 78 ist Open PGP in Thunderbird integriert. Zusätzliche Programme sind nicht erforderlich, was die Konfiguration vereinfacht.

Bei der Vertrauenswürdigkeit setzte PGP bisher auf ein System von Beglaubigungen durch andere Benutzer (Web of Trust). Das wurde jedoch missbraucht, weshalb der von Thunderbird für die Suche nach Schlüsseln genutzte Server *https://keys.openpgp.org* dieses Verfahren nicht mehr unterstützt. Für mehr Sicherheit kann man den eigenen Schlüssel auch von einer übergeordneten Instanz beglaubigen lassen. Für Besitzer eines Personalausweises mit aktivierter Online-Ausweisfunktion ist das kostenlos über *https://pgp.governikus.de/pgp* möglich. Auch diese Beglaubigung ignoriert *https://keys.openpgp.org*. Es ist daher sinnvoll, den Schlüssel auf anderen Wegen zu veröffentlichen, beispielsweise auf dem eigenen Webserver.

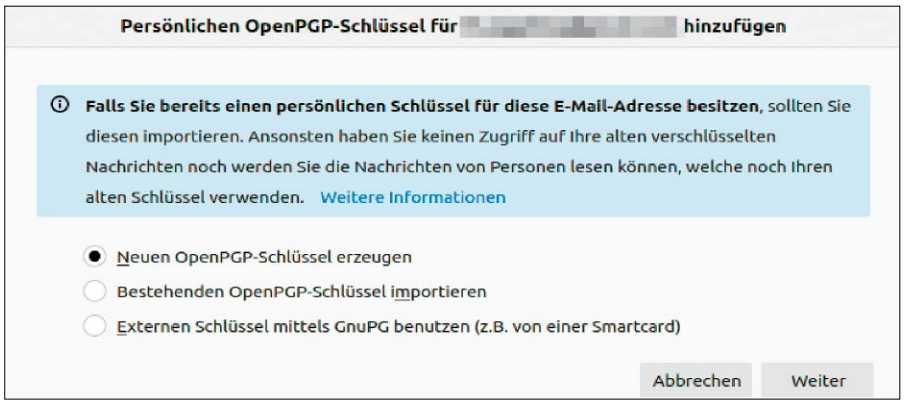
Open PGP in Thunderbird konfigurieren

Thunderbird sollte möglichst aktuell sein, damit Open PGP einwandfrei funktioniert. Gehen Sie auf das Menü mit den drei horizontalen Linien („Hamburger-Menü“) am rechten Rand des Fensters und dann auf „Hilfe → Über Thunderbird“.

Bei Redaktionsschluss war über die Standard-Paketquellen nur die Version 68 verfügbar, es ist aber Thunderbird ab Version 78 erforderlich. Sollte inzwischen noch keine Aktualisierung auf die neue Version vorliegen, verwenden Sie ein PPA. Fügen Sie es im Terminal hinzu (Ubuntu 20.04 und Linux Mint 20):

```
sudo add-apt-repository
  ppa:ubuntu-mozilla-security/ppa
sudo apt-get update
sudo apt-get upgrade
```

Wir haben nach der Aktualisierung die Kon-



PGP-Schlüssel: Neue Open-PGP-Schlüssel erstellen Sie über einen Assistenten in Thunderbird. Wer bereits PGP-Schlüssel besitzt, kann diese für das Konto importieren.

figuration unter Ubuntu 20.04 in Thunderbird 78.5.1 durchgeführt.

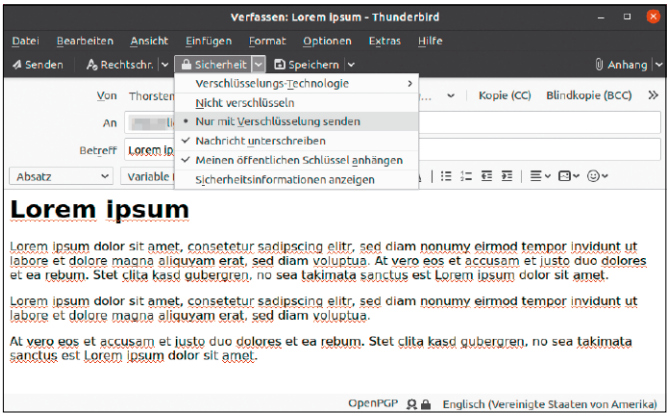
Schritt 1: Wir gehen davon aus, dass Thunderbird bereits für Ihr E-Mail-Konto konfiguriert ist. Klicken Sie im Hamburger-Menü auf „Konto-Einstellungen“ und dann beim gewünschten Konto auf „Ende-zu-Ende-Verschlüsselung“. Klicken Sie auf „Schlüssel hinzufügen“.

Schritt 2a: Wenn Sie bereits über Schlüssel verfügen, wählen Sie die Option „Bestehende OpenPGP-Schlüssel importieren“, klicken auf „Weiter“ und dann auf „Datei für den Import auswählen“. Wählen Sie Ihren privaten Schlüssel, klicken Sie auf „Öffnen“ und danach auf „Weiter“. Dann tippen Sie das Passwort für den Schlüssel ein und bestätigen mit „OK“. Per Klick auf „Weiter“ schließen Sie den Assistenten. Zurück in den „Konto-Einstellungen“ wählen Sie den eben importierten Schlüssel aus.

Schritt 2b: Wer noch keinen Schlüssel besitzt, belässt die Option „Neuen OpenPGP-Schlüssel erzeugen“, klickt auf „Weiter“ und dann auf „Schlüssel erzeugen“. Klicken Sie auf „Bestätigen“. Der neue Schlüssel wird automatisch für das Konto aktiviert.

Schritt 3: Klicken Sie auf „OpenPGP-Schlüssel verwalten“. Wählen Sie den Schlüssel aus und gehen Sie im Menü auf „Datei → Sicherheitskopie für geheime(n) Schlüssel erstellen“. Wählen Sie einen Speicherort und klicken Sie auf „Speichern“. Vergeben Sie ein sicheres Passwort, das Sie mit „OK“ bestätigen. Gehen Sie auf „Datei → Schlüssel in Datei exportieren“ und speichern Sie darüber auch den öffentlichen Schlüssel. Sie benötigen beide Dateien und das Passwort, wenn Sie Thunderbird auf einem anderen PC oder nach einer Neuinstallation mit Open PGP einrichten wollen.

Schritt 4: Die Schlüsseldaten sind ungeschützt in der Datei „key4.db“ im Thunderbird-Benutzerprofil gespeichert. Für mehr Sicherheit gehen Sie im Hamburger-Menü auf „Einstellungen“ und dann auf „Datenschutz & Sicherheit“. Setzen Sie ein Häkchen vor „Master-Passwort verwenden“ und legen Sie das Passwort fest. Abschließend können Sie Ihren öffentlichen Schlüssel bei *https://keys.openpgp.org* hochladen oder – bei Bedarf beglaubigt – auch an anderen Orten veröffentlichen.



Nachricht verfassen: Im Menü legen Sie fest, ob die E-Mail verschlüsselt oder nur unterschrieben werden soll. Der öffentliche Schlüssel lässt sich ebenfalls anhängen.

E-Mails verschlüsseln und signieren

Wenn Sie einem Empfänger, der ebenfalls PGP nutzt, erstmals eine Nachricht senden, wählen Sie unter der Schaltfläche „Sicherheit“ die Einträge „Nicht verschlüsseln“, „Nachricht unterschreiben“ und „Meinen öffentlichen Schlüssel anhängen“. Der Empfänger kann dann in Thunderbird über die Schaltfläche „OpenPGP“ Ihren öffentlichen Schlüssel importieren. Bei der Antwort auf die E-Mail wählt der Empfänger die gleichen Einstellungen und Sie importieren seinen öffentlichen Schlüssel. Danach können Sie verschlüsselte E-Mails austauschen oder Nachrichten signieren.

Den öffentlichen Schlüssel, etwa von der Webseite eines Empfängers, können Sie auch vorab importieren. Öffnen Sie die Schlüsselverwaltung über „Extras → OpenPGP-Schlüssel verwalten“ und gehen Sie auf „Datei → Öffentliche(n) Schlüssel aus Datei importieren“.

Wer einen Schlüssel prüfen möchte, öffnet per Doppelklick die „Schlüsseleigenschaften“, notiert die Angabe hinter „Fingerabdruck“ und fragt den Besitzer, ob der Wert mit dem Original übereinstimmt. ■

PGP FÜR WEBMAIL NUTZEN

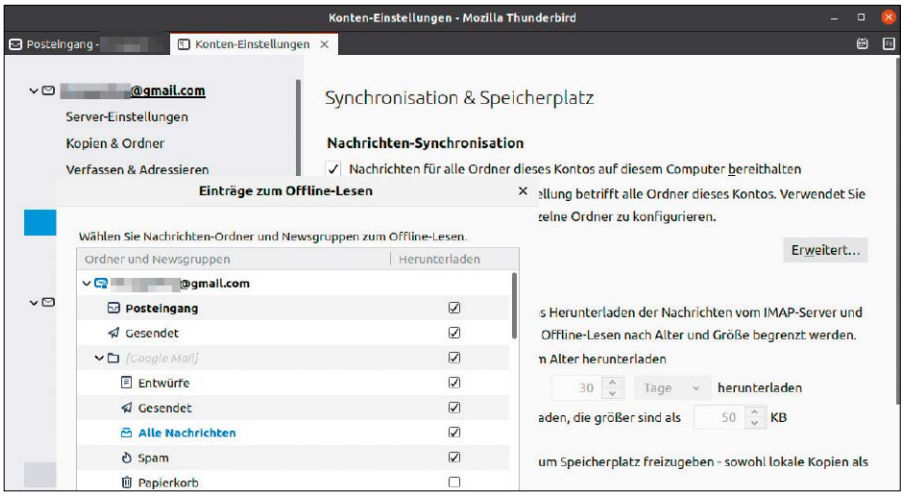
Wer E-Mails im Browser liest, muss nicht auf PGP verzichten. Mailvelope (*https://www.mailvelope.com*) gibt es als Add-on für Chrome, Edge und Firefox. Für Privatanwender ist die Nutzung kostenlos. Mailvelope arbeitet mit Google Mail, GMX, Web.de, 1&1, T-Online und einigen anderen Webmaildiensten zusammen.

Nach der Installation importieren Sie über die Schlüsselverwaltung des Add-ons vorhandene Schlüssel oder erstellen ein neues Schlüsselpaar. Öffnen Sie dann beispielsweise *https://mail.google.com*. Neben der Schaltfläche „Schreiben“ klicken Sie das Mailvelope-Symbol an und müssen dem Add-on danach die Nutzung der Gmail-API erlauben. Die verschlüsselte oder signierte E-Mail verfassen Sie danach in einem eigenen Editorfenster.

E-Mails sichern und umziehen

In E-Mails können wichtige Informationen enthalten sein, die man dauerhaft aufbewahren möchte oder sogar muss. Regelmäßige Datensicherung ist daher empfohlen oder ein zweiter E-Mail-Server als Backup.

VON THORSTEN EGGELING



Nachrichten zum Offlinelesen: Bei IMAP liegen die Daten erst einmal nur auf dem Server. In Thunderbird lässt sich aber konfigurieren, welche Ordner komplett heruntergeladen werden.

Bei der Verwendung von Webmailern liegen die E-Mails nur auf dem Server des Anbieters. Kommt es zu Störungen oder der Anbieter stellt sein Angebot ein, können E-Mails verloren gehen. Mit einem E-Mail-Programm wie Thunderbird hat man mehr Sicherheit. Die E-Mails können auch lokal gespeichert werden und sind dann auch ohne Internetverbindung abrufbar. E-Mails lassen sich auch auf einen anderen Server kopieren und dadurch sichern. Das ist auch sinnvoll, wenn man zu einem anderen Anbieter wechseln möchte. Ein Backup vom Server auf die lokale Festplatte und ein späterer Import sind ebenfalls möglich.

Thunderbird konfigurieren

Auch wer sonst nur einen Webmailer im Browser nutzt, sollte für Backups Thunderbird verwenden. Das E-Mail-Programm bietet die einfachsten Möglichkeiten, Sicherungen über eine grafische Oberfläche anzulegen.

E-Mail-Konten einrichten: Wenn Sie Thunderbird bisher nicht nutzen und das erste Mal starten, erscheint ein Assistent für die Konfiguration. Sie tragen Ihren Namen, E-Mail-Adresse und Passwort ein und klicken auf „Weiter“. Für die meisten bekannten E-Mail-Anbieter findet Thunderbird die nötigen Einstellungen automatisch. Sie haben in der Regel die Wahl zwischen den Protokollen „IMAP (Nachrichten auf dem Server speichern)“ oder „POP3 (Nachrichten auf dem Computer speichern)“. Sie sollten IMAP wählen, weil das Protokoll mehr Flexibilität bietet.

Hat Thunderbird die Daten für den Provider gefunden, genügt ein Klick auf „Fertig“. Andernfalls klicken Sie auf „Manuell einrichten“ und tragen die Serveradresse und Zugangsdaten gemäß der Anleitung Ihres Anbieters ein. Bei einigen E-Mail-Providern müssen Sie über den Webmailer in den Kontoeinstellungen den IMAP- und/oder POP3-Zugriff erst erlauben. Für eine Sicherung auf der Festplatte genügt der standardmäßige „Lokale Ordner“. Wenn Sie die Nachrichten auf einen anderen Server übertragen wollen, richten Sie ein weiteres Konto ein. Blenden Sie die Menüleiste mit der Alt-Taste ein, gehen Sie auf „Bearbeiten → Konten-Einstellungen“ und dann auf „Konto-Aktionen → E-Mail-Konto hinzufügen“.

Nachrichteninhalte speichern: Bei einem IMAP-Server werden die Nachrichten direkt geladen und angezeigt. Thunderbird ist jedoch auch für Situationen ohne Internetzugriff vorbereitet und speichert die Mails auch in lokalen Dateien. Die Optionen dafür finden Sie in den „Konto-Einstellungen“ beim jeweiligen Konto unter „Synchronisation & Speicherplatz“. Es muss ein Häkchen vor „Nachrichten für alle Ordner dieses Kontos auf diesem Computer bereithalten“ gesetzt sein. Klicken Sie auf die Schaltfläche „Erweitert“ und setzten Sie Häkchen hinter alle Ordner, die Thunderbird zum Offlinelesen speichern soll.

Schalten Sie Thunderbird per Klick auf das Symbol links unten im Fenster in den Offlinemodus. Klicken Sie auf „Jetzt herunterladen“. Damit werden alle E-Mails heruntergeladen, die bisher noch nicht lokal gespeichert sind. Das ist die Voraussetzung dafür, dass vollständige Backups durchgeführt werden können.

E-Mails auswählen und kopieren

Thunderbird kann nur E-Mails kopieren, aber keine kompletten Ordner. Deshalb legen Sie zuerst den Zielordner an. Gehen Sie im Kontextmenü von „Lokale Ordner“

oder des IMAP-Zielservers auf „Neuer Ordner“ und vergeben Sie eine passende Bezeichnung, beispielsweise „Posteingang-Backup“. Gehen Sie dann zum Posteingang des Kontos, von dem Sie E-Mails sichern wollen. Markieren Sie die gewünschten Nachrichten per Mausklick. Halten Sie die Strg-Taste gedrückt, um mehrere Nachrichten zu markieren, mit Strg-A markieren Sie alle E-Mails. Danach wählen Sie im Kontextmenü „Kopieren in → Lokale Ordner → Posteingang-Backup“.

E-Mails mit Pseudofilter automatisch sichern

Für eine automatische Sicherung können Sie einen Filter einrichten, der die Nachrichten automatisch in einen Zielordner kopiert.

Schritt 1: Gehen Sie in der Menüleiste (Alt-Taste) auf „Extras → Filter“. Stellen Sie hinter „Filter für:“ das Konto ein, von dem Sie Nachrichten kopieren möchten.

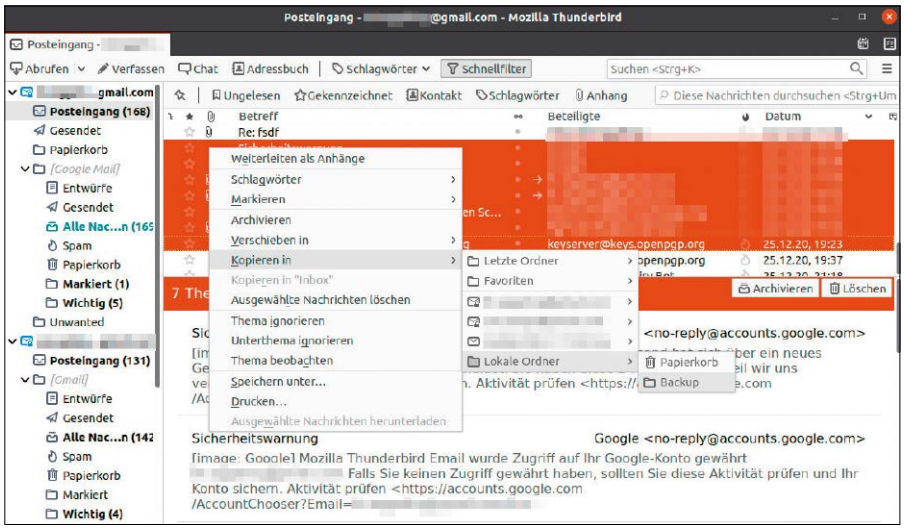
Schritt 2: Klicken Sie auf „Neu“ und vergeben Sie hinter „Filter-Name:“ eine aussagekräftige Beschreibung. Bei den Bedingungen ändern Sie „Betreff“ auf „Von“. Dahinter wählen Sie „enthält nicht“. Tippen Sie eine Bedingung ein, die garantiert niemals erfüllt wird, beispielsweise eine ungültige E-Mail-Adresse.

Schritt 3: Unter „Auszuführende Aktionen:“ stellen Sie „Kopieren der Nachricht in:“ ein und wählen dahinter den gewünschten Zielordner, beispielsweise „Lokale Ordner → Posteingang-Backup“. Klicken Sie auf „OK“. Hinter „Ausgewählte(n) Filter anwenden auf:“ stellen Sie „Posteingang“ ein. Zum Abschluss klicken Sie auf „Jetzt ausführen“.

Backup aller Thunderbird-Daten erstellen

Thunderbird speichert alle Daten im Home-Verzeichnis im versteckten Ordner „.thunderbird“. Um diesen sichtbar zu machen, gehen Ubuntu-Nutzer im Dateimanager Nautilus auf das Hamburger-Menü (drei horizontale Striche) und setzen ein Häkchen hinter „Verborgene Dateien anzeigen“. Unter Linux Mint finden Sie die Option im Dateimanager Nemo unter „Ansicht → Verborgene Dateien anzeigen“.

Damit tatsächlich alle Nachrichten im Backup enthalten sind, schalten Sie Thunderbird per Klick auf das Symbol links unten im Fenster in den Offlinemodus und laden dann alle Nachrichten herunter (siehe „Thunderbird konfigurieren“). Beenden Sie Thunderbird und kopieren Sie den Ordner „.thunderbird“ in ein Backupverzeichnis. Um Platz zu sparen, können Sie die Sicherung auch in ein ZIP- oder „tar.xz“-Archiv einpacken.



Backup für Ordnerinhalte: Markieren Sie die Nachrichten, die Sie sichern wollen. Über den Kontextmenüpunkt „Kopieren in“ speichern Sie die Nachrichten in einen anderen Ordner.

Auf einem anderen Rechner oder nach einer Linux-Neuinstallation kopieren Sie „.thunderbird“ in Ihr Home-Verzeichnis. Wenn Sie Thunderbird starten, entsprechen Konfiguration und Datenbestand dem Zeitpunkt des Backups. Die Thunderbird-Version muss allerdings identisch oder neuer sein, sonst wird die Datenübernahme verweigert.

Daten über ein Add-on sichern

Das Thunderbird-Add-on „ImportExportTools NG“ ermöglicht den Export einzelner E-Mail-Ordner, aller Ordner eines Kontos oder nur der Nachrichten aus einem Ordner. Außerdem unterstützt das Add-on automatische Backups. Exportierte Ordner oder Nachrichten lassen sich in ein anderes Konto importieren oder in „Lokale Ordner“. Das Add-on installieren Sie über das Menü „Add-ons“, indem Sie nach „ImportExportTools NG“ suchen und dann auf „Zu Thunderbird hinzufügen“ klicken. Das Add-on zeigt sich im Kontextmenü von Konten und Ordnern als „ImportExportTools NG“ mit

NACHRICHTENINHALTE SUCHEN UND LESEN

Thunderbird speichert Nachrichten in einem Textformat. Es ist daher nicht schwierig, Inhalte im Thunderbird-Profilordner beziehungsweise einem Backup davon zu finden. Thunderbird muss dazu nicht installiert sein. Stattdessen kommt das Tool grepmail zum Einsatz und zum Lesen der E-Mails das Programm mutt:

```
sudo apt install grepmail mutt
```

Öffnen Sie ein Terminal und gehen Sie in den Ordner, in dem sich die Dateien befinden:

```
cd ~/.thunderbird/[Profil]/ImapMail
```

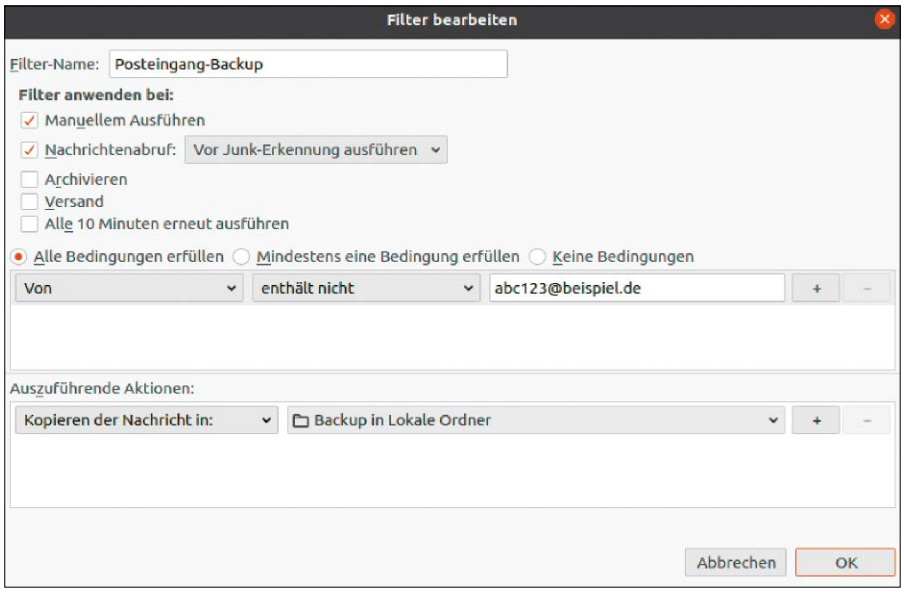
Im Ordner „ImapMail“ befinden sich die Dateien der IMAP-Konten, im Ordner „Mail“ die der anderen Konten. Eine Suche führen Sie mit

```
grepmail -F -R "[Suchbegriff]" . > gefunden.mbox
```

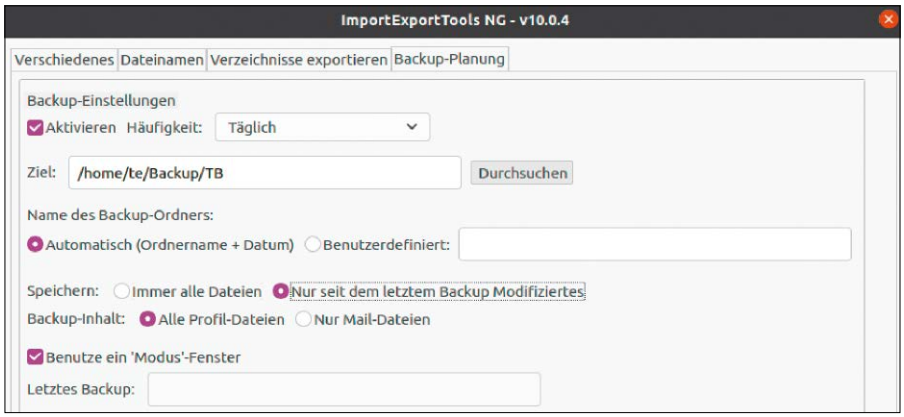
durch. Mit regulären Ausdrücken für „[Suchbegriff]“ lässt sich die Suche weiter eingrenzen. Die erzeugte Datei kann jeder Texteditor öffnen. Für die korrekte Darstellung der Inhalte verwenden Sie mutt:

```
mutt -f gefunden.mbox
```

Die Frage nach dem Ordner „/home/[User]/Mail“ beantworten Sie mit „N“. Danach können Sie in den Nachrichten blättern.



Automatische Sicherung: Mit einem Filter lassen sich Nachrichten beispielsweise aus dem Posteingang in einen anderen Ordner kopieren. Geeignet ist ein Ordner unter „Lokale Ordner“.



Regelmäßiges Backup: In der Konfiguration des Add-ons „ImportExportTools NG“ legen Sie einen Backupplan für die Sicherung des gesamten Profils oder nur der Nachrichten fest.

Untermenüeinträgen. Bei einem Konto können Sie „ImportExportTools NG → Alle Ordner des Kontos exportieren“ wählen. Bei IMAP-Konten erhalten Sie dann eine Meldung, dass Sie nur die lokale Kopie exportieren. Achten Sie darauf, dass Sie vor Nutzung des Add-ons on alle Nachrichten heruntergeladen haben (siehe „Thunderbird konfigurieren“). Wählen Sie einen Zielordner und klicken Sie auf „Öffnen“.

Sollten Sie verschachtelte Ordner angelegt haben, wählen Sie „Alle Ordner (mit Hierarchie) exportieren. Das Add-on ist bisher jedoch nicht in der Lage, die Ordnerhierarchie wieder zu importieren. Beim Import über „Mbox-Dateien importieren“ können Sie die Option „Ein Verzeichnis wählen, in dem (auch in Unterverzeichnissen) MBox-Dateien zum Importieren gesucht werden“ anklicken. Es werden dann alle Unterordner berücksichtigt, sie erscheinen aber direkt unterhalb des Hauptordners.

Automatisches Backup: Über „Extras → Add-on-Einstellungen → ImportExportTools NG“ erreichen Sie die Konfiguration des Add-ons. Auf der Registerkarte „Backup-Planung“ lässt sich das automatische Backup aktivieren. Hinter „Häufigkeit:“ stellen Sie ein, wann das Backup erfolgen soll, beispielsweise „Täglich“. Geben Sie hinter „Ziel:“ einen Ordner an, in dem Sie das Backup speichern wollen. Es empfiehlt sich, hinter „Speichern:“ die Option „Nur seit dem letzten Backup Modifiziertes“ zu wählen. Andernfalls sichert das Add-on immer das gesamte Thunderbird-Profil, was bei umfangreichen Ordnern zu lange dauert. Wenn ein Backup ansteht, zeigt das Add-on beim Beenden von Thunderbird eine Meldung, die Sie mit „OK“ bestätigen.

Dateien wiederherstellen: Abhängig von der gewählten Backupmethode, kopieren Sie über den Dateimanager das letzte vollständige Backup in den Thunderbird-Profilordner und – wenn konfiguriert – zusätzlich alle nachfolgenden Teilbackups.

E-Mail-Umzug mit imapsync

Das Kommandozeilentool imapsync ist auf den Transfer von IMAP-Ordnern von einem Server auf einen anderen spezialisiert. Sie setzen es ein, wenn Sie den Mailanbieter wechseln und die bisherigen IMAP-Ordner umziehen wollen.

Imapsync installieren: Für den Download gehen Sie auf *https://github.com/imapsync/imapsync*, klicken auf „Releases“ und laden die aktuelle Programmversion herunter. Entpacken Sie die „tar.gz“-Datei im Downloadverzeichnis. Öffnen Sie die Datei „~/Downloads/imapsync-1.977/INSTALL.d/INSTALL.Ubuntu.txt“ in einem Editor (Pfad bei Bedarf anpassen). Markieren Sie den Abschnitt von „sudo apt-get install \“ bis einschließlich „cpanminus“ und kopieren Sie ihn mit Strg-C in die Zwischenablage.

Öffnen Sie dann ein Terminal und geben Sie diesen Befehl ein:

```
sudo apt install build-essential
```

Danach fügen Sie den Inhalt der Zwischenablage mit Strg-Shift-V ein und bestätigen mit der Eingabetaste. Installieren Sie die benötigten Pakte. Wechseln Sie in das Downloadverzeichnis und starten Sie dort einen Test:

```
cd ~/Downloads/imapsync-1.977
./imapsync --testslive
```

Kopieren Sie die Datei „imapsync“ in den Ordner „/usr/local/bin“:

```
sudo cp imapsync /usr/local/bin
```

Imapsync nutzen: Das Tool erwartet als Parameter den Quell- und Zielserver sowie die Anmeldeinformationen. Ein typischer Aufruf kann so aussehen:

```
./imapsync --host1 [Quelle] --user1
  [User1] --password1
  '[Passwort1]'--host2 [Ziel]
  --user2 [User2] --password2
  '[Passwort2]' --dry
```

Ersetzen Sie die Platzhalter in eckigen Klammern durch die Serveradressen sowie Benutzernamen und Passwörter. Der Schalter „--dry“ führt einen Testlauf durch. Wurde dieser ohne Fehlermeldungen absolviert, lassen Sie die Option weg. ■

Eigene Internetdienste und Dyn DNS

Den Router und das heimische Netzwerk von überall aus und jederzeit erreichen zu können, ist sinnvoll und hilfreich. Damit der Zugriff aus dem Internet sicher und zuverlässig funktioniert, ist aber etwas Vorarbeit erforderlich.

VON THORSTEN EGGELING

Mit 40 MBit pro Sekunde Upload(!)-Geschwindigkeit oder mehr lassen sich zu Hause Serverdienste einrichten, die überall in der Welt erreichbar sind. Wenn nicht zu viele Personen gleichzeitig darauf zugreifen, reicht das mindestens für den Datenaustausch mit Familie und Freunden. Ist die Uploadkapazität geringer, funktioniert es ebenfalls, macht aber weniger Spaß.

Damit ein Server im eigenen Netzwerk aus dem Internet erreicht werden kann, ist eine spezielle Konfiguration erforderlich. Mit einer IPv4-Adresse vom Internetprovider ist der Aufwand gering, steht nur IPv6 zur Verfügung, wird es etwas komplizierter. Auf die Sicherheit sollte man besonders achten. Regelmäßige Systemupdates sind bei Servern Pflicht. Beschränken Sie den Zugang auf einen kleinen Personenkreis und sichern Sie den Server durch zusätzliche Maßnahmen ab.

IP-Adressen und Zwangstrennung

Jeder Router für den DSL- oder Kabelanschluss erhält vom Internetanbieter eindeutige öffentliche IP-Adressen, im optimalen Fall aus dem IPv4- und IPv6-Bereich. Wie diese lauten, erfahren Sie unter *https://ipv6-test.com*. Wird hier keine IPv4-Adresse angezeigt, ist der Router von außen nur über IPv6 erreichbar.

Ein Client muss daher ebenfalls IPv6 unterstützen. Das ist jedoch nicht immer gewährleistet, was die Zuverlässigkeit von Portfreigaben einschränkt.

Nach einem Neustart erhält der Router neue IP-Adressen, außerdem bei der Zwangstrennung durch den Internetprovider. Das ist bei einigen Anschlüssen alle 24 Stunden der Fall, bei anderen alle 180 Tage. Eine feste IP-Adresse gibt es nur bei ausgewählten Tarifen meist gegen Aufpreis.

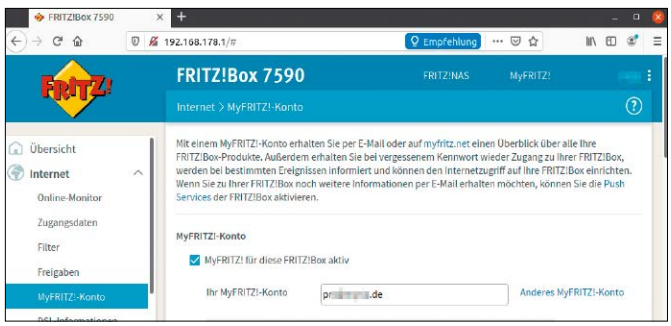


Keine konstanten IP-Adressen: Internetprovider trennen DSL-Verbindungen meist regelmäßig. Die Fritzbox sorgt immerhin für einen verlässlichen Zeitraum für die Zwangstrennung.

Die Fritzbox ist standardmäßig so konfiguriert, dass die Verbindung täglich zu einem bestimmten Zeitraum getrennt wird, um der zufälligen Zwangstrennung zuvorzukommen. Sie finden die Einstellungen in der Konfigurationsoberfläche der Fritzbox (standardmäßig *http://192.168.178.1* oder *http://fritz.box*) unter „Internet → Zugangsdaten → Internetzugang“ nach einem Klick auf „Verbindungseinstellungen ändern“.

Dynamisches DNS für die Fritzbox

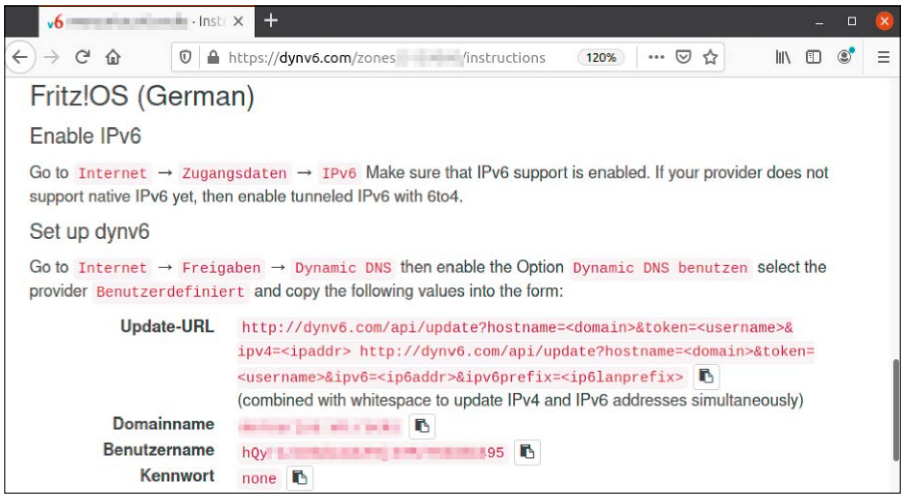
Dynamisches DNS oder Dynamic Domain Name System (Dyn DNS oder DDNS) hilft bei ständig wechselnden IP-Adressen. Der



Myfritz-Konto: Fritzbox-Nutzer erhalten einen kostenlosen Domainnamen vom Hersteller. Der ist allerdings nicht für Dienste geeignet, die nur über IPv6 erreichbar sind.

Router oder die Server im Heimnetzwerk sind damit immer über einen festen Domainnamen erreichbar. Besitzer einer Fritzbox können dafür das kostenlose Myfritz-Konto verwenden. Der AVM-Dienst unterstützt IPv4 und IPv6. Allerdings können Sie über IPv6 nur zur Fernwartung auf die Fritzbox selbst zugreifen, nicht aber auf andere Geräte im Netzwerk (siehe nächster Punkt).

Für Myfritz registrieren Sie sich über die Konfigurationsoberfläche unter „Internet → Myfritz-Konto“ mit Ihrer E-Mail-Adresse. Nach einer Bestätigung des neu angelegten Kontos tragen Sie die zugehörigen Zugangsdaten im Myfritz-Bereich der Fritzbox ein. Wenige Minuten später ist die Fritzbox bereits unter der neuen Dyn-DNS-Webadresse aus der Ferne erreichbar.



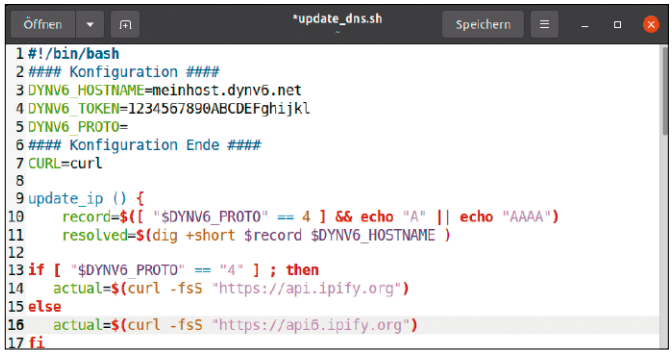
Konfiguration für Dynv6: Der Anbieter zeigt eine personalisierte Anleitung für die Fritzbox. Über IPv6 ist aber auch hier nur die Fritzbox erreichbar – und kein Server im Netz.

Dynamisches DNS für alle Router

Fast alle Router lassen sich auch mit einem unabhängigen Dyn-DNS-Dienst nutzen. Bei einem Netgear-Router finden Sie die Einstellungen unter „Erweitert → Erweiterte Einstellungen → Dynamisches DNS“, bei einem Modell von TP-Link unter „Erweitert → Netzwerk → Dynamisches DNS“. Bei Speedport-Routern der Telekom lässt sich ein Dyn-DNS-Dienst unter „Internet → Dynamisches DNS → Dynamisches DNS aktivieren“ einrichten. Eine Fritzbox lässt sich über „Internet → Freigaben → DynDNS“ konfigurieren.

Dynv6 konfigurieren: Meist sind verbreitete Dyn-DNS-Dienste auswählbar, teilweise auch eine benutzerdefinierte Konfiguration, etwa bei der Fritzbox. Wir empfehlen das kostenlose „Free Dynamic DNS“-Konto des Anbieters Dynv6 (*https://dynv6.com*), weil es IPv4 und IPv6 unterstützt und einfach zu konfigurieren ist. Auf der Startseite tippen Sie den gewünschten Domainnamen ein, wählen dahinter eine Domain wie „dynv6.net“ oder „v6.rocks“, geben Ihre E-Mail-Adresse ein und klicken auf „Go!“. Sie erhalten eine E-Mail, in der Sie auf „Confirm my account“ klicken. Anschließend werden Sie aufgefordert, ein Passwort festzulegen. Nach der Anmeldung landen Sie auf der Seite „My Zones“, auf der Sie den Namen Ihrer Domain anklicken. Klicken Sie auf „Instructions“. Hier finden Sie eine personalisierte Anleitung, wie Sie die Fritzbox für den Dienst konfigurieren.

Besonderheiten bei IPv6: Allerdings gilt auch bei Dynv6 die Einschränkung, dass der Zugriff auf Geräte im Netzwerk nur über IPv4 erfolgen kann. Über die IPv6-Adresse erreichen Sie ausschließlich die Fritzbox. Die Ursache dafür: Die Fritzbox teilt dem Dyn-DNS-Dienst ihre eigene öffentliche IPv6-Adresse mit. Erforderlich ist aber die öffentliche IPv6-Adresse des Servers im eigenen Netzwerk. Bei IPv6 kommt kein NAT zum Einsatz, das Anfragen an die öffentliche IP zur privaten IP im Netz weiterleitet. Stattdessen gibt die Fritzbox den Zugang auf die IPv6-Adresse des Servers frei.



Update per Bash-Script: Ein Script auf dem Server übermittelt die IPv6-Adresse des PCs an *https://dynv6.com*, über die er aus dem Internet weltweit erreichbar ist.

Dyn-DNS-Update per Script: Damit die korrekte IPv6-Adresse bei Dynv6 ankommt, verwenden Sie auf dem Server ein Bash-Script, das Sie unter *https://devwelt.de/snippets/5* finden. Das Script speichern Sie in einer Textdatei mit dem Namen „update_dyndns.sh“ im Home-Verzeichnis und machen es mittels

```
chmod 755 ~/update_dyndns.sh
```

ausführbar. Öffnen Sie die Datei in einem Editor:

```
nano ~/update_dyndns.sh
```

Tragen Sie hinter „DYNV6_HOSTNAME=“ den Domainnamen ein, den Sie bei Dynv6 konfiguriert haben. Hinter „DYNV6_TOKEN=“ gehört der Benutzername, der Ihnen auf *https://dynv6.com* unter „Instructions“ für die Fritzbox-Konfiguration angezeigt wird. Bei „DYNV6_PROTO=“ geben Sie nichts weiter an, wenn das Update für IPv4 und IPv6 erfolgen soll. Andernfalls tippen Sie dahinter „4“ oder „6“ ein.

Starten Sie das Script jetzt noch nicht, weil Sie zuvor den Router und den Server konfigurieren müssen.

IPv6-Adressen und Portweiterleitungen

Ubuntu und Linux Mint konfigurieren sich mit temporären IPv6-Adressen. Für einen Server ist das nicht zu gebrauchen, weil er über feste IP-Adressen ansprechbar sein muss. Um das zu ändern, führen Sie im Terminal diesen Befehl aus:

```
sudo nano /etc/
  sysctl.d/10-ipv6-privacy.conf
```

Ändern Sie die Werte

```
net.ipv6.conf.all.use_tempaddr = 0
net.ipv6.conf.default.use_
  tempaddr = 0
```

und speichern Sie die Datei. Dann starten Sie Linux neu. Rufen Sie *https://ipv6-test.com* und sehen Sie sich die IPv6-Adresse an.

Wie genau die Konfiguration des Routers durchzuführen ist, hängt vom Modell ab. Auf *https://portforward.com* finden Sie Anleitungen für zahlreiche Geräte in englischer Sprache.

Fritzbox konfigurieren: Bei einer Fritzbox mit aktuellem Fritz-OS (Version 06.83 oder höher) gehen Sie auf „Internet → Freigaben" und dort auf „Portfreigaben". Klicken Sie auf „Gerät für Freigaben hinzufügen" und wählen Sie hinter „Gerät" Ihren Server aus. „IPv6 Interface-ID" passen Sie an, wenn nötig. Die eingetragenen Werte müssen den letzten vier durch „:" getrennten Gruppen entsprechen, die Sie auf dem Server zuvor über *https://ipv6-test.com* 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 automatisch Freigaben für IPv4 und IPv6. Erstellen Sie bei Bedarf weitere Freigaben für „HTTPS-Server" (Port 443) und nach Auswahl von „Andere Anwendungen" etwa für einen OpenSSH-Server (Port 22).

Dynv6 aktualisieren: Jetzt starten Sie das im vorherigen Punkt vorbereitete Script im Terminal mit

```
~/update_dyndns.sh
```

Kontrollieren Sie auf *https://dynv6.com*, ob die IPv4- und IPv6-Adresse stimmen. Damit das Script automatisch die Adressen aktualisiert, starten Sie es nach Zeitplan. Im Terminal verwenden Sie

```
crontab -e
```

und fügen die Zeile

```
0 6 * * * /home/[User]/update_
  dyndns.sh
```

hinzu. Das Script wird dann jeden Tag um 06:00 Uhr ausgeführt.

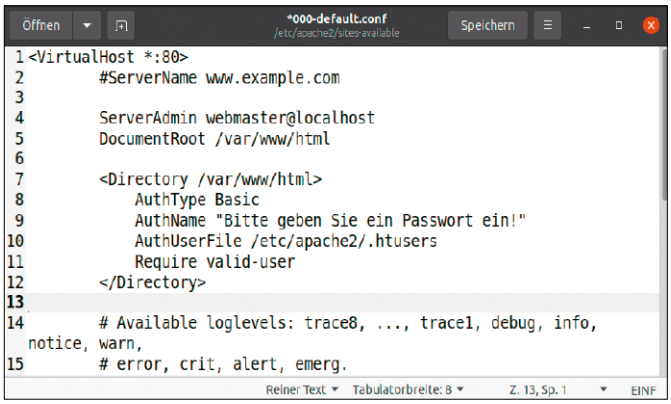
Serverdienste einrichten

Sie können auf Ihrem heimischen PC Webserver wie Apache oder Nginx installieren und somit beliebige Webanwendungen im Internet bereitstellen. Eine ausführliche Anleitung finden Sie unter *www.pcwelt.de/1607540*. Die Installation des Content-Management-Systems Wordpress haben wir unter *www.pcwelt.de/1607540* beschrieben. Für den Datenaustausch mit Kollegen und Bekannten eignet sich wahrscheinlich Nextcloud ab besten. Damit können Sie Fotos und Videos hochladen und gemeinsam an Dokumenten arbeiten. Nextcloud installieren Sie am schnellsten über ein Snap-Paket. Wie das geht, haben wir unter *www.pcwelt.de/2335413* beschrieben. Das funktioniert auch unter Linux Mint 20, wobei Sie dort Snap erst freischalten müssen:

```
sudo rm /etc/apt/preferences.d/
  nosnap.pref
sudo apt update
sudo apt install snapd
```

Für mehr Sicherheit betreiben Sie Nextcloud über eine verschlüsselte HTTPS-Verbindung. Das dafür nötige Zertifikat erhalten Sie kostenlos bei *https://letsencrypt.org*. Auf der Webseite finden Sie Anleitungen für die Installation des Zertifikats für alle Webserver und Betriebssysteme. In die Snap-Installation lässt sich das Zertifikat besonders einfach integrieren, was wir unter *www.pcwelt.de/2303648* beschrieben haben.

Nichts für fremde Augen: Eine Directoryregel in der Apache-Konfiguration sorgt dafür, dass Benutzer erst nach der Anmeldung Zugriff auf die Website erhalten.



Mehr Sicherheit für den Webserver

Wenn nur bestimmte Personen Zugriff auf die Webseiten erhalten sollten, lässt sich der Zugang mit einem Passwort schützen. Erzeugen Sie zuerst eine Datei für die Authentifizierung:

```
sudo htpasswd -c -B /etc/apache2/.
  htusers sepp
```

Sie werden aufgefordert, ein Passwort zu vergeben. Bauen Sie in einen Anweisungsblock in die Serverkonfiguration „/etc/apache2/sites-available/000-default.conf" ein:

```
<Directory /var/www/html>
AuthType Basic
AuthName "Bitte geben Sie ein
  Passwort ein!"
AuthUserFile /etc/apache2/.htusers
Require valid-user
</Directory>
```

Der Zugang wird jetzt nur nach Anmeldung mit dem Benutzernamen „sepp" und dem vergebenen Passwort gewährt. ■

GESCHEITERTE LOG-IN-VERSUCHE LIMITIEREN

Das Tool fail2ban überwacht Logdateien und sperrt IP-Adressen nach zu vielen ungültigen Anmeldeversuchen. Sie installieren das Tool mit

```
sudo apt install fail2ban
```

Kopieren Sie die Basis-Konfigurationsdatei, damit diese bei einem Update nicht überschrieben wird:

```
sudo cp /etc/fail2ban/jail.{conf,local}
```

Standardmäßig fühlt sich fail2ban nur für SSH-Anmeldungen zuständig, was sich in „/etc/fail2ban/jail.local" ändern lässt. Bauen Sie unter Abschnitte wie „[apache-auth]" (Apache-Anmeldung) oder „[apache-badbots]" (Spam-Roboter) jeweils die Zeile

```
enabled = true
```

ein. Danach starten Sie den Dienst mit

```
sudo systemctl restart fail2ban
```

neu. Welche Angriffe fail2ban bemerkt und welche IPs gesperrt werden, erfahren Sie in der Logdatei „/var/log/fail2ban.log".

Im Anmarsch: Fritz-OS 7.50

Die Fritzbox von AVM ist in Deutschland der Quasistandard bei Homeroutern. Das liegt nicht zuletzt am exzellenten Fritz-OS, das viel kann und das sich auch noch benutzerfreundlich präsentiert. In einigen Monaten soll Version 7.50 signifikante Neuerungen bringen.

VON HERMANN APFELBÖCK



Um es vorweg zu relativieren: Das anstehende Fritz-OS 7.50 wird wohl nur auf jüngerer Fritzbox-Hardware Einzug halten. Ein Upgradepfad für ältere Router ist unwahrscheinlich. Aktuell bietet AVM eine sogenannte „Labor"-Version 7.39 (*https://avm.de/fritz-labor/*), die den Umfang des künftigen Fritz-OS 7.50 im Betastadium abbildet. Experimentierfreudige Nutzer können die neue Firmware bereits jetzt aufspielen, bislang allerdings nur auf die aktuellen Topmodelle Fritzbox 7590 oder 7590 AX. In den folgenden Wochen werden weitere Modelle hinzukommen, aber voraussichtlich nur relativ aktuelle Geräte. Diese Geräteliste wird dann auch für endgültige Version 7.50 gelten. Insgesamt bringt Fritz-OS 7.50 erstaunlich viele Verbesserungen, das dominierende Highlight ist aber zweifellos die Umstellung bei VPN (Virtual Private Network) vom IPSec-Protokoll auf Wireguard.

VPN mit Wireguard-Protokoll

Fritzboxen können als VPN-Client und via Myfritz-Konto auch als VPN-Server arbeiten, sie ermöglichen also auch die verschlüsselte Fernnutzung des heimischen Internetzugangs. In den Rollen als VPN-Client und -Server mussten die AVM-Router in den letzten Jahren aber Kritik einstecken, weil der Durchsatz dabei nur befriedigend ausfiel.

Exkurs: Allerdings ist manchem Nutzer wohl auch nicht klar, dass der Download auf dem Clientgerät in der Ferne für den heimischen Router zunächst Download und dann Upload zum Ferngerät bedeutet und die Uploadbandbreite bei den meisten Verträgen eher schmal ausfällt. Dafür ist VPN nicht verantwortlich.

Fritz-OS 7.50 wird das bisherige genutzte IPSec-Protokoll durch Wireguard ersetzen. Da Wireguard direkt im Linux-Kernel integriert ist (somit auch in der Fritz-OS-Firmware), sollten höhere Geschwindigkeiten zu erreichen sein als mit IPSec. Auch sind die Kryptografiemethoden bei Wireguard gegenüber IPSec reduziert und damit effizienter. Erste Messungen mit der Laborversion belegen tatsächlich, dass dies den Durchsatz um mindestens 50 Prozent steigert. Optimistische Tester erwarten nach weiterem Feintuning bis zur finalen Version sogar noch weitere Steigerung.

Im Zuge der technischen Umstellung wird auch die Einrichtung von VPNs in der Konfigurationsoberfläche vereinfacht („Internet → Freigaben → VPN → VPN Verbindung hinzufügen"). Die Übernahme der komplizierten Anmeldedaten für Serveradresse und Kennwort wird durch neue Optionen vereinfacht. Für Smartphones als VPN-Client lässt sich ein QR-Code erzeugen, für PCs oder Notebooks eine Datei zum direkten Import. Das ist nicht nur bequemer, sondern vermeidet auch Lese- und Tippfehler.

Weitere Verbesserungen und neue Funktionen

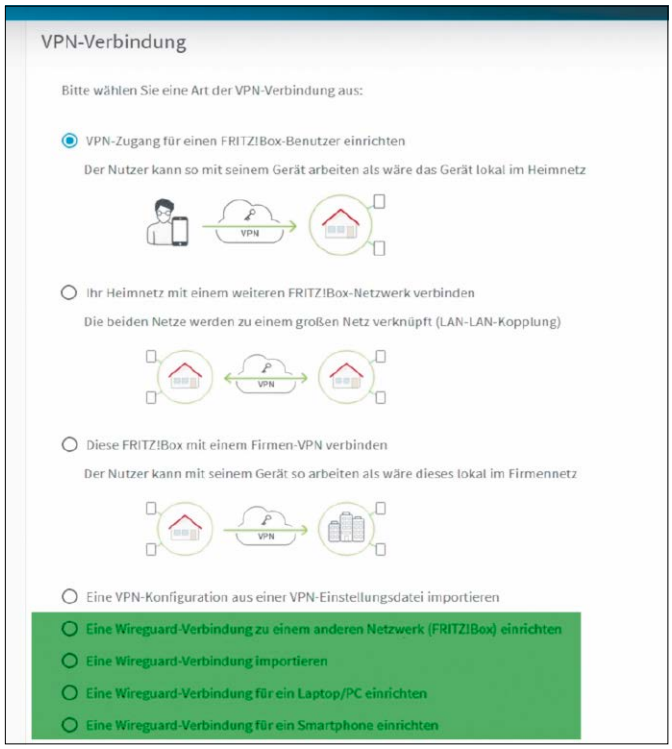
WLAN und Mesh-Repeater: Fritzboxen in der Rolle als sekundärer WLAN-Mesh-Repeater werden mit Fritz-OS 7.50 schneller. Mit der neuen Version stehen beide Bänder (2,4 und 5 GHz) für die optimale Verbindung zwischen der primären Fritzbox und dem Mesh-Repeater zur Verfügung. Bislang konnten Geräte im Betriebsmodus „Mesh Repeater" nur jeweils ein WLAN-Band nutzen (2,4 oder 5 GHz). Die neue Funktion steht bislang nur für die Fritzbox 7590 zur Verfügung.

Fritzfon-Telefone: Die Telefone von AVM (M2, C4, C5, C6) erhalten einen neuen Terminkalender und eine optionale Anruferansage: Statt eines Klingeltons sind in Zu-

sammenarbeit mit Fritz-OS 7.50 dann auch Sprachansagen wie „Chef ruft an“ möglich, was im Beispiel voraussetzen würde, dass ein Eintrag „Chef“ im Adressbuch angelegt ist. Diese neue Funktion nennt AVM „Sprachklingeln“. Nicht im Adressbuch gespeicherte Anrufer können zudem pauschal gesperrt oder auf einen Anrufbeantworter umgeleitet werden, wenn das Adressbuch als verbindliche „Positivliste“ definiert wird.

Fritz NAS: Die optionale NAS-Rolle der Fritzbox (also als Samba-Server) wird insofern noch unkomplizierter, als neben FAT und NTFS nun auch Datenträger mit exFAT angeschlossen werden können. Dies entspricht der Entwicklung beim Linux-Kernel und erweitert die Möglichkeiten um ein einfaches, rechteloses Format, das im Unterschied zu FAT auch große Film- und Imagedateien transportieren kann. Die Heimnetzfreigaben werden außerdem übersichtlicher, weil Fritz-OS 7.50 unter „Geräte und Heimnetzfreigabe“ künftig die berechtigten Konten und ihre Zugriffsrechte anzeigt.

Smarthome: Für das Smarthome wird das kommende Fritz-OS 7.50 neue Vorlagen zu Aktionen für den WLAN-Gastzugang, Anrufbeantworter und Pushmail geben. Außerdem unterstützt die Fritzbox Fenstersensoren für die Erkennung geöffneter Fenster und erweitert die Steuerung von Heizkörpersensoren.



Erweiterte VPN-Einrichtung unter Fritz-OS 7.50: Neben der technischen Umstellung auf Wireguard wird auch der Konfigurationsdialog erweitert.

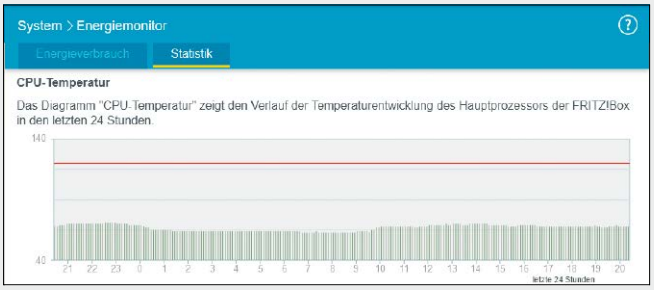
Konfigurationsoberfläche: Die Oberfläche des integrierten Webservers wird überarbeitet, um sich dynamisch an unterschiedliche Displaygrößen der Zugriffsgeräte anzupassen. Ziel ist es, auf großen PC-Monitoren wie auf kleinen Smartphone-Displays Übersicht und Lesbarkeit zu gewährleisten. Automatisches Ausblenden des Übersichtsmenüs auf kleinen Auflösungen beherrscht die Oberfläche allerdings schon länger. ■

FRITZ-OS UND DIE HARDWARE

Schön, dass Fritz-OS immer mehr Funktionen bietet. Die Hardware muss es aber aushalten, denn die Aufgabenlast ist je nach Einsatz beträchtlich: DSL- oder Kabelverbindungen mit bis zu 1000 MBit/s, LAN-Switch mit Vier-GBit-Ports, Wi-Fi-Funk Version 5 (ac) oder 6 (ax), DECT-Funk für Telefonie und Smarthome-Aktoren, Samba-Server für zwei USB-3.0-Geräte, UPnP-Medienserver, Streaming von Kabel-TV für vier Kanäle (Quad-Tuner), VPN als Server oder Client (und – wie im Haupttext zu lesen – demnächst mit Wireguard-Protokoll). Wer dies alles und dauerhaft dem kleinen SOHO-Router abverlangt, schafft sich nach unserer Erfahrung einen zusätzlichen Heizkörper, der früher oder später kapituliert.

Welche Kernhardware in der Fritzbox (und in vergleichbaren Heimroutern) die Arbeit erledigt, ist kein wirkliches Geheimnis, aber auch keine Information, die Routerhersteller gerne präsentieren: 512 MB RAM, neueste Modelle allenfalls ein GB RAM, dazu eine stromsparende Intel-Dualcore-CPU mit 1 bis 1,5 GHz, neueste Modelle eventuell Quadcore: Damit erreichen aktuelle Fritzboxen kaum die Leistung bescheidener Platinenrechner.

Unser Plädoyer: Das Angebot von Fritz-OS ist vorbildlich und Sie sollten nutzen, was Sie wirklich brauchen, aber – eingedenk der Hardware – ignorieren oder reduzieren, was Sie nicht brauchen. Als Medienserver scheint der Router generell unterdimensioniert („Heimnetz → Mediaserver“), der Einsatz als Samba-Server („Heimnetz → USB/Speicher“) ist realistischer, sofern keine anderen Netzgeräte diesen Job übernehmen. Wer die DECT-Leistung („Telefonie → DECT“) verringert, senkt nachhaltig und meist ohne Nachteile die Gerätetemperatur. Das Funknetz kann man nachts komplett abschalten („WLAN → Zeitschaltung“) und ungenutzte LAN-Ports auf den „Green Mode“ schalten („Heimnetz → Netzwerk → Netzwerkeinstellungen“).

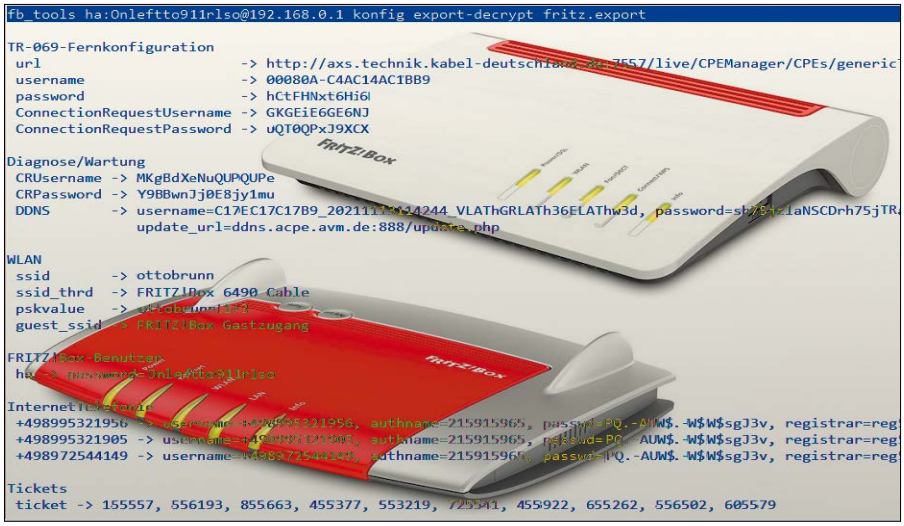


Wie geht's dem Router? Meist gibt schon Handauflegen deutliche Auskunft, die Aussagen der Fritzbox unter „System → Energiemonitor“ sind aber präziser – und hier recht entspannt.

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



Gut Informierte wissen wahrscheinlich, dass sich die Fritzbox-Konfiguration durch PHP-Scripts auslesen und in vielen Belangen sogar steuern lässt. Theoretisch genügen dafür relativ komplizierte Befehle der Download- und Uploadtools wget und curl. Komfortabler ist das Paket miniupnpc mit seinem Programm upnpc – dies allerdings mit eng begrenzter Reichweite. Das aktuell wohl umfangreichste PHP-Projekt zur Fritzbox-Steuerung ist die Sammlung fb_tools (Fritzbox-Tools) von Michael Engelke. Was man damit alles anstellen kann, zeigt dieser Beitrag.

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
```

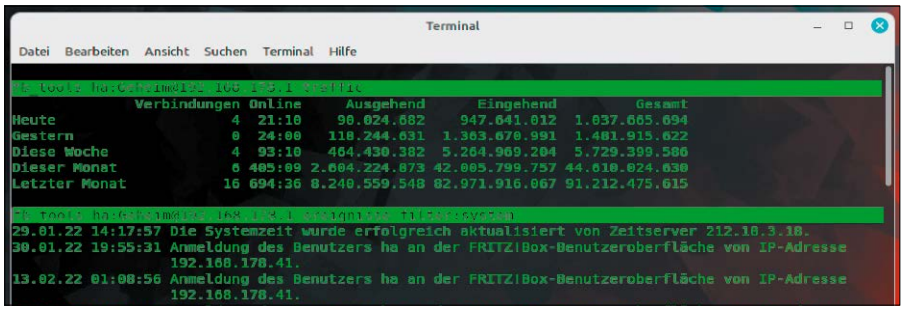
mit der Abfolge „[Konto:Kennwort@Gerät]“. Und noch ein akademisches Detail: Wer sich in mehreren Netzen befindet, muss den angesprochenen Router statt mit „fritz.box“ genau adressieren (was aber auch sonst nie schadet):

```
fb_tools sepp:Geh3im@192.168.178.1
 anrufliste
```

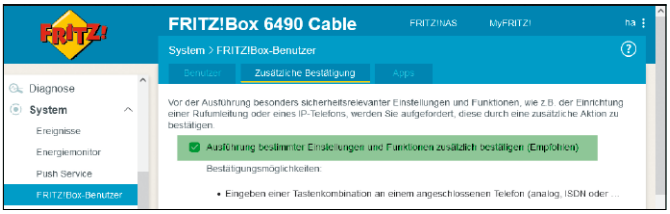
Mit dieser Syntax und somit korrekter Anmeldung sind aber auf jüngeren Fritzboxen immer noch nicht sämtliche Funktionen realisierbar. Die Lösung dafür liegt in der Fritzbox-Konfiguration unter „System → Fritz!Box-Benutzer → Zusätzliche Bestätigung → Ausführung bestimmter Einstellungen und Funktionen 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. ■

Alte Router weiterverwenden

Nicht mehr genutzte DSL-Router lassen sich oft auch anderweitig einsetzen. Teilweise bietet bereits die Standardsoftware interessante Funktionen, die man nur aktivieren muss. Noch mehr ist mit alternativer Firmware möglich.

VON THORSTEN EGGELING



Zu schade für den Elektroschrott: Alte DSL-Router können beispielsweise als WLAN-Access-Point arbeiten. Einige Modelle lassen sich auch mit alternativer Firmware weiternutzen.

Schnellere Internetanschlüsse erfordern meist neue DSL-Router. Das Altgerät liegt dann nutzlos herum oder landet auf dem Elektroschrott. In den Geräten steckt aber immer noch wertvolle Hardware, die sich auch weiterhin sinnvoll nutzen lässt. Das Betriebssystem der meisten Router und anderer Netzwerkgeräte basiert auf Linux. Es liegt daher nahe, das System durch eine verbesserte Version zu ersetzen. Das ist vor allem lohnenswert, wenn der Hersteller keine Updates mehr liefert und Sicherheitslücken zu befürchten sind. Eine neue Firmware kann außerdem zusätzliche Funktionen bieten. Ersatz-Firmware steht jedoch nicht für alle Router bereit. Es lohnt sich aber zu prüfen, ob für Altgeräte nicht ein verbessertes System verfügbar ist.

1. Fritzbox als WLAN-Access-Point einsetzen

Eine Fritzbox lässt sich als einfacher Ethernet-Switch konfigurieren, der per Kabel mit dem Hauptrouter verbunden wird. Das ermöglicht den Anschluss zusätzlicher Geräte per Ethernet-Kabel oder den WLAN-Zugang, der die Reichweite des Haupt-WLANs vergrößert. Wir beschreiben die erforderlichen Schritte am Beispiel einer betagten Fritzbox 3270 v3, die etwa ab 2009 verkauft wurde. Neuere Fritz-OS-Versionen unterstützen die gleichen Funktionen, die Beschriftung der Menüpunkte und Optionen kann jedoch abweichen.

Schritt 1: Schließen Sie die Fritzbox 3270 per Ethernet-Kabel an den PC an, andere Netzwerkverbindungen unterbrechen Sie vorübergehend. Rufen Sie die Oberfläche im Webbrowser über *http://fritz.box* oder *http://192.168.178.1* auf.

Schritt 2: Klicken Sie am unteren Rand des Fensters auf „Ansicht: Standard“, um auf die erweiterte Ansicht umzuschalten. Nur dann sehen Sie alle Optionen.

Schritt 3: Gehen Sie auf „Internet → Zugangsdaten“. Stellen Sie neben „Internetanbieter“ die Option „Weitere Internetanbieter“ ein und wählen Sie darunter „Anderer Internetanbieter“. Hinter „Name“ geben Sie eine aussagekräftige Bezeichnung ein, beispielsweise „AccessPoint“. Aktivieren Sie im Abschnitt „Anschluss“ die Option „Externes Modem oder Router“. Unter „Betriebsart“ stellen Sie „Vorhandene Internetverbindung mitbenutzen (IP-Client-Modus)“ ein. Klicken Sie auf „Verbindungseinstellungen ändern“ und aktivieren Sie die Option „IP-Adresse automatisch über DHCP beziehen“. Hinter „DHCP-Hostname“ tragen Sie eine aussagekräftige Bezeichnung ein. Alternativ können Sie die Option „IP-Adresse manuell festlegen“ aktivieren und eine feste IP-Adresse eintragen. Hinter „Standard-Gateway“ geben Sie die IP-Adresse des Hauptrouters ein. Nach einem Klick auf „Übernehmen“ startet die Fritzbox neu.

Schritt 4: Verbinden Sie den LAN-Port 1 der Fritzbox per Ethernet-Kabel mit Ihrem Netzwerk. Auch beim PC stellen Sie die Netzwerkverbindung wieder her. Für den Zugriff auf die Benutzeroberfläche der Fritzbox 3270 verwenden Sie die eingestellte oder per DHCP bezogene IP-Adresse.

Schritt 5: Gehen Sie im Menü auf „WLAN → Funknetz“. Konfigurieren Sie das Funknetz mit der gleichen SSID, die Sie auch in Ihrem Standard-WLAN verwenden. Unter „WLAN →

Sicherheit“ geben Sie den zugehörigen Netzwerkschlüssel ein. Ihre Geräte können sich dann automatisch mit dem jeweils stärksten WLAN verbinden, ohne dass der Nutzer etwas davon bemerkt.

2. Fritzbox als WLAN-Repeater konfigurieren

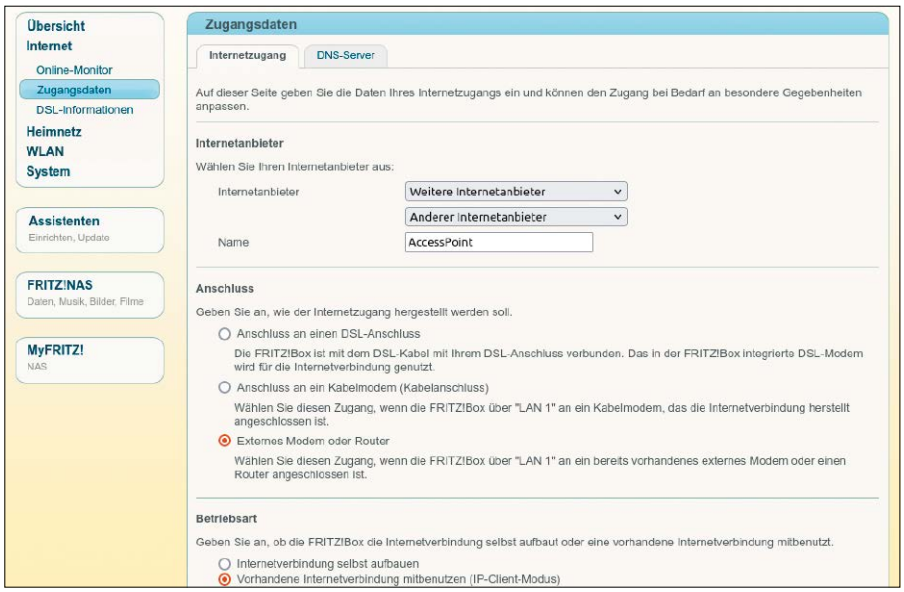
Die Reichweite des Funknetzwerks lässt sich auch ohne zusätzliche Kabel erweitern. Man stellt einen WLAN-Repeater an einem Ort auf, an dem das Signal noch gut genug ankommt. Der Repeater arbeitet dabei als Signalverstärker. Der Nachteil: Repeater können in der Regel Signale nicht gleichzeitig senden und empfangen, wodurch sich die effektive Bandbreite halbiert.

Neuere Fritz-OS-Versionen unterstützen ein Mesh-Netzwerk, was die Konfiguration vereinfacht. Eine Liste der unterstützten Fritzbox-Modelle stellt AVM unter *https://m6u.de/FMESH* bereit. Voraussetzung dafür ist in jedem Fall, das alle Geräte Fritz-OS 7 oder neuer verwenden. Eine Anleitung zur Einrichtung eines Repeaters ist über *https://m6u.de/MESHR* abrufbar. Für unser Beispiel verwenden wir zwei ältere Fritzboxen 7270, die unter Fritz-OS 06.06 laufen.

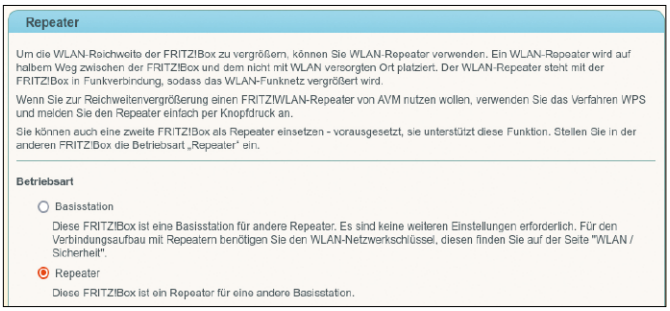
Schritt 1: Schließen Sie die Fritzbox, die als Repeater verwendet werden soll, per Ethernet-Kabel an den PC an. Trennen Sie die WLAN-Verbindung, wenn vorhanden. Rufen Sie die Benutzeroberfläche über die Standard-IP *http://192.168.178.1* oder *http://fritz.box* auf. Wählen Sie in der linken Spalte der Fritzbox-Oberfläche „Heimnetz → Heimnetzübersicht“, gehen Sie auf „Netzwerkeinstellungen“ und klicken Sie auf „IPv4-Adressen“. Hier tragen Sie eine neue Adresse ein, etwa „192.168.178.100“. Bestätigen Sie per Klick auf „OK“.

Schritt 2: Melden Sie sich über die neue IP-Adresse erneut an. Gehen Sie auf „WLAN → Funknetz“ und aktivieren Sie das Funknetz. Ebenfalls auf dieser Seite setzen Sie ein Häkchen vor die Optionen „Name des WLAN-Funknetzes sichtbar“ und „Alle neuen WLAN-Geräte zulassen“. Klicken Sie zum Speichern der Einstellungen auf „Übernehmen“.

Schritt 3: Verbinden Sie die zweite Fritzbox per LAN-Kabel direkt mit dem Rechner. Melden Sie sich über *http://192.168.178.1* oder *http://fritz.box* an. Wenn noch nicht geschehen, aktivieren Sie das WLAN unter „WLAN → Funknetz“ und vergeben unter „WLAN → Sicherheit“ einen Schlüssel. Gehen Sie auf „WLAN → Repeater“ und aktivieren Sie die Option „Basisstation“. Zum Speichern der Einstellungen klicken Sie auf „Übernehmen“. Es sind keine weiteren Einstellungen erforderlich. Lassen Sie die Fritzbox eingeschaltet.



Zweites Leben: Wenn eine Fritzbox nicht mehr als DSL-Router taugt, kann man sie als WLAN-Access-Point verwenden. Die Standardfirmware bietet die nötigen Optionen.



Mehr Reichweite fürs WLAN: Eine Fritzbox im Repeatermodus erweitert ein vorhandenes WLAN. Das Signal muss am Aufstellungsort aber noch stark genug sein.

Schritt 4: Verbinden Sie wieder die Repeater-Fritzbox per Kabel und melden Sie sich jetzt über die IP-Adresse „192.168.178.100“ an. Gehen Sie zu „WLAN → Repeater“. Unter „Betriebsart“ aktivieren Sie die Option „Repeater“. Setzen Sie ein Häkchen beim WLAN der anderen Fritzbox. Tragen Sie den WLAN-Netzwerkschlüssel ein und klicken Sie „Übernehmen“. Jetzt wird die WLAN-

MEHR SOFTWARE FÜR DIE FRITZBOX

Auch auf einigen Fritzbox-Modellen lässt sich Openwrt installieren, so beispielsweise auf der Fritzbox WLAN 3370 oder Fritzbox 4040 (siehe *https://openwrt.org/toh/start*). Die Installation der Firmware erfolgt hier jedoch nicht über die Weboberfläche, sondern per FTP. Der nötige FTP-Zugang ist aber nur ungefähr fünf Sekunden nach dem Einschalten des Gerätes verfügbar. Eine detaillierte Beschreibung finden Sie auf der jeweiligen Geräteseite.

Unter *https://github.com/Freetz-NG/freetz-ng* gibt es Software für Fritzboxen, mit der sich ein eigenes Firmwareimage erstellen lässt. Es verwendet Fritz-OS als Basis, weshalb sich das System aus rechtlichen Gründen nicht installationsfertig ausliefern lässt. Freetz-ng ermöglicht die Installation zusätzlicher Softwarepakete auch bei älteren Fritzboxen, die von Openwrt nicht unterstützt werden. Eine ausführliche Anleitung finden Sie unter *www.pcwelt.de/1955419*.

Verbindung zwischen den beiden Fritzboxen hergestellt. Danach erscheint die Meldung „Die Einrichtung wurde erfolgreich abgeschlossen“ und Sie können den Repeater etwa in einem anderen Stockwerk aufstellen – typischerweise auf der Hälfte der Strecke zwischen Basisstation und WLAN-Empfänger.

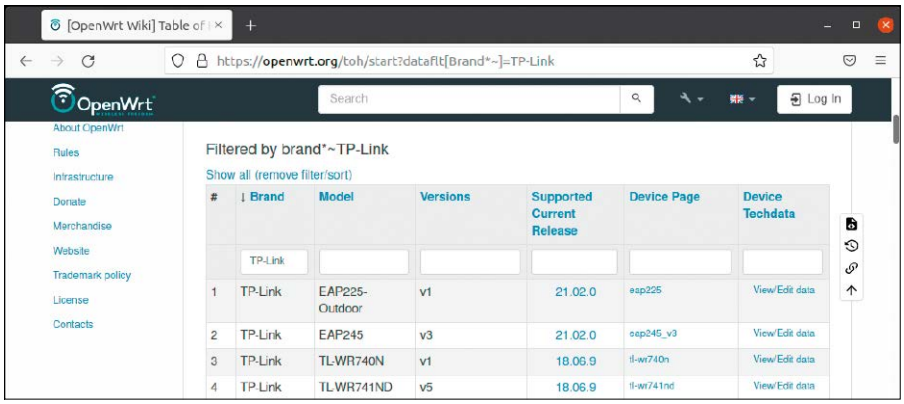
WLAN-Verbindungen: Da Fritzbox-Basisstation und -Repeater den gleichen Netzwerknamen, Funkkanal sowie die gleichen Sicherheitseinstellungen verwenden, brauchen Sie bei den bisher verwendeten WLAN-Clients keine Änderungen vorzunehmen. Sie verbinden sich automatisch mit der Fritzbox, die das stärkere Signal liefert.

3. Alternative Routerfirmware nutzen

Die Software eines Routers ist in einem nichtflüchtigen Speicherbaustein abgelegt (Flashspeicher). Der Inhalt lässt sich über die Bedienoberfläche im Browser ersetzen, was bei Firmwareupdates genutzt wird. Alternative Software muss aber genau zum Gerätemodell passen. Die Hersteller bestücken die Router oft mit unterschiedlicher Hardware, ändern die Modellbezeichnung aber nicht. Das Typenschild auf der Unterseite verrät meist Zusatzinformationen, etwa ein Anhängsel bei der Modellnummer oder Revisionsnummern wie „v2“ oder „v3“.

Openwrt (*https://openwrt.org*) ersetzt die Herstellerfirmware komplett und stattet den Router mit einem reduzierten, aber flexibel erweiterbaren Linux-System aus. Openwrt bietet in der Regel deutlich mehr Optionen als die Originalfirmware. Einige Hersteller bieten die Firmware für ihre Router ausdrücklich an, beispielsweise Cudy (*www.cudytech.com*).

Ob ein bestimmtes Routermodell unterstützt wird, erfahren Sie unter *https://openwrt.org/toh/start*. Die Tabelle lässt sich nach dem Namen des Herstellers filtern. In der Spalte „Versions“ sehen Sie die Revisionsnummern des jeweiligen Modells. Nach einem Klick auf „View/Edit data“ in der Spalte „Device Techdata“ erfahren Sie, welcher Chipsatz verwendet wird und wie viel Flashspeicher und RAM verfügbar sind. Für die aktuelle Openwrt-Version 21.02 sind mindestens 16 MB Flash und 128 MB RAM erforderlich. Ältere Router sind oft mit weniger ausgestattet. Dann ist eventuell die Installation einer älteren Version von Openwrt möglich.



Neue Firmware für zahlreiche Router: Openwrt bietet einen durchsuchbare Hardwaredatenbank. Hier erfahren Sie, ob Ihr konkretes Routermodell unterstützt wird.

Der Link in der Spalte „Device Page“ führt zu einer Seite mit ausführlichen Infos zum jeweiligen Gerät. Hier erfahren Sie, welche Hardwarerevisionen unterstützt werden und welche Probleme möglicherweise zu erwarten sind.

Es gibt außerdem Links zur Originalfirmware („Firmware OEM Stock“), die Sie für den Notfall immer bereithalten sollten. In einem Abschnitt wie „De-Bricking“ erfahren Sie, wie sich die Originalfirmware installieren lässt, wenn die Openwrt-Installation fehlschlägt.

Für die Erstinstallation laden Sie die Software über den Link aus der Spalte „Firmware OpenWrt Install“ herunter. Ist Openwrt bereits installiert, laden Sie ein Update über den Link in der Spalte „Firmware OpenWrt Upgrade“ herunter.

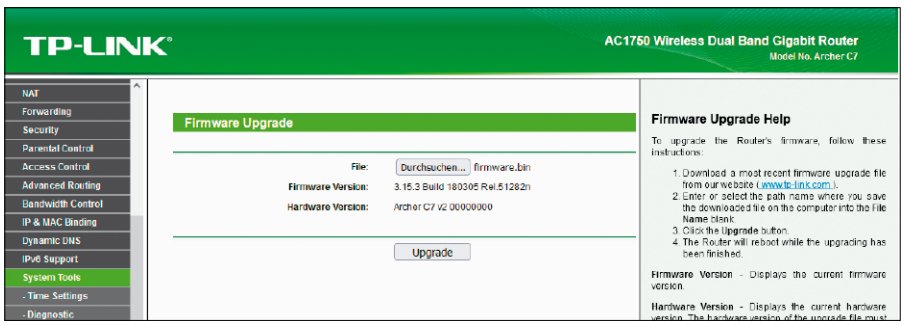
4. Openwrt-Firmware installieren

Als Beispiel verwenden wir den Altrouter TP-Link Archer C7 AC1750 v2. Der Download will uns zur Datei „openwrt-21.02.2-ath79-generic-tplink_archer-c7-v2-squashfs-factory.bin“ führen, die sich allerdings nur für die internationale Version des Routers eignet. Auf der Übersichtsseite *https://downloads.openwrt.org/releases/21.02.2/targets/ath79/generic/* wird die Datei „openwrt-21.02.2-ath79-generic-tplink_archer-c7-v2-squashfs-factory-eu.bin“ angeboten, die sich für ein in Deutschland gekauftes Gerät eignet. Benennen Sie die Datei in „factory.bin“ um. Vielen Routern bereiten zu lange Dateinamen beim Firmwareupgrade Probleme.

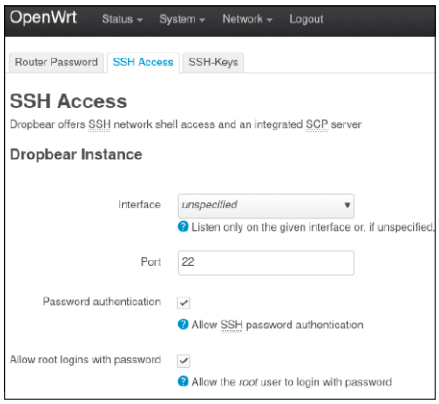
Schritt 1: Verbinden Sie den Router („LAN 1“) per Ethernet-Kabel direkt mit dem PC. Den WAN-Port verbinden Sie per Kabel mit Ihrem primären DSL-Router oder Kabelmodem.

Schritt 2: Die Oberfläche des Routers ist standardmäßig über *http://192.168.0.1* erreichbar und unter „System Tools → Firmware Upgrade“ lässt sich das System aktualisieren. Nach einem Klick auf „Browse“ wählen Sie die Datei „factory.bin“ aus und klicken auf „Upgrade“.

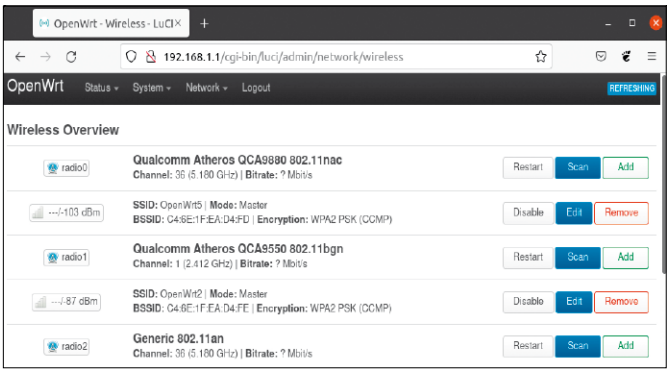
Schritt 3: Nach der Installation erreichen Sie die Routeroberfläche über *http://192.168.1.1*. Gehen Sie im Menü auf „System → Administration“. Vergeben Sie ein Passwort für den Benutzer „root“. Unter „SSH Access“ sollten Häkchen vor „Password authentication“ und „Allow the root



Einfaches Upgrade: Beim TP-Link-Router Archer C7 AC1750 lässt sich das Openwrt-Image komfortabel über die standardmäßige Upgradefunktion installieren.



Fernwartung: In Openwrt sollte man immer den SSH-Server aktivieren. Die Terminalfernwartung ist bei Installation und Update von Softwarepaketen nützlich.



WLAN erweitern: In Openwrt lassen sich zusätzliche USB-Adapter einbinden („radio2"), was beim Repeaterbetrieb die Übertragungsleistung verbessert.

user to login with password" gesetzt sein, damit Sie über SSH auf das Openwrt-System zugreifen können. Per Klick auf „Save & Apply" speichern Sie die Einstellungen.

Schritt 4: Um das Gerät als WLAN-Access-Point einzurichten, gehen Sie auf „Network → Wireless". Beim TP-Link Archer C7 AC1750 gibt es einen 5-GHz-Adapter („radio 0") und einen für 2,4 GHz („radio 1") und darunter jeweils eine Zeile für das zugehörige Netzwerk. Klicken Sie auf „Edit" und konfigurieren Sie das WLAN unter „Interface Configuration". Hinter „Network" wählen Sie „LAN" und auf der Registerkarte „Wireless Security" legen Sie den Netzwerkschlüssel fest. Klicken Sie auf „Save & Apply", um die Einstellungen zu speichern. Danach aktivieren Sie das WLAN per Klick auf „Enable".

Die Verbindung zum Hauptrouter erfolgt per Ethernet-Kabel in der Buchse „WAN". Die Schnittstelle ist bereits standardmäßig für DHCP konfiguriert.

5. Openwrt als WLAN-Repeater einrichten

Ein Openwrt-Router eignet sich besser als WLAN-Repeater als eine Fritzbox. Voraussetzung dafür sind allerdings USB-Buchsen und ein vom System unterstützter USB-WLAN-Adapter. Ansonsten sind nur die eingebauten WLAN-Chips nutzbar, was die Übertragungsrate reduziert. Openwrt kann außerdem – anders als die Fritzbox – das WLAN von Routern beliebiger Hersteller weiterleiten.

USB-Adapter einbinden: Wenn Sie einen zusätzlichen WLAN-Adapter verwenden wollen, stellen Sie unter Linux im Terminal eine SSH-Verbindung zum Router her:

```
ssh root@[Router-IP]
```

Aktualisieren Sie die Paketdatenbank und installieren Sie ein erforderliches Paket:

```
opkg update
opkg install usbutils
opkg install luci-proto-relay
```

Verbinden Sie den WLAN-Adapter. Mit

```
lsusb
```

fragen Sie die USB-ID des Adapters ab. Über eine Suche bei *https://deviwiki.com* finden Sie dann heraus, welches Kernel-Modul für das Gerät zuständig ist. Bei *https://openwrt.org/packages/table/start* kann man nach dem zugehörigen Openwrt-Paket suchen (Spalte „Name") und die Installation erfolgt dann im Terminal:

```
opkg install [Modulname]
```

Starten Sie den Router neu. Unter „Network → Wireless" ist jetzt das neue Gerät „radio2" zu sehen. Danach konfigurieren Sie den Router als Repeater:

Schritt 1: Schließen Sie den Openwrt-Router per Ethernet-Kabel direkt an den PC an und rufen Sie die Oberfläche über *http://192.168.1.1* auf.

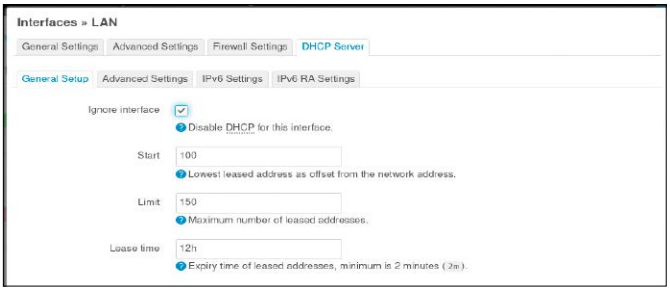
Schritt 2: Gehen Sie auf „Network → Interfaces" und klicken Sie hinter „LAN" auf „Edit". In unserem Beispiel gehen wir davon aus, dass das Netzwerk des WLAN-Access-Points 192.168.0.0/24 verwenden soll. Wenn das WLAN-Netzwerk bisher mit 192.168.1.0/24 konfiguriert ist, ändern Sie die IP-Adresse des Openwrt-Routers beispielsweise auf 192.168.2.1 und melden sich danach erneut an. Bearbeiten Sie die LAN-Verbindung erneut und setzen Sie unter „DHCP Server" ein Häkchen hinter „Ignore interface". Klicken Sie auf „Save & Apply".

Schritt 3: Gehen Sie auf „Network → Wireless". Klicken Sie bei einem der Netzwerkadapter auf die Schaltfläche „Scan" und dann beim gewünschten Netzwerk auf „Join Network". Tippen Sie hinter „WPA passphrase" den Netzwerkschlüssel des WLAN-Access-Points ein, klicken Sie auf „Submit" und danach auf „Save & Apply".

Schritt 4: Rufen Sie „Network → Interfaces" auf und klicken Sie auf „Add new interface". Als Bezeichnung tippen Sie beispielsweise „repeater_bridge" ein. Hinter „Protocol of the new interface" wählen Sie „Relay bridge" und klicken auf „Submit". Vergeben Sie hinter „Local IPv4 address" eine freie IP-Nummer aus dem Bereich des WLAN-Access-Points, beispielsweise 192.168.0.30. Hinter „Relay between networks" wählen Sie „lan" und „wwan" und speichern die Änderungen. Starten Sie den Router über „System → Reboot" neu.

Schritt 4: Gehen Sie auf „Network → Firewall" und klicken Sie unter „Zones" in der Spalte „lan" auf „Edit". Hinter „Covered networks" fügen Sie das Netzwerk „wwan" hinzu und klicken auf „Save & Apply".

Konfigurieren und aktivieren Sie unter „Network → Wireless" die gewünschten WLAN-Netze, wie in Punkt 4, Schritt 4 beschrieben. Dabei ist nichts Besonders zu beachten. ■



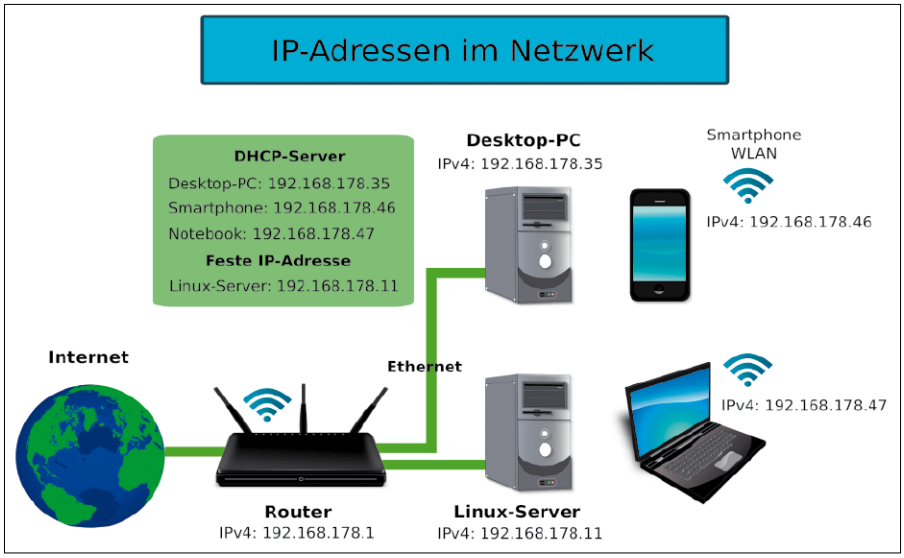
Repeaterkonfiguration: Der DHCP-Server muss deaktiviert werden. Da sich alle Geräte im gleichen Netzwerk befinden, erfolgt die Adressvergabe weiter über den primären Router.

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

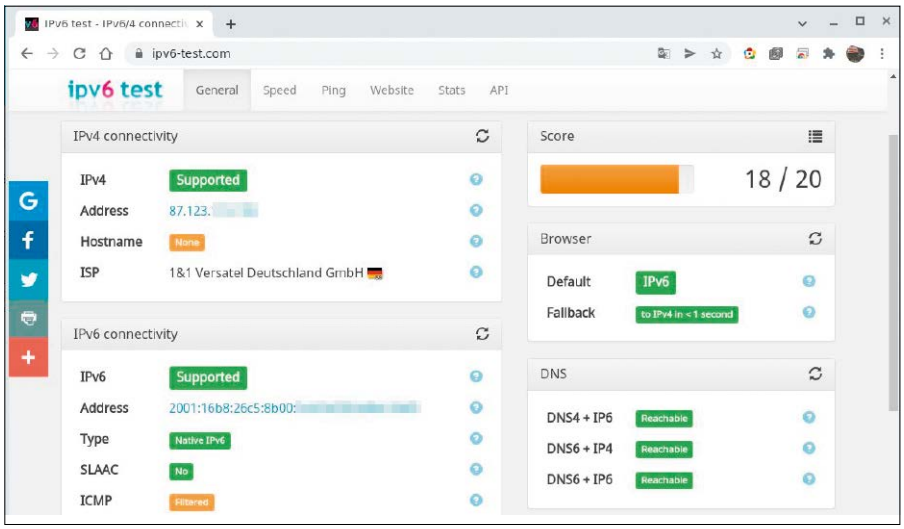
Diese Adressen sind komplizierter aufgebaut, dafür sind davon genügend für (zur Zeit) jedes einzelne Gerät auf der Welt vorhanden (340 Sextillionen, 2 hoch 128). Die

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
```

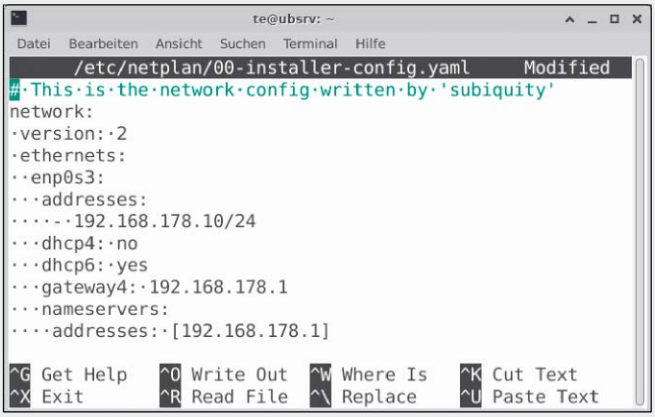
an und prüfen Sie die korrekte Funktion. Nach 90 Sekunden werden die vorherigen Einstellungen wiederhergestellt. Über

```
sudo netplan apply
```

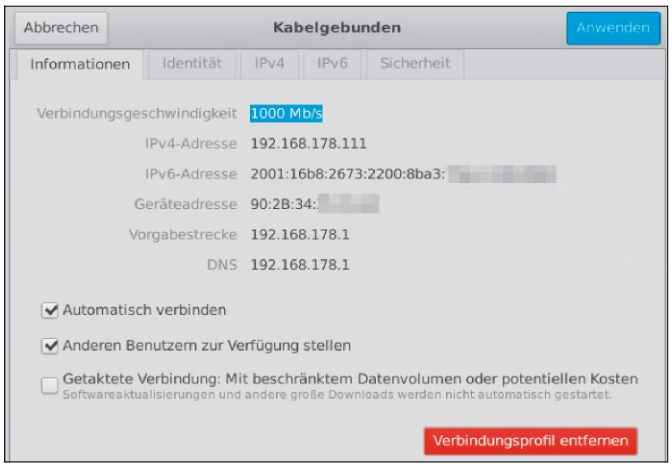
lässt sich die Konfiguration dauerhaft anwenden. Ubuntu Server verwendet keine Privacy Extensions, die IPv6-Adresse bleibt somit gleich. Wer eine zufällige Interface-ID benötigt, ergänzt die Zeile

```
ipv6-privacy: true
```

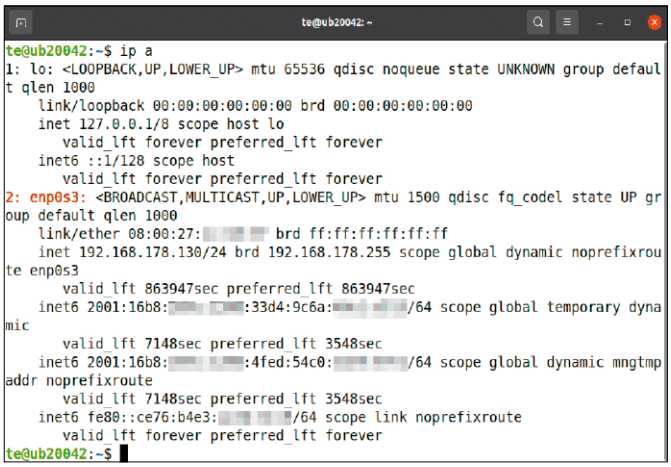
direkt unter „dhcp6: yes“.



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

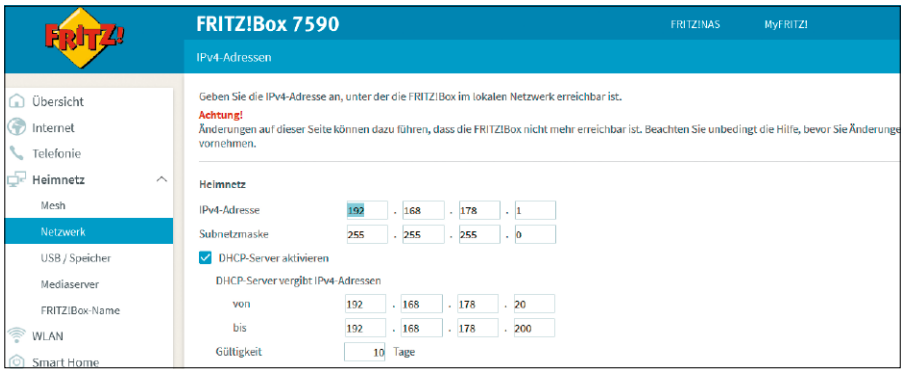
```
nmblookup [Rechnername]
```

nutzen, um sich die IP-Adresse ausgeben zu lassen.

6. Feste IPv4-Adresse einstellen

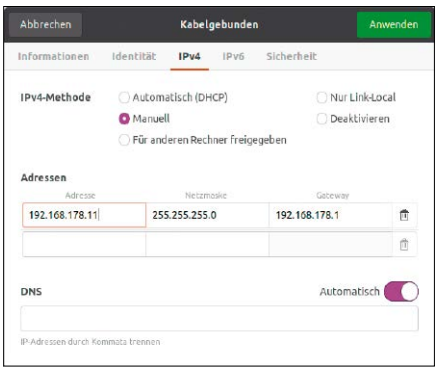
Einige Serverdienste lassen sich nur mit einer IP-Adresse und nicht mit dem Namen des Rechners konfigurieren. Ein Linux-Server sollte daher zuverlässig immer die gleiche IPv4 erhalten, was den Zugriff unabhängig von der Namensauflösung und auch über das Internet gewährleistet, wenn im Router Portfreigaben 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

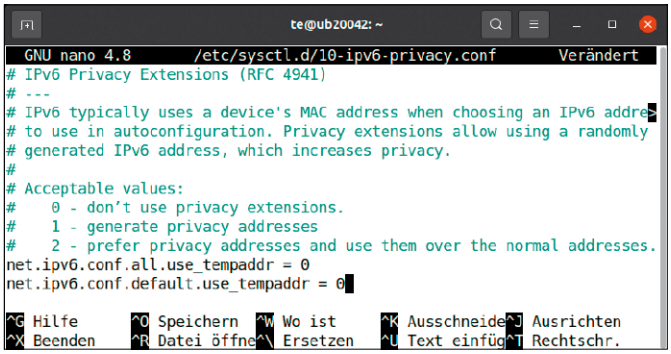
Eine feste IPv6-Adresse ist nur erforderlich, wenn ein Serverdienst auch oder nur über dieses Protokoll von außen aus dem Internet erreichbar sein soll. Öffnen Sie die Konfigurationsdatei im Terminal:

```
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. ■

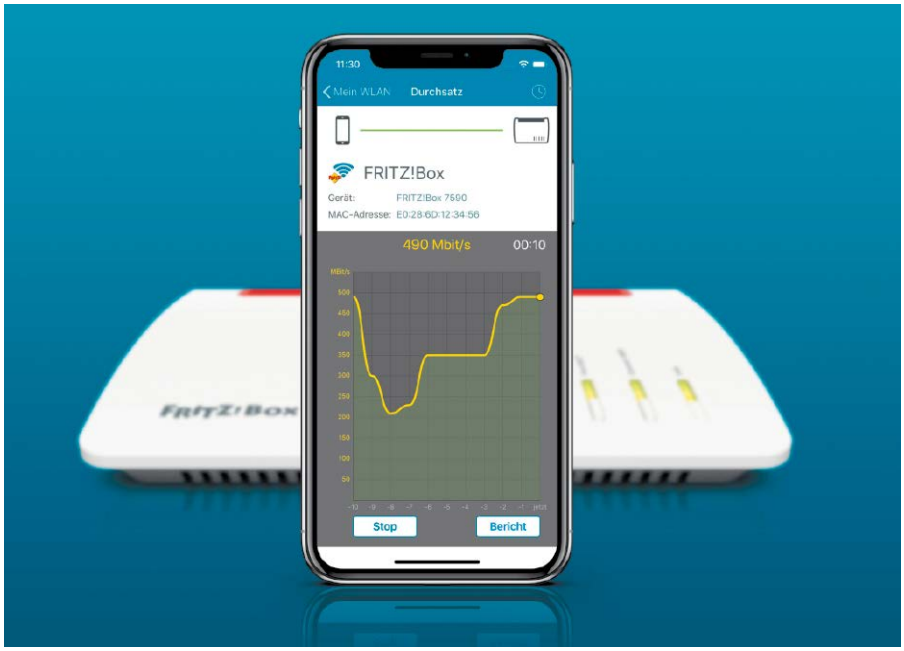


Unveränderliche Adresse: Wenn man die Privacy Extensions in der Datei „10-ipv6-privacy.conf“ abschaltet, bleibt die IPv6 gleich. Im Internet ist der PC dann allerdings identifizierbar.

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.

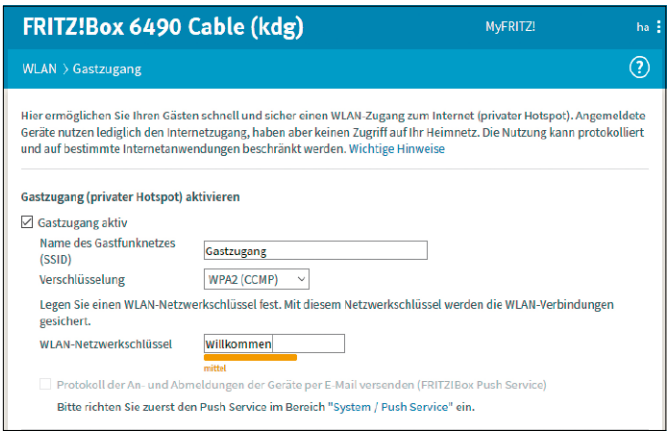
Optionale MAC-Filterung: WLAN-Router sind im Normalfall so eingestellt, dass sich jedes Gerät am Funknetz anmelden darf, sofern der Benutzer das WLAN-Kennwort richtig eingibt. Das ist bequem, aber nicht sicher. In der Fritzbox finden Sie die Einstellung unter „WLAN → Sicherheit" ganz unten in der Option „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.



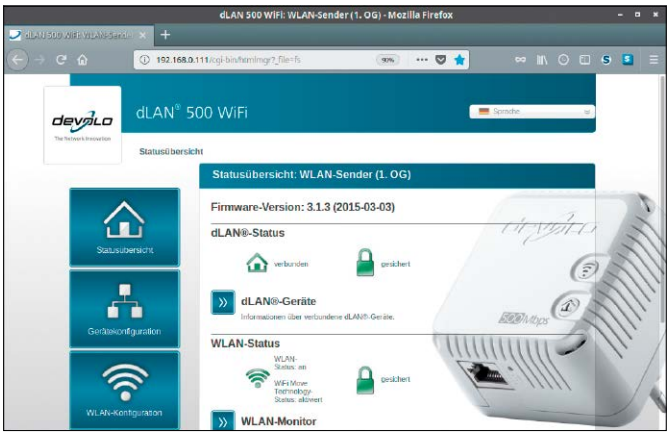
Vorkonfigurierter Gastzugang für Besucher: Sie müssen das primäre WLAN-Kennwort nicht preisgeben und halten Besucher vom lokalen Netzwerk fern (Client Isolation).

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. ■

Linux-Server fürs Heimnetz

Braucht ein privates Heimnetz, ein kleines Homeoffice tatsächlich Serverlösungen? Sagen wir es so: Wer nur einen PC benutzt, kommt auch mit einer USB-Festplatte zur Datensicherung aus. Aber gelebter Alltag ist das längst nicht mehr.

VON HERMANN APFELBÖCK

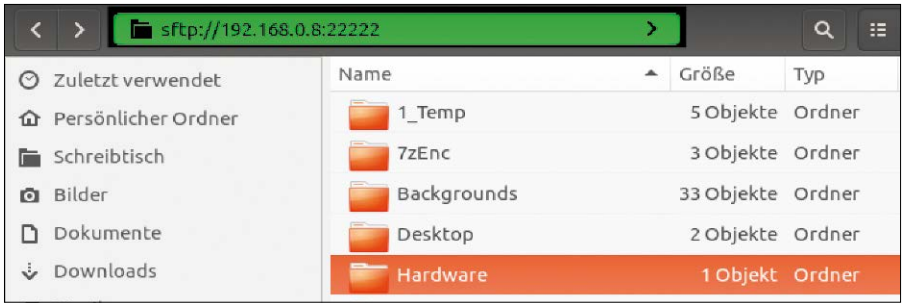
Sobald mehrere Geräte regelmäßig die gleichen Daten nutzen, austauschen und bearbeiten, wird das Hantieren mit USB-Medien unzumutbar und führt obendrein zu Chaos (was ist wo aktuell?). Das Delegieren an die Cloud ist Datenstriptease, außerdem langsam und quantitativ eingeschränkt. Kein Zweifel: Linux-Serverlösungen machen das Heimnetz attraktiver und bequemer. Welche der zahlreichen Serveranwendungen sich für Ihre Zwecke eignet, kann dieser kurze Beitrag nicht beantworten und erst recht keine Anleitung zur Einrichtung leisten. Was wir hier vorhaben, ist eine knappe Kategorisierung der wichtigsten Serverdienste.

Hinweis zur Hardware: Ein Homeserver ist keine Investition. Alle nachfolgend genannten Serverlösungen kann jeder aktuelle Desktoprechner nebenbei anbieten, sofern er dauerhaft läuft. Auch Heimrouter wie die Fritzbox bieten Dienste als Daten- und Medienserver quasi nebenher, sind damit aber tendenziell überfordert. Ideal sind preisgünstige Platinenrechner (Raspberry Pi 4, Odroid N2+) oder ausgemusterte Notebooks.

SSH/VNC: Administrative Serverdienste

SSH-Server: Praktisch jeder Linux-Server verdient neben seinen eigentlichen Diensten den zusätzlichen SSH-Server. Hauptaufgabe von SSH ist die Fernadministration eines Serversystems im Terminal. Zur Einrichtung und Aktivierung genügt der Befehl

```
sudo apt install openssh-server
```



Nur Linux zu Linux? Dann genügt als Austauschprotokoll SFTP und somit der zugrunde liegende Open-SSH-Server.

und ein zugreifender Rechner ist dann mit (Beispiel)

```
ssh sepp@192.168.178.20
```

schnörkellos im Terminal des Servers, sofern ein Systemkonto (hier „sepp“) und dessen Passwort bekannt sind.

SSH kann auch als Datenserver genügen (unter Verzicht auf Samba), solange Windows nicht mitspielt. Der Datenzugriff in Linux-Dateimanagern erfolgt mit „sftp://sepp@192.168.178.20“ Samba-like und sogar performanter (SFTP ist das Dateiprotokoll von SSH).

VNC-Server: Optional, aber „nive to have“ ist der Fernzugriff auf den grafischen Serverdesktop via VNC-Protokoll (Virtual Network Computing). Als Software auf dem Linux-Server eignet sich zum Beispiel x11vnc, als Zugriffsclient das Programm Remmina unter Linux, unter Windows etwa Tight VNC (*www.tightvnc.com*). Die Einrichtung als ständig laufender Service ist nicht ganz so einfach wie bei Open SSH.

Samba: Der Datenserver

Samba-Netzwerkfreigaben sind die gebräuchlichste Methode für Datenzentralen im gemischten Netzwerk. Auch kommerzielle NAS-Geräte oder Router verwenden Samba-Freigaben, selbst wenn sie das – wie etwa die Fritzbox – nicht explizit beim Namen nennen. Linux, Windows, Mac-OS können standardmäßig auf Samba-Freigaben zugreifen und für Android und iOS gibt es einschlägige Apps (File Explorer, Total Commander und andere).

Am Linux-Serversystem muss die Samba-Serverkomponente installiert werden:

```
sudo apt install samba
```

Die Einrichtung des Samba-Servers kann sehr einfach oder komplex ausfallen, je nach Benutzermenge und Freigabeort. Allereinfachste Varianten sind die Freigabe

- aller Home-Verzeichnisse („[homes]“ in der Konfigurationsdatei „/etc/samba/smb.conf“)
- eines Datenordners für ein einziges (Pseudo-)Konto, das dann alle zugreifenden Rechner verwenden.

Im zweiten Fall müsste nur folgender Beispieleintrag ans Ende der „/etc/samba/smb.conf“ gesetzt werden:

```
[Archiv]
path = /srv/Archiv
valid users = darfsamba
write list = darfsamba
```

Genannte Konten müssen doppelt existieren – als Systemkonto („adduser darfsamba“) und als Sambakonto („smbpasswd -a darfsamba“). Wer sich die manuelle Einrichtung des Samba-Servers gar nicht zutraut, kann auch ein Serversystem wie Easynas oder Open Media Vault installieren (*www.openmediavault.org*), schränkt damit aber die Rechnerhardware auf diese Rolle ein.

UPnP/DLNA: Der Medienserver

UPnP/DLNA-Server haben gegenüber dem trockenen Dateizugriff via Samba (oder auch SSH/SFTP) mehrere Vorteile: Erstens bringen sie Video- und Audiomedien auch an Geräte wie Smart-TVs, die mit Samba- oder SSH-Datenfreigaben nichts anfangen können. Zweitens ist die Präsentation der Medien nach Auswertung der Titel und Mediantags ungleich attraktiver. An schlanken bis wuchtigen Alternativen solcher Streamingzentralen besteht kein Mangel (Readymedia, Gerbera, Kodi, Plex und andere).
Trotz allem Schick etwa bei Kodi und Plex erweisen sich logisch sortierte Verzeichnislisten via Samba & Co. in der Praxis oft als überlegen: Qualitativ spielt es keine Rolle, ob ein Film über Samba oder UPnP/DLNA abgespielt wird. Der Samba-Dateizugriff ist einfacher, schneller, sparsamer und zuverlässiger, weil die Auswertung der Mediantags immer Fehler und Lücken hinterlässt. Ferner beherrschen gerade jene Geräte, die auf UPnP/DLNA angewiesen sind, nur einen Teil der Medienformate, die heterogene Sammlungen enthalten. Wer beliebige Inhalte auf einem Smart-TV wiedergeben will, fährt oft besser mit einem per HDMI angeschlossenen PC oder Platinenrechner.

Apache & Co: Der Webserver

Ein großes Thema für einen kleinen Artikel: Schon bei der Wahl des Webservers selbst gibt es mit Apache, Nginx, Lighttpd, Node.js eine Entscheidungsaufgabe, die wir hier abkürzen: Apache hat die größte Verbreitung, unterstützt im Unterschied zu manchem Konkurrenten alle Anwendungen und ist gut dokumentiert. Dass andere Webserver als schlanker und schneller gelten, spielt für eine heimische Intranetlösung keine Rolle, selbst wenn sie nur auf einem Raspberry läuft.
Anwendungen für Webserver gibt es in jeder Skalierung. Allgemein und verbindlich ist nur, dass das jeweilige Inhaltsangebot über die IP-Adresse (und eventuelle Portangabe) des Servergeräts im gesamten Heimnetz über jeden Browser abrufbar ist. Der folgende kleine Überblick zu den zahlreichen Webserver-Diensten nennt nur einige beliebte Anwendungen:
Foto: Coppermine, Piwigo, Lychee
Kalender: Baikal, Webcalendar
Wiki/Dokumentenzentrale: Dokuwiki, Mediawiki, Wordpress
Audio: Ampache, Funkwhale, Volumio
„Most-in-One“: Nextcloud
Jeder dieser Web- oder Intranetdienste hat auf der Projektseite seine Installationsanleitung, die auch die Anbindung an Apache (Nginx & Co.) erklärt. Einzige Ausnahme ist hier Volumio als geschlossenes System, das alles bereits mitbringt. In der Regel fordert jede Webanwendung zur Installation den Webserver (Apache), die Script-Sprache PHP und meistens eine Datenbank (My SQL). Da die Einrichtung Schritt für Schritt mit kopierbaren Terminalbefehlen erklärt wird, ist der Vorgang keine ganz große Hürde. Da Neulinge aber oft nur nachvollziehen, ohne den Hintergrund zu verstehen, sind Fehler nicht selten. Für Einsteiger lohnt sich daher in jedem Fall die Suche nach Komplettlösungen. Für prominente Kandidaten wie Mediawiki oder Nextcloud gibt es Containerformate, die alles inklusive Konfiguration beinhalten.
Damit wird etwa die sehr komplexe Webserver-Anwendung Nextcloud (Datenzentrale, Terminkalender, Fotogalerie, Adressverwaltung und mehr) äußerst einfach zugänglich: Nextcloud ist unter Ubuntu-Systemen mit einem Befehl

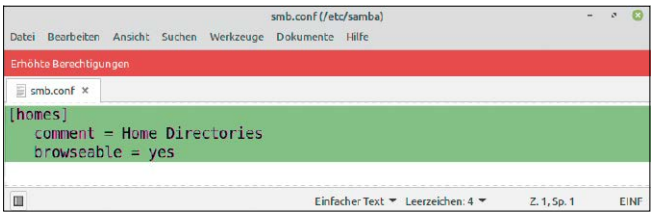
```
sudo snap install nextcloud
```

komplett installiert und sofort unter „http://[Server-IP]“ mit jedem Browser im Netz erreichbar. Mit

```
sudo nextcloud.enable-https self-signed
```

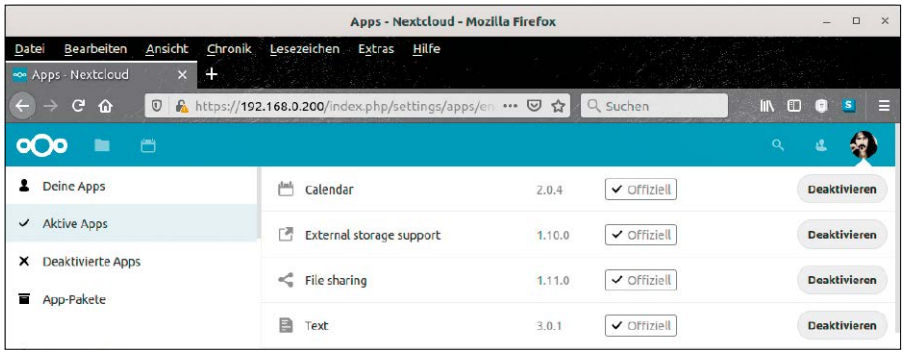
beheben Sie noch den Schönheitsfehler, dass Browser heute auch im lokalen Netz verschlüsseltes HTTPS erwarten. ■

Pauschalfreigabe aller „Homes“: Das ist eine sehr einfache Lösung, um mehreren Benutzern auf einem Samba-Server eine persönliche Ablage und eine Backupoption zu schaffen.





Medienzentralen wie hier Kodi sind neben trockenem Samba oder SSH ungleich attraktiver, konnten aber als Server via UPnP/DLNA nie so recht überzeugen.

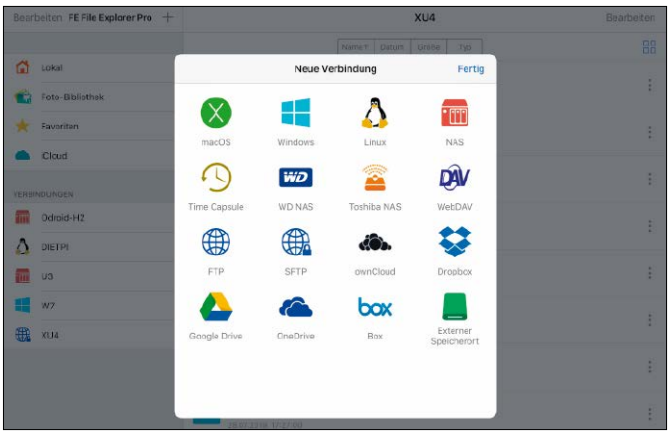


Nextcloud: Die an sich komplexe Webanwendung ist leicht installiert (als Snap) und vorbildlich modular. Schalten Sie einfach ab, was Sie nicht brauchen.

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.

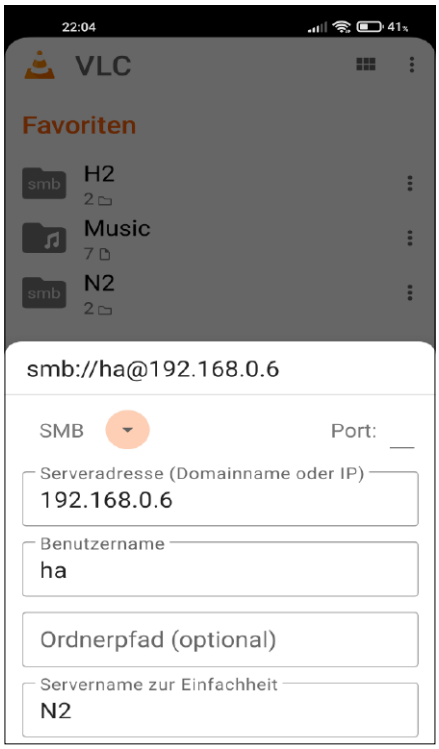
Mit der „+"-Schaltfläche rechts unten ist eine neue Verbindung schnell eingerichtet und dauerhaft gespeichert. Für lokale Netzressourcen ist nach Auswahl des Servertyps, also etwa „Windows", „Linux" oder „SFTP", die lokale IP-Adresse die wichtigste Angabe, das optionale Speichern von „User" und „Password" 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.

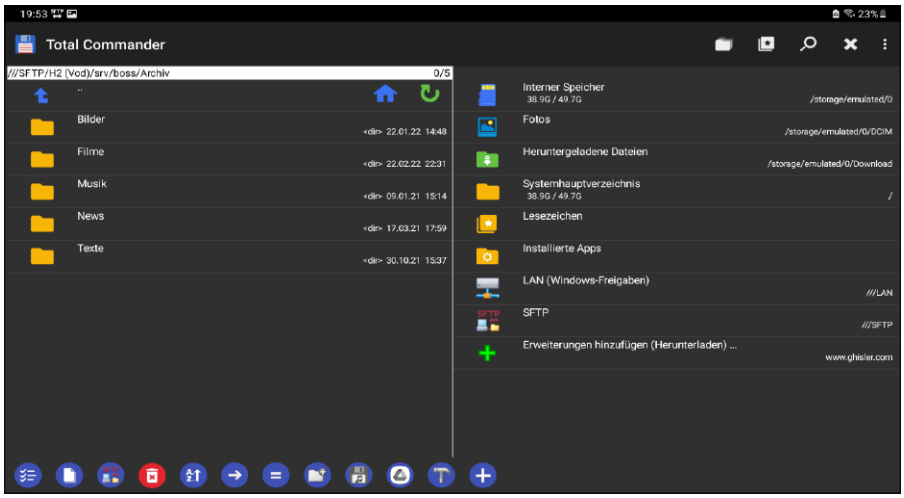


Allzweckwaffe für Medienwiedergabe: Geht es ausschließlich um Film- und Musikwiedergabe vom Heimserver, dann genügt der VLC-Mediaplayer.

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.



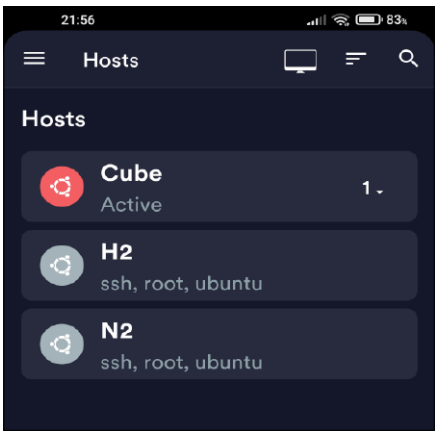
Total Commander mit LAN- und SFTP-Plug-in: Als Dateimanager ist die Android-App unschlagbar. Die Medienwiedergabe delegiert er an VLC & Co., wobei er Audio auch selbst übernehmen kann.

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.

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 172). 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

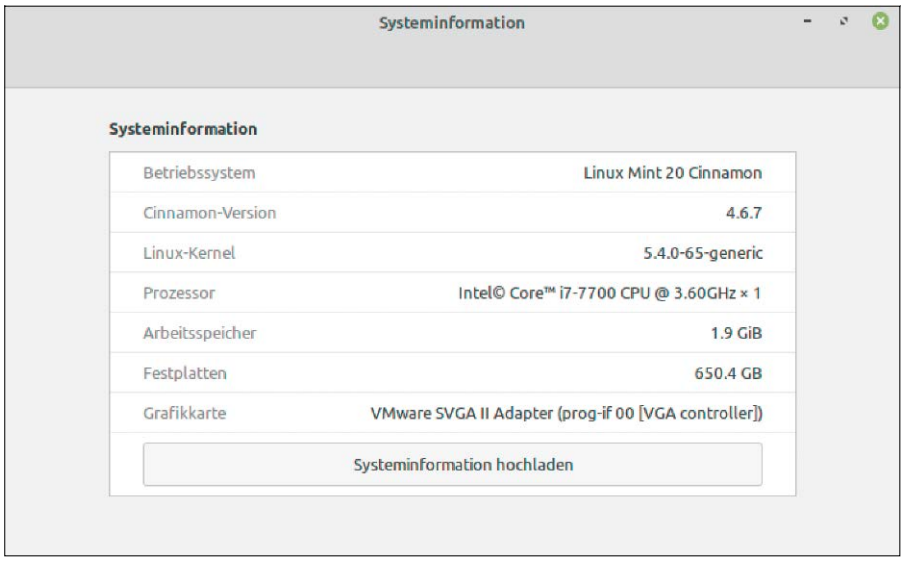
Ein Computer besteht aus zahlreichen Hardwarekomponenten und für alle ist ein eigener Treiber erforderlich. Unter Linux sind Treiber, die hier als Kernel-Module bezeichnet werden, im Betriebssystemkern (Kernel) enthalten oder werden von diesem bei Bedarf geladen. Neue Kernel erscheinen alle zwei bis 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 erst kurz 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 und so weiter). 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.

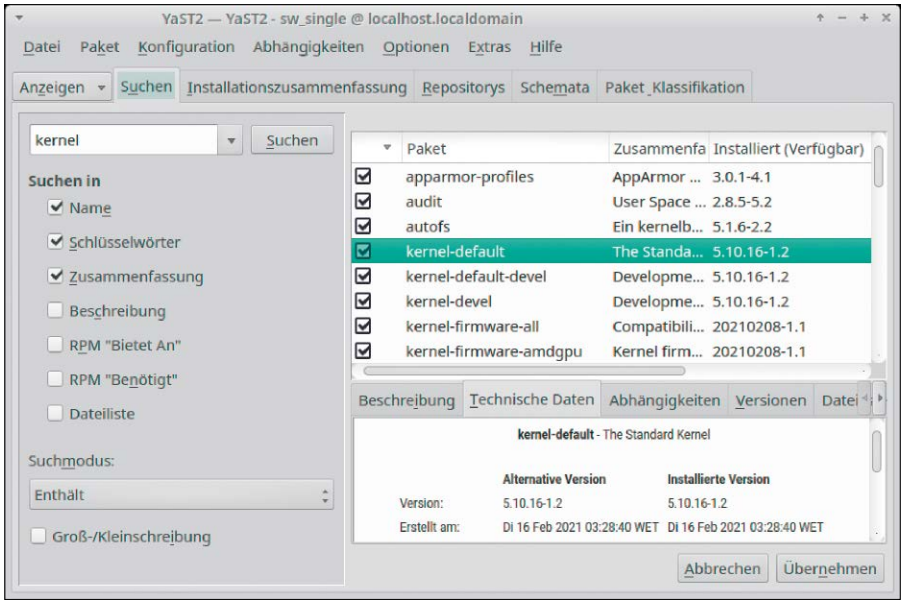
Ein Spezialfall liegt vor, wenn das Installationssystem den Netzwerkadapter nicht erkennt. Dann ist auch kein Update auf einen neueren Kernel möglich, der die Hardware unterstützt.

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 172). 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.

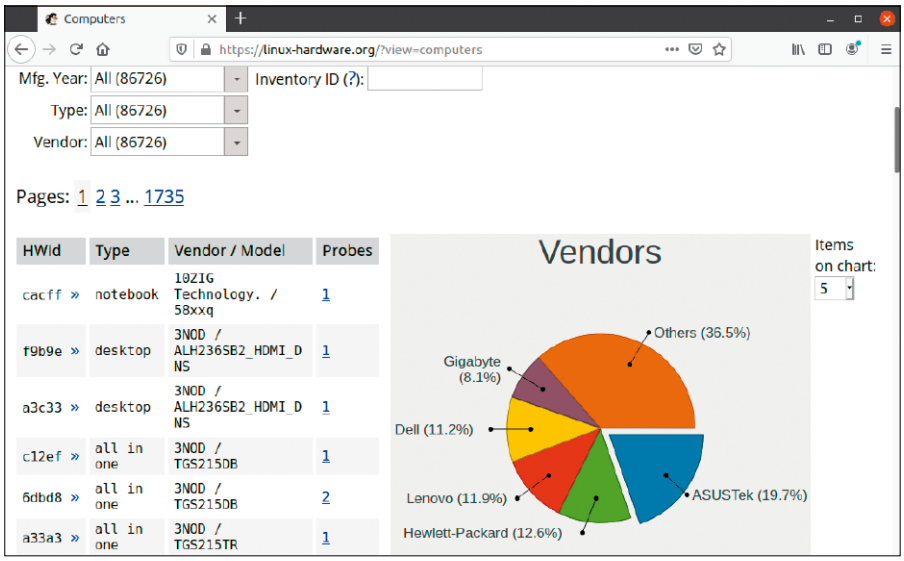
3. Geeignete Hardware für Linux finden

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

```
te@ub1804: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
01:00.1 Audio device [0403]: NVIDIA Corporation GP106 High Def
inition Audio Controller [10de:10f1] (rev a1)
        Subsystem: ZOTAC International (MCO) Ltd. GP106 High D
efinition Audio Controller [19da:1438]
        Kernel driver in use: snd_hda_intel
        Kernel modules: snd_hda_intel
02:00.0 Ethernet controller [0200]: Realtek Semiconductor Co.,
 Ltd. RTL8111/8168/8411 PCI Express Gigabit Ethernet Controlle
r [10ec:8168] (rev 15)
        Subsystem: Micro-Star International Co., Ltd. [MSI] RT
L8111/8168/8411 PCI Express Gigabit Ethernet Controller [1462:
7a70]
        Kernel driver in use: r8169
        Kernel modules: r8169
te@ub1804:~$
```

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 172).

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:

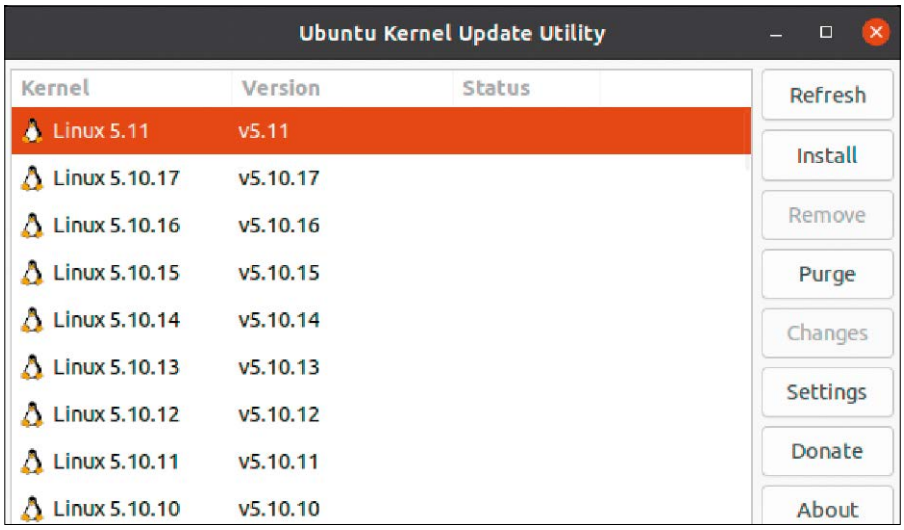
```
sudo apt-get install --install-
  recommends linux-generic-
  hwe-20.04 xserver-xorg-hwe-20.04
```

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 168) 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.

Festplatten und SSDs

Linux unterstützt von Haus aus Festplatten und SSDs an allen gängigen Anschlüssen. Brandaktuelle Hardware läuft ebenfalls auf Anhieb, allerdings sind noch nicht alle Diagnosewerkzeuge auf dem neuesten Stand.

VON THORSTEN EGGELING



Der Standard bei den meisten PCs und Notebooks ist eine Festplatte oder SSD am SATA-Anschluss. Aktuelle Geräte bieten neben SATA auch einen M.2-Steckplatz für die SSD. Reicht der Speicherplatz im Gerät nicht aus, kommen externe Laufwerke zum Einsatz (siehe ab Seite 166). Linux kommt generell gut mit allen Laufwerkstypen zurecht. Für optimale Leistung und Funktion sollte man jedoch einiges beachten und Einstellungen bei Bedarf anpassen. Weitere Tipps und Tricks zu SSDs und HDDs finden Sie außerdem ab Seite 180.

SATA-Einstellungen prüfen

Die Firmware aktueller PCs und Notebooks bietet in der Regel nur zwei Modi für die SATA-Ports: AHCI und Raid. Raid (Redundant Array of Independent Disks) aktiviert man nur, wenn mehrere Festplatten in einem Verbund zusammengeführt werden sollen. AHCI (Advanced Host Controller Interface) ist für die optimale Geschwindigkeit von Laufwerken erforderlich und standardmäßig aktiviert. Ältere Geräte bieten meist zusätzlich den Modus „IDE“, der die Transferleistung deutlich reduziert.

Sie finden die SATA-Einstellungen im Bios/Firmwaresetup des Rechners meist in Menüs wie „Advanced → Integrated Peripherals“, „SATA Configuration“, „SATA Mode Selection“ oder „PCH Storage Configuration“. Auf einer Übersichtsseite („Main“, „System Status“ oder ähnlich) finden Sie meist Informationen, an welchen SATA-Port die Festplatten angeschlossen sind. Auf neueren Hauptplatinen gibt es nur SATA-Ports mit schnellen sechs GBit/s (SATA III) und Sie können einen beliebigen Port verwenden. Ältere Modelle sind auch mit langsameren Ports ausgestattet (SATA I, SATA II), an denen die Systemfestplatte besser nicht angeschlossen wird. Im Handbuch der Hauptplatine können Sie nachlesen, welche Anschlüsse SATA III bietet.

M.2/NVMe-SSDs nachrüsten

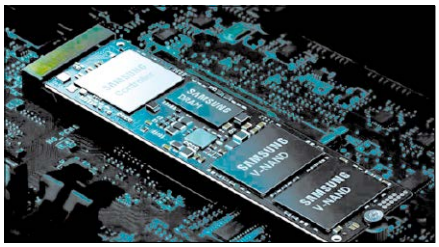
In neueren Notebooks stecken meist SSDs in Form einer platzsparenden M.2-Karte, deren Größe einem RAM-Speicherriegel entspricht. Einen herkömmlichen SATA-Anschluss für ein 2,5-Zoll-Laufwerk gibt es manchmal ebenfalls.

Desktoprechner werden eher mit einer preisgünstigeren SATA-SSD oder sogar nur mit einer SATA-Festplatte ausgeliefert. Die Hauptplatine ist aber meist auch mit M.2-Steckplätzen ausgestattet.

M.2-SSDs gibt es in zwei Ausführungen. Ältere Modelle werden über die SATA-Schnittstelle angebunden, neuere mit der Bezeichnung NVMe (Nonvolatile Memory Express) über den noch deutlich schnelleren PCI-Express-Bus. Meist bietet wenigstens einer der M.2-Steckplätze auf der Hauptplatine beide Modi. Im SATA-Modus fällt einer der anderen SATA-Anschlüsse weg, bei PCI-Express lassen sich weiterhin alle verfügbaren SATA-Ports nutzen. Wie der Rechner zu bestücken ist und ob zusätzlich Biosnötig sind, kann man im Handbuch zur Hauptplatine nachlesen.

Geschwindigkeit von Laufwerken messen

Durchschnittliche Festplatten (SATA III) lesen und schreiben mit circa 100 MB pro Sekunde. SATA-SSDs erreichen ungefähr 500 MB/s beim Lesen und die Transferrate beim Schreiben liegt meist etwa 50 bis 100 MB/s darunter. NVMe-SSDs am PCI-Port sind noch deutlich schneller. Im PCIe-4.0-Steckplatz sind in der Praxis mehr als 5000 MB/s erreichbar, bei PCIe 3.0 ×4 sind es ungefähr 3000 MB/s. Beim Schreiben liegen die Transferraten vor allem bei besonders preisgünstigen Modellen manchmal deutlich darunter, teilweise nur bei um die 1000 MB/s. Allerdings spielt das nur eine Rolle, wenn man besonders große Dateien kopiert. Für den schnellen Start von Betriebssystem und Anwendungen kommt es eher auf die kurzen Zugriffszeiten an – und hier sind SATA- und NVMe-



Blitzschnelle SSDs: NVMe-SSDs sind mit dem PCI-Express-Port verbunden und liefern überragende Transferraten. Allerdings sind die kleinen Steckkarten teurer als SATA-SSDs.

SSDs herkömmlichen Festplatten in jedem Fall haushoch überlegen.

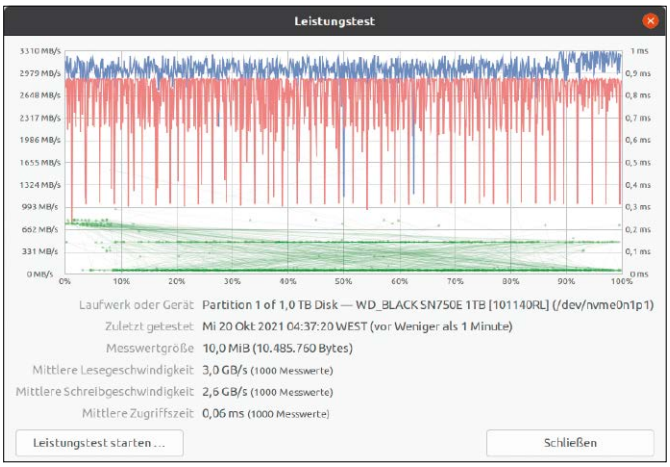
Die Geschwindigkeit von Laufwerken lässt sich im Terminal ermitteln. Sollten mehrere Festplatten vorhanden und in das Dateisystem eingehängt sein, wechseln Sie mit *cd* in ein Verzeichnis, das auf der Festplatte liegt, die Sie prüfen wollen. Starten Sie dort diese drei Befehle:

```
dd if=/dev/zero of=tempfile bs=1M
  count=2048 conv=fdatasync,notrunc
echo 3 | sudo tee /proc/sys/vm/drop_
  caches
dd if=tempfile of=/dev/null bs=1M
  count=2048
```

Die erste Zeile erzeugt eine Datei mit einer Größe von zwei GB und gibt die Schreibgeschwindigkeit aus. Danach wird der Cache gelöscht, um dann die Lesegeschwindigkeit zu ermitteln.

Wer eine grafische Ausgabe bevorzugt, sucht bei Ubuntu über „Aktivitäten“ oder bei Linux Mint im Menü nach „Laufwerke“ (Gnome-Disks). Auf eingehängten Partitionen kann das Tool jedoch keine Schreibtests durchführen. Deshalb booten Sie den Rechner mit einem Ubuntu/Linux-Mint-Installationsmedium und starten Gnome-Disks hier. Für einen Test wählen Sie das gewünschte Laufwerk im linken Teil des Fensters und eine Partition im rechten Teil. Drücken Sie die Tastenkombination Umschalt-F10, gehen Sie im Menü auf „Leistungstest für Partitionen“ und klicken Sie auf „Leistungstest starten“. Setzen Sie ein Häkchen vor „Schreib-Leistungstest ausführen“, wenn die Partition nicht eingehängt ist, und klicken Sie auf „Leistungstest starten“.

Sollten die gemessenen Werte deutlich niedriger sein als zu erwarten, hängt das Laufwerk entweder nicht an einem SATA-III-Port, das SATA-Kabel ist von minderer Qualität oder es ist defekt. Wenn bei NVMe-SSDs die Messungen deutlich unter den Angaben des Herstellers liegen, verwenden Sie – wenn vorhanden – einen anderen M.2-Steckplatz. Auf einigen Hauptplatinen bietet ein Steckplatz nur PCIe 3.0 ×2 (was für M.2-SATA-SSDs ausreicht) und der andere das schnellere PCIe 3.0 ×4 für NVMe-SSDs.



Geschwindigkeit ermitteln: Das Standardtool „Laufwerke“ (Gnome-Disks) bietet einen komfortablen Leistungstest. Für den Schreibtest der Systempartition wird es in einem Livesystem gestartet.

Zustand von Laufwerken prüfen

Gnome-Disks („Laufwerke“) kann auch die SMART-Werte (Self-Monitoring, Analysis and Reporting Technology) auslesen und Hinweise auf mögliche Defekte oder Alterserscheinungen von Laufwerken geben. Rufen Sie mit der F10-Taste das Menü des Tools auf und gehen Sie auf „SMART-Werte und Selbsttests“. Die Tabelle zeigt die einzelnen Werte, beispielsweise die aufsummierten „Betriebsstunden“. Hinter „Allgemeine Einschätzung“ sollte „Das Laufwerk ist in Ordnung“ stehen. Andernfalls ist es Zeit, an einen Austausch zu denken. Bei neuen SSDs steht hinter „wear-leveling-count“ in der Spalte „Normalisiert“ der Wert „100“. Er reduziert sich mit der Zeit. Sobald er nahe „0“ ist, sollten Sie den Datenträger ersetzen.

NVMe-SSDs unterstützt Gnome-Disks bislang nicht. Dafür installieren Sie im Terminal mit dem Befehl

```
sudo apt install nvme-cli
```

ein zusätzliches Tool. Der Befehl

```
sudo nvme list
```

zeigt dann die verfügbaren NVMe-Geräte an. Mit beispielsweise

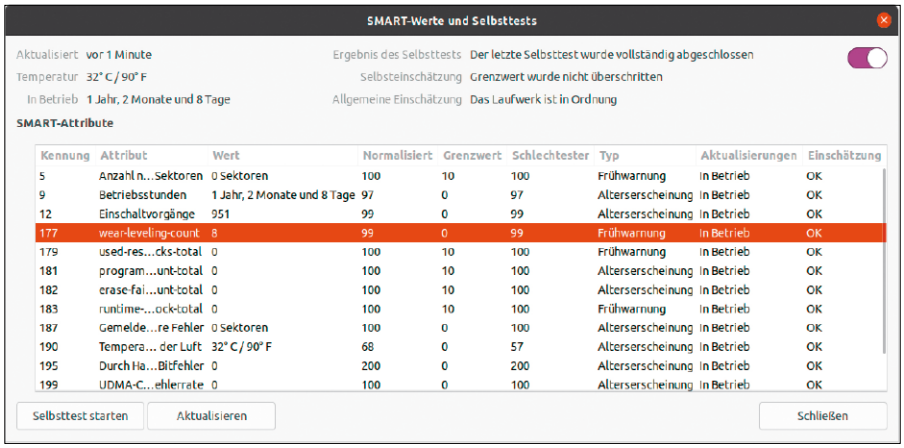
```
sudo nvme smart-log /dev/nvme0n1
```

holen Sie die SMART-Informationen zum NVMe-Laufwerk „/dev/nvme0n1“ ein. Die Werteliste ist bisher nicht bei allen Geräten vollständig – „wear-leveling-count“ beispielsweise kann fehlen.

Bei Intel-SSDs liefert

```
sudo nvme intel smart-log-add
  [Gerätepfad]
```

die fehlenden Informationen. Für SSDs anderer Hersteller ist diese Option noch nicht verfügbar. ■



Wie gesund ist die SSD? Das Tool „Laufwerke“ kann SMART-Werte auslesen und eine allgemeine Einschätzung des Zustands liefern. Das funktioniert derzeit jedoch nicht bei NVMe-SSDs.

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.

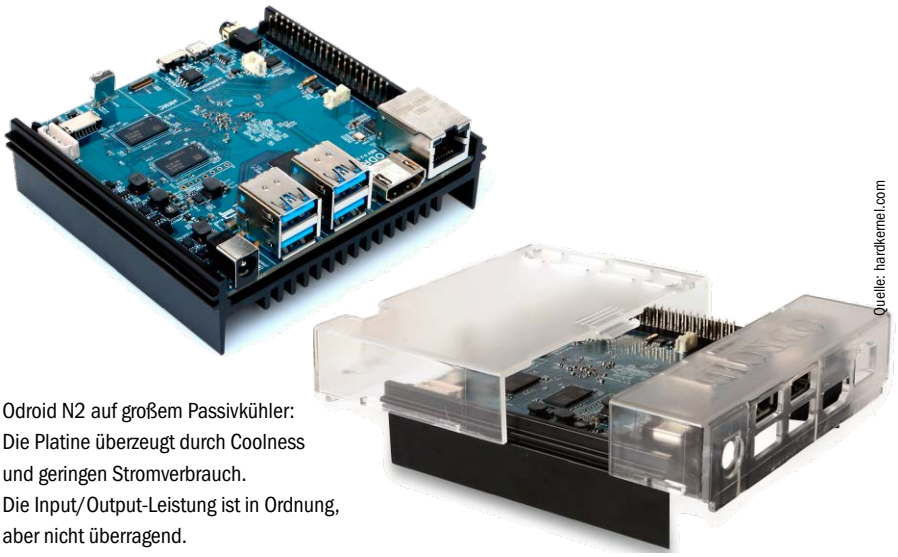
Eine weitere Schwäche sind mangelnde oder mangelhafte Betriebssysteme. Die hardwaretechnisch ansprechenden Banana-Platinen haben mit dem inzwischen eingestellten Bananian ein besonders unrühmliches Negativbeispiel.

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.

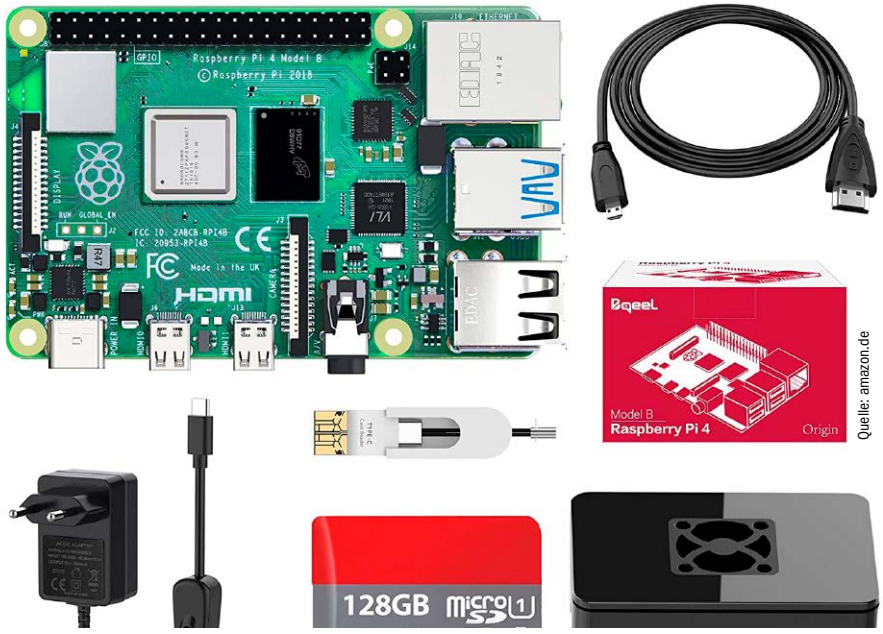
Raspberry Pi 4: Der Universelle

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.

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						



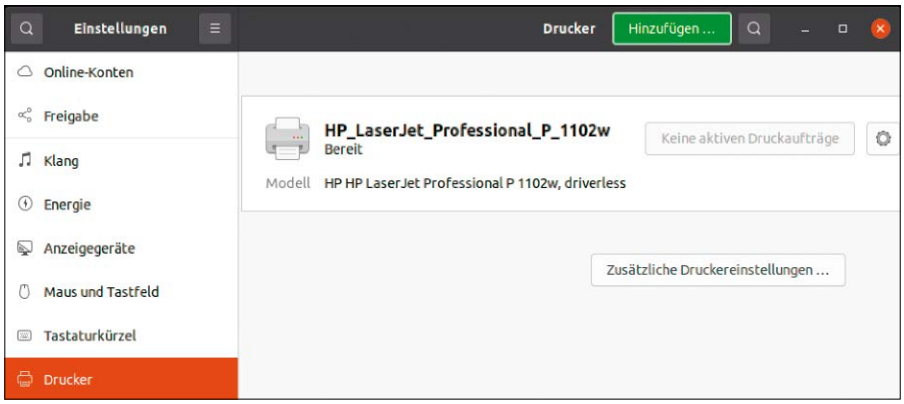
USB statt HDMI: Monitore mit USB-Hub erhalten über ein Typ-C-Kabel Bildsignale, ferner können sie Notebooks mit Strom versorgen und es lassen sich USB-3.0-Geräte anschließen.

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



Druckereinrichtung: Sobald Sie in den Einstellungen auf „Drucker“ gehen, erkennt Ubuntu das Gerät automatisch. Das funktioniert auch mit Netzwerkdruckern, deren Netzzugang konfiguriert ist.

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*). ■

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.

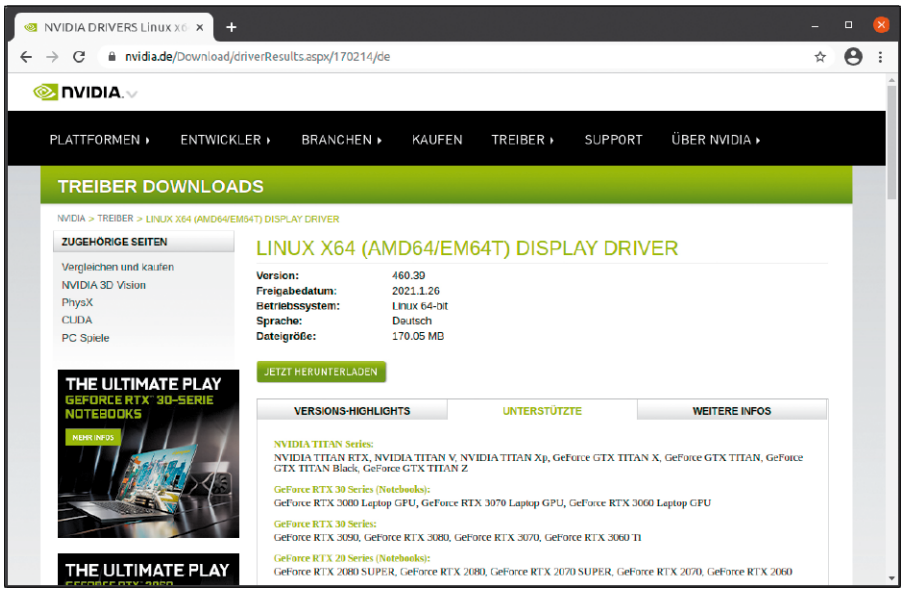
Bei voller 4K-Auflösung von 3840 × 2160 Pixeln sehen zwar Videos prima aus, Desktopelemente sind aber oft schwer zu erkennen. Bei Ubuntu 20.04 können Sie in den „Einstellungen“ unter „Anzeigegeräte“ die „Fraktionelle Skalierung“ aktivieren. Hinter „Skalieren“ stellen Sie dann beispielsweise „125 %“ ein. 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*.

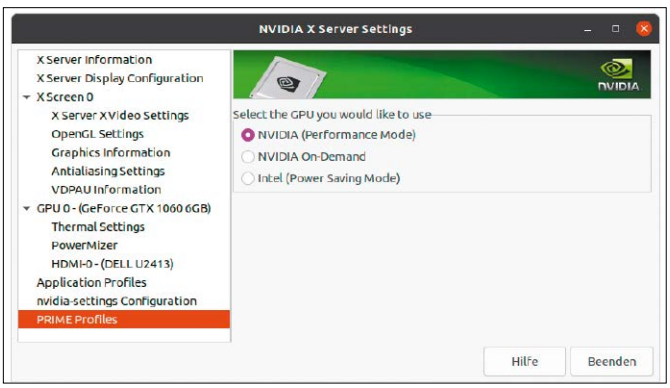
5. Energiesparen durch Treiberwechsel

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.

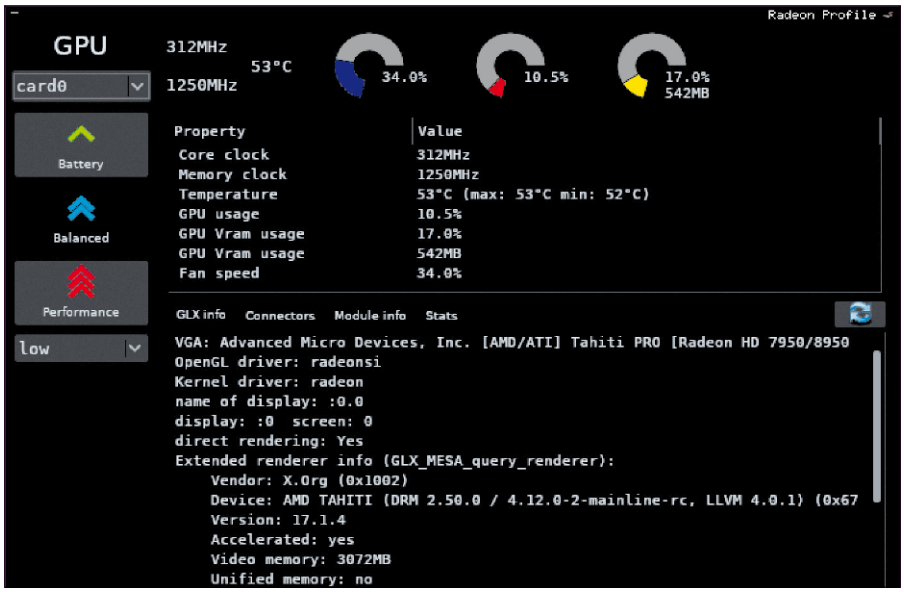
Deutlich mehr Einstellungen gibt es, wenn der Treiber „amdgpu“ zum Einsatz kommt. Damit kann man beispielsweise manuell die Lüfterdrehzahl einstellen. Installieren Sie Radeon-Profile über ein PPA:

```
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
```

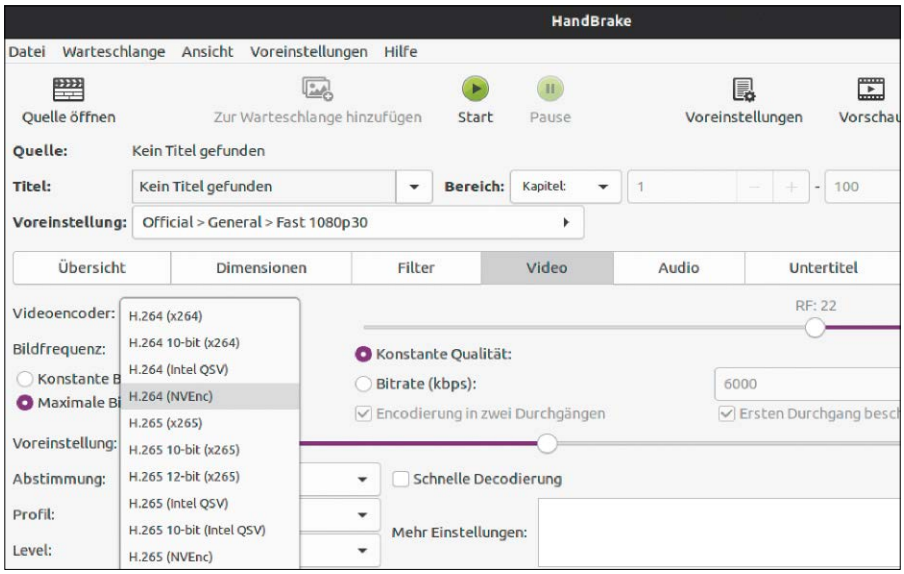
Nutzer von Linux Mint 20 können den ersten Befehl weglassen, weil dort Flatpak standardmäßig vorhanden ist. Wer die Intel-GPU (ab Intel Skylake, sechste Generation mit Intel HD Grafik oder besser) verwenden möchte, klickt zusätzlich unter *https://handbrake.fr/downloads.php* auf „QuickSync Plugin Download (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.

Externe Geräte für den PC



Der USB-Port ist der Standard für den Anschluss weiterer Hardware an PCs und Notebooks. Die meisten dort angeschlossenen Geräte laufen unter Linux wie erwartet, es gibt aber auch Ausnahmen und Einschränkungen.

VON THORSTEN EGGELING

Für den USB-Port gibt es nicht nur Datenträger, sondern WLAN- und Ethernet-Adapter, Bluetooth- und TV-Adapter, Drucker, Scanner und Multifunktionsgeräte. Die Unterstützung durch Linux ist in der Regel gut, wenn es sich um weitverbreitete Geräte handelt. Wie bei anderer Hardware auch, werden sehr neue Geräte jedoch manchmal nicht erkannt und benötigen aktuellere Kernel. Teilweise stellen Hersteller auch eigene Treiber zur Verfügung.

1. USB-Geräte und Linux-Unterstützung

Externe Festplatten und USB-Sticks sind weitestgehend standardisiert und bereiten unter keinem Betriebssystem Probleme. Für Drucker, Scanner und Multifunktionsgeräte gibt es Unterstützung, wenn die Geräte von einem bekannten Hersteller stammen und weitverbreitet sind. Von besonders preisgünstigen Geräten vom Discounter um die Ecke ist jedoch abzuraten. Auf jeden Fall sollte man vor einem Neukauf Informationen zur Linux-Tauglichkeit einholen.

WLAN- und TV-Adapter gehören eher in die Kategorie der problematischen Geräte. Oft werden innerhalb einer Modellserie unterschiedliche Chips verbaut und die Hersteller führen spezielle Anpassungen durch. Selbst wenn der Chipsatz im Prinzip von Linux unterstützt wird, funktioniert das Gerät dann trotzdem nicht. Manchmal fehlt nur die nötige Firmwaredatei, was sich dann einfach beheben lässt. Einige Geräte lassen sich aber trotz aller Bemühungen nicht unter Linux verwenden. Auch hier gilt: Informieren Sie sich vor dem Kauf über die Erfahrungen anderer Benutzer unter Linux. Selbst bei Geräten, die der Hersteller mit Linux-Unterstützung bewirbt, ist Vorsicht geboten. Taucht „Linux“ bei den Voraussetzungen in der Liste der Systeme auf, ist oft nicht klar, was damit genau gemeint ist. Oft gibt es den Quellcode eines Treibers, den man selbst kompilieren muss. Das funktioniert dann jedoch nur ab oder bis zu einer bestimmten Kernel-Version.

2. Angeschlossene USB-Geräte analysieren

Sobald ein USB-Gerät mit dem PC verbunden wird, versucht der Kernel, es zu erkennen und den passenden Treiber zu laden. Was genau vor sich geht, erfährt man über einen Befehl im Terminal (Strg-Alt-T):

```
sudo dmesg -wH
```

Das Fenster füllt sich mit den Kernel-Meldungen und die letzten Zeilen enthalten Infos zum neu verbundenen Gerät. War das Gerät bereits verbunden, stecken Sie es ab und dann wieder an. Scrollen Sie im Fenster nach oben, um ältere Meldungen zu sehen. Mit Strg-C brechen Sie die Ausgabe ab. Die relevanten Meldungen beginnen mit „New USB device found“, danach folgen Zeilen, die auf den neu geladenen Treiber hinweisen, etwa „registered new driver interface [Treiber]“ oder ähnlich. Bei einer USB-Festplatte sehen Sie Meldungen wie „USB Mass Storage device detected“ und „sd 8:0:0:0: [sdb] Attached SCSI disk“. „Direct firmware load [...] failed“ deutet auf eine fehlende Firmwaredatei. In der Regel steht in der Nähe der Zeile auch, wie die Firmwaredatei heißt. Suchen Sie über *https://packages.ubuntu.com* („Durchsuchen des Inhalts von Paketen“), ob die Datei in einem Paket der Distribution enthalten ist. Wenn nicht, suchen Sie über eine Internet-Suchmaschine danach.

3. Treiber für Linux finden

Wenn dmesg Fehlermeldungen liefert oder es keinen Hinweis auf einen geladenen Treiber gibt, dann unterstützt der Kernel das Gerät nicht. Im Terminal ermitteln Sie mit

```
sudo lsusb
```

die angeschlossenen USB-Geräte und mit

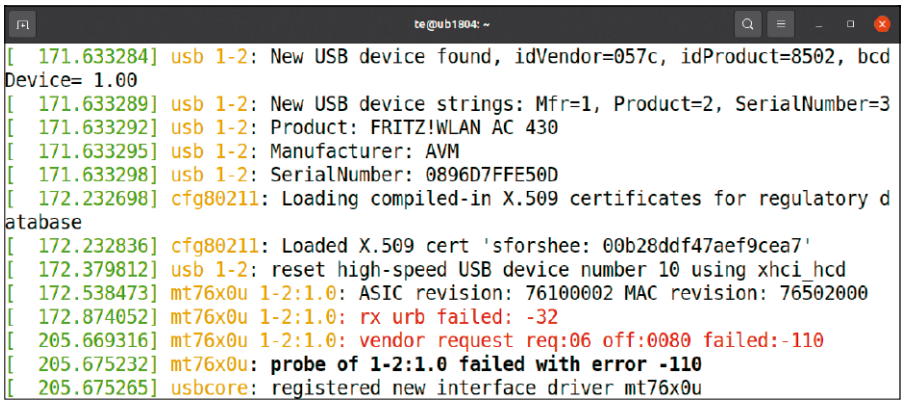
```
modprobe -c | grep -i "[Hersteller-
  ID].*[Product-ID]"
```

finden Sie heraus, ob tatsächlich kein Treiber geladen wurde. Suchen Sie im Internet nach der USB-ID, um weitere Informationen zu erhalten.

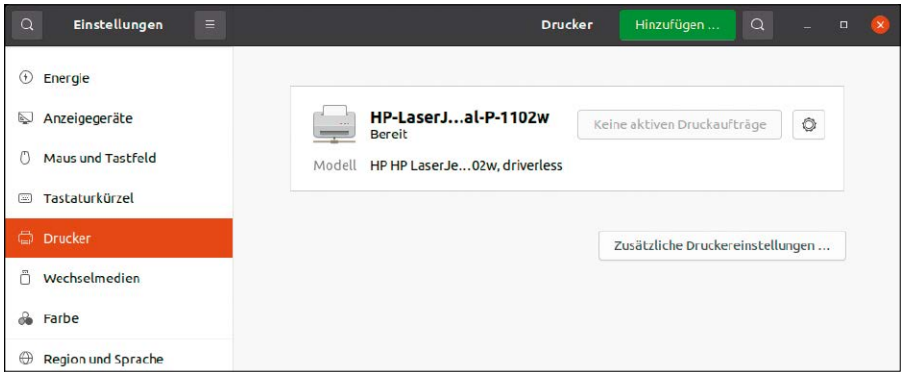
Unter *https://wiki.ubuntuusers.de/WLAN/Karten* finden Sie eine Liste mit WLAN-Sticks vieler bekannter Hersteller. Suchen Sie auf der Seite nach der USB-ID oder der Modellbezeichnung. Es gibt Hinweise, ab welcher Ubuntu-Version ein Adapter direkt unterstützt wird, ob eine neuerer Kernel erforderlich ist (siehe Artikel ab Seite 156) oder ein Treiber manuell installiert werden muss.

Die Anleitungen sind jedoch nicht immer ganz aktuell oder passen trotz identischer USB-ID nicht zu jedem Gerät. Der WLAN-Stick AC 430 von AVM (057c:8502) beispielsweise, sollt laut *https://wiki.ubuntuusers.de* vom Mainline-Kernel 5.3rc3 unterstützt werden (siehe Artikel ab Seite 156, Punkt 5). Bei unserem Testgerät war das nicht der Fall, möglicherweise aufgrund von Änderungen während des Produktionszeitraums. An dieser Stelle sollte man sich überlegen, ob sich weiterer Zeitaufwand lohnt oder ob man nicht besser einen unterstützten WLAN-Adapter für 20 Euro erwirbt.

Für TV-Karten und TV-USB-Adapter gibt es weiterführende Informationen unter *https://wiki.ubuntuusers.de/TV-Karten* und *https://www.linuxtv.org/wiki/index.php/Hardware_device_information*. Oft ist eine zusätzliche Firmwaredatei erforderlich, manchmal gibt es auch Treiber direkt von Hersteller, beispielsweise für den USB-Adapter TBS-5520 SE und ähnliche Modelle (*https://github.com/tbsdtv/linux_media/wiki*).



Hardwareerkennung: Die Ausgabe von dmesg zeigt, dass der Treiber mt76x0u für den AVM WLAN-Stick AC 430 zwar geladen wird, dabei aber Fehler auftreten.



Drucken ohne Probleme: Ubuntu erkennt Drucker meist automatisch und richtet die nötige Software ein. Nur in Einzelfällen muss man Drucker manuell hinzufügen und Treiber installieren.

4. Drucker und Scanner

Ubuntu und Linux Mint machen es den Benutzern einfach. Sobald Sie den Drucker per USB-Kabel mit dem PC verbinden, beginnt die Suche nach dem passenden Treiber automatisch. Bereits über das WLAN angemeldete Drucker werden ebenfalls automatisch gefunden.

Wenn nicht, gehen Sie bei Ubuntu 20.04 in den „Einstellungen“ auf „Drucker“, unter Linux Mint im Menü auf „Systemverwaltung→ Drucker“ und fügen einen neuen Drucker hinzu.

Sollte kein Standardtreiber vorhanden, aber der Download möglich sein, erscheint ein Dialog, in dem Sie Download und Installation bestätigen.

Einige Hersteller bieten eigene Treiberpakete und Software für Linux an. Bei HP beispielsweise finden Sie über *https://www.developers.hp.com/hp-linux-imaging-and-printing* eine Liste mit unterstützten Geräten und Funktionen sowie der nötigen Treiberversion. Das Softwarepaket „HP Linux Imaging and Printing“ (HPLIP) richten Ubuntu und Linux Mint automatisch ein. Auf der HP-Website gibt es aber meist eine etwas aktuellere Version für neuere Geräte. Auch Brother, Canon und Epson bieten gute Unterstützung für Linux. Hier finden Sie Treiber jeweils über den Supportbereich. ■

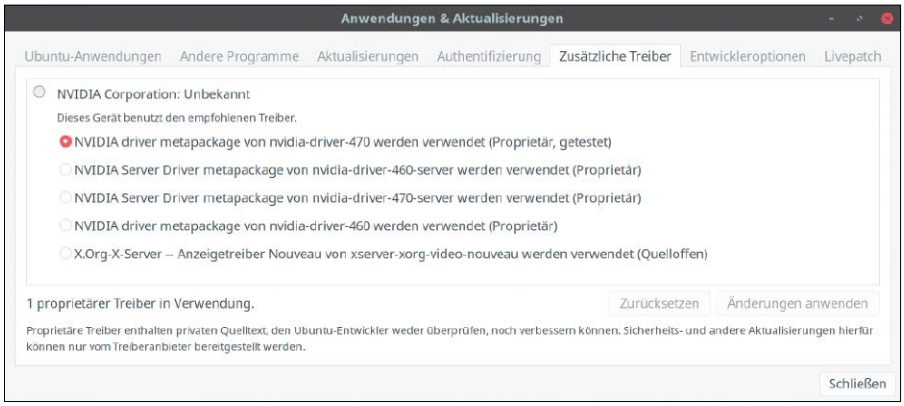
STEUERSOFTWARE FÜR TASTATUREN

USB-Tastaturen funktionieren nach unseren Erfahrungen ohne Einschränkungen. Sondertasten, etwa für die Multimedia-Steuerung, lassen sich ebenfalls nutzen. Manchmal muss man die Tastenfunktionen aber erst zuordnen. Bei Ubuntu 20.04 erfolgt das in den „Einstellungen“ unter „Tastaturkürzel“, bei Linux Mint über „Einstellungen → Tastatur → Tastenkombinationen“. Sollte das Einstellungsfenster nicht auf den Tastendruck reagieren, ignoriert Linux die Tastenanschläge, weil der passende Treiber fehlt.

Suchen Sie im Internet nach dem Tastaturmodell oder der USB-ID. Bei verbreiteten Tastaturen werden Sie schnell fündig: Über *https://m6u.de/G710* finden Sie beispielsweise einen Treiber für das Modell Logitech G710+, über den sich auch die Tastaturbeleuchtung steuern lässt. Bei einer Logitech G213 funktionieren zwar alle Tasten, die LEDs bleiben aber dunkel. Über *https://m6u.de/G213* finden Sie ein Python-Script, mit dem Sie die Beleuchtung der RGB-Tastatur aktivieren.

Treiber und Firmware

Linux unterstützt die meiste Hardware standardmäßig. Sollte ein sehr neues Gerät jedoch ausnahmsweise nicht funktionieren, muss man auf einen neueren Kernel oder eine andere Distribution umsteigen.



Bessere Treiber: Standardtreiber installieren Ubuntu und Linux Mint automatisch. Über „Zusätzliche Treiber" lassen sich optimierte Treiber für Grafikchips einrichten.

VON THORSTEN EGGELING

Bei Linux sind die wichtigsten Basistreiber im Kernel enthalten. Weitere Treiber, die als Kernel-Module bezeichnet werden, lädt der Kernel dynamisch nach – je nach erkannter Hardware. Dazu kommen optimierte Treiber vor allem für Grafikchips. Sehr neue Hardware wird vom Kernel manchmal nicht unterstützt. Dann muss man eine neuere Distribution oder einen neueren Kernel verwenden. Besondere Bios/Firmwareeinstellungen sind für Linux nicht erforderlich. Wer Windows 11 parallel installieren möchte, sollte jedoch auf die korrekte Konfiguration von TPM und Secure Boot achten.

Treiber für Linux

Ubuntu oder Linux Mint richtet bei der Installation Standardtreiber für die Hardware ein. Optimierte Treiber, etwa für Grafikchips, kann und sollte man nachinstallieren. Ubuntu-Nutzer suchen über die „Aktivitäten" nach „Treiber" und klicken auf „Zusätzliche Treiber". Bei Linux Mint führt der Weg über das Menü „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.

Ob eine Hardware von Linux unterstützt wird, ermittelt Sie am besten bereits vor dem Kauf. Eine Internetsuche nach der Mainboardbezeichnung, dem Notebook- oder Gerätemodell in Kombination mit dem Suchwort „Linux" sollte zu den Erfahrungen anderer Anwender führen.

Vorhandene Hardware untersuchen

Hat man die Hardware bereits gekauft, hilft eine genauere Analyse weiter, wenn ein Gerät nicht erkannt wird. Verwenden Sie im Terminal folgende Befehle:

```
sudo lspci -knn > lspci.txt
sudo usb-devices > usb.txt
```

„lspci.txt" enthält dann Informationen zu den über PCI angebundenen Komponenten. Hinter „Kernel driver in use:" und „Kernel modules" steht jeweils der Name des geladenen Treibers. Fehlt die Angabe, wurde kein Treiber geladen. Aber auch wenn ein Treiber verwendet wird, muss er nicht in jedem Fall korrekt arbeiten. Darüber gibt dann der Befehl

```
dmesg | grep -i [Treibername]
```

Auskunft. Wenn hier eine Fehlermeldung auftaucht, wurde wahrscheinlich der falsche Treiber geladen.

„usb.txt" zeigt für USB-Geräte Infos zum geladenen Treiber an. Steht hier „Driver=(none)", dann wurde offenbar kein Treiber gefunden. Verwenden Sie dmesg, direkt nachdem Sie das USB-Gerät verbunden haben. Fehlermeldungen können beispielsweise auf eine fehlende Firmwaredatei hinweisen, nach der man im Internet suchen kann.

Passende Treiber finden

Der Kernel ermittelt den nötigen Treiber anhand der Hardware-ID. Bei PCI-Geräten steht diese in „lspci.txt" direkt hinter der Gerätebeschreibung in der Form [Hersteller-ID:Geräte-ID]. USB-Geräte zeigen in „usb.txt" die IDs hinter „Vendor=" und „ProdID=".

Dazu ein Beispiel: Für einen Realtek 2,5-Gigabit-Ethernet-Controller gibt lspci unter Ubuntu 20.04 ohne Kernel-Updates (Kernel-Version 5.4) folgende Zeilen aus:

```
Realtek Semiconductor Co., Ltd.
  RTL8125 2.5GbE Controller
  [10ec:8125] (rev 05)
DeviceName: RTL8111E Giga LAN
Kernel modules: r8169
```

Ein Treiber wurde also geladen, jedoch zeigt

```
dmesg | grep -i r8169
```

den Fehler „r8169 0000:03:00.0: unknown chip XID 641" und der Netzwerkadapter funktioniert nicht. Es ist am einfachsten, im Internet nach dieser Fehlermeldung zu suchen. Man stößt dann relativ schnell darauf, dass der Realtek-Netzwerkchip RTL8125B heißt und erst ab Kernel 5.9 unterstützt wird.

Neuer Kernel für Linux

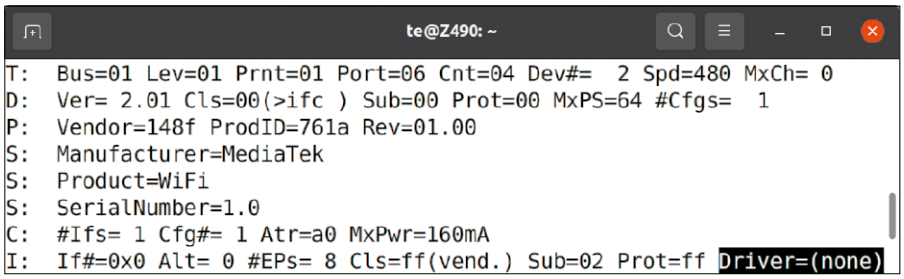
Ubuntu hält den Kernel möglichst aktuell. Wer 20.04 im April 2020 installiert hat, sollte durch Updates inzwischen bei Kernel 5.11 angekommen sein. Damit arbeitet auch das Modul r8169 für den Realtek-

Chip einwandfrei. Für die Neuinstallation sollte man eine aktuelle ISO-Datei verwenden – zur Zeit Ubuntu 20.04.3 LTS (*https://ubuntu.com*).

Linux Mint ist bei der Kernel-Auswahl konservativer. Die aktuelle Version 20.2 verwendet weiterhin Kernel 5.4. Wer den HWE-Kernel installieren möchte, geht im Menü auf „Systemverwaltung → Aktualisierungsverwaltung“ und dann auf „Ansicht → Linux-Kernel“. Zur Zeit steht hier Kernel 5.11 zur Verfügung. Die Neuinstallation kann bei Linux Mint schwieriger sein, etwa wenn der Netzwerkadapter nicht unterstützt wird. In diesem Fall kann man einen funktionierenden WLAN-Adapter temporär anschließen.

Wer Probleme mit sehr neuer Hardware vermeiden möchte, greift zu einer Distribution mit kürzeren Updatezyklen, beispielsweise Ubuntu 21.10 oder 22.10 (ab Oktober) mit Supportende jeweils neun Monate später. Den aktuellsten stabilen Kernel gibt es bei *www.kernel.org* derzeit in Version 5.17. Ebenfalls empfehlenswert sind Fedora (*https://getfedora.org*), Open Suse Tumbleweed (*https://de.opensuse.org/Portal:Tumbleweed*) oder Endeavour-OS (*https://endeavouros.com*).

Den 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 20.04 LTS oder Linux Mint 20.02.



Fehlender Treiber: Wenn usb-devices „Driver=(none)“ anzeigt, bietet der Kernel keinen Treiber für die Hardware. Mit einem Kernel-Upgrade lässt sich das in der Regel beheben.

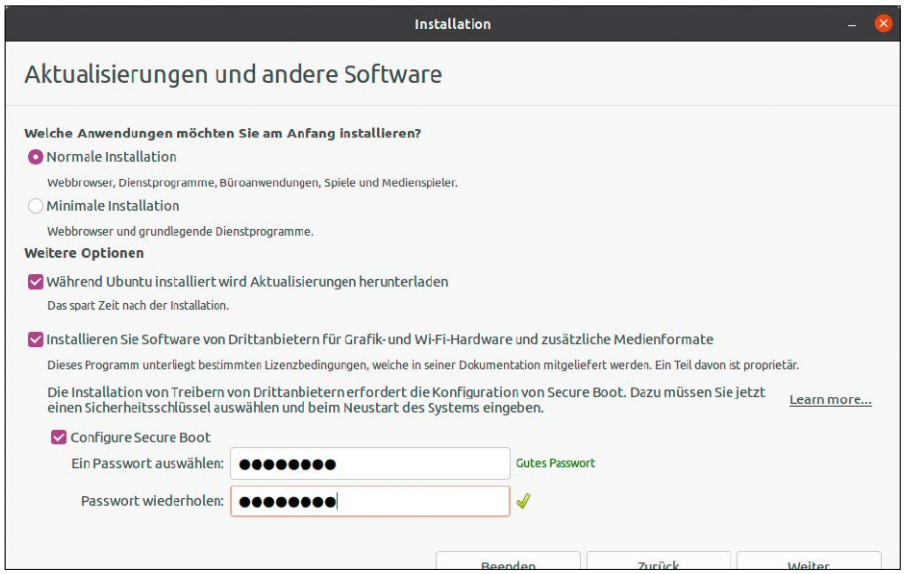


Neuer Kernel für Linux Mint: Die Distribution bleibt in der Version 20.x standardmäßig bei Kernel 5.4. Über die „Aktualisierungsverwaltung“ lässt sich eine aktuellere Version installieren.

Firmwareeinstellungen anpassen

Windows 11 benötigt Secure Boot. Das wird allerdings vom Windows-Setupprogramm nur bei Installation und Upgrade geprüft. Danach kann man Secure Boot im Firmwaresetup auch abschalten. Für die meisten Linux-Distributionen stellt Secure Boot kein Problem dar. Ist die Funktion aktiviert, setzt man bei einer Ubuntu-Neuinstallation Häkchen vor „Installieren Sie Software von Drittanbietern für Grafik- und Wi-Fi-Hardware und zusätzliche Medienformate“ sowie „Configure Secure Boot“ und vergibt darunter ein Passwort. Linux Mint bietet entsprechende Optionen. Nach dem Neustart meldet sich das „MOK management“. Hier wählt man „Enroll MOK“, „Continue“ und „Yes“, tippt das zuvor vergebene Passwort ein und bestätigt mit „OK“. Damit wird der Signaturschlüssel in der Firmware hinterlegt.

Wer Software installiert, die zusätzliche Kernel-Module erstellt, muss diese dann allerdings auch signieren. Wie das geht, steht in der Dokumentation der Software. Mit abgeschaltetem Secure Boot lässt sich dieser Aufwand jedoch vermeiden. TPM 2.0 muss für Windows 11 für ebenfalls aktiviert sein. Auf Linux hat das aber keine Auswirkungen. Rufen Sie die Firmwareeinstellungen auf, um die Option dafür – wenn vorhanden – zu aktivieren. Die Einstellungen für TPM finden Sie meist unter einem Menü wie „Security“ oder „Advanced“. Aktivieren Sie Optionen wie „Security Device Support“ oder ähnlich. Meist haben Sie die Wahl zwischen „PTT“ (Intel) beziehungsweise „fTPM“ (AMD). ■



Secure Boot mit Linux: Bei aktivem Secure Boot ist für zusätzliche Treiber ein Passwort erforderlich. Das Zertifikat übergibt man beim ersten Neustart einmalig an die Firmware.

Hardwarerecycling mit Linux



Mit sparsamen Desktopdistributionen und spezialisierten Serversystemen lädt Linux dazu ein, für ausgemusterte Geräte wieder passende Rollen zu finden. Für manche Aufgabe kann sich sogar der explizite Nachkauf älterer Hardware lohnen.

VON HERMANN APFELBÖCK

Dieser Beitrag richtet sich Heimanwender, die für nicht mehr taufrische Hardware eine passende Rolle suchen oder aktuell den Kauf eines NAS-Geräts oder Ein-Platinen-Rechners für eine Serverrolle überlegen. Ältere Hardware kann unter Linux noch einen richtig guten Job machen. Insbesondere nicht mehr desktoptaugliche Notebooks mit akzeptablem Stromverbrauch sind in der Serverrolle einem Raspberry Pi oder einem NAS-Gerät oft vorzuziehen.

Kriterien für taugliche Hardware

CPU, RAM, USB, Ethernet und Stromverbrauch entscheiden wesentlich, ob ein Altgerät als Linux-Server oder sogar als Desktop taugen kann. Mit folgenden Fragen und Kriterien treffen Sie eine Vorauswahl:

- Wie steht es um die CPU-Leistung? Brauchbare bis gute Leistung bieten 64-Bit-CPUs mit zwei Kernen und einer Taktrate von einem GHz aufwärts.
- Genügt der Arbeitsspeicher? Zwei bis vier GB RAM sind für Server und sparsame Desktops völlig ausreichend, darunter wird es knausrig.
- USB 3.0 ist wünschenswert, wenn das Altgerät als Datenserver arbeiten soll. USB 2.0 ist für diese Rolle bereits grenzwertig. Für andere Rollen, etwa als kleiner Intranet-Webserver, spielt die USB-Schnittstelle keine Rolle.
- Gigabit-Ethernet (in Verbindung mit USB 3.x) ist für einen Datenserver wünschenswert. Fast Ethernet (100 MBit/s) kann für kleine Home-Sicherungen und Apache-Dienste ausreichen.
- Verursacht das Altgerät störende Betriebsgeräusche? Sind diese am geplanten Standort tolerabel?
- Wie gelingt die Linux-Installation? Der Rechner muss ein internes DVD-Laufwerk besitzen oder ein externes DVD-Laufwerk via USB erkennen oder (und am einfachsten) via USB bootfähig sein.
- Wie steht es beim Stromverbrauch? Ein Gerät in der Serverrolle sollte zumindest tagsüber permanent laufen. Mehr als zehn bis 20 Watt im Idle-Betrieb sind nicht optimal.
- Funktionieren Sound und WLAN? Falls das Gerät später Sound liefern oder im WLAN funken soll, testen Sie die Funktionsfähigkeit vorab mit einem Linux-Livesystem.

Notebooks im Fokus

Im Prinzip gibt es bei fast allen der oben genannten Kriterien einen persönlichen Ermessensspielraum und eine Relation zur geplanten Rolle. Auch die Singlecore-CPU eines alten Netbooks kann mit einem GB RAM etwa einen Apache-Server mit einem kleinen Notizen-Wiki im Heimnetz anbieten. Und bekanntermaßen gibt es selbst für mehr als 15 Jahre alte 32-Bit-CPUs ohne PAE-Erweiterung noch Recycling-Distributionen wie Antix oder Bodhi Linux.

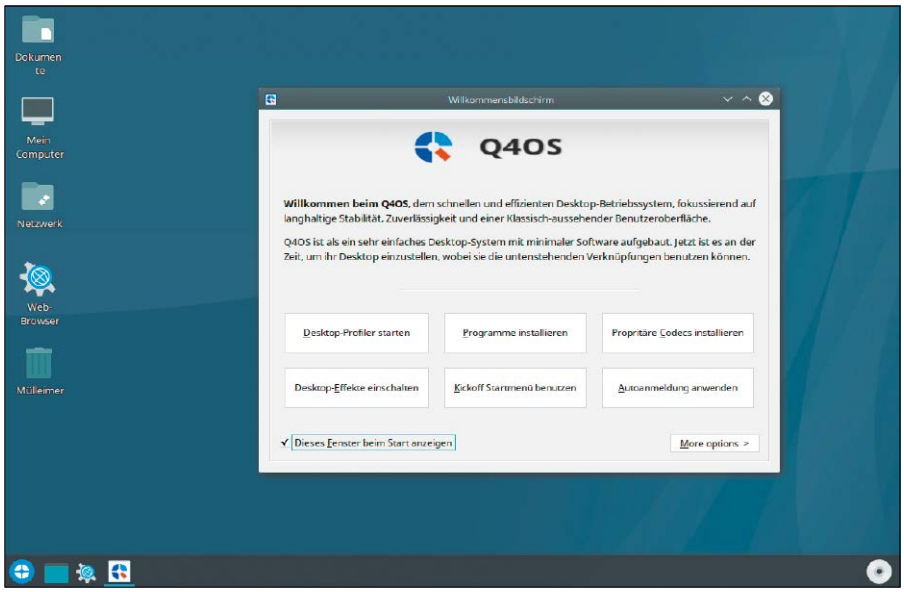
Trotzdem sehen wir die lohnendsten Re- und Upcycling-Kandidaten bei bis zu zehn Jahre alten **Notebooks,** auf denen Windows, Ubuntu, Browser und Office keinen Spaß mehr machen. Die werden mit einer sparsamen Linux-Distribution wieder zum flotten Desktop und sind vor allem in einer Serverrolle leistungsfähiger als Platinenrechner. Nicht zu vergessen: Im Unterschied zu ARM-Platinen bietet die x86-Architektur von Notebooks die uneingeschränkte Auswahl aller Linux-Distributionen. Notebooks haben überdies bauartbedingte Vorteile. Auch auf einem per SSH- oder Weboberfläche verwalteten Server sind Kontrollmonitor, Tastatur, Maus willkommen. Auch die Stromversorgung für passiv angeschlossene USB-Datenträger ohne eigenen Netzadapter funktioniert zuverlässiger als bei Platinenrechnern.

Kluge Home-Admins halten daher heute vermehrt Ausschau nach soliden Notebooks als Serverhardware. Gute gebrauchte Notebooks mit i3-CPU aufwärts, vier GB RAM aufwärts sowie USB 3.0 und Gigabit-Ethernet kosten typischerweise 200 bis 400 Euro



Quelle: amazon.de

Notebook statt NAS oder Platine: Das gebrauchte Thinkpad X230 bringt für etwa 230 Euro alles mit, was ein Linux-Server braucht – i3-CPU, vier GB RAM, USB 3.0, Gigabit-Ethernet.



Leichte Desktop-Last für alte Hardware: Q4-OS ist eine Alternative zu gewöhnungsbedürftigen Minimalisten oder einem bereits zu großen Xubuntu.

(siehe *www.gebrauchtcomputer24.de* oder „Refurbished"/"Vorführware" bei *www.conrad.de, www.pollin.de*). Das ist dann B-Ware mit optischen Mängeln oder renovierte Gebrauchtware („refurbished"). Erfreulich: Der Akku als Hauptverschleißteil spielt beim stationären Dauereinsatz keine Rolle.

Netbooks: Diese Miniatur-Notebooks haben im Prinzip alle genannten Argumente der Notebooks auf ihrer Seite und sind zudem stromsparend und leise. Andererseits sind sie aber mit Atom- oder Celeron-CPU und meist nur einem GB RAM einfach zu leistungsschwach. Nur für kleine Nebenrollen wie bereits oben angesprochen – etwa als Apache-Dienst – bleiben sie im Spiel.

Ausbau-PCs: Wenn Ausbau-PCs ihre Zeit als Desktop trotz Aufrüsten überschritten haben, ist weitere Rollensuche eher zweifelhaft: Die Größe spricht ebenso gegen einen Einsatz im Wohnzimmerschrank wie Betriebsgeräusche durch alte Lüfter und Festplatten. Außerdem verbrauchen PC-Veteranen schon im Idle-Betrieb gerne 60 Watt (ohne Monitor) und sind eher ungünstige Kandidaten für eine Serverrolle.

Geeignete Distributionen

Altrechner als Desktop: Nicht allzu betagte Notebooks können auch die Rolle eines Desktopsystems übernehmen, wenn Sie eine geeignete Distribution verwenden. In die engere Wahl kommen MX Linux (*https://mxlinux.org*), *Q4-OS (https://q4os.org/)* oder *Xubuntu (https://xubuntu.org/)*. Diese Distributionen sind sparsam und unkompliziert. Ganz spezialisierte Oldie-Unterstützer wie Antix, Bodhi Linux, Puppy Linux sind noch anspruchsloser, aber im Benutzeralltag gewöhnungsbedürftig.

Altrechner als Server: Serverdienste sind Software und somit prinzipiell auf jedem Linux nachrüstbar. Trotzdem sind spezialisierte Serverdistributionen gerade auf schwächerer Hardware von Vorteil, weil sie auf Serverfunktionen fokussieren und auf überflüssige Komponenten verzichten.

- Wer mit einem Headless-Server klarkommt, der per SSH verwaltet wird, dann sind Debian, Open Suse Leap oder Ubuntu Server eine gute Wahl. Eine puristische Wahl ist der Netboot-Installer von Ubuntu (*http://cdimage.ubuntu.com/netboot*) mit freier Auswahl der benötigten System- und Serverkomponenten.
- Wer für einen Datenserver eine Konfigurationsoberfläche bevorzugt, ist mit dem NAS-System Open Media Vault gut beraten (*www.openmediavault.org*). Das Download-ISO ist der textbasierte Installer. Bei der Installation sollten Sie Festplatten als Systemziel meiden, weil das System den ganzen Datenträger übernimmt und der restliche Platz verschwendet wäre. Für OMV genügt ein USB-Stick mit 16 GB. Nach der Installation erfolgt die Konfiguration über das Netzwerk via Browser in einer Weboberfläche. Dafür benötigen Sie lediglich die IP-Adresse des OMV-Rechners.

Für Empfehlungen für einzelne Software und Dienste, die sich für ältere Hardware eignet, ist hier kein Platz. Im Umfeld von kleinen und mittleren Webserver-Diensten gibt es jedoch kaum Gegenanzeigen. Selbst eine Nextcloud stemmt jedes ältere Notebook mühelos, wobei die Ansprüche dieser Homecloud aber natürlich von der Menge der aktivierten „Apps" abhängen. Die Installation der Nextcloud kann im einfachsten Fall als Snap-Container erfolgen (*sudo snap install nextcloud*).

Ethernet-Leistung verbessern

Die Leistungsdaten eines Geräte-Oldies sollten vorab passen, denn das Aufrüsten alter Hardware lohnt selten. Eine Ausnahme gibt es aber: Ältere Notebooks haben oft nur einen Fast-Ethernet-Netzadapter (100 MBit/s). Das mag oft ausreichen, so richtig servertauglich ist das Tempo jedoch nicht. Der Netzdurchsatz lässt sich aber mit der bescheidenen Investition in einen USB-to-Ethernet-Adapter deutlich verbessern. Solche Adapter an USB 3.0 erreichen für etwa 20 Euro schnelles Gigabit-Tempo – einfach an einen USB-Port anschließen und am anderen Ende das Ethernet-Kabel einstecken. Treiberprobleme sind nicht zu erwarten. Gigabit-Leistung erreichen Sie aber nur in Kombination mit USB 3.0, mit USB 2.0 immerhin auf etwa 300 MBit/s. ■



Quelle: amazon.de

Gigabit-Ethernet via USB: Diese Aufrüstmaßnahme ist nicht teuer (10 bis 20 Euro) und macht Altrechner servertauglich.

Energiehunger von Notebooks bändigen



Notebooks laufen prima unter Linux. Im direkten Vergleich zu Windows auf demselben Gerät fällt aber oft die kürzere Akkulaufzeit auf. Mit ein paar Einstellungen lässt sich das verbessern.

VON THORSTEN EGGELING UND DAVID WOLSKI

Im Fokus der Linux-Entwickler stehen meist Server, wo Linux am häufigsten anzutreffen ist. Die knapp bemessene Zeit für die Treiberentwicklung wird daher vorwiegend in die Verbesserung der Rechenleistung investiert. Stromsparfunktionen, die zudem spezielle Anpassungen an das jeweilige Gerät erfordern, werden oft nicht ausreichend optimiert. Außerdem sind einige Stromsparfunktionen aus Kompatibilitätsgründen nach der Installation eines Linux-Systems noch nicht aktiviert. Wenn der Akku nicht lange genug durchhält, kann man das ändern. Zwei Tools helfen bei der Konfiguration.

Energiebedarf des Notebooks ermitteln

Vor der Optimierung sollte man den Leistungsbedarf des Geräts messen. Später lässt sich dann beurteilen, ob eine Maßnahme tatsächlich etwas bewirkt. Verwenden Sie in einem Terminal die Befehlszeile

```
cat /sys/class/power_supply/BAT?/
  power_now
```

Bei abgezogenem Netzteil erhalten Sie einen Wert in Mikrowatt, der den aktuellen Energiebedarf des Linux-Systems liefert. Teilt man den beispielsweise angezeigten Wert „19980000“ durch 1 000 000, ergibt das 19,98 Watt. Ebenfalls im Terminal arbeitet der Energiemonitor Powertop von Intel, der zahlreiche Informationen liefert. Das Tool liegt in den Standard-Paketquellen aller wichtigen Linux-Distributionen bereit. Nutzer von Debian, Ubuntu oder Linux Mint installieren Powertop mit

```
sudo apt-get 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 der Tab-Taste navigieren Sie zur jeweils nächsten Kategorie.

Auf der Seite „Einstellbarkeit“ gibt Powertop eine Reihe von Empfehlungen zur Systemkonfiguration aus, die aktivierte und deaktivierte Stromsparfunktionen zeigt. Temporär aktiviert ein Druck auf die Eingabetaste eine einzelne Option. Um alle vorgeschlagenen zusätzlichen Stromsparfunktion einzuschalten, verwenden Sie diesen Befehl:

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

Da dies nur für die aktuelle Sitzung gilt, sollte ein Cronjob diesen Befehl bei jedem Systemstart starten. Nach der Eingabe von

```
sudo crontab -e
```

tragen Sie den zusätzlichen Job

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

als weitere Zeile ein.

Ruhezustand zum Energiesparen nutzen

Wenn man den Rechner gerade nicht aktiv benutzt, hilft der Ruhezustand (Suspend) beim Stromsparen. Die Funktionen dafür sind standardmäßig konfiguriert. Bei Ubuntu 20.04 beispielsweise klicken Sie auf das Symbol rechts oben in der Leiste und gehen auf „Ausschalten / Abmelden → Bereitschaft“. In diesem Modus wird der Hauptspeicher weiter mit Strom versorgt. Wenn Sie den Rechner per Tastatur oder Maus wieder aufwecken, laufen weiterhin alle zuvor gestarteten Programme. Allerdings funktioniert das nicht immer ohne Probleme. Manchmal wacht der Rechner nicht auf oder die WLAN-Verbindung funktioniert nicht mehr. Sehen Sie im Firmwaresetup (Bios) nach, ob es Optionen für die Stromsparzustände gibt. Sofern vorhanden, sollte „Suspend to RAM (S3)“ aktiviert sein.

In den „Einstellungen“ können Sie bei Ubuntu 20.04 unter „Energie“ festlegen, ob der Rechner nach einer bestimmten Zeit automatisch in Bereitschaft gehen soll. Außerdem gibt es Optionen für die automatische Abschaltung von WLAN und Bluetooth bei Nichtbenutzung.

Nutzer von Linux Mint finden ähnliche Optionen über das Menü und „Einstellungen → Energieverwaltung“.

Schlafzustand (Hibernation) aktivieren

Dieser Modus ist standardmäßig nicht verfügbar und muss manuell aktiviert werden. Im Schlafzustand wird der Inhalt des Hauptspeichers auf die Festplatte geschrieben und der Rechner dann komplett ausgeschaltet. Dadurch lässt sich mehr Energie sparen als beim Ruhezustand. Ubuntu 20.04 und Linux Mint 20 verwenden die Swapdatei „/swapfile“ als Auslagerungsdatei. Darin wird auch der RAM-Inhalt beim Schlafzustand gespeichert.

Schritt 1: Die Swapdatei muss dafür doppelt so groß sein wie der Hauptspeicher im Gerät. Die Größe von Swapfile und RAM ermitteln Sie mit diesen beiden Befehlszeilen:

```
swapon -s
cat /proc/meminfo
```

Schritt 2: Ist die Swapdatei nicht vorhanden oder zu klein, erstellen Sie eine neue – bei acht GB RAM beispielsweise mit diesen vier Zeilen:

```
sudo dd if=/dev/zero of=/swapfile
 bs=1M count=16000
sudo chmod 600 /swapfile
sudo mkswap /swapfile
sudo swapon -v /swapfile
```

Schritt 3: Kontrollieren Sie die Einbindung der Swapdatei in der Datei „/etc/fstab“ und fügen Sie folgende Zeile bei Bedarf neu hinzu (*sudo nano /etc/fstab*):

```
/swapfile none swap sw 0 0
```

Starten Sie danach Linux neu.

Schritt 4: Installieren Sie jetzt zwei zusätzlich Softwarepakete:

```
sudo apt install hibernate uswsusp
```

Danach ermitteln Sie mit

```
sudo swap-offset /swapfile
```

den Offset und mit

```
findmnt -no SOURCE,UUID -T /
 swapfile
```

die UUID für die Partition, auf der die Datei liegt.

Schritt 5: Öffnen Sie die Grub-Konfigurationsdatei mit diesem Befehl:

```
sudo nano /etc/default/grub
```

Ändern Sie die Angaben wie folgt:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet
 splash resume=UUID=[UUID] resume_
 offset=[Offset]"
```

Für die Platzhalter in eckigen Klammern setzen Sie die in Schritt 4 ermittelte UUID und den Offset ein.

Schritt 6: Öffnen beziehungsweise erstellen Sie die Konfigurationsdatei für die initiale Ramdisk:

```
sudo nano /etc/initramfs-tools/
 conf.d/resume
```

Tragen Sie dort diese Zeile ein:

```
resume=UUID=[UUID] resume_
 offset=[Offset]
```

Die Platzhalter ersetzen Sie wieder wie in Schritt 5.

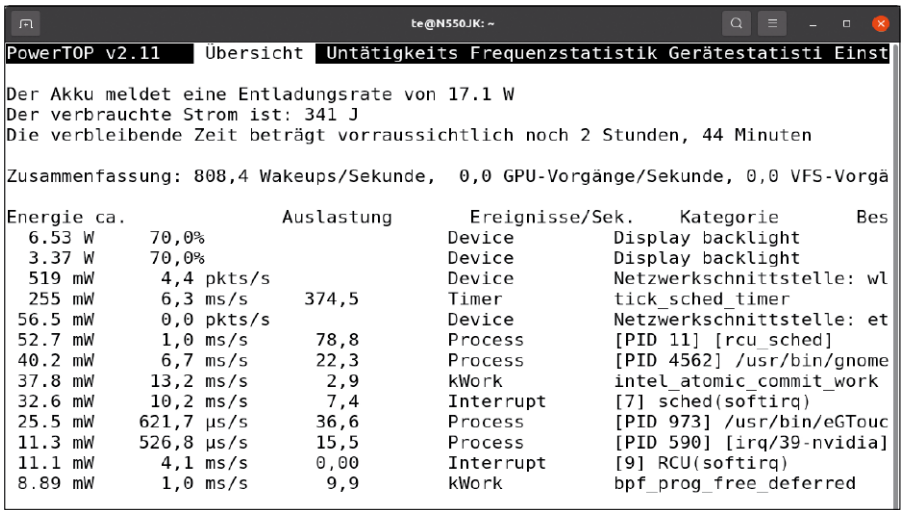
Schritt 7: Um die Konfiguration zu aktualisieren, verwenden Sie diese zwei Befehle:

```
sudo update-grub
sudo update-initramfs -u -k all
```

Starten Sie Linux neu. Danach aktivieren Sie den Ruhezustand:

```
sudo systemctl hibernate
```

Wenn das System nach dem Einschalten des Rechners anstandslos fortgesetzt wird, können Sie den Schlafzustand verwenden. Für die bequemere Nutzung installieren Sie unter Ubuntu 20.04 die Gnome-Erweiterung „Simpler Off Menu“ (*https://m6u.de/som*). „Hibernate“ lässt sich damit neben „Bereitschaft“ in das Menü der Systemleiste einbauen. Damit sich Gnome-Erweiterungen über die Website installieren lassen, aktivieren Sie zuerst das Firefox-Add-on „Gnome Shell integration“ (*https://m6u.de/gsi*) und installieren das Paket „chrome-gnome-shell“. Wer Linux Mint Cinnamon nutzt, installiert das Applet „Shutdown Menu with Icons“ („Herunterfahren-Menü mit Icons“). Wenn Sie bisher noch keine Applets eingerichtet haben, finden Sie eine Anleitung unter *www.pcwelt.de/2374433*.



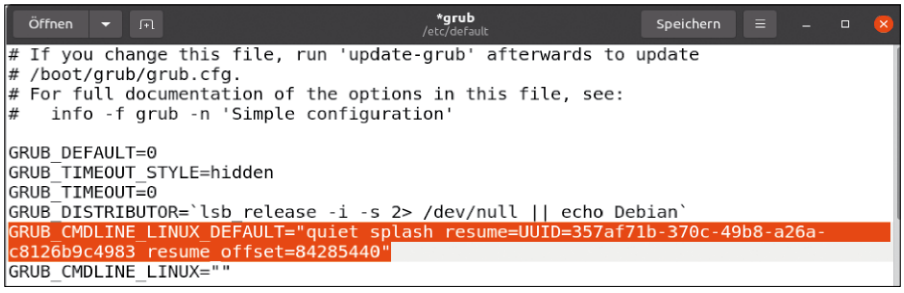
Energiebedarf ermitteln: Powertop zeigt die Entladungsrate des Akkus und die Leistungsaufnahme von Geräten und Prozessen an. Außerdem hilft das Tool bei der Optimierung.

Stromsparfunktionen über TLP aktivieren

Zahlreiche Feineinstellungen zum Betrieb mit möglichst wenig Energiebedarf fasst das Projekt „Linux Advanced Power Management“ (TLP) zusammen. Die Installation von TLP erfolgt unter Debian/Ubuntu/Mint mittels

```
sudo apt-get install tlp
```

und aktiviert ein grundlegendes Set an Stromsparfunktionen. Die Konfiguration erfolgt über die Datei „/etc/tlp.conf“, die englischsprachige Kommentare zu jeder Einstellung enthält. Ausführliche Erklärungen auf Deutsch finden Sie unter *http://thinkwiki.de/TLP_Einstellungen*. ■



Hibernate-Modus: Damit Linux weiß, wo der RAM-Inhalt für den Schlafzustand gespeichert werden soll, muss die UUID des Laufwerks in der Datei „/etc/default/grub“ konfiguriert sein.

Tipps & Tricks zu Festplatten und SSDs

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

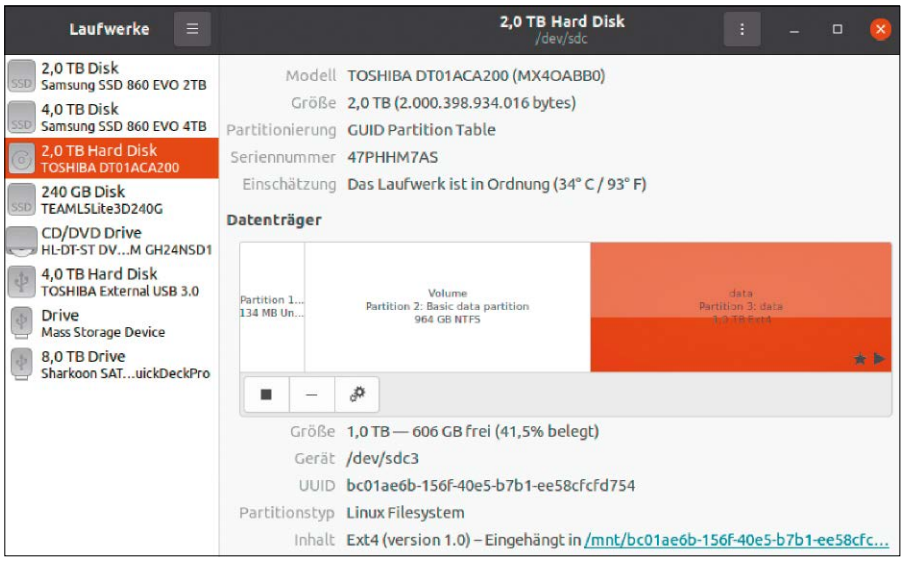
```
sudo fwupdmgr get-devices
```

eine Liste der erkannten Geräte. Die drei Befehlszeilen

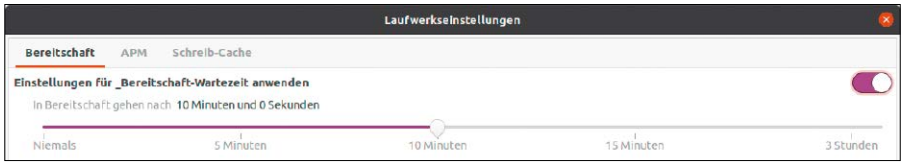
```
sudo fwupdmgr refresh
sudo fwupdmgr get-updates
sudo fwupdmgr update
```

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.

Smartphones & Tablets entrümpeln

Wenn Smartphone-Speicher überlaufen, handelt es sich um kein technisches, sondern um ein psychologisches Problem. Handys & Tablets sind (jedenfalls noch) keine Massenspeicher. Das sollte man lernen, zumal es an Konnektivität nicht mangelt.

VON HERMANN APFELBÖCK

Die heute gängigen 128 und 256, oft sogar 512 GB Speicherkapazität sind für mobile Geräte mit vorwiegend rezeptiven Aufgaben mehr als ausreichend. Tatsächlich versteht aber vor allem die jüngere Smartphone-Generation solche Mobilgeräte nicht als sekundären, mobilen „Thin Client", sondern als Hauptdevice, mit dem man so ziemlich alles macht. Dann sind auch dreistellige Gigabyte-Kapazitäten bald gefüllt. Wer Handynutzer in der eigenen Familie zum Aufräumen motivieren will, hat – abgesehen von offensichtlichen Kapazitätslimits – gute Argumente:

1. Handys müssen nur enthalten, was mobil relevant ist.

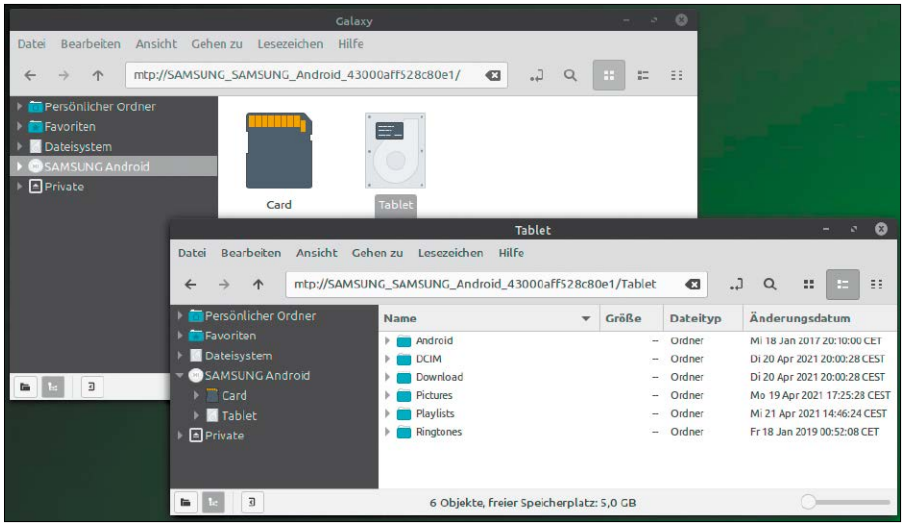
2. Ohne externe Sicherung gehen alle Daten im ungünstigsten Fall komplett verloren (Verlust oder Defekt des Geräts).

3. Man kann Bilder und Videos auch so auslagern, dass sie im exklusiven Zugriff des Handynutzers verbleiben – etwa auf einem USB-Datenträger oder verschlüsselt auf einem Netzserver.

Überflüssige Apps löschen

Zehn bis 20 Gigabyte sind durch Löschen ungenutzter Programme schnell gewonnen. Auf Android-Geräten gehen Sie – am einfachsten – über „Menü" in die allgemeine App-Übersicht. Nicht systemrelevante Apps zeigen nach dem Antippen die Option „Deinstallieren" und Ziehen darauf tut genau das. Genauere Kontrolle bietet der „Anwendungsmanager".

Auf iPhone und iPad wählen Sie in den Einstellungen unter „Allgemein" die Option „iPhone-Speicher" oder „iPad-Speicher". Gehen Sie die Liste durch, wobei die Sortierung nach Größe, der App-Name sowie der Vermerk „Zuletzt benutzt" helfen. Auf große, nicht mehr benötigte Programme tippen Sie und wählen „App löschen". Die Option „App auslagern" bedeutet eine Sicherung in die iCloud und ist allenfalls eine Option, wenn eine ausgelagerte App vorübergehend etwas Platz schaffen soll.



USB-Direktverbindung zwischen Mobilgerät und PC: Das ist die empfohlene und schnellste Methode, durch Datentransfer zum PC vermüllte Handys und Tablets aufzuräumen.

Apps und Daten auf SD-Karte auslagern

Apple-Geräte haben keinen SD-Karten-Slot, und auch auf Android-Tablets ist dieser keineswegs Standard. Sofern aber das Android-Gerät einen besitzt, ist Speichernot leicht zu beheben. Für eine schnelle SD-Karte mit viel Platz – etwa 512 GB – sind dann aber durchaus 80 bis 100 Euro fällig. Dass die Karte dann via Dateimanager Benutzerdaten vom internen Speicher aufnehmen kann, ist selbstverständlich. Android kann aber auch viele Apps (nicht alle) vom internen Speicher auf die SD-Karte auslagern. Wenn Sie die Apps unter „Einstellungen → Allgemein → Anwendungsmanager" durchgehen, ist bei vielen Programmen die Option „Auf SD-Karte verschieben" (oder ähnlich) aktiv. Per Fingertipp auf diese Schaltfläche starten Sie die Aktion.

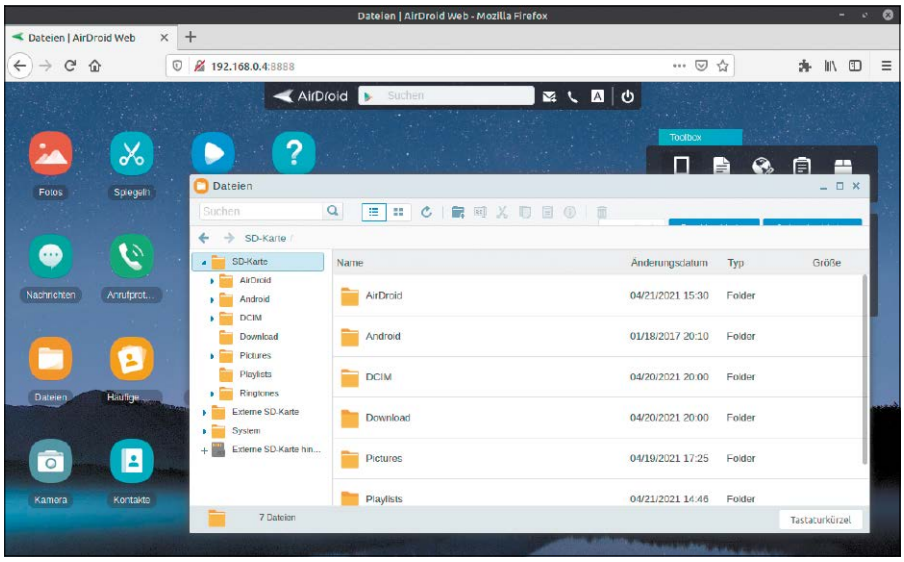
Benutzerdaten via USB zum PC

Große Aufräumaktion sollten – ungeachtet zahlreicher weiterer Methoden – durch direkten USB-Anschluss des Mobilgeräts an PC oder Notebook geschehen. Das verspricht schnellen Datendurchsatz und – zumindest bei Android-Geräten – guten Datenüberblick. Angeschlossene Mobilgeräte

werden unter allen Betriebssystemen via MTP gemountet (Media Transfer Protocol), das Linux- wie Windows-Dateimanager beherrschen. Massentransporte via Rsync oder Robocopy sind allerdings erschwert, weil Terminals MTP nicht selbst beherrschen. Wenn Sie das Terminal bevorzugen, ist Linux eindeutig die bessere Wahl, weil hier das Mobilgerät im Mountpfad unter „/var/run/user/1000/gvfs/[...]“ (Gnome & Co.) anzutreffen und daher auch etwa für Rsync zu benutzen ist.

Den meisten Nutzern wird der manuelle, aber komfortable Maustransport im Dateimanager genügen. Dies ist nach USB-Anschluss des Android-Geräts sofort möglich, sobald Smartphone oder Tablet entsperrt sind. Der interne Speicher zeigt sich im Dateimanager als „Phone“ oder „Tablet“, eine eventuelle SD-Karte als „Card“.

Auch iPhones und iPads lassen sich mit USB am PC anschließen, zeigen dabei aber nur die Mediendateien. Das ändert selbst ein installiertes iTunes am Windows- oder Mac-PC nur graduell. Da aber Videos, Bilder und Musik die Hauptmenge der Benutzerdaten ausmachen dürften, lässt sich das Mac-Gerät trotz dieses Filters effizient aufräumen.

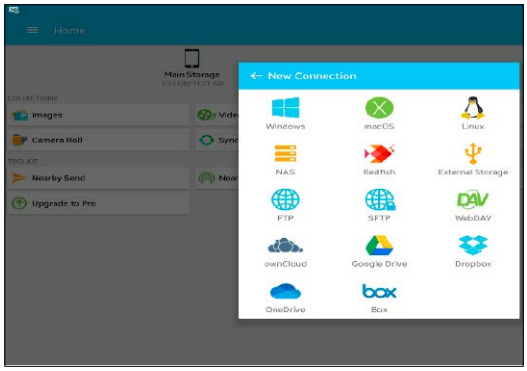


Airdroid-Dateitransfer: Die Oberfläche der Android-App lässt sich mit jedem PC-Browser starten. Neben einem allgemeinen Dateimanager gibt es Filter für Medientypen, Kontakte und Apps.

Andere Wege des Datenexports

USB ist der schnellste Übertragungsweg und braucht keine weiteren Hilfsmittel. Trotzdem werden viele Nutzer den Weg über das WLAN bevorzugen, zumal manche App komfortabler ist als ein Dateimanager am PC. Eine seit Jahren bewährte App für Android ist Airdroid, das nach seinem Start auf dem Android-Gerät einen Webserver etabliert, der dann mit jedem Browser via WLAN zu erreichen ist. Eine Anmeldung und Registrierung bei Airdroid ist dazu nicht notwendig: Man muss nur die IP-Adresse des Mobilgeräts kennen, Standardport ist 8888, also insgesamt dann etwa „http://192.168.178.10:8888“. Airdroid bietet gezielten Zugriff auf Fotos, Musik, Videos, Kontakte, Apps, hat aber auch einen allgemeinen Dateimanager. Beim Massentransport von Dateien ist Airdroid insofern etwa umständlich, als dabei immer erst ZIP-Archive entstehen, die Sie erst wieder entpacken müssen.

Samba, FTP, SSH: Vielleicht nicht für den großen Frühjahrsputz, aber für periodisches Auslagern kleinerer Datenmengen ist die Verbindung zu einem heimischen Server die beste Methode. Oft ist ja der Linux- oder Windows-PC gar nicht das endgültige Ziel der Daten, sondern nur die Zwischenstation zum zentralen Samba-Server. Das geht dann auch direkt mit Hilfe der passenden App.



Videos, Bilder, MP3s ab zum Heimserver! Apps wie hier der FE File Explorer oder der Total Commander verbinden Mobilgeräte zu jedem Samba/Windows- oder SSH-Server im Heimnetz.

Unter iOS ist der kostenlose FE File Explorer beste Wahl, der Samba/Windows, FTP, SFTP (SSH), Webdav unterstützt. Für 5,49 Euro gibt es die werbefreie Pro-Version, die zusätzlich viele Cloudspeicher verbindet. Denselben FE File Explorer gibt es auch für Android, wenngleich dort die Oberfläche etwas anders gestaltet ist (Pro-Version für 4,69 Euro). Technisch genügt auf Android aber auch der altehrwürdige Total Commander, der sich per Plug-ins mit Samba, FTP, SFTP (SSH), Webdav verbindet. Die Plug-ins müssen aber einzeln aus dem Google Store nachinstalliert werden und erscheinen dann im Hauptverzeichnis. Für jedes Plug-in wie etwa „LAN (Windows-Freigaben“) können dann Server inklusive Authentifizierungsdaten angelegt werden.

Temporäre Daten entfernen

Temporäre Daten wie etwa der Browsercache sind keine nennenswerten Speicherfresser. Auf Android-Geräten erhalten Sie unter „Einstellungen → Allgemein → Speicher“ einen Überblick und können „Zwischengespeicherte Daten“, ferner auch „Sonstige Daten“ löschen. Für einzelne Apps gibt es unter „Einstellungen → Allgemein → Anwendungsmanager“ die Option „Daten löschen“.

iOS-Geräte bieten unter den „Einstellungen“ für Apps, die Cachedaten anlegen, eine Löschoption – so etwa für den Browser Safari „Verlauf- und Websitedaten löschen“. Signifikanten Ertrag bringen solche Aktionen allenfalls dann, wenn sie monatelang nicht ausgelöst wurden.

Für Android wie iOS gibt es werbefinanzierte oder kostenpflichtige Cleaner-Apps im Dutzend, die mit viel Show nicht viel mehr als das erledigen. Den großen Platzgewinn bringen sie nicht, schon gar nicht, wenn Sie das Mobilgerät vorher mit den Mitteln des Systems aufgeräumt haben. Die entscheidenden Brocken sind immer die Apps und die eigenen Mediendateien. ■

Aufgeräumte Elektronik



So einfach geht's: Kabelmarker für Strom-, Ethernet- oder USB-Kabel sorgen für klare Zuordnung.

Bitte aufräumen, saugen, wischen! Hardwareprofis empfehlen einmal jährlich den Rundgang durch die heimische PC- und Unterhaltungselektronik. Neben der Beseitigung von Staub und Schmutz lohnen sich auch allerlei nachhaltige Ordnungshilfen.

VON HERMANN APFELBÖCK

Die folgenden Tipps, Produkte und Basteleien sind Anregungen für eine saubere und gut organisierte Infrastruktur sowohl für PC-Arbeitsplätze und Platinenrechner als auch für Unterhaltungselektronik im Wohnzimmer. Für manche Ratschläge gilt periodisches Abarbeiten im Sinne von „Frühjahrsputz", andere Maßnahmen genügen einmal, um dauerhaft für Ordnung und Durchblick zu sorgen.

Kabelchaos rund um Router & TV

Machen wir uns nichts vor: Wenn im Wohnzimmer Router, PC, Receiver, TV, CD-Player, Hi-Fi-Anlage, Telefon, Subwoofer (und ...?) beisammenstehen, dann ist Kabelsalat unvermeidlich. Immerhin lässt sich aber die Zuordnung von Ende und Anfang der Spaghettikabel organisieren. Es ist überaus hilfreich zu wissen, welcher Stromstecker in der Steckerleiste zum Router, welcher zum TV oder PC gehört.

Kabelmarker und Beschriftungen: Für Stromabnehmer genügt es meist schon, dessen Stecker mit einer Klebeetikette zu beschriften. Wer dem Selbstkleber misstraut, kann mit Klarsicht-Tesafilm nachhelfen. Professioneller sind Kabelmarker mit dem zusätzlichen Vorteil, dass sie auch auf Kabel anzubringen sind, die keine beklebbare Fläche anbieten. Cablebugs sind solide Plastikhülsen, die sich auch auf Ethernet-Kabel aufklemmen und beschriften lassen. Für zehn Euro ist jeder Privathaushalt mehr als ausreichend versorgt (40 Stück, *http://amzn.to/17JOjjS*). Noch einfacher sind Kabeletiketten, die Sie mit einem wasserfesten Marker beschriften können (750 Stück für 12 Euro, *https://amzn.to/3vfAWYK*).

Einzeln schaltbare Steckerleisten: Zu wissen, welcher Stecker zu welchem Abnehmer gehört, ist die Hauptsache. Weiteren Komfort bieten Steckerleisten mit einzeln schaltbaren Ports. Dafür kann man bei Markenware wie Brennenstuhl richtig Geld investieren, aber wenn es nur um die Schaltfunktion geht, sind Steckerleisten mit sechs schaltbaren Steckdosen ab etwa 12 Euro zu haben. Das empfiehlt sich insbesondere für Platinenrechner, Router, Access Points, die keinen Powerknopf haben oder schlecht zugänglich sind.



Quelle: conrad.de

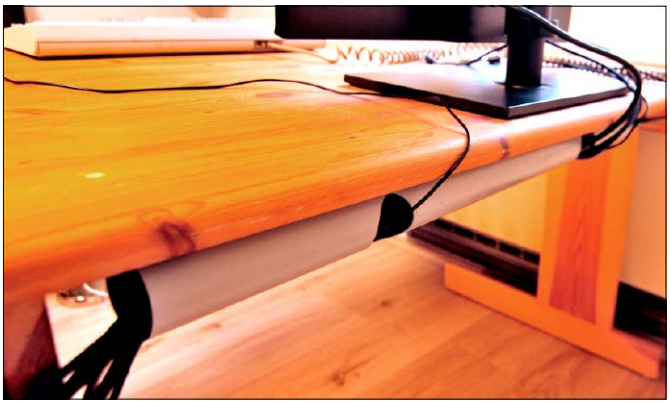
Steckerleisten mit einzeln schaltbaren Ports sind für Geräte ohne Powerknopf eine große Hilfe.

Kabelchaos am und unterm Schreibtisch

Am Schreibtisch brauchen neben PCs und Notebooks etliche Peripheriegeräte Strom- und Verbindungskabel. Die kaum vermeidbaren Kabelknäuel sind nicht schön und erschweren das Saugen und Wischen von Schreibtisch und Boden. Lösungen gibt es zuhauf, sollten aber gut überlegt sein: IT-Profis und Bastler wissen, dass in der IT die perfekte Lösung von heute vielleicht schon morgen gestrig ist. Wer daher häufig Hardware-, Peripherie-, Systemkonstellationen ändert, fährt mit dem unschönem, aber jederzeit zugänglichen Kabelwust vermutlich am pragmatischsten. Für Anwender mit relativ konstanter Ausstattung eignen sich folgende Lösungen:

Mit der Webrecherche nach **Kabelschacht** (auch „Kabelrinne", „Kabelkanal", „Kabelwanne") finden Sie zahlreiche, flexible, zum Teil abwinkelbare Produkte, die sich hängend unter der Tischplatte oder seitlich befestigen lassen. Je nach Material geht es ab 20 Euro auch Richtung dreistellig. Bastler können aber auch Rohrreste und PVC-Schläuche verwenden, die als Kabelkanal mit mehreren Öffnungen für die Kabel unter den Schreibtisch kommen – verschraubt oder nur geklebt. Das ist nicht schön, bleibt aber auf der unteren Stirnseite des Tisches praktisch unsichtbar.

Eher Richtung Kosmetik tendieren kleinere Lösungen wie **Kabelboxen.** Solche Boxen



Unterm Schreibtisch montiertes Kabelrohr: Zur Befestigung an der Unterseite der Arbeitsplatte dienen Holzschrauben und Unterlegscheiben.



Kleine Lösung für kleine IT: Eine Kabelbox kann eine Steckerleiste und einige kleinere Ladegeräte verräumen.

Quelle: amazon.de

verstecken typischerweise immerhin eine Steckerleiste mit sechs Ports, dazu das eine oder andere Netzteil und natürlich überschüssige Kabellängen. Die Preise liegen zwischen 10 bis 30 Euro (zum Beispiel *http://amzn.to/2cWWd66*)

Kabelclips (auch „Kabelhalter") und ähnliche Lösungen eignen sich erstens zur Kabelführung, zweitens als griffbereiter Standort für nicht ständig genutzte USB- oder Kopfhörerkabel. Die Clips werden in der Regel nur oben oder seitlich selbstklebend am Schreibtisch befestigt und halten dann drei bis sieben Kabel griffbereit an Ort und Stelle. Die Preise für ein Sortiment solcher Clips liegen unter zehn Euro.

Kabelhüllen oder **Kabelschläuche** mit Reißverschluss können mehrere Kabel sauber zu einem Strang zusammenfassen. Die einfachste Lösung für eine Verkabelung, die sich selten ändert, ist ein Spiralband, in das Sie die einzelnen Kabel einfädeln. Solche Bänder gibt es ab sechs Euro für zehn Meter (*http://amzn.to/1LWLxLs*). Eleganter sind Reißverschluss-Systeme wie jenes von Bluelounge (*http://amzn.to/1I4oq0N*, 25 Euro), das mit einem Y-Stück auch Verzweigungen erlaubt.

Kabelchaos in der Asservaten-Schublade

Im IT-Haushalt sammeln sich Ethernet-, Strom-, HDMI-, Sata-, USB-, Ladekabel aller Art, die als Ersatzlager dienen. Daneben lagern Lade- und Datenkabel obsoleter Geräte, die man noch nicht entsorgen wollte. Eine gewisse Ordnung in dieser Kabelsammlung, welche die Einzelteile separiert und die Verknotung verhindert, ist mit minimalen Aufwand möglich: Dazu reichen die typischen Kartonröhren, die von verbrauchten Küchenrollen übrigbleiben. Der stabile Karton nimmt auch widerspenstige Kabel auf. Während universelle Kabelsorten wie Ethernet oder HDMI keine Beschriftung benötigen, ist solche für spezielle Daten- oder Ladekabel von alten Einzelgeräten sehr zu empfehlen – etwa für Audioplayer, Dockingstations oder Smartphones. Dann wissen auch später noch, zu welchem Gerät die Kabel gehören.

Staub und Schmutz beseitigen

Wenn sich beim Auskippen einer PC-Tastatur (besser im Freien) eine kleine Zwischenmahlzeit präsentiert und Monitor oder Smartphone-Display des Rauchers nach gründlichem Wischen den Gelbstich verlieren, dann sind das Verbesserungen, die über pure Hygiene deutlich hinausgehen. Die Hardware selbst wird solche Verschmutzungen aber klaglos überstehen. Nicht mehr nur ein Hygieneproblem sind hingegen massiv verstaubte Ausbau-PCs und Platinenrechner sowie verstopfte Lüftungsschlitze von Notebooks. Dann drehen sich aktive Lüfter verlangsamt oder gar nicht mehr, und der CPU und Grafikkarte droht Überhitzung.

Auch die Kühlrippen passiver Kühlkörper verlieren ihre Wirkung, wenn dicke Staubschichten den Wärmeaustausch dämpfen.



Quelle: amazon.de

Griffbereit statt unterirdisch: Kabelclips arretieren Datenkabel in Griffnähe am Schreibtisch.

Staub auf den Leiterbahnen von Motherboards und Platinen kann im Extremfall sogar Kontakte überbrücken und Kurzschlüsse auslösen.

Abhilfe? Für Platinenrechner empfiehlt sich aus genannten Gründen immer ein Gehäuse, das den Großteil der Verschmutzung fernhält. Gelegentlich, mindestens einmal jährlich sollte ein Staubsauger in unterster Stufe Platinenrechner, Ausbau-PCs und Notebook-Lüftungsschlitze säubern. ■



Kostenlos in Ordnung: Die Kartonröhren von Küchenrollen sortieren die Kabelvorräte ohne Kabelsalat.

Fernwartung mit SSH

Wer sich mit dem Thema Homeserver beschäftigt, benötigt einige Grundlagenkenntnisse. Wir liefern diese und wichtigste Einsatzbeispiele für Linux-Systeme im Heimnetz. Hier stellen wir zunächst das wichtige Fernwartungs-Tool SSH vor.

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.

Dieser Artikel geht auf den stets unentbehrlichen Serverdienst Open SSH ein, der nicht nur zur Fernwartung dient, sondern auch unkomplizierten Datenaustausch und Softwareverteilung ermöglicht. Im folgenden Beitrag legen wir fundierte Grundlagen für die Einrichtung von (Apache-)Webdiensten und Datenservern mit Samba.

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:

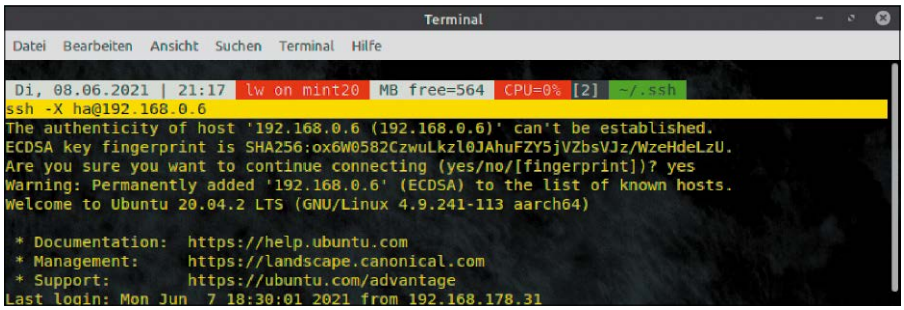
```
ssh ha@192.168.178.20
ssh ha@raspberry
```

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

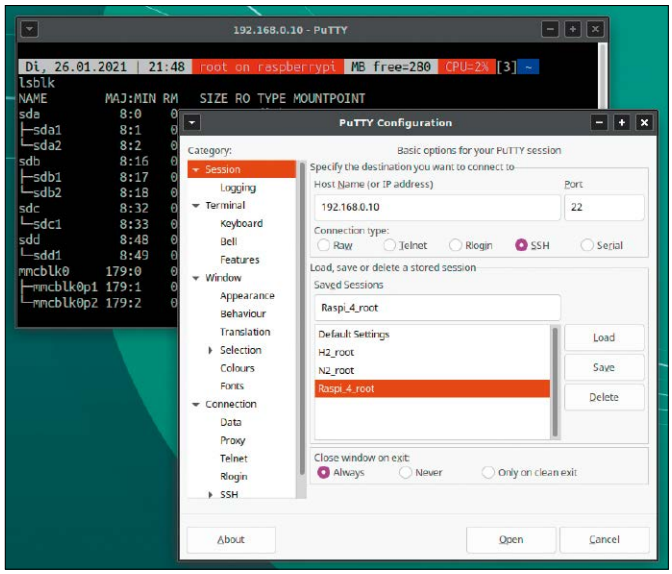
```
ssh -p 2222 ha@192.168.178.20
```

den expliziten Schalter „-p“.

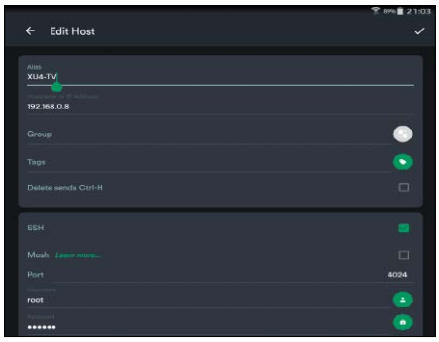
4. SSH-Terminal: Windows als Client

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.

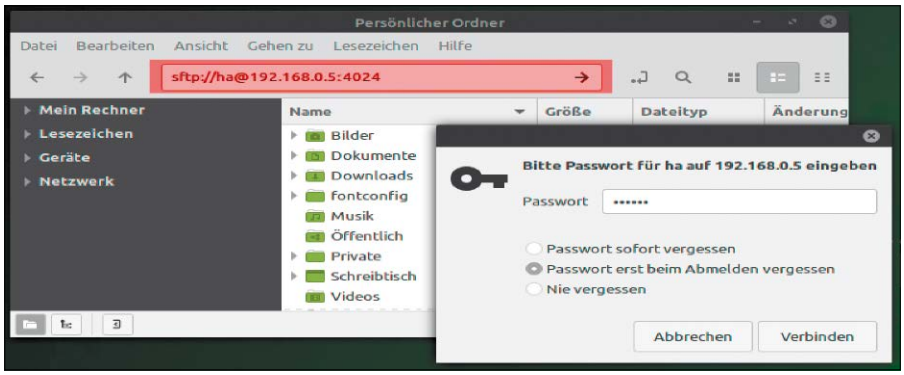
Die Basiskonfiguration ist einfach: Sie geben unter „Host Name“ entweder den Hostnamen oder die IP-Adresse des Servers an. Mit „Connection type: SSH“ und dem vorge-



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.

gebenen 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 (auf Heft-DVD) gibt es den Klon Kitty (*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 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

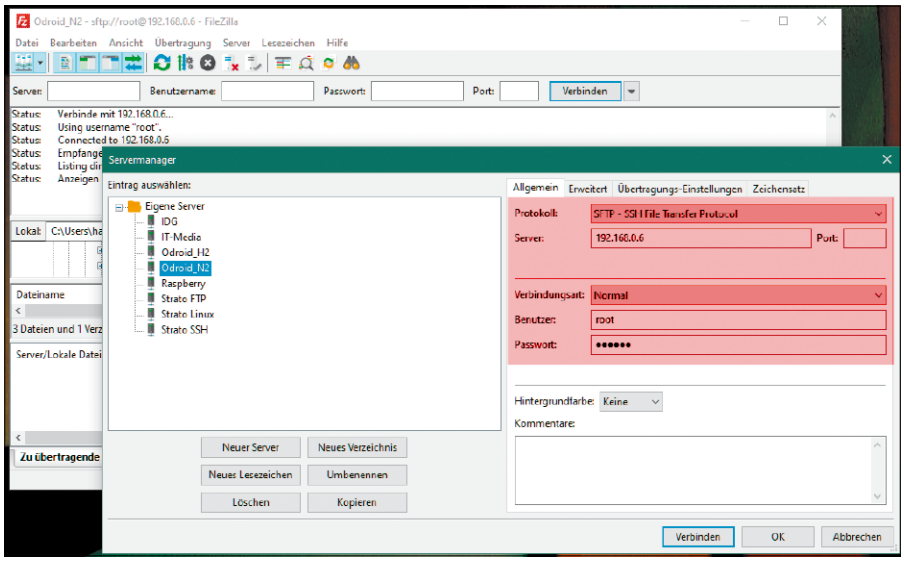
Die Eingabe eines kurzen Systemkennworts beim Start einer SSH-Sitzung ist an sich eine zumutbare Pflicht. Es gibt aber Szenarien, die – jenseits des Komfortaspekts – einen passwortlosen Zugang sinnvoll machen. Das gilt besonders für automatisierte Datensicherung (etwa mit rsync), die ohne Interaktion ablaufen soll, aber auch für den störungsfreien Start von ausgelagerter Software. Mit

```
ssh-keygen
```

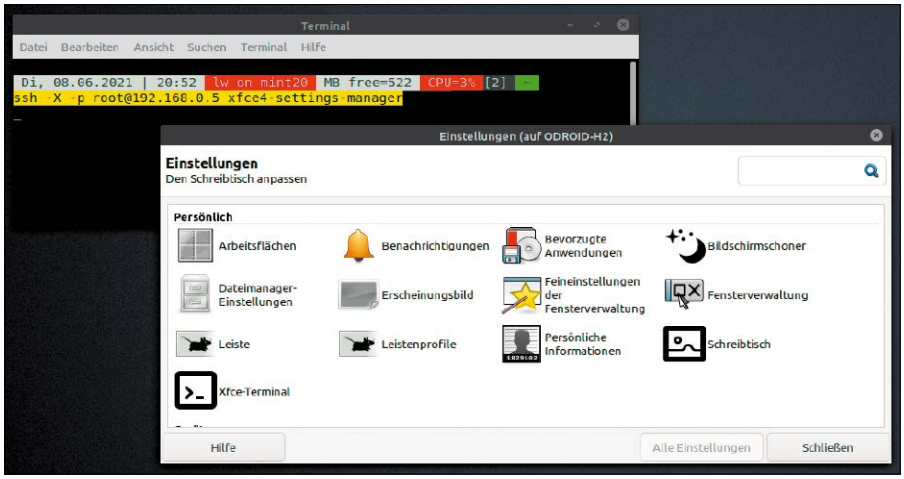
erstellen Sie zunächst auf Linux-Client-PC (nicht auf dem Server!) einen Zugangsschlüssel. Weitere Optionen sind dabei möglich, aber nicht zwingend. Der Schlüssel wird standardmäßig unter „~/.ssh/id_rsa.pub“ gespeichert, was Sie bestätigen müssen. Das ferner abgefragte Passwort zum Schutz des Schlüssels 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.



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.

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. ■

```
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
```

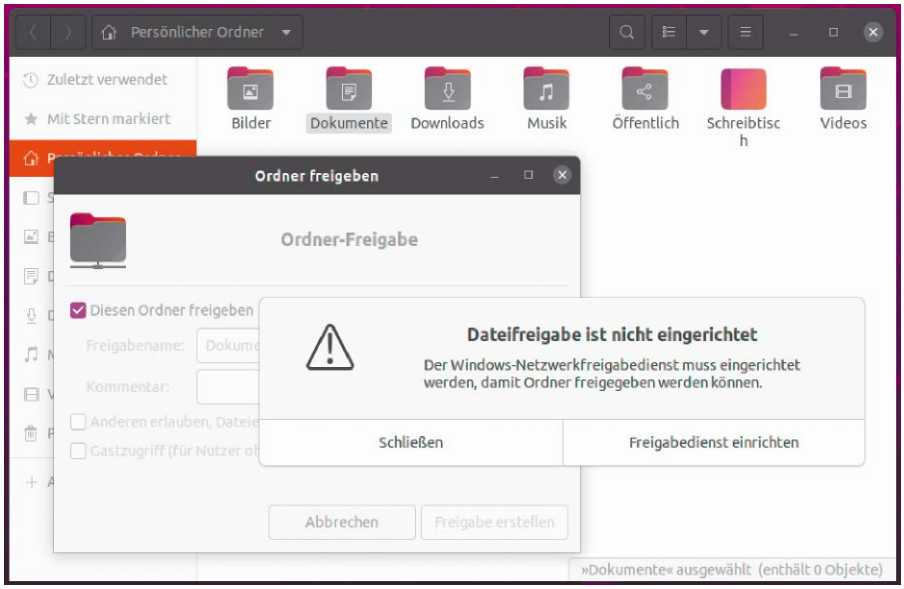
SSH ohne Kennwortabfrage: Der Clientrechner muss einen Schlüssel erzeugen (ssh-keygen), der dann zum Server kopiert wird (ssh-copy-id).

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 und Webanwendungen. Aber auch für diese sind Kenntnisse der manuellen Konfiguration von Vorteil. Wir liefern diese Grundkenntnisse.



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.

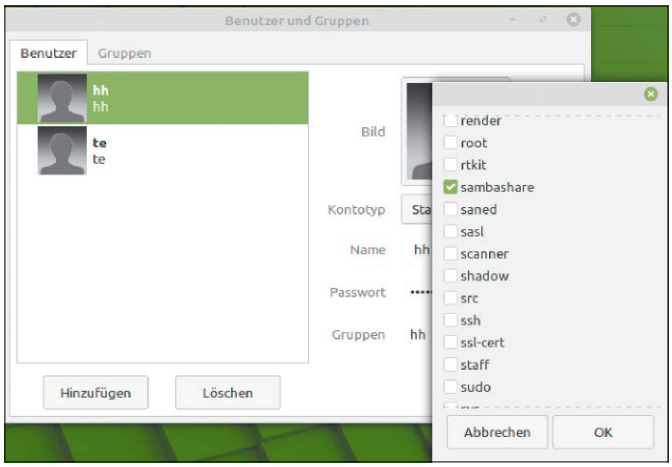
3. Samba-Konfiguration und globale Freigaben

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.

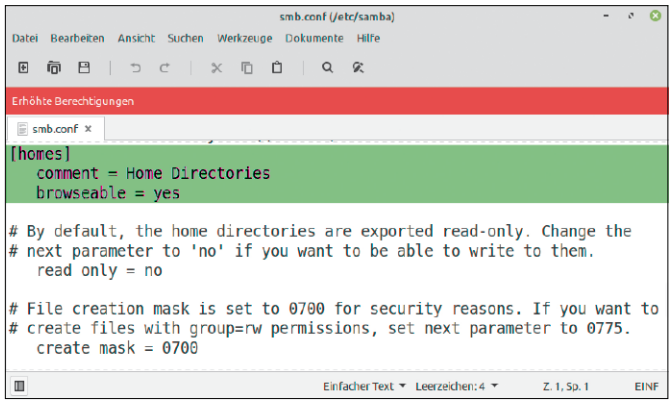
Änderungen in der „smb.conf“ werden wirksam, wenn Sie den Samba-Server die Konfigurationsdatei neu einlesen lassen:

```
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“.



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.

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

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 {} +
```

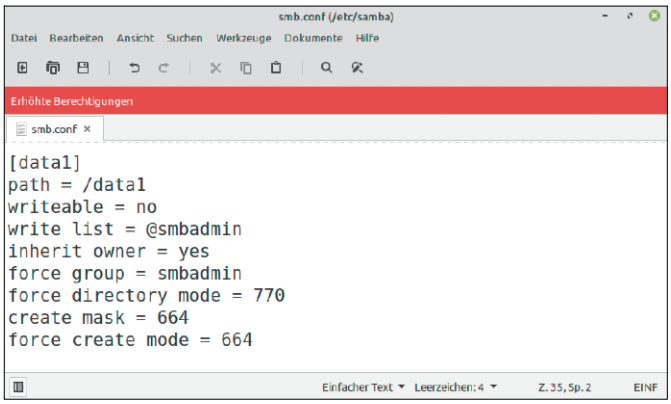
Die letzten drei Befehlszeilen arbeiten rekursiv, berücksichtigen also auch unter „/data1“ bereits vorhandene Ordner und Dateien. Die neu erstellte Gruppe „smbadmin“ – die Bezeichnung können Sie frei wählen – und der Besitzer „root“ erhalten Vollzugriff, andere Benutzer inklusive Gäste dürfen weiterhin 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
```

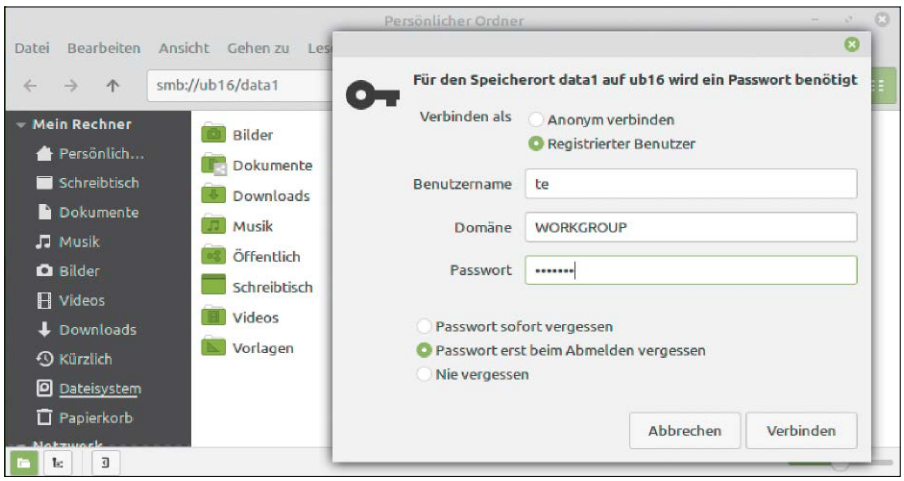
„write list = @smbadmin“ gewährt der Gruppe „smbadmin“ Schreibzugriff.

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

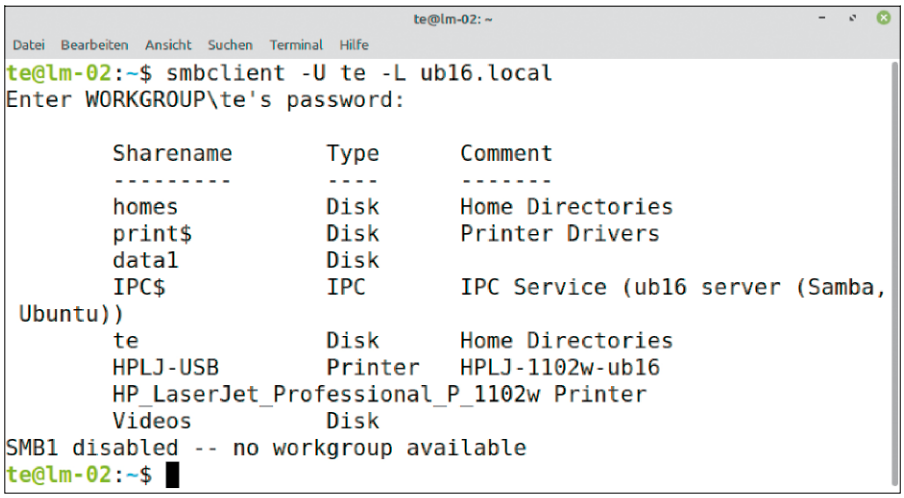
```
sudo serviceclt restart smbd
```

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. ■

Verlag

IT MEDIA PUBLISHING GMBH & CO KG

IT Media Publishing GmbH & Co. KG
Gotthardstr. 42, 80686 München
E-Mail: *info@it-media.de*
www.it-media.de

Chefredakteur: Sebastian Hirsch
(v.i.S.d.P – Anschrift siehe Verlag)

Druck: Mayr Miesbach GmbH
Am Windfeld 15, 83714 Miesbach

Inhaber- und Beteiligungsverhältnisse: Alleinige Gesellschafterin der IT Media Publishing GmbH & Co. KG ist die IT Media Publishing Verwaltungs GmbH, München, Geschäftsführer Sebastian Hirsch.

WEITERE INFORMATIONEN

Redaktion

Gotthardstr. 42, 80686 München
E-Mail: *info@it-media.de*
www.it-media.de
Chefredakteur: Sebastian Hirsch (verantwortlich für den redaktionellen Inhalt)
Stellvertretender Chefredakteur: Thomas Rau
Chef vom Dienst: Andrea Kirchmeier
Redaktion: Arne Arnold
Redaktionsbüro: MucTec (*hapfelboeck@googlemail.com*)
Freie Mitarbeiter Redaktion: Dr. Hermann Apfelböck, Thorsten Eggeling, David Wolski
Titelgestaltung: Schulz-Hamparian, Editorial Design / Thomas Lutz
Freier Mitarbeiter Layout/Grafik: Alex Dankesreiter
Freie Mitarbeiterin Schlussredaktion: Andrea Röder
Freier Mitarbeiter digitale Medien: Ralf Buchner
Herstellung: Melanie Arzberger

Einsendungen: Für unverlangt eingesandte Beiträge sowie Hard- und Software übernehmen wir keine Haftung. Eine Rücksendegarantie geben wir nicht. Wir behalten uns das Recht vor, Beiträge auch auf anderen Medien, etwa auf DVD oder online, zu veröffentlichen.

Copyright: Das Urheberrecht für angenommene und veröffentlichte Manuskripte liegt bei der IT Media Publishing GmbH & Co. KG. Eine Verwertung der urheberrechtlich geschützten Beiträge und Abbildungen, insbesondere durch Vervielfältigung und/oder Verbreitung, ist ohne vorherige schriftliche Zustimmung des Verlags unzulässig und strafbar, soweit sich aus dem Urheberrechtsgesetz nichts anderes ergibt. Eine Einspeicherung und/oder Verarbeitung der auch in elektronischer Form vertriebenen Beiträge in Datensysteme ist ohne Zustimmung des Verlags unzulässig.
Haftung: Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Die Veröffentlichungen in der LinuxWelt erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Auch werden Warennamen ohne Gewährleistung einer freien Verwendung benutzt.

Bildnachweis: AdobeStock – daboost, AdobeStock – hywards;
sofern nicht anders angegeben: Anbieter

Anzeigen

Anzeigenleitung:
Brigitta Reinhart
RMS GmbH
Tel. 089/464729
E-Mail: *breinhart@it-media.de*

Vertrieb

Vertrieb Handelsauflage:
MZV GmbH & Co. KG, Ohmstraße 1
85716 Unterschleißheim
Tel. 089/31906-0
Fax 089/31906-113
E-Mail: *info@mzv.de*
Internet: *www.mzv.de*
Druck: Mayr Miesbach GmbH
Am Windfeld 15, 83714 Miesbach
Tel. 08025/294-267

Verlag

IT Media Publishing GmbH & Co. KG
Gotthardstr. 42, 80686 München
E-Mail: *info@it-media.de*
www.it-media.de
Sitz: München, Amtsgericht München, HRA 104234
Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949:
Alleinige Gesellschafterin der IT Media Publishing GmbH & Co. KG ist die **IT Media Publishing Verwaltungs GmbH,** Sitz: München, Amtsgericht München, HRB 220269
Geschäftsführer: Sebastian Hirsch

ISSN 1860-7926







KUNDENSERVICE

LinuxWelt-Kundenservice für Einzelheft-Käufer:
DataM-Services GmbH
Postfach 9161
97091 Würzburg
Tel.: 0931/4170-177
Fax: 0931/4170-497
(Mo bis Fr, 8 bis 17 Uhr)
E-Mail: *idg-techmedia@datam-services.de*

LinuxWelt-Kundenservice für Abonnenten: Fragen zum bestehenden Abonnement / Premium-Abonnement, zum Umtausch defekter Datenträger, zur Änderung persönlicher Daten (Anschrift, E-Mail-Adresse, Zahlungsweise, Bankverbindung) bitte an
Zenit Pressevertrieb GmbH
LinuxWelt-Kundenservice
Postfach 810580
70522 Stuttgart
Tel: 0711/7252-233
(Mo bis Fr, 8 bis 18 Uhr)
Fax: 0711/7252-333
E-Mail: *linuxwelt@zenit-presse.de*
Erscheinungsweise:
6x jährlich

Jahresbezugspreise:
LinuxWelt mit DVD:
53,50 € (D), 59,50 € (A, CH, Benelux) inkl. Versandkosten

Bankverbindung für Abonnenten:
Postbank Stuttgart, IBAN
DE56 6001 0070 0029 0547 04, BIC PBNKDEFFXXX

Sie können Ihr Abonnement jederzeit zur nächsten Ausgabe kündigen.
Bestellungen können innerhalb von 14 Tagen ohne Angabe von Gründen in Textform (zum Beispiel Brief, Fax, E-Mail) oder durch Rücksendung der Ware widerrufen werden.

LINUX WELT

Mini-Angebot!

Satte **33 %** gespart!

3x LinuxWelt inkl. Prämie*



Als Print-Abonnent der **LinuxWelt** erhalten Sie Ihre Ausgabe in der PC-WELT App **IMMER GRATIS** inklusive DVD-Inhalte zum Download.

Jetzt testen:

3 x LinuxWelt als Heft frei Haus mit Gratis-DVD +
3 x LinuxWelt direkt aufs Smartphone & Tablet mit interaktivem Lesemodus +
10,- € Geldprämie*

=18,- € (anstatt 25,50 EUR)

Jetzt bestellen unter
www.pcwelt.de/linuxwelt oder per Telefon: 0711/7252233 oder ganz einfach:

1. Formular ausfüllen **2. Foto machen** **3. Foto an linuxwelt@zenit-presse.de**

Ja, ich bestelle das LinuxWelt Mini-Angebot für 18,- € und erhalte 3 Ausgaben inkl. Prämie

Möchten Sie die LinuxWelt anschließend weiter lesen, brauchen Sie nichts zu tun. Sie erhalten die LinuxWelt für weitere 6 Ausgaben zum aktuellen Jahresabopreis von z.Zt. 53,50 EUR. Danach ist eine Kündigung zur übernächsten Ausgabe jederzeit möglich.

ABONNIEREN

Vorname / Name
Straße / Nr.
PLZ / Ort
Telefon / Handy
Geburtstag TT MM JJJJ
E-Mail

BEZAHLEN

○ Ich bezahle bequem per Bankeinzug. ○ Ich erwarte Ihre Rechnung.

Geldinstitut
IBAN
BIC
Datum / Unterschrift des neuen Lesers

LWPM062018

* wird mit Abo-Preis verrechnet

LinuxWelt erscheint im Verlag IT Media Publishing GmbH & Co. KG, Gotthardstraße 42, 80686 München, Registergericht München, HRA 104234, Geschäftsführer: Sebastian Hirsch.
Die Kundenbetreuung erfolgt durch ZENIT Pressevertrieb GmbH, Postfach 810580, 70522 Stuttgart, Geschäftsführer: Joachim John



Affordable Business Allrounder

TUXEDO Aura 15 - Gen2

AMD Ryzen 7 5700U
8 Cores | 16 Threads

USB-C 3.2 Gen2
DisplayPort 1.4 & Power Delivery

1,99 cm | 1,65 kg
Thin & Lightweight

4G / LTE
Mobile high-speed web access

100% Linux

5 Jahre Garantie

Lifetime Support

Gefertigt in Deutschland

Deutscher Datenschutz

Support vor Ort

TUXEDO COMPUTERS 18 JAHRE JUBILÄUM

tuxedocomputers.com