LINUX WELT XXL

SONDERHEFT XXL
2/2023 Mai – Juli
€ 12,90 Schweiz sfr 25,80
Österreich, Benelux € 14,40



NEU!
196 Seiten!

Linux statt Windows

Das Umsteiger-Handbuch 2023

Einfach auf Linux umsteigen
Das beste System finden · Linux richtig installieren · Software laden · Alles konfigurieren · Backup einrichten …

Linux im Praxiseinsatz
Linux & Windows parallel nutzen · System einfacher bedienen · Paketmanager ausreizen · Sicherheits-Tools nachrüsten …

Hilfe bei Problemen
Bootprobleme lösen · Netzwerkfehler beseitigen · Treiber finden · Daten retten · System optimieren …

PLUS: Linux für alte Rechner



SPECIAL

Linux auf dem Stick
→ Multiboot-USB-Stick einsetzen
→ Systeme & Daten mitnehmen
→ Linux per Stick retten

NEU: 2 DVDs

DVD im Heft

Multiboot-DVD

Mega Umsteiger-DVD

Linux Mint 21.1

- LinuxWelt Rettungssystem 9.4
- Elementary OS 7
- Garuda Linux KDE

33 Handbücher für Linux



Extra Download-DVD

Bootfähige **Service-Systeme**

- **Rescuezilla** Backup und Restore
- **Wifislax** WLAN-Test
- **Systemrescue** Rettungssystem
- **Gparted Live** Partitionierer



Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

PC-WELT

Virtuelle PCs & Multiboot



Jetzt am Kiosk!

Sonderheft
für nur
9,90 €

Auf Download-DVD: Das große Komplett-Paket

Bestellen unter
www.idgshop.de/tech 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 SH 4/23 Virtuelle PCs & Multiboot für nur 9,90 €.

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

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

Tschüss Microsoft, hallo Linux!

Microsoft sorgt derzeit dafür, dass immer mehr Anwender auf Linux umsteigen. Denn der Konzern aus Redmond vergrault seine Nutzer mit Windows 11 jeden Monat ein bisschen mehr. Wer das neue Windows auf älteren Rechnern installiert hat, bekommt nun eine Warnung angezeigt. Andere Windows-Nutzer schaffen das Update auf die neue Version gar nicht erst, weil ihre Hardware angeblich zu schwach ist. Nicht nur in solchen Fällen heißt die beste Alternative: Linux statt Windows!

Das Umsteiger-Handbuch 2023 bietet aktuelle Infos über das kostenlose, sichere und stabile Linux. Im Heft finden Sie ein spannendes Duell zwischen Windows und Linux, bei dem beide Systeme punkten können. Ab Seite 12 erfahren Sie, warum Linux am Ende die bessere Wahl ist. Und natürlich finden Sie viele Tipps für den Umstieg auf Linux und für die Praxis.

Auf der beiliegenden Heft-DVD nutzen Sie das einsteigerfreundliche Linux Mint als Livesystem. Sie können Mint einfach von der DVD booten und gefahrlos ausprobieren, bevor Sie sich für eine Installation entscheiden. Einfacher geht es kaum.

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 34,6 Prozent und erhalten zudem eine Geldprämie im Wert von 10 Euro.
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.
34,6 Prozent sparen plus Geldprämie: Mit dem Mini-Abo zahlen Sie nur 17,50 statt 26,75 Euro. Und zusätzlich erhalten Sie eine Geldprämie im Wert von 10 Euro!
Alle Infos: Das Mini-Abo können Sie ganz einfach über *www.pcwelt.de/linuxwelt* 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.

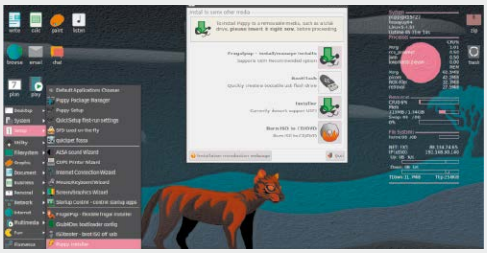




Umsteiger-Handbuch

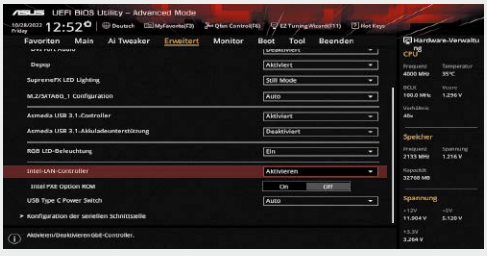
Damit der Umstieg auf Linux leichtfällt, zeigen wir in unserem Schwerpunkt „Linux mit Windows“ nicht nur, was Linux besser kann, sondern erklären auch, wie Sie Linux zunächst parallel zu Windows installieren. **S. 12**

Immer mobil: Linux auf dem Stick S. 74



Linux läuft problemlos auf einem USB-Stick. So haben Sie Ihr System ebenso immer dabei wie ein gutes Rettungssystem.

Pannenhilfe für Linux und Hardware S. 178



Auch Linux macht mal Zicken. Unsere Tipps bei Problemen mit dem System sowie mit Hard- und Software helfen dann weiter.

Im Heft & auf DVD

6 Linux passt immer
Die Heft-DVD lädt zum Ausprobieren von Linux ein und präsentiert drei Distributionen sowie das LinuxWelt-Rettungssystem

8 Die Heft-DVD: Distributionen
Sorgfältige ausgewählte aktuelle Linux-Systeme sollen als formidable Zweitsysteme Windows ergänzen und zum Umstieg einladen

Linux mit Windows

12 Linux & Windows: Im Duell
Die beiden Betriebssysteme treten in 16 Kategorien gegeneinander an

18 Parallelinstallation: Linux neben Windows
Optimierte Koexistenz: Das müssen Sie beim Parallelbetrieb beachten

22 Linux oder Windows virtuell
Hausherr und Gast: Die Rollen bestimmen Sie je nach Zielsetzung

26 Teamwork im Netzwerk
Produktiv: Das Netzwerk verteilt Aufgaben an Windows oder Linux

Wichtige Linux-Systeme

30 Das neue Linux Mint 21
Linux Mint 21 distanziert sich weiter von seiner Ubuntu-Systembasis

34 Linux Mint 21: Upgrade, Installation, Einrichtung
So bringen Sie Linux Mint 21 auf Ihr Zielgerät

38 Linux Mint 21: Cinnamon-Tuning
Optimierungsoptionen für Cinnamon und Dateimanager Nemo

41 Neu in Ubuntu 22.04 LTS
Kernel – System – Software – Desktops

46 Ubuntu 22.04 LTS: Installationen & Upgrades
So bringen Sie Ubuntu 22.04 auf jeden Rechner

50 Ubuntu 22.04 LTS: Einrichtung und Optimierung
Ein Ratgeber für erste Systempflichten und Desktopanpassung

54 Ubuntu 22.04 LTS: Systemoptimierung
So machen Sie aus dem eleganten Ubuntu ein funktionales System

58 Ubuntu-Troubleshooting
So beseitigen Sie die größten Mängel von Ubuntu 22.04

Linux für alte Hardware

62 Alte Rechner neu belebt
Wo sich Recycling lohnt: Viele, aber nicht alle Altgeräte eignen sich für neue Rollen unter Linux

66 Linux für Oldies
Desktop- und Serversysteme: Diese Distributionen sind spezialisiert auf ältere Hardware

70 Alte Datenträger nutzen
Kleine, ältere SSDs & Festplatten: Nur SSDs haben Jobgarantie

72 Mac-Upcycling mit Linux
Linux auf alten Macs: Eine schlanke Distribution macht langsame Apple-PCs wieder flott

Standards

3 Editorial
194 Impressum

Linux-Wissen für Einsteiger

96 **Dateien und Ordner organisieren**
Kopieren, Verschieben, Benennen, Organisieren: So arbeiten Sie effektiver mit Dateimanager, Terminal und interessanten Hilfstools

100 **Backups: Schnell, sicher & bequem**
Werkzeuge und Strategien: So vereinfachen Sie sich die Pflichten der Datensicherung

104 **Softwareeinstellungen sichern und übertragen**
Export und Import: So übertragen Sie Softwareeinstellungen von einem System zum nächsten

108 **Linux-Konfigurationsdateien**
Grundlagen – Tabelle – Tipps: So verwalten Sie die Linux-Konfiguration komfortabler

112 **Flatpak & Snaps: Tipps und Tricks**
Containerformate: Das sind die wichtigsten Kommandos für (De-) Installation und Optimierung

116 **Paketmanager und Paketkonflikte**
Ursachen von Paketkonflikten und ihre Lösung: Was tun, wenn Paketmanager wie apt streiken?

120 **Durchblick im Kernel-Chaos**
Konservative LTS-Distribution oder Rolling Release: Was tun, wenn Hardware jüngere Kernel fordert?

122 **Linux-Systeme vereinfachen**
So lassen sich Linux-Systeme unter Verzicht auf hohe Sicherheitsansprüche deutlich vereinfachen

126 **Apache für Einsteiger**
Mit diesen Grundlagen zur Apache-Konfiguration bauen Sie sich Ihre ersten Webanwendungen

Linux für den USB-Stick

74 **Mobile Daten mit Linux**
Formatierung, Verschlüsselung, mobiles Home: Linux bietet mehr als einfachen Datentransport

78 **Mobile Linux-Livesysteme**
Live, Persistenz oder Maßanzug: So nutzen Sie USB-Sticks für Reparatur- oder Zweitsysteme

81 **Der Multibootstick**
Livesystem-Suite: Tools für Linux und Windows arrangieren den perfekten mobilen Werkzeugkasten



84 **Installationen auf dem USB-Stick**
Nachhaltige Zweitsysteme: Reguläre Installation auf USB bietet den vollen Desktopkomfort

86 **Mobil-Tipps & Szenarien**
Der richtige Stick: So erzielen Sie mehr Leistung und Bootsicherheit und erweitern die Mobiloptionen

88 **Die schnellsten Mobilsysteme (für USB)**
Distributionen für USB-Sticks: Die richtigen Systeme bieten Performance und Anpassungskomfort

92 **Multiboot: Rettungssysteme & Systeminstallation**
Neue Bootoptionen: Wie Sie Linux- und Windows-Images von USB oder von Festplatte starten

Sicherheit & Datenschutz

130 **Basics: Sicherheitsregeln**
Systemschutz, Internetsicherheit, Datenschutz: Eigene Maßnahmen

134 **Home-Verschlüsselung für Ubuntu/Mint**
Ersatz für veraltetes Ecrypt FS: Gocrypt sorgt für Verschlüsselung des Home-Verzeichnisses

136 **NAS/Fritzbox absichern**
Weniger ist sicherer: Warum Sie nicht alle Bonusdienste von NAS-Geräten nutzen sollten

138 **VPN: Schritt für Schritt**
Wie Sie VPN einrichten und was Sie davon erwarten dürfen

142 **Firewall & Dienste-Check**
So erkennen Sie offene Ports und die verantwortlichen Dienste oder Programme

144 **Achtung: Einbruch!**
Spezialtools wie Lynis und Tripwire melden Manipulationen

146 **Wichtige Sicherheitstools**
Ein Plädoyer für Firewall, Passwortmanager, Virenscanner, Apparmor

150 **Tails 5.7: Anonym im Web**
Rigoros spurlos: So nutzen Sie das Livesystem mit Datenschutzfokus

Netzwerken mit Linux

152 **Durchblick im Netzwerk**
Was Linux nicht anzeigt: So ermitteln Sie, was im Netz läuft

156 **Netzwerkhardware**
Netzwerkausbau und Optimierung: Diese Hardware brauchen Sie für ein schnelles Netzwerk

160 **Serverlösungen für Linux**
Serverdienste: Clientgeräte und Anspruch bestimmen die Auswahl

164 **Netzwerktipps & -tools**
So vereinfachen und optimieren Sie den Zugriff auf Netzgeräte

168 **Nextcloud im Heimnetz**
Die Nextcloud-Dienste: Was sich für den Intraneteinsatz lohnt

172 **Fritzbox-Geheimnisse**
Fritz-OS-Hacks und Fritzbox-Hardware: Im AVM-Router steckt mehr und weniger, als Sie vermuten

175 **Remotedesktop mit X2go**
X2go statt VNC: X2go ist langsamer, anspruchsvoller, aber zuverlässig

176 **Google-Fonts online/offline**
Vorsicht mit Google-Schriften: So schützen Sie sich vor Abmahnung und Schadensersatzforderung

Pannenhilfe für Linux

178 **Hardware und Treiber**
Problemlösungen für inkompatible Hardware: So vermeiden, umgehen und korrigieren Sie Hardwareärger

182 **Boot- und Startprobleme**
Wie Sie Hardware- und Bootmanager-Probleme unterscheiden und beheben

184 **Netzwerkstörungen**
Hardware oder Konfiguration? Mit strategischer Suche finden Sie die Ursache von Netzwerkstörungen

186 **Instabile Software**
So analysieren Sie Logdateien und Fehlermeldungen beim Aufruf

188 **Datenrettung**
Forensische Methoden & Werkzeuge zur Datenrettung

190 **Wenn der Desktop streikt**
Keine Oberfläche? Viele Ursachen!

192 **Zugriffs- & Rechteprobleme**
Wie Sie Rechtekonflikte vermeiden und korrigieren

Linux passt immer

Auf Servern sowie PCs ist Linux schon länger zu Hause und auch Notebooks stellen kein Problem mehr dar. Dieses Sonderheft will dazu einladen, Linux auf einem eigenen Rechner zu installieren – und diesen so noch ein paar Jahre zu betreiben.



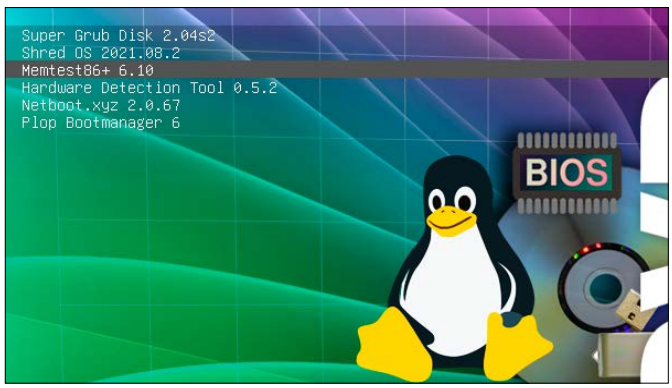
VON DAVID WOLSKI

Windows, Mac-OS oder gar Linux? Keine schwere Entscheidung: Heute stellt sich Anwendern die Frage nicht mehr, wie ein harter Übergang von Windows oder Mac-OS zu Linux aussehen könnte. Denn in einer Schublade findet sich oft noch ein älterer Laptop, der kein aktuelles Windows 11 mehr stemmen kann und auch mit Windows 10 keine gute Figur mehr macht. Diese Geräte laufen mit Linux meist noch tadellos einige Jahre. Es sind auch dann nicht die schnellsten Systeme, doch sogar manche Oldtimer mit Core-2-Duo-Prozessor von Intel bleiben mit der richtigen Linux-Distributionen benutzbar und vor allem auch sicher. So kann ein älterer Zweit-PC oder Laptop die eigenen Systeme erst mal um Linux ergänzen, das so seine Stärken zeigen kann und ganz entspannt, jenseits der Hektik der täglichen IT zum Experimentieren einlädt.

Umstieg oder Einstieg leicht gemacht

Es ist aber nicht so, dass Linux vornehmlich ein Bastel- und Experimentiersystem wäre. Selbstverständlich gibt es für Linux eine Menge Tools zur Softwareentwicklung mehr als für Windows. Aber das ist nur eine der vielen Eigenschaften des freien Betriebssystems – und ein wichtiges Erbe aus den frühen 90er-Jahren, als der Linux-Kernel als wichtigste Komponenten entstand. Mittlerweile sind Befehlszeilenkenntnisse bei der Installation oder der Verwendung des Systems nicht mehr zwingend. Nützlich zwar, aber nicht mehr eine unumgängliche Voraussetzung. Denn mit aktuellen Desktops ist auch Linux sehr einladend und intuitiv. Drei der Linux-Distributionen auf Heft-DVD sind genau nach diesen Kriterien ausgewählt, präsentieren Arbeitsumgebungen, die mal für Einsteiger, mal für Fortgeschrittene interessant sind. Denn das ist einer der weiteren Vorteile von Linux: Die enorme Anpassungsfähigkeit und Flexibilität, mit der die tonangebenden Linux-Distributionen jeweils eine bestimmte Zielgruppe ansprechen und deren jeweiligen Anforderungen gerecht werden.

Dass Windows weiterhin auf dem Desktop Marktführer ist und noch einige Weile bleiben wird, steht außer Zweifel. Tatsächlich ist es aber gar nicht so einfach, die Verbreitung von Linux zu quantifizieren. Nach einer Erhebung der Frage-Antwort-Website



Die Extras & Tools im Multibootmenü: Neu hinzugekommen ist seit der letzten Ausgabe das Speichertestprogramm Memtest86+ 6.10 in einer frischen Version. Auch Netboot.xyz 2.0.67 ist aktualisiert.

Stackoverflow unter den eigenen Anwendern, zumeist Softwareentwickler, gibt es nun belastbares Zahlmaterial: Während 49 Prozent der Entwickler Windows für die Arbeit verwenden, nutzen 40 Prozent dafür Linux und 33 Prozent der Befragten geben Mac-OS als Betriebssystem für die Arbeit an. Bei vielen IT-Professionals läuft selbstverständlich mehr als ein Betriebssystem und Linux ist nach dieser Erhebung oft eines davon.

Ausprobieren: Die Heft-DVD will zum Ausprobieren von Linux einladen und präsentiert nach dem Boot auf einem Rechner mit 64-Bit-CPU von Intel oder AMD ein Bootmenü, das drei Distributionen sowie unser Rettungssystem zur Auswahl stellt. Das installierte Betriebssystem bleibt dabei unangetastet und Linux Mint, Elementary OS und Garuda Linux können erst mal zeigen, wie deren Desktop aussieht, bevor es dann später eventuell an eine Installation geht. Die nächsten vier Seiten präsentieren die Systeme im Detail.

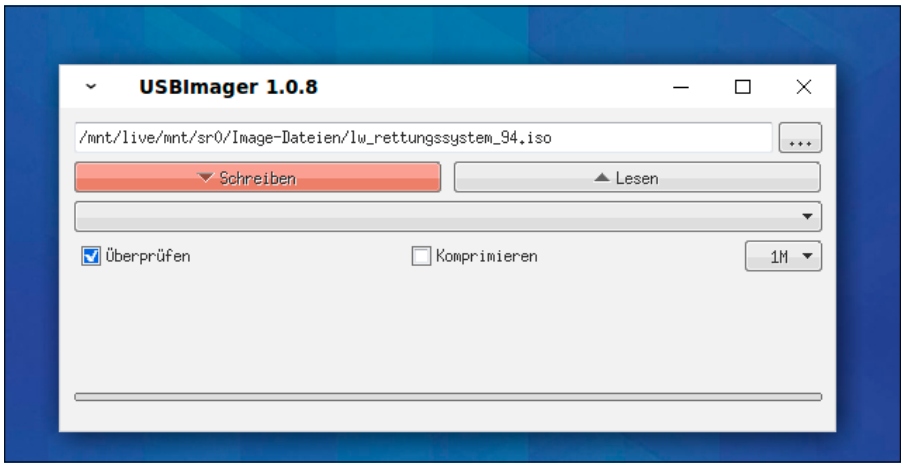
Auf den Stick: Von USB-Laufwerken booten

Optische Laufwerke sind in modernen Desktop-PCs kaum noch und in Notebooks gar nicht mehr zu finden. Der Inhalt der Heft-DVD ist deshalb auch für USB-Sticks geeignet, bootet auch dann im Bios-Modus älterer PCs oder im Uefi-Modus aktueller Rechner. Ein willkommener Nebeneffekt: Die Systeme startet von USB deutlich flotter als von dem vergleichsweise langsamen optischen Datenträger. Alle vier Systeme sind auch jeweils als originalgetreue ISO-Datei auf der DVD, im Unterverzeichnis „Image-Dateien".

Aus jeweils diesen Dateien ist im Nu ein bootfähiger USB-Stick erstellt: Zur Übertragung eignet sich das grafische Tool USB Imager 1.08, ein Open-Source-Programm für Linux, Windows und Mac-OS mit deutschsprachiger Oberfläche (auf Heft-DVD, Download aller Versionen unter *https://gitlab.com/bztsrc/usbimager*).

Extras und Tools

Zur Reparatur und Fehleranalyse bietet das Multibootmenü der DVD in der Rubrik „Extras und Tools" eine Reihe an kleineren Livesystemen und startfähigen Werkzeugen. Mit von der Partie ist die Super Grub Disk 2, die installierte Linux-Systeme, aber auch Windows booten kann, auch wenn deren Bootloader überschrieben wurde. Der Plop Bootmanager hilft dabei, von USB-Laufwerken zu booten, auch wenn das Bios dies nicht unterstützt. Das Hardware Detection Tool (HDT) zeigt die Ausstattung eines Rechners. Memtest 86+ 6.10 testet den Speicher eines PCs und das neue Shred-OS 2021.8 löscht mechanische Festplatten.



Der USB Imager, hier unter Linux: Das kleine Open-Source-Programm schreibt die ISO-Dateien von Linux-Distributionen und Livesystemen auf USB-Sticks und kann die Daten auch gleich überprüfen.

Download-DVD

Zusätzlich zur Heft-DVD bietet diese Ausgabe eine Download-DVD mit den vier Servicesystemen Rescuezilla für Backup und Restore, Wifislax für WLAN-Tests, Systemrescue als Rettungssystem und Gparted Live als Partitionierer. Sie finden das ISO der DVD unter *https://github.com/LinuxWelt*. ■

AUF DVD



Distributionen

8 Linux Mint 21.1 „Vera" (64 Bit)
Das aktuelle Mint mit Detailverbesserungen, Cinnamon-Desktop und ohne Snap-Pakete. Die Basis ist hier ein Ubuntu 22.04.1.

9 Elementary OS 7
Die ansehnliche Linux-Distribution basiert ebenfalls auf Ubuntu (22.04) und liefert aber den eigenen Desktop Pantheon, der an Mac-OS X orientiert ist.

10 Garuda Linux KDE Light
Für Fortgeschrittene: Eine Spielart von Arch Linux, das ursprünglich für Gamer geschaffen wurde und jetzt auch auf Desktops eine gute Figur macht.

11 LW-Rettungssystem 9.4
Der gut gefüllte Werkzeugkasten aus der LinuxWelt-Redaktion für Windows-Pannen und Linux-Notfälle bringt viele neue Tools.

Extras und Tools
Super Grub Disk, Memtest, HDT, Netboot.xyz, Shred-OS und der Plop Bootmanager booten von DVD.

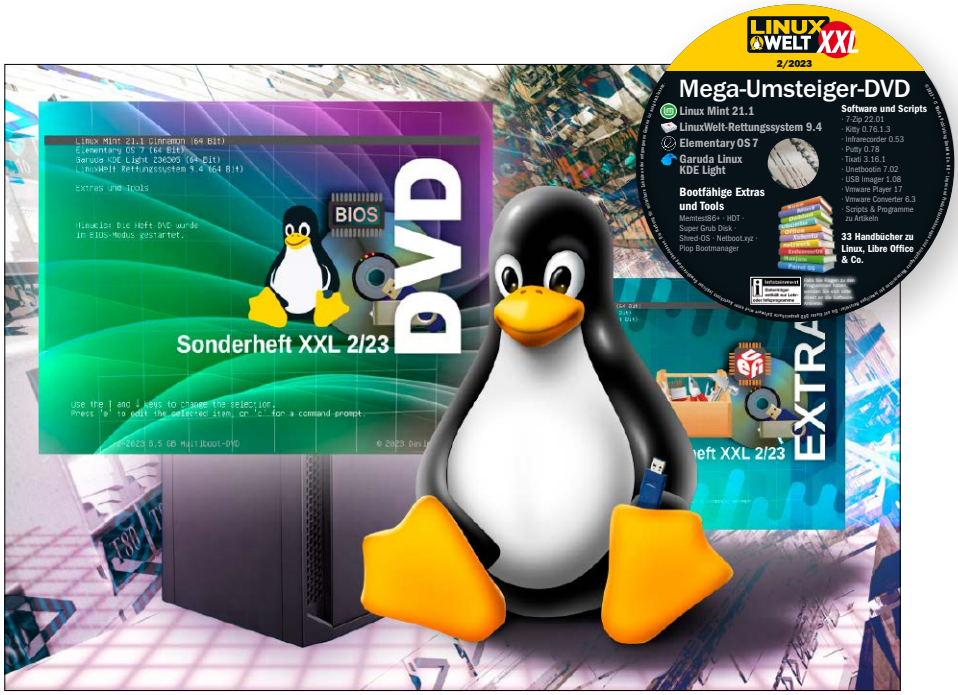
Software und Shell-Scripts
Vmware Player und Vmware Converter sind nur zwei der Highlights der Softwaresammlung zu den Artikeln im Heft.

Das LinuxWelt-Bücherregal
Für diese Ausgabe haben wir 33 Handbücher (PDFs) zu Linux, Open Source und Libre Office zusammengestellt, deren Lizenzen oder Autoren die Verbreitung über die DVD erlauben.

Heft-DVD: Eine Scheibe Linux

Eine sorgfältige Auswahl aktueller Linux-Systeme: Vier Mal Linux zum Ausprobieren, Installieren und als Problemlöser. Der Schwerpunkt liegt auf Distributionen, die als formidables Zweitsystem Windows ergänzen und zum Umstieg einladen.

VON DAVID WOLSKI



Die Extra-DVD zum Sonderheft: Hier warten vier weitere Linux-Systeme in einem Multibootmenü. Der Schwerpunkt liegt hier bei Reparatur, Administration und Sicherheits-Checks im WLAN.

Ganz gleich, ob das bislang hauptsächlich genutzte Betriebssystem Windows oder Mac-OS ist: Berührungsängste mit Linux sind 2023 nicht mehr angebracht. Zwar ist es nicht lange her, als es noch eine Menge technisches Verständnis und Wissen um die Eigenschaften von Unix brauchte, um allein einen Desktop unter Linux mit optimaler Auflösung und Hardwarebeschleunigung auf den Bildschirm zu zaubern. Diese Zeiten sind vorbei – und wir wagen sogar zu behaupten, dass ein Linux-System aus dem Umkreis Ubuntus heute sogar einfacher und schneller als Windows installiert ist. Die randvoll gefüllte Dual-Layer-DVD (8,5 GB) liefert dazu eine sorgfältige Auswahl an insgesamt drei Linux-Distributionen und ein Livesystem (alle 64 Bit) aus der LinuxWelt-Redaktion, die dabei sowohl Anfängern als auch Fortgeschrittenen entgegenkommen.

Linux Mint 21.1

Zwar ist Linux Mint eine inoffizielle Ausgabe aus dem Kreis der Ubuntu-Systeme, aber es kümmert sich mit seinen gewachsenen Modifikationen speziell um die Anforderungen neuer Linux-User. Die vorliegende Version von Linux Mint basiert auf Ubuntu 22.04.1 LTS und hat zudem Neuerungen von den Mint-Entwicklern an Bord. Neu ist etwa die Ausgabe des Desktops Cinnamon mit Fehlerbehebungen. Die Entwickler geben an, dass Cinnamon 5.6 mit leicht überarbeiteten Themes ausgestattet ist. Es gibt neue Sounds, der Dateimanager ist dem Windows-Explorer im Aussehen ähnlicher und auf dem Desktop werden standardmäßig keine Symbole platziert. 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. Im Abschnitt „Details“ ist angegeben, ob es sich beim ausgewählten Programmpaket um einen Flatpak-Container handelt. Flatpaks bringen ihre eigene Systemumgebung mit und laufen isoliert von Systembibliotheken, um eventuelle Konflikte zu vermeiden. Das hat den Vorteil, dass mit Linux Mint 21.1 jetzt auch neuere Gnome-Programme installiert werden können, die mit den älteren Bibliotheken des Cinnamon-Desktops nicht kompatibel sind. Snaps von Ubuntu werden nicht unterstützt. Wieder enthalten sind die X-Apps von Mint. Diese sind nicht mehr nur Mint-Abspaltungen bekannter Linux-Programme mit neuem Namen, sondern 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.

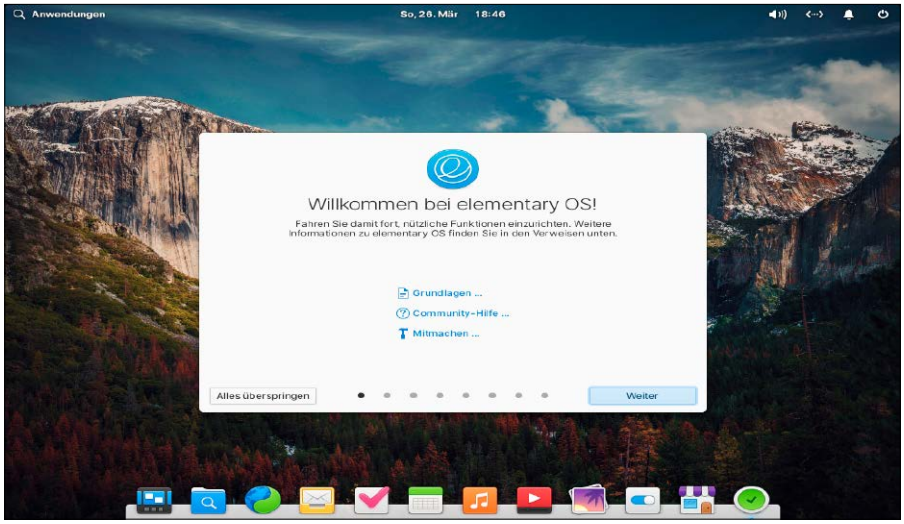
Die Notizblock-Anwendung Sticky Notes für den Desktop hat eine Suchfunktion erhalten. Von diesen Entwicklungen abgesehen, entspricht Linux Mint 21.1 weitgehend dem Stand von Ubuntu 22.04.1 und bringt beispielsweise Libre Office 7.3 mit, aber auch den neuesten Firefox.

Auch Linux Mint 21.1 ist eine LTS-Ausgabe mit Updates bis April 2027. Linux Mint 21.1 Cinnamon liegt als leicht installierbares Livesystem vor und das sehr komfortable Installationsprogramm entspricht jenem von Ubuntu 22.04.1.

Website: *www.linuxmint.com*
Dokumentation:
www.linuxmint.com/documentation.php

Elementary OS 7

VON DAVID WOLSKI



Der Charme von Mac-OS: Der sehenswerte Desktop Pantheon kommt auch mit hochauflösenden Bildschirmen klar. Elementary OS 7 darf von sich behaupten, den elegantesten Linux-Desktop zu haben.

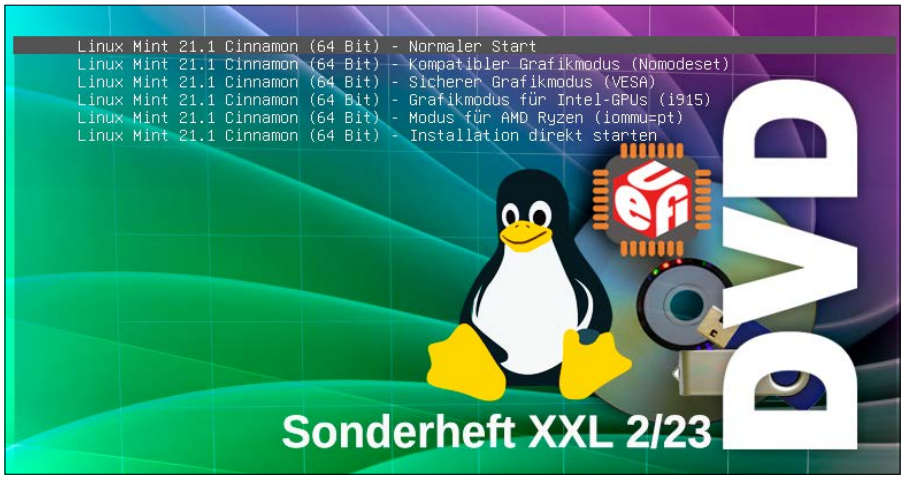
So wie Linux Mint hat auch Elementary OS seine Anfänge in einem Ergänzungspaket für Ubuntu. Daraus ist eine Ubuntu-Variante mit vielen frischen Ideen und einem eigenständigen Desktop geworden, der dem System das Flair von Mac-OS X verleiht. Es entwickelte sich aber zu einem eigenständigen Linux-System, das jeweils auf der aktuellen LTS-Version von Ubuntu aufbaut. Die kürzlich erschienene Version von Elementary OS basiert auf Ubuntu 22.04 als Systemgrundlage, setzt aber ebenfalls auf einen eigenen Desktop namens Pantheon. Dieser kann mit weiteren ästhetischen Verbesserungen aufwarten – denn darum geht es dieser inoffiziellen Ubuntu-Variante vornehmlich: Um eine Arbeitsumgebung auf Hochglanz, die sich auch jenseits von Linux mit modernen Desktops messen kann. Wie Gnome 3 basiert diese Desktopumgebung auf GTK3 und nutzt eine Abspaltung des Gnome-Windowmanagers. An die Verwandtschaft zu Gnome erinnert ein Panel am oberen Bildschirmrand, aber davon abgesehen regieren bei Elementary OS klassische Bedienelemente: Es gibt einen Programmstarter und ein Dock, das sowohl als Ablagefläche für häufig benötigte Anwendungen dient als auch laufende Programme anzeigt. Der Desktop ist wie Gnome sorgfältig ins Deutsche übersetzt.

Elementary OS 7 bootet zunächst zu einem grafischen Menü, das Spracheinstellungen und gewünschte Tastaturbelegung abfragt. Es stehen dann zum Ansehen und Ausprobieren ein „Testmodus“ zur Auswahl und eine flotte Installation mit „Laufwerk löschen und installieren“ sowie „Angepasst installieren (für Fortgeschrittene)“ mit ein paar Optionen zur Partitionierung mehr. Es kommt ein anderer Installer als der übliche Ubuntu-Installer Ubiquity zum Einsatz. Die Installation ist dafür blitzschnell, wobei ein Benutzer und das gewünschte Passwort erst nach dem ersten Boot angelegt werden.

Es sind nicht viele Anwendungen vorinstalliert und es obliegt somit den Anwendern, über das mitgelieferte Ubuntu Software Center oder über apt in der Kommandozeile die gewünschten Programme wie Libre Office, Firefox, Inkscape und Gimp selbst nachzurüsten. Dazu gibt es ein App Center sowie den Paketmanager apt in der Kommandozeile. In der Ausgabe 7 hat die Distribution Unterstützung für das App-Containerformat Flatpak. Flatpaks bringen ihre eigene Systemumgebung mit und laufen isoliert von Systembibliotheken, um eventuelle Konflikte zu vermeiden. Auch sind Flatpaks, wie Snaps, unabhängig von dem Paketformat einer Linux-Distribution und verlangen lediglich nach einer installierten Container-Runtime. Diese ist nun bei Elementary OS für Flatpaks vorinstalliert und kann Flatpaks aus dem hauseigenen App Center installieren.

Die universelle Flatpak-Quelle der Gnome Foundation (*https://flathub.org*) ist nicht eingebunden, allerdings kann Elementary OS die dort veröffentlichten Flatpaks per Doppelklick auf die heruntergeladene Definitionsdatei im Browser auch einrichten.

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

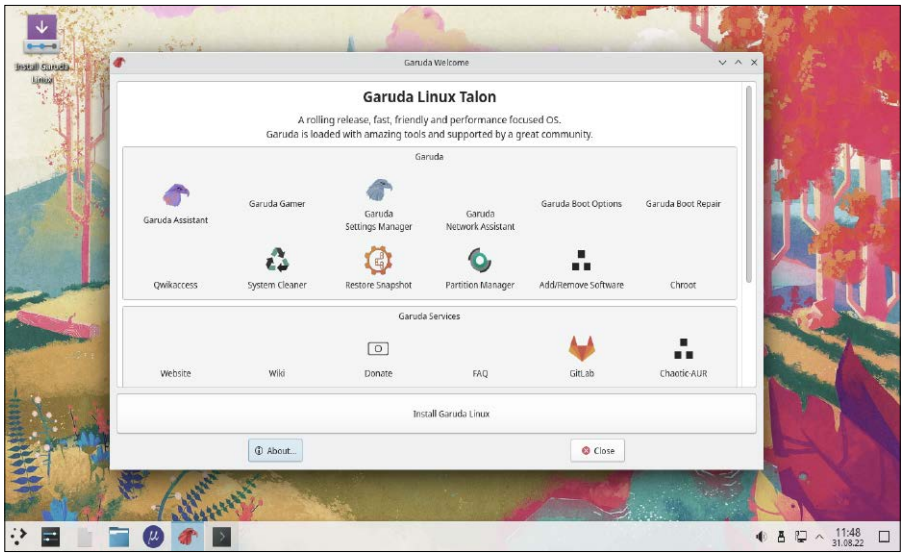


Das Multibootmenü der Heft-DVD: Für häufiger benötigten Bootparameter der Linux-Systeme, etwa für widerspenstige Grafikchips und sehr neue CPUs, haben wir Menüpunkte bereits vorbereitet.

Garuda Linux KDE Light

VON DAVID WOLSKI

Eher für Fortgeschrittene: Garuda ist ein Arch Linux mit grafischem Installer und vielen cleveren Ideen wie einem komprimierten BTRFS-Dateisystem. Garuda (mit KDE und in 64 Bit auf Heft-DVD) hat nicht umsonst in den letzten Monaten viel Aufmerksamkeit auf sich gezogen. Denn es ist ein ideenreiches und bunt funkelndes Arch-Linux-System für Fortgeschrittene, die dennoch nicht jede Optimierung selbst vornehmen möchten und einen komfortablen Installationsweg über ein Livesystem bevorzugen. Garuda war bislang mit mehreren Gigabyte pro Installationsmedium zu groß für unsere Heft-DVDs, passt nun aber in der Light-Variante mit KDE Plasma 5.25 genau neben die anderen Desktopsysteme dieser Ausgabe.

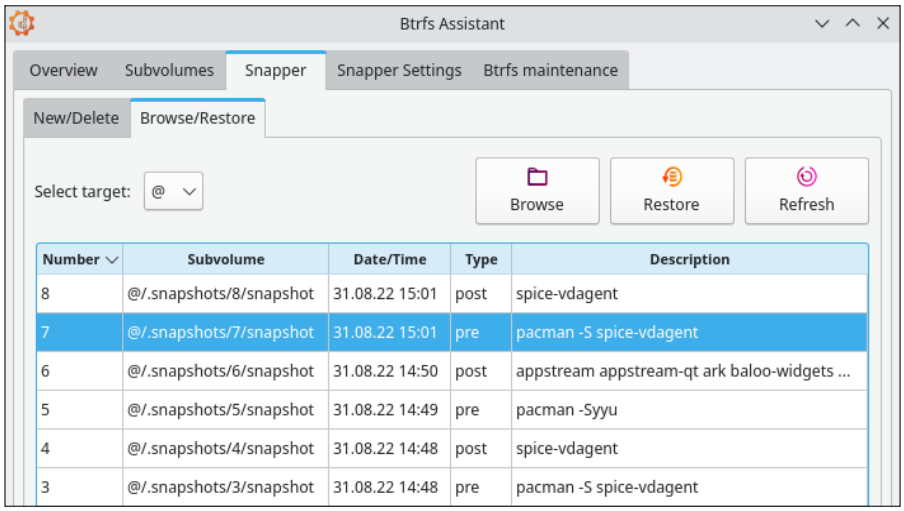


Garuda ist ein Arch Linux mit grafischer Installation, Administrationstools und vielen cleveren Ideen. Ein Menü grüßt zur weiteren Einrichtung, dient aber auch zur vereinfachten Systempflege.

Ein Verzicht auf allzu viele grafische Eigenheiten ist Garuda Linux, das in Deutschland und Indien entwickelt wird, überhaupt nicht abträglich. Im Gegenteil – denn es gibt unter der Oberfläche eine Menge cleverer Ideen. Diese verlangen Aufmerksamkeit, um dieses Arch-Linux-System optimal zu nutzen, dessen Zielgruppe ganz klar fortgeschrittene Anwender sind. Installiert ist Garuda mit dem Installer Calamares aber ähnlich schnell und einfach wie Manjaro.

Standardmäßig mitinstalliert wird die Variante „Zen" des Linux-Kernels, die für eine bessere Latenz auf Desktopsystemen einige Tweaks und Patches enthält. Für Systeme mit eher wenig Arbeitsspeicher ist ZRAM bereits aktiviert, das für eine höhere Effizienz die Hälfte des Speichers als komprimierten Swapbereich reserviert. Dies verdoppelt das verfügbare RAM beinahe. Gepackt ist auch das BTRFS-Dateisystem, das Garuda standardmäßig bei der Installation erstellt: Der Kompressionsalgorithmus Zstandard (Zstd) sorgt dafür, dass mehr Daten auf das Systemlaufwerk passen. Die Platzersparnis kommt in Garuda sehr gelegen, denn wie auch in Open Suse Leap sind „Snapshots" für das Systemvolume über den Dienst Snapper aktiviert, der nahtlos mit BTRFS zusammenarbeitet und die Momentaufnahmen als BTRFS-Subvolumes speichert. Momentaufnahmen halten bei einem Update des Systems den letzten Zustand als Differenz fest und stellen diesen als Bootoption im Grub-Bootloader zur Auswahl. Es ist damit möglich, nach einem Update mit unerwünschten Nebenwirkungen, die es bei Arch Linux durchaus mal geben kann, schnell zu einem vorherigen Zustand zurückzukehren. Diese Snapshots belegen jeweils 6 GB auf einer typischen Garuda-Installation und werden automatisch nach jedem Einsatz des Paketmanagers pacman erstellt. Enthalten sind nur Systemordner wie „/usr", „/var/lib" und auch „/etc", das Home-Verzeichnis bleibt außen vor, sonst wäre der Platzbedarf unrealistisch hoch. Ein regelmäßiges manuelles Aufräumen oder Abschalten der automatisch generierten Snapshots im grafischen BTRFS Assistant reduziert die Datenmenge.

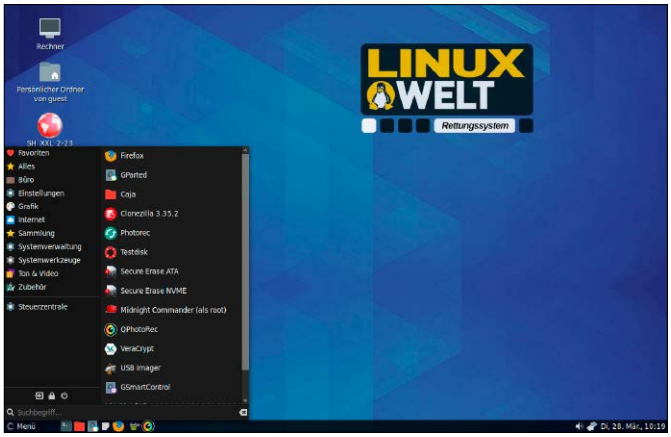
Webseite: *https://garudalinux.org*
Dokumentation:
https://wiki.garudalinux.org/en/home



Wo ist der Platz geblieben? Die Snapshotfunktion von Snapper belegt für jeden der Systemzustände rund 6 GB auf der BTRFS-Systempartition. Hier ist regelmäßiges Aufräumen angesagt!

LinuxWelt-Rettungssystem 9.4

VON DAVID WOLSKI



Blick in den Werkzeugkasten: Die wichtigsten Tools müssen Sie im LinuxWelt-Rettungssystem nicht lange suchen. Zu diesen haben wir haben unter „Favoriten“ schon Verknüpfungen angelegt.

Aufgefrischt: Das neue LinuxWelt-Rettungssystem 9.4 enthält neue Tools und Browser. In dieser Ausgabe stehen Gparted 1.4, die Kommandozeilentools Testdisk, Photorec, Ext4magic zur Wiederherstellung gelöschter Dateien im Mittelpunkt sowie das Datenträger-Imaging-Programm Clonezilla und der Verschlüsseler Veracrypt 1.25. Neu hinzugekommen sind außerdem Qphotorec, Clam AV und Clam-AV-GUI. 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 dislocker an fortgeschrittene Anwender richten, so ist die Oberfläche des Livesystems einladend und einfach gehalten. Es sind NTFS-Treiber mit an Bord und der Dateimanager kann Windows-Partitionen damit direkt öffnen. Windows-Partitionen werden zunächst im Nur-Lesen-Modus eingehängt. Um den Schreibmodus zu aktivieren, dient der Punkt „Windows-Partitionen (RW)“ im Anwendungsmenü unter „Favoriten”. Kleinere, aber wichtige Tools in der Shell wie der Portscanner Nmap und das Tool Dislocker zum Einhängen von verschlüsselten Windows-Partitionen ergänzen das neue System. Nach dem Start des Mate-Desktops wartet der übliche Network-Manager rechts oben darauf, eine WLAN-Verbindung aufzubauen. In der unteren Leiste des Mate-Desktops finden sich Verknüpfungen für den bequemen Zugriff auf die wichtigsten Programme. Neu im Terminal ist das Wiederherstellungstool ddrescue zum Auslesen beschädigter Datenträger in Imagedateien, die dann beispielsweise an Photorec übergeben werden können. Aktualisiert ist auch Photorec/Testdisk auf die Version 7.2 WIP, die gelöschte Dateien besser anhand der Metadaten identifizieren kann.

Im Verzeichnis „Image-Dateien“ liegt die ISO-Datei des Systems auf DVD vor, die mit Tools wie dem USB Image Writer (Linux, Windows, Mac-OS, auf Heft-DVD) auf einen USB-Stick geschrieben werden kann, um einen Rechner davon zu booten. Das Rettungssystem läuft im Bios- und Uefi-Modus und die ISO-Datei kann auch mit Ventoy (auf Heft-DVD, Download unter *https://github.com/ventoy/Ventoy*, Open-Source für Windows und Linux) verwendet werden. ■

ZUM DOWNLOAD: DIE EXTRA-DVD



Noch mehr Linux-Systeme: Seit letztem Jahr bieten wir zu jedem Heft noch ein weiteres Image mit ausgewählten Systemen in einer Multiboot-Umgebung, die jeweils einen neu eingerichteten Werkzeugkasten liefern.

Dieses Image (4,5 GB) liegt als Download per HTTP und per Bittorrent auf *https://bit.ly/3LY1oBV* bereit. Folgende Systeme liefert dieses Extra-Image für USB-Sticks ab 8 GB Kapazität oder für selbst gebrannte DVD-R diesmal mit:

Rescuezilla 2.4.2: Das Livesystem greift die Idee von Clonezilla auf und bietet mit Partclone ein mächtiges Tool zum Backup von Partitionen. Rescuezilla bietet eine grafische Oberfläche im Livesystem. Es unterstützt Bios sowie Uefi und liegt auch als ISO-Datei vor. Es kann Images über das Protokoll SFTP auch über das Netzwerk sichern und die gespeicherten Images sind zu Clonezilla kompatibel.

Wifislax 3.3: Das (englischsprachige) Livesystem aus Spanien stattet ein Livesystem mit Tools zur Netzwerkanalyse in Drahtlosnetzwerken aus. Mit dabei sind auch Lin SSID, Angry IP Scanner und Zenmap.

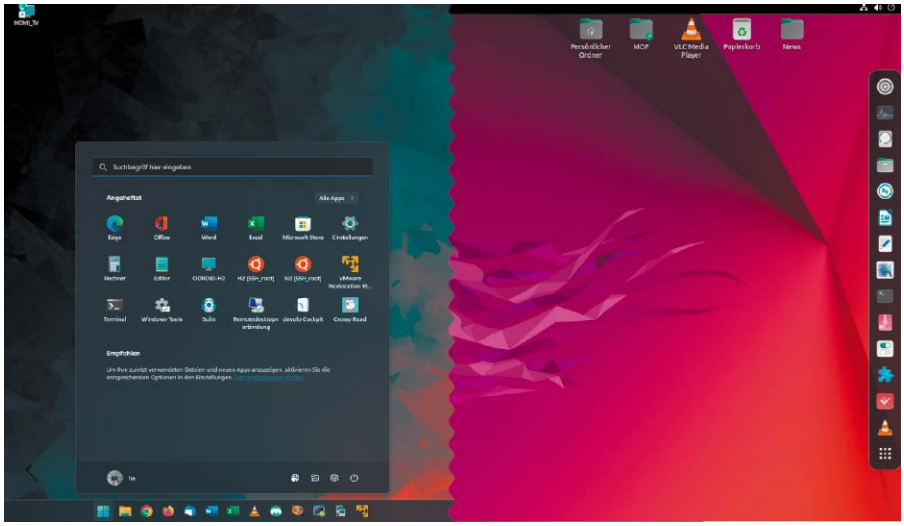
Systemrescue 10: Dieses Livesystem ist als universelles Rettungs- und Notfallsystem konzipiert, um liegen gebliebene Linux- und Windows-Systeme wieder flottzumachen – oder zumindest mit Hilfe der mitgelieferten Kommandozeilentools die Daten dort von den Datenträgern zu retten. Man muss allerdings kein Kommandozeilen-Akrobat sein, um die Tools von Systemrescue nutzen zu können: Da es sich auf einer grafischen Oberfläche angenehmer arbeiten lässt, verfügt es über einen XFCE-Desktop mit Verknüpfungen zu den wichtigsten Programmen.

Gparted Live 1.5.0: Auch dieses Image liefert wieder den nützlichen Partitionierer Gparted in der neuesten Version in einem Livesystem der Entwickler mit. Version 1.5.0 liefert viele Fehlerhebungen. Gparted ist auch für Windows-Anwender relevant, wenn es um die Neupartitionierung von Datenträgern ohne Datenverlust geht.

Linux & Windows: Das Duell

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

VON HERMANN APFELBÖCK



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

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

1. Leistung (1): Der Bootprozess

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

Windows 7,8
Ubuntu 13,6

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

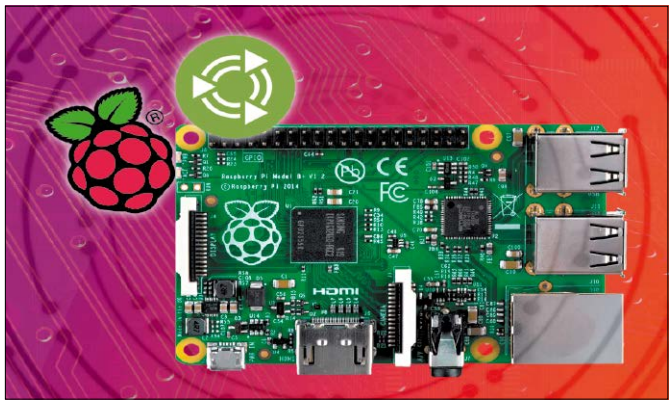


Autostart-Anwendungen: Verglichen mit Windows bleibt das unter Linux stets überschaubar. Das liegt nicht zuletzt daran, dass sich die Software nicht selbst um Updates kümmern muss.

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

2. Leistung (2): Betriebsperformance

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



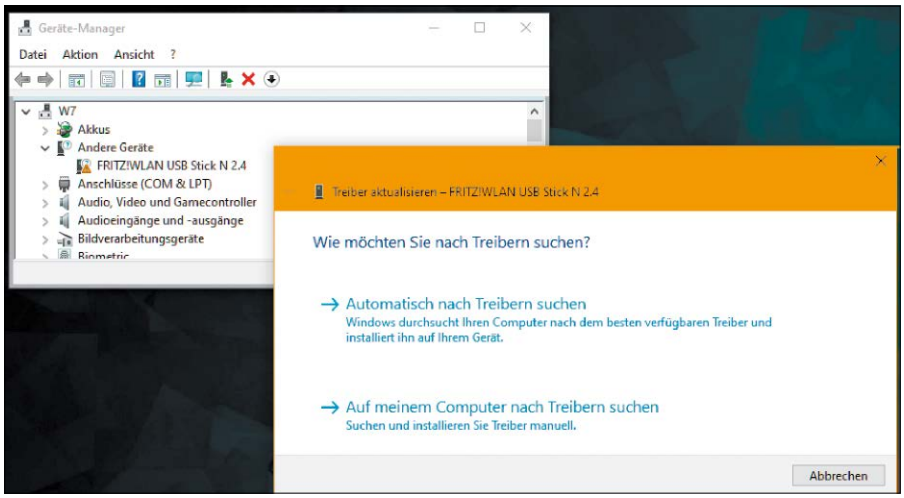
Linux läuft überall: Für ARM-Platinen oder x86-Altgeräte gibt es keine Windows-Alternativen.

3. Leistung (3): Skalierbarkeit

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

4. Hardware (1): Allgemein

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



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

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

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

Ergebnis: 2 Punkte für Windows

5. Hardware (2): Ältere Peripherie

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

Ergebnis: 1 Punkt für Linux

6. Hardware (3): Notebooks

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

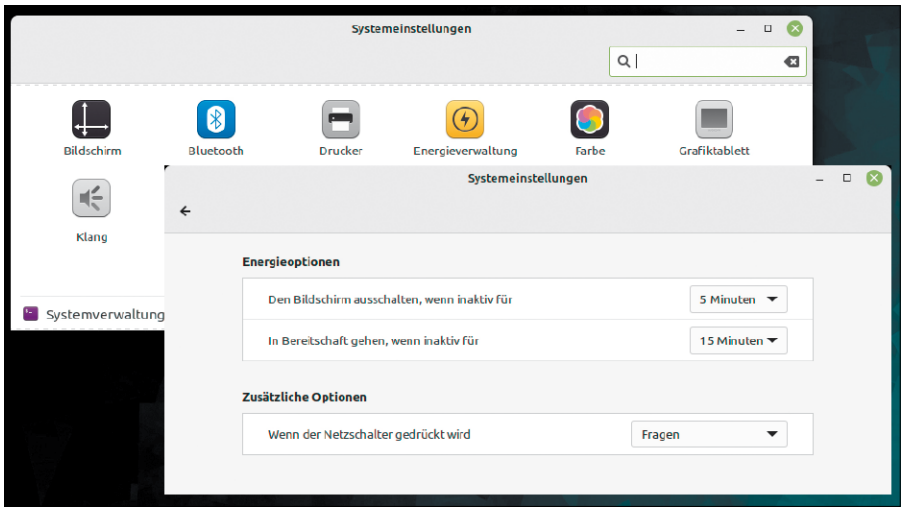
Manchmal werden auch Funktions- und Sondertasten von Notebooks von Linux nicht unterstützt. Mit Anleitungen aus dem Internet und etwas Aufwand lässt sich das Problem meistens beheben, sofern das Know-how des Nutzers ausreicht. Generell ist es ratsam, sich vor dem Notebookkauf über die Linux-Kompatibilität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

Ergebnis: 1 Punkt für Windows

7. Software & Spiele

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

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



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

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

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

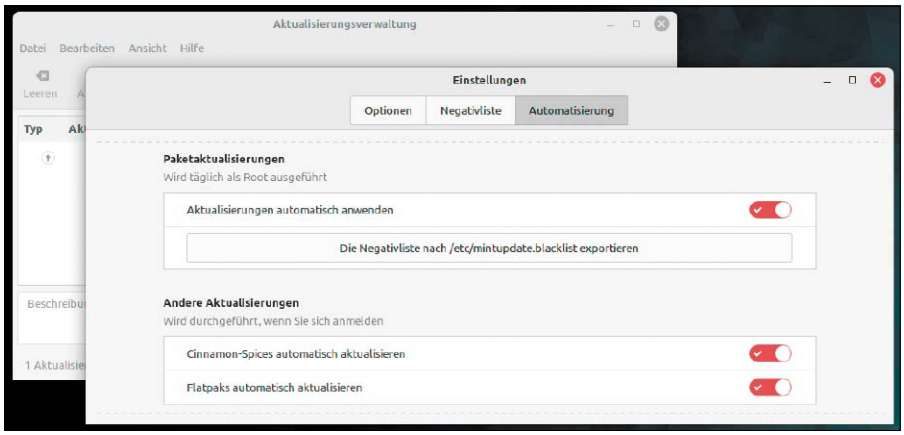
Ergebnis: 2 Punkte für Windows

8. Updates & Upgrades

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

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

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



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

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

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

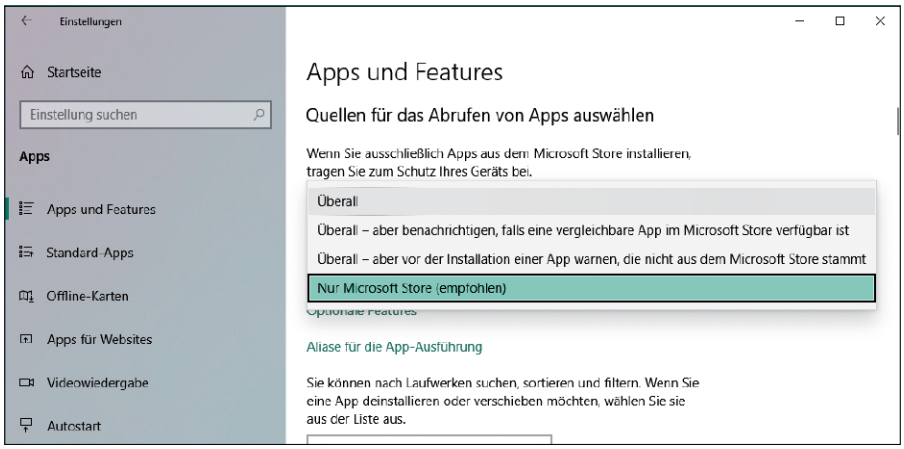
Ergebnis: 1 Punkt für Linux

9. Sicherheit im Web

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

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

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



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

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

Ergebnis: 2 Punkte für Linux

10. Datenschutz & Verschlüsselung

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

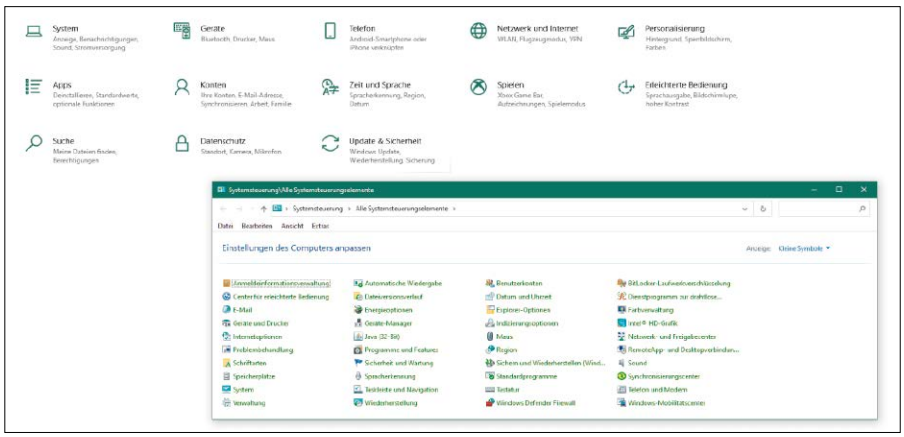
Windows sammelt anonyme Nutzungsdaten, eventuell auch personenbezogene Infos über Cortana, Defender, Aktivitätsverlauf. Wer die Onedrive-Anbindung kritiklos nutzt, übergibt Microsoft in jedem Fall persönliche Daten. Einiges kann man abschalten, aber nicht alles. In der Home-Edition von Windows 11 entsteht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

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

Ergebnis: 1 Punkt für Linux

11. Mobilität auf USB

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



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

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

Ergebnis: 1 Punkt für Linux

12. Systemkonfiguration (1): Die Zentralen

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

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

Ergebnis: 1 Punkt für Linux

13. Systemkonfiguration (2): Low Level

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



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

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

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

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

Ergebnis: 1 Punkt für Windows

14. Oberfläche (1): Allgemein

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

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

Ergebnis: 1 Punkt für Windows

15. Oberfläche (2): Flexibilität

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

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

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

Ergebnis: 1 Punkt für Linux

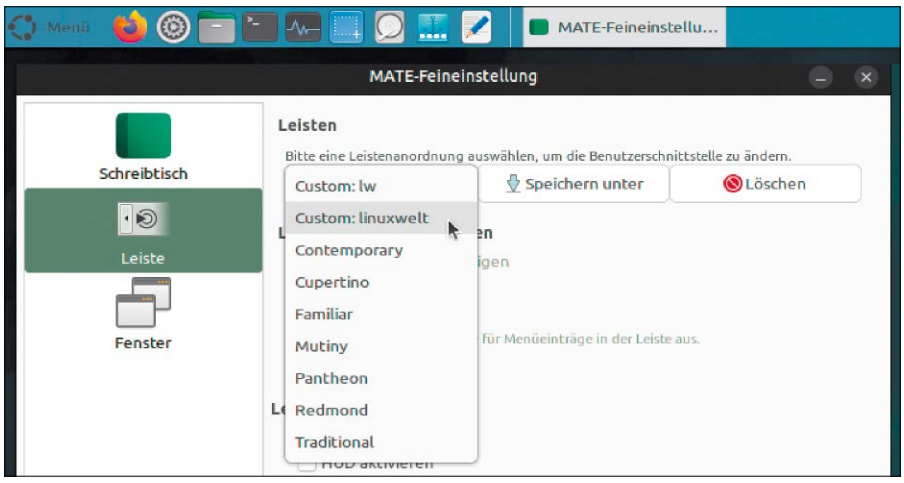
16. Kosten & Lizenzmodell

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

Ergebnis: 1 Punkt für Linux

LINUX GEGEN WINDOWS

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



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

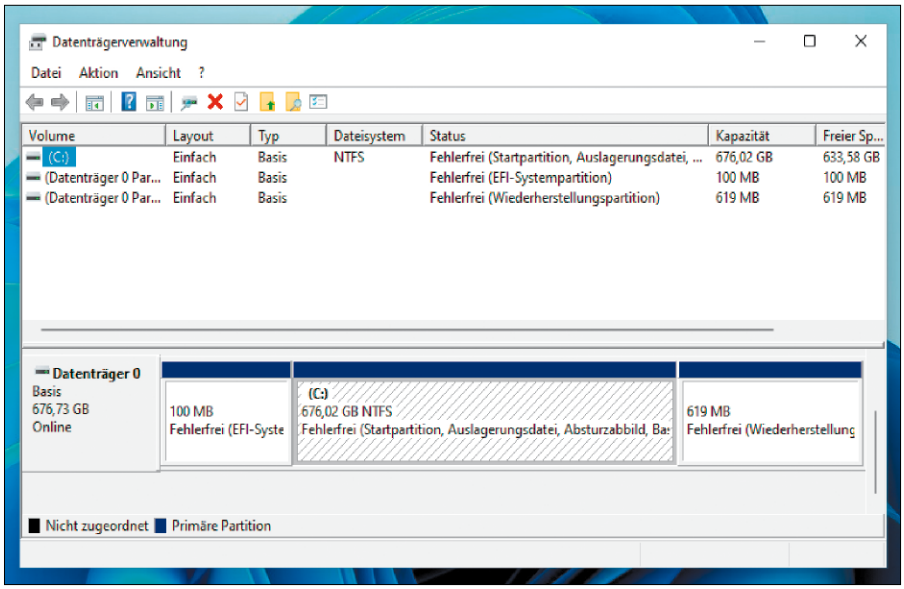
Linux neben Windows

Wer als Linux-Umsteiger nicht komplett auf Windows verzichten kann, installiert beide Betriebssysteme nebeneinander auf dem PC. Bei Bedarf wählt man dann beim Start des Rechners das gewünschte System.

VON THORSTEN EGGELING

Die meisten Linux-Distributionen rechnen damit, eine Windows-Installation auf dem PC vorzufinden. Das Setuptool bietet dann an, automatisch Platz für Linux zu schaffen und das System neben Windows auf einer eigenen Partition einzurichten. Das gelingt mit wenigen Mausklicks, berücksichtigt aber keine Windows-Eigenheiten. Wir schlagen daher eine manuelle Partitionierung vor. Steht eine zweite Festplatte zur Verfügung, kann man auch diese für Linux nutzen. Eine Alternative ist die Linux-Installation auf einem USB-Laufwerk.

Dieser Artikel bezieht sich auf Ubuntu 22.04 sowie Windows 10/11. Bei Linux Mint 21 und anderen Systemen sind die Abläufe ähnlich.



Typische Konfiguration: Bei den meisten PCs ist nur eine Partition für Windows konfiguriert. Diese lässt sich verkleinern, um eine Partition für Linux zu erzeugen.

1. Situation auf dem PC untersuchen

PCs und Notebooks mit vorinstallierten Windows 10 oder 11 starten immer im Uefi-Modus und die Festplatte verwendet ein GPT-Partitionsschema. Ob das auch auf Ihrem Computer der Fall ist, prüfen Sie unter Windows mit der Datenträgerverwaltung. Starten Sie diese über das Menü, das Sie mit der Tastenkombination Win-X aufrufen. Sie sehen die „EFI-Systempartition“ mit 100 MB, die Startpartition „C:“ und dahinter die „Wiederherstellungspartition“. Wenn der Hersteller es so eingerichtet hat, kann dahinter noch eine zusätzliche Datenpartition vorhanden sein.

Wenn keine „EFI-Systempartition“ zu sehen ist, der Computer aber eine Uefi-Firmware bietet, sollten Sie den Umstieg auf GPT/Uefi erwägen. Eine Anleitung dafür finden Sie unter *www.pcwelt.de/1191432*.

Uefi unterstützt die parallele Installation mehrerer Betriebssysteme besser als der veraltete Bios-Modus. Aber auch auf älteren Rechnern ohne Uefi-Firmware kann man Linux neben Windows auf der Festplatte einrichten.

2. Die Linux-Installation vorbereiten

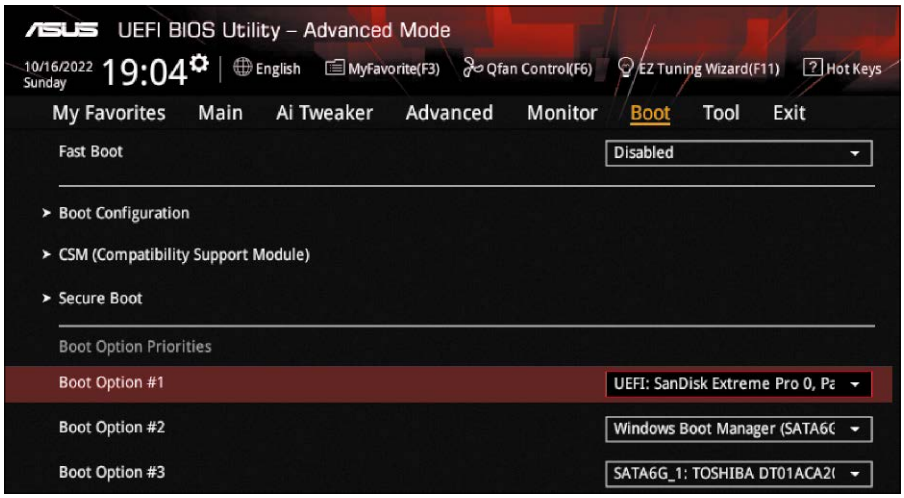
Bevor Sie etwas an der Partitionierung ändern (siehe Punkt 3), erstellen Sie ein Backup. Sie können die gesamte Festplatte als Abbild beispielsweise mit Clonezilla sichern, das im LinuxWelt-Rettungssystem (auf Heft-DVD) enthalten ist. Räumen Sie vorher unter Windows auf, damit möglichst viel freier Platz auf der Systempartition vorhanden ist. Dazu nutzen Sie die Datenträgerbereinigung und lagern selten genutzte und besonders große Dateien auf eine andere Festplatte aus.

Linux-Installationsmedium erstellen: Laden Sie die ISO-Datei des gewünschten Linux-Systems herunter. Unter Windows kann man damit im Windows-Explorer über den Kontextmenüpunkt „Datenträgerabbild brennen“ eine bootfähige DVD erstellen. Ein USB-Stick ist aber schneller und mit einem Tool wie Rufus (*https://rufus.ie*) oder Win 32 Disk Imager (beide auf Heft-DVD) aus der ISO-Datei einfach zu erstellen.

Bios/Firmwaresetup: Legen Sie die DVD ein oder verbinden Sie den USB-Stick mit dem PC. Das Bios-Setup rufen Sie über Tasten wie Esc, F2 oder Entf kurz nach dem Einschalten des PCs auf. Von Windows aus gelangt man so in das Uefi-Firmwaresetup: Klicken Sie im Windows-Anmeldebildschirm rechts unten die „Ein/Aus“-Schaltfläche an. Dabei halten Sie die Umschalt-Taste gedrückt und klicken im Menü der Schaltfläche auf „Neu starten“. Gehen Sie auf „Problembehandlung → Erweiterte Optionen → UEFI-Firmwareeinstellungen“ und klicken Sie dann auf „Neu starten“.

Ändern Sie in der Rechnerfirmware bei Bedarf die Bootreihenfolge. Das DVD- oder USB-Laufwerk muss an erster Stelle stehen, damit sich der PC von Installationsmedium

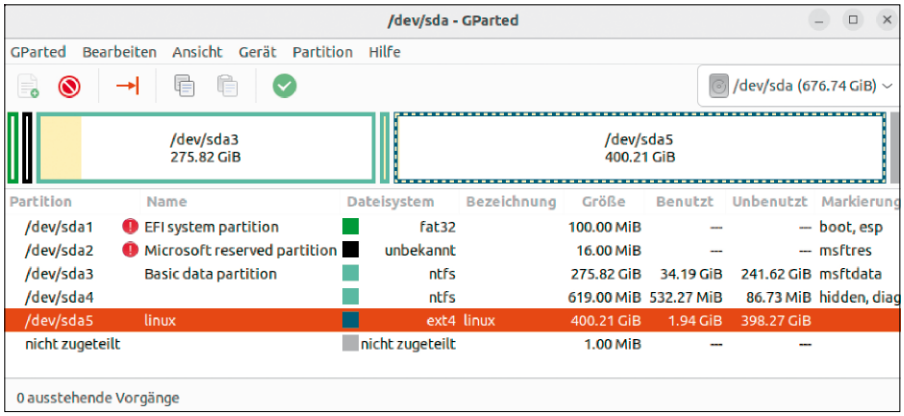
booten lässt. Bei einer Uefi-Firmware mit aktiviertem CSM oder „Legacy Boot“ achten Sie darauf, dass der Eintrag mit vorangestelltem „Uefi“ gebootet wird, wenn Windows in diesem Modus installiert ist.
Ist in der Firmware „Fastboot“ aktiviert, werden USB-Geräte beim Start des Rechners nicht initialisiert, was den Bootvorgang beschleunigt. Allerdings ist es dann oft nicht möglich, im Bootmenü von Linux-Installationssystemen zu navigieren. Aktivieren Sie „USB legacy“ oder ähnlich und deaktivieren Sie „Fastboot“. Später, nach der Installation, machen Sie diese Änderung rückgängig, um wieder vom Schnellstart zu profitieren.



Firmwareeinstellungen: Deaktivieren Sie – wenn vorhanden – „Fastboot“ und setzen Sie das Linux-Installationsmedium in der Bootreihenfolge an die erste Position.

3. Festplatte neu partitionieren

Jedes Betriebssystem benötigt eine eigene Partition. Ist bisher nur eine Partition vorhanden, muss man diese verkleinern, um Platz für Linux zu schaffen. Wenn eine zweite Partition verfügbar ist, räumt man diese für Linux frei.
Steht eine zweite physische Festplatte alleine für Linux zur Verfügung, trennen Sie die Datenverbindung der Windows-Systemfestplatte vom PC. Dann lässt sich Linux komplett unabhängig von Windows installieren (siehe Punkt 4) und beeinflusst den Windows-Bootmanager nicht.
Schritt 1: Beenden Sie Windows mit „Neu starten“ statt mit „Herunterfahren“. Nur dann werden alle Änderungen in das Dateisystem geschrieben. Booten Sie den PC vom Installationsmedium. Bei Ubuntu wählen Sie als Sprache „Deutsch“ und klicken auf „Ubuntu ausprobieren“.
Schritt 2: Starten Sie das Partitionierungstool Gparted über eine Suche im Menü (Linux Mint) oder über „Aktivitäten“ (Ubuntu). Klicken Sie die Windows-Partition an und gehen Sie auf „Partition → Größe ändern/Verschieben“. Ziehen Sie den Anfasser rechts von der grafischen Partitionsdarstellung an die gewünschte Position oder geben Sie einen Wert hinter „Neue Größe (MiB)“ ein. Der freie Speicherplatz muss für Linux mindestens 20 GB groß sein. Deutlich mehr ist besser, um genügend Reserve zu haben. Klicken Sie auf „Größe ändern/Verschieben“.
Schritt 3: Klicken Sie die Wiederherstellungspartition an, die Gparted jetzt hinter dem freien Bereich anzeigt. In der Spalte „Markierungen“ steht „hidden, diag“. Gehen Sie auf „Partition → Größe ändern/Verschieben“ und verschieben Sie den Balken der Partition ganz an den Anfang. Nach einem Klick auf „Größe ändern/Verschieben“ erscheint ein Hinweis, den Sie per Klick auf „OK“ bestätigen. Diese Maßnahme ist nötig, weil die Wiederherstellungspartition direkt hinter der Windows-Systempartition liegen muss. Windows aktualisiert den Inhalt bei einem Upgrade, verkleinert bei Bedarf die Windows-Partition und vergrößert die Wiederherstellungspartition. Liegt die Linux-Partition zwischen den beiden Windows-Partitionen, kann diese Aktion misslingen. Windows aktualisiert dann die Wiederherstellungspartition nicht, legt eine neue an oder zerstört im schlimmsten Fall die Linux-Partition.



Geänderte Partitionierung: Nach den Umbaumaßnahmen liegen Windows- und Wiederherstellungspartition direkt hintereinander. Danach folgt die Linux-Partition.

Schritt 4: Im jetzt freien Bereich legen Sie über „Partition → Neu“ eine Linux-Partition mit dem Dateisystem Ext4 an. Wenn die Festplatte groß genug ist, können Sie zusätzlich noch eine NTFS-Partition für den Datenaustausch mit Windows erstellen. Das ist nicht zwingend erforderlich, weil Linux auf die Windows-Partition zugreifen kann – schreibend allerdings nur, wenn Sie Windows über „Neu starten“ beenden oder der Schnellstart deaktiviert ist.
Schritt 5: Bisher hat Gparted die Änderungen nur vorgemerkt. Gehen Sie auf „Bearbeiten → Alle Vorgänge ausführen“, um die Anpassungen vorzunehmen.

4. Linux neu installieren

Starten Sie im Linux-Installationssystem das Setupprogramm über das Desktopicon und folgen Sie den Anweisungen des Assistenten.
Variante 1: Sie haben die Windows-Festplatte abgeklemmt (empfohlen) und die zukünftige Linux-Festplatte ist das einzige angebotene Laufwerk: Wählen Sie die Option „Festplatte löschen und Ubuntu installieren“. Da nur ein Laufwerk vorhanden ist,



Windows-Festplatte abgeklemmt: Mit nur einer Festplatte für Linux kann nach Auswahl der Option „Festplatte löschen und Ubuntu installieren“ nichts schiefgehen.

wird hier neben dem System auch die Linux-Bootumgebung installiert.

Variante 2: Ist die Windows-Festplatte angeschlossen, aber ein zweites Laufwerk für Linux vorhanden, entscheiden Sie sich ebenfalls für „Festplatte löschen und Ubuntu installieren“. Nach dem Klick auf „Weiter“ geben Sie dann die Zielfestplatte an. Prüfen Sie die Einstellung genau, um nicht die falsche Festplatte zu löschen. Die Linux-Bootumgebung wird dann auf der Windows-Festplatte eingerichtet, das System auf der Linux-Festplatte.

Variante 3: Sie haben auf der Windows-Festplatte eine Partition für Linux erstellt. Im Fenster „Installationsart“ verwenden Sie die Option „Etwas Anderes“. Wählen Sie die in Punkt 3 für Linux vorbereitete Ext4-Partition und klicken Sie auf „Ändern“. Hinter „Benutzen als:“ stellen Sie „Ext4-Journaling-Dateisystem“ ein und hinter „Einbindungspunkt:“ wählen Sie „/“. Bestätigen Sie mit „OK“.

Gleich, welche Variante Sie gewählt haben, klicken Sie zum Abschluss auf „Jetzt installieren“ und folgen den weiteren Anweisungen. Bei Variante 2 und 3 erscheint nach dem Neustart ein Bootmenü, in dem Sie zwischen Windows und Linux wählen.

Wer sich für Variante 1 entschieden hat, schließt die Windows-Festplatte wieder an und ruft das Firmwaresetup auf. Stellen Sie die Linux-Festplatte (Bios/CSM) oder den Uefi-Booteintrag „ubuntu“ als Startlaufwerk ein und booten Sie Linux. Im laufenden Linux geben Sie im Terminal diesen Befehl ein:

```
sudo update-grub
```

Damit nehmen Sie die Windows-Installation in das Grub-Bootmenü auf. Starten Sie den Rechner dann neu. Im Menü können Sie jetzt zwischen Ubuntu und Windows wählen. Wird in der Firmware hingegen die Windows-Festplatte als erstes Bootgerät ausgewählt, startet Windows direkt – ohne Multiboot-Auswahl.

5. Linux-Installation auf USB

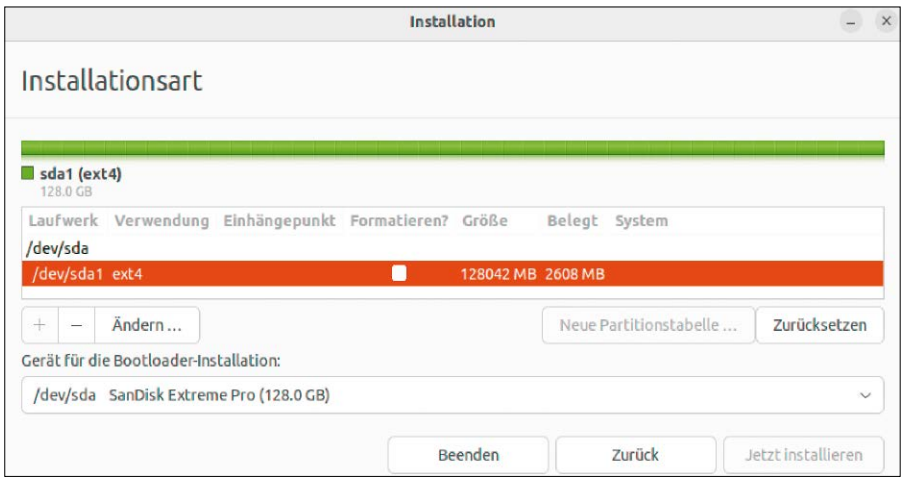
Linux behandelt USB-Laufwerke genauso wie interne Festplatten. Das Setupprogramm integriert Linux standardmäßig in die Uefi- oder Bios-Bootumgebung auf der Windows-Festplatte. Das führt zu Problemen, falls das USB-Laufwerk nicht verbunden ist. Der PC versucht, den Grub-Bootmanager zu starten, der findet das Linux-System nicht und man landet in der Grub-Shell. Bei Uefi-PCs ist das kein ernsthaftes Problem, weil man im Firmwaresetup einfach den Windows-Bootmanager aktivieren kann. Im Bios/CSM-Modus lassen sich Windows oder Linux aber erst wieder starten, wenn man das USB-Laufwerk wieder angeschlossen hat.

Bios/CSM-Modus: Wenn Windows in diesem Modus eingerichtet ist, installieren Sie Linux ähnlich wie in Punkt 4 bei der Variante 3 beschrieben. Booten Sie das Installationsmedium aber nicht im Uefi-Modus. Erstellen Sie mit Gparted eine Ext4-Partition auf dem USB-Laufwerk.

Im Setuptool wählen Sie „Etwas Anderes“ und weisen dem Laufwerk den Einbindungspunkt „/“ zu. Unter „Gerät für die Bootloader-Installation“ wählen Sie das USB-Laufwerk. Die Linux-Bootumgebung wird dadurch nicht auf der Windows-Festplatte eingerichtet.

Uefi-Installation: Das Setupprogramm ignoriert die manuelle Auswahl für die Bootloader-Installation. Der Bootloader landet daher in der Efi-Partition auf der Windows-Festplatte. Es spielt keine Rolle, ob Sie das Installationssystem im Bios/CSM- oder Uefi-Modus gestartet haben. Das Problem lässt sich umgehen, indem Sie die Windows-Festplatte für die Installation abklemmen. Sie benötigen einen USB-Stick oder eine DVD als Installationsmedium und ein weiteres USB-Laufwerk als Ziel der Installation.

Virtuellen PC verwenden: In Virtualbox unter Windows oder Linux kann eine USB-Installation ohne Gefahr erfolgen. Richten Sie eine virtuelle Maschine (VM) ohne virtuelle Festplatte ein und booten Sie das System von der ISO-Datei des Linux-Systems. Binden Sie das USB-Laufwerk über „Geräte → USB“ ein. Da nur ein Laufwerk vorhanden ist, erfolgt die Installation wie in Punkt 4, Variante 1. Ubuntu 22.04 und Linux Mint 21 richten im Bios-Modus (bei Linux in Virtualbox Standard) auf dem externen Laufwerk die Bootumgebungen für Uefi-PCs und ältere Geräte mit Bios ein. Das portable Linux lässt sich daher auf fast beliebigen PCs booten. ■



USB-Installation: In Virtualbox lässt sich Linux auf einem USB-Laufwerk sicher installieren, ohne die Bootumgebung auf der Festplatte des PCs zu gefährden.

LINUX WELT

Mini-Angebot!

Satte **34,6 %** gespart!

3 x LinuxWelt + Geldprämie*



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 (Plus: Vorab erhalten Sie eine Ausgabe gratis) +
3 x LinuxWelt direkt aufs Smartphone & Tablet mit interaktivem Lesemodus +
10,- € Geldprämie (Wird mit dem Abopreis verrechnet)

=17,50 € (anstatt 26,75 Euro)

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 17,50 € und erhalte 3 Ausgaben + Geldprämie

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. Das Angebot ist innerhalb Deutschlands gültig.

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

LWPM062018

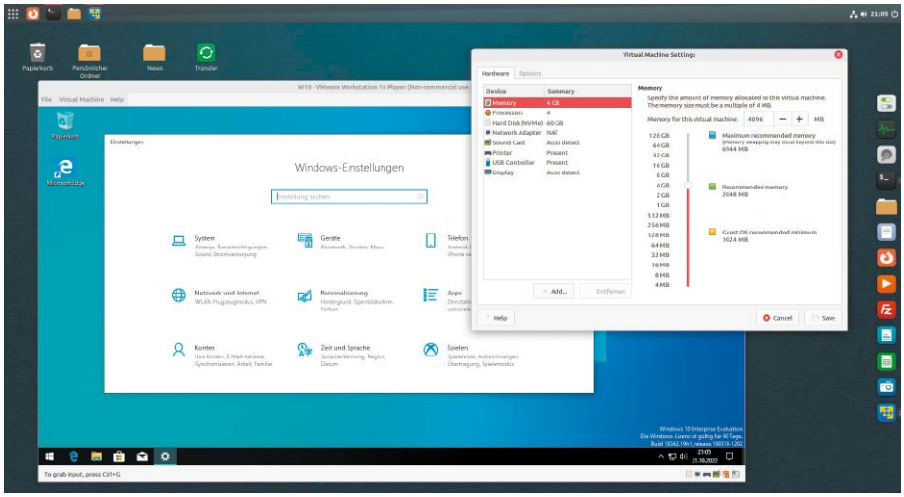
* wird mit Abo-Preis verrechnet

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

Linux & Windows: Virtualisierung

Virtualisierung schafft eine komfortable Verbindung zwischen Linux und Windows, egal welches System als Host oder Gast fungiert. Anders als bei Multiboot muss man das Hauptsystem nicht mehr verlassen, um die Vorteile des anderen Systems zu nutzen.

VON HERMANN APFELBÖCK



Als Virtualisierer stehen Oracle Virtualbox (*www.virtualbox.org*) und Vmware Player zur Wahl. Virtualbox ist die funktionsreichere Alternative, trotzdem fokussieren wir uns hier auf Vmware, weil eine der hier vorgestellten Lösungen (Szenario 3) nur damit funktioniert. Für andere Szenarien können Sie ebenso gut Virtualbox benutzen. Die Vorgehensweise unterscheidet sich, die Prinzipien sind aber analog.

Virtualisierung: Software & Hardware

Den kostenlosen Vmware Player erhalten Sie auf den Seite *www.vmware.com/de/products/workstation-player.html* (aktuell Version 16.2.4). Für Windows gibt es einen EXE-Installer (580 MB), für Linux einen „Bundle"-Installer (508 MB), den Sie nach dem Download mit

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

ausführbar schalten und installieren.

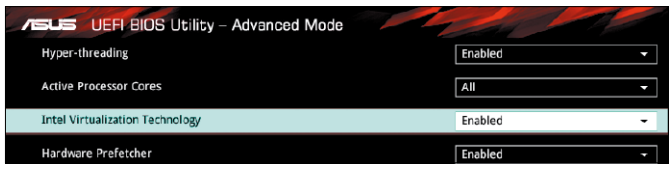
Die Hardwarevoraussetzungen für virtuelles Windows oder Linux sind keine Hürde: Acht GB RAM sind ausreichend, solange es um Office, Browser, Bildbearbeitung geht. Als Prozessor sollte eine Zwei- oder Vierkern-CPU mit mindestens zwei GHz vorliegen, die Virtualisierung mit Intel VT-X oder AMD-V nativ unterstützt. Ob dies zutrifft, kann unter Linux der Befehl lscpu ausgeben, wobei unter „Flags" (oder „Markierungen") der Eintrag „vmx" (Intel) oder „svm" (AMD) auftauchen sollte. Unter Windows fällt uns nur der Gang ins Firmware-Setup ein oder das Werkzeug Coreinfo (*www.sysinternals.com*), um diese Eigenschaft zu ermitteln.

Ein virtuelles Linux benötigt mindestens 20 bis 50 GB, Windows mindestens 60 GB Platz. Bei der VM-Konvertierung eines bestehenden Windows ist noch deutlich mehr erforderlich (100 bis 200 GB). VMs können auf USB, Festplatte oder SSDs gespeichert werden, sind aber natürlich am schnellsten auf SSD. Da VMs auf Dateiebene praktisch nur aus der großen virtuellen Festplatte und der Konfigurationsdatei bestehen (*.vmdk und .*vmx bei Vmware), ist auch ein späterer Umzug möglich.

Szenario 1: Virtuelles Surf-Linux

Eine Linux-Surf-VM unter Windows ist eine bequeme Lösung für sicherheitsbewusste Windows-Anwender.

Die Internetnutzung erfolgt dann in der sicheren VM, und den Datenaustausch zwischen Windows-Host und Linux-Gast kann man via Virtualisierer oder per Netzfreigabe optimieren. Aber natürlich sollten die Grenzen bewusst bleiben: Der virenverseuchte Installer eines Windows-Programms ist in der Linux-VM wirkungslos, erhält aber bei der Weitergabe an den Windows-Host wieder sein ganzes Schadpotenzial.

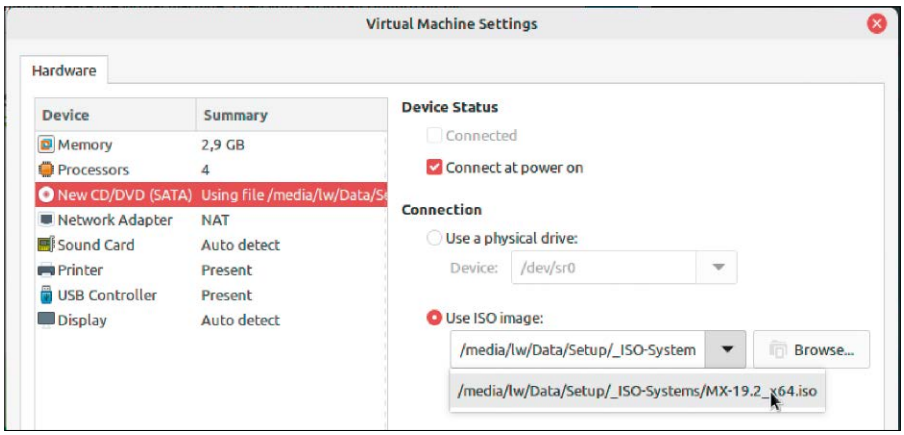


Firmwareeinstellungen: 64-Bit-CPUs bieten Hardwarebeschleunigung für virtuelle Maschinen. Manchmal müssen Sie die Option aber erst manuell aktivieren.

Linux als VM einrichten: Bei einem virtuellen Linux zum Surfen geht es im Wesentlichen nur um den Browser und daher genügt eine sparsame Distribution wie etwa ein kleines Lubuntu. Wählen Sie aber in jedem Fall eine vertraute Distribution mit komfortablem Installer. Dann fallen Setup und Systempflege umso leichter.

Nach dem Start des Vmware Players klicken Sie auf „Create a New Virtual Machine“ und wählen die Option „I will install the operating system later“. Nach Klick auf „Next“ wählen Sie „Linux“ und als „Version“ aus der Liste, was der einzurichtenden Distribution am nächsten kommt – etwa „Ubuntu 64-bit“ (für alle Ubuntus, Mint u. a.). Wenn die vorgegebenen Listeneinträge der Distribution gar nicht entsprechen, hilft das generische „Other Linux 5.x kernel“.

Nach „Next“ vergeben Sie einen Namen für das virtuelle System. Danach legen Sie eine großzügige Größe der virtuellen Festplatte fest, am besten als „single file“, denn dies steigert die Geschwindigkeit. Nach „Next“, „Finish“ und „Close“ ist die Arbeit noch nicht erledigt, denn das System hat noch kein Installationsmedium. Daher klicken Sie jetzt auf „Edit virtual machine settings“ auf „CD/DVD (SATA)“. Unter „Connection“ wählen Sie „Use ISO image“ und navigieren mit „Browse“ zum ISO-Image des gewünschten Systems. Speichern Sie die Änderungen per Klick auf „Save“. „Power on“ startet die VM und dort installieren Sie das gewünschte Linux wie gewohnt.



ISO-Image nachtragen: Die neue VM kann erst starten und dann installiert werden, wenn das Installationsmedium eingetragen ist.

Szenario 2: Windows-10-Installation als VM

Die Einrichtung einer Windows-10-VM verläuft ähnlich wie für Linux beschrieben. Jedoch sollten Sie nach „Create a New Virtual Machine“ im ersten Dialog hier unbedingt die Option „I will install the operating system later“ wählen. Andernfalls verwendet Vmware für Windows immer „Easy Install“ mit Eingabe eines Produktschlüssels. Den kann man zwar vorläufig ignorieren, aber danach scheitert die Installation von Evaluierungsversionen nach unserer Erfahrung regelmäßig.

In den weiteren Schritten geben Sie „Microsoft Windows“, die passende Version, einen Namen für die VM und das Zielverzeichnis („Location“) an. Die vom Player vorgeschlagenen zwei GB Arbeitsspeicher sollten Sie hochsetzen (vier GB), die 60 GB für die virtuelle Festplatte ebenfalls, sofern möglich. Genau wie in Szenario 1 ergänzen Sie dann noch mit „Edit virtual machine settings“ das Installations-ISO-Image (oder eine physische DVD im Laufwerk).

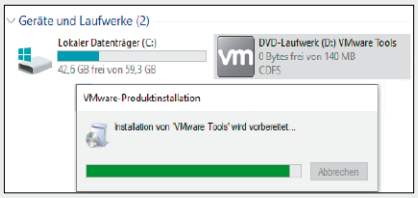
Unabhängig vom Technischen benötigen Windows-VMs etwas mehr Strategie wegen der Lizenz und Aktivierung. Idealerweise haben Sie noch ein älteres, ungenutztes Windows mit Produktschlüssel. Wenn es in erster Linie um den Einsatz von lokaler Windows-Software geht, sind auch abgelaufene Versionen kein Hindernis. Andernfalls greifen Sie zu Evaluierungsversionen von Windows 10 oder 11, die automatisch aktiviert sind und 90 Tage ohne Einschränkung funktionieren. Die ISO-Downloads finden Sie auf der Seite *www.microsoft.com/de-de/evalcenter* unter „Windows“. Der Download erfordert eine Registrierung mit Angabe von Name, Telefonnummer und Mailadresse.

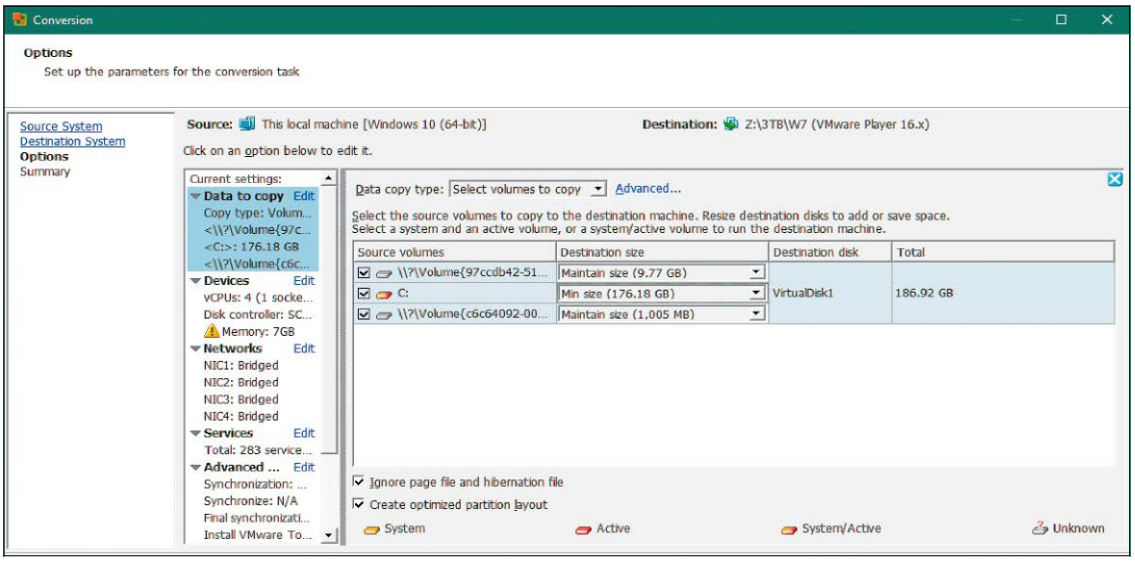
Evaluierungsversionen haben einen großzügigen Testzeitraum, der sich mit dem Terminalbefehl „slmgr -rearm“ (mit Administratorrecht) noch verlängern lässt. Während der Frist können Sie sich jederzeit entscheiden, das Test-Windows durch den Kauf eines gültigen Produktschlüssels in ein vollwertiges System umzuwandeln („Einstellungen → Aktivierung → Product Key ändern“). Für nachhaltiges Arbeiten mit kommerzieller Software in der VM ist dies meist unverzichtbar.

Tipp: Wenn Sie eine physische Windows-Installation auflösen und durch eine VM unter Linux ersetzen, notieren Sie sich unbedingt den Produktschlüssel der physischen Installation. Am einfachsten geht das mit der Windows-App „ShowKeyPlus“, die im offiziellen Microsoft Store verfügbar ist. Mit diesem Schlüssel machen Sie dann die Evaluierungsversion in der VM zur Vollversion. Auch auf alten Notebooks finden Sie auf der Unterseite Aufkleber mit längst obsoleten, aber eventuell noch gültigen Schlüsseln. Mindestens Windows-8-Schlüs-

VMWARE-TOOLS INSTALLIEREN

Insbesondere die Leistung einer Windows-VM lässt sich über Vmware-Tools deutlich verbessern. Zur Installation gehen Sie im Fenster der VM auf „Player → Manage → Install VMware Tools“ (Linux: „Virtual Machine → Install VMware Tools“). Eventuell müssen Sie erst im Windows-Explorer der VM das noch von der VM-Installation bestehende CD/DVD-Laufwerk aushängen. Danach erscheint automatisch das virtuelle DVD-Laufwerk mit den Vmware-Tools und Sie folgen einfach der Standardaktion mit nachfolgender Installation. Nach einem Neustart können Sie die Bildschirmauflösung durch Ändern der Fenstergröße bestimmen und der Mauszeiger muss nicht mehr mit Strg-Alt befreit werden.





Windows in VM umwandeln: Der Vmware Vcenter Converter erledigt das beeindruckend, doch der hier abgebildete Konfigurationsschritt verlangt Sorgfalt und Know-how.

sel sollten für Windows-10-Evaluierungsversionen noch funktionieren.

Szenario 3: Bestehendes Windows als VM klonen

Die Windows-Neuinstallation in einer VM, in der dann die notwendige Software nachinstalliert wird, ist die sauberste Lösung. Die bequemste ist sie nicht, denn Sie müssen Setup, Anpassungen und Softwareinstallationen erledigen. Es gibt auch die Möglichkeit, ein bestehendes Windows komplett in eine VM zu überführen.

Vorbereitung: Vor einer solchen Konvertierung ist es Pflicht, das Windows-System gründlich zu entschlacken. Das spart Platz auf der virtuellen Festplatte und beschleunigt die Umwandlung. 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 mit der Option „Systemdateien bereinigen“ und allen sonstigen Optionen, um überflüssige Dateien zu löschen. Alle Benutzerdateien, die Sie unter Windows nicht unbedingt brauchen, verschieben Sie auf einen externen Datenträger, um sie später auf das Linux-System zu übertragen.

Werkzeug: Als Konvertierungswerkzeug benötigen Sie den Vmware Vcenter Converter Standalone. Die englischsprachige Software erhalten Sie auf *www.vmware.com/de/products/converter.html*. Die Erlaubnis zum Download gibt es erst nach Hinterlegen eines Kontos (Mailadresse und Kennwort). Version 6.3.0 stammt ganz aktuell vom Oktober 2022. Laden und installieren Sie die Datei (210 MB) auf das Windows-System, das Sie in eine VM überführen möchten.

Den Vmware-Converter starten Sie nach Rechtsklick mit der Option „Als Administrator ausführen“, weil Sie sonst das laufende System nicht kopieren dürfen. Verwenden Sie die Schaltfläche „Convert machine“, im Folgedialog die Optionen „Powered on“ und „This local machine“. Nach „Next“ stellen Sie oben um auf „Vmware Workstation or other VMware virtual machine“. Neben „Select Vmware product“ wählen Sie den für private Nutzung kostenlosen „Vmware Player 16.x“ (es sei denn, Sie besitzen kostenpflichtige Vmware-Software).

Übernehmen Sie den voreingestellten Hostnamen. Im Feld darunter bestimmen Sie unter „Select a location...“ den Zielpfad für die virtuelle Festplatte.

Bei einer – trotz Aufräumen – mehr als halb gefüllten Festplatte müssen Sie vorläufig ein externes Laufwerk wählen, weil sonst der Platz für die virtuelle Platte nicht ausreicht.

Nach „Next“ folgt ein komplexer Konfigurationsdialog: Unter „Data to copy“ markieren Sie neben der Systempartition (meist „C:“) auch die bootrelevanten Partitionen „\\?\Volume...“. Eventuelle weitere Festplatten („D:“...) lassen Sie weg. Die Größe der Systempartition „C:“ können Sie einschränken (unter „Destination size“), allerdings nicht kleiner als die aktuelle Belegung. Falls diese „Min size“ immer noch sehr groß ausfällt, sollten Sie erwägen, Windows noch weiter zu verschlanken.

Unter „Devices“ müssen Sie die „Memory“-Einstellung bearbeiten. Zum Beispiel sind bei acht GB für die VM vier GB eine vernünftige Größe. Auf der Registerkarte „Other“ vergeben Sie für die „Cores“ die Hälfte der verfügbaren für die VM. Diese Anpassungen sind wichtig, weil die VM sonst das physische Maximum erhielte und das Hostsystem zum Erliegen brächte. Fatal sind falsche Vorgaben aber nicht, weil sich diese später in der einfachen VMX-Konfigurationsdatei korrigieren lassen. 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 bis zwei Stunden dauert. Das Ergebnis besteht aus einer sehr großen VMDK-Datei mit der virtuellen Festplatte und der kleinen VMX-Konfigurationsdatei.

Korrekturen: Abbrüche des Converters mit der Meldung „Failed“ sind nicht selten, aber korrigierbar. In unseren Tests hat es geholfen, im Quell-Windows unter „Einstellungen → Windows-Sicherheit“ den Echtzeitschutz vorübergehend zu deaktivieren. Außerdem ist es naheliegend, im Konfigurationsdialog unter „Services“ eventuelle Vmware- oder Virtualbox-Dienste abzuschalten (falls das laufende Windows seinerseits als VM-Host arbeitet). Bei dieser Gelegenheit können Sie Systemdienste, die Sie im virtuellen Zielsystem sicher nicht benötigen, im Register „Destination services“ abwählen. Das ist im Prinzip heikel, aber auf Virtualisierungsdienste können Sie im virtuellen Windows in jedem Fall verzichten. ■

PC-WELT PLUS

Stellen Sie uns auf die Probe!

3 x PC-WELT Plus zum Testpreis



Jetzt testen:
3x PC-WELT Plus
gedruckt & digital

16,99€

Satte **22%** gespart!

Als Print-Abonnent der **PC-WELT** erhalten Sie Ihre Ausgabe in der PC-WELT App **IMMER GRATIS** inklusive DVD-Inhalte zum Download.

- ✓ **3x PC-WELT Plus als Heft frei Haus** mit je 2 Doppel-DVDs und 32 Seiten Spezialwissen
- ✓ **3x PC-WELT Plus direkt aufs Smartphone & Tablet** mit interaktivem Lesemodus

Jetzt bestellen unter
www.pcwelt.de/testen 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 Plus Testabo für 16,99 €.

Möchten Sie die PC-WELT Plus anschließend weiter lesen, brauchen Sie nichts zu tun. Sie erhalten die PC-WELT Plus für weitere 12 Ausgaben zum aktuellen Jahresabopreis von z.Zt. 87,60 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

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

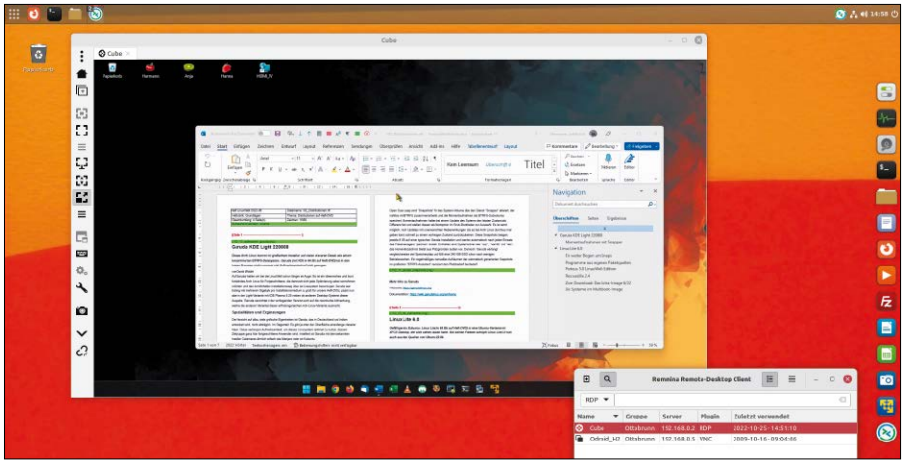
PWPMA14141

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

Linux & Windows als Team

Multiboot? Virtualisierung? So weit muss man nicht immer gehen: Linux und Windows bieten eine Reihe direkter Kommunikationswege. Darüber können die beiden Betriebssysteme nicht nur Daten, sondern auch Software und Aufgaben teilen.

VON HERMANN APFELBÖCK



Dank Netzwerk muss nicht jedes System alle Daten und Programme selbst besitzen und verwalten. Samba, SSH und Remotedesktop sind klassische Vermittler zwischen Linux und Windows (sowie auch Mac-OS und Android). Für das überaus produktive SSH ist Windows zwar nicht geboren, kann aber mit etwas Nachhilfe uneingeschränkt mitspielen.

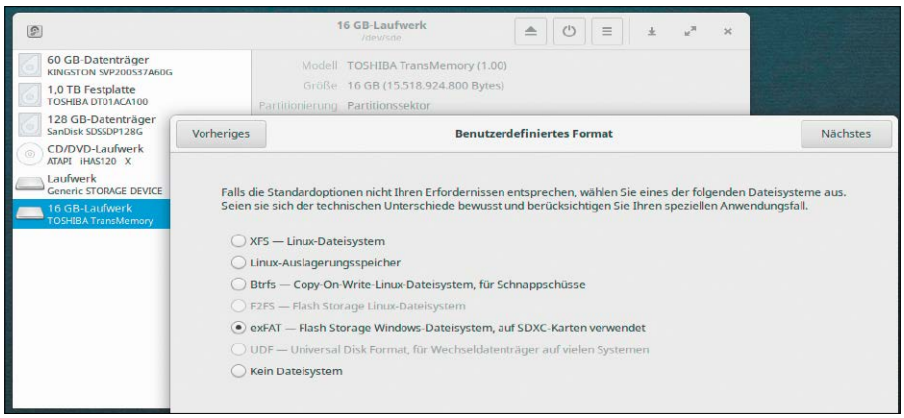
1. Datenträger für Linux & Windows

Linux-Anwender sind gut beraten, beim Formatieren auf Windows-Nutzer Rücksicht zu nehmen. Mit einem Linux-Dateisystem (Ext4, XFS, BTRFS, ZFS …) formatierte USB-Medien sind unter Windows schlicht nicht verwendbar. Von Windows kommt nur der destruktive Vorschlag, den Datenträger zu formatieren. Daher ist es unausweichlich, für mobile oder interne Datenlaufwerke (bei Multiboot) auf ein Microsoft-Dateisystem auszuweichen.

• Sind nur Linux und Windows im Spiel, ist NTFS erste Wahl. Linux wie Windows haben dort Lese- und Schreibzugriff und Linux wie Windows können mit NTFS formatieren. Beachten Sie aber, dass NTFS unter Linux im Prinzip als rechteloses Dateisystem gilt: Wenn von Windows-Seite Dateirechte oder spezielle NTFS-Eigenschaften wie Komprimierung oder Verschlüsselung angelegt wurden, werden diese unter Linux nicht ankommen.

• Für kleine USB-Laufwerke, die nur dem schnellen Datenaustausch dienen sollen, eignet sich einfaches FAT32, das alle Systeme ohne Hilfsmittel beherrschen und auch selbst formatieren können. Das Größenlimit für den Datenträger von 32 GB unter Windows ist künstlich. Linux kann auch größere Datenträger mit FAT32 formatieren. Entscheidender ist das Limit von vier GB für eine Einzeldatei. Für USB-Medien, die keine Filmdaten oder ISO-Images aufnehmen müssen, reicht FAT32 aber völlig aus.

• Wer ISO-Images und Filme austauschen will, kann auch exFAT verwenden. Linux beherrscht exFAT inzwischen standardmäßig. Linux-Werkzeuge wie Gnome-Disks („Laufwerke“) können ihrerseits mit exFAT formatieren.



Dateisystem exFAT für USB: Das einfache Microsoft-Dateisystem hat keine Größenbegrenzung für Einzeldateien und ist auf Linux-Desktops inzwischen Standard.

2. Netzwerkgespräche mit Samba

Samba ist das Linux-Äquivalent zu Windows-Freigaben (SMB) und die verbreitete Linux-Komponente, um Daten für Windows, Linux, Android und Mac-OS freizugeben. Weder auf Windows- noch auf Linux-Seite ist zusätzliche Software notwendig für den Zugriff.

Jedes Linux kann also die Freigaben von Windows-Systemen nutzen und umgekehrt. In beiden Richtungen gelten die üblichen Regeln, dass ein zugreifender Benutzer sowohl die Netzwerkerlaubnis als auch die nötigen lokalen Dateirechte besitzen muss.

Freigaben von Windows: Das Windows-Konzept der „Heimnetzgruppe" ist nicht Linux-kompatibel, daher muss im Explorer unter „Optionen → Ansicht" der „Freigabe-Assistent" abgeschaltet werden. Danach erfolgen Freigaben mit klassischen Kontenberechtigungen, konkret mit der Explorer-Kontextoption „Zugriff gewähren auf → Erweiterte Freigabe". Zugreifende Clients – Linux wie Windows – müssen sich mit einem Systemkonto (des Windows-Servers) und Kennwort ausweisen.

Freigaben von Linux: Auf dem Linux-Rechner muss die Serverkomponente von Samba installiert sein, was mit

```
sudo apt install samba samba-common
```

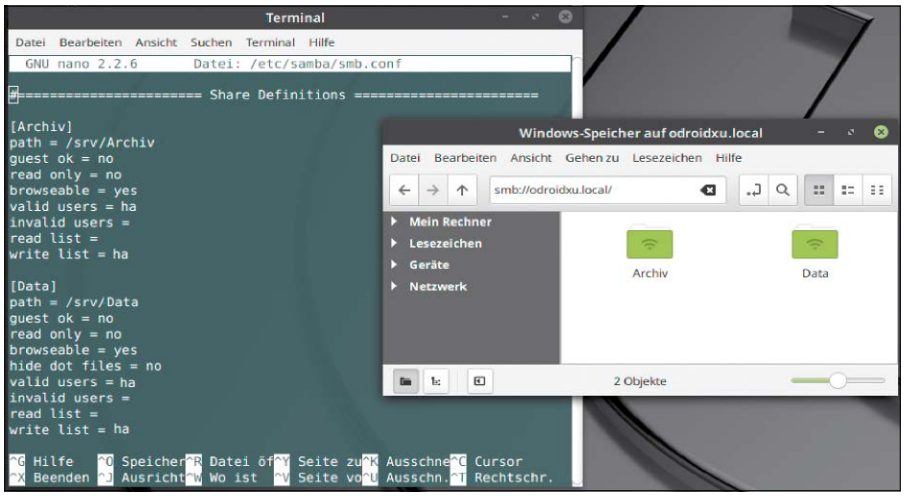
schnell erledigt ist. Der Serverdienst wird damit dauerhaft eingerichtet. Administrative Freigaben (auf eingeschränkte Benutzerfreigaben gehen wir nicht ein) sind über die zentrale Datei „/etc/samba/smb.conf" mit root-Recht (sudo) schnell angelegt. Eine neue Freigabe lässt sich am Ende der Datei unter „Share Definitions" im Minimalfall mit wenigen Zeilen erstellen:

```
[Daten]
path = /srv/daten
writeable = yes
write list = lw
```

Dieses Beispiel gibt das Verzeichnis „/srv/daten" unter der Bezeichnung „Daten" für das Konto „lw" frei. Der Benutzer „lw" muss ein Systemkonto (*sudo adduser lw*) und ein Samba-Konto besitzen (*sudo smbpasswd -a lw*), wobei der Einfachheit halber das identische Kennwort zu empfehlen ist. Änderungen an der Konfigurationsdatei „smb.conf" benötigen einen Neustart des Samba-Dienstes:

```
sudo systemctl restart smbd
```

Zugriffskomfort: Seit Jahren erscheinen Samba-Freigaben nicht mehr unter „Netzwerk" im Windows-Explorer, Windows-Freigaben nicht mehr in den Linux-Dateimanagern. Es ist also mindestens einmal nötig, im Windows-Explorer manuell eine Samba-Adresse wie „\\192.168.178.20", im Linux-Dateimanager „smb://192.168.178.20" einzugeben. Die Adresse lässt sich dann im Windows-Schnellzugriff dauerhaft anheften, analog unter Linux als Lesezeichen („Lesezeichen → Lesezeichen hinzufügen").



Samba-Freigabe in der „smb.conf": In diesem Fall darf nur ein einziges Konto („ha") zugreifen – ob über Linux oder Windows, spielt keine Rolle.

3. SSH und Linux

SSH ist der Standard beim Fernzugriff auf Linux-Systeme und hat zwei Aspekte: Erstens lassen sich über das Netzwerk alle Terminaltools des Servers nutzen (auf Wunsch auch grafische Programme), zweitens ist das Transferprotokoll SFTP inklusive. SFTP beherrscht jeder Linux-Dateimanager: Die im Dateimanager eingegebene Adresse

```
sftp://192.168.178.20/srv/
```

öffnet das Verzeichnis „/srv" auf dem entfernten Rechner. Dabei muss sich der Zugriff mit einem gültigen Systemkonto und zugehörigem Systempasswort ausweisen. Zum Ausführen von Programmen am entfernten Server bringt jedes Linux die Clientkomponente („ssh") standardmäßig mit. Der Befehl

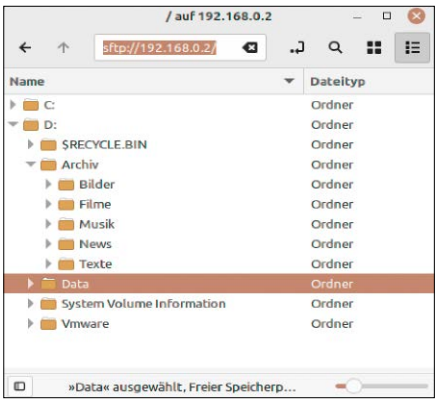
```
ssh lw@192.178.1.30
```

führt zum Prompt am entfernten System, der folgende Befehl

```
ssh lw@192.178.1.30 -t "mc /srv/"
```

startet ein bestimmtes Programm direkt. Den Start von grafischen Programmen ermöglichen die Schalter „-X" oder „-Y":

```
ssh -Y lw@192.178.1.30 -t gnome-
 disks
```



Datenzugriff und Mediennutzung: SSH impliziert das Datenprotokoll SFTP, das alle Linux-Dateimanager verstehen. In diesem Fall ist der Server offensichtlich ein Windows.

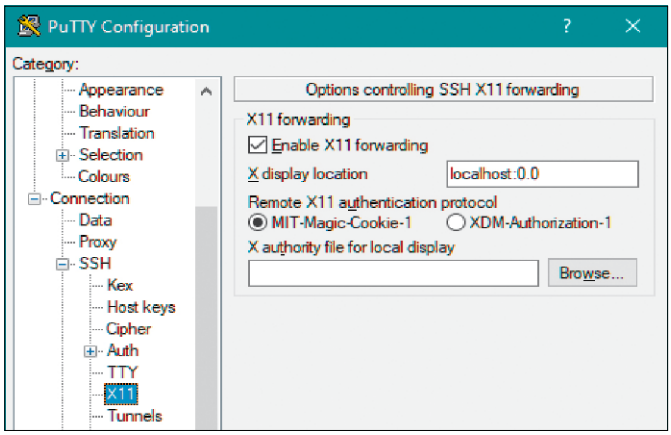
Diese Option macht aufwendigere Remotedesktop-Lösungen (siehe Punkt 7) für Linux so gut wie überflüssig. Im Prinzip ist SSH eine Allzweckwaffe im Netzwerk, die auf keinem Linux fehlen sollte. Die Installation der Serverkomponente ist mit

```
sudo apt install openssh-server
```

sofort erledigt. Damit läuft der Serverdienst dauerhaft und mit Standardwerten gemäß der Konfigurationsdatei „/etc/ssh/sshd_config".

4. SSH und Windows

Windows 11 und jedes aktualisierte Windows 10 bringen heute unter „\Windows\System32\OpenSSH" die volle Ausstattung für SSH mit (Client und Server). Die Syntax des Befehls ssh (Client) ist identisch mit jener unter Linux. Die Serverkomponente findet sich in der Dienstekonsole „Servi-



SSH-Client Putty: Für das Ausführen grafischer Linux-Programme ist das externe Tool nach wie vor die unkomplizierteste Wahl (im Bild die maßgebliche Einstellung).

ces.msc" als „OpenSSH SSH Server" und lässt sich dort ad hoc starten und mit Starttyp „Automatisch" auch als ständiger Dienst einrichten.

Windows als SSH-Server: Mit SSH-Server ist der Windows-Rechner genauso zu erreichen, wie Sie das von einem Linux-Server kennen. Über SFTP (Datenprotokoll von SSH) steht das komplette Dateisystem für den Datenaustausch zur Verfügung. Jeder Linux-Dateimanager wird also mit der Adresseingabe (Beispiel)

```
sftp://192.168.178.12/
```

das Dateisystem des Windows-Rechners anzeigen. Das erlaubt nicht nur das Kopieren von Daten, sondern auch die Nutzung von Medien.

Weniger produktiv ist der klassische Shell-Zugriff mit

```
ssh ha@192.168.0.12
```

auf einen Windows-SSH-Server – aus dem einfachen Grund, dass die Windows-Kommandozeile nicht so komfortable Tools besitzt wie etwa htop oder mc. Da auch typische Dateiwerkzeuge wie Rsync fehlen, bleibt die Kommunikation mit Linux eingeschränkt.

Windows als SSH-Client: Wer nur das Terminal eines entfernten Linux-SSH-Servers nutzen will, kommt mit dem nativen Windows-SSH-Client jederzeit ans Ziel. Weitergehende Optionen wie X11-Forwarding grafischer Linux-Programme sind hingegen erschwert. Hier ist der klassische SSH-Client Putty nach wie vor besser (siehe Punkt 5). Für den Datenaustausch mit SSH-Servern bleibt das externe Tool Filezilla weiter unentbehrlich (*www.filezilla-project.org*). Filezilla bietet das Protokoll SFTP an und erreicht SSH-Server mit seiner IP und den Authentifizierungsdaten („Verbindungsart: Normal").

SSH im Linux-Subsystem: Auf Umwegen lassen sich Einschränkungen von Windows als SSH-Client und Server umgehen: Wer unter Windows ein Linux-Subsystem laufen hat (siehe Punkt 6), erhält alle Linux-Standards hinsichtlich SSH. Das Subsystem kann im Unterschied zum Windows-Host auch typisches Linux-Werkzeug wie Rsync oder Midnight Commander installieren. Einziger Nachteil: Die Serverkomponente lässt sich hier nicht als Dauerdienst einrichten, sondern muss bei Bedarf manuell gestartet werden (*sudo service ssh start*).

5. Grafische Linux-Programme via SSH

Wie schon angesprochen, kann SSH auch grafische Programme (X11-Forwarding). Zuständig sind die Schalter „-X" oder „-Y" (weniger sicher, aber im lokalen Netzwerk vertretbar) beim Start der SSH-Sitzung am Clientrechner. Windows kann hier ohne Fremdhilfe nicht mitspielen, weil ein X-Server für die Fensterdarstellung erforderlich ist. Wer das Teamwork zwischen Linux und Windows optimieren will, sollte dieses Manko beheben. Ungeachtet mancher Alternativen wie X410, das im Microsoft Store für teures Geld angeboten wird, schlägt sich der altgediente, kostenlose Vcxsrv tadellos (früher Xming, Download *https://sourceforge.net/projects/vcxsrv*):

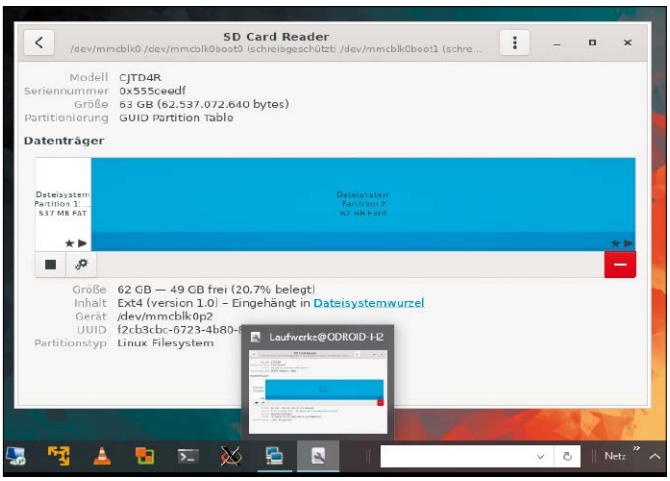
1. Starten Sie Vcxsrv nach der Installation unter Windows. Als „Display settings" ist „Multiple windows" am flexibelsten. Danach genügt „Start no client", weil Sie die Programme auf der Kommandozeile starten möchten. Mit dieser Einstellung lädt Vcxsrv erst mal nur den X-Server und wartet auf Gäste.

2. Beim nativen Windows-SSH-Client ist der Start grafischer Programme erschwert, weil sich keine Displayvariable für den X-Server setzen lässt. Verwenden Sie am besten Putty (*www.putty.org*) als SSH-Client (SSH im WSL-Subsystem geht aber auch, siehe Punkt 6). Die Basiskonfiguration in Putty ist einfach: Sie geben unter „Host Name" die IP-Adresse des Servers an, „SSH" ist als Verbindung voreingestellt. Vergeben Sie einen Namen unter „Saved Sessions", speichern Sie mit „Save" und öffnen Sie den Eintrag mit „Load", um weitere Details zu konfigurieren. Für grafische Programme wichtig ist die Option „Connection → Data → X11". Diese muss aktiviert werden und neben „X display location" tragen Sie „localhost:0.0" ein. Gehen Sie dann in der Navigation ganz oben auf „Session" und auf „Save".

3. Nach „Open" landen Sie zunächst im Terminal. Für dort gestartete grafische Programme übernimmt dann Vcxsrv die Darstellung:

```
firefox & disown
```

Somit lässt sich etwa der Browser eines sicheren Linux-Systems unter Windows nutzen – ohne Multiboot, ohne Virtualisierung.



Grafisches Linux-Laufwerkstool eines SSH-Servers unter Windows: Dazu braucht Windows einen X-Server (hier Vcxsrv), der vorher gestartet werden muss oder permanent läuft.

6. Grafische Linux-Programme aus dem Subsystem

Unter Umständen ist kein SSH erforderlich, um unter Windows grafische Linux-Software zu verwenden. Dann nämlich, wenn unter Windows WSL aktiv ist und dort eine Linux-Distribution installiert wurde. WSL – „Windows-Subsystem für Linux" – lässt sich unter „Systemsteuerung → Programme und Features → Windows-Features […]" installieren; Linux-Systeme für WSL gibt es in Menge im Microsoft Store.

1. Starten Sie unter Windows zunächst Vcxsrv, genauso wie in Punkt 5 für SSH beschrieben.

2. Starten Sie dann das Linux-Subsystem. Falls nur eines vorliegt, geht das am einfachsten mit dem Kommando „wsl".

3. Auf der Shell des Subsystems starten Sie die gewünschte Anwendung, etwa den Browser:

```
firefox & disown
```

Die Linux-Anwendung erscheint in der Taskleiste wie ein Windows-Programm und kann dort auch beendet werden. Falls ein Hinweis „no DISPLAY environment…" erscheint, dann öffnen Sie im Subsystem die Datei „~/.bashrc" und ergänzen dort entweder ganz am Anfang oder am Ende die folgende Zeile

```
export DISPLAY=localhost:0.0
```

und starten dann das Subsystem neu.

Natürlich müssen im Subsystem die grafischen Programme installiert sein, die Sie mit Vcxsrv auf den Windows-Bildschirm holen wollen. Installationen erfolgen mit dem dortigen Terminalpaketmanager dort wie gewohnt, also etwa mit apt

```
sudo apt install firefox […]
```

unter Debian/Ubuntu.

7. Linux-Remotedesktop

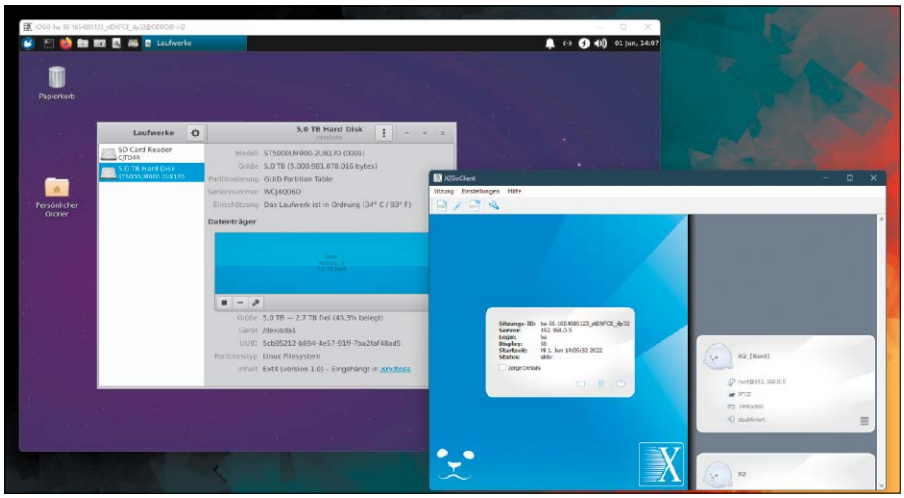
Remotedesktop-Lösungen bieten den Fernzugriff auf den kompletten Desktop. Als Remoteserver für Linux empfehlen wir ungeachtet schlankerer VNC-Alternativen das Tool X2go (*https://wiki.x2go.org*). Die X2go-Serverkomponente ist in den Standard-Paketquellen erhältlich:

```
sudo apt install x2goserver
```

Dabei wird die Software auch gleich dauerhaft als Systemdienst „x2goserver" eingerichtet. Die bevorzugte Desktopumgebung für X2go auf dem Serverrechner ist XFCE, die mittels

```
sudo apt install xubuntu-desktop
```

bei Bedarf nachgerüstet werden sollte. Beachten Sie, dass der Standarddesktop bestehen bleibt – die XFCE-Oberfläche wird nur für den X2go-Zugriff benötigt.



Linux-Server mit X2go: Wer den ganzen Desktop eines entfernten Linux-Rechners bedienen will, ist mit X2go gut beraten. Clients gibt es für Windows, Linux und Mac.

Den X2go-Remoteserver gibt es nur für Linux, X2go-Zugriffsclients hingegen für Linux, Windows und Mac-OS. Den passenden Client installieren Sie dann auf allen Systemen, die auf den Server zugreifen sollen. Unter Debian/Ubuntu kann dies mit

```
sudo apt install x2goclient
```

aus den Standardquellen erfolgen. Den Client für Windows gibt es auf *https://wiki.x2go.org* unter „Download" („mswin").

Im X2go-Client legen Sie mit „Sitzung → Neue Sitzung" den neuen Server an. Hinter „Sitzungsname" vergeben Sie eine Bezeichnung und neben „Host:" tragen Sie die IP-Adresse des Servers ein. Hinter „Login" geben Sie das Systemkonto am Serversystem ein. Unter „Sitzungsart" wählen Sie idealerweise „XFCE" – sofern zutreffend. Weitere Optionen wie „Freigegebene Ordner" können den Austausch zwischen Client und Server optimieren.

Nach Doppelklick auf einen gespeicherten Eintrag müssen Sie nur noch das Systemkennwort eingeben und sich mit „OK" verbinden. Die saubere Methode, eine X2go-Sitzung wieder zu beenden, ist nicht der „Beenden"-Knopf des X2go-Fensters, sondern eine Abmeldung im Remote-Fenster – also über das Hauptmenü oder das Sitzungsmenü.

8. Windows-Remotedesktop

Die Serverkomponente des Remotedesktops fehlt in Windows Home und ist nur in Pro-Editionen enthalten (ein wichtiges Argument für Pro). Liegt diese vor, kann der Serverdienst unter „Einstellungen → System → Remotedesktop" aktiviert werden. Damit kann sich nun jedes weitere Windows mit der Clientkomponente „Remotedesktopverbindung" (mstsc.exe) mit diesem Rechner verbinden. Dabei reicht im Prinzip die Angabe der IP-Adresse des Zielrechners. Für häufigeren Zugriff lohnt es sich aber, die weiteren Optionen durchzugehen, die Einstellungen als RDP-Datei abzuspeichern und die Verbindung künftig damit zu starten.

Linux-Rechner verbinden sich am besten mit Remmina. Remmina („Betrachter entfernter Schreibtische") ist oft vorinstalliert und beherrscht neben Linux-Protokollen auch Windows RDP. Falls Remmina fehlt, hilft diese Nachinstallation:

```
sudo apt install remmina remmina-
  plugin-rdp
```

In Remmina klicken Sie auf die „+"-Schaltfläche und tippen hinter „Bezeichnung" einen Namen für die Verbindung ein. Hinter „Protokoll" stellen Sie „RDP" ein. Bei „Server" tragen Sie die IP-Adresse des Windows-Rechners ein, bei „Benutzername" und „Benutzerpasswort" die Anmeldedaten für das Windows-System. Auch hier lohnt es sich, alle Einstellungen durchzugehen, vor allem die Qualitätsoptionen unter „Erweitert". Später genügt ein Doppelklick auf den Eintrag.

Am Windows-Desktop kann nur ein Benutzer arbeiten. Die Remote-Anmeldung ist nur möglich, wenn das System aktuell nicht benutzt wird oder der Benutzer dieses auf Zuruf oder Anruf verlässt. ■

Das neue Linux Mint 21

Linux Mint 21 ist das Desktop-Linux schlechthin, hat sich im Gegensatz zu Ubuntu ganz dieser Rolle verschrieben und rangiert auf distrowatch.com deutlich vor seiner Ubuntu-Basis. Version 21 bleibt seinem Kurs treu, auf die Desktopnutzer zu achten.

VON HERMANN APFELBÖCK



2022 ein neues Linux Mint 21: Der Mint-Versionszähler will es so – der ist unabhängig von der Jahreszahl und wird erst 2024 die „22“ erreichen. Linux Mint 21 „Vanessa“ basiert auf Ubuntu 22.04 LTS und wird als Langzeitversion fünf Jahre versorgt – also bis 2027. Genau wie seine Ubuntu-Basis verwendet Version 21 den nicht mehr ganz taufrischen Linux-Kernel 5.15 vom Oktober 2021, der aber wichtige Verbesserungen für die Dateisysteme Ext4, BTRFS und NTFS sowie für Samba-Netzwerkfreigaben enthält. Wie gewohnt wird es auch eine „Edge“-Version von Linux Mint 21 mit jüngerem Kernel, im aktuellen Fall mit Kernel 5.17 geben, die allerdings zum Zeitpunkt dieses Artikels noch nicht zur Verfügung stand.

Traditionell bietet Linux Mint 21 neben der Hauptedition mit dem angestammten Cinnamon-Desktop die alternativen Ausgaben mit Mate und XFCE. Diese zusätzlichen Mint-Editionen erhalten natürlich alle allgemeinen Neuerungen bei Kernel, Systembasis, Installer, X-Apps und Programmversionen, verbleiben aber mit Mate 1.26 und XFCE 4.16 bei den Desktopversionen des Mint-Vorgängers. Daher gibt es keinen Grund, auf diese Editionen nachfolgend spezieller einzugehen.

Keine der drei Editionen stellt hohe Hardwareansprüche. Als Minimalanforderung nennt das Mint-Team ohne Differenzierung für alle drei Ausgaben mindestens zwei (empfohlen: vier) GB RAM und 20 (empfohlen: 100) GB auf Festplatte. Dies sind Ansprüche, die heutzutage allenfalls für virtuelle Maschinen eine Überlegung wert sind. Wer dort RAM sparen will, kommt für die XFCE-Edition tatsächlich auch noch mit zwei GB RAM aus. Eine ältere Dualcore-CPU mit Zwei-GHz-Takt ist für XFCE ausreichend, für Cinnamon und Mate darf es auch etwas moderner sein.

ISO-Downloads und Heft-DVD

Linux Mint liegt zu Redaktionsschluss als Version 21.1 vor. Sie erhalten die Version wie gewohnt über die Projektseite *https://linuxmint.com/download.php*. Der Download umfasst für alle Varianten circa 2,5 GB und ist kostenlos. Das ISO-Image kann dann mit den üblichen Mitteln (Etcher, Win 32 Disk Imager, Gnome-Disks) bootfähig auf USB kopiert werden, um es danach am Zielrechner zu booten und das System mit dem Livemedium zu installieren. Linux-Welt-Leser, welche die Hauptedition mit Cinnamon neu installieren möchten, können die beiliegende Heft-DVD verwenden. Nähere Anleitungen, das System neu zu installieren oder die ältere Version 20.3 auf „Vanessa“ zu hieven, lesen Sie im nachfolgenden Artikel. Dort gehen wir auch auf das runderneuerte Tool „Mintupgrade“ für Linux Mint 20.3 näher ein. Dieses Werkzeug erschien rechtzeitig zur Version 21, hat seinen Platz aber natürlich auf dem Vorgängersystem 20.3.

Frische Software mit klassischem Firefox

Erwartungsgemäß liefert Mint 21 neben erneuerter Kernel- und Ubuntu-Basis frische Softwarepakete mit – unter anderem Firefox 103, Thunderbird 91.11 und Libre Office 7.3.5. Aus unserer Sicht eine der größten und erfreulichsten Überraschungen in Linux Mint 21 ist der Firefox als klassisches DEB-Paket, das fortan offenbar vom



Firefox als klassisches DEB-Paket: Der Browser nennt sich „Mozilla Firefox for Linux Mint“ und wird jetzt offensichtlich vom Mint-Team aktuell gehalten.

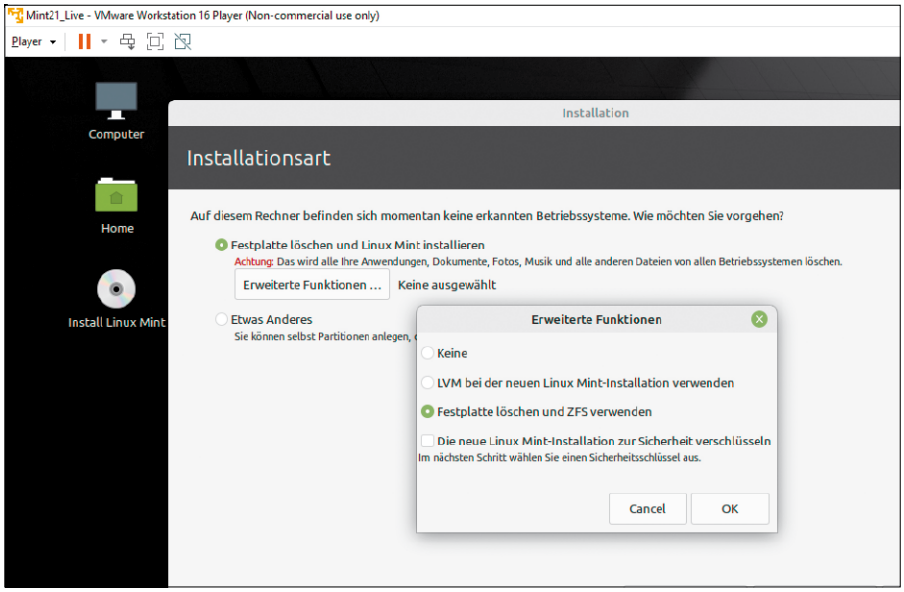
Mint-Team gepflegt wird. Der Browser heißt jetzt „Mozilla Firefox for Linux Mint mint-001 - 1.0“ (siehe „Hilfe → Über Firefox“). Somit bleibt sich Linux Mint bei der Verweigerung von Snap-Containern und verschmäht die einfache Übernahme des Firefox-Snaps aus den Ubuntu-Quellen. Damit war zu rechnen, jedoch war es wahrscheinlicher, dass Mint zu einem anderen Standardbrowser wie Chromium greifen würde, statt sich die Pflege der Firefox-Updates ans Bein zu binden.

Dem Anwender sollte es recht sein: Er erhält damit weiterhin den sympathischen Open-Source-Browser als flotte DEB-Installation. Und für Firefox bedeutet dies echte Wertschätzung und aktive Unterstützung.

Hinweis: In Ablehnung des proprietären Snapstores von Ubuntu/Canonical (snapcraft.io) schlägt sich Linux Mint bekanntlich auf die Seite des offenen Flatpak-Containerformats. Flatpak-Software ist sowohl über die „Anwendungsverwaltung“ als auch über das Terminaltool flatpak zu beziehen. Allerdings hält sich Linux Mint auch in Version 21 zurück und bietet dies nur als Option an. Standardmäßig ist keine einzige Flatpak-Software vorinstalliert.

Setupoptionen: Ecrypt FS und ZFS

Nach wie vor hält Linux Mint fest an der einfachen Home-Verschlüsselung mit Ecrypt FS. Die Option „Meine persönlichen Daten verschlüsseln“ erscheint im Installationsprogramm beim Anlegen des primären Benutzerkontos im Dialog „Wer sind Sie?“. Beachten Sie, dass Ubuntu diese Option mit Ecrypt FS schon seit 2018 als zu unsicher verworfen hat. Andererseits hat Linux Mint nicht unrecht, wenn es diese Home-Verschlüsselung weiterhin als bequem (korrekte Nutzeranmeldung öffnet den „Home-Tresor“) und die Sicherheitsbedenken als akademisch einstuft. Trotzdem: Wer auf Nummer sicher gehen will, entscheidet sich an früherer Stelle des Setups („Installationsart“) unter „Erweiterte Funktionen“ für LVM und „...Installation...verschlüsseln“.

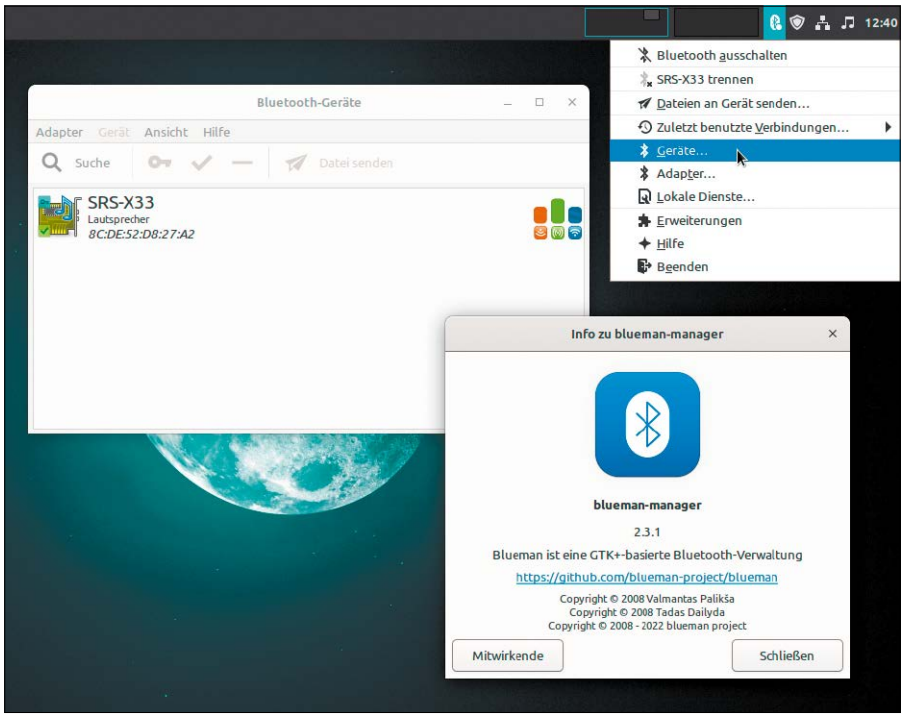


Installer mit ZFS-Angebot: Ubuntu hat dieses überdimensionierte Dateisystem seit 2019 im Installer. Linux Mint tilgte diese Option lange Zeit, zieht aber jetzt mit Version 21 nach.

ZFS-Unterstützung: So gar nicht zur Desktopausrichtung von Linux Mint passt die neue Option des ZFS-Dateisystems im Installationsprogramm. Diese wird jetzt erstmals vom originalen Ubuntu-Installer übernommen und findet sich im Dialog „Installationsart“ unter „Erweiterte Funktionen“. Wir raten auf allen typischen Desktoprechnern mit vier bis 16 GB RAM von dieser Möglichkeit ab. ZFS ist ein beeindruckendes Dateisystem, gehört aber eindeutig auf große Server mit sehr großer Speicherausstattung und einem großen Datenträgerpool. Als notwendige Konsequenz dieser Installationsoption muss Linux Mint 21 dann auch eine ganze Reihe von Systemdiensten für ZFS mitbringen. Die sind allesamt unnötig, falls Linux Mint 21 mit einem Standarddateisystem wie Ext4 installiert wird. Im später folgenden Special zu systemd können Sie nachlesen, wie Sie überflüssige ZFS-Dienste auf Wunsch abschalten.

Bluetooth-Manager Blueman

Die Ablösung des bisherigen Blueberry-Applets – eine X-App des Mint-Teams – erfolgt nicht freiwillig. Das grafische Front-End für Gnome Bluetooth wurde schlicht



Ablösung beim Bluetooth-Manager: Blueman ist funktionsreicher als der Vorgänger Blueberry.

inkompatibel und musste ersetzt werden. Als Nachfolger ist jetzt Blueman an Bord, der sich problemlos in alle drei für Linux Mint relevanten Desktops integriert (Cinnamon, Mate, XFCE). Der geänderte Bluetooth-Manager erscheint wie sein Vorgänger als Applet in der Systemleiste. Optisch ist Blueman gegenüber dem Vorgänger Blueberry kein Gewinn, aber dafür bietet er bessere Konnektivität für Audiogeräte und mehr Funktionen. Zur erweiterten Funktionalität gehört auch die Tatsache, dass alle Einstellungen und Bluetooth-Geräte nicht nur über das grafische Applet (bluemantray), sondern auch komplett über das Terminal anzusteuern sind. Dafür zuständig sind die Unterprogramme blueman-manager und blueman-adapters (und weitere).

Wertvolle Ubuntu-Korrekturen

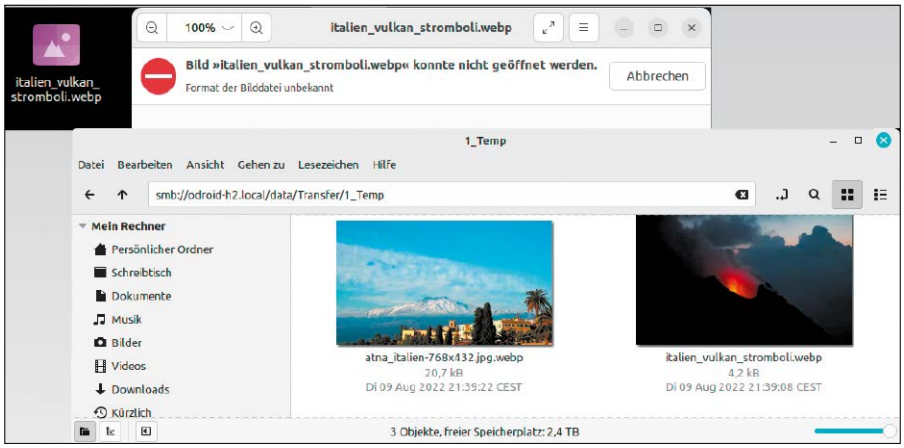
1. Kein Ubuntu-Programmkiller: Ubuntu 22.04 LTS hat einen neuen kleinen systemd-Dienst eingeführt: systemd-oomd steht für „out of memory“ („oom“, das schließende „d“ ist Standard bei systemd-Diensten) und ist ein Killer von Benutzerprogrammen, wenn ernste Speicherengpässe drohen. Im Prinzip ist es richtig, das Gesamtsystem vor einem drohenden Stillstand zu schützen, aber systemd-oomd arbeitet offenbar zu aggressiv und schießt Anwendungen wie Gimp oder Libre Office allzu voreilig ab. Eine sensiblere Version ist zwar in Arbeit, aber darauf wollte sich das Mint-Team offenbar nicht verlassen. Linux Mint 21 hat den Killerdienst nicht übernommen.

2. Bibliothek für Appimages: Bei Ubuntu 22.04 war es sicher nur ein Versehen und Linux Mint 21 hatte seit April ausreichend Zeit, von dieser peinlichen Panne zu erfahren und sie jetzt zu vermeiden: In Ubuntu 22.04 fehlt nämlich eine winzige Bibliothek (libfuse2) mit der Konsequenz, dass Software im relativ verbreiteten Appimage-Containerformat beim Start kommentarlos den Dienst verweigert. Die kleine Bibliothek ist natürlich schnell nachinstalliert, wenn man die Ursache kennt, aber Linux Mint 21 bringt die Datei natürlich wieder standardmäßig mit.

3. Kein Dualboot-Problem: Nach Installationen von Ubuntu 22.04 neben Windows fehlt unter Umständen der Eintrag für Windows im Grub-Menü. Das ist kein destruktiver Bug, weil das Windows-System existiert und funktioniert und nur der Menüeintrag fehlt. Schuld ist die abgeschaltete Grub-Komponente os-prober zur Erkennung von weiteren Betriebssystemen. Linux Mint 21 hat diese Komponente wieder standardmäßig aktiviert. Diese Maßnahme ist benutzerfreundlich, andererseits durchaus kontrovers zu bewerten, denn der os-prober wurde nach (akademischen?) Sicherheitsbedenken in diversen Distributionen deaktiviert – nicht nur unter Ubuntu.

Kleinigkeiten bei den X-Apps

Schon Linux Mint 18 (2016) hatte die ersten X-Apps eingeführt. Es handelt sich um Gnome-Zubehör wie Gedit (Texteditor) oder Totem (Videoplayer), das unabhängiger von Gnome werden und optisch für alle GTK-Oberflächen passen soll, also unter anderem zu den drei Mint-Desktops Cinnamon, Mate, XFCE. Xed (Gedit), Xplayer (Totem), Xviewer (Eog) und Xreader (Evince) waren die frühesten Vertreter, inzwischen sind die Eigenentwicklungen Warpinator (Netzaustausch), Bulky (Renamer), Thingy („Zuletzt verwendet“-Bibliothek) hinzugekommen. Version 21 übernimmt jetzt auch Timeshift in die vom Mint-Team gepflegten X-Apps. Für die Mint-Nutzer bedeutet dies gut gepflegte Zubehörprogramme, die in anderen Distributionen gänzlich fehlen (Warpinator, Thingy, Bulky, Webapp-Manager) oder dort



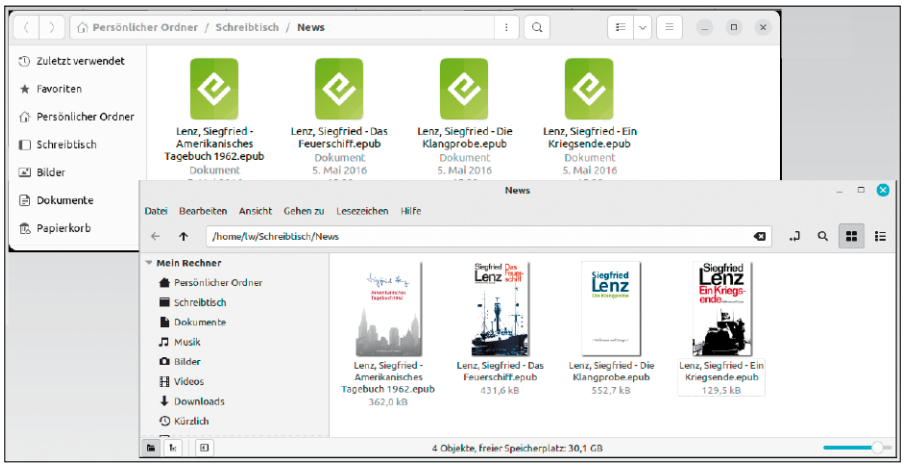
Mint beherrscht das Webp-Bildformat: Während Ubuntu mit Eog (oben) das Format verweigert, ist die X-App (Xviewer) in Linux Mint 21 dafür gerüstet (unten).

nicht dieselbe Funktionalität bieten (Xed, Xplayer, Xviewer, Xreader). Die funktionalen Vorteile bleiben aber oft bei marginalen Details. Auch für Mint 21 meldet der Mint-Chef Lefèbvre nur Kleinigkeiten bei Xviewer, Bulky und **Webapp-Manager.** Letzterer ist ein hübsches Tool, um Websites wie ein isoliertes lokales Programm abzulegen, und unterstützt dabei jetzt neben Firefox und Chrome weitere Browser.

Das Snapshot- und Sicherungstool **Timeshift** ist seit Versionen als oberste Benutzerpflicht fest in Linux Mint integriert. Auch diese Software gehört ab sofort zu den X-Apps des Mint-Teams. Dies geschieht nicht ganz freiwillig, nachdem der bisherige Timeshift-Entwickler neue Wege einschlägt.

Eine wirklich nützliche Ergänzung ist die **Webp-Bildunterstützung:** Das von Google seit 2010 entwickelte Webp-Bildformat wird langsam, aber unaufhaltsam populärer. Insbesondere Websites profitieren von der Kombination guter Bildqualität bei geringer Größe. Browser haben mit dem Format längst kein Problem, Dateimanager oder Bildviewer hingegen schon. Unter Ubuntu zeigt der Dateimanager keine Thumbnails für Webp-Bilder und der Bildbetrachter (eog) meldet „Format unbekannt". Unter Linux Mint 21 beherrscht das Format sowohl die X-App Xviewer als auch der Dateimanager Nemo (via „Thumbnailer", siehe unten). Auch die Übernahme als Hintergrundbild ist problemlos.

Thumbnailers für mehr Icons: Eine kleine, aber hübsche Komfortfunktion ab Linux Mint 21 nennt sich Thumbnailers. Dahinter verbirgt sich eine kleine Sammlung von X-Apps (zum Beispiel xapp-epub-thumbnailer), welche die Vorschaufunktion im Dateimanager Nemo verbessern. Es handelt sich also um keine Benutzerprogramme, sondern um Hintergrundhelfer für Nemo und sie treten nur dann in Aktion, wenn in den Nemo-Einstellungen unter „Vorschau" die Vorschaubilder aktiviert sind (dies übrigens nur bei lokalen Dateien, nicht im Netzwerk). Aktuell unterstützte Formate sind Appimage, MP3, Epub, Webp, RAW-Bilder.



Nautilus in Ubuntu und Nemo in Mint: Während Nautilus (oben) nur ein generisches Icon anzeigt, kann Nemo (unten) dank des Epub-Thumbnailers Inhaltliches anbieten.

Cinnamon 5.4: Umbau ohne Highlights

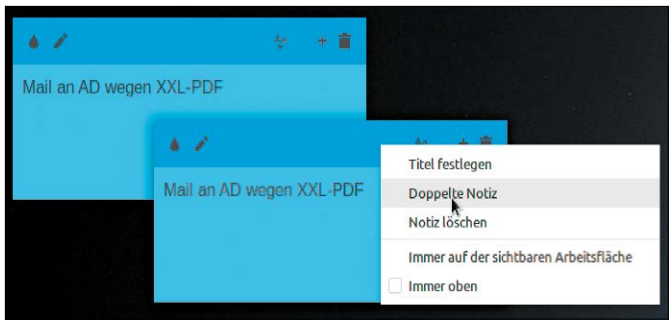
Alle Infos bis hierher gelten für alle Mint-Editionen. Dieser letzte Abschnitt bezieht sich ausschließlich auf den Cinnamon-Desktop der Hauptedition. Die Änderungen bei Cinnamon 5.4 sind unter der Haube zwar bedeutsam, haben aber nur geringe Auswirkung auf Funktionalität und Bedienung. Dem Mint-Team ging es vor allem darum, den Fenstermanager Muffin (eine inzwischen uralte Abspaltung des Gnome-Fenstermanagers Mutter) wieder näher an seine „Mutter" zu bringen. Damit wird es künftig wieder einfacher, nützliche Codeanpassungen bei Gnome/Mutter nach Cinnamon/Muffin zu portieren.

Dies hat vorerst zum Teil auch nachteilige Konsequenzen: Cinnamon lässt die detaillierte Anpassung der Fenstereffekte unter den Tisch fallen. Eine Basiskonfiguration unter „Systemeinstellungen → Effekte" bleibt aber bestehen. Ein echtes Opfer des aktualisierten Desktops ist die beliebteste aller Cinnamon-Erweiterungen „Transparente Leisten" (siehe „Systemeinstellungen → Erweiterungen → Herunterladen"). Sie lässt sich installieren, funktioniert aber nicht mehr. Ob auch andere Erweiterungen betroffen sind, haben wir nicht systematisch getestet.

Andererseits verspricht Cinnamon 5.4 verbesserte fraktionelle Skalierung (siehe „Systemeinstellungen → Bildschirm"), ein verbessertes Applet „Schreibtisch anzeigen" zur Desktopanzeige, eine vereinfachte Konfiguration für „Aktive Ecken" sowie verbesserte Menü-, Sound- und Power-Applets in der Systemleiste. Alle diese Neuerungen dürften sich aber primär auf Fehlerbehebungen beziehen und sind nicht funktionsreicher als bisher.

Neues Leistensymbol: Eine kleine Zusatzinfo ist hinzugekommen. Automatisierte Vorgänge wie die Systemaktualisierung oder Timeshift-Snapshots melden sich jetzt mit einem Zahnradsymbol in der Systemleiste. Dies soll den Benutzer informieren, dass das System durch Hintergrundprozesse beansprucht ist und eventuell etwas langsamer reagiert. Beachten Sie aber, dass dieses Symbol nichts über die tatsächliche Systembelastung aussagt, die eventuell trotz dieser Prozesse moderat bleibt.

Wayland? Trotz Umbauarbeiten bleibt der Cinnamon-Desktop weiterhin ausschließlich beim Xorg-Fensterprotokoll. Diesbezüglich liegt Cinnamon derzeit technisch deutlich hinter Gnome und KDE. Die ganz große Eile ist für dieses Linux-Langzeitprojekt aber nicht geboten, zumal sich auch für Wayland-taugliche Desktops aktuell immer noch X11/Xorg empfiehlt. ■



Sticky Notes (Desktopnotizen): Das kleine Zubehör erhält jetzt eine Kopieroption – eine Marginalie, die der Haupttext unter den Tisch fallen lässt.

Upgrade, Installation, Einrichtung

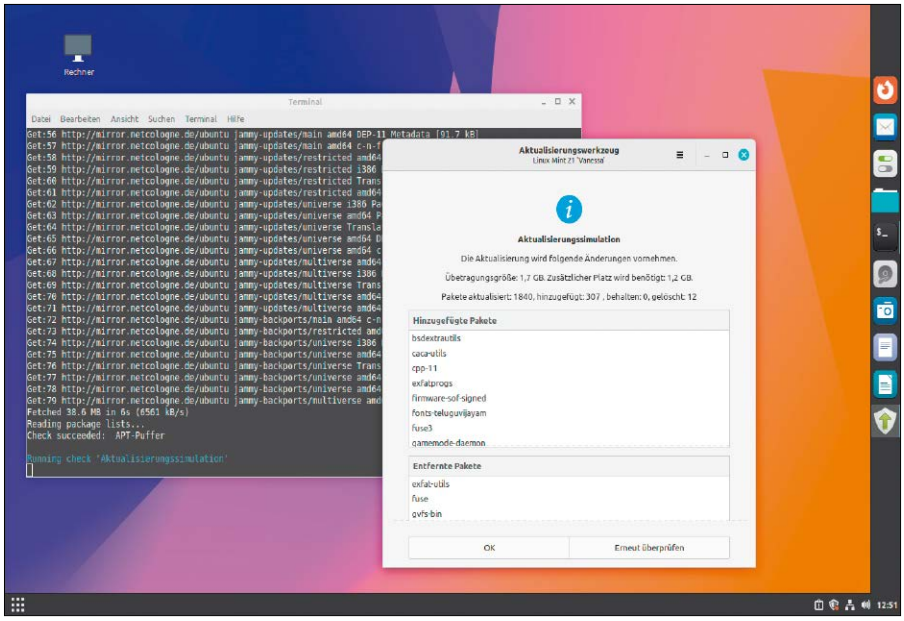
Dieser Beitrag bringt Linux Mint 21 und 21.1 auf den Rechner und erläutert Einrichtungspflichten und erste Optimierungsschritte. Bei den meisten Aufgaben unterscheidet sich Version 21 nicht von den Vorgängern, daher halten wir die Infos fokussiert und knapp.

VON HERMANN APFELBÖCK

Linux Mint war lange „upgrade-scheu“, danach immer noch skrupulös bei externen Paketquellen. Das neue Upgradetool macht den Vorgang toleranter, fehlertoleranter und nach unserer Erfahrung risikolos. Für Neuinstallationen gilt die bekannte Sorgfaltspflicht hinsichtlich Uefi- und Bios-Modus, insbesondere wenn bereits ein System vorliegt. Ansonsten bleibt der Installer in Linux Mint 21.1 mit einer kleinen Ausnahme unverändert. Und für alles, was nach einer Neuinstallation notwendig oder empfehlenswert ist, gelten ebenfalls die bekannten Regeln.

Upgrade von Version 20.3 auf 21

Der häufigste Weg zur Version 21 ist sicher nicht die Neuinstallation, sondern das Upgrade. Für das Upgrade des Vorgängers 20.3 gibt es ein völlig neu geschriebenes grafisches Tool „mintupgrade“. Das Werkzeug erledigt diverse Checks, prüft die Erreichbarkeit der eingestellten Paketquellen (Spiegelserver), erlaubt auch eventuell vorhandene externe Quellen wie PPAs und löst Konfliktsituationen. Wie tief die Problemerkennung tatsächlich geht, können wir schlecht abschätzen, da sich in unserem Fall keine Konflikte ergaben. Dass die Mint-Entwickler aber gewiss nicht an jede Situation und jede Nutzerdummheit gedacht haben, lässt sich daran ablesen, dass das mintupgrade auch auf einem nagelneu installierten Mint 21 alle Phasen brav durchläuft, um am Ende zu melden, dass es hier „0 Bytes“ und „0 Pakete“ zu installieren gibt.



Verbessertes Upgradetool für Version 20.3: Das Upgrade auf Mint 21 akzeptiert auch Fremdquellen und ist damit toleranter als alle Vorgänger.

Das Werkzeug macht natürlich nur auf dem Vorgänger Linux Mint 20.3 Sinn. Bevor Sie es mittels

```
sudo apt install mintupgrade
```

installieren, bringen Sie erst das System mit *sudo apt update* und *sudo apt upgrade* auf den aktuellen Stand. Starten Sie dann das Tool im Terminal:

```
sudo mintupgrade
```

Das grafische Fenster dient nur als Assistent, der einige „OK“- und bei Bedarf „Beheben“- und „Prüfen“-Klicks entgegennimmt. Begleitend läuft die eigentliche Aktion im Terminal, das umfassend über jeden einzelnen Schritt informiert. Der grafische Assistent ist deutsch übersetzt, die Terminalausgabe englisch.

Neuinstallation mit dem Mint-Livesystem

Die Cinnamon-Edition 21.1 können Sie mit der Heft-DVD installieren. Die ISO-Abbilder aller der drei Mint-Editionen finden 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 gewünschte ISO-Image schreiben Sie nach dem Download mit einem Werkzeug wie Etcher, Win 32 Disk Imager (unter Windows) oder Gnome-Disks auf einen USB-Stick und booten damit Ihr Zielgerät. Ob Heft-DVD oder ISO-Download – es handelt sich in jedem Fall um ein Livesystem, das das Ausprobieren der je-

weiligen Edition ermöglicht und die Installation über den Desktoplink „Install Linux Mint“. Alle drei Mint-Editionen verwenden das identische Installationsprogramm.

Das leidige Installationsthema Bios/MBR versus Uefi/GPT nötigt zu einer Reihe von Fallunterscheidungen, die man aber relativ einfach abkürzen kann: Der moderne Uefi/GPT-Partitionsstil ist eigentlich stets zu bevorzugen, egal ob eine Solo- oder eine Multibootinstallation erfolgen soll. Für den Einsatz von Bios/MBR gibt es nur genau zwei Ausnahmen:

1. Linux Mint soll im Multiboot neben einem anderen System installiert werden, das im Bios-Modus vorliegt (das ist dann in jedem Fall ein weiteres Linux, da Windows immer Uefi/GPT verwendet).

2. Linux Mint soll auf USB installiert werden.

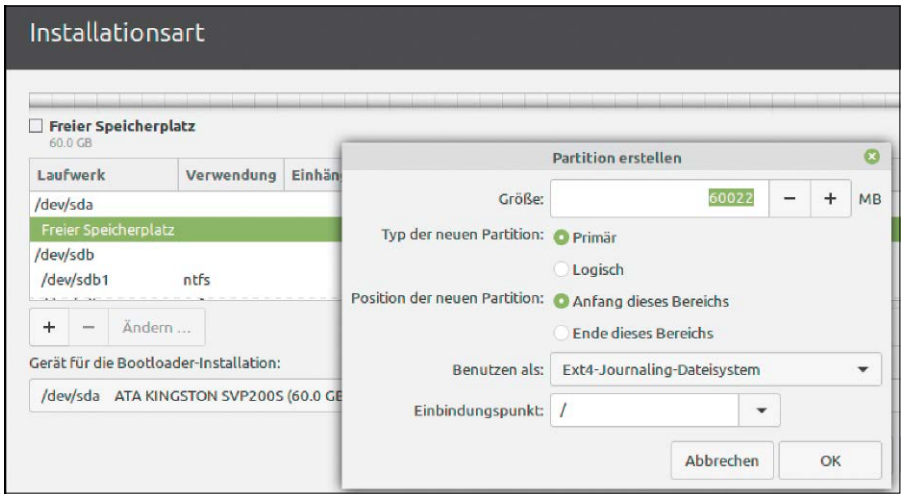
Den aktuellen Partitionsstil eines existierenden Systems können einschlägige Tools ermitteln – unter Windows die „Datenträgerverwaltung“, unter Linux Mint das Standardwerkzeug Gnome-Disks. Uefi/GPT erscheint hier als „GUID Partition Table“, der Bios/MBR-Modus als „Master Boot Record“. Ist dann entschieden, ob Sie mit Uefi/GPT oder aufgrund der genannten Ausnahmen mit Bios/MBR-Partitionstabelle installieren müssen, dann booten Sie das Installationsmedium (etwa unsere Heft-DVD) im passenden Modus. Dazu verwenden Sie nach dem Einschalten des Zielgeräts das Bootmenü des Bios (Taste F2, F8, F12 oder Esc – leider nicht standardisiert) und wählen den Datenträger mit dem Installationsmedium. Der sollte dort zweimal erscheinen – einmal mit „Uefi“ und einmal ohne (das ist der Bios-Modus).

Der Installer Ubiquity

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

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

B. 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 [...]“.



Um eines von mehreren bestehenden Systemen durch Mint zu ersetzen, müssen Sie die Partition löschen und den „freien Speicherplatz“ mit Ext4 ausstatten. Einhängepunkt ist „/“.

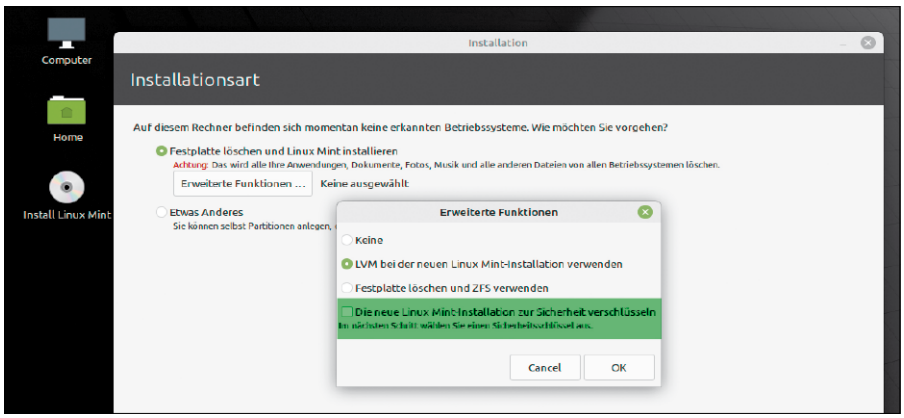
Wenn Sie Linux Mint als alleiniges System verwenden wollen und ein eventuell bestehendes System nicht mehr brauchen, wählen Sie in beiden Situationen die Option „Festplatte löschen“. Dabei wird die Festplatte formatiert, der Datenbestand (und ein eventuelles System) gelöscht und das neue System eingerichtet.

Wenn Sie das bestehende System benötigen, wählen Sie die Option „Linux Mint neben Windows Boot Manager installieren“ (so bei einem installierten Windows). 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 Partitionsgrößen justieren Sie mit der Aufteilungsmarkierung und der Maus.

Eine weitere Multiboot-Installation ergibt sich auf einem Rechner, der bereits zwei oder mehr Systeme enthält, und nun eines der bestehenden Systeme durch Linux Mint ersetzt werden soll. In diesem Fall wählen Sie im Fenster „Installationsart“ den Punkt „Etwas Anderes“. Dort löschen Sie in der Laufwerkliste 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“.

Der Installer: Erweiterte Optionen

Wie schon im voranstehenden Artikel angesprochen, übernimmt Linux Mint 21 gemäß Ubuntu die Installationsoption mit ZFS-Dateisystem. Die Option erscheint im Dialog „Installationsart“ unter „Erweiterte Funktionen“. Davon raten wir auf allen Desktopsystemen generell ab, da sie nur RAM kostet und bei typischen Festplattenkapazitäten keine Vorteile bringt. Unter



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

„Erweiterte Funktionen“ gibt es aber auch noch den Punkt „LVM...verwenden“, der dann die Verschlüsselung der Mint-Installation freischaltet. Diese Partitionsverschlüsselung (Cryptsetup) ist vor allem für mobile Notebooks die beste Wahl für zuverlässigen Datenschutz. Sie ist sicherer und performanter als die Home-Verschlüsselung (die das Mint-Setup im späteren Dialog „Wer sind Sie?“ weiterhin anbietet). Im späteren Benutzeralltag muss nur bei jedem Systemstart die Partition mit dem Passwort aufgeschlossen werden.

Einzige Einschränkung: LVM und Partitionsverschlüsselung setzen voraus, dass Sie Linux Mint die gesamte primäre Festplatte überlassen. Multiboot oder komplexere Partitionsaufteilungen sind nicht vorgesehen. Die Festplatte muss folglich leer sein oder darf nur noch Daten enthalten, die Sie nicht mehr benötigen.

Pflichten nach dem Setup

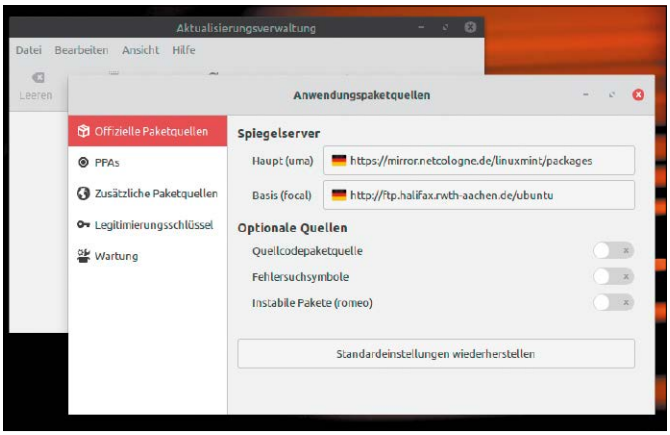
Nach einer Neuinstallation sind einige Einstellungen und Nachbesserungen unverzichtbar. Einige, aber nicht alle wichtigen Aufgaben zeigt der „Willkommen“-Bildschirm (mintwelcome) unter „Erste Schritte“.

Aktualisierungsverwaltung: Das Wichtigste ist zunächst ein erster Besuch in den Paketquellen. Daher gehen Sie in die „Aktualisierungsverwaltung“ und klicken auf „Auffrischen“ und danach auf „Aktualisierungen installieren“. Gleichbedeutend dazu sind diese Terminalbefehle:

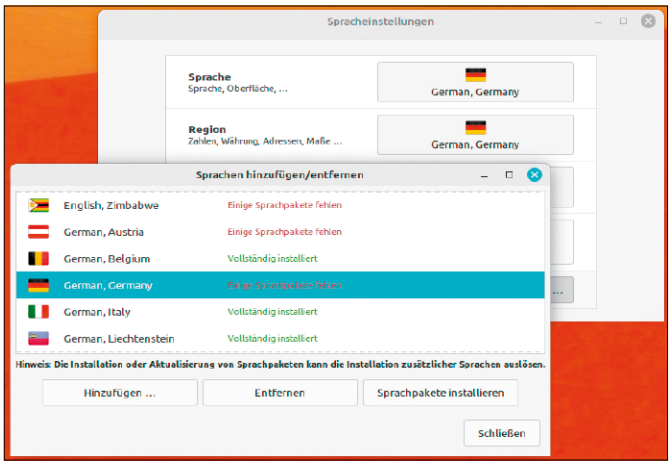
```
sudo apt update
sudo apt upgrade
```

Ab sofort ist dann auch die Installation zusätzlicher Software möglich. Feineinstellungen der Aktualisierungsverwaltung finden Sie unter „Bearbeiten → Einstellungen“. Unter „Optionen“ ist der Abschnitt „Automatisch auffrischen“ der wichtigste. Aktivieren Sie diese Option, damit das System am Spiegelserver automatisch nachsieht, ob neue Updates bereitstehen.

Eher unkritisch sind die Zeitintervalle: Der Punkt „Erstmals auffrischen“ bezieht sich auf den Systemstart. Setzen Sie die Voreinstellung mit „10“ Minuten deutlich nach hinten, wenn Sie nach Start das System üblicherweise erst mal intensiv nutzen. Weitere Updatechecks sind dann nicht alle zwei Stunden erforderlich (Voreinstellung) und können auf „Tage“ erhöht werden, sodass sie für normale Sitzungen komplett entfallen.



Der heiße Draht zu Updates und Software: Schnelle regionale Spiegelserver nützen Ihnen und den Distributionsanbietern (Mint und Ubuntu) gleichermaßen.



Nach der Installation fehlen immer einige deutsche Sprachpakete. Dies korrigieren Sie unter „Systemeinstellungen → Sprachen“.

Spiegelserver: Eine frühe Aktion, die sich gleich nach der Installation lohnt, ist die Auswahl optimaler Spiegelserver unter „Anwendungspaketquellen“: Spiegelserver sind die beiden Webserver mit Mint- und Ubuntu-Paketen, woher das System die Software bezieht. Beim Klick auf die voreingestellten Server startet automatisch ein Geschwindigkeitstest, der die schnellsten Server anzeigt. Spiegelserver bieten zwar nur die Software aus den „Offiziellen Paketquellen“ (also keine externe PPAs oder Software wie Google Chrome), diese sind aber die wichtigsten und umfangreichsten: Der Server für „Haupt (vanessa)“ liefert die Updates für Mint-eigene Komponenten und der noch wichtigere Server für „Basis (jammy“) die Updates der Ubuntu-Paketquellen.

Treiberverwaltung: Der nächste Weg geht nach „Systemverwaltung → Treiberverwaltung“, um proprietäre Herstellertreiber zu installieren – in der Regel Grafiktreiber. Die Treibersuche erfolgt automatisch.

Sprachunterstützung: Bei der Installation legen Sie zwar die Sprache „Deutsch“ fest, was jedoch noch kein konsequent deutschsprachiges System ergibt. Nach der Installation sollten Sie daher die Sprachpakete unter „Systemeinstellungen → Sprachen“ komplettieren. Beim Aufruf dieses Unterpunkts erscheint automatisch der Hinweis, dass noch Sprachpakete fehlen und nachgeladen werden können. Nachdem Sie zugestimmt haben, setzen Sie „Deutsch“ global mit „Systemweit anwenden“. Die Aktion wirkt aber erst nach der nächsten Anmeldung.

Monitoreinstellungen: Linux Mint erkennt die optimale Bildschirmauflösung automatisch. Bei einem Betrieb mit zwei Monitoren ist es aber notwendig, den primären Bildschirm und die optimale Anordnung der Monitore unter „Systemeinstellungen → Bildschirm“ festzulegen. Hier arrangieren Sie die gewünschte Dual-Monitor-Anordnung einfach mit der Maus. Ein oft übersehener Punkt für optimale Monitordarstellung ist der Punkt „Systemeinstellungen → Schriften → Skalierungsfaktor der Schrift“. Der steht standardmäßig auf „1,0“ und lässt sich in Zehntelschritten verkleinern oder vergrößern.

Netzwerkadapter: Mit Kabelverbindung ist Linux Mint sofort im Netz und im Internet. Bei WLAN-Adaptern besteht die übliche Pflicht, sich am WLAN anzumelden. Dies funktioniert über das Netzwerksymbol in der Systemleiste. Wenn der WLAN-Adapter hardwaretechnisch nicht erkannt wird, fehlen dort die Option „Funknetzwerk aktivieren“ sowie die Anzeige der nahen Funknetze. Eventuell helfen eine vorübergehende Kabelverbindung und das Nachladen des proprietären Treibers (unter „Treiberverwaltung“).

Es gibt allerdings WLAN-Chips, die unter Linux nicht funktionieren.

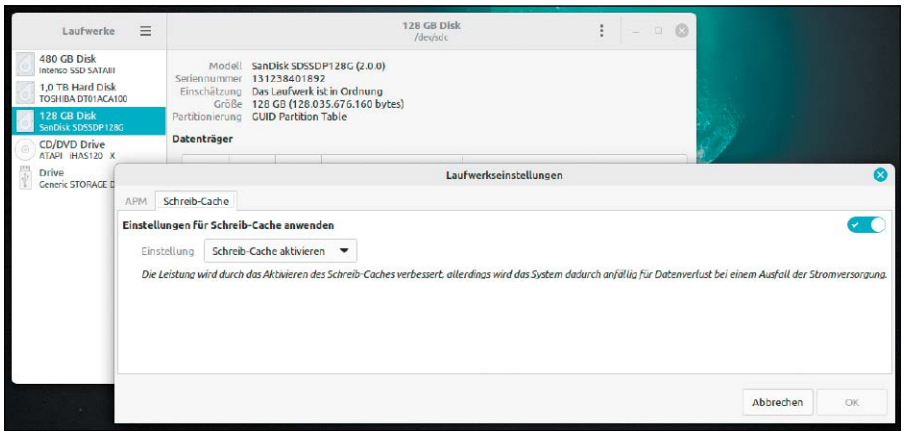
Check unter „Laufwerke“: Die Durchsicht der Datenträger unter „Laufwerke“ (Gnome-Disks) kann einen erheblichen Mangel offenbaren: Klicken Sie jedes Laufwerk an und kontrollieren Sie über das „Punkte“-Menü und den Eintrag „Laufwerkseinstellungen“, ob der „Schreib-Cache“ aktiv ist.

Timeshift: Linux Mint besteht auf Sicherung durch Timeshift-Snapshots. Dagegen ist nichts einzuwenden, bringt aber nur wirkliche Vorteile, wenn man es richtig macht. Beim allerersten Timeshift-Start führt ein Assistent durch die Einrichtungsschritte. Zunächst wird der „Schnappschusstyp“ abgefragt. Übernehmen Sie die Methode „rsync“, sofern Sie Linux Mint mit Ext4-Dateisystem installiert haben (Standard). Im nächsten Schritt geht es um den „Schnappschussort“, also um den Zieldatenträger der Sicherung. Timeshift erlaubt aus technischen Gründen nur Partitionen mit Linux-Dateisystem (notwendig wegen Hardlink-Technik und Sicherung der Dateirechte). Standardziel, wenn nur eine Festplatte vorliegt, ist das Wurzelverzeichnis, wo ein zusätzlicher Ordner „timeshift“ entsteht. Ideal ist ein unabhängiger zweiter Datenträger als Ziel – der muss dann aber immer zur Verfügung stehen, sofern Sie einen automatisierten Timeshift-Plan verwenden.

Im nächsten Schritt definieren Sie einen Zeitplan („Schnappschussebenen“) und die Menge der gespeicherten Systempunkte. Bei normaler Nutzung sollten wöchentliche Sicherung und drei bis fünf aufbewahrte Sicherungspunkte genügen. Mit „Weiter“ und „Beenden“ ist die Einrichtung abgeschlossen und voll automatisiert.

Im letzten Schritt des Assistenten (im Timeshift-Dialog auch unter „Benutzer“ zu erreichen) kann auch das „home“- und „root“-Verzeichnis eingeschlossen werden. Das ist nicht Standard, weil sich Timeshift als reine Systemsicherung versteht. Tatsächlich ist die Sicherung aller Benutzerdateien aus Mengen- und Zeitgründen nicht zu empfehlen und eher die Aufgabe von Mintbackup oder einem Rsync/Tar-Job. Aber die Option „Nur versteckte Dateien einschließen“ ist zu empfehlen, weil dies die komplette Benutzerkonfiguration einschließt inklusive aller Desktop- und Softwareeinstellungen.

Der erste Sicherungspunkt, den Sie am besten gleich manuell auslösen („Erstellen“), legt ein komplettes Backup der Systemverzeichnisse ab und ist daher zeitaufwendig. Weitere Wiederherstellungspunkte fallen wesentlich kleiner und schneller aus, da Timeshift nur noch geänderte Dateien speichert und unveränderte Dateien als Hardlinks zum letzten Sicherungspunkt abbildet.

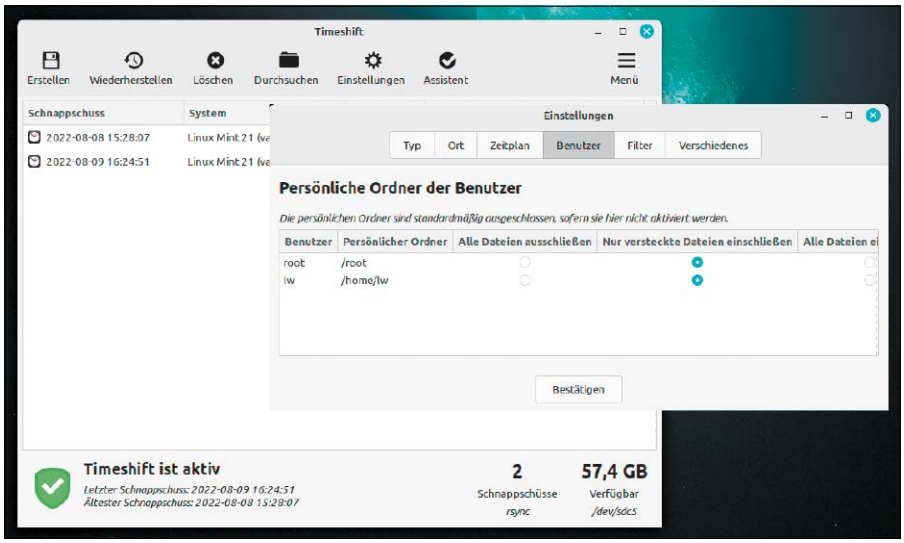


Schneller Schreibcache: Diese wichtige Leistungsoption aktivieren Sie mit Gnome-Disks („Laufwerke“) je Datenträger mit einem Mausklick.

Die spätere Wiederherstellung eines Snapshots mit dem grafischen Timeshift-Dialog scheint einfach: Das Tool zeigt in seiner Liste alle Punkte nach Alter geordnet. „Wiederherstellen“ schreibt den vorher markierten Punkt zurück, verunsichert dabei aber mit einigen Auswahlfeldern („/boot“, „/boot/efi“, „/home“, „Bootloader-Optionen“). Wesentlich klarer ist die Aktion im Terminal:

```
sudo timeshift --restore
```

Hier zeigt Timeshift die Liste der verfügbaren Snapshots an und der gewünschte kann mit der angegebenen Kennziffer ausgewählt werden. Danach müssen Sie nur noch die Frage verneinen, ob der Grub2-Bootloader neu installiert werden soll. Die Terminalmethode hat den zusätzlichen Vorteil, dass sie im Notfall auch ohne grafischen Desktop noch funktioniert. ■



Timeshift-Einstellung: Das Tool ist an sich kein Backup für Benutzerdaten, aber die versteckten Konfigurationsdateien unter „/home“ und „/root“ sollte es mitnehmen.

Linux Mint 21: Cinnamon-Tuning

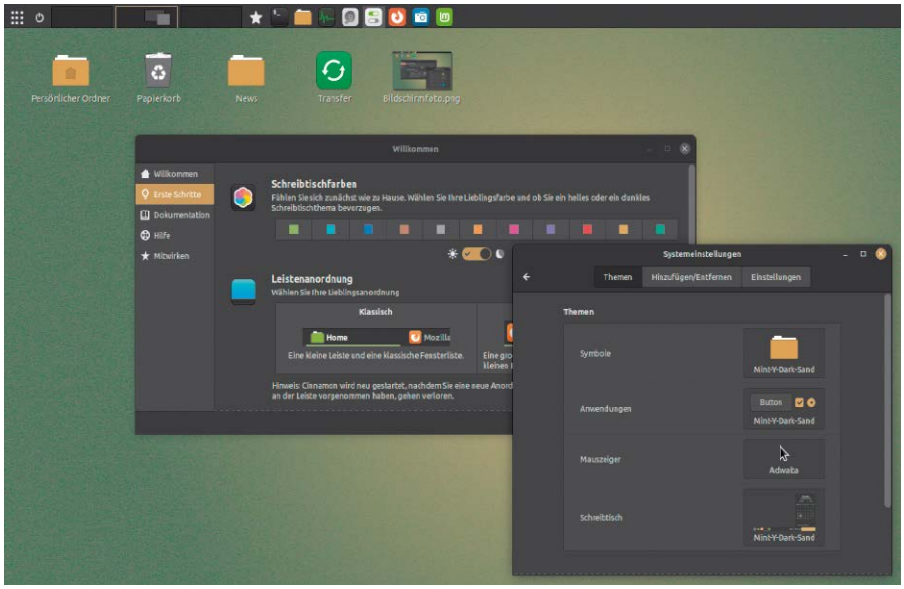
Linux Mint definiert sich maßgeblich über die Cinnamon-Oberfläche. Der Desktop ist aufgeräumt, anpassungsfähig und umsteigerfreundlich mit Windows-Analogien. Die jüngsten Umbauten in Cinnamon 5.4 bringen allerdings auch kleinere Rückschritte.

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 hier ganz auf diesen Desktop. Die Mint-Editionen mit Mate und XFCE bleiben außen vor.

Wichtige Cinnamon-Einstellungen

Cinnamon bietet umfassende Anpassungsmöglichkeiten über einschlägige Punkte in den „Systemeinstellungen“:
„Themen“ definieren das Aussehen von Cinnamon. Der Unterpunkt „Symbole“ bestimmt die Icon-Optik am Desktop und im Dateimanager und der Punkt „Anwendungen“ legt die Farbgebung für Programmfenster und Titelleisten fest. Leider gibt es hier keine Varianten mehr mit klarem Kontrast – also mit dunkler Titelleiste und hellem Fenster oder umgekehrt. Am ehesten ist dies noch mit „HighContrast“ zu erreichen. Der „Mauszeiger“ bietet wenig Auswahl, kann aber über „Systemeinstellungen → Maus und Touchpad“ hinsichtlich Größe und Verhalten genauer definiert werden. Der weitere Unterpunkt „Schreibtisch“ legt die Farben des Hauptmenüs und der Systemleiste fest. Hier gibt es eine große Anzahl attraktiver Themen, die man aus dem Internet nachladen kann (siehe unten „Spices (3)“).
Die optimale Kombination der Elemente zu finden, ist nicht ganz einfach und mit Experimentieren verbunden. Anfänger 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.



„Willkommen“ mit vereinfachter Themenwahl: Hier genügen ein bis zwei Klicks zur Einstellung der Cinnamon-Optik. Feiner geht’s unter „Systemeinstellungen → Themen“.

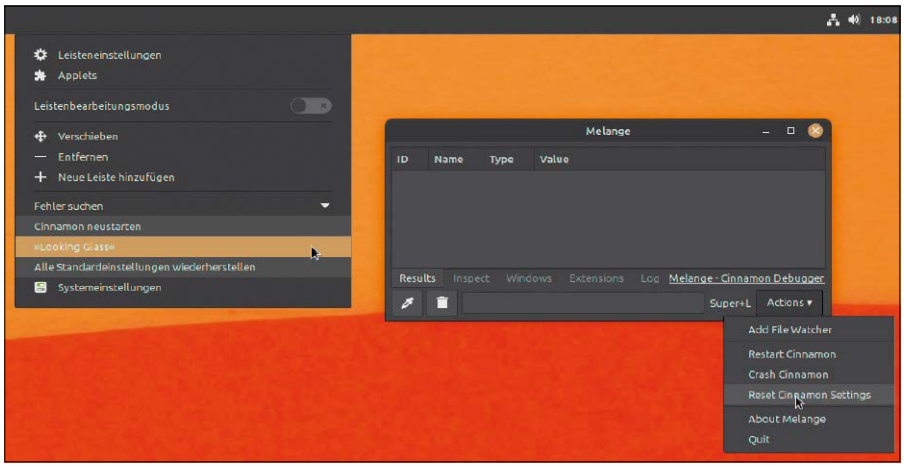
Der Punkt **„Schreibtisch“** (nicht zu verwechseln mit „Themen → Schreibtisch“) ist insofern wichtig, weil Cinnamon hier die Auswahl der Standardsymbole am Desktop anbietet („Papierkorb“, „Netzwerk“, „Eingehängte Datenträger“). Unabhängig von dieser Feineinstellung kann die Drop-down-Liste rechts oben mit „Keine Schreibtischsymbole“ alle Icons am Desktop auch komplett abschalten.
Hintergrundbild: Den Hintergrund 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.
„Aktive Ecken“ lösen durch Mausbewegung in eine Bildschirmecke eine Desktopaktion oder ein Programm aus. Aktive Ecken neben wichtigen Klickzielen wie dem Hauptmenü oder Programmtitelleisten sind allerdings kontraproduktiv. Da Titelleisten standardmäßig oben sind, die Systemleiste standardmäßig unten, gibt es eigentlich keinen geeigneten 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. Voreingestellte Standardaktionen sind Multitasking-Hilfen wie alle Fenster oder

Arbeitsflächen anzuzeigen. Die Option „Einen Befehl ausführen“ kann auch jedes selbst definierte Programm starten.

Die Cinnamon-Reparaturoptionen

Cinnamon bietet eine automatisierte Speicherüberwachung. Unter „Systemeinstellungen → Allgemein“ erscheint der Punkt „Speichergrenze“. Hier können Sie Cinnamon ein Limit vorgeben. Voreingestellt sind „2048“, minimal zulässig sind „1024“ MB – und das sollte mehr als ausreichen. Der Verbrauch wird laut Voreinstellung alle 300 Sekunden überprüft. Bei Überschreiten des Limits erfolgt ein Zwangsneustart von Cinnamon, alle anderen Programme laufen weiter. Weitere Problemlöser bietet Cinnamon in mehreren Abstufungen:

- Hotkey Strg-Alt-Esc startet die Oberfläche neu. Technisch identisch ist der Rechtsklick auf der Systemleiste und die Option „Fehler suchen → Cinnamon neustarten“.
- Hotkey Strg-Alt-Rücktaste ist die härtere Variante: Sie schließt die komplette Sitzung und führt zum Anmeldebildschirm zurück.
- Weiteres Troubleshooting bietet das Tool cinnamon-looking-glass. Es lässt sich durch Rechtsklick auf die Systemleiste und „Fehler suchen → Looking Glass“ starten. Hier gibt es unter der Schaltfläche „Actions“ (rechts unten) die 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 der Terminalbefehl `dconf reset -f /org/cinnamon/` erledigen.



Eingebaute Problemlöser: Bei Cinnamon-Problemen helfen die Hotkeys Strg-Alt-Esc und Strg-Alt-Rücktaste und dieses Tool, das über den Leistenkontext zu erreichen ist.

Arbeiten mit virtuellen Arbeitsflächen

Das Handling für virtuelle Arbeitsflächen ist unter Cinnamon vorbildlich. Als Standard-Hotkeys dienen Strg-Alt-Cursor rechts/links zum Wechsel und Strg-Alt-Cursor-oben zur Übersicht. Die zusätzlich gedrückte Umschalt-Taste verschiebt das aktuelle Fenster auf die nächste Arbeitsfläche. Zusätzlich gibt es das optionale Applet „Arbeitsflächenwechsler“ für die Systemleiste, das per Klick auf eines der kleinen Fenster zur betreffenden Arbeitsfläche wechselt.

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. Programmfenster lassen sich per Drag & Drop auf andere Desktops verschieben.

Die Anzahl der virtuellen Desktops können Sie in der Arbeitsflächenübersicht (Strg-Alt-Cursor-oben) verringern 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 ändern.

Spices: Externe Cinnamon-Gewürze

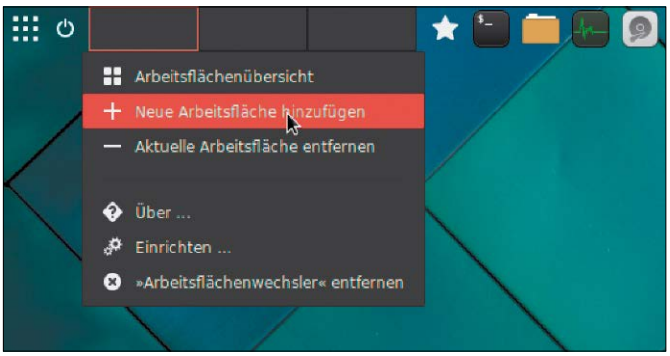
Cinnamon ist modular und lässt sich durch Spices („Gewürze“) erweitern. Die Sammelstelle lautet *https://cinnamon-spices.linuxmint.com*. Im Prinzip können Sie alle Spices dort beziehen und in jene Ordner entpacken, wie es die Webseite beschreibt. Der einfachere Weg führt aber über die „Systemeinstellungen“.

Die Spices unterteilen sich in vier Kategorien – „Themen“ (Optik), „Applets“ (für die Systemleiste), „Desklets“ (Desktop-Gadgets) und „Erweiterungen“. Wenn Sie in den Systemeinstellungen einen der Unterpunkte „Applets“, „Desklets“, „Erweiterungen“ wählen, zeigt das Register „Verwalten“ die auf dem System vorhandenen Spices, die Sie mit Plus- oder Minus-Taste aktivieren oder abschalten. Spices, die nicht zum Systemstandard gehören, lassen sich durch das Löschsymbol auch ganz löschen.

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.

Spices (1): „Desklets“ sind unnötig

Cinnamon kennt keine Einschränkung, den Desktop als Dateiablage, Programmstarter (Rechtsklick und „Neuen Starter hier erstellen“) oder Infofläche zu nutzen. Desklets sind zusätzliche grafische Desktopelemente, doch bleibt der Nutzwert dieser Spices-Kategorie eher begrenzt. Die Desklets „Digitaler Bilderrahmen“ für eine kleine Diashow und das „Uhr-Desklet“ hat Mint standardmäßig an Bord. Sie müssen unter „Systemeinstellungen → Desklets“ nur akti-



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

viert und konfiguriert werden. Unter den nachladbaren Desklets (Systeminfos, Uhren, Notizen, Wetter) werden Sie kaum unentbehrliche Tools finden.

Spices (2): Inkompatible „Erweiterungen“

Diese Spices-Kategorie bietet hauptsächlich optische Ergänzungen wie „Desktop Cube“ oder „Opacify Windows“. Unterm Strich sind Erweiterungen wie Desklets eher Spielerei, aber es gäbe Ausnahmen. Die eindeutig beliebteste Erweiterung „Transparent Panels“ funktioniert unter Version 21 und Cinnamon 5.4 aber nicht mehr. Wer transparente Systemleisten nutzen will, muss sich in der Spices-Kategorie „Themen“ umsehen.

Eine funktionsreiche Cinnamon-Erweiterung ist „Smart Panel“ und eröffnet diverse komfortable Klicks und Mausradaktionen auf der primären Cinnamon-Systemleiste (Arbeitsflächenwechsel, Fenstertransparenz, Programmstarter). Aber auch „Smart Panel“ ist inkompatibel mit Cinnamon 5.4. Damit verbleiben unter Mint 21 praktisch nur noch funktionierende Erweiterungen, die in die Kategorie Schnickschnack fallen.

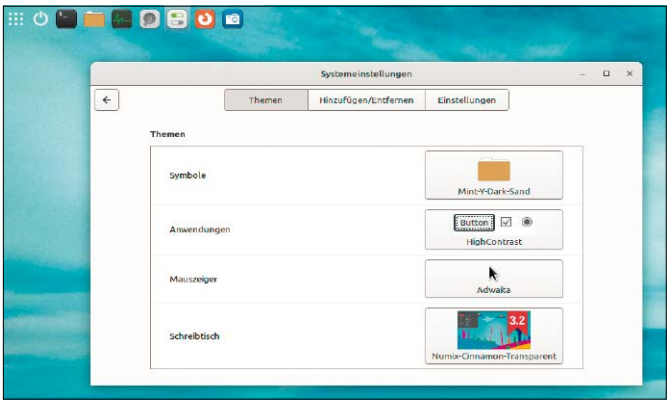
Spices (3): Optische Themen

Der aktuelle Ausfall der besten Cinnamon-Erweiterungen macht diese Spices-Kategorie wichtiger denn je. Transparente Systemleisten bietet etwa das externe Thema „Numix-Cinnamon-Transparent“ (auch in der Variante „Semi-Transparent“). Weitere bemerkenswerte Themen sind „Cinnamon-Kashmir-Blue“ oder „Cinnamox-Rhino“. Wie schon oben beschrieben, werden heruntergeladene Themen über den Punkt „Systemeinstellungen → Themen → Schreibtisch“ aktiviert. Wenn Sie mit vielen Themen experimentieren, sollten Sie unter „Hinzufügen/Entfernen“ gelegentlich aufräumen, um das Angebot überschaubar zu halten.

Spices (4): Applets für die Systemleiste

Das Angebot der Systemleiste wird durch Applets geregelt, die sich erweitern und reduzieren lassen. 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.

Optionale „Themen“ wie dieses mit Leistentransparenz bestimmen nur die Optik von Menü und Leisten („Schreibtisch“). Die weiteren Elemente harmonisch abzustimmen, ist gar nicht einfach.

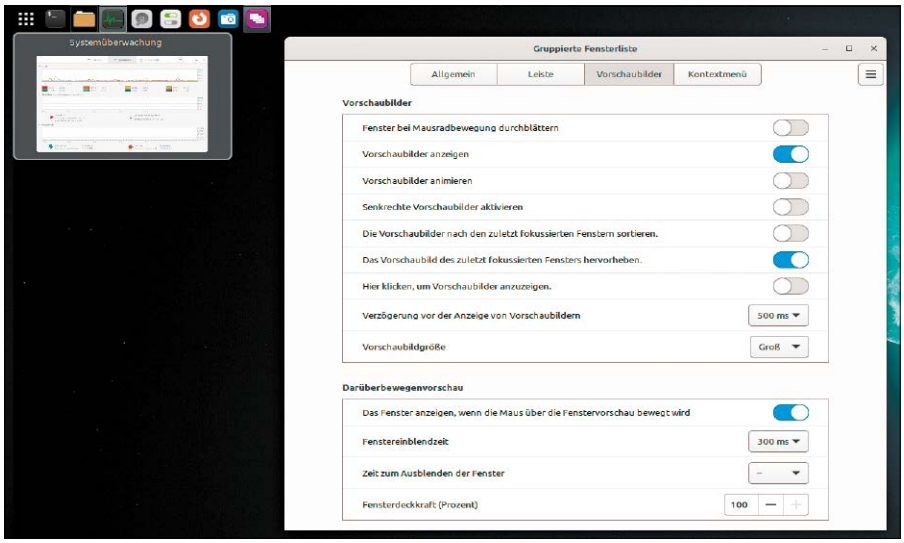


Applets ein- und ausschalten: Nach Rechtsklick auf eine freie Stelle in der Leiste erhalten Sie die Option „Applets zur Leiste hinzufügen“ (identisch mit „Systemeinstellungen → Applets“). Die aktiven Applets zeigen ein Häkchen. Mit der Minus-Schaltfläche schalten Sie das Element ab, mit der Plus-Schaltfläche ein. Viele Applets bieten eine eigene Konfiguration („Einrichten“ oder „Einstellungen“). So lohnen etwa das Hauptmenü- oder das Klang-Applet in jedem Fall einen Besuch.

Applet-Empfehlungen: Kaum entbehrlich sind die Applets „Menü“ und eine „Fensterliste“ wie vorzugsweise die „Gruppierte Fensterliste“. Typischerweise sollten auch „Klang“, „Netzwerkverwaltung“, „Kalender“ und „Meldungen“ nicht fehlen. Alles Weitere ist geräteabhängig, nutzungsspezifisch oder optional: Applets wie „Places“, „Places Center“, „Favoriten“ erlauben den Sofortzugriff auf lokale Datenträger und Netzwerkfreigaben.

Das Applet „Gruppierte Fensterliste“: Das Applet kombiniert eine dynamische Taskliste der laufenden Programme mit einem Favoritenstarter und ist weitgehend funktionsidentisch mit der Windows-Taskleiste. Zum dauerhaften Anheften eines Programms wählen Sie bei einem laufenden Task nach Rechtsklick einfach „An der Leiste anheften“.

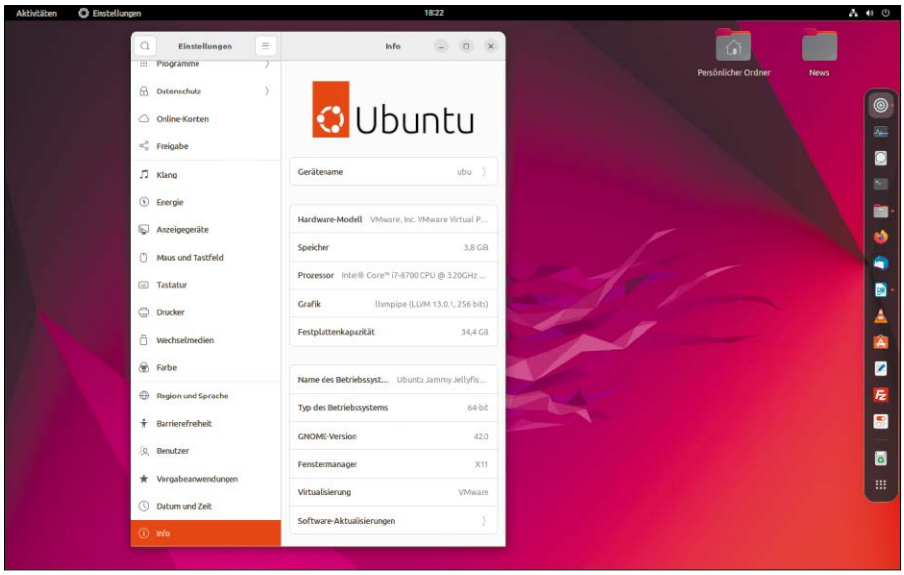
Das Menü-Applet: Das Startmenü zeigt eine nach Kategorien sortierte Programmübersicht, ein Instant-Search-Feld zur Suche, Programmfavoriten („Favoriten“) und Schalter zum Abschalten oder Abmelden. Aber das Startmenü kann komplett umgebaut werden, auch Favoriten oder Shutdown-Schalter sind optional (und durch spezielle Applets zu ersetzen). Nach Rechtsklick auf das Menüsymbol und „Einrichten“ gibt es eine Reihe von Basiseinstellungen, welche Elemente das Menü anzeigen soll. Neben „Symbol“ und „Text“ können Sie den Menünamen ändern. ■



„Gruppierte Fensterliste“: Das Leistenapplet kopiert die Windows-Taskleiste, ist attraktiv und funktionsreich, hat aber für unseren Geschmack eine überfrachtete Konfiguration.

Wichtige Version: Ubuntu 22.04 LTS

Im April 2022 war es wieder so weit – gerade Jahreszahl und April-Ausgabe: Das bedeutet bei Ubuntu alle zwei Jahre eine wichtige Version mit Langzeitunterstützung. Der Support beträgt bei solchen Versionen bekanntlich (maximal) fünf Jahre – also bis 2027.



VON HERMANN APFELBÖCK

Die LTS-Versionen der Ubuntu-Firma Canonical sind Meilensteine für die Linux-Gemeinde. Viele Ubuntu-Nutzer, erst recht Serveradministratoren warten bei Neuinstallationen und Upgrades grundsätzlich die LTS-Versionen ab und lassen die halbjährlichen Zwischenversionen links liegen. Ganz Vorsichtige warten sogar auf das erste Point Release mit Fehlerbereinigungen, das im aktuellen Fall 22.04.1 LTS heißt und im August 2022 erschienen ist.

„Ein" neues Ubuntu 22.04 LTS („Jammy Jellyfish")? Nein – viele, denn ein neues Ubuntu bedeutet stets sieben neue Ubuntus: Neben Canonicals Hauptedition mit Gnome-Desktop und der Serveredition gibt es fünf offizielle Ubuntu-Varianten, die den Systemcode schon während der Entwicklung erhalten und zeitgleich mit der Hauptedition erscheinen: Kubuntu, Xubuntu, Lubuntu, Ubuntu Mate, Ubuntu Budgie. Diese unterscheiden sich durch den jeweils anders gewählten Desktop (KDE, XFCE, LXQT, Mate, Budgie), zum Teil auch beim Installationsprogramm. Die Systembasis ist identisch.

Auch zahlreiche inoffizielle Ubuntu-Derivate wie Linux Mint, Peppermint-OS, Elementary OS oder Zorin-OS erneuern ihre Systembasis im Turnus von Ubuntu LTS und dessen Point Releases. Dies dauert erfahrungsgemäß etliche Monate und wird bis Juli/August zu aktualisierten, auf Ubuntu 22.04 basierten Versionen führen.

Neues bei Systembasis und Software

Wer Ubuntu kennt, weiß seit Jahren, dass die Ubuntu-Firma Canonical neue Versionen pünktlich wie ein Uhrwerk veröffentlicht und nicht darauf wartet, dass zugkräftige Innovationen abgeschlossen sind (siehe auch Kasten „Ubuntu-Release-Politik"). Was die Entwickler nicht termingerecht abschließen, bleibt dann einfach außen vor und wird geschoben.

Für die Version 22.04 waren zwei größere Innovationen angekündigt, nämlich ein neuer Installer (ein großes Projekt), ferner ein eigenständiger Firmwareinstaller (im kleineren Systemzubehör anzusiedeln). Beides fiel unter den Tisch und ist wohl für die nächste Zwischenversion im Herbst zu erwarten. Daher verbleiben nur wenige generelle Neuerungen, die für alle Ubuntu-Varianten gelten. Das Wichtigste ist der **Linux-Kernel 5.15**, der signifikante Verbesserungen enthält. Neben Feintuning beim Standarddateisystem Ext4 und beim alternativen Dateisystem BTRFS sind zwei Details hervorzuheben: Der Kernel-eigene Treiber für das NTFS-Dateisystem hat neben Lesezugriff nun auch Schreibzugriff auf dem Microsoft-Dateisystem. Durch den Wegfall des externen Treibers NTFS-3G ergeben sich Leistungsverbesserungen. Schneller werden auch Samba-Netzwerkfreigaben, weil ein neues Kernelmodul bisherige Aufgaben des Samba-Servers selbst übernimmt.

Firefox ist Standardbrowser in allen offiziellen Ubuntu 22.04. Wie es die Zwischenversion 21.10 bereits vorgemacht hat, wird Firefox nun ausschließlich als Snap-Paket angeboten. Auch die Übergangsfrist, neben dem Firefox-Snap noch ein traditionelles DEB-Paket anzubieten, ist mit Ubuntu 22.04 beendet. Folglich müssen nun auch alle anderen Ubuntu-Varianten das Snap-Paket verwenden, das nun direkt vom Her-



Nur noch als Snap: Nachdem Canonical Firefox als traditionelles DEB-Paket aus den Quellen entfernt hat, müssen alle Ubuntu-Derivate Snaps integrieren – oder auf Firefox verzichten.

steller Mozilla gepflegt wird. Wie sich die demnächst nachfolgenden inoffiziellen Derivate in dieser Situation verhalten werden, wird durchaus spannend: Wer einen Firefox anbieten will, wird auch einen Snap-Daemon anbieten müssen – womit Distributionen wie Linux Mint bekanntermaßen Schmerzen haben.

Ob das Firefox-Snap technische Nebenwirkungen hat, muss sich noch zeigen. Interessant wird vor allem die Frage, ob bei einem Systemupgrade von LTS-Version 20.04 auf Ubuntu 22.04 der Übergang vom traditionell installierten Firefox zur Snap-Variante überall lückenlos funktioniert – ob also das Nutzerprofil mit allen Daten übernommen wird.

Wayland nur in der Hauptedition

Canonical will mit Ubuntu seit Jahren den neuen Displayserver Wayland vorantreiben, der früher oder später das alte Xorg ersetzen soll. In der Ubuntu-Hauptedition mit Gnome-Desktop ist Wayland jetzt Standard. Damit folgt die LTS-Version der Entscheidung der letzten Interimsversionen 21.04 und 21.10. In allen anderen offiziellen Editionen ist Wayland jedoch nicht einmal als Option anzutreffen. Selbst in Kubuntu 22.04, dessen KDE-Plasma-Desktop in der Wayland-Unterstützung ebenfalls weit fortgeschritten ist, fehlt die Wayland-Option. Der Einsatz des alternativen Displayservers Wayland kann unter Kubuntu aber nachgerüstet werden. Mit

```
sudo apt install plasma-workspace-wayland
```

genügt eine relativ kleine Komponente, um nach der nächsten Anmeldung die Wayland-Option am Anmeldebildschirm anzubieten. Diese ist relativ unscheinbar links unten neben „Virtuelle Tastatur“ anzutreffen. Die Wahl lautet „Plasma (X11)“ und „Plasma (Wayland)“. Wayland bietet eine vereinfachte, mithin leistungsstärkere Grafik- und Videoausgabe und bedeutet eine der größten aktuellen Umstellungen am Linux-Desktop. Diese ist, das ist allgemeiner Konsens, überfällig und mittelfristig unaufhaltsam. Trotzdem geht die Wayland-Unterstützung der Linux-Desktops zäh voran: Gnome geht voraus, KDE und Mate sind immerhin in Sichtweite. Aber es gibt nach wie vor selbst unter Gnome so viele Baustellen, dass oft altes Xorg als Standard vorgezogen wird.

UBUNTU-RELEASE-POLITIK

Ubuntu STS, Ubuntu LTS, Point Releases: Man sollte die Ubuntu-Release-Politik kennen, um zwischen Interimsversionen, Langzeitversionen und Servervariante richtig entscheiden zu können.

• **Ubuntu STS (Short Term Support):** Es gibt halbjährliche Zwischenversionen im April und im Oktober. Diese erhalten als Versionsnummer die jeweilige Jahreszahl mit Monat – also etwa 23.04 für die nächste Zwischenversion (April 2023). Solche Interimsversionen bieten den neuesten Stand von Linux-Kernel, Desktop- und Softwareentwicklung, haben aber mit jeweils neun Monaten Support nur relativ kurze Gültigkeit. Wer den flotten Zyklus mitmachen will, muss halbjährlich das Upgrade auf die nächstfolgende Version erledigen. Das ist über die „Aktualisierungsverwaltung“ weitgehend automatisierbar.

• **Ubuntu LTS (Long Term Support):** Im April aller geradzahligen Jahre erscheinen die LTS-Versionen mit fünf Jahren Support für Canonicals Hauptversion mit Gnome und drei Jahre Support für alle weiteren offiziellen Flavours (Kubuntu & Co.). Für einen sorgenfreien Langzeitbetrieb sind auch drei Jahre völlig ausreichend, sofern man Kubuntu & Co. alle zwei, drei Jahre per Upgrade über die „Aktualisierungsverwaltung“ auf die nächstfolgende LTS-Version hievt.

• **Point Releases:** LTS-Versionen erhalten etwa halbjährlich „Point Releases“, die dann von 1 bis 5 nummeriert werden – also 22.04.1, 22.04.2 und so fort. Diese versammeln auf erneuerten ISO-Installationsmedien alles, was eine LTS-Version bislang an Updates erhalten hat. Hauptsächlicher Zweck dieser Point Releases ist es, bei Neuinstallationen unnötige Downloads zu vermeiden. Es ist technisch problemlos, heute ein originales Ubuntu 22.04 zu installieren und dann mit der Aktualisierungsverwaltung auf den Stand der Dinge zu bringen, jedoch erspart ein späteres Installationsmedium 22.04.x umfangreiche Downloads für Anwender sowie für die Spiegelserver. Für laufende Ubuntu-Systeme spielen Point Releases keine Rolle, da alle nötigen Updates online installiert werden.

Point Releases haben noch eine zweite Funktion: Sie liefern ab dem zweiten Point Release einen neueren Linux-Kernel. Diese Ergänzung nennt Ubuntu LTS Enablement Stack-Support oder auch HWE-Stack (Hardware Enablement Stack). Der HWE-Stack soll die konservativen LTS-Versionen auf dem aktuellen Stand halten und zur Installation auf neuester Hardware befähigen. Lediglich beim Ubuntu Server bleibt der HWE-Stack standardmäßig inaktiv. Optional ist der HWE-Stack aber auch dort erreichbar („Boot & Install with HWE Kernel“).

So ist die Anzeige grafischer Programme über das Netzwerk via SSH noch nicht möglich (X11-Forwarding). Tools wie xprop (Fenstereigenschaften), xkill (Fensterkiller) oder scrot (Bildschirmfoto) arbeiten unter Wayland nicht erwartungsgemäß. Auch Gnome-Erweiterungen funktionieren nicht unter Wayland.

Wenn daher die Ubuntu-Hauptedition Wayland als Standard setzt, ist das innovativ, aber nicht unbedingt benutzerfreundlich. Typischen Desktopnutzern, die eine Desktop-Fehlfunktion nicht zielsicher auf ein Wayland-Problem eingrenzen können, empfehlen wir die Rückkehr zu Xorg. Diese Möglichkeit ist auf allen Linux-Desktops, die Wayland verwenden, am Anmeldebildschirm vorgesehen. In Ubuntu 22.04 finden Sie rechts unten ein Zahnradsymbol und hier das Angebot „Ubuntu on Xorg“.



Displayserver Wayland ist Standard in der Gnome-Hauptedition, lässt sich aber auf Xorg umschalten. Die restlichen Ubuntus bleiben alle bei Xorg.

Editionen (1): Ubuntu 22.04 (Gnome)

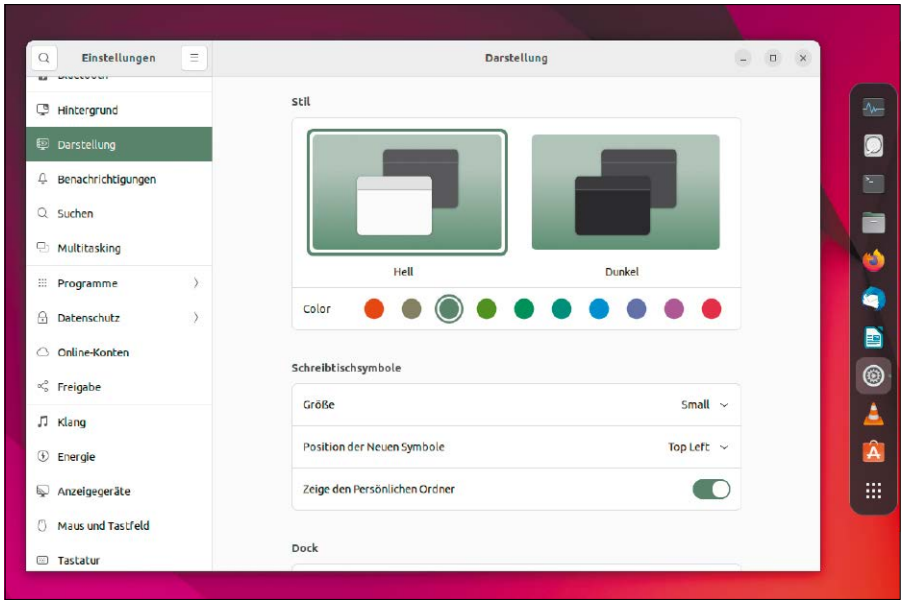
Canonicals Hauptedition profitiert vom jüngst erschienenen Gnome 42, dessen Neuheiten es größtenteils übernimmt. Gnome 42 bietet einen systemweiten Dunkelmodus. In den Systemeinstellungen (gnome-control-center) gibt es unter „Darstellung“ an oberster Stelle die Entscheidung zwischen „Hell“ und „Dunkel“. Was Benutzern als triviale Optikänderung erscheinen mag, ist eine komplexe Aufgabe, da es gilt, alle Klick-Controls in Menüs, Fenstern und Titelleisten für beide Darstellungsweisen gut sichtbar und kontrastiv zu gestalten. Neu an gleicher Stelle („Darstellung“) sind die Akzentfarben gleich unterhalb der „Hell/Dunkel“-Wahl. Die Akzentfarbe wirkt sich auf Symbole und Markierungen aus und hat damit erheblichen Einfluss auf die Gesamtoptik. Eine gezielte Auswahl lohnt sich.

Die Gnome-Systemeinstellungen sind generell überarbeitet. Neben dem schon genannten Punkt „Darstellung“ sind die Punkte „Multitasking“, „Datenschutz“ und „Online-Konten“ hervorzuheben.

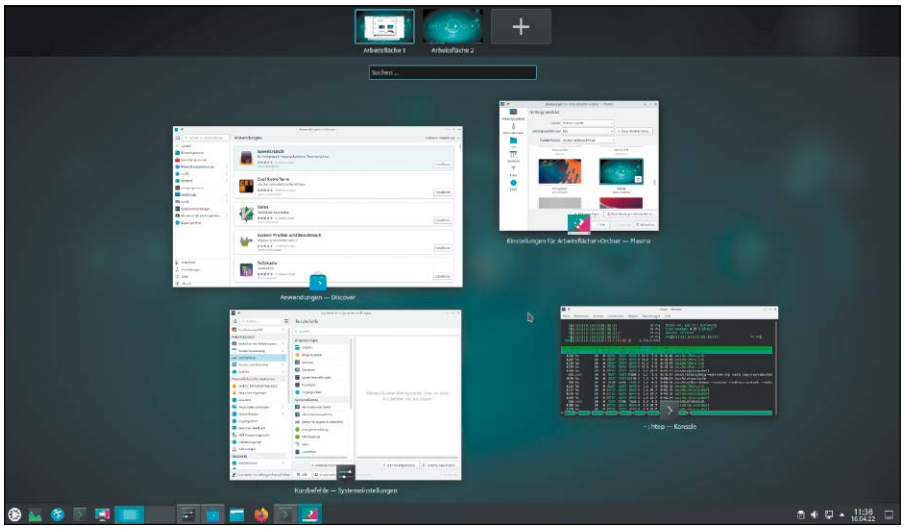
Ein neues, Gnome-eigenes Screenshot- und Screencast-Werkzeug macht externe Tools überflüssig. Nach der Taste „Druck“ erscheint ein Auswahldialog für Vollbild, Fenster oder Auswahlmarkierung. Mit dem zentralen Aufnahmeknopf landet das Bild in der Zwischenablage und als Datei unter „~/Bilder/Bildschirmfotos/“ (auf deutschem System).

Dorthin gibt es auch noch einen direkten Klickweg, weil die Meldung „Bildschirmfoto aufgenommen“ das Angebot „In Dateien anzeigen“ macht. Falls eine Desktop-Videoaufzeichnung gewählt wird, erscheint in der Systemleiste ein Sekundenzähler der Aufzeichnung, die mit Klick darauf beendet wird. Videos landen unter „~/Videos/Bildschirmaufzeichnungen“. Das Tool ist exzellent und einfach, andererseits aber kein Ding, worauf die Ubuntu-Gemeinde sehnsüchtig gewartet hätte.

Wie gehabt bleibt Ubuntu Gnome das Schwergewicht unter den Ubuntu-Flavours: Ein bis 1,5 GB RAM-Verbrauch wird das System immer anzeigen – ohne jede Softwarenutzung. Ideale Hardware für das System sind jüngere PCs und Notebooks. Dennoch haben die Ubuntu-Entwickler es geschafft, das Desktopsystem auch auf dem Raspberry Pi 4 mit nur zwei GB RAM zu flüssigem Betrieb zu überreden, dies allerdings nur durch die Kernel-Funktion zswap mit komprimierter Auslagerung.



Hauptedition mit Gnome: Der Desktop erweitert seine Darstellungsoptionen um einen globalen Dunkelmodus und Akzentfarben.



Kubuntu 22.04 mit KDE 5.24: Bei der neuen Übersicht mit allen Fenstern und Arbeitsflächen (Super-W) hat sich KDE offenbar von den Gnome-Aktivitäten inspirieren lassen.

Editionen (2): Kubuntu 22.04 (KDE)

Kubuntu hat als Standardsoftware die üblichen Kandidaten wie Firefox (Snap), Thunderbird, Libre Office und VLC in den aktuellen Versionen an Bord. Beim generell exzellenten KDE-Systemzubehör ist das aktualisierte Softwarecenter Discover 5.24 herauszuheben. Die KDE-Plasma-Oberfläche ist mit Version 5.24 ebenfalls brandaktuell und zeigt als wichtigste Neuerung nach der Tastenkombination Super-W eine Komplettübersicht über geöffnete Fenster, virtuelle Arbeitsflächen (oben) und Suchfeld. Diese Übersicht entspricht optisch wie funktional der „Aktivitäten"-Übersicht von Gnome. Neben dem schnellen Wechsel zu einem anderen Fenster ist per Drag & Drop auch die Umverteilung auf andere Arbeitsflächen möglich. In den gewohnt minutiösen Systemeinstellungen will sich KDE nicht von Gnome überholen lassen und zeigt unter „Erscheinungsbild → Farben" bereits seit Version 5.23 eine Palette von Akzentfarben, um Menüeinträge oder Dateiobjekte im Dateimanager einzufärben. Typisch KDE geht der Plasma-Desktop einen Schritt weiter als Gnome und erlaubt auch benutzerdefinierte Farben.

Kubuntu 22.04 ist wie die Gnome-Hauptedition eine gute Wahl für modernere Hardware. System plus Desktop können sich ab Start mit etwa 600 bis 700 MB RAM bescheiden, werden aber nach längerer Sitzung mindestens ein GB RAM beanspruchen.

Editionen (3): Xubuntu 22.04 (XFCE)

Bei Xubuntu gibt es selten Spektakuläres zu berichten, weil dessen Oberfläche XFCE meist über Jahre stagniert. Auch das in Xubuntu 22.04 enthaltene XFCE 4.16 hat seine letzten Änderungen bereits Ende 2020 erlebt. Trotzdem gilt Xubuntu nach der Hauptedition (Gnome) als das beliebteste Ubuntu, weil es geringe Ansprüche an die Hardware stellt, mit praktisch jeder CPU und GPU läuft und in der aktuellen Version 22.04.2 mit etwa 500 MB für System plus Desktop auskommt. Das ist etwas mehr als bei Lubuntu, aber dafür gibt es hier ein Menü mit Suchfunktion und einen zwar sachlichen, aber hervorragend konfigurierbaren Desktop mit intuitiv einstellbaren Systemleisten.

An Software liefert Xubuntu die üblichen Standardkandidaten Firefox (Snap), Thunderbird, Libre Office und sogar Gimp mit. Seit der letzten Zwischenversion 21.10 ist auch das mächtige Systemtool Gnome-Disks („Laufwerke") standardmäßig vorinstalliert. Es gibt auch noch die Variante Xubuntu „Core". Sie hat einen reduzierten Softwareumfang und muss in jedem Fall ergänzt werden.

Editionen (4): Lubuntu 22.04 (LXQT)

Die näheren Ursachen sind uns nicht bekannt: Lubuntu 22.04 verbleibt bei der Desktopversion LXQT 0.17, obwohl seit Anfang des Jahres die LXQT-Version 1.0 vorliegt. Das ist auch noch in der neueren Lubuntu-VErsion 22.04.2 der Fall.Hier stehen wohl die Stabilitätsansprüche einer LTS-Edition vor dem Innovationsanspruch.

Lubuntu war früher das ganz kleine Ubuntu. Der damals für das „L" verantwortliche LXDE-Desktop ist ein grafischer Dienstleister – nicht mehr. Mit dem seit Lubuntu

UBUNTU 22.04.2 LTS: EDITIONEN IM ÜBERBLICK

Von den offiziellen Ubuntu-Editionen ist Ubuntu mit Gnome die Haupt-Edition. Alle Systeme außer der Serveredition bieten ein bootfähiges Livesystem. Sie bieten sowohl direkt nach dem Start der Installations-DVD als auch nach dem Start des Livesystems eine Installationsoption. Erzeugen Sie aus der heruntergeladenen ISO-Datei einer Edition eine DVD oder einen bootfähigen USB-Stick und starten Sie damit Ihr System.

Ubuntu 22.04.2 LTS, Hauptedition mit Gnome, Download *https://ubuntu.com/download/desktop* (4,6 GB)
Xubuntu 22.04.2 LTS (XFCE-Desktop), Download *https://xubuntu.org/download* (2,9 GB)
Kubuntu 22.04.2 LTS (KDE-Desktop), Download *https://kubuntu.org/getkubuntu* (4,7 GB)
Lubuntu 22.04.2 LTS (LXQT-Desktop), Download *https://lubuntu.me/downloads* (2,7 GB)
Ubuntu Mate 22.04.2 LTS (Mate-Desktop), Download *https://ubuntu-mate.org/download* (3,1 GB)
Ubuntu Budgie 22.04.2 LTS (Budgie-Desktop), Download *https://ubuntubudgie.org/downloads* (3,0 GB)
Ubuntu Unity 22.04.1 LTS (Unity-Desktop), Download *https://ubuntuunity.org/download* (3,5 GB)
Ubuntu Server 22.04.2, Installer für Server (Desktop optional), Download *https://ubuntu.com/download/server* (1,8 GB)

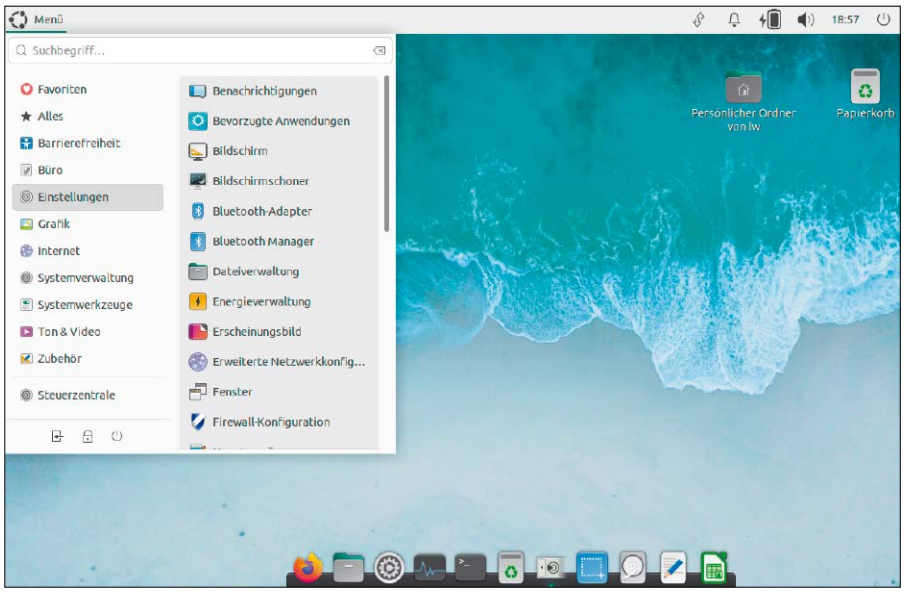
18.10 genutzten LXQT-Desktop wird die Oberfläche deutlich attraktiver, verliert aber auch ein wenig den expliziten Sparfokus. Mit 380 bis 450 MB RAM-Verbrauch ab Anmeldung bleibt Lubuntu 22.04 aber immer noch das eindeutig sparsamste Ubuntu. Außerdem ist Lubuntu besonders schnell betriebsbereit und weiterhin das reaktionsschnellste Ubuntu. Die Bedienung mit sehr einfachem Hauptmenü und die Anpassungsmöglichkeiten sind funktional, aber nicht mehr als befriedigend.

Bei der Softwareausstattung kommt Lubuntu nicht an Schwergewichten wie Firefox (auch hier als Snap), Libre Office, VLC oder KDE-Partitionsmanager vorbei, begnügt sich aber sonst mit sparsamen Alternativen wie Dateimanager Pcmanfm oder Taskmanager Htop. Dies lässt sich auf Wunsch mit dem ansehnlichen Discover aus dem KDE-Umfeld jederzeit korrigieren. Discover ist wie in Kubuntu in der nagelneuen Version 5.24 enthalten. Das Werkzeug vereinigt Softwarecenter (inklusive Flatpak) mit Aktualisierungsverwaltung und Firmwareupdater.

Editionen (5): Ubuntu 22.04 Mate

Ubuntu Mate hat neben der mittlerweile obligatorischen Snap-Umgebung und etlichen vorinstallierten Snap-Paketen (Firefox, Software-Boutique, Ubuntu-Mate-Welcome) auch einen Flatpak-Daemon vorinstalliert, ohne allerdings bereits Flatpaks mitzuliefern. Version 22.04 enthält weiterhin den Mate-Desktop 1.26, der schon in der Zwischenversion Ubuntu 21.10 eingesetzt wurde. Version 1.26 erhielt diverse neue Detailfunktionen wie einen sicheren Gastzugang für Fremdnutzer, eine Extra-Sidebar für Lesezeichen im Dateimanager und erweiterte Optionen zur Fensterpositionierung. Die zunehmende Wayland-Unterstützung entlang den Mate-Versionen 1.22, 1.24 und 1.26 wird zwar betont (siehe *https://mate-desktop.org*), jedoch verzichtet Ubuntu Mate 22.04 auf eine entsprechende Anmeldeoption.

Ubuntu Mate zielt auf Nutzer, die einen klassischen und dabei anpassungsfähigen Desktop jenseits von Gnome und KDE bevorzugen. Der Desktop ist relativ anspruchslos, das System fordert aber mit etwa 600 MB RAM ab Anmeldung doch deutlich mehr als Xubuntu (oder gar Lubuntu).



Ubuntu Mate 22.04: Der Mate-Desktop bleibt bei Version 1.26 wie bereits in der STS-Version 21.10.

Editionen (6): Ubuntu 22.04 Budgie

Diese Ubuntu-Variante präsentiert den Budgie-Desktop in Version 10.6.1. Die Gnome-ähnliche Oberfläche unterscheidet sich von Gnome durch klassische Elemente wie Menü, Systemleiste und einblendbare Seitenleiste. Sie punktet durch vorbildliche Bedienerführung mit kontrastiver Optik und klarem Schriftbild. Die Hardwareanforderungen sind etwas geringer als jene der Hauptedition mit Gnome und liegen etwa auf Höhe der Kubuntu-Edition.

Der überarbeitete „Window Shuffler“ ist eine Budgie-Spezialität, um Tasks in vorgegebene Fensterlayouts zu arrangieren, der Shuffler kann aber auch als Programm-Multistarter dienen. Zahlreiche kleinere Detailverbesserungen gibt es für die Leistenapplets, das Menüapplet und die ausklappbare und somit platzsparende „Raven“-Infoleiste.

Ubuntu Budgie hat neben dem Zwangs-Snap Firefox auch sein Willkommentool als Snap integriert. Die sonstige Standardsoftware entspricht mit aktuellem Libre Office, Thunderbird, Celluloid, Rhythmbox weitgehend den typischen Kandidaten. ■



Hübsche Gnome-Variante: Ubuntu Budgie ist eine attraktive Alternative zur Hauptedition für Nutzer, die sich am Desktop traditionelle Bedienelemente wie ein Hauptmenü wünschen.

Ubuntu 22.04 LTS: Installation & Upgrade

Installation und Upgrade entsprechen bei Version 22.04 dem, was wir von den Vorgängern kennen. Der Ubiquity-Installer von Ubuntu, Xubuntu, Ubuntu Mate/Budgie ist unverändert, Calamares in Kubuntu/Lubuntu ist technisch unverändert, aber etwas aufgeräumter.

VON HERMANN APFELBÖCK

Ubuntu 22.04 LTS wird den Linux-Desktop mindestens für die beiden nächsten Jahre bestimmen. Aktuelle Nutzer der Vorgängerversionen werden für den Systemwechsel zum bequemen Onlineupgrade greifen. Bei Neuinstallationen gibt es generell mehr zu bedenken, zunächst die Editionswahl, danach die Entscheidung für die passende Installationsvariante. Dieser Beitrag erklärt die Optionen bei Installation und Upgrade.

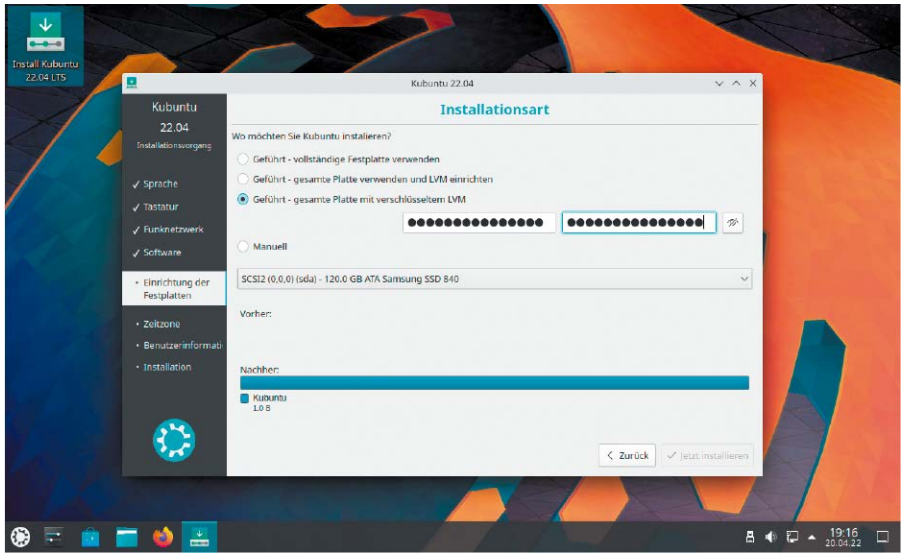
1. Das Upgrade älterer Versionen

Wer bereits ein Ubuntu laufen hat, kann ohne Datenverlust oder Datenumzug den Umstieg auf Version 22.04 ausführen. Voraussetzung ist

- der LTS-Vorgänger Ubuntu 20.04 oder
- die letzte Zwischenversion Ubuntu 21.10.

Stellen Sie ferner sicher, dass im Systemwerkzeug „Anwendungen & Aktualisierungen“ im Register „Aktualisierungen“ ganz unten die Benachrichtigung „Für Langzeitunterstützungsversionen“ eingestellt ist. Unter Kubuntu und Lubuntu finden Sie dieses Systemwerkzeug in Discover über den Punkt „Einstellungen“ und dort „Software Sources“. Das Tool ist hier nicht vollständig deutsch übersetzt und das Register lautet „Updates“. Hier sollte neben „Release Upgrade“ die Option „Long term support releases only“ eingestellt werden.

Aus Stabilitätsgründen wird das Upgrade auf 22.04 erst nach dem ersten Point Release auf Version 20.04.1, das im August 2022 erschienen ist, angeboten und wer LTS-Versionen aus ebendiesen Stabilitätsgründen schätzt, hat bis dahin gewartet.



Datenträgerverschlüsselung: Diese Option ist in allen Ubuntus einfach einzurichten, sofern das neue System die komplette Festplatte übernehmen darf (siehe Punkt 5).

Im Prinzip ist auch ein früheres Upgrade möglich, indem man sich nicht nur bei LTS-Versionen informieren lässt, sondern „Für jede neue Version“ („Any version“). Dies gilt dann auch für das aktuelle 22.04 vor dem ersten Point Release. Auf die Meldung der Aktualisierungsverwaltung, dass Version 22.04 verfügbar ist, antworten Sie dann mit Klick auf „Aktualisieren“.

Das Upgrade dauert länger als eine Neuinstallation, da alle Dateien aus dem Internet bezogen werden.

2. Neuinstallation: Welches Ubuntu?

Die Wahl der Edition wird zunehmend eine Frage des Desktop-Geschmacks, weil viele Editionen bei den Ressourcenansprüchen nahe beisammenliegen. Lubuntu mit LXQT-Desktop bleibt das Leichtgewicht, ist aber längst nicht mehr so sparsam wie früher mit LXDE. Die Mate-Edition hält sich konstant als Mittelgewicht. KDE Plasma (Kubuntu) hat sich tendenziell verschlankt, ist aber ein Kandidat, dessen Verbrauch bei längerer Sitzungsdauer deutlich wächst. Am anspruchsvollsten ist die Hauptversion mit Gnome, gefolgt von der Budgie-Edition. Beim Speicherbedarf nennt das Tool Htop (bei vier GB RAM) folgenden belegten Speicher nach der Systemanmeldung:

Ubuntu (Gnome)	1000 MB
Ubuntu Budgie	870 MB
Kubuntu (KDE)	750 MB
Ubuntu Mate	600 MB
Xubuntu (XFCE)	570 MB
Lubuntu (LXQT)	450 MB

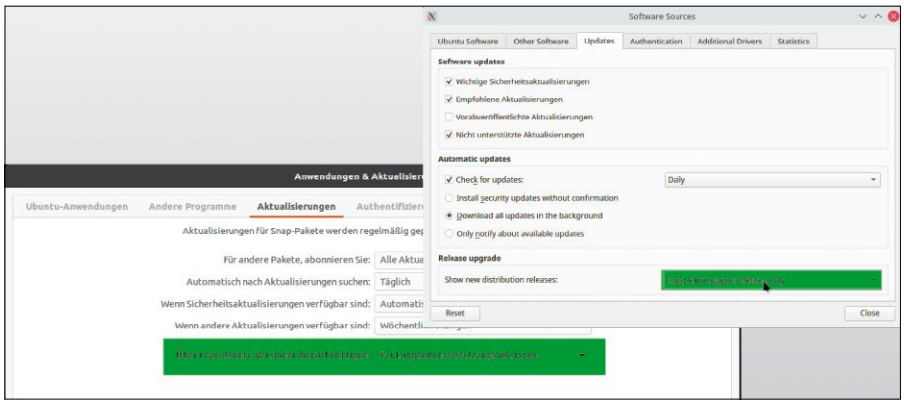
Lubuntu und Xubuntu kommen auch mit älteren CPUs und einfachsten Grafikchips klar. Bei Ubuntu Mate lässt sich der Effekt-Compositor abschalten („Steuerzentrale → MATE Tweak → Fenster“) und somit die Oberfläche auch mit Grafikchips ohne Hardwarebeschleunigung nutzen. Dazu verhilft der Unterpunkt „Fensterverwaltung“ mit der Option „Marco (kein Komposit)“. Gnome-, Budgie- und KDE-Editionen sollten auf eine Open-GL-Grafik treffen, was aber seit Jahren bei allen Intel/ATI/Nvidia-Chips Standard ist.

Für noch nicht wirklich alte Hardware der letzten fünf, sechs Jahre mit Quadcore-CPUs und Intel/ATI/Nvidia-Grafik und vier GB RAM aufwärts ist keine Ubuntu-Edition eine Herausforderung, sodass Lubuntu, Xubuntu und Ubuntu Mate letztlich Kandidaten für Altrechner sind oder auf Servern eine Behelfsoberfläche ausliefern sollen. Das glasklare und anpassungsfähige Xubuntu bleibt aber immer eine Empfehlung (auch auf neuer Hardware), sofern Desktop-Ästhetik nicht die entscheidende Rolle spielt.

Gnome, KDE, Budgie? Das ansprechende, aber hermetische Gnome-Konzept mit Vollbild-„Aktivitäten“ und Anwendungsübersicht muss man mögen, das kleinteilige Optionen-Überangebot von KDE ebenso (Kubuntu). Aus unserer Sicht wird Ubuntu Budgie im Kreis der offiziellen Ubuntus zunehmend zum attraktivsten Kandidaten. Der Budgie-Desktop zähmt seine Gnome-Basis mit klassischen Bedienelementen und ist weniger hermetisch als Gnome selbst, braucht allerdings für Anpassungen etwas Gewöhnung an die zuständigen Budgie-Komponenten („Budgie Themes“, „Budgie Desktop Einstellungen“, „Budgie Applets“).

3. Neuinstallation: Das Installationsmedium

Um die Hauptedition, Xubuntu oder einer der weiteren Editionen mit KDE-, Budgie-, Mate- und LXQT-Desktop zu installieren, müssen Sie deren ISO-Abbilder aus dem Web laden. Die Adressen finden Sie im vorangehenden Artikel im Kasten auf Seite 44. Um ein ISO-Image bootfähig auf einen USB-Stick zu schreiben, verwenden Sie unter Linux wahlweise Etcher (*https://etcher.io/*), KDE-Partitionmanager oder Gnome-Disks („Abbild wiederherstellen“). Unter Windows eignen sich Etcher, der Win 32 Disk Imager (*https://sourceforge.net/projects/win32diskimager/*) oder der USB Imager (auf Heft-DVD). Die Tools sind selbsterklärend und erwarten nur die (korrekte!) Angabe des Zieldatenträgers und der Abbilddatei.



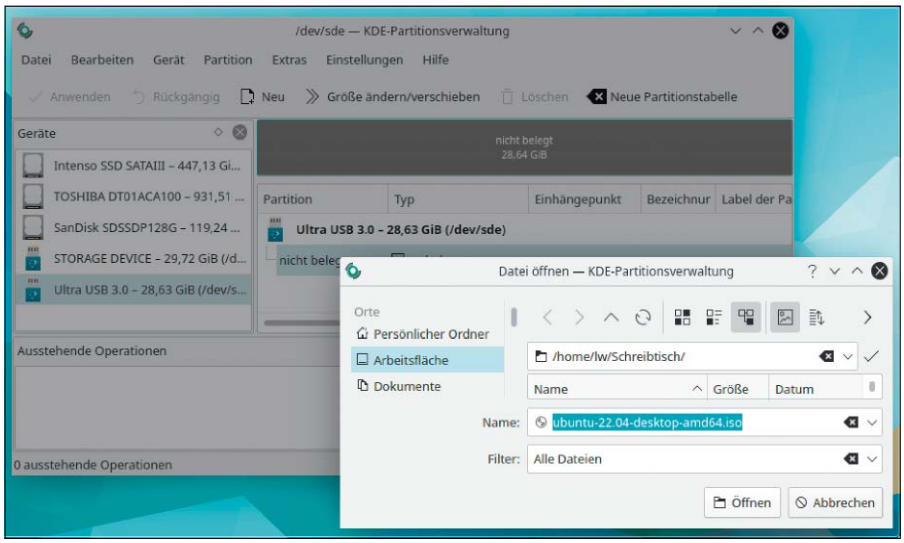
Das Upgrade: Ubuntu 20.04 LTS und 21.10 bieten das Upgrade auf die LTS-Version 22.04, sofern „Anwendungen & Aktualisierungen“ korrekt eingestellt ist (Kubuntu: „Software Sources“).

Einzig irritierend kann im Win 32 Disk Imager die Tatsache sein, dass er standardmäßig nur IMG-Dateien zeigt und erst der globale Filter „*.*“ die Anzeige aus Auswahl von ISO-Dateien ermöglicht.

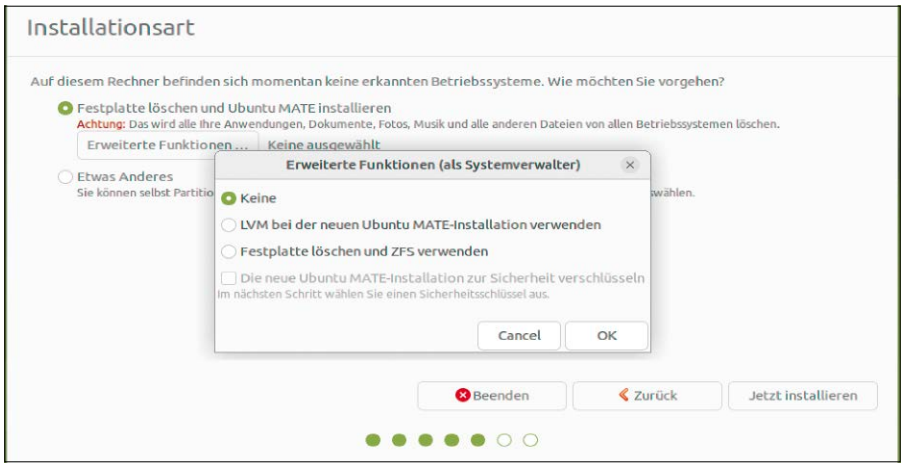
4. Installation (1): Als alleiniges System

Zur Installation booten Sie den gewünschten Zielrechner mit dem Installationsmedium – entweder mit einer DVD oder dem vorbereiteten USB-Stick. Standardmäßig sind PCs und Notebooks so eingestellt, dass sie automatisch von DVD booten. Sollte dies anders konfiguriert sein, müssen Sie nach dem Einschalten das Bootmenü des Bios aufrufen. Dies erledigt eine Funktionstaste, häufig F2, F8 oder F12, gelegentlich auch Esc. Im Bootmenü wählen Sie dann das DVD-Laufwerk, das Sie an Kennzeichnungen wie „Internal CD/DVD“ oder „Atapi“ erkennen. Wenn Sie ein Ubuntu-Livesystem von USB booten, verwenden Sie ebenfalls das Bootmenü.

Bootmenü und „Uefi“: Im Bios-Bootmenü erscheinen alle Bootmedien in doppelter Ausführung – einmal mit, einmal ohne die führende Kennzeichnung „Uefi“. Bei der Installation als einziges System spielt die Wahl keine Rolle. Bei einer Multiboot-Installation neben einem bereits bestehenden System muss der Modus des bereits bestehenden Systems gewählt werden – in der Regel „Uefi“ (bei bestehendem Windows immer). Bei einer Ubuntu-Installation auf ein USB-Laufwerk wählen Sie hingegen immer den Eintrag ohne „Uefi“. Alle sechs



Werkzeuge zum Kopieren bootfähiger ISO-Abbilder auf USB sind nicht rar. Dies beherrschen natürlich auch die Linux-Laufwerksspezialisten (Option „Wiederherstellen“) wie hier das KDE-Tool.



Einfache Soloinstallation (hier Ubuntu Mate): Die primäre Festplatte wird gelöscht und das neue System ohne jede weitere Option installiert.

Ubuntu-Editionen liegen als bootfähiges Livesystem vor, das ein Ausprobieren ermöglicht sowie die Installation aus dem Livesystem über den Desktoplink („Ubuntu 22.04 installieren“).

Die erste Entscheidung nach dem Start ist die Umstellung von „English“ auf „Deutsch“. Dies ist keine bloße Komfortfrage für die Installation selbst, sondern bestimmt bereits über die Spracheinstellungen des künftigen Systems. An dieser Stelle gäbe es neben „Ubuntu ausprobieren“ auch die Option, direkt zu installieren. Das hat aber außer ein paar gewonnenen Sekunden nur Nachteile. Es kann nie schaden, zunächst das Livesystem zu begutachten und dabei das Funktionieren der Hardware (Grafik, Sound, Festplatten, WLAN, USB, Funktionstasten) zu verifizieren.

Das Livesystem ermöglicht zudem via Terminal und Systemtools komfortable Kontrolle über die Laufwerke oder eine schnelle Internetrecherche. Lassen Sie daher Ubuntu besser zum Desktop durchstarten und wählen Sie erst hier die Installerverknüpfung.

Nach Auswahl der Tastaturbelegung zeigt der Installer neben der Option der Drittanbieter-Software (zu empfehlen) auch die Abfrage nach einer minimalen Installation (nicht in Lubuntu und Xubuntu). Diese bringt nur die Systemtools und den Browser mit. Im Normalfall ist daher die normale Installation zu empfehlen.

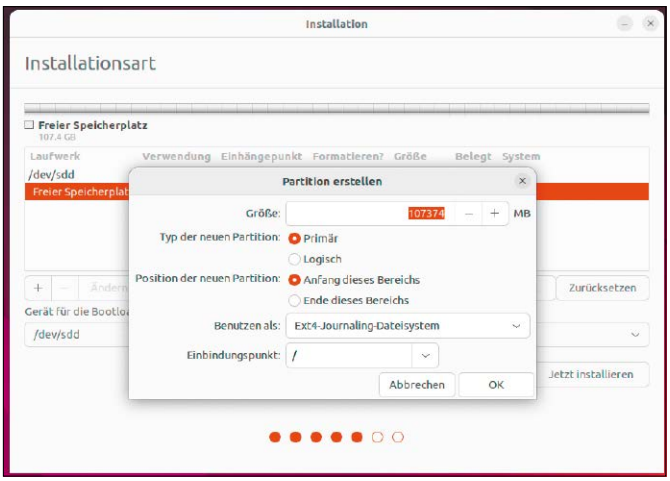
Im nächsten Schritt erscheint der entscheidende Dialog „Installationsart“ mit zwei möglichen Szenarien:

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

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

Für die Einrichtung von Ubuntu als alleiniges System verwenden Sie in beiden Situationen „Festplatte löschen“. Die übrigen Optionen des Dialogs („Erweiterte Funktionen“ – nicht in Kubuntu/Lubuntu) lassen Sie ungenutzt und beginnen mit „Jetzt installieren“ den Vorgang. Die Festplatte wird formatiert, der Datenbestand (und ein eventuelles System) gelöscht und Ubuntu eingerichtet.

Als letzte Aufgabe gilt es noch, den Erstbenutzer des Systems zu definieren. Der erhält in Ubuntu standardmäßig sudo-Recht und ist somit nach korrekter Kennworteingabe zu Aktualisierungen, Installationen und Systemwartung berechtigt.



Manuelles Partitionieren: Diese Aktion ist notwendig, wenn Ubuntu auf USB installiert (auf „/dev/sdd“ im Bild) oder ein bestimmtes vorhandenes System durch Ubuntu ersetzt werden soll.

5. Installation (2): Systemverschlüsselung

Verschlüsselung ist insbesondere für mobile Notebooks wichtig. Der Systemdatenträger lässt dann auch beim Booten durch Fremdsysteme keinen Einblick in die Daten zu. Beachten Sie, dass diese Option nur für eine Installation als alleiniges System in Betracht kommt. Der Standardinstaller bietet diese Option unter „Installationsart“ und hier unter dem Hauptpunkt „Festplatte löschen und Ubuntu installieren“. Darunter gibt es die Schaltfläche „Erweiterte Funktionen“ und hier wiederum die Option „LVM“. Sobald Sie LVM wählen, wird das entscheidende Kästchen „[...] Installation verschlüsseln“ aktiv. Wenn Sie dann auf „Weiter“ klicken, folgt die Abfrage des Sicherheitsschlüssels (Kennwort).

In Kubuntu ist die Aktion noch einfacher, weil der Calamares-Dialog „Einrichtung der Festplatten“ die Option „Geführt – gesamte Festplatte mit verschlüsseltem LVM“ direkt anbietet, darunter auch gleich die Kennworteingabe. Lubuntu zeigt die Option „Verschlüssele System“ (älterer Calamares-Dialog). Der Rest der Installation verläuft in allen Ubuntus wie gewohnt. Wenn Sie später das System booten, erscheint stets die Abfrage „Please unlock disk“ und der Systemstart setzt nur fort, wenn das richtige Kennwort eingegeben wird.

6. Installation (3): Auf USB

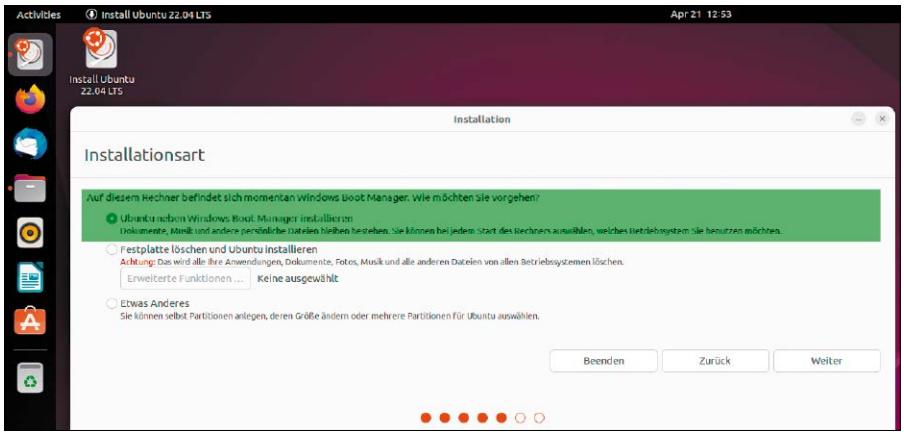
Jedes Ubuntu lässt sich auch auf USB installieren. Hier gelten gegenüber der in Punkt 4 erklärten Schritte zwei wichtige Unterschiede:

1. Das Installationsmedium muss im Bios-Bootmenü mit dem Eintrag ohne „Uefi“ gestartet werden (also im „Bios“-Modus).

2. Da Ubuntu-Installer stets die erste interne Festplatte „/dev/sda“ als Ziel vorschlagen, müssen Sie manuell das richtige Laufwerk festlegen. Daher wählen Sie im Fenster „Installationsart“ die Option „Etwas Anderes“. Das USB-Laufwerk muss neu partitioniert und formatiert werden, alle darauf befindliche Daten gehen verloren. Klicken Sie also auf die „-“-Schaltfläche, um vorhandene Partitionen zu entfernen. 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.
Kubuntu/Lubuntu: Beim Calamares-Installer lautet der maßgebliche Schritt „Einrichtung der Festplatten“. Hier benötigen Sie für USB-Installation den Unterpunkt „Manuell“. Nach „Weiter“ erhalten Sie eine Laufwerksliste, können dort ein USB-Medium wie „/dev/sdb1“ löschen und neu anlegen – mit den gleichen Einstellungen wie für den Standardinstaller Ubiquity beschrieben.

7. Installation (4): Multiboot

Ubuntu-Installer erkennen vorhandene Systeme. Etwas knifflig ist jedoch die Unterscheidung zwischen Bios- und Uefi-Partitionsschema. Sobald zwei oder mehr Systeme parallel installiert werden, wird der Partitionsstil – Bios/MBR versus Uefi/GPT – entscheidend.
Die Parallelinstallation kann nur gelingen, wenn das Livesystem in jenem Modus gestartet wird, in dem das bereits installierte System läuft. Andernfalls kann der Installer das vorhandene System nicht erkennen und wird dieses bei der Ubuntu-Installation überschreiben.
Auf PCs mit Windows 10/11 herrscht der Uefi-Modus. Weitere Systeme müssen auf die gleiche Weise eingerichtet werden. Den aktuellen Partitionsstil des existierenden Systems können einschlägige Tools ermitteln, unter Windows die „Datenträgerverwaltung“ und unter Ubuntu Gparted, Gnome-Disks oder der KDE-Partitionsmanager. GPT erscheint hier als „gpt“, der MBR-Modus als „msdos“.



Der Installer hat das bestehende Windows erkannt. Wenn Sie „neben Windows Boot Manager“ installieren, entsteht durch Verkleinern der Windows-Partition eine neue für Ubuntu.

Booten Sie das Ubuntu-Installationsmedium über das Bios-Bootmenü (siehe Punkt 4). Für Uefi-Parallelinstallation wählen Sie den Eintrag mit „UEFI“. Einen eindeutigen Hinweis, dass Sie im richtigen Modus sind, liefert danach der Ubuntu-Installer, sofern er das vorhandene System anzeigt und die Option „Ubuntu neben [XXX] installieren“ anbietet oder auch allgemein „Ubuntu daneben installieren“, wenn mehrere Systeme vorliegen.
Starten Sie im Livesystem die Installation über das Desktopicon. Was das Fenster „Installationsart“ („Einrichtung der Festplatte“) dann anbietet, hängt von der Situation ab. Wir gehen hier von einer Parallelinstallation neben Windows aus, jedoch gelten diese Infos auch für ein bereits bestehendes Linux im Uefi-Modus:
A. Gibt es nur eine Festplatte, die von Windows belegt ist, sehen Sie die Option „Ubuntu 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 Ubuntu schafft. Die Partitionsgröße lässt sich ändern, indem Sie die Aufteilungsmarkierung mit der Maus verschieben.
B. Ist neben einem installierten Windows oder Linux eine freie Partition vorhanden, erkennt der Installer das automatisch. Auch in diesem Fall wählen Sie die Option „Ubuntu neben Windows Boot Manager installieren“.
C. Sind zwei oder mehr Systeme vorhanden, dann führt das Angebot, „Ubuntu neben [XXX]“ zu installieren, zu einer weiteren Aufteilung und Partitionierung wie unter Variante A.
Wenn Sie das neue System nicht zusätzlich installieren, sondern eines der bestehenden Systeme durch das neue ersetzen möchten, gehen Sie anders vor und wählen „Etwas Anderes“. Die weiteren Schritte sind so, wie für die Installation auf USB beschrieben (Punkt 6): Sie löschen mit der „-“-Schaltfläche die Partition des obsoleten Systems und erstellen dann im „Freien Speicherplatz“ mit der „+“-Schaltfläche eine neue Partition mit dem Dateisystem Ext4 und dem Mountpunkt „/“. ■

UBUNTU UND ZFS

Wer die Optionen einer Ubuntu-Installation genau analysiert, wird bei der Partitionierung unter „Erweiterte Optionen“ auch den Punkt „ZFS“ antreffen (nicht in Kubuntu/Lubuntu). Eine Empfehlung für Desktopnutzer ist ZFS nicht. Es handelt sich um ein von Sun Microsystems/Oracle entwickeltes Dateisystem, das nach heutigem Ermessen keine Größenbegrenzungen kennt. Mit Logical Volume Manager, Raid-Controller, Snapshots, Fehlerkorrektur, Datenkomprimierung und Datenverschlüsselung gehört ZFS auf Server mit großen Datenmengen und hohen Ansprüchen auf Ausfallsicherheit. ZFS fordert großzügige Cacheverwaltung und viel RAM. Am Desktop ist Datensicherheit mit klassischen Backups sicher einfacher zu haben.

Ubuntu 22.04: Einrichten & optimieren

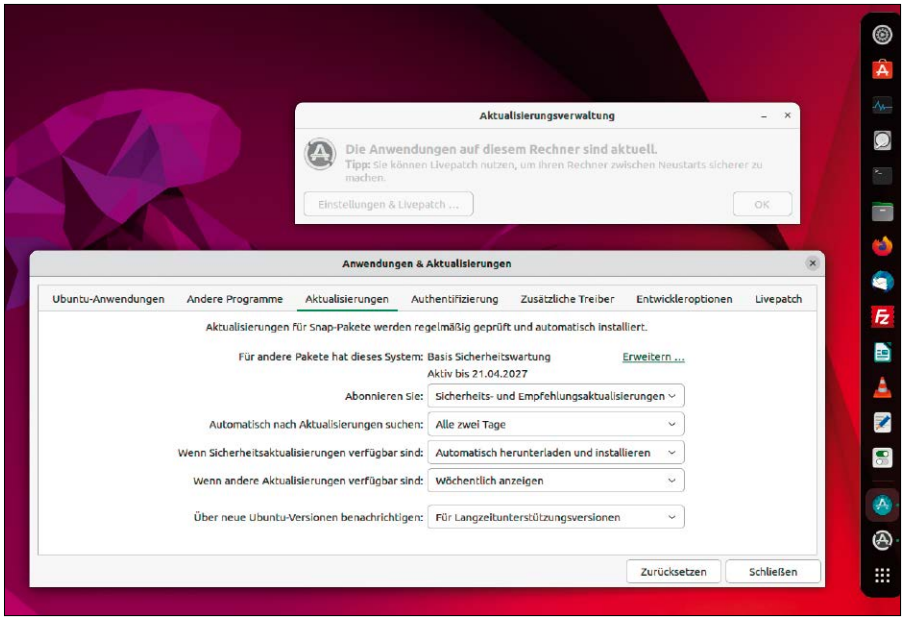
Nach einer Ubuntu-Neuinstallation sind einige fundamentale Einstellungen empfehlenswert bis unverzichtbar. Dieser Beitrag bespricht die Pflichten der Systemeinrichtung und benennt die Zentralen der Desktopanpassung für alle Ubuntu-Editionen.

VON HERMANN APFELBÖCK

Dieser knappe Beitrag richtet sich vor allem an Nutzer, die das neue Ubuntu frisch installieren. Dabei geht es um drei Aspekte, die in aller Kürze thematisiert werden:

- allgemeine, für alle Ubuntu-Editionen geltende Pflichten der Ersteinrichtung
- die praktische Nutzung aller neuen Funktionen
- Optimierung und Desktopschliff für alle sechs Ubuntu-Editionen

Insbesondere der dritte Punkt wird sich auf Hinweise auf die wesentlichen Konfigurationstools beschränken, die aber zumindest für die wichtigsten Aufgaben den zielsicheren Griff zum richtigen Werkzeug zeigen sollten.



Updates und Software: Die „Aktualisierungsverwaltung“ (update-manager) ist ausführendes Organ, die Basiseinstellungen definiert das Tool software-properties („Anwendungen & Aktualisierungen“).

Aktualisierung, Paketquellen, Treiber

Jedes neu installierte Ubuntu muss zunächst über die „Aktualisierungsverwaltung“ (update-manager) auf den aktuellen Stand gebracht werden. In Kubuntu/Lubuntu ist dieses Tool nicht einzeln verfügbar, sondern Bestandteil der Softwarezentrale „Discover“. Überall funktioniert die Alternative

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

im Terminal.

Im weiteren Alltag sorgt die Aktualisierungsverwaltung dafür, dass Updates automatisch eingepflegt werden. Das Systemtool führt mit der Schaltfläche „Einstellungen“ zum maßgeblichen Basistool „Anwendungen & Aktualisierungen“ (software-properties-gtk), analog Discover mit „Einstellungen“ zu „Software Sources“ (software-properties-qt). Hier definieren Sie, welche Updates wie häufig gesucht werden und ob diese automatisch installiert werden. Unentbehrlich sind „Sicherheitsaktualisierungen“.

Im Tool software-properties-gtk/qt empfiehlt sich dann gleich der Weg zur Registerkarte „Zusätzliche Treiber“, um Herstellertreiber zu suchen und gegebenenfalls zu installieren.

Das Tool eröffnet im ersten Register „Ubuntu-Anwendungen“ außerdem die Option, einen lokalen Spiegelserver zu wählen: Spiegelserver sind die Webserver, woher das System künftig alle Updates und Programme bezieht.

Von einem schnellen „Server für Deutschland“ profitieren sowohl die Benutzer als auch die dadurch entlasteten primären Ubuntu-Server. Noch ein Punkt in software-properties-gtk (nicht in Kubuntu/Lubuntu) ist zu erwähnen: Das Register „Livepatch“ ganz rechts ist ein spezieller Canonical-Service für LTS-Versionen, um Sicherheitslücken vorläufig im laufenden System zu schließen, ohne einen störenden Neustart zu erfordern. Für Desktopsysteme, die sowieso jeden Tag gestartet werden, ist der Livepatch völlig irrelevant.

Sprache, Monitor, Netzwerk und Drucker

Bei der Installation legen Sie zwar (hoffentlich) die Sprache „Deutsch“ und die Region „Deutschland“ fest, was jedoch noch kein

konsequent deutschsprachiges System ergibt. Nach der Installation ist es zu empfehlen, in den „Einstellungen“ die Sprachpakete zu komplettieren. Der Punkt heißt „Region & Sprache“ (Ubuntu), auch nur „Sprachen“ (etwa in Xubuntu) oder „Regionaleinstellungen“ (Kubuntu). Die Nachinstallation der fehlenden Sprachpakete wirkt erst nach einer Neuanmeldung.

Anzeige: Bei einem Monitor wählen Ubuntus automatisch die optimale Auflösung. Bei mehreren Monitoren ist es hingegen notwendig, den primären Bildschirm und die optimale Anordnung der Monitore festzulegen. Die wichtigsten Optionen finden Sie unter „Einstellungen → Geräte → Anzeigegeräte“ („Einstellungen → Anzeige und Monitor“), wobei Sie für eine Dual-Monitor-Anordnung die symbolisierten Bildschirme einfach mit der Maus arrangieren.

Netzwerk: Mit Kabelverbindung ist jedes Ubuntu sofort im Netz. Bei WLAN-Adaptern besteht die übliche Pflicht, sich am eigenen WLAN anzumelden. Dies funktioniert über das Netzwerksymbol in der Systemleiste (Network-Manager). Nach Auswahl des WLAN-Netzes und Eingabe des Kennworts wird das Zugangskennwort dauerhaft gespeichert. Wenn der WLAN-Adapter hardwaretechnisch nicht erkannt wird, fehlen dort die Option „Funknetzwerk aktivieren“ sowie die Anzeige der nahen WLANs. Dann hilft eventuell eine vorübergehende Kabelverbindung und das Nachladen des proprietären Treibers (wie schon oben im Punkt „Aktualisierung, Paketquellen, Treiber“). Es gibt allerdings USB-WLAN-Dongles, die unter Ubuntu nicht funktionieren.

Netzwerkdrucker: Der Punkt in den Systemeinstellungen lautet „Drucker“ oder „Printers“ (unter Gnome und Budgie ist dann der Zwischenschritt „Zusätzliche Druckereinstellungen“ erforderlich). Dann wählen Sie „Hinzufügen“ und „Netzwerkdrucker“. Taucht der Drucker nicht auf, hilft die Angabe der IP-Adresse des Druckers und „Suchen“. Wird der Drucker gefunden, versucht Linux, das Modell und den passenden Treiber zu ermitteln.

Freigegebene Drucker: Bei von Windows oder Linux freigegebenen Druckern verwenden Sie nach „Drucker“ den Punkt „Windows Drucker via SAMBA“. Nach „smb://“ tragen Sie die IP-Adresse des Freigaberechners ein, also zum Beispiel „smb://192.168.178.25/Epson“ („Epson“ wäre hier der Freigabename). Die Anmeldedaten für die Netzfreigabe kann man dauerhaft speichern. Auch hier muss Linux danach einen passenden Druckertreiber finden (was nicht immer gelingt).



Sprachpakete ergänzen: Oft ist nach der Ubuntu-Installation (hier Xubuntu) die Lokalisierung nicht vollständig. Prüfen Sie die Konfiguration und installieren Sie Fehlendes nach.

Energieeinstellungen: Ubuntus beschränken sich auf Sparoptionen, die das größte Potenzial besitzen – die Bildschirmabschaltung und der Suspendmodus („Bereitschaft“). Unter „Systemeinstellungen → Energie“ (oder „Energieverwaltung“) finden Sie den Timer für den Bereitschaftsmodus („Automatisch in Bereitschaft gehen“ oder „Standby-Modus“). Nach der angegebenen Frist geht der Rechner in stromsparende Bereitschaft, sofern keine Eingabeaktivität festgestellt wurde. Für das Verdunkeln und Ausschalten des Bildschirms bei Inaktivität finden Sie die Optionen an gleicher Stelle.

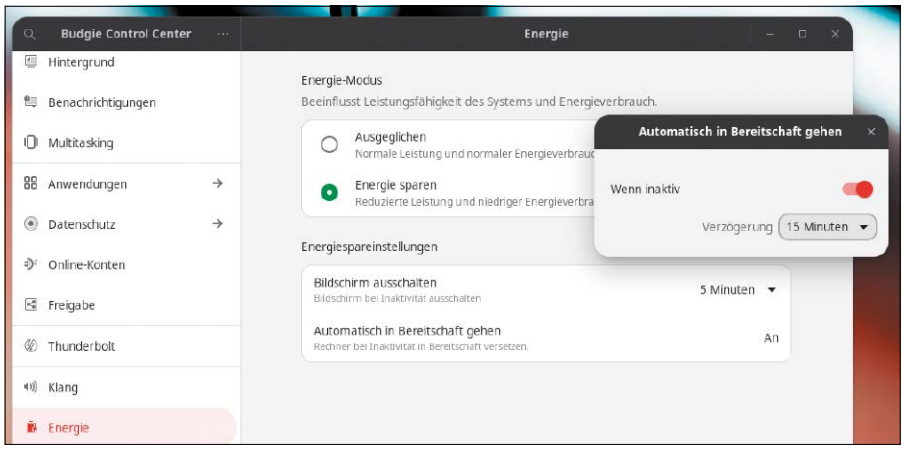
Codecs: Falls bei der Installation „Drittanbieter-Software“ aktiviert wurde, bringt Ubuntu den MP3-Codec mit. Folgender Terminalbefehl

```
sudo apt install ubuntu-restricted-extras libxvidcore libdvd-pkg
```

rüstet weitere Audio- und Videocodecs und die Bibliothek zur DVD-Wiedergabe nach.

Internetkonten: Unter „Einstellungen → Internetkonten“ machen Sie Gnome und Budgie mit Ihren Webkonten bekannt. KDE (Kubuntu) nennt diese Option „Online-Zugänge“. Nach einer Anmeldung bei Google, Facebook, Microsoft, Nextcloud werden einige Programme direkt mit dem Webdienst verknüpft.

Nützlich ist etwa die Verbindung des Dateimanagers zum Google-Konto, sofern Sie Google Drive verwenden, das dann im Dateimanager unter „Netzwerk“ erscheint. Xubuntu, Lubuntu und Ubuntu Mate fehlt diese Option.



Energieoptionen: Ubuntus bieten Bildschirmabschaltung und Bereitschaft nach einstellbarer Inaktivitätsfrist. Auf Notebooks kommen Helligkeitsregler und WLAN-Abschaltung dazu.



Extratool: Gnome-Tweaks bleibt wichtig, weil es Schriftenskalierung und Fensterfokus einstellen kann.

Ubuntu Gnome

Die Hauptedition ändert nichts am grundlegenden Gnome-Prinzip mit den „Aktivitäten“ (Windows-Taste) und der großen Anwendungsübersicht (Windows-A). Jedoch wird Ubuntu mit dem neuen Gnome 42 anpassungsfähiger. Die „Einstellungen“ (gnome-control-center) erlauben unter „Darstellung“ die bereits genannten Akzentfarben, ferner eine Windows-11-ähnliche abgerundete Darstellung des Favoritendocks („Leistenmodus“ abschalten) und ein differenziertes Verhalten des Docks (automatisches Ausblenden und Anzeige im Multimonitorbetrieb). Außerdem erscheint in den „Einstellungen“ der neue Punkt „Multitasking“: Hier wurde zum Teil integriert, was früher nur durch das Zusatztool Gnome-Tweaks erreichbar war: Die Bildschirmecke links oben lässt sich als aktive Ecke definieren, um die „Aktivitäten“ auszulösen. Ferner kann hier das automatische Skalieren von Fenstern (Einrasten) sowie Anzahl und Verhalten von virtuellen Arbeitsflächen konfiguriert werden – auch im Dualmonitor-Betrieb. Gut versteckt unter „Barrierefreiheit“ („Sehen“) können Desktopanimationen deaktiviert werden. Das Gnome-integrierte Screenshottool (nach „Druck“-Taste) ist selbsterklärend und vorbildlich, solange man keinen Wartetimer für die Aufnahme benötigt.

Trotz der erweiterten „Einstellungen“, die dringend eine ordnende Kategorisierung verdient hätten, scheint das Zusatzpaket Gnome-Tweaks („Optimierungen“) weiter sinnvoll: Nur hier kann man stufenlos eine exakte Schriftenskalierung einstellen (unter „Barrierefreiheit“ nur grob), den Fensterfokus ohne Mausklick anfordern und modale Unterdialoge vom Hauptfenster abkoppeln.

Ubuntu Budgie

Die Budgie-Edition nehmen wir hier an zweiter Stelle, weil der Gnome-ähnliche Budgie vergleichbare Einstellungsoptionen erwarten lässt. Tatsächlich fehlt hier aber im gnome-control-center („Einstellungen“) der Punkt „Darstellung“ komplett, da er bei Budgie in ein eigenes Tool „Budgie Desktop Einstellungen“ (budgie-desktop-settings) ausgelagert ist. Dieses kompensiert die neuen Gnome-Optionen aber gleichwertig. Hier gibt es ein „Dunkles Thema“ und die unter „Stil“ sollten für jeden Geschmack etwas bieten. Allerdings sind die zahlreichen angebotenen Farbkombinationen etwas unübersichtlich verglichen mit der eleganten Wahl der Akzentfarben in Ubuntu Gnome.

Die weiteren Optionen der „Budgie Desktop Einstellungen“ gehen über Gnome-Einstellungen deutlich hinaus, erlauben Schriftskalierung, Fensterfokus, Abhängen modaler Dialoge, Konfiguration der Systemleiste(n) und machen zusätzliches Gnome-Tweak überflüssig. Ein weiteres Desktoptool ist als „Budgie Themes & Layout“ direkt oder über „Budgie Welcome“ zu erreichen. Dies ist nur für die Ersteinrichtung zu empfehlen, weil solche Themenwechsel viele bisherige Einstellungen verwerfen.

Für die alltägliche Systemnutzung verwendet Budgie ein klassisches Menü (wahlweise kategorisiert oder alphabetisch), das Favoritendock Plank, Systemleistenapplets und die ausklappbare Infoleiste „Raven“ (Kalender, Musikwiedergabe, Systeminformationen). Trotz etlicher Hinweise in den Budgie Release Notes zeigen alle diese Elemente keine nennenswerten Neuerungen.

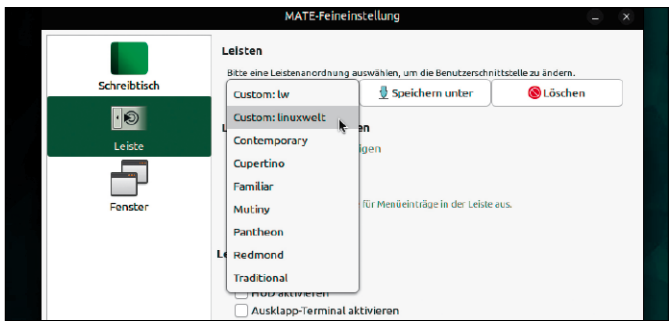
Ubuntu Mate

Mate nutzt für Desktopanpassungen seine eigene „Steuerzentrale“ (Mate-Control-Center), die auch gleich alles Wesentliche zur Systemverwaltung verlinkt – etwa die Aktualisierungsverwaltung oder das Laufwerkstool Gnome-Disks. Für optische Anpassung sind insbesondere die Applets „Erscheinungsbild“ und „Mate Tweak“ zuständig. Beim „Erscheinungsbild“ gibt es nicht nur eine feste Auswahl an Fensterthemen, sondern mit „Anpassen“ weitergehende Feineinstellungen. Leicht zu übersehen ist unter „Erscheinungsbild → Schriften“ die Schaltfläche „Details“, die zu einer stufenlosen Schriftenanpassung führt (DPI).

Das Applet „Mate Tweak“ wurde für Version 22.04 überarbeitet, um beim Punkt „Leiste“ für alle Bildschirmgrößen exakte Leistenanordnungen zu garantieren, die dann auch



Ubuntu Budgie: Hier sind alle Darstellungsoptionen (jenseits des gnome-control-center) in ein eigenes Tool „Budgie Desktop Einstellungen“ ausgelagert.



Mate Tweak mit Leistenlayouts: Die Funktion ist überarbeitet und sorgt für exakte Anordnung auch bei benutzerdefinierten Leistenarrangements.

für benutzerdefinierte Arrangements gelten (die sich mit „Speichern unter“ ablegen lassen). Das Leistenlayout ist der wichtigste Punkt von Mate Tweak, das ferner unter „Fenster“ das Fensterverhalten und den Effektkompositor und unter „Schreibtisch“ die Desktopicons definiert.

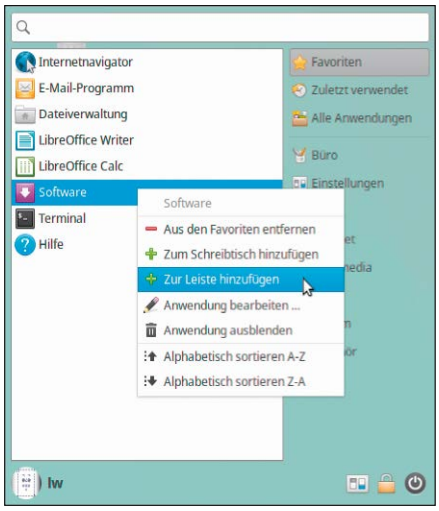
Mate liefert – für ein Ubuntu ungewöhnlich – neben Snap auch eine Flatpak-Umgebung mit, die allerdings nicht aktiviert ist, da zunächst keine Flatpak-Quelle eingetragen ist. Dies kann der Befehl

```
flatpak remote-add --if-not-exists
  flathub https://flathub.org/repo/
  flathub.flatpakrepo
```

nachholen.

Xubuntu (XFCE)

Bei Xubuntu 22.04 bleiben die Release Notes der Macher praktisch stumm. Außer einer unscheinbaren Verbesserung des Hauptmenüs („Whisker“) gibt es am Desktop definitiv nichts Neues. XFCE versammelt ahnlich wie Mate unter „Einstellungen“ (Xfce4-Settings-Manager“) die wichtigsten Tools zur Systemverwaltung und alles, was zur optischen Anpassung dient. Der Punkt „Erscheinungsbild“ bestimmt die Farbgebung von Menüs und Fensterelementen (Register „Oberfläche“). „Erscheinungsbild → Schriften“ erlaubt die stufenlose Skalierung der Schriften. Der weitere Punkt „Fensterverwaltung“ bringt Feintuning für das Aussehen und Verhalten aller Programmfenster – etwa Höhe und Farbe der Titelleiste, Einrastverhalten beim Ziehen an den Bildschirmrand und Fokus durch Mouseover („Fokus folgt Mauszeiger“). Der Punkt „Schreibtisch“ bestimmt über die Standardsymbole am Desktop.

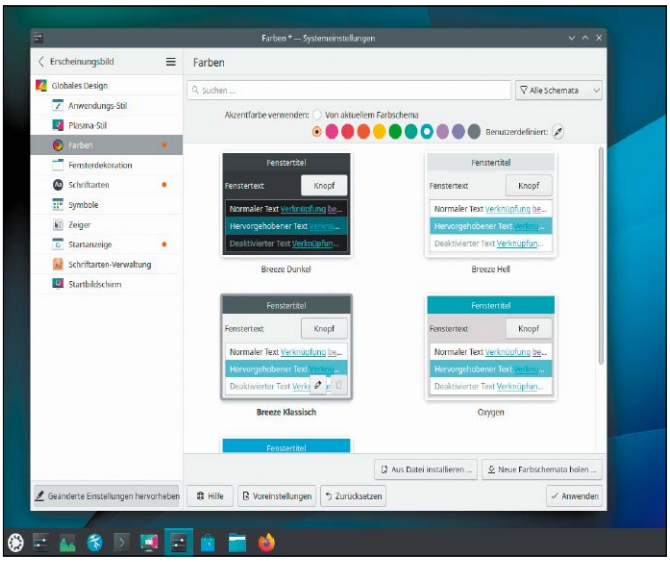


Xubuntu-Tuning: Der XFCE-Desktop macht es einfach, Leiste und Arbeitsfläche individuell zu bestücken.

Systemleiste und Standardmenü sind intuitiv bedienbar und per Kontextmenü vorbildlich zu personalisieren. Per Rechtsklick im Menü landen Starter wahlweise am Desktop, in der Systemleiste oder in den Whisker-Favoriten. Zahlreiche Applets für Systemleisten sind nach Rechtsklick auf die Leiste über „Leiste → Neue Elemente hinzufügen“ erreichbar.

Kubuntu (KDE)

Auf die auffälligste Neuerung haben wir bereits hingewiesen: Der Hotkey Windows-W aktiviert eine globale Übersicht über alle Fenster und virtuelle Desktops und zeigt zudem ein Instant-Search-Suchfeld. Das ähnelt der Gnome-Übersicht, ansonsten ist unter KDE bekanntlich alles anders. Wer KDE anpassen möchte, beginnt am besten mit Rechtsklick auf den Desktop und „Arbeitsfläche einrichten“ mit Hintergrundbild, Arbeitsfläche als Dateiablage („Ort“). Die Systemeinstellungen sind in die Abschnitte „Erscheinungsbild“, „Arbeitsbereich“, „Persönliche Informationen“, „Netzwerk“ und „Hardware“ unterteilt. Das „Erscheinungsbild“ ist maßgeblich für die Optik von KDE Plasma. Das „Arbeitsbereich-Design“ ermöglicht einen grundlegenden Themenwechsel und sollte dauerhaft entschieden werden. Feineinstellungen unter „Erscheinungsbild“ bieten die Optionen „Farben“ und „Anwendungsstil“. Unter „Schriftarten → DPI für Schriften erzwingen“ kann KDE einen individuellen DPI-Wert skalieren. Die Kontrollleiste insgesamt mit Größe, Position, Appletangebot und Anordnung lässt sich nur im Bearbeitungsmodus verändern (Rechtsklick und „Bearbeitungsmodus starten“). Eine intuitive Bestückung ist aber auch via Menü möglich (Rechtsklick und „Zur Kontrollleiste hinzufügen“) sowie durch Rechtsklick auf die Leiste und „Miniprogramme hinzufügen“.



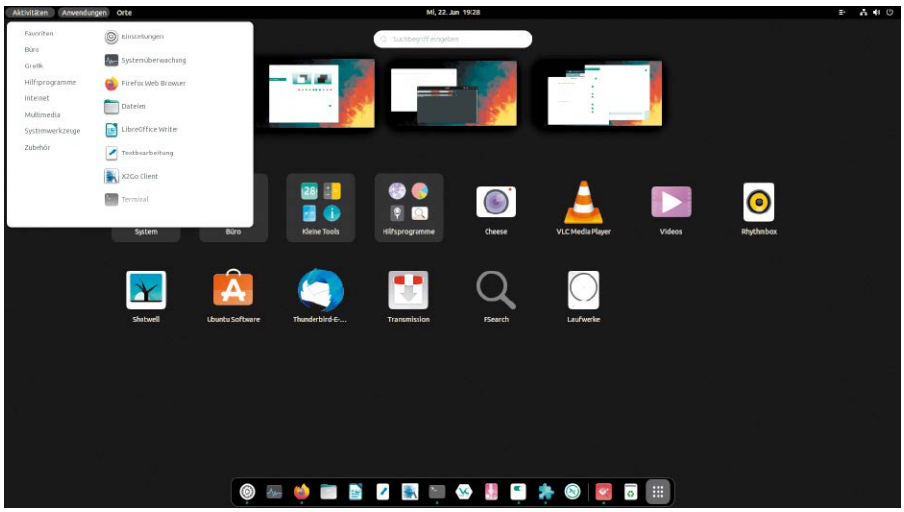
Akzentfarben in Kubuntu: Das hübsche, aber nicht lebenswichtige Feature bietet KDE schon seit Längerem. Das aktuelle Gnome (Hauptedition) zieht jetzt nach.

Lubuntu (LXQT)

Lubuntu hatte sich mit Version 20.04 und dem Umstieg von LXDE auf LXQT neu definiert. Seitdem tut sich auf dem Desktop allerdings wenig, zumal Version 22.04 bei der LXQT-Version 0.17 geblieben ist. LXQT folgt traditionellen Elementen mit Taskleiste und Anwendungsmenü mit Kategoriengliederung und sehr einfachem Suchfeld. Unter „Einstellungen → LXQT-Systemeinstellungen“ gibt es das „Konfigurationszentrum“ (lxqt-config) oder den direkten Sprung zu Einzelapplets wie „Erscheinungsbild“, „Schreibtisch“ oder „Fenstermanager“. Diese drei Punkte sind diejenigen, die sich für erste Anpassungen anbieten: Unter „Erscheinungsbild“ gibt es Desktop- und Iconthemen und den Punkt „Schriften“. Für den Desktop gelten Extraeinstellungen für Icons und Schriftgrößen, die Sie unter „Schreibtisch“ bestimmen. Hier ist auch einzustellen, ob der Desktop als Dateiablage dienen soll. Die individuelle Einrichtung der Systemleiste(n) erfolgt durch Rechtsklick und „Leiste konfigurieren“ (Größe, Position, Farbe). Die Auswahl der „Bedienelemente“ (Leistenapplets) beschränkt sich auf das Wesentlichste (Menu, Taskliste, Lautstärke, Schnellstarter). ■

Ubuntu 22.04 optimieren

Die vorangegangenen Beiträge haben Ubuntu 22.04 inklusive der offiziellen Varianten vorgestellt. Dieser Artikel fokussiert sich auf Optimierungsoptionen in Canonicals Hauptedition mit dem Gnome-Desktop.



VON HERMANN APFELBÖCK

Obwohl sich an Gnome und etlichen Sonderlichkeiten von Ubuntu 22.04 die Geister scheiden, ist Canonicals Hauptedition ohne Zweifel ein elegantes und schnelles System. Dieser Artikel geht von einem installierten und prinzipiell eingerichteten Ubuntu aus (Aktualisierung, Spiegelserver, Sprache, Anzeige, Netzwerk, Energieeinstellungen). Wir machen einen Rundgang, rüsten nach, was fehlt, und optimieren die Oberfläche. Denn es bleibt unverständlich, warum manches unentbehrliche Zubehör nicht mitgeliefert wird, das die Akzeptanz der Ubuntu-Hauptedition entscheidend fördern könnte.

1. Vorab: Empfohlene Ergänzungen

Die folgenden kleinen Helfer sind klassisch über *apt install [Name]* aus den Paketquellen zu beziehen. Die zuerst genannten Tools dürfen als unentbehrlich gelten, danach folgen optionale, aber empfehlenswerte Ergänzungen:

libfuse2 ist eine unscheinbare Bibliothek, die unter Ubuntu 22.04 schlicht vergessen wurde. Sie ist notwendig, um Software im Appimage-Format starten zu können.

gnome-tweaks erscheint auf deutschem System als „Optimierungen“. Die Bedeutung des Tools ist gesunken, seit es keine Gnome-Erweiterungen mehr verwaltet. Die Angebote unter „Fenster“ und „Schriften“ sind aber weiterhin unentbehrlich.

gnome-shell-extension-manager ist auf deutschem Ubuntu als „Erweiterungs Manager“ anzutreffen. Er ist alternativlos, um Gnome-Erweiterungen zu beziehen, zu (de-)aktivieren und zu konfigurieren, nachdem die frühere Möglichkeit über Firefox neuerdings ausfällt.

dconf-editor ist eine grafische Hilfe, um die Einstellungen von Gnome- und Gnome-Software zu steuern. Wer das standardmäßige gnome-control-center („Einstellungen“) sowie das Tool gnome-tweaks genau analysiert, wird feststellen, dass dort die allermeisten relevanten Optionen bequemer zugänglich sind. Dennoch bleiben Ausnahmen, und hier kann der „dconf-Editor“ aushelfen.

nautilus-admin ist eine winzige, aber nützliche Erweiterung für den Dateimanager, um per einfacher Kontextoption root-Zugriff zu erhalten.

p7zip-full, also der Packer 7-Zip, ist nicht nur für den Austausch von Packerarchiven sinnvoll, sondern vor allem wegen seiner Verschlüsselungsoption attraktiv. Dazu folgt ein Komfort-Tipp an späterer Stelle (Punkt 8).

Optionale Ergänzungen sind **preload** (Programmbeschleuniger), **plocate** (Suchindexer für das Terminal) und der **classicmenu-indicator**, der ein sehr einfaches klassisches Menü in der Systemleiste anbietet.

Dies alles sind kleine klassische Pakete. Gnome-Erweiterungen sind auf andere Weise zu beziehen, wie im späteren Punkt 6 (Gnome-Shell-Extension-Manager) näher erläutert wird.

2. Die Bedienungsgrundlagen

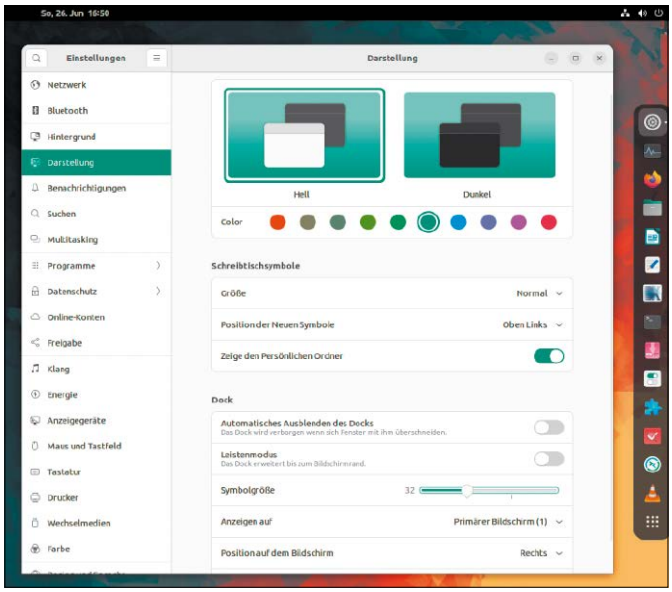
Als Umschalter und Programmstarter dient die Übersichtsseite „Aktivitäten“, die über die Windows-Taste (Super) oder durch Klick auf „Aktivitäten“ in der Systemleiste erreichbar ist.

Das Resultat ist multifunktional, denn es erscheint ganz oben das Suchfeld zur Programmsuche, darunter eine Übersicht der virtuellen Desktops und in der Bildschirmmitte eine Taskübersicht aller Fenster des aktuellen Desktops.

Der Hotkey Super-A startet eine alternative Gesamtübersicht, ebenfalls mit Suchfeld und Desktops, aber hier mit der Gesamtübersicht aller Programme (quasi das Startmenü von Gnome). Aufräumen dieser Übersicht durch Zusammenfassen passender Programme ist per Drag & Drop elegant zu erledigen. Die entstehenden Sammelordner lassen sich sprechend benennen.
Trotz der „Aktivitäten" gibt es Alternativen, die sich nicht von anderen Desktops unterscheiden: Hotkey Alt-Tab wechselt zwischen Programmen, Hotkey Strg-Alt-Rechts/Links wechselt zum nächsten virtuellen Desktop. Anders als originales Gnome liefert Ubuntu standardmäßig das Favoritendock mit. Dort enthaltene Starter können Sie nach Rechtsklick mit der Option „Aus Favoriten entfernen" beseitigen. Umgekehrt fügen Sie neue Programme am einfachsten über die Anwendungsübersicht hinzu (Super-A), indem Sie dort ein Programm nach Rechtsklick im Dock anheften („Zu Favoriten hinzufügen").

3. Das Gnome-Control-Center

Die zentralen „Einstellungen" sind etwas chaotisch, aber ergiebig.
Die **wesentliche Optik** bestimmen die Punkte „Hintergrund" und „Darstellung". Letztere bietet neuerdings einen dunklen Modus sowie Akzentfarben, die sich auf Icons, Markierungen und Menüs auswirken. Das Favoritendock kann hinsichtlich Symbolgröße und Position (rechts, links ...) angepasst werden.
Virtuelle Desktops: Eine oft unterschätzte Kategorie ist „Multitasking". Dass man mit der linken oberen Bildschirmecke die Aktivitäten-Ansicht auslösen kann („Funktionale Ecke"), ist eher marginal. Der Punkt „Arbeitsflächen" ist hingegen produktiv: Wer statt den dynamischen Desktops eine feste Anzahl bevorzugt (nach unserer Ansicht genügen zwei bis vier), kann das hier einstellen. Für den Desktopwechsel sind standardmäßig die Hotkeys Strg-Alt-Rechts/Links vorgesehen, nimmt man die Umschalt-Taste hinzu, wird das aktive Fenster mit transportiert. Interessant für den Multimonitorbetrieb ist die zusätzliche Option, virtuelle Desktops nur auf dem primären Bildschirm zu wechseln: Damit erhält man sich auf dem zweiten Bildschirm ein konstantes Bild (Programm), während der Hauptbildschirm die Desktops wechseln kann.
Tastenkombinationen: Unter „Einstellungen → Tastatur → Tastaturkürzel" werden Sie viele aktivierte Standard-Hotkeys antreffen, die Sie nie nutzen.

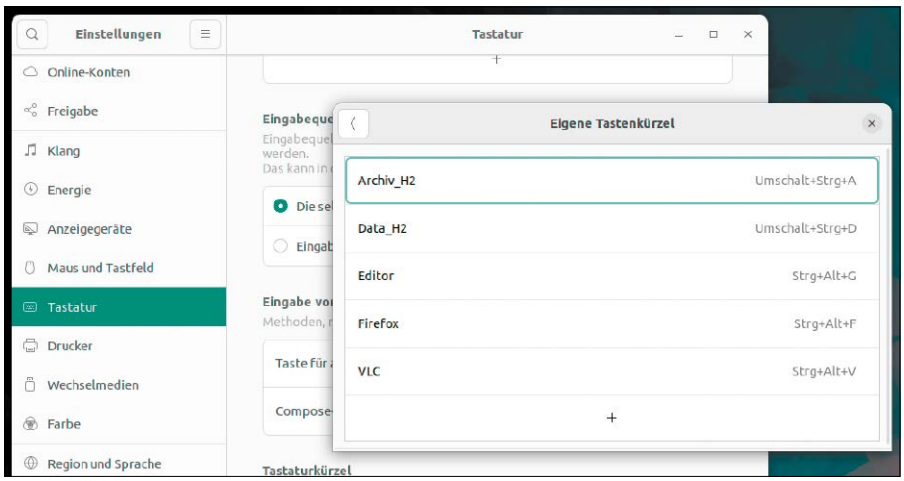


Der Dialog „Darstellung" im Gnome-Control-Center: Hier ist viel Optik komprimiert – Dunkel-Hell-Thema, Akzentfarben, Dockgröße, Dockposition und Schreibtischsymbole.

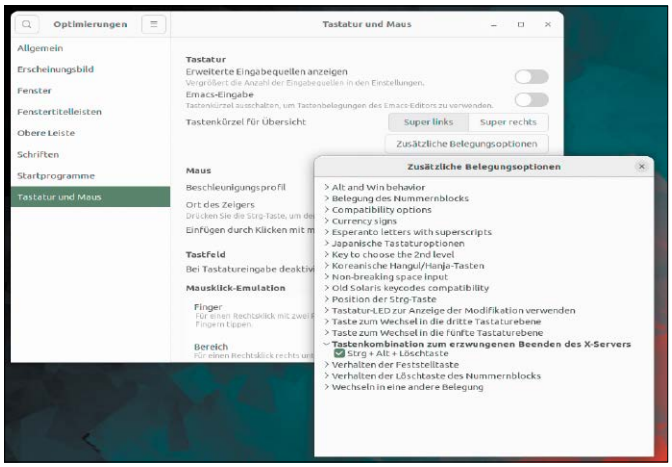
Hotkeys, die Sie definitiv nicht brauchen, können Sie abschalten. Um einen Standard-Hotkey zu deaktivieren, gehen Sie auf die Eingabetaste und nutzen im Folgedialog „Tastenkombination festlegen" die Rücktaste. Die Aktion ist dann noch mit „Festlegen" zu bestätigen. Auf die beschriebene Weise können Sie auch jeden Standard-Hotkey neu belegen, indem Sie statt der Rücktaste die gewünschte neue Tastenkombination drücken.
An unterster Stelle des Fensters „Tastaturkürzel" finden Sie die Rubrik „Eigene Tastaturkürzel". Sie eröffnet die Möglichkeit, Programmen oder Dateiobjekten einen individuellen Hotkey zuzuweisen (die Rubrik „Starter" zeigt nur eine kleine Anzahl von Programmprominenz wie Terminal, „Einstellungen" oder Standardbrowser). Unter „Eigene Tastaturkürzel" ist jedes beliebige Programm erreichbar. Sie wählen „Tastenkombination hinzufügen", geben einen „Namen" ein (unwichtig) sowie den „Befehl" (wichtig). Der Befehl kann schlicht „vlc" lauten, aber auch komplexer „nautilus smb://192.168.178.8/archiv". Mit „Tastenkombination festlegen" drücken Sie dann den Hotkey Ihrer Wahl.

4. Die „Optimierungen" (gnome-tweaks)

Der Funktionsumfang von gnome-tweaks („Optimierungen") ist nicht groß, aber relevant:
Der Punkt „Schriften" erlaubt eine stufenlose exakte Schriftenskalierung. Die stan-



Hotkeys anpassen und erstellen: Einfache Tastaturstarter sind unter „ Einstellungen –› Tastatur –› Tastaturkürzel" schnell erstellt und sorgen für Schnellstarts ohne Pixelsuche.



Gnome-Tweaks („Optimierungen“): Das Tool ist allein schon wegen der Schriftenskalierung eine Empfehlung. Die Optionen zur Tastenbelegung sind in einem Untermenü versteckt.

dardmäßigen „Einstellungen“ bieten unter „Barrierefreiheit“ dagegen nur die, nicht genauer skalierbare Option „Große Schrift“.

Der Punkt „Fenster“ kann modale Unterdialoge vom Hauptfenster abkoppeln. Außerdem gibt es hier die Option, den „Fensterfokus“ bereits beim „Überfahren“ mit der Maus zu ändern (also ohne Klick). Ein oft nicht geläufiges Feature: Fenster lassen sich nicht nur mit der Titelleiste, sondern an jeder Position verschieben, wenn man die Super-Taste drückt. Diese „Fenster-Aktionstaste“ können Sie hier abschalten oder auf Alt-Taste verlegen.

Der Punkt „Erscheinungsbild“ kann die Fensteroptik, Titelleisten und Icons wesentlich verändern. Ergiebig ist das aber nur, wenn die schmale Auswahl der vorinstallierten Themes und Iconsets durch Gnome-Themen aus dem Web erweitert wird.

Unter **„Tastatur und Maus“** finden Sie Angebote, Tasten stillzulegen, neu zu belegen oder zu vertauschen. Die interessantesten Optionen verstecken sich im Unterpunkt „Zusätzliche Belegungsoptionen“. So ist etwa die „Tastenkombination zum erzwungenen Beenden des X-Servers“ inaktiv und kann hier scharf geschaltet werden. Allerdings ist „Strg+Alt+Löschtaste“ nicht etwa Strg-Alt-Entf, sondern Strg-Alt-Rücktaste.

5. Der Dconf-Editor

Was immer in den generellen „Einstellungen“, in den „Optimierungen“ oder in Programmeinstellungen zu finden ist, ist dort bequemer zu nutzen. Der relativ unübersichtliche Dconf-Editor hilft aus, wo die Reichweite der anderen Werkzeuge endet. Ein Beispiel ist etwa die Einstellung im Dateimanager Nautilus, statt des „Krümel“-Pfades immer den editierbaren Pfad in der Adresszeile anzuzeigen. Die findet sich beim Dconf-Editor unter „org → gnome → nautilus → preferences → always-use-location-entry“. Ein zweites Beispiel: Beim Abmelden über das Sitzungsmenü erscheint noch einmal ein Rückfrage. Die lässt sich unter „org → gnome → gnome-session → logout-prompt“ deaktivieren. Noch ein Beispiel? Der klassische Taskwechsel mit Alt-Tab berücksichtigt standardmäßig nur die Fenster des aktuellen, virtuellen Desktops. Der Schalter unter „org → gnome → shell → window-switcher“ stellt dies um, sodass alle Programme aller Desktops erreichbar sind.

6. Der Gnome-Shell-Extension-Manager

Dieses Tool ist für Ubuntu-Nutzer mehr oder weniger Pflicht. Damit lassen sich die installierten Gnome-Erweiterungen („Installed“) ein- und ausschalten, komplexere über das Zahnradsymbol genauer konfigurieren. Ferner kann das Register „Browse“ weitere Gnome-Extensions nachinstallieren.

Das Tool erscheint als „Erweiterungs Manager“ in der Gnome-Übersicht. Bei der Websuche nach neuen Erweiterungen mit „Browse“ nutzen Sie am besten parallel einen Browser und die Adresse *https://extensions.gnome.org*. Hier ist nämlich Blättern und Stöbern möglich, während das lokale Tool nur einen kleinen Ausschnitt anzeigt. Interessante Erweiterungen können dann aber mit dem Tool im „Browse“-Fenster gesucht werden, wonach kompatible Extensions die Schaltfläche „Installieren“ anbieten. Installiertes landet in der Übersicht „Installed“ und kann dort aktiviert, deaktiviert und konfiguriert werden.

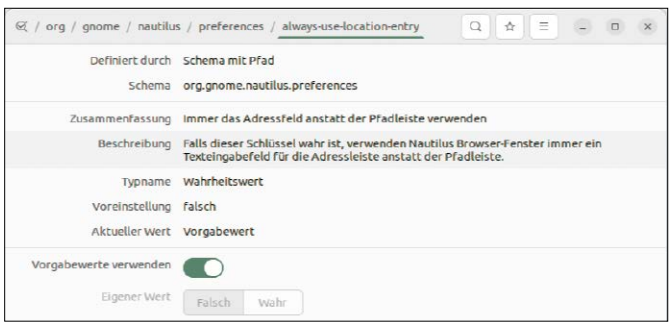
Eine Übersicht über die zahlreichen Extensionen ist hier nicht möglich, allenfalls die eine oder andere Empfehlung: **„Applications Menu“** bietet ein klassisches Kategorienmenü in der Systemleiste – das Menü ist schlicht, aber hübscher als der spartanische Classicmenu-Indicator.

„Places Status Indicator“ erscheint in der Systemleiste als „Orte“ und repräsentiert genau das, was der Nautilus-Dateimanager in der Navigationsleiste anbietet – die Standardverzeichnisse und die Lesezeichen.

„Floating Dock“ ist ein verspieltes, frei platzierbares Dock auf dem Desktop. Es zeigt sich nach der Installation als Icon mit drei weißen Punkten. Ein Klick blendet die Dock-Favoriten ein – standardmäßig identisch mit jenen, die das Ubuntu-Standarddock präsentiert. Mit anderen Worten: „Floating Dock“ ist als platzsparender, beweglicherer Ersatz für das Ubuntu-Dock gedacht, das man daher deaktivieren sollte. Das Dock bietet neben den Favoriten nach Rechtsklick auch noch Beenden-Optionen.

7. Icons auf dem Desktop

Gnome verbietet eigentlich Icons auf dem Desktop. Bei Ubuntu sorgt die vorinstallierte Gnome-Erweiterung „Desktop Icons NG“ (DING) für einige Desktopsymbole und Datenablage am Desktop. Das Wesentliche erreicht man über Rechtsklick am Desktop und „Arbeitsfläche-Einstellungen“ oder – identisch– mit dem Gang in die „Einstellungen“ und „Darstellung → Schreibtischsymbole“. Beides bleibt aber marginal – eine detaillierte Auswahl der Desktopsymbole bietet nur der Gnome-Shell-Extension-



Dconf-Editor: Die meisten Dconf-Einstellungen sind über reguläre Einstellungsmenüs erreichbar. Der Dconf-Editor geht aber, wie hier bei Nautilus, über offizielle Optionen hinaus.

Manager (Punkt 6). In der Zahnrad-Konfiguration der „Desktop Icons NG“ können Home-Ordner, Papierkorb, externe Laufwerke und Netzwerklaufwerke am Desktop aktiviert werden. Außerdem gibt es Positions- und Größeneinstellungen.

Eigene Desktopverknüpfungen? So wirklich dringend sind diese nicht, wenn das Dock für Programmfavoriten sorgt und die Erweiterung „Desktop Icons NG“ für wichtige Orte. Nichtsdestotrotz: Programmstarter erreichen Sie ganz einfach so (Beispiel):

```
cp /usr/share/applications/vlc.
  desktop ~/Schreibtisch/
```

Der so kopierte VLC-Starter muss dann am Desktop per Rechtsklick und „Start erlauben“ noch genehmigt werden. Desktopverknüpfungen zu Ordnern erstellen Sie hingegen am einfachsten per Softlink:

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

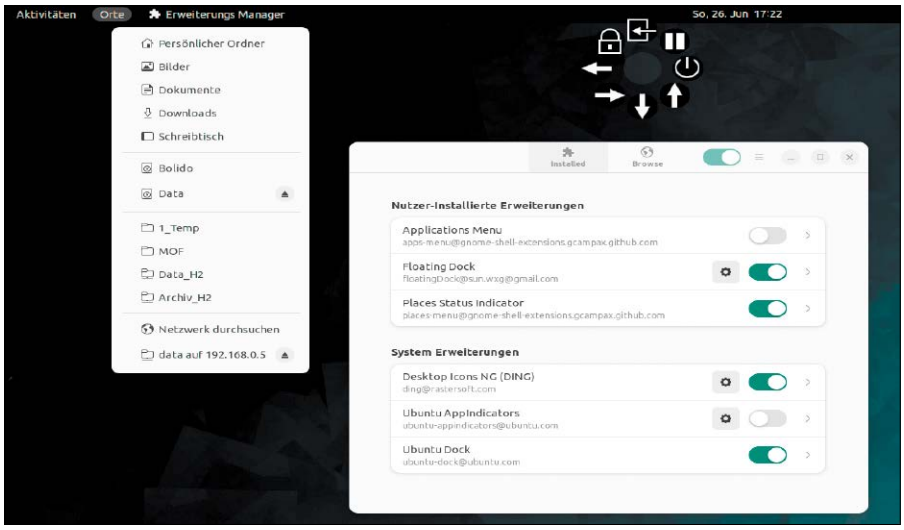
Das Ziel der Verknüpfung (hier „~/downloads“) muss dauerhaft verfügbar sein. Nicht gemountete Laufwerke oder Netzpfade führen zu Fehlern. Der Softlink ist also nicht geeignet, einen Automount auszulösen.

8. Nautilus-Erweiterungen

Der Dateimanager präsentiert sehr karge „Einstellungen“. Stets zu empfehlen ist die Option „Dauerhaft löschen“, die einen gleichnamigen Kontexteintrag aktiviert, um Dateiobjekte sofort zu löschen (ohne Papierkorb). Weitere Optionen sind zuschaltbar oder abstellbar, aber nur mit der Kenntnis der betreffenden Nautilus-Erweiterungen: So basieren etwa die Freigabeoption oder der Terminalstart im Nautilus-Kontext auf den Erweiterungen **nautilus-share** und **nautilus-extension-gnome-terminal**. Wer sie nicht braucht, kann sie per *sudo apt purge […]* vom System entfernen. Eine fehlende Erweiterung, die wir andererseits für wichtig erachten, nennt sich „nautilus-admin“. Ist diese installiert, zeigt der Dateimanager das zusätzliche Kontextmenü „Als Systemverwalter öffnen“. Geänderte Erweiterungen gelten immer erst nach der nächsten Anmeldung und eine Übersicht über alle Nautilus-Erweiterungen erhalten Sie so:

```
apt-cache search nautilus*
```

Noch individueller wird Nautilus durch selbst gebaute Erweiterungen. Da Ubuntu 22.04 das Tool nautilus-actions zum Ausbau des Nautilus-Menüs aktuell nicht mehr unterstützt, lassen wir diese Möglichkeit außen vor. Es gibt aber noch eine Option:



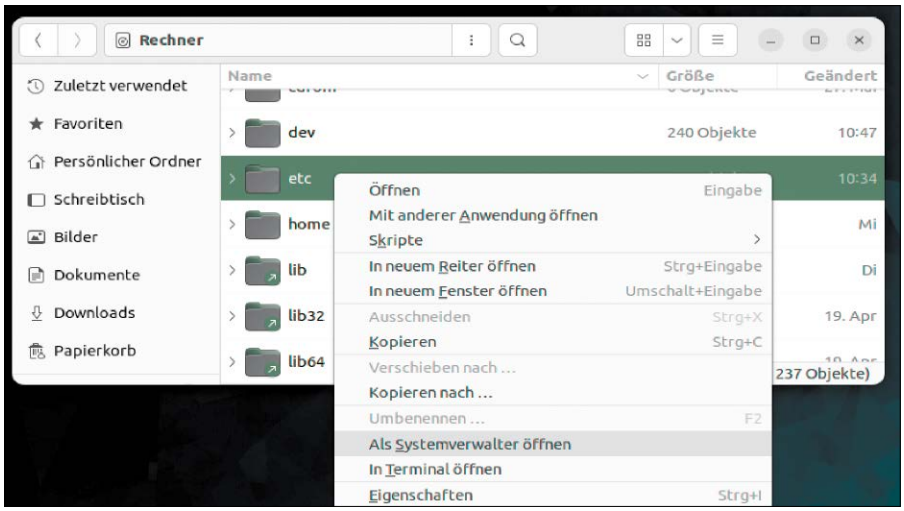
Gnome-Shell-Extension-Manager: Wer die Ubuntu-Oberfläche aufpeppen oder zähmen will, kommt an diesem Tool nicht vorbei (hier mit „Floating Dock“ und „ Places Status Indicator“).

Nautilus stellt unter „~/.local/share/nautilus/scripts“ ein spezielles Verzeichnis bereit: Hier enthaltene Shells-Scripts erscheinen im Kontextmenü unter „Skripte“, wenn mindestens ein Script vorliegt. Darunter zeigen sich die Scripts mit ihren Dateinamen (Endung „.sh“ ist nicht erforderlich). Ein nützliches Beispiel ist ein Script namens „Ver- und Entschlüsseln“ für schnelle Verschlüsselung von Ordnern und Dateien mit 7-Zip:

```
echo "$1" | grep ".7zEnc"
if [ $? -eq 0 ]
 then
 7z x -p"Das.G3heime.PASSW0RT" $1
 else
 7z a -p"Das.G3heime.PASSW0RT" -t7z
 -mhe=on $1.7zEnc $1
fi
```

Der entscheidende Vorteil gegenüber einer manuellen Nutzung mit dem Archivmanager dürfte klar sein: Das Passwort steht fest, wird beim Ein- und Auspacken per Script übergeben und muss nicht eingegeben werden. Da das Kennwort offen im Dateisystem liegt, eignet sich die Methode zwar nicht zum lokalen Datenschutz, aber sehr gut zum Versand von Daten in die Cloud.

Noch ein Hinweis: Verwenden Sie solche Scripts nur im Dateimanager, nicht am Desktop. Das Verhalten am Desktop ist – wie oft unter Gnome – nicht konsistent. In unserem Beispiel funktioniert das Verschlüsseln, aber nicht das Auspacken. Im Dateimanager unter „Schreibtisch“ gibt es kein Problem. ■



Nautilus-Erweiterungen: Viele Kontextoptionen basieren auf externen Tools, so auch der Wechsel zum root-Recht über die Erweiterung „nautilus-admin“.

Problemlösungen für Ubuntu 22.04

Auch LTS-Versionen Ubuntus sind nicht frei von Versäumnissen der Entwickler oder von eigenwilligen, unpraktischen Standardeinstellungen. Die folgende Sammlung präsentiert häufige Probleme und deren Lösungen in Ubuntu 22.04 LTS und Varianten.

VON DAVID WOLSKI

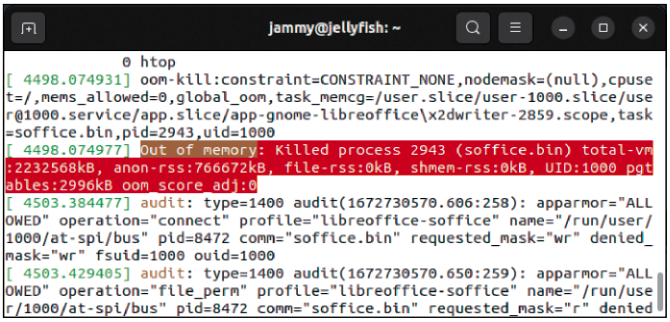


Kaum eine andere Distribution bekommt bei jeder Ausgabe so viel Aufmerksamkeit wie Ubuntu. Die Entwicklung von Ubuntu und die einzelnen Softwarepakete sind weiterhin eng mit Debian GNU/Linux verbunden, da dies die Basis für Ubuntu stellt. Auch im Entwicklerteam gibt es einige personelle Überschneidungen. Die Größe der Ubuntu-Community erlaubt eine Veröffentlichung alle sechs Monate und eine Ausgabe mit Langzeitsupport von fünf Jahren im Zweijahresrhythmus. Die praktische Erfahrung seit April hat gezeigt, dass Ubuntu 22.04 nicht weniger Probleme macht als noch die LTS-Version 22.04. Einige Schwierigkeiten mit Firefox als Snap-Paket und mit dem aggressiven Out-of-Memory-Killer von Systemd verlangen Nacharbeiten, die eine LTS-Version Ubuntus eigentlich vermeiden sollte. Einige dieser Probleme und Lösungen sind keine Fehler, sondern einfach auf einem Desktopsystem unpraktische Standardeinstellungen. Canonical hat mit seiner Linux-Distribution heute eher Server- und Cloud-instanzen als den Endanwender-Desktop im Fokus.

Die folgenden Themen behandeln Stolperfallen und Ungereimtheiten, die uns in der Redaktion selbst in Ubuntu 22.04 begegnet sind oder für welche auf der Frage-Antwort-Webseite *https://askubuntu.com* besonders häufig nach Lösungen gesucht wird. Einige der präsentierten Lösungen sind auch für Ubuntu 22.10 beziehungsweise im kommenden 23.04 relevant, denn auch dort werden wieder Snap-Pakete zu bändigen sein.

OOMD: Aggressiver Programmkiller

Server sollen auch in Situationen mit wenig freiem Arbeitsspeicher weiterlaufen und dürfen im Falle eines Speichermangels nicht einfach stehenbleiben. Systemd hat deshalb den Out-of-Memory-Dämon (OOMD) für Server eingeführt, der besonders speicherhungrige Prozesse bei knappem Arbeitsspeicher radikal beendet. Ab Ubuntu 22.04 ist dieser Programmkiller auch auf Desktopinstallation aktiviert und verursachte vielen Anwendern Probleme, weil vor allem Browserinstanzen auf Rechnern mit weniger als vier GB RAM oft abgeschossen wurden.



Übereifriger Programmkiller: OOMD ist in Ubuntu 22.04, 22.10 und 23.04 unterwegs. Auf Desktopsystemen mit weniger als vier GB RAM hilft ein Abschalten des Dienstes.

In Ubuntu 22.04.1 LTS und 22.10 gab es deshalb außerplanmäßige Updates für OOMD: Der Out-of-Memory-Dämon hat in der Konfigurationsdatei „/usr/lib/systemd/system/-.slice.d/10-oomd-root-slice-defaults.conf“ die Ergänzung „ManagedOOM Swap=auto“ erhalten und ignoriert deshalb zumindest Auslagerungsaktivitäten. Auf Systemen mit wenig Arbeitsspeicher wird OOMD auf Desktops aber weiterhin Programme beenden, die plötzlich sehr viel RAM beanspruchen. Um das Verhalten zurückverfolgen, dient folgendes Kommando, das die letzten Aktionen des automatischen Programmkillers in den Kernel-Meldungen mit den Zeilen „Out of memory“ zeigt:

```
sudo dmesg
```

Um OOMD in Ubuntu dauerhaft zu deaktivieren, dient dieser Befehl:

```
systemctl disable --now systemd-oomd
```

Nach unserer Einschätzung ist OOMD auf Desktopsystemen nicht hilfreich und nicht notwendig.

Snaps: Updates anhalten

Über ein gewöhnliches Systemupdate mittels apt wird Snap-Software nicht aktualisiert. Stattdessen verfügen Snaps über eine separate Updatefunktion, die alle installierten Pakete dieser Art täglich automatisch viermal aktualisieren will. Im Terminal zeigt das Kommando

```
snap refresh --time
```

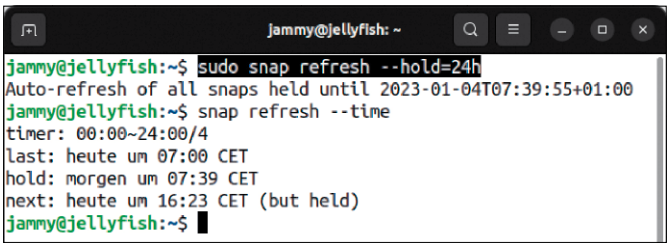
an, wann der nächste Check erfolgen soll. Diese kurze Frequenz hat einen Haken: Läuft eine Snap-Anwendung, so kann das Paket nicht aktualisiert werden und wird seit Ubuntu 22.04 auf den nächsten Updatecheck verschoben. Um neue Versionen installierter Snaps manuell zu installieren, kann dann der eingegebene Befehl

```
sudo snap refresh
```

manuell eine Aktualisierung ausführen. Unterwegs mit einem Notebook, wenn eine Internetverbindung deutlich langsamer ist, sorgt das automatische Update von Snaps wegen der knappen Bandbreite für Ungemach und wird eventuell gar nicht fertig. Für diesen Fall gibt es die neue Möglichkeit, Updates auszusetzen. Dafür ist eine aktuelle Version des Snapd-Rahmenwerks nötig, welche der Befehl

```
sudo snap refresh snapd --channel=latest/edge
```

installiert. Anschließend kann die Eingabe des Kommandos



Einen Tag lang anhalten: Damit Snap-Aktualisierungen im Hintergrund nicht Bandbreite verschwenden, können diese Updates mit diesem Befehl aufgeschoben werden.



Wo bleibt der Sound? Die Mixeranwendung Pavucontrol kann die Audioeinstellungen, Geräte und Ausgänge überprüfen. In diesem Beispiel fehlt in Ubuntu 22.04 eine Konfigurationsdatei.

```
sudo snap refresh --hold=24h
```

die automatische Installation von neuen Snap-Versionen für 24 Stunden anhalten.

Pipewire und Pulseaudio

Bei der Wahl der Soundserver setzt Ubuntu 22.04 auf einen Mix aus dem herkömmlichen Pulseaudio und dem modernen Pipewire. Letzteres ist im System für Screensharing und Web RTC in Browsern unter Wayland zuständig. Die sonstigen Aufgaben bei der Soundausgabe erledigt weiterhin Pulseaudio.

Es passiert vor allem bei Upgrades von älteren Ubuntu-Systemen auf 22.04, dass Pulseaudio in diesem Gespann zunächst nicht funktioniert. Die Mixeranwendung Pavucontrol ist zur Überprüfung nötig, ob die Ausgabe überhaupt unter „Konfiguration“ eingeschaltet ist. Sie muss aber zunächst mit

```
sudo apt install pavucontrol
```

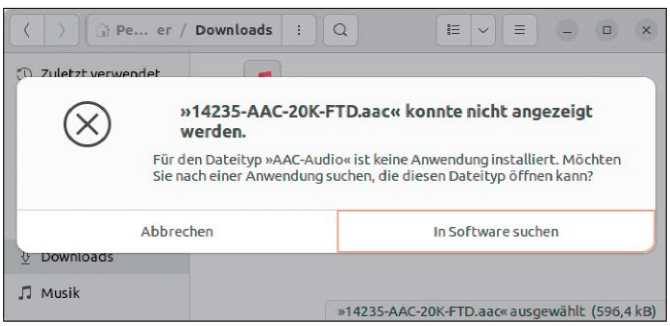
installiert werden. Gibt es keine Ausgänge für Pulseaudio beziehungsweise nur ein Ausgabegerät namens „dummy“, so ist meist die Konfiguration nach einem Upgrade nicht komplett. Die beiden Befehle

```
sudo touch /usr/share/pipewire/media-session.d/with-pulseaudio
systemctl --user restart pipewire-session-manager
```

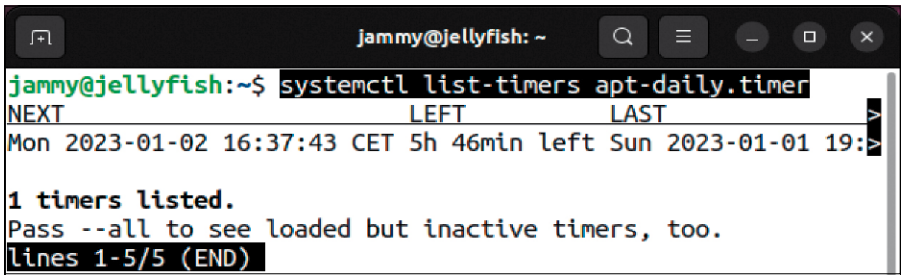
korrigieren das Problem.

Nachrüsten: Codecs und Extras

Ubuntu liefert in seinen Paketquellen nicht nur Open-Source-Programme aus, sondern auch Linux-Software, die einer kommerziellen oder auch unklaren Lizenz unterlie-



Diese Suche läuft oft ins Leere: Gnome versucht, ein passendes Programm für eine Mediendatei zu finden, und kann auch nach Codecs suchen, aber dies gelingt meistens nicht.



Wann ist die nächste Systemaktualisierung? Die von Haus aus aktivierten „Unattended Upgrades" blockieren den Paketmanager bei umfangreichen Updates eine ganze Weile.

gen. Dazu zählen einige Audio- und Videocodecs und Truetype-Fonts von Microsoft, die für die Darstellung einiger Webseiten und Dokumente vorteilhaft sind. Die von einigen Gnome-Programmen angebotene Suche nach Codecs in den Paketquellen ist nicht immer erfolgreich. Zuverlässiger ist es, gleich nach der Ubuntu-Installation alle häufig benötigten Codecs und Extras in einem Terminalfenster mit diesem Befehl

```
sudo apt-get install ubuntu-
 restricted-extras gstreamer1.0-
 plugins-bad gstreamer1.0-plugins-
 ugly
```

nachzurüsten.

Blockiertes apt: Unattended Upgrades

Eher für Server interessant, aber auch in der Desktopausgabe von Ubuntu 22.04/22.10 aktiviert, ist die automatische Installation von Sicherheitsupdates im Hintergrund über den Dienst „Unattended Upgrades". Damit die Server der Paketquellen dabei nicht überlastet werden, lösen Ubuntu-Systeme den Download an zufälligen Zeiten aus. Wann das eigene System wieder ein Hintergrundupdate startet, zeigt das Kommando

```
systemctl list-timers apt-daily.
 timer
```

in der Kommandozeile an.

Bei langsamen Internetverbindungen oder im WLAN führt dies nach dem Start des Systems immer wieder dazu, dass der Paketmanager apt längere Zeit nicht für andere Aktionen verfügbar ist, weil im Hintergrund Updates installiert werden. Der Hinweis von apt in der Kommandozeile lautet dann „E: Could not get lock /var/lib/dpkg/lock - open (11: Ressource unavailable)".

Wenn dies ein immer wieder auftretendes Problem ist, dann empfiehlt es sich, die Aktualisierungen besser regelmäßig manuell mit *sudo apt upgrade* einzuspielen und die automatischen Sicherheitsupdates abzuschalten. Auf Desktopsystemen ist dies völlig legitim. Um den Dienst zu konfigurieren, dient der Aufruf dessen Konfigurations-Scripts:

```
sudo dpkg-reconfigure -plow
 unattended-upgrades
```

In einem angezeigten textbasierten Menü schaltet dann die Auswahl „Nein" die automatischen Updates aus.

Paketmanager: Werbung abschalten

Wer in Ubuntu 22.04 mit apt in der Kommandozeile Updates und das Paketmanagement vornimmt, erhält beim Aufruf im Terminal hin und wieder Werbung für Ubuntu Pro. Dies ist ein Extraservice Canonicals, welcher nach einer Registrierung insgesamt zehn Jahre Updates für Ubuntu LTS verspricht. Nach Kritik an den zusätzlichen Nachrichten hat Canonical verraten, dass sich diese Werbeeinblendungen mit dem Kommando

```
sudo pro config set apt_news=false
```

sehr einfach abschalten lassen.

Server: Einfachere Netzwerkkonfiguration

Während Debian-Server ihre Netzwerkeinstellungen im alten Stil über die Datei „/etc/network/interfaces" erledigen, nutzt der Ubuntu Server schon seit Ausgabe 18.04 LTS seine eigene Konfigurationsmethode über Netplan.io. Es handelt sich dabei um einen Parser für das YAML-Format, um auch komplexe Netzwerkkonfigurationen abzubilden. Netplan.io ist aber speziell für die Ubuntu-Server-Ausgabe gemacht und in keiner anderen Linux-Distributionen per Standard eingerichtet. Von Canonical gibt es auf der Webseite *https://netplan.io* eine Vorstellung mit englischsprachigen Beispielen zum Einstieg.

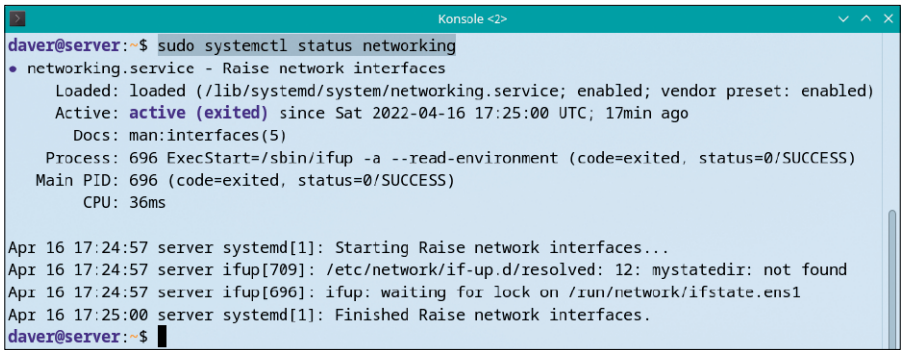
Netplan.io ist nur eine Abstraktionsschicht mit eigener Syntax. Wer diese nicht verwenden will, kann wieder die herkömmliche Netzwerkkonfiguration im Debian-Stil auf einem Ubuntu-Server nutzen, der dabei aber vorübergehend offline geht. Das ist beim Wechsel zu bedenken. Zuerst gilt es, den Hardwarenamen der Netzwerkschnittstelle zu ermitteln, die der Befehl

```
ip a
```

im Abschnitt „2:" für Ethernet anzeigt und die beispielsweise „enp3s0" lautet. Diese Angabe muss man sich notieren, denn sie ist für die herkömmliche Konfigurationsdatei wichtig.

ALTERNATIVE NETZWERK-KONFIGURATION

```
#loopback
#Datei /etc/network/interfaces
auto lo
iface lo inet loopback
#Ethernet, "enp3s0" bitte anpassen
auto enp3s0
allow-hotplug enp3s0
iface enp3s0 inet dhcp
```



Herkömmliche Netzwerkkonfiguration in Ubuntu 22.04 nutzen: Die Ausgabe von systemctl zum traditionellen Netzwerkdienst zeigt, ob der Umstieg geklappt hat, und hilft bei der Fehlersuche.

Den herkömmlichen Debian-Netzwerkdienst installiert dann dieses Kommando:

```
sudo apt install ifupdown
```

Wie bei Debian erwartet dieser Dienst eine klassische Konfigurationsdatei namens „/etc/network/interfaces“, die mit root-Recht erstellt wird:

```
sudo nano /etc/network/interfaces
```

Diese Datei erhält den Inhalt, wie er im Kasten „Alternative Netzwerkkonfiguration“ hier abgebildet ist. Die Angabe „enp3s0“, also der vorher ermittelte Hardwarename der Schnittstelle, muss unbedingt angepasst werden. Damit die Netzwerkschnittstelle automatisch über DHCP ihre IPv4- und IPv6-Adressen bezieht, verlangt auch noch die Datei „/etc/dhcp/dhclient.conf“ eine Ergänzung: Ganz unten fügt man hier diese Zeile ein:

```
send dhcp-client-identifier =
  hardware;
```

Nun kann vor dem Neustart des Serversystems der Systemd-Dienst für Netplan.io mit folgendem Kommando deaktiviert werden:

```
sudo systemctl mask networkd-
  dispatcher systemd-networkd-wait-
  online systemd-networkd.socket
  systemd-networkd
```

Danach steht der Neustart des Ubuntu-Systems mit *sudo reboot* an und dort zeigt dann die Eingabe von

```
sudo systemctl status networking
```

an, ob alles geklappt hat.

Schlägt die Initialisierung des Netzwerks fehl, so liegt dies meist an einer ungültigen Hardwareadresse der Ethernet-Schnittstelle und es lohnt sich hier eine erneute Kontrolle auf die Ausgabe von „ip a“.

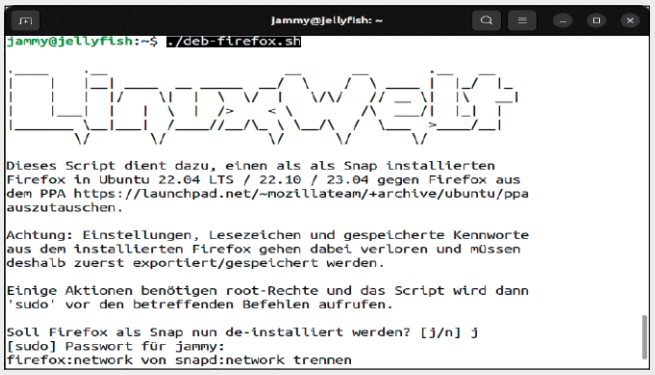
Ubuntu-Server bei Internetprovidern: Ist ein Ubuntu-Server nur per SSH erreichbar, dann ist diese Operation durchaus riskant, denn schlimmstenfalls ist die Maschine erst mal nicht erreichbar. Es empfiehlt sich deshalb zuvor als Nothaken, die Möglichkeiten einer Verbindung zum Server per KVM oder webbasierter Konsole zu aktivieren oder auch gleich alle Schritte über eine Notfallkonsole auszuführen. Die meisten Serveranbieter und Clouddienste bieten diese an. ■

FIREFOX UND CHROMIUM ALS DEB-PAKET

Als Canonical ausgerechnet Chromium und dann auch noch den Standardbrowser Firefox als Snap-Paket in Ubuntu auslieferte, war die Skepsis bei vielen Anwendern zu Recht groß. Denn die Browser starten als Snap zu langsam und einige Add-ons wollten auch nicht mehr funktionieren, weil Berechtigungen fehlen. Mittlerweile hat Canonical bei der Einbindung von Firefox nachgebessert – der Start ist deutlich flotter und viele Erweiterungen wie etwa die Gnome-Browsererweiterung zur Einbindung von Gnome-Shell-Extensions von *https://extensions.gnome.org* funktionieren wieder. Dennoch bleibt der Start auf Systemen mit schwächeren CPUs zunächst bei beiden Browsern schleppend, denn Snaps liefern ein gepacktes Dateisystem mit, das erst mal dekomprimiert werden will.

Firefox und Chromium gibt es in den aktuellen Ubuntus nicht mehr in den offiziellen Paketquellen. Allerdings liefern weiterhin PPAs, also externe Paketquellen, die Webbrowser stets aktuell in der üblichen Form als DEB-Paket aus: Für Firefox gibt es von der Mozilla Foundation das PPA *https://launchpad.net/~mozillateam/+archive/ubuntu/ppa* und für Chromium bietet sich *https://launchpad.net/~phd/+archive/ubuntu/chromium-browser* an. Eine Schwierigkeit ist es aber, Firefox oder Chromium als Snap erst einmal loszuwerden. Denn bei dem vorhandenen DEB-Paket in den Standard-Paketquellen handelt es sich um einen Platzhalter, der immer wieder das Snap installiert. Auch ein Systemupdate würde den als DEB installierten Firefox wieder gegen das Snap-Paket austauschen.

Es ist also mehr zu beachten: Per apt-Pinning muss das nachträglich installierte DEB eine höhere Priorität bekommen als das Snap-Paket aus den regulären Quellen. Gut ist es außerdem, falls die unbeaufsichtigten Updates aktiviert sind, diese auf Firefox beziehungsweise Chromium automatisch auf den neusten Stand bringen. Insgesamt kommen hier eine Menge kleine Handgriffe im Terminal zusammen, die in der Wiederholung auf mehreren Ubuntu-Systemen lästig werden. Wir haben deshalb für die Installation von Firefox und Chromium über die



Firefox als DEB-Paket: Das Script von Heft-DVD deinstalliert das Snap-Paket in Ubuntu 22.04 und holt den Browser vom offiziellen PPA der Mozilla Foundation.

genannten PPAs jeweils ein Shell-Script erstellt, dass diese Handgriffe übernimmt und dabei gut nachvollziehbar ist. Für Firefox ist das Script „deb-firefox.sh“ im Unterverzeichnis „Software“ auf der Heft-DVD und für Chromium erledigt „deb-chromium.sh“ die Installation. Zuvor werden die Browser als Snap erst deinstalliert, falls vorhanden. Diese Aktionen verlangen nach dem sudo-Passwort und fragen dies im Terminal zuvor ab. Um eines der Scripts zu starten, kopiert man es in einen beliebigen Ordner, macht es mit

```
chmod +x deb-firefox.sh
```

ausführbar und ruft es dann mit

```
./deb-firefox.sh
```

auf. Das Script „deb-chromium.sh“ verlangt die gleiche Behandlung. Die weiteren Schritte sind in der Ausgabe des jeweiligen Scripts erläutert und es gibt auch eine kurze Anleitung, wieder das Snap zu installieren, falls gewünscht.

Hinweis: Eine Deinstallation des Snap-Pakets löscht alle vorhandenen Profildaten, Lesezeichen und eventuell gespeicherten Passwörter. Diese Daten sollte man deshalb zuvor exportieren und danach im klassischen DEB-Browser wieder importieren.

Alte Rechner neu belebt



Muss man grundsolide ältere PCs, Notebooks und Netbooks entsorgen, weil sie heutigen Standards nicht mehr entsprechen? Es kommt darauf an – auf die Rolle, die das Gerät erfüllen soll, aber auch auf objektive Hardware-Limits.

VON HERMANN APFELBÖCK

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 sogar überlegen. Trotzdem gibt es klare Grenzen, wo sich Hardwarerecycling nicht mehr lohnt oder jedenfalls nicht mehr Spaß macht. In diesem Artikel geht es um die Hardwarekriterien, die ein Altgerät zum Recyclingkandidaten machen – oder eben nicht. Der nachfolgende Beitrag bespricht dann Rollen und Einsatzzwecke und die dafür passende Linux-Systeme. Zwei weitere Artikel gehen spezieller auf alte Datenträger und Mac-Hardware ein.

Der erste Hardwarecheck

Auch auf 20 Jahre alter Hardware bringen Sie noch ein Linux zum Laufen, aber es wird schwierig, dafür sinnvolle Rollen zu finden. Die Mindestanforderungen für ein Gerät, das sich mit befriedigender Leistung wiederbeleben lässt, liegen etwa auf dem Niveau der kleinen Platinenrechner Raspberry & Co. Anhand der folgenden Kriterien treffen Sie eine Vorauswahl:

- **Prozessor:** Brauchbare bis gute Leistung bieten 64-Bit-CPUs mit zwei Kernen und einer Taktrate von einem GHz aufwärts. Diese etwa für Netbooks typische Ausstattung reicht für kleine Serverrollen, grenzwertig auch noch als Zweitdesktop und zum Surfen. Theoretisch finden Sie sogar ab einer CPU Pentium III oder AMD Athlon und 256 MB RAM spezialisierte Linux-Distributionen, die solcher Hardware angemessen sind. Mehr als ein irgendwie noch laufendes System ist damit aber nicht zu erwarten.
- **Prozessoreigenschaften:** Das CPU-Thema PAE – eine Eigenschaft, um mit 32-Bit-CPUs mehr als 3,2 GB RAM zu adressieren – sollte man ad acta legen. Hardware ohne PAE-fähige CPU ist ein Fall für den Elektronikschrott, wenngleich manche Linux-Spezialdistributionen solche CPUs immer noch unterstützen (Varianten mit dem Stichwort „non-pae“, „legacy“). Generell sind 32-Bit-Prozessoren so veraltet (mindestens 15 Jahre), dass Recyclingversuche wenig Freude versprechen. Nennenswerte Ausnahmen sind alte Netbooks mit Intel-Atom-CPUs, die zwar größtenteils mit 32 Bit arbeiten, aber für kleine Serverrollen durchaus genügen.
- **Arbeitsspeicher:** Zwei bis vier GB RAM sind für sparsames Desktop-Linux ausrei-

chend für kleine Serverrollen ist ein GB RAM die absolute Untergrenze.

• **Netzadapter:** Betagte Rechner haben oft einen Fast-Ethernet-Adapter (100 MBit/s). Diese Netzwerkleistung ist für einen Zweitdesktop oder kleinen Heimserver ausreichend; wirklich servertauglich ist dieses Tempo allerdings nicht (siehe aber Kasten „Kostengünstiges Upcycling“).

• **USB:** USB 3.0 wäre optimal, wenn das Altgerät als Datenserver arbeiten soll. USB 2.0 sollte aber für jeden Zweitdesktop und auch noch für einen Datenserver mit moderaten Ansprüchen genügen, für einen kleinen Intranet-Webserver allemal. Geräte mit USB 1.x sind hingegen nicht mehr alltagstauglich.

• **Stromverbrauch:** PC-Veteranen verbrauchen kaum unter 60 bis 70 Watt (ohne Monitor) und sind schon aus diesem Grund schlechte Kandidaten für eine Neubelebung als Server-Dauerläufer. Notebook-Oldies liegen bei 40 bis 45 Watt. Zum Vergleich: Aktuelle Platinenrechner und Notebooks begnügen sich mit fünf bis maximal 20 Watt. Geräte für den Dauerbetrieb sollten diese Marke nicht oder allenfalls moderat überschreiten: Mit 20 Watt ist ein Gerät im Dauerbetrieb kein Stromfresser: Die Jahresrechnung eines solchen Miniservers im Dauereinsatz beträgt dann bei einem aktuellen Strompreis von 35 Cent pro Kilowatt etwa 65 Euro. Einfache Messgeräte sind ab acht

Je älter die Hardware, desto höher meist der Stromverbrauch: Ob ein Gerät – als Dauerläufer – in Betracht kommt, kann ein Messgerät prüfen (ab zehn Euro). Der abgebildete digitale Hama-Stecker liegt bei etwa 25 Euro.



Quelle: de.hama.com

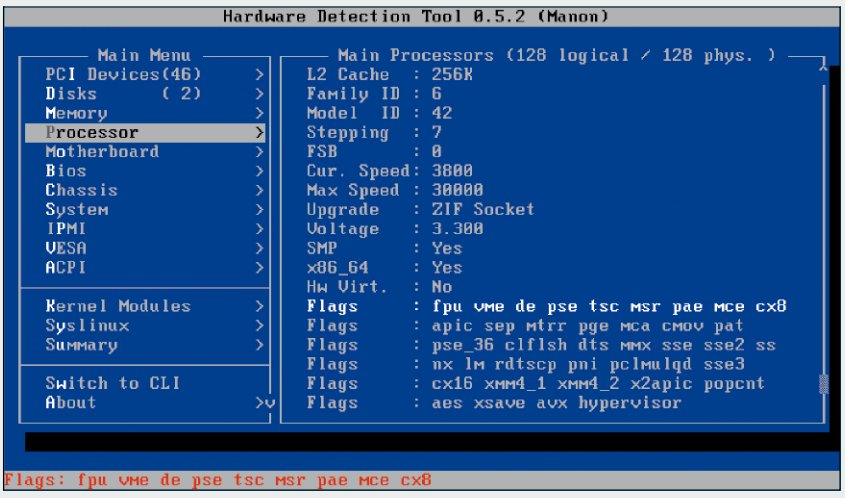
HARDWAREANALYSE MIT HDT

Wer ein altes Notebook aus dem Keller kramt, muss erst einmal wissen, welche Hardware in diesem Gerät steckt. Was leistet die CPU, wie viel RAM steckt auf dem Motherboard? Funktioniert die Festplatte noch und wie groß ist sie? Wenn auf dem Gerät noch ein System läuft, kommen Sie mit Tools wie inxi (Linux) oder msinfo32 (Windows) an die Infos.

Unabhängig von einem System sind Sie mit dem bootfähigen Minisystem Hardware Detection Tool (HDT, *www.server elements.com*), das auf jeder LinuxWelt-DVD unter „Extras und Tools“ startbereit ist. Falls kein optisches Laufwerk vorliegt, können Sie das HDT-ISO mit einem Linux-Laufwerkstool oder dem Win 32 Disk Imager (auf Heft-DVD) auf einen USB-Stick kopieren. Das setzt dann aber die Bootfähigkeit via USB voraus.

In HDT verwenden Sie den „Menu mode“. Dieser zeigt unter „Summary“ das CPU-Modell mit Angabe über 32 oder 64 Bit sowie die RAM-Kapazität. Genauer wird es unter den Kategorien „Processor“ und „Memory“, die sich mit den Cursortasten ausklappen lassen. Unter „Processor“ erscheinen das CPU-Modell und die Architektur-Info („x86_64“ - „Yes“ oder „No“) sowie alle CPU-Eigenschaften als „Flags“ (so auch die früher vieldiskutierte „pae“-Eigenschaft.). Infos zu internen Festplatten liefert HDT unter „Disks“.

Wichtig für die Tauglichkeit als Datenserver sind die Angaben unter „PCI-Devices“: Sie informieren über Grafikkarte, Soundchip, Ethernet (Fast oder Gigabit?), WLAN-Chip (altes 801.11g, brauchbares 801.11n oder aktuelleres 801.11ac?). Ein K.-o.-Kriterium ist die USB-Version. USB 3.0 erkennen Sie schon äußerlich an den blauen USB-Buchsen. Ob jedoch USB 2.0 vorliegt oder inakzeptables USB 1.x, ist äußerlich nicht ersichtlich und auch unter HDT nicht ganz eindeutig zu ermitteln: Was HDT unter „PCI-Devices“ für den „USB (Host) Controller“ anzeigt, ist oft erst anhand der gezeigten Produkt-IDs zu recherchieren. Allgemein indizieren unter HDT die Abkürzungen „OHCI“ eine USB-Version 1.1, „EHCI“ Version 2.0 und „XHCI“ Version 3.0. Ganz eindeutig ist dies nicht, da auch Bezeichnungen wie OHCI2 auftauchen, was dann für USB 2.0 spricht. Die Recherche der USB-Version ist eventuell schneller durch einen empirischen Test zu erledigen, wobei ein Kopiertempo von 20 bis 30 MB/s die USB-Version 2.0 indiziert.



HDT-Tool auf Heft-DVD: Das Werkzeug zeigt alle Hardwarekomponenten eines Rechners, unter anderem auch die detaillierten Prozessoreigenschaften.



Altes Netbook als Datenserver: Das ist mindestens Homeoffice-tauglich, wenngleich Geschwindigkeitsrekorde mit Fast Ethernet und USB 2.0 nicht zu erwarten sind.

Euro erhältlich und zeigen die Leistungsaufnahme in Watt an (pro Stunde).

• **Geräuschentwicklung:** Welche Betriebsgeräusche verursacht das Altgerät? Die Frage spielt keine Rolle, wenn das Recycling in einer Serverrolle im Keller stattfindet, aber im Wohnzimmer sind surrende Lüfter und singende Festplatten störend.

• **Bootfähigkeit:** Altrechner sind oft nicht bootfähig über USB. Wenn dann auch kein funktionierendes optisches Laufwerk vorliegt, wird es eng. Selbst wenn Sie das künftige Linux-System auf die interne Festplatte installieren, brauchen Sie zumindest für die Installation den Bootvorgang von einem externen Laufwerk.

• **Sound und Wi-Fi:** Welche weitere Peripherie soll genutzt werden – und gibt es dafür Treiber? Wenn das Gerät Sound liefern oder im WLAN funken soll, müssen Sie die Funktionsfähigkeit vorab testen – am besten mit einem Linux-Livesystem.

Alte PCs und Platinen: Kaum zu retten

Wenn Ausbau-PCs ihre Zeit als Desktop trotz Aufrüsten überschritten haben, ist weitere Rollensuche zweifelhaft: Die Größe spricht ebenso gegen einen Einsatz im Wohnzimmerschrank wie Betriebsgeräusche durch alte Lüfter und Festplatten. Außerdem verbrauchen PC-Veteranen viel zu viel Strom und sind denkbar eher ungünstige Kandidaten für eine Serverrolle.

Zehn Jahre nach dem ersten Raspberry Pi werden auch die Nachteile von Ein-Platinen-Rechnern deutlich: Sie veralten rasend schnell. Wer von Anfang an mitgespielt hat und mehrfach auf leistungsstärkere Nachfolger oder Alternativplatinen umgestiegen ist, hat jetzt vermutlich die eine oder andere Platine in der Schublade, mit der sich nichts Ernsthaftes mehr anstellen lässt. Im Vergleich zu aktuellen Platinen sind die frühen Einkerner mit 512 MB RAM, langsamen Fast Ethernet und fehlendem WLAN bestenfalls noch Bastlermaterial.

Netbooks: Gut genug für Nebenrollen

12 bis 15 Jahre alte Netbooks sind komplette PCs mit kostengünstigen, leistungs-

KOSTENGÜNSTIGES UPCYCLING

Viele alte Rechner taugen noch für die eine oder andere Rolle. Wenn nicht, ist teures Aufrüsten kaum sinnvoll. Falls nicht zufällig passendes RAM, eine kleine SSD oder gar CPU, Grafikkarte in der Schublade herumliegen, lohnen Investitionen in der Regel nicht mehr. Zwei Ausnahmen gibt es:

Ethernet: Ältere Netbooks/Notebooks haben in der Regel nur einen Fast-Ethernet-Netzadapter (100 MBit/s). Das mag oft ausreichen, servertauglich ist das Tempo jedoch nicht, was spätestens bei Film- oder ISO-Dateien unangenehm auffällt. Der Netzdurchsatz lässt sich mit der Investition in einen USB-to-Ethernet-Adapter deutlich verbessern. Der in seinem Umfeld nicht ganz billige Delock Adapter (circa 22 Euro) mit schnellem USB 3.0 und schnellem Gigabit-Ethernet ist eine Empfehlung, weil er auf jedem von uns getesteten Gerät – vom Netbook/Notebook bis zum Platinenrechner – auf Anhieb funktionierte: einfach an einen USB-Port anschließen und am anderen Ende das Ethernet-Kabel. Die volle Netzwerkleistung (1000 MBit/s) erhalten Sie aber nur, wenn das Altgerät USB 3.x anbietet. Mit USB 2.0 erreicht der Adapter immerhin noch circa 300 MBit/s.

WLAN-Adapter: Ein fehlender oder veralteter Wi-Fi-Chip ist gleichfalls mit einer kleinen Investition zu beheben, die ein mittelaltes Gerät noch jederzeit rechtfertigt. Zahlreiche Linux-kompatible Wi-Fi-USB-Sticks wie Edimax EW-7811UN, Asus N10 Nano, Fritz-Wlan-USB-Stick-N v2.4, Hama WLAN-USB-Stick 54, CSL 300, Panda 300 N oder Hercules 300 N mini kosten etwa zehn bis maximal 25 Euro. Beachten Sie, dass alle WLAN-USB-Sticks USB 2.0 benötigen, um ihre Leistung ausschöpfen zu können.



Gigabit-Ethernet via USB: Diese Aufrüstmaßnahme ist nicht teuer (10 bis 25 Euro je nach USB- und LAN-Leistung) und macht Altrechner servertauglich.

Quelle: amazon.de

schwächeren und stromsparenden Komponenten. Typisch sind Intel-Atom-CPUs (seltener Celeron) mit bis zu 1,66 GHz, einem bis zwei GB RAM, USB-2.0-Ports, Fast Ethernet, WLAN (802.11n), Audiochip (Mikroeingang und Lautsprecherausgang), Kartenleser, kleines Display mit der Auflösung 1024 × 600. Die mechanische Festplatte bietet meistens 160 bis 250 GB. Netbooks arbeiten zwar nicht lüfterlos, aber leiser als Notebooks. Der Stromverbrauch liegt auch bei Hochlast unter 20 Watt, im Leerlauf unter zehn Watt.

Mit solchen Eigenschaften erreichen alte Netbooks nicht die Leistung eines aktuellen Raspberry Pi 4, kommen aber durchaus für kleine Serverrollen im Netzwerk in Betracht. Ein Einsatz als Dateiserver ist mit USB 2.0 und Fast Ethernet nicht optimal, aber machbar. Gar keine Gegenanzeigen gibt es, wenn das Netbook Aufgaben übernimmt, die kein hohes Datenaufkommen haben: Das kann eine abgespeckte Nextcloud sein oder ein Intranet-Wiki wie Mediawiki (benötigt komplettes LAMP-Paket mit Linux, Apache, My SQL und PHP, siehe *www.mediawiki.org*) oder Dokuwiki (benötigt Linux, Apache und PHP, siehe *www.dokuwiki.org*).

Notebooks: Zweitdesktop oder Top-Server

Eindeutig die lohnendsten Recyclingkandidaten sind bis zu zehn Jahre alte 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 und NAS-Geräte. Neben den allgemeinen Vorteilen des Notebooks wie Display, Tastatur, Maus, Stromversorgung für USB kann das Notebook in der Regel die schnellere CPU und mehr RAM vorweisen. Lediglich der Stromverbrauch ist beim Notebook etwas höher: Nicht allzu alte Notebooks verbrauchen bis zu 25 Watt.

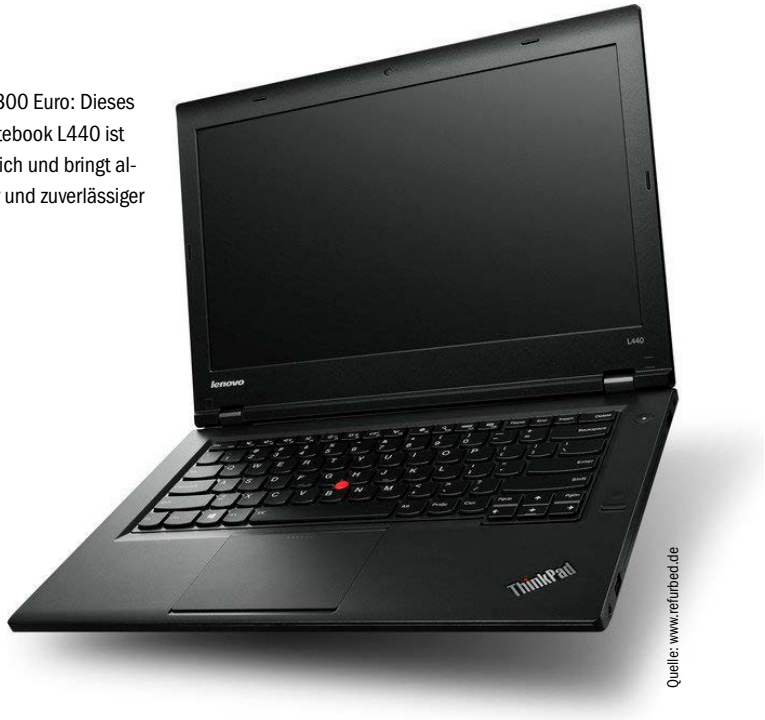
Kluge Home-Admins halten daher heute vermehrt Ausschau nach soliden Notebooks als Serverhardware. Gute gebrauchte Notebooks mit i3-CPU aufwärts, vier bis acht GB RAM sowie USB 3.0 und Gigabit-Ethernet kosten typischerweise 200 bis 400 Euro. Ein WLAN-Chip mit 802.11n, oft sogar 802.11ac ist ebenfalls Standard.

Besonders zu empfehlen sind nach unserer Erfahrung die Thinkpads von Lenovo, ferner auch Pro Books oder Elitebooks von HP. Eine größere Auswahl von Notebooks als B-Ware mit optischen Mängeln oder als renovierte Gebrauchtware („refurbished") finden Sie bei vielen Händlern. Einige Beispiele folgen unten.

Die Preisangaben beziehen sich auf das jeweils günstigste Angebot (Anfang September 2022), das die oben genannten Hardwareanforderungen erfüllt:

www.amazon.de (z. B. „Thinkpad gebraucht" ab 220 Euro)
www.conrad.de („Refurbished" oder „B-Ware" ab 199 Euro)
www.esm-computer.de (ab 199 Euro)
www.gebrauchtcomputer24.de/ (ab 199 Euro)
www.itsco.de/notebooks („B-Ware" ab 144 Euro)
www.luxnote-hannover.de („B-Ware-Pool", ab 199 Euro)
www.pollin.de („Refurbished" ab 249 Euro)
www.refurbed.de (ab 160 Euro)

Beachten Sie, dass der größte Schwachpunkt gebrauchter Notebooks für den Einsatz als stationärer Linux-Server keine Rolle spielt – der Akku nämlich. Wenn Netbooks oder Notebooks im Dauerbetrieb an der Steckdose hängen, können Sie den Akku komplett entfernen. Das Display, das bei Servern nur eine Nebenrolle spielt, folglich klein sein und auch Pixelfehler aufweisen darf, sollte per Funktionstasten so dunkel wie möglich eingestellt werden. ■



Homeserver für 200 bis 300 Euro: Dieses gebrauchte Thinkpad-Notebook L440 ist für etwa 200 Euro erhältlich und bringt alles mit, was ein schneller und zuverlässiger Linux-Server braucht.

Quelle: www.refurbed.de

RICHTIG ENTSORGEN

Der Friedhof für Altgeräte, für die sich beim besten Willen keine sinnvolle Rolle mehr findet, ist der Wertstoffhof mit seiner Ecke für den Elekronikschrott.

Solche Hardware stattdessen zu verschenken oder zu spenden, ist gar keine so „edle" Idee: Die Weitergabe delegiert letztlich nur die Entsorgungsarbeit an Dritte, denn auch Schüler, Senioren oder Nutzer in Entwicklungsländern brauchen ein funktionierendes Gerät, das ins Internet geht und in tolerierbarer Zeit Daten transportiert.

Vor der endgültigen Entsorgung ist ein Check dringend zu empfehlen: Das Gerät soll weg, aber nicht die persönlichen Daten! Micro-SD-Karten in Platinenrechnern oder Notebook-Kartenlesern sind leicht zu übersehen. Festplatten gehören entweder sauber überschrieben, zerstört oder zur Weiternutzung ausgebaut, falls sich das noch lohnt. Ob sich die Entnahme von RAM-Bausteinen, DVD-Laufwerken oder PCI-Karten lohnt, ist ebenfalls eine Ermessensfrage.

Linux für Oldies: Software und Rollen

Je nach Leistungsstärke der Altgeräte eröffnet sich enger oder breiter Spielraum für deren Einsatzgebiet. Dieser Beitrag gibt Empfehlungen für anspruchslose Desktopdistributionen und für realistische Serverrollen.

VON HERMANN APFELBÖCK

Alte Hardware kann oft produktiv weitergenutzt werden, wenn man anspruchslosere Rollen festlegt und/oder Systemleichtgewichte installiert. Mit diesem kreativen Akt retten Sie alte Hardware in ein neues Leben und beheben eventuelle Defizite im Homeoffice. Linux leistet dabei den entscheidenden Beitrag, weil es praktisch für jede Hardware und für jede Spezialrolle Systeme und Serverkomponenten bereitstellt.

Altgeräte in der Desktoprolle

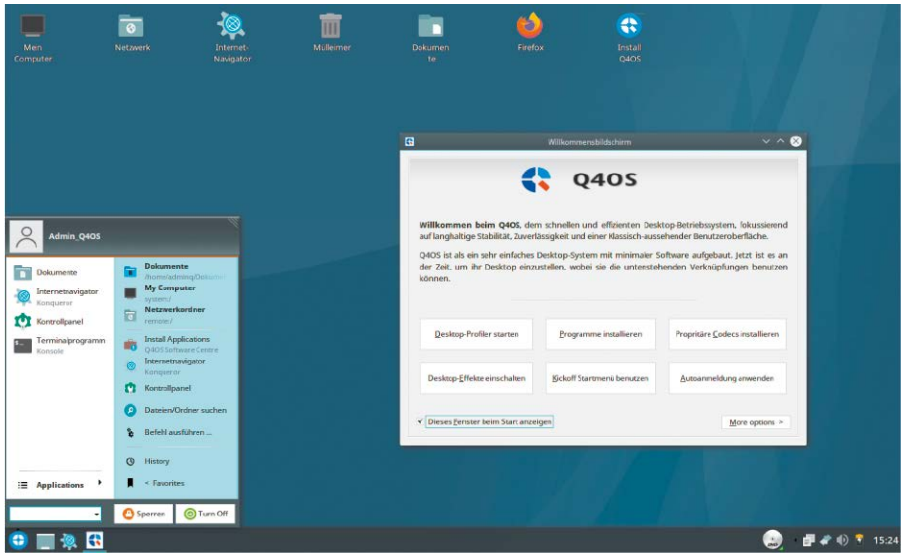
Eine Desktopnutzung bedeutet immer deutlich höhere Ansprüche an CPU, RAM und Grafik als ein Servereinsatz. Nicht allzu betagte Rechner können aber die Desktoprolle übernehmen, wenn Sie eine geeignete Linux-Distribution verwenden. Oft handelt es sich um Rechner, die zwar kein Windows oder Ubuntu Gnome mehr stemmen, aber mit einem schlanken Öko-Linux mühelos klarkommen. Technisch ist solches Upcycling keine Herausforderung, weil das jeweilige System nur installiert werden muss – dies in der Regel als alleiniges System ohne Rücksicht auf bestehende Verhältnisse. Schwierig ist dabei nur, die Distribution zu finden, die zur Hardware und zum Nutzer passt. Wir beginnen der Vollständigkeit halber ganz unten – bei Distributionen für ganz alte Hardware.

Desktops (1): Systeme für 32-Bit-CPUs (non-pae)

Linux-Systeme für moosalte 32-Bit-CPUs ohne PAE-Erweiterung gibt es kaum noch. Dies halten wir für angemessen, weil das Exhumieren solcher mindestens 20 Jahre alter Hardwareleichen kaum zu empfehlen ist. Auskunft über das PAE-Flag gibt das externe Tool HDT (auf Heft-DVD) oder in einem laufenden Linux-System der Terminalbefehl lscpu:

```
lscpu | grep pae
```

Bleibt die Ausgabe leer, hat der Prozessor kein PAE. Auf solcher Hardware werden Sie beim Start mittelgroßer Programme Geduld brauchen, erst recht bei Nutzung eines modernen Browsers. Selbst mit schlanken Linux-Browsern wie Midori bleiben die Reaktionszeiten mangelhaft. Trotzdem nennen wir hier drei der wenigen verbliebenen Distributionen, die weiterhin solche Hardware unterstützen. Beachten Sie, dass diese Distributionen selbstverständlich auch 64-Bit-Varianten anbieten und zum Teil später näher inhaltlich charakterisiert werden:



Öko-Distributionen sind selten Desktop-Schönheiten. Q4-OS gelingt mit dem schlanken Trinity-Desktop ein ansehnlicher Kompromiss.

Sparky Linux führt unter *https://sparkylinux.org/download/stable/* nach wie vor eine „non-pae"-Variante (mit LXQT-Desktop). Das unten nicht mehr charakterisierte Sparky ist mit LXDE-Desktop (es gibt auch diverse weitere) äußerst anspruchslos und schon mit 512 MB RAM problemlos zu betreiben.

Antix Linux (*https://antixlinux.com*) liefert seine 32-Bit-Varianten regelmäßig für „non-pae"-Kernel aus, ohne dass dies beim Download oder im Imagenamen explizit erwähnt würde.

Bodhi Linux bietet unter *www.bodhilinux.com/download* ein „Legacy Release", das dann noch klarer als „32 Bit non-pae" ausgewiesen wird.



Bodhi Linux hat sogar noch eine (ältere 5.1) 32-Bit-non-pae-Variante im Angebot. Das System ist extrem anspruchslos und schnell, aber mit Moksha-Desktop gewöhnungsbedürftig.

Desktops (2): Systeme für 32-Bit-CPUs

Die Unterstützung für 32-Bit-Hardware (mit PAE-Erweiterung) schwindet von Jahr zu Jahr, denn immerhin sind selbst die jüngsten Geräte mit 32-Bit-CPUs mittlerweile mindestens 15 Jahre alt. Zu ermitteln ist die Prozessorarchitektur am einfachsten mit dem Terminalbefehl lscpu, der in der zweiten Zeile als „CPU Operationsmodus" („CPU op mode") entweder nur „32-bit" bei „32-Bit-CPUs", hingegen „32-bit, 64-bit" bei 64-Bit-CPUs ausgibt. 64-Bit-CPUs können bekanntlich sowohl ein 32-Bit- wie ein 64-Bit-Linux verwenden. Nicht zuletzt dies ein guter Grund, nachfolgend einige empfehlenswerte 32-Bit-Distributionen zu nennen. Auf 32-Bit-Hardware müssen Sie solche Systeme installieren, auf 64-Bit-Hardware können Sie diese installieren, was grundsätzlich deutlich Arbeitsspeicher einspart (oft 200 MB im Vergleich zum identischen 64-Bit-System). Stehen nur ein oder zwei GB RAM zur Verfügung, sind 32-Bit-Distributionen auch auf 64-Bit-Hardware vorzuziehen. Die Nachteile von 32-Bit-Systemen sollten bei den hier relevanten Zielgeräten keine Rolle spielen: Es ist kein Uefi/GPT-Multiboot möglich und die Größe der Systempartition darf zwei TB nicht überschreiten.

Die meisten der verbleibenden sparsamen 32-Bit-Distributionen basieren auf Debian. Auch hier darf der Hinweis nicht fehlen, dass alle diese Distributionen selbstverständlich auch 64-Bit-Varianten anbieten:

Antix ist der Spezialist für „antike" Hardware. Mit 32-Bit-Debian-Basis und minimalem Desktop fordert es kaum mehr als 150 MB und läuft schon mit 512 MB RAM und auf Pentium-CPUs, die auf die Jahrtausendwende zurückdatieren. Lohnende Kandidaten sind aber zehn bis maximal 15 Jahre alte Notebooks, die Antix wieder zu richtig schnellen Systemen macht. Die Auswahl der richtigen Variante auf *https://antixlinux.com/download/* sollte mit „full" beantwortet werden. Antix ist mit einfachem Fenstermanager (icewm) weder attraktiv noch pflegeleicht und nur eine Empfehlung für Hardware, die ein absolut anspruchsloses System benötigt.

Bodhi Linux (*www.bodhilinux.com*) ist Ubuntu-basiert, aber ungleich schneller und kleiner. Die 32-Bit-Version ist standardmäßig für Non-PAE-CPUs ausgerichtet und fordert nur 150 MB für System und Desktop. Bodhi bootet schnell und ist am Desktop frappierend flott. Der eigenwillige Moksha-Desktop ist aber mindestens gewöhnungsbedürftig. Gravierender noch sind fehlende Konfigurationszentralen. Wer Monitoreinstellungen, Partitionen, Benutzerkonten bearbeiten will, ist überwiegend auf das Terminal angewiesen – nichts für Linux-Anfänger!

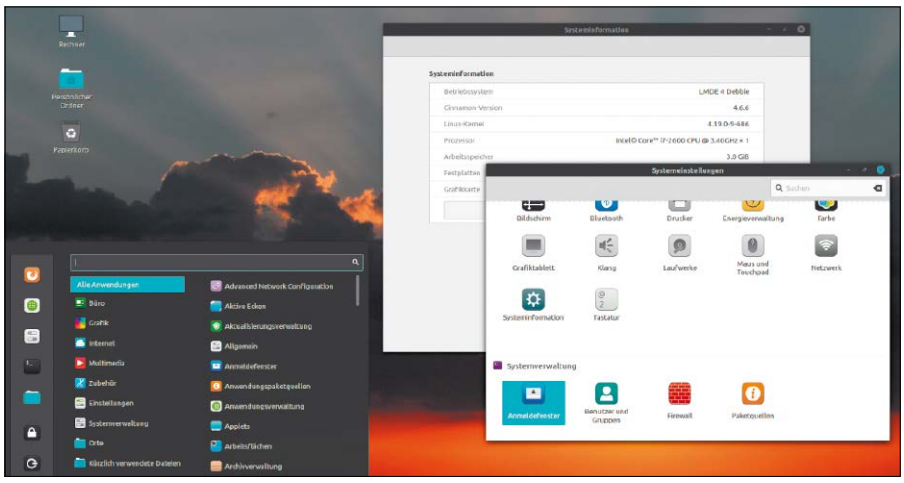
Q4-OS (*https://q4os.org*) gehört zu unseren Öko-Favoriten, weil ihm der Kompromiss zwischen Minimalismus und komfortablem Desktop gelingt. Das System mit der sparsamen KDE-Abspaltung Trinity konsumiert nach dem Start etwa 300 MB. Die Arbeitsfläche ist eine klassische Dateiablage, das Menü ähnelt dem Stil alter Windows-Versionen und die Systemleiste („Kontrollleiste") enthält mit Schnellstarter, Fensterliste und Indikatoren die typischen Elemente. Über das „Kontrollpanel" lässt sich jedes Element KDE-typisch individuell einrichten.

Kanotix (*www.kanotix.com*) ist ebenfalls ein guter Kompromiss für Nutzer, die ein unkompliziertes System suchen und sich auf der Oberfläche auf keine Experimente einlassen wollen. Als Desktop arbeitet ein schlankes LXDE, das sich bekanntlich durch Funktionalität auszeichnet, aber nicht durch ästhetischen Schick. Das vollständig deutschsprachige System belegt nach der Anmeldung etwa 350 MB RAM.

Folgende weitere, in 32 Bit verfügbare Distributionen werden für ältere Hardware immer wieder empfohlen, spielen aber bereits in einer Mittelklasse-Liga nahe Xubuntu und Lubuntu.

MX Linux 21.1 (*https://mxlinux.org*) mit XFCE ist der größere Bruder von Antix und gleichfalls noch in 32 Bit verfügbar. Mit etwa 500 MB Eigenbedarf für die 32-Bit-Variante sind ältere Notebooks mit zwei bis vier GB ein ideales Ziel für die Distribution.

Linux Mint LMDE5: Die Linux Mint Debian Edition (*https://linuxmint.com/download_lmde.php*) ist stets etwa später dran als das Ubuntu-basierte Mint, bietet aber wie dieses den beliebten Cinnamon-Desktop, der auf dieser schlanken Basis kaum mehr als 500 MB nach der Anmeldung fordert. Das komfortable System ist eine Option für bis zu zehn Jahre alte Hardware.



Linux Mint auf Diät: Die schlanke Debian Edition gibt es auch noch in 32 Bit und ist damit eine Alternative zu den Ubuntu-Leichtgewichten Lubuntu und Xubuntu (beide 64 Bit).

Desktops (3): Systeme für 64-Bit-CPUs

Für Altgeräte mit 64-Bit-CPU und mit vier GB RAM oder mehr sind 64-Bit-Distributionen zu empfehlen, allerdings nur solche mit reduzierten Ansprüchen an CPU, RAM und Grafik. Hier kommen genau die Kandidaten in Betracht, die bereits für 32-Bit-Hardware genannt wurden und allesamt auch in 64 Bit zur Verfügung stehen. Hinzu kommen noch die zwei anspruchslosesten Ubuntu-Editionen Lubuntu und Xubuntu mit LXQT- und XFCE-Desktop. Spezialisierte Oldie-Unterstützer wie Antix, Bodhi oder Q4-OS sind diese Ubuntus nicht, aber im Benutzeralltag pflegeleichter als diese Spezialisten.

Xubuntu 22.04: Nachdem Lubuntu (*www.lubuntu.me*) mit LXQT-Desktop (früher LXDE) nur noch um 100 MB sparsamer ausfällt als Xubuntu (etwa 500 MB nach Anmeldung), ist Xubuntu unsere Ubuntu-Empfehlung für ältere, aber noch nicht moosalte Hardware.

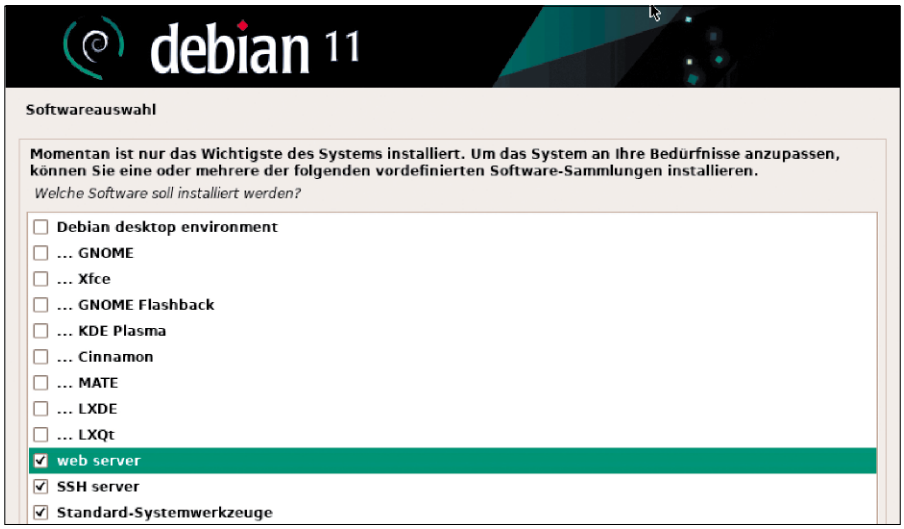
Xubuntu (*https://xubuntu.org*) bietet eine klassische Oberfläche, eine komfortable Einstellungszentrale und weitreichende sowie logische Anpassungsoptionen. Ein ähnlich unkomplizierter Kandidat bei ähnlichen Hardwareansprüchen ist die bereits genannte **Linux Mint Debian Edition** mit Cinnamon. Damit kann man den ungeliebten, wuchtigen Snaps (Firefox) aus dem Weg gehen, die auf Altrechnern noch weniger erwünscht sind als sonst.

Altgeräte in der Serverrolle

Während Altgeräte als Desktop über den Status eines Zweitsystems selten hinauskommen, können ältere Notebooks und Netbooks in der Rolle als Heimserver voll überzeugen. Im Prinzip sind Serverdienste auf jedem Desktop-Linux nachrüstbar. Trotzdem sind spezialisierte Serverdistributionen gerade auf schwächerer Hardware von Vorteil, weil sie auf Serverfunktionen fokussieren und auf überflüssige Komponenten verzichten.

Server (1): Headless-Server

Wer die Systemverwaltung per Kommandozeile beherrscht, kommt mit einem Headless-Server ohne Desktop und Eingabegeräte klar, der ausschließlich per SSH konfiguriert wird. Für leistungsschwache Hardware ist das ideal und falls der Server nur eine Konfiguration etwa als Samba- oder Webserver benötigt, hält sich der Aufwand in Grenzen. Gute Kandidaten für solche Server sind Debian, Ubuntu Server oder Open Suse Leap.



Basis für Serversetups: Der Debian-Netboot-Installer ist ein reines Setupprogramm mit einer kleinen Vorauswahl von System- und Serverkomponenten.

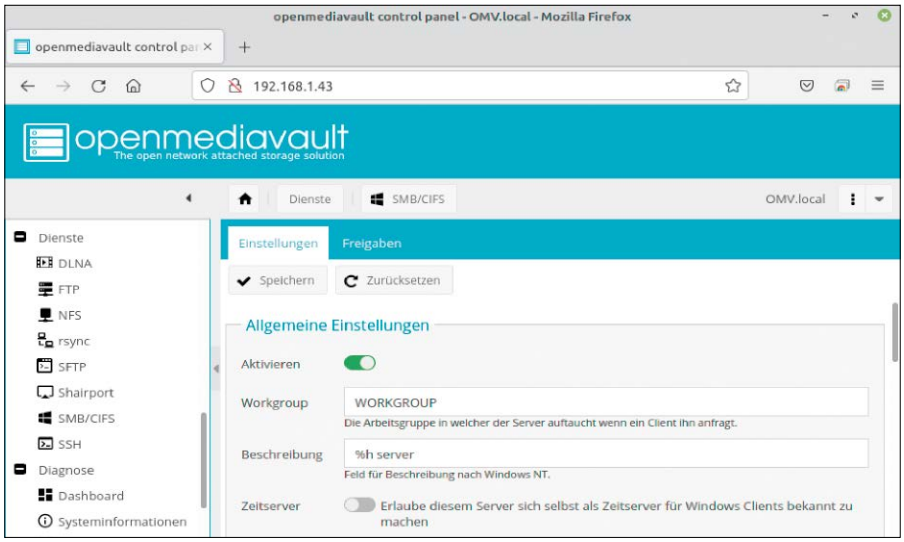
Debian: Für Debian laden Sie das Installerimage von *www.debian.org/distrib/netinst* für die passende Architektur (i386 für 32 Bit oder amd64 für 64 Bit). Dieses schreiben Sie auf einen USB-Stick. Nach dem Booten auf dem Zielgerät treffen Sie weitere Entscheidungen im Installer. Was Sie neben dem Basissystem haben wollen, fragt der Installationsassistent ab: Wichtig ist, „OpenSSH server" auszuwählen, andere Komponenten wie „web server" lassen sich auch später via SSH nachinstallieren.

Mit der Installation von Serverkomponenten wie Samba oder Apache ist es natürlich nicht ganz getan. Diese laufen dann zwar, müssen aber noch im SSH-Terminal konfiguriert werden. Nur SSH läuft voraussetzungslos: Sie brauchen nur die IP-Adresse des Serversystems und die Zugangsdaten des bei der Installation eingerichteten Kontos.

Server (2): Open Media Vault

Der pure Headlessbetrieb setzt Terminal-Know-how voraus und überfordert manche Home-Admins. Eine Alternative, die jedes ältere Gerät stemmt (was nicht für alle NAS-Systeme gilt), ist das Debian-System Open Media Vault (*www.openmediavault.org*). OMV ist nicht „einfach", aber einfacher und hübscher als pure SSH-Administration.

OMV bringt Serverdienste wie Samba, FTP, SSH standardmäßig mit. Das Download-ISO



Freies NAS-System: Open Media Vault macht aus einem Notebook einen Datenserver, der über eine Weboberfläche verwaltet wird.

ist ein Installer, der die wenigen Schritte gut erklärt. Nach der Installation erfolgt die Konfiguration über das Netzwerk via Browser (für die Konfigurationsoberfläche nutzt OMV den mitinstallierten Webserver Nginx). Sie benötigen lediglich die IP-Adresse des OMV-Rechners. Voreingestellt zur Anmeldung ist der Benutzer „admin“ mit dem Passwort „openmediavault“.

Angeschlossene Datenträger (Ext, FAT, NTFS, exFAT) lädt OMV beim Systemstart automatisch und zeigt sie als physische Festplatten unter „Datenspeicher → Reale Festplatten“. Wesentliche Einstellungen finden Sie unter „Dienste“, wo Sie für Netzfreigaben an Windows, Linux, Mac-OS „SMB/CIFS“ aktivieren. Danach kann im Register „Freigaben“ ein Datenträger oder Ordner freigegeben werden. Die zugriffsberechtigten Konten richten Sie unter „Zugriffskontrolle → Benutzer“ ein. Unter „Zugriffskontrolle → Freigegebene Ordner“ finden Sie die vorher unter „SMB/CIFS“ eingerichteten Freigaben, die hier über „Privilegien“ (Netzwerkrechte) detaillierter konfiguriert werden können.

Server (3): Nextcloud

Eine Nextcloud-Instanz ist auf älterer Hardware mit ein, zwei GB RAM problemlos zu betreiben, denn Nextcloud-Server sind modular und lassen sich fast beliebig skalieren und reduzieren. Viele Komponenten können schon bei der Installation, viele weitere im laufenden Betrieb abgewählt werden. Beispiele für eine reduzierte Spezialisierung wären der Einsatz als Samba-ähnliche Datenzentrale, als Notizensammlung oder auch nur als Intranetkalender.

Ein weiteres Motiv für Nextcloud ist die unkomplizierte Installation inklusive Apache-Webserver als Snap-Container. In Ubuntu ist die Snap-Umgebung standardmäßig dabei, auch beim Ubuntu-Server. Bei Bedarf kann dies mit

```
sudo apt install snapd
```

ergänzt werden und zur eigentlichen Installation von Nextcloud genügt dann dieser Terminalbefehl:

```
sudo snap install nextcloud
```

Danach ist die Nextcloud sofort einsatzbereit und mit der IP-Adresse des Servers mit jedem Browser erreichbar. Auf der Anmeldemaske vergeben Sie Kontonamen und Passwort für den Systemverwalter. Das Häkchen vor „Empfohlene Apps installieren“ können Sie deaktivieren, wenn Sie nur ganz bestimmte Komponenten verwenden möchten. Die benötigten Apps erreichen Sie später jederzeit über die Einstellungen („Zahnrad“ rechts oben) und den Menüeintrag „Apps“.

Server (4): Kodi-Mediencenter pur

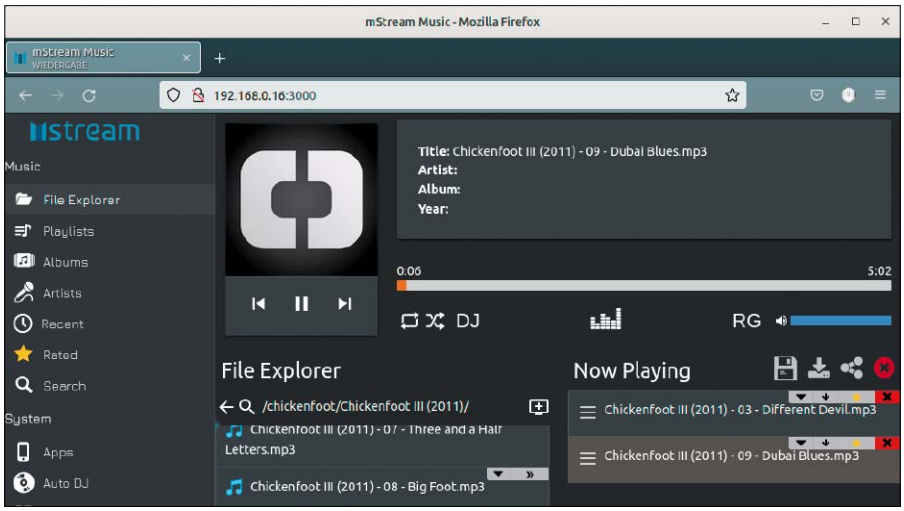
Was ein Raspberry Pi schafft, ist auch einem mittelalten Notebook zuzumuten, insbesondere dann, wenn es ausschließlich für diese Aufgabe abgestellt wird: Für das bekannte Mediencenter Kodi gibt es spezielle Linux-Distributionen, die als eigenständiges System ausschließlich Kodi starten. Das sehr schlanke Libre Elec („Just enough OS for Kodi“) gibt es für zahlreiche Platinenrechner, aber auch für x86-PCs. Download und Schreiben auf USB oder SD ist mit dem kleinen Tool „LibreELEC USB-SD Creator“ komfortabel automatisiert (*https://libreelec.tv*), peinlich nur, dass es das Tool derzeit nur für Windows gibt. Das Tool holt das gewünschte Installerimage („Generic AMD/Intel/Nvidia“ für PCs und Notebooks) aus dem Netz und schreibt es auf USB oder SD-Karte. Nach dem Booten dieses Images auf dem Zielgerät kopiert der Installer das System auf einen zweiten endgültigen USB-Stick. Eine Installation auf Festplatten ist nicht vorgesehen, diese sollen die Film- und Musikmedien anbieten. Kodi arbeitet als Abspielstation und als Samba- und UPnP-Server, sofern diese Serverdienste unter „Einstellungen → Dienste“ aktiviert werden.



Kodi pur: Libre Elec liefert eine minimale Systembasis für das Mediencenter. Das abgebildete Tool vereinfacht den Download und das Kopieren auf USB-Stick.

Server (5): Audioserver Mstream

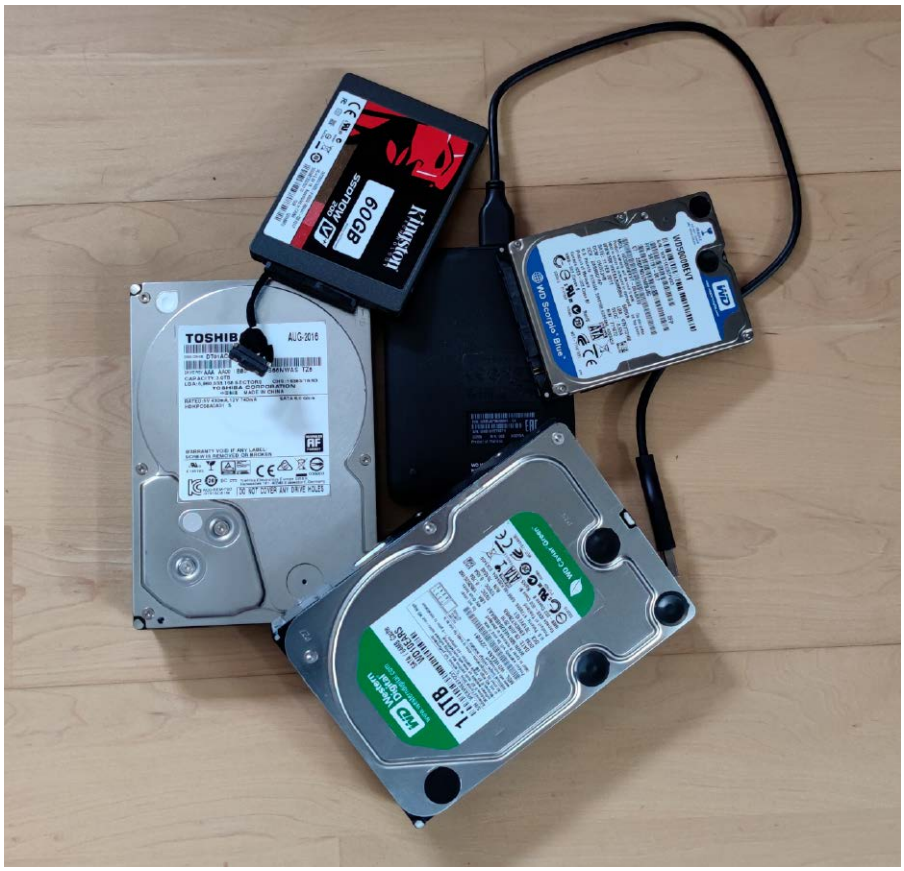
Mit einem Mediacenter wie Kodi ist ältere Hardware vor allem dann überfordert, wenn sie etwa auch noch als Desktop arbeiten soll. Die Rolle als Audioserver ist aber auch nebenher realistisch. Eine rundum empfehlenswerte Lösung für eine zentrale Musiksammlung (keine Filme und Bilder) ist das Electron-Programm Mstream, das unter *https://mstream.io/* zu beziehen ist – für Linux aktuell ausschließlich als Appimage (für x86-Architektur mit 64 Bit sowie für ARM in 32 und 64 Bit). Das heruntergeladene Appimage muss man nur ausführbar schalten und starten. Danach erscheint es am lokalen Desktop in der Systemleiste, vor allem aber in jedem Browser mit „http://[IP-Adresse]:3000“. Die Nutzung und Bedienung des englischsprachigen Servers ist schick, funktional und einfach. Das Einrichten der Musikordner geschieht über den Punkt „Admin Panel“. ■



Hübscher zentraler Musikserver: Die Serveranwendung Mstream stemmt ein älterer Rechner auch noch neben anderen Aufgaben.

Was tun mit alten Datenträgern?

Die allermeisten Datenträger gehen nicht kaputt, sondern werden aufgrund zu geringer Kapazitäten nach einigen Jahren unpraktisch bis nutzlos. Das Wiederbeleben alter Datenträger kann sich lohnen, ist aber nicht immer sinnvoll.



VON HERMANN APFELBÖCK

Betriebssysteme, Software und Benutzerdateien fordern immer mehr Platz: Linux-Containerformate sind extreme Speicherfresser, Medienformate werden immer anspruchsvoller, weil die Qualitätsansprüche steigen. Wenn aktuell vier TB auf mechanischen Festplatten für annähernd 100 Euro zu haben sind, dann werden Datenträger weitgehend überflüssig, die mit einem TB oder 500 GB vor etlichen Jahren noch Standard waren. Bei SSD sind die Kapazitäten deutlich geringer, aber auch hier verdoppeln sich die Standardgrößen alle zwei Jahre. Dieser Beitrag diskutiert, ob Datenträger vergangener Jahre noch Nutzbringendes leisten können.

Alte SSDs haben Jobgarantie

Wenn SSDs aufgrund mangelnder Kapazität in ursprünglicher Rolle ausgedient haben, finden Admins und Bastler immer eine produktive Zweitverwertung – selbst für kleine Datenträger mit nur 60 oder 120 GB. Als Daten- und Serverspeicher scheiden solche SSDs allerdings nicht nur wegen der geringen Größe aus, sondern auch deshalb, weil die SSD-Leistung bei Benutzerdaten und beim Netzwerkzugriff kaum Vorteile bringt. Es sollte sich also um das System oder um systemnahe Dienste handeln. Folgende Szenarien sind zu überlegen:

A. Ältere Notebooks: Zehn Jahre alte Notebooks haben oft noch die originale mechanische 2,5-Zoll-Festplatte mit 300 bis 500 GB im Betrieb. Deren Austausch durch eine 2,5-Zoll-SSD ist keine technische Herausforderung (Kreuzschraubendreher genügt) und macht aus einem lahmen Gerät sofort ein befriedigendes bis flottes. Überlegen muss man trotzdem: 60, 80, 120 GB genügen zwar nachhaltig für ein schlankes oder mittleres Linux-System, aber Daten und Medien muss das System Servern oder externen USB-Laufwerken überlassen.

B. Platinenserver: Betriebssysteme für Platinen werden überwiegend auf SD-Karten geschrieben. Selbst wenn diese schnell sind (UHS-1 ist Pflicht, besser UHS-2), ist eine kleine SSD eindeutig besser und für platinentypische Aufgaben genügt selbst eine 60-GB-SSD locker. Die Auswahl SATA-boottauglicher Platinen ist aber schmal: Odroid M1, Odroid H2, Banana Pi sind nativ dabei, der Raspberry Pi 4 nur mit Erweiterungsboard (Geekworm X825 für circa 37 Euro). Beim Raspberry kommt einschränkend hinzu, dass die SSD über USB 3.0 angeschlossen und dadurch gebremst wird. Das Booten über USB muss eventuell außerdem noch durch ein Firmware-

upgrade und einige Anpassungen vorbereitet werden: Nur für Bastler!

C. Portable Programme: Dieses Szenario kann sich in Ausbau-PCs lohnen, die das System auf einer mechanischen Festplatte betreiben oder deren System-SSD zu klein wird. Nach dem Einbau einer älteren kleinen SSD nimmt diese portable Programme auf, die hier signifikant schneller laden. Windows ist hier im Vorteil, weil es dafür Hunderte von kleinen und großen portablen Programmen gibt (siehe *https://portableapps.com/*). Vergleichbar unter Linux ist Software im Appimage-Format (siehe *https://appimage.github.io/apps/*). Die Software muss nur auf die schnelle SSD kopiert werden und startet dort unabhängig von System und Systempfaden.

D. SSD als Cache für die mechanische Systemfestplatte: Für diese reizvolle Idee gibt es mit Bcache, Dmcache, LVM-Cache mehrere Ansätze, die aber allesamt nicht mehrheitstauglich sind. Noch die praktikabelste Methode ist der LVM-Cache, der aber nur für Datenlaufwerke funktioniert, weil der Grub-Bootloader keinen LVM-Verbund von System- und Cachelaufwerk starten kann.

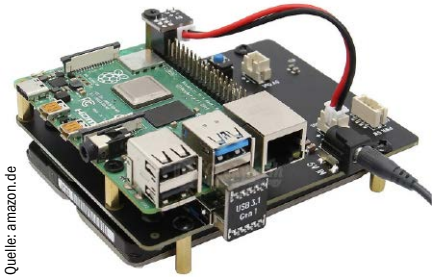
Alte Festplatten realistisch beurteilt

Mechanische Festplatten mit vier TB kosten etwa 100 Euro – je nach Qualität auch weniger oder mehr. Eine ältere Platte mit einem TB ist folglich maximal 25 Euro wert. Noch kleinere Kapazitäten lohnen kein Upcycling etwa durch Zukauf eines USB-SATA-Adapters. Hinzu kommt ein multiplizierter Stromverbrauch, wenn statt einer großen Festplatte mehrere ältere zum Einsatz kommen. Mit zwei oder drei 3,5-Zoll-Festplatten an USB gerät der Gesamtverbrauch eines kleinen Platinenrechners schnell in den Bereich eines großen Ausbau-PCs. Mit acht Watt im Leerlauf und bis zu 15 Watt bei Hochlast ist pro Platte zu rechnen. 2,5-Zoll-Platten verbrauchen im Leerlauf zwei Watt, bei Last bis zu zehn Watt.



Quelle: amazon.de

USB-SATA-Adapter ohne Stromversorgung: Solche Stecker eignen sich für 2,5-Zoll-Laufwerke und SSDs und kosten fünf bis 20 Euro. Achten Sie unbedingt auf USB 3.0.



Quelle: amazon.de

Zusatzplatine von Geekworm für SATA-Datenträger: Die Datenverbindung läuft über USB 3.0, das beim Raspberry 4 neuerdings bootfähig ist. Die Einrichtung erfordert dennoch erfahrene Anwender.



Quelle: conrad.de

Dockingstationen vermeiden Kabelsalat, Kapazität und Leistung sind aber oft heikel zu recherchieren. Die abgebildete Renkforce USB 3.2 ist eines der günstigsten Modelle.

USB-SATA-Adapter: Sollen ausgebaute Festplatten extern angeschlossen werden, sind Hardwareinvestitionen unumgänglich. Für 2,5-Zoll-SATA-Festplatten oder SSDs genügt ein USB-SATA-Adapter ohne Netzteil, da 2,5-Zoll-Geräte über den USB-Anschluss mit Strom versorgt werden. Die günstigsten Adapter beginnen bei etwa fünf Euro. Mindestens 12 Euro kostet ein Adapter, der für 3,5-Zoll-Laufwerke die notwendige Stromversorgung mitbringt.

USB-3.0-Hubs: Wer mehrere Festplatten nutzen will, kommt mit den USB-Ports am Rechner oft nicht aus. USB-Hubs lösen das Problem, sollten für ausreichende Stromversorgung aber immer aktiv, also mit eigenem Netzteil gewählt werden. Beim Anschluss an Raspberry & Co. ist ein aktiver Hub sogar Pflicht. Für entsprechende USB-3.x-Hubs mit Netzteil sind mindestens 20 Euro fällig.

Dockingstations: Festplatten-Dockingstations sind aufgeräumte Lösungen, die den Kabelsalat erheblich reduzieren. Alle einfach einzuschiebenden Festplatten werden von der Dockingstation mit Strom versorgt, was Netzteile und Steckdosen einspart. Außerdem gibt es nur noch ein einziges Datenkabel zum Rechner (meist USB 3.x). Damit sich eine flexible 4-Bay-Station, die mindestens 70 Euro (Renkforce USB 3.2), aber auch über 200 Euro (Startech 4-Bay-Dockingstation) kosten kann, noch so eben lohnt, kommen nur Laufwerke ab zwei TB in Betracht.

Allerdings ist eine solche Station ein Wert für sich und kann künftig auch größere Datenträger aufnehmen. ■

NUR INTAKTE DATENTRÄGER NUTZEN!

Eine neue Rolle für alte Datenträger kommt nur in Betracht, wenn diese technisch einwandfrei sind. Den Zustand fragen Sie mit SMART ab (Self-Monitoring, Analysis and Reporting Technology). Datenträger, die keine SMART-Antworten geben, sind sehr alt und in der Regel Elektronikschrott.

Gnome-Disks und der KDE-Partitionmanager können SMART-Werte abgreifen und anzeigen. Gnome-Disks bietet im Drei-Punkt-Menü mit der Option „SMART-Werte und Selbsttests“ ausführliche Auskunft zum markierten Laufwerk. Wichtigste Aussage oberhalb der Einzelwerte ist das Resümee „Das Laufwerk ist in Ordnung“. Das Gnome-Tool kann aber keine Geräte am USB-Port analysieren.

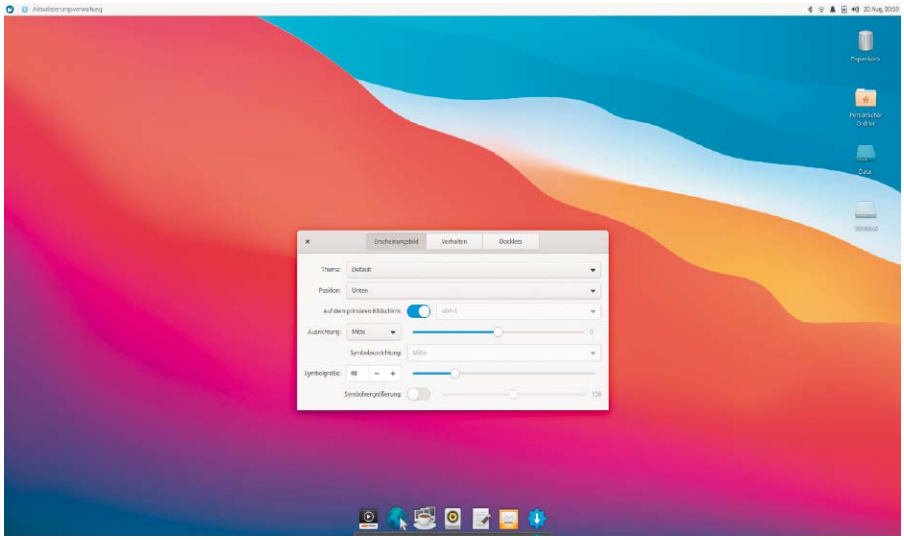
Der KDE-Partitionmanager äußert sich unter „Gerät → SMART-Status“ knapper, jedoch sollten die Angaben „SMART-Status: Gut“ und „Gesamtbewertung: Gesund“ genügen. Das KDE-Tool hat den großen Vorteil, auch Festplatten am USB-Port zu prüfen. Alternativ können Laufwerke an USB auch die „smartmontools“ im Terminal aushelfen:

```
sudo smartctl -H /dev/sd[x]
```

Wenn dieser Health-Test mit „PASSED“ beantwortet wird, ist die allgemeine Tauglichkeit des Laufwerks schon erwiesen.

Mac-Upcycling mit Linux

Wenn die Hardware noch problemlos läuft, aber sich das aktuelle Mac-OS nicht mehr flüssig betreiben lässt, kann Linux einem älteren Rechner mit Apple-Logo ein zweites Leben schenken.



VON STEPHAN LAMPRECHT

Apple versorgt seine Computer verhältnismäßig lang mit Updates. Aber irgendwann ist hier auch ein natürliches Ende erreicht. Entweder kann die neuste Version des Betriebssystems gar nicht mehr installiert werden oder alles geht so langsam, dass es keinen Spaß mehr macht. Wer ältere Mac-Hardware sinnvoll weiternutzen will, sollte die Installation von Linux ausprobieren.

Abschied von Mac-OS

In diesem Artikel gehen wir davon aus, dass Sie sich endgültig von Mac-OS verabschieden wollen, also keine Dualboot-Option benötigen. Dabei bleiben die Vorarbeiten überschaubar, aber es ist zu empfehlen, eine Sicherung des aktuellen Stands der Festplatte durchzuführen. Falls Sie später doch noch eine Datei benötigen, die nicht via Cloud oder Time Machine gesichert war, können Sie auf ein Abbild (etwa von Carbon Copy Cloner) immer noch darauf zugreifen. Sobald das Installationsprogramm von Linux seine Arbeit verrichtet hat, geht das natürlich nicht mehr. Falls Sie für den Mac Schriften erworben haben, die Sie weiterverwenden wollen, sichern Sie mit dem Finder die Ordner „/System/Library/Fonts“ und „~/Library/Fonts“ zur Sicherheit auf einem externen Datenträger.

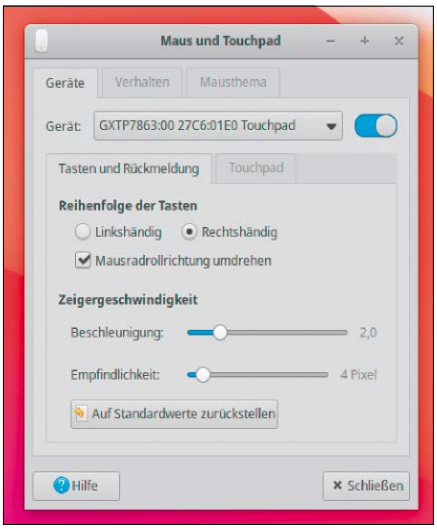
Xubuntu ist schnell und flexibel

Generell haben Mac-Besitzer die freie Wahl, was die Distribution betrifft. Ob Mac Book, iMac oder Mac Mini: Die grundlegenden Funktionen sollten Sie direkt nach der Installation reibungslos nutzen können. Probleme kann manchmal das WLAN bereiten, was sich aber mit etwas Recherche im Internet beheben lässt. Auch Spezialtasten auf dem Keyboard, wie die Regelung der Bildschirmhelligkeit oder Lautstärke, werden in den meisten Fällen problemlos erkannt. Nur beim Bereitschaftsmodus kommt es gelegentlich zu Problemen, die sich dann nur mit einem Neustart beheben lassen.

Da inzwischen nahezu alle Distributionen Livesysteme anbieten, ist vorheriges Ausprobieren zu empfehlen. Für diesen Artikel haben wir uns für Xubuntu entschieden. Das ist optisch nicht so nah am Mac wie etwa Elementary OS, dafür ressourcenschonend und schnell. Und es kann Richtung Mac-Desktop getrimmt werden. Laden Sie sich die aktuelle Version 22.04 von *https://xubuntu.org/*. Mittels Balena Etcher (*www.balena.io*) übertragen Sie die Datei dann auf einen USB-Stick. Sobald das erledigt ist, wird sich ein Mac-OS beklagen, dass es mit dem Datenträger nichts anfangen kann. Werfen Sie das USB-Laufwerk einfach aus.

Start und Installation

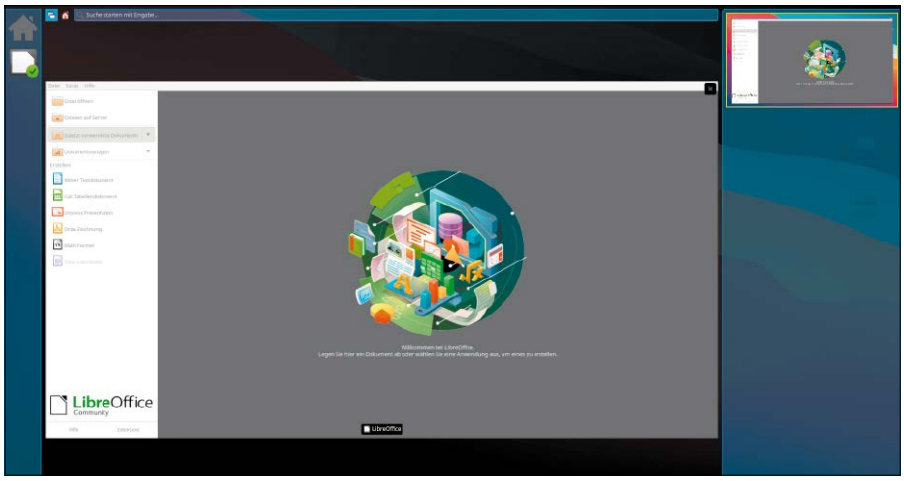
Der alte Mac sollte mit einer kabelgebundenen Maus und Tastatur verbunden werden. Kabellose Bluetooth-Eingabegeräte von Apple helfen nicht weiter, da diese beim Start von Xubuntu nicht erkannt werden. Stecken Sie den USB-Stick mit dem Betriebssystem an und starten Sie den Mac neu. Dabei halten Sie die Alt-Taste gedrückt („Wahl“- respektive „Option“-Taste). Der Mac wird sich erkundigen, welches System er starten soll. Statt „Macintosh HD“ nutzen Sie „EFI Boot“. Folgen Sie nun einfach den Anweisungen auf dem Bildschirm und lassen Sie die Installationsroutine ihre Arbeit machen. Am Ende werden Sie dazu aufgefordert, den Datenträger zu entfernen, und der Mac startet neu. Jetzt können Sie sich unter Xubuntu anmelden. Wer sich von alten Gewohnheiten und der vertrauten Um-



Mausverhalten: Mit einem Mausklick in den Einstellungen bringen Sie Xubuntu bei, beim Scrollen die Richtung des Macs zu nutzen.



Zubehörprogramme: Mit Synapse erzielen Mac-User das von Spotlight gewohnte Launcher-Feeling.



Xfdashboard: Diese Desktoperweiterung fürs Multitasking unter XFCE erinnert funktional an Exposé.

gebung von Mac-OS vollständig verabschieden will, ist damit bereits am Ende der Migration angelangt.

So wird Xubuntu etwas mehr zum Mac

Je nachdem, wie viel Zeit Sie investieren wollen, können Sie mit einigen Umbauten das neue System mehr wie einen Mac gestalten. Das betrifft die Optik wie auch das Verhalten.

Apple stellt die Hintergrundbilder der OS-Versionen zum Download bereit. Über die Bildersuche von Google finden Sie rasch die gewünschte Grafik. Nach dem Download klicken Sie mit der rechten Taste auf den Desktop und wählen „Schreibtischeinstellungen“ aus. Im Register „Hintergrund“ navigieren Sie zum Ordner mit dem Download und wählen das Bild aus. Wechseln Sie anschließend in „Symbole“. Über „Symbol → Orientierung“ können Sie die Icons an den gewohnten Platz „oben rechts senkrecht“ anordnen. Aktivieren Sie im Abschnitt „Standardsymbole“ auch noch die Option „Entfernbare Datenträger“. Das System fragt nach, ob es die vorhandenen Elemente auch gleich neu anordnen soll. Klicken Sie anschließend auf das Icon in der linken oberen Ecke des Desktops, um das Hauptmenü zu öffnen. Gehen Sie zu „Einstellungen → Maus und Touchpad“. Mit der Option „Mausradrollrichtung umdrehen“ legen Sie das Scrollen wie auf dem Mac fest.

Für langjährige Mac-Nutzer ist die Fenstersteuerung unter Xubuntu ungewohnt. In den Einstellungen finden Sie ebenfalls die „Fensterverwaltung“. Im Register „Stil“ können Sie im Abschnitt „Anordnung der Knöpfe“ die Symbole für Minimieren und Schließen mit der Maus auf die gewohnte linke Seite ziehen. Ebenfalls über die Einstellungen rufen Sie „Erscheinungsbild“ auf. Unter „Oberfläche“ wählen Sie das Theme „Adwaita“ und im Register „Symbole“ den Stil „Elementary XFCE“.

Zusätzliche Software für die Kür

Wem diese Kosmetik noch nicht ausreicht, kann mit zusätzlichen Programmpaketen weitere Funktionen des Macs nachrüsten. Ein für viele Mac-Nutzer zentrales Element ist das Dock – der Schnellstarter am unteren Rand des Bildschirms. Über das Anwendungsmenü rufen Sie das „Terminal“ auf und installieren das Plank-Dock:

```
sudo apt install plank
```

Das Programm finden Sie dann unter „Alle Anwendungen“ im Anwendungsmenü. Die Bedienung ist intuitiv und funktioniert wie auf dem Mac. Laufende Programme werden automatisch im Dock angezeigt und markiert. Mit einem Rechtsklick auf eines der Symbole sorgen Sie dafür, dass diese dauerhaft im Dock bleiben. Oder Sie ziehen das Symbol aus dem Anwendungsmenü auf das Dock. Weitere Einstellungen von Plank erreichen Sie, wenn Sie auf einem beliebigen Dock-Symbol bei gedrückter Strg-Taste einen Rechtsklick ausführen. Mit dem Terminalkommando

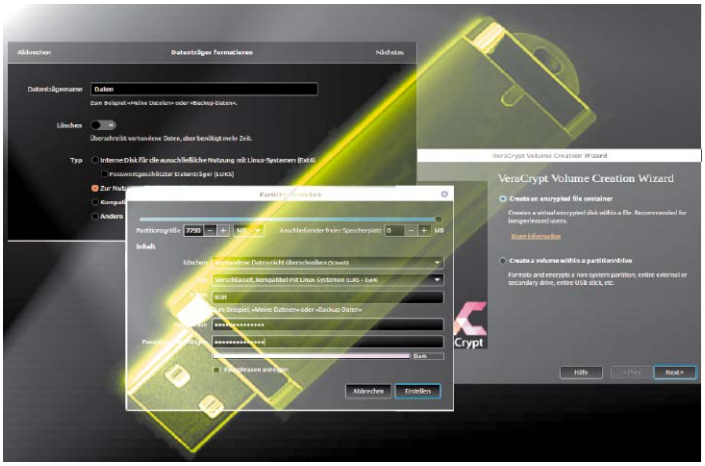
```
sudo apt install synapse
```

installieren Sie einen Launcher, der an Spotlight unter Mac-OS erinnert und Dateien sowie Anwendungen schnell findet. Einmal über das Anwendungsmenü gestartet, rufen Sie die Eingabezeile mit „Strg-Leertaste“ auf. In der rechten oberen Ecke finden Sie ein kleines Symbol, über das Sie die Einstellungen des Programms aufrufen. Dort ist auch die Option zu finden, um die App bei jedem Start des Systems automatisch auszuführen.

Wer Zeit investiert, kann noch mehr Mimikry betreiben. Hier erweist sich die Flexibilität von Linux als echter Vorteil. Es gibt fast nichts, was sich nicht an die Wünsche des Anwenders anpassen lässt. Zu bedenken ist dabei lediglich, dass sich das System damit immer weiter von seinem ursprünglichen Zustand entfernt, was es dann bei der Suche nach Support etwas schwerer macht, passende Tipps umzusetzen. Mit einem tieferen Eingriff in das System (mit dem Kommando *localectl*) können Sie die Funktion von rechter und linker Alt-Taste tauschen. Mit dem „vala-panel-appmenu“ legen Sie ein Anwendungsmenü fest, das die Funktionalität auf dem Mac nachahmt, und mit „Xfdashboard“ holen Sie sich eine Desktopfunktion, die an die Fensterübersicht „Exposé“ der Mac-Oberfläche Gnome erinnert. ■

Mobile Daten mit Linux

Der Heftschwerpunkt „Linux für den USB-Stick“ zeigt alle Methoden und Szenarien, die offenes Linux auf mobilen Medien – insbesondere auf USB – bereithält. Der Startbeitrag diskutiert den scheinbar einfachsten Einsatzzweck – des Datentransports.



VON HERMANN APFELBÖCK

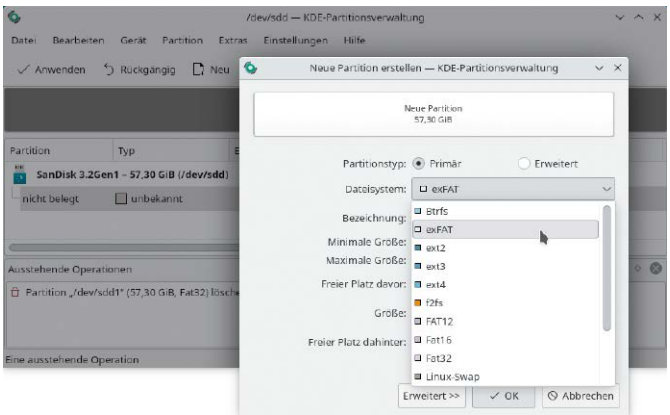
Linux läuft ohne Einschränkung auf USB-Datenträgern und mit USB 3.x fast wie auf Festplatte. Auch das Brennen auf DVD ist nach wie vor eine Option, freilich mit entsprechend reduzierter Geschwindigkeit. Insgesamt lädt diese Flexibilität dazu ein, Livesysteme oder sogar ordentlich installierte Distributionen als Zweit- oder Servicesysteme auf USB-Medien einzurichten. Diese sind dann transportabel oder erlauben zu Hause und im Büro einen schnellen Systemwechsel. Einsatzzwecke sind Rettungs- und Reparatursysteme, ganze Multibootsammlungen solcher Reparaturtools oder sichere Livesysteme zum Surfen. Auch der Einsatz als mobiles Büro oder Allzweckdesktop auf USB-Stick ist realistisch. Wir beginnen diesen Heftschwerpunkt allerdings mit der einfachsten und verbreitetsten Aufgabe, die USB-Datenträger meistens erfüllen: als Speicherplatz für Daten aller Art.

Der simple Datenstick

Benötigt ein USB-Datenträger, der nur Daten wie Texte, Musikstücke oder Filme transportieren soll, überhaupt Aufmerksamkeit oder technische Überlegungen? Nicht viel, aber bei ganz gedankenloser Nutzung kann man trotzdem ärgerliche Fehler machen. Bei der Formatierung des Medium ist es eine Überlegung wert, mit welchen Systemen der Stick später gelesen werden soll. Ein mit Linux-Dateisystemen wie Ext4, XFS, BTRFS formatiertes USB-Medium kann unter Windows gar nicht gelesen werden, unter Mac-OS nicht standardmäßig. Hinzu kommen die Dateirechte, die einen simplen Datenaustausch auch auf Linux-Empfängern eventuell erschweren.

Das Microsoft-Dateisystem NTFS ist eine vertretbare Wahl für Linux und Windows (unter Mac-OS nur lesbar). Hier sind weder technische Zugriffsprobleme noch Rechteprobleme noch Kapazitätslimits zu befürchten. Unproblematisch für den Datentransport ist ferner exFAT, ebenfalls ein Microsoft-Dateisystem, das inzwischen jedes Linux mit jüngerem Kernel ohne Nachinstallation versteht, ebenso Mac-OS und Windows sowieso. Entscheidender Vorteil gegenüber dem allseits kompatiblen FAT/FAT32 ist die unlimitierte Dateigröße: Bei FAT32 sind es nur vier GB pro Datei, ein Limit, das Filme oder ISO-Dateien schnell überschreiten. exFAT ist ein einfaches und „rechteloses“ Dateisystem, was einem Austauschdatenträger ebenfalls entgegenkommt. Jedes System und jeder Benutzer darf darauf lesen und schreiben.

In bestimmten Fällen ist das universale FAT32 aber unvermeidlich: Wenn ein Smart-TV (ohne Vermittlung durch PC und HDMI) Medien direkt am eigenen USB-Anschluss abspielen soll, kommt in der Regel nur FAT32 in Betracht. Andere Dateisysteme erkennen die TV-Geräte nicht. Ebenso steht es bei Tablets, wenn per OTG-USB-Anschluss ein USB-Stick eingelesen werden soll. Da es in solchen Fällen, insbesondere beim TV in der Regel um das Abspielen von Filmdateien geht, ist das Vier-GB-Limit eventuell lästig und kann nur durch Aufteilen großer Filmdateien kompensiert werden (mit Videoeditoren wie Openshot).



exFAT unter Linux: Für den unkomplizierten Austausch mit Windows sind Microsoft-Dateisysteme oft die einfachste Wahl bei der Formatierung von USB-Medien.

Die portable Softwaresammlung

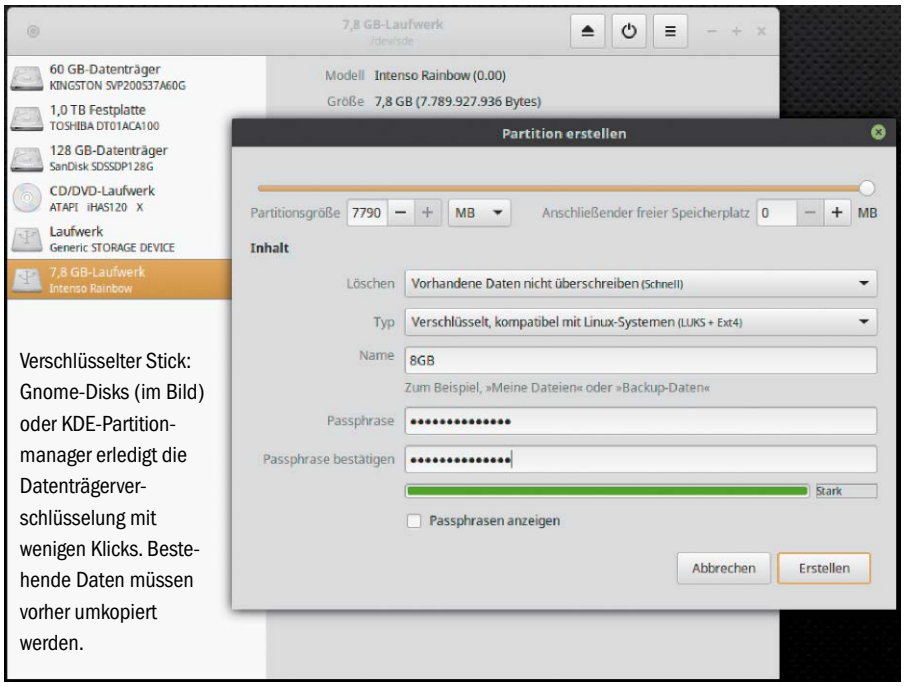
Die einzige Möglichkeit, Linux-Software auf USB zu bevorraten und mobil auf beliebigen Linux-Systemen zu nutzen, sind die distributionsunabhängigen Appimages. Appimages finden Sie verstreut im Web, indem Sie etwa nach „libreoffice appimage“ suchen. Die größte Sammlung solcher Appimages bietet *www.appimagehub.com*. Auch die Website *www.linux-apps.com* bietet im Listenfeld rechts oben den Filter „AppImage“. Es genügt, die gewünschte Software herunterzuladen und auf USB zu kopieren. Im Prinzip ist dann jedes Appimage-Programm direkt vom Stick einfach per Doppelklick zu starten.

Dabei ist nur eine Einschränkung zu beachten: Wenn Appimages direkt vom USB-Medium starten sollen, muss dieses mit einem Dateisystem formatiert sein, das erweiterte Dateiattribute vorsieht – also etwa Linux Ext4 oder Windows NTFS. Auf FAT32 und exFAT ist es nicht möglich, dem Appimage das notwendige „Ausführen“-Bit zuzuweisen (was je nach Distribution automatisch abgefragt wird oder manuell im Dateimanager über „Eigenschaften“ erledigt wird). Als Programmarchiv kann ein FAT-Stick aber trotzdem dienen. Zur Ausführung kopieren Sie die gewünschte Appimage-Datei dann einfach auf das Linuxsystem, das dann die Schaltung des „Ausführen“-Bits erlaubt.

Der verschlüsselte Datenstick

USB-Sticks- und -Festplatten sind klein und handlich – und gehen verloren oder bleiben am falschen Ort liegen. Daher ist Verschlüsselung für ein Laufwerk, das mehr als ein paar belanglose MP3-Dateien transportiert, fast ein Muss. Cryptsetup/Luks ist eine einbruchssichere Methode für schützenswerte USB-Daten. Ohne Zugangskennwort gestatten die Datenträger keinerlei Einblick in die Verzeichnisstruktur und in die Daten. Luksverschlüsselte USB-Medien können aber nur unter Linux geöffnet, gelesen und beschrieben werden. Wer seine verschlüsselten Daten auch unter Windows lesen will, muss andere Methoden nutzen (siehe unten).

Luks hat längst Einzug in grafische Systemwerkzeuge gehalten. Die KDE-Umgebung bietet den KDE Partition Manager (Partitionmanager), Gnome-affine Desktops (Gnome, Mate, Cinnamon, XFCE) haben das Tool „Laufwerke“ (Gnome-Disks) an Bord. Wir beschreiben die wenigen Klicks zur Verschlüsselung eines USB-Laufwerks am Beispiel von Gnome-Disks. Beachten Sie aber, dass Luks nicht „on the fly“ verschlüsselt: Der Datenträger wird für die Verschlüsselung komplett neu formatiert, daher müssen eventuelle Daten vorübergehend auf ein anderes Laufwerk kopiert werden.



Verschlüsselter Stick: Gnome-Disks (im Bild) oder KDE-Partitionmanager erledigt die Datenträgerverschlüsselung mit wenigen Klicks. Bestehende Daten müssen vorher umkopiert werden.

Sie schließen den USB-Stick an und starten das Tool „Laufwerke“. Dort hängen Sie das Laufwerk mit dem viereckigen Symbol links unterhalb der Partitionsanzeige aus. Löschen Sie mit der Minus-Schaltfläche eventuell bestehende Partitionen. Klicken Sie dann auf das Zahnradsymbol und auf „Partition formatieren“. Im Folgedialog wählen Sie als „Typ“ den Eintrag „Verschlüsselt, kompatibel mit Linux-Systemen (LUKS + Ext4)“. Der Eintrag „Name“ ist nicht erforderlich, macht aber den späteren Mountpunkt lesbarer. Danach geben Sie zweimal die „Passphrase“ – also das Kennwort ein. Ein Klick auf „Formatieren“ schließt den Vorgang ab. Sie können den Datenträger nach der Formatierung sofort mit Gnome-Disks einhängen und nutzen, indem Sie auf den unteren Balken der symbolischen Anzeige klicken und die Partition mit dem Pfeilsymbol links einhängen.

Für künftige Nutzung genügen Dateimanager wie Nautilus, Nemo, Dolphin. Wenn Sie das USB-Medium anschließen, erscheint automatisch der Dialog „Geben Sie eine Passphrase zum Entsperren [...] ein“. Nach Eingabe des korrekten Kennworts ist das Medium entsperrt und im Dateimanager unter „Geräte“ benutzbar. Auf Wunsch kann das Kennwort im Schlüsselbund des Systems gespeichert werden (unsicherer). Im Dateimanager können Sie den Datenträger später auch wieder trennen („Laufwerk sicher entfernen“).

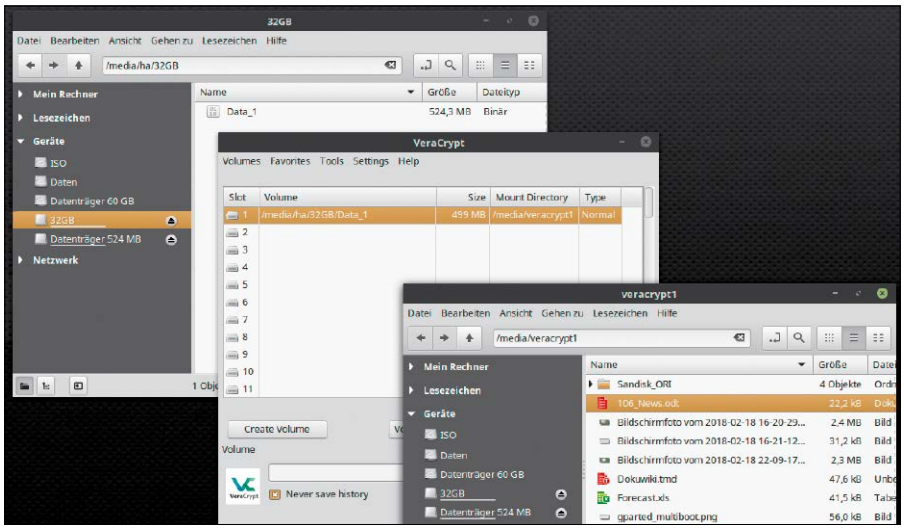
Veracrypt: Daten für Windows und Linux

Bei Luks-Verschlüsselung bleiben andere Betriebssysteme außen vor. Sollen auch Windows und Mac-OS Zugriff haben, brauchen Sie eine plattformübergreifende Lösung. Wir empfehlen die Software Veracrypt, die Sie unter Ubuntu & Co. am besten mittels

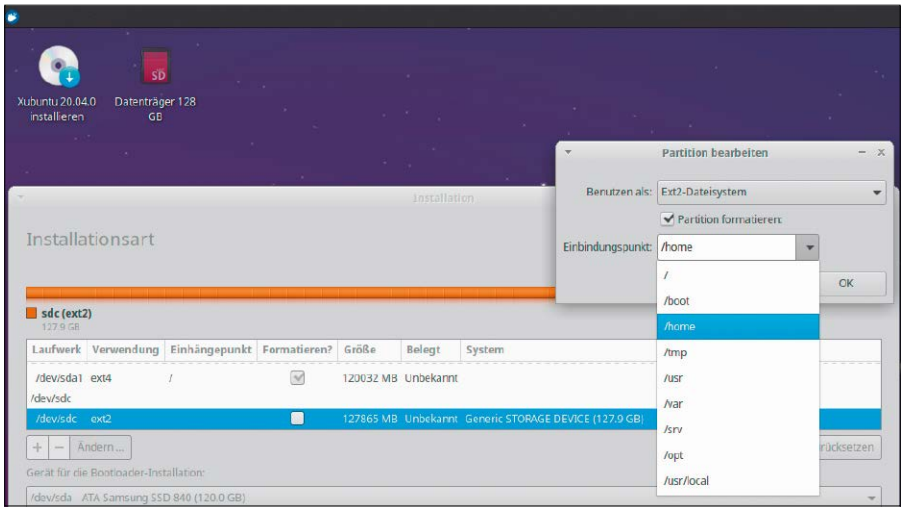
```
sudo add-apt-repository
  ppa:unit193/encryption
sudo apt-get update
sudo apt-get install veracrypt
```

aus einem PPA installieren und für Windows und Mac-OS von *https://veracrypt.fr/en/Downloads.html* herunterladen und installieren.

Vor dem Einsatz der Software sollten Sie sicherstellen, dass das USB-Laufwerk mit NTFS formatiert ist. FAT32 ist nicht geeignet, weil dort eine verschlüsselte Containerdatei nur vier GB fassen könnte. Ein Linux-Dateisystem scheidet ebenfalls aus, weil dann Windows nicht zugreifen könnte. Um eine neue Containerdatei anzulegen, klicken Sie im Hauptfenster auf „Create Vo-



Veracrypt ist erste Wahl zur Verschlüsselung von Daten, die unter Linux, Windows und Mac-OS genutzt werden. Im Bild ist ein kleiner 500-MB-Container „Data_1“ auf USB-Stick unter Linux geladen.



Mobiles Home: Eine Extrapartition auf USB oder SD (im Bild) ermöglicht ein einheitliches Home-Verzeichnis für mehrere Systeme und lässt sich bei Neuinstallationen auch direkt einbinden.

lume“, 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. Danach kommt die Passwortvergabe. Hier gibt es diverse Zusatzoptionen, die Sie im Normalfall ignorieren.

Bei den nachfolgenden „Format Options“ für das innere Dateisystem des Containers wählen Sie wie beim generellen Dateisystem für das Laufwerk erneut NTFS. Ein USB-Laufwerk, das Sie unter Linux wie Windows nutzen möchten, muss nicht nur selbst ein allgemein kompatibles Dateisystem haben, sondern auch der Veracrypt-Container muss mit einem solchen formatiert sein. Zur Schlüsselerstellung auf Basis des Passworts erwartet Veracrypt Mausbewegungen im eigenen Fenster.

Um den Container zu verwenden, gehen Sie mit „Select File“ im Hauptdialog zur Containerdatei. Ein Klick auf „Mount“ öffnet diese im Dateimanager. Linux lädt die Container standardmäßig nach „/media/veracrypt [nummer]“, Windows auf freie Laufwerkbuchstaben. Auf diesen Datenträgern arbeiten Sie wie auf einem normalen Laufwerk. „Dismount“ im Hauptdialog entlädt den Container, der damit wieder geschützt ist. 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.

Das mobile Home-Verzeichnis

Mobilität besonderer Qualität bietet ein transportables Home-Verzeichnis auf USB-Medium oder SD-Karte. Diese Option ist für Nutzer mehrerer Linux-PCs attraktiv, macht aber auch Neuinstallationen zum Spaziergang. Da das Szenario ein wenig Planung benötigt, ist es weniger verbreitet, als es das verdiente. Mindestens einmal muss bei der Linux-Installation diese Möglichkeit bedacht werden. Sobald das mobile Home aber einmal besteht, lässt es sich nachträglich auch in anderen Systemen einbinden.

Linux-Installer bieten die separate Home-Partition nicht standardmäßig an, sondern fordern dazu manuelle Partitionierung. Als Voraussetzung muss neben der internen Festplatte für das System ein USB-Laufwerk oder eine SD-Karte für das Home angeschlossen sein. Kapazitäten von 64 bis 256 GB sind dabei eher die Untergrenze.

Im Ubuntu-Installer wählen Sie im Dialog „Installationsart“ die Option „Etwas Anderes“, in Calamares (Kubuntu, Lubuntu, Manjaro) entspricht das der Option „Manuell“. Dann wählen Sie das Laufwerk, auf dem Sie das System installieren möchten – in der Regel die erste interne Festplatte „/dev/sda“ –, löschen dort alles und legen im entstandenen freien Speicherplatz neue Partitionen an. Beginnen Sie mit einer Partition vom Dateisystemtyp „EFI-System-Partition“. Dort ist nur eine Größenangabe erforderlich (100 MB genügen). Den verbleibenden Speicherplatz auf der internen Festplatte übergeben Sie mit voller Kapazität, mit dem Linux-Dateisystem Ext4 und dem Einbindungspunkt „/“ an das Betriebssystem.

Auf dem zweiten USB- oder SD-Datenträger erstellen Sie nun die Home-Partition. Der passende Einbindungspunkt „/home“ wird im Drop-down-Feld angeboten. Als Dateisystem verwenden Sie auch hier Ext4. Wenn Sie das handliche „Home“ auch unterwegs begleiten soll, können Sie statt Ext4 auch Luks-Verschlüsselung verwenden („physikalisches Volume für Verschlüsselung“).

Einfache Nutzung: Den Home-Datenträger können Sie wie jedes USB/SD-Medium an jedes andere (Linux-)System anschließen und haben damit nicht nur die persönlichen Benutzerdateien, sondern auch alle Konfigurationsdateien vorliegen. Somit las-

sen sich ausgewählte Daten (oder auch alle) in das jeweils lokale „/home“ übertragen.

Mobiles Home: Darüber hinaus ist es möglich, den Home-Datenträger als physisches Medium und als „Home“ in ein anderes Linux-System einzubinden (selbst wenn dort bisher keine externe Home-Partition eingerichtet ist). Diese Maßnahme ist am umfassendsten, wenn dieselben Benutzerkonten und ein ähnliches oder identisches System vorliegen, weil dann auch alle Desktop- und Softwareeinstellungen greifen. Liegt ein anderes Linux vor, gehen viele Konfigurationsvorgaben ins Leere, was aber keine Konflikte oder Probleme verursacht.

Ermitteln Sie zunächst mit

```
lsblk -f
```

die UUID-Kennung des USB- oder SD-Mediums. Danach tragen Sie das Laufwerk mit Mountpunkt „/home“ in die Datei „/etc/fstab“ ein:

```
UUID=[…] /home ext4 defaults 0 0
```

Die UUID haben Sie vorher ermittelt; das Dateisystem „ext4“ passen Sie bei Bedarf an, falls lsblk ein anderes Dateisystem gemeldet hatte. Danach schließen Sie alle Programme und beenden im Terminal die grafische Oberfläche, indem Sie den Displaymanager beenden. Welchen Manager (gdm3, lightdm, sddm, lxdm) das System verwendet, zeigt die Datei „/etc/X11/default-display-manager“. Für Ubuntu (Gnome) und Linux Mint (Cinnamon) wären diese Befehle einschlägig:

```
sudo service gdm3 stop
sudo service lightdm stop
```

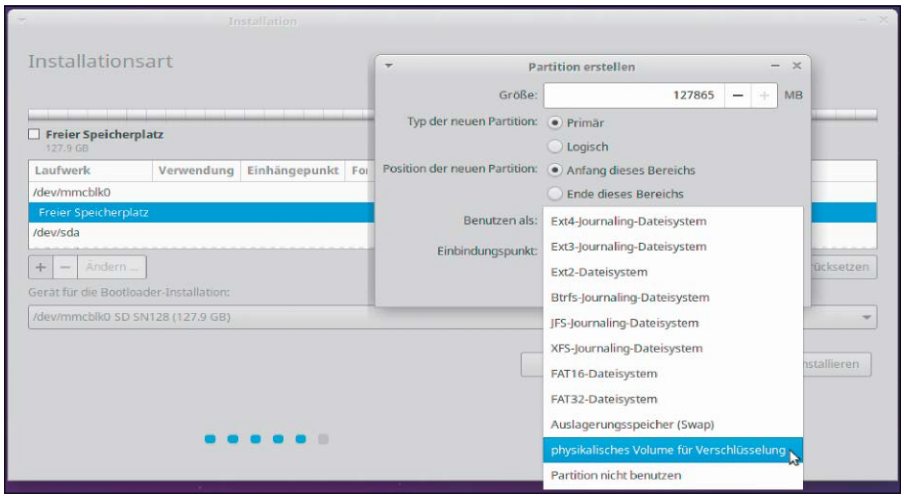
Vom „schwarzen“ Monitor kommen Sie mit Strg-Alt-F2 zur Textkonsole. Mit den nachfolgenden Kommandos benennen Sie das bisherige Home um, erstellen einen neuen Home-Ordner, mounten das externe Home-Laufwerk in diesen Mountpunkt und kopieren (bei Bedarf) alle Daten des alten „/home“ in das neue:

```
sudo mv /home /home.bak
sudo mkdir /home
sudo mount -a
sudo rsync -aXS /home.bak/ /home/
```

Nach

```
sudo reboot
```

verwendet das System den neuen Datenträger als Home. ■



Falls mobiles Home auch das Haus verlässt: Ubuntu-Installer bieten unter den Dateisystemen diese Option für Luks-verschlüsselte (Home-)Partitionen.

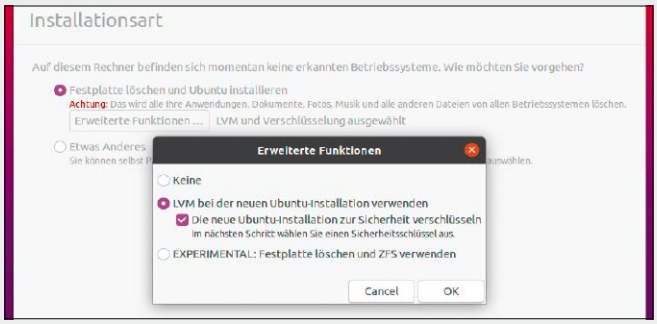
DATENSCHUTZ FÜR NOTEBOOKS

Im Fokus dieses Beitrags stehen USB-Medien. Aber auch Notebooks sind mobil, bleiben unbeaufsichtigt oder werden vergessen, und die Benutzeranmeldung bietet bekanntlich keinen Datenschutz: Es genügt, das Notebook mit einem Fremdsystem zu booten, um an alle Festplatteninhalte zu gelangen. Der beste Schutz ist eine Cryptsetup/Luks-verschlüsselte Systempartition. Das Einzige, was ein Datendieb ohne Kenntnis des Kennworts anhand der Partitionierungsfakten erkennen könnte, ist die trockene Tatsache der Luks-Verschlüsselung.

Luks-Verschlüsselung der Systempartition ist nur bei der Linux-Installation möglich – nicht mehr nachträglich. Verbreitete Linux-Installer wie Ubiquity, Calamares oder Yast bieten diese Option per einfachen Klick an. Der entscheidende Unterpunkt im Installationsprogramm lautet „Installationsart“ oder „Partitionen/Partitionieren“. Beachten Sie, dass Sie für die Luks-Verschlüsselung dem Installer die gesamte primäre Festplatte überlassen müssen. Die Festplatte sollte daher leer sein oder nur noch Daten enthalten, die Sie nicht mehr benötigen.

Für Luks-Verschlüsselung wählen Sie zunächst die Hauptoption „Festplatte löschen…“. Danach können Sie im Ubuntu-Installer das Kästchen „Die neue Installation … verschlüsseln“ wählen. In Calamares lautet der Punkt „Verschlüssele System“. Wenn Sie mit diesen Vorgaben auf „Weiter“ klicken, folgt noch die Abfrage des Kennworts. Der Rest der Installation verläuft wie gewohnt.

Wenn Sie künftig das System booten, erscheint stets die Abfrage „Please unlock disk […]“. Dort geben Sie das Kennwort ein und erst danach setzt der Systemstart fort. Die Benutzung ist transparent – abgesehen von der Kennworteingabe arbeiten Sie wie mit einem unverschlüsselten System.

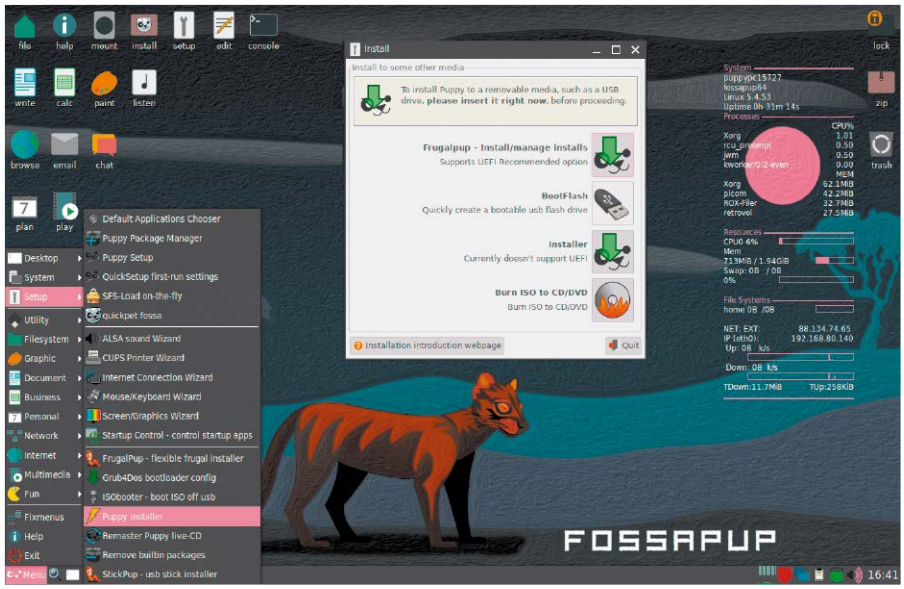


Verschlüsselung der Systempartition bei der Installation: Diese Option ist in allen Ubuntus einfach einzurichten, sofern das neue System die komplette primäre Festplatte übernehmen darf.

Mobile Linux-Livesysteme

Wer ein unabhängiges Mobilsystem zur Hand haben will, nutzt eine flotte Linux-Distribution auf USB. Das funktioniert frappierend einfach und ist in fünf Minuten erledigt. Optional und für besondere Ansprüche gibt es auch technisch aufwendigere Varianten.

VON HERMANN APFELBÖCK



Livesysteme eignen sich zum Testen von Systemen und Software, als sichere Surfsysteme fürs Banking oder für riskante Webaktionen, als Schulungssysteme, als Reparatur- und Rettungssysteme, als Sicherheitssysteme. Prinzipbedingt sind Livesysteme eingefroren und erlauben keine Änderungen – auch nicht auf beschreibbaren USB-Datenträgern. Das Dateisystem wird in den Arbeitsspeicher geladen und die in der Sitzung durchaus möglichen Änderungen gehen beim Herunterfahren wieder verloren. Je nach Einsatzzweck ist die Anpassungsfähigkeit des Livesystems auch gar nicht erforderlich. Insbesondere spezialisierte Servicesysteme wie etwa ein Gparted live oder ein Rescuezilla erledigen ihren Job ohne Notwendigkeit für Erweiterungen oder Anpassungen.

Anders steht es bei Livesystemen, die einen portablen Zweit- oder Ersatzdesktop anbieten sollen. Hier sind geänderte Desktopeinstellungen, Browseranpassungen oder Nachinstallationen hochwillkommen – und auch dies ist in vielen Livesystemen sehr einfach zu realisieren.

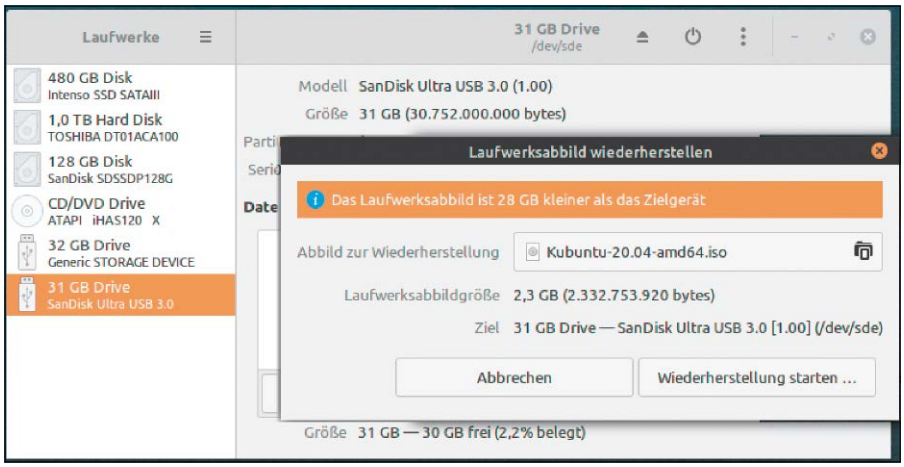
Pure eingefrorene Livesysteme

Linux live auf USB ist einfach. Technische Basis hierfür ist die Tatsache, dass heutige ISO-Abbilder nicht mehr das sind, was sie ursprünglich waren – Speicherabbilder im ISO-Format 9660 für optische CD/DVDs. Die ISO-Downloads aller namhaften Distribution enthalten eine hybride Bootumgebung: Damit können sie immer noch traditionell auf DVD gebrannt werden, sie booten aber auch von USB-Medien. Nach wie vor gibt es Ausnahmen wie etwa die Livesysteme der Puppy-Familie, aber bei allen Debian/Ubuntu- oder Arch-verwandten ISO-Downloads dürfen Sie von hybrider Bootfähigkeit ausgehen.

Daher genügt für den bootfähigen Transport auf USB-Stick eine einfache Rohkopie des ISO-Abbilds auf den Datenträger. An Kopierwerkzeugen besteht kein Mangel. Der Einfachheit halber klammern wir über- oder unterdimensionierte Kandidaten wie Rufus (Windows), Etcher (alle Systeme), dd (Linux-Terminal) aus und verweisen auf nur zwei Werkzeuge:

Linux: Jede namhafte Distribution enthält ein grafisches Laufwerkstool – entweder den KDE-Partitionmanager oder Gnome-Disks unter Gnome, Cinnamon & Co: Hier markieren Sie das gewünschte Ziellaufwerk und verwenden im KDE-Partitionmanager das Menü „Partition → Wiederherstellen“. In Gnome-Disks finden Sie über das Zahnradsymbol zur Option „Partitionsabbild wiederherstellen“. In beiden Tools erhalten Sie dann ein Navigationsfenster, um das zu kopierende ISO-Abbild auszuwählen.

Windows: Der einschlägige Rohkopierer unter Windows heißt Win 32 Disk Imager (auf Heft-DVD, Download unter *http://sourceforge.net/projects/win32diskimager*). Hier genügt es, die Quelldatei („Image File“) und das Zielgerät („Device“) anzugeben. Da das Tool standardmäßig nur IMG-Dateien anzeigt, wählen Sie als Dateifilter „*.*“, um auch ISO-Quelldateien auswählen zu können. Die Schaltfläche „Write“ startet den Kopiervorgang.



Bootfähige Kopie eines ISO-Abbilds auf USB-Stick: Am Desktop-Linux erledigen die Standardtools Gnome-Disks (im Bild) oder KDE-Partitionmanager diesen Job.

Flexible Livesysteme („Persistenz“)

Um Livesystemen in immerhin begrenztem Umfang Anpassungen und Installationen zu ermöglichen, haben spezialisierte Livedistributionen wie Knoppix, Puppy oder Porteus ihre eigenen Persistenzoptionen. „Persistenz“ bedeutet, dass Systemänderungen in einer separaten Partition oder Datei außerhalb des Read-only-Dateisystems gespeichert und beim Systemstart in das Dateisystem eingehängt werden. Dies ermöglicht – untypisch für Livesysteme – einen erstaunlich anpassungsfähigen Betrieb.

Unetbootin: Für alle Ubuntu-basierten, also für ziemlich viele Livesysteme, kann das kleine Tool Unetbootin einen Persistenzspeicher auf USB-Sticks einrichten (auf Heft-DVD, Download unter *https://unetbootin.github.io/*, für Linux, Windows und Mac-OS). Diese Persistenzoption ist eines der Hauptmotive, um Unetbootin einer Rohkopie mit dd oder dem Win 32 Disk Imager vorzuziehen.

Um ein ISO-Image bootfähig auf USB-Stick zu befördern, wählen Sie im Dialog unten die Option „Abbild“ und navigieren dann mit der Schaltfläche „…“ zur gewünschten Datei. Nach Klick auf „Öffnen“ erscheint der komplette Pfadname im Eingabefeld. Danach wählen Sie neben „Typ“ die Option „USB-Laufwerk“ und neben „Laufwerk“ geben Sie die Kennung des USB-Sticks an. Der Klick auf „OK“ startet den Kopiervorgang. Kontrollieren Sie die Laufwerkskennung des USB-Sticks genau, denn Unetbootin wird den Datenträger komplett überschreiben.

Für den flexiblen Persistenzspeicher tragen Sie im Unetbootin-Fenster neben der Option „Platz um Dateien zwischen Neustart zu erhalten“ die gewünschte MB-Angabe ein. 1000 bis 4000 MB (und mehr) sind je nach Kapazität des USB-Sticks sinnvolle bis großzügige Werte.

Maßgeschneiderte Livesysteme

Cubic (Custom Ubuntu ISO Creator) ist ein grafisches Front-End für alle Ubuntu-basierten ISO-Abbilder, das in diese Images neue Dateien einbaut und danach ein geändertes, maßgeschneidertes ISO schreibt. Damit erweitern und optimieren Sie die Standardabbilder von Ubuntu & Co. um Software und Benutzerdateien. Das Tool installieren Sie mit folgenden Terminalbefehlen:

```
sudo apt-add-repository ppa:cubic-
 wizard/release
sudo apt update
sudo apt install cubic
```

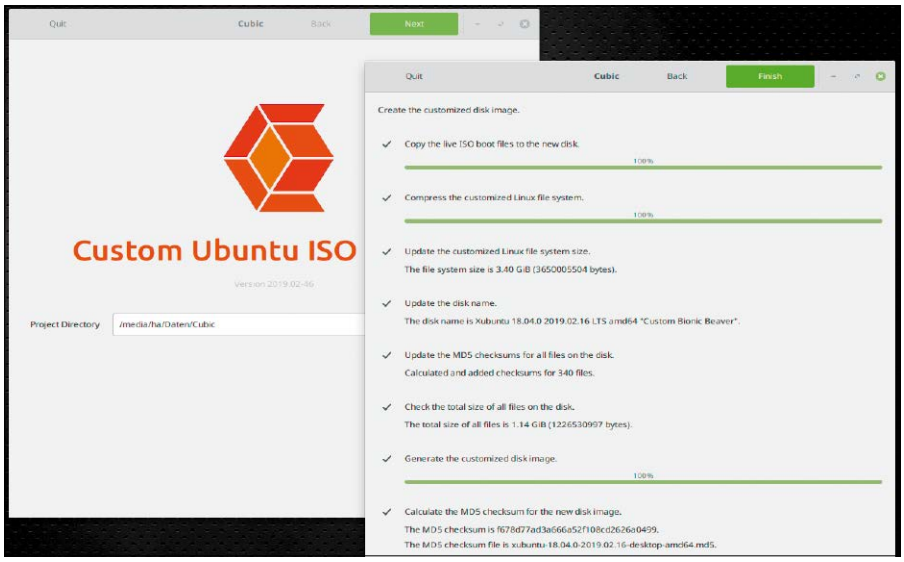
Nach dem Start geben Sie ein (beliebiges) „Project Directory“ an, wo Cubic das Livesystem zusammenbauen soll. Nach „Next“ und „Select“ wählen Sie das ISO-Image des originalen Systems. Nach weiterem „Next“ können Sie jetzt alle Anpassungen erledigen. Mit *apt install […]* rüsten Sie nach, was dem originalen Livesystem nach Ihrer Meinung fehlt. Benutzer- und Konfigurationsdateien können Sie per Drag & Drop vom laufenden System in die Cubic-Konsole ziehen und dann mit der „Copy“-Schaltfläche in das Livesystem integrieren. Gehen Sie vorher mit *cd* vorher in das gewünschte Verzeichnis – genau dort werden die Dateien später vorliegen. Um neue Ordner und Dateien richtig anzulegen, sollten Sie die Ordnerstruktur des originalen Livesystems gut kennen. Mit „Next“ verlassen Sie die chroot-Konsole, mit weiterem „Next“ die Paketübersicht. Danach wird das angepasste System zusammengebaut. Das fertige ISO schreiben Sie mit den üblichen Werkzeugen auf USB.

Cubic oder Systemback? Trotz Beschränkung auf Ubuntu & Co. ist Cubic derzeit das komfortabelste Tool, um Livesysteme maßzuschneidern. Das ehemals exzellente Tool Systemback sollte an dieser Stelle zumindest erwähnt werden: Es konnte ein installiertes Linux aus dem laufenden Betrieb in ein Livesystem umwandeln. Systemback wird immer noch angeboten, aber nicht mehr gepflegt. Im aktuellen Zustand muss es als unbrauchbar eingestuft werden.

Cubic oder Persistenz? Wer sich ein Livesystem mit dem einen oder anderen zusätzlichen Tool und etlichen Desktopanpassungen wünscht, ist mit Persistenz gut beraten. Das ist technisch die deutlich leichtere Übung. Cubic ist ein Tool für Fort-



Livesysteme durch persistenten Speicher aufwerten: Unetbootin macht mit dieser Option alle Ubuntu-basierten Livesysteme anpassungsfähig.



Mit Cubic erweitern Sie ein Ubuntu-Standard-ISO um zusätzliche Software, Konfigurations- oder Benutzerdateien und schreiben ein maßgeschneidertes Ubuntu-Livesystem.

geschrittene, nicht zuletzt mit dem Vorteil, dass ein Admin ein optimiertes Livesystem für eine ganze Mitarbeitertruppe bereitstellen kann.

Empfohlene Live-Kandidaten

Für den schnellen Ad-hoc-Einsatz müssen Sie nicht viel überlegen: Fast alle ISO-Installationsmedien aktueller Desktopsysteme bieten auch den Livebetrieb. Wer also etwa ein Kubuntu oder Linux Mint gewöhnt ist und eben mal schnell ein Livesystem benötigt, macht damit nichts falsch, zumal er die enthaltenen Tools und den Desktop kennt. Prädestiniert für häufigen Liveeinsatz sind dicke Desktopsysteme im Unterschied zu den nachfolgend genannten Spezialisten allerdings nicht.

Knoppix: Knoppix ist der Live-Klassiker schlechthin (Download unter *www.knopper.net/knoppix-mirrors*). Deutschsprachig, mit exzellenter Hardwareerkennung, opulenter Softwareausstattung und anspruchslosem LXDE-Desktop ist Knoppix erste Wahl für Zweit- oder Surfsysteme (optional mit Anonymisierer „Knoppix → TOR Proxy“). Das ISO-Abbild kann mit den üblichen Tools auf USB-Stick kopiert werden. Für häufige Nutzung empfiehlt sich die Persistenzoption, die bei Knoppix „Overlay-Partition“ heißt. Dazu müssen Sie aus einem laufenden Knoppix ein zweites erstellen. Das maßgebliche Tool „Flash Knoppix“ finden Sie unter „Knoppix → Knoppix auf Flash kopieren“. Nach Auswahl des Zieldatenträgers folgt die „Installation auf FAT32 mit zusätzlicher Overlay-Partition“.

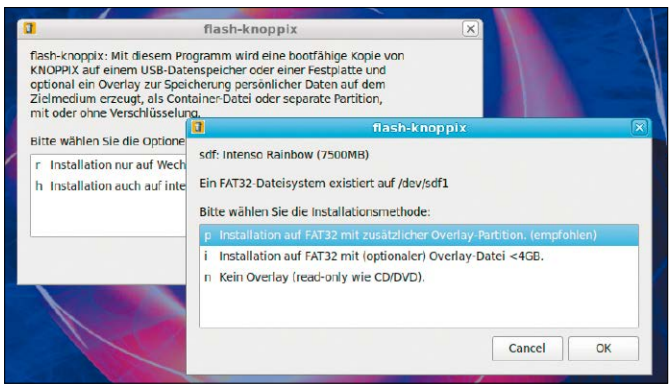
Puppy: Alle Varianten der Puppy-Familie sind spezialisierte Livesysteme (überwiegend englischsprachig), die auf kleinen ISO-Abbildern kaum glaubliche Softwaresammlungen unterbringen. Zur Live-Spezialisierung gehört ein eigenes Konzept für persistenten Speicher. Die zahlreichen Puppys erhalten Sie unter *http://distro.ibiblio.org/puppylinux/*. Wir empfehlen das ansehnliche „puppy-fossa“, also das jüngste Ubuntu-basierte Puppy. Puppys sind leider nicht hybrid, booten also nur von CD/DVD.

Um ein Puppy auf USB-Stick einzurichten, ist der Umweg über eine CD unerlässlich (etwa mit Brasero unter Linux). Booten Sie einen Rechner mit dieser CD. Das Puppy-System wird am Desktop den Dialog „Quick Setup“ anzeigen, den Sie ignorieren können. Stecken Sie den USB-Stick ein, der das Puppy Linux aufnehmen soll, und klicken Sie am Desktop auf „Install“ (identisch mit „Setup → Puppy Installer“ im Menü). Im Tool wählen Sie dann die Option „Boot Flash“, danach den USB-Stick und im nächsten Dialog GPT- oder MBR-Boot. Da aktuell noch fast alle Rechner beide Partitionsmodi booten, ist die Wahl nicht kritisch. Nach abgeschlossener Aktion „copying files“ brauchen Sie das temporäre System auf CD nicht mehr und booten das Puppy-System vom USB-Stick.

Das neue Puppy auf USB begrüßt Sie wieder mit „Quick Setup“. Hier lohnt es sich nun, alles sorgfältig einzustellen, Anpassungen vorzunehmen und über den Desktoplink „Install → Install Applications“ oder das Tool „Quickpet“ Software nachzuinstallieren. Sobald Sie ein angepasstes Puppy-System zum ersten Mal herunterfahren, erscheint „First shutdown. Save session...“. Das bedeutet, dass die Änderungen im Livesystem dauerhaft gespeichert werden können. Nach „Save“, optionaler Verschlüsselung und „Save in a folder“ legt das System den Speicherbereich an und fährt herunter.

MX Linux: MX Linux ist ein attraktives, aber genügsames System mit XFCE-Desktop (*https://mxlinux.org*). MX Linux versteht sich als Desktopsystem, ist aber auch für den Liveeinsatz optimiert: Das Livesystem zeigt im Bootmenü den Punkt „Persist“, der mit F5 ausgeklappt wird. Von den angezeigten Optionen ist „persist_all“ am einfachsten. Damit ist ein flexibles MX Linux im Livebetrieb möglich.

Noch besser: Im Hauptmenü finden Sie unter „MX-Tools“ die Programme „MX Schnappschuss“ und „MX Live USB Erzeugung“. Der „Schnappschuss“ schreibt das laufende System in eine ISO-Datei, das dann mit „MX Live USB Erzeugung“ auf USB-Stick übertragen wird. Wer auf diesem Weg ein optimal ausgestattetes Livesystem einrichten will, braucht aber zunächst als Quelle ein ordentlich installiertes MX Linux. ■



Knoppix mit eigener Persistenzoption: Die zurecht empfohlene Overlaypartition ermöglicht dem Livesystem Installationen und Desktopanpassungen.

Der Multiboot-Stick

USB-Sticks fassen 32, 64, 128 Gigabyte und mehr, USB-Festplatten mehrere Terabyte. Für ein einziges Livesystem ohne Größenwachstum wäre das pure Platzverschwendung. Es bietet sich an, solche Medien mit einem ganzen Werkzeugkasten zu füllen.

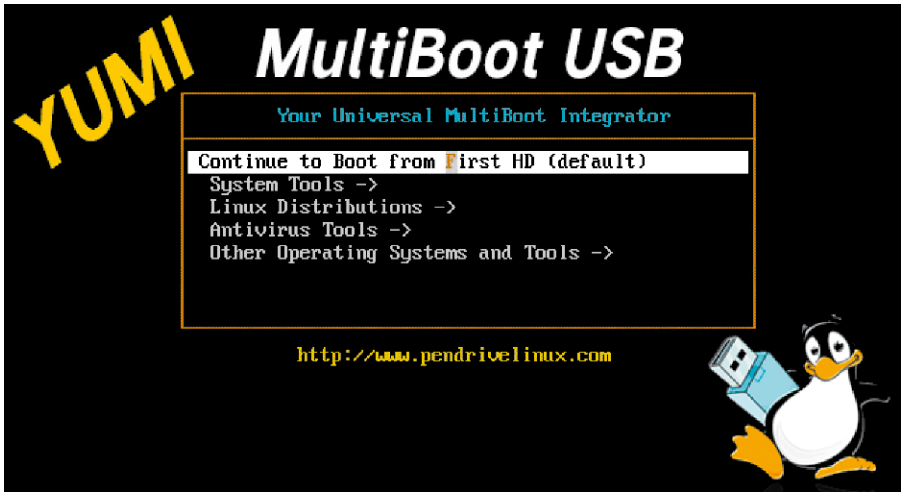
VON HERMANN APFELBÖCK

Die in den vorangegangenen Beiträgen genannten Tools wie Unetbootin oder Win 32 Disk Imager befördern genau ein Systemabbild bootfähig auf den USB-Datenträger. Auf große USB-Datenträger passt natürlich wesentlich mehr, zum Beispiel ein Installationsarchiv der wichtigsten Linux-Distributionen oder eine Sammlung von Reparatur- und Zweitsystemen. Es gibt einschlägige Tools unter Linux wie Windows, um solche Multiboot-Sammlungen bequem zusammenzubauen. Wir erklären den Einsatz der Tools Multibootusb (unter Linux) und Yumi (unter Windows) und empfehlen Livesysteme, die für solche Multiboot-Sticks prädestiniert sind.

Multibootusb und Yumi arrangieren im Handumdrehen eine stattliche mobile Sammlung von Distributionen für Reparatur, Zweitdesktop oder Installationen. Ein so erstellter Multiboot-Stick enthält allerdings ausschließlich Linux-Livesysteme. Multibootusb ebenso wie Yumi können aber immerhin für Ubuntu-basierte Systeme persistenten Speicher einrichten, was bei ausreichender Kapazität stets zu empfehlen ist.

Persistenz macht Livesysteme deutlich flexibler, Livesysteme bleiben sie aber dennoch. Ideale Systemkandidaten für Multiboot-Sticks sind daher nicht unbedingt Desktopsysteme, sondern Reparatur-, Analysesysteme und Virenscanner sowie diverse monofunktionale Spezialisten wie Partitionierer oder Boothelfer.

Hinweis: Beachten Sie in diesen Zusammenhang auch den Beitrag ab Seite 6. Dort geht es um die LinuxWelt-DVD. Auch der komplette System- und Toolbestand der Heft-DVD lässt sich bootfähig auf USB-Sticks übertragen.



Multibootusb: Livesystem-Sammlung auf USB

Wer eine Sammlung an Livesystemen unterbringen will, hat unter Linux die Wahl zwischen Multisystem und Multibootusb. Aufgrund der einfacheren Bedienung empfehlen wir Multibootusb. Eventuell finden Sie das Tool in den offiziellen Paketquellen Ihrer Distribution, und dann ist es mit dem Paketnamen „python3-multibootusb“ leicht zu installieren (etwa unter Debian, Ubuntu & Co.):

```
sudo apt install python3-
  multibootusb
```

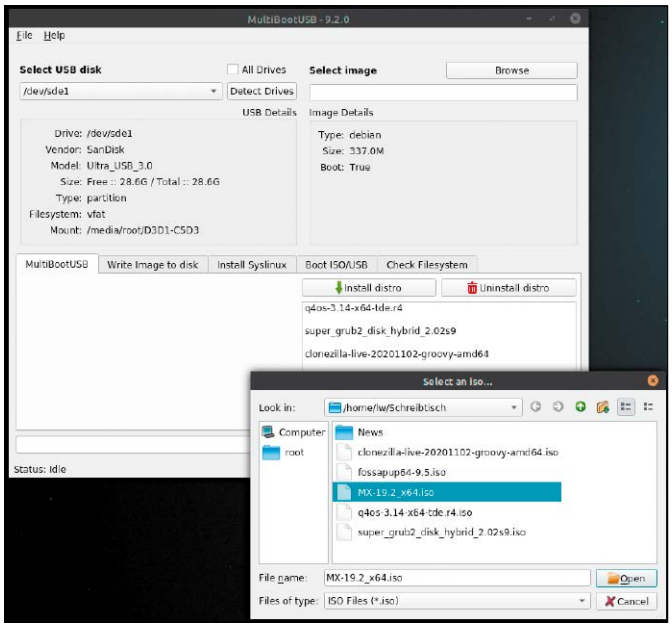
Ist dies nicht der Fall, gibt es das Python-Tool als fertiges RPM- und DEB-Paket sowie auch als EXE für Windows unter *https://github.com/mbusb/multibootusb/releases*. Einschlägig für Debian/Ubuntu ist das DEB-Paket „python3-multibootusb_9.2.0-1_all.deb“, das nach dem Download und Doppelklick schnell installiert ist. Danach erscheint es im Hauptmenü oder ist mit

```
sudo multibootusb
```

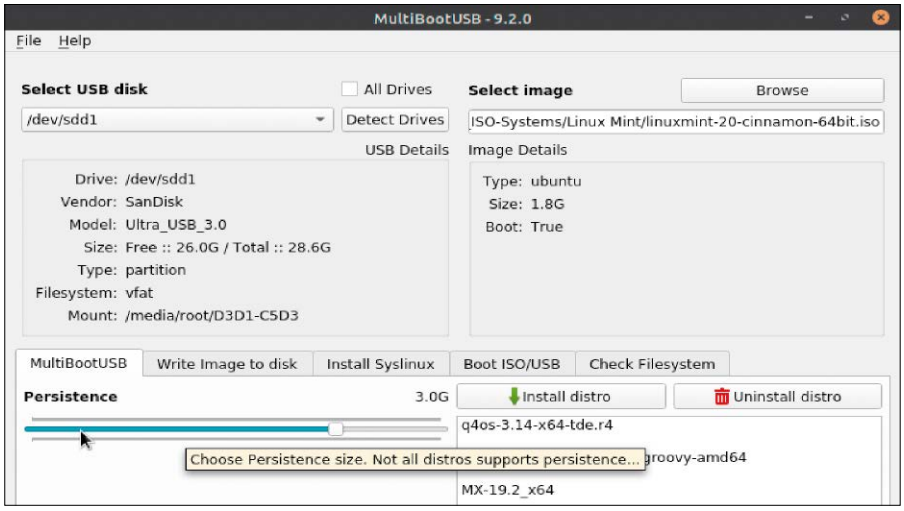
startklar. Die Oberfläche ist gewöhnungsbedürftig, zumal der wesentliche Arbeitsmodus mit den Registerkarten in der unteren Hälfte zu steuern ist. Standardmäßig ist aber der für unseren Zweck einschlägige Modus „MultiBootUSB“ voreingestellt.

Den vorher eingelegten Stick, der FAT32-formatiert sein sollte, stellen Sie dann oben mit „Select USB disk“ ein, wobei Sie die Partition /dev/sdx1“ wählen, nicht das Gerät „/dev/sdx“. Mit „Select image“ und „Browse“ geht es dann zum ersten ISO-Image, das dann mit „Install distro“ (Fenster unten rechts) auf das Laufwerk geschrieben wird. Bei allen Debian/Ubuntu-Systemen erscheint zusätzlich im Fenster links ein Schieberegler für einen persistenten Speicherbereich. Wo immer das angeboten wird, sollten Sie das annehmen, um das Livesystem anpassungsfähig zu machen.

Die Fortschrittsanzeige hatte früher die Macke, schnell auf 80, 90 oder 99 Prozent zu wachsen, dann aber lange zu stagnieren. Dies ist inzwischen so ins Gegenteil verschlimmbessert, dass relativ lange gar nichts passiert. Das ist aber nur ein Schönheitsfehler: Warten Sie einfach ab, bis das Tool die finale Bestätigung zeigt.



Auswahl des nächsten ISO-Abbilds in Multibootusb: Trotz eigenwilliger Oberfläche ist die Zusammenstellung von bootfähigen Livesystemen ganz einfach.



Achten Sie auf den Persistenzregler: Die Option wird bei allen Ubuntu-Desktops angeboten und ist immer zu empfehlen. Für ein paar Anpassungen müssen es aber keine Gigabyte sein.

Auf diese Weise befüllen Sie das USB-Medium, während Multibootusb alle vorhandenen Systeme in seiner Liste rechts unten anzeigt. Diese Liste dient auch der späteren Übersicht und erlaubt mit „Uninstall distro" nachträgliches Löschen eines Livesystems. Das spätere Bootmenü des USB-Sticks zeigt alle Livesysteme ohne Kategorisierung in der Reihenfolge der Einrichtung.

Yumi unter Windows

Wer es sich aussuchen kann, ob er seinen Multiboots-Stick unter Linux oder Windows einrichten will, fährt mit Yumi unter Windows fast komfortabler. Einziges Ärgernis ist, dass auf der Seite *www.pendrivelinux.com/yumi-multiboot-usb-creator* überall übergroße Download-Schaltflächen blinken, die aber nicht das kleine Tool herunterladen. Man muss sich – dies ignorierend – ein Stück nach unten arbeiten, bis man unter „YUMI Legacy" und „YUMI UEFI+BIOS" auf die gesuchten Schaltflächen „Download YUMI" trifft. Wenn die Firmware der Rechner, auf denen später der Multibootstick starten soll, den Bios-Modus noch unterstützt, nehmen Sie „YUMI Legacy". In der Regel ist dies vertretbar, weil Uefi-Firmware meistens via Compatibility Support Module (CSM) auch den älteren Bios/MBR-Boot bietet. Yumi Legacy – aktuell Version 2.0.9.3 – ist flexibler, insofern es die Livesysteme auf FAT32- und NTFS-Datenträger kopieren kann. Yumi-Uefi – aktuell Version 0.0.4.3 – benötigt zwingend FAT32, was dann sehr große Livesysteme wie Knoppix ausschließt (Vier-GB-Limit).

Schließen Sie das USB-Medium immer vorher an, bevor Sie Yumi starten. Das Tool hat keine Refresh-Funktion, um USB-Laufwerke nachträglich einzulesen. Ansonsten ist Yumi („Your USB Multiboot Installer") zwar englischsprachig, aber unschlagbar einfach in der Benutzung – quasi ein Unetbootin mit Wiederholschleife. Yumi benötigt unter Windows keine Installation – einfach die ausführbare Datei starten. Die wenigen Schritte sind ähnlich wie bei Unetbootin:

Sie wählen in „Step 1" das gewünschte Zielaufwerk, in „Step 2" die Distribution und im letzten Schritt „Step 3" das ISO-Image der gewünschten Linux-Distribution. Bei der Auswahl der ISO-Datei zeigt Yumi nur Dateiobjekte an, die zum Distributionsnamen passen, den Sie vorher in „Step 2" gewählt haben. Daher ist es in der Regel zu empfehlen, die unscheinbare Option „Show all ISOs" zu aktivieren, um diesen Filter zu umgehen. Bei allen Ubuntu-basierten Systemen erscheint nach „Step 3" ein zusätzlicher „Step 4", mit dem Sie dem System einen persistenten Speicher und damit Anpassungsfähigkeit spendieren können. Yumi gibt für die Persistenz ein Maximum von etwa vier GB vor (pro System).

Nach absolvierter Kopie fragt Yumi jedes Mal automatisch nach: „Would you like to add more ISOs...". Mit „Ja" oder „Yes" können Sie dann nach demselben Strickmuster weitere Systeme aufnehmen, solange der Platz des Datenträgers reicht.

Beim späteren Booten des Datenträgers erscheint das Yumi-Bootmenü: Es bietet an oberster Stelle das Booten von der Festplatte an sowie unter „Linux Distributions" die eingerichteten Desktop-Livesysteme auf USB. Das Yumi-Bootmenü hat mit „System Tools", „Other OS" und „Unlisted ISOs" noch weitere Kategorien. Es wird mitunter zum Suchspiel, wo das gewünschte Livesystem eingeordnet ist, aber die Sortierung ist durchaus logisch.

Yumi kann auf einem Multiboot-Stick auch nachträglich Systeme hinzufügen oder wieder entfernen. Beim Erweitern gehen Sie einfach so vor wie oben beschrieben. Sie erhalten dabei keinen Hinweis auf die bereits vorhandenen Systeme, aber diese bleiben unangetastet. Für das Löschen aktivieren Sie rechts oben die unscheinbare Option „View or Remove Installed Distros".

Diese Option ist auch nützlich, um sich einen Überblick über die bereits bestehenden Systeme zu verschaffen.

Kandidaten für Live-Multiboot

Die Tatsache, dass ein USB-Stick Platz für 50 Livesysteme bietet, sollte Sie nicht dazu verleiten, dies planlos auszunutzen. Es ist nicht sinnvoll, Distributionen anzusammeln, die sich zu 50, 80 oder hundert Prozent funktional überschneiden. Was Sie wirklich benötigen, müssen Sie selbst entscheiden, aber die folgenden Vorschläge zeigen ein plausibles Arrangement für einen nützlichen Werkzeugkasten.

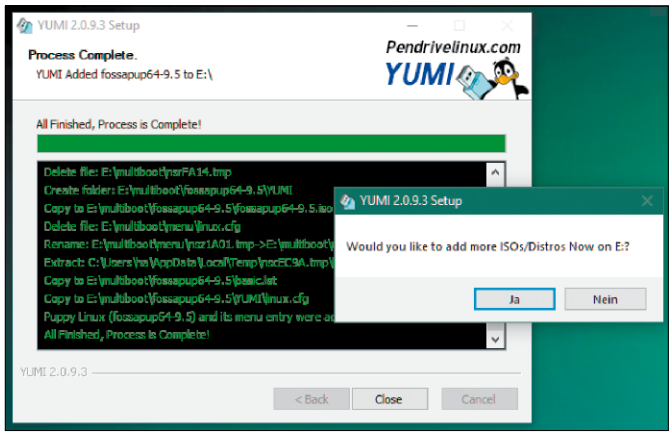
• **Ein Desktopsystem,** nämlich das Ihnen bestvertraute, sollten Sie grundsätzlich mitnehmen. Optimalerweise ist es mit großzügiger Persistenz eingerichtet, danach angepasst und deutsch lokalisiert, sodass es als Livesystem Ihren Desktop-Gewohnheiten möglichst nahekommt.

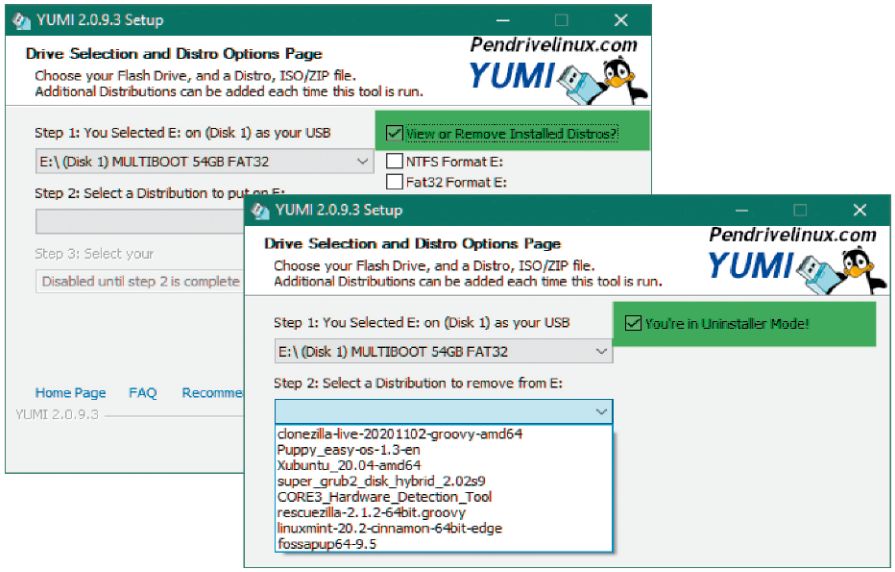
• **Ein zusätzliches Surfsystem** ist neben einem Desktopsystem nur notwendig, wenn gewisse Sonderansprüche bestehen: Slax (*www.slax.org*) ist besonders klein und schnell und bietet nur Browser, Terminal, Dateimanager und VLC. Tails (*https://tails.boum.org*) pflegt einen Sonderstatus als Livesystem mit anonymisierendem TOR-Browser. Peppermint-OS (*http://peppermintos.com*) tendiert Richtung Allzwecksystem, hat aber seinen Fokus auf Web und Cloud.

• **Knoppix,** das Allzweck-Livesystem, ist eigentlich immer eine Empfehlung, da es fast alles enthält, was auch speziellere Reparatursysteme mitbringen (*www.knopper.net/knoppix-mirrors*). Die große DVD-Variante bringen Sie allerdings nicht auf einem FAT32-Stick unter (Vier-GB-Limit). Knoppix ist auf einer Multiboot-Sammlung somit nur mit „Yumi Legacy" auf einem NTFS-Stick zu realisieren. Die kleine CD-Variante von Knoppix bringen Sie überall unter.

• **Super Grub2 Disk:** Der winzige Spezialist ist ein unentbehrlicher Kandidat für den Multibootstick (*https://sourceforge.net/projects/supergrub2/files/latest/download*). Er durchsucht mit der Option „Detect and show boot methods" alle Datenträger des Rechners nach Betriebssystemen und startet dann das ausgewählte System. Der Nothelfer ist unentbehrlich, wenn der Bootloader nach einer Windows-Installation oder einer fehlerhaften Linux-Installation fehlt oder defekt ist. Das Tool repariert aber nicht. Die Grub-Reparatur muss mit

Das nächste für Yumi: Das Tool leistet unter Windows ähnliche Arbeit wie Multibootusb, ist aber noch einfacher zu bedienen.





Yumi im Uninstaller-Modus: Die unscheinbare Option „View or Remove..." wechselt den Modus. Jetzt zeigt Yumi die bereits vorhandenen Systeme und bietet die Deinstallation.

```
sudo grub-install --recheck /dev/
  sd[a]
sudo update-grub
```

im laufenden System erfolgen.

• **Rescuezilla (Clonezilla):** Rescuezilla und Clonezilla erledigen das Backup und Restore kompletter Datenträger oder Partitionen (*https://rescuezilla.com/*, *http://clonezilla.org/*). Clonezilla beherrscht neben verbreiteten Linux- und Windows-Dateisystemen auch BTRFS, Reiser, HFS+, exFAT und spricht alle Netzprotokolle (Samba, SSH, NFS, Webdav). Rescuezilla beschränkt sich auf Ext2, Ext3, Ext4, NTFS und FAT und für Kopien im Netz auf Samba. Für typische Endanwender ist dies keine Einschränkung und Rescuezilla mit grafischer Bedienung die bessere Wahl.

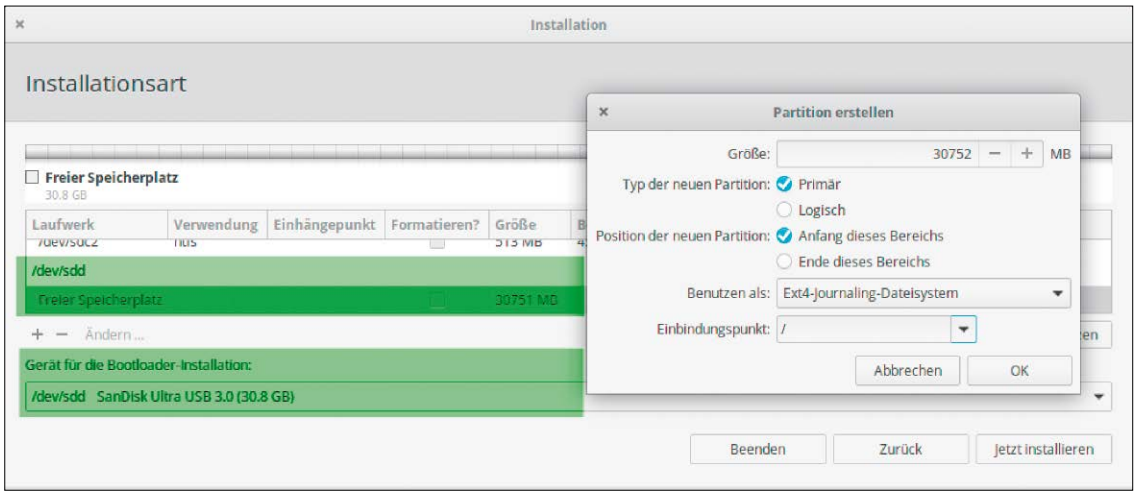
• **Gparted Live:** Das anspruchslose Livesystem der Gparted-Entwickler (*https://gparted.org*) sorgt für den Partitionierer Gparted auf einem unabhängig gestarteten Zweitsystem. Dies ist oft wichtig, um die Systempartition von außen zu verkleinern. Gparted ist zwar auf vielen Livesystemen vertreten, aber bei Gparted Live müssen Sie nicht raten. Außerdem ist dort Gparted brandaktuell.

• **Antivirenscanner für Windows:** Unabhängige AV-Scanner auf Basis eines Linuxsystems sind sauber und zuverlässiger als jeder Virenscan auf einem eventuell bereits kompromittierten Windows. Daher gibt es von allen namhaften AV-Firmen wie Avira, Bitdefender, Kaspersky solche Livesysteme. Typisches Suchmuster für die Downloadseiten ist (Beispiel) „kaspersky rescue".

• **PC-WELT-Notfallsystem:** Auch diese Empfehlung richtet sich an Windows-Nutzer, denn dieses Reparatursystem (*www.pcwelt.de/1168242*) enthält zwar auch allgemeine Linux-Prominenz wie Gparted und Clonezilla, ist aber auf Windows-Reparaturen spezialisiert. ■

Installationen auf USB

Linux auf USB-Stick ist nicht auf den Livebetrieb beschränkt. Ein regulär auf USB oder auch auf SD-Karte installiertes Linux ist mobil, sicher und genauso ausbaufähig und anpassungsfähig wie eine Installation auf Festplatte.



Ubuntu-Installation auf USB: Hier wird gerade die Systempartition eingerichtet („/dev/sdd1“). Der Bootloader muss natürlich ebenfalls auf den USB-Datenträger („/dev/sdd“).

VON HERMANN APFELBÖCK

Trotz erstaunlicher Anpassungsfähigkeit durch Persistenz haben Livesysteme ihre Grenzen. Linux live sollten Sie immer als funktionale Lösung verstehen, die Sie unkompliziert zur benötigten Software bringt: Reparaturprogramme, AV-Scanner, Partitionierer oder Browser. Ein gepflegtes Zweitsystem mit persönlichen Benutzerdaten sollte ein Livesystem trotz Persistenz schon deshalb nicht werden, weil es keine Sicherheit bietet. Wem der Stick in die Hände fällt, darf als Live-User alles (Livesysteme wie Knoppix und Puppy mit verschlüsseltem Persistenzspeicher sind rar). Aber mehr noch: Livesysteme ohne Persistenz veralten ganz schnell, und auch mit Persistenz stößt die Aktualisierungsfähigkeit irgendwann an Kapazitätsgrenzen oder an technische Grenzen.

Im Bild gesprochen: Linux live sorgt für den mobilen Werkzeugkasten und Pannendienst. Ein Wohnmobil mit Büro und Unterhaltung, das Sie jahrelang pflegen und erweitern können, erhalten Sie nur mit einer regulären Linux-Installation auf USB.

Installationen auf USB

Wer ein Desktopsystem auf USB-Stick installieren will, sollte ein Medium mit mindestens 32 GB, besser 64 GB und mehr verwenden. Ein ordentlich installiertes Linux benötigt wesentlich mehr Platz als ein Livesystem und braucht für nachhaltige Aktualisierung ordentlich Puffer. Außerdem kommen im Betrieb Konfigurationsdaten und Benutzerdaten hinzu. Große Sticks sind in der Regel auch schneller. Zu empfehlen (auch für Livesysteme) sind schnelle Sticks vom Typ USB 3.2 Gen1, die erstaunlicherweise selbst mit älterem USB 2.0 spürbar schneller lesen und schreiben.

Bei der Wahl der Linux-Distribution gibt es, ungeachtet der späteren Empfehlungen, keinerlei prinzipiellen Beschränkungen. Für die Installation benötigen Sie wie immer erst einmal das laufende Livesystem mit dem Installer. Der Linux-Installer wird stets die erste interne Festplatte „/dev/sda“ als Ziel vorschlagen. Für eine Installation auf ein USB-Gerät müssen Sie daher manuell die richtige Zielpartition festlegen. Im Ubuntu-Installer Ubiquity wählen Sie dazu im Fenster „Installationsart“ die Option „Etwas Anderes“. Bei anderen Installationsprogrammen wie Calamares lautet der einschlägige Punkt „Manuell“ oder ähnlich. Das Laufwerk muss neu partitioniert und formatiert werden, wobei alle darauf befindlichen Daten verloren gehen. Klicken Sie zunächst auf die „-“-Schaltfläche, um vorhandene Partitionen zu entfernen. Eventuell müssen Sie eine neue Partitionstabelle erstellen, um das Laufwerk löschen zu können. Danach erstellen Sie auf „Freier 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 unbedingt dasselbe USB-Laufwerk aus, auf dem Sie installieren – etwa „/dev/sdb“. Es ist entscheidend, auch den Bootloader auf das USB-Laufwerk zu schreiben, andernfalls startet das System nur auf dem Rechner, mit dem Sie installiert haben.

Verschlüsselung? Wenn Sie voraussichtlich mit dem USB-Laufwerk viel unterwegs sind, gilt dasselbe, was wir ab Seite 74 für Datensticks und Notebooks empfehlen: Das Laufwerk sollte verschlüsselt werden. Für diesen Fall wählen Sie in der Liste der Datei-

systeme nicht Ext4, sondern verwenden den Eintrag „physikalisches Volume für Verschlüsselung“. Dieser Eintrag ist gleichlautend bei den beiden verbreiteten Desktopinstallern Ubiquity und Calamares und meint die Datenträgerverschlüsselung mit Luks/Cryptsetup. Nach zweifacher Eingabe des Kennworts verläuft der Rest der Installation wie gewohnt.

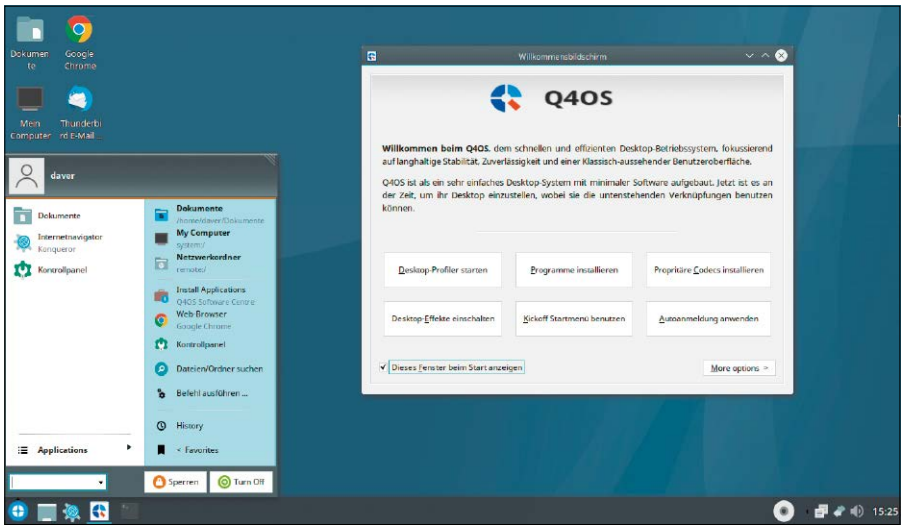
Keine Treiber: Für ein Linux-System auf USB gibt es nur eine nennenswerte Einschränkung: Sie sollten keine keine proprietären Treiber installieren, wenn die Distribution auf unterschiedlicher Hardware funktionieren soll.

Kandidaten für den Mobilbetrieb

Wer mit USB 3.0 rechnen kann und beim USB-Stick nicht knausert, wird selbst mit großen Desktopdistributionen wie Ubuntu (Gnome), Kubuntu (KDE) oder Linux Mint (Cinnamon) keine lästigen Bremsen erleben. Wenn aber ein mobiles Linux auch auf älterer Hardware flüssig laufen muss, sollte man seine Ansprüche relativieren. Die nachfolgenden Empfehlungen sind anspruchslos genug, um auf jedem USB-Stick schnell zu starten und flüssig zu arbeiten. Auf USB 3.0 und schnellen Sticks ist praktisch kein Unterschied zu einer Festplatteninstallation spürbar. Diese Systeme laufen aber auch mit USB 2.0 noch flott.

Q4-OS ist mit Debian-Unterbau und Trinity-Desktop schnell und anspruchslos (Download unter *http://q4os.org*, auf Trinity-Variante achten!). Das System startet auf USB-3.0-Stick in 13 Sekunden und belegt nach der Anmeldung für System und Desktop nur etwa 350 MB RAM. Der Desktop Trinity basiert auf KDE 3. Diese längst eingestellte KDE-Version wirkt etwas retro, ist aber KDE-typisch anpassungsfähig. Die Arbeitsfläche ist eine klassische Dateiablage, das Menü im Stil alter Windows-Versionen und die Systemleiste („Kontrollleiste“) enthält mit Schnellstarter, Fensterliste und Indikatoren die typischen Elemente.

Die Installation erledigt hier der Debian-Installer, wobei unter „Festplatten partitionieren“ der Eintrag „Manuell“ und danach als Ziel die richtige Kennung des USB-Sticks „/dev/sd[n]“ gewählt werden muss. Wichtig für USB: Auch der Debian-Installer bietet Luks-Verschlüsselung, die hier als „gesamte Festplatte mit verschlüsseltem LVM“ angeboten wird. Nach der Installation muss die deutsche Lokalisierung nachgeholt werden,



Leichte Last für USB-Sticks: Q4-OS mit Trinity-Desktop und Debian-Unterbau ist klassisch, anpassungsfähig und schlanker als jede Ubuntu-Variante.



MX Linux: Die Debian-Basis, ein sehr hübscher XFCE-Desktop und eine Vielzahl von Desktop- und Systemtools sind die Kennzeichen dieses Leichtgewichts.

was das System selbst anbietet. Danach startet der „Desktop-Profiler“, um die zunächst schmale Softwareausstattung zu komplettieren.

MX Linux: Diese Distribution (Download unter *https://mxlinux.org*) nutzt auf Debian-Basis den klassischen XFCE-Desktop. Der MX-eigene Installer ist relativ funktionsarm, hat aber die wichtige Luks-Systemverschlüsselung komfortabel integriert. Der XFCE-Desktop zeigt sich ab Installation von der feinsten Seite und die MX-eigenen System- und Einstellungstools fördern darüber hinaus die Anpassung zu einem individuellen Desktop. Die Softwareausstattung ist opulent, zum Teil redundant. MX Linux ist ein Semi-Rolling-Release, das nicht nur Sicherheitsupdates einspielt, sondern zwischendurch auch die Softwareversionen auffrischt. Solange dies funktioniert, müssen Sie MX Linux niemals neu installieren.

Xubuntu: Wer sich auf keine Experimente einlassen will, greift zu einem kleineren Ubuntu wie Xubuntu (XFCE) oder Lubuntu (LXQT). Diese Ubuntus stellen keine Anforderung an die Hardware. Nach unserer Einschätzung ist Xubuntu der beste Kompromiss, Desktopkomfort mit relativ geringen Ressourcenansprüchen zu kombinieren. Installation, Konfiguration und Personalisierung sind überall ausgereift, durchdacht und umfassend. Wie bei allen Ubuntus ist im Installer auch die Luks-Datenträgerverschlüsselung vorgesehen. ■

Mobil-Tipps und Szenarien

Ob live oder installiert: Für den ansprechenden Linux-Einsatz auf USB ist erst einmal die Leistung der Hardware verantwortlich, also des USB-Laufwerks und der USB-Schnittstelle. Und eventuell sind erst einmal Bootprobleme auszuräumen.

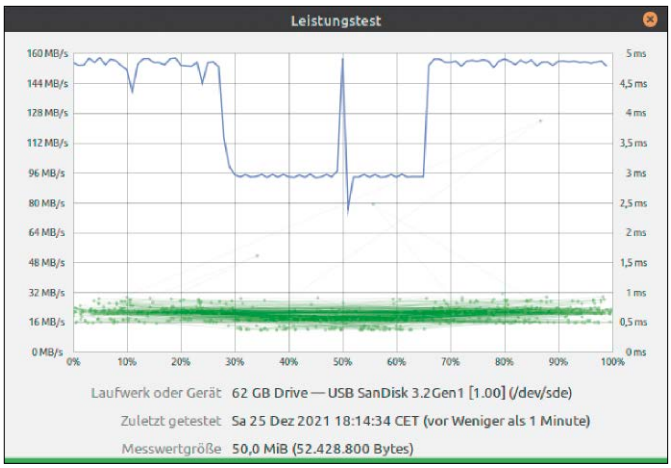
VON HERMANN APFELBÖCK

Dieser Beitrag nennt typische Problemzonen beim Einsatz von Linux-Systemen auf USB-Datenträgern. Außerdem ergänzen wir die bisher genannten Szenarien um einige knappe Vorschläge, die zeigen sollen, dass es bei „Linux für den USB-Stick" keine Denkverbote gibt.

Schnelle USB-Sticks

Wenn die Leistung von Livesystemen oder installiertem Linux auf USB-Sticks enttäuscht, liegt das nicht am Prinzip, sondern am USB-Stick oder an der USB-Schnittstelle. Von einem Medium, das keine 20 MB pro Sekunde lesen kann, können Sie keinen überragenden Mobilbetrieb erwarten. Ein solcher USB-Stick ist dann eher ein Kandidat für den einfachen Datentransport. Wer etliche Sticks vor sich liegen hat und wissen will, welcher sich am besten für den Systembetrieb eignet, sollte das Tool Gnome-Disks zu Rate ziehen (und unter KDE bei Bedarf nachinstallieren). Die Option lautet „Leistungstest für Laufwerk". Eine hier gemessene mittlere Lesegeschwindigkeit von 50 bis 100 MB/s ist geeignet und befriedigend, was darüber liegt, umso besser.

Grundsätzlich gilt bei USB-Sticks, dass die Größe zugleich ein Geschwindigkeitsindikator ist: Sticks mit großer Speicherkapazität sind schneller als kleine. Wer auf Geschwindigkeit Wert legt, sollte nicht unter 64 GB beginnen. Ideale Kandidaten mit 64, 128 GB und mehr sind aktuell folgende Produkte: Sandisk Extreme, Transcend Jetflash, Corsair Voyager, Kingston HyperX Savage. Für Sticks dieser Größe und Leistung muss man 40 Euro aufwärts investieren.



Schnelle USB-Sticks bevorzugt: Auf dem hier getesteten Stick (Tool: Gnome-Disks) wird mobiles Linux später alle Leistungserwartungen erfüllen.

Der „saubere" USB-Stick

Bereits genutzte USB-Datenträger enthalten mitunter mit Altlasten (Partitionstabelle, Partitionierung), die eine Säuberung für neue Livesysteme oder Installationen erschweren. Dann sind Laufwerkstools eventuell nicht in der Lage, Partitionen zu löschen, oder Werkzeuge wie Unetbootin oder Multibootusb kopieren erst munter los und scheitern später beim Bootvorgang. Verwenden Sie am besten einen mit FAT32 oder NTFS formatierten Stick, der vorher unter Linux oder Windows komplett gesäubert wurde. Am sichersten gewährleistet dies das Schreiben einer neuen Partitionstabelle. Unter Linux verwenden Sie dafür das Tool Gparted („Gerät → Partitionstabelle erstellen" und hier den Typ „msdos"), den Partitionmanager von KDE („Gerät → Neue Partitionstabelle") oder Gnome-Disks („Laufwerk formatieren" und „Kompatibel mit allen Systemen").

Unter Windows kommt es häufiger vor, dass die grafische Datenträgerverwaltung (diskmgmt.msc) Linux-Partitionen – insbesondere mit LVM und Luks-Verschlüsselung – nicht bearbeiten will. Was dann unter Windows aber praktisch immer hilft, ist eine Eingabeaufforderung mit Administratorrecht und dem Tool diskpart.

Mit

```
diskpart
list disk
select disk x
clean
```

ist der Datenträger bereinigt und kann danach im Explorer neu formatiert werden. Achten Sie sorgfältig auf die richtige Kennziffer („x").

Booten mit USB-Sticks

Bootprobleme mit USB gibt es eine ganze Reihe. Auf nicht allzu alter Hardware sind diese aber korrigierbar. Die typischen Fehlerquellen:

1. USB-Sticks mit Linux-System sollten nicht am USB-Hub, sondern direkt am PC angeschlossen sein. Bei Bootproblemen entfernen Sie am besten alle anderen USB-Geräte, die am Rechner hängen. Wenn der Stick



Booten von USB: Der einfachste Weg, den gewünschten Boot-Datenträger für den anstehenden Systemstart zu bestimmen, ist das Bootmenü des Bios.

an anderen PCs bootet, ist der Fehler im Bios und nicht beim Stick zu suchen (siehe folgende Punkte).

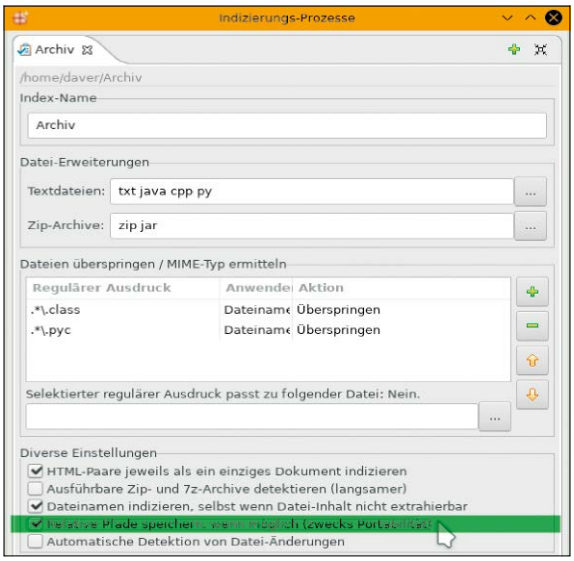
2. Standardmäßig priorisiert das Bios Festplatte und DVD als Boot-Datenträger. Die Bootreihenfolge lässt sich im Bios-Setup generell umstellen, das ist aber für gelegentliche Starts von Linux-Livesystemen auf USB nicht nötig: Es genügt, das Bootmenü des Bios abzurufen, indem Sie nach den Einschalten des Gerät frühzeitig eine bestimmte Taste drücken. Das Bootmenü zeigt dann die möglichen Bootquellen an und erlaubt die Auswahl des Sticks. Die Taste für das Bootmenü ist nicht standardisiert – oft hilft Esc, F8, F9, seltener F10, F11, F12. Das Bios-Bootmenü zeigt dann alle angeschlossenen Geräte an und Sie können das gewünschte USB-Medium manuell auswählen.

3. In seltenen Fällen werden USB-Geräte im Bios-Bootmenü nicht berücksichtigt. Deaktivieren Sie dann die Bios-Option „Fastboot" (meist Standard).

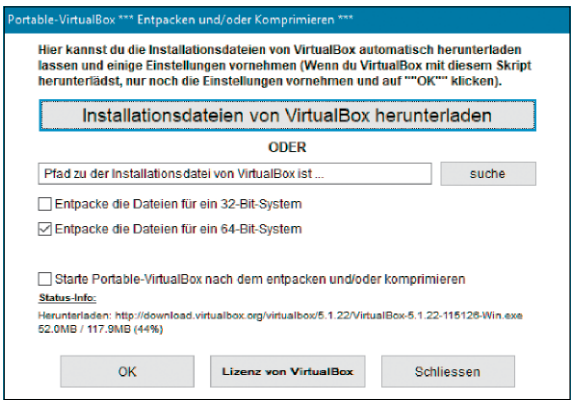
4. Die Bios-Option „Secure-Boot" (meist Standard) ist eine Bremse für Linux-Exoten, die keinen digital signierten Bootloader besitzen. Prominente Desktopsysteme sind davon nicht betroffen. Deaktivieren Sie die Bios-Option bei Bedarf.

Mobile Szenarien

Das Suchtool Docfetcher (*http://docfetcher.sourceforge.net*) läuft auf jedem System mit Java-Runtime. Daher sind der portable Einsatz auf USB und die Nutzung einer Dokumentensammlung inklusive Docfetcher-Indexsuche unter Linux wie Windows möglich. Dazu muss der USB-Datenträger ein Dateisystem verwenden, das jedes System versteht – etwa NTFS. Ferner ist bei der Indexerstellung eine wichtige Option zu beachten: Wenn Sie nach Rechtsklick im „Suchbereich" einen neuen Index erstellen, erscheint nach Auswahl des gewünschten Datenordners das Fenster „Indizierungs-Prozesse". Ganz unten (scrollen!) gibt es die Option „Relative Pfade speichern, wenn möglich (zwecks Portabilität)".



Docfetcher auf USB: Die Option „Relative Pfade" ist wichtig, wenn Docfetcher auf einem portablem Datenträger unter Linux wie Windows funktionieren soll.



Installer für portables Virtualbox: Dieser Dialog ist kein Glanzstück grafischer Benutzerführung, aber wenn Sie erst den großen Button tätigen und dann entpacken, kommen Sie ans Ziel.

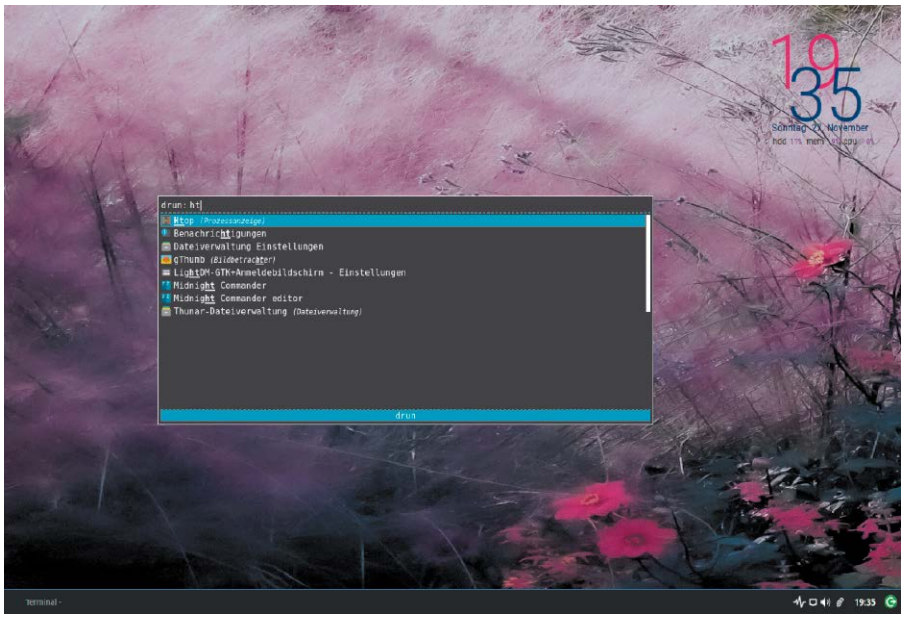
Dokuwiki/Mediawiki: Wer seine Notizen, Adressen, Anleitungen und Infosammlungen in einem Wiki auf Apache- oder Nginx-Basis abruft, bearbeitet und erweitert, kann sein Wiki auch auf USB-Stick transportieren. Voraussetzung ist dort ein ordentlich installiertes Linux-System mit Apache/Nginx, Wiki-Software und mindestens PHP. Eine Datenbank benötigt das einfachere Dokuwiki (*www.dokuwiki.org*) nicht. Dokuwiki ist ein guter Mobil-Begleiter, weil der Datenabgleich mit der heimischen Wiki-Installation leicht fällt: Nur das Unterverzeichnis „/data" enthält die Inhalte und ist mit rsync leicht zu synchronisieren.

Virtualbox Portable: Windows-Nutzer, die gelegentlich ein Linux-Zweitsystem benötigen, sollten den Einsatz von Virtualbox Portable in Betracht ziehen. Damit starten Sie den Virtualisierer auf jedem Windows-System und dann die dort die eingerichtete(n) Linux-VM(s). Diese Methode erspart typischen Windows-Nutzern das Hantieren mit ISO-Images und benötigt kein Booten des Fremdsystems.

Portable Virtualbox gibt es auf *www.vbox.me*. Nach dem Download entsteht der Ordner „Portable-VirtualBox" mit allen nötigen Komponenten, der dann auf USB kopiert werden kann. Das portable Virtualbox hat keine Einschränkungen und kann jegliche Linux-Distributionen auf Basis von ISO-Dateien einrichten. Ein kleines Ärgernis sind die Windows-Laufwerkskennungen: Wenn ein virtuelles System auf einem USB-Stick mit der Kennung „E:" eingerichtet wurde, funktioniert es nicht, wenn der Stick auf dem nächsten Rechner zufällig die Kennung „D:" oder „F:" erhält. Die einfachste Abhilfe ist es, dem USB-Medium vorab und dann bei späterer Nutzung grundsätzlich den Buchstaben „A:" zu verpassen. Das ist in der Windows-Datenträgerverwaltung (diskmgmt.msc) mit wenigen Klicks erledigt („Laufwerksbuchstaben und -pfade ändern"). ■

Schnelles Linux auf USB

Zweitsysteme auf USB eignen sich als mobile Allzwecksysteme, als sichere Surfsysteme oder als Reparatur- oder Backup-Dienstleister. Für die erstgenannten Einsatzgebiete ist Geschwindigkeit Pflicht, aber auch generell darf es gerne schnell gehen.



VON HERMANN APFELBÖCK

Gesucht wird das schnellste und beste Linux auf USB als Allzweck-Zweitsystem. Was wir in diesem Beitrag empfehlen werden, sind dann allerdings nicht die typischen Minimalisten oder Live-Spezialisten, die sich als Kandidaten scheinbar aufdrängen. Denn das Ergebnis sollte mehrheitstauglich und halbwegs komfortabel ausfallen – und das wirft diverse typische Mobil-Spezialisten aus dem Rennen.

Zur Info: Alle aufgeführten USB-Bootzeiten wurden mit einem 64-GB-Stick Sandisk Ultra 3.20 gemessen, allerdings auf einem älteren PC mit USB 3.0 (Gen1). Die Leistung kann auf ganz moderner Hardware besser ausfallen als hier gemessen, schlechter nur mit USB 2.0.

Aussortiert: Spezialsysteme für Bastler

Es gibt einige bekannte Minimalisten, die sich auf den Livebetrieb als Zweit- oder Servicesystem spezialisiert haben. Ursprüngliche Zielsetzung von Live-Pionieren wie Knoppix und Puppy war allerdings eine Lösung für eine extreme Mangelsituation, die eigentlich aus der Zeit gefallen ist: Das System sollte mit CD-Kapazität zurechtkommen, die Nur-Lesbarkeit dieses Mediums muss mit virtuellen Dateisystemen im RAM kompensiert werden und dabei noch mit wenig RAM auf alter Hardware auskommen. Das sind Mangelbedingungen, die auf moderner Hardware und auf heutigen USB-Sticks eigentlich hinfällig sind. Minimalisten wie Porteus, Slax, Slitaz, Sparky, Tiny Core, Trisquel Mini oder Watt-OS setzen diese Techniken dennoch im Sinne einer Spezialisierung fort.

Aus diesem Grund sortieren wir außer Knoppix alle oben genannten Kandidaten aus, obwohl ein Slax ein USB-Schnellbooter ist (10 bis 12 Sekunden) und ein Puppy Linux wieselflink im Alltagsbetrieb arbeitet. Es gibt aber noch weitere Gründe: Slitaz (*www.slitaz.org/de*) und Tiny Core (*http://tinycorelinux.net*) sind Reduktionsrekorde ohne echte Alltagsrelevanz. Slax (*www.slax.org*), Puppy Linux (*http://distro.ibiblio.org/puppylinux*) und Porteus (*http://porteus.org*) sind allenfalls für Bastler relevant: Allein schon, deren nicht-hybride ISO-Images (nur auf CD/DVD-bootfähig) auf USB zu befördern, nötigt zu manuellen Schritten (Slax) oder zum Umweg über eine CD oder eine virtuelle Maschine (Puppy, Porteus). Weiterführende Anpassungen des Livesystems sind entweder kompliziert (Slax, Porteus) oder inhaltlich unbefriedigend: Die Puppy-Systeme bieten für ihr eigenes Paketformat wenig Software und diese praktisch nur englischsprachig.

Bei etlichen weiteren Minimalisten wie Sparky (*https://sparkylinux.org*), Trisquel (*https://trisquel.info*) oder Watt-OS (*http://planetwatt.com*) ergeben sich keine offensichtlichen Vorteile gegenüber einem Debian oder Derivaten wie MX Linux und Q4-OS.

Livesysteme: Ubuntu oder Knoppix?

Ein pures, unveränderliches Livesystem taugt nicht als Zweitsystem. Erst eine Persistenzoption für eigene Dateien, Anpassun-



Klein, schnell und eingebaute Persistenz: Puppy-Livesysteme können technisch überzeugen, sind aber nicht pflegeleicht und lassen (deutschsprachige) Software vermissen.

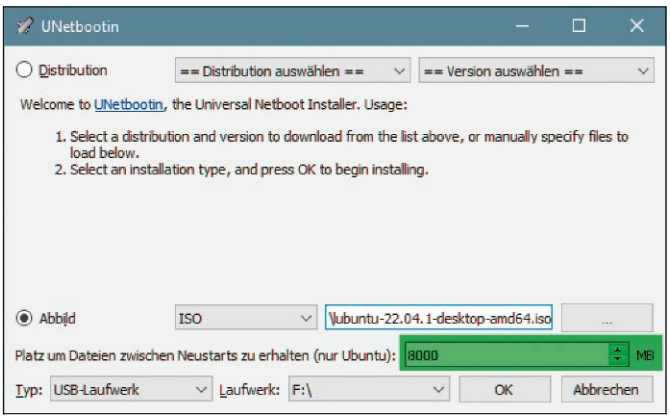
gen und Nachinstallationen macht das Zweitsystem attraktiv. Die Auswahl solcher anpassungsfähiger Livesysteme wäre trotz der oben aussortierten Live-Spezialisten enorm, weil jedes Ubuntu-basierte ISO-Installationsmedium über das Tool Unetbootin (auf Heft-DVD) mit Persistenz auf USB geschrieben werden kann. Sie müssen dazu im Unetbootin-Fenster neben der Option „Platz um Dateien zwischen Neustart zu erhalten" nur eine MB-Angabe eintragen. 2000 bis 8000 MB sind je nach Kapazität des USB-Sticks sinnvolle bis großzügige Werte. Unetbootin meldet dann beim Aktionsschritt 3 („Installiere Startverwalter") zusätzlich die Aktion „Erstellen der Persistenz".

Optimal sind Live-Ubuntus allerdings nicht, weil sie aufgrund eines standardisierten Checks des Livemediums nicht sonderlich schnell booten. 40 Sekunden sind auch bei kleinem Lubuntu oder Xubuntu für jeden Start einzurechnen. Aus Leistungsgründen sind Ubuntu-Distributionen daher eher ein Fall für ordentliche Installation auf USB. Noch ein zweiter Grund spricht gegen Live-Ubuntu auf USB: Es gibt dabei keine Möglichkeit, das USB-Medium durch Verschlüsselung zu schützen.

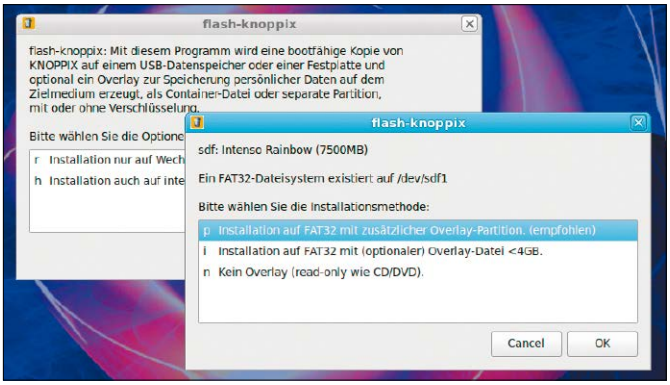
Das Debian-basierte Knoppix ist der Live-Klassiker schlechthin und ein „No-Brainer". Wem der relativ einfache LXDE-Desktop nicht zu schlicht ist, kann mit Knoppix definitiv nichts falsch machen. Deutschsprachig, mit exzellenter Hardwareerkennung, opulenter Softwareausstattung und anspruchslosem LXDE-Desktop ist Knoppix erste Wahl für ein Zweit- oder Surfsystem. Mit USB-Bootzeiten von 20 Sekunden zum eingabebereiten Desktop gehört Knoppix zu den schnellen Livestartern, wenngleich er mit Spezialisten wie Slax oder Porteus nicht ganz mithalten kann. Im laufenden Betrieb und beim Start von Programmen ist die Knoppix-Leistung durchschnittlich, aber jederzeit agil. Knoppix hat aber zusätzlich den unschätzbaren Vorteil, dass weder der LXDE-Desktop viel Eingewöhnung fordert noch Software nachinstalliert werden muss. Knoppix hat wirklich alles an Software und Tools am Start.

Der Download von einem der Mirrorserver unter *www.knopper.net/knoppix-mirrors* beträgt für die aktuellste Version 9.1 circa 4,4 GB. Achten Sie in der Liste der ISO-Dateien auf „-DE" im Dateinamen („Knoppix_V9.1DVD-2021-01-25-DE.iso"). Das hybride ISO-Abbild kann mit den üblichen Tools auf USB-Stick kopiert werden.

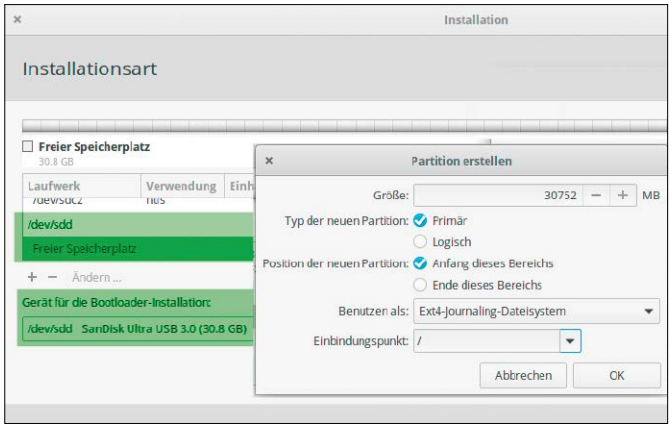
Für häufige Nutzung ist die Persistenzoption unentbehrlich, die bei Knoppix „Overlay-Partition" heißt. Dazu müssen Sie aber aus einem bereits laufenden Knoppix ein zweites erstellen. Das maßgebliche Tool „Flash Knoppix" finden Sie unter „Knoppix → Knoppix auf Flash kopieren". Nach Auswahl des Zieldatenträgers folgt die „Installation auf FAT32 mit zusätzlicher Overlay-Partition". Die Abfrage zur Größe der Overlaypartition können Sie auf einem USB-Stick einfach mit „OK" übernehmen. Dann erhält die Overlaypartition auf dem Stick die komplette Restkapazität, die das eigentliche Knoppix-System übriglässt. Eine letzte Frage betrifft den optionalen Verschlüsselungsschutz der Overlaypartiti-



Unetbootin und Ubuntu live mit Persistenz: Das ist besser als ein pures Livesystem, aber kaum optimal. Kleine Ubuntus sind regulär auf USB-Stick installiert schneller und flexibler.



Live-Klassiker Knoppix mit Persistenz: Die Overlay-Partition ermöglicht dem Livesystem Desktop-Anpassungen, Installationen und Deinstallationen.



USB-Installationen: Systempartition und Bootloader müssen als Ziel den USB-Stick erhalten. Mehr ist bei der Partitionierung nicht nötig, wenn die Installation im Bios-Modus erfolgt.

on. Es handelt sich um die einzige Möglichkeit, einen USB-Stick mit Knoppix systemweit zu schützen, weil Knoppix als Livesystem keine Benutzerverwaltung hat. Die Verschlüsselung schützt neben dem Knoppix-System auch die persönlichen Daten auf dem USB-Stick.

Mit Overlaypersistenz erlaubt Knoppix Anpassungen aller Art, auch Nachinstallationen und Entfernen überflüssiger Pakete. (De-)Installationen sind wahlweise über apt im Terminal zu realisieren oder auch über Synaptic.

USB-Installation: Schnelle Kandidaten

Jedes Linux lässt sich regulär auf USB-Stick installieren. Ein installiertes mobiles Linux auf USB oder SD-Karte ist genauso updatefähig, ausbau- und anpassungsfähig wie auf Festplatte. Anders als beim Livesystem (mit oder ohne Persistenz) ist hier ein USB-Stick mit mindestens 32 GB Kapazität zu empfehlen, besser größer.

Die Installation geschieht typischerweise im Livesystem, dessen ISO-Image Sie zunächst herunterladen, kopieren und dann im Bios-Modus starten. Bei der Partitionierung während der Installation müssen Sie dann den USB-Datenträger als Zielpartition für das System angeben, zweitens unbedingt auch als Zielort für den Bootloader. Die Vorgehensweise ist für die empfohlenen Systeme anschließend noch genauer beschrieben.

Bei der Wahl der Distribution gibt es keine prinzipiellen Beschränkungen. Aber im Sinne eines möglichst schnellen Bootvorgangs und einer agilen Systemnutzung gibt es besser und schlechter geeignete Distributionen.

Kleine Ubuntus: Im Gegensatz zum Livebetrieb booten auf USB installierte Ubuntus recht flott zum Desktop. Schnellster Starter ist das Ubuntu-basierte Bodhi Linux (*www.bodhilinux.com*), das in 13 Sekunden zum Desktop lädt. Bodhi ist auch im Betrieb und bei Programmstarts überragend schnell, lässt aber bequeme Konfigurationszentralen vermissen und hat einen gewöhnungsbedürftigen Moksha-Desktop. Unsere Ubuntu-Empfehlung ist daher das unkomplizierte Lubuntu, das – installiert auf USB 3.x – nach 21 Sekunden am Log-in ist.

Für die Lubuntu-Installation benötigen Sie das ISO-Image von *https://lubuntu.me/downloads/* (2,5 GB). Das hybride ISO-Abbild kann mit den üblichen Tools (Etcher, Gnome-Disks, USB-Imager et cetera) auf einen USB-Stick kopiert werden. Damit booten Sie einen Rechner, laden das Bios-Bootmenü (Esc, F8, F9, seltener F10, F11, F12) und dort den Stick im Bios-Modus (ohne „Uefi"). Das Livesystem bietet dann die Installation mit dem Tool Calamares an, die Sie auf einen zweiten und eigentlichen USB-Stick absolvieren. Der beim Setup wesentliche Punkt „Partitionen" muss also oben bei „Speichermedium" auf den USB-Stick verweisen. Über „Manuelle Partitionierung" löschen Sie dann eventuell vorhandene Partitionen des Sticks und erstellen auf dem nun „freien Platz" eine primäre Ext4-Partition mit Einhängepunkt „/". Die unscheinbare Option „Verschlüsseln" sorgt bei Bedarf für Vollverschlüsselung des Sticks. Zurück im Hauptdialog muss ganz unten die Option „Installiere Bootloader auf" unbedingt ebenfalls auf das USB-Laufwerk gesetzt werden, damit das USB-System später an jedem Rechner starten kann.

Hinweis: Andere Ubuntus wie Xubuntu oder Bodhi Linux verwenden einen anderen Installer (Ubiquity). Die Vorgehensweise unterscheidet sich dort deutlich, die prinzipielle Vorgehensweise ist aber entsprechend. Die Abbildung auf dieser Seite zeigt den einschlägigen Installer-Dialog.

Q4-OS ist mit Debian-Unterbau und Trinity-Desktop schnell und anspruchslos (Download unter *http://q4os.org*, auf Trinity-Variante achten!). Für einen reinen Livebetrieb ist es nicht ideal, weil es nach der Auswahl der deutschen Lokalisierung die nötigen Pakete stets erst aus dem Internet nachlädt und damit kaum unter einer Minute zu starten ist. Es ist aber ein idealer Kandidat für die reguläre Installation auf USB. Dazu muss das hybride Download-ISO erst auf einen USB-Stick kopiert und im Livesystem Q4-OS, das im Bios-Modus gestartet werden muss, auf einen zweiten und endgültigen USB-Stick installiert werden.

Die Installation erledigt hier ein eigener, aber Calamares-ähnlicher Installer, wobei unter „Software" am besten „Q4OS-Desktop" mit vollständiger Programmausstattung zu wählen ist. Unter „Partitionen" muss ganz oben unbedingt das richtige Speichermedium aktiviert werden, wobei Sie dann alles Vorhandene „Löschen" und mit „Erstellen" die Systempartition mit Einhängepunkt „/" anlegen. Eine Partitionsverschlüsselung mit Luks ist hier ebenfalls vorgesehen. Nach „OK" muss noch der Bootloader im Dialog ganz unten auf das USB-Laufwerk gesetzt werden.

Nach der Installation holen Sie die deutsche Lokalisierung nach, was das System selbst anbietet. Danach startet der „Desktop-Profiler", um die Softwareausstattung zu komplettieren.

Das installierte System startet auf USB-3.0-Stick in 15 Sekunden und belegt nach der Anmeldung für System und Desktop knapp 400 MB RAM. Der Desktop Trinity basiert auf dem eingestellten KDE 3 und wirkte lange Zeit reichlich retro. In den jüngsten Versionen (aktuell 4.10) hat sich die Oberfläche optisch gründlich modernisiert, und eingängig, übersichtlich sowie anpassungsfähig war sie schon immer. Die Arbeitsfläche ist eine klassische Dateiablage, das Menü ähnelt dem Stil älterer Windows-Versionen und die Systemleiste („Kontrollleiste") enthält mit Schnellstarter, Fensterliste und Indikatoren die typischen Elemente.

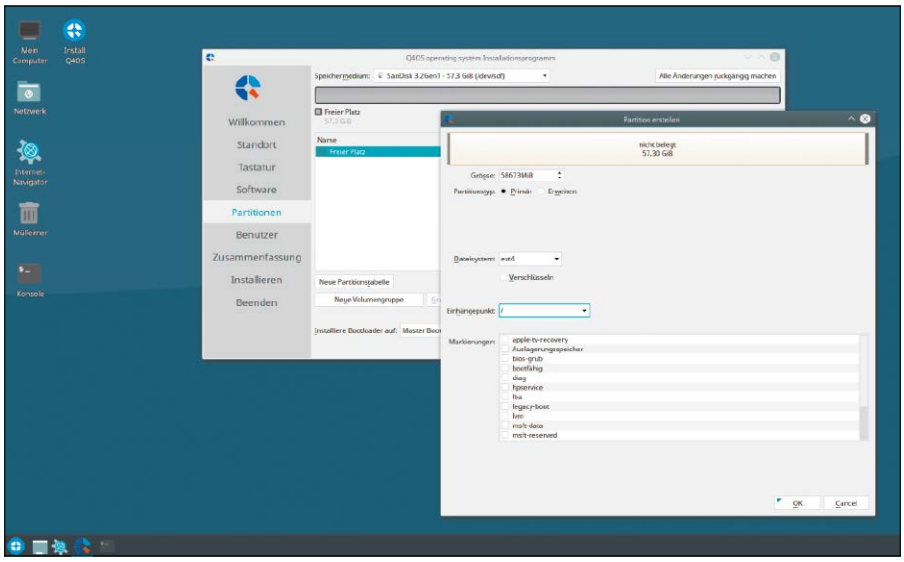
MX Linux: Diese Distribution (Download unter *https://mxlinux.org*) nutzt auf Debian-Basis entweder den klassischen XFCE-Desktop (1,7-GB-ISO) oder den besonders schlanken Fenstermanager Fluxbox (1,4-

GB-ISO), der sich lediglich einige XFCE-Anleihen wie den Xfce4-Appfinder leistet (als Menüersatz). Die Fluxbox-Variante ist für ein mobiles Zweitsystem eine schlanke Wahl, XFCE die komfortablere. Die eine oder andere englischsprachige Beschreibung oder Menübezeichnung muss man bei MX Linux aber in beiden Desktops in Kauf nehmen.

Auch für MX Linux muss zunächst das hybride Download-ISO auf einen USB-Stick kopiert werden. Mit dem Livesystem von MX Linux, das im Bios-Modus gestartet werden muss, wird es dann auf den zweiten und endgültigen USB-Stick installiert.

Das Setup verläuft einfach und linear, wenngleich ein paar Fragen mehr gestellt werden: Im Bootmenü des Livesystems wählen Sie zunächst mit F2 die Sprache „Deutsch“ und mit F3 die Zeitzone „Berlin“. Dann starten Sie den obersten Eintrag „MX-21.2“. Eventuelle Fragen nach der Grafikkarte quittieren Sie ohne Auswahl mit Eingabetaste, starten zum Desktop des Livesystems und klicken auf den Installer-Link am Desktop. Als „Art der Installation“ verwenden Sie „Normale Installation“ und wählen dann im Drop-down-Feld darunter sorgfältig den USB-Stick, der das Installationsziel ist. Beachten Sie darunter die Option „Verschlüsseln“, die System und Stick durch Luks-Datenträgerverschlüsselung schützt. Während der Installer dann bereits kopiert, werden die Daten für den Erstbenutzer, die Sprache und die Zeitzone, ein root-Kennwort, ein Computername sowie die Samba-Arbeitsgruppe abgefragt. Der Vorgang ist etwas umständlicher als bei Ubuntu & Co., aber letztlich einfacher, als diese Einstellungen später im laufenden System zu suchen.

Nach ordentlicher Installation auf USB 3.0 beträgt die Startzeit zur Desktopanmeldung etwa 18 Sekunden. Der RAM-Bedarf liegt unter 500 MB. Alle Programme, auch größere Brocken wie Browser oder LibreOffice-Komponenten, sind frappierend reaktionsschnell. Die Fluxbox-Variante von MX Linux ist tempomäßig mit Bodhi Linux vergleichbar, dabei aber deutlich pflegeleichter.



Q4-OS bei der USB-Installation: Die Distribution mit klassischem Trinity-Desktop hat sich optisch modernisiert und ist schneller und schlanker als jedes Ubuntu.

Systemoptimierung: Ausmisten und erweitern

Für ein ordentlich auf USB installiertes Linux-System gibt es nur eine nennenswerte Einschränkung: Installieren Sie besser keine proprietären Treiber, wenn das System auf unterschiedlicher Hardware funktionieren soll. Ansonsten haben Sie alle Möglichkeiten, Software zu installieren, Software zu entfernen sowie das System zu optimieren.

Software installieren und beseitigen: Alle hier empfohlenen Kandidaten verwenden das Debian-Paketformat und lassen sich über den apt-Paketmanager erweitern und entschlacken. Folglich können Sie in allen genannten Systemen in der üblichen Manier etwa mit

```
sudo apt install filezilla
```

Software ergänzen und Unnötiges mit *sudo apt remove […]* entsorgen.

Autostarts und Dienste: Um den Desktopstart und den Speicherbedarf zu optimieren, suchen Sie die „Startprogramme“ auf. Wenn eine solche Zentrale fehlt, hilft auch direkte Dateibearbeitung unter „/etc/xdg/autostart“ und „~/.config/autostart“. Komponenten, die Sie auf einem Mobilsystem nicht benötigen (Datensicherung, Blueman, Orca, Welcome …) deaktivieren Sie per Mausklick in der Zentrale oder durch Umbenennen auf Dateiebene.

Wer noch einen Schritt weiter gehen will, kann die gestarteten Dienste durchforsten:

```
sudo service --status-all
```

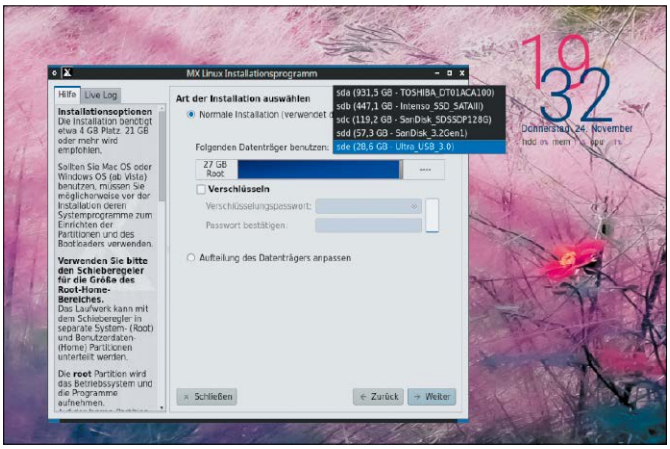
Dieser Befehl (statt systemctl) funktioniert sowohl unter systemd als auch ohne systemd – so etwa unter MX Linux. So sind die Dienste Cups (Drucken), Whoopsie (Fehlerreport), Apport (Fehlerprotokoll) oder Apparmor (Sicherheitserweiterung) auf einem Mobilsystem vermutlich entbehrlich. Einen Dienst stoppen Sie mit

```
sudo service whoopsie stop
```

und entfernen ihn später mit

```
sudo rm /etc/init.d/whoopsie
```

komplett, sofern er sich dauerhaft als überflüssig erweist. ■



Unser Favorit bei der Installation auf USB: MX Linux mit Fluxbox garantiert einen überaus agilen Programmalltag auf USB-Stick.

Multiboot mit ISO-Dateien

Linux-Distributionen und Rettungssysteme lassen sich von einem USB-Stick booten, auf dem sich aber immer nur ein System unterbringen lässt. Wir stellen Tools vor, die den Start mehrerer Systeme von einem USB-Laufwerk ermöglichen.

VON THORSTEN EGGELING

Linux-Distributionen werden in der Regel als ISO-Dateien für CDs und DVDs ausgeliefert. Die Dateien sind aber so konstruiert, dass sich damit auch ein bootfähiger USB-Stick für die Linux-Installationen erstellen lässt. Allerdings kann man immer nur ein einzelnes System vom USB-Stick starten, da die Bootumgebungen der verbreiteten Linux-Distributionen weitestgehend identisch sind. Kopiert man ein zweites Installationssystem auf den Stick, werden die Dateien des vorherigen Systems überschrieben.

Wer mehrere Linux-Distributionen und vielleicht Windows vom USB-Stick installieren möchte, kann die ISO-Dateien auch direkt booten. Wir stellen Tools vor, die das ermöglichen. Das ist auch für Rettungs- und Reparatursysteme nützlich, die sich ebenfalls auf einem USB-Stick unterbringen lassen. Die Anzahl ist nur durch die Kapazität des Laufwerks begrenzt. Die Methode ist keinesfalls nur auf USB-Sticks anwendbar. ISO-Dateien lassen sich genauso gut von einer USB-Festplatte oder dem eingebauten SATA-Laufwerk booten.



Bootstick erstellen: Das Tool „Startmedienersteller" belegt den USB-Stick komplett mit allen Partitionen aus der ISO-Datei. Das ist unpraktisch, wenn man unterschiedliche Systeme starten möchte.

Wie ein Linux-Livesystem bootet

Die ISO-Dateien vieler Linux-Installationsmedien enthalten zwei Bootmanager. Isolinux (*https://wiki.syslinux.org*) ist für den Start auf älteren PCs mit herkömmlichem Bios (Basic Input Output System) oder auf neueren Uefi-Geräten mit aktiviertem CSM (Compatibility Support Module) zuständig. Neben einem ISO-9660-Dateisystem enthält das ISO zusätzlich die Eltorito-Erweiterung, mit der eine CD/DVD erst bootfähig wird. Eltorito kann ein Festplatten- oder Floppy-Abbild mit einem Minisystem starten, über das dann das Linux-System geladen wird. Es ist aber flexibler, stattdessen den Programmcode von Isolinux in den Speicher zu laden und dann den Bootvorgang fortzusetzen. Isolinux bietet ein umfangreiches Menüsystem, über das man bereits vor der Installation beispielsweise die Sprache auswählen, eine Hilfe aufrufen oder zusätzlich Kernel-Parameter übergeben kann.

Der zweite Bootmanager heißt Grub2 (*www.gnu.org/software/grub*). Er kommt bei PCs mit Uefi-Firmware zum Einsatz. Neuere Distributionen wie Ubuntu 22.04 verwenden ihn auch für den Bios-Modus. Auf die Grub-Konfiguration verwenden die Distributoren bisher keine große Mühe. Obwohl auch dieser Bootloader sich ansprechend gestalten lässt, zeigt sich das Grub-Menü meist in schlichtem Schwarzweiß und bietet keine Vorauswahl der Sprache.

Booten vom USB-Stick: Im einfachsten Fall wird der Inhalt der ISO-Datei exakt auf den USB-Stick kopiert, beispielsweise mit

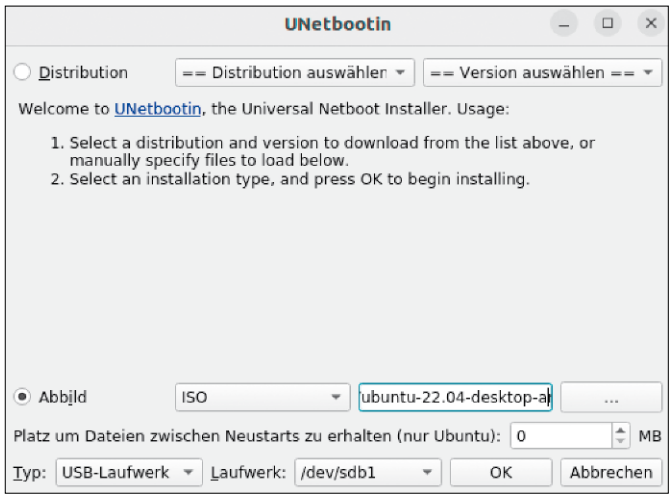
```
sudo dd if=[Boot-DVD.iso] of=/dev/
  sd[X]
```

„[X]" steht für die Laufwerksbezeichnung. Dabei gehen alle vorhanden Daten verloren. Das gleiche Ergebnis erzielt man unter Ubuntu mit dem Tool „Startmedienersteller" für die grafische Oberfläche. Nutzer von Linux Mint finden ein ähnliches Programm im Startmenü unter „Zubehör → USB-Abbilderstellung".

Auf dem Stick befinden sich dann die gleichen Partitionen wie auf der DVD. Eine große schreibgeschützte ISO-9660-Partition enthält die Systemdateien und deren Inhalt ist im Dateimanager sichtbar. In den ersten

512 Bytes ist außerdem ein MBR (Master Boot Record) untergebracht, damit das System auch auf Bios-PCs booten kann. Dahinter folgt die ESP-Partition (Efi System Partition) für Uefi-PCs mit den Grub2-Bootloader-Dateien. Selbst wenn der USB-Stick mehr Speicherplatz bietet, als die ISO-Datei benötigt, ist der Rest nicht mehr nutzbar. Nach der Linux-Installation kann man den Stick neu formatieren, um ihn für andere Zwecke zu verwenden.

Tools wie Unetbootin (*https://unetbootin.github.io*) oder Rufus (nur für Windows, *https://rufus.ie*) funktionieren anders. Beide kopieren die Dateien aus dem ISO auf den USB-Stick, der für Linux mit dem Dateisystem FAT32 formatiert sein muss. Unetbootin installiert für Bios-PCs in jedem Fall den Bootloader Syslinux und erstellt automatisch eine passende Konfigurationsdatei. Rufus richtet Syslinux nur ein, wenn das System Isolinux verwendet. Andernfalls wird der Grub2-MBR auf Bios-PCs verwendet. Für Uefi-PCs sind bei beiden Tools keine besonderen Maßnahmen erforderlich, weil die PC-Firmware auf einer FAT32-Partition den Bootloader im Ordner „/EFI/boot/“ findet. Anders als bei dd steht der nicht belegte Platz auf dem USB-Stick weiter zur Verfügung. Die Installationsdateien eines weiteren Linux-Systems lassen sich jedoch nicht zusätzlich auf das Laufwerk kopieren.



Unetbootin: Auch dieses Tool kann nur ein einzelnes System auf den USB-Stick kopieren und verändert zudem das Bootmenü. Dafür bleibt aber Speicherplatz für andere Zwecke übrig.

Ventoy: Installationsabbilder direkt vom Stick starten

Der Bootloader Grub2 kann ISO-Abbilder einbinden und das enthaltene System starten. Dafür ist eine Konfigurationsdatei erforderlich, die den Pfad zu ISO-Datei, Kernel und Ramdisk-Datei („initrd“) enthält. Das Tool Ventoy (*www.ventoy.net*) automatisiert die Grub2-Konfiguration so gut wie möglich. Es findet ISO-Dateien auf dem USB-Stick und erstellt automatisch ein dazu passendes Menü, über das sich das gewünschte System booten lässt. Mit Ventoy kann man die meisten bekannten Linux-Distributionen und Windows verwenden. Eine Liste der getesteten ISO-Dateien ist unter *www.ventoy.net/en/isolist.html* einsehbar.

Schritt 1: Zur Installation laden Sie die „tar.gz“-Datei für Linux von *https://github.com/ventoy/Ventoy/releases* herunter. Entpacken Sie das Archiv und starten Sie dann Ventoy-GUI.x86_64. Sollte das Programm auf Ihrem PC nicht starten, lässt sich Ventoy im Webbrowser nutzen: Gehen Sie im Terminal in den Ordner, wo Sie das Tool entpackt haben. Dort starten Sie dieses Script:

```
sudo ./VentoyWeb.sh
```

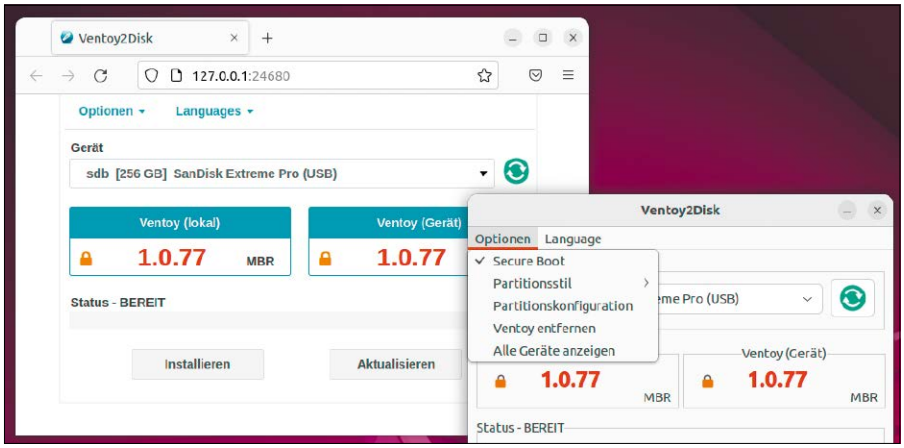
Es zeigt die URL an, über die sich die Weboberfläche im Browser erreichen lässt, standardmäßig *http://127.0.0.1:24680*.

Schritt 2: Stellen Sie über „Language“ als Sprache „German (Deutsch)“ ein. Unter „Optionen“ aktivieren Sie „Secure Boot“. Das ist nur für Windows 11 erforderlich, weil sich Windows 10 oder Linux auch bei deaktiviertem Secure Boot installieren lässt. Wählen Sie unter „Gerät“ den USB-Stick aus und klicken Sie auf „Installieren“. Der Stick wird neu formatiert, alle enthaltenen Daten gehen verloren. Wenn Sie „Optionen → Alle Geräte anzeigen“ wählen, bietet Ventoy auch Festplatten als Ziel an. Prüfen Sie daher die Einstellung genau, damit Sie nicht versehentlich das falsche Laufwerk formatieren.

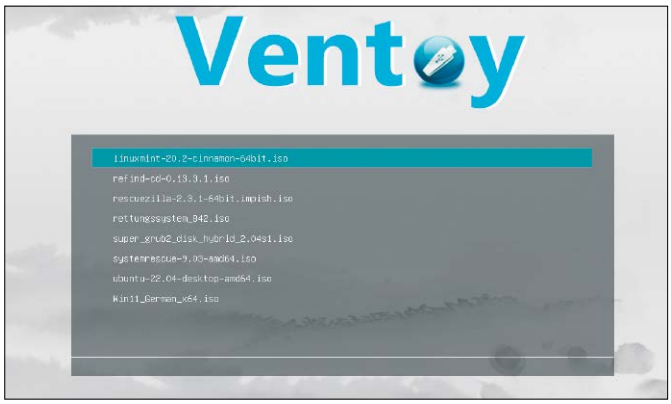
Ventoy belegt eine kleine 32-MB-Partition, auf der Grub2, die Bootloader-Dateien für Uefi und einige Tools untergebracht sind. Ein Master Boot Record wird ebenfalls auf den USB-Stick geschrieben, damit auch Bios-PCs davon booten können.

Die zweite Partition wird mit dem Dateisystem ExFAT formatiert und steht auch als Datenspeicher weiter zur Verfügung. Die meisten Linux-Systeme kommen mit der ExFAT-Partition zurecht, aber nicht alle. Soll nur Linux installiert werden, formatiert man die „Ventoy“-Partition mit dem Dateisystem Ext4 neu. Das erhöht die Kompatibilität und verbessert die Leistung. Wer auch Windows installieren möchte, wählt das Dateisystem NTFS. Das eignet sich auch für Linux, weil der Kernel den dafür nötigen Treiber seit Langem enthält.

Schritt 3: Kopieren Sie die gewünschten ISO-Dateien auf den Stick und booten Sie den PC damit. Beim ersten Start und bei aktiviertem Secure Boot erscheint die Mel-



USB-Stick mit Ventoy: Das Tool lässt sich als Desktopanwendung oder im Browser starten. Für Uefi-PCs müssen Sie die Option „Secure Boot“ aktivieren, sofern diese im Bios aktiv ist.



Ventoy-Bootmenü: Alle für Ventoy bereitgestellten ISO-Dateien erscheinen automatisch im Menü. Die Funktionen der F-Tasten sind am unteren Bildschirmrand zu sehen.

dung „Access denied“, die Sie mit „OK“ übergehen. Danach drücken Sie eine beliebige Taste, gehen auf „Enroll key from disk“, wählen „VTOYEFI“ und danach „Enroll _This_Key_In_Mokmanager.cer“. Zum Abschluss gehen Sie auf „Continue“, „Yes“ und „Reboot“.

Ventoy zeigt ein Menü für die Systemauswahl. Darüber starten Sie das gewünschte Installationssystem und die Einrichtung läuft wie gewohnt ab. Über die Taste F2 („Browser“) haben Sie außerdem Zugriff auf die Festplatten im PC und können dort gespeicherte ISO-Dateien auswählen und booten.

Ventoy: Livesystem mit Persistenz

Livesysteme lassen sich auch als Rettungs- oder Zweitsystem nutzen. Die Konfiguration und zusätzlich installierte Software existieren jedoch nur im RAM und gehen bei einem Neustart verloren. Ubuntu und Linux Mint bieten aber mit „Persistenz“ eine Funktion, über die sich individuelle Anpassungen speichern lassen und dann auch beim nächsten Start wieder zur Verfügung stehen.

Schritt 1: Ventoy unterstützt eine Persistenzdatei, die Sie im Terminal mit

```
sudo ./CreatePersistentImg.sh
```

erstellen. Standardmäßig erzeugt das Script die Datei „persitence.dat“, die Platz für ein GB Daten bietet. Wer eine größere Datei benötigt, legt beispielsweise mit

```
sudo ./CreatePersistentImg.sh -s
  2048
```

eine Größe von zwei GB fest. Kopieren Sie die Datei in den Ordner „ventoy“ auf dem USB-Stick.

Schritt 2: Starten Sie das Script „Ventoy Plugson“ im Terminal:

```
sudo ./VentoyPlugson.sh /dev/sd[X]
```

Den Platzhalter „[X]“ ersetzen Sie durch den Buchstaben, über den der USB-Stick erreichbar ist. Das Script zeigt mit *http://127.0.0.1:24681* die URL für die Weboberfläche an, die Sie im Browser aufrufen.

Schritt 3: Gehen Sie auf „Persistence Plugin“ und klicken Sie auf „+ Add“. Hinter „File Path“ fügen Sie den kompletten Pfad zur ISO-Datei ein, die die Persistenzdatei verwenden soll (Beispiel):

```
media/[User]/Ventoy/ISO/ubuntu-
  22.04-desktop-amd64.iso
```

„[User]“ ersetzen Sie durch Ihren Benutzernamen.

Hinter „Dat File“ tragen Sie den Pfad zur zuvor kopierten Persistenzdatei ein (Beispiel):

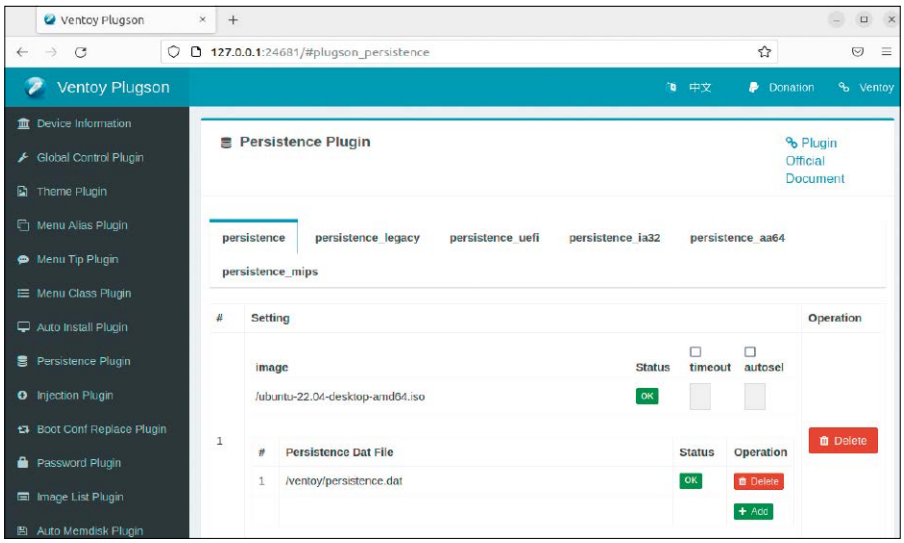
```
/media/[User]/Ventoy/ventoy/
  persistence.dat
```

Klicken Sie auf „OK“, um die Änderungen zu speichern. Das Tool erstellt die Konfigurationsdatei „ventoy.json“ im Ordner „ventoy“. Beim Start des Livesystems lässt Ventoy die Wahl zwischen „boot without persistence“ und „boot with /ventoy/persistence.dat“. Bei der Konfiguration von „Persistence Plugin“ können Sie ein Häkchen vor „timeout“ setzen und darunter die Zeit für einen Countdown eintragen. Nach Ablauf der Zeit startet das System automatisch mit Persistenz.

Ventoy: Optionen für die Windows-Installation

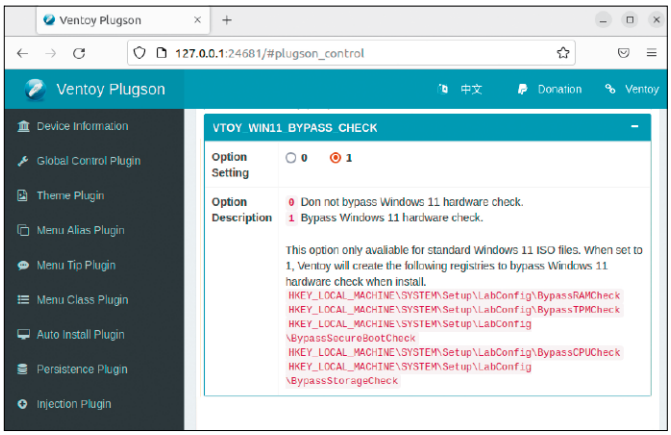
Über Ventoy lassen sich nicht nur ISO-, sondern auch WIM-Dateien booten (Windows-Images). Der Vorteil: Ein individuell angepasstes Installationsabbild („install.wim“) lässt sich direkt verwenden, ohne dass man eine neue ISO-Datei erstellen muss. Nützlich ist das beispielsweise, wenn man unter Windows mit Rufus (*https://rufus.ie*) einen Installationsstick erstellt, der die Hardwareanforderungen von Windows 11 umgeht (Option „Extended Windows 11 Installation (no TPM / no Secure Boot)“).

Damit das Verfahren funktioniert, muss die Ventoy-Partition auf dem Stick mit dem Dateisystem NTFS formatiert sein. Außerdem ist das Wimboot-Plug-in für Ventoy erforderlich. Laden Sie es über *https://m6u.de/WBOOT* herunter. Erstellen Sie auf dem Ventoy-Stick den Ordner „ventoy“ und kopieren Sie die Datei „ventoy_wimboot.img“ hinein. Danach kopieren Sie den gesamten Ordner „sources“ vom Rufus-Stick auf den Ventoy-Stick. Wenn Sie den PC davon booten, wählen Sie im Menü „boot.wim“, um das Installationssystem von Windows 11 zu starten.



Zusätzliche Konfiguration: Über die Webanwendung Plugson können Sie weitere Optionen festlegen. Einstellungen eines Ubuntu-Livesystems beispielsweise lassen sich in einer Persistenzdatei speichern.

Ventoy bietet auch für Original-ISO-Dateien von Microsoft eine Option, den Hardwarecheck bei der Windows-11-Installation zu umgehen. Starten Sie Ventoy Plugson wie vorher beschrieben. Unter „Global Control Plugin“ aktivieren Sie im Abschnitt „VTOY_WIN11_BYPASS_CHECK“ die Option „1“. Dadurch werden bei der Windows-Installation die unter der Option genannten Registry-Einträge hinzugefügt und Windows lässt sich dann auf Hardware installieren, die offiziell nicht unterstützt wird. Da es sich um eine inoffizielle Methode handelt, ist nicht garantiert, dass Windows stabil läuft und dass die Installation mit dem Registry-Patch auch in zukünftigen Windows-Versionen möglich ist.



Windows 11: Die Hardwareprüfung des Microsoft-Systems lässt sich über Registry-Einträge aushebeln, die Ventoy bei der Windows-Installation automatisch einbauen kann.

Grml-Rescueboot: ISO-Dateien von Festplatte starten

ISO-Dateien lassen sich in das Grub-Menü des installierten Systems einbauen. Das ist nützlich, wenn Sie beispielsweise ein Livesystem regelmäßig als sicheres Surfsystem verwenden oder Rescuezilla für Backups starten.

Schritt 1: Installieren Sie unter Ubuntu 20.04, 22.04 oder Linux Mint 20 das Paket „grml-rescueboot“:

```
sudo apt install grml-rescueboot
```

Schritt 2: Standardmäßig soll der Ordner „/boot/grml“ die ISO-Dateien aufnehmen, den Sie mit

```
sudo mkdir /boot/grml
```

erstellen. Wenn das Verzeichnis „/boot“ auf einer eigenen Partition liegt, die nicht genügend Platz bietet, können Sie den Pfad in der Datei „/etc/default/grml-rescueboot“ ändern. Beispielsweise mit dieser Zeile:

```
ISO_LOCATION="/grml"
```

Erstellen Sie das angegebene Verzeichnis.

Schritt 3: Passen Sie die Datei „/etc/default/grub“ an. Hier müssen die Zeilen

```
GRUB_TIMEOUT_STYLE=menu
GRUB_TIMEOUT=10
```

enthalten sein, damit das Grub-Menü angezeigt wird. Beim Wert hinter „GRUB_TIMEOUT=“ geben Sie die Anzahl der Sekunden an, nach denen der Standardeintrag automatisch gestartet wird.

Schritt 4: Kopieren Sie die gewünschten ISO-Dateien in den konfigurierten Ordnern und führen Sie danach

```
sudo update-grub
```

aus. Wenn Sie den Rechner neu starten, sehen Sie zusätzliche Einträge im Grub-Menü, über die sich die ISO-Dateien booten lassen.

Zusätzliche Anpassungen für grml-rescueboot: Das Grub-Menü wird mit *update-grub* über Scripts im Ordner „/etc/grub.d/“ erzeugt. Die Datei „42_grml“ sucht nach Dateien im ISO-Ordner und erstellt die dafür passenden Einträge. Das Script setzt darauf, dass im ISO die Datei „/boot/grub/loopback.cfg“ enthalten ist, die Optionen für das direkte Booten der ISO-Datei enthält. Bei gängigen Distributionen ist die Datei vorhanden, bei einigen anderen aber nicht. Das bekannte System Rescue (*www.system-rescue.org*) beispielsweise oder auch Gparted Live (*https://gparted.org*) lassen sich daher nicht booten. Das Script „42_grml“ lässt sich aber dafür anpassen. Die relevanten Zeilen für System Rescue sehen Sie in der Abbildung. Dazu gehört noch „/grml/sysresc_loop.cfg“, das als Ersatz für „/boot/grub/loopback.cfg“ dient. Die Beispieldateien können Sie über *https://m6u.de/mubo* herunterladen.

In unseren Konfigurationsdateien finden Sie außerdem Optionen für Gparted Live und das LinuxWelt-Rettungssystem sowie Anpassungen für Ubuntu 22.04, damit das System gleich mit deutschsprachiger Oberfläche startet. ■

Öffnen — 42_grml — /etc/grub.d — Speichern

```
115 if [ "$grml" = "systemrescue-9.02-amd64.iso" ]; then
116   cat << EOF
117 menuentry "${title}" {
118 ${grub_prep}
119         iso_path="${rel_dirname%/}/${grml}"
120         export iso_path
121         rmmod tpm
122         configfile /grml/sysresc_loop.cfg
123 }
124 EOF
125 else
126   cat << EOF
127 menuentry "${title}" {
128 ${grub_prep}
129         iso_path="${rel_dirname%/}/${grml}"
130         export iso_path
131         kernelopts=" $CUSTOM_BOOTOPTIONS $additional_param "
132         export kernelopts
133         # support booting recent GRUB versions on UEFI systems
134         rmmod tpm
135         loopback loop "${rel_dirname%/}/$grml"
136         set root=(loop)
137         configfile /boot/grub/loopback.cfg
138 }
139 EOF
140 fi
141 done
```

Öffnen — sysresc_loop.cfg — /grml — Speichern

```
1 menuentry " System Rescue 9.0.2 (64 Bit) - Normaler Start" {
2     probe -u $root --set=rootuuid
3     set imgdevpath="/dev/disk/by-uuid/$rootuuid"
4     loopback loop $iso_path
5     probe -l loop --set=isolabel
6     linux  (loop)/sysresccd/boot/x86_64/vmlinuz scandelay=1 archisolabel=$isolabel
  img_dev=$imgdevpath img_loop=$iso_path archisobasedir=sysresccd iomem=relaxed setkmap=de
7     initrd (loop)/sysresccd/boot/intel_ucode.img (loop)/sysresccd/boot/amd_ucode.img (loop)/
  sysresccd/boot/x86_64/sysresccd.img
8 }
```

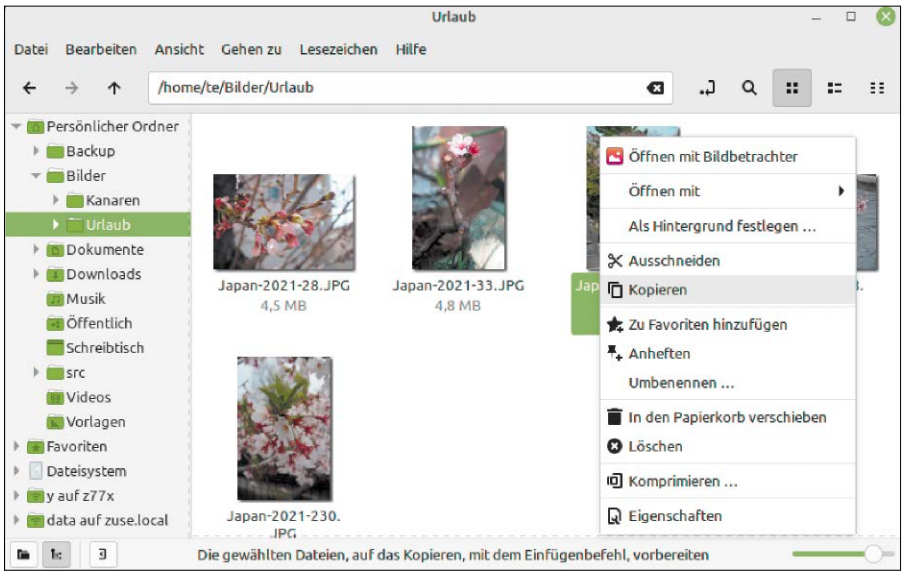
Reiner Text — Tabulatorbreite: 8 — Z. 6, Sp. 112 — EINF

Individuelle Grub-Konfiguration: Für einige Distributionen sind Anpassungen im der Datei „42_grml“ nötig. System Rescue beispielsweise lässt sich ansonsten nicht aus einem ISO starten.

Dateien und Ordner organisieren

Der Umgang mit Dateien und Ordnern gehört zum PC-Alltag. Die Linux-Dateimanager sind den meisten Aufgaben gewachsen, mit ein paar Tricks und zusätzlichen Werkzeugen lässt sich jedoch einiges optimieren.

VON THORSTEN EGGELING



Für die meisten Benutzer ausreichend: Ein Dateimanager wie Nemo (Linux Mint) ist das komfortabelste Tool, wenn es darum geht, Dateien zu kopieren oder umzubenennen.

Für Backups müssen Dateien oder Ordner kopiert, für eine Neuorganisation verschoben oder je nach Inhalt sinnvoll umbenannt werden. Im Dateimanager lässt sich das komfortabel erledigen, entweder über Menüpunkte oder Tastenkombinationen. Wer gerne mit der Maus arbeitet, kann auch Drag & Drop verwenden. Man spart einiges an Mühe und findet Dateien schneller wieder, wenn man sich ein sinnvolles Ablagesystem überlegt. Wie stellen Tools vor, die Sie dabei unterstützen. Das Meiste kann man jedoch mit Bordmitteln bewältigen, entweder im Dateimanager oder im Terminal.

Elemente im Dateisystem

Das Dateisystem orientiert sich an Arbeitsweisen, die schon vor Einführung des Computers galten. In jedem gut organisierten Haushalt oder Büro stehen Aktenhefter, in denen man Dokumente ablegt. Dem entsprechen auf dem PC Ordner und Dateien. Die deutschsprachigen Bezeichnungen „Datei“ und „Verzeichnis“ beschreiben den Gegenstand nur ungenau, weil diese ursprünglich eher für eine Sammlung zusammengehöriger Daten beziehungsweise Inventarlisten verwendet wurden.

Deswegen ist es passender, zunächst nur von Elementen im Dateisystem zu sprechen, von denen es zwei gibt. Das eine heißt „Verzeichnis“ (Synonym: „Ordner“) und kann mehrere Elemente enthalten (Verzeichnisse und Dateien).

Das andere wird als „Datei“ bezeichnet und es enthält Daten wie Text, Tabellen oder Videoinhalte. Für Basisoperationen wie Kopieren, Verschieben oder Umbenennen spielt es jedoch keine Rolle, ob es sich bei einem Element um eine Datei oder einen Ordner handelt.

Unter Linux gibt es die Besonderheit, dass auch Geräte Elemente im Dateisystem sind. Eine Festplatte lässt sich beispielsweise über „/dev/sda“ ansprechen („device file“). Diese Dateien dienen Programmen als Schnittstelle zum Gerät, der Benutzer sollte sie nicht direkt verwenden.

Unterhalb von „/sys“ und „/proc“ erstellt der Kernel automatisch Ordner und Dateien in einem virtuellen Dateisystem. Darüber lassen sich Informationen zur Hardware auslesen. Im Terminal liefert beispielsweise

```
cat /proc/cpuinfo
```

jederzeit aktuelle Daten zum Prozessor. Einige Dateien sind auch beschreibbar, um Optionen für Kernel oder Treiber temporär zu setzen. Von diesen speziellen Fällen abgesehen, sollte man in diesen Ordnern nichts ändern oder löschen.

Effektiv mit dem Dateimanager arbeiten

In fast allen Linux-Dateimanagern gelten dieselben Tastenkombinationen und auch die Kontextmenüs von Dateien und Ordner schauen ähnlich aus. Mit Strg-C kopieren Sie ein Element des Dateisystems und mit Strg-V fügen Sie es ein. Nach einem rechten Mausklick sind die entsprechenden Menüpunkte „Kopieren“ und „Einfügen“ zu sehen. Strg-C wirkt sich auf das zuvor angeklickte Element aus, mit Mausklicks bei gedrückter Strg-Taste lassen sich mehrere Dateien oder Ordner markieren. Strg-A

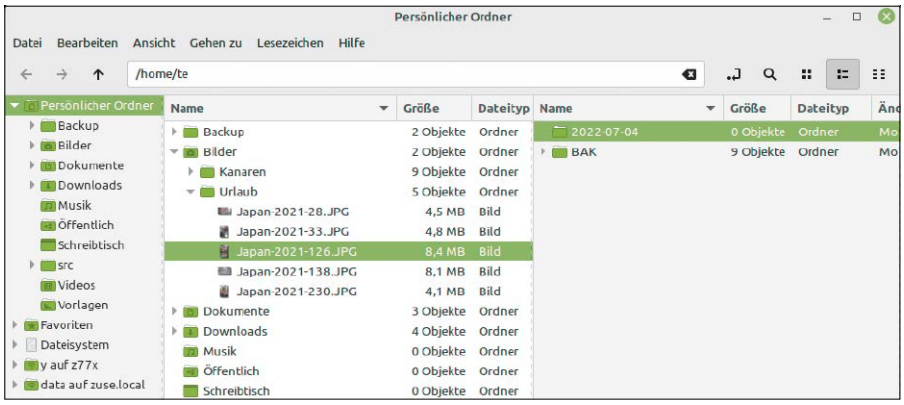
markiert alle Elemente. Verwenden Sie Strg-X statt Strg-C, wenn Sie Elemente verschieben wollen. Danach wechselt man in den Zielordner, in den man alles mit Strg-V einfügt.

Für den Datenaustausch dient bei Strg-C/Strg-V die Zwischenablage. Die Operationen finden nur im Hauptspeicher statt, wobei nicht die tatsächlichen Dateien, sondern nur Verweise kopiert werden. Sonst wäre der Speicher bei großen Dateien schnell voll. In der Zwischenablage landet im Wesentlichen nur Text. Wenn Sie im Dateimanager eine Datei mit Strg-C kopieren und dann in einem Texteditor Strg-V drücken, wird daher der Dateiname inklusive Pfad eingefügt. Wurden mehrere Elemente kopiert, speichert die Zwischenablage eine Liste der Pfade und Dateinamen. Eine Ausnahme sind Bilder, die Sie mit Strg-C in einem Bildbearbeitungsprogramm kopieren. Die Zwischenablage enthält dann das Bild, nicht nur den Verweis.

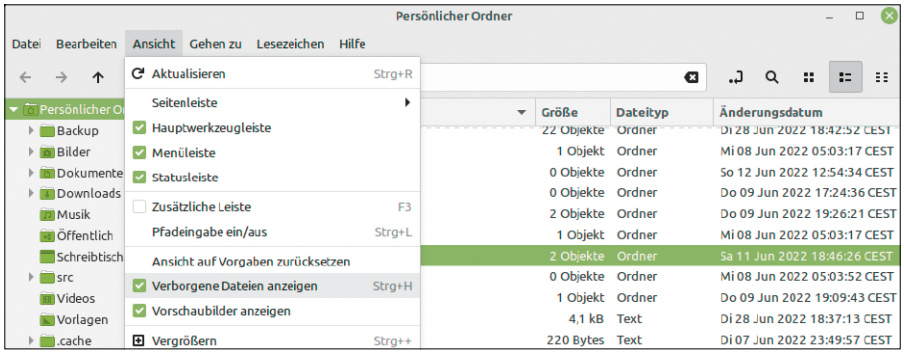
Mehrere Fenster nutzen: Kopieraktionen lassen sich bequemer durchführen, wenn Sie zwei Fenster des Dateimanagers öffnen. Nutzer von Ubuntu und Linux Mint verwenden dafür die Tastenkombination Strg-N. In einem Fenster wechseln Sie zum Quellverzeichnis und im anderen zum Zielverzeichnis. Sie müssen dann nicht umständlich zwischen den Ordnern navigieren. Außerdem lassen sich Elemente einfach mit der Maus in das andere Fenster verschieben. Wenn Sie dabei die Strg-Taste gedrückt halten, werden die Dateien kopiert. Liegt das Zielverzeichnis auf einem anderen Laufwerk, wird die Datei per Drag & Drop kopiert. Im Ubuntu-Dateimanager (Nautilus) halten Sie dabei die Strg- und Shift-Taste gedrückt, wenn Sie eine Datei verschieben wollen. Beim Dateimanager von Linux Mint (Nemo) genügt die Shift-Taste.

Als Alternative kann man in fast allen Linux-Dateimanagern mit Strg-T Tabs öffnen, in denen Sie sich unterschiedliche Ordner anzeigen lassen. Per Drag & Drop auf die Titelleiste eines Tabs verschieben Sie Ordner oder Dateien. Halten Sie dabei die Strg-Taste gedrückt, wenn Sie die Elemente kopieren wollen. Beim Linux-Mint-Dateimanager öffnet die F3-Taste eine geteilte Ansicht, was zielgenaues Drag & Drop auch in ein Unterverzeichnis ermöglicht.

Hinweis: Ordner und Dateien im Home-Verzeichnis, deren Namen mit einem Punkt beginnen, enthalten Konfigurationsdaten.



Zwei-Panel-Ansicht: Der Dateimanager von Linux Mint bietet eine geteilte Ansicht. Man muss dann nicht umständlich in den Zielordner wechseln und Drag & Drop wird vereinfacht.



Alles sehen im Dateimanager: Wenn Sie versteckte Konfigurationsdateien und Ordner kopieren wollen, müssen Sie sich die verborgenen Dateien anzeigen lassen.

Diese zeigt der Dateimanager standardmäßig nicht an. Um das zu ändern, hilft ad hoc der Hotkey Strg-H, dauerhaft die Einstellung „Verborgene Dateien anzeigen“.

Umbenennen nach Muster

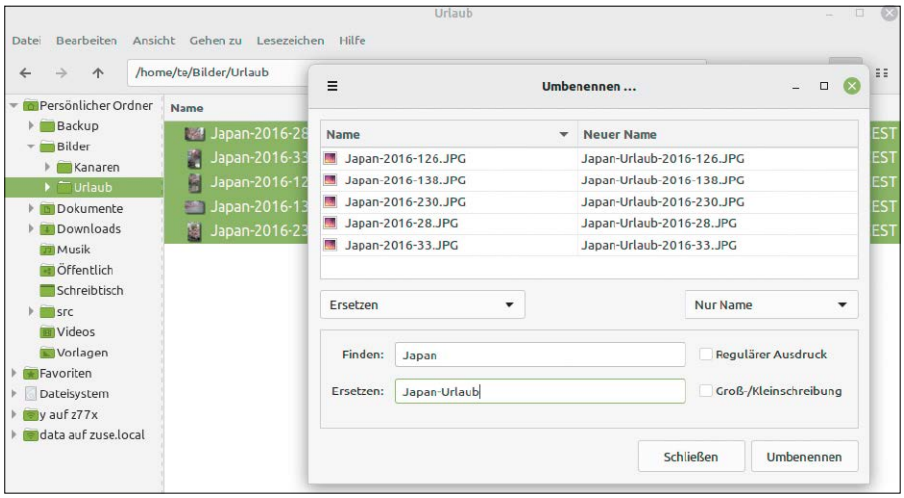
Im Dateimanager lässt sich der Name von Dateien und Ordnern über die Taste F2 oder den Kontextmenüpunkt „Umbenennen“ ändern. Sind mehrere Elemente ausgewählt, zeigen die Dateimanager von Ubuntu und Linux Mint einen Dialog für die Mehrfachumbenennung. Sie können beispielsweise Teile der Dateinamen ersetzen oder Text hinzufügen. Es erscheint eine Vorschau mit dem Ergebnis, ein Klick auf „Umbenennen“ führt die Änderungen durch. Wem dieser Funktionsumfang nicht ausreicht, der installiert mit

```
sudo apt install gprename
```

ein zusätzliches Tool. Gprename zeigt in der linken Spalte einen Ordner-Browser und rechts davon die Dateiliste. Die Funktionen zum Umbenennen befinden sich im unteren Bereich. Neben Schaltern wie „Alles klein“ gibt es unter „Ersetzen/Löschen“ eine Ersetzungsfunktion, die reguläre Ausdrücke versteht.

DATEIEN PER FILTER AUSWÄHLEN UND KOPIEREN

Die Suchfunktion (Strg-F) der Dateimanager von Ubuntu und Linux Mint arbeitet wie ein Filter. Sie können damit die Sicht auf einen Zweig des Dateisystems gemäß bestimmter Kriterien einschränken. Die Suchmaske kann eine Dateinamenserweiterung wie „jpg“ oder „pdf“ sein oder ein Teil des Dateinamens. Wenn Sie die Bezeichnungen mit Datum und Stichwörtern ergänzt haben, lassen sich beispielsweise Elemente mit einem bestimmten Stichwort einfach finden. Die Dateiliste im Suchergebnis können Sie mit Strg-A auswählen und die Dateien dann wie gewohnt kopieren, verschieben oder löschen.



Dateien umbenennen: Sind mehrere Dateien markiert, öffnet sich bei „Umbenennen“ ein Fenster, über das sich Dateinamen oder Namensteile suchen und ersetzen lassen.

Der KDE-Dateimanager Dolphin bietet nur die Umbenennung mit einem neuen Namen und die automatische Nummerierung. Für KDE ist daher das Tool Krename empfehlenswert, das sich mit

```
sudo apt install krename
```

installieren lässt. Über „Hinzufügen“ wählen Sie die Elemente aus, die Sie umbenennen möchten. Auf der Registerkarte „4. Dateiname“, stellen Sie unter „Einfacher Dateiname“ Präfix und Suffix ein. Über die Schaltfläche mit dem „i“ in einem Kreis wählen Sie jeweils die passende Funktion, beispielsweise „[date]“ für das aktuelle Datum. Auf der Registerkarte „Fortgeschrittenen-Modus für Dateinamen“ sehen Sie die Variablen hinter „Vorlage:“. Die Zeile lässt sich bei Bedarf anpassen. Eine Vorschau zeigt das zu erwartende Ergebnis, erst der Klick auf „Fertigstellen“ führt die Änderungen durch.

Dateien und Ordner strukturiert ablegen

Wenn viele persönliche Dateien auf der Festplatte liegen, sollte man über ein strukturiertes Ablagesystem nachdenken. Die Linux-Standardinstallation liefert dafür mit Ordnern für unterschiedliche Dateitypen wie „Dokumente“, „Bilder“ und „Videos“ bereits eine Vorlage. Wie man weiter vorgeht, hängt von den eigenen Vorlieben ab. Aussagekräftige Bezeichnungen für Ordner und Dateien können ein Baustein sein.

Karl Voit hat sich in seinem Blog (*https://karl-voit.at*) einige Gedanken zur effektiven Dateiablage gemacht. Seine einfache Methode: Man bringt Datum und Stichwörter („tags“) in Datei- und/oder Ordnernamen unter, was man manuell durch Umbenennen erledigen kann. Ein gewünschtes Element lässt sich dann über die Navigation im Dateimanager, aber auch über die Suchfunktion schneller finden. Zur Vermeidung von Fehlern und zur Vereinfachung sollte man das Python-Script „date2name“ (*https://github.com/novoid/date2name*) verwenden. Zur Vorbereitung installieren Sie im Terminal

```
sudo apt install python3-pip
```

Das Tool lässt sich dann mit

```
pip3 install date2name
```

im Home-Verzeichnis im Verzeichnis „.local/bin“ installieren, das Sie mit

```
source ~/.profile
```

in den Suchpfad aufnehmen. Mit der Zeile

```
date2name [Dateiname]
```

baut das Script das Änderungsdatum am Anfang des Dateinamens ein. Ersetzen Sie den Platzhalter durch den Namen der Datei. Ein weiteres Tool (*https://github.com/novoid/filetags*) installiert dieser Befehl

```
pip3 install filetags
```

und der Aufruf erfolgt so:

```
filetags [Dateiname]
```

Danach tippen Sie das gewünschte Stichwort ein und bestätigen mit der Eingabetaste. Mehrere Stichwörter lassen sich mit Leerzeichen getrennt vergeben. Der resultierende Dateiname kann dann beispielsweise so aussehen:

```
2022-07-04 Artikel_Dateien –
  entwurf.odt
```

Scripts in den Dateimanager einbauen: Für mehr Komfort startet man solche Tools über den Dateimanager. Erstellen Sie eine Textdatei mit dem Namen „date.sh“ und diesem Inhalt (zwei Zeilen):

```
#! /bin/bash -e
$HOME/.local/bin/date2name "$@"
```

Machen Sie die Datei mit

```
chmod +x date.sh
```

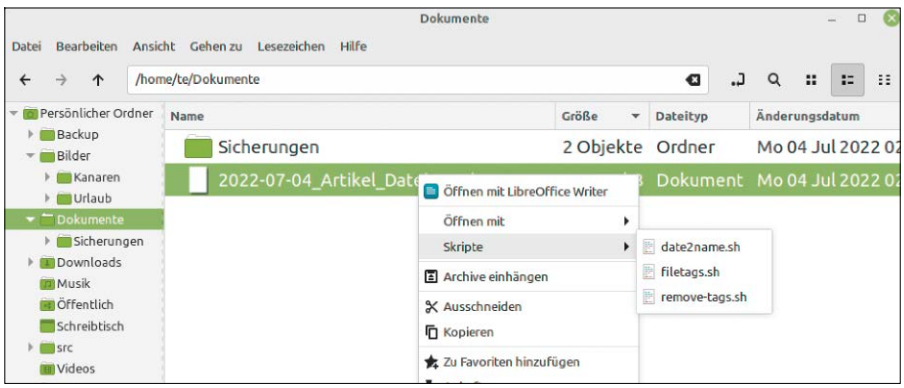
ausführbar. Eine zweite Textdatei erhält den Namen „filetags.sh“ mit diesem Inhalt (zwei Zeilen):

```
#! /bin/bash -e
gnome-terminal -- python3 $HOME/.
  local/bin/filetags "$@"
```

In einer dritten Datei „remove-tags.sh“ ändern Sie die zweite Zeile in

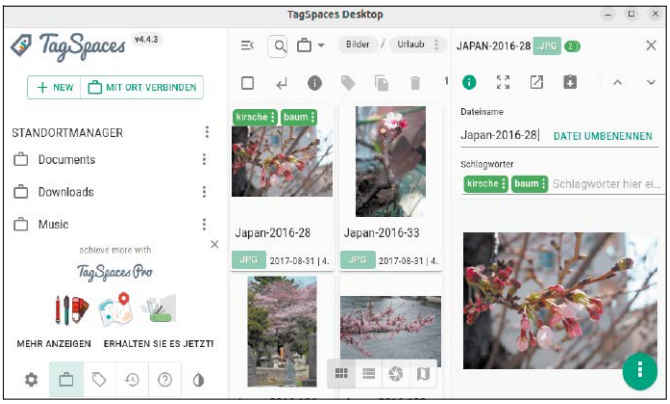
```
gnome-terminal -- python3 $HOME/.
  local/bin/filetags --remove "$@"
```

Machen Sie auch diese Dateien ausführbar und verschieben Sie alle Dateien in den Ordner „.local/share/nautilus/scripts“ (Linux Mint: „.local/share/nemo/scripts“). Klicken Sie eine Datei im Dateimanager mit der rechten Maustaste an und wählen Sie im Kontextmenü „Scripte → date2name.sh“, um das Datum in den Namen einzubauen. Nach dem Klick auf „Scripte → filetags.sh“ öffnet sich ein Terminal, über das Sie Stichwörter vergeben. Mit „Scripte → remove-tags.sh“ entfernen Sie Stichwörter.



Dateien einheitlich kennzeichnen: Die Tools date2name und filetags kann man über ein Script in den Dateimanager einbauen und dann Datum und/oder Stichwörter in die Namen einsetzen.

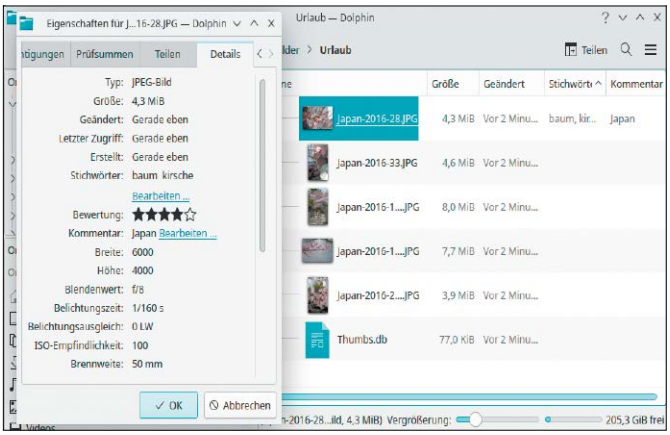
Tipp: Der Dateimanager Tagspaces (*www.tagspaces.org*) arbeitet nach einem ähnlichen Prinzip. Auch er baut die Begriffe einfach in den Dateinamen ein und zeigt Vorschaubilder inklusive der vergebenen Schlagwörter. Über die Suchfunktion lassen sich Dateien mit bestimmten Schlagwörtern schnell finden.



Alternativer Dateimanager: Tagspaces kann Stichwörter in Dateinamen einbauen und auch wieder entfernen. Die Stichwörter lassen sich für die Suche nutzen.

Dateimanager mit Stichwortfunktion

Im KDE-Dateimanager Dolphin lassen sich Elemente im Dateisystem mit Metadaten verknüpfen. Zur Verfügung stehen Stichwörter, Kommentare und Bewertungen. Die Metadaten kann man jedoch erst verwenden, wenn die Inhalte in den Suchindex aufgenommen werden. Dazu rufen Sie die „Systemeinstellungen“ auf, gehen auf „Suchen → Dateisuche“, setzen Häkchen vor „Dateisuche aktivieren“ und „Auch Dateiinhalt indizieren“. Danach klicken Sie auf „Anwenden“. Nur Dateien in Ihrem Home-Verzeichnis werden indiziert. Über „Ordnereinstellung hinzufügen“ lassen sich weitere Ordner angeben.



KDE-Dateimanager Dolphin: In den Eigenschaften einer Datei können Sie Stichwörter unterbringen, die der Dateimanager anzeigt und nach denen Sie bei der Suche filtern können.

Im Dateimanager klicken Sie einen Ordner oder eine Datei mit der rechten Maustaste an und gehen auf die Registerkarte „Details“. Hier können Sie jeweils nach einem Klick auf „Hinzufügen“ Stichwörter und Kommentare festlegen. Hinter „Bewertung:“ klicken Sie auf eines der Sternchen. Die Metadaten sind im Dateimanager in der Detailansicht (Strg-3) zu sehen. Nach einem rechten Mausklick auf den Spaltenkopf können Sie angeben, welche Spalten Sie sehen wollen.

Mit Strg-F blenden Sie die Suchleiste ein. Ist die Registerkarte „Dateiname“ aktiv, sucht Dolphin nach Dateien und Ordnern, deren Name den Suchbegriff enthält. Aktivieren Sie die Registerkarte „Inhalt“, wenn Sie auch den Dateiinhalt durchsuchen möchten. Nach einem Klick auf „Beliebige Bewertung“ fügen Sie Bewertungen als Suchkriterium hinzu. Unter „Stichwörter hinzufügen“ setzen Sie Häkchen vor die Stichwörter, auf die Sie die Suche einschränken wollen.

Mit Dateien im Terminal arbeiten

Im Terminal versprechen Tools wie cp (kopieren) oder mv (verschieben) nicht besonders viel Komfort. Mit den richtigen Optionen sind es zwar mächtige Werkzeuge, für Gelegenheitsnutzer aber nur eingeschränkt zu empfehlen. Der Zugang zum Terminal-Dateimanager Midnight Commander erschließt sich dagegen schneller. Installieren Sie den Klassiker mit

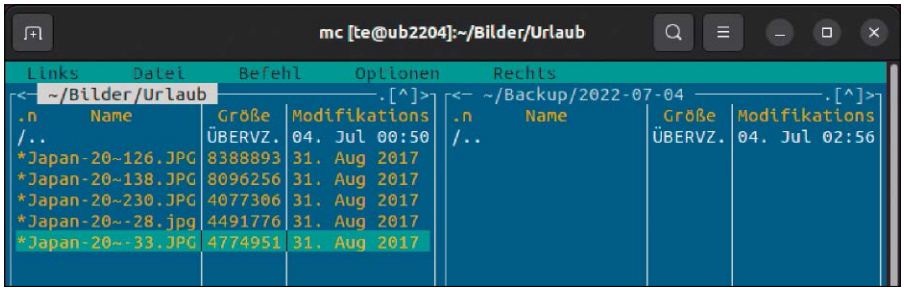
```
sudo apt install mc
```

und starten Sie ihn mit diesem Befehl:

```
mc
```

Das Programm zeigt zwei Panels, in denen sich zwei unterschiedliche Ordner darstellen lassen. Mit der Tab-Taste wechseln Sie zwischen den Panels und navigieren mit den Cursortasten und der Eingabetaste. Mit F5 kopieren Sie das markierte Element in den Ordner, den das andere Panel anzeigt. Drücken Sie mehrfach die Taste Einfg, wenn Sie mehrere Elemente markieren möchten. Die F6-Taste dient zum Verschieben, F8 zum Löschen und mit F7 erstellt man neue Ordner. Alle F-Tasten-Befehle sind am unteren Rand zu sehen und lassen sich auch mit der Maus klicken.

Den Umgang mit dem Terminal erleichtert der Midnight Commander ebenfalls. Mit Alt-Enter fügen Sie den Namen der markierten Datei in die Eingabezeile ein. Strg-O blendet den Midnight Commander aus und zeigt das Terminal. Sie können die Befehlszeile bearbeiten und beispielsweise den Namen eines Tools voranstellen, mit dem Sie die Datei öffnen möchten. Mit Strg-O kehren Sie zum Midnight Commander zurück. ■



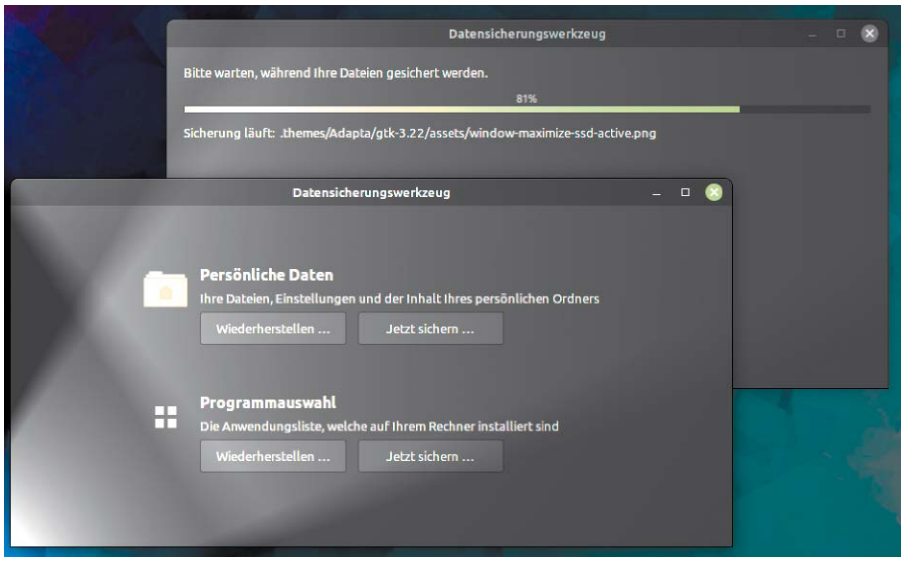
Im Terminal arbeiten: Midnight Commander eignet sich für die schnelle Navigation im Dateisystem. In der Zwei-Panel-Ansicht lassen sich Dateien bequem in andere Ordner kopieren.

Backups: Grundlagen und Tipps

Datensicherung ist unbeliebt, aber ein notwendiges Übel jeder großen wie kleinen IT-Infrastruktur. Mit den richtigen Tools kostet nur die erste Einrichtung Zeit. Danach läuft das Meiste automatisch ab. Lediglich Mobilgeräte verlangen manuelle Arbeit.

VON HERMANN APFELBÖCK

Wer seiner Hardware, seinem Betriebssystem und sich selbst ohne Rückversicherung vertraut, ist naiv oder faul oder beides. Die Katastrophe kann sich Zeit lassen, aber sie kommt. Dabei gibt es Werkzeuge und Maßnahmen genug, um Benutzerdaten oder das gesamte System zu sichern. Es stellt sich nur die Frage, welchen Aufwand welche Daten verdienen. Dieser Beitrag stellt die unwiederbringlichen Benutzerdateien ins Zentrum – Texte, Buchhaltung, Tabellen, Fotos, Medien. Systemschutz und Konfigurationssicherung bleiben weitgehend außen vor.



Mintbackup: Funktionsarme Klick-Front-Ends wie dieses für Tar sind nur für absolute Anfänger. Für periodische Sicherung bleiben die Terminaltools erste Wahl.

Datensicherung: Tar oder Rsync?

Sie können es mit grafischen Werkzeugen wie Freefilesync (*https://freefilesync.org*), mit Déjà Dup (Ubuntu-Standard) oder mit Mintbackup (Mint-Standard) versuchen: Am Ende sind die unglaublich schnellen und weit funktionsreichen Kommandowerkzeuge Tar und Rsync doch die beste Wahl für die Datensicherung. Einmal den richtigen Befehl recherchiert, läuft die Sicherungsroutine künftig nach einer knappen Alias-Eingabe oder sogar als Cronjob dauerhaft und zuverlässig.

Rsync hat den großen Vorteil, dass alle Daten auch auf dem Sicherungsziel uneingeschränkt verfügbar sind. Tar benötigt entweder das komplette Auspacken des Archivs oder einen Archivmanager für den Zugriff auf einzelne Dateiobjekte (File-Roller unter Gnome & Co., Ark unter KDE). Je nach Größe der Tar-Archive fordert das Laden im Archivmanager Zeit. Vorteile von Tar sind andererseits optionale, platzsparende Komprimierung und die Unabhängigkeit von Dateirechten, da diese ungeachtet der Dateisysteme auf Quelle und Ziel in das Archiv geschrieben werden. Wer Rechteproblemen aus dem Weg gehen will, sollte Tar verwenden. Streng genommen ist nur Tar ein echtes Backupwerkzeug, weil es die Daten in abgeschlossene Archive packt, während Rsync eine identische Datenhierarchie schafft und die Unterscheidung von Quelle und Ziel dem Nutzer überlässt.

Eine typische Tar-Aktion startet am besten immer im zu sichernden Verzeichnis (also vorher *cd […]*). Das erspart die Angabe des Quellordners (dann immer nur „.“), was bei Tar immer wieder Irritationen verursacht. Der Tar-Befehl selbst beginnt dann mit den maßgeblichen Optionen („-c“ für „create“, Schalter „-f“ für Zieldatei immer am Ende) und nennt dann das Zielarchiv:

```
cd ~
tar -czvf /media/lw/data/home.tar.
  gz .
```

Der Schalter „-z“ fordert optional, aber zu empfehlen, eine gzip-Komprimierung, denn Tar selbst ist eigentlich ein reiner Archivierer ohne Komprimierung. Schalter „-v“ macht den Vorgang gesprächiger.

Um ein Backup wieder zu entpacken, gehen Sie wieder zunächst mit *cd […]* in das Zielverzeichnis. Dann fordern Sie – wieder ohne Angabe des Zielordners – mit Schalter „x“ das Extrahieren an dieser Stelle:

```
cd ~
tar -xvzf /media/lw/data/home.tar.
  gz
```

Damit wird die Ordnerstruktur des Backups mit allen Dateien in den aktuellen Pfad entpackt. Beachten Sie, dass Tar gleichnamige Dateien ohne Rückfrage überschreibt. Aufgrund mancher Syntax- und Pfad-Sonderlichkeiten empfehlen wir Tar nur für schnelle platzsparende Backups wichtiger Ordner. Für periodische inkrementelle Sicherung großer Archive ist Rsync besser geeignet.

Datensicherung mit Rsync

Rsync macht eigentlich keine Backups, sondern gespiegelte Dateistrukturen, es komprimiert nicht und es erfordert etwas mehr Augenmerk auf die Dateirechte. Dennoch ist Rsync das beste Sicherungswerkzeug und hat für jeden Sonderfall eine Lösung. Rsync kennt zahlreiche Spezialoptionen, aber oft genügt der Sammelschalter „a“ (Archive), ergänzt durch „P“ (Progress), um ausreichend informiert zu werden:

```
rsync -aP /Quellpfad/ /Zielpfad
```

Dies berücksichtigt alle Unterverzeichnisse des Quellpfads. Beachten Sie beim Quellordner immer den abschließenden Slash (/). Für periodische Sicherungen zeitsparend ist Schalter „u“ (Update), also insgesamt „rsync -auP […]“. Der Updateschalter „u“ spart viel Zeit, indem er bereits bestehende Dateien überspringt.

Ein kompletter Beispielbefehl kann dann etwa so lauten:

```
rsync -auP /home/lw/ /media/lw/usb/
  backup
```

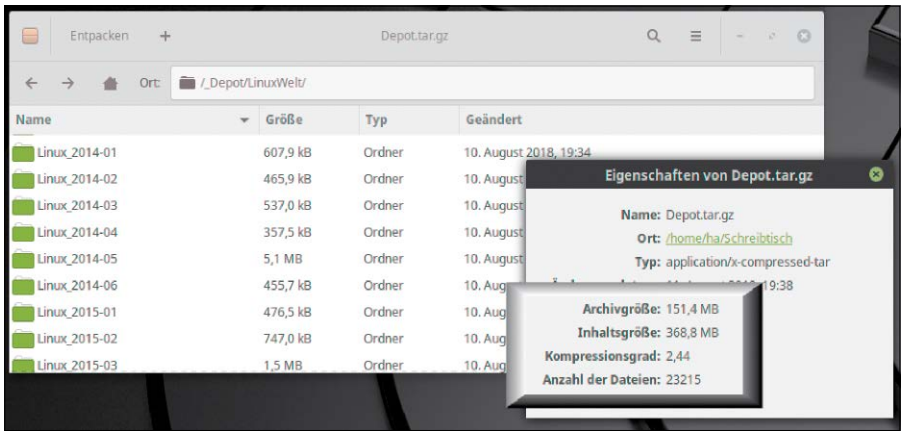
Das erste nach den Schalteroptionen angegebene Verzeichnis ist der Quellordner (mit Slash), das zweite das Backupziel. Das Beispiel geht davon aus, dass ein USB-Laufwerk mit dem Label „usb“ unter „/media/lw“ eingehängt ist. Das angegebene Verzeichnis („backup“) wird automatisch erstellt, falls es bei der allerersten Sicherung noch nicht existiert.

Eine 1:1-Spiegelung erzwingt der zusätzliche Schalter „--delete“:

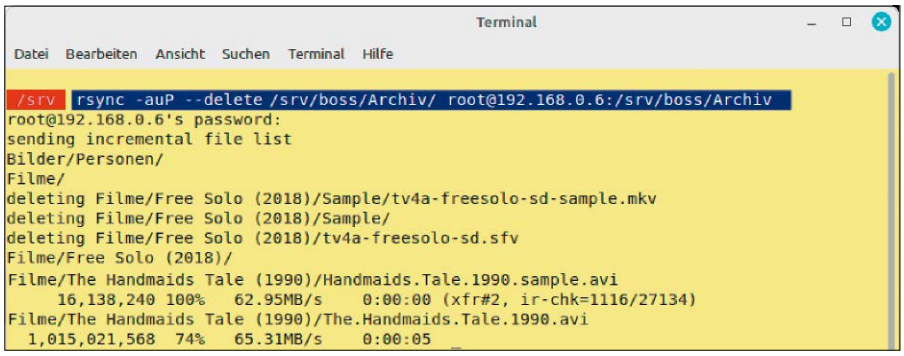
```
rsync -auP --delete /home/lw/ /
  media/lw/usb/backup
```

Was an der Quelle seit dem letzten Kopiervorgang gelöscht wurde, wird auch auf dem Ziel gelöscht – sehr praktisch, aber nicht ungefährlich: Verwenden Sie die Delete-Option nur, wenn das Ziel wirklich nur ein Backup ist, auf dem niemals produktiv gearbeitet wird. Im Zweifel ist ein vorheriger Testlauf mit „--dry-run“ nützlich:

```
rsync -auP --delete –dry-run /home/
  lw/ /media/lw/usb/backup
```



Komprimierte Backups mit Tar: „tar.gz“-Archive sind sehr schnell erstellt und mit grafischen Archivmanagern wie File-Roller oder Ark auch ohne Entpacken zu benutzen.



Spiegelsynchronisierung mit Rsync (hier mit SSH): Solche 1:1-Kopien mit „--delete“-Schalter sind nur zu empfehlen, wenn das Backupziel nie direkt bearbeitet wird.

Ein besonderer Vorteil von Rsync ist die Verbindung per SSH im Netzwerk. Die Sicherung folgt diesem Schema

```
rsync -auP lw@192.168.0.20:/home/
  lw/ /home/lw
```

oder mit

```
rsync -auP /home/lw/
  lw@192.168.0.20:/home/lw
```

in die andere Richtung.

Tipps zu Rsync und Datenorganisation

Ausnahmen, Sonderfälle und Optimierungsoptionen gibt es bei Backups zuhauf. Dieser Beitrag geht nur auf das Wichtigste ein:

Dateisysteme und Rechte: Quelle und Backupziel sollten idealerweise gleiche Dateisysteme verwenden: Beide rechtelos ist ebenso unproblematisch wie beide mit Linux-Rechten. Sichert man aber von Ext4 etwa auf exFAT, dann wird Rsync mit dem Archivschalter „a“ scheitern, weil es die Dateirechte nicht kopieren kann. In diesem Fall hilft der Rekursivschalter „r“, der auf die Rechtekopien verzichtet:

```
rsync -ruP […]
```

Exclude-Optionen: Gerade bei der Home-Sicherung fordern diverse Ordner Zeit und Platz, die gar keine Sicherung benötigen. Rsync hat auch dafür eine Lösung:

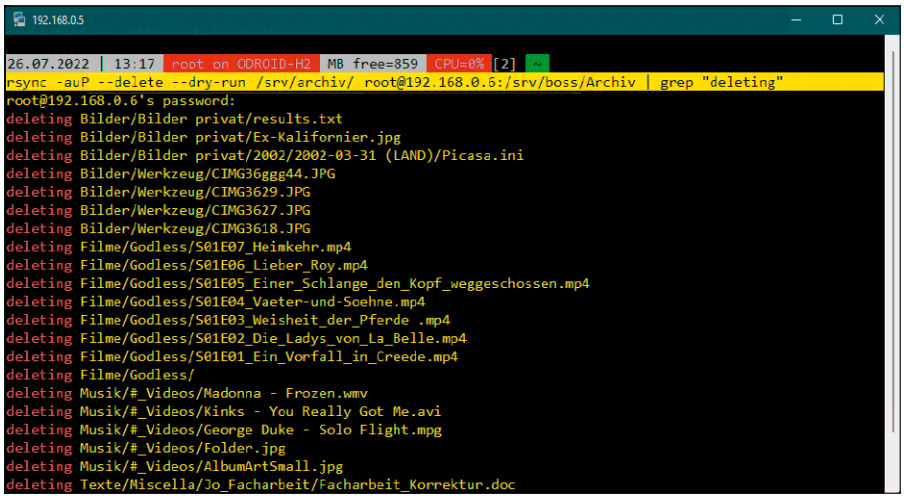
```
rsync -auP --exclude ".cache"
  --exclude ".mozilla" /home/lw/ /
  media/lw/usb/backup
```

Generell ist aber zu hinterfragen, ob die vorgesehenen Home-Ordner wie „Bilder“, „Dokumente“ (ähnlich wie „Eigene Dateien“ unter Windows) tatsächlich ideale Orte für Benutzerarchive sind. Backups und Datenübersicht sind einfacher, wenn alle wesentlichen Benutzerdaten auf einem eigenen Datenträger liegen.

Netzwerksicherung (SSH): Bei der Rsync-Sicherung via SSH wird natürlich interaktiv das Kontokennwort abgefragt. Um die Sicherung weitgehend (Alias) oder vollständig (Cronjob) zu automatisieren, können Sie die Passworteingabe durch Anmeldung mit Schlüsseldatei ersetzen. Mit

```
ssh-keygen
ssh-copy-id -i ~/.ssh/id_rsa.pub
  lw@192.168.0.6
```

erstellen Sie den Schlüssel auf dem lokalen



Rsync-Testlauf mit Schalter „--dry-run“: Was Rsync mit der Option „--delete“ ausrichten würde, können Sie vorab kontrollieren.

Rechner und kopieren dessen öffentlichen Teil zum SSH-Server. Ab der nächsten SSH-Anmeldung ist kein Passwort mehr erforderlich.

Automatisch mit Cronjob: Die SSH-Schlüsselanmeldung vorausgesetzt, lässt sich periodische Sicherung komplett automatisieren. Nach *crontab -e* genügt etwa folgender Eintrag (eine Zeile):

```
0 12 * *  * /usr/bin/rsync -ruP
 /srv/boss/Data/
 root@192.168.0.6:/srv/boss/Data
```

Zu empfehlen ist das aber nur, wenn das Backupziel zum angegebenen Zeitpunkt (hier täglich um 12:00 Uhr) garantiert erreichbar ist.

Rsync und Windows: Als SSH-Client kann auch Windows mit Rsync arbeiten, sofern dort ein Linux-Subsystem installiert ist. Den benötigten Windows-Pfad finden Sie im Subsystem unter „/mnt“, und folgender Beispielbefehl (eine Zeile)

```
rsync -ruP /mnt/d/Data/
 lw@192.168.0.6:/srv/boss/Data
```

würde dann den Ordner „D:\Data“ per SSH zum Server sichern.

CLOUD UND EIGENE DATENTRÄGER

Die Sicherung aller Benutzerdaten auf Cloudserver ist nicht nur Datenschutz-Frevel, sondern scheitert auch schlicht am Uploadtempo und am Speicherplatz. Selbst bezahlte Kontingente bei Dropbox, Google, Onedrive & Co. sind für heutige Datensammlungen kaum ausreichend. Externe USB-Festplatten sowie Platinenserver oder NAS-Geräte am Gigabit-Ethernet bieten hingegen Unabhängigkeit, informationelle Selbstbestimmung und optimales Übertragungstempo.

Einen unbestrittenen Vorteil haben Daten im Cloudspeicher allerdings: Sie bleiben auch dann erhalten, wenn Ihre Wohnung ausbrennt oder Rechner samt Backuphardware geklaut werden. Zwar rechnet niemand mit dem Schlimmsten, aber wo stehen Sie, wenn es doch eintritt?

Methode 1: Verwahren Sie neben der hauseigenen Sicherung einen zusätzlichen Sicherungsdatenträger an anderer Stelle, etwa am Arbeitsplatz im Büro oder bei regelmäßig besuchten Verwandten/Freunden. Bequem ist das nicht, denn den Datenbestand müssen Sie zumindest in gewissen Abständen (vierteljährlich?) aktualisieren. Ob es notwendig ist, den Datenträger an seinem Aufbewahrungsort zu verschlüsseln, müssen Sie selbst entscheiden.

Methode 2: Sie sichern besonders wichtige Daten zusätzlich auf einen Cloudspeicher. Das steht erst einmal in eklatantem Widerspruch zur Datenschutz-Disziplin, kann aber durch Verschlüsselung der Daten legitimiert werden. Als einfachste Methode eignet sich ein Packer wie 7-Zip mit Kennwortoption.

Mobilgeräte: Fotos und Videos sichern

Smartphones und Tablets unterstützen von Haus aus keine Sicherungsoptionen auf lokale PCs oder Server, sondern präferieren Kopien nach Google Drive oder in die iCloud. Das scheint bequem, ist aber weder schnell noch ökologisch noch datenschutzkonform. Sicherungen auf lokale Server oder PCS sind natürlich trotzdem möglich, allerdings nicht so bequem automatisierbar wie bei PCs und Notebooks.

Direktanschluss: Sichern und Auslagern von Benutzerdaten erfolgt technisch am schnellsten durch Anschluss des Mobilgeräts an PC oder Notebook per USB. Das verspricht schnellen Datendurchsatz und – zumindest bei Android-Geräten – guten Datenüberblick. Angeschlossene Mobilgeräte werden unter allen Betriebssystemen via MTP gemountet (Media Transfer Protocol). Sobald das Mobilgerät nach dem Anschluss die „Dateiübertragung“ (oder ähnlich) erlaubt, erscheint das Gerät als Massenspeicher im jeweiligen Dateimanager.

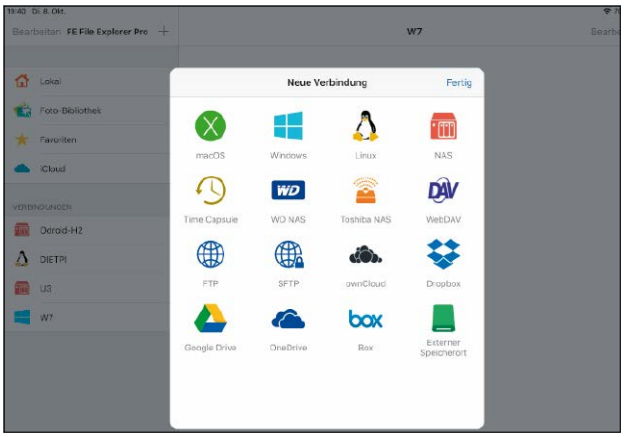
Den meisten Nutzern wird der manuelle, aber komfortable Maustransport im Dateimanager genügen. Massentransporte via Rsync (Linux) oder Robocopy (Windows) sind erschwert, weil Terminals das MTP-Protokoll nicht beherrschen. Wenn Sie das Terminal bevorzugen, ist Linux die bessere Wahl, weil hier das Mobilgerät unter „/var/run/user/1000/gvfs/[...]“ (Gnome & Co.) anzutreffen und daher auch für Rsync zu benutzen ist.

Auch iPhones und iPads lassen sich mit USB am PC anschließen, zeigen dabei aber nur die Mediendateien. Da Videos, Bilder und Musik aber die Hauptmenge der Benutzerdaten ausmachen dürften, lassen sich die meisten Daten des Mac-Geräts trotz dieses Filters effizient sichern.

WLAN und Smartphone-App: Der USB-Anschluss ist zwar der schnellste Übertragungsweg, trotzdem werden viele Nutzer den Weg über das WLAN bevorzugen. Hierfür ist zwar kein Mobilgerät standardmäßig gerüstet, aber es gibt eine ganze Reihe bewährter Apps. Da die Verbindung des Mobilgeräts zu einem heimischen Samba- oder SSH-Server den besten Kopierkomfort bietet, empfehlen wir den FE File Explorer. Die kostenlose Version ist arg beschränkt und die knapp fünf Euro für Apple-Geräte wie für Android sind für die Pro-Version gut angelegt. Ein lokaler Server ist mit dem Plus-

Symbol und Auswahl des Servertyps schnell eingerichtet: Die Optionen „Windows“, „MacOS“, „Linux“, „NAS“ meinen alle dasselbe – nämlich Samba/Windows-Freigaben. Außerdem gibt es SFTP (SSH), FTP und Webdav. Zum einmal mit Zugangsdaten eingerichteten Server gelangen die Daten dann über „Main Storage“, Markieren der Ordner oder Dateien und „Copy“. Dann erscheint die Auswahl des oder der eingerichteten Server und hier navigieren Sie dann weiter zum gewünschten Zielverzeichnis.

Unter Android für Sicherungen und Dateiarbeiten fast noch besser ist der kostenlose Total Commander, der per Plug-ins Samba, SFTP (SSH), FTP und Webdav beherrscht. Die benötigten Plug-ins (SFTP und Samba sollten genügen) müssen aus dem Google Store nachinstalliert werden und erscheinen dann im Hauptverzeichnis. Für jedes Plug-in wie etwa „SFTP“ oder „LAN (Windows-Freigaben“) können dann die Server inklusive Authentifizierungsdaten hinterlegt werden. Kopieren und Verschieben ist in der Zwei-Fenster-Ansicht zwischen dem lokalen Dateisystem des Mobilgeräts und dem entfernten Dateisystem des Servers denkbar einfach, sofern beide Fenster angezeigt werden (bei Smartphones nur bei horizontaler Nutzung). ■



Dateitransfer auf Samba, SFTP (SSH), FTP und Cloud: Für iPads und iPhones ist der FE File Explorer erste Wahl, unter Android der Total Commander fast noch besser.

LAUFWERKSIMAGES UND KLONEN

Laufwerkssicherung schließt alle Systemdaten inklusive Benutzerdateien ein, geht damit über Datensicherung weit hinaus und ist daher hier als Exkurs ausgegliedert. Als Backup sind Laufwerkimages kaum geeignet, weil sie periodisch wiederholt werden müssten. Es handelt sich um eine Systemschutzmaßnahme (Imagekopie) oder um den Umzug auf einen größeren Datenträger (Klonen).

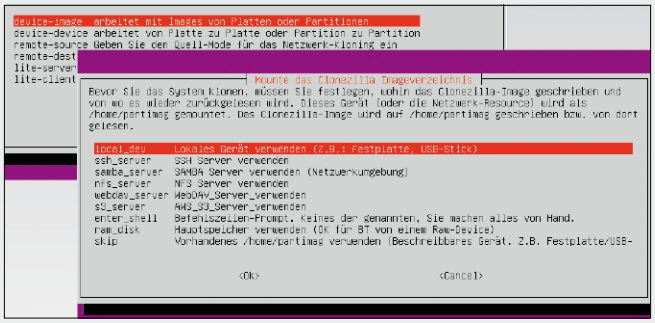
Einschlägige Werkzeuge sind die Livesysteme Rescuezilla und Clonezilla. Wir beschränken uns hier auf das umfassendere Clonezilla. Unter *https://clonezilla.org/downloads.php* gibt es mehrere Varianten. Wir empfehlen das Ubuntu-basierte „alternative stable“ (als „file type“ ISO wählen). Das Livesystem kann mit den üblichen Mitteln (Gnome-Disks, Etcher, Win 32 Disk Imager) auf USB-Stick kopiert werden.

Ist der Rechner mit dem zu kopierenden Datenträger mit Clonezilla gebootet, wählen Sie die erste Option „Clonezilla live“, danach „de-DE.UTF“ und deutsches Tastaturlayout. Nach einigen Standardfragen laden Sie im Fenster „Starte Clonezilla“ das eigentliche Tool.

Imagebackups: Dafür dient die oberste Option „device-image“ und danach „local_dev“, falls auf ein lokales (USB-)Laufwerk gesichert wird. Für eine Sicherung ins Netzwerk wählen Sie statt „local_dev“ das gewünschte Netzwerkprotokoll – also „samba_server“ oder „ssh_server“ (und weitere) – und geben IP-Adresse des Servers und Anmeldedaten an. Verwenden Sie den Modus „Beginner Einsteiger“ und die Option „savedisk“, sofern Sie ein Abbild der gesamten Festplatte erstellen möchten. Dies ist im Zweifel immer zu empfehlen, weil Clonezilla dann alle Partitionen inklusive Bootmanager sichert. Dabei spielt es keine Rolle, ob Windows, Linux oder beide installiert sind.

Imagewiederherstellung: Auch hier starten Sie Clonezilla mit „device_image“ und „local_dev“ (bei lokaler Sicherung). Wählen Sie die Partition und das Verzeichnis aus, in dem ein zuvor gesichertes Image liegt. Gehen Sie auf „Beginner“ und dann auf „restoredisk“ (wenn Sie einzelne Partitionen gesichert haben, verwenden Sie „restoreparts“). Clonezilla findet auf dem Backupmedium alle Abbilder und präsentiert sie in einer Liste. Danach wählen Sie die Zielpartition aus, in die das Image zurückgeschrieben werden soll.

Klonen: Dies schreibt den Inhalt eines Datenträgers direkt auf einen zweiten. Wichtig ist nur, dass der neue Datenträger gleich groß oder größer ist als das bisherige Laufwerk. Sie wählen zunächst „device-device“, dann „Beginner Einsteiger“ und anschließend „disk_to_local_disk“. Geben Sie zunächst den Datenträger an, den Sie kopieren wollen, danach das Ziellaufwerk. In den Folgedialogen übernehmen Sie mit Eingabetaste alle Voreinstellungen. Wenn der neue Datenträger größer ist als der ursprüngliche, dann bleibt nach dem Klonen hinter der letzten Partition ungenutzter Plattenplatz. Dies korrigieren Sie später unter Linux mit Gparted, unter Windows mit der Datenträgerverwaltung.



Clonezilla: Typischerweise arbeiten Sie mit Images (Bild oben) und mit lokalen Datenträgern (Bild unten). Zum direkten Klonen führt die Option „device-device“.

Einstellungen sichern und wiederherstellen

Nach einer Linux-Installation oder auf einem andern PC muss man nicht alles umständlich neu konfigurieren. Die bisherigen Einstellungen lassen sich übertragen. Das funktioniert für viele Programme auch beim Wechsel von Windows zu Linux.

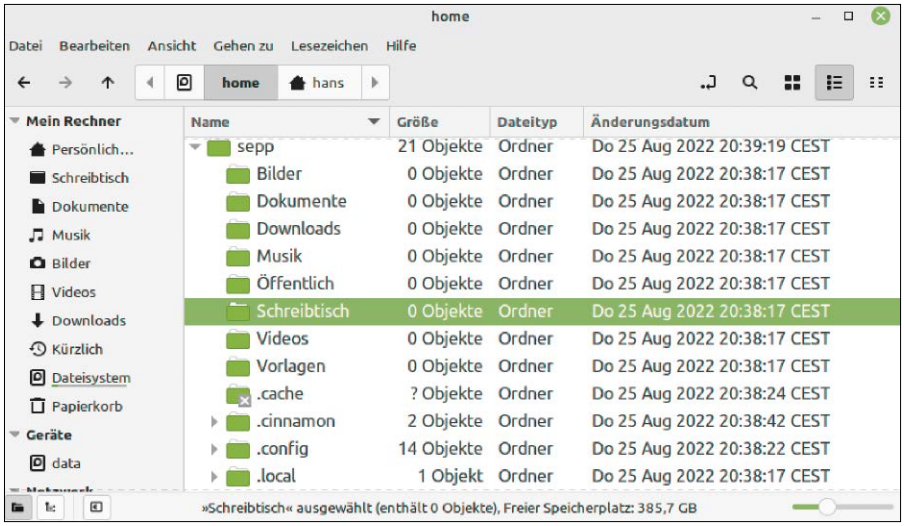
VON THORSTEN EGGELING

Die meisten Open-Source-Anwendungen legen ihre Einstellungen in einfachen Textdateien ab. Sie können die Dateien daher einfach kopieren und die gleiche Konfiguration auf einen anderen Rechner übertragen. Außerdem kann man die Dateien bei Bedarf auch in einem Texteditor öffnen, die Konfiguration einsehen und bearbeiten. Wenn auf allen PCs das gleiche Betriebssystem läuft oder die gleiche Version einer Linux-Distribution neu installiert wird, kann man es sich einfach machen. Ein Backup des Home-Verzeichnisses genügt. Die Wiederherstellung kann jedoch unerwünschte Folgen haben, wenn eine andere Desktopumgebung zum Einsatz kommt. Wenn möglich und ausreichend, sollten Sie daher besser gezielt nur die Konfigurationen der einzelnen Anwendungen sichern. Das gilt auch für die Übertragung von Einstellungen auf ein anderes Betriebssystem, beispielsweise von Windows auf Linux und umgekehrt.

Eine Grundregel: Verwenden Sie neuere Konfigurationsdateien nicht zusammen mit einer älteren Version der Software. Darauf sind die Programme nicht vorbereitet, was zu Fehlern oder Abstürzen führen kann. Ältere Konfigurationsdateien sollten hingegen keine Probleme bereiten, weil Programme diese Situation auch bei einem regulären Upgrade berücksichtigen.

Home-Verzeichnis sichern

Für den Umzug aller Einstellungen erstellen Sie ein Backup des Home-Verzeichnisses und stellen es auf einem anderen PC oder nach einer Linux-Neuinstallation wieder her.



Home-Verzeichnis: Im eigenen Verzeichnis sind nicht nur Benutzerdateien gespeichert, sondern auch alle Einstellungen für die Programme und die Desktopoberfläche.

Backup erstellen: Melden Sie sich bei der Desktopoberfläche ab, wechseln Sie mit der Tastenkombination Strg-Alt-F1 zu einer virtuellen Konsole (siehe Kasten „Virtuelle Konsolen nutzen“) und loggen Sie sich ein. Zwingend erforderlich ist das nicht, es gewährleistet aber, dass alle Dateien sicher im Backup landen – auch solche, die eventuell gerade geöffnet und gesperrt sind. Für ein einfaches Backup verwenden Sie diese Befehlszeile:

```
tar cvpf [/Backup-Ordner]/home.tar
  $HOME
```

Die Option „c“ sorgt dafür, dass tar ein neues Archiv erstellt, „v“ aktiviert ausführliche Meldungen und durch „p“ bleiben die Zugriffsrechte erhalten. „f“ steht für „File“, der nachfolgende Dateiname gibt das Zielverzeichnis an. Zuletzt folgt mit „$HOME“ das Verzeichnis, das gesichert werden soll. Die Shell ersetzt die Variable durch den Pfad zu Ihrem Home-Verzeichnis. Das tar-Archiv wird nicht komprimiert, was die Verarbeitung beschleunigt, jedoch größere Dateien erzeugt. Den Platzhalter „[/Backup-Ordner]“ ersetzen Sie durch den Zielordner. Das Dateisystem spielt keine Rolle. tar-Archive lassen sich problemlos auch auf NTFS- oder ExFAT-Partitionen sichern.

Wenn mehrere Benutzerkonten vorhanden sind, können Sie alle Home-Verzeichnisse zusammen sichern. Stellen Sie dem tar-Kommando ein „sudo“ voran und verwenden Sie statt „$HOME“ den Pfad „/home“ als Quellverzeichnis.

Archivgröße reduzieren: Dazu schließen Sie unnötige oder anderweitig gesicherte Ordner vom Backup aus und aktivieren die Komprimierung (Beispiel):

```
tar --exclude=.cache
```

```
--exclude=Downloads -cvpzf [/
Backup-Ordner]/home.tar.gz $HOME
```

„--exclude=[Ordner]“ bauen Sie so häufig wie nötig ein. Den Ordner „.cache“ können Sie immer ausschließen, andere Ordner wie „Downloads“, die eventuell viele Dateien enthalten, sichern Sie bei Bedarf getrennt. Die zusätzliche Option „z“ weist tar an, das Archiv mit Gzip zu komprimieren. Das drückt sich auch im Dateinamen aus, dem Sie ein „.gz“ anhängen.

Sicherung wiederherstellen: Auf einem anderen PC mit einer frischen Installation oder nach der Linux-Neuinstallation richten Sie Benutzerkonten mit den gleichen Bezeichnungen ein wie auf dem System, von dem das Backup stammt. Melden Sie sich bei der grafischen Oberfläche ab, wechseln Sie mit Strg-Alt-F1 zur virtuellen Textkonsole und melden Sie sich an. Mit den Befehlen

```
sudo mv /home /home.bak
cd /
sudo tar xvf [/Backup-Ordner]/home.
 tar
```

stellen Sie das oder die Home-Verzeichnisse aus dem Backup wieder her. Die erste Zeile benennt den bisherigen Ordner „/home“ um. Sollten sich darin bereits neue Dateien befinden, kopieren Sie diese später in das neue Home-Verzeichnis. Beachten Sie, dass tar Ordner mit relativen Pfadangaben sichert. Deshalb müssen Sie mit „cd /“ in das Wurzelverzeichnis wechseln.

Mozilla Firefox

Firefox speichert alle Benutzereinstellungen und Daten im Ordner „.mozilla“ im Home-Verzeichnis des Benutzers. Alle Ordner, die mit einem Punkt beginnen, sind versteckt und im Dateimanager nicht sichtbar. Um das zu ändern, gehen Ubuntu-Nutzer im Dateimanager Nautilus auf das Hamburger-Menü (drei horizontale Striche) und setzen ein Häkchen hinter „Verborgene Dateien anzeigen“. Unter Linux Mint gehen Sie im Dateimanager Nemo auf „Ansicht → Verborgene Dateien anzeigen“.

Firefox verwendet Profilordner unterhalb von „.mozilla/firefox“. Mit welchem Profil Firefox startet, ist in der Datei „.mozilla/firefox/profiles.ini“ festgelegt. Informationen zum Speicherort des Profilordners („Wurzelordner“) liefert der Browser über die URL „about:profiles“ in der Adresszeile. Per Klick auf „Ordner öffnen“ lassen Sie sich den Ordner im Dateimanager anzeigen. Hinter „Lokaler Ordner“ steht der Speicherort für den Dateicache, den Sie für ein Backup nicht berücksichtigen müssen.

```
te@teub20:~$ tar cvpf /media/te/0AD2-77DF/home.tar $HOME
tar: Entferne führende „/“ von Elementnamen
/home/te/
/home/te/mintupgrade-2022-08-25T190050.log
/home/te/.bashrc.001
/home/te/Musik/
/home/te/.xsession-errors
/home/te/Dokumente/
/home/te/Dokumente/LoremIpsum.odt
/home/te/.ssh/
/home/te/.ssh/known_hosts
/home/te/.xsession-errors.old
/home/te/Bilder/
/home/te/Bilder/Urlaub/
/home/te/Bilder/Urlaub/Japan-2016-126.JPG
/home/te/Bilder/Urlaub/Japan-2016-33.JPG
/home/te/Bilder/Urlaub/Japan-2016-28.JPG
```

Backup mit tar: Das Home-Verzeichnis sichert man am besten auf einem USB-Laufwerk in einer virtuellen Konsole. Dann besteht keine Gefahr, dass Dateien aktuell gesperrt sind.

Firefox ist bei neueren Ubuntu-Versionen als Snap-Paket installiert und der Profilordner ist im Home-Verzeichnis unterhalb von „snap/firefox/common/.mozilla/firefox“ zu finden. Firefox unter Windows verwendet das Verzeichnis „AppData\Roaming\Mozilla\Firefox\Profiles\“ im Ordner des Benutzers. Einstellungen speichert Firefox teilweise in Textdateien mit der Dateinamenserweiterung „.json“, aber auch in Sqlite-Datenbanken. Der Inhalt der Datenbanken lässt sich über ein Tool wie DB Browser for Sqlite betrachten (Paket: „sqlitebrowser“). Wer sich über die Funktion der einzelnen Dateien informieren will, geht auf *https://m6u.de/MOZP*.

Backup erstellen: Vor einem Backup beenden Sie den Browser. Sonst sind einige Dateien gesperrt und das Backup wäre unvollständig. Wenn Sie das Profil auf einen anderen Linux-PC übertragen wollen, können Sie den Ordner „.mozilla“ komplett sichern. Verwenden Sie dafür im Dateimanager den Kontextmenüpunkt „Komprimieren“. Wer die Kommandozeile bevorzugt, verwendet tar im Terminal, entsprechend wie im vorherigen Abschnitt für das Home-Verzeichnis beschrieben.

Es genügt allerdings auch, nur das eigentliche Profil zu sichern, beispielsweise „.mozilla/firefox/66sglt82.default-release“. Beim

VIRTUELLE KONSOLEN NUTZEN

Linux-Systeme für Desktopnutzer starten standardmäßig eine grafische Oberfläche. Bei Servern wird darauf meist verzichtet, weil sich das System unabhängig vom Standort über SSH fernwarten lässt. Sind Monitor und Tastatur angeschlossen, zeigt der Bildschirm eine virtuelle Konsole, über die sich Nutzer beim System anmelden können. In der Konsole startet eine Linux-Shell, in der sich wie in einem Terminalfenster der grafischen Oberfläche arbeiten lässt.

Virtuelle Konsolen gibt es auch bei Desktopsystemen. Von der grafischen Oberfläche aus gelangt man bei Debian, Ubuntu und Linux Mint mit den Tastenkombination Strg-Alt-F1 bis Strg-Alt-F6 zu den Konsolen eins bis sechs. In jeder kann man sich unabhängig voneinander anmelden. Von einer virtuellen Konsole aus genügt Alt-F1 bis Alt-F6 zum Wechsel in eine andere Konsole. Alt-F7 aktiviert wieder die siebte Konsole, in der die grafische Oberfläche läuft.

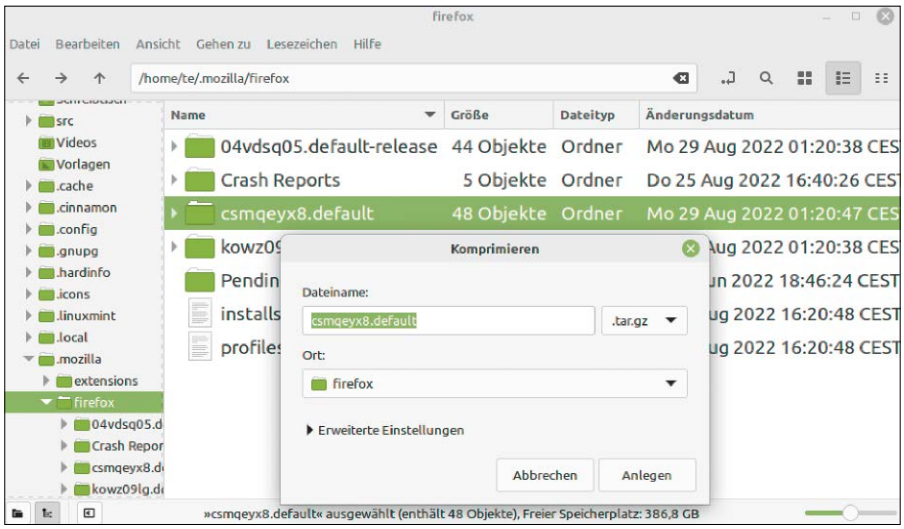
USB-Laufwerke werden in virtuellen Konsolen ohne vorherige Anmeldung bei der grafischen Oberfläche nicht automatisch eingebunden. Soll eine USB-Festplatte Ziel für ein Backup des Home-Verzeichnisses sein, ermitteln Sie zuerst den Gerätepfad:

```
lsblk -p
```

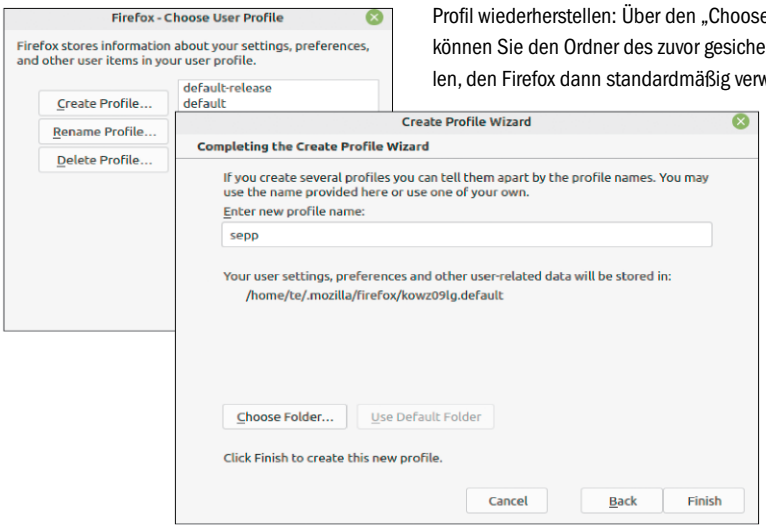
Lautet das Ergebnis beispielsweise „/dev/sdb2“, verwenden Sie diese Befehlszeile:

```
udisksctl mount -b /dev/sdb2
```

Bestätigen Sie den Befehl mit Ihrem Passwort. Das Laufwerk wird wie gewohnt unterhalb von „/media/[User]“ eingebunden.



Firefox-Profil: Im Dateimanager lässt sich der Profilordner bequem archivieren. Der Browser darf dabei nicht laufen, weil sonst nicht alle Dateien erfasst werden.



Profil wiederherstellen: Über den „Choose Profile Wizard“ können Sie den Ordner des zuvor gesicherten Profils wählen, den Firefox dann standardmäßig verwendet.

Umzug von Windows auf Linux oder umgekehrt ist das sogar empfehlenswert, weil Windows das Unterverzeichnis „Profiles“ verwendet und Linux nicht. Stellt man den kompletten „.mozilla“-Ordner wieder her, muss man sonst die Pfade umständlich in der Datei „profiles.ini“ anpassen.

Dateien wiederherstellen: Alleinige Linux-Nutzer benennen ein eventuell schon vorhandenes Verzeichnis „.mozilla“ um und entpacken die vollständige Sicherung in das Home-Verzeichnis.

Enthält das Backup nur den Profilordner, kopiert man diesen in den Ordner „.mozilla/firefox“, beziehungsweise bei Windows nach „AppData\Roaming\Mozilla\Firefox\Profiles“. Windows-Nutzer benötigen zum Entpacken von tar-Archiven die kostenlose Software 7-Zip (*www.7-zip.org*). Starten Sie dann den Browser im Terminal oder unter Windows nach Win-R so:

```
firefox -p
```

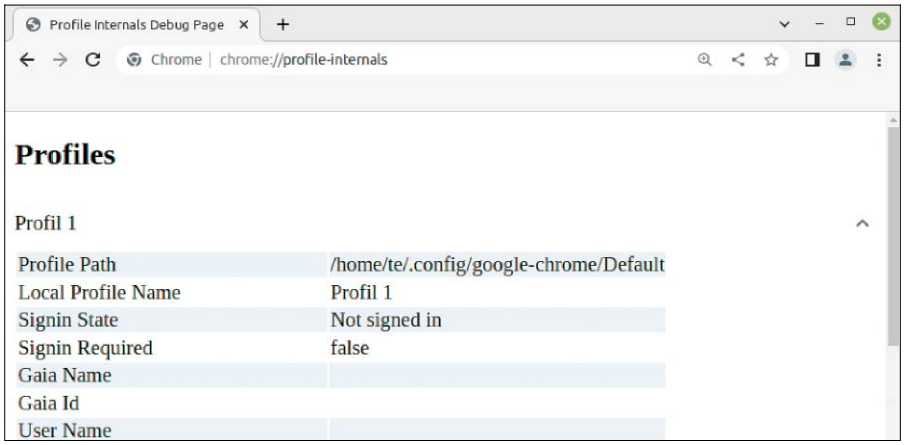
Es zeigt sich das Fenster „Firefox – Benutzerprofil wählen“ (oder „Choose User Profile“), in dem Sie auf „Create Profile“ klicken. Bei einigen Firefox-Versionen erscheint das Fenster auch mit deutschsprachigen Beschriftungen. Klicken Sie auf „Next“, tippen Sie eine aussagekräftige Bezeichnung für das Profil ein und klicken Sie auf „Choose Folder“. Wählen Sie den Ordner, in den Sie das Profilverzeichnis entpackt haben. Sollten Sie den Ordner nicht sehen, wählen Sie im Kontextmenü „Verborgene Dateien anzeigen“. Zum Abschluss klicken Sie auf „Finish“ und dann auf „Start Firefox“.

Bitte beachten Sie, dass der Profilumzug nur funktioniert, wenn die gleiche oder eine höhere Firefox-Version installiert ist wie zuvor. Andernfalls akzeptiert ein älterer Browser das neuere Profil nicht und Sie müssen Firefox aktualisieren.

Besonderheiten beim Snap-Paket: Entpacken Sie bei der Wiederherstellung den Profilordner nach „snap/firefox/common/.mozilla/firefox“. Er lässt sich über die Profilauswahl („firefox -p“) einbinden wie zuvor beschrieben. Der Umzug klappt auch zwischen Snap- und DEB-Paket-Installationen und umgekehrt. Lediglich die Spracherweiterungen aktiviert Firefox nicht. Um das zu ändern, rufen Sie *https://addons.mozilla.org/de/firefox/language-tools* auf, klicken auf „Deutsch (DE) Language Pack“ und dann auf „Enable“.

Google Chrome

Google Chrome nutzt unter Linux den Ordner „.config/google-chrome“ und unter Windows „AppData\Local\Google\Chrome\



Wo liegt das Chrome-Profil? Die interne URL „chrome://profile-internals“ zeigt die vorhandenen Profile und den Speicherort unter „.config/google-chrome“.

User Data“ als Datenspeicher. Darin ist die allgemeine Browserkonfiguration abgelegt, das Standard-Benutzerprofil liegt im Unterverzeichnis „Default“. Weitere Profile wie „Guest Profile“ oder zusätzlich selbst erstellte Profile sind hier ebenfalls zu finden. Profilbezeichnungen und Speicherorte kann der Browser auch über die URL „chrome://profile-internals“ anzeigen.
Chrome speichert auch die Cachedaten im Benutzerprofil. Wer das Backup klein halten möchte, sollte den Cache vorher löschen. Dazu gehen Sie rechts oben im Dreipunkt-Menü auf „Weitere Tools → Browserdaten löschen“. Setzen Sie ein Häkchen vor „Bilder und Daten im Cache“, und klicken Sie auf „Daten löschen“.
Beenden Sie Google Chrome und erstellen Sie ein Backuparchiv, beispielsweise im Linux-Dateimanager über den Kontextmenüpunkt „Komprimieren“. Zur Wiederherstellung entpacken Sie das Archiv in den Konfigurationsordner.

Thunderbird

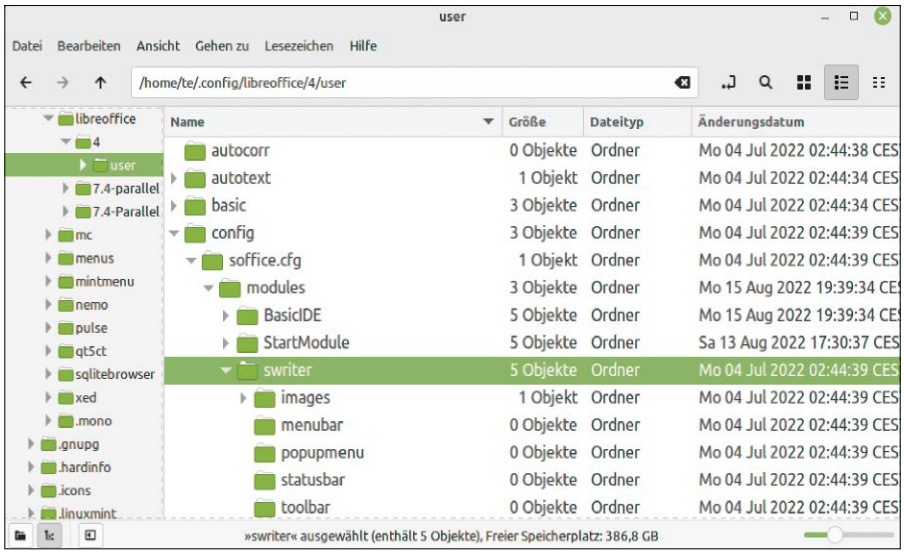
Das E-Mail-Programm legt seine Einstellungen im Home-Verzeichnis ab, unter Linux im Ordner „.thunderbird“. Die Windows-Version verwendet „AppData\Roaming\Thunderbird“. Die Struktur ist ähnlich wie bei Firefox, Details zu den Dateien und Ordnern erfahren Sie über *https://m6u.de/THUP*. Vor einem Backup schließen Sie das Programm und folgen der Anleitung für Firefox. Es genügt, den aktiven Profilordner zu sichern.
Für die Wiederherstellung kopieren Sie den Inhalt des Backuparchivs in Ihrem Home-Verzeichnis nach „.thunderbird“ beziehungsweise unter Windows nach „AppData\Roaming\Thunderbird“. Starten Sie dann Thunderbird so:

```
thunderbird -p
```

Klicken Sie auf „Next“, tippen Sie eine Bezeichnung für das Profil ein und klicken auf „Choose Folder“. Wählen Sie den Ordner, in den Sie das Profilverzeichnis entpackt haben. Zum Abschluss klicken Sie auf „Finish“ und dann auf „Start Thunderbird“.

Libre Office

Libre Office speichert die Benutzerkonfiguration seit Version 4.0 im Ordner „.config/libreoffice/4/user“, unter Windows in „AppData\Roaming\LibreOffice\4\user“. Mehrere Profile sind nicht vorgesehen. Es lassen sich jedoch bei Bedarf ältere und neuere



Libre-Office-Konfiguration: Das Büropaket speichert alle Einstellungen sowie Textbausteine und Wörterbücher im Ordner „.config/libreoffice/4/user“.

Versionen des Programms nebeneinander mit unterschiedlichen Profilen nutzen (siehe dazu auch den Artikel ab 58). Im Benutzerprofil speichert Libre Office im Ordner „config“ die Einstellungen für Symbolleisten und Menüleisten. „autotext“ nimmt Textbausteine auf, die Sie über „Extras → Autotext“ definiert haben, und in „wordbook“ liegen benutzerdefinierte Wörterbücher. Informationen zu den weiteren Ordnern können Sie über *https://m6u.de/LOPR* abrufen.
Vor einem Backup beenden Sie alle Office-Programme und sichern das Benutzerprofil beispielsweise mit (zwei Zeilen)

```
cd ~
tar cvpf [/Backup-Ordner]/LO.tar
  .config/libreoffice/4/user
```

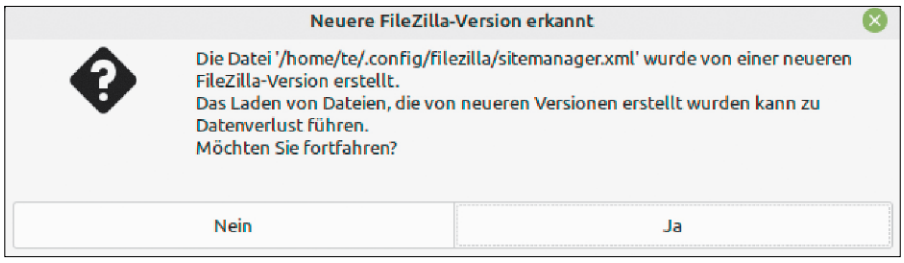
Für die spätere Wiederherstellung verwenden Sie dann diese Befehle:

```
cd ~
tar xvf [/Backup-Ordner]/LO.tar
```

Da tar die Pfade relativ speichert, müssen Sie immer zuerst mit „cd ~“ in Ihr Home-Verzeichnis wechseln, damit die Dateien im richtigen Ordner landen.

Filezilla

Der FTP- und SFTP-Client Filezilla verwendet unter Linux den Konfigurationsordner „.config/filezilla“ und unter Windows „AppData\Roaming\FileZilla“. Hier liegen nur wenige Dateien, beispielsweise „filezilla.xml“ für die Basiskonfiguration und die wichtige Datei „sitemanager.xml“. Dort sind die Einstellungen für alle FTP-Server gespeichert, die Sie über „Datei → Servermanager“ erstellt haben. Sichern Sie den kompletten Ordner in einem Backuparchiv und stellen Sie dieses auf dem Zielrechner wieder her.
Auch bei Filezilla sollte die Programmversion, von der das Backup stammt, mit der auf dem Zielrechner identisch sein. War diese neuer, weist Filezilla bei Verwendung von „Datei → Servermanager“ auf möglichen Datenverlust hin. In diesem Fall klicken Sie auf „Ja“ und prüfen die Einstellungen. Nach einem Klick auf „OK“ speichert Filezilla die Datei „sitemanager.xml“ mit der älteren Versionsnummer und warnt nicht erneut. ■

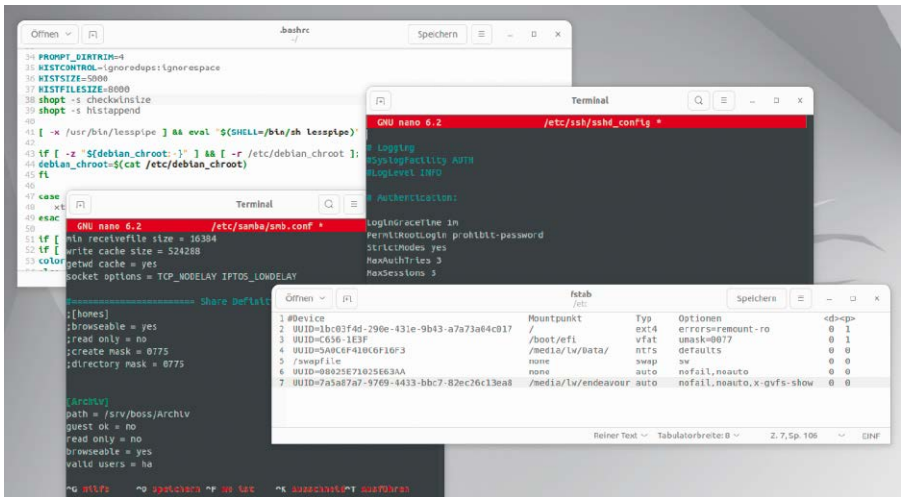


Filezilla-Profilumzug: Wenn das Profil von einer neueren Version stammt, erhalten Sie eine Warnung. Der Import klappt trotzdem, die komplette Datenübernahme ist aber nicht garantiert.

Konfigurationsdateien unter Linux

Linux-Software wird durch Dateien im einfachen Textformat konfiguriert. Wie die Datei heißt und wo sie liegt, folgt gewissen Regeln, ist aber nicht standardisiert. Kommentierungsdisziplin und eine Verwaltungszentrale vereinfachen den Zugriff.

VON HERMANN APFELBÖCK



Linux-Systemkomponenten wie Anwendungsprogramme werden durch verstreute, aber meist leicht zu lokalisierende Textdateien konfiguriert (siehe Punkt 1: „Pfade und Namen“). Der zentralisierte Ansatz dconf unter Gnome-affinen Desktops bleibt marginale Nebensache, zumal er nur für die Benutzerkonfiguration und grafische Anwendungsprogramme gilt (siehe Punkt 2: „Dconf-Zentrale“). Ohne verbindliche Standardisierung bleibt es mehr oder weniger der jeweiligen Software überlassen, wo sie ihre Einstellungen speichern und einlesen will. Das gilt auch für das Format der Konfigurationsdateien: Neben unstrukturierten, immerhin kommentierten Textdateien stehen gegliederte Standardformate wie INI, XML oder JSON mit vordefinierten Sektionen, die jeweils unterschiedliche Anweisungen erwarten.

Wer in diesem ziemlich anarchischen Wust den Durchblick gewinnen will, sollte Pfade und Namen wichtiger Konfigurationsdateien im Blick haben, eigene Eingriffe kennzeichnen und sich den Zugriff auf wichtige Dateien so einfach wie möglich machen. Vorschläge dazu und eine zentrale Verwaltungslösung im Midnight Commander zeigen die Punkte 3 und 4. Eine umfangreiche kommentierte Tabelle ergänzt den Beitrag.

1. Pfade und Namen

Konfigurationsdateien mit systemweiter Geltung liegen praktisch alle im Pfad „/etc“ und ihre Bearbeitung benötigt folglich root-Recht. Je nach Umfang erscheint eine Einzeldatei direkt unter „/etc“ wie etwa „/etc/fstab“ (einzuhängende Datenträger), „/etc/passwd“ (Benutzerkonten), „sysctl.conf“ (Kernel-Parameter), häufiger aber in Unterverzeichnissen wie „/etc/samba/smb.conf“ oder „/etc/ssh/sshd_config“, wenn die betreffende Software mehrere Konfigurationsdateien benötigt. Eine umfassende Aufstellung ist unrealistisch, da sich je nach Menge der genutzten Dienste und der installierten Programme auf jedem System andere Konstellationen finden. Zuverlässig wird aber jede installierte Software – unabhängig von der verwendeten Distribution – eine Konfigurationsdatei oder einen Ordner unter „/etc“ anlegen, dessen Name auf die Software verweist oder den identischen Namen verwendet. Strenge Regeln gibt es nicht: Manche Konfigurationsdateien tragen den exakten Namen der zugehörigen Software wie etwa „nginx.conf“ oder „vsftpd.conf“, andere heißen schlicht „ini“ oder „config“ und die Zuordnung zur Software erschließt sich durch einen Ordnernamen wie „mc“.

Zur Bearbeitung kann jeder beliebige Editor dienen, Nano und MC (mcedit) bevorzugt für SSH-Server, Gedit, Xed oder Geany auf grafischen Desktops. Praktisch alle Editoren verbessern die Lesbarkeit durch unterschiedliche Farbmarkierungen für Kommentare oder Sektionsüberschriften.

Für benutzerspezifische Einstellungen gibt es den Sammelordner „/home/[user]/.config“, jedoch halten sich nicht alle Programme an diese Vorgabe. Einige Programme legen die Benutzerkonfiguration einfach als versteckte Einzeldatei direkt unter „/home/[user]“ ab, so etwa die Bash-Shell mit der Datei „/home/[user]/.bashrc“ oder der Texteditor Nano mit „/home/[user]/.nanorc“. Etliche, zum Teil wichtige Software erstellt einen versteckten Ordner unter „/home/[user]/“ wie etwa „/home/[user]/.thunderbird“ oder „/home/[user]/.kodi“ oder „/home/[user]/.x2go“.

Typischerweise spielen die Benutzereinstellungen unter „/home“ für manuelle Anpas-

sungen eine geringe Rolle: Die meisten der hier versammelten Konfigurationsanweisungen gehören zu grafischen Programmen wie Browser, Office, Thunderbird, Kodi, die sich bequem an der grafischen Oberfläche einstellen lassen. Manuelles Lesen oder Bearbeiten ist oft weder vorgesehen noch erwünscht. Aber es gibt natürlich Ausnahmen: An der „~/.bashrc“ (Bash-Vorgaben: Variablen, Prompt, Aliases) kommt wohl kein Linux-Nutzer vorbei, während Eingriffe in „~/.conkyrc“ (Conky-Systemmonitor), „~/.inputrc“ (Terminaleingabestandards) „~/.nanorc“ (Nano-Konfiguration) wohl schon eher Richtung Bastler gehen. „rc“ steht jeweils für „run commands“. Trotzdem gibt es Situationen, in denen es hilfreich ist, die benutzerspezifischen Konfigurationsdateien aufzusuchen: Wenn eine Software nicht mehr startet, können Sie unter „/home/[user]/“ alle benutzerbezogenen Einstellungen des Programms löschen. So wird etwa der Chrome-Browser nach Löschen des Ordners „/home/[user]/.config/google-chrome“ wieder so starten, als wäre er eben neu installiert. Nicht bei jeder Software ist die Benutzerkonfiguration so eindeutig an einer Stelle zu lokalisieren: Einstellungen für den Cinnamon-Desktops (Linux Mint) verteilen sich auf die Ordner „/home[user]/.cinnamon“, „/home[user]/.config/cinnamon-session“ sowie „/home/[user]/.config/dconf“, wobei der wichtigste dconf-Teil nicht lesbar ist (binär).

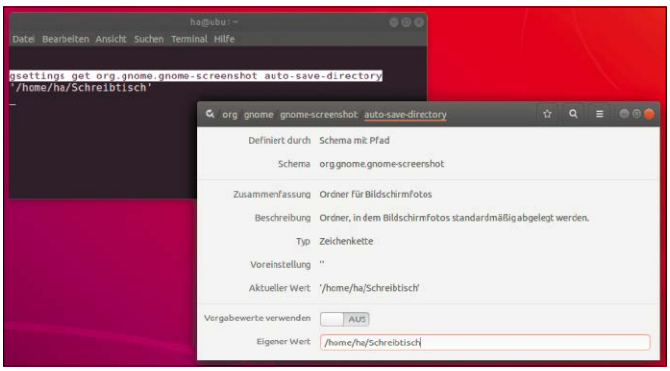
Da die dconf-Datei auch Anweisungen für andere Software enthalten kann, ist deren komplettes Löschen nicht ratsam.

Größte Vorsicht ist angebracht, wenn der Konfigurationsordner auch Benutzerdaten enthält. Dies ist an sich untypisch, aber bei Mailprogrammen wie Thunderbird oder Sylpheed die Regel.

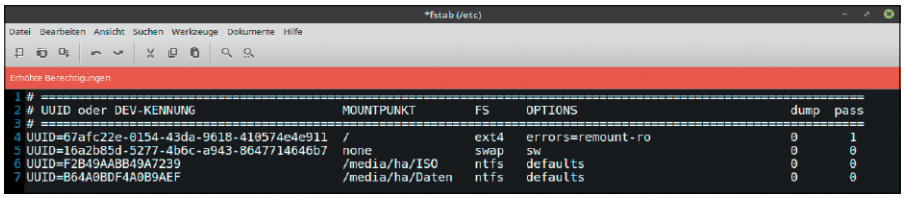
2. Die Dconf-Zentrale

Wer die komplette Benutzerkonfiguration einsehen will, kommt an speziellen Hilfswerkzeugen nicht vorbei, denn nicht alles liegt in lesbaren Textdateien vor. Bei Gnome-affinen Oberflächen (Gnome, Cinnamon, XFCE, Mate, LXDE) gibt es Ansätze zur Standardisierung und Zentralisierung der Softwareeinstellungen. Diese Konzepte werden nicht konsequent und nur neben den traditionellen Textdateien genutzt.

Das ältere Gconf (Gnome Configuration) versammelt seine Konfigurationsdateien unter „/home/[user]/.gconf“ in Form von



Dconf-Editor und sein Terminalkollege Gsettings: Gnome-affine Oberflächen versammeln Desktop- und Programmeinstellungen in der Dconf-Zentrale.



Sauber formatierte fstab: Die Konfigurationsdatei erhält durch Leerzeichen eine gut lesbare Tabellenform.

strukturierten XML-Dateien und ist praktisch obsolet. Das seit Gnome 3 eingeführte Dconf-Konzept benutzt statt XML-Dateien eine einzige Binärdatei „/home/[user]/.config/dconf/user“. Zum manuellen Lesen und Bearbeiten dieser Zentrale dient der grafische Dconf-Editor, der mit dem gleichnamigen Paketnamen überall erreichbar ist. Wichtiger ist aber das alternative Kommandozeilentool Gsettings, das sich ebenfalls überall nachrüsten lässt. Die Syntax für die jeweilige Einstellung folgt dabei exakt der Hierarchie, wie sie der Dconf-Editor anzeigt – etwa:

```
gsettings set org.gnome.desktop.
  background picture-uri /home/lw/
  bild.png
```

Die Hierarchie „org.gnome.desktop.background“ finden Sie identisch im grafischen Editor. Das Beispiel setzt einen neuen Bildschirmhintergrund. Dconf-Einstellungen gelten hauptsächlich für Gnome-Programme wie Dateimanager, Mailprogramm, Editor, Brennprogramm, Bildschirmfoto und den Desktop selbst. Andere Benutzerprogramme verlassen sich auf ihre traditionellen Textdateien. Für systemweite Dienste gibt es sowieso keine Alternative, da deren Konfiguration nicht im Benutzerkontext erfolgen kann.

3. Kommentieren & Formatieren

Welche Anweisungen eine Software in der Konfigurationsdatei erwartet, ist so unterschiedlich wie die Software selbst. Einheitlich ist nur, dass je eine Zeile eine abgeschlossene Anweisung darstellt. Es gibt unstrukturierte Dateien, wo es keine Rolle spielt, an welcher Stelle eine Anweisung steht, so etwa in der Konfiguration des SSH-Servers unter „/etc/ssh/sshd_config“. Andere Konfigurationsdateien wie etwa die Samba-Konfiguration „/etc/samba/smb.conf“ oder die Desktopdateien unter „/usr/share/applications“ gliedern in Sektionen, die unterschiedliche Anweisungen erwarten.

Wer sich mit Linux-Diensten wie SSH, Apache, Samba beschäftigt, liest häufig den Hinweis, dass die Konfigurationsdateien „gut kommentiert“ seien. Tatsächlich sind aber schnell Stunden investiert, um etwa den Anweisungsumfang des SSH-Servers zu verstehen. Typischerweise sind die meisten Optionen mit „#“ oder „;“ auskommentiert. Dazu gibt es englischsprachige Textkommentare vor den eigentlichen Anweisungen, welche die Bedeutung erklären. Hauptproblem dabei ist, dass es keine Aussagen zur Relevanz der Anweisung gibt und viele Einstellungen kaum alltagsrelevant sind.

Vereinfachen Sie daher Dateien wie „/etc/ssh/sshd_config“ (SSH-Server) oder „/etc/samba/smb.conf“ (Samba-Netzfreigaben), indem Sie alle irrelevanten Einträge und Kommentare einfach löschen. Bevor Sie das tun, kopieren Sie die Datei (Beispiel):

```
sudo cp sshd_config sshd_config.
  original
```

Damit kommen Sie bei Bedarf später wieder an alle Optionen. Eine eindeutige Extension wie „.original“ ist hilfreich, um schnell alle bearbeiteten Dateien aufzufinden.

Auf der anderen Seite ist es sehr zu empfehlen, eigene Eingriffe zu kommentieren und dies so, dass sich die Einträge von Standardkommentaren unterscheiden – etwa:

```
#lw# SSH-Port 22 nach 22222 geändert
Port 22222
```

Dann erkennen Sie eigene Eingriffe sofort, auch wenn Sie die Datei monatelang nicht angefasst haben.

„Formatieren" von Konfigurationsdateien: Konfigurationsdateien wie „/etc/fstab" oder die crontab (*crontab -e*) sind kompliziert genug, obendrein aber noch schwer lesbar. Das liegt daran, dass die an sich existierenden Spalten wegen unterschiedlicher Textlängen visuell nicht abzugrenzen sind. Als Trenner für die Parameter dienen Leerzeichen oder Tabulatoren.

LINUX-KONFIGURATIONSDATEIEN

Wichtige Konfigurationsordner	Beschreibung
/etc/[Software]/*	globale Konfigurationseinstellungen für „[Software]" (etwa /etc/apt, /etc/tlp, /etc/lightdm, /etc/gimp ...)
/etc/apt/*	Konfiguration und Paketquellen für apt-Paketmanager (Debian/Ubuntu/Mint u. a.), unter Arch Linux /etc/pacman.d
/etc/ssh/*	Konfiguration des SSH-Servers/SSH-Clients (sshd_config / ssh_config)
/etc/xdg/autostart/*.desktop	systemweite automatische Tasks nach der Systemanmeldung
/home/[user]/.[Datei]	etliche Programme schreiben die benutzerspezifische Konfigurationsdatei direkt ins Home-Verzeichnis (etwa ~/.conkyrc)
/home/[user]/.[Pfad]	etliche Programme erstellen für die benutzerspezifische Konfiguration einen Ordner im Home-Verzeichnis (etwa ~/.mozilla)
/home/[user]/.config/*	Sammelordner für benutzerspezifische Softwarekonfiguration (etwa ~/.config/mc/)
/home/[user]/.config/autostart/*.desktop	benutzerspezifische automatische Tasks nach der Systemanmeldung
/home/[user]/.local/*	benutzerspezifische Anpassungen wie selbst erstellte Starter oder Dateimanager-Erweiterungen (etwa ~/.local/share/nautilus/scripts)
/usr/share/applications/*.desktop	anpassbare Programmverknüpfungen für den grafischen Desktop
/usr/share/xsessions	Anlaufstelle, wo der Anmeldebildschirm (Displaymanager) die installierten Desktops findet (*.desktop) und dann anbietet
/var/log/*	Sammelordner für Log- und Protokolldateien: syslog, auth.log (Anmeldungen), dpkg.log (apt), dmesg (Kernel), Samba, Apache
/var/spool/cron/crontabs/*	Benutzer- und root-Jobs für Cron (zeitgesteuerte Tasks), Editieren mit *crontab -e* oder *sudo crontab -e* (für root-Jobs)
/var/www/*	Standardordner für Apache/Nginx-Webdienste; Konfiguration plus Daten (etwa /var/www/nextcloud oder /var/www/wordpress)
Systemkonfiguration	**Beschreibung**
/etc/apt/sources.list	Paketquellen für das Paketverwaltungssystem (apt) unter Debian/Ubuntu/Mint, s. a. PPA-Quellen unter /etc/apt/sources.list.d/*
/etc/crontab	globale Jobs für den Crondienst (meist ungenutzt, siehe /var/spool/cron/crontabs/)
/etc/default/grub	Basiskonfiguration des Bootmanagers Grub, weitere editierbare Anpassungen unter /etc/grub.d/40_custom
/etc/fstab	Filesystem Table: Gerätekennung, Mountpunkt und Optionen der automatisch zu ladenden Datenträger
/etc/hdparm.conf	optionale Einstellungen für Datenträger, z. B. „spindown"-Anweisungen bei Inaktivität
/etc/inputrc	globale Eingabestandards für das Terminal (Tasten Pos1, Ende, Bild_auf/ab etc.)
/etc/mime.types	Zuordnung von Dateitypen und Dateierweiterungen
/etc/modules-load.d	legt fest, welche externen Kernel-Module beim Systemstart geladen werden
/etc/motd	marginal, aber eventuell irritierend: Standardmeldungen beim Einloggen mit (SSH-)Terminal
/etc/passwd	Liste aller internen und explizit eingerichteten Benutzerkonten
/etc/rc.local	globale Autostarts beim Systemstart (vor der Useranmeldung): nur Terminalbefehle
/etc/sudoers	Benutzerliste für sudo-berechtigte Konten, Standardeditor visudo, typischer Eintrag: [Kontoname] ALL=(ALL:ALL) ALL
/etc/systemd/system.conf	Basiseinstellungen des Init-Dienstes systemd
/etc/sysctl.conf	Steuerung des Linux-Kernels, u. a. Swapiness, IPv4, IPv6, Notfall-Hotkeys (siehe *sysctl --all*)
/var/spool/cron/crontabs/[user]	Benutzer- und root-Jobs für Cron (zeitgesteuerte Tasks), Editieren: *crontab -e* oder *sudo crontab -e* (für root-Jobs)
Netzwerk- und Internetdienste	**Beschreibung**
/etc/apache2/apache2.conf	Hauptkonfigurationsdatei des Apache-Webserver
/etc/apache2/sites-available/000-default.conf	Konfigurationsdatei für aktive Apache-Dienste – fundamental: „<VirtualHost *:[Port]>" und „DocumentRoot [Pfad]"
/etc/network/interfaces	klassische Netzwerkkonfiguration, auf grafischen Systemen durch Networkmanager ersetzt und obsolet
/etc/NetworkManager	Netzwerkkonfiguration mit Network-Manager, Adapterkonfiguration unter /etc/NetworkManager/system-connections
/etc/nginx/nginx.conf	Hauptkonfigurationsdatei des Nginx-Webserver
/etc/nginx/sites-available/default	Konfigurationsdatei für aktive Nginx-Dienste: fundamental: „server listen:[Portangabe]" und „location [Pfad]"
/etc/ssh/ssh_config	Konfguration des Open-SSH-Clients (benötigt in der Regel keine Änderungen)
/etc/ssh/sshd_config	Konfiguration des SSH-Servers (Port, User, Kennwortsicherheit)
/home/[user]/.ssh/rc	benutzerspezifisches Script, das beim Start einer SSH-Sitzung vom Server abgearbeitet werden, wenn sich [user] anmeldet
/etc/samba/smb.conf	Samba-Konfiguration mit Freigaben unter „Share Definitions". Wichtigste Angaben „[Freigabename]" und „path="

Da die Menge der trennenden Leerzeichen oder Tabulatoren keine Rolle spielt, bietet es sich an, solche Dateien mit diesen simplen Mitteln in eine übersichtliche Tabellenform zu bringen.

4. Zentrale für Konfigurationsdateien

Erfahrende Linux-Nutzer kennen die Orte und Dateinamen wichtiger Einstellungen und wer nur die eine oder andere Datei häufiger benötigt, wird mit Aliases im Terminal auskommen. Dafür genügen in der Datei „~/.bashrc“ Einträge wie dieser:

```
alias samba='sudo gedit /etc/samba/
  smb.conf'
```

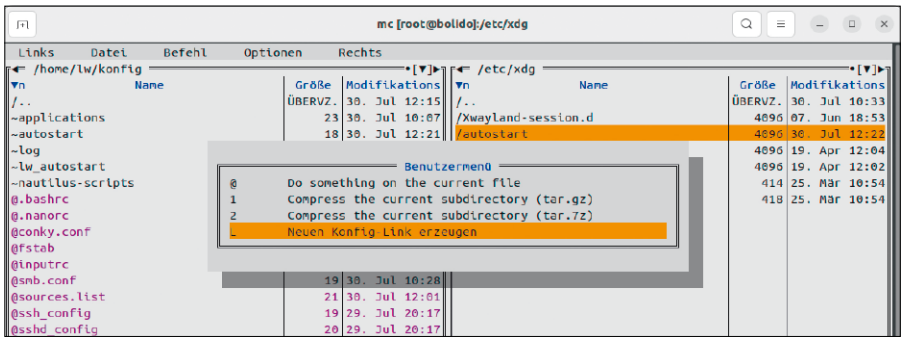
Danach reicht im Terminal die Eingabe *samba*, um diese Konfigurationsdatei zu editieren. Wer häufig mit verschiedenen Dateien zu tun hat, kommt mit solchen Alias-Abkürzungen aber an seine Grenzen.

Die LinuxWelt hat für diesen Kontext bereits Verwaltungslösungen vorgeschlagen, die hübsch, aber relativ unflexibel ausfielen. Die nachfolgend beschriebene Idee greift auf den Midnight Commander (MC) zurück, der sowieso nirgends fehlen sollte und mit kleiner Bastelei einen glänzenden Konfigurationseditor abgibt. Wer diesen Dateimanager beherrscht und das Konzept versteht, kann die Lösung nach Wunsch anpassen. Mit folgender Anleitung sollte aber jeder Anwender klarkommen:

1. Sie benötigen ein leeres Verzeichnis „konfig“ im Home-Ordner:

```
mkdir ~/konfig
```

Der Name ist im Prinzip beliebig.



Midnight Commander als Konfigurationseditor: Die in einem Extraordner als Softlinks versammelten Dateien sind ohne Sucherei einsehbar und editierbar.

2. Sie brauchen ein Alias in der Datei „~/.bashrc“ für den optimalen MC-Start:

```
alias konfig='sudo mc /home/lw/
  konfig /etc/'
```

Ersetzen Sie „lw“ durch Ihren Kontonamen. „sudo“ ist wichtig, damit Sie später auch systemweite Dateien bearbeiten können.

3. In das Verzeichnis „~/konfig“ werden nun Softlinks zu allen benötigten Dateien und Ordnern angelegt. Das geht ultrabequem, wenn der MC mithilft. Starten Sie mit *konfig* oder *sudo mc* den Dateimanager und gehen Sie auf „Befehl → Menüdatei bearbeiten“ und hier auf „Benutzer“ (das ist root, da der MC mit sudo gestartet wurde). Tragen Sie am Ende der Menüdatei drei Zeilen ein:

```
=
L    Neuen Konfig-Link erstellen
     ln -s "%d/%f" --target-directory
       =/home/lw/konfig
```

Die (eine!) Befehlszeile mit „ln“ erstellt Softlinks im „konfig“-Ordner. Ersetzen Sie „lw“ durch Ihren eigenen Kontonamen. Das führende „=“ macht den Eintrag zum vormarkierten Standard. Wenn Sie das MC-Menü sonst kaum verwenden, können Sie der Übersicht halber das Meiste löschen.

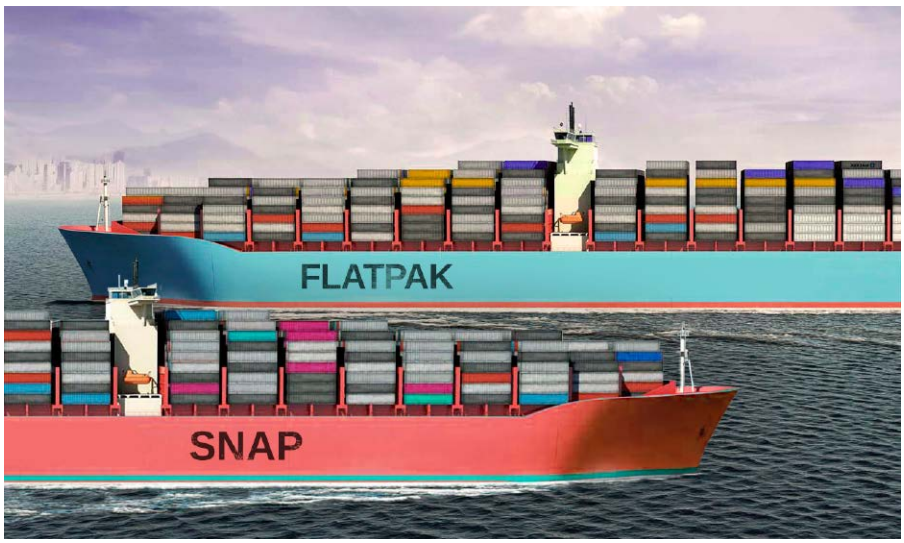
4. Die spätere Benutzung ist einfach: Sie starten den MC mit „konfig“, lesen oder bearbeiten vorhandene Einträge unter „~/konfig“ mit F3 und F4. Einen neuen Link erstellen Sie, indem Sie zum gewünschten Dateiobjekt navigieren, mit F2 das Menü auslösen und dort den Eintrag „Neuen Konfig-Link erstellen“ wählen (ist vormarkiert und benötigt nur noch die Eingabetaste). Wenn Ihnen ein Linkname wie „@.bashrc“ nicht sprechend genug erscheint, benennen Sie ihn mit F6 um. Die Zieldatei des Softlinks ist davon nicht betroffen. Softlinks im Konfig-Ordner, die Sie später nicht mehr brauchen, löschen Sie einfach mit F8. Nicht zuletzt wichtig: Die Dateirechte bleiben bewahrt, egal ob benutzerspezifische oder systemweite Einstellungen bearbeitet werden. ■

LINUX-KONFIGURATIONSDATEIEN (FORTSETZUNG)

Bash-Shell und Konsole	Beschreibung
/etc/bash.bashrc	globales Start-Script der Bash-Shell für Aliases, Functions, Variablen, die systemweit gelten sollen
/etc/profile	globales Bash-Start-Script für Log-in-Shells – also nur bei einer Shell-Neuanmeldung (SSH oder virtuelle Konsole)
/home/[user]/.bash_history	benutzerspezifisches Kommandoprotokoll der Bash-Shell, standardmäßig die 500 letzten Eingaben ($HISTFILESIZE)
/home/[user]/.bash_login	optionales benutzerspezifisches Start-Script
/home/[user]/.bash_logout	optionales benutzerspezifisches End-Script beim Beenden jeder Bash-Shell
/home/[user]/.bashrc	benutzerspezifisches Start-Script der Bash-Shell für Aliases, Functions, Variablen
/home/[user]/.profile	benutzerspezifisches Bash-Start-Script für Log-in-Shells – also nur bei einer Shell-Neuanmeldung (SSH oder virtuelle Konsole)
Diverse Software	**Beschreibung**
/etc/[Software]/*	globale Konfigurationseinstellungen für „[Software“], etwa /etc/mc/ oder /etc/gimp/
/home/[user]/.config/*	Sammelordner für benutzerspezifische Softwarekonfiguration (etwa ~/.config/mc/)
/home/[user]/.config/dconf/user	binäre Konfigurationszentrale für Desktop und Desktopprogramme (Editor: dconf-editor)
/home/[user]/.[Datei]	etliche Programme schreiben die benutzerspezifische Konfigurationsdatei direkt ins Home-Verzeichnis (etwa ~/.conkyrc oder ~/.nanorc)
/home/[user]/.[Pfad]	etliche Programme erstellen für die benutzerspezifische Konfiguration einen Extraordner im Home (etwa ~/.mozilla oder ~/.ssh)

Tipps zu Snaps und Flatpaks

Kompilieren war gestern: App-Container vereinfachen unter Linux die Installation neuer Programme, die nicht in den Paketquellen liegen. Zwei Formate buhlen dabei um die Gunst der Anwender: Flatpaks und Snaps.

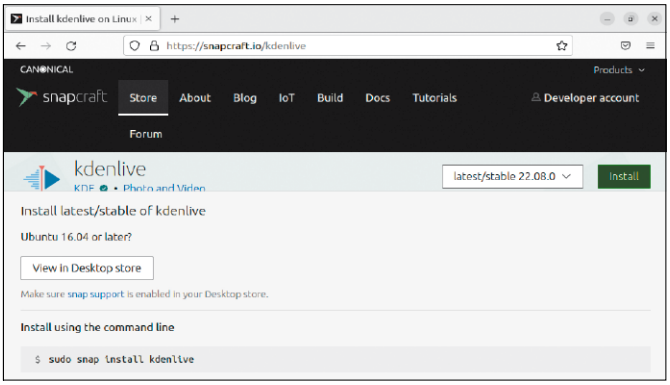


VON DAVID WOLSKI

Zwischen den App-Formaten Snap von Canonical für Ubuntu und dem allgemeiner gehaltenen Flatpak der Gnome Foundation ist eine Rivalität entstanden. Beide wollen die Softwareinstallation unter Linux für Anwender erleichtern und Entwicklern einen einfacheren Weg bieten, Programme in universellen Containern auszuliefern. Diese Container setzen auf einer Runtime auf, die in einer Linux-Distribution als Voraussetzung vorhanden sein muss, dürfen aber anders als herkömmliche Linux-Pakete ihre eigenen Bibliotheken mitbringen. Jeder App-Container ist von anderen Apps sowie vom Kernsystem abgeschottet und installiert sich in sein eigenes Verzeichnis, damit keine Konflikte entstehen.

Zwei Formate mit einem Ziel

Der Vorteil ist also die Verfügbarkeit von Programmen oder Programmversionen, die nicht im Kanon einer Linux-Distributionen erscheinen. Verlangt eine Software neuere oder nicht vorhandene Bibliotheken, so ist damit die Installation in Linux dennoch möglich, weil Flatpaks oder Snaps auch diese individuellen Komponenten enthalten. Es muss auch nicht zwingend Open Source sein, weil Entwickler diese App-Formate selbst veröffentlichen und nicht über eine Linux-Distribution. Anwender müssen daher Einzelteile wie Bibliotheken und Binärdateien nicht selbst zusammensuchen, sondern holen sich den kompletten Container vom Hersteller oder von einem moderierten App Store. Es gibt dabei selbstverständlich Überschneidungen an Bibliotheken und deshalb eine grundlegende App-Infrastruktur bei Snaps und Flatpaks: Beispielsweise müssen GTK oder Gnome-Bibliotheken nicht immer in jedem Container neu mitgeliefert werden, sonst wären diese Apps noch größer (und langsamer). Stattdessen gibt es über die Snap- oder Flatpak-Runtime auch übergreifende Basispakete. Es handelt sich bei beiden App-Formaten um Open-Source-Technologien, die Linux-Distributionen ergänzen können und nachrüstbar sind. Die Snap-Runtime ist auch in Debian, Fedora, Arch Linux und anderen Systemen installierbar – desgleichen auch Flatpak. Auch die Koexistenz auf demselben System ist völlig in Ordnung – in Ubuntu Mate 22.04 sind beide Laufzeitumgebungen sogar schon vorinstalliert. Ein komplet-



Snapcraft.io: Die Webseite ist wie ein App Store aufgebaut und bietet eine durchsuchbare Übersicht zu Snaps, ferner auch Anleitungen zur Installation der Snap-Runtime.

ter Ersatz für die bewährten Paketsysteme sind diese Container nicht und alle Distributionen verwenden auch weiterhin ihr natives Paketformat. Während Ubuntu für Snaps vorbereitet ist und einige dieser Container bereits mitliefert, bevorzugen alle anderen Linux-Distributionen Flatpak. In diesem Beitrag geht es aber nicht um eine Gegenüberstellung, sondern um Installation und Verwaltung dieser App-Formate.

Snapcraft.io: Snaps finden

Ubuntu macht es ab Ausgabe 22.04 dem eigenen Snap-Format nicht leicht, seine Vorteile auszuspielen. Ausgerechnet der Browser Firefox ist nicht mehr als natives Paket installiert, sondern als Snap. Der Browser ist dabei schlicht ein ungünstiger Kandidat für die Vorzüge von Snap-Paketen. Denn einer der Vorteile ist eben Verfügbarkeit von Programmen als Snap, die nicht als DEB-Paket vorliegen – oder nur in alten Versionen. Gelungene Beispiele für die Paketierung als Snap sind Skype, Spotify für Linux oder der umfangreiche Videoeditor Kdenlive mit seinen vielen speziellen Bibliotheken. In der Kommandozeile kann der Befehl

```
snap search [Begriff]
```

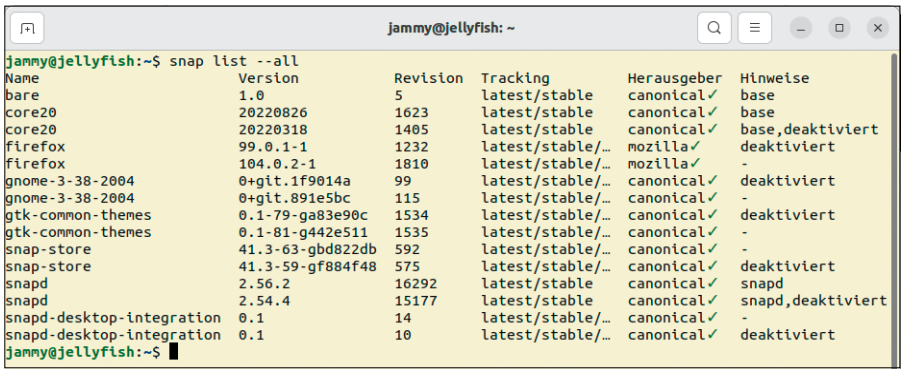
verfügbare Snap-Pakete zu dem angegeben Suchbegriff auflisten. Das geht aber auch noch einfacher: Um das Angebot von Snaps kennenzulernen, lohnt sich ein Besuch der Website *https://snapcraft.io*. Neben einer Vorstellung von populären Snaps auf der Einstiegsseite gibt es links oben eine Suchfunktion für Programmnamen und Stichwörter. Zu jedem Programm zeigt die betreffende Seite unter „Install" eine kurze Befehlszeile oder aber eine Verknüpfung, um das Programm in Ubuntu über das Softwarecenter zu öffnen.

Alle installierten Snaps auflisten

Ubuntu 22.04 und dessen offizielle Varianten liefern neben dem erwähnten Firefox einige vorinstallierte Snaps bereits mit. In einem Terminalfenster zeigt der Befehl

```
snap list --all
```

die vorhandenen Snap-Pakete und deren Versionen an. Die Snap-Runtime behält nämlich bis zu drei Versionen einer so installierten Programms auf dem System, um bei Bedarf den Schritt zurück zu einer älteren Version zu ermöglichen. Dies verschärft die allgemein unangenehme Eigenschaft von Containern: Sie benötigen sehr viel



Was ist installiert? Eine Auflistung aller Snaps gelingt nur in der Kommandozeile. Zur Berechnung des Platzbedarfs ist ein Blick ins Verzeichnis „/var/lib/snapd/snaps" nötig.

Platz auf dem Datenträger, der auf kleinen SSD- und NVME-Laufwerken schon mal zum Problem wird.

Das Kommando

```
du -h /var/lib/snapd/snaps/*
```

listet alle Snap-Verzeichnisse mit ihrem jeweiligen Platzbedarf auf und

```
du -sh /var/lib/snapd/snaps
```

zeigt, auf wie viel Platz sich das insgesamt aufaddiert.

Snaps: Manuell aktualisieren

Snaps sind als Containerformat von der üblichen Paketverwaltung mit apt komplett entkoppelt. Sie verlangen zur Installation sowie zur Aktualisierung eine andere Vorgehensweise. Über ein gewöhnliches Systemupdate werden diese alternativen Programmpakete nämlich nicht aktualisiert. Stattdessen verfügt das Snap-Rahmenwerk über eine separate Updatefunktion, die alle installierten Snaps täglich automatisch aktualisieren will. Auf Rechnern, die nicht dauernd eingeschaltet sind, beispielsweise auf Notebooks, wird das automatische Update nicht immer zuverlässig ausgeführt. Mit dem Befehl

```
sudo snap refresh
```

können Sie die Aktualisierung aller Snaps jederzeit manuell ausführen.

FLATPAK UND SNAPD NACHRÜSTEN

Auch wenn sich Ubuntu auf das eigene Snap-Format festgelegt hat, so ist ein Nachrüsten von Flatpaks auch hier leicht möglich. Einem Mix aus Snaps und Flatpaks steht nichts entgegen, denn die unabhängig voneinander entwickelten App-Container kommen sich nicht in Quere. Ein eventuelles Limit, wie viele Snaps und Flatpaks auf einem System sinnvoll sind, ist aber deren Platzbedarf. Denn der ist bei beiden Formaten erheblich – einige dieser Apps belegen schnell etliche Gigabyte Plattenplatz. In Ubuntu und Debian liegen die Flatpak-Voraussetzungen in den Standard-Paketquellen. Das Kommando

```
sudo apt install flatpak
```

holt das Flatpak-Verwaltungstool ab, um anschließend für die Installation von Apps eine Flatpak-Quelle einzurichten.

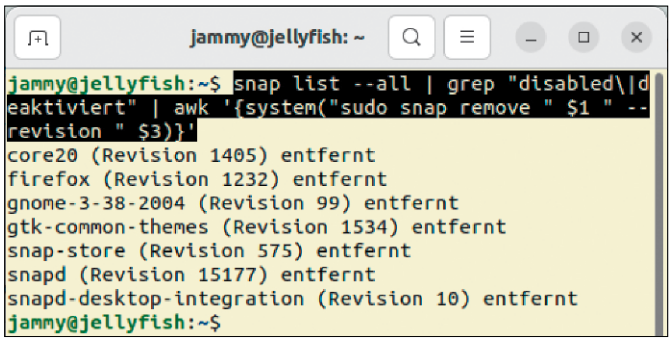
Umgekehrt ist es in Debian, Fedora oder Manjaro kein Problem, Snapd als Runtime für Snap-Pakete auf das System zu holen. Das Paket „snapd" findet sich in den Standardquellen und ist in Debian beispielsweise mit

```
sudo apt install snapd
```

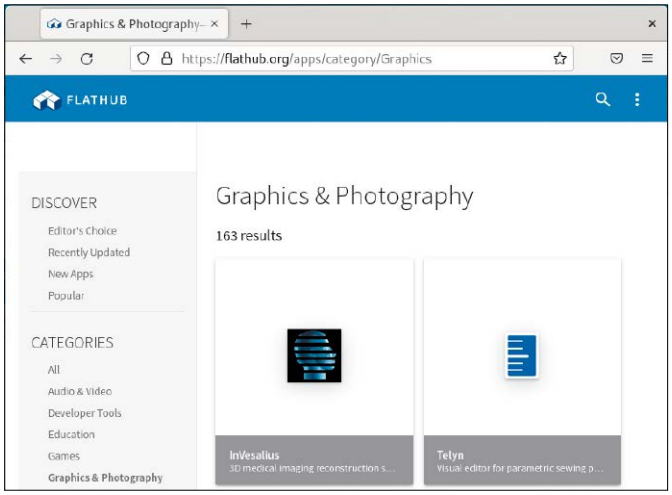
schnell nachgerüstet. Das trifft auch für die Ubuntu-Varianten Kubuntu und Lubuntu zu, bei welchen Snapd auch erst mal fehlt. Eine Ausnahme ist Linux Mint, auf welchem die Installation von Snapd durch eine Regel des Paketmanagers apt blockiert ist. Wer unter Linux Mint Snaps möchte, muss erst mit dem Befehl

```
sudo mv /etc/apt/preferences.d/nosnap.pref ~/nosnap.backup
```

die Blockadedatei verschieben. Der genannte Befehl verschiebt die Konfigurationsdatei dazu in das Home-Verzeichnis.



Snaps aussortieren: Ein länger genutztes Ubuntu-System behält auch die letzten zwei älteren Versionen von installierten Snaps. Dieser Befehl entfernt diese Versionen.



Zentrale für Flatpaks: Flathub ist nur eine von vielen Flatpak-Quellen. Unter der Ägide der Gnome Foundation entsteht unter *https://flathub.org* aber das umfangreichste Repository.

Snaps: Alte Versionen entfernen

Laufen alle installierten Snaps unproblematisch, ist es nicht nötig, die älteren Versionen zu behalten. Archivierte, aber inaktive Snaps sind in der tabellarischen Übersicht von „snap list --all" in der letzten Spalte „Notes" mit dem Begriff „disabled" beziehungsweise „deaktiviert" versehen. Eine gezielte Deinstallation eines dieser Snaps gelingt mit diesem Kommando:

```
sudo snap remove [Name] --revision
  [Revision]
```

Den korrekten „Namen" erfahren Sie in der gleichnamigen Spalte „Name" des list-Befehls und den Wert von „Revision" aus der gleichnamigen Spalte „Revision". Um beispielsweise das Snap „gnome-calculator" in der Revision 260 zu entfernen, dient dieser Befehl:

```
sudo snap remove gnome-calculator
  --revision 260
```

Diese Aktion ist in der Befehlszeile per verknüpften Kommandos auch automatisierbar. Die Zeile

```
snap list --all | grep
  "disabled\|deaktiviert" | awk
  '{system("sudo snap remove " $1 "
  --revision " $3 ")}'
```

deinstalliert alle archivierten und inaktiven Snaps in einem Durchgang.

Flatpaks: Ein Programm installieren

Die Idee hinter Flatpaks geht auf Red Hat und die Gnome Foundation zurück und vorgestellt wurden diese App-Container erstmals 2016 in Fedora 24 und Gnome 3.22. Dieses zweite verbreitete Containerformat Flatpak hat aktuell ein höheres Momentum als Snap, ist offener, benötigt allerdings noch mehr Plattenplatz als Snap. Unter anderem favorisiert Linux Mint Flatpak als Containerformat und in Ubuntu Mate ist es ebenfalls von Haus aus nutzbar. Flatpaks sind also weder an eine Distribution gebunden noch an die Desktopumgebung Gnome.

Im Gegensatz zu Snaps (zentraler Canonical-Snapstore *snapcraft.io*) sind Flatpaks nicht zentralisiert. Linux-Distributionen wie auch Softwareentwickler veröffentlichen eigene Flatpaks auf verschiedenen Repositorys und liefern Installationsanleitungen auf ihren eigenen Web- oder Github-Seiten. Aktuell ist die Site *https://flathub.org* die eindeutig wichtigste Anlaufstelle für die Suche nach Flatpaks. Rund 1700 Einträge finden sich dort mit Beschreibung. Das Wachstum ist konstant und die Site soll mit Hilfe der Gnome Foundation zu einem App Store für Linux wachsen. Die Seite bietet eine Suchfunktion, eine Liste an neu vorgestellten Flatpaks sowie Programmkategorien zum Durchstöbern. Die Unterseite zu einem Programm liefert Versionsangaben und ganz unten die Kommandozeilen zur Einrichtung in der Shell.

In Linux-Distributionen ist in der Regel wenig mehr vorinstalliert als das Verwaltungstool flatpak für die Kommandozeile. Um etwas installieren zu können, ist zuerst die Einbindung einer externen Quelle nötig. Das Kommando

```
flatpak remotes
```

listet die vorhandenen Paketquellen auf. Um das empfehlenswerte und gut gefüllte Repository Flathub aufzunehmen, dient dieser Befehl:

```
sudo flatpak remote-add flathub
  https://flathub.org/repo/
  flathub.flatpakrepo
```

Danach kann die Abfrage

```
flatpak search [Begriff]
```

nach Programmen suchen. Wichtig ist in dieser Auflistung die „Application ID", anhand derer sich ein Programm mit

```
flatpak install [Application ID]
```

installieren lässt. Dies funktioniert ohne vorangestelltes „sudo", denn um die Rechteverwaltung im Dateisystem kümmert sich flatpak selbst. Das Programm steht deshalb nicht nur dem aktuell angemeldeten Konto zur Verfügung.

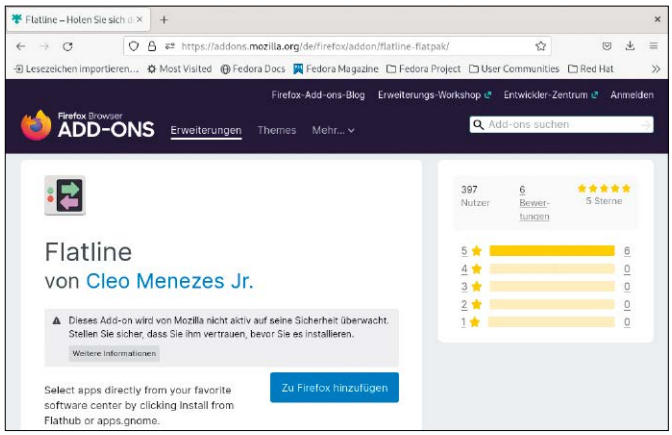
Flatline: Flatpaks über den Browser

Auf flathub.org bietet jede Seite zu einem Programm auch gleich die Schaltfläche „Install", die aber nicht viel mehr tut, als eine Datei mit der Endung „.flatpakref" herunterzuladen. Diese dient zunächst zur Weiterverarbeitung im Terminal mit diesem Befehl:

```
flatpak install --from [Datei].
  flatpakref
```

Der Sprung ins Terminal zur Flatpak-Installation ist aber nicht unbedingt nötig, denn es gibt für Flathub eine Browsererweiterung für Firefox, um die Einrichtung von Flatpaks zu vereinfachen: Das Add-on Flatline steht im Erweiterungsverzeichnis Mozillas unter *https://addons.mozilla.org/de/firefox/addon/flatline-flatpak* bereit. Damit

sich nach einem Klick auf „Install“ zu einem Programm auf Flathub etwas tut, muss dazu auch das Repository *https://flathub.org/repo/flathub.flatpakrepo* hinzugefügt sein wie vorher gezeigt. Der Install-Button bietet dann an, die Installationsprozedur über den grafischen Paketmanager (etwa Gnome Software oder Discover) zu öffnen, und der Exkurs in die Kommandozeile kann daher entfallen. Ein Dialog bietet außerdem an, diese Verknüpfung immer auf diese bequeme Weise zu öffnen.



Flatline: Diese Browsererweiterung für Mozilla ist eine Installationshilfe für Flathub und kann direkt die grafischen Werkzeuge Gnome Software oder Discover aufrufen.

Inventur: Verwaltung in der Shell

Genau wie bei Snaps so fällt auch die Verwaltung von Flatpaks nicht an den nativen Paketmanager der Distribution. In Gnome-Software sowie in Discover (KDE) ist es aber möglich, Flatpaks auf grafischem Weg wieder zu deinstallieren. Eine Filterfunktion, die nur Flatpaks zeigt, fehlt allerdings, daher muss die Auflistung der Flatpaks und ihrer Runtimes weiterhin in der Kommandozeile erfolgen. Die Eingabe

```
flatpak list
```

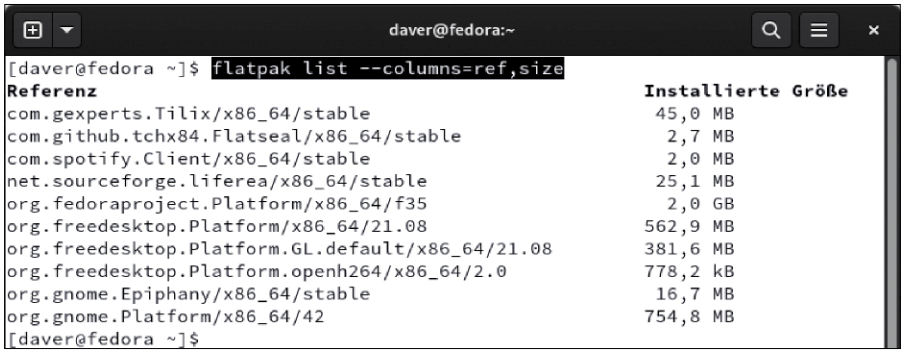
zeigt die schon installierten Flatpaks an. Geht es um die Einschätzung des Platzbedarfs aller Flatpaks, dann hilft dieses Kommando

```
flatpak list --columns=ref,size
```

weiter, das eine tabellarische Liste der Apps und ihrer jeweiligen Größe ausgibt. Über den Befehl

```
flatpak uninstall [Name]
```

ist ein Flatpak im Terminal ohne lange Suche auch wieder deinstalliert, wobei hier keine genaue Angabe der Applikations-ID notwendig ist – der Name reicht aus. Auch hier ist kein „sudo“ nötig.



Flatpaks und der Umfang auf dem Datenträger: Eine Auflistung der Flatpak-Apps mit Größenangabe ist auch bei diesem Format nur in der Kommandozeile möglich.

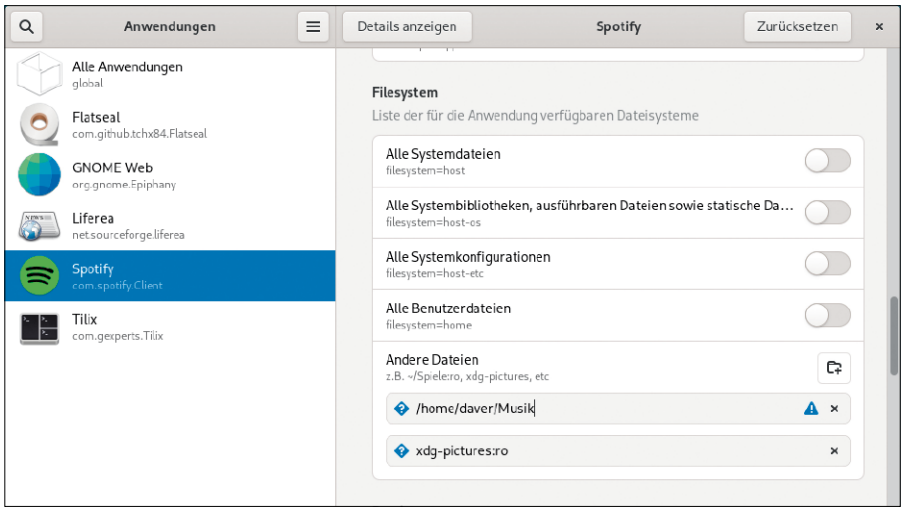
Flatseal: Berechtigungen von Flatpaks

Die Ziele von Flatpak sind recht hoch gesteckt: Als abgeschottete Programme, die Cgroups und Namespaces des Linux-Kernels zur Prozessorisolierung nutzen, sollen Flatpak-Apps auf dem Desktop in einer sicheren Sandbox mit Rechteverwaltung laufen. Anwender können bestimmen, welche Ressourcen ein Flatpak nutzen darf. Zur Anzeige und Verwaltung der Berechtigungen installierter Flatpaks gibt es das grafische Tool Flatseal, das seinerseits als Flatpak vorliegt. Um das Tool zu installieren, ist es am einfachsten, wieder Flathub als Quelle zu nutzen. Flatseal findet sich dort unter *https://flathub.org/apps/details/com.github.tchx84.Flatseal*, ist aber auch im Terminal mittels

```
flatpak install flathub com.github.tchx84.Flatseal
```

zu installieren. Nach einem Aufruf zeigt das Tool links alle installierten Flatpaks an, rechts jeweils deren Berechtigungen. Die meisten Apps liefern eine Standardkonfiguration mit allen nötigen Rechten, um korrekt zu funktionieren. Eine Berechtigung, die gelegentlich Anpassungen verlangt, ist der Zugriff auf Verzeichnisse außerhalb von Home.

Diese Rechte sind in Flatseal in der Kategorie „Filesystem“ untergebracht und das Ordnersymbol unter „Andere Dateien“ kann hier weitere Pfade hinzufügen, auf die der aktuelle Benutzer selbst Zugriff hat. ■



Wer darf was? Flatseal kann die Flatpak-Zugriffsrechte anpassen. Das ist beispielsweise nützlich, wenn Programme den Zugriff auf Ordner jenseits des Home-Verzeichnisses verlangen.

Paketmanager: Tipps und Fehlersuche

Installationen, Updates und Systemupgrades bereiten bei Linux nur selten Probleme. Wenn jedoch Fehler auftreten, ist die Reparatur oft nicht einfach. Wir geben Tipps zur Nutzung der Paketverwaltung und Ratschläge zur Behebung von Fehlern.

VON THORSTEN EGGELING



Die technische Basis der Paket-Infrastruktur ist bei Debian, Ubuntu sowie Linux Mint identisch und seit vielen Jahren bewährt. Trotzdem kann es zu Fehlern kommen: Systemupdates beispielsweise schlagen fehl oder es lassen sich keine neuen Programme installieren. Viele Probleme lasen sich einfach lösen, bei schweren Fehlern in der Systeminstallation kann die Fehlersuche jedoch aufwendig werden.

Das Ubuntu/Debian-Paketformat

Das Paketmanagement bei Debian, Ubuntu und verwandten Systemen ist zwar komplex, aber trotzdem transparent und nachvollziehbar. System und Software werden mit Hilfe von Softwarepaketen installiert, die in DEB-Dateien vorliegen. Dabei handelt es sich um gepackte Archive, die ausführbare Dateien, Bibliotheken und Konfigurationsdateien enthalten. Ebenfalls enthalten sind meistens einige Scripts, die beim Setup beispielsweise Konfigurationsdateien anpassen oder Systembenutzer erstellen. Eine DEB-Datei enthält aber selten alle Dateien, die zum Start des jeweiligen Programms erforderlich sind. Fast alle Tools und Anwendungen benötigen zusätzliche Programmbibliotheken, die oft Funktionen für mehrere Programme bereitstellen. Im DEB-Paket ist daher eine Textdatei mit Informationen über die Abhängigkeiten von anderen Paketen sowie optionalen Empfehlungen für zusätzliche Pakete enthalten. Der Distributor muss dafür sorgen, dass alle Pakete für ein System zusammenpassen und alle Abhängigkeiten erfüllbar sind. Die Pakete stammen jedoch nicht aus einer Hand. Es sind weltweit zahlreiche Entwickler („Maintainer“) an der Erstellung der Pakete beteiligt. Vor allem bei selten genutzten Programmen kommen daher Installationsfehler vor, die vielleicht bisher vom Anbieter nicht entdeckt wurden. Eine Suche nach der Fehlermeldung im Internet kann weiterhelfen. Eine Quelle für Informationen ist *https://bugs.launchpad.net/ubuntu*. Hier kann man nach Paketen suchen und sich die gemeldeten Fehler anzeigen lassen.

DEB-Dateien sind digital signiert und es gibt Prüfsummen für die enthaltenen Dateien. Der Paketmanager verweigert die Installation, wenn Signaturen oder Prüfsummen ungültig sind. Manchmal ist auch ein falsch gesetztes Systemdatum die Ursache. Liegt es zu weit in der Vergangenheit oder Zukunft, wird der Schlüssel als ungültig angesehen.

Tipp: Wer sich den Inhalt einer DEB-Datei genauer ansehen möchte, kann die Dateien extrahieren. Installieren Sie dazu das Archivprogramm ar mit

```
sudo apt install binutils
```

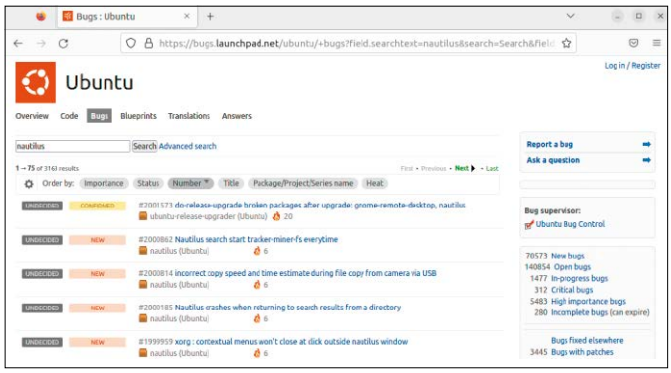
und entpacken Sie dann eine DEB-Datei mit

```
ar xv [Name der Datei]
```

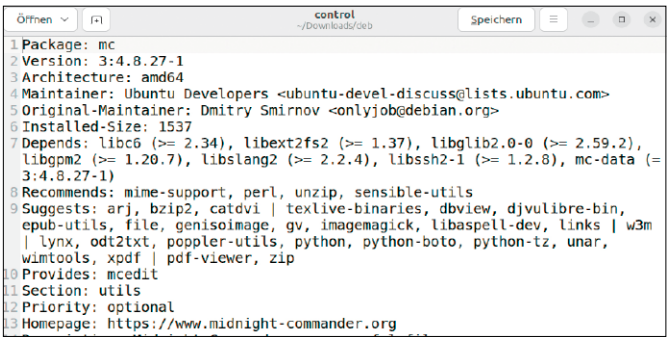
Das Ergebnis sind die Dateien „control.tar.zst“ und „data.tar.zst“ (oder .gz), die Sie mit

```
tar xvf [tar.zst-Datei]
```

entpacken. Dabei entstehen Order, in denen die ausführbaren Dateien und Konfigurationsdateien zu finden sind. „control“ enthält eine Beschreibung des Pakets und Informationen zu Abhängigkeiten, „md5sums“ die Prüfsummen der Dateien.



Fehlerberichte: Bei *https://bugs.launchpad.net/ubuntu* finden Sie eingesandte Fehlerberichte zu einzelnen Ubuntu-Paketen und oft auch Problemlösungen.

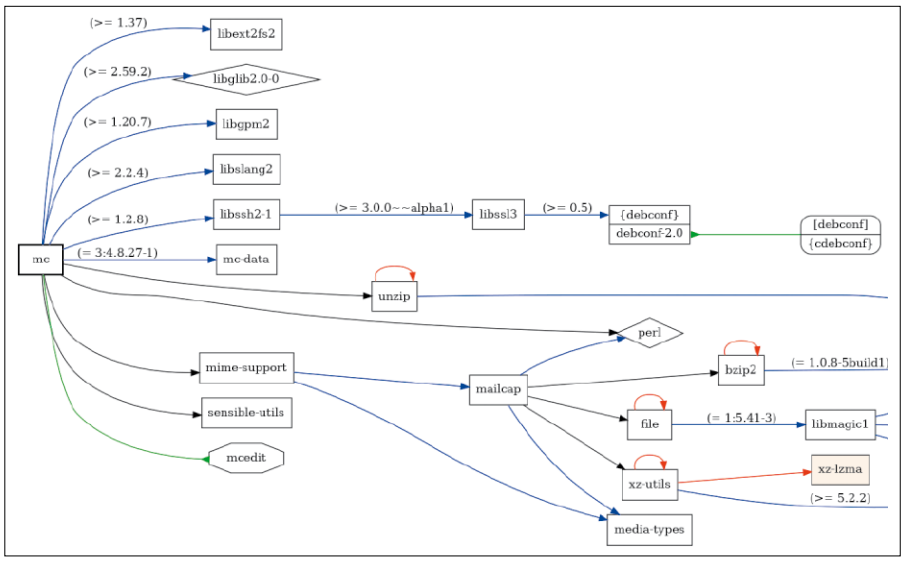


Paket-Internat: Die Datei „control“ in einem DEB-Paket enthält alle Informationen. Hinter „Depends:“ beispielsweise stehen die Paketabhängigkeiten inklusive Versionsnummern.

Pakete und Abhängigkeiten

In der Paketdatenbank sind die Informationen zu allen installierten Paketen gespeichert. Wird ein neues Programm installiert, lässt sich darüber prüfen, ob zusätzlich erforderliche Tools und Bibliotheken bereits vorhanden sind. Wenn nicht, werden diese automatisch mitinstalliert. Bei der Deinstallation eines Pakets werden gemeinsam genutzte und automatisch installierte Komponenten nicht entfernt. Anders sieht es aus, wenn man etwas deinstalliert, das von anderen Paketen benötigt wird. Es erscheint ein Hinweis, welche Pakete außerdem entfernt werden. Diese Meldung sollte man immer sehr ernst nehmen und genau prüfen. Wenn man die Situation nicht sicher einschätzen kann, sollte man auf die Deinstallation verzichten.

Die Abhängigkeiten von anderen Paketen müssen exakt erfüllt sein. Anwendungen benötigen die gleiche oder eine höhere Nebenversion von Programmbibliotheken, mit denen sie erstellt wurden. Bei Linux ist es Standard, dass bei der Hauptversion einer Programmbibliothek zwar neue Funktionen hinzukommen können, alte aber nicht wegfallen. Beim Upgrade, etwa von einer Version 6.x auf 7.x, ist das nicht immer der Fall. Im optimalen Fall verwenden alle Programme einer Distribution die gleichen Versionen der Programmbibliotheken. Das ist allerdings nicht immer möglich. Linux löst das Problem mit Versionsnummern in den Dateien. Unterhalb von „/usr/lib“ können beispielsweise die Dateien „libx.so.1“ und „libx.so.2“ liegen und jedes Programm findet dann die jeweils benötigte Version. Nach einem Update kann die Datei dann „libx.so.2.1.1“ heißen. In diesem Fall verweist der symbolische Link mit der Nummer der Hauptversion „libx.so.2“ auf „libx.so.2.1.1“ und für die Programme hat sich nichts geändert.



Nötige Pakete: Das Tool debtree bereitet den meist komplexen Abhängigkeitsbaum grafisch auf. Selbst ein einfaches Tool wie Midnight Commander benötigt mehrere Pakete.

Bei komplexeren Programmen ergibt sich ein sehr weit verzweigter Baum von Abhängigkeiten („dependency tree“) und die Paketverwaltung installiert zahlreiche Pakete. Wer es genauer wissen möchte, kann mit der Befehlszeile

```
debtree [Paketname] | dot -Tpng > bild.png
```

eine grafische Darstellung der Abhängigkeiten eines Pakets erstellen. Die Pakete „debtree“ und „graphviz“ müssen dafür installiert sein.

Paketverwaltung im Terminal

Das zentrale Programm zur Paketverwaltung heißt unter Ubuntu und verwandten Systemen dpkg. Es wird im Hintergrund von allen Tools zur Paketverwaltung genutzt. Das Tool lädt jedoch keine Paketdateien herunter und prüft keine Abhängigkeiten. Deshalb werden Sie es nur selten direkt nutzen. Eine heruntergelade DEB-Datei lässt sich bei Bedarf im Terminal mit

```
sudo dpkg -i [DEB-Datei]
```

installieren. Bei mehreren Dateien verwenden Sie im Downloadordner

```
sudo dpkg -i *.deb
```

Sollten die Paketabhängigkeiten nicht bereits erfüllt sein, verwenden Sie danach diesen Befehl:

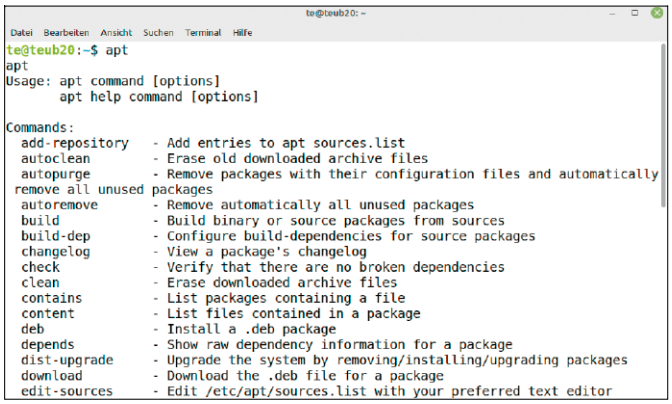
```
sudo apt -f install
```

Das Tool apt prüft die Abhängigkeiten und installiert alle fehlenden Pakete.

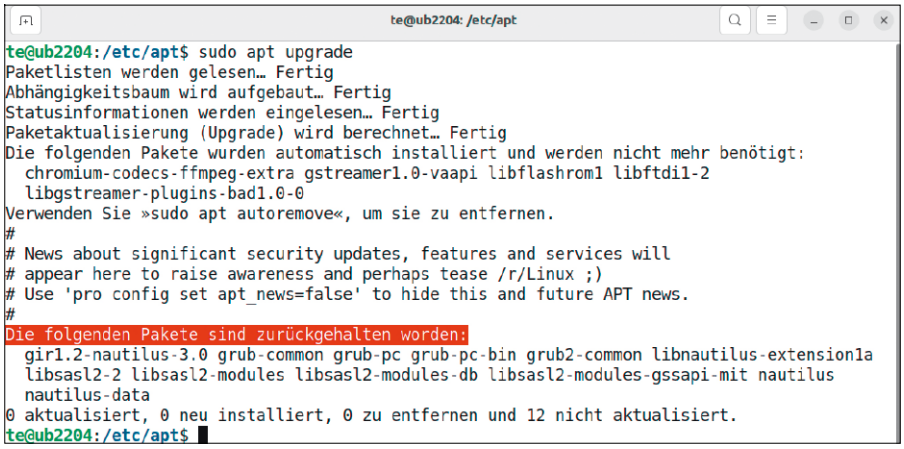
Seit Version 1.1 (ab Ubuntu 16.04) kann man DEB-Dateien auch direkt über apt installieren, wobei die Abhängigkeiten automatisch aufgelöst werden:

```
sudo apt install ./[DEB-Datei]
```

„install“ erwartet als Parameter den vollständigen Pfad zur Datei oder im Down-



Mint-Spezialität: Der Start von apt zeigt zahlreiche Optionen. Tatsächlich handelt es sich um ein Wrapper-Script, das je nach Option unterschiedliche Tools startet.



Auf später verschoben: Bei dieser Meldung sind Updates für die genannten Pakete verfügbar. Die Installation erfolgt jedoch erst, wenn mögliche Fehler beseitigt wurden.

load-Verzeichnis ein vorangestelltes „./“. Mehrere Pakete lassen sich mit

```
sudo apt install ./*.deb
```

einrichten.

Reguläre Nutzung von apt: Standardmäßig greift apt auf die in „/etc/apt/sources.list“ und unter „/etc/apt/sources.list-d“ konfigurierten Repositorien zurück. Die typische Anwendung für das Update von Paketen erfolgt mit den zwei Zeilen

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

„update“ aktualisiert die Paketdatenbank, „upgrade“ lädt die Dateien herunter und beginnt mit der Installation. Fehler können auftreten, wenn ein Server gerade nicht erreichbar ist. Probieren Sie es später noch einmal oder kontrollieren Sie die URLs in den Paketquellen. Manchmal ist auch die Paketdatenbank blockiert, wenn im Hintergrund ein automatisches Update läuft (siehe Artikel ab Seite 58).

Eine fehlende IPv6-Unterstützung kann ebenfalls zu Problemen führen. In der Fehlermeldung wird dann bemängelt, dass beispielsweise der Server „2001:67c:1562::15“ (security.ubuntu.com) nicht erreichbar ist. Da alle Server auch über IPv4-Adressen verfügen, lässt sich das Problem über die apt-Konfiguration beben. Erstellen Sie mit

```
sudoedit /etc/apt/apt.conf.d/
  99force-ipv4
```

eine zusätzliche Konfigurationsdatei mit dem Inhalt

```
Acquire::ForceIPv4 "true";
```

Das Tool apt und die Paketmanager für die grafische Oberfläche verwenden jetzt nur noch IPv4-Adressen.

Unterschiede zwischen apt oder apt-get: apt ist bei Ubuntu eine vereinfachte Version von apt-get. Das Tool bietet die gebräuchlichsten Funktionen, beispielsweise

```
sudo apt install [Paketname]
```

zur Installation neuer Pakete. Mehrere Pakete lassen durch Leerzeichen getrennt angeben, beispielsweise

```
sudo apt install apache2
  libapache2-mod-php php php-mysql
  mysql-server
```

für die Installation des Webservers Apache, PHP und der Datenbank My SQL. Für die Deinstallation eines Pakets verwenden Sie

```
sudo apt remove [Paketname]
```

Das Tool apt-get bietet fast die gleichen Optionen, aber noch einige zusätzliche. Es verhält sich aber teilweise anders. „upgrade“ bei apt-get aktualisiert nur die installierten Pakete, entfernt aber keine Pakete und fügt auch keinen neuen hinzu. Der Linux-Kernel beispielsweise wird damit nicht aktualisiert, weil es sich um ein neues Paket handelt. „apt upgrade“ installiert – wenn nötig – auch neue Pakete, entfernt aber ebenfalls keine Pakete.

Besonderheiten bei Linux Mint: Die Distribution verwendet beim Aufruf von apt ein Script aus dem Ordner „/usr/local/bin“. Abhängig von der verwendeten Option ruft es /usr/bin/apt, apt-get oder andere Tools auf. Bei „update“ und „upgrade“ beispielsweise kommt /usr/bin/apt zum Einsatz, bei „clean“ (heruntergeladene Pakete löschen) oder „check“ (unerfüllte Abhängigkeiten finden) wird apt-get verwendet.

Ungewöhnliche Meldungen von apt: Manchmal gibt „apt upgrade“ eine Info zu automatisch installierten Paketen aus, die nicht mehr benötigt werden. Sie können dann bedenkenlos

```
sudo apt autoremove
```

verwenden, um die Pakete zu entfernen.

Eine auffällige Meldung ist: „Die folgenden Pakete sind zurückgehalten worden:“. Darunter steht eine Liste mit den betroffenen Paketen. Dahinter verbergen sich Updates, deren problemlose Funktion noch nicht sichergestellt ist.

Die Pakete werden nach und nach an die Benutzer ausgeliefert, und die Entwickler beobachten dann die eingesandten Fehlerberichte. Bei Ubuntu heißt das Verfahren „Phasing“.

```
apt list --upgradable
```

gibt die Paketnamen der Updates inklusive der neuen Versionsnummern aus. Mit

```
apt show [Paketname] = [Neue
  Versionnummer]
```

lässt sich der Status eines Pakets ermitteln. Der Wert hinter „Phased-Update-Percentage:“ startet bei zehn Prozent und wird alle sechs Stunden um zehn Prozent erhöht, wenn keine Fehler gemeldet werden. Sie müssen daher nur bis zu maximal 54 Stunden auf die Installation warten, weitere Aktionen sind nicht erforderlich. Auskunft über die jeweils betroffenen Pakete liefert *https://people.canonical.com/~ubuntu-archive/phased-updates.html*.

Probleme beim Ubuntu-Upgrade beheben

Besondere Aufgabe erfüllen „apt full-upgrade“ und „apt-get dist-upgrade“. Beide arbeiten identisch und führen Updates auch dann durch, wenn sich Paketabhängigkeiten geändert haben, neue Pakete erforderlich sind oder installierte entfernt werden müssen. Zum Einsatz kommt eines der beiden Kommandos, wenn Sie ein Upgrade auf die nächste Ubuntu-Version im Terminal anstoßen wollen. Denn die Voraussetzung dafür ist ein möglichst vollständig aktualisiertes System. Verwenden Sie die folgenden vier Befehle:

```
sudo apt update
sudo apt upgrade
sudo apt-get dist-upgrade
sudo do-release-upgrade
```

In der Regel arbeitet „apt-get dist-upgrade“ unproblematisch. Man sollte es dennoch nicht als standardmäßigen Ersatz für „apt upgrade“ verwenden, weil bei Fehlern unter Umständen wichtige Pakete entfernt werden. In jedem Fall sollten Sie die Ausgaben des Befehls beachten und das Verhalten prüfen, wenn Deinstallationen durchgeführt werden sollen.

Die Ausführung von do-release-upgrade scheitert, wenn Systemaktualisierungen nicht für alle installierten Pakete möglich sind. Dieser Zustand kann nur eintreten, wenn aktuellere Software aus PPA-Repositorien installiert wurde, worauf apt auch hinweist. Man sollte zuerst versuchen, die PPA-Fremdsoftware zu deinstallieren. Vorher ist ein Backup des Systems oder wenigstens der persönlichen Dateien ratsam, weil das erfolgreiche Upgrade nicht mehr garantiert werden kann.

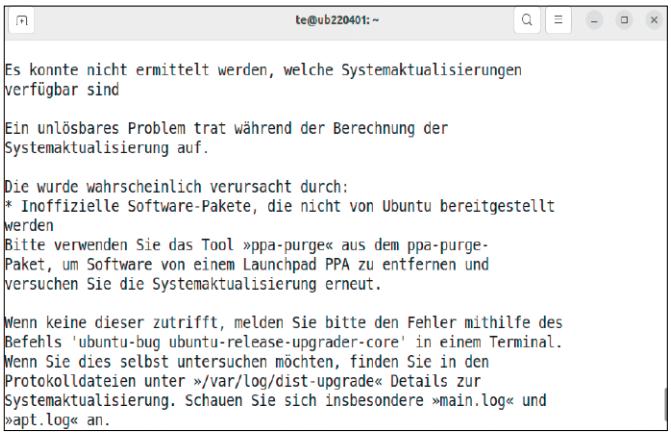
do-release-upgrade deaktiviert zuerst fremde Repositorien in den Listen unter „/etc/apt/sources.list.d“, was man später wieder rückgängig machen muss. Danach kann man ppa-purge verwenden, um die Fremdsoftware zu entfernen. Installieren Sie dieses Tool mit

```
sudo apt install ppa-purge aptitude
```

und verwenden Sie es dann so:

```
sudo ppa-purge -o [Besitzer des PPA]
  -p [Name des PPA]
```

Die Werte für die beiden Platzhalter ermitteln Sie aus der URL in der zugehörigen Datei des PPAs unter „/etc/apt/sources.list.d“. Lautet diese beispielsweise „*https://ppa.launchpadcontent.net/SeppHuber/daily-builds*“, verwenden Sie die Befehlszeile



Massive Probleme: Fremdpakete können das Ubuntu-Upgrade verhindern. Bevor es gelingt, müssen alle Pakete durch die meist älteren Originale der Distribution ersetzt werden.

```
sudo ppa-purge -o SeppHuber-p
  daily-builds
```

Das Tool versucht, die Pakete aus dem PPA zu entfernen und – wenn vorhanden – die Pakete durch die gleichnamigen aus den Standard-Repositorien zu ersetzen. Um defekte Abhängigkeiten danach zu reparieren, führen Sie

```
sudo apt -f install
```

aus. Anschließend starten Sie erneut

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

Sollte das Upgrade erneut fehlschlagen, prüfen Sie die Logdatei „/var/log/dist-upgrade/main.log“. Am Ende der Datei weisen Angaben hinter „Error“ auf defekte Pakete hin, die das Upgrade verhindern. Entfernen Sie diese Pakete mit „apt remove [Paketname]“, auch wenn es sich um wichtige Systempakete handelt. Notieren Sie sich die Paketnamen für die spätere Neuinstallation. Danach sollte do-release-upgrade keine Probleme mehr melden.

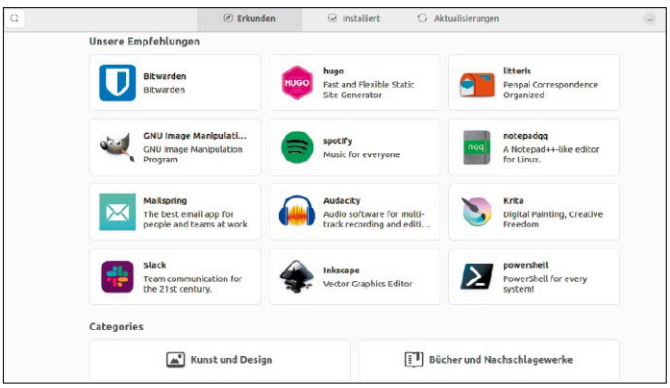
Paketverwaltung über die grafische Oberfläche

Im Terminal ist apt besonders nützlich, wenn man mehrere Pakete gleichzeitig installieren will. Außerdem gibt das Tool meist weiterführende Fehlermeldungen aus, die bei der Suche nach Problemen helfen. Man muss allerdings die Namen der Pakete kennen, die man installieren will.

Mehr Komfort bietet die grafische Zentrale „Ubuntu Software“ oder die „Anwendungsverwaltung“ von Linux Mint. Man kann sich die Empfehlungen oder in den Kategorien Programme und Beschreibungen ansehen und neue Programme einrichten. Ubuntu Software zeigt hauptsächlich Desktopanwendungen. Die Installation von Tools für das Terminal oder von Diensten ist daher hier nicht möglich.

Das Werkzeug Synaptic vereint die Vorteile einer grafischen Oberfläche mit denen von apt. Das Tool ist bei Linux Mint bereits vorinstalliert. Ubuntu-Nutzer können es über Ubuntu Software nachinstallieren. Synaptic bietet eine Suchfunktion und mehrere Filter, über die sich die Ansicht auf die gewünschte Software einschränken lässt. Das Tool im Vergleich zu Ubuntu Software etwas unübersichtlicher, dafür liefert die Suche schnellere Ergebnisse.

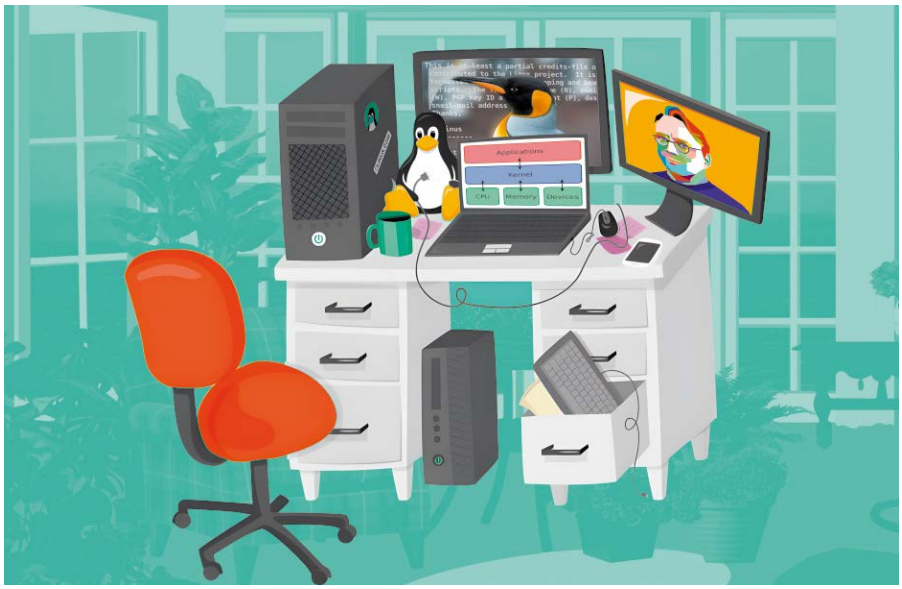
Anders als mit Ubuntu Software oder seinem Mint-Pendant lassen sich mit Synaptic alle verfügbaren Programme installieren, also auch Tools für die Kommandozeile, Bibliotheken und Entwicklerpakete. ■



Anwendungen für jeden Geschmack: Ubuntu Software zeigt, welche Programme verfügbar sind. Beschreibungen, Screenshots und Bewertungen helfen bei der Auswahl.

Durchblick im Kernel-Chaos

Um den Linux-Kernel muss man sich spätestens dann kümmern, wenn Hardware unter Linux nicht funktioniert. Es ist allerdings nicht ganz einfach herauszufinden, welche Kernel-Version man benötigt.



VON THORSTEN EGGELING

Der Kernel ist ein zentraler Bestandteil des Betriebssystems. Er sorgt für die Einbindung der Hardware, stellt Softwareschnittstellen dafür bereit und er verwaltet den Speicher sowie die Prozesse. Neuere Kernel verbessern die Hardwareunterstützung. Falls das für neue Geräte erforderlich ist, muss man einen aktuelleren Kernel verwenden. Ubuntu und Linux Mint bietet unterschiedliche Methoden für die Installation.

Wann ein neuer Kernel erforderlich ist

Im optimalen Fall läuft nach der Linux-Installation alles rund, die Hardware im PC arbeitet anstandslos und ohne Fehler. In diesem Fall unterstützt der Kernel die verwendeten PC-Komponenten und es gibt keinen Handlungsbedarf.

Anders sieht es aus, wenn einzelne Geräte nach der Installation nicht funktionieren oder neue Hardware hinzugekommen ist, die von der genutzten Linux-Distribution nicht unterstützt wird. Zuerst sollte man ermitteln, ob es einen Kernel gibt, der die betroffene Hardware unterstützt.

Eine Analyse der Hardware lässt sich besonders einfach über *https://linux-hardware.org* durchführen. Nutzer von Ubuntu oder Linux Mint installieren das nötige Tool im Terminal mit

```
sudo apt install hw-probe
```

und starten es danach so:

```
sudo -E hw-probe -all -upload
```

Sie erhalten dabei eine URL, die Sie im Browser aufrufen. Auf der Seite sehen Sie unter „Host“, welchen Kernel Ihr System aktuell verwendet. Unter „Devices“ sind alle internen und externen Geräte mit Namen und IDs aufgelistet. Steht in der Spalte „Status“ der Eintrag „works“ oder „detected“, sollte das Gerät funktionieren. Beim Status „failed“ wurde kein Treiber gefunden, geladen oder konfiguriert. Wenn vorhanden, verweist ein Kasten rechts daneben auf eine mögliche Lösung.

Klicken Sie „failed“ an, um weitere Infos zum Gerät zu erhalten. Bei einer Meldung wie „We have not found a driver for the device in any Linux kernel versions up to 6.1“ gibt es bisher keinen Kernel, der die Hardware unterstützt. Oft befindet sich ein Treiber aber bereits in der Entwicklung. Sie finden dann Links zu Informationen über einen passenden Treiber, den Sie in der Regel selbst kompilieren müssen. Die Situation ist günstiger, wenn ein Treiber in einer aktuelleren als der auf Ihrem PC installierten Kernel-Version zu finden ist. Welche Möglichkeiten Sie dann haben, erklären die nachfolgenden Abschnitte.

Neue und neuere Kernel

Der Linux-Kernel wird fortlaufend weiterentwickelt und mit neuen Modulen (Treibern) für aktuelle Hardware ausgestattet. Einige Linux-Distributionen setzen auf besonders hohe Stabilität und aktualisieren die Hauptversion des Kernels während des Supportzeitraums nicht automatisch oder nur selten. Auskunft über die Kernel-Versionen gibt *www.kernel.org*. Die Langzeitunterstützung (LTS) geht zur Zeit (Stand Dezember 2022) zurück bis Kernel 4.9. Aktuelle LTS-Distributionen verwenden meist Kernel 5.4 bis 5.19.

Wer einen deutlich jüngeren Kernel benötigt, steigt am einfachsten auf eine Distribution um, die fortlaufend aktualisiert wird

(„Rolling Release“). Beispiele dafür sind Manjaro (*https://manjaro.org*) oder Open Suse Tumbleweed (*https://software.opensuse.org/distributions/tumbleweed*). Die Aktualität betrifft jedoch alle Pakete und nicht nur den Kernel. Die Pakete sind weniger ausgiebig getestet, weshalb man mit Inkompatibilitäten rechnen muss, die sich nur durch manuelle Eingriffe beheben lassen.

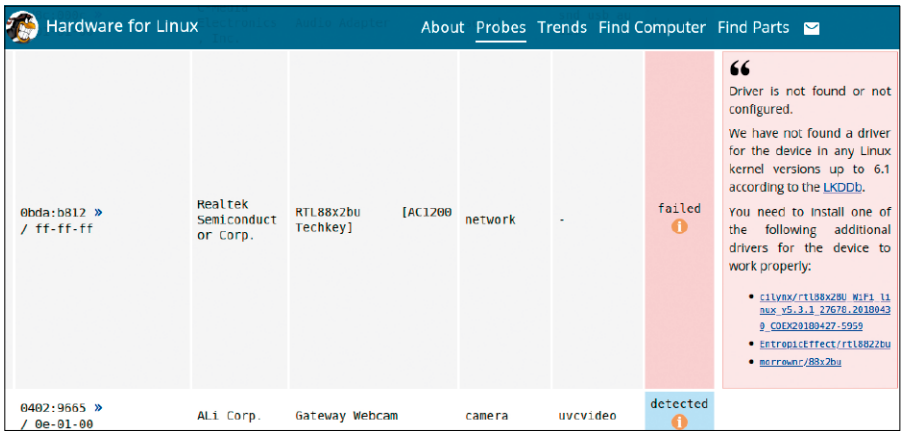
Langsame Entwicklung bei Ubuntu & Co.

Für Ubuntu erscheinen etwa halbjährig Point Releases (22.04.1, 22.04.2, und so weiter). Enthalten sind jeweils alle bisherigen Updates und ab Point Release xx.xx.2 nach knapp einem Jahr auch ein neuer Kernel (also ab Frühjahr 2013). Wer Ubuntu neu installiert, verwendet möglichst die aktuellste ISO-Datei von *https://ubuntu.com/download/desktop* und erspart sich damit umfangreiche Updatedownloads. Ein installiertes Ubuntu wird automatisch auf ein Point Release aktualisiert. Ubuntu 20.04 beispielsweise erhält den Kernel 5.15 (20.04.5), der auch in Ubuntu 22.04/ 22.04.1 enthalten ist.

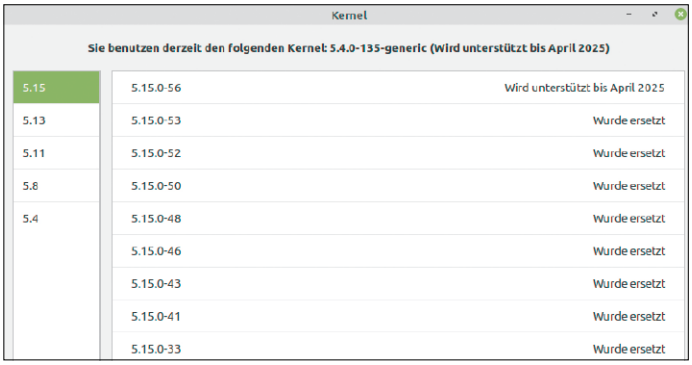
Wer den neueren Kernel schon jetzt benötigt, wechselt von Ubuntu 22.04 auf 22.10. Die STS-Version (Short Term Support) bietet auch neuere Programme, arbeitet aber möglicherweise nicht so zuverlässig wie ein LTS-Ubuntu. Ein Wechsel zur nächsten LTS-Version ist erst im April 2024 möglich (Ubuntu 24.04). Für die Umstellung starten Sie „Anwendungen & Aktualisierungen“ und gehen auf „Aktualisierungen“. Wählen Sie hinter „Über neue Ubuntu-Versionen benachrichtigen“ den Eintrag „Für jede Version“. Rufen Sie „Aktualisierungsverwaltung“ auf. Die neue Version wird Ihnen angeboten und lässt sich per Klick auf „Aktualisieren“ einrichten.

Linux Mint verfolgt eine konservativere Updatestrategie als Ubuntu. Ohne Eingriff des Benutzers bleibt es bei der ursprünglichen Kernel-Version. Linux Mint 20 basiert auf Ubuntu 20.04 und bringt daher den Kernel in der Version 5.4 mit. Point Releases gibt es ebenfalls, der Kernel bleibt aber standardmäßig bei Version 5.4.

Wer einen neueren Kernel benötigt, geht in der Aktualisierungsverwaltung auf „Ansicht → Linux Kernel“, wählt den aktuellsten Kernel (zur Zeit 5.15) und klickt auf „Installieren“. Danach ist das System auf dem gleichen Stand wie Ubuntu 20.04.5.



Hardware prüfen: Der Bericht auf *https://linux-hardware.org* zeigt an, für welches Gerät Treiber fehlen. Man muss den Treiber selbst kompilieren oder zu einem neueren Kernel wechseln.



Neue Kernel für Linux Mint: Die Distribution installiert neue Kernel nicht automatisch. Über die Aktualisierungsverwaltung lassen sich Upgrades auswählen – sofern verfügbar.

Ein Upgrade auf Linux Mint 21 (basiert auf Ubuntu 22.04) ist ebenfalls möglich. Dazu führt man im Terminal diese beiden Befehlszeilen aus:

```
sudo apt install mintupgrade
sudo mintupgrade
```

Folgen Sie den Anweisungen des Assistenten. Das aktualisierte System verwendet Kernel 5.15, was Stand Dezember 2022 die höchste verfügbare Version für Ubuntu 20.04/22.04 sowie Linux Mint 20/21 ist.

Individuellen Kernel verwenden

Ubuntu und Linux Mint lassen sich auch mit einem deutlich neueren Kernel ausstatten, als die Distributionen bieten. Die DEB-Pakete für die Installation sind unter *https://kernel.ubuntu.com/~kernel-ppa/mainline* zu finden. Die neuesten Versionen lassen sich allerdings nicht in den LTS-Ausgaben installieren, weil einige Bibliotheken zu alt sind. Man kann den Kernel selbst erstellen, was mit einem gewissen Zeitaufwand verbunden ist.

Eine ausführliche Anleitung können Sie über *https://m6u.de/BMKE* abrufen. Derzeit lassen sich die Kernel-Versionen 5.16 bis 6.0 unter Ubuntu 20.04/22.04 sowie Linux Mint 20/21 kompilieren.

Ungenutzte Kernel entfernen

Ubuntu und Linux Mint entfernen ältere Kernel nicht automatisch, was der Sicherheit dient. Halten Sie beim Start des PCs die Umschalt-Taste gedrückt. Im Grub-Menü lässt sich dann über „Advanced options for Ubuntu“ ein älterer Kernel starten. Bei einem bereits länger genutzten System sammeln sich zahlreiche Kernel-Versionen an. Problematisch können Installationen mit einer eigenen Bootpartition sein. Ist diese nicht ausreichend bemessen, schlägt die Installation einen neuen Kernels fehl. Im schlimmsten Fall führt das zu einem undefinierten Zustand und Linux startet nicht mehr. Sie sollten daher die Befehlszeile

```
sudo apt autoremove
```

regelmäßig ausführen. Damit entfernen Sie nicht mehr verwendete Pakete inklusive alter Kernel-Versionen. Nebenbei geht dann auch die Installation neuer Kernel schneller, weil der Paketmanager die Ramdisk-Dateien und Treiber für weniger Kernel-Instanzen erzeugen muss. ■

Linux-Systeme vereinfachen

Desktopnutzer haben meist weder den Ehrgeiz noch die Voraussetzungen, in die Tiefen der Rechteverwaltung oder Webserver-Konfiguration hinabzusteigen. Das heißt aber nicht zwingend, dass man auf Linux-Vorzüge verzichten müsste.

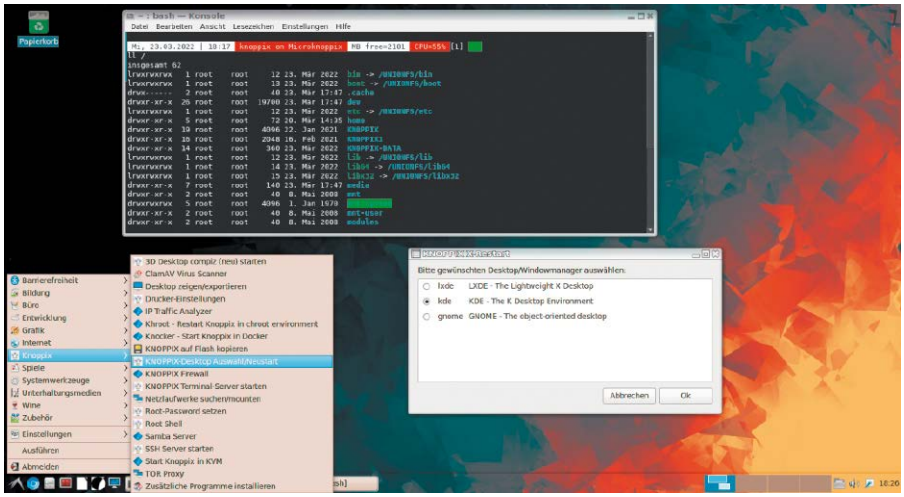
VON HERMANN APFELBÖCK

Einfacher ist besser: Die nachfolgenden Tipps und Anregungen zielen auf grundlegende Systemvereinfachungen. Sie richten sich an typische Desktopnutzer und an Home-Admins, die einen unkomplizierten Systemalltag gegenüber hohen Sicherheitsansprüchen klar priorisieren. In einem privaten Umfeld sind alle beschriebenen Maßnahmen jederzeit zu vertreten.

Livesystem als Arbeitssystem

Auch heutzutage ist es noch möglich, ein ganz simples (Single-User-)Desktopsystem à la Windows 98 zu verwenden, das ohne Benutzerrechte, ohne Anmeldung einfach zum Desktop durchstartet. Die Lösung sind Linux-Livesysteme mit einem einzigen Live-User mit allen Rechten. Davon gibt es jede Menge, aber für produktiven Einsatz sollte es ein möglich anpassungsfähiges mit einem alltagstauglichen Desktop sein sowie mit einer Einrichtungsoption auf interne Festplatten.

Als den wahrscheinlich besten Kandidaten empfehlen wir Knoppix. Der Live-Klassiker steht derzeit bei Version 9.1 und ist über *www.knopper.net/knoppix-mirrors* zu beziehen. Achten Sie in der Liste der ISO-Dateien auf „-DE“ im Dateinamen, um das deutschsprachige System herunterzuladen. Das Knoppix-ISO ist im ersten Schritt mit den üblichen Tools wie dd, Gnome-Disks, Etcher (*https://etcher.io*) oder Win 32 Disk Imager auf USB-Stick zu kopieren. Aus dem gestarteten Livesystem können Sie Knoppix dann für den Dauerbetrieb auf die Festplatte des Geräts übertragen. Das maßgebliche Tool



Simples Linux gewünscht? Livesysteme wie Knoppix sind Ein-Benutzer-Systeme ohne Anmeldung und Dateirechte. Für flexible Anpassungen und Verschlüsselung sorgt eine Overlaypartition.

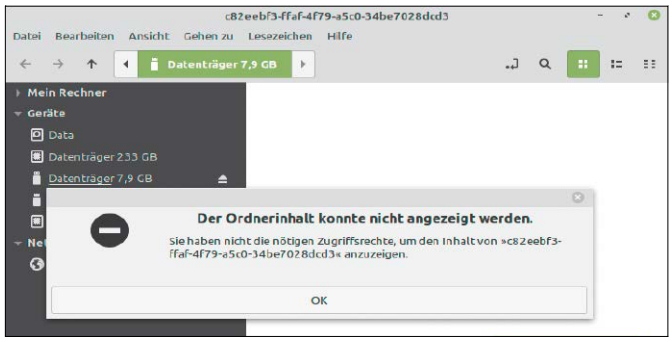
finden Sie im Menü unter „Knoppix → Knoppix auf Flash kopieren“. Das Werkzeug ist der Installationsassistent für Kopien auf beschreibbare USB- und SD-Medien, kann aber auch für die Einrichtung auf Festplatten genutzt werden – gleich der erste Dialog fragt ab, ob auch interne Festplatten als Ziel infrage kommen. Nach Auswahl des gewünschten Zieldatenträgers wählen Sie „Installation auf FAT32 mit zusätzlicher Overlay-Partition“. Die nächste Abfrage „Möchten Sie Knoppix remastern?“ wäre nur relevant, wenn Sie das Knoppix-System, mit dem Sie gerade installieren, bereits individuell angepasst haben. Die Abfrage zur Größe der Overlaypartition übernehmen Sie einfach mit „OK“: Dann erhält die Overlaypartition die komplette Kapazität, die das eigentliche Knoppix-System übrig lässt. Schließlich können Sie entscheiden, ob die beschreibbare Overlaypartition verschlüsselt werden soll. Es handelt sich um die einzige Möglichkeit, ein Knoppix-System systemweit zu schützen. Für ein mobiles Notebook sollten Sie diese Option nutzen, bei einem stationären heimischen Rechner entscheiden Sie je nach Umfeld.

Die Knoppix-Installation mit Overlaypartition macht das Livesystem anpassungsfähig: Es bietet Platz für persönliche Daten und erlaubt dauerhafte Anpassungen, Installationen, Deinstallationen (apt im Terminal oder Synaptic-Paketverwaltung).

Knoppix hat neben dem spröden LXDE-Standarddesktop auch noch Gnome und KDE Plasma an Bord. Die Umstellung erfolgt ganz einfach über den Menüpunkt „Knoppix → Knoppix-Desktop Auswahl/Neustart“. Knoppix startet so lange mit einem einmal gewählten Desktop, bis Sie über den genannten Menüpunkt wieder zu einer anderen Oberfläche wechseln.

Einfacher Austausch von USB-Datenträgern

Wenn USB-Sticks oder -Festplatten nur dem unkomplizierten Datenaustausch dienen, ist es besser, bei der Formatierung des Datenträgers auf die Linux-Dateisysteme Ext4, XFS, BTRFS zu verzichten. Unter Windows sind diese Dateisysteme generell nicht lesbar, aber auch unter Linux erst einmal unhandlich: Diese Dateisysteme tragen als Besitzer immer das Konto ein, das den Datenträger formatiert hat. Dies hat zur Folge, dass auf anderen Linux-Systemen zunächst kein Zugriff erlaubt ist, was dann erst umständlich durch Ändern des Besitzrechts und der Dateirechte korrigiert werden muss. Unkompliziert und quasi rechtelos verhalten sich USB-Laufwerke, die mit den Dateisystemen NTFS, FAT32 oder exFAT formatiert sind. Sie erscheinen sofort automatisch im Dateimanager und jedes beliebige Konto erhält standardmäßig Lese- und Schreibzugriff.



Der USB-Stick verweigert den Zugriff. Grund ist eine Formatierung mit Ext4 (XFS, BTRFS), das den formatierenden Nutzer zum Besitzer des Datenträgers macht.

Groß-/Kleinschreibung ignorieren

In Linux ist die Beachtung der Groß- und Kleinschreibung zwingend: Den Befehl „LSBLK“ gibt es nicht und ein Schalter „-X“ bedeutet etwas anderes als „-x“. Trotzdem kann man sich die Terminalnutzung insofern vereinfachen, als die Tab-Autocompletion auch bei inkorrekter Schreibweise anschlägt. Dann wird das Terminal etwa nach

```
cd v[Tabulatortaste]
```

zum Ordnernamen „Vorlagen“ erweitern, obwohl „v“ klein geschrieben wurde. Diese Toleranz erreicht man systemweit (für alle Benutzer) mit dem Eintrag

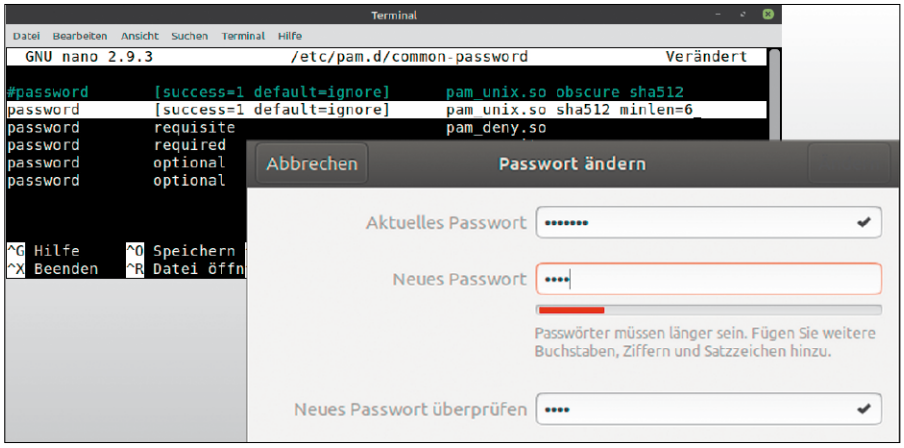
```
set completion-ignore-case on
```

in der Datei „/etc/inputrc“. Der Eintrag benötigt sudo-Recht.

Einfacheres Systempasswort

Wer über sudo das System verwaltet, muss das Systempasswort häufig eingeben. Komplexe Kennwörter sind da eher lästig – und auf einem Desktopsystem auch nicht notwendig. Abgesehen vom Erstbenutzer, der bei der Installation eingerichtet wird, stellen Ubuntu & Co. aber erhöhte Komplexitätsanforderungen (Mindestlänge, Sonderzeichen) an das Passwort für alle weiteren Konten. Das gilt auch, falls Sie das Passwort für das Erstbenutzerkonto nachträglich ändern möchten.

Wie immer unter Linux gibt es eine Stelle, um diese Standards zu steuern: Öffnen Sie die Datei „/etc/pam.d/common-password“ mit root-Recht in einem Editor, so finden Sie in der ersten „password“-Zeile die Anweisung „obscure“. Das erzwingt eine Mindestkomplexität des Passworts (Sonderzeichen) und kann einfach gelöscht werden. Durch die Ergänzung „minlen=5“ (Beispiel) am Ende derselben Zeile können Sie die Mindestlänge auf den gewünschten Wert herabsetzen.



Einfachere Systempasswörter erlauben: Eine Konfigurationsdatei bestimmt über Komplexität und Mindestlänge der Kennwörter.

Passworteingabe im Terminal

Standardmäßig schreibt man im Terminal das sudo-Kennwort ohne Rückmeldung im Blindflug – eine auf Desktopsystemen eher paranoide Sicherheitseinstellung, um die Länge des Passworts zu verbergen. Es ist aber kein Problem, sich die getippten Buchstaben mit Stellvertreterzeichen „*“ anzeigen zu lassen. Der Aufruf

```
sudo visudo
```

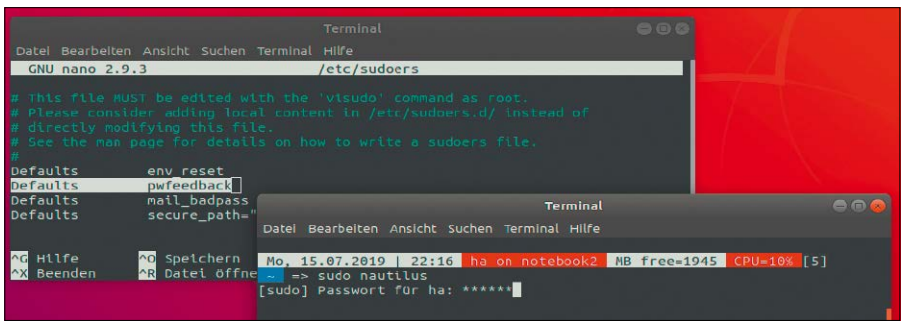
öffnet die Datei „/etc/sudoers“ im voreingestellten Editor. Unter

```
Defaults env_reset
```

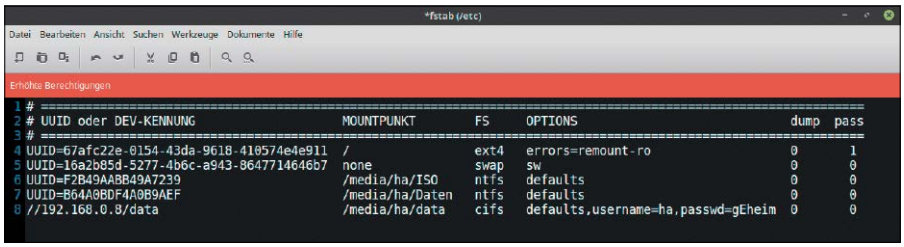
fügen Sie die zusätzliche Zeile

```
Defaults pwfeedback
```

ein. Nach dem Speichern (Strg-O) und Beenden des Editors (Strg-X) zeigt die sudo-Abfrage ein Sternchen pro eingegebenem Zeichen.



Kennworteingabe mit Feedback: Eine Option in der Datei „/etc/sudoers“ sorgt dafür, dass bereits eingegebene Zeichen des Kennworts durch Sternchen bestätigt werden.



Kommentierte und sauber formatierte „/etc/fstab“: Diese wichtige Datei erhält durch Leerzeichen eine gut lesbare Tabellenform.

Konfigurationsdateien vereinfachen

Wer sich mit Linux-Diensten wie SSH, Apache, Samba beschäftigt, liest häufig den lapidaren Hinweis, dass die zugehörigen Konfigurationsdateien „gut kommentiert“ seien. Tatsächlich sind aber schnell Stunden investiert, um den kompletten Anweisungsumfang etwa für den SSH-Server zu verstehen („/etc/ssh/sshd_config“). Typischerweise sind die meisten Optionen mit „#“ oder „;“ auskommentiert. Dazu gibt es englischsprachige Textkommentare vor den eigentlichen Anweisungen, welche die Bedeutung erklären. Hauptproblem dabei ist, dass es keine Aussagen zur Relevanz der jeweiligen Anweisung gibt und viele Einstellungen kaum alltagsrelevant sind.

Vereinfachen Sie Dateien wie „/etc/ssh/sshd_config“ (SSH-Server) oder „/etc/samba/smb.conf“ (Samba-Netzfreigaben), indem Sie alle nicht relevanten, alle auskommentierten Anweisungen und alle auskommentierten Kommentierungen einfach löschen.

Aber – stop! Bevor Sie das tun, kopieren Sie die Datei mit (Beispiel)

```
sudo cp sshd_config sshd_config.
  original
```

Damit kommen Sie bei Bedarf später wieder an alle Optionen und Erklärungen. Eine eindeutige, nur hierfür verwendete Extension wie „.original“ ist obendrein hilfreich, um schnell alle bereits bearbeiteten Konfigurationsdateien aufzufinden – etwa mit locate

```
locate *.original
```

oder einem anderen Suchtool.

Konfigurationsdateien wie „fstab“ oder „crontab“ sind obendrein schwer lesbar. Das liegt daran, dass die Parameter wegen unterschiedlichen Textlängen visuell schlecht abzugrenzen sind. Als Trenner für die Parameter dienen Leerzeichen oder Tabulatoren. Da die Menge der Leerzeichen und Tabulatoren in diesen Konfigurationsdateien keine Rolle spielt, bietet es sich an, solche Dateien mit diesen simplen Mitteln in eine übersichtliche Tabellenform zu bringen.

Snap- und Flatpak-Container

Snap- und Flatpak-Container erhöhen erst einmal die Komplexität eines Linux-Systems. Außerdem ist die enorme Größe dieser Softwarecontainer (insbesondere von Flatpaks) ein triftiger Grund, Snaps und Flatpaks bei Anwendungsprogrammen aus dem Weg zu gehen. Für einige Serveranwendungen bedeuten diese Container aber eine enorme Vereinfachung. Wenn der Container neben der eigentlichen Anwendung auch gleich den Serverdienst mitbringt, entfällt die Einrichtung des Servers (Apache oder Nginx).

Auf *https://flathub.org* und *https://snapcraft.io* gibt es etliche Servercontainer wie Minidlna, Openhab oder Plexmediaserver. Ein prominentes Beispiel ist Nextcloud als Snap-Container inklusive Apache-Webserver. Voraussetzung für solche Containerinstallationen ist in jedem Fall, dass die zugehörige Umgebung auf dem System installiert ist, für Snaps das Paket „snapd“. Zur Installation der Nextcloud genügt dann dieser Terminalbefehl:

```
sudo snap install nextcloud
```

Danach ist die Nextcloud sofort unter der IP-Adresse des Serverrechners im Netzwerk erreichbar. Das soll nicht unterschlagen, dass die Nextcloud als Web- oder Intranetanwendung eine komplexe Software bleibt, aber um das darunterliegende Apache und PHP muss sich der Nutzer nicht mehr kümmern.

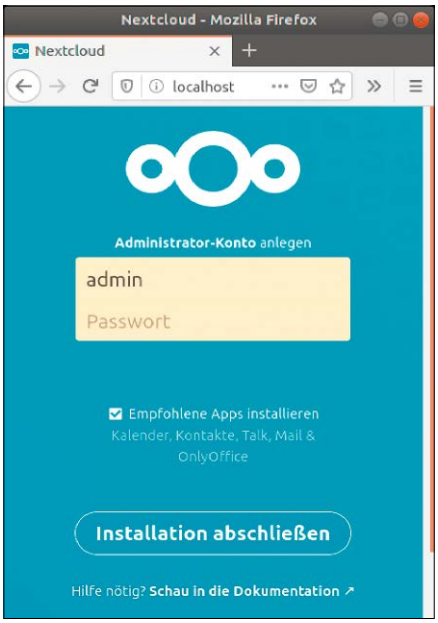
Bei einigen weiteren Snap-Serveranwendungen sind mindestens zusätzliche Schritte nötig wie das Starten (Beispiel)

```
sudo snap start upnp-server
```

oder eventuell eine Nachfrage (Beispiel)

```
sudo snap info upnp-server
```

über die Funktionsweise und Erreichbarkeit des Servers.



Serveranwendungen als Container: Einige komplexe Webanwendungen wie hier Nextcloud liefern im (Snap-)Container den Server gleich mit und sind damit mühelos zu installieren.

Docker-Container: Docker ist ein weiteres auf Serveranwendungen spezialisiertes Containerformat. Es kann die Einrichtung vieler Web- und Intranetdienste wie Wordpress oder Joomla deutlich vereinfachen. Andererseits erfordert Docker aber eine gründliche Einarbeitung in seine eigene Kommandoverwaltung und ist daher kein Thema für typische Desktopanwender, die mit Containerformaten in erster Linie der Serververwaltung aus dem Weg gehen wollen.

Vereinfachte Samba-Freigaben

Bei Linux-Datenservern mit Samba gibt es immer wieder Zugriffsprobleme. Ursache sind in der Regel nicht die relativ einfachen Netzwerkrechte, sondern mangelnde lokale Rechte auf dem Dateisystem des Servers. Jeder Netzwerkzugriff setzt auf dem Server zwei Konten voraus – das Samba-Konto mit der Erlaubnis für den Netzzugriff und das Systemkonto für das Zugriffsrecht im Dateisystem.

Im privaten Umfeld lässt sich die Rechteproblematik mit folgenden zwei Szenarien fundamental vereinfachen. Im Prinzip ist auch deren Kombination möglich, was aber den simplifizierenden Charme verringert:

A. Sie legen auf dem Serversystem für alle Teilnehmer ein Systemkonto

```
sudo adduser anna
sudo adduser bert
```

und ein Samba-Konto an:

```
sudo smbpasswd -a anna
sudo smbpasswd -a bert
```

Zur besseren Übersicht ist es zu empfehlen, die (im Prinzip unabhängigen) Kennwörter für Systemkonto und Samba-Konto identisch zu wählen. Danach genügt es, in der Samba-Konfigurationsdatei „/etc/samba/smb.conf“ die Zeile

```
; [homes]
```

zu suchen und das Semikolon zu entfernen. Nach einem Neustart (oder nach *sudo systemctl restart smbd*) hat jedes Konto vollen Netzzugriff auf sein „Home“. Probleme mit den Dateirechten können im eigenen „Home“ nicht auftreten. Für Datenschutz ist ebenfalls gesorgt, weil jedes Konto nur sein eigenes „Home“ sieht.

B. Für ein zentrales Serverangebot für alle mit Film, Musik, Fotos und Dokumenten sind die genannten Home-Freigaben ungeeignet. Eine allgemeine Freigabe lässt sich im einfachsten Fall mit einem einzigen System- und Samba-Konto realisieren:

```
sudo adduser darfsamba
sudo smbpasswd -a darfsamba
```

In der Konfigurationsdatei „smb.conf“ genügt dann am Ende unter „Share Definitions“ folgender Block (Beispiel):

```
[Data]
path = /srv/data
valid users = darfsamba
write list = darfsamba
```

Nun muss im Freigabepfad („/srv/data“) nur noch sichergestellt sein, dass das Pseudo-Konto den Dateibesitz hat (*sudo chown -R darfsamba:darfsamba /srv/data*).

Der Vorteil: Alle Geräte und Teilnehmer greifen mit einem einzigen Konto zu, womit alle Rechteprobleme ausgeschlossen sind.

Der Nachteil: Jeder, der Name und Passwort des Pseudo-Kontos kennt, darf alles. Sie müssen also den Teilnehmern vertrauen, dass sie weder fahrlässig noch destruktiv unterwegs sind.

Mobiles „Home“-Verzeichnis

Ein transportables Home-Verzeichnis auf USB oder SD ist erst einmal komplizierter, denn dessen Einrichtung erfordert bei der Installation einen zusätzlichen Schritt bei der Partitionierung. Einmal eingerichtet bedeutet es aber eine erhebliche Vereinfachung. Dann steht für mehrere Systeme dasselbe vertraute Home zur Verfügung, desgleichen auch bei Neuinstallationen. Linux-Installer bieten die separate Home-Partition nicht standardmäßig an, sondern fordern dazu manuelle Partitionierung. Neben der internen Festplatte für das System muss ein USB-Laufwerk oder eine SD-Karte für das Home angeschlossen sein. Kapazitäten von 64 bis 256 GB sind dabei eher die Untergrenze. Im Ubuntu-Installer wählen Sie im Dialog „Installationsart“ die Option „Etwas Anderes“, in Calamares (Kubuntu, Lubuntu, Manjaro) entspricht das der Option „Manuell“. Dann wählen Sie das Laufwerk, auf dem Sie das System installieren möchten – in der Regel die erste interne Festplatte „/dev/sda“, löschen dort alles und legen im entstandenen freien Speicherplatz neue Partitionen an. Beginnen Sie mit einer Partition vom Dateisystemtyp „EFI-System-Partition“. Dort ist nur eine Größenangabe erforderlich (100 MB genügen). Den verbleibenden Speicherplatz auf der internen Festplatte übergeben Sie mit voller Kapazität, mit Dateisystem Ext4 und Einbindungspunkt „/“ an das Betriebssystem.

Auf dem zweiten USB- oder SD-Datenträger erstellen Sie nun die Home-Partition. Der passende Einbindungspunkt „/home“ wird im Drop-down-Feld angeboten. Als Dateisystem verwenden Sie auch hier Ext4.

Wichtig: Wenn der externe Home-Datenträger bereits das vollständige Home von einem anderen Linux mitbringt, müssen Sie unbedingt auf die Formatierungsoption verzichten, um alle Daten zu erhalten.

Den Home-Datenträger können Sie später als Datenlaufwerk an jedes andere Linux-System anschließen und haben damit nicht nur die persönlichen Benutzerdateien, sondern auch alle Konfigurationsdateien vorliegen. Somit lassen sich ausgewählte Daten (oder auch alle) in das jeweils lokale „/home“ übertragen.

Darüber hinaus ist es möglich, den Home-Datenträger als reguläres „Home“ in andere Linux-Systeme einzubinden. Wie das bei einer Neuinstallation gelingt, wurde bereits oben beschrieben. Bei einem System, das bislang keine eigene Home-Partition nutzt, ermitteln Sie zunächst mit

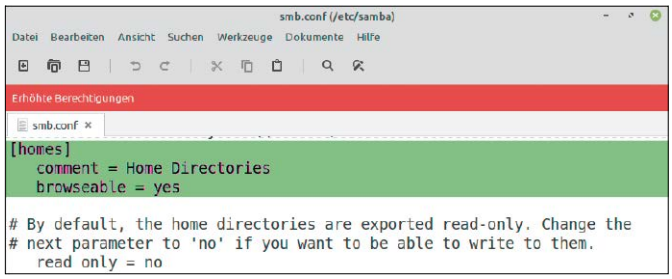
```
lsblk -f
```

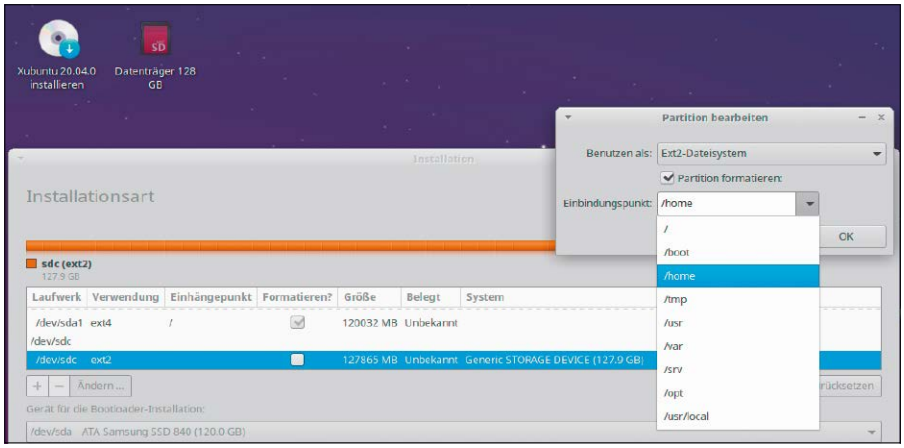
die UUID-Kennung des USB- oder SD-Mediums. Danach tragen Sie das Laufwerk mit Mountpunkt „/home“ in die Datei „/etc/fstab“ ein:

```
UUID=[…] /home ext4 defaults 0 0
```

Die UUID haben Sie vorher ermittelt; das Dateisystem „ext4“ passen Sie bei Bedarf an, falls lsblk ein anderes Dateisystem gemeldet hatte. Nach einem Neustart verwendet das System den neuen Datenträger als Home. ■

Freigaben für alle Systembenutzer: Entfernen Sie die Kommentarzeichen beim Block „[homes]“. Dann kann jeder Benutzer von anderen PCs aus auf sein Home-Verzeichnis zugreifen.





Eine Home-Partition auf USB oder SD ermöglicht ein Home-Verzeichnis für mehrere Systeme und lässt sich auch in Neuinstallationen einbinden.

Apache für Einsteiger

Wer Inhalte online stellen will (egal ob im WWW oder im lokalen Netz), benötigt einen HTTP-Webserver. Apache ist dafür der populärste Kandidat, bietet bereits solo viele Optionen, ist aber oft Basis für CMS-, Wordpress-, Nextcloud- oder Wiki-Lösungen.

VON HERMANN APFELBÖCK

Apache ist nicht die einzige Serversoftware zum Ausliefern von Webseiten über das HTTP-Protokoll. Sie ist aber die prominenteste und universellste, außerdem meistverbreitet und am besten dokumentiert. Alternativen wie Nginx oder Lighttpd sind hinsichtlich Aufbau und Konfiguration ähnlich und punkten durch eventuelle Geschwindigkeitsvorteile. Dieser Beitrag konzentriert sich ausschließlich auf Apache, zumal Leistungsvorteile von Nginx oder Lighttpd beim hier beschriebenen Einsatz im lokalen Netz nicht ins Gewicht fallen.

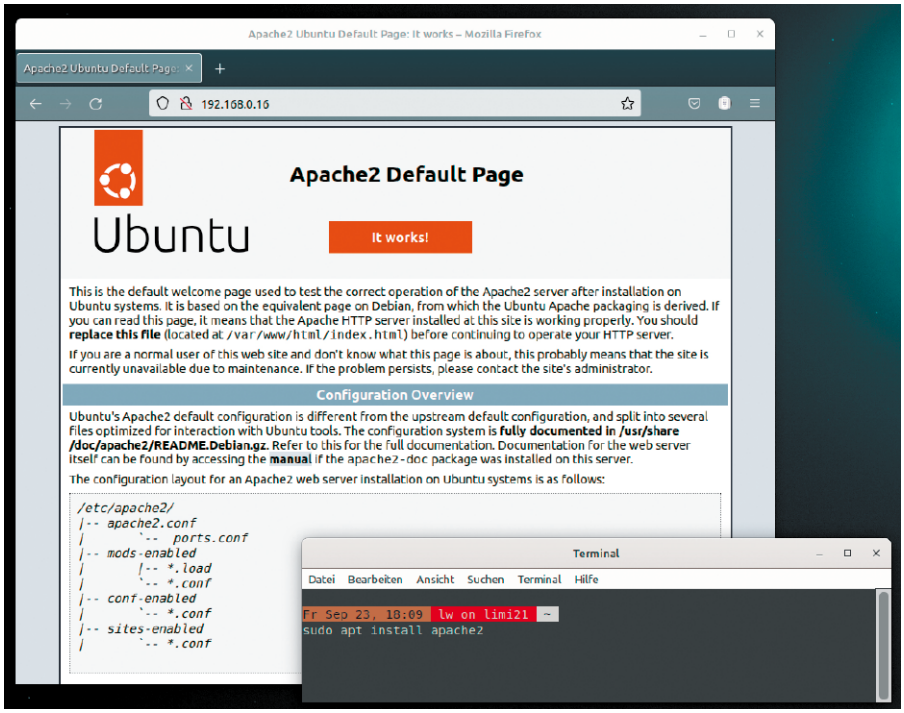
Installation des Apache-Servers

Meistens wird die Apache-Installation gleich im Rahmen eines kompletten LAMP-Servers beschrieben (Linux-Apache-My-SQL-PHP). Unter der Annahme, dass Linux bereits vorliegt, verbleiben der Webserver Apache, die Datenbank My SQL (oder Maria DB) und die Script-Sprache PHP. Notwendig sind diese Zutaten tatsächlich für viele Webanwendungen, aber nicht überall. Apache kann auch ohne Datenbank und PHP immerhin statische HTML-Seiten ausliefern – eine Option, die für ein Intranetportal oder eine Homepage genügen kann.

Installation: Für die Installation des puren Webservers verwenden Sie im Terminal

```
sudo apt install apache2
```

Damit ist der Serverdienst auch sofort und automatisch gestartet. Im Browser auf dem betreffenden Rechner rufen Sie *http://localhost* auf und sehen dann die Apache-Standardseite („/var/www/html/index.html“). Auf allen anderen Rechnern im Netzwerk verwenden Sie die IP-Adresse des neuen Servers, also etwa „http://192.168.178.20“. Die IP-Angabe funktioniert natürlich auch auf dem Serverrechner selbst. Die IP-Adresse erfahren Sie auf dem Server mit „ip address“ oder über das Netzwerksymbol und „Netzwerkeinstellungen“ auf dem Desktop des Servers.



Das ist weit mehr, als es scheint: Wenn Apache nach der Installation diese Standardseite („index.html“) im Browser anzeigt, ist der Weg für andere und eigene Inhalte geebnet.

Hinweis: Die unkomplizierte Apache-Installation, die den Webserver auch gleich startet, hat nur eine wichtige Bedingung: Es darf auf dem System kein Snap-Container vorliegen, der seinen eigenen Apache-Server mitbringt (etwa Nextcloud). Die daraus resultierenden Konflikte sind eine Herausforderung und für Apache-Einsteiger unbedingt zu vermeiden.

Purer Apache für statische Portale

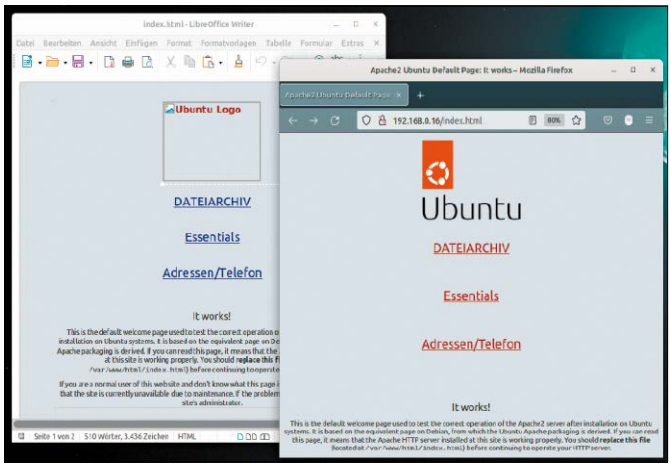
Nach der beschriebenen Installation liefert der Webserver die einzige statische Datei „index.html“ aus dem Standardpfad „/var/www/html/“ – mit der Apache-Meldung „It works!“ und einigen Infos. Mit anderen Worten: Beim Abruf der Serveradresse (Beispiel)

```
http://192.168.178.20
```

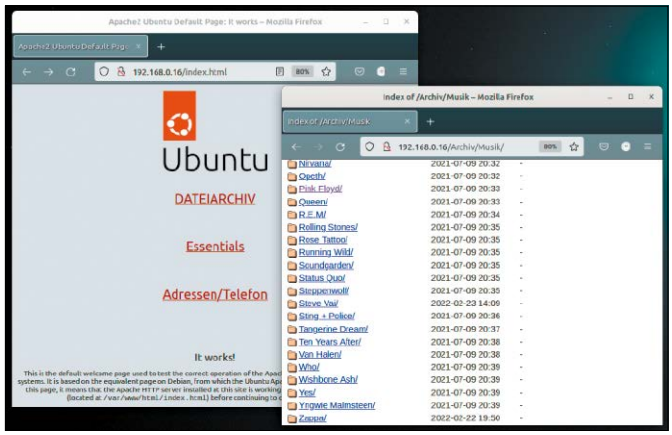
im Browser sieht der Webserver in seinem „DocumentRoot“-Verzeichnis nach, welche HTML-Dateien dort vorliegen. Die Datei „index.html“ (oder „index.php“, wenn PHP aktiv ist) ist die Standarddatei, die er ohne Namensangabe automatisch lädt. Liegen unter „/var/www/html/“ weitere HTML-Dateien vor, lädt Apache diese, sofern man sie im Browser explizit anfordert – etwa:

```
http://192.168.178.20/infos.html
```

Für eine Sammlung statischer Infodateien würde es also schon genügen, unter „/var/www/html/“ einige HTML-Dateien abzulegen. Die automatisch gestartete „index.



Statische Inhalte: Ein paar Anpassungen der originalen „index.html“ und eigene HTML-Dateien machen aus „It works!“ schnell ein eigenes Portal.



Standardmodul „autoindex“: Wo die Datei „index.html“ fehlt, bietet Apache eine Ordnernavigation. Alles, was der Browser kann, lässt sich anzeigen oder abspielen (Text, PDF, Audio).

html“ wäre dann am besten durch eine Übersichtsseite zu ersetzen, die dann die Hyperlinks auf weitere Unterseiten anbietet. Bequeme HTML-Editoren für solche Aufgaben sind nicht rar: Mit Writer aus Libre Office oder Word aus Microsoft Office sind vorhandene Texte im Handumdrehen nach HTML umgewandelt oder bei Bedarf auch nachbearbeitet.

Damit sind aber die Möglichkeiten längst nicht ausgeschöpft. Neben HTML-Dateien sind zahlreiche andere Dateiformate unter „/var/www/html/“ sinnvoll, die jeder Browser anzeigen oder wiedergeben kann – pure Texte, PDFs oder auch Audiodateien. Diese kann Apache aufgrund des standardmäßig aktivierten Modules „autoindex“ ohne zusätzliche Software bereitstellen. Es genügt also, unter „/var/www/html“ Ordner wie „Texte“ oder „Musik“ zu erstellen und dorthin die gewünschten Dateien oder gleich ganze Verzeichnisstrukturen zu kopieren. Überdies ist es möglich, einen Datenträger einfach nach „/var/www/html/[Name]“ zu mounten und auf diese Weise über Apache zugänglich zu machen. Die Navigation im Browser erfolgt intuitiv wie in einem Dateimanager. Dateiformate, die der Browser nicht anzeigen oder wiedergeben kann, führen standardmäßig zum Download auf das zugreifende System.

Konfigurationsdateien und Terminalbefehle

Wie angesprochen sucht Apache seine Inhalte standardmäßig unter „/var/www/html/“. Dieses Startverzeichnis ist nicht hart codiert, sondern durch eine Apache-Konfigurationsdatei vorgegeben:

/etc/apache2/sites-enabled ist der wichtigste Ordner für die Konfiguration und enthält standardmäßig nur die Datei „000-default.conf“. Abgesehen von den #-Kommentarzeilen enthält die Datei nur eine Handvoll aktiver Anweisungen: Für Apache-Neulinge relevant ist vorläufig nur die Tatsache, dass hier das Apache-Startverzeichnis als

```
DocumentRoot /var/www/html
```

eingetragen ist und der Server über Port 80 kommuniziert:

```
<VirtualHost *:80>
```

Port 80 ist der Standardport für HTTP-Server mit dem Privileg, dass die Portangabe beim Zugriff unterbleiben darf. Standardmäßig ist daher der Zugriff mit „http://[Adresse]“ funktionsidentisch mit „http://[Adresse]:80“ und führt zu den Inhalten im „DocumentRoot“.

Diese Direktiven zeigen, dass Apache bei Bedarf auch andere Ports nutzen (etwa für eine zweite Serverinstanz) und dafür ein anderes Startverzeichnis („DocumentRoot“) verwenden kann. Einsteigern empfehlen wir, diese Vorgaben unverändert zu belassen. Unsere Hinweise auf diese Konfigurationsdatei und „DocumentRoot“ sind aber trotzdem Pflicht, weil manches fatal erscheinende Apache-Problem nur daran liegt, dass dieser Pfad nicht stimmt, sondern etwa „/var/www/html/wordpress“ lauten muss.

Noch ein Hinweis zum „DocumentRoot“: Der Startpfad ist zwar editierbar und variabel, aber aus Sicherheitsgründen nicht beliebig. Er sollte immer unter „/var/www/html“ liegen, bei Bedarf in gesonderten Unterverzeichnissen wie schon oben für das Beispiel „wordpress“ angedeutet. Die Datei „000-default.conf“ unter „/etc/apache2/sites-enabled“ ist nur ein Link auf die gleichnamige Konfigurationsdatei im Ordner „/etc/apache2/sites-available“. Ob eine Apache-Serverinstanz aktiv ist, entscheidet daher allein die Tatsache, dass ein Link unter „sites-enabled“ existiert. Für das Ein- oder Ausschalten – also das Setzen oder Entfernen des Links – gibt es diese Hilfsbefehle im Terminal:

```
sudo a2ensite #Einschalten
sudo a2dissite #Ausschalten
```

Die verfügbaren Instanzen werden automatisch zur Auswahl angezeigt. Leider erledigen diese Kommandos (und alle anderen „a2*“-Befehle) nicht selbständig, Apache über diese Änderung zu informieren. Dies muss danach mit

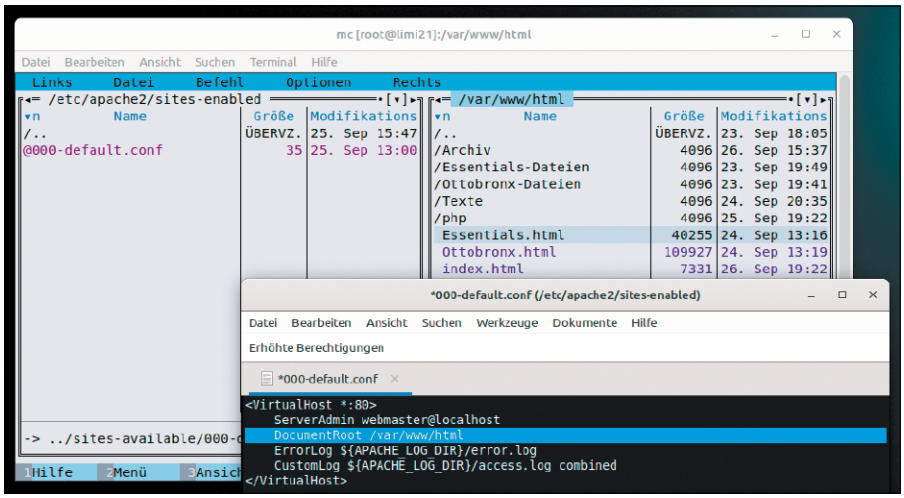
```
sudo systemctl restart apache2
```

erfolgen.

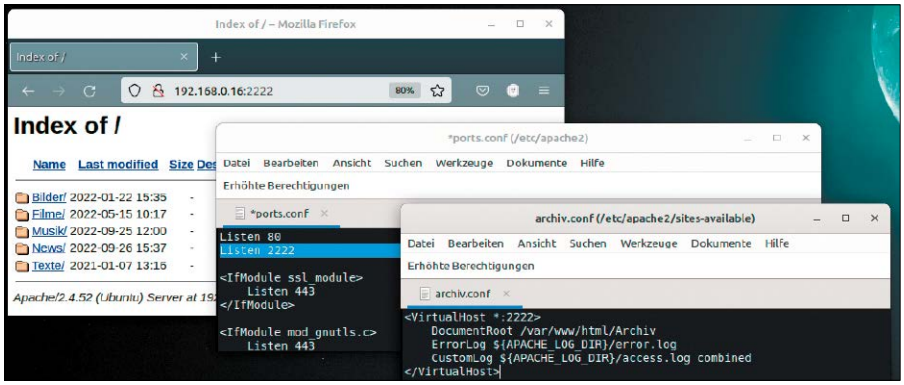
Dieser Befehl ist auch nach jeder Änderung in den Konfigurationsdateien nötig, damit der Webserver diese neu einliest.

/etc/apache2/ports.conf: Hier ist festgelegt, welche Netzwerkports der Webserver berücksichtigt. Standardmäßig sind das Port 80 (HTTP) und Port 443 (HTTPS). Einsteiger sollten dies so belassen. Einen triftigen Grund, dies zu ändern, gibt es nur, wenn der Server (unter „/etc/apache2/sites-enabled“) mehrere Instanzen ausliefern soll und daher verschiedene „VirtualHosts“ mit unterschiedlichen Ports benötigt. Ein weiterer zwingender Grund wäre ein zweiter aktiver HTTP-Server wie Nginx, der die Ports 80 und 443 für sich beansprucht.

/etc/apache2/apache2.conf: Dies ist die primäre Apache-Konfigurationsdatei, die



Aktive Website (000-default.conf): Die Basiskonfiguration besteht praktisch nur aus der Portangabe (80) und dem Startverzeichnis, ab welchem Apache die Daten ausliefert.



Konfigurationsdatei „ports.conf“: Die Datei ist nur relevant, wenn Apache eine zweite Site anbieten soll. Diese muss dann eine andere Portnummer erhalten.

vor und über einzelnen Serverinstanzen steht. Eventuelle Konfigurationsprobleme sind am wenigsten hier zu suchen, erst recht nicht, wenn man die „apache2.conf“ unverändert belässt.

/etc/apache2/mods-enabled: Exakt wie bei den Apache-Webseiten „/etc/apache2/sites-“ gibt es auch für Apache-Module die korrespondierenden Verzeichnisse „/etc/apache2/mods-available“ und „/etc/apache2/mods-enabled“. Auch hier gilt das identische Muster, dass installierte und verfügbare Module („available“) durch eine Verlinkung nach („enabled“) aktiviert werden. Und auch hier gibt dafür die passenden Terminalhilfen a2enmod und a2dismod. Einsteigern ist zwar vom Ein- und Ausschalten von Apache-Modulen zunächst abzuraten, aber die Optionen des modularen Aufbaus sollten von Beginn an bewusst sein. So liefert Apache zwar nach

```
sudo a2dismod autoindex
sudo systemctl restart apache2
```

weiterhin HTML-Seiten aus, bietet ohne „autoindex“ aber keine Ordnernavigation mit beliebigen Dateiinhalten.

/etc/apache2/conf-enabled: Das Ordnerpaar „conf-available/conf-enabled“ nennen wir der Vollständigkeit halber. Aufbau und Linkmethode sind analog wie bei „sites“ und „mods“, desgleichen wieder die zugehörigen Terminalhilfen a2enconf und a2disconf. Anlass zu Eingriffen gibt es hier aber nicht.

Die Rechte im „DocumentRoot“

Welche Dateirechte unter „DocumentRoot“ gelten sollen, hat zwei Aspekte: Der erste ist schnell abgehakt, sofern wir hier vereinfachend davon ausgehen, dass nur eine Person für den Apache-Server verantwortlich ist und statische Inhalte nach „DocumentRoot“ kopieren oder dort auf Dateiebene ändern muss: Das kann dann einfach mit sudo im Terminal oder einem Dateimanager mit Systemverwalter-Rechten geschehen. Der zweite Aspekt ist, dass Apache selbst zumindest Lesezugriff auf alle Dateien und Ordner im „Document Root“ haben muss. Schreibrecht für Apache ist erforderlich, wenn der Webserver Basis einer CMS-Anwendung wie Mediawiki oder Wordpress ist, die interaktives Anlegen und Ändern von Inhalten vorsehen. Da Apache unter Debian/Ubuntu & Co. mit den Rechten des Kontos „www-data“ läuft, ist folgende Besitzvergabe für „Document Root“ zu empfehlen:

```
sudo chown -R www-data:www-data /
  var/www/html
```

Durch den Parameter „-R“ wirkt sich der Befehl rekursiv auf alle Unterordner und Dateien aus. Danach gehören alle Dateien und Ordner dem Benutzer „www-data“ und der gleichnamigen Gruppe. Dies als Voraussetzung können dann die Rechte mit diesen zwei Befehlszeilen

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

so gesetzt werden, dass der Besitzer (www-data) Vollzugriff erhält, andere Konten nur Leseberechtigung. Diese Berechtigungen für Apache müssen gegebenenfalls für neue externe Inhalte wiederholt werden, die mit root-Recht nach „DocumentRoot“ kopiert wurden.

Dynamische HTML-Server

Ein purer Apache mit statischen HTML-Seiten und optionaler Datenfreigabe mit Modulen wie dav oder autoindex bietet viele Möglichkeiten und ist dabei schnell und relativ einfach. Trotzdem werden die meisten Nutzer eine dynamische Lösung wie Wordpress, Mediawiki, Dokuwiki oder Drupal bevorzugen.

Das ist technisch komplexer, weil jede Seite erst beim Abruf auf Basis von Markdown-Seiten oder Datenbankinhalten als HTML-Seite generiert wird. Es bedeutet auch größeren Lernaufwand, weil jede CMS-Lösung Einarbeitung fordert. Aber selbst ein kaum enger spezialisiertes CMS wie Wordpress bietet doch enorme Vorteile – Seitenübersicht, einheitliches und leicht änderbares Aussehen für alle Seiten, einfache Verlinkung und zentrale Ressourcennutzung (Bilder et cetera), Suchfunktion, Onlinebearbeitung …

PHP installieren: Für CMS-Anwendungen benötigt Apache in jedem Fall die Script-

Sprache PHP. Für eine PHP-Basisinstallation genügt dieser Befehl (Debian/Ubuntu):

```
sudo apt install php
```

Für Apache wird dabei unter „/etc/apache2/mods-enabled“ automatisch das neue Modul php8.1 aktiviert (das ist Stand Ende 2022 und kann sich künftig ändern). Anweisungen, das PHP-Modul für Apache einzeln zu installieren und mit a2enmod zu aktivieren, sind daher in der Regel überflüssig.

PHP ist unkompliziert installiert, aber gerne ein Stolperstein nach Systemupgrades, die Apache nicht über eine neue PHP-Version informieren. Dies muss man bei Bedarf mit (Beispiel)

```
sudo a2dismod php7.4
sudo a2enmod php8.1
```

manuell nachholen, wobei Sie bei mehreren unter „/etc/apache2/mods-available“ angezeigten Versionen die ältere abschalten und die neuere aktivieren.

Datenbank installieren: PHP erzeugt dynamisch HTML-Seiten, wobei als Quelle meistens – aber nicht immer – eine SQL-Datenbank wie My SQL oder Maria DB dient. Ob ein Serverprojekt überhaupt eine Datenbank benötigt, ferner welche der beiden Datenbanken das CMS bevorzugt, ist den jeweiligen Systemvoraussetzungen zu entnehmen (siehe etwa Wordpress: *https://de.wordpress.org/about/requirements/*). Da My SQL und Maria DB zu hundert Prozent kompatibel sind und Maria DB ressourcenschonender ist, wird heute meistens Maria DB empfohlen, das mit

```
sudo apt install mariadb-server
```

zu installieren ist und damit auch sofort als Systemdienst läuft. Nach diesen Voraussetzungen kann dann das gewünschte CMS installiert werden.

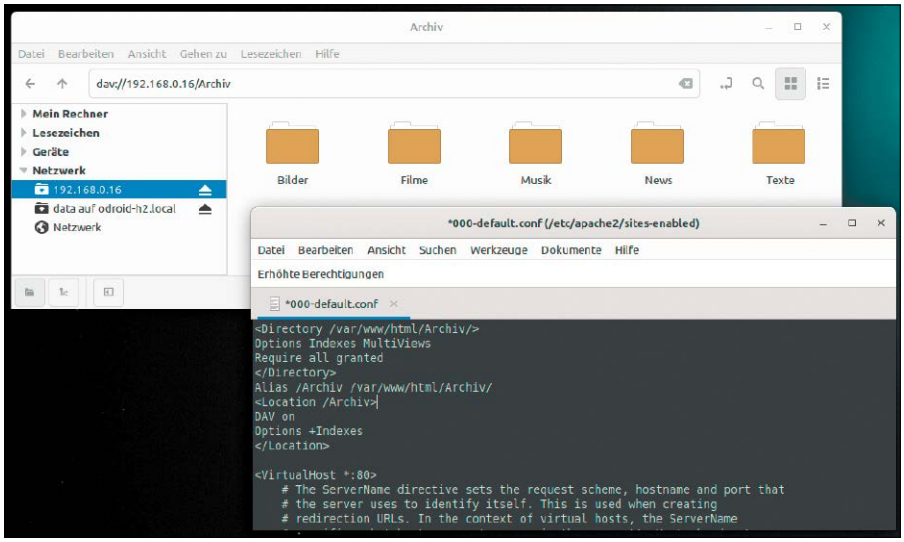
Aufgrund der Vielfalt und Unterschiede von Serverlösungen gehen wir hier auf PHP-Konfiguration, Datenbankverwaltung und CMS-Projekte nicht weiter ein. Denn eigentlich haben wir damit das engere Thema „Apache-Server“ bereits verlassen. Als Vermittler zwischen Apache und Datenbank/CMS dient die PHP-Script-Sprache. Apache selbst hat keine Informationen oder Konfigurationsangaben zur Datenbank.

Apache-Module: Autoindex, Webdav und mehr

Modul „autoindex“: Wie schon beschrieben, kann Apache ohne zusätzliche Software mit dem aktivierten Modul „autoindex“ Text- und PDF-, Audio- oder Bilddateien an alle Browser im Netzwerk ausliefern. Die Grenzen dieser einfachen Datenfreigabe setzt einerseits der Browser, der viele, aber eben längst nicht alle Formate liefern kann. Insbesondere bei Film- und Office-Formaten wird es dünn. Zweitens fehlt natürlich die Möglichkeit, Dateien auf den Server zu kopieren.

```
sudo a2enmod
Your choices are: access_compat actions alias allowmethods asis auth_basic auth_dig
est auth_form authn_anon authn_core authn_dbd authn_dbm authn_file authn_socache au
thnz_fcgi authnz_ldap authz_core authz_dbd authz_dbm authz_groupfile authz_host aut
hz_owner authz_user autoindex brotli buffer cache cache_disk cache_socache cern_met
a cgi cgid charset_lite data dav dav_fs dav_lock dbd deflate dialup dir dump_io ech
o env expires ext_filter file_cache filter headers heartbeat heartmonitor http2 ide
nt imagemap include info lbmethod_bybusyness lbmethod_byrequests lbmethod_bytraffic
 lbmethod_heartbeat ldap log_debug log_forensic lua macro md mime mime_magic mpm_ev
ent mpm_prefork mpm_worker negotiation php8.1 proxy proxy_ajp proxy_balancer proxy_
connect proxy_express proxy_fcgi proxy_fdpass proxy_ftp proxy_hcheck proxy_html pro
xy_http proxy_http2 proxy_scgi proxy_uwsgi proxy_wstunnel ratelimit reflector remot
eip reqtimeout request rewrite sed session session_cookie session_crypto session_db
d setenvif slotmem_plain slotmem_shm socache_dbm socache_memcache socache_redis soc
ache_shmcb speling ssl status substitute suexec unique_id userdir usertrack vhost_a
lias xml2enc
Which module(s) do you want to enable (wildcards ok)?
```

Zum (De-)Aktivieren von Apache-Modulen gibt es die Kommandos a2enmod und a2dismod. Ohne Modulangabe erscheint die relativ unübersichtliche Gesamtliste zur Auswahl.



Webdav-Freigabe statt Samba: Alle Linux-Dateimanager erhalten über die IP-Adresse mit vorangestelltem „dav://“ vollen Zugriff auf einen Webdav-Ordner.

Module „dav“ und „dav_fs“: Mit aktiviertem Webdav erlaubt Apache Lese- und Schreibzugriff auf Dateiebene. Dafür muss man zunächst zwei weitere Apache-Module aktivieren:

```
sudo a2enmod dav dav_fs
```

Angenommen, im „DocumentRoot“ gibt es ein „Archiv“ („/var/www/html/archiv“), das per Webdav freigegeben werden soll. Dazu muss nun die bereits aktive Site „/etc/apache2/sites-enabled/000-default.conf“ ergänzt werden, indem Sie oberhalb von „</VirtualHost>“ diese Zeilen eintragen:

```
<Directory /var/www/html/Archiv/>
Options Indexes MultiViews
Require all granted
</Directory>
Alias /archiv /var/www/html/Archiv/
<Location /archiv>
DAV on
Options +Indexes
</Location>
```

Nachdem Apache mit

```
sudo systemctl restart apache2
```

neu gestartet wurde, kann jeder Linux-Dateimanager mit

```
dav://[IP-Adresse]/Archiv
```

zugreifen – und zwar ohne jede Legitimierung mit Lese- und Schreibrecht.

Modul „userdir“: Ein weiteres interessantes Freigabemodul ist „userdir“, das Sie mit

```
sudo a2enmod userdir
```

aktivieren. Der Systemnutzer kann dann unter „/home“ das Verzeichnis „public_html“ erstellen und dort HTML-Dateien unterbringen, die dann über die Adresse „http://[IP-Adresse]/~[User]“ im Webserver erreichbar sind. ■

Sichere Daten: Die Grundregeln

Große IT oder Homeoffice: Die Grundregeln für Datensicherheit und Datenschutz sind identisch. Der Unterschied ist „nur“ quantitativ, aber natürlich erheblich – je mehr Nutzer, Geräte, Systeme und Daten, desto anspruchsvoller wird die Aufgabe.

VON HERMANN APFELBÖCK



© David Wolski

Dieser Heftschwerpunkt zeigt Maßnahmen, um Router, Desktop-PCs, Mobilgeräte und Serversysteme gegen Angriffe und Datenspionage abzuschirmen. Der einleitende Beitrag ergänzt diese Einzelmethoden durch einen Überblick über die Grundziele der IT-Sicherheit und über die dafür nötigen operativen Maßnahmen.

Prinzipien: Worum geht's?

Im Detail – hinsichtlich der Einzelmaßnahmen für Geräteschutz, Benutzer- und Zugangskontrolle, Softwarekonfiguration, Backup und Verschlüsselung – sind die Themen Datensicherheit und Datenschutz hochkomplex. Im Prinzip geht es aber nur um drei Problemfelder, und diese sind im überschaubaren Geräte- und Nutzerpark privater Endanwender durchaus beherrschbar:

1. Datenverlust durch interne Fehler: (Hardware-/Systemausfälle, Benutzerpannen): Dies ist das mit Abstand häufigste Szenario für massiven Datenverlust. Die wichtigsten Maßnahmen, hier vorzubeugen, wird dieser Beitrag in aller Kürze aufzeigen, zumal dieser Aspekt in den folgenden Artikeln nicht mehr auftritt.

2. Datenverlust durch externe Schadsoftware (Virenbefall und gehackte Server): Dieses Szenario wird oft paranoid überschätzt. Es ist nicht so, dass Killerviren über das Ethernet-Kabel in den Rechner kriechen oder durch das Funknetz einfliegen. Vielmehr etabliert der Heimrouter für alle angeschlossenen Geräte ein privates Netz, das vom öffentlichen Netz unabhängig ist und jeden Zugriff aus dem Internet ablehnt. Eine Sendung aus dem öffentlichen Netz an den Router wird nur in genau zwei Situationen erlaubt und „durchgelassen“:

A. Der Benutzer hat im Router explizit eine Portfreigabe geschaltet, um den Internetzugriff auf einen Serverdienst zu erlauben. Dabei kann es sich etwa um einen Datenserver, eine Nextcloud oder eine Smart-Home-Funktion handeln, die er von außerhalb nutzen möchte. Dieses Thema kommt in den nachfolgenden Beiträgen zur Sprache und wird nachfolgend nur noch kurz erwähnt. Der allgemeine Rat: Portfreigaben für Serverdienste sind nur etwas für erfahrene Anwender.

B. Damit ein Nutzer am öffentlichen Netz teilnehmen kann, müssen eintreffende Sendungen erlaubt sein, wenn er sie selbst angefordert hat. Das kann eine HTML-Seite, ein Download oder eine Mail sein. Technisch geschieht Folgendes: Eine lokale IP macht eine Anfrage (etwa Mausklick auf Link) auf einem Webserver. Der Router merkt sich die lokale IP, schickt die Anfrage an den Server im öffentlichen Netz. Die Sendung kommt zurück an die öffentliche IP des Heimrouters, der diese aufgrund aktiven Anfrage aus dem lokalen Netz akzeptiert und dann an jene lokale IP schickt, woher der Auftrag kam.

Somit ist klar: Es kommt nichts von außen, was nicht von innen angefordert wurde. Jedoch ist nicht zu verhindern, dass sich die Nutzer aktiv Sendungen ins lokale Netz holen, die sie besser nicht abrufen sollten – etwa ausführbare Downloads und Mails mit schädlichen Anhängen. Theoretisch ist schon der Klick in Webseiten oder HTML-Mails problematisch, wenn dadurch ausge-

löste Web-Scripts auf ungepflegte Browser mit Sicherheitslücken treffen. Die wichtigsten Maßnahmen, um die alltägliche Browser- und Mailnutzung abzuhärten, ist ebenfalls ein knappes Thema dieses Beitrags.

3. Datenpreisgabe an Unbekannte (verlorene Datenträger, offene Funknetze, Daten in der Cloud – auch Mail, Browsersynchronisierung): Dies scheint die objektiv harmloseste Bedrohung. Aber was eine versehentliche oder selbst verschuldete Preisgabe personenbezogener Daten anrichten kann, hängt von der Menge und der Qualität der Daten ab. Was US-Big-Data-Sammler aus Verlaufsprotokollen oder unverschlüsselten Clouddateien an persönlichen Interessensprofilen akkumulieren, ist lästig bis alarmierend. Regelrecht existenzgefährdend sind aber verlorene Datenträger, die sensible geschäftliche oder persönliche Informationen direkt enthalten oder die Zugangsdaten zu solchen Informationen wie Firmenserver, Bank, Bezahldienst et cetera. Dieses Datenschutzthema wird später nur mehr in einem speziellen Beitrag zur Home-Verschlüsselung (mit Gocryptfs) behandelt, daher gibt es hier einige wichtige Grundregeln.

Maßnahmen (1): Systemschutz & Backup

Wer seiner Hardware, seinem Betriebssystem und sich selbst ohne Rückversicherung vertraut, ist naiv, faul, fahrlässig. Die Katastrophe kann sich Zeit lassen, aber sie kommt (garantiert). Maßnahmen, die den Fortbestand aller Benutzerdaten oder des gesamten Systems sichern, gibt es in Menge. Dabei stellt sich nur die Frage des Umfangs und Aufwands.

Datenbackups mit Rsync: Unter Linux, wo Neuinstallationen und Softwarewiederherstellung geringen Aufwand bedeuten, stehen die Benutzerdateien eindeutig im Vordergrund. Und dafür sind Backups oder Synchronisierungen mit Rsync oder Tar eindeutig erste Wahl. Grafische Alternativen wie Freefilesync (*www.freefilesync.org*) scheinen auf den ersten Blick komfortabler, aber ein einmal geprüftes und als Alias abgelegtes Backupkommando ist schneller, effizienter und automatisierbar.

Tar hat den Vorteil, dass die Dateisysteme von Quelle und Ziel keine Rolle spielen, da alle Attribute intern gesichert werden, außerdem gibt es optionale Komprimierung. Die Daten landen in Archiven, die jeder Archivmanager auch ohne Auspacken nutzen kann. Das von uns bevorzugte Rsync hat den Vorteil, dass alle Daten auch auf dem Sicherungsziel uneingeschränkt zu benutzen sind. Es sichert auf interne und externe Laufwerke, Netzwerkfreigaben und jeden Rechner, auf dem ein SSH-Server läuft. Rsync hat reichlich Schalter, doch fasst die Option „-a“ oder „--archive“ häufig benötigte Funktionen zusammen.



Rescuezilla schreibt Systemimages: Diese Aktion ist eine Systemschutzmaßnahme. Für periodische Datensicherung ist der Einsatz des externen Livesystems zu aufwendig.

```
rsync --archive /home/ha/ /media/
  ha/usb/backup
```

Das Beispiel geht davon aus, dass das Ziellaufwerk „/media/[...]“ eingehängt ist. Beachten Sie beim Quellordner immer den abschließenden Slash (/). Für periodische Sicherung ergänzen Sie den Schalter „--update“ oder „-u“, damit nur neue Daten kopiert werden:

```
rsync --archive --update /home/ha/
  /media/ha/usb/backup
```

Die Schalter „--verbose“ („-v“) und „--progress“ („-P“) sind immer zu empfehlen, um den Vorgang gesprächiger zu machen.

Eine 1:1-Spiegelung erzwingt der Schalter „--delete“:

```
rsync -auvP --delete /home/ha/ /
  media/ha/usb/backup
```

Was in der Quelle „/home/ha“ seit dem letzten Kopiervorgang gelöscht wurde, wird auch auf dem Ziel gelöscht. Mit falschen Pfadangaben wäre das fatal, daher ist vorher ein Testlauf mit „--dry-run“ anzuraten (*rsync -av --delete --dry-run* ...).

Rsync kann von jedem Netzwerkrechner Daten beziehen oder dorthin kopieren, wo ein SSH-Server läuft. Die Sicherung folgt diesem Schema

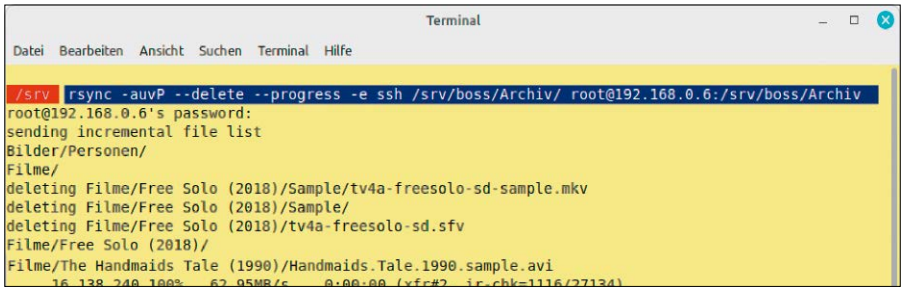
```
rsync -auvP -e ssh ha@192.168.0.20:
  /home/ha/ /home/ha
```

oder mit

```
rsync -auvP -e ssh /home/ha/
  ha@192.168.0.20:/home/ha
```

in die andere Richtung.

Laufwerkssicherung: Diese Rückversicherung ist kompromisslos und schließt Systemdaten wie Benutzerdateien ein. Zur bloßen Datensicherung sind solche Laufwerkimages aber zu aufwendig, weil sie periodisch wiederholt werden müssten, um den geänderten Datenbestand zu repräsentieren. Erforderliche Werkzeuge sind die Livesysteme Rescuezilla (*https://rescuezilla.com*) oder Clonezilla (*https://clonezilla.org*), weil das Kopieren im laufenden System technisch scheitern würde. Clonezilla



Rsync-Abgleich – lokal, im Netz und auch mit SSH: Solche 1:1-Kopien mit Delete-Schalter sorgen für exakt identischen Datenbestand auf Quelle und Ziel.

beherrscht einige Netzwerkfähigkeiten mehr (beim Sicherungsziel) sowie optionale Komprimierung und Verschlüsselung der Imagesicherung. Außerdem kann es einen Datenträger ohne Zwischenschritt einer Imagesicherung direkt auf einen zweiten „klonen" (Option „device-device"). Das grafische Rescuezilla ist andererseits wesentlich bedienfreundlicher.

Nichts gesichert? Livesystem zur Datenrettung! Streikt das System, aber nicht die Hardware, ist auch ohne Backup noch nichts verloren. Nach dem Rechnerboot mit einem beliebigen, möglichst vertrauten Linux-Livesystem haben Sie vollen Zugriff auf das Home-Verzeichnis und können alle oder ausgewählte Dateien auf ein externes (drittes) Laufwerk retten.

Maßnahmen (2): Sicher im Internet

Eingangstür vom öffentlichen Web ins lokale Netz ist der Router. Die Hackerindustrie klopft permanent und massenhaft beliebige öffentliche IP-Adressen ab – auch Ihren Router, wenn es der Zufall will. Wer Dienste nach außen öffnet, und sei es auch nur eine winzige Smarthome-Funktion, fährt etwas sicherer, wenn der Router im Stealth-Modus arbeitet (Fritzbox: „Internet → Filter → Listen → Firewall im Stealth Modus"). Er antwortet dann nicht auf Ping-Anfragen aus dem Internet. Hacker-Scripts schicken schnelle Pings oft einem Portscan voraus, um Zeit zu sparen.

Gegen direkte Portscans Ihrer öffentlichen Adresse ist kein Kraut gewachsen, aber auch hier gibt es höhere Hürden: Wenn Sie Ihrem Dienst statt des Standardports (nach außen) einen selbst gewählten fünfstelligen Port zuweisen, werden die meisten Scans nichts finden, weil sie aus Zeitgründen nur etliche Standardports abfragen.

Das Funknetz: Das WLAN muss natürlich verschlüsselt sein (Fritzbox: „WLAN → Sicherheit → Verschlüsselung"). WPA2 oder WPA3 und ein komplexes Kennwort halten die Nachbarn fern, die andernfalls nicht nur mitsurfen könnten, sondern auch Zugang zu den Daten im Heimnetz erhielten. Immerhin besteht hier aber eine weitere Zugangshürde, weil Netzfreigaben in der Regel ebenfalls eine Benutzeranmeldung erfordern.

MAC-Filterung ist eine weitere Abhärtungsmaßnahme, die nur noch definierte Hardware ins WLAN lässt (Fritzbox: „WLAN → Sicherheit"). Jedes später hinzukommende Gerät im Haushalt oder jedes Besuchergerät muss später explizit mit seiner MAC-Adresse erlaubt werden („WLAN-Gerät hinzufügen").

Das Betriebssystem: Mit Linux können Sie genau wie unter Windows unfreiwillig Schadsoftware in Downloads, Mails oder Web-Scripts herunterladen – dies aber praktisch ohne Folgen: Linux ist gegen Schadsoftware so gut wie immun, weil fast alle Viren und Würmer für Windows programmiert sind. Solange die Trägerdateien nicht im lokalen Netz auf Windows-Rechner kopiert werden, besteht keine Gefährdung.

Linux statt Windows: Malwareschutz im Internet ist tatsächlich so einfach zu erreichen, und dies unabhängig vom jeweiligen Browser, Mail-, Chat-, FTP-, Usenet- oder Torrent-Client.

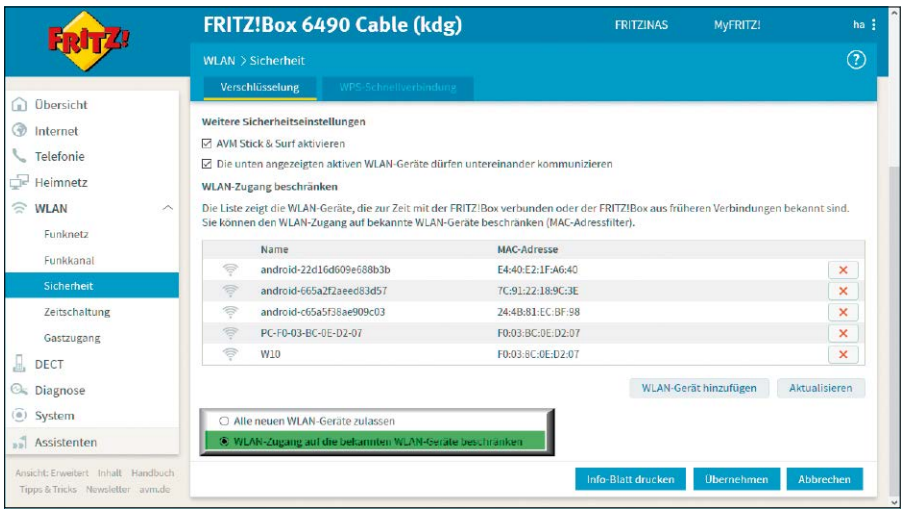
Für Windows-Nutzer ist es daher der beste Rat, mit einem schlanken Linux in einer virtuellen Maschine (VM) ins Internet zu gehen. Der Bedienkomfort einer VM (unter Virtualbox oder Vmware) ist deutlich höher als mit externen Linux-Surfsystemen, für die man sein Standardsystem verlassen und den Rechner neu booten muss. Wenn ein Desktoprechner mindestens vier bis acht GB RAM mitbringt und einen aktuellen Prozessor, läuft das Linux mit Browser in der VM praktisch genauso flüssig wie in einem nativen System.

Der Browser: Ungeachtet der Linux-Immunität gegenüber Viren bleibt die Gefahr von Java-, Javascript- und PHP-Script, die über Browser-Sicherheitslücken Code einschleusen (meistens Windows-Code, aber rechnen muss man mit allem). Auch Linux-Browser müssen daher ständig aktualisiert werden. Dies geschieht automatisch und zeitnah, aber nur, sofern die Paketquellen dies gewährleisten. So wird bei Debian derzeit ein Aktualisierungsstau kritisiert, der zu veralteten Browsern führt. Ubuntu delegiert seit Version 22.04 die Verantwortung für Firefox an Mozilla. Ein aktueller Firefox ist somit garantiert, allerdings im unbeliebten Snap-Container.

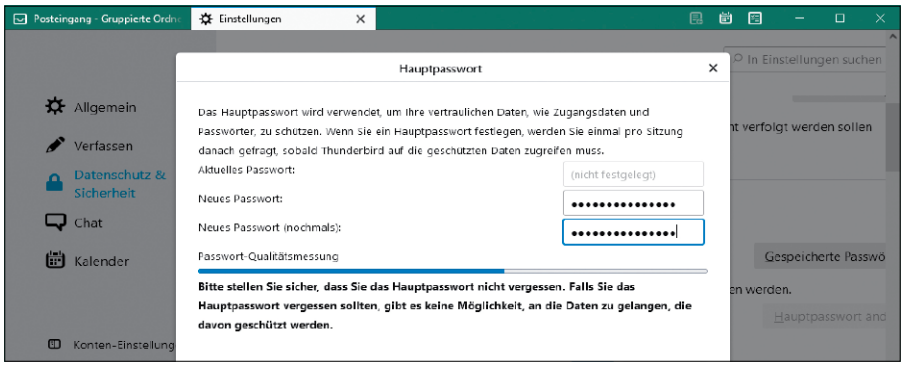
Theoretisch können Browser alle Script-Aktivitäten abschalten (Firefox, „about:config", „javascript.enabled" oder Chrome, „Einstellungen → Datenschutz und Sicherheit → Website-Einstellungen → JavaScript"). Das ist aber kaum praktikabel, da es dann Fehlermeldungen hagelt. Ein Kompromiss ist das Add-on Noscript für Chrome und Firefox. Es blockiert Javascript, Java und andere ausführbare Inhalte. Damit ist Noscript der Schädlingsstopp schlechthin, aber ebenfalls unbequem, weil fast jede Webseite Script-Code verwendet. Immerhin landen einmal erlaubte Sites in einer Whitelist und müssen später nicht mehr bestätigt werden, aber zunächst müssen Sie auf vielen interaktiven Seiten die Script-Ausführung manuell erlauben.

Das Mailprogramm: Mails an sich sind nicht gefährlich. Aber sie sollten Mails bleiben und nicht ins Web gehen. Und Mailanhänge von Unbekannten haben auf dem System nichts verloren. Beim unter Linux meistgenutzten Mailclient Thunderbird lohnen sich folgende Optionen:

Die Einstellung „Ansicht → Nachrichteninhalt → Reiner Text" verhindert die hübsche Anzeige von HTML-Format, damit aber auch trügerische Tarnoptik und Links. Ein Kompromiss ist „Vereinfachtes HTML". Unter „Extras → Einstellungen → Datenschutz &



WLAN-Kennwort genügt nicht: Diese Option lässt nur noch die per MAC-Adresse bekannten Geräte ins Funknetz.



Sinnvoll auf Notebooks: Das Thunderbird-Hauptpasswort verschlüsselt die Mailcontainer, sodass bei Fremdzugriff weder die Nachrichten noch die Zugangsdaten lesbar sind.

Sicherheit“ sollte „Externe Inhalte in Nachrichten erlauben“ abgeschaltet sein. Nützlich ist ferner weiter unten die interne Phishing-Heuristik: „Nachrichten auf Betrugsversuche (Phishing) untersuchen“.

Wenn Sie dann noch auf Notebooks Ihre Zugangsdaten schützen, sind Sie auch datenschutztechnisch auf der sicheren Seite. Thunderbird bietet dafür das „Hauptpasswort“ („Extras → Einstellungen → Datenschutz & Sicherheit → Hauptpasswort verwenden“. Dadurch werden die Zugangsdaten verschlüsselt, sodass ein Fremdzugriff auf Dateiebene erfolglos ist. Eine weitere Datenschutz-Bitte, der nicht alle Seiten folgen werden, ist die Option „Websites eine „Do Not Track“-Mitteilung senden“. Dies ist aber sowieso hinfällig, sofern sich man die Mails als Reintext zeigen lässt.

Maßnahmen (3): Datenschutz und Verschlüsselung

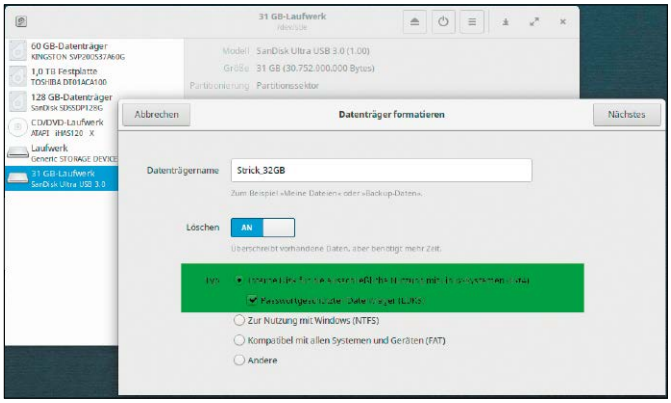
Notebooks, USB-Medien, Cloud: Alles, was das Haus und das lokale Netz verlässt, kann in fremde Hände gelangen oder ist in fremden Händen. Verschlüsselung sorgt dafür, dass die Daten nichts preisgeben.

1. Mobile Notebooks: Bei Notebooks, die viel unterwegs sind, sollte man mit kleineren Lösungen erst gar nicht anfangen: Hier empfiehlt sich eine Linux-Installation mit verschlüsselter Systempartition (Luks/Cryptsetup). Das verlorene oder unbeaufsichtigte Notebook lässt dann auch beim Booten durch ein Fremdsystem keinerlei Einblick in die Daten zu. Die meisten Linux-Installer (Ubuntu-Derivate, Debian-Derivate, Open Suse, Fedora, Manjaro und andere) bieten diese Option im Partitionierungsdialog direkt an. Voraussetzung ist dabei immer, dass Sie dem Löschen der primären Festplatte zustimmen und das neue System diese komplett übernehmen darf. Cryptsetup-verschlüsselte Systeme haben nur eine winzige unverschlüsselte Boot-Partition, alles andere wird erst aufgesperrt, wenn nach „Please unlock disk [...]“ das korrekte Passwort eingegeben wird.

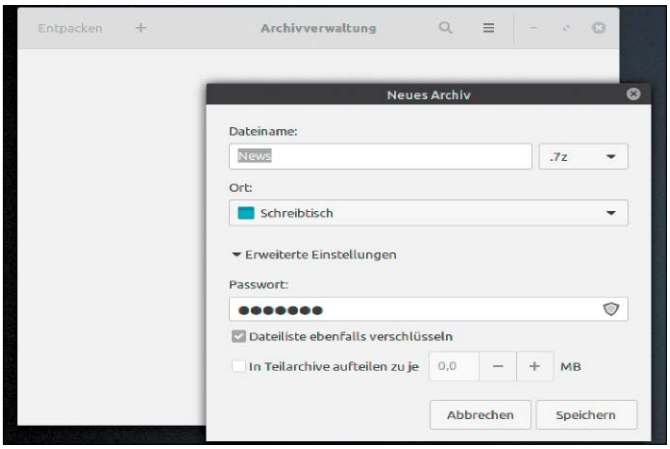
2. USB-Medien: USB-Datenträger lassen sich ebenfalls mit Luks/Cryptsetup verschlüsseln. Die Maßnahme ist aber gut zu überlegen, weil damit ein Austausch mit Windows- oder Mac-Systemen ausscheidet. Die Aktion ist mit Gnome-Disks oder dem KDE-Partitionmanager ganz einfach: Nach „Partition formatieren“ wählen Sie als „Typ“ den Eintrag „Verschlüsselt, kompatibel mit Linux-Systemen (LUKS + Ext4)“ und vergeben die „Passphrase“ – also das Kennwort.

3. Cloud, USB und sensible Dateien: Einfachster Schutz bei geringeren Datenmengen ist die Ad-hoc-Verschlüsselung von Einzeldateien oder eines Ordners. Ohne Einschränkung anwendbar ist der Packer 7Zip (Paket „p7zip-full“). Passwortgeschützte Archive eignen sich für Dateien in der Cloud, können aber auch für mobile Datenträger ausreichen. Da es 7-Zip für Linux, Windows und Mac-OS (7zX) gibt, ist der Austausch solcher Archive problemlos.

7-Zip erscheint unter Linux nicht als selbständiges Programm, sondern integriert sich in die „Archivverwaltung“. In Zusammenarbeit mit dieser Archivverwaltung oder 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“ an. Unter „Erweiterte Einstellungen“ vergeben Sie das Passwort. ■



Komplettverschlüsselung für USB-Medien: Mobile USB-Sicherheit ist ganz einfach über Gnome- und KDE-Laufwerktools erreichbar. Eine Nutzung unter Windows ist dann allerdings nicht möglich.



Packer 7-Zip als Datenschützer: In der Archivverwaltung muss das Format „.7z“ gewählt werden, damit die Verschlüsselungsoption angeboten wird.

Home: Individuell verschlüsselt

Private Daten auf Notebooks verlangen immer besonderen Schutz. Aber auch auf Mehrbenutzersystemen sollten Daten verschlüsselt sein. In Ubuntu/Debian sorgt Gocrypt FS für eine individuelle und komfortable Home-Chiffrierung.

VON DAVID WOLSKI



Die sicherere Verschlüsselung vertraulicher Daten ist im Unternehmensumfeld meist Pflicht, um Auflagen der IT-Compliance zu erfüllen. Aber auch die Vorstellung, dass wichtige Daten auf einem privat genutzten Laptop mit dem Verlust des Geräts in fremde Hände fallen, ist nicht angenehm. Die aktuellen Linux-Distributionen wie Ubuntu 22.04 bieten bei der Einrichtung über Cryptsetup/Luks eine Komplettverschlüsselung des Systems an.

Diese Methode gilt als sehr sicher, ist aber nicht ohne Einschränkungen und zusätzliche Komplexität: Auf Linux-Systemen, die auch Serverrollen erfüllen und unbeaufsichtigt booten sollen, ist die Luks-Systemverschlüsselung nicht praktikabel. Denn beim Systemstart muss jemand zugegen sein, um das Passwort zur Entschlüsselung der Partitionen einzugeben. Zudem ist dieses Passwort für alle Anwender auf dem System gleich. Für eine individuelle Verschlüsselung ist diese Methode also nicht geeignet.

Gocrypt FS und Fuse: Ein neuer Ansatz

Ein alternativer Weg, der jenem von Ecrypt FS ähnelt, der bis Ubuntu 18.04 für die Verschlüsselung von Home-Verzeichnissen sorgte, ist Gocrypt FS. Gocrypt FS ist ein ausgereiftes, in Go geschriebenes Tool zur Erstellung verschlüsselter Dateisysteme über das Kernel-Modul „File System In Userspace“ (Fuse). Die Einrichtung ist in Debian/Ubuntu mit wenig Aufwand erledigt, denn es finden sich bei diesen Distributionen alle Zutaten in den Standard-Paketquellen. Zudem gibt es schon ein Grundgerüst zur automatischen Entschlüsselung bei der Anmeldung über die Konfiguration von PAM (Pluggable Authentication Modules), die sich unter Linux um die Delegation von Log-in-Informationen an die verschiedenen Systemkomponenten kümmert.

Gegenüber Ecrypt FS, das Linux Mint 21 weiterhin verwendet, hat Gocrypt FS den Vorteil, in aktiver Entwicklung zu sein und weniger Bugs zu haben. Zwei leicht verschmerzbare Minuspunkte gibt es, die nicht verschwiegen werden sollen: So wie auch Ecrypt FS wird das verschlüsselte Home beim Abmelden eines Benutzers nicht ausgehängt, sondern nur bei einem Neustart. Zweitens ist Gocrypt FS im Vergleich zu Luks-Partitionen langsamer bei den Datenträgerzugriffen, weil es sich um ein Fuse-Dateisystem handelt.

Vorbereitung und Installation

In wenigen Handgriffen ist ein verschlüsseltes Home in Debian/Ubuntu eingerichtet. Aus den Paketquellen installiert zunächst das Kommando

```
sudo apt install gocryptfs libpam-
  mount
```

die benötigten Pakete. Gocrypt FS übergibt die Anlage eines verschlüsselten Home zunächst dem Administrator. Das Paket „libpam-mount“ ist dabei das Bindeglied zwischen dem Log-in als Benutzer und der Entschlüsselung des Home-Verzeichnisses per Mountbefehl, Fuse und Gocrypt FS.

Nach der Installation dieser Pakete geht es auch schon an die Erstellung des verschlüsselten Ordners für einen neu angelegten User, welcher hier im Beispiel „benutzer“ heißen soll. Es ist nicht möglich, von einem Benutzerkonto den eigenen Ordner zu verschlüsseln, dafür ist immer ein zweiter User

mit sudo-Privilegien oder root nötig. Zuerst wird das vorhandene Home-Verzeichnis des abgemeldeten Benutzers mit allen seinen Dateien im Terminal in einen temporären Ordner verschoben

```
sudo mv /home/benutzer /home/
 benutzer.tmp
```

und ein neues, später verschlüsseltes Verzeichnis angelegt:

```
sudo mkdir /home/benutzer.enc
```

Dieser Ordner wird nun verschlüsselt und später nach der Anmeldung nach „/home/benutzer“ unverschlüsselt eingehängt. Um den Ordner vorzubereiten, dient folgender Befehl:

```
sudo gocryptfs -init /home/
 benutzer.enc
```

Gocrypt FS fragt nun das gewünschte Passwort ab, das identisch mit dem Systemkennwort von „benutzer“ sein muss. Gocrypt FS legt eine JSON-Datei mit dem Password-Hash im Ordner ab und zeigt zur späteren Entschlüsselung im Falle eines vergessenen Kennworts auch einmalig einen Generalschlüssel an, den man unbedingt sicher verwahren sollte. Nun erstellen die folgenden beiden Kommandos

```
sudo mkdir /home/benutzer
sudo gocryptfs /home/benutzer.enc /
 home/benutzer
```

das neue, leere Verzeichnis „/home/benutzer“ als Einhängepunkt und hängen dort den entsperrten Gocrypt-FS-Ordner ein. Aus dem zuvor erstellten temporären Home-Verzeichnis kopiert dann

```
sudo cp -rT /home/benutzer.tmp /
 home/benutzer
```

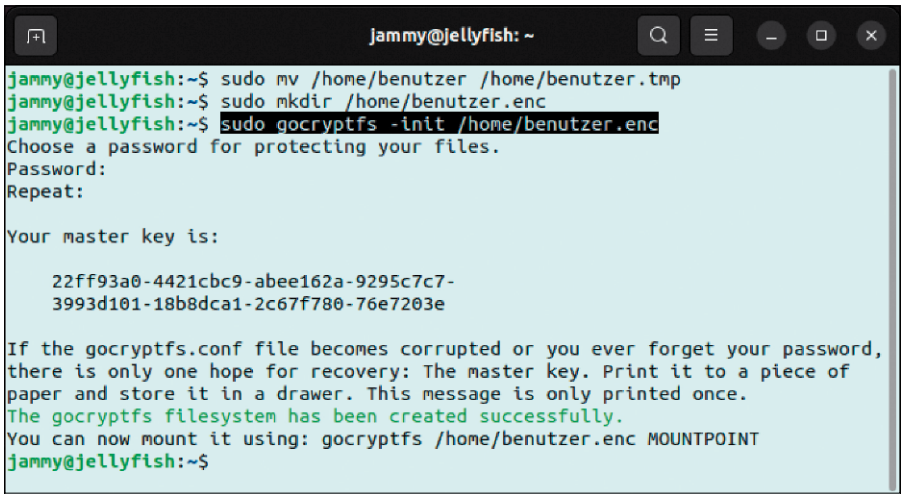
alle Dateien rekursiv zurück ins neue Home, wobei Gocrypt FS alles chiffriert speichert. Damit alles wieder dem „benutzer“ gehört, ist die Rechteanpassung mit

```
sudo chown -R benutzer:benutzer /
 home/benutzer /home/benutzer.enc
```

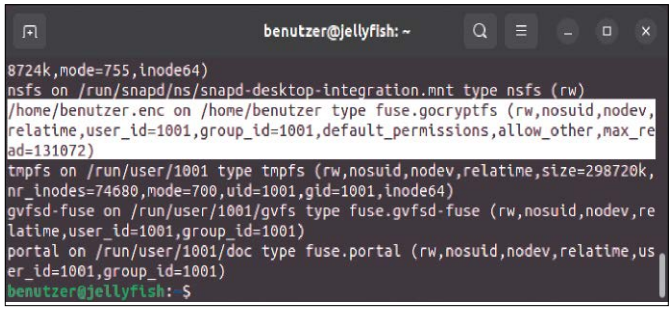
nötig und ein Aushängen des neuen Home-Verzeichnisses, das anschließend auch zusammen mit dem temporären Ordner gelöscht wird:

```
sudo fusermount -u /home/benutzer
sudo rm -r /home/benutzer
```

Keine Sorge: Bei einer Anmeldung wird es aus dem verschlüsselten Ordner auf dem Datenträger von Gocrypt FS neu erzeugt.



Den neuen Ordner vorbereiten: Dafür ist ein separates Benutzerkonto mit sudo-Berechtigungen nötig. Gocrypt FS zeigt einmalig einen Wiederherstellungsschlüssel für Notfälle an.



Eingehängt und entschlüsselt: Die Ausgabe des Befehls „mount“ zeigt, dass PAM den Ordner „/home/benutzer.enc“ automatisch nach dem Log-in verfügbar gemacht hat.

PAM: Ein Regelwerk für Gocrypt FS

Nun ist nochmal Aufmerksamkeit verlangt. Denn das Home von „benutzer“ ist vorbereitet und soll künftig nach der Anmeldung des Users gleich entschlüsselt an Ort und Stelle sein. Das verlangt zwei Anpassungen in Konfigurationsdateien. Einmal in der Datei „/etc/fuse.conf“, in welcher das Kommentarzeichen (#) vor der letzten Zeile

```
user_allow_other
```

entfernt wird und danach nicht nur root den Zugriff auf das neue Home erlaubt. Die zweite Änderung betrifft das anfangs installierte Modul „libpam-mount“ von PAM, das seine Einstellungen aus der Datei „/etc/security/pam_mount.conf.xml“ bezieht. In diese Datei, die mit root-Rechten oder vorangestellten „sudo“ in einem Texteditor geöffnet wird, kommt nun, genau vor dem abschließenden Tag „</pam_mount>“ diese Definition in eine durchgehende Zeile:

```
<volume user="benutzer"
 fstype="fuse" options="nodev,nos
 uid,quiet,nonempty,allow_other"
 path="/usr/bin/gocryptfs#/
 home/%(USER).enc" mountpoint="/
 home/%(USER)"/>
```

Ab jetzt funktioniert die Anmeldung des Benutzers „benutzer“ über die Konsole oder den grafischen Displaymanager und hängt über das gegebene Anmeldepasswort das Home-Verzeichnis unverschlüsselt ein.

Soll auf dem System ein weiterer Benutzer ein verschlüsseltes Home bekommen, dann sind alle Schritte mit dem anderen Usernamen nochmal auszuführen. Für jeden Benutzer ist auch wieder eine Zeile in der Datei „/etc/security/pam_mount.conf.xml“ hinter „user=“ erforderlich. ■

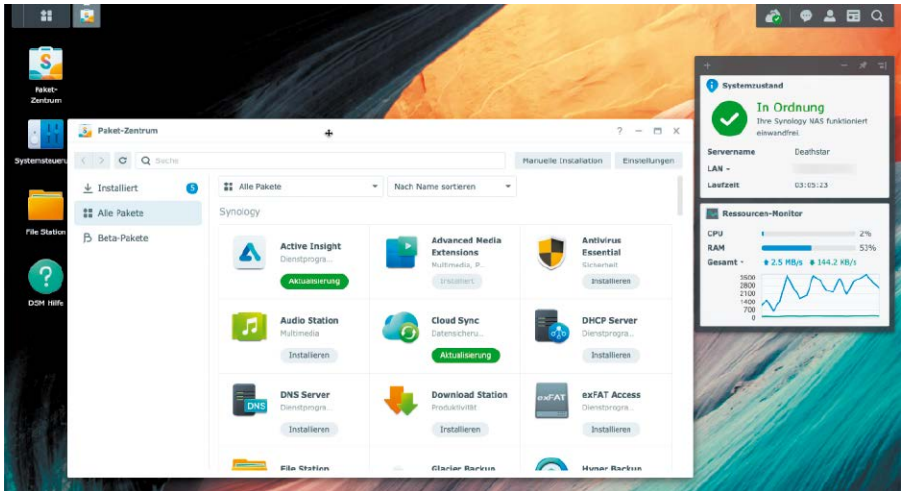
PRO & CONTRA

+ automatische Entschlüsselung bei der Anmeldung
+ verwendet kein systemweites Passwort
+ wenig Aufwand in Debian/Ubuntu
+ Weniger Bugs als das eingestellte Ecrypt FS
– manuelle Einrichtung zu Beginn erforderlich
– Gocrypt FS ist langsamer als Cryptsetup/Luks
– Gocrypt-FS-Ordner wird nicht automatisch ausgehängt

So wird Ihr NAS sicherer

Aus Sorge um Datenschutz und Datensicherheit bevorzugen viele Anwender den Einsatz eines eigenen Netzwerkspeichers gegenüber der Cloud. Aber ganz so einfach ist das nicht. Auch NAS-Geräte müssen abgesichert werden.

VON STEPHAN LAMPRECHT



Die ideale Welt sieht in Hinblick auf die Datensicherheit so aus: Das NAS liegt isoliert im heimischen Netzwerk, das von Bedrohungen von außen durch eine Firewall geschützt ist. Ein Datenverkehr zwischen dem offenen Netz des Internets und den heimischen Geräten wäre damit unmöglich. Allerdings existiert dieses ideale Szenario spätestens dann nicht mehr, wenn im Haushalt auch Elemente für das Smart Home installiert sind. Denn zu deren Komfort gehört der Fernzugriff über das Internet. Ein Hub oder ein smartes Thermostat könnte Angreifern also als Sprungbrett für Attacken dienen. Das ließe sich dadurch lösen, dass das NAS in einem separaten Netz liegt. Aber wer macht sich schon die Mühe? Deswegen lohnt es sich, die Sicherheit des Netzwerkspeichers gezielt zu verbessern.

Den Admin-Zugang sichern

Die meisten Geräte werden mit dem Standardnutzer „admin“ ausgeliefert, dem dann auch noch das triviale Passwort „admin“ zugeordnet ist. Das versuchen die Hersteller dadurch zu heilen, dass sie die Nutzer schon während der ersten Einrichtung dazu auffordern, dieses allzu einfache Passwort zu ändern. Noch besser ist es, auf das Standardbenutzerkonto „admin“ ganz zu verzichten. Schließlich haben Bots für Brute-Force-Attacken mit diesem Benutzernamen bereits 50 Prozent der benötigten Informationen. Legen Sie also einen neuen Nutzer an, dem Sie ein starkes Passwort mitgeben. Diesen ordnen Sie dann die Rechte eines Administrators zu. Nachdem Sie sich davon überzeugt haben, dass das funktioniert hat, loggen Sie sich mit diesem Konto ein und deaktivieren (oder löschen) das vorherige Admin-Konto. Auf einem aktuellen Synology-NAS wechseln Sie in die Systemsteuerung und wählen „Benutzer & Gruppen“. Mittels „Bearbeiten“ finden Sie auf der nachfolgenden Bildschirmseite dann die Option zum Deaktivieren. Ebenso kann die Einrichtung einer Zwei-Faktor-Authentifizierung sehr sinnvoll sein. Im Betriebssystem der Synology ist das unter „Sicherheit, Konto“ bereits eingebaut. Der zweite Faktor wird dann in den persönlichen Einstellungen der Benutzer aktiviert.

Unnötige Dienste abschalten

Besonders in heterogenen Umgebungen neigen Einsteiger dazu, zu viele Dienste zu aktivieren. In einem Haushalt, in dem neben Linux auch Windows- und Mac-Systeme zum Einsatz kommen, scheint es nur konsequent, wenn auch die passenden Freigabeprotokolle eingeschaltet werden. Neben dem eigentlichen Datenprotokoll lassen sich dann auch gleich noch Dienste aktivieren, die den Zugriff auf das NAS vereinfachen. Das sieht trivial aus, ist es aber nicht. Denn es gibt auch (wenn auch wenige) Konstellationen, in denen es zu Filelock-Problemen kommen kann, wenn Clients über unterschiedliche Protokolle parallel auf die gleiche Freigabe zugreifen.

Sie werden etwa häufig lesen, dass Sie im Falle von Apple am besten AFP nutzen. Das sei performanter und ideal. Tatsächlich schwenkt Apple aber immer zusehends auf SMB um. SMB-Freigaben versteht jedes Linux, Windows und Mac-OS. NFS wiederum, einstmals von Sun entwickelt, ist perfekt für Linux-Umgebungen.

Schauen Sie kritisch unter „Systemsteuerung → Dateidienste“ nach (Synology, ähnlich bei anderen NAS-Systemen), was dort

alles aktiviert ist. Über das SMB-Protokoll können Sie unter Windows eine Freigabe als Netzlaufwerk auch direkt via IP-Adresse anlegen. Die Netzwerkerkennung von Windows ist komfortabel, aber eben nur optional. Gleiches gilt auch für das Apple-Pendant Bonjour. Besonders vorsichtig sollten Sie mit Portfreigaben sein. Denn mit jedem Port, den Sie öffnen oder weiterleiten, schaffen Sie einen zusätzlichen Kanal von außen in das lokale Netz.

Cloudservices? Mit Risiken!

Fast jeder NAS-Hersteller bietet einen optionalen Zugang via Cloud auf das NAS an. Damit soll dann der Zugriff von unterwegs auf Fotos, Musik, Dateien und Verwaltungsfunktionen besonders einfach werden. Ein passendes Benutzerkonto ist schnell eingerichtet und via App auf dem Smartphone gelangen Sie dann tatsächlich von überall auf alle Daten und Verwaltungsfunktionen des heimischen NAS-Geräts. Technisch handelt es sich hier einfach um einen Dienst für dynamische DNS-Einträge.

Wie schon bei den oben genannten Diensten sollten Sie sorgfältig abwägen, ob Sie solchen Fernzugriff tatsächlich benötigen. Sie begeben sich damit in die Abhängigkeit vom Hersteller, der sich um die Sicherheit dieser Dienste und seiner Anmeldeportale kümmern muss. Tritt dort eine Sicherheitslücke auf, sind Sie zwar nicht der einzige Betroffene, das hilft Ihnen dann aber auch nicht weiter.

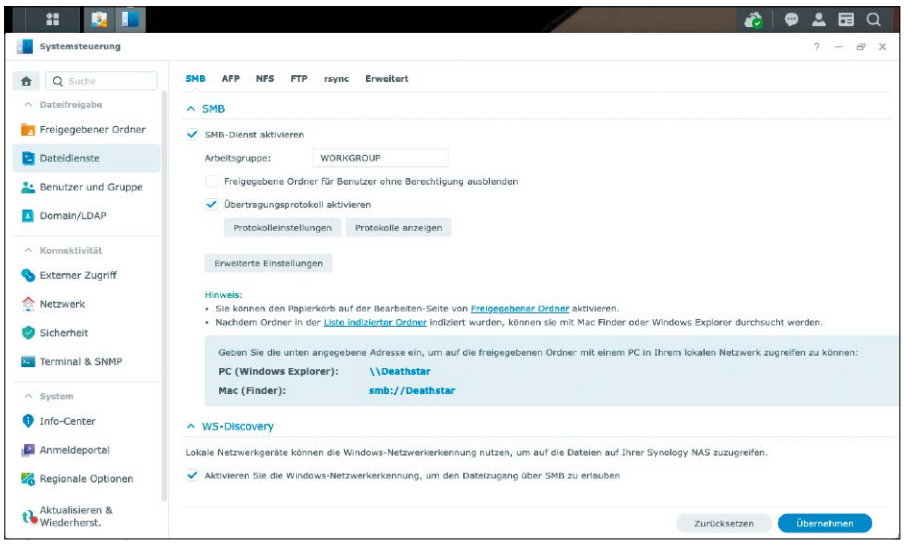
Falls Sie diese Dienste abschalten: Wie präsentieren Sie dann etwa unterwegs Ihre Fotos? Eine denkbare Alternative wäre ein zusätzlicher Raspberry Pi als Server. Es gibt unzählige Anwendungen, die Galerien für Fotos anbieten. Und mittels eines Programms wie Rsync können Sie auf dem NAS gespeicherte Bilder mit dem Raspberry abgleichen. Sie kommen also zum gleichen Ergebnis, ohne den Zugang zum zentralen Datenspeicher freizugeben.

Ein NAS bleibt besser ein NAS

Was gibt es nicht alles an Softwarepaketen für die NAS-Modelle der führenden kommerziellen Hersteller? Der Zugriff auf diese Wundertüte ist verführerisch, schließlich handelt es sich ja um einen kleinen Computer in einem kompakten Gehäuse, der rund um die Uhr läuft. Der Ansatz, ein NAS durch allerlei Zusatzfunktionen aufzubohren, stammt noch aus der Zeit, als kompakte und stromsparende Computer noch ziemlich teuer waren. Spätestens mit dem Raspberry Pi wurde das anders. Dessen Ausstattung überholt inzwischen ältere NAS-Systeme in der Leistung deutlich.



Eine der wichtigsten Sicherheitsmaßnahmen für jedes NAS-System besteht darin, den bereits vorhandenen User „admin“ zu deaktivieren oder zu löschen.



Alles abschalten, was nicht benötigt wird oder redundant ist: Apple kommt gut mit SMB zurecht. Kontrollieren Sie, welche sonstigen Dienste noch aktiv sind – E-Mail vielleicht?

Sie sollten sich also genau überlegen, ob Sie sich einen Gefallen tun, wenn Sie ein Serversystem wie Wordpress auf dem gleichen System laufen lassen, das alle wichtigen Dokumente und Erinnerungen speichert. Besser für Wartung und Sicherheit ist es, das NAS auf seine Kernfunktion zu beschränken. Wenn es Bedarf an weiteren Serverfunktionen gibt, sollte für einen Raspberry noch Platz sein. Diese Investition sollten Ihnen die Daten wert sein.

Nicht nur Synology hat in den vergangenen Jahren viel unternommen, die Sicherheit der Geräte zu verbessern. Mit wachsender Verbreitung wurden diese aber auch verstärkt Ziel von Attacken. Es lohnt sich, den Bereich „Sicherheit“ in der Systemsteuerung genauer anzuschauen. Hier finden Sie Optionen, um Passwörter regelmäßig erneuern zu lassen, können deren Stärke vorgeben und auch zu häufige Anmeldeversuche blockieren.

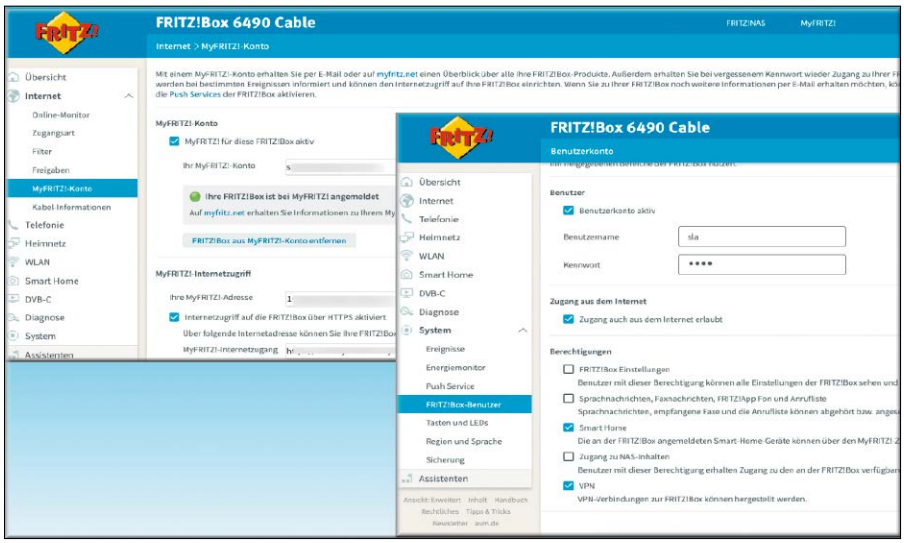
Ob nun ein NAS eines kommerziellen Herstellers oder Raspberry-Server im Eigenbau: Sie sollten das System stets aktuell halten. Wird eine Aktualisierung des Betriebssystems angeboten, installieren Sie diese möglich zügig. Bei einem kommerziellen NAS wird es zudem auch gelegentlich neue Firmware geben, die Sie ebenfalls einspielen sollten.

Alle Maßnahmen nützen nichts, falls das Gerät gestohlen oder irreparabel geschädigt ist. Deswegen benötigt ein NAS mit wertvollen Daten streng genommen ein weiteres Datenbackup, das an einem anderen Ort liegt. ■

Mit VPN sicher und anonym

Mit einem VPN bleiben vertrauliche Daten auch in einem fremden Netzwerk sicher. Aber nicht alle VPN-Lösungen sind gleich. Wir erklären, wie Sie VPN einsetzen und eigene Server aufsetzen.

VON STEPHAN LAMPRECHT



Fritzbox als VPN-Server: Dazu muss „MyFritz“ aktiviert und einem Nutzer der Zugang per VPN erlaubt werden.

Der Grundgedanke hinter einem „Virtual Private Network“ besteht darin, eine sichere Verbindung zwischen zwei verschiedenen Netzen herzustellen. Dabei wird die Infrastruktur einer potenziell feindlichen Umgebung verwendet. Da die Signale zwischen beiden Netzen verschlüsselt werden, läuft die Kommunikation sicher in einer Art Tunnel ab. Deswegen werden VPN-Verbindungen oft als „Tunnel“ bezeichnet. Via VPN können sich die Mitarbeitenden mit dem Unternehmensnetzwerk verbinden, genauso, als säßen sie am Schreibtisch im Büro. Das weltweite Internet schrumpft somit auf die Funktion eines ziemlich langen LAN-Kabels. Wenn Sie über diese VPN-Verbindung mit Ihrem Browser einen Server aufrufen, nutzen Sie die IP-Adresse des VPN-Netzwerks, also nicht die vom DSL- oder Kabelprovider zugewiesene Adresse. Genau damit werben kommerzielle Anbieter.

Was leistet ein VPN?

Ziemlich marktschreierisch, wie es sich für Werbung gehört, bieten im abendlichen TV-Programm eine Reihe von Unternehmen die Nutzung ihrer VPN-Verbindungen an: Nur damit könne man heute sicher und anonym im Internet surfen. Wie bei Werbung üblich, ist das nicht völlig falsch, hat aber einen Haken. Kommerzielle VPN-Anbieter können die Grundlagen des Internets nicht aushebeln. Damit Datenpakete zwischen zwei Punkten ausgetauscht werden können, benötigt ein Client eine IP-Adresse. Sie bekommen also auch bei Nutzung des Angebots eine IP-Adresse zugewiesen. Nur ist die nicht mit der tatsächlichen IP-Adresse Ihres Anschlusses identisch. Insofern surfen Sie „anonym“. Dazu gleich noch einmal mehr. Erst einmal zum Nutzen eines VPN selbst.

Sie benötigen Server und Client: Um ein VPN einzusetzen, benötigen Sie einen VPN-Server. Der kümmert sich um den Verbindungsaufbau und sichert im Hintergrund den Datenverkehr. Und Sie müssen auf dem Client, also Ihrem Computer, Tablet oder Smartphone, eine VPN-Verbindung einrichten, die dann die Daten des Servers nutzt.

Was kann das eigene VPN und was kann es nicht? Für Firmen ist die Nutzung eines VPN schon allein deshalb interessant, weil über die Verbindung zum Computer auch Informationen rauschen, die besser vertraulich bleiben. Aber auch für Privatanwender gibt es gute Gründe: Wenn Sie unterwegs ein fremdes WLAN nutzen, können Sie nicht sicher sein, dass dieses nicht kompromittiert wurde und Informationen mitgeschnitten werden, zum Beispiel Kreditkarteninformationen. Mit einem VPN bleiben diese Informationen verschlüsselt und uneinsehbar. Ein gewichtiges Argument der kommerziellen Anbieter liegt aber nicht in der Vertraulichkeit der Verbindungen, sondern in der Umgehung des Geoblockings: Einfach die Software des Anbieters nutzen, eine IP-Adresse des gewünschten Landes auswählen und schon können Sie sich auch Videos oder Sportübertragungen ansehen, die aus Deutschland nicht abrufbar sind. Oder umgekehrt, wenn Sie sich gerade im Ausland befinden.

Anonym sind Sie damit indes nicht, denn die Adressräume wurden von den Anbietern reserviert. Wenn Sie auf Anonymität angewiesen sind, müssen Sie darauf vertrauen, dass der Anbieter Ihre tatsächliche IP-Adresse und Ihre Daten für sich behält. Einen Anbieter, mit dem wir gute Erfahrun-

gen gemacht haben, nennen wir am Ende des Artikels. Um wirklich anonym zu bleiben, müssten Sie sich aber eher mit einer Lösung wie dem TOR-Browser anfreunden. Wenn es aber in erster Linie darum geht, sichere Verbindungen in einer fremden Netzumgebung aufzubauen, ist ein VPN perfekt. Wie Sie dies erreichen, zeigen wir anhand von Beispielen mit sehr unterschiedlichem technischen Aufwand.

Der schnelle Weg zum VPN: Die Fritzbox

Ein einfacher Weg zum VPN besteht darin, die eigene Fritzbox als VPN-Server zu nutzen. Befinden Sie sich also im fremden WLAN eines Cafés oder Hotels, stellen Sie eine Verbindung mit Ihrer heimischen Fritzbox her. Rufen Sie anschließend eine Internet-URL auf, wird diese von Ihrer Fritzbox ausgeliefert. Das funktioniert problemlos, wenn Ihr Anschluss via IPv4 erreicht werden kann. Die Nutzer eines Kabelanschlusses benötigen einen regulären Dual-Stack. Zeigt die Fritzbox, dass sie DS-Lite verwendet, kommt diese VPN-Methode nicht infrage.

Die Einrichtung des VPN-Zugangs verläuft bei allen anderen Anschlüssen so: Als Basis dient der von AVM angebotene Cloud-Dienst „MyFritz!“. Melden Sie sich an Ihrer Fritzbox an und gehen Sie auf „Internet → MyFritz!-Konto“. Sofern Sie noch kein solches Konto besitzen, geben Sie eine gültige E-Mail-Adresse ein und folgen den Schritten für die Registrierung. Im Verlauf müssen Sie die E-Mail-Adresse bestätigen, werden auf die AVM-Seite weitergeleitet und legen ein (starkes!) Passwort an.

Sobald Sie ein solches Konto besitzen, zeigt Ihnen der Besuch des Menüs, dass die Fritzbox mit dem Dienst verbunden ist, ferner auch die öffentliche Internetadresse der Fritzbox. Unter dem Feld mit der URL befindet sich der Schalter für die Einrichtung eines Nutzers, der auf die Fritzbox extern zugreifen darf. Klicken Sie auf „FritzBox-Benutzer einrichten“. Nun vergeben Sie einen Benutzernamen und ein Passwort. Nach „Übernehmen“ muss die Eingabe mit einer Tastenkombination eines angeschlossenen Telefons bestätigt werden oder mit der Fritz-Taste auf dem Router. Um jetzt den Zugang zu testen, benötigen Sie eine externe Verbindung etwa über das Smartphone mit mobilen Daten und bei ausgeschaltetem WLAN. Sie nutzen dabei die erwähnte URL und verwenden den Benutzernamen und das Passwort des gerade angelegten Benutzers. Jetzt wechseln Sie über „System → Fritzbox-Benutzer“ und klicken auf das Stiftsymbol neben dem Benutzer. Hier aktivieren Sie dann die Option „VPN“. Nach „Übernehmen“ ist der Zugang realisiert.

Im nachfolgenden Dialog sehen Sie eine Zusammenfassung der Zugangsdaten. Drucken Sie sich diese am besten aus. Mit diesen Informationen können Sie jetzt auf anderen Geräten eine VPN-Verbindung herstellen (siehe Kasten „VPN-Zugang nutzen“).

```
root@sla-Inspiron-15-5518: /etc/wireguard
sla@sla-Inspiron-15-5518:~$ sudo -i
[sudo] Passwort für sla:
root@sla-Inspiron-15-5518:~# cd /etc/wireguard
root@sla-Inspiron-15-5518:/etc/wireguard# umask 077
root@sla-Inspiron-15-5518:/etc/wireguard# wg genkey | sudo tee privatekey | wg pubkey | sudo tee pubkey
AxdTy8fs1cwvPii8TyKFUynits2zhlyQe/aUZ+ti0QI=
root@sla-Inspiron-15-5518:/etc/wireguard# ls
privatekey  pubkey
```

Um Wireguard einzusetzen, müssen auf dem Server und dem Client Schlüsselpaare erzeugt werden, die dann wechselseitig hinterlegt werden.

```
root@sla-Inspiron-15-5518: /etc/wireguard
root@sla-Inspiron-15-5518: /etc/wireguard
 GNU nano 5.6.1                          /etc/wireguard/wg0.conf
[Interface]
PrivateKey =
Adress = 192.168.207.1/24
ListenPort = 51820
SaveConfig = true


PostUp = ufw route allow in on wg0 out on eth0
PostUp = iptables -t nat -I POSTROUTING -o eth0 -j MASQUERADE
PostUp = ip6tables -t nat -I POSTROUTING -o eth0 -j MASQUERADE
PreDown = ufw route delete allow in on wg0 out on eth0
PreDown = iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
PreDown = ip6tables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
```

Die Verbindungen und erlaubten Clients werden in Wireguard in einer Konfigurationsdatei hinterlegt.

Wireguard: Eigener VPN-Server unter Ubuntu

Mehr Möglichkeiten haben Sie, wenn Sie einen eigenen VPN-Server einrichten. Mit Wireguard gibt es eine relativ einfach zu installierende Lösung. Um Wireguard benutzen zu können, benötigen Sie einen Rechner, auf dem Linux läuft und der über das Internet zu erreichen ist. Das darf auch eine virtuelle Maschine im Internet sein. Das ist vor allem dann eine gute Lösung, wenn Sie den VPN-Zugang nur verwenden wollen, wenn Sie unterwegs sind.

VPN-PROTOKOLLE

Für die sichere Kommunikation via VPN müssen sich Client und Server verständigen. Grundlage ist dabei ein gemeinsames Datenprotokoll. Die drei wichtigsten sind folgende:

- **Open VPN** ist quelloffen und recht verbreitet, beim Aufbau eines Servers allerdings nicht einfach zu durchschauen. Software wie Pi VPN räumt aber viele Hürden aus dem Weg. Auf Open VPN basieren auch häufig die Ansätze kommerzieller Anbieter.
- **Wireguard** ist eine freie VPN-Software, die ein eigenes Protokoll nutzt und für die meisten Betriebssysteme zur Verfügung steht.
- **L2TP/IPSec** sind streng genommen zwei Protokolle, die stets in Kombination genutzt werden. Es wird häufig im professionellen Umfeld genutzt, wenn Administratoren Homeoffice-Arbeitsplätze oder externe Standorte mit dem Unternehmensnetzwerk verbinden wollen. Die Fritzbox nutzt ein Derivat dieses Protokolls für ihr VPN.

Daheim starten Sie einfach die Instanz beim Hoster und nach Ihrer Rückkehr wird sie wieder beendet.

Zur Installation von Wireguard genügt bei vielen Distributionen ein Befehl:

```
sudo apt install wireguard
```

Nutzen Sie eine LTS-Version von Ubuntu, wie das bei virtuellen Maschinen oft der Fall ist, werden Sie die Paketquellen erst ergänzen müssen. Dies folgt dem bekannten Muster:

```
sudo add-apt-repository
  ppa:wireguard/wireguard
sudo apt update
sudo apt install wireguard
```

Im nächsten Schritt sorgen Sie dafür, dass alle Pakete, die an der Wireguard-Schnittstelle ankommen, weitergeleitet werden. Dazu öffnen Sie die Datei „/etc/sysctl.conf“. Hier tragen Sie zwei Zeilen ein:

```
net.ipv4.ip_forward=1
net.ipv6.conf.all.forwarding=1
```

Eventuell sind die Zeilen vorhanden und es genügt, das Kommentarzeichen „#“ zu entfernen. Speichern Sie die Datei und aktualisieren Sie die Konfiguration mit diesem Befehl:

```
sysctl -p
```

Die Kommunikation bei Wireguard wird mittels öffentlicher und privater Schlüssel auf dem Server und dem Client abgesichert. Deswegen muss das Schlüsselpaar zunächst auf dem Server angelegt werden. Das geht – mit root-Recht – so:

```
cd /etc/wireguard
umask 077
wg genkey | sudo tee privatekey | wg
  pubkey | sudo tee pubkey
```

Anschließend liegen im Verzeichnis „/etc/wireguard“ zwei Dateien, die unschwer als privater und öffentlicher Schlüssel zu erkennen sind. Jetzt kommt die einzige Hürde. Wireguard arbeitet als Router in seinem VPN-Netz. In der Konfiguration müssen Sie daher eine virtuelle Netzwerkschnittstelle schaffen, die hier mit „wg0“ bezeichnet werden soll. Der Router muss einen Adressraum verwalten, der sich mit den IP-Adressen Ihres eigentlichen Netzwerks nicht in die Quere kommt. Mit einem Editor legen Sie die Datei „/etc/wireguard/wg0.conf“ an und tragen dort folgende Zeilen ein:

```
[Interface]
PrivateKey = [privaten Key hier
  eintragen]
Address = 192.168.207.1/24,
  fd0d:86fa:c3bc::1/64
ListenPort = 51820
SaveConfig = true
```

Ein Wort zu den Adressen. Der erste Wert definiert den IPv4-Bereich 192.168.207.1 bis 192.168.207.254, der im Netzwerk des Autors nicht verwendet wird. Wenn Sie IPv6-Adressen nutzen wollen, ist die Schaffung einer sogenannten „Unique Local Address“ nicht so einfach, weil es nahezu unendliche Möglichkeiten gibt. Unter *https://simpledns.plus/private-ipv6* können Sie sich einen zufällig generierten Adressraum erstellen lassen. Das erleichtert die Sache. Speichern Sie die Datei.

Jetzt geht es an das Forwarding der Pakete. Dazu finden Sie zunächst die Netzwerkschnittstelle des Servers heraus, die öffentlich erreichbar ist. Führen Sie in einem Terminal das Kommando

```
ip route list default
```

aus. Bei den ausgegebenen Strings suchen Sie nach dem Eintrag mit dem Zusatz „dev“. Dahinter steht dann der Name der Schnittstelle, etwa „eth0“. Jetzt öffnen Sie erneut die Datei „/etc/wireguard/wg0.conf“ und fügen am Ende der Datei diesen Codeblock ein.

```
PostUp = ufw route allow in on wg0
  out on eth0
PostUp = iptables -t nat -I
  POSTROUTING -o eth0 -j MASQUERADE
PostUp = ip6tables -t nat -I
  POSTROUTING -o eth0 -j MASQUERADE
PreDown = ufw route delete allow in
  on wg0 out on eth0
PreDown = iptables -t nat -D
  POSTROUTING -o eth0 -j MASQUERADE
PreDown = ip6tables -t nat -D
  POSTROUTING -o eth0 -j MASQUERADE
```

Nach dem Speichern der Datei müssen Sie noch der Firewall gestatten, Datenverkehr zum Port von Wireguard durchzulassen:

```
sudo ufw allow 51820/udp
sudo ufw allow OpenSSH
```

Mit root-Recht stoppen Sie einmal die Firewall (*sudo ufw disable*) und starten Sie erneut (*sudo ufw enable*), damit die Änderungen aktiv werden. Wenn Wireguard beim Start des Systems aktiviert werden soll, konfigurieren Sie noch den Dienst:

```
sudo systemctl enable wg-quick@wg0.
  service
sudo systemctl start wg-quick@wg0.
  service
```

Dies gilt für alle Ubuntu & Co. mit Systemd.

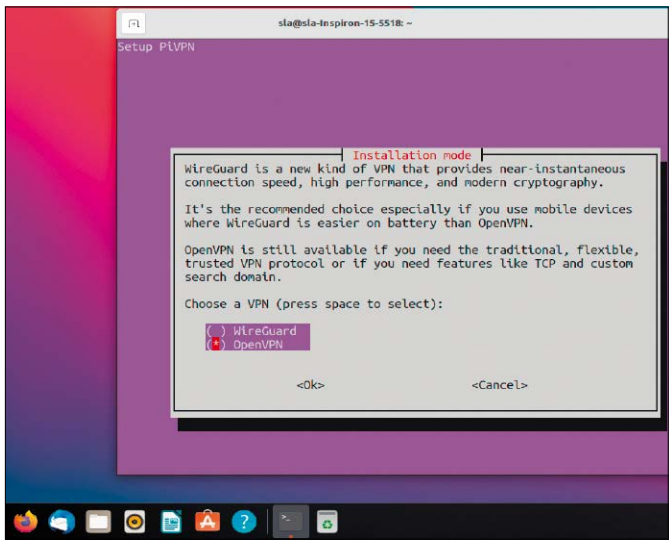
Wireguard: Clientgeräte einrichten

Für mobile Clients mit Android und iOS gibt es in den App Stores die passende Software zur Einrichtung. Soll ein Linux-Client eingerichtet werden, installieren Sie darauf Wireguard. Anschließend müssen Sie dort – wie gezeigt – ein Schlüsselpaar erzeugen. Mit einem Editor wie Nano

```
sudo nano /etc/wireguard/wg0-
  client.conf
```

legen Sie auf dem Client eine eigene Konfigurationsdatei an. Bei der Wahl des Namens sind Sie völlig frei, die Ähnlichkeit mit der Serverdatei ist hier beabsichtigt, um die Unterschiede deutlich zu machen. Die Datei erhält zunächst einmal folgenden Inhalt:

```
[Interface]
PrivateKey = [privaten Key hier
  eintragen]
# Wir zählen einfach die IP-Adresse
  um "1" hoch
```



Pi VPN wurde eigentlich für den Raspberry Pi entwickelt. Es funktioniert aber auch unter Ubuntu und anderen Distributionen und vereinfacht die Einrichtung von Open VPN erheblich.

```
Address = 192.168.207.2/24
Address = fd0d:86fa:c3bc::2/64
[Peer]
PublicKey = [öffentlicher Key des
 Servers]
AllowedIPs = 192.168.207.1/24
Endpoint = [Server-IP oder Domain-
 Name]:51820
```

Das ist die grundlegende Konfiguration. Wenn Sie vorhaben, jeglichen IP-Verkehr durch den Tunnel zu schicken, müssen noch ein paar Ergänzungen vorgenommen werden. Diese lesen Sie am besten in der offiziellen Dokumentation des Projekts nach. Sie müssen dem Server anschließend noch mitteilen, dass sich der Client verbinden darf. Das geht mit einem einfachen Kommando im Terminal:

```
wg set wg0 peer [öffentlicher
 Schlüssel des Clients] allowed-ips
 192.168.207.2/24
```

Läuft der Server, starten Sie eine Verbindung auf dem Client im Terminal:

```
sudo wg-quick up wg0
```

Damit sollte die Verbindung stehen.

VPN mit Raspberry Pi und Open VPN

Eine Alternative zu Wireguard ist Open VPN. Damit und mit einem Raspberry Pi können Sie einen VPN-Server verblüffend einfach umsetzen. Möglich macht dies das Projekt Pi VPN (*https://www.pivpn.io/*). Ursprünglich ausschließlich für Open-VPN-Verbindung gestartet, kann es heute auch das Wireguard-Protokoll verwenden. Die Installation und Einrichtung sind inzwischen auch nicht mehr ausschließlich auf den Raspberry beschränkt.

Mit dem Kommando

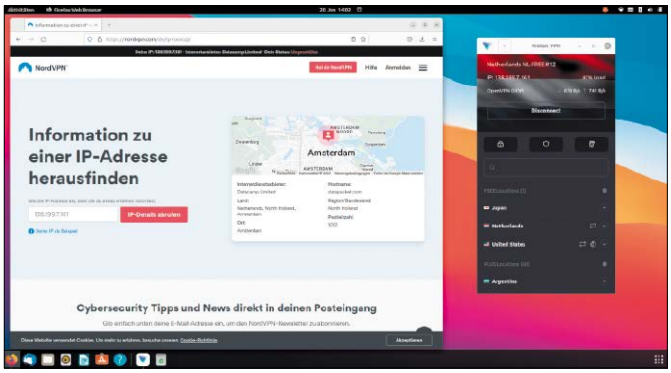
```
curl -L https://install.pivpn.io |
 bash
```

starten Sie die Einrichtung und Konfiguration, die problemlos bei IPv4-Adressen funktioniert. Hier gelten also die gleichen Einschränkungen am Kabelanschluss, wie sie bereits erwähnt wurden.

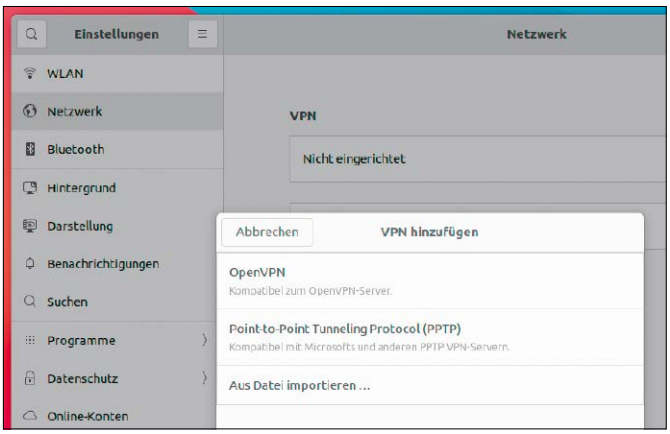
Das Programm begleitet Sie durch alle Schritte inklusive der optionalen Auswahl eines alternativen DNS-Servers. Auch auf die Portweiterleitung am Router werden Sie hingewiesen. Hier kann tatsächlich nichts schiefgehen. Einmal abgeschlossen, legen Sie mittels

```
pivpn add
```

einen Client an, der dann auch die Zugangsdatei erzeugt.



Der kommerzielle Anbieter Proton aus der Schweiz hat einen untadeligen Ruf. Die Installation und Nutzung gehen leicht von der Hand.



Open VPN erzeugt für Clients eine Zugangsdatei. Deren Informationen lassen sich etwa im Network-Manager von Ubuntu einfach importieren.

Kommerzieller Anbieter: Proton VPN

Kommerzielle Angebote reduzieren den technischen Aufwand auf ein Minimum. Ob der VPN-Anbieter allerdings Ihre Daten speichert oder ob Sie tatsächlich anonym surfen, ist eine Frage des Vertrauens. Einen untadeligen Ruf genießt das Schweizer Unternehmen Proton, das auch einen kostenfreien VPN-Zugang anbietet. Dieser finanziert sich aus den Gebühren der Nutzer, die sich für das kostenpflichtige Abo entschieden haben, das mehr Geschwindigkeit und mehr Konfigurationsoptionen bietet (für fünf bis zehn Euro pro Monat). Die Einrichtung unter Ubuntu ist extrem einfach. Sie holen sich von der Website *https://protonvpn.com* das Installationspaket und installieren es per Doppelklick.

Damit werden zunächst nur die Paketquellen hinzugefügt. Nach dem Update der Quellen installieren Sie mit

```
sudo apt update
sudo apt install protonvpn
```

die Software.

Das war dann auch schon alles: Programm starten, die Zugangsdaten zum Proton-Account eintragen – das genügt und Sie können die gewünschte geografische Verbindung auswählen und nutzen. ■

VPN-ZUGANG NUTZEN

Wie nutzen Sie eine VPN-Verbindung auf den Clients? Kommerzielle Anbieter stellen entweder eine eigene Software für die Einwahl zur Verfügung oder zumindest die passende Konfigurationsdatei. Unter Ubuntu können Sie unter den Einstellungen im Bereich „Netzwerk“ und „VPN“ eine neue Verbindung mit einem Klick auf das Pluszeichen hinzufügen. Sie haben anschließend die Auswahl, die Details aus einer Datei zu importieren. Solche Dateien erzeugt auf Wunsch auch Open VPN. Bei Wireguard nutzen Sie entweder die passende App für mobile Geräte oder müssen, wie im Haupttext beschrieben, die Software installieren und die Konfiguration anpassen.

Schotten dicht: Ports und Dienste

Was läuft hier? Auf Linux-Systemen, die schon lange in Betrieb sind, einige Experimente mitgemacht haben oder von anderen Personen eingerichtet wurden, ist eine Überprüfung der laufenden Dienste und geöffneten Ports empfehlenswert.

VON DAVID WOLSKI



Die großen, gut gepflegten Linux-Distributionen Debian, Ubuntu, Fedora und Open Suse sind auch für den Einsatz auf Servern geschaffen. Sie müssen im Grundzustand, also nach einer Installation, in einer sicheren Konfiguration vorliegen und dürfen nicht ungefragt Serverdienste starten, die Ports ins Netzwerk öffnen. Wer schon mal kleine Server von der Sorte Raspberry Pi eingerichtet hat, weiß, dass dieser geschlossene Ansatz auf Kosten von Komfort und Bequemlichkeit geht. Er verhindert aber, dass ein Linux-System schon in seiner Standardkonfiguration angreifbar ist oder mit unzureichenden Standardpasswörtern Zugriff auf laufende Serverdienste eröffnet.

Übersicht: Server und geöffnete Ports

Auf einem Server verschaffen Tools in der Kommandozeile per Innenansicht den Überblick, welche laufenden Prozesse auf einem Netzwerkport geöffnet haben. Diese bieten einen unverstellten Blick auf die Zuordnung von Ports und Diensten über den Kernel, ohne dabei einen vorgeschalteten Portfilter zu beachten.

Netstat: Der traditionelle Weg, geöffnete Ports anzuzeigen, führt über das Tool netstat. In aktuellen Linux-Distributionen ist es nicht mehr vorinstalliert, liegt aber im Paket „net-tools“ in den verbreiteten Linux-Distributionen bereit und ist in Debian/Ubuntu mit dem Befehl

```
sudo apt install net-tools
```

zu installieren. Anschließend liefert

```
sudo netstat -tulp
```

eine tabellarische Übersicht zu Protokollart (TCP oder UDP), verwendeten Netzwerkadressen und verbundenen Adresse bei aktiven Verbindungen. In den letzten beiden Spalten namens „PID/Program name“ und „State“ zeigt das Tool Status und Prozessnamen der Dienste. Steht beim Status „LISTEN“, dann wartet der Prozess auf eingehende Verbindungen. Die Portzuordnung erfolgt in der Spalte „Local Address“ hinter einem Doppelpunkt. Steht hier also beispielsweise „0.0.0.0:22“, bedeutet das, dass ein Dienst auf allen verfügbaren Netzwerkadressen („0.0.0.0“) auf dem Port 22 lauscht. Dies ist üblicherweise der SSH-Server und am Ende der Zeile werden hier eine Prozessnummer und der Prozessname angegeben sein – „sshd“ in diesem Beispiel.

Lsof: In neueren Linux-Distributionen wird zunehmend statt dem älteren, nicht stetig weiterentwickelten netstat das Tool lsof empfohlen. Die Eingabe

```
sudo lsof -P -i tcp | grep LISTEN
```

erstellt eine ähnliche, etwas übersichtlichere Tabelle lauschender Prozesse mit Namen und Portnummer. Die Dienst- und Prozessnamen stehen hier gleich am Anfang jeder Zeile.

Zuordnung von Prozess und Dienst: Zum grundsätzlichen Verständnis offener Ports gehört die Tatsache, dass sich ein Netzwerkport nicht wie eine Tür schließen lässt. Vielmehr muss der verantwortliche Task oder Dienst beendet sein, um damit auch den Port zu schließen. Noch wichtiger ist die Tatsache, dass offene Ports im lokalen Heimnetz kein Risiko bedeuten, solange diese nicht per Portfreigabe im Router für das Internet geöffnet werden. Die von lsof oder netstat angezeigten Namen verweisen

entweder auf ein Programm oder auf einen Dienst. Die meisten Linux-Distributionen nutzen heute Systemd zur Diensteverwaltung und ein Befehl wie dieser

```
sudo systemctl status sshd
```

zeigt dann Informationen zum befragten Dienst an. In diesem Beispiel handelt es sich um den Open-SSH-Server. Alle diese Schritte dienen zur Identifizierung, was auf einem Linux-System unter der Haube läuft. Wenn es klar ist, dass ein Dienst überflüssig ist, so hilft ein Trick dabei, diesen testweise abzuschalten: Das Kommando

```
sudo shutdown -r 10
```

setzt einen automatischen Neustart des Systems in zehn Minuten an und

```
sudo systemctl stop sshd
```

stoppt den angegebenen Dienst, hier den Open-SSH-Server. Nun hat man zehn Minuten Zeit zu testen, ob der Linux-Server weiterhin wie gewünscht funktioniert. Klar, ausgerechnet den SSH-Dienst abzuschalten, dürfte in den meisten Fällen kontraproduktiv sein, denn nun ist keine neue Anmeldung mehr über das Netzwerk per SSH möglich. Dies ist aber nicht weiter schlimm, denn nach zehn Minuten startet der Server neu und reaktiviert den Dienst wieder. Erst das Kommando

```
sudo systemctl disable --now sshd
```

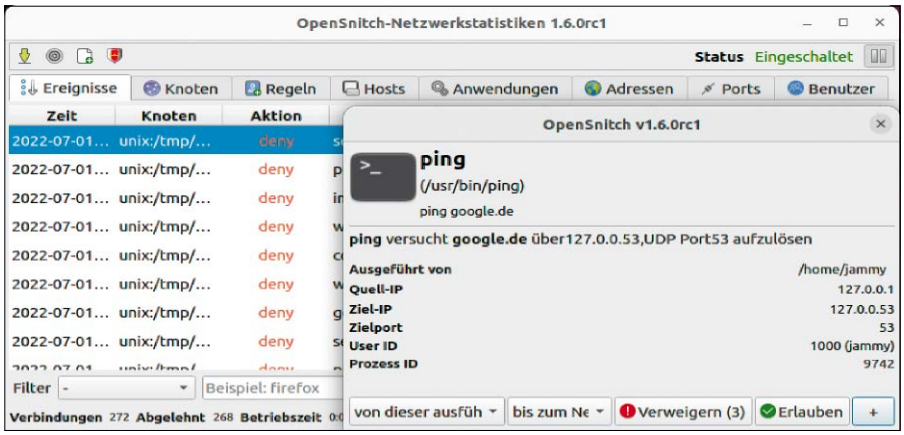
würde den angegebenen Dienst dauerhaft abschalten.

Opensnitch: Check für Desktopsysteme

Von Mac-OS X ist das Tool Little Snitch bekannt, das die angeforderten Netzwerkverbindungen von Programmen überwacht. Das grafische Python-Tool Opensnitch überträgt das Konzept auf den Linux-Desktop und erlaubt einen Blick darauf, was Anwendungen ins Netzwerk senden und von dort empfangen. Das englischsprachige Tool für Fortgeschrittene liegt unter *https://github.com/evilsocket/opensnitch/releases* auf der Github-Webseite des Entwicklers. Die Installation unter Ubuntu und Abkömmlingen wie Linux Mint erfolgt über die angebotenen DEB-Dateien „opensnitch_[Version]_amd64.deb“ und „python3-opensnitch-ui_[Version].deb“, die man in ein leeres Verzeichnis herunterlädt und dort dann mit dem Befehl

```
sudo dpkg -i *.deb
sudo apt -f install
```

installiert. Der zweite Befehl löst die weiteren Abhängigkeiten auf und Opensnitch wird dann noch einige Python-Pakete automatisch nachinstallieren.



Eingehende und ausgehende Verbindungen aufzeigen: Opensnitch ist eine Desktopfirewall (Anwendungsfirewall) für Linux, die Programmen den Netzwerkzugriff auch verweigern kann.

Ubuntu ab Version 22.04: Bevor die Oberfläche von Opensnitch funktioniert, ist noch die Installation einer zusätzlichen Bibliothek mittels

```
sudo apt install python3-pip
pip3 install --ignore-installed
  grpcio
```

nötig. Auf dem Linux-System startet Opensnitch einen Systemd-Dienst und legt ein Symbol im Infobereich der Systemleiste ab, das in einem Fenster die Netzwerkverbindungen nach Prozessen aufschlüsselt. Außerdem schlägt Opensnitch immer Alarm und zeigt die Verbindungsdetails an, sobald eine Anwendung zum ersten Mal eine Netzwerkverbindung herstellt. Die Verbindung kann der Button „Allow connection“ erlauben oder mit „Block connection“ verbieten. Wer das Tool später nicht mehr benötigt, kann es mit dem Befehl

```
sudo apt remove --purge opensnitch
```

wieder vom System entfernen (und damit auch den zugehörigen Wächterdienst).

Paketfilter: UFW-Regeln erstellen

Paketfilter sind sinnvoll, wenn Serverports für das Internet freigegeben sind und somit Dienste öffentlich nach außen anbieten. Auf üblichen Desktopsystemen ist dies standardmäßig nicht der Fall und Linux-Distributionen installieren deshalb auch keine Firewallregeln. Ubuntu macht es aber heute mit dem Tool ufw (Uncomplicated Firewall) vergleichsweise einfach, Regeln für das nicht ganz triviale Kernel-Paketfilter zu erstellen.

Mit dem Kommando

```
sudo apt install ufw
```

ist das Tool bei Bedarf installiert. Die Syntax ist einfach gehalten und erstellt im Hintergrund die komplexeren nftables-Regeln. Um beispielsweise nur den Port 22 (SSH) zu erlauben, genügt dieser Befehl:

```
sudo ufw allow 22
```

Anschließend wird die Firewall mit

```
sudo ufw enable
```

gestartet und mit

```
sudo ufw status
```

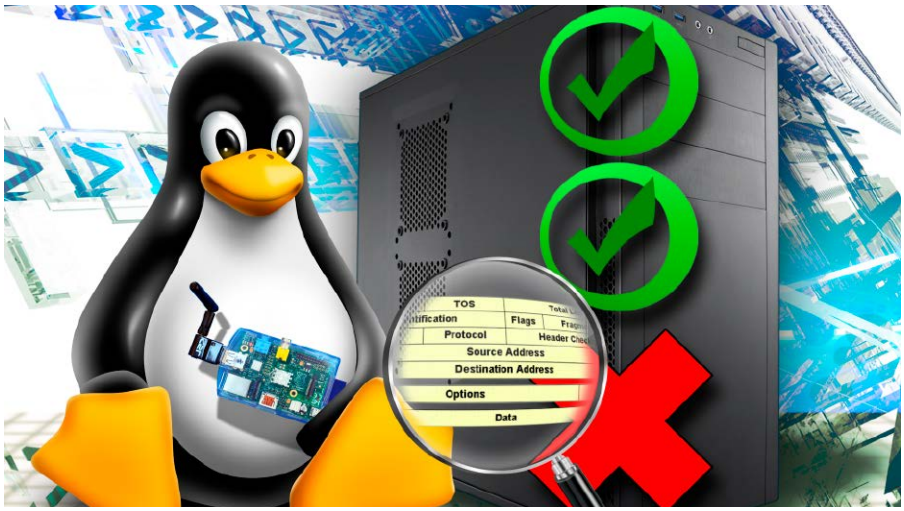
überprüft. ■

„WELL KNOWN PORTS“: BEKANNTE HAUSNUMMERN

Die Portnummern zwischen 1 und 1023 sind reservierte Ports für häufig verwendete Serverdienste, auf die Clients einen typischen Dienst erwarten dürfen. So nutzen beispielsweise Webserver für HTTP den Port 80 und für HTTPS den Port 443. Diese „Well Known Ports“ ermöglichen den Clients die Verbindung zu Servern, ohne dass eine explizite Konfiguration notwendig wäre. Um die Organisation dieser Portnummern kümmert sich die Internet Assigned Numbers Authority (IANA) und stellt die aktuelle Liste mit weiteren Dokumenten unter *www.iana.org/assignments/port-numbers* bereit. Eine deutschsprachige Übersicht hat die Wikipedia (Liste_der_standardisierten_Ports).

Einbrüche erkennen

Wer will auf meinen Linux-Server? Gibt es eventuell doch eine übersehene oder ungepatchte Schwachstelle, die ungebetene Gäste anlockt? Aktive Überwachungsmethoden informieren über verdächtige Aktivitäten auf Linux-Servern.



VON DAVID WOLSKI

Erschwingliche Ein-Platinen-Computer und günstige Cloudinstanzen haben den Aufwand erheblich gesenkt, einen Linux-Server zu betreiben. Bei jedem von außen erreichbaren Server sind aber rigorose Sicherheitsvorkehrungen Pflicht, die das System sicher halten und einen Einbruch unwahrscheinlich machen. Das betrifft auch heimische Miniserver, die nur an einer DSL-Leitung hängen und lediglich über eine dynamische Hostadresse erreichbar sind. Auch dort werden ungebetene Besucher anklopfen und Einlass begehren. Dieser Beitrag zeigt erst zwei einfache Methoden, das System per Logauswertung im Auge zu behalten, und geht dann auf das Intrusion Detection System (IDS) Tripwire ein.

Vor Einbrüchen: Das System checken

Ein Linux kann nur so nur sicher sein, wie es seine Konfiguration zulässt. Automatisierte Checks helfen, potenziell unsichere Einstellungen, manipulierte Dateien und typische Konfigurationsfehler aufzuspüren. Je nachdem, welche Serverdienste auf einem System aktiv sind, wählt Lynis die passenden Tests aus seiner Datenbank und liefert eine englischsprachige Auswertung in seiner eigenen Logdatei. Die stets aktuelle Version von Lynis ist auf der Entwickler-Seite bei Github verfügbar und mit einigen Befehlen schnell eingerichtet: Zuerst holt

```
git clone https://github.com/
  CISOfy/lynis
```

die Dateien von Github. Dann geht es mit

```
cd lynis
```

in das Verzeichnis, wo der Befehl

```
sudo chown -R 0:0 *
```

den Scripts die benötigten Berechtigungen gibt. Der Befehl

```
sudo ./lynis audit system
```

führt das Tool mit sudo-Recht aus. Lynis zeigt den Fortschritt und Warnungen im Terminalfenster. Nach dem Abschluss des Testlaufs präsentiert Lynis Empfehlungen zur Absicherung des Systems sowie URLs mit Hintergrundinformationen. Die Warnung zu „systemd-analyze security“ kann man dabei ignorieren, denn dabei geht es nur um optionale Sandbox-Funktionen von Systemd, welche Linux-Distributionen in ihrer Standardkonfiguration nicht nutzen.

Logwatch: Über Angriffe informiert

Eine schnell eingerichtete automatische Auswertung von Logdateien, die Angriffsmuster über das Netzwerk zeigt, liefert das Programm Logwatch. Es erstellt täglich einen Bericht über ungewöhnliche Vorkommnisse auf dem System. Auf Servern mit einem Mailserver wie Postfix/Sendmail/Exim2 kann es den Bericht auch per Mail an einen User auf dem lokalen System senden, die dieser per „mutt“ abruft – also mit dem Mailprogramm in der Shell. Soll ein Benutzer wie root auf dem System die Zusammenfassung im lokalen Postfach erhalten, so genügt dazu auch ein lokaler Mailserver ohne Verbindung zu einem anderen SMTP-Server im Internet.

Debian, Raspbian, Ubuntu, Fedora, Open Suse und Arch bieten alle das Paket „logwatch“ in ihren Paketquellen. In Debian & Co. wird es mit

```
sudo apt install logwatch
```

installiert. Das Kommando

```
sudo logwatch
```

präsentiert im Terminal eine Übersicht zu Ereignissen. Erkannte Scans gegen einen Webserver wie Apache und Nginx sowie SSH-Angriffe sind ganz oben aufgelistet.

Tripwire: Einen Stolperdraht spannen

Auf wichtigen oder exponierten Linux-Servern kann ein IDS (Intrusion Detection System) helfen, unautorisierte Manipulationen an vordefinierten Dateien sofort zu erkennen. Prominente Konfigurationsdateien von Webservern bieten sich dafür an. Das wäre für einen Server der größte anzunehmende Unfall und das System wird danach als Ganzes nicht zu retten sein. Die Gewissheit darüber ist aber enorm wichtig, denn

unentdeckte Einbrüche, übernommene Server unter fremder Kontrolle sind ein wahrer Alptraum.

Ein lange bewährtes IDS auf Dateisystemebene ist Tripwire („Stolperdraht"). Es kontrolliert Dateien nach vorher erstellten Checksummen, welche in einer geschützten signierten Datenbank hinterlegt sind. Auf Änderungen hin schlägt Tripwire Alarm – nach einem manuellen Check, automatisch per E-Mail oder auch in einer eigenen Logdatei. Zu beachten ist, dass Tripwire auch bei unbeaufsichtigten Updates anschlägt und die Berichte dann sehr umfangreich werden. Es verlangt daher etwas Übung, die Berichte zu lesen. Tripwire ist dennoch einfach genug, um beispielsweise das Verzeichnis eines Webservers und bestimmte Konfigurationsdateien im Auge zu behalten. Die Installation gelingt in den tonangebenden Distributionen über die Standard-Paketquellen, in Debian/Ubuntu über dieses Kommando:

```
sudo apt install tripwire
```

Die Installation sorgt auch gleich für die erste Initialisierung des Wächters mit einigen Abfragen.

1. Mailversand: Soll der Administrator Mails von Tripwire erhalten, so kann hier Postfix konfiguriert werden. „Nur lokal" ist die richtige Option für den Mailempfang nur auf dem gleichen System.

2. Passwörter: Die Abfrage nach der Erzeugung der Site-Passphrase für Tripwire und des lokalen Schlüssels beantwortet man mit „Ja". Ebenso die Frage, ob die Tripwire-Konfigurationsdatei und Richtliniendatei neu erzeugt werden sollen. Gut merken muss man sich die dann vergebenen neuen Passwörter für die Tripwire-Administration, denn sie werden später immer wieder verlangt.

3. Neue Regel definieren: In diesem Beispiel soll Tripwire das Apache-Konfigurationsverzeichnis „/etc/apache2/sites-available" mitüberwachen. Dazu öffnet man die Datei „/etc/tripwire/twpol.txt" mit root-Recht oder vorangestelltem „sudo" in einem Texteditor. Ans Ende der Datei kommen folgende Zeilen:

```
(
rulename = "Apache2",
severity= $(SIG_HI)
)
{
/etc/apache2/sites-available ->
 $(SEC_CRIT);
}
```



Lynis in Aktion: Der Scanner präsentiert gefundene Sicherheitslücken, potenzielle Probleme und Empfehlungen, um die Sicherheit eines Linux-Systems systematisch zu verbessern.



Tripwire schlägt an: In unserem hinzugefügten überwachten Verzeichnis „/etc/apache2/sites-available" gab es Änderungen an Dateien, wie Tripwire in seinem Bericht auflistet.

Anschließend erzeugt das Kommando

```
sudo twadmin -m P /etc/tripwire/
 twpol.txt
```

die Regel-Datei neu und fragt dazu die zuvor vergebene Site-Passphrase ab.

4. Datenbank erstellen: Nun soll Tripwire die Checksummen der überwachten Dateien erstellen, was der Befehl

```
sudo tripwire --init
```

nach der Eingabe des Tripwire-Passworts („local passphrase") erledigt. Dieser Schritt ist immer nach Änderungen am System und Aktualisierungen notwendig, um neue Checksummen zu erzeugen.

5. Check ausführen: Eine manuelle Überprüfung führt nun der Befehl

```
sudo tripwire --check
```

aus. Wurde die Apache-Konfiguration zwischenzeitlich geändert, so moniert die Ausgabe von Tripwire dies im Abschnitt „Rule Name: Apache2" und listet dort die betroffenen Dateien auf. ■

VIRENSCANNER: FÜR DATEISERVER WICHTIG

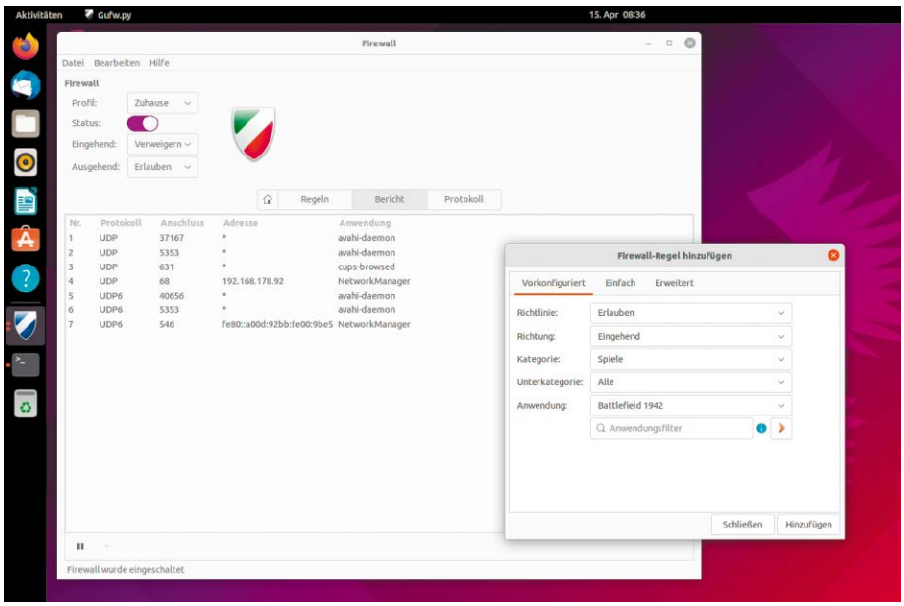
Für ein stets aktualisiertes Linux-System ist Malware kaum ein Risiko, zumal die Zahl von wirksamen Linux-Viren verschwindend gering ist. Eine reale Gefahr ist aber die versehentliche Verbreitung von Windows-Viren und Würmern in Netzwerken über einen Linux-Dateiserver, dem zwar die Malware nichts ausmacht, der diese aber im Netzwerk verteilt. Linux-Anwender sollten daher verdächtige Downloads, insbesondere ausführbare Windows-Dateien, zum Check auf den von Google betriebenen Onlinedienst Virustotal (*www.virustotal.com*) hochladen und analysieren lassen.

Für automatisierte Scans per Kommandozeile gibt es für Linux den Virenscanner Clam AV. Die Erkennungsraten für Malware liegen bei Tests bei 76 Prozent, damit ist Clam AV im Mittelfeld. Verweise auf Paketquellen für verbreitete Linux-Distributionen liefert die Projektwebseite. Für Nextcloud als Dateiserver gibt es Clam AV übrigens auch als Plug-in.

Sicherheitswerkzeug für Linux

Wie können Sie die Sicherheit eines Linux-Systems wirkungsvoll erhöhen? Wir stellen hier interessante Sicherheitstools vor, deren Einsatz Sie je nach Nutzung und Netzwerksituation in Betracht ziehen sollten.

VON STEPHAN LAMPRECHT



Spätestens dann, wenn Sie das heimische Netzwerk verlassen, sollten Sie die im System enthaltene Firewall aktivieren. Dank grafischer GUI ist die Konfiguration nicht schwierig.

Rund um das Thema Linux-Sicherheit existieren eine ganze Reihe von Mythen, die von vielen Anwendern kritiklos übernommen werden. Das kann fahrlässig sein. So wäre es doch schade, wenn ausgerechnet Ihr Linux-PC das Sprungbrett für das Einschleusen von Malware oder Ransomware wäre, die Ihr Smarthome lahmlegt. Mit den hier vorgestellten Tools härten Sie ihr System und tragen zu mehr Sicherheit bei.

Firewall einschalten und konfigurieren

Eine Firewall auf dem PC gehört sicherlich zu den unbeliebtesten Programmen überhaupt. Ambitionierte Anwender, denen der Systemadministrator für ihre Windows-Rechner eine solche Firewall installiert hat, gehen oft gleich daran, diese umgehend wieder zu deaktivieren.

Auch unter Linux gehört es zu einem der großen Mythen, dass man auf einem Einzelplatzrechner gar keine Firewall benötigt. Eine eigene Meinung zu haben, ist in vielerlei Hinsicht wichtig. Aber von der völligen Nutzlosigkeit einer Firewall sind offenbar die Entwickler der meisten Distributionen nicht überzeugt und statten die Systeme mit einer aus.

Eine Firewall am lokalen PC ist tatsächlich (fast) nutzlos, wenn das System immer im lokalen Netzwerk betrieben wird, das durch eine leistungsfähige und aktivierte Firewall des Routers geschützt ist. Das trifft allerdings eher selten zu. Zwar besitzen alle handelsüblichen Router für das Heimnetzwerk eine Firewall, deren Güte ist aber variabel und kann kaum vom Nutzer beeinflusst werden. Wer nicht zu tief in die Konfiguration der persönlichen Firewall einsteigen will, sollte sich für sein Ubuntu- respektive Debian-basiertes System den grafischen Aufsatz GUFW installieren. Dazu genügt im Terminal ein Befehl:

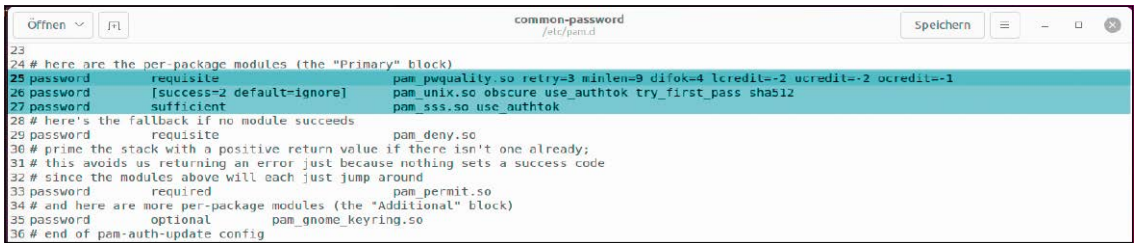
```
sudo apt install gufw
```

Die Software taucht dann als „Firewall Konfiguration“ auf. Dank vordefinierter Profile und Anwendungen fällt die Konfiguration nicht schwer. Mittels Schieberegler schalten Sie die Firewall ein. Im Abschnitt „Bericht“ erkennen Sie mit einem Blick, welche Dienste auf welchen Ports aktiv sind, während Sie im Register „Regeln“ dann einfach mit einem Klick auf das Pluszeichen weitere Filter anlegen und einrichten. Unter „Vorkonfiguriert“ brauchen Sie sogar nur zwischen den angebotenen Anwendungen zu wählen, um dann sinnvolle Filterregeln auszuwählen. Einfacher geht es kaum.

Das System ist damit deutlich besser geschützt. Verlassen Sie sich also besser nicht auf die Mythen, sondern nutzen Sie die Firewall, insbesondere wenn Notebooks auch in fremden Netzwerken zum Einsatz kommen.

Bessere Passwörter am Familien-PC

Die Sache mit den Passwörtern ist auch so eine Sache. Wie Befragungen immer wieder ergeben, bevorzugen viel zu viele Nutzer triviale Passwörter. Die meisten Linux-Systeme sind zwar so konfiguriert, dass sie einen Warnhinweis liefern, wenn ein zu einfaches Passwort vergeben wird. Am



Vergabe von allzu einfachen Passwörtern verhindern: Dafür lassen sich verbindliche Regeln einrichten, die komplexe Passwörter zwingend einfordern.

Ende akzeptieren sie es aber dennoch. Um den inneren Schweinehund zu überwinden oder bei Multiuser-Systemen die Vergabe von komplexen Passwörtern zu erzwingen, können Sie selbst mit ganz einfachen Mitteln etwas tun.

Hilfreich ist der Einsatz des PAM-Moduls pwquality. Das installieren Sie zusammen mit einem Wörterbuch, das bereits eine Reihe von Trivialpasswörtern enthält. Zur Einrichtung des Tools genügt dieser Befehl:

```
sudo apt install libpam-pwquality
  cracklib-runtime
```

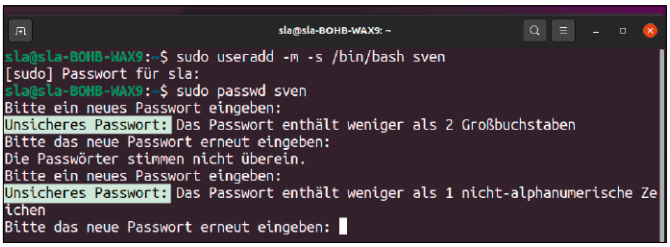
Die Runtime ist möglicherweise bereits auf Ihrem System vorhanden. Einmal installiert, können Sie jetzt die Regeln für neue Passwörter nach Ihren Vorstellungen verschärfen. Dazu öffnen Sie mit root-Recht die Datei „/etc/pam.d/common-password“. Suchen Sie hier nach dieser Zeile:

```
password requisite pam_pwquality.
  so retry=3
```

Diese ergänzen Sie dann um weitere Parameter. Mit „minlen“ legen Sie die Mindestlänge des neuen Passworts fest, mit „difok“ definieren Sie, wie viele Zeichen eines bestehenden Passworts weitergenutzt werden dürfen. Die Parameter „lcredit“ und „ucredit“ stehen für die Zahl der Klein- und Großbuchstaben, die verwendet werden müssen. Die Angabe der notwendigen Ziffern regelt „dcredit“, Sonderzeichen fordert „ocredit“. Die entsprechenden Angaben stehen jeweils hinter einem Gleichheitszeichen. In die Einzelheiten des Systems einzusteigen, würde etwas den Rahmen sprengen. Kurioserweise müssen Sie den Zahlen in diesem konkreten Fall ein negatives Vorzeichen voranstellen, obwohl Sie damit definieren, wie viele dieser Zeichen vorkommen sollen. Eine konkrete Zeile im Editor könnte dann so aussehen:

```
password requisite pam_pwquality.
  so retry=3 minlen=9 difok=4
  lcredit=-2 ucredit=-2 ocredit=-1
```

Speichern Sie die Datei und starten Sie den Rechner neu. Wenn Sie jetzt als root etwa versuchen, das Passwort eines bestehenden Nutzers zu verändern, greifen die Regeln. Das System informiert Sie, welche Elemente Sie noch verändern müssten, damit es sich um ein gültiges Passwort handelt.



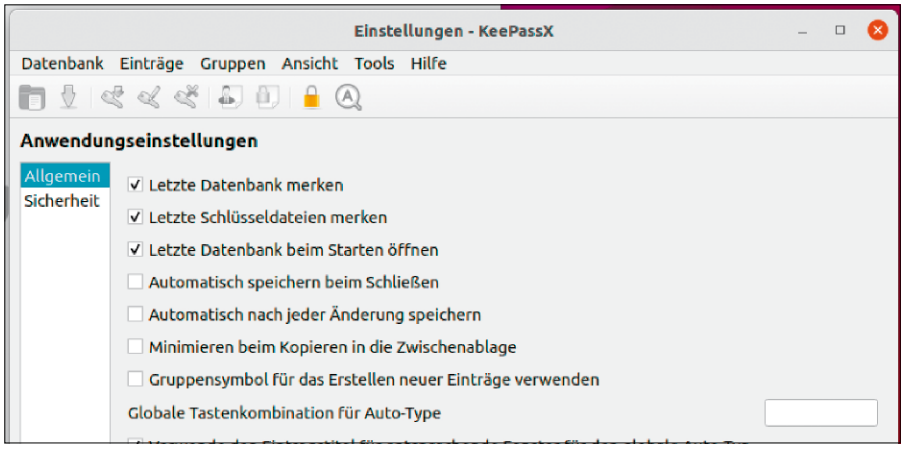
Passwortkontrolle: Einmal aktiviert, darf nicht einmal root beim Einrichten neuer Nutzer schwache Passwörter vergeben.

Ein Passwortmanager gehört dazu

Das Internet steckt voller guter Tipps, wie ein sicheres Passwort aussehen kann und wie man sich auch komplexere Passwörter einfacher merken kann. Vieles davon funktioniert bestimmt auch, stammt aber meist noch aus der Zeit, als sich die Nutzerinnen und Nutzer nur die Zugangsdaten zum Onlinebanking, die Anmeldung am Arbeits-PC und vielleicht noch den Zugang zu einem Shop merken mussten. Inzwischen nutzen wir alle so viele Webdienste, dass es eine echte Herausforderung ist, sich das alles zu merken.

Ein Passwortmanager ist daher ein Sicherheitstool, dessen Einsatz uneingeschränkt zu empfehlen ist. Besonders komfortabel wird das unter Einbeziehung der Cloud. Denn damit funktioniert der Zugang mit unterschiedlichen Systemen und die Passwörter sind stets aktuell. Ein Favorit der Redaktion ist das Programm Bitwarden, das es in Versionen für Linux, Mac, Windows und mobile Geräte gibt. Zudem gibt es Erweiterungen für alle verbreiteten Browser, die das Ausfüllen von Anmeldedialogen deutlich vereinfachen.

Wer beim Gedanken zusammenzuckt, dass die eigenen Passwörter in der Cloud liegen, kann Bitwarden auch auf einem eigenen Server betreiben. Das ist aber nur dann sinnvoll, wenn man bereit ist, sich dann auch um die Sicherheit dieses Systems aktiv zu kümmern. Bitwarden selbst ist kostenlos, für erweiterte Funktionen, wie etwa ein Zugang für Dritte im Notfall oder die direkte Integration von 2FA-Absicherungen, wird eine moderate Gebühr von zehn Dollar im Jahr fällig. An dieser finanziellen Hür-



Ein guter Passwortmanager wie Bitwarden oder Keepassx (im Bild) trägt zur Sicherheit bei, weil man sich komplexe Passwörter nicht merken muss.

de sollte die Sicherheit nicht scheitern. Die Bedienung ist einfach und eine Installation unter Linux etwa mit

```
sudo snap install bitwarden
```

schnell erledigt.

Wem Cloudlösungen grundsätzlich missfallen, kann stattdessen mit einer eigenen Passwortdatei hantieren und diese beispielsweise verschlüsselt auf einem USB-Stick stets mit sich führen. Eine gute Lösung für einen lokalen verschlüsselten Passworttresor ist der Keepassx. Das seit Jahrzehnten bewährte Programm gehört zur Grundausstattung der Paketquellen aller Distributionen.

Viren und Rootkits erkennen

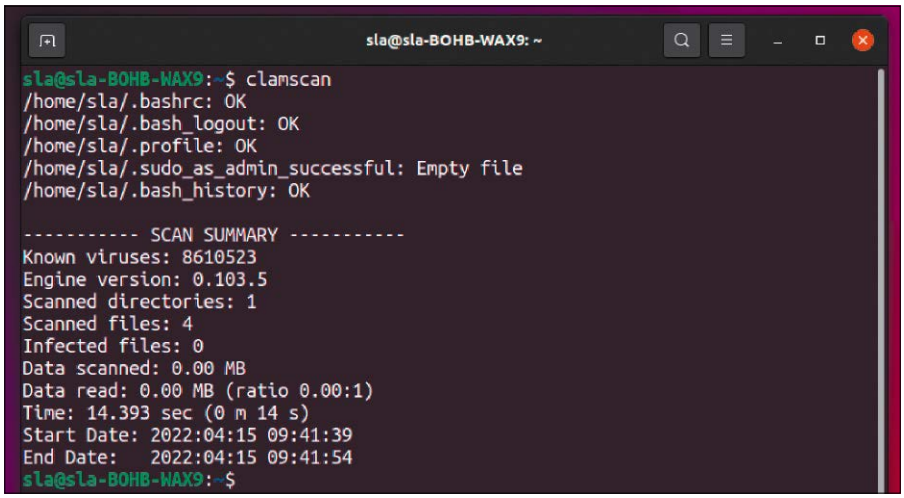
An dieser Stelle zu einem weiteren gefährlichen Mythos unter Linux – die angebliche Sicherheit vor Viren und anderen Schädlingen. Spricht das schmale Angebot an Virenscannern für Linux nicht dafür, dass Linux-Systeme unverwundbar sind? Das ist eher eine Frage der Perspektive. Gerade weil so viele Anwender glauben, dass es keine Schädlinge für Linux gibt, existiert wenig Nachfrage nach Lösungen, die sich dann wirtschaftlich entwickeln ließen. Fairerweise ist aber anzumerken, dass die grundlegende Architektur von Linux es Entwicklern von Schadprogrammen tatsächlich schwer macht.

Was trotzdem für den Einsatz eines Scanners spricht, ist neben dem Eigen- auch der Fremdschutz. Wenn jeder, der erkältet ist, im öffentlichen Raum eine Maske tragen würde, bekämen nicht so viele Menschen seinen Schnupfen ab. Wer sein System nach Schädlingen untersucht, unterbricht die Verbreitungskette. Abhilfe bringt das einfache Kommando:

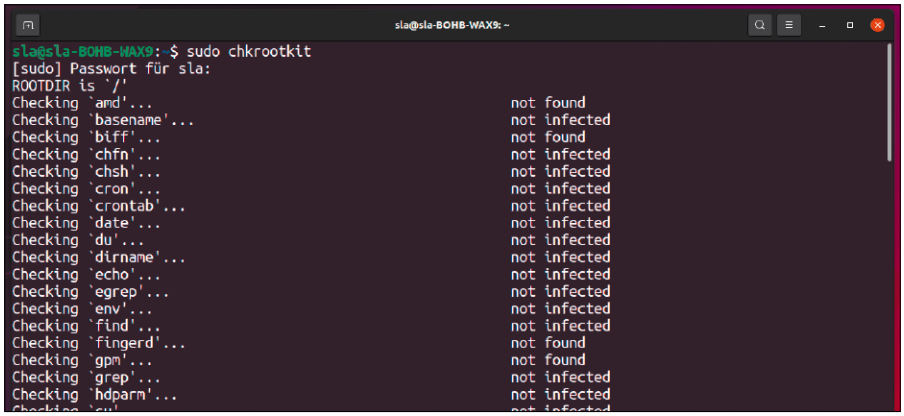
```
sudo apt install clamtk
```

Dies installiert die Antivirenlösung Clam AV inklusive grafischer Oberfläche. Die Oberfläche des grafischen Aufsatzes (Clam AV ist auch über ein Terminal und via Scripts zu benutzen) macht die Arbeit mit der Software einfach. Für einen Scan einer neuen Datei oder eines neu angelegten Ordners steht der Bereich „Analyse“ zur Verfügung, über den Sie eine manuelle Überprüfung starten.

Damit Sie sich nicht um die Aktualisierung der Definitionsdateien kümmern müssen, ist es ratsam, im „Planer“ der Software eine Uhrzeit zu definieren, zu der das System täglich nach Updates sucht. Dort können Sie ebenfalls einen täglichen automatischen Scan einrichten. Dazu wählen Sie mit den Schaltern die jeweilige Stunde aus und übernehmen die Eingabe mit einem Klick auf das Pluszeichen. Sie erhalten anschließend den Hinweis, dass eine tägliche Überprüfung respektive Aktualisierung geplant ist.



Der Einsatz eines Virenscanners sollte auch unter Linux zu den Hygienemaßnahmen gehören. Es erhöht die Sicherheit und unterbricht Verbreitungsketten.



Das Tool Chkrootkit: Zur eigenen Routine sollte auch die Überprüfung auf Rootkits gehören.

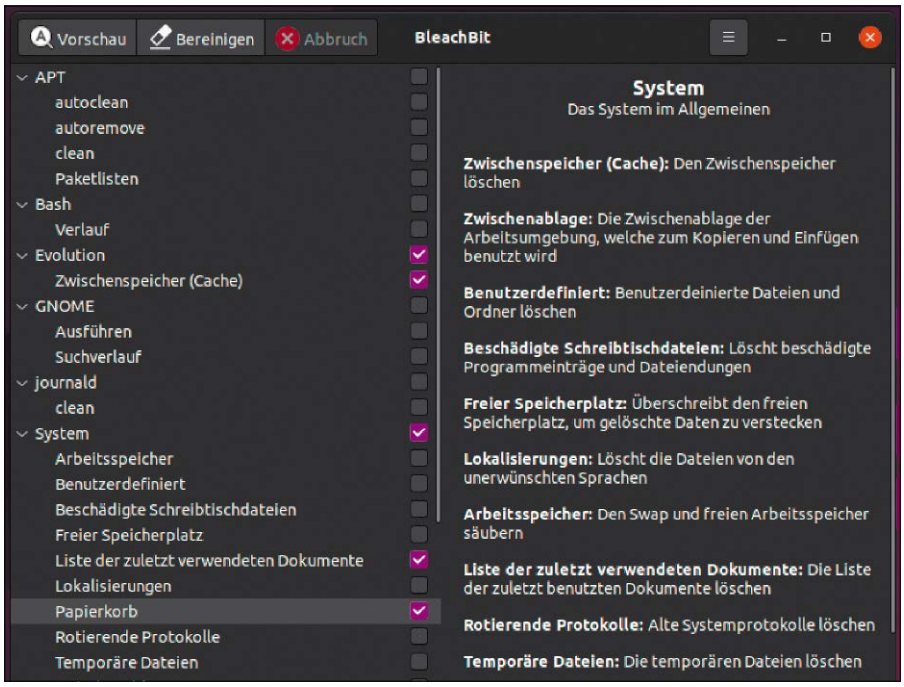
Ebenfalls eine gute Maßnahme, die zur Verbesserung der Sicherheit des Systems beiträgt, ist die regelmäßige Suche nach Rootkits. Dabei handelt es sich um eine besondere Form der Schadsoftware, mit der Angreifer versuchen, auf einem System root-Recht zu gewinnen. Bekanntlich stehen damit alle Türen offen.

Das kleine Werkzeug Chkrootkit ist ein Programm für die Kommandozeile, die nach bekannten Rootkits sucht. Das geht schnell und kann automatisiert erfolgen, wenn Sie die Ausführung als Cronjob definieren. Chkrootkit ist in allen Distributionen mit gleichnamigem Paketnamen zu beziehen. Danach führen Sie das Programm einfach in einem Terminal aus. Strenggenommen ist nicht auszuschließen, dass Chkrootkit selbst kompromittiert worden ist. Besonders Vorsichtige werden also das Programm in einem externen Livesystem verwenden. Zusätzlich kann der Einsatz einer ähnlichen Software wie Rkhunter sinnvoll sein, um sich eine Zweitmeinung zu sichern.

Bleachbit beseitigt Spuren

Auf jedem System sammeln sich Datenreste und Informationen, die für andere Nutzer oder Angreifer von Interesse sein könnten. Das betrifft nicht zuletzt temporär angeschlossene Datenträger wie USB-Sticks und Speicherkarten. Wer sein System härten und die Sicherheit vergrößern möchte, sollte solche Datenreste regelmäßig entfernen. Eine Software, die einen guten Kompromiss zwischen Bedienbarkeit und Leistungsvermögen bietet, ist Bleachbit, das in den Paketquellen der meisten Distributio-

nen vorliegt. Nach dem Programmstart haben Sie die Gelegenheit, aus einer ganzen Reihe von Optionen die Bereiche auszuwählen, um die sich die Anwendung kümmern soll. Das kann der Zwischenspeicher eines Mailprogramms sein oder das Überschreiben von freiem Speicherplatz in der Form, dass hier auch Experten keine sinnvollen Informationen wiederherstellen können. Bleachbit überlässt Ihnen die Entscheidung darüber, welche Informationen Sie löschen wollen. Nach der Auswahl der Bereiche führt dann das Kommando „Bereinigen" die Aufgaben durch. Über das Menü der Anwendung finden Sie auch die Funktionen „Datei schreddern" und „Ordner schreddern", mit denen Sie die Inhalte von Datenträgern dauerhaft löschen. Das clevere Programm sollte in keiner Toolsammlung fehlen.



Datenreste regelmäßig entfernen und nicht mehr benötigte Datenträger unlesbar überschreiben: Diese Aufgaben gehen mit Bleachbit leicht von der Hand.

Anwendungen im Käfig

Liegen auf dem Arbeitsrechner besonders sensible Daten, können Sie die Ausführung von Programmen mit einem besonderen Schutz versehen. Dazu laufen die Anwendungen in einer Sandbox, also in einer vom Rest des Systems isolierten Umgebung. Bei der Konfiguration solcher Spezialwerkzeuge müssen Sie unbedingt die Dokumentationen der Entwickler lesen, um bei der Einrichtung keine Fehler zu machen. Es besteht nämlich sonst die Gefahr, dass Sie den Schutz so hoch ansetzen, dass die Anwendung gar nicht mehr startet.

Zu den Klassikern auf diesem Gebiet gehört Apparmor. Diese Sicherheitsergänzung wird standardmäßig in Ubuntu genutzt und ist dort auch aktiv. Das zeigt Ihnen dieser Terminalbefehl:

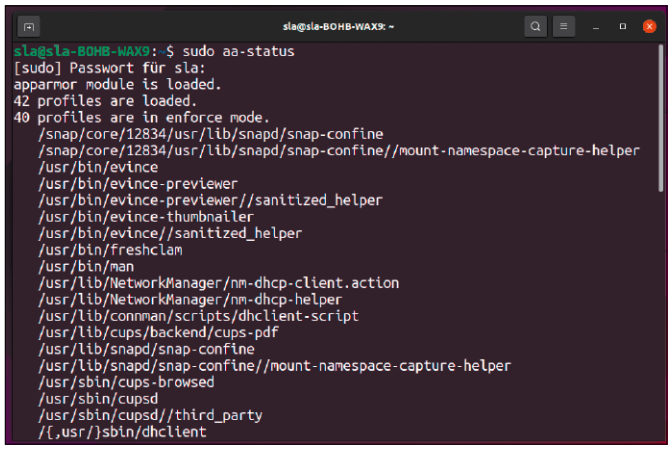
```
sudo aa-status
```

Apparmor basiert auf individuellen Profilen für die verschiedenen Anwendungen und kontrolliert jedes einzeln. Wer eigene Profile anlegen will, kann das tun, sollte dann aber auch wissen, was er da genau einrichtet. Im Fokus der Anwendung liegen Programme, die Netzwerkzugriff benötigen, oder auch Programme für die Büroarbeit, da darüber Schädlinge aller Art auf dem System landen können. Apparmor kennt mehrere Modi. In der Regel wird ein System im Complain-Modus ausgeliefert. Dabei werden Aktionen, die gegen die Regeln verstoßen, nicht unterbunden, sondern lediglich protokolliert. Das soll dann den Anwendern erlauben, gezielt die Profile zu verändern. Der Anwender kommt mit Apparmor kaum in Kontakt: Er startet Programme wie gewohnt und im Hintergrund laufen dann die Regeln ab.

Ein ebenfalls leistungsstarkes Programm für das Sandboxing ist Jailsafe, das Sie allerdings manuell installieren müssen. Weil es viele Funktionen bietet und sich Anfänger schnell verbasteln können, ist es nicht unumstritten. Auch Jailsafe arbeitet mit Profilen, die sich anpassen lassen. Um eine Anwendung innerhalb einer Sandbox auszuführen, genügt in einem Terminal der Aufruf von „firejail [Programm]", also etwa:

```
firejail firefox
```

Dadurch wird die Software dann gekapselt vom Rest des Systems ausgeführt.



Mit Apparmor landen Programme in der Sandbox. Das verringert die Anfälligkeit, das gesamte System zu kompromittieren.

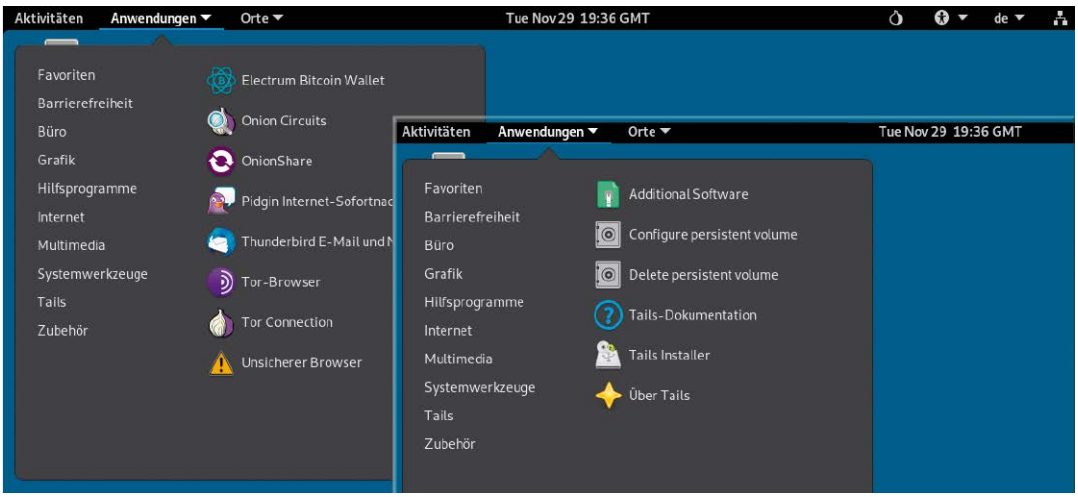
Backups: Die Grundlage für Sicherheit

Die richtigen Werkzeuge und eine sicherheitsbewusste Systemkonfiguration tragen zur erhöhten Sicherheit des Systems bei. Aber keine Maßnahme kann Attacken völlig verhindern oder den Befall mit Malware absolut ausschließen.

Die wichtigste Sicherheitsmaßnahme darf deshalb am Ende eines solchen Artikels nicht fehlen: Kümmern Sie sich um regelmäßige Datensicherungen. Ob Sie die Daten per Rsync mit einem NAS oder externen Server abgleichen oder ein Tool wie Duplicity einsetzen, spielt keine Rolle. Entscheidend ist, dass alle wichtigen Daten mindestens zweimal vorliegen. ■

Surfsystem Tails

Das auf Datenschutz und Anonymisierung spezialisierte Tails wird laufend verbessert. Das Livesystem wird häufig aktualisiert, nicht zuletzt um neuere Versionen von TOR-Browser und Mailclient anzubieten. Eine Neuerung ist der Metadaten-Cleaner.



Die Tails-Menüs mit den wichtigsten Tools: Das Livesystem liefert eine komplette Ausstattung für einen anonymisierten Internetzugang.

VON HERMANN APFELBÖCK

Wir nehmen die jüngsten Updates des Debian-basierten Tails („The Amnesic Incognito Live System“) zum Anlass, das prominente Surfsystem, seine Nutzung und seine Relevanz genauer vorzustellen. Unwichtiges wie den neuen „Metadata-Cleaner“ aus Version 5.7 lassen wir unberücksichtigt. Er ist eine unscheinbare Ergänzung: Er löscht lediglich aus ausgewählten Foto-, Office- und Mediendateien internen Infos.

Restriktives Tails: Ein Fall für Sonderfälle

Geht es „nur“ um sicheres Surfen, ist Tails gewiss nicht die adäquate Lösung. Dafür genügt schon Linux. Wenn Sie es noch sicherer haben wollen, verwenden Sie in Firefox die Add-ons Noscript und uBlock Origin (genau wie unter Tails). Für Datenschutz und Abwehr von Tracking sorgt in Firefox der „Private Modus“.

Und wer selbst das noch steigern will, nutzt den Browser in einer virtuellen Maschine mit einem kleinen Linux. Bequemer als Tails ist selbst die letzte Variante allemal.

Tails zeigt, dass kompromissloser Datenschutz umgekehrt proportional zu komfortabler Systembenutzung ist.

Tails ist ein Komplettpaket, das lokal auf der benutzten Hardware überhaupt keine Spuren hinterlässt und im Internet keinerlei persönliche Spuren, nicht einmal die IP-Adresse. Damit ist das Debian-System ohne Zweifel eine effektive Anonymisierungswaffe: Der Firefox-basierte TOR-Browser schickt Webanfragen verschlüsselt durch drei zufällige Stationen des TOR-Netzwerks (Entry-, Zwischen- und Exit-Node) zum öffentlichen Zielserver.

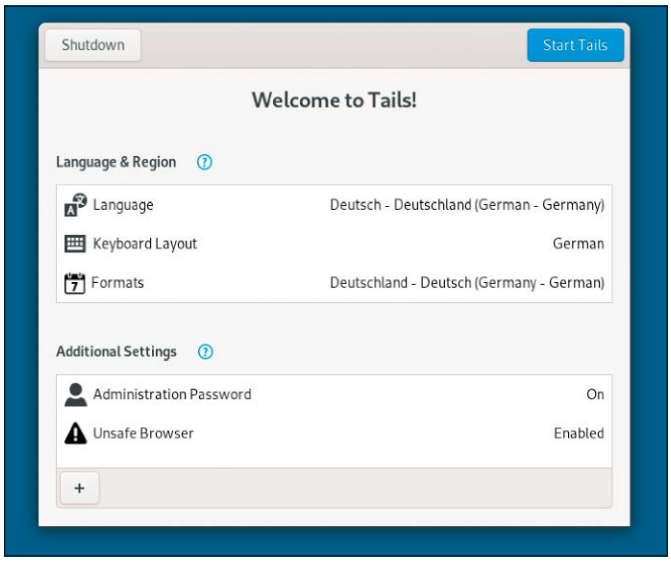
Der Zielserver erfährt folglich nur die IP-Adresse des Exit-Nodes, nicht diejenige des Rechners, von dem die Anfrage ursprünglich stammt. Innerhalb der TOR-Knoten kennt der Entry-Node zwar die IP-Adresse des Absenders, aber nicht den Inhalt der Anfrage (verschlüsselt), der Zwischen-Node weder die IP noch den Inhalt, der Exit-Node den Inhalt, der von dort unverschlüsselt zum Zielserver geht. Für den Rückweg gilt dasselbe. Die Nachverfolgung einer konkreten Internetaktion via TOR-Netz und TOR-Browser zu einer individuellen Person ist praktisch ausgeschlossen, es sei denn, es wären zufällig mehrere von Polizei und Geheimdiensten kontrollierte Nodes beteiligt. Der TOR-Browser funktioniert im gesamten öffentlichen Internet. Für das Darknet und dessen „Onion“-Sites ist das TOR-Netzwerk Bedingung.

Wer anonymes Surfen tatsächlich benötigt (in erster Linie Aktivisten, Regimegegner, Journalisten, Whistleblower, Hacker und Kriminelle), muss allerdings diverse Nachteile in Kauf nehmen, die aber allesamt berechtigt und in Tails technisch sauber umgesetzt sind:

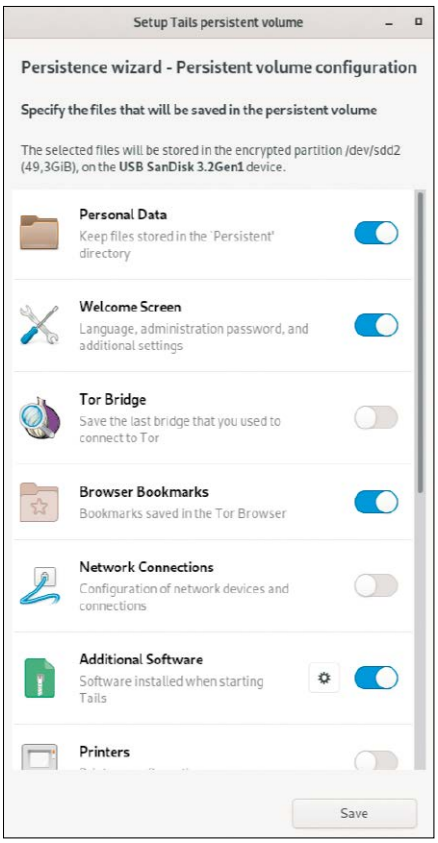
1. Das Livesystem schreibt sein komplettes Dateisystem in den Arbeitsspeicher und ist kaum unter 40, 50 Sekunden am „Welcome“-Dialog.

2. „Welcome“ ist immer zu absolvieren, um deutsche Tastatur/Region einzustellen, optional den verschlüsselten Persistenzspeicher aufzuschließen (Kennwort) und eventuell Extra-Optionen (root-Passwort, „Unsicherer Browser“) zu setzen. Erst danach kann mit „Start Tails“ der Gnome-Desktop starten.

3. Ein gemischtsprachiges System (englisch-deutsch) ist trotz deutscher Lokalisierung zu akzeptieren.



„Welcome“ muss sein: Deutsche Lokalisierung und eventuelle Sonderwünsche sind bei jedem Systemstart zu absolvieren. Persistenz kann hier aber manchen Klick einsparen.



Amnesie-Ausnahmen: Einige Einstellungen, zusätzliche Software und Benutzerdateien kann das Tails im Persistenzspeicher ablegen. Das macht die Nutzung ein Stück komfortabler.

4. Tails ist ein restriktives Livesystem, das auch lokal keine Spuren hinterlassen will und dem Liveuser „Amnesia“ standardmäßig keinen Zugriff auf lokale Festplatten, USB-Laufwerke oder Netzfreigaben erlaubt. Wem das zu weit geht, muss am „Welcome“ unter „Additional Settings“ das root-Passwort freischalten. Dies ist auch Voraussetzung für die Nachinstallation zusätzlicher Software (mit Persistenz als zweite Voraussetzung).

5. Lokale Netzadressen etwa des Heimrouters oder eines Apache-Servers sind im TOR-Browser unzugänglich, da hier alle Adressen über externe TOR-Knoten gehen. Für einen Zugriff auf lokale Adressen muss im „Welcome“-Dialog der „Unsichere Browser“ freigeschaltet werden.

6. Der Weg ins Internet via TOR-Browser benötigt immer zwei Aktionen – erst den Zugang zum TOR-Netz via „Tor Connection“ (Zwiebelsymbol in den Gnome-Favoriten), danach den Start des TOR-Browsers.

7. Das TOR-Netz ist langsamer als direkte Internetverbindungen. Statt zweier Sendungen (Anfrage und Antwort) handelt es sich hier um insgesamt acht Stationen. Noch entscheidender ist aber, dass ein einziger langsamer Node den gesamten Durchsatz bremst. Unterm Strich ist das TOR-Netz die letzten Jahre aber deutlich schneller geworden. Das liegt schlicht daran, dass die Bandbreiten ständig wachsen und sich kaum mehr ein TOR-Node unter 30 MBit/s findet (siehe dazu das Tails-Tool „Onion Circuits“).

8. Unter Tails sind personalisierte Aktionen zu meiden. Ein Beispiel wäre etwa die Anmeldung am Google- oder Microsoft-Konto. Da die Anmeldung vom Exit-Node des TOR-Netzwerks kommt, müssen Google und Microsoft einen Fremdzugriff vermuten (unbekanntes Gerät, ungewöhnliche Region) und sperren eventuell das Konto.

Installation und Persistenz

Tails wird unter *https://tails.boum.org/install* im ISO- und im IMG-Format angeboten. Das eher irritierende „Windows – Mac-OS – Linux“-Angebot dient dort nur dazu, den Benutzer gleich zu den passenden Imagetools zu führen. Das ISO verwenden Sie für DVDs oder für virtuelle Maschinen, das IMG-Format für USB-Sticks. Letzteres schreiben Sie unter Linux etwa mit Gnome-Disks oder dem KDE-Partitionmanager auf den USB-Stick, unter Windows mit dem Win 32 Disk Imager.

Im ausgelieferten Zustand macht Tails seinem Namen alle Ehre. Wenn Sie unter „Welcome“ nur auf „Deutsch“ setzen, auf „Additional Settings“ verzichten und keine Persistenz einrichten, wird das Livesystem sein Amnesie-Versprechen am lokalen System hundertprozentig einhalten. Die Webanonymisierung via TOR wurde bereits besprochen.

Wer es etwas bequemer haben will, sollte das Tresorsymbol im Gnome-Favoritendock nutzen. Dieses Tool tails-persistence-setup etabliert auf dem Tails-USB-Stick eine Luks-verschlüsselte Extrapartition. Dabei wird die verbleibende Restkapazität neben der Systempartition verwendet. Die Luks-Partition kann später beim Systemstart im „Welcome“-Fenster durch Kennworteingabe entsperrt werden. Das ist optional und kann auch entfallen, wenn die Dienste der Persistenz aktuell nicht benötigt werden.

Was die verschlüsselte Partition speichern soll, kann der Nutzer in einem hübschen Optionsdialog detailliert auswählen: Die wichtigsten Optionen sind „Personal Data“ (Benutzerdateien, später unter „Orte → Persistent“ erreichbar), „Additional Software“ (Nachinstallationen), „Browser Bookmarks“ (Lesezeichen im TOR-Browser) und „Welcome Screen“. Letztere Option ist nützlich, weil dann das Aufschließen der Persistenz alle Welcome-Optionen automatisch erledigt.

Um zusätzliche Software in den Persistenzspeicher zu installieren, muss unter „Welcome“ das root-Konto freigeschaltet werden. Außerdem erscheint nach jeder Installation eine Abfrage, die mit „Install Every Time“ zu beantworten ist. Trotzdem kann nachinstallierte Software später natürlich nur dann genutzt werden, wenn beim Start der Persistenzspeicher geöffnet wurde. ■

Orientierung im Heimnetzwerk

Linux-Systeme zeigen etwa im Dateimanager standardmäßig kaum oder keine Informationen zu Geräten im Netzwerk. Wer IP-Adressen und Ports beispielsweise für eine Weboberfläche sucht, ist auf andere Tools angewiesen.

VON THORSTEN EGGELING

Auch in kleinen Heimnetzwerk laufen heutzutage zahlreiche Geräte: Router, PCs, Notebooks, TV-Geräte, Smartphones, Tablets und einiges mehr sind miteinander verbunden. Im Vordergrund steht dabei, allen Geräten den Internetzugang zu ermöglichen. Nebenbei können die Geräte auch miteinander kommunizieren oder sie stellen Dienste bereit, etwa für den Austausch von Dateien oder das Multimedia-Streaming.

Falls es Probleme im Netzwerk gibt, sind diese nicht einfach zu untersuchen. Nicht immer ist sofort ersichtlich, welche Geräte Dienste anbieten und wie diese zu erreichen sind. Es ist daher hilfreich herauszufinden, was im Netzwerk läuft und wie die Geräte konfiguriert sind.

IP-Adressen, Ports und Protokolle

Jedes Gerät im Netzwerk besitzt eine eindeutige IP-Adresse (siehe Artikel ab Seite 164). Rechner A fordert beispielsweise im lokalen Netz über den Browser eine Webseite von Rechner B an. Der Webserver schickt das Ergebnis an Rechner A beziehungsweise an die IP-Adresse, von der die Anfrage stammt. Bei Internetzugriffen läuft es ähnlich ab. Allerdings sorgt der IP-Filter in der Firewall des Internet/DSL-Routers dafür, dass die IP-Adresse von Rechner A nicht direkt erreichbar ist. Der Router ersetzt per NAT (Network Address Translation) die IP von Rechner A durch die öffentliche IP des Routers, die der Internetanbieter zuweist. Er merkt sich die Herkunft der Anfrage und liefert die Antwort des Webservers an Rechner A im lokalen Netzwerk aus.

```
te@ub2204: ~
te@ub2204:~$ ping4 -c 5 ub220402
PING  (192.168.178.176) 56(84) bytes of data.
64 bytes from ub220402.fritz.box (192.168.178.176): icmp_seq=1 ttl=64 time=0.851 ms
64 bytes from ub220402.fritz.box (192.168.178.176): icmp_seq=2 ttl=64 time=0.697 ms
64 bytes from ub220402.fritz.box (192.168.178.176): icmp_seq=3 ttl=64 time=0.717 ms
64 bytes from ub220402.fritz.box (192.168.178.176): icmp_seq=4 ttl=64 time=0.664 ms
64 bytes from ub220402.fritz.box (192.168.178.176): icmp_seq=5 ttl=64 time=0.747 ms

---  ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 0.664/0.735/0.851/0.063 ms
te@ub2204:~$ ping4 -c 5 ub220402.fritz.box
PING  (192.168.178.176) 56(84) bytes of data.
64 bytes from ub220402.fritz.box (192.168.178.176): icmp_seq=1 ttl=64 time=0.696 ms
64 bytes from ub220402.fritz.box (192.168.178.176): icmp_seq=2 ttl=64 time=0.721 ms
64 bytes from ub220402.fritz.box (192.168.178.176): icmp_seq=3 ttl=64 time=0.866 ms
64 bytes from ub220402.fritz.box (192.168.178.176): icmp_seq=4 ttl=64 time=0.861 ms
64 bytes from ub220402.fritz.box (192.168.178.176): icmp_seq=5 ttl=64 time=0.981 ms

---  ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
```

Namen im Netzwerk: Mit ping4 lässt sich prüfen, ob ein Rechner über seinen Namen und auch über einen lokalen Domainnamen wie „.fritz.box“ oder „.local“ erreichbar ist.

Da man sich IP-Adressen eher schlecht merken kann, kommt im lokalen Netzwerk und Internet die Namensauflösung zum Einsatz. Jedes Gerät besitzt einen Namen, den es bei einer DHCP-Abfrage an den Router übermittelt. Es erhält per DHCP seine eigene IP-Adresse und der Router merkt sich den Namen des Gerätes. Statt der IP-Adresse kann man daher den Gerätenamen verwenden und – abhängig vom Modell des Routers – beispielsweise auch „MeinPC.local“ oder „MeinPC.fritz.box“ (Fritzbox). Im Internet erledigen DNS-Server die Namensauflösung. Die Server wissen, dass etwa zu google.de die IP-Adresse 216.58.212.163 gehört, und intern kommunizieren Router, Browser und Webserver über diese IP-Adresse. Im Terminal lässt sich mit `ping4 -c 5 [Gerätename oder Domain]` herausfinden, ob die Namensauflösung funktioniert.

Der Vollständigkeit halber sei erwähnt, dass jedes Gerät in der Regel zwei IP-Adressen erhält – nach den Standards IPv4 und IPv6. IPv6 ist in lokalen Netzwerken jedoch kaum relevant, weshalb wir hier nicht weiter darauf eingehen.

Ports und Protokolle: Ein Gerät kann mit nur einer IP-Adresse mehrere unterschiedliche Serverdienste anbieten. Der jeweilige Server „lauscht“ an einem bestimmten Netzwerkport und nimmt auf diesem Anfragen entgegen. Eine Auswahl gängiger Ports finden Sie in der Tabelle „Wichtige Ports und Protokolle“. Unter Linux findet man die Portdefinitionen mit Kurznamen und teilweise auch mit näherer Beschreibung in der Datei „/etc/services“.

Die Ports bis einschließlich 1023 kann man unter Linux nur mit root-Rechten konfigurieren und man sollte sich an die Standards halten, um Fehlfunktionen zu vermeiden. Port 80 beispielsweise nutzen Webserver (HTTP), Port 22 SSH-Server. Die Ports von 1024 bis 49151 dürfen Benutzer in der Regel auch ohne besondere Rechte verwenden. 49152 bis 65535 sind als dynamische Ports zur freien Verwendung durch Anwendungen gedacht (zu den Standards siehe *https://www.rfc-editor.org/rfc/rfc6335*).

Neben den Ports spielen zwei Protokolle bei der Datenübertragung eine wichtige Rolle: TCP (Transmission Control Protocol) und UDP (User Datagram Protocol). Diese Protokolle legen fest, wie gültige Datenpakete beim Transport strukturiert sein müssen. TCP verwenden beispielsweise Webserver, E-Mail-Programme und SSH-Server. UDP dient in der Regel zur Übertragung kleiner Datenpakete für DHCP, DNS oder ähnliche Dienste. Die Unterscheidung der beiden Protokolle kann für die Konfiguration von Portfreigaben beziehungsweise einer Firewall wichtig sein.

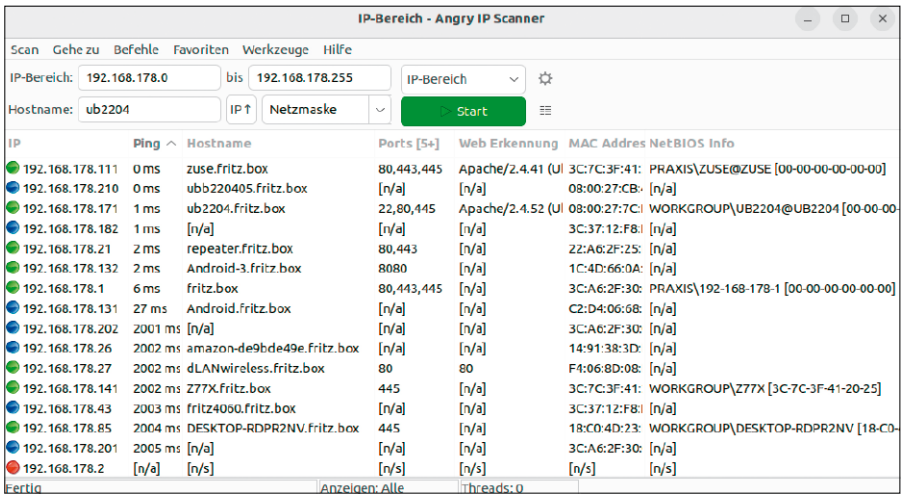
IP-Adressen und Ports

Zuerst ermitteln Sie im Terminal mit

```
ip a
```

den IP-Bereich, den Ihr Netzwerk verwendet (siehe Artikel ab Seite 156). Rufen Sie die Konfigurationsoberfläche des Routers im Browser auf – beispielsweise mit „http://192. 168.178.1“ oder „http://192. 168.0.1“. Bei einer Fritzbox funktioniert auch der Hostname „http://fritz.box“. Router bieten in der Regel eine Funktion, über die sich die aktiven Verbindungen anzeigen lassen. Bei einer Fritzbox gehen Sie auf „Heimnetz → Netzwerk“. Hier sehen Sie allerdings nur die Gerätenamen und IP-Adressen, nicht aber die offenen Ports.

Im Terminal lassen sich die geöffneten Ports mit nmap ermitteln (siehe Artikel ab Seite 164). Wer eine grafische Oberfläche bevorzugt, verwendet Angry IP Scanner (*https://angryip.org*). Im Downloadbereich finden Sie unter „Linux“ DEB-Pakete für Ubuntu und Linux Mint. Im gestarteten Programm geben Sie den IP-Bereich an und gehen auf „Werkzeuge → Einstellungen“. Auf der Registerkarte „Ports“ legen Sie fest, welche Ports das Tool untersuchen soll, beispielsweise „22,80,443,445,8000-8100“. Speichern Sie die Konfiguration per Klick auf „OK“, danach klicken Sie auf „Start“. Klicken Sie auf „Ping“ und dann auf „Sortiere nach Ping“. Die Tabelle zeigt jetzt die aktiven Geräte zuerst an.



IP-Bereich prüfen: Angry IP Scanner ermittelt, welche Geräte im Netzwerk aktiv und welche Ports geöffnet sind. Welche Ports das Tool prüfen soll, lässt sich einstellen.

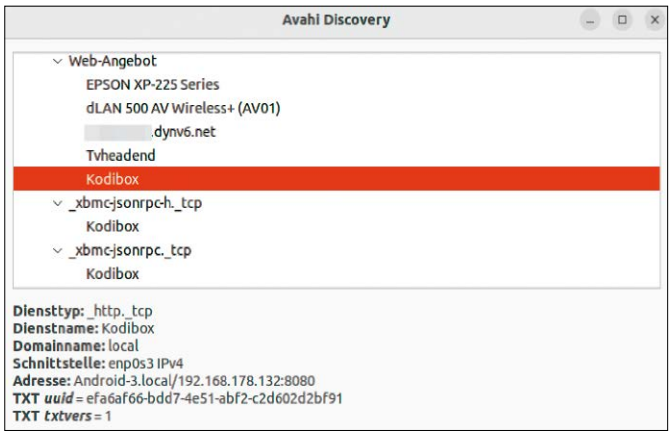
Dienstankündigungen im Netzwerk untersuchen

Nach einigen Diensten muss man im Netz nicht suchen, sie machen sich selbst bekannt. Linux nutzt dafür Avahi, das bei den meisten Distributionen standardmäßig installiert ist. Avahi ist kompatibel mit Bonjour (Mac-OS) und auch unter dem Namen Zeroconf bekannt. Über diese Technik senden Netzwerkdienste und auch viele Geräte wie Drucker, Multimedia-Abspieler, Router und Powerline-Adapter Informationen zur Konfiguration in das Netzwerk.

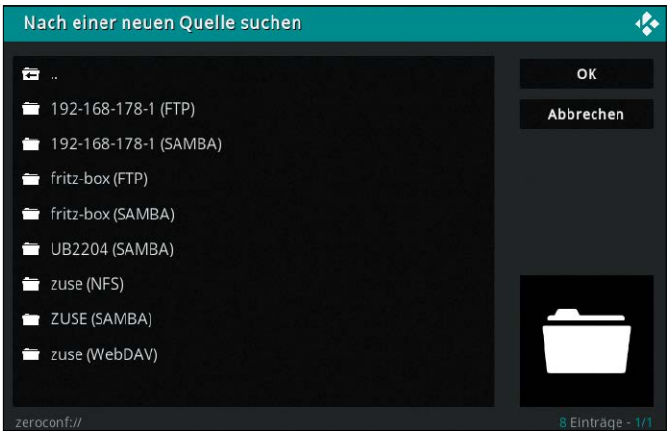
Standardmäßig nutzt Linux Avahi nur rudimentär. Der Ubuntu-Dateimanager beispielsweise zeigt unter „Andere Orte“ Samba-Freigaben anderer Linux-Rechner an. Heimnetzfreigaben (SMB und FTP) einer Fritzbox tauchen ebenfalls auf. Avahi wird außerdem bei der automatischen Erkennung und Konfiguration von Netzwerkdruckern genutzt.

WICHTIGE PORTS UND PROTOKOLLE (AUSWAHL)

Port	TCP	UDP	Beschreibung
7	TCP	UDP	Echo, für Ping-Abfragen
20	TCP	UDP	FTP, Dateitransfer
22	TCP	UDP	SSH, Fernzugriff
23	TCP	–	Telnet, Fernzugriff
25	TCP	–	SMTP, E-Mail senden
80	–	–	HTTP, Webserver
110	TCP	–	POP3, E-Mail empfangen
115	TCP	–	SFTP, Dateitransfer
137–139	TCP	UDP	Microsoft Netbios (für SMB)
143	TCP	UDP	IMAP, E-Mail empfangen
443	TCP	–	HTTPS, Webserver SSL
445	TCP	–	SMB, Dateitransfer
587	TCP	–	SMTP, E-Mail senden
993	TCP	–	IMAPS, E-Mail empfangen SSL
995	TCP	–	POP3S, E-Mail empfangen SSL
5353	–	UDP	Multicast DNS (mDNS, Zeroconf, Bonjour)
8000–8999	TCP	UDP	Alternative HTTP-Ports
49152–65535	TCP (teilweise)	UDP	Dynamische Portbereiche



Einige, aber nicht alle Dienste melden sich hier: Avahi Discover zeigt Server an, die ihr Angebot im Netzwerk bekannt geben. Die Information enthält Name, IP-Adresse und Port des Dienstes.



Medienquellen in Kodi finden: Der „Zeroconf-Browser“ zeigt beispielsweise Samba-, NFS- und FTP-Freigaben an. Für die direkte Einbindung muss aber ein Zugang ohne Anmeldung möglich sein.

Avahi kommt auch bei einigen Anwendungen zum Einsatz. In der Oberfläche des Mediencenters Kodi (Konfiguration siehe *https://www.pcwelt.de/article/1152089*) kann man beim Hinzufügen von Medienquellen auf die Option „Zeroconf-Browser“ gehen und dann den Server wählen. Dabei gibt es jedoch eine Einschränkung. Solcher Zugriff kann nur funktionieren, wenn der betreffende Server keine Anmeldung benötigt. Deshalb ist beispielsweise NFS (Network File System) besonders gut geeignet. Einen Artikel zur Konfiguration eines NFS-Servers finden Sie unter *https://www.pcwelt.de/article/1153455*. Eine FTP-Freigabe etwa von einer Fritzbox gibt man alternativ über „Netzwerkfreigaben hinzufügen“ an. Dabei kann man Benutzernamen und Passwort eintragen.

Avahi-Ankündigungen finden: Eine Übersicht der Server, die sich bei Avahi melden, liefert das nützliche Tool avahi-discover, das Sie über das gleichnamige Paket installieren. Die Baumansicht zeigt die angebotenen Diensttypen und Dienstnamen. Samba-Freigaben sind unter „Microsoft Windows Network“ zu finden und Drucker unter „UNIX Printer“.

Im Abschnitt „Web-Angebot“ sind die Geräte enthalten, die eine Weboberfläche anbieten. Ein Klick auf den Dienstnamen zeigt die Details. Hinter „Adresse“ stehen die IP-Nummer und der Port.

Diese Informationen sind hilfreich, etwa wenn Dienste nicht für den Standard-HTTP-Port 80 konfiguriert sind. Vollständig ist die Liste jedoch nicht. Eine Fritzbox beispielsweise gibt ihre Konfigurationsoberfläche nicht über Avahi bekannt.

Avahi für weitere Dienste nutzen

Avahi wird automatisch für Samba-Freigaben verwendet, wenn der Samba-Server installiert ist. Eine zusätzliche Konfiguration ist nicht erforderlich. Für die Netzwerkprotokolle NFS, Webdav oder SFTP kann man Konfigurationsdateien im Ordner „/etc/avahi/services“ ablegen. Eine Beispieldatei „sftp-ssh.service“ für SFTP/SSH finden Sie im Ordner „/usr/share/doc/avahi-daemon/examples“ und eine Konfigurationsdatei für NFS können Sie über *https://m6u.de/AVAS* abrufen. Sobald Sie die Datei speichern, taucht auf anderen Linux-PCs im Dateimanager unter „Andere Orte“ (Ubuntu) oder „Netzwerk“ (Linux Mint) ein neuer Eintrag auf, beispielsweise „[Rechnername] (SSH/SFTP)“.

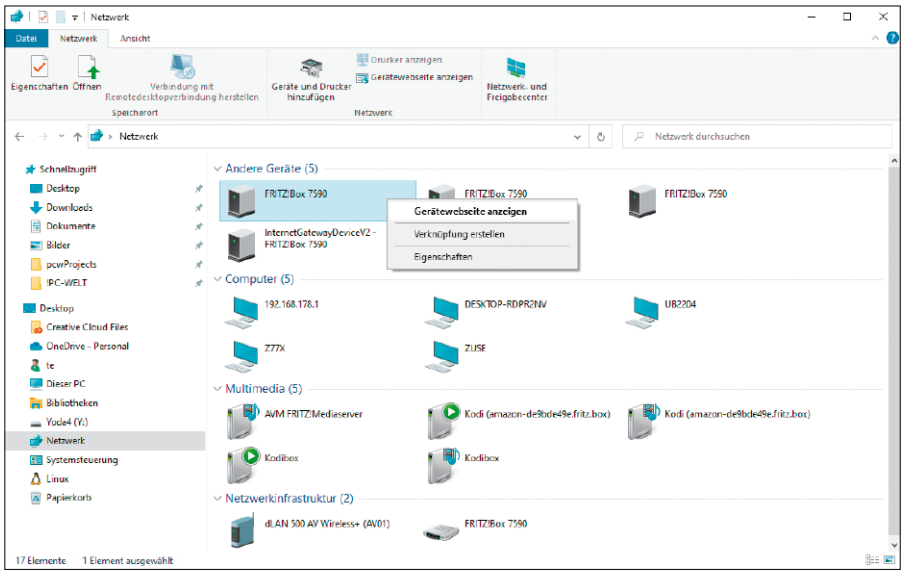
Die Sichtbarkeit von Samba-Freigaben

Windows verwendet für die Suche nach Netzwerkressourcen WS-Discovery (Web Services Dynamic Discovery) statt Avahi. Der Windows-Explorer zeigt unter „Netzwerk“ Dateifreigaben, Drucker, Geräte mit Weboberflächen oder Multimedia-Geräte an. Samba-Freigaben fehlen, weil Linux WS-Discovery bisher standardmäßig nicht unterstützt. Durch manuelle Eingaben gelingt der Zugriff unter beiden Systemen trotzdem (siehe Artikel ab Seite 160).

Komfortabler ist es jedoch, WS-Discovery in Linux nachzurüsten. Ab Ubuntu 22.04 oder Linux Mint 21 lässt sich der Dienst mit

```
sudo apt install wsdd
```

installieren.



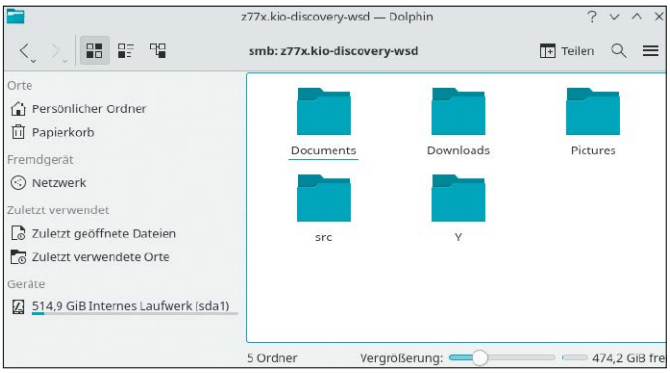
Gesprächigeres Windows: Der Windows-Explorer zeigt fast den gesamten Gerätepark im Netzwerk an. Über das Kontextmenü gelangt man – wenn vorhanden – zur Gerätewebseite.

Nutzer älterer Systeme installieren wsdd manuell (*https://github.com/christgau/wsdd*). Der Dienst wird automatisch gestartet und dann tauchen Linux-Freigaben sofort im Windows-Explorer auf.

Hinweis: Es gibt einen ähnlichen Dienst mit dem Namen wsdd2, der sich aber nur für das smb3-Server-Modul eignet, das seit Kernel 5.15 verfügbar ist. Mehr Infos dazu finden Sie über *https://m6u.de/BMKE*.

Windows-Freigaben unter Linux sehen: Es gibt erste Ansätze, zumindest die KDE-Oberfläche mit WS-Discovery bekannt zu machen. Die nötige Erweiterung für den KDE-Dateimanager Dolphin ist in Kubuntu 22.04 und 22.10 enthalten, funktioniert jedoch sehr unzuverlässig. Besser sieht es bei KDE Neon aus (*https://neon.kde.org*), das zwar auf Ubuntu 22.04 basiert, aber eine neuere KDE-Version mitbringt. In Dolphin klickt man auf „Freigegebene Ordner (SMB)" und sieht alle Windows- und Linux-Rechner mit SMB-Freigaben. Beim Klick auf eine Windows-Freigabe verwendet der Dateimanager den Pfad „smb://[Server].kio-discovery-wsd/" und die freigegebenen Ordner erscheinen. Es ist bisher nicht bekannt, wann diese Funktion in die Dateimanager von Gnome oder Cinnamon eingebaut wird.

Tipp: Damit Dolphin auch Netzwerkressourcen wie FTP-, SFTP- oder NFS-Server anzeigt, installieren Sie das Paket „kde-zeroconf". Sie erreichen die Dienste dann im Dateimanager per Klick auf „Netzwerkdienste".



Windows-Freigaben in Dolphin: Die neueste Version des KDE-Dateimanagers beherrscht WS-Discovery und kann daher Windows-Server und deren Freigaben anzeigen.

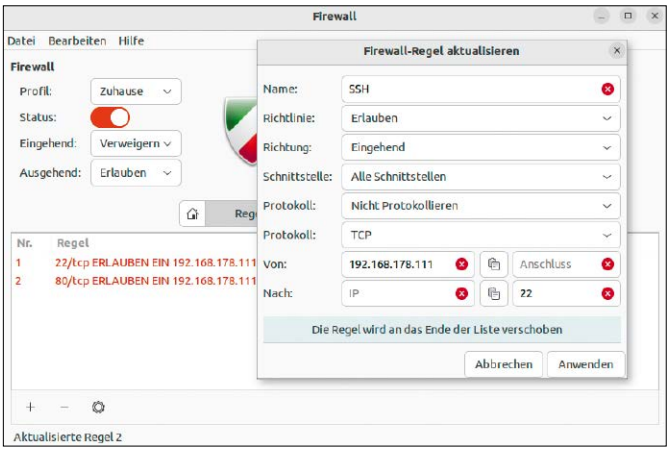
Schutz durch die Firewall konfigurieren

Bei Ubuntu und Linux Mint ist die Firewallsoftware ufw standardmäßig installiert, allerdings nicht aktiv. Im privaten Netzwerk ist eine Firewall in der Tat überflüssig, weil der Internetrouter die Geräte im Netzwerk bereits vor Zugriffen aus dem Internet schützt. Ein Motiv, die Firewall trotzdem zu aktivieren, ist die potenzielle Gefährdung durch andere Rechner im Netzwerk – insbesondere, wenn diese unter Windows laufen. Auf einem Notebook, das man auch in fremden Netzen verwendet, sollte man die Firewall daher aktivieren. Das gilt jedoch nur, wenn Serverdienste auf dem Rechner laufen. Andernfalls sind keine Ports geöffnet und ein Angriff ist unmöglich. Eine Firewall bietet jedoch keinen Schutz vor böswilligen Websites oder virenverseuchten Downloads. Davon sind Linux-Systeme aber weit weniger betroffen als Windows.

Firewall mit Profilen: Eine aktivierte Firewall birgt immer die Gefahr, dass der Zugriff auf Dienste ungewollt verhindert wird. Die ufw-Konfiguration ist jedoch recht übersichtlich und bei Problemen kann man die Firewall jederzeit wieder ausschalten. Für die komfortable Konfiguration installieren Sie das Tool gufw („Firewall-Konfiguration") über das gleichnamige Paket. Es bietet die drei Profile „Büro", „Öffentlich" und „Zuhause", zwischen denen Sie je nach Aufenthaltsort umschalten. Wenn Sie „Büro" oder „Öffentlich" wählen, wird die Firewall aktiviert, was an der Stellung des Schalters hinter „Status" zu erkennen ist. Die Einstellung bleibt auch nach einem Neustart erhalten. Bei aktivierter Firewall werden die Zugriffe auf alle Ports blockiert. Der Unterschied zwischen diesen beiden Profilen ist die Einstellung hinter „Eingehend". „Ablehnen" bei „Öffentlich" verweigert den Zugriff ohne Rückmeldung an das aufrufende Programm. Es scheint dann so, als ob beispielsweise kein Webserver läuft, und die Verbindung wird sofort abgebrochen. „Verweigern" hat eine ähnliche Wirkung, informiert den Client aber darüber, dass keine Verbindung möglich ist. In der Praxis führt das dazu, dass etwa ein Webbrowser länger benötigt, bis er Verbindungsversuche wegen Zeitüberschreitung abbricht.

Spezialkonfiguration für das Heimnetz: Im heimischen Netzwerk setzen Sie das Profil auf „Zuhause". Die Firewall wird deaktiviert und Netzwerkgeräte können auf alle Serverdienste zugreifen. Wer eine erhöhte Sicherheit benötigt, kann die Firewall auch im Heimnetz aktivieren und beispielsweise den Zugriff auf den SSH-Server auf bestimmte IP-Adressen beschränken. Klicken Sie auf die „+"-Schaltfläche und gehen Sie auf „Erweitert". Tragen Sie einen Namen ein, beispielsweise „SSH". Hinter „Protokoll:" wählen Sie „TCP" und hinter „Von:" geben Sie die IP-Adresse des berechtigten Rechners ein. Die Portnummer dahinter lassen Sie leer. In die Zeile „Nach:" tragen Sie keine IP-Adresse, aber den Port „22" ein und per Klick auf „Anwenden" fügen Sie die Regel hinzu.

Entsprechend definieren Sie weitere Portregeln für diese oder andere IP-Adressen. Bitte beachten Sie, dass die Firewall erst einmal alle eingehenden Anfragen blockiert. Sie müssen daher für jeden Port eine Regel erstellen, den der PC im Netzwerk anbieten soll. ■



Extremschutz: In der Firewall lässt sich für das lokale Netzwerk konfigurieren, dass beispielsweise nur einer einzigen IP-Adresse der Zugang zu einem SSH-Server erlaubt ist.

Netzwerkhardware: Ausbau & Optimierung

Für Heimnetze genügt es oft, die Fähigkeiten des Routers konsequent zu nutzen und die Endgeräte an optimaler Stelle zu betreiben – verkabelt oder via Funknetz. Letzteres geht nicht? Auch kein Problem: Ethernet und WLAN lassen sich verlängern.

VON HERMANN APFELBÖCK



Dieser Beitrag zeigt den Umgang mit der wichtigsten Netzwerkhardware und Optionen des Netzwerkausbaus. Dabei geht es ausschließlich um das lokale Netz in den eigenen vier Wänden mit seinen typischen Geräten. Ein Großteil dieser Infos gilt betriebssystemunabhängig: Für Router, Switch, Access Point, Repeater, Powerline spielt das System der Endgeräts keine Rolle.

Der Heimrouter

Moderne Router vereinen eine Reihe von Hardwarefunktionen – Switch für (meist) vier Ethernet-Anschlüsse, Funknetz, DECT-Telefonie, NAS, Verbindung zum öffentlichen WAN. Alle Funktionen lassen sich in der Konfigurationsoberfläche über jeden Browser steuern. Hardwaretechnisch unerlässlich ist

- das Aktivieren und Einrichten des Funknetzes (Fritzbox: „WLAN → Funknetz“, Passwort unter „WLAN → Sicherheit“)
- das Festlegen der Ethernet-Leistung (Fritzbox: „Heimnetz → Heimnetzübersicht → Netzwerkeinstellungen“).

Router wie die Fritzbox sind im Browser über Standard-Hostnamen wie „fritz.box“ erreichbar, in jedem Fall aber mit der lokalen IP-Adresse. Die IP lautet oft „192.168.178.1“ oder „192.168.0.1“. Die Router-IP ermitteln Sie bei Bedarf mit

```
ip a
```

und ersetzen im letzten Block der IPv4-Adresse die angezeigte Ziffer (die IP des aktuellen Geräts) durch die „1“.

Um im allerersten Schritt an die Konfigurationsoberfläche heranzukommen, muss ein Gerät im Netz angemeldet sein. Dazu genügt ein mit Ethernet-Kabel verbundener PC mit einem beliebigen Betriebssystem.

Aufgrund der zentralen Rolle wäre es optimal, wenn der Router auch einen zentralen Standort einnimmt. Je mehr Geräte Sie an den vier Ethernet-Ports in unmittelbarer Nähe nutzen können, desto besser. Das gilt ganz besonders für Geräte, die viel Datentransfer zu leisten haben, etwa Highspeed-Downloads oder Backups. Geräte mit Serverfunktion sind ebenfalls für schnelle Kabelverbindung prädestiniert, NAS bieten in der Regel gar kein Funknetz. Die oft unbefriedigende Netztauglichkeit von TV-Geräten lässt durch HDMI-Anschluss eines PCs oder eines Raspberry Pi vollständig kompensieren, der wiederum per Ethernet am Router hängt.

Für die optimale Reichweite des Funknetzes wäre eine zentrale Lage ebenfalls wünschenswert. Tatsache ist aber, dass Router oft ungünstig stehen, erzwungen durch die Nähe zum DSL- oder Kabelanschluss.

Ethernet: Das Kabelnetzwerk

Kabelgebundene Ethernet-Verbindungen sind schnell und unbeeinflusst von äußeren Störungen. PCs, Notebooks und Smart-TVs sind standardmäßig mit einer RJ-45-Buchse für Ethernet-Kabel ausgerüstet – in der Regel ein Gigabit-Ethernet-Adapter. Über Gigabit-Ethernet (1000 MBit/s) lassen sich theoretisch 125 MB/s übertragen. Nach Abzug der Verwaltungsdaten sollten rund 100 MB/s bleiben. Wenn das Tempo nicht erreicht wird, muss das aber nicht am Netzwerk liegen: Mechanische Festplatten,



Viele Ethernet-Ports für volles Tempo: Alle Endgeräte am Switch unterhalten sich unabhängig von der sonstigen Netzleistung mit Gigabit-Tempo.



10-GB-Netzadapter gibt es für PCIe-Ports oder Thunderbolt, 10-GB-Switches mit Ports bis zu 10 GBit/s. Für Heimnetze ist das noch kaum praktikabel, weil die Datenträger zu langsam sind.

insbesondere an USB, können das Netztempo ausbremsen, vor allem wenn viele kleine Dateien zu übertragen sind.

Fast Ethernet (100 MBit/s) ist obsolet, zumal es heutzutage sogar die WAN-Bandbreite aus dem Internet unterschreiten kann. Router und Switches mit Fast Ethernet sollten ersetzt werden. Ältere Rechner ohne Serveraufgaben können mit dem langsamen 100-MBit-Adapter aber natürlich weiterhin mitspielen.

Kabelausbau: Ein Ausbau der Ethernet-Verkabelung über den zentralen Router hinaus ist kostengünstig, aber aufwendig. Für Gigabit-Ethernet sind Cat-5e-Kabel zu empfehlen, die aber oft irreführend als „Cat 5" bezeichnet werden. Wer zukunftssichere Kabel verlegen möchten, greift zu Cat-6- oder Cat-7-Kabeln. Um Kabel in weitere Räume zu bringen, genügen 8-mm-Bohrer. Den weiteren Aufwand beim Abisolieren der Kabel und Crimpen der RJ-45-Stecker kann man sich dadurch ersparen, dass man Stecker wie Telegärtner J00026A2001 (*http://amzn.to/2pRA2jo*, circa 13 Euro) verwendet, die sich werkzeuglos an das Cat-Kabel anschließen lassen. Ohne Bastelei geht es aber auch hier nicht. Außerdem sind die Stecker etwas größer und finden in einem Switch nicht direkt nebeneinander Platz.

Ein für Privathaushalte relevantes Längenlimit für Ethernetkabel gibt es nicht: Bis zu 100 Meter bleiben verlustfrei, für noch längere Strecken müsste dann ein zwischengeschalteter Switch das Signal auffrischen.

Switch: Ethernet-Switches sind intelligenter Verteiler, die Datenpakete nur an das Gerät leiten, für das sie bestimmt sind. Externe Gigabit-Switches etwa von Netgear ermöglichen daher Gigabit-Tempo zwischen den direkt angeschlossenen Geräten. Dabei spielt es keine Rolle, mit welchem Tempo die Daten vom Router zum Switch gelangen. In einem Raum mit eventuell mäßiger WLAN- oder Powerline-Abdeckung kommunizieren dann immerhin alle Endgeräte hinter dem Switch mit Gigabit-Tempo. Kleinere Switches haben meistens fünf oder acht Ports und kosten etwa 25 bis 40 Euro. An welchen Port Sie welches Gerät anschließen, spielt keine Rolle.

10-GBit-Netzwerk: Gigabit-Ethernet dürfte im Heimnetz noch viele Jahre Standard bleiben, wenngleich längst 10 GBit/s verfügbar ist. Das liegt nicht nur daran, dass eine PCIe-Karte wie Asus 10Gbase-T XG-C100C aktuell knapp 100 Euro kostet. Entscheidender sind die notwendigen Aufrüstmaßnahmen mit erheblichen Folgekosten. Mit Festplatten und SSDs an SATA-Ports, USB 3.0/3.1 ist nämlich keine Verbesserung zu erzielen. Alle beteiligten Endgeräte müssten PCIe-SSDs, USB 3.2 oder Thunderbolt 3 verwenden, um vom 10-GBit-Netzwerk zu profitieren.

BREITBANDHARDWARE INS WAN

Auf die Hardware, die Ihr Internetprovider bereitstellt, haben Sie nur insofern Einfluss, als Sie im besten Fall zwischen verfügbaren Techniken und Breitbandverträgen das Geeignete auswählen. Ob tatsächlich eine offene Auswahl besteht zwischen einem DSL mit sechs bis 16 MBit/s, VDSL mit 100 bis 250 MBit/s, Kabel mit 100 bis 1000 MBit/s oder Glasfaser mit derzeit 300 bis 1000 MBit/s, ist regional höchst unterschiedlich. Während Telekom & Co. derzeit in Großstadtregionen (wo Kunden mit VDSL oder Kabel und 100- bis 500-MBit-Verbindungen null Leidensdruck haben) mit Glasfaserangeboten hausieren, bleiben die Kunden am Land auf Sechs-MBit-DSL sitzen.

Wie viel MBit/s braucht man wofür? Die Breitbandwährung MBit/s ist eine unhandliche Größe, die Sie am besten grob durch zehn teilen, um den MB-Durchsatz zu schätzen: Mit sechs MBit/s, also weniger als ein MB pro Sekunde, funktionieren Mail, soziale Netzwerke und HTML-Surfen in leidlicher Geschwindigkeit. 16 MBit/s ermöglichen Surfen, Softwaredownloads und Videostreaming mit erheblichen Qualitätsabstrichen. Ab 50 MBit/s sind auch größere Downloads wie Linux-ISO-Images keine Geduldsprobe und Streamen hoher Qualität wird störungsfrei. 100 MBit/s, also 10 bis 12 MB pro Sekunde, sollten auch Intensivnutzern und Downloadjunkies genügen, wobei dies mit den Personen im Haushalt oder Betrieb zu multiplizieren ist: Für mehrere Intensivnutzer in einem Haushalt sind 250- oder 500-MBit-Verträge nicht mehr abwegig.

Diese Anmerkungen zur Breitbandverbindung ins öffentliche WAN (Wide Area Network) sind auch für das lokale LAN (Local Area Network) und dessen Ausbau relevant. Je größer die Bandbreite aus dem Internet, desto wichtiger wird ein schnelles lokales Netz: Nichts ist ärgerlicher als eine 500-MBit-Verbindung ins Internet, von der am Endgerät nur ein Bruchteil ankommt, weil das lokale Netz schwächelt. Gründe für ein schnelles Heimnetz gibt es aber natürlich in Menge auch bei dünner DSL-Verbindung nach draußen: Das Backup vom PC zum NAS oder Platinenserver soll möglichst schnell durchlaufen, das Tablet soll Filme vom lokalen Server störungslos wiedergeben und die Remotedesktop-Verbindung ist am angenehmsten mit 32-Bit-Farben.



Powerline-Adapter: Diese Methode der Netzerweiterung ist solide, aber selten der versprochene Ferrari. Die „Pass-Thru"-Steckdose sorgt dafür, dass kein Stromanschluss verloren geht.

Powerline: Die Ethernet-Brücke

Wo direkte Verkabelung zu mühsam erscheint, ist eine Brücke über das Stromnetz eine echte Alternative. Powerline (auch Power LAN oder DLAN) ist eine Kabelvernetzung, die für die Hauptdistanz die Stromleitung nutzt, die kurzen Restwege übernehmen dann wieder Ethernet-Kabel. Für die angeschlossenen Endgeräte – egal ob Linux, Windows oder Mac-OS – handelt es sich um eine Ethernet-Verbindung. Die Adapter haben mindestens einen und bis zu drei Ethernet-Anschlüsse (es gibt auch Modelle mit zusätzlichem WLAN).

Im Handel finden Sie Adapter von AVM, Devolo oder Netgear. Abgesehen von der jüngeren Magic-Generation bei Devolo entsprechen die Adapter dem Homeplug-Standard: Sie funktionieren also auch mit älteren Homeplug-Adaptern. Geräte mit unterschiedlicher Übertragungsleistung lassen sich kombinieren, erreichen dann aber natürlich nur die Bandbreite des schwächsten Glieds.

Powerline benötigt mindestens zwei Adapter. Starterkits mit zwei Geräten kosten je nach Leistung etwa 100 bis 200 Euro. Ein Adapter kommt in eine Steckdose in der Nähe des Routers und wird per Ethernet-Kabel mit diesem verbunden. Den zweiten (dritten …) Adapter bringen Sie in der Nähe des Endgerätes unter und verbinden ihn über ein Ethernet-Kabel mit PC oder Notebook.

Vor der Erstbenutzung verbinden sich die zwei Adapter durch Drücken des Verschlüsselungsknopfes am Gehäuse, ein späterer Ausbau ist beim Hersteller Devolo auch durch die Cockpit-Software und manuelle Eingabe der Geräte-ID möglich.



Software für Devolo-Powerline: Das Tool ist ganz nützlich, da es Adapter ein- und ausschalten kann. Außerdem führt es zur Konfigurationsoberfläche des Geräts – falls eine existiert.

Powerline: Optimierungen

Powerline-Verbindungen sind sicher und relativ schnell – in der Regel jedem WLAN-Ausbau überlegen. Sie erreichen aber nicht annähernd den theoretischen Durchsatz von 500, 1200 oder gar 2400 MBit/s (Devolo Magic). Im Bestfall und bei kürzeren Distanzen erreichen die Adapter 40 Prozent der theoretischen Bruttoleistung, in ungünstigen Fällen aber auch nur 20 Prozent. Die von Herstellern angegebene Maximaldistanz von 300 Metern ist pure Theorie: Brauchbare Leistungen sind nur bei kurzen Strecken zu erwarten (10 bis 50 Meter).

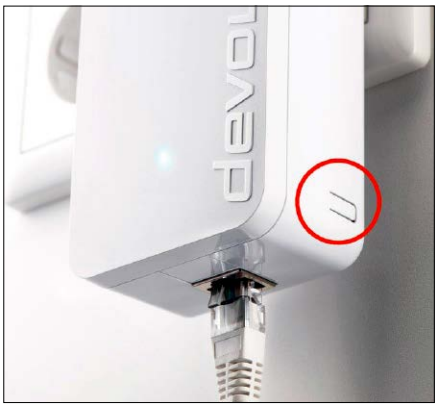
Neben der Distanz der Adapter und der Qualität der Stromleitung können andere Stromverbraucher im Haushalt den Durchsatz beeinträchtigen. Auch die Wahl der Steckdose ist kritisch: Im gleichen Raum können unterschiedliche Steckdosen Unterschiede bis zu 300 Prozent erzielen!

Die Adapter sollten immer direkt in die Wandsteckdose und niemals in Steckerleiste. Immer zu empfehlen sind daher die etwas teureren Adapter mit integrierter Steckdose („Pass-Thru"): Die Steckdose kann dann für andere Stromverbraucher oder für eine Steckerleiste genutzt werden. Ganz sorgenfrei ist das dennoch nicht, denn damit erschweren Sie sich die ganz einfache Troubleshooting-Maßnahme, einen DLAN-Adapter ein- und wieder auszustecken, falls dieser mal rot blinkt und die Arbeit verweigert.

Mit der Software Devolo Cockpit (*www.devolo.de/service/downloads*, auch für Linux) lassen sich Devolo-Adapter konfigurieren und ein- und ausschalten, was in Problemfällen die Störung fast immer behebt. Für den eigentlichen Betrieb der Adapter ist die Software nicht erforderlich.

WLAN: Das Funknetzwerk

Wireless LAN ist eine bequeme und kostengünstige Vernetzungstechnik – keine Kabel, geringer Arbeitsaufwand und alle Netzwerkgeräte bleiben mobil. Ein WLAN-Access-Point ist bereits im Router enthalten. Das Funknetz muss also nur aktiviert und mit Kennwort versehen werden. Notebooks, Tablets und Smartphones besitzen standardmäßig einen WLAN-Chip, PCs können am USB-Port nachgerüstet werden.



Powerline-Adapter einrichten: Durch zeitnahes Drücken der Verschlüsselungstaste am Gehäuse zweier Devolo-Adapter verbinden sich die Geräte.

WLAN-Geräte werden mit hohen Transferraten beworben. Beim derzeit noch meistverbreiteten Standard 802.11ac (Wi-Fi 5) gelten 1300 MBit/s als theoretisches Maximum, bei 802.11ax (Wi-Fi 6) sogar 9600 MBit/s. Reichweite und Geschwindigkeit einen WLANs hängen aber erheblich von Distanz, baulichen Gegebenheiten und weiteren Störeinflüssen ab. Bei Stahlbetonwänden und Ziegelmauern mit Feuchtigkeit reicht das Signal eventuell kaum in den nächsten Raum. Viele Funknetze der Nachbarschaft und andere elektrische Geräte verschlechtern die Signalqualität zusätzlich. Wenn das Funksignal für wichtige Räume nicht ausreicht, sind die typischen Optimierungstipps selten zielführend: Optimale Frequenz- und Kanalwahl erledigen moderne Router mit automatischen Einstellungen und ein Ortwechsel des Router scheitert in der Regel an den Gegebenheiten. Ohne zusätzliche Hardware sind



Repeater holen das Funknetz ein Stück näher an den Arbeitsplatz. Erwartungsgemäß reibungslos verstehen sich Fritz-Repeater mit Fritzbox-Routern.



Powerline-Wi-Fi-Adapter liefern das WLAN an jede Steckdose und jeden Ort (Basisadapter am Router vorausgesetzt). Klassische Access Points sind meistens noch leistungsstärker.



Access Point und seine Konfigurationsoberfläche: Ethernet-Kabel in die Buchse und in der Konfiguration ein neues WLAN anlegen – schon funkt das Gerät an gewünschter Stelle.

WLAN-Reichweitenprobleme nicht nachhaltig zu beheben (siehe unten). Im Zweifel über WLAN-Signalstärken gibt es diverse objektive Testmöglichkeiten. Fritzbox-Besitzer greifen am besten zur Android- und iOS-App „Fritz!App WLAN“.

WLAN-Optimierungen

WLAN-Repeater sind Signalverstärker der WLAN-Basisstation. Sie sollten in eine Wandsteckdose angesteckt werden, wo das Signal der Basisstation noch einigermaßen zu empfangen ist. Die Mitte zwischen Basisstation und Endgerät ist ein oft genannter Pauschaltipp, ein Platz nahe am Endgerät kann aber durchaus bessere Resultate liefern. Die Ersteinrichtung erfolgt entweder über die WPS-Taste an Router und Repeater oder manuell über die Repeater-IP-Adresse (die im Router zu ermitteln ist).

Ein Repeater kann den Datendurchsatz durchaus verdoppeln. Die unterschiedlichen Preise zwischen 30 und 120 Euro rechtfertigen sich durch theoretische Sendeleistungen von 300 bis 1700 MBit/s, durch Dualband-Fähigkeit (2,4 und fünf GHz) und Funktionen wie zusätzliche Ethernet-Anschlüsse. Da Repeater aber eher eine Notlösung bleiben, sind hochpreisige Repeater aber selten sinnvoll.

Powerline-Wi-Fi-Adapter: Powerline-Adapter können auch das Funknetz ausbauen, indem der entfernte Adapter (bei den Endgeräten) per Wi-Fi weiterfunkt. Devolo, AVM und andere bieten Powerline-Starterkits mit Basisadapter und Wi-Fi-Adapter ab etwa 90 Euro. Wenn bereits eine Powerline-Basis vorliegt, gibt es Wi-Fi-Erweiterungsadapter auch solo für etwa 50 Euro. Im Prinzip sind solche Lösungen nichts anderes als Access Points mit vergleichbaren Funktionen (Gastnetz, Kindersicherung, Zeitschaltung), die sich über eine Konfigurationsoberfläche steuern lassen.

Access Point: Wenn das Funknetz einen wichtigen Raum nicht abdeckt, dort aber Ethernet-Kabel oder Powerline vorliegt, kann ein Access Point die Mobilgeräte an dieser Stelle versorgen. Das Gerät muss im Prinzip nur mit einem Ethernet-Kabel verbunden werden. Detaillierte Einstellungen erlaubt eine Konfigurationsoberfläche für den Browser, notwendig sind nur Funknetzname (SSID) und Kennwort. Access Points sind in der Regel die schnelleren Geräte gegenüber Repeater und Powerline-Wi-Fi. Die deutlichen Preisunterschiede von 25 bis 150 Euro rechtfertigen sich durch die Wi-Fi-Version, wobei aber günstige Geräte mit Wi-Fi 5 (802.11ac) für einen Raum ausreichen können.

Oft genügt auch ein alter Router für diese Rolle, nachdem dort die Rolle als DHCP-Server (Verteilung von IP-Adressen) deaktiviert ist und auch sonst am besten alles außer WLAN. Im Übrigen verfahren Sie wie bei einem Access Point, definieren also SSID und Zugangskennwort.

Netzwerkadapter am Endgerät

Smartphone, Tablets und Notebooks besitzen standardmäßig einen WLAN-Chip, bei PCs und NAS-Geräten ist ein Gigabit-Ethernet-Port Standard. Wenn ein Netzadapter fehlt (eventuell auch ein zweiter für ein zweites Netzwerk), ist PCs, Notebooks, NAS- und Platinenrechnern leicht abzuhelfen. Fehlendes Ethernet können Ethernet-Adapter am USB-Port ergänzen. Das Zubehör sollte wie der Delock USB-Ethernet-Adapter (Delock 62121, ab 30 Euro, *https://tinyurl.com/25mzrwtu*) USB 3.x und Gigabit-Ethernet leisten. Billigere USB-Adapter bieten oft nur Fast Ethernet und/oder USB 2.0.

Ein fehlender WLAN-Chip bei PCs ist ebenfalls über USB zu kompensieren. Preisgünstige WLAN-Sticks für 10 bis 20 Euro gibt es zuhauf, sie sind aber nicht alle Linux-kompatibel. Daher sollte vor einem Kauf die Übersicht auf *https://wiki.ubuntuusers.de/WLAN/Karten* befragt werden. Die Infos zeigen, dass Linux die allermeisten Adapter der Anbieter Asus, AVM, D-Link, TP-Link unterstützt. ■



Ethernet via USB: Für unzureichend ausgestattete Notebooks ist dies eine nützliche Ergänzung (Delock 62121, circa 30 Euro für USB 3.x und Gigabit-Ethernet).



WLAN-Stick für USB-Port: PCs ohne Funkchip bekommen Sie für 20 bis 40 Euro mit einem USB-WLAN-Stick ins Funknetz.

Serverdienste für den Datenaustausch

Das Netzwerk hat zwei Aufgaben: Zum einen soll es jedes Endgerät ins Internet bringen, zum anderen die Endgeräte untereinander verbinden. Nur um den zweiten Aspekt wird es hier gehen, und dieser Aspekt ist der kompliziertere und kreativere.

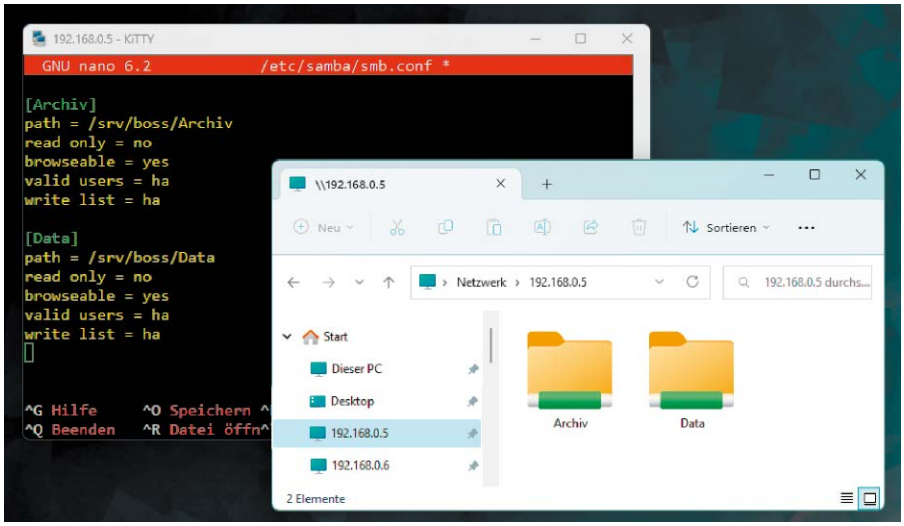
VON HERMANN APFELBÖCK

Verantwortlich für einen schnellen Internetzugang sind der Breitbandvertrag und die Hardware (siehe dazu ab Seite 156). Softwaretechnisch ist da wenig Spielraum. Im lokalen LAN sieht das ganz anders aus: Die Endgeräte können auf verschiedenen Wegen miteinander sprechen, um Daten, Medien, Software auszutauschen und verschiedene Rollen zu übernehmen. Voraussetzung ist in jedem, auch im einfachsten Fall, ein Serverdienst, der auf die Netzwerkanfragen anderer Endgeräte wartet. Dieser Beitrag erklärt die wichtigsten Serverdienste für ein typisches heterogenes Heimnetz mit Linux, Windows, Android, iOS, TV-Gerät als beteiligte Clients am Endgerät, mit Linux und Windows als potenzielle Server.

Serverdienste erfordern im Prinzip keine Investitionen in Extrahardware. Jeder Linux- oder Windows-Rechner, der ständig läuft, kann solche Dienste nebenbei übernehmen. Auch ein Router wie die Fritzbox kann für geringere Ansprüche genügen. Wer eine von sonstigen Aufgaben unabhängige Hardware im Dauerbetrieb bevorzugt, ist mit einem Raspberry Pi 4 oder einem ausgemusterten Notebook kostengünstig und gut beraten.

Windows- und Samba-Freigaben

Windows- und Samba-Freigaben sind die gebräuchlichste Methode für Datenzentralen im Netzwerk, da sie für jedes Gerät mit jedem Betriebssystem zu erreichen sind. Als Datenserver kommen PCs und Barebones mit Windows, PCs und Platinenrechner mit Linux (auch Router wie die Fritzbox) in Frage.



Linux-Samba dient in erster Linie Windows. Alle anderen Betriebssysteme, auch iOS und Android, sind mit SSH/SFTP-Diensten einfacher und funktionsreicher versorgt.

Server (1) Windows: Unter Windows ist die Serverkomponente Standard, die Freigabe für einen im Explorer markierten Ordner daher ohne Vorbereitung möglich. Aufmerksamkeit erfordert lediglich die Tatsache, dass das vereinfachende Windows-Konzept der „Heimnetzgruppe" nicht Linux/Android/Apple-kompatibel ist. Für Freigaben im gemischten Netzwerk muss daher im Explorer unter „Optionen → Ansicht" der „Freigabe-Assistent" abgeschaltet werden. Danach erfolgen Freigaben mit der Explorer-Kontextoption „Zugriff gewähren auf → Erweiterte Freigabe → Diesen Ordner freigeben". Danach kann über „Berechtigungen" im großzügigsten Fall „Jeder" den „Vollzugriff" erhalten. „Jeder" heißt nicht wirklich „Jeder", sondern nur „Jeder", der auf dem Windows-System ein Konto besitzt. Zugreifende Clients müssen sich folglich mit einem Systemkonto (des Windows-Servers) und Kennwort ausweisen. Zugriffsprobleme sind – genau wie bei Linux-Samba-Freigaben – selten netzwerkbedingt, sondern meistens auf mangelnde Dateirechte zurückzuführen. Das Windows-Konto, das über das Netzwerk zugreifen will, muss die nötigen lokalen Dateirechte besitzen. Diese können am Windows-System bei Bedarf über „Eigenschaften → Sicherheit" für den freigegebenen Ordner korrigiert werden.

Server (2) Linux: Auf Linux-Desktopsystemen ist die Samba-Serverkomponente selten vorinstalliert. Das ist mit aber

```
sudo apt install samba
```

schnell nachzuholen. Die Einrichtung des Samba-Servers kann dann einfach oder komplex ausfallen, je nach Benutzermenge und Freigabeort. Einfache und gut kombinierbare Varianten sind die Freigaben

• aller Home-Verzeichnisse
• eines bestimmten Datenordners für ein bestimmtes Konto.

Für den ersten Fall genügt das Freischalten der Zeile

```
;[homes]
```

und der nachfolgenden fünf Zeilen in der Konfigurationsdatei „/etc/samba/smb.conf“, indem jeweils das Semikolon entfernt wird. Dies ermöglicht allen Nutzern einen persönlichen und gegeneinander abgeschirmten Datenbereich auf dem Server. Beachten Sie dabei, dass die Home-Verzeichnisse in der Regel auf der Systempartition liegen, die für solche Freigabe ausreichend Platz bieten muss.

Für die Freigabe einer allgemeinen Daten- und Mediensammlung ist es rechtetechnisch am einfachsten, den betreffenden Pfad für ein einziges Pseudokonto freizugeben, das dann alle verwenden. Für diesen Fall müsste nur folgender Beispieleintrag ans Ende der Datei „smb.conf“:

```
[Archiv]
path = /srv/Archiv
writeable = no
valid users = archiv
write list = archiv
```

Das erlaubte Zugriffskonto (hier nur mit Leserecht) lautet hier also „Archiv“. Zugriffskonten müssen immer doppelt existieren – als Systemkonto und als Samba-Konto. Für das „Archiv“-Beispiel muss also mit

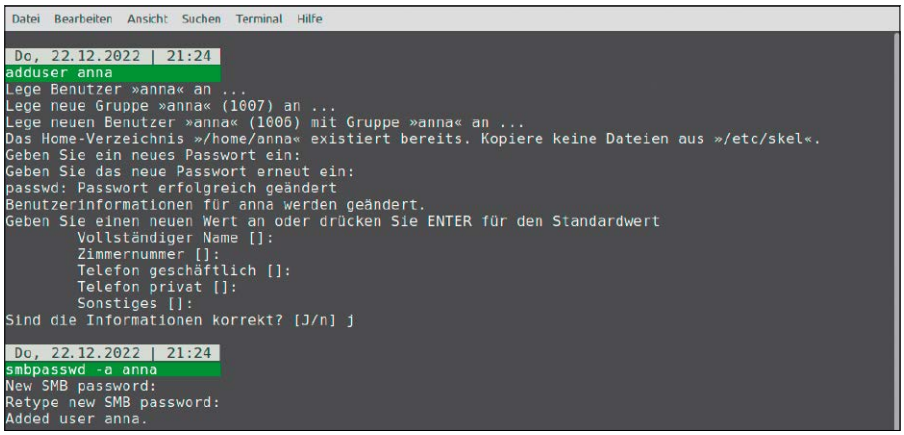
```
adduser archiv
smbpasswd -a archiv
```

ein Systemkonto und ein Samba-Konto angelegt werden – der Einfachheit halber beides mit demselben Kennwort. Für die oben angesprochene Freigabe von Home-Verzeichnissen gilt das analog: Wenn eine Person „Anna“ auf dem Server eine Home-Freigabe erhalten soll, ist dies mit

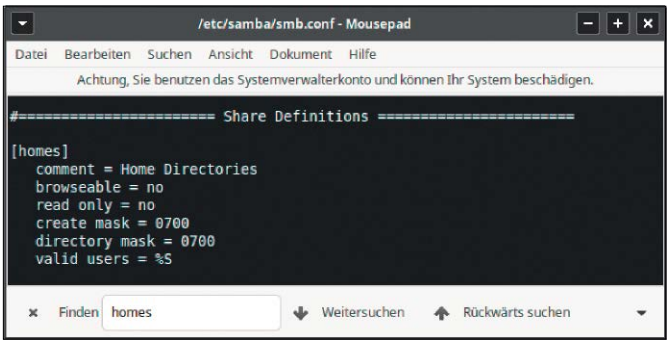
```
adduser anna
smbpasswd -a anna
```

vorzubereiten.

Server (3) Router (Fritzbox): Alle Router bieten eine NAS-Funktionalität, also Linux-Samba-Freigaben. In der Fritzbox-Konfigurationsoberfläche (*http://fritz.box* im Browser) aktivieren Sie dazu unter „Heimnetz → USB / Speicher → Geräte und Heimnetzfreigabe“ die Option „Speicher (NAS) [...] aktiv“, weiter unten unter „Heimnetzfreigabe“ ferner die Option „Zugriff über ein Netzlaufwerk (SMB) aktiv“. Damit ist der Samba-Server eingeschaltet. Die Fritzbox verlangt für den Zutritt außerdem ein Konto unter „System → Fritz!Box-Benutzer“. Das entspricht der Einrichtung von Systemkonto und Samba-Konto unter Linux wie oben beschrieben. In der Fritzbox-Konfiguration ist das mit „Benutzer hinzufügen“ und der Option „Zugang zu NAS-Inhalten“ zu erledigen. Künftig sind an die Fritzbox angeschlossene USB-Geräte (Ext2/3/4, NTFS, FAT, FAT32) per Samba freigegeben.



Systemkonto plus Samba-Konto: Dies sind die Grundvoraussetzungen für jeden Samba-Netzwerkzugriff. Das Kennwort kann identisch gewählt werden.



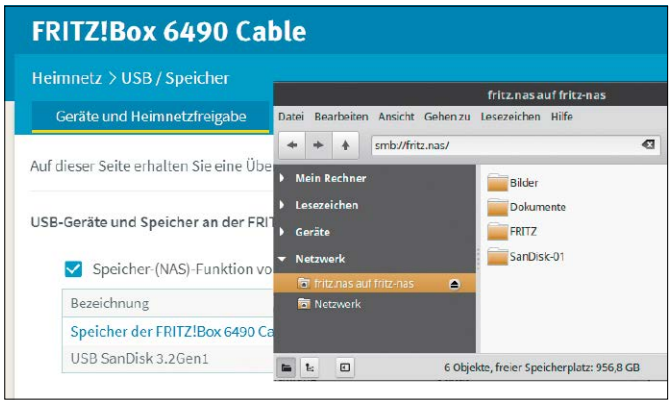
Samba mit Home-Freigaben: Das ist der einfachste Weg, für mehrere User eine Netzwerkheimat zu schaffen.

Clients (1) Windows: Linux- wie Windows-Freigaben erscheinen nicht automatisch unter „Netzwerk“ im Windows-Explorer. Es ist also mindestens einmal nötig, im Explorer manuell eine Samba-Adresse wie „\\192.168.178.1“ oder „\\fritz.nas“ einzugeben – also nach doppelten Backslash entweder die lokale IP-Adresse oder der Rechnername. Der Server (hier die Fritzbox) lässt sich dann im Windows-Schnellzugriff dauerhaft anheften und künftig mit einem Klick erreichen, sofern man sich die Zugangsdaten speichern lässt.

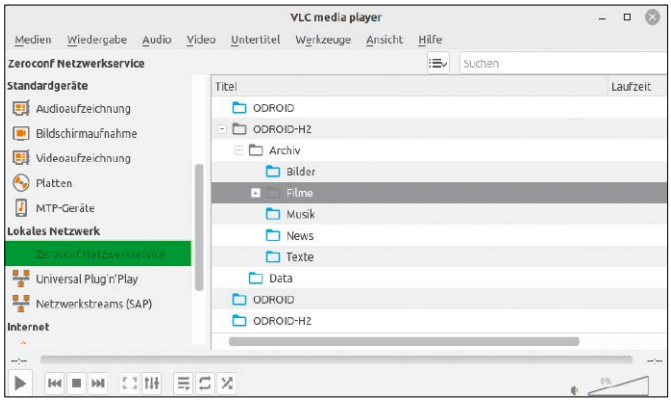
Clients (2) Linux: Auch in Linux-Dateimanagern erscheinen Freigaben nicht automatisch. Hier helfen Adressangaben wie „smb://192.168.178.1“ oder „smb://fritz.nas“. Und auch hier empfiehlt es sich, die lästige Adressangabe durch ein Lesezeichen in der Navigationsspalte des Dateimanagers zu ersetzen („Lesezeichen → Lesezeichen hinzufügen“ oder Drag & Drop der Netzressource).

Clients (3) Android/iOS: Als typische Abspielgeräte sollten Tablets und Smartphones Windows- und Samba-Freigaben nativ unterstützen, tun es aber nicht. Eine Extra-App muss her und der FE File Explorer ist dafür die beste Empfehlung: Neben Samba- und Windows-Freigaben kann er auch FTP, SFTP, Webdav und Clouddienste erreichen. Die kostenlose Version erlaubt allerdings nur eine einzige eingerichtete Serverquelle und nur wenige Audio- und Videoformate. Die Bezahlversion ist mit knapp fünf Euro die Investition wert. Bei Windows- und Samba-Freigaben ist nach Auswahl des Servertyps „Windows“ die lokale IP-Adresse anzugeben, das Speichern von „User“ und „Password“ vereinfacht den Zugriff.

Clients (4) VLC: Für Video- und Audiowiedergabe aller Art sollte man immer den VLC-Player priorisieren. Der zeigt Linux-Samba-Freigaben (aber keine Windows-Freigaben) automatisch und spielt von dort alle Medien. Das funktioniert auf allen Plattformen, aber nicht ganz identisch: Der



Fritz-NAS in der Konfiguration und im Linux-Dateimanager: Samba-Freigaben von USB-Geräten an der Fritzbox kosten wenig Aufwand.



Der VLC-Player findet Samba-Server. Das ist die praktischste Methode für die Medienwiedergabe auf Linux-, Windows-, Android- oder iOS-Clients.

Weg auf PCs führt über „Ansicht → Wiedergabeliste“ auf den Punkt „mDNS Netzwerk Diensterkennung“ (in älteren Versionen auf „Zeroconf Netzwerkservice“). In der Android-Variante zeigen sich Samba-Server unter „Dateien → Lokales Netzwerk“, in der iOS-Variante unter „Netzwerk → Dateiserver“.

SSH/SFTP mit Windows-Hürden

Die ausführliche Beschreibung für die Windows/Samba-Dienste hatte nur den einen Grund, dass kaum ein Heimnetz ohne Windows auskommt. Ohne Windows-Clients ist SSH mit seinem Dateiprotokoll SFTP völlig ausreichend und obendrein funktionsreicher.

Linux-Server: Die SSH-Serverkomponente ist auf Linux-Desktops meistens nicht vorinstalliert, aber mit dem Befehl

```
sudo apt install openssh-server
```

schnell nachgerüstet und damit auch sofort einsatzbereit. SSH erledigt drei Aufgaben gleichzeitig: Erstens erreicht man übers Netz das Terminal des Servers inklusive aller Terminalprogramme. Zweitens eröffnet das integrierte Protokoll SFTP Datenaustausch und Medienwiedergabe für jeden Linux- und Mac-OS-Dateimanager, aber auch für Android/iOS mit geeigneten Apps. Drittens können via X11-Forwarding grafische Programme des Servers genutzt werden.

Alle Einstellungen des Serverdienstes sind in der Datei „/etc/ssh/sshd_config“ zu steuern. Eine mögliche Anweisung, die einen Eingriff verdient, ist

```
X11Forwarding yes
```

statt auskommentierten „#X11Forwarding no“ (Standard). Weitere Änderungen sind in einem unkritischen Heimnetz selten nötig: Zwar hat standardmäßig jedes Systemkonto des Linux-Servers die Erlaubnis zum SSH-Fernzugriff, aber nur sudo-berechtigte Konten dürfen überall lesen und schreiben. Bei Bedarf kann die zusätzliche Zeile (egal wo)

```
AllowUsers sepp […]
```

den SSH-Zugriff auf bestimmte Konten beschränken.

Clients (1) Linux und Mac-OS: In das Terminal des Servers führt etwa folgendes Kommando (Beispiel)

```
ssh sepp@192.168.178.20
```

und ein Aufruf wie

```
ssh -X sepp@192.168.178.20
  thunderbird
```

kann auch grafische Programme des Servers auf dem lokalen System nutzen. Im Heimnetz noch wichtiger ist die Tatsache, dass Linux-Dateimanager das SSH-Dateiprotokoll beherrschen und mit einer Adresse (Beispiel)

```
sftp://sepp@192.168.178.20/srv/
  archiv/
```

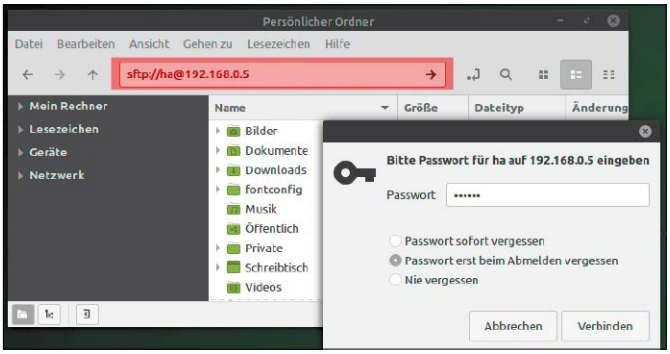
Samba-like und performanter an die Serverdateien kommen. Die Adresseingabe ist lästig, lässt sich aber durch ein Lesezeichen auf einen Mausklick abkürzen.

Clients (2) Android und iOS: Mobilgeräte können standardmäßig mit SFTP ebenso wenig umgehen wie mit Samba. Die schon für Samba empfohlene App FE File Explorer schließt diese Lücke vorbildlich. Für die SSH-Terminalnutzung gibt es ebenfalls Apps wie das kostenlose Termius.

Clients (3) Windows: Windows hat neuerdings einen nativen SSH-Client (neben dem verbreiteten Extratool Putty), aber X11-Forwarding und Dateiaustausch bleiben eingeschränkt. Im Prinzip geht mit Zusatztools (Vcxsrv für X11, *https://sourceforge.net/projects/vcxsrv*, ferner Filezilla für SFTP, *www.filezilla-project.org*) einiges mehr, aber für richtig komfortable Daten- und Mediennutzung müsste der Windows-Explorer SFTP-tauglich werden.

UPnP-Medienserver

UPnP-Server haben ihre Vorteile gegenüber der trockenen Dateiebene mit Samba oder SFTP: Sie bringen Video und Audio auch an Geräte wie Smart-TVs, die mit



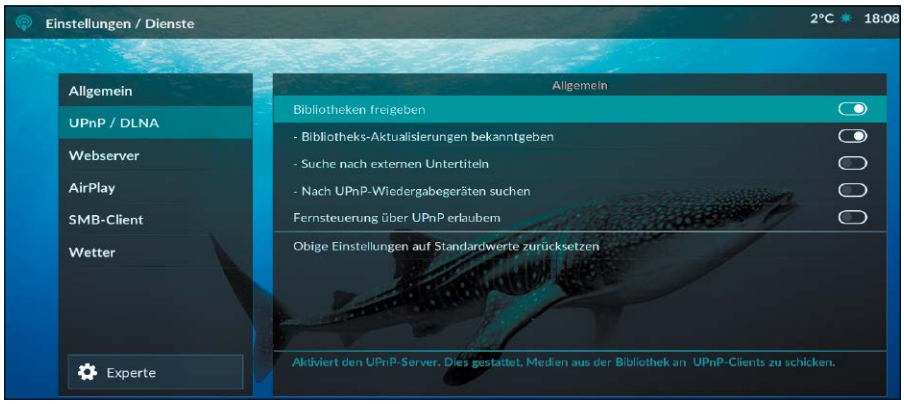
Datenzugriff und Mediennutzung per SFTP: Linux-Dateimanager sprechen SFTP und verbinden sich mit einem SSH-Server. Mac-OS, Android und iOS spielen ebenfalls mit.

Samba und SFTP nichts anfangen können. Außerdem sorgt die Auswertung der Medientags für schicke Präsentation und bessere Suchoptionen, die aus großen Sammlungen vergrabene Schätze holen können. Wirklich wertig wird UPnP im Vergleich zum einfacheren Samba- oder SFTP-Streaming aber nur, wenn das Video- und Musikmaterial sprechende Titel und zuverlässige Medientags besitzt.

Windows benötigt als UPnP-Server im Prinzip keine Extrasoftware, denn dies kann der Windows Media Player über „Streamen → Medienstreaming aktivieren" erledigen. Was der Player liefern soll, kann über „Organisieren → Bibliotheken verwalten" bestimmt werden. Die Medien erscheinen dann auf UPnP-kompatiblen Geräten wie etwa Smart-TVs oder auch im VLC- oder Banshee-Player unter „Universal Plug'n'Play".

Linux/Windows mit Kodi: An Streamingservern unter Linux besteht kein Mangel (Readymedia, Gerbera, Kodi, Plex, Emby), wobei aber Minimalisten wie Readymedia oder Gerbera den Geschmack dieser Zielgruppe eher verfehlen dürften. Erster Kandidat ist und bleibt das plattformunabhängige Kodi. Downloads für Windows oder Mac-OS sowie Installationsanleitungen für Linux gibt es unter *https://kodi.tv/download*. Damit das Medienangebot unter Kodi von UPnP-fähigen Playern wie VLC, Windows Media Player oder auch einem Smart-TV im Netzwerk gefunden wird, müssen Sie unter „System → Einstellungen → Dienste" den Dienst „UPnP/DLNA" aktivieren und dann die Option „Bibliotheken freigeben". Damit wird Kodi zum Streaming-Server.

Übers Netzwerk zu finden sind aber nur Medien, die Kodi in seine Bibliotheken eingelesen hat. Dies muss für alle Medientypen explizit erfolgen. Gehen Sie in Kodi auf „Videos → Dateien", wählen Sie „Videos hinzufügen" und klicken Sie auf „Durchsuchen". Nach Auswahl der Quelle lässt sich bei Videos der Inhalt festlegen. Zur Wahl stehen „Filme", „Serien" und „Musikvideos". Abhängig von der Auswahl lädt Kodi Coverbilder und Beschreibungen herunter. Nach einem Klick auf „Einstellungen" sollten Sie hinter „Bevorzugte Sprache" den Wert auf „de" festlegen, damit diese Informationen in deutscher Sprache erscheinen. Für Musik und Bilder läuft die Konfiguration entsprechend ab.



Kodi-Mediencenter als UPnP-Server: Mit diesen Einstellungen kann Kodi die Medien für andere Clients über das Netzwerk bereitstellen und auf andere Geräte streamen.

Remotedesktops

Remotedesktops bieten den Fernzugriff auf den kompletten grafischen Desktop. Dieser Netzwerkdienst eignet sich optimal zur Nutzung von Software, die nur auf dem Serversystem vorliegt, aber auch etwa für direkte Downloads auf dem dafür vorgesehenen Zielrechner.

Linux-Server: Als Remoteserver für Linux empfehlen wir X2go. Die Serverkomponente wird nach

```
sudo apt install x2goserver
```

als Systemdienst eingerichtet. Für optimale Darstellung empfiehlt sich am Server zusätzlich der Desktop XFCE:

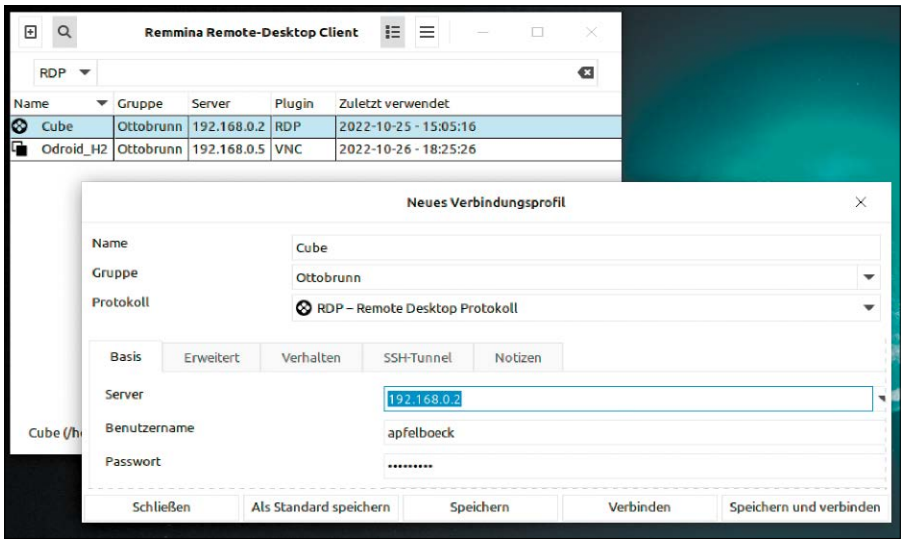
```
sudo apt install xubuntu-desktop
```

Zugriffsclients gibt es für Linux, Windows und Mac-OS unter *https://wiki.x2go.org*, für Debian/Ubuntu auch in den Standardquellen (*sudo apt install x2goclient*). Im X2go-Client definieren Sie mit „Sitzung → Neue Sitzung" den Server, was danach im Wesentlichen nur die Angaben der korrekten LAN-IP-Adresse und des bevorzugten Desktops erfordert (XFCE).

Windows-Server: Den Remotedesktop-Server (RDP) gibt es nur in Windows Pro. Liegt diese vor, kann der Serverdienst unter „Einstellungen → System → Remotedesktop" aktiviert werden. Windows-Clients verbinden sich mit der standardmäßig installierten Software „Remotedesktopverbindung" und Angabe der IP-Adresse des Servers. Linux-Rechner verwenden am besten Remmina, das nach

```
sudo apt install remmina remmina-
  plugin-rdp
```

inklusive RDP-Plug-in nachzuinstallieren ist. Für den Zugriff muss in Remmina als Protokoll „RDP" und die IP-Adresse des Windows-Rechners eingegeben werden, alles Weitere ist optional. ■

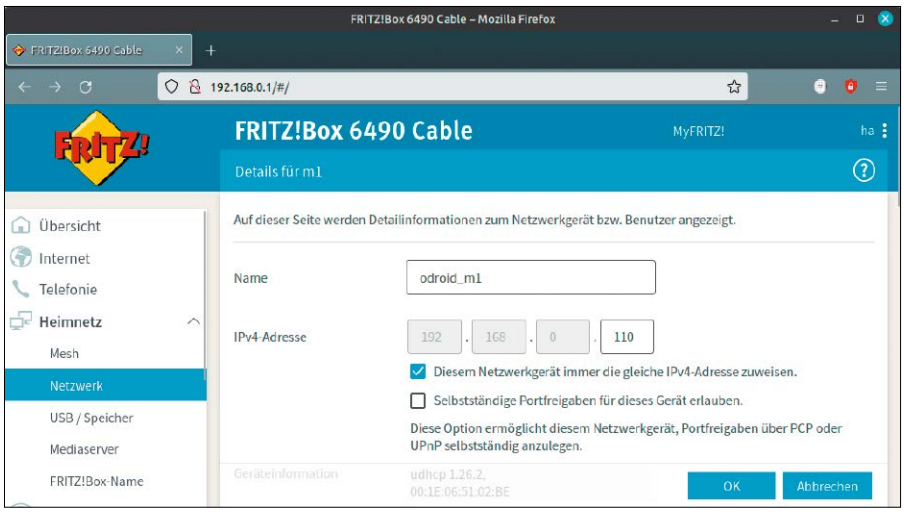


Remoteclient Remmina: Die lokale IP-Adresse und das RDP-Protokoll genügen, um in Linux einen Windows-Desktop zu nutzen.

Tipps & Tools für das Netzwerk

Die folgenden Tipps, Infos und Tools beziehen sich allesamt auf das lokale Heimnetz. Dabei geht in erster Linie darum, den Zugriff auf Netzgeräte zu vereinfachen und den Datenaustausch zu optimieren.

VON HERMANN APFELBÖCK



Feste IPv4-Adresse für Server aller Art: Jeder Rechner kann eine feste IP über seine Netzwerkeinstellungen anfordern. Einfacher ist die Vergabe in der Routerkonfiguration.

Tipps, IP-Konfiguration und Netzwerktools können keinen defekten Adapter und kein mangelhaftes Funknetz kompensieren – dazu ist Hardware erforderlich. Aber Sie erreichen Geräte schneller und kommunizieren umweglos, wenn Sie die IP-Konfiguration in die Hand nehmen und die passenden Werkzeuge zum Datenaustausch verwenden.

Feste IP-Adresse für Server

Alle Geräte mit Serverfunktion (Samba, SSH, Apache-Webserver, UPnP, Remotedesktop, Torrent) benötigen eine feste IP-Adresse – im lokalen Netz dringend, für Portfreigaben ins Internet zwingend. Nur dann funktionieren SSH-Verbindungen, Samba-Freigaben mit IP-Adresse oder IP-Lesezeichen im Browser zuverlässig. Heimrouter vergeben (als DHCP-Server) die lokalen IP-Adressen für die einzelnen Geräte keineswegs willkürlich. Es kann sein, dass ein Rechner oder ein Smartphone monatelang stets die identische IP-Adresse erhält, ohne dass dies explizit verlangt worden wäre. Das Bestreben, konstante Adressen zu vergeben, ist also schon Router-Standardverhalten. Die Garantie, dass ein NAS-Server beispielsweise die „10“ im vierten und letzten Byte der Adresse erhält, haben Sie aber nur, wenn dies ausdrücklich gefordert wird.

Jedes Netzgerät hat eine Systemeinstellung, um statt zufälligem IP-Bezug („DHCP“ oder „Automatisch“) eine feste IP anzufordern. Die nennt sich dann „Manuell“ (Linux, Mac) oder „Statisch“ (Android). Die empfohlene Methode ist aber der Weg zum Router. Der hat alle Geräte und Adressen im Blick, warnt vor Fehlern und erledigt die Aufgabe in der Konfigurationsoberfläche mit bequemen Eingabefeldern (während auf Linux-Servern eventuell Terminal und Konfigurationsdateien notwendig wären). Wenn Sie in der Fritzbox unter „Heimnetz → Netzübersicht“ in der Zeile des gewünschten Geräts das Stiftsymbol für die Bearbeitung anklicken, sehen Sie dort die Option „Diesem Netzwerkgerät immer die gleiche IPv4-Adresse zuweisen“.

Nach Klick auf „Ändern“ können Sie an vierter Stelle der Adresse die Wunschnummer eingeben. Der Router wird dann noch einen Hinweis bringen, dass diese IP erst nach dem nächsten Neustart des Geräts gelten wird.

Browserlesezeichen für Server

Wichtige Geräte im lokalen Netz bieten ihre Konfigurationsoberfläche über einen Webserver an, den Sie im Browser erreichen: Dazu gehört in jedem Fall die Oberfläche des Heimrouters, häufig weitere Netzgeräte mit integriertem Webserver wie Access Points, Repeater, NAS-Geräte, Medienserver, Netzwerkdrucker, eventuell auch eigene Serverdienste. Es lohnt sich also, im Browser Ihrer Wahl Lesezeichen für diese lokalen Adressen anzulegen. Dies funktioniert bei allen Browsern durch einfaches Drag & Drop aus der Adresszeile in Lesezeichenleiste. Danach ist noch über „Lesezeichen bearbeiten“ (oder ähnlich) ein sprechender Name zu empfehlen. Damit erreichen Sie künftig die Konfiguration all dieser Geräte mit einem Klick, ohne über IP oder Hostnamen nachdenken zu müssen. Voraussetzung ist, dass alle diese Geräte eine konstante IP-Adresse besitzen.

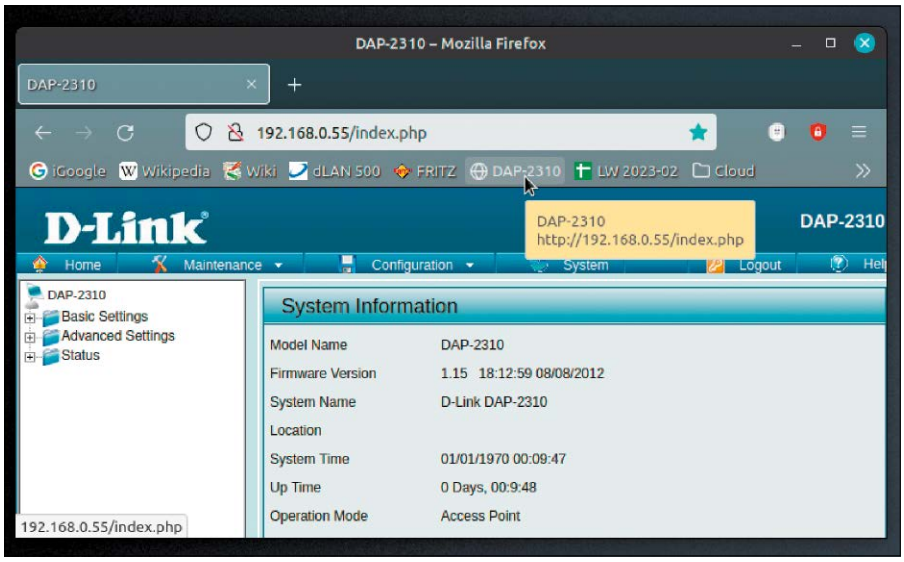
Die Subnetzmaske

Spätestens dann, wenn Sie bei einem Linux-oder Windows-Rechner eine benutzer-

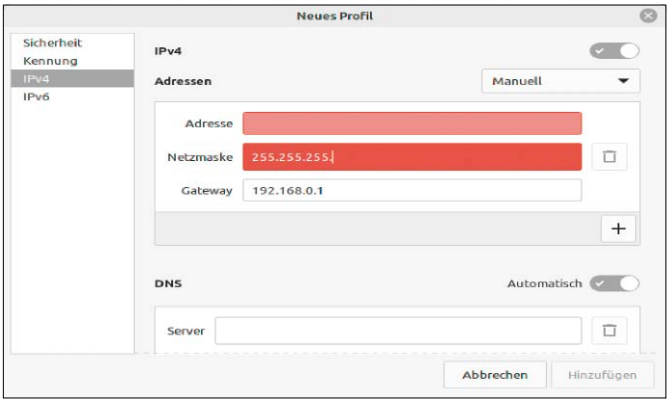
definierte IPv4-Adresse beziehen wollen (und das nicht am Router tätigen, sondern am Endgerät), kommt die Netzmaske ins Spiel. Diese wird neben der gewünschten IP und dem Standardgateway (Router-IP) abgefragt. Wer jahrelang mit Heimnetz-IPs zu tun hatte, der tippt automatisch „255.255.255.0“ ein. Das ist in allen Heimnetzen korrekt, aber warum eigentlich?

Die Bitmaske mit vier Bytes besagt, dass die ersten drei Bytes (also 24 Bits) belegt sind und daher nicht für Geräte vergeben werden können. Lediglich das vierte und letzte Byte bleibt frei zur Verfügung. Dies führt zu der typischen Situation im Heimnetz, dass die ersten drei Byte durch die Gatewayadresse (Router) vorgegeben sind (etwa 192.168.178) und nur die letzte Stelle (das vierte Byte) von „2“ bis „254“ für Geräte-IP genutzt werden kann. Die „1“ reserviert sich der Router, desgleichen reserviert ist „255“ als Rundrufadresse (Broadcast).

Anders als ein Netzclient fragt der Router bei einer festen IP-Vergabe nicht nach der Subnetzmaske – aus dem einfachen Grund, weil er sie kennt und selbst verwaltet. Theoretisch kann ein Router wie die Fritzbox durch die Subnetzmaske die Anzahl der möglichen Geräte sowohl verringern als auch erweitern („Heimnetz → Netzwerk → Netzwerkeinstellungen → IPv4-Einstellungen“). Die kleinste mögliche Subnetzmaske wäre „255.255.255.252“, die neben dem Router nur noch genau ein Netzgerät zuließe, während eine Netzmaske „255.255.254.0“ maximal 510 Geräte erlaubt, die Netzmaske „255.255.252.0“ mehr als tausend. Ein Ändern der Netzmaske in einem funktionierenden Netz mit diversen Clients wäre allerdings fatal und wird daher von einigen Providern generell gesperrt. Wo es erlaubt ist, wäre es nur bei der Ersteinrichtung des Netzes eine Überlegung wert, den Standard „255.255.255.0“ zu verlassen.



Browserlesezeichen für lokale Geräte: Sorgen Sie dafür, dass Sie die Routeroberfläche und andere Netzgeräte mit Webserver mit einem Klick erreichen.



Netzmaske oder Subnetzmaske: Die lautet in Heimnetzen immer „255.255.255.0“, weil die ersten drei Bytes vergeben sind und nur das letzte Byte für Netzgeräte frei bleibt.

Isolierte(r) Rechner oder Rechnergruppe

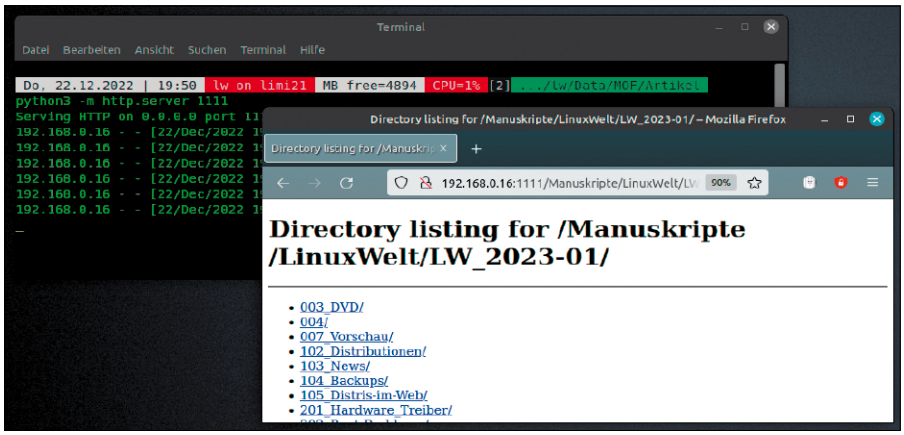
Wie praktisch alle Heimrouter bietet die Fritzbox zwei Netzwerke mit je eigenem Adressraum. Davon machen die allermeisten Nutzer nur Gebrauch, wenn sie ein WLAN-Gastnetz für Besucher anbieten wollen (Fritzbox: „WLAN → Gastzugang“). Das hat den doppelten Vorteil, dass das primäre Zugangskennwort geheim bleibt und dass alle Geräte im Gastnetz aufgrund des eigenen Adressraum isoliert bleiben („Client Isolation“): Die Geräte können zwar ins Internet, sehen aber weder Netzfreigaben noch generell Geräte im lokalen Netz, folglich auch keine lokalen Serverdienste wie etwa die Konfigurationsoberflächen des Routers oder eines NAS-Systems.

Router wie die Fritzbox können aber auch Ethernet-verbundene Geräte in das Gastnetz verlegen. Beim AVM-Router ist dafür der Ethernet-Port „LAN 4“ vorgesehen. Der lässt sich unter „Heimnetz → Netzwerk → Netzwerkeinstellungen“ mit einem Mausklick in das Gastnetz befördern: „Gastzugang für LAN 4 aktiv“. Weitere Einstellungen gibt es hier nicht: Für alle Geräte, die direkt oder indirekt (Switch, Powerline) am LAN-Port 4 angeschlossen sind, gilt dann der gesonderte Adressraum und „Client Isolation“ vom sonstigen Heimnetz. Auf diese Weise können Sie zwei getrennte Netze etwa für Homeoffice und Familie etablieren, ohne über Zugangsrechte und Kennwörter grübeln zu müssen. Standardadressraum bei der Fritzbox für das Zweitnetz ist 192.168.179.xxx. Der lässt sich aber – wie der primäre Adressraum – unter „Heimnetz → Netzwerk → Netzwerkeinstellungen → IP-Adressen“ auch ändern (nur bei Ersteinrichtung des Netzwerks zu empfehlen!).

Python: Einfache HTTP-Freigabe

Nahezu jedes Linux-System, übrigens auch das Linux-Subsystem unter Windows (falls installiert), kennt eine sehr einfache Option, einen Ordnerinhalt inklusive aller Unterordner ganz einfach anderen Teilnehmern im Netzwerk per Browser zugänglich zu machen.

Der Script-Interpreter Python, der in den meisten Linux-Distributionen vorinstalliert ist, enthält einen kleinen Webserver, der mit einem einzigen Befehl im Terminal aus dem gewünschten Verzeichnis heraus in Gang gesetzt wird:



HTTP-Server mit Python: Mit einem Terminalbefehl ist ein Webserver für das aktuelle Verzeichnis inklusive aller Unterordner eingerichtet.

```
python3 -m http.server 4444
```

Älteres Python benötigt diesen Aufruf:

```
python -m SimpleHTTP-Server 4444
```

Der Port (hier „4444“) ist jenseits von Standardports frei wählbar. Jeder Browser im lokalen Netz kann dann auf die Dateien in diesem Verzeichnis inklusive aller Unterverzeichnisse zugreifen. Soll der Miniserver immer im gleichen Verzeichnis starten, wäre ein Alias (Beispiel)

```
alias http='cd /srv/data/; python3
 -m http.server 4444'
```

eine schnelle Abkürzung unter Linux oder ein Link wie

```
wsl --cd /mnt/d/data/ --exec python
 -m SimpleHTTPServer 4444
```

ein Schnellstarter unter Windows (mit Linux-Subsystem).

Hat der „Server“-PC beispielsweise die IP-Adresse 192.168.0.2, so kommt man auf jedem Rechner mit dem Browser und der Adresse

```
192.168.0.2:4444
```

zur Freigabe. Hier geht dann alles, was heutige Browser beherrschen – Lesen, Abspielen, Anzeigen diverser Text-, Bild-, Audio- und Videoformate. Bei Formaten, die der Browser nicht beherrscht, ist der Download die Standardaktion. Wenn der Mini-Webserver in einem Verzeichnis auf eine Datei „index.html“ trifft, zeigt er erwartungsgemäß deren Inhalt. Strg-C im Terminal beendet den Mini-Webserver auf dem Server-System wieder.

Datenserver: Mehr als nur Datenhalde

Platinenserver- und NAS-Geräte werden meistens als reine Daten- und Backuphalde genutzt. Diese Rolle ist zwar wertvoll, aber ein solcher Server kann mehr, wie folgende Beispiele andeuten sollen:

Identische Programme auf mehreren PCs können Konfiguration, Vorlagen oder Sicherungskopien auf dem Server ablegen – mit dem Ergebnis, dass Sie auf allen Rechnern dieselbe Umgebung vorfinden. So akzeptiert der Firefox-Browser nach dem Startschalter „firefox -profile [...]“ jeden Pfad als Quelle für sein Benutzerprofil. Unter Libre Office lassen sich Backup- und Arbeitsverzeichnisse unter „Extras → Optionen → LibreOffice → Pfade“ auch auf Netzfreigaben verlegen.

Wenn es die Netzwerkleistung erlaubt, können portable Windows-Programme wie Filezilla auch komplett vom Netzlaufwerk laufen. Unter Linux kommen Tools im Appimage-Format in Betracht. Besonders flexibel sind Kommandointerpreter wie Bash, Powershell oder Cmd. Hier genügt es schon, das Netzlaufwerk in den Systempfad aufzunehmen und somit Scripts nur noch an einer Stelle pflegen zu müssen.

Es ist aber offensichtlich, dass solche Maßnahmen statt Komfort Ärger und Verzögerungen verursachen, wenn die Netzfreigabe nicht konstant verfügbar ist. Der Server muss also erstens zuverlässig laufen und zweitens immer eingebunden sein (siehe folgenden Tipp).

Mounten von Netzwerklaufwerken

Für stets erforderliche Netzressourcen reichen Lesezeichen im Dateimanager (und das damit manuell ausgelöste Mounten in das lokale Linux-Dateisystem) nicht aus. Die Freigabe sollte besser schon beim Systemstart zur Verfügung stehen und dafür in der Datei „/etc/fstab“ eingehängt werden. Das dafür nötige Paket „cifs-utils“ ist in der Regel bereits vorinstalliert. Eine Mountanweisung für eine Samba/Windows-Freigabe sieht im Prinzip so aus:

```
//[Server-IP]/[Freigabename] /
 [Mountverzeichnis] cifs
 [Optionen] 0 0
```

Die Optionen sind in diesem Fall aber nicht einfach, weil die Samba-Erlaubnis und Dateirechte berücksichtigt werden müssen. Ein konkretes Beispiel könnte dann folgendermaßen aussehen:

```
//192.168.178.10/Daten /mnt/Daten
 cifs rw,_netdev,auto,nofail,user
 name=sepp,password=geheim,uid=10
 00,gid=1000,file_mode=0644,dir_
 mode=0755 0 0
```

Der Mountpfad (hier unter „/mnt“) muss existieren. Das Beispiel geht davon aus, dass der lokale Benutzer und das Samba-Konto gleichlautend sind („sepp“). UID und GID des (lokalen) Linux-Benutzerkontos ermitteln Sie mit

```
id -u [Konto]
id -g [Konto]
```

Diese Anweisungen und die Rechtemasken sind nötig, damit der Benutzer auf die Freigabe Schreibzugriff erhält. Weitere Optionen wie „nofail“ und „_netdev“ machen den Vorgang fehlertoleranter. Verwenden Sie den Befehl *sudo mount -a*, um sich über Erfolg oder Misserfolg des fstab-Eintrags ohne Neustart zu informieren.

Netzwerktempo: Messungen

Für Tempomessungen im lokalen Netz gibt es Dutzende von Apps und Tools. Wer wissen will, wie viel Durchsatz in seinem Gigabit-Netz durch Powerline- und Funknetzbremsen noch übrigbleibt, kopiert am



Freigaben automatisch mounten: Mit einer Anweisung in der Datei „/etc/fstab“ lässt sich eine Samba/Windows-Freigabe ab Systemstart in das Dateisystem einhängen.

besten einfach eine große Datei von einer Netzfreigabe zum lokalen Rechner. Egal ob unter Linux oder Windows, wird der Dateimanager dabei auf jeden Fall eine Angabe in „MB/s“ anzeigen.

Spezielle Tools sind nur dann sinnvoll oder notwendig, wenn mit einem mobilen Android- oder iOS-Gerät an unterschiedlichen Orten gemessen werden soll. Fritzbox-Besitzer greifen am besten zur Android- und iOS-App „Fritz!App WLAN“. Über „Verbinden“ können Sie das Funknetz wechseln, falls das Heimnetz mehrere Sender hat, und unter „Mein WLAN“ gibt es die Option „WLAN messen“. Je nachdem, wie gut oder schlecht die Qualität der WLAN-Verbindung ist, schlägt der Pegel nach oben oder unten aus. Auf diese Weise können Sie ganz einfach ausmessen, in welchen Bereichen das Funksignal schwach ist. Mit „Stop“ beenden Sie die Echtzeitmessung und erhalten einen Bericht.

Nmap: Netzwerkübersicht

Was läuft in meinem Netz – und gehört das alles tatsächlich zu meinem Netz? Bei solchen Fragen hilft der Gang zur Routeroberfläche oder das Tool nmap. Nmap ist mit dem Paketnamen „nmap“ in allen Distributionen erhältlich.

Folgende nmap-Kommandos

```
nmap -sP 192.168.178.*
nmap -sP 192.168.178.* | grep
  "report"
```

schicken eine einfache Ping-Anfrage an alle 255 Adressen des Adressraums. Der Ping-Scan zeigt alle laufenden Netzgeräte mit Hostnamen und IP-Adresse. Ohne Ping-Parameter („-sP“) macht nmap sorgfältige und zeitaufwendige Portscans: Sie erhalten zu jedem Rechner Hostnamen, IP-Adresse, MAC-Adresse und die Liste aller offenen Ports. Ist der intensive Vorgang für den gesamten lokalen Adressraum zu langwierig, lässt sich auch ein einzelner PC befragen (*nmap 192.168.178.10*).

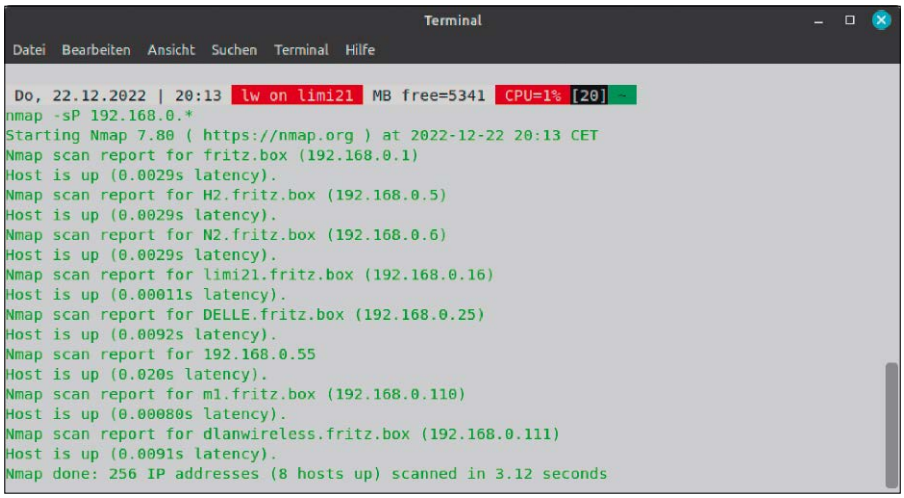
Risiken für ein Heimnetz entstehen durch offene Ports, die den Zutritt über das Internet in das lokale Netz erlauben. Kontrolle über eventuell vergessene Portfreigaben erhalten Sie im Router (Fritzbox: „Internet → Freigaben → Portfreigaben“). Mit nmap können Sie einen Test realisieren, der auch innere Feinde in Form von laufender Schadsoftware entlarvt. Dazu brauchen Sie Ihre öffentliche IP-Adresse. Die kennt Ihr Router („Übersicht“ in der Fritzbox), sie kann aber auch mit einem Tool wie inxi ermittelt werden (*inxi -i*). Die öffentliche WAN-IP, beispielweise 178.23.136.15, prüfen Sie dann mit diesem Kommando:

```
sudo nmap -Pn 178.23.136.15
```

Dabei untersucht nmap die Standardports von 1 bis 1000. Als Ergebnis sollten Sie, sofern Ihr Netz für das Internet komplett geschlossen sein soll, die Antwort erhalten „All scanned ports are filtered“. Ist das nicht der Fall, gehen Sie mit der angezeigten Portnummer der Sache auf den Grund:

```
sudo nmap -sV -Pn -p[Nummer]
  178.23.136.15
```

Mit Schalter „-sV“ zeigt nmap an, welches Programm oder welcher Dienst diesen Port benutzt. Ist dieser Prozess unerwünscht, beenden und deinstallieren Sie den Verursacher.



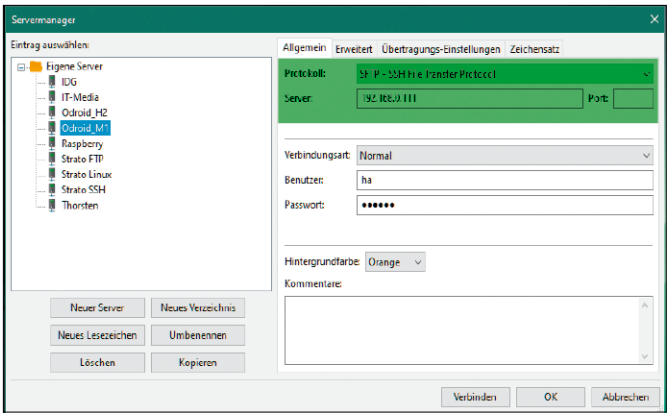
Überblick mit nmap: Der Portscanner nmap taugt auch für einfache Ping-Abfragen im lokalen Adressraum und löst dabei die Hostnamen auf.

MC und Filezilla für SSH

Der Midnight Commander (MC) sollte schon deshalb auf keinem System fehlen, weil er den direkten Datenaustausch mit SSH/SFTP-Servern über die Option „Shell-Verbindung“ beherrscht (in den Menüs „Links/Rechts“).

Wie bei SSH auf der Kommandozeile geben Sie hier die IP-Adresse an, optional gleich mit dem gewünschten User, also etwa „root@192.168.0.10“, gegebenenfalls auch mit abweichender Portangabe „root@192.168.0.10:4444“. Nach Eingabe des Kennworts zeigt der Midnight Commander in einer Fensterhälfte das Dateisystem des Servers, in der anderen das des zugreifenden Systems.

Auch Windows-Systeme dürfen mitmachen, sofern dort ein Windows Subsystem for Linux installiert ist und dort wiederum der Midnight Commander. Wer sich mit Windows ohne Subsystem mit SFTP-Servern verbinden will, greift am besten zum bewährten Filezilla (*www.filezilla-project.org*). SSH-Server sind in dessen Servermanager („Datei → Servermanager“) mit IP-Adresse, Port (Standard 22), SFTP-Protokoll und den Zugangsdaten schnell eingerichtet. ■



Wichtiger SSH/SFTP-Client unter Windows: Das Open-Source-Tool Filezilla muss auf jedes Windows-System, das mit SSH-Servern arbeiten will.

Nextcloud im Heimnetz

Dateien lassen sich über diverse Methoden im eigenen Netzwerk bereitstellen. Eine individuell eingerichtete Nextcloud ist sicher nicht die einfachste Servervariante, bietet aber breite Funktionalität und hohen Komfort.

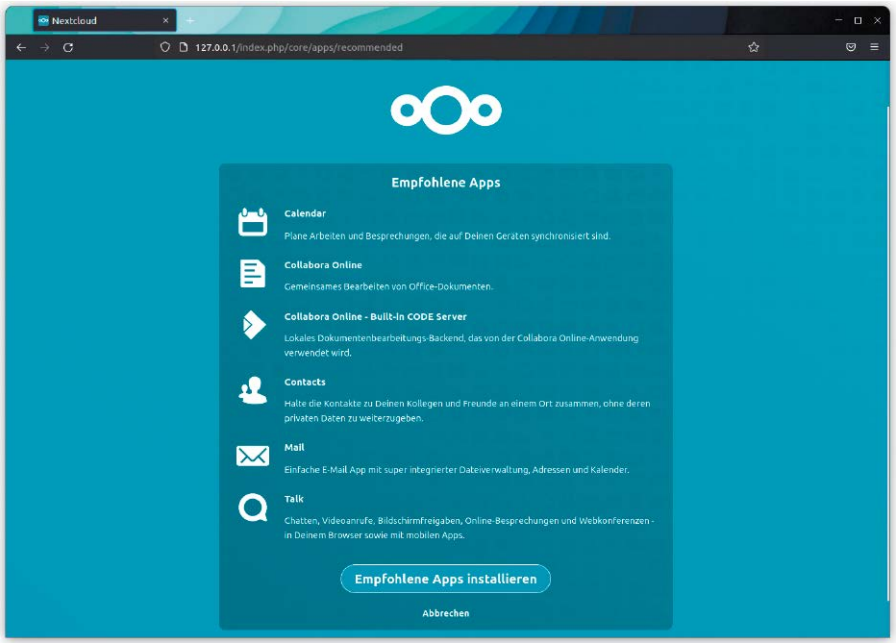
VON HERMANN APFELBÖCK

LinuxWelt-Leser wissen es: Dies ist nicht der erste Beitrag zur Nextcloud (oder Owncloud). Allerdings setzen wir hier einen inhaltlichen Fokus auf die vielseitigen Anwendungsmöglichkeiten dieser Cloudsoftware. Wir behandeln die Nextcloud als Intranetserver im lokalen Netz, gehen dafür aber genauer auf die Apps und Optionen ein, die ein Nextcloud-Server hier sinnvollerweise anbieten kann. Daher vereinfachen wir auch das Thema der Installation und verzichten komplett auf den Aspekt der Öffnung für den Internetzugriff.

Einfache Installation als Snap

Für eine Nextcloud im Homeoffice oder im Kleinbetrieb mit einer Handvoll Mitarbeiter genügt ein Ein-Platinen-Rechner wie der Raspberry 4. Je nach Menge aktuell angemeldeter Nutzer und aktivierter Apps hat die Hardware aber durchaus zu arbeiten: Vier GB RAM sollten vorliegen, ferner für längerfristigen Einsatz ein größerer und schneller Systemdatenträger (schnelle SD-Karte oder Sata-SSD/HDD mit 128 GB aufwärts), idealerweise ergänzt durch ein größeres USB-Laufwerk, das später in die Nextcloud eingebunden wird.

Nextcloud erfordert einen kompletten LAMP-Server und eine nicht ganz einfache Apache- und Datenbankkonfiguration. Ungeachtet gewisser Nachteile (etwas mehr Ressourcenbedarf, theoretische Apache-Konflikte und lokale Pfadumleitungen) ist für eine Nextcloud im Intranet-Homeoffice die Einrichtung als Snap die mit Abstand einfachste Installationsvariante.



Es genügt nämlich dieser Befehl:

```
sudo snap install nextcloud
```

Danach ist der Webserver am lokalen Rechner bereits im Browser mit der Adresse *http://localhost* erreichbar. Vergeben Sie einen Kontonamen und das zugehörige Kennwort. Dies wird der primäre Administrator der Nextcloud-Instanz. Dann klicken Sie auf „Installieren“. Anschließend erhalten Sie das Angebot „Empfohlene Apps“, um damit schon mal eine Grundausstattung einzurichten. Nicht alle diese Module sind für den Einsatz im lokalen Netz einschlägig, aber doch einige. Überflüssige lassen sich später leicht wieder entfernen. Auf anderen Rechnern im Netz erreichen Sie die Instanz mit der IP-Adresse des Server-Rechners in dieser Form (Beispiel):

```
192.168.178.20/index.php
```

Für häufigen Einsatz empfiehlt sich ein Browserlesezeichen.

Tipp 1: Wir haben das Nextcloud-Snap auf mehreren Systemen getestet, und in der Regel funktioniert der Browser-Zugriff mit „[IP-Adresse]/index.php“ auf Anhieb. Der Browser wird zwar die unverschlüsselte HTTP-Adresse als „nicht sicher“ melden, aber das muss Sie im lokalen Netzwerk nicht kümmern. Falls die Seite wider Erwarten nicht erreichbar ist, kontrollieren Sie in der Konfigurationsdatei „config.php“

```
sudo nano /var/snap/nextcloud/
  [Version]/nextcloud/config/
  config.php
```

den Abschnitt „trusted_domains“. Dieser sollte einen Eintrag mit der IP-Adresse des Servergeräts enthalten. Steht hingegen nur

```
0 => 'localhost',
```

so ergänzen Sie darunter diese weitere Zeile (IP anpassen!)

```
1 => '192.168.178.20',
```

und starten das System neu.

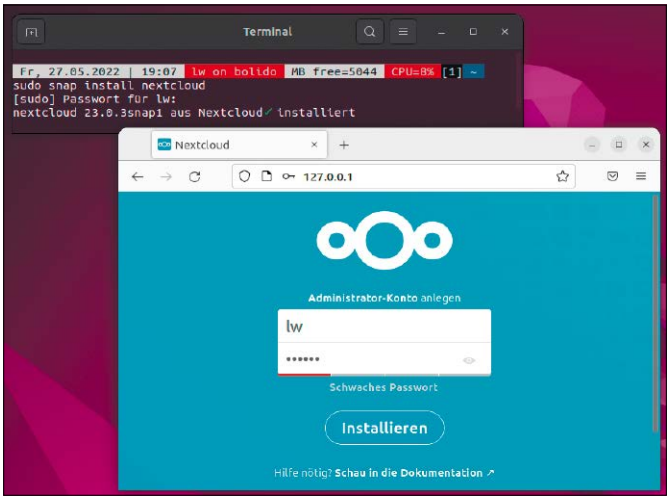
Tipp 2: Eine Snap-Installation ist ungünstig, wenn auf dem System bereits ein Apache-Webserver läuft. Das führt nicht nur zu Ressourcenverschwendung, sondern auch zu Portkonflikten. Der Apache-Server im Nextcloud-Snap nutzt standardmäßig die Ports 80 (HTTP) und 443 (HTTPS). Dies lässt sich im Prinzip umstellen (*sudo snap set nextcloud ports.http=81*), jedoch empfehlen wir im Hinblick auf einfache Verhältnisse das Nextcloud-Snap nur für Rechner ohne Apache.

Erste Schritte in Nextcloud

Alle administrativen Aufgaben erreichen Sie über das Benutzermenü (Kontosymbol ganz rechts oben). Administratorkonten sehen hier mit „Apps“ und „Benutzer“ zusätzliche Menüeinträge, außerdem bietet das Menü „Einstellungen“ für Administratoren einen zusätzlichen globalen Bereich „Verwaltung“ (während normale Benutzer hier nur das Angebot „Persönlich“ vorfinden). Eine erste Aktion, die sowohl für den Admin wie für spätere Benutzer anfällt, ist der Gang zu „Persönlich → Persönliche Informationen“, um hier Sprache und Gebietsschema auf „Deutsch“ zu setzen. Alle weiteren Angaben sind optional.

Als nächsten Schritt des Erstbenutzers und Admins lohnt sich ein Blick unter „Verwaltung“ und dort „Sicherheit“ sowie „Teilen“. Für eine lokale Nextcloud-Instanz (aber nur hier!) sind einige Standards übertrieben. So können etwa die Komplexitätsanforderungen an die Zugangskennwörter deutlich reduziert werden. Es ist zweckmäßig, dies bereits vor dem Anlegen zusätzlicher Teilnehmer festzulegen.

Eine weitere wichtige Anlaufstelle unter der nur für Admins zugänglichen „Verwaltung“ ist der Punkt „System“. Der bietet einen grafischen Systemmonitor und zeigt unter „Festplatte“ die gemounteten Laufwerke. Das ist besonders bei einer Snap-Installation relevant, weil hier die Mountpunkte intern umgeleitet werden. Die Pfade sind später für die Einbindung externer Datenträger wichtig und können an dieser Stelle einfach kopiert werden. Die benötigten

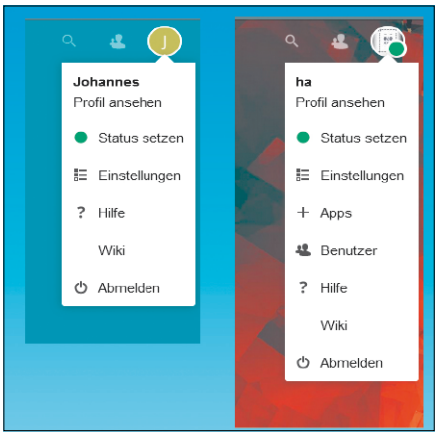


Einfacher geht's nicht: Mit einem Kommando ist der Nextcloud-Server samt Apache, Datenbank und PHP startbereit.



Manchmal erforderlich, meistens nicht: Wenn Browser die Nextcloud-Anmeldung verweigern, dann hilft es, die IP-Adresse des Nextcloud-Servers manuell als „trusted_domain“ nachzutragen.

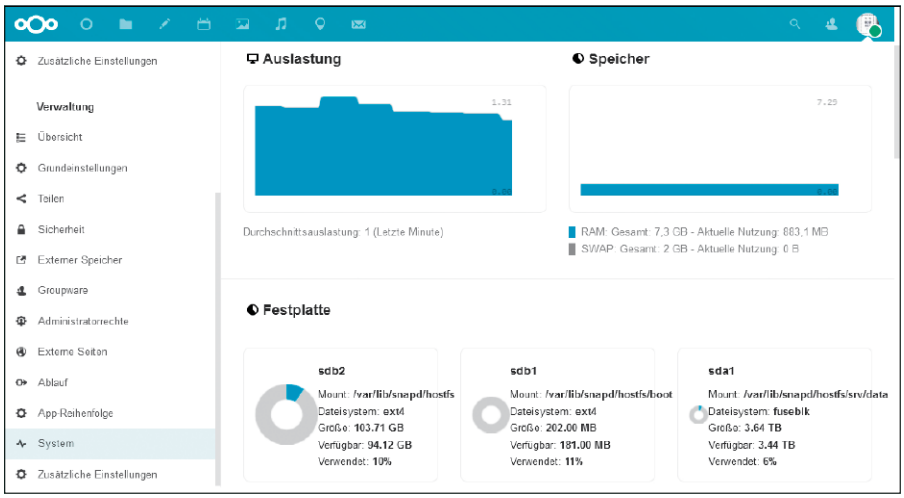
Konten legen Sie dann über das Benutzermenü mit dem Eintrag „Benutzer“ und dann „Neuer Benutzer“ an. Mindestens erforderlich sind der Kontoname und das Passwort. In der Spalte „Gruppen“ können Sie das neue Konto als „admin“ deklarieren, sofern der neue Benutzer administrative Rechte erhalten soll. Dieser Nextcloud-Dialog bietet auch die Einrichtung weiterer Gruppen („+ Gruppe hinzufügen“), jedoch sollte die einfache Standardunterscheidung zwischen Admin-Konten und normalen Benutzerkonten ausreichen. Die neuen Benutzer können später über „Einstellungen → Persönlich“ selbst für deutsche Lokalisierung, für sonstige Konteneigenschaften sorgen und auch ein neues Passwort einrichten. Theoretisch können Sie als Admin die Lokalisierung und Kontoinfos auch vorab (durch Anmeldung in den neuen Konten) eintragen, um den Teilnehmern eine Eingangshürde zu nehmen.



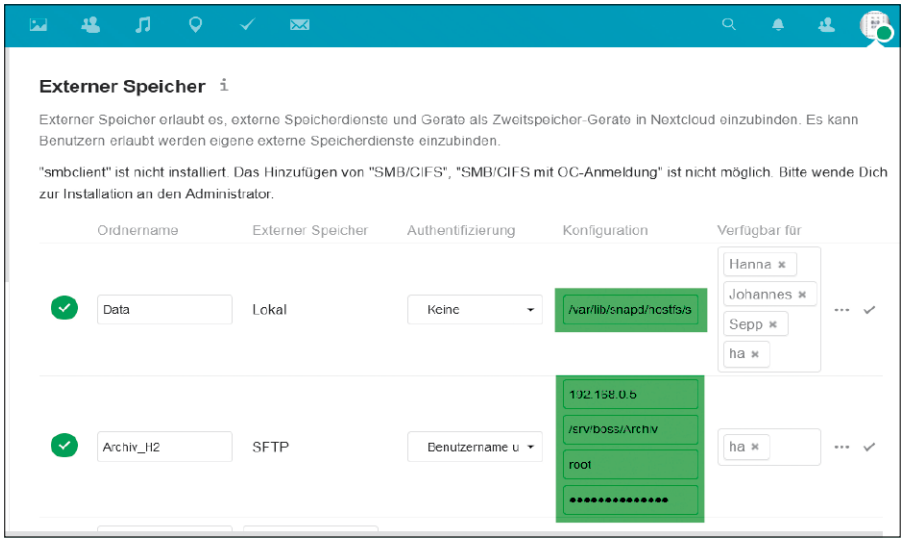
Das Benutzermenü von Admin versus Benutzer: Admins dürfen Apps und Benutzer installieren und ändern. Auch der Umfang der „Einstellungen“ ist beim Benutzer nur „Persönlich“.

Auswahl der gewünschten Apps

Die Nextcloud ist ein modularer Kosmos mit sehr vielen optionalen Plug-ins („Apps“). Es wäre eine Illusion zu glauben, eine neu installierte Nextcloud nach einer Stunde produktiv nutzen zu können. Den Grundstein legt der Administrator über die Auswahl der aktiven Apps. Wird nach Klick auf das Benutzermenü links oben das Menü „+Apps“ gewählt, erscheint ein umfangreiches und relativ unübersichtliches Angebot: „Deine Apps“ listet alle installierten



Nextcloud-Systemmonitor: Diese Infos unter „Einstellungen –› Verwaltung –› System“ sind nur für den Admin zugänglich. Wichtig sind – gerade beim Nextcloud-Snap – die angezeigten Mountpfade.



Wichtige App für andere Apps: „External storage support“ integriert lokale Laufwerke und Netzressourcen und ist damit die Voraussetzung für Multimedia- und Daten-Apps.

– aktive wie inaktive – Module alphabetisch auf, während „Aktive Apps“ und „Deaktivierte Apps“ die installierten Module der Gesamtliste entsprechend filtern. Der Punkt „App-Pakete“ zeigt einige vorgeschlagene App-Bundles, die als Gruppe installiert, aktiviert oder deaktiviert werden können. Die Bundles „Hub-Paket“ und „Groupware-Paket“ sind meistens unentbehrlich, aber auch größtenteils schon vorhanden, wenn Sie bei der Installation das Angebot „Empfohlene Apps“ angenommen haben.

Ein weiterer App-Filter ist der nächste Navigationspunkt „Vorgestellte Apps“. Hier handelt es sich um bewährte Module der Nextcloud-Entwickler, die in technischer Hinsicht allesamt als Empfehlungen gelten können, was aber natürlich noch nichts über ihre inhaltliche Relevanz für eine lokale Intranetlösung aussagt. Was in der Navigation dann darunter folgt, also ab „Anpassung“ abwärts, sind rein inhaltliche Sammlungen: Hier steht dann in einer Kategorie wie „Dateien“ oder „Organisation“ Unentbehrliches neben Wichtigem bis Marginalem oder sehr Speziellem. Technisch ungetestete Apps werden aber ausdrücklich als solche angezeigt und ihre Installation bleibt im Ermessen des Nutzers.

Diverse Versions-, Kommentar- oder Kollaborationsmodule sind im privaten Kontext verzichtbar. Im Zweifel erhalten Sie in der App-Übersicht nach Klick auf den App-Eintrag eine englischsprachige, meistens sehr knappe Beschreibung. Da die Nextcloud die Apps im laufenden Betrieb ein- und ausschalten kann, bedeutet es aber wenig Aufwand, sich von der Notwendigkeit einer Komponente durch einfaches Ausprobieren zu überzeugen. Fast überall zu empfehlen sind in der Regel folgende Module:

- **„Calendar“** (Kalender-App)
- **„Dashboard“** (nicht notwendige, aber hübsche Startseite)
- **„External storage support“** (externe Datenträger und Freigaben)
- **„File Sharing“** (Datenaustausch unter Nextcloud-Benutzern)
- **„Mails“** (kompletter Mailclient)
- **„Music“** (Player und Musikverwaltung)
- **„Notes“** (einfache Notizen)
- **„PDF Viewer“** (PDF-Anzeige)
- **„Photos“** (Bildviewer mit Diashow)
- **„Text“** (einfacher Texteditor)
- **„Video player“** (Medienwiedergabe)

Je mehr von den größeren, serverrelevanten Apps Sie aktivieren (und gegebenenfalls vorher herunterladen), desto mehr füllt sich die Symbolleiste oben neben dem Nextcloud-Logo. Die einzelnen Apps sind dann per Klick auf ihr Symbol erreichbar. Alle Optionen, die sich im linken Navigationsbereich zeigen, beziehen sich immer ausschließlich auf die aktuell gewählte App.

Nextcloud-Apps: Spreu und Weizen

Nach dieser summarischen Auflistung wichtiger Apps stellt sich die Frage, welche Module für eine heimische Cloud sinnvoll und produktiv sind. Im Prinzip genügen schon zwei, drei oder eine Handvoll ausgewählter Apps, um einen Nextcloud-Server zu rechtfertigen. Typische Kollaborationsapps wie „Contacts“ (Kontakte), „Tasks“ (Aufgaben und Termine) und „Talk“ (Textchats und Videochats) sind für eine Intranetcloud weniger relevant. Auch Office-Kollaboration steht hier kaum an vorderster Stelle: „Collabora Online“ bietet zwar Kompatibilität mit Microsoft-Formaten, benötigt aber die Anbindung zu einem externen Server und ist relativ langsam.

Unverzichtbare App „Dateien“: „Dateien“ ist eine nicht mehr abwählbare Standard-App. Über das „+“-Zeichen legen Sie hier neue Ordner an oder laden einzelne oder mehrere Dateien vom lokalen System in die Nextcloud. Auch Drag & Drop vom lokalen Dateimanager in das Dateien-Fenster funktioniert. Selbst wenn die App „Dateien“ nur als Datenhalde für die Teilnehmer dient, ist dies eine bequeme Zentrale, da man sich

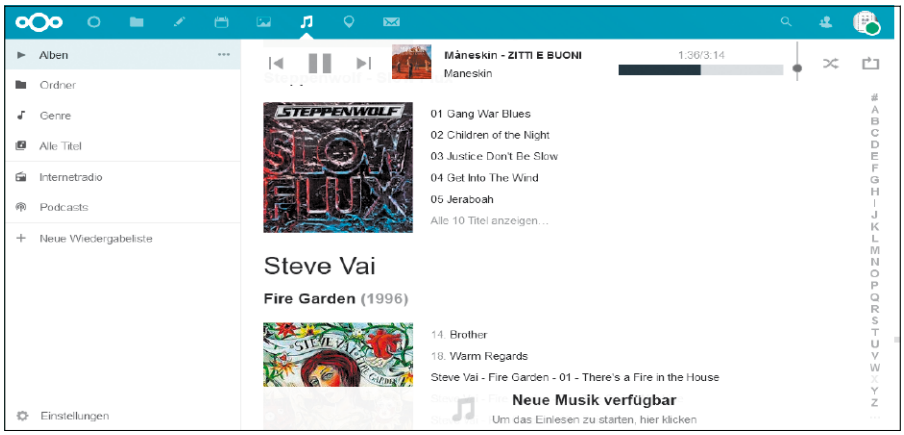
im Unterschied zu einem Samba-Server um die Benutzerrechte nicht kümmern muss. Falls andere Nextcloud-Nutzer Ihre Dateien verwenden oder herunterladen sollen, klicken Sie auf das Teilen-Symbol neben einer Datei oder einem Ordner und tippen dann im Feld unter „Teilen“ den Benutzernamen ein.

„External storage support“: Diese App – deutsch „Externer Speicher“ – erweitert die persönliche Nextcloud-Dateiablage für die Benutzer um einen allgemein zugänglichen Dateibestand. Damit wird die Nextcloud zu einem universellen Datenserver im Netz. Bei dieser App wird gerne die Einbindung von SFTP-Server (SSH), FTP-Server, Amazon, Webdav, SMB/CIFS betont. Weit wichtiger als diese Optionen, die meist schlicht zu langsam sind, ist die Einbindung von Datenträgern, die direkt am Nextcloud-Rechner angeschlossen sind. Auch dies erfordert den „External storage support“.

Die aktivierte Funktion erreichen Sie als Administrator mit „Einstellungen → Verwaltung → Externer Speicher“. Vergeben Sie einen sprechenden Ordnernamen, der später bei allen Benutzern auf oberster Ebene in der „Dateien“-App erscheinen wird. In der Auswahl „Speicher hinzufügen“ wählen Sie „Lokal“ für einen direkt am Nextcloud-Rechner angeschlossenen Datenträger. Als „Ort“ tragen Sie den Mountpunkt des Mediums ein. Bei einer Snap-Nextcloud ist dies allerdings nicht reale Mountordner, sondern ein umgeleiteter unter „/var/lib/snapd/hostfs/...“. Den richtigen Pfad finden Sie am einfachsten unter „Verwaltung → System → Festplatte“.

Die App „Externer Speicher“ eignet sich auch hervorragend zum Zusammenführen von verteilten Netzressourcen. So sind etwa Linux-Rechner mit SSH-Server schnell im Dateien-Bereich der Nextcloud eingetragen. Statt „Lokal“ wählen Sie hier „SFTP“, als „Authentifizierung“ die Option „Benutzername und Passwort“ und als „Konfiguration“ tragen Sie die IP-Adresse ein (gegebenenfalls mit Portangabe – etwa 192.168.0.178.20:2222), darunter den Mountpunkt der benötigten Ressource, ferner SSH-Benutzer (!) und dessen Kennwort. Welche Nextcloud-Benutzer auf einen externen Speicher zugreifen dürfen, lässt sich exakt einstellen. Eventuell ist es sinnvoll, die Freigabe generell schreibgeschützt zu setzen.

„Music“ – ein vollständiger Audioserver: Als Audiowiedergabe konkurrieren mehrere Nextcloud-Apps. Die App „Music“ bietet neben der Wiedergabe eine Medienverwaltung und berücksichtigt auch die Metadaten. „Music“ darf den Rang eines zwar schlichten, aber kompletten Medienservers beanspruchen. Neu eingebundene Nextcloud-Ressourcen („Externer Speicher“) können erfasst werden, sobald sie in der App unter „Ordner“ auftauchen: Dann erscheint im Hauptfenster unten „Neue Musik verfügbar“ und ein Klick darauf startet den Medienscan. Dieser kann durch einen App-Wechsel jederzeit unterbrochen und später fortgesetzt werden. Dies ist vorbildlich, weil somit die Nextcloud nicht durch langwierige Scans dauerhaft ausgebremst wird. Einmal eingelesene Songs sind über „Alben“, „Genre“ oder „Titel“ erreichbar.



„Musik“ als Beispiel einer Nextcloud-App: Der Navigationsbereich links sowie die dortigen „Einstellungen“ beziehen sich immer ausschließlich auf die aktuell gewählte App.

Die „Mail“-App: Allein der Nextcloud-Mailclient kann ein ausreichender Grund für eine Nextcloud sein. Statt nämlich auf diversen Rechnern je einen Mailclient à la Thunderbird oder Outlook zu verwenden, können alle Nextcloud-Nutzer ihre Mails im Browser via Nextcloud abfragen. Das Nextcloud-Modul ist ansehnlich und verwaltet für jeden Nutzer mehrere Mailkonten (im Navigationsbereich „Einstellungen → E-Mail-Konto hinzufügen“). In der Regel genügen zum Einrichten die Mailadresse und das Zugangskennwort. Mobile Geräte sollten aber weiterhin ihr eigenes Mailprogramm behalten, um auch außerhalb des lokalen Netzes Nachrichten zu empfangen.

„Photos“ und „Notes“: „Notes“ bietet einfache Notizen mit inhaltlichen Kategorien. Letztere sind über das unscheinbare „...“-Menü (rechts oben) über „Details“ zu vergeben. Die App speichert die Notizen einfach im Klartext ab und sortiert sie dabei in Ordner mit den Namen der Kategorien. Die Foto-App ist ebenfalls einfach, erkennt bei angeklickten Ordnern enthaltene Bilddateien und zeigt diese als Thumbnail-Vorschau. Beim Klick erscheint das Einzelbild und erlaubt Blättern oder automatische Diaschau. Eine Bearbeitung ist nicht möglich.

Hübsche optionale Ergänzungen: „Maps“ („Karten“) integriert Openstreetmap-Karten in die Nextcloud und ermöglicht dort individuelle Einträge mit Ortsfavoriten, Fotos und Strecken.

Der „EPUB/CBZ/PDF ebook reader“ ergänzt den auf PDFs beschränkten „PDF-Viewer“ um weitere Formate.

„External Sites“ – nicht zu verwechseln mit „External storage“ – ist eine unscheinbare Funktion, um URLs aus dem Intranet oder dem Internet in Nextcloud zu integrieren. Das ist ein netter Service für unbedarfte Nextcloud-Nutzer, die ihrem Browser keine Lesezeichen beibringen können. Die über „Einstellungen → Verwaltung → Externe Seiten“ erreichbare Funktion kann beliebige Adressen in das Benutzermenü aufnehmen (Position „Einstellungsmenü“). Als Symbol im „Kopfbereich“ (also quasi als App) ist nur für eine einzige externe Seite sinnvoll, weil das Symbol nicht beschriftet ist.

Zahlreiche winzige Apps bringen keine Serverfunktionen, erhöhen aber den Bedienkomfort. „Right Click“ ist selbsterklärend und vorinstallierter Standard. Das optionale „AppOrder“ kann die Reihenfolge der angezeigten Apps in der Symbolleiste oben nach Wunsch anpassen. Auch solche kleine Apps sind über „Einstellungen → Verwaltung“ (oder „Einstellungen → Persönlich“) zu konfigurieren. ■

Fritzbox-Geheimnisse

In der Fritzbox steckt mehr, aber auch weniger, als Sie vermuten. Die folgenden Tipps haben Interna und Optionen im Fokus, die auch bei souveräner Nutzung der Routerkonfiguration nicht auf der Hand liegen.

VON HERMANN APFELBÖCK

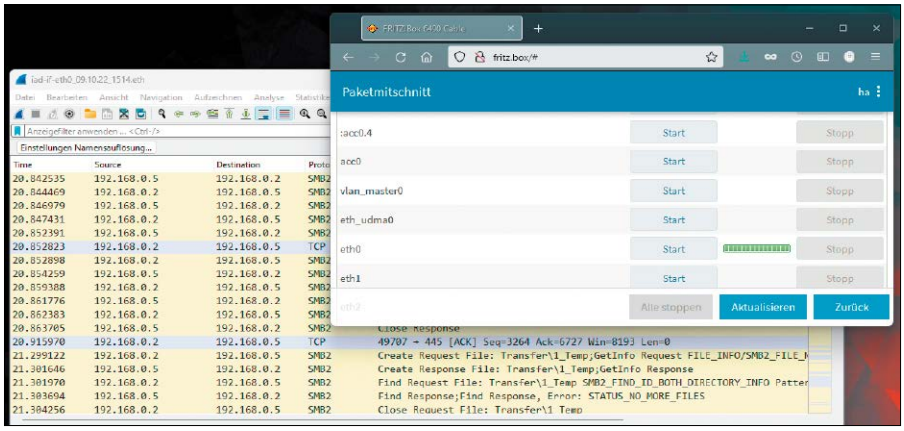
Dieser Artikel richtet sich an Nutzer, welche die Fritzbox-Oberfläche nicht zum ersten Mal öffnen. Dennoch hier der unvermeidliche Hinweis für Anfänger: Die Konfiguration erreichen Sie mit jedem Browser, der sich im selben Netz befindet. Verwenden Sie entweder den Hostnamen *http://fritz.box* oder die Adresse *http://192.168.178.1* (falls Sie den Standardadressraum nicht angepasst haben).

Das Geheimnis der Kernhardware

Bei kleinen, stromsparenden Geräten mit Embedded Systems ist es üblich, über die Kernhardware (CPU und RAM) den Mantel des Schweigens zu breiten. NAS und Router machen da keine Ausnahme – und die Fritzbox auch nicht. Hersteller AVM stellt WLAN-Leistung, Gigabit-LAN-Switch, USB 3.0-Ports oder Fritz-OS-Funktionen ins Rampenlicht, aber nirgends CPU und RAM. Die Site *https://boxmatrix.info*, deren Zuverlässigkeit wir anhand von Stichproben bestätigen können, nennt für die meisten Modelle 512 MB RAM, zum Teil noch weniger, ganz selten ein ein GB oder mehr (Fritzbox Cable 6690). Als Prozessoren arbeiten in älteren Modellen ARM-CPUs, in jüngeren kleine Intel-CPUs mit einem, meist zwei Kernen, die typischerweise mit einem GHz takten, oft weniger, sehr selten mehr. Damit liegt die Leistung einer Fritzbox weit unter der eines Raspberry Pi. Andererseits spricht die Fünf-Jahres-Garantie dafür, dass AVM weiß, was diese Hardware im Dauerbetrieb aushält. Das liegt aber nicht zuletzt daran, dass 95 Prozent der Nutzer gar nicht auf die Idee kommen, optionale Funktionen des Routers zu aktivieren.

Praktische Konsequenzen? Handauflegen oder ein Kontrollblick unter „System → Energiemonitor → Statistik“ kann bei intensivem Fritzbox-Einsatz nicht schaden. Handwarm ist ein Router immer, falls er dauerhaft heiß läuft, ist Zurückhaltung zu empfehlen:

- Als Medienserver („Heimnetz → Mediaserver“) ist die Fritzbox schlicht unterdimensioniert.
- Als NAS-Server („Heimnetz → USB/Speicher“) kommt die Fritzbox nur dann ernsthaft in Betracht, wenn USB 3.0 vorliegt. Das ist nicht bei allen Modellen der Fall. Für die NAS-Funktion sorgt ein kleiner Samba-Server, der die Hardware im Homeoffice- oder Familienumfeld nicht überfordern sollte.
- Wer die DECT-Leistung verringert („Telefonie → DECT → DECT-Funkleistung verringern“ und „DECT Eco“), senkt die Gerätetemperatur – nach unserer Erfahrung ohne Reichweitenprobleme.
- Das Funknetz kann man nachts komplett abschalten („WLAN → Zeitschaltung“).
- LAN-Ports mit langsamen Clients und kaum genutzte USB 3.0-Anschlüsse lassen sich auf einen langsameren „Green Mode“ schalten („Heimnetz → Netzwerk → Netzwerkeinstellungen“).
- An der Fritzbox angeschlossene TV-Receiver, die permanent aufzeichnen (absichtlich oder versehentlich), machen die Fritzbox zum Heizkörper. Kontrollieren Sie die Receivereinstellungen.



Wireshark-Paketmitschnitte: Das muss man wollen, können – und erst mal finden. Die Fritzbox-Oberfläche bietet diese Option standardmäßig nicht an.

Mitschnitt, Leistungsmessung und Support

Einige Optionen sind in der Fritzbox-Konfiguration fast unauffindbar versteckt. Unterhalb der linken Navigationsspalte finden Sie Links wie „Ansicht“, „Inhalt“, „Handbuch“. Der Punkt „Inhalt“ führt zu einer Sitemap der gesamten Oberfläche und darunter finden Sie den Link „Fritz!Box Support“ (die Seite lässt sich auch direkt aufrufen mit *http://fritz.box/html/support.html*). Auf dieser Support-seite gibt es zwei interessante Optionen:

„Paketmitschnitt“ (hierzu führt auch die Abkürzung *http://fritz.box/html/capture.html*): Mit Start und Stop schneiden Sie hier den Internetverkehr gesamt, nur jenen über Ethernet oder auch nur jenen via WLAN mit. Auch der LAN-Verkehr im Heimnetz ist insgesamt („lan“) zu protokollieren – oder auf einen LAN-Port (der Fritzbox) begrenzt („eth0“, „eth1“…) oder zusätzlich noch auf eine IP gefiltert. Das Protokoll ist allerdings nicht direkt lesbar, sondern

muss in Wireshark geladen werden. Wireshark gibt es in allen Linux-Distributionen in den Standard-Paketquellen, für andere Betriebssysteme unter *www.wireshark.org*. Der Fritzbox-Mitschnitt kann hier über „Datei → Öffnen“ geladen werden. Es erfordert gute Netzwerkkenntnisse und Erfahrung mit Wireshark-Filtern (unterhalb der Werkzeugleiste), um aus dem enormen Datenwust die relevanten Infos zu ermitteln. So kann etwa der Filter „http“ Webanfragen filtern oder „ip.addr == 192.168.0.13“ die Datenmenge auf ein einziges Gerät einschränken.

„Durchsatzmessungen“: Auf Smartphones und Tablets wird man zur übersichtlichen „Fritz!App WLAN“ greifen, um die WLAN-Leistung zu messen. Anders liegt der Fall bei PCs und Notebooks. Hier kann das bewährte Iperf genutzt werden. Auf der Fritzbox-Supportseite aktivieren Sie unter „Durchsatzmessungen” die Option „Messpunkt für einen Iperf-Client [...] aktivieren“ und bestätigen mit „Einstellung übernehmen“. Das startet den Serverteil der Iperf-Messung. Auf dem Linux-System benötigen Sie ebenfalls das Paket „iperf“, das in allen Paketquellen vorliegt. Die Geschwindigkeit messen Sie dann unter Linux im Terminal:

```
iperf -c [Fritzbox-IP]
```

Schalter „-c“ bedeutet, dass Iperf als Client gestartet wird, und die Fritzbox-IP verweist auf die Serverkomponente. Iperf sendet und empfängt dann zehn Sekunden lang Daten und zeigt anschließend das Ergebnis.

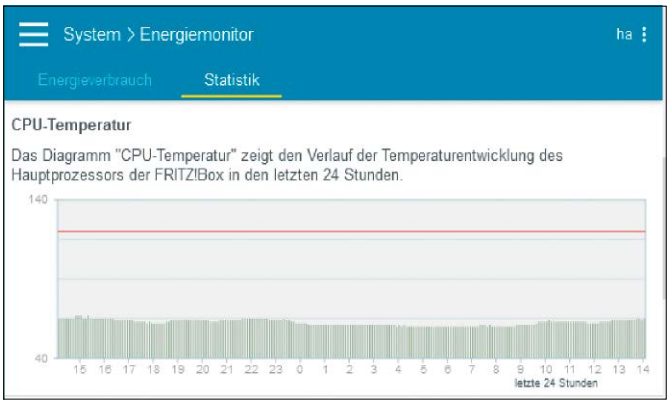
Notfall-IP der Fritzbox

Sollte eine Fritzbox über *http://fritz.box* nicht mehr erreichbar sein, etwa weil Sie eine falsche IP-Adresse eingestellt haben, dann hilft der eingebaute Notzugang. Die Konfiguration lässt sich immer auch über die Adresse 169.254.1.1 aufrufen. Hier können Sie dann Konfigurationsfehler manuell beheben (einschlägig: „Heimnetz → Heimnetzübersicht → Netzwerkeinstellungen“ und „Internet → Freigaben“ und „Internet → Filter“). Schlimmstenfalls kann die Box unter „System → Sicherung → Werkseinstellungen“ komplett zurückgesetzt werden.

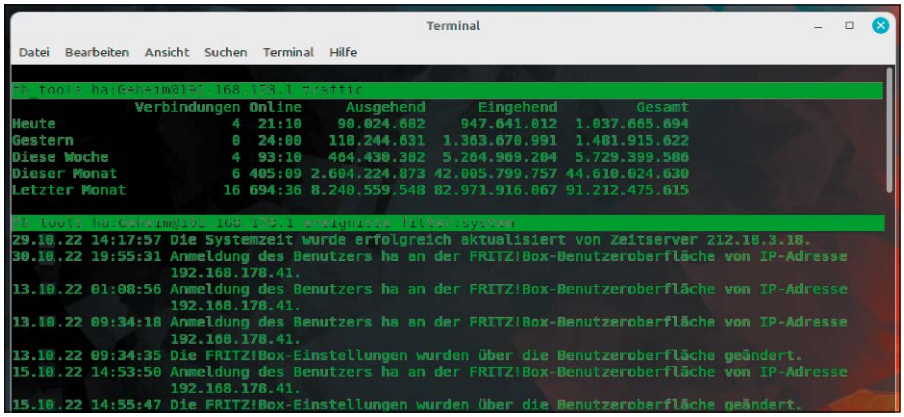
Notbetrieb bei Providerstörung

Die Fritzbox bietet über USB die Möglichkeit, einen LTE-Stick anzuschließen und damit online zu gehen. Unter „Internet → Mobilfunk“ erscheint dann die zusätzliche Option „Mobilfunkverbindung automatisch aktivieren, wenn die DSL-Verbindung unterbrochen wird“. Der Mobilfunk springt automatisch ein, wenn DSL ausfällt.

Ohne LTE-Stick können Smartphones aushelfen. Verbinden Sie das Handy per USB mit der Fritzbox. Auf dem Smartphone aktivieren Sie einen Punkt wie „Drahtlos & Netzwerke → Tethering & mobiler Hotspot → USB-Tethering“ (oder ähnlich lautend). Auch jetzt bietet die Fritzbox unter „Internet” den Eintrag „Mobilfunk“. Aktivieren Sie dort den Eintrag „Internetzugang über Smartphone oder USB-Tethering“. Danach kommen alle Geräte über die Fritzbox ins Internet – mit vermutlich geringer Bandbreite allerdings.



Wie geht's der Fritzbox? Die Grafik unter „System –› Energiemonitor –› Statistik“ gibt Auskunft und liegt hier entspannt weit unter der kritischen roten Linie.



PHP-Fritzbox-Tools: Der Einblick in das Systemprotokoll oder in die Trafficstatistik („Online-Zähler“) gehört zu den einfacheren Kommandos der Fritzbox-Tools.

Fritzbox per Kommandozeile

Die fb_tools (Fritzbox-Tools) sind eine Sammlung von PHP-Scripts zur Steuerung der Fritzbox über Terminalbefehle. Die Tools können – mit einigen wenigen Ausnahmen – nicht mehr als das, was ein Fritzbox-Nutzer auf der Konfigurationsoberfläche erledigt. Aber man kann damit von außen Infos auslesen und Funktionen starten. Da PHP unter Linux vorliegt, genügt für Debian/Ubuntu & Co. der Download des DEB-Pakets „fb-tools.deb“ von *www.mengelke.de/Projekte/FritzBox-Tools* und die Installation im Terminal:

```
sudo dpkg -i fb-tools.deb
```

Einige einfache Befehle funktionieren ohne Anmeldung:

```
fb_tools systemstatus
fb_tools getip
```

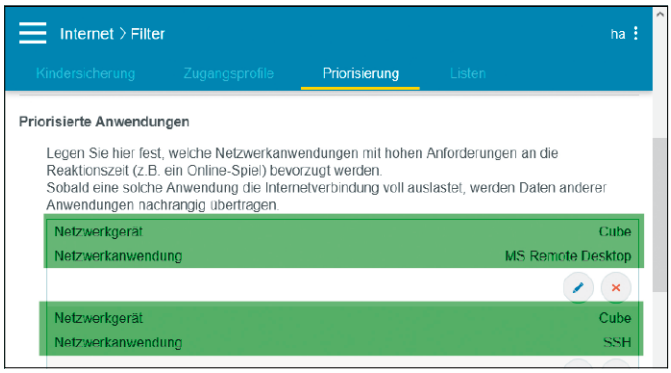
Damit erhalten Sie die Basisdaten über Laufzeit, Neustarts und die öffentliche IP-Adresse. Weitere Funktionen setzen aber eine Anmeldung voraus, die dem eigentlichen Befehl mitgegeben wird:

```
fb_tools sepp:Geh3im@fritz.box
  anrufliste
```

Mit dieser Anmeldesyntax sind aber immer noch nicht sämtliche Funktionen realisierbar. Ursache dafür ist die Fritzbox-Option „System → Fritz!Box-Benutzer → Zusätzliche Bestätigung → Ausführung [...]zusätzlich bestätigen“. Es ist Ermessensfrage, ob man dies dauerhaft abschalten will. Danach sind etwa folgende Aktionen möglich:

```
fb_tools [...] traffic
```

Der Mode „traffic“ gibt die Daten aus, die in der Konfigurationsoberfläche unter „Inter-



Priorisierung: Das Gerät „Cube“ erhält hier für zwei bestimmte Netzanwendungen Vorrang.

net → Online-Monitor → Online-Zähler“ zu finden sind, und dieses Kommando

```
fb_tools […] reconnect
```

macht eine Neuverbindung zum Provider.

Priorisierung von Geräten

Standardmäßig darf jedes Gerät im Netzwerk die volle Bandbreite beanspruchen. Das ist überall, wo es konfliktfrei funktioniert, der einfachste Zustand. Wenn aber der Arbeits-PC gebremst wird, weil auf Tablets Youtube-Videos laufen, kann die Fritzbox helfen: Der Punkt lautet „Internet → Filter → Priorisierung“. Über „Neue Regel“ unter „Priorisierte Anwendungen“ geben Sie das Gerät an, das ungebremst arbeiten soll. Der Vorrang kann auf eine bestimmte Anwendung wie etwa SSH beschränkt werden oder für den privilegierten Rechner global gelten („alle“ unter „Netzwerkanwendungen“). Am zielgenauesten ist eine Priorisierung für wichtige Anwendungen auf einem wichtigen Gerät: Nach „Neue Regel“ muss dann das Gerät und danach eine Netzwerkanwendung wie „SSH“ oder „MS Remote Desktop“ gewählt werden. Durch mehrere Regeln lassen sich auch mehrere Anwendungen auf einem Gerät priorisieren, aber eben nicht blindlings alle.

Die für eine Priorisierung angebotenen „Netzwerkanwendungen“ können über „Internet → Filter → Listen” manuell erweitert werden. Nach dem Klick auf „Netzwerkanwendung hinzufügen” legen Sie einen neuen Eintrag ein, beispielsweise für ein Onlinespiel. Darunter müssen Sie allerdings die Protokolle und Ports wissen. Die können Sie entweder individuell recherchieren oder auf der umfassenden Site *https://portforward.com/ports.htm*) nachlesen. ■

KLEINE FRITZBOX-GIMMICKS

Genaue Systemversion ermitteln

Unter „Übersicht“ zeigt die Fritzbox nur die grobe Fritz-OS-Version. Wer es genau wissen will, kann mit der Adresse *http://fritz.box/jason_boxinfo.xml* die exakte Revision ermitteln. Die Ausgabe zeigt noch etwas mehr, so etwa die Seriennummer der Fritzbox. Die im Haupttext genannten Fritzbox-Tools übertreffen die Infos dieser internen Adresse aber deutlich.

Variable Netzwerkinfos



„Heimnetz → Netzwerk“ ist vermutlich eine der meistbesuchten Seiten der Fritzbox-Konfiguration. Der unscheinbare Knopf „+/-“ rechts oben dürfte aber den meisten Nutzern entgehen: Damit können Sie Infospalten ein- oder ausblenden. Die Info zur MAC-Adresse der Netzgeräte ist standardmäßig inaktiv.

Individuelle Klingeltöne

Gleich am Klingelton zu hören, ob der Anruf(er) wichtig oder lästig ist, ist vielleicht Schnickschnack, aber durchaus informativ. Die Fritzbox zeigt unter „Telefonie → Telefoniegeräte → Geräteübersicht“ bei „Mobilteil 1“ (kann variieren) ein Stiftsymbol („Bearbeiten“) und hier die „Klingeltöne“. Auf dieser Seite können Sie maximal fünf MP3-Dateien vom PC auf den Fritzbox-Speicher laden. Das Zuweisen der Audiodateien zu den gewünschten Rufnummern geschieht auf dem Fritzfon. Im „Telefonbuch“ gehen Sie zum gewünschten Kontakt. Über „Optionen → Ändern“ finden Sie an unterster Stelle „AVM Klingelton“ und darunter „Fritz!Box Einstellung“. Hier erscheinen dann die gespeicherten MP3-Dateien, und die gewünschte weisen Sie dem Kontakt zu.

(Un-)freundliche WLAN-Koexistenz

Standardmäßig ist unter „WLAN → Funkkanal“ die Option „Funkkanal-Einstellungen automatisch setzen“ aktiv. Das sollte fast immer einen zuverlässigen Betrieb garantieren. Wer sich kompetent fühlt, die besten Funkkanäle für die 2,4- und 5-GHz-Frequenzen selbst zu ermitteln, kann die „Funkkanal-Einstellungen anpassen“. Hier gibt es außerdem unter „Weitere Einstellungen“ die Default-Option „WLAN-Koexistenz aktiv“. Wenn Sie diese abschalten, funkt Ihr WLAN ohne Rücksicht auf Funknetze der Nachbarn im gleichen Frequenzbereich. Damit wird Ihr WLAN zwar kein destruktiver Jammer, aber doch tendenziell unfreundlich.

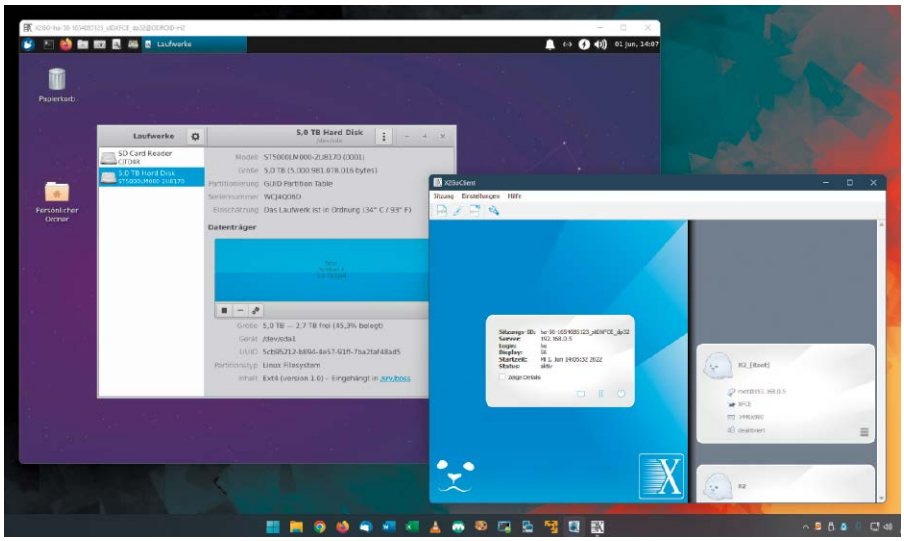
TV-Kabelsender live streamen

Eine Cable-Fritzbox kann das Fernsehbild per WLAN oder Ethernet streamen. Für die Wiedergabe eignet sich der VLC-Player, den es für jedes Gerät gibt. Auf mobilen Geräten benötigen Sie zusätzlich die App „Fritz!App TV” aus dem App Store. Einmal installiert sollte die App die Fritzbox automatisch finden, und dann kann das Smartphone oder Tablet fernsehen.

Am PC stellen Sie dem VLC die Senderliste zur Verfügung, welche die Fritzbox unter „DVB-C → Senderleiste“ (zwei Listen für SD- und HD-Qualität) anzeigt und mit „Senderliste erzeugen” als Datei exportiert. Diese Datei ziehen Sie einfach in das VLC-Fenster. Nach Doppelklick auf den gewünschten Sender beginnt der Player die Wiedergabe.

Remotedesktop mit X2go

Dieser Beitrag ist in erster Linie eine Empfehlung, weniger ein technischer Ratgeber. Die Benutzung des hier empfohlenen Remotetools X2go ist nämlich auch für Einsteiger keine Herausforderung.



Ein Windows, ein Remoteserver und dazwischen X2go: Dieses Remotedesktop-Tool ist wackeligen und hakeligen VNC-Lösungen eindeutig vorzuziehen.

VON HERMANN APFELBÖCK

Die Open-Source-Software X2go (*https://wiki.x2go.org*) ermöglicht den Fernzugriff auf den Desktop eines anderen Linux-Systems. Die Serverkomponente lässt sich nur unter Linux installieren, Zugriffsclients gibt es hingegen außer für Linux auch für Windows und Mac-OS.

Nehmen wir es vorweg: X2go ist nicht mit jedem Linux-Desktop kompatibel. Außerdem ist das Remotetool verglichen mit VNC-Lösungen oder gar SSH ein eher schwerer Brocken sowohl bei der Server- wie bei der Clientkomponente. Der Aufbau der entfernten grafischen Oberfläche ist immer etwas zäh. Alle diese Einschränkungen nimmt man aber bereitwillig in Kauf: Denn X2go funktioniert einfach gut:

- Da X2go intern auf SSH aufbaut, muss man sich keine zusätzliche Zugangsverwaltung aneignen. Auf dem „Server" müssen nur X2go und der Open-SSH-Server laufen.
- Sobald X2go die entfernte Oberfläche angeboten hat, erfolgt die Bedienung jederzeit mit alltagstauglicher Geschwindigkeit.
- Der Remotedesktop ist ungeachtet der in der X2go-Konfiguration angegebenen Auflösung später beliebig skalierbar.
- X2go kümmert sich um Maus, Tastatur, Sound, Drucken und Datenaustausch.

Kompatible Desktops und Installation

Obwohl die X2go-Clientkomponente so gut wie alle Linux-Desktops in ihrer Konfiguration anbietet, gelten derzeit nur XFCE, LXDE, Mate und Openbox als vollständig kompatibel.

Die X2go-Serverkomponente muss auf dem „Server"-System installiert werden. Sie ist mittlerweile in den meisten Repositorys direkt erhältlich, daher genügt zur Installation folgender Befehl:

```
sudo apt install x2goserver
  x2goserver-xsession
```

Wer unter Ubuntu & Co. die neueste Version nutzen will, kann das Servertool auch aus seinem PPA beziehen:

```
sudo add-apt-repository ppa:x2go/
  stable
sudo apt update
sudo apt install x2goserver
  x2goserver-xsession
```

Der Server wird dabei automatisch und dauerhaft als Systemdienst „x2goserver" eingerichtet.

Die X2go-Clientkomponente installieren Sie dann auf allen Systemen, die auf den Server zugreifen sollen. Unter Debian/Ubuntu kann dies mit

```
sudo apt install x2goclient
```

aus den Standardquellen erfolgen. Clientsoftware für Windows- und Mac-Systeme gibt es auf *https://wiki.x2go.org* unter „Download" (mswin, OS X), die Sie dort wie gewohnt installieren.

Verbindungen herstellen

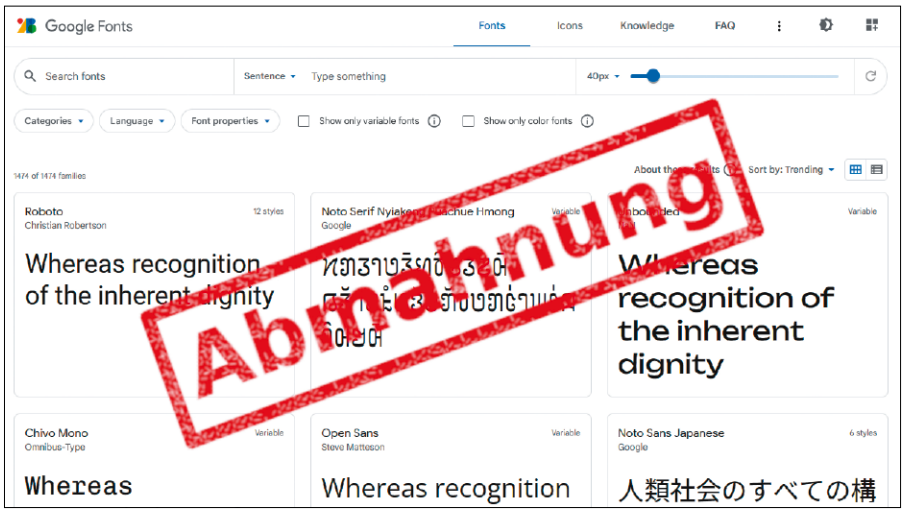
Ähnlich bekannten SSH- oder VNC-Tools speichert der X2go-Client die einmal eingestellte Konfiguration eines Servers, sodass später der Doppelklick auf den Eintrag genügt. Natürlich sind mehrere Servereinträge möglich, aktiv genutzt werden kann aber nur jeweils einer.

Starten Sie den Client. Mit „Sitzung → Neue Sitzung" legen Sie den ersten Server an. Vergeben Sie hinter „Sitzungsname" eine Bezeichnung, die den Rechner klar identifiziert – etwa „Raspberry4". Neben „Host:" tragen Sie die IP-Adresse des Servers ein. Wie immer in solchen Fällen sollte die IP-Adresse statisch feststehen (was Sie bei Bedarf im Heimrouter festlegen). Hinter „Login" geben Sie das Systemkonto am Serversystem ein und neben „SSH-Port" die Portnummer, falls sie vom Standard „22" abweicht. Unter „Sitzungsart" wählen Sie idealerweise „XFCE" – sofern zutreffend. Am Ende klicken Sie auf „OK", um die Einstellungen zu speichern. ■

Abmahnungen wegen Google-Fonts

Man sollte die eigene Website prüfen, bevor ein Schreiben vom Anwalt im Postkasten liegt. Zur Zeit werden vermehrt Abmahnungen verschickt, die den Download von Google-Fonts bemängeln.

VON THORSTEN EGGELING



Google bietet kostenlose Schriftarten für Websites an. Wenn diese ohne Zustimmung des Besuchers von Google-Servern geladen werden, kann das rechtliche Folgen haben.

Verstößt der Betreiber einer Website gegen geltendes Recht, kann das juristische Konsequenzen haben. Seit einiger Zeit mehren sich Meldungen über Abmahnungen, die neben der Unterlassung auch Schadenersatz fordern. Dabei wird die Einbindung von Google-Fonts abgemahnt, welche die IP-Adresse eines Besuchers an das US-Unternehmen übermitteln. Um solchen Ärger zu vermeiden, sollten Sie Google-Fonts rechtssicher in Ihre Website einbauen.

Was sind Google-Fonts?

Mit geeigneten Schriftarten lässt sich die Darstellung von Text auf Webseiten deutlich verbessern. Der Browser lädt die Fonts aus dem Internet und verwendet sie statt der auf dem Rechner installierten Schriftarten. Google stellt für diesen Zweck zahlreiche Schriftarten unter einer Open-Source-Lizenz kostenlos bereit (*https://fonts.google.com*). Die Einbindung in eine Website erfolgt dann über eine CSS-Datei etwa so:

```
<link rel='stylesheet' id='google-
  web-fonts-css' href='//fonts.
  googleapis.com/css?family=Open+S
  ans%3Aregular%7COpen+Sans%3A700&
  #038;ver=1.1.6' type='text/css'
  media='all' />
```

In der CSS-Datei sind Download-URLs für die Fonts enthalten (Beispiel):

```
src: url(http://fonts.gstatic.com
  /s/opensans/v34/memvYaGs126MiZpBA
  UvWbX2vVnXBbObj2OVTS-muw.woff2)
  format('woff2');
```

Die Downloads erfordern zusätzliche Bandbreite, wodurch sich der Aufbau von Webseiten verlangsamt. CSS-Dateien und Fonts lädt der Browser allerdings in seinen Cache. Ein erneuter Download ist später in der Regel nicht erforderlich. In älteren Browsern (vor 2020) wurden identische Google-Fonts auch beim Besuch anderer Websites aus dem Cache geladen. Aus Sicherheitsgründen wird das nicht mehr unterstützt. Der Vorteil einer zentralen Bevorratung in einem CDN (Content Delivery Network) entfällt und man kann die Fonts daher auch vom eigenen Server ausliefern.

Eigene Webseiten prüfen: Ob in Ihrer Internetpräsenz Google-Fonts zum Einsatz kommen, finden Sie im Browser heraus. Nach einem rechten Mausklick in die Seite wählen Sie in Firefox „Seitenquelltext anzeigen“. Suchen Sie (mit Strg-F) im Quelltext nach „google“ und „gstatic“. Wenn CSS-Dateien oder Fonts von Google geladen werden, finden Sie im Quellcode entsprechende Verweise. Etwas genauer geht es mit den Entwicklerwerkzeugen, die sich über den Kontextmenüpunkt „Untersuchen“ einblenden lassen. Gehen Sie auf „Netzwerkanalyse“, setzen Sie ein Häkchen vor „Cache deaktivieren“ und laden Sie die Webseite über Strg-R neu. Klicken Sie auf „Schriften“. In der Spalte „Host“ sehen Sie, woher die eingebundenen Schriftarten stammen. Sollte es sich nicht um Ihre eigene Domain handeln, sollten Sie Maßnahmen ergreifen. Prüfen Sie nicht nur die Startseite, sondern auch Unterseiten.

Über *https://www.e-recht24.de/google-fonts-scanner* können Sie Ihre Website zusätzlich prüfen und erhalten dabei weiterführende Informationen zur Rechtslage.

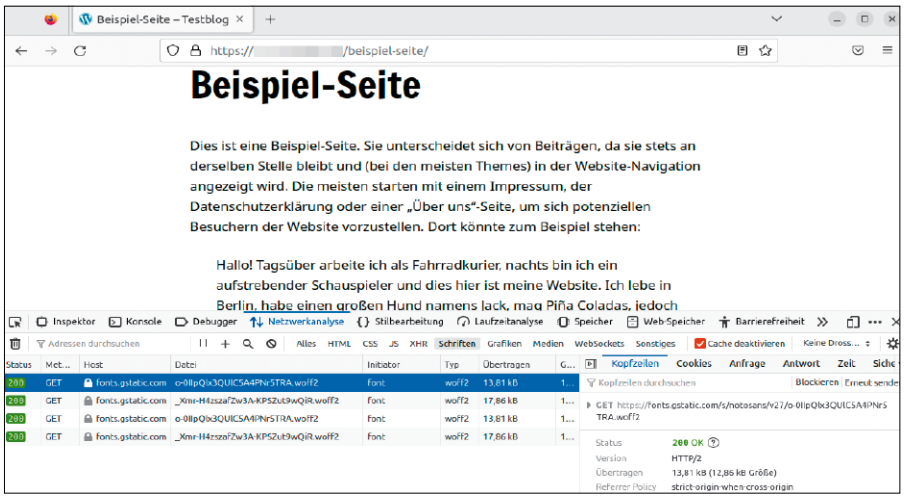
Rechtliche Probleme mit fremden Inhalten

Bei jedem Aufruf einer Webseite oder beim Download erfährt der Webserver die IP-Adresse des Besuchers. Dabei handelt es

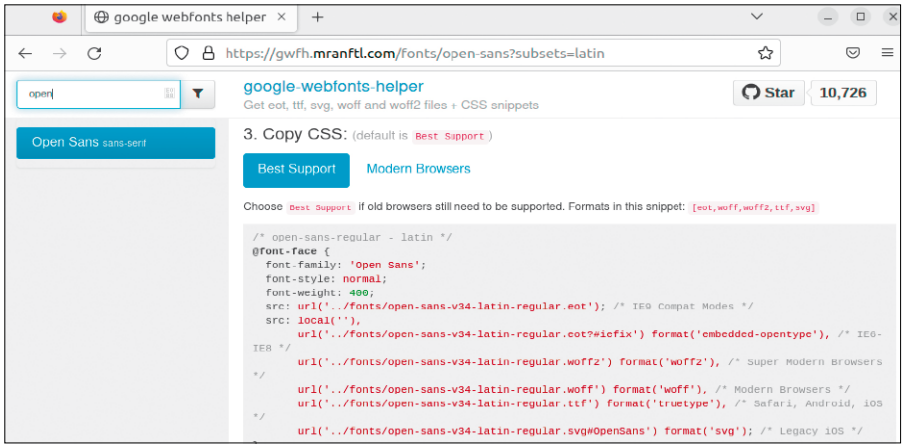
sich laut DSGVO (*https://dsgvo-gesetz.de*) um personenbezogene Daten, weil sich mit der IP-Adresse die Identität des Besuchers ermitteln lässt. Ein Webserver darf diese Daten nur so lange sammeln, wie es technisch notwendig ist. In den Logdateien beispielsweise müssen die IP-Adressen pseudonymisiert werden, damit keine Rückschlüsse auf die Identität des Besuchers möglich sind. Wenn Sie den Webserver nicht selbst betreiben, also keinen vollen Zugriff auf dessen Konfiguration haben, muss der Webhoster nach Artikel 28 DSGVO für die Einhaltung der rechtlichen Bestimmungen sorgen. Der Hoster bietet Ihnen dafür eine Vereinbarung zur Auftragsverarbeitung an.
Sobald Sie fremde Dienste in Ihre Webseiten einbinden, werden die Inhalte von anderen Webservern abgerufen, die ebenfalls die IP-Adresse des Besuchers erfahren. Das gilt für Google-Fonts, Google-Adsense, Youtube, Twitter, Facebook und viele andere. Es gilt als rechtssicher, wenn Sie bei jedem externen Inhalt nach der Einwilligung des Besuchers Ihrer Webseiten fragen („Opt-in“). Teilweise kann auch eine Information in der Datenschutzerklärung reichen sowie die Möglichkeit, externe Inhalte generell abzuwählen („Opt-out“). Wirkungsvoll ist außerdem ein Fenster, das vor Aufruf der Website erscheint, in dem Sie die Zustimmung zu Cookies sowie zur Datenschutzerklärung und allen darin genannten Funktionen einholen.
Auch für externe Dienste ist eine Vereinbarung zur Auftragsverarbeitung beim jeweiligen Anbieter erforderlich. Für Werbeeinblendungen über Adsense stellt Google die nötigen Erklärungen und DSGVO-Mitteilungen bereit, für Google-Fonts bisher aber nicht. Unter *https://developers.google.com/fonts/faq/privacy* heißt es lediglich, dass Google IP-Adressen nicht speichert und nicht analysiert.

Abmahnungen wegen Google-Fonts vermeiden

In den bisher bekannt gewordenen Abmahnungen geht es um eine Forderung auf Unterlassung, die eher als unstrittig gelten kann. Dazu wird ein Schadenersatz in Höhe von 140 bis 170 Euro gefordert, teilweise zuzüglich Anwaltsgebühren, was dann mehr als 200 Euro ergibt.
Die Abmahner könnten Ihre Forderungen mit dem Urteil des LG München vom 20.01.2022 (Aktenzeichen: 3 O 17493/20, *https://m6u.de/LGMU*) begründen. Darin wurde der Beklagte zu einem Schadenersatz von 100 Euro verurteilt. Im Urteil heißt es zum Abruf der Google-Fonts: „Die Übermittlung der IP-Adresse, erfolgte damit nicht nur einmalig. Der damit verbundene Eingriff in das allgemeine Persönlichkeitsrecht ist im Hinblick auf den Kontrollverlust des Klägers über ein personenbezogenes Datum an Google, ein Unternehmen, das bekanntermaßen Daten über seine Nutzer sammelt und das damit vom Kläger empfundene individuelle Unwohlsein so erheblich, dass ein Schadensersatzanspruch gerechtfertigt ist.“.
Wer eine Abmahnung erhält, kann die Forderung entweder begleichen oder sich (bevorzugt) anwaltlichen Rat suchen. Zur Zeit ist noch nicht ausreichend geklärt, ob Massenabmahnungen sich tatsächlich auf „individuelles Unwohlsein“ berufen können.



Webseiten prüfen: Ob Fonts von Google eingebunden sind, lässt sich im Browser mit den Entwicklertools herausfinden. Unter „Host“ erscheint dann „fonts.gstatic.com“ oder ähnlich.



Fonts lokal hosten: Google-Webfonts-Helper liefert den CSS-Code für die Einbindung von Schriftarten und bietet Fontdateien in passenden Formaten zum Download an.

Fonts lokal bereitstellen: In jedem Fall sollte man Google-Fonts über den eigenen Webserver ausliefern. Dabei bietet der Google-Webfonts-Helper (*https://gwfh.mranftl.com*) Unterstützung. Nach Auswahl der gewünschten Schriftart erhält man den nötigen CSS-Code und einen Downloadlink für die Fontdateien. Beides kopiert man auf den Webserver und bindet den CSS-Code in die Seiten ein.
Nutzer von Wordpress installieren das Plug-in OMGF (*https://daan.dev/wordpress/omgf*), das sich über „Einstellungen → Optimize Google Fonts“ konfigurieren lässt. Nach einem Klick auf „Speichern & Optimieren“ baut es eine zusätzliche CSS-Datei mit den Fontdefinitionen ein. Die zugehörigen Fontdateien werden im Ordner „/wp-content/uploads/omgf“ gespeichert und dann von Ihrem eigenen Webserver ausgeliefert. ■

Hardware & Treiber für Linux

Gängige Linux-Distributionen bringen Treiber für fast jede Hardware mit. Sollte ein Gerät nicht vollständig unterstützt werden oder gar nicht funktionieren, gibt es auch dafür Lösungen.



VON THORSTEN EGGELING

Computerhardware wird vor allem für den Windows-Markt produziert. Vom Gerätehersteller können Linux-Nutzer kaum Unterstützung erwarten und zusätzliche Treiber für Linux gibt es in der Regel nicht als Setup-Paket. Es ist daher ratsam, sich bereits vor dem Kauf neuer Hardware über die Linux-Tauglichkeit zu informieren. Auf älteren PCs oder Notebooks lässt sich Linux meist ohne besondere Auffälligkeiten installieren. Aber auch hier kann es in Ausnahmefällen vorkommen, dass der Bildschirm schwarz bleibt, einzelne Funktionen unter Linux nicht bereitstehen oder neuere Hardware am USB-Anschluss nicht erkannt wird. Einige Probleme lassen sich durch Konfigurationsänderungen oder durch Wechsel der Linux-Distribution beheben. Am Anfang steht jedoch die Untersuchung der Hardware. Die kann ergeben, dass sich das Gerät mit einem neueren Kernel oder einem zusätzlichen Treiber nutzen lässt.

Hardwaremacken umgehen

PC-Hardware folgt keinen eindeutigen Standards. Für die Hersteller ist nur eins wichtig: Windows muss anstandslos laufen. Der eine oder andere Fehler in der Firmware oder auf der Hauptplatine wird dann bei Bedarf über einen Treiber repariert, den es für Linux aber nicht gibt. Besonders Notebooks, die auf Microsoft Windows zugeschnitten sind, bereiten mit ihren zahlreichen Bios-Versionen, abweichenden ACPI-Stromsparfunktionen und Chipsatzvarianten häufiger Ärger. Mal bleibt der Bildschirm dunkel, mal geht nach den ersten Bootmeldungen nichts mehr weiter. Bei der Linux-Neuinstallation helfen dann oft spezielle Kernel-Parameter weiter.

Wenn Sie Ubuntu 22.04 oder Linux Mint 21 vom Installationsmedium booten, begrüßt Sie das Grub-Bootmenü. Mit dem ersten Eintrag „Try or Install Ubuntu“ beziehungsweise „Start Linux Mint 21 Cinnamon 64-Bit“ startet das System mit den Standardeinstellungen.

Sollte der Bildschirm schwarz bleiben oder unlesbar sein, kann der zweite Menüeintrag „Ubuntu (safe graphics)“ oder „Start Linux Mint 21 Cinnamon 64-Bit (compatibility mode)“ weiterhelfen. Dabei werden Optionen an den Kernel übergeben, die die Hardwaresteuerung beeinflussen. Jedes Linux-System bietet eine Reihe von Kernel-Optionen – in der Dokumentation oft auch als Bootparameter oder Cheatcodes bezeichnet.

Über das Grub-Bootmenü lassen sich zusätzliche Optionen angeben. Dazu drückt man nach der Markierung eines Bootеintrags die Taste E und erhält dann einen Mini-Texteditor für den jeweiligen Eintrag gezeigt. Die Navigation im Textfeld erfolgt mit den Cursortasten. Grundsätzlich müssen Kernel-Parameter in die Zeile eingetragen werden, die mit „linux“ beginnt, aber vor „--“. Nach der Änderung startet die Taste F10 den Bootеintrag mit den neuen Einstellungen.

Bitte beachten Sie, dass im Grub-Editor eine englischsprachige Tastaturbelegung gilt. Bleibt der Bildschirm nach einem zunächst erfolgreichen Start dunkel, so liegt dies meist an nicht ausreichend unterstützten Grafikchips. Folgende Optionen können in diesem Fall weiterhelfen.

xforcevesa: Bei der Angabe dieser Option nutzt der Kernel für die Anzeige der grafischen Oberfläche nur den Vesa-Modus. Dieser Modus läuft auf den meisten Grafikchips, ohne jedoch deren spezielle Merkmale wie Hardwarebeschleunigung und Fähigkeiten zu nutzen.

nomodeset: Aktuelle Linux-Kernel können den Bildschirmmodus auf eigene Faust wechseln und schalten schon während des Bootvorgangs in einen grafischen Modus. Dies funktioniert nicht bei allen Grafikchips – so haben einige Modelle von Nvidia Probleme damit. Mit „nomodeset“ verzichtet der Kernel auf den Wechsel in den Grafikmodus und bleibt bei purem Text. Ubuntu und Linux Mint verwenden diese Option bei Auswahl des zweiten Menüeintrags.

Auf einigen Notebooks verhindern inkompatible Stromsparfunktionen im ACPI (Advanced Configuration and Power Interface) den Linux-Start. Linux Mint verwendet beim Menüeintrag „Start Linux Mint 21 Cinnamon 64-Bit (compatibility mode)“ einige der nachfolgend genannten Optionen.

acpi=off oder **noacpi** zwingt Linux dazu, ACPI komplett zu ignorieren und damit ohne Stromsparfunktionen und Leistungsmanagement für CPU und GPU zu starten. Auch Hyperthreading und die Lüfterregelung sind abgeschaltet.

acpi=ht: Mit dieser Option beachtet der Linux-Kernel gerade mal so viele ACPI-Fähigkeiten der Hardware, dass Hyperthreading der CPU funktioniert. Andere Stromsparfunktionen bleiben dagegen deaktiviert.

acpi=strict weist die ACPI-Unterstützung des Kernels an, nur ACPI-Merkmale der vorhandenen Hardware zu beachten, die exakt dem Standard folgen. Auf problematischen Notebooks ist diese Option immer einen Versuch wert.

acpi_osi=linux umgeht die Abfrage des Linux-Kernels, ob das ACPI eines Rechners kompatibel ist. Sinnvoll ist dieser Parameter, wenn einige Stromsparfunktionen nicht verfügbar sind oder die Drehzahlsteuerung der Lüfter nicht funktioniert.

Eine weitere Komponente nennt sich „Local APIC“ und nimmt die Interrupt-Anforderungen auf jedem Prozessorkern entgegen. Der Parameter „nolapic“ löst vielfältige Probleme mit heiklen Bios-Versionen, reduziert aber in jedem Fall die Zahl der vorhandenen CPU-Kerne auf einen. Geeignet ist dies nur als erste Hilfe, bis ein Bios-Update oder eine neue Kernel-Version echte Abhilfe schafft.

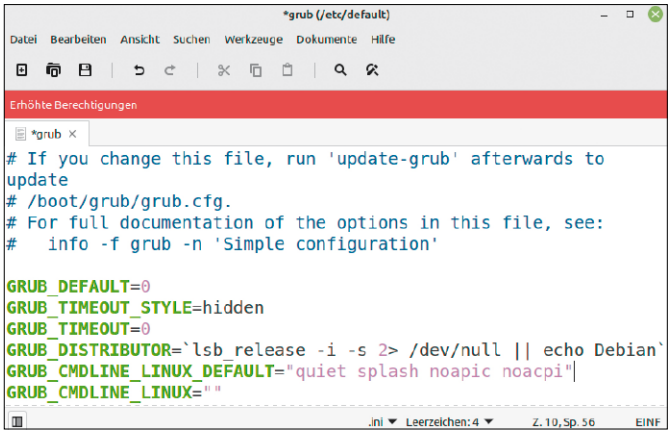
noapic: Verhindert, dass APIC für die Auflösung von Hardwarekonflikten auf Interrupt-Ebene verwendet wird. Der Parameter hilft auf Systemen mit einem unverträglichen Bios und inkompatiblen ACPI-Funktionen weiter. Eine häufig erfolgreiche Kombination bei besonders widerspenstigen Notebooks ist diese:

```
acpi=off noapic nolapic
```



Kernel-Optionen: Hardwareprobleme lassen sich im Grub-Bootmenü teilweise mit zusätzlichen Optionen umgehen. Linux Mint bietet einige standardmäßig an.

Kernel konfigurieren: Damit Ubuntu oder Linux Mint Kernel-Optionen bei jedem Start verwenden, müssen diese in die Datei „/etc/default/grub“ eingetragen werden.



iommu=soft: Die „Input-Output Memory Management Unit“ (IOMMU) ist ein Merkmal einiger Hauptplatinen und erlaubt Peripheriegeräten den direkten Speicherzugriff. Dies funktioniert zusammen mit Linux nicht immer, was zum Ausfall von USB-Ports oder Netzwerkchip führt. Dieser Parameter aktiviert zusammen mit abgeschaltetem IOMMU im Bios/Uefi, ein softwaremäßiges IOMMU.

Für Ubuntu und Co. liefert die englischsprachige Hilfeseite *https://help.ubuntu.com/community/BootOptions* eine Übersicht geläufiger Bootparameter. Die komplette Liste der Parameter mit Beschreibung für Entwickler bietet die offizielle Kernel-Dokumentation unter *https://www.kernel.org/doc/html/latest/admin-guide/kernel-parameters.html*.

Nach der Linux-Installation: Für ein installiertes System lassen sich die gewünschten Kernel-Optionen via Bootloader genauso angeben wie im Live- und Installationssystem.

Damit eine Änderung permanent gilt, ist die Bearbeitung einer Konfigurationsdatei mit sudo-Recht nötig:

```
sudo -H gedit /etc/default/grub
```

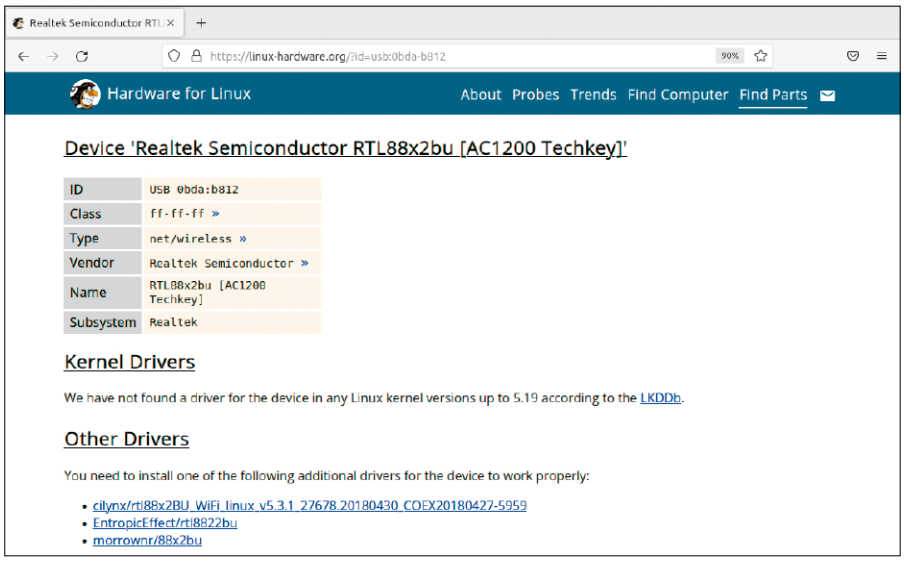
Die Zeile

```
GRUB_CMDLINE_
  LINUX="[parameter1]=[wert1]
  [parameter2]=[wert2]"
```

definiert die manuell hinzugefügten Angaben. Stehen hier schon Optionen, so ergänzen Sie zusätzlich nötigen nach einem Leerzeichen in dieser Zeile. Nach Änderung und Sicherung der Konfigurationsdatei ist die Änderung aber noch nicht wirksam, denn erst muss noch der Bootloader mit diesem Terminalbefehl aktualisiert werden:

```
sudo update-grub
```

Erst danach startet das Linux-System standardmäßig mit den hinzugefügten Kernel-Optionen.



Kein Treiber: Hardware Infos findet man bei *https://linux-hardware.org*. Für das Gerät mit der ID „0bda:b812“ ist bis einschließlich Version 5.19 kein Kernel-Modul vorhanden.

Hardware untersuchen und Infos finden

Jedes interne und externe Gerät besitzt eine eindeutige ID, die über den Herstellerund das Gerät informiert. Diese IDs lassen sich im Terminal mit den folgenden drei Befehlszeilen auslesen und in einer Datei speichern:

```
sudo lshw -numeric -html > lshw.html
sudo lspci -nn > lspci.txt
sudo lsusb -v > lsusb.txt
```

In der Datei „lshw.html“ finden Sie allgemeine Informationen zum PC, etwa den Typ der Hauptplatine, die Firmwareversion und den Prozessortyp. „lspci.txt“ zeigt Informationen über per PCI (Peripheral Component Interconnect) angebundene Komponenten, beispielsweise Soundchips („Audio device“), Grafikkarten („VGA compatible controller“) und Netzwerkchips („Ethernet controller“). In der Datei „lsusb.txt“ sehen Sie, welche Geräte mit den USB-Ports verbunden sind.

Ein Beispiel: Mit lsusb finden Sie die ID „0bda:b812“. Der erste Teil „0bda“ verweist auf den Hersteller „Realtek Semiconductor Corp.“ (siehe USB ID Repository: *https://usb-ids.gowdy.us/read/UD*), der zweite Teil „b812“ kennzeichnet das Gerät. Eine Internetsuche nach der kompletten ID liefert einige Ergebnisse, darunter auch *https://linux-hardware.org/?id=usb:0bda-b812*. Hier erfährt man, dass bis einschließlich Kernel 5.19 kein Treiber für diesen WLAN-Stick mit dem Chipsatz „RTL88x2bu“ verfügbar ist. In der Liste unter „Status“ sind einige Analysen zu finden, die Nutzer an *https://linux-hardware.org* gesendet haben. Bei den meisten steht „failed“ – das Gerät ließ sich also nicht in Betrieb nehmen. Die ersten Einträge mit „works“ weisen darauf hin, dass ein Treiber von *https://github.com/morrownr/88x2bu* für diese Hardware erforderlich ist.

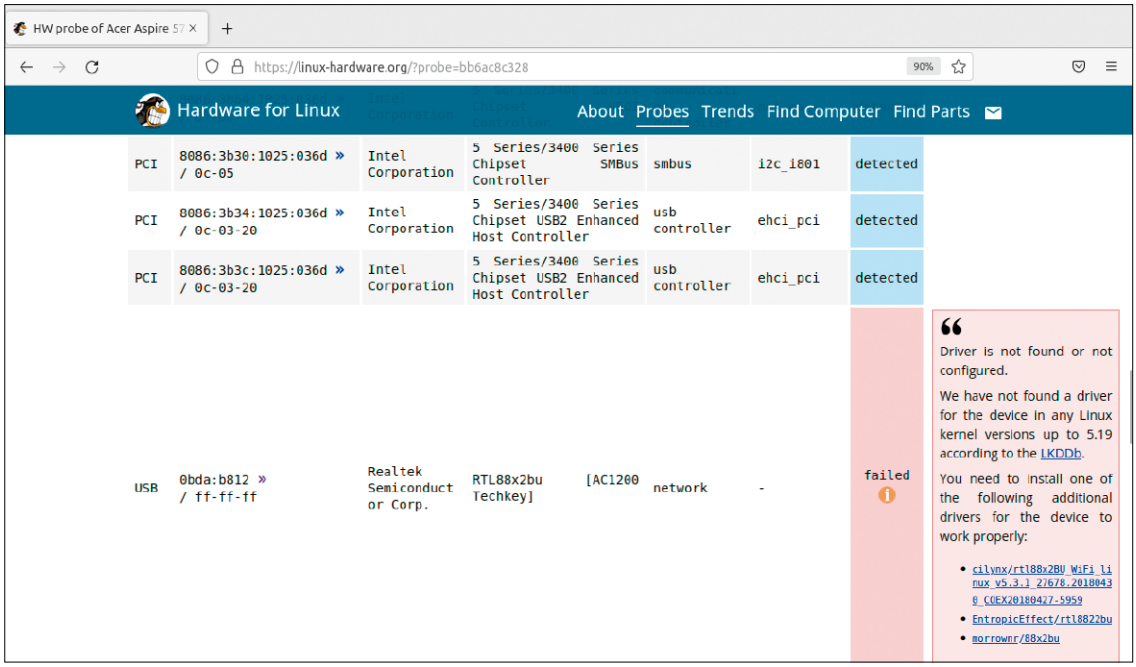
Analysedaten einsenden: Statt nach der Geräte-ID zu suchen, kann man die Daten seines PCs selbst anonym bei *https://linux-hardware.org* hochladen und dort prüfen lassen. Nutzer von Ubuntu oder Linux Mint installieren das nötige Tool im Terminal:

```
sudo apt install hw-probe
```

und starten es so:

```
sudo -E hw-probe -all -upload
```

Sie erhalten eine URL, die Sie im Browser aufrufen. In der Übersicht unter „Devices“ sind dann alle Geräte aufgelistet. Steht in der Spalte „Status“ der Eintrag „works“ oder „detected“, sollte das Gerät funktionieren. Ausrufungszeichen deuten jeweils darauf hin, dass es bei einzelnen Benutzern Probleme gab. Ein Klick darauf führt zu weiteren Informationen. Beim Status „failed“ wurde kein Treiber gefunden, geladen oder konfiguriert. Sofern vorhanden, führt ein Kasten



Problemlösung: Nach Einsendung der Hardwareanalyse zeigt *https://linux-hardware.org* an, welches Gerät nicht funktioniert und was dagegen zu tun ist.

rechts daneben zur Lösung. Weiter unten auf der Seite unter „Logs“ kann man sich per Klick etwa auf „Hwinfo“, „Lspci“ oder „Lsusb“ die Ausgaben der jeweiligen Tools anzeigen lassen.

Neue Kernel oder Treiber

Die Infos von *https://linux-hardware.org* können ergeben, dass ein neuerer Kernel die Hardware unterstützt. Welchen Kernel Ihr System aktuell nutzt, finden Sie im Terminal mit dem Befehl

```
uname -a
```

heraus. Ubuntu 22.04 und Linux Mint 21 verwenden zur Zeit die Kernel-Version 5.15. Wer einen neueren Kernel benötigt, muss ihn selbst erstellen. Eine Anleitung für Ubuntu und Linux Mint finden Sie über *https://m6u.de/BMUK*. Alternativ kann man zu einer Distribution wechseln, die deutliche aktuellere Updates bietet („Rolling Release“). Manjaro Linux beispielsweise ist aktuell schon bei Kernel 6.0.2 (*https://manjaro.org*).

Treiber kompilieren: Wenn der Quellcode verfügbar ist, kann man den Treiber selbst erstellen. Dabei gibt es zwei Herausforderungen: Der Quellcode muss zum laufenden Kernel passen und die nötigen Schritte können sich je nach Treiber unterscheiden. Lesen Sie daher immer die zugehörigen Anleitungen sorgfältig durch. Exemplarisch liefern wir eine kurze Anleitung für den oben genannten WLAN-Stick mit dem Chipsatz „RTL88x2bu“.

Schritt 1: Öffnen Sie ein Terminal und installieren Sie einige zusätzliche Pakete:

```
sudo apt install git build-
  essential dkms linux-headers-
  $(uname -r)
```

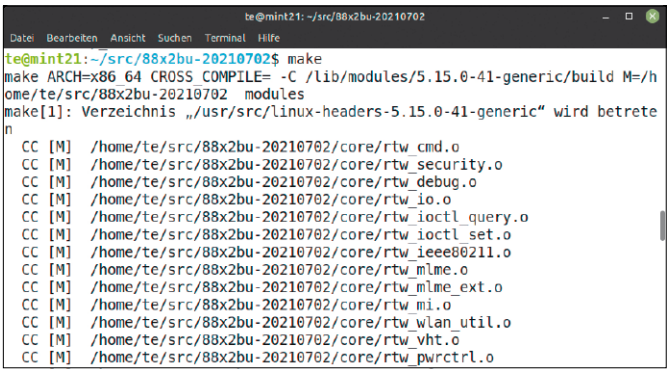
Schritt 2: Gehen Sie auf *https://github.com/morrownr/88x2bu-20210702* und klicken Sie auf „Code“. Kopieren Sie die URL unter „HTTPS“. Dann erstellen Sie ein Arbeitsverzeichnis und laden den Quelltext des Treibers herunter (vier Zeilen):

```
mkdir -p ~/src
cd ~/src
git clone [URL]
cd 88x2bu-20210702
```

Statt „[URL]“ fügen Sie die zuvor kopierte Adresse ein. Passen Sie die Pfadangabe hinter „cd“ entsprechen der Treiberversion an.

Schritt 3: Führen Sie die folgenden drei Befehle aus:

```
make clean
make
sudo insmod 88x2bu.ko
```



Treiber kompilieren: Nach dem Download des Treiber-Quellcodes genügt in der Regel der Befehl „make“, der ein neues Modul für den laufenden Kernel erstellt.

Damit wird der Treiber aus dem aktuellen Ordner „~/src/88x2bu-20210702“ geladen. Mittels

```
dmesg
```

lassen Sie sich die letzten Kernel-Meldungen ausgeben, die über den erfolgreich geladenen Treiber informieren oder Fehlermeldungen anzeigen. Für die meisten Treiber folgt abschließend dieser Befehl:

```
sudo make install
```

Damit wird der Treiber in einen Ordner unterhalb von „/lib/modules/[Kernel-Version]“ kopiert und ab dem nächsten Linux-Start automatisch geladen. Bei unserem Beispieltreiber ist das nicht erforderlich, weil ein Script die Aufgabe übernimmt (siehe Schritt 4).

Die WLAN-Hardware funktioniert jetzt und Verbindungen lassen sich wie gewohnt über den Netzwerkmanager herstellen.

Wenn allerdings Secure Boot aktiviert ist, erzeugt der Befehl insmod eine Fehlermeldung: Der Treiber wird nicht geladen, weil er nicht digital signiert ist. Sie müssen dann entweder Secure Boot im Firmwaresetup deaktivieren oder den Treiber signieren (siehe *https://m6u.de/KNMD*).

Schritt 4: Der Treiber von *https://github.com/morrownr/88x2bu-20210702* lässt sich komfortabel per Script einrichten:

```
sudo ./install-driver.sh
```

Sie werden gefragt, ob Sie die Konfigurationsdatei „/etc/modprobe.d/88x2bu.conf“ mit den Treiberoptionen bearbeiten möchten. In der Regel ist das nicht nötig, Erklärungen zu den Optionen sind in der Konfigurationsdatei enthalten. Wenn Sie Linux jetzt neu starten, wird der neue Treiber automatisch geladen und die WLAN-Hardware lässt sich nutzen. ■

LINUX UND NEUE HARDWARE

Vor der Anschaffung neuer Hardware sollte man sich immer über die Linux-Kompatibilität informieren. Bei Notebooks oder PCs können Händler nur selten Auskunft geben, außer sie sind auf Linux-Hardware spezialisiert. Hersteller von WLAN- oder TV-Sticks geben manchmal Linux in der Liste der unterstützten Betriebssysteme an. Dann kann es sein, dass sich das Gerät mit gängigen und aktuellen Linux-Distributionen direkt in Betrieb nehmen lässt. Oft ist die Linux-Unterstützung jedoch nur theoretisch vorhanden. Konkret: Es funktioniert eventuell nur mit einer bestimmten Distribution oder Kernel-Version. Oder es ist nur Sourcecode verfügbar, aus dem man den Treiber selbst kompilieren muss.

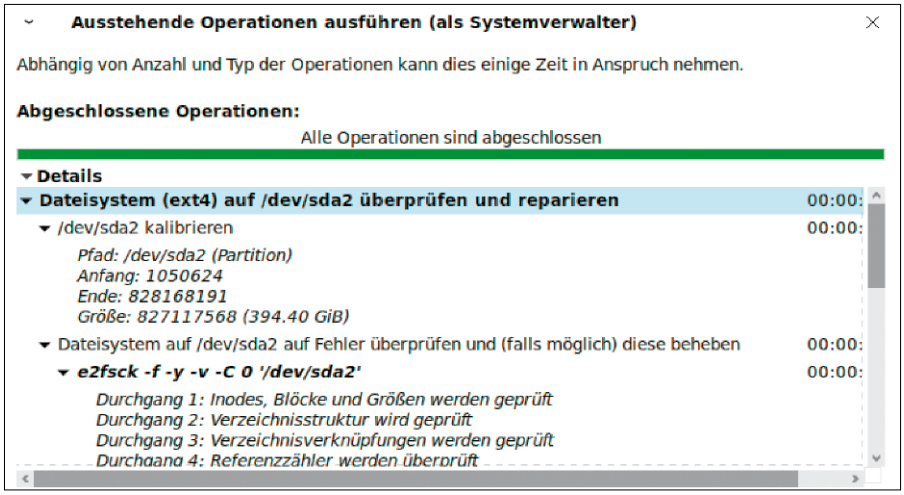
Lesen Sie daher die Rezensionen und Bewertungen anderer Käufer und suchen Sie im Internet nach den Erfahrungen von Linux-Nutzern. Basiskomponenten wie SATA-Adapter, Onboard-Ethernet und Grafikchips bereiten selten Probleme. Oft sind es auch nur Kleinigkeiten, die nicht funktionieren – lästig ist das trotzdem. Bei Notebooks beispielsweise reagieren manchmal die Tasten für die Bildschirmhelligkeit oder Lautstärke nicht, das Touchpad lässt sich nicht nutzen oder der Akku wird unter Linux zu schnell leer. Die Lösungen, die man im Internet findet, sind so vielfältig wie die Hardwarekomponenten. Im besten Fall ist nur eine kleine Änderung in der Konfiguration nötig oder ein Firmwareupdate. Wenn ein Gerät unter Linux aber als Problemkandidat bekannt ist, sollte man Abstand nehmen.

Linux-Bootprobleme beseitigen

Wenn Linux nicht mehr bootet, kann eine defekte Festplatte oder ein korruptes Dateisystem die Ursache sein. Meist ist aber nur die Bootumgebung beschädigt, was sich dann relativ leicht reparieren lässt.

VON THORSTEN EGGELING

Es kann durch Updates, ein Systemupgrade oder durch eine Windows-Installation verursacht werden: Linux bootet nicht mehr. Symptome sind, dass der Bildschirm nach dem Einschalten des PCs schwarz bleibt oder eine Fehlermeldung des Bootmanagers Grub erscheint. Dieser Zustand ist von Problemen mit der Desktopumgebung zu unterscheiden (siehe Artikel ab Seite 190). Auch dabei kann zwar der Monitor schwarz bleiben, doch zeigt die Laufwerks-LED nach dem Start über eine längere Zeit deutliche Aktivitäten, was auf ein arbeitendes System schließen lässt.



Dateisystem prüfen: Defekte im Dateisystem können den Linux-Start verhindern. Analyse und Reparatur lassen sich in einem Rettungssystem mit Gparted durchführen.

1. Hardware untersuchen und Daten retten

Als Erstes prüfen Sie, ob die Festplatte oder SSD noch ansprechbar ist. Dazu rufen Sie das Firmwaresetup auf, was meist über Tasten wie Esc, F2 oder Entf kurz nach dem Einschalten des PCs gelingt. Oft sehen Sie die verfügbaren Laufwerke bereits auf der Übersichtsseite oder in einem Menü wie „Boot“. Das Linux-Laufwerk beziehungsweise das Laufwerk mit dem Bootmanager muss in der Bootreihenfolge an der ersten Stelle stehen. Bei einem Uefi-PC ist das bei Ubuntu und Linux Mint ein Eintrag, der mit „ubuntu“ beginnt. Sollte das Linux-Laufwerk nicht dabei sein, prüfen Sie im PC die Verbindung mit dem Datenkabel und die Stromversorgung.

Für weitere Untersuchungen booten Sie den PC mit dem LinuxWelt-Rettungssystem von der LinuxWelt-DVD. Aus der ISO-Datei im Ordner „Image-Dateien“ können Sie auch einen USB-Stick erstellen. Verwenden Sie dafür Unetbootin (auf der LinuxWelt-DVD). Zusätzliche Infos zu bootfähigen USB-Sticks finden Sie unter *www.pcwelt.de/2089747*.

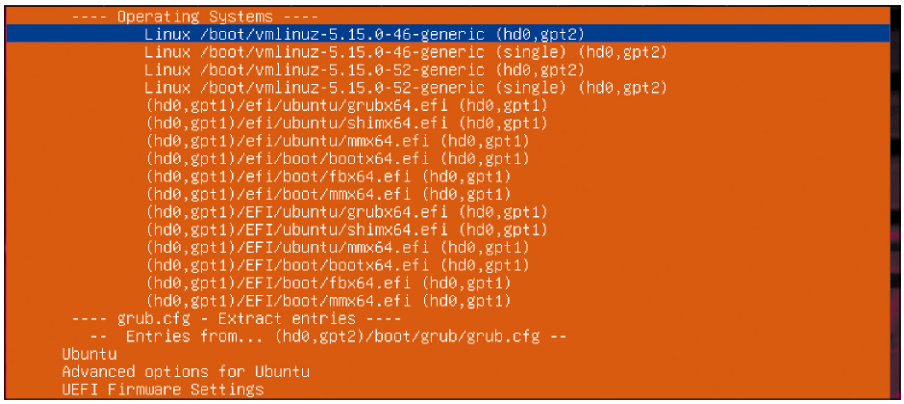
Starten Sie im Rettungssystem den Dateimanager per Doppelklick auf das Icon „Rechner“ auf dem Desktop. Unter „Geräte“ lässt sich die Linux-Partition mit einem Mausklick einhängen. Sie können dann Dateien aus Ihrem Home-Verzeichnis auf einen externen Datenträger sichern (siehe auch den Artikel ab Seite 188). Das ist sinnvoll, wenn das System aufgrund zeitweiser Ausfälle oder wegen Defekten im Dateisystem nicht bootet.

Starten Sie das Tool Gparted über das Menü und „Systemwerkzeuge“ oder über das Icon in der Taskleiste. Wählen Sie das Linux-Laufwerk rechts oben aus und klicken Sie die Linux-Partition mit der rechten Maustaste an. Wählen Sie im Menü „Aushängen“, wenn Sie die Partition zuvor über den Dateimanager eingebunden haben. Danach wählen Sie „Überprüfen“ und bestätigen die Aktion über „Bearbeiten → Alle Operationen ausführen“. Wenn das Dateisystem repariert werden konnte, sollte Linux wieder starten. Andernfalls ist wahrscheinlich die Bootumgebung defekt und muss repariert werden.

2. Linux über Zweit-Grub starten

Super Grub Disk 2 (*www.supergrubdisk.org*) lässt sich von der LinuxWelt-DVD über den Menüpunkt „Extras und Tools“ booten. Für einen USB-Stick laden Sie die ISO-Datei vom Hersteller herunter. Achten Sie darauf, dass der PC bei einem Uefi-System über den Booteintrag mit dem vorangestellten „Uefi“ bootet. Gehen Sie im Menü auf „Detect and show boot methods“. Super Grub

Disk 2 sucht nach bootfähigen Systemen und zeigt diese an. Es genügt, den gewünschten Eintrag unter „Operating Systems“ zu wählen, beispielsweise „Linux /boot/vmlinuz-5.15.0-41-generic (hd0, gpt2)“. Grub lädt den Kernel direkt und startet das System. Das funktioniert auf Bios- und Uefi-Systemen. Im erfolgreich gestarteten Linux reparieren Sie anschließend die Bootumgebung (siehe Punkt 3).



Booten im Notfall: Wenn zumindest der Linux-Kernel auf der Festplatte zu finden ist, lässt sich Linux über ein Rettungsmedium mit Super Grub Disk 2 starten.

3. Grub-Bootumgebung wiederherstellen

Starten Sie das System über Super Grub Disk 2 (siehe Punkt 2) und öffnen Sie ein Terminalfenster. Bei einer Uefi-Installation ermitteln Sie zuerst, ob die Uefi-Partition vorhanden und in das Dateisystem eingebunden ist. Der Befehl

```
mount | grep boot
```

sollte beispielsweise „/dev/sda1 on /boot/efi type vfat“ ausgeben. Im Ordner „/boot/efi/EFI/ubuntu“ liegen die Bootloader-Dateien mit der Dateinamenserweiterung „.efi“. Wenn das nicht der Fall ist, ermitteln Sie mittels

```
sudo parted -l
```

(kleines „L“) die Partitionen. Eine FAT32-Partiton, meist mit der Bezeichnung „EFI System Partition“, hat beispielsweise die Nummer „1“ („dev/sda1“). Binden Sie die EFI-Partition mit

```
sudo mount /dev/sda1 /boot/efi
```

ein. Danach verwenden Sie die folgenden Befehle:

```
sudo grub-install --recheck
sudo update-grub
```

Kontrollieren Sie in der Datei „/etc/fstab“, ob die Partitionen korrekt eingebunden werden. Vergleichen Sie ferner die Werte hinter „UUID=“ (Laufwerkskennung) mit der Ausgabe von

```
blkid
```

und korrigieren Sie bei Bedarf die Angaben in der Datei „/etc/fstab“.

Bios-System: Standardmäßig wird der Bootloader auf dem Systemlaufwerk installiert, sofern Sie bei der Installation nichts anderes gewählt haben. Bei einer Neuinstallation richten Ubuntu 22.04 und Linux Mint 21 das Laufwerk im GPT-Stil ein. Der Befehl

```
sudo parted -l
```

zeigt dann eine „EFI System Partition“. Die spielt jedoch im Moment keine Rolle und ist für den Fall gedacht, dass Sie die Festplatte später in einem neuen PC mit Uefi-Firmware verwenden wollen. Grub ist auf der Bios-Boot-Partition installiert, bei der in der Spalte „Flags“ der Wert „bios_grub“ steht. Das Installationslaufwerk lässt sich mit

```
mount | grep "on / type"
```

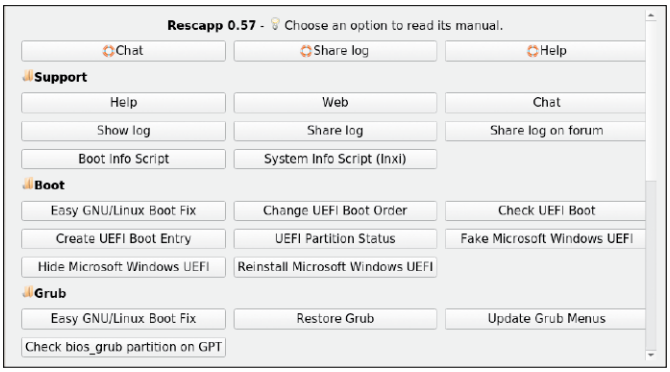
ermitteln. Wenn „sda“ in der Ausgabe auftaucht, ist Linux auf der ersten Festplatte installiert, bei „sdb“ auf der zweiten. Sie können auch die zweite Festplatte als Ziel der Grub-Installation angeben, müssen dann aber die Bootreihenfolge im Firmwaresetup entsprechend anpassen.

Für die erneute Grub-Installation verwenden Sie diese beiden Befehle:

```
sudo grub-install --recheck /dev/sdx
sudo update-grub
```

Für „sdx“ tragen Sie die Bezeichnung für die Boot-Festplatte ein, beispielsweise „/dev/sda“.

Wichtig: Geben Sie nur den Gerätenamen ohne Partitionsnummer an.



Reparaturen durchführen: Mit Rescatux lassen sich die meisten Probleme mit der Bootumgebung beheben. In der Regel führt „Easy GNU/Linux Boot Fix“ zum Erfolg.

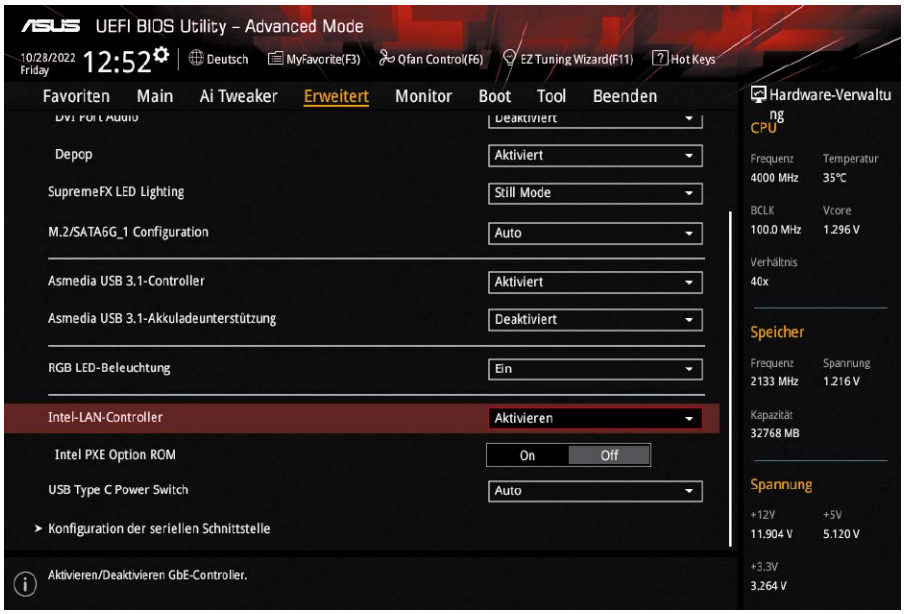
4. Grub-Reparatur über ein Rettungssystem

Rescatux (*www.supergrubdisk.org/rescatux*) bietet Werkzeuge für die grafische Oberfläche, mit denen sich Linux reparieren lässt. Sie finden das System auch in der ISO-Datei der Extra-DVD der LinuxWelt 1/2023 unter *https://bit.ly/3la5pbw*. Booten Sie den PC mit Rescatux. Im Fenster „Rescatux-Startup-Wizard“ klicken Sie auf „Yes“, womit Sie die Standardeinstellungen wählen. Danach klicken Sie auf „Start Rescapp“.

Per Klick auf „Menu“ gelangen Sie zu einem Fenster mit Schaltflächen für die eigentlichen Funktionen. „Easy GNU/Linux Boot Fix → Run“ ermöglicht die Reparatur des Grub-2-Bootloaders. Das Tool durchsucht alle Laufwerke nach Partitionen und bietet diese zur Auswahl an. Hier wählt man jene Partition aus, die das Linux-System beherbergt, beispielsweise „sda2 Linux_Mint_21_Vanessa“. Nach einem Klick auf „OK“ fragt das Tool nach der Zielfestplatte für Grub. In der Regel wählen Sie „sda“, außer Sie haben Bootloader- und Systemlaufwerk auf getrennten Festplatten eingerichtet. Klicken Sie auf „OK“. Jetzt lässt sich bei Bedarf die Uefi-Bootreihenfolge anpassen. Setzen Sie den Eintrag „ubuntu“ an die erste Stelle. Nach einem Klick auf „OK“ wird die Reparatur durchgeführt. Beenden Sie Rescatux und starten Sie dann das installierte Linux-System. ■

Netzwerkfehlern auf der Spur

Wenn das Netzwerk nicht wie gewohnt funktioniert, liegt eine fehlerhafte Konfiguration vor oder die Hardware ist defekt. Linux bietet einige Tools, mit denen sich das Netzwerk analysieren lässt.



Firmwareeinstellungen: Onboard-Netzwerkadapter lassen sich im Setup deaktivieren, was auch mal versehentlich geschehen kann. Dann kann die Hardware von Linux nicht erkannt werden.

VON THORSTEN EGGELING

Netzwerkausfälle sind schwer zu diagnostizieren, weil dafür mehrere Komponenten die Ursache sein können. Für diesen Artikel gehen wir davon aus, dass der DSL-Router eine Internetverbindung hergestellt hat, dass WLAN oder die Ethernet-Verbindung sowie weitere beteiligte Geräte wie WLAN-Access-Point, Switch oder Repeater funktionieren. Die Grundvoraussetzungen lassen sich am einfachsten mit einem zweiten PC, Notebook, Tablet oder Smartphone prüfen. Sind externe Fehlerquellen ausgeschlossen, kann das Problem nur beim betroffenen PC oder seinem Betriebssystem liegen.

Netzwerkkonfiguration im Terminal prüfen

Ermitteln Sie zuerst die IP-Adresse des DSL-Routers oder Kabelmodems. Als Standard wird oft 192.168.0.1 oder 192.168.1.1 verwendet, bei einer Fritzbox 192.168.178.1. Sehen Sie im Handbuch oder auf der Unterseite des Routers nach. Sie können auch ein Gerät mit funktionierender Netzwerkverbindung verwenden und die nachfolgenden Befehle hier ausführen. In einem Terminal finden Sie die IP-Adresse des PCs mit dem Befehl

```
ip a
```

heraus. Unter „1:“ steht hinter „inet“ immer die IP-Adresse „127.0.0.1“ des Loopback-Adapters („lo“), der internen Aufgaben dient. Danach folgen unter „1:“, „2:“, und so weiter die Angaben für Ethernet und WLAN-Adapter. Lautet die IP-Adresse in einem Fritzbox-Netzwerk beispielsweise „192.168.178.175“ (Adressbereich „192.168.178.2“ bis „192.168.178.254“), dann hat das Gerät eine korrekte IP-Adresse per DHCP (Dynamic Host Configuration Protocol) vom Router erhalten. Steht hinter „inet“ eine IP aus einem anderen Bereich oder gar keine Adresse, kann keine Verbindung zum Netzwerk aufgebaut werden. Mit

```
route -n
```

führen Sie einen weiteren Test durch. In der Spalte „Router“ muss die IP-Nummer des Routers stehen, beispielsweise „192.168.178.1“ bei einer Fritzbox.

Dabei gibt es eine Ausnahme: Wenn die Verbindung über einen zweiten Router oder einen WLAN-Access-Point aufgebaut wird, können diese für ein eigenes Netzwerk konfiguriert sein. Die Geräte leiten den Datenverkehr dann von einem zum anderen Netzwerk. In diesem Fall prüfen Sie, ob Access Point oder Router eine Verbindung zum DSL-Router herstellen können. Um diese Fehlerquelle auszuschließen, verbinden Sie das Ethernet-Kabel oder WLAN direkt mit dem DSL-Router.

Ist der Netzwerkadapter aktiv? Wenn außer „lo“ kein Netzwerkadapter und damit auch keine Konfiguration angezeigt wird, ist der Adapter vielleicht nur abgeschaltet. Bei Notebooks lassen sich Ethernet- und WLAN-Adapter meist über eine Tastenkombination deaktivieren (Flugmodus) und auch wieder aktivieren. Kontrollieren Sie auch im Firmwaresetup des Rechners, ob der Netzwerkadapter aktiviert ist.

PCs verfügen meist über Kontroll-LEDs, die den Status anzeigen. Bleiben diese trotz funktionstüchtigem Ethernet-Kabel dunkel, kann der Netzwerkadapter defekt sein.

Erreichbarkeit von Geräten testen

Der nächste Test prüft, ob ein Gerät im lokalen Netz auf Anfragen antwortet. Der Befehl

```
ping -c 5 192.168.178.1
```

unternimmt fünf Versuche, eine Fritzbox zu erreichen. Ersetzen Sie die IP-Adresse durch die Ihres Routers und probieren Sie auch andere Adressen im Netzwerk aus. Bei der Ausgabe „Destination Host Unreachable" ist die Zieladresse nicht erreichbar, andernfalls erhalten Sie eine Antwort mit der benötigten Antwortzeit in Millisekunden. Ein positives Ergebnis sollte zumindest beim Router immer erscheinen, wenn „ip a" zuvor eine korrekte Konfiguration ausgegeben hat. Einzelne Geräte können jedoch die Ping-Anfragen blockieren.

DNS-Server für das Web: Mit einer Befehlszeile wie

```
ping -c 5 -4 google.com
```

prüfen Sie die Namensauflösung über den DNS-Server. Der Rückgabewert enthält die IPv4-Adresse. Wenn nicht, ist der DNS-Server gerade nicht erreichbar oder falsch konfiguriert. Im Webbrowser lassen sich dann ebenfalls keine Seiten mehr über den Domainnamen aufrufen. Für einen Test der Namensauflösung für IPv6 ersetzen Sie „-4" durch „-6". Mit dem Befehl

```
resolvectl status
```

lässt sich prüfen, welcher DNS-Server konfiguriert ist. Wenn Sie selbst nichts anderes eingestellt haben (siehe nächster Punkt), erhält ein PC die Adresse des DNS-Servers per DHCP vom DSL-Router. Ist dieser nicht erreichbar, würde allerdings die Namensauflösung bei keinem Gerät im Netzwerk funktionieren.

Fehlersuche über die grafische Oberfläche

Für das Netzwerk ist bei Linux meist der Netzwerkmanager zuständig. Ubuntu-Nutzer finden die Konfiguration in den „Einstellungen" unter „Netzwerk" oder „WLAN", Nutzer von Linux Mint gehen im Menü auf „Einstellungen → Netzwerk". Bei den genutzten Verbindungen muss der zugehörige Schalter aktiviert sein. Per Klick auf das Zahnradsymbol gelangt man unter beiden Systemen und bei jeder Verbindungsart zur Konfiguration. Auf der Übersichtsseite „Informationen" (Linux Mint: „Details") werden die wichtigsten Werte wie IPv4-Adresse, Vorgabestrecke (Gateway) und DNS-Server angezeigt. Für das WLAN werden Signalstärke und Verbindungsgeschwindigkeit angezeigt. Bei schlechten Werten reduzieren Sie den Abstand zum WLAN-Router oder finden einen besseren Standort für den Router.

Erreichbarkeit testen: Rechner im lokalen Netzwerk und im Internet liefern auf eine Ping-Anfrage eine Rückmeldung, wenn sie aktiv sind und die Netzwerkverbindung vorhanden ist.

```
te@mint21: ~
Datei  Bearbeiten  Ansicht  Suchen  Terminal  Hilfe
te@mint21:~$ ping -c 5 -4 google.com
PING  (142.250.74.206) 56(84) bytes of data.
64 bytes from fra24s02-in-f14.1e100.net (142.250.74.206): icmp_seq=1
 ttl=119 time=15.9 ms
64 bytes from fra24s02-in-f14.1e100.net (142.250.74.206): icmp_seq=2
 ttl=119 time=14.8 ms
64 bytes from fra24s02-in-f14.1e100.net (142.250.74.206): icmp_seq=3
 ttl=119 time=14.9 ms
64 bytes from fra24s02-in-f14.1e100.net (142.250.74.206): icmp_seq=4
 ttl=119 time=15.8 ms
64 bytes from fra24s02-in-f14.1e100.net (142.250.74.206): icmp_seq=5
 ttl=119 time=14.3 ms

---  ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 14.294/15.137/15.910/0.613 ms
te@mint21:~$
```



Konfiguration prüfen: Die Übersichtsseite der Einstellungen zeigt die wichtigsten Werte an. Unter „IPv4" und „IPv6" sollte in der Regel alles auf „Automatisch" stehen.

Standardmäßig ist unter „IPv4" alles auf „Automatisch" eingestellt. Dadurch erhält der Rechner alle Werte automatisch vom DHCP-Server im Router. Das sollte auch so bleiben, außer man benötigt eine feste IP-Adresse für einen Server. Bei Auswahl der Option „Manuell" kann man eine eigene IP-Adresse eintragen, die dann aber im Netzwerk nicht anderweitig vergeben sein darf und zum IP-Adressbereich des Routers passen muss.

Unter „IPv6" gibt es die gleichen Optionen und auch hier sollte überall „Automatisch" aktiviert sein. Für die Verbindung zu anderen Rechnern im lokalen Netzwerk spielt IPv6 keine Rolle. Beim Aufruf von Adressen im Internet kann aber IPv6 zum Einsatz kommen, wenn DSL-Router und Internetanbieter das unterstützen. Da bisher alle Server im Internet auch eine IPv4-Adresse besitzen, ist die Technik (noch) nicht zwingend erforderlich.

Firewall prüfen: Bei Ubuntu und Linux Mint ist die Firewallsoftware ufw („Uncomplicated Firewall") installiert, aber standardmäßig nicht aktiviert. Wenn ufw eingeschaltet ist, blockiert die Firewall alle eingehenden Verbindungen, wodurch sich Serverdienste wie SSH nicht erreichen lassen. Bei Linux Mint ist das Konfigurationstool Gufw vorinstalliert („Einstellungen → Firewall-Konfiguration"). Ubuntu-Nutzer installieren es im Terminal so:

```
sudo apt install gufw
```

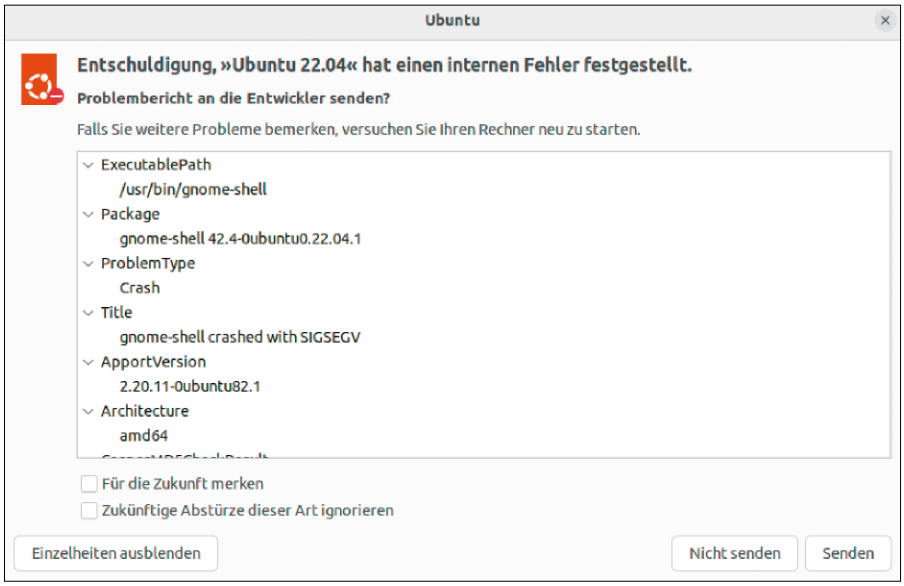
Sollte die Firewall aktiviert sein, stellen Sie den Schalter hinter „Status" auf „Aus" und prüfen die Netzwerkfunktionen. In der Regel kann die Firewall deaktiviert bleiben, außer Sie benötigen eine spezielle Konfiguration für einzelne Serverdienste im lokalen Netzwerk.

Durch die Firewall im DSL-Router sind direkte Zugriffe über das Internet auf den PC ohnehin blockiert. Wenn Sie gezielt Portfreigaben eingerichtet haben, müssen Sie eine zweite Firewall auf dem PC dafür ebenfalls konfigurieren – das erhöht die Sicherheit nicht und bedeutet nur unnötigen Konfigurationsaufwand. ■

Softwareprobleme und -defekte

Was tun, wenn Software hängt oder nicht erwartungsgemäß funktioniert? Unter Linux gibt es mehrere Methoden für die Diagnose von Softwareproblemen und deren anschließende Reparatur.

VON THORSTEN EGGELING



Absturzbericht: Ubuntu meldet Fehler bei Programmen, die aus den Standardrepositorien stammen. Den Bericht kann man für weitere Untersuchungen an die Entwickler senden.

Nicht jede Anwendung läuft so stabil, wie sie sollte, und manchmal startet ein Programm unter Linux gar nicht. Ist nur ein einzelnes Programm betroffen, kann es am Programm selbst, seiner Konfiguration oder an defekten Dateien liegen. Die Analyse von Logdateien und die Meldungen eines Programms im Terminal können bei der Fehlersuche helfen.

Mehr Infos zu Programmabstürzen

Linux-Anwendungen geben beim Absturz nur selten Fehlermeldungen auf dem Desktop aus. Das Programmfenster schließt sich plötzlich und nicht gespeicherte Daten gehen verloren. Auch beim Start einer Anwendung gibt es oft keinen sichtbaren Hinweis auf Probleme. Tatsächlich startet das Programm aber und stürzt sofort ab.

Programmabstürze werden aber in der Regel protokolliert. Im Terminal verwenden Sie direkt nach einem Absturz den Befehl

```
sudo dmesg
```

oder

```
sudo cat /var/log/kern.log
```

Eventuell gibt es in „/var/log/“ oder seinen Unterverzeichnissen weitere Logdateien mit sachdienlichen Hinweisen.

Bei den Desktopsystemen von Ubuntu ist der Dienst Apport vorinstalliert. Er protokolliert Abstürze und gibt eine Meldung wie „Entschuldigung, ‚Ubuntu 22.04‘ hat einen internen Fehler festgestellt.“ aus. Nach einem Klick auf „Einzelheiten anzeigen“ erfährt man mehr über den Fehler und per Klick auf „Senden“ kann man den Problembericht an die Ubuntu-Entwickler übermitteln. Apport ist allerdings nur für Pakete aus den Standardquellen zuständig, nicht für Software aus anderen Quellen. Wer sich einen Fehlerbericht nachträglich noch einmal ansehen möchte, verwendet diese Befehlszeile:

```
sudo -H /usr/share/apport/apport-gtk /var/crash/[Dateiname].crash
```

Den Platzhalter „[Dateiname]“ ersetzen Sie durch den gewünschten Dateinamen aus dem Ordner „/var/crash“.

Linux Mint verwendet systemd-coredump für die Sammlung von Absturzberichten. Damit wird alles erfasst, was auch in „/var/log/kern.log“ zu finden ist. Im Terminal gibt

```
coredumpctl list
```

die gesammelten Fehlermeldungen inklusive der Prozess-ID aus und mit

```
coredumpctl info [Prozess-ID]
```

lässt man sich detaillierte Meldungen zu einem einzelnen Fehler ausgeben.

Fehlersuche über das Terminal

Viele Programme, auch grafische, geben im Terminal Meldungen aus, die bei der Fehlersuche helfen. Haben Sie zum Beispiel ein neues Programm installiert, das beim Aufruf nicht startet, dann öffnen Sie ein Terminal und tippen den Namen des Programms hier ein. Treten Probleme auf, können Sie in der Ausgabe nach Fehlermeldungen suchen.

Manchmal erscheint nur Meldungen wie „Speicherzugriffsfehler“, „Segmentation fault“ oder „Segfault“ (Schutzverletzung). Das Programm ist dann defekt oder nicht für das System geeignet. Dann hilft nur, auf eine Aktualisierung zu warten oder eine ältere Version zu verwenden. Oft gibt es

auch alternative Versionen (Snap-Apps, Flatpak, Appimage), die stabiler laufen.

Fehlende Bibliotheken: Eine Meldung im Terminal wie diese

```
error while loading shared
  libraries: libcurl.so.4: cannot
  open shared object file: No such
  file or directory
```

zeigt an, dass die Programmbibliothek „libcurl.so.4“ nicht auf dem System installiert ist. Das Programm kann daher nicht starten. Solche Fehler treten meist nur bei Software aus fremden Quellen auf.

In welchem Paket die fehlende Datei enthalten ist, ermitteln Sie über *https://packages.ubuntu.com* (auch für Linux Mint). Unter „Durchsuchen des Inhalts von Paketen“ tippen Sie für unser Beispiel „libcurl“ ein. Wählen Sie dann die Option „Pakete, die Dateien enthalten, deren Name den Suchbegriff enthalten“, darunter die gewünschte Distribution und die Architektur, in der Regel „amd64“.

„Jammy“ ist der Codename für Ubuntu 22.04, was auch die Basis von Linux Mint 21 („Vanessa“) ist. „Focal“ gehört zu Ubuntu 20.04 und Linux Mint 20 („Una“, „Uma“, „Ulyssa“ und „Ulyana“). Nach einem Klick auf „Suchen“ erfahren Sie, dass „libcurl.so.4“ im Paket „libcurl4“ enthalten ist. Danach installieren Sie mit

```
sudo apt install libcurl4
```

das fehlende Paket.

Ablaufverfolgung bei Fehlern

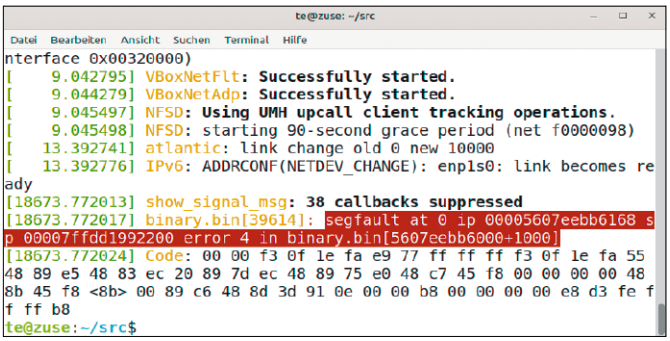
Sie haben gerade ein Programm neu installiert, doch nach dem Aufruf passiert scheinbar gar nichts. Selbst die Suche in den Logfiles ergibt keinen Hinweis auf Fehler. Aber auch für scheinbar hoffnungslose Fälle hält Linux Werkzeuge parat. Das Tool Strace folgt dem Ablauf eines Programms auf Schritt und Tritt und ist oft der letzte Notnagel, wenn Sie sonst keine Fehler oder Hinweise finden. Strace ist oft vorinstalliert, andernfalls richten Sie es über den Paketmanager ein (Paketname „strace“).

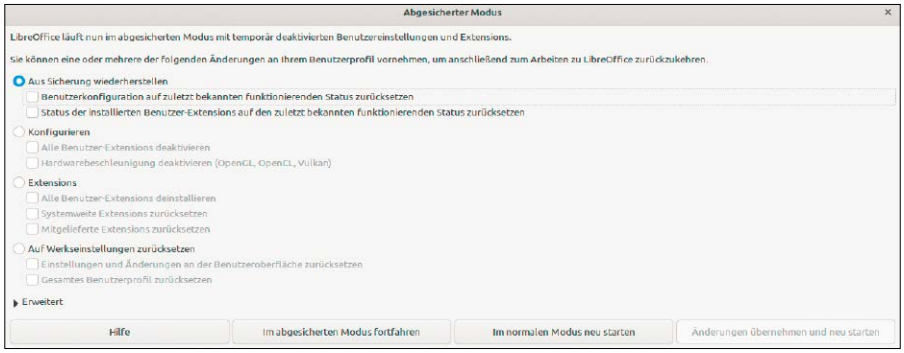
Da Strace jeden Systemaufruf mitprotokolliert, geht schnell der Überblick verloren. Wenn ein Programm während der Startphase abstürzt, können aber die letzten Zeilen der Strace-Ausgabe einen Hinweis darauf liefern, was in den letzten Millisekunden falsch gelaufen ist.

Sie können jedes Programm in einem Terminalfenster mit

```
strace -f [Programmname]
```

Logdateien untersuchen: Wenn ein Programm nicht startet, findet man Fehlermeldungen (hier „segfault“) beispielsweise in der Datei „/var/log/kern.log“.





Abgesicherter Modus: Wird Libre Office mit „--safe-mode“ gestartet, kann man einige Einstellungen deaktivieren oder zurücksetzen und damit Fehler eingrenzen oder beheben.

beobachten. Wenn das Programm beispielsweise eine Konfigurationsdatei nicht findet oder sie wegen falscher Zugriffsrechte nicht öffnen kann, finden Sie in der Ausgabe etwa die Zeile:

```
open("[Datei]", O_RDONLY) = -1
  ENOENT (No such file or directory)
```

„[Datei]“ enthält den Namen der betroffenen Datei, der Rückgabewert „-1“ weist fast immer auf einen Fehler hin. Allerdings gibt Strace auch Fehler aus, wenn ein Programm beispielsweise eine nur optionale Datei nicht findet, was aber keineswegs zum Absturz führt. Suchen Sie im Internet nach dem Dateinamen in Kombination mit dem Programmnamen, um weitere Informationen zu erhalten.

Für die bequemere Untersuchung leiten Sie die Ausgabe von Strace in eine Datei um:

```
strace -f --output=Logfile.txt
  [Programmname]
```

Die Textdatei „Logfile.txt“ öffnen Sie dann in einem Editor.

Fehler in der Konfiguration umgehen

Wenn ein Programm bisher funktioniert hat und nicht gerade aktualisiert wurde, muss es einen externen Grund für die Fehlfunktion geben, beispielsweise eine defekte Konfigurationsdatei. Am einfachsten ist es, einen neuen Linux-Benutzer anzulegen und mit einem frischen Profil zu starten. Tritt der Fehler hier nicht auf, muss es an einer Benutzereinstellung beziehungsweise Konfigurationsdatei liegen. Um welche es sich genau handelt, muss man durch Ausprobieren herausfinden – oder man benutzt einfach das neue Profil.

Einige Anwendungen kennen Schalter, über die sich eine zerstörte Konfiguration umgehen lässt (abgesicherter Modus). Starten Sie beispielsweise Libre Office im Terminal so:

```
soffice --safe-mode
```

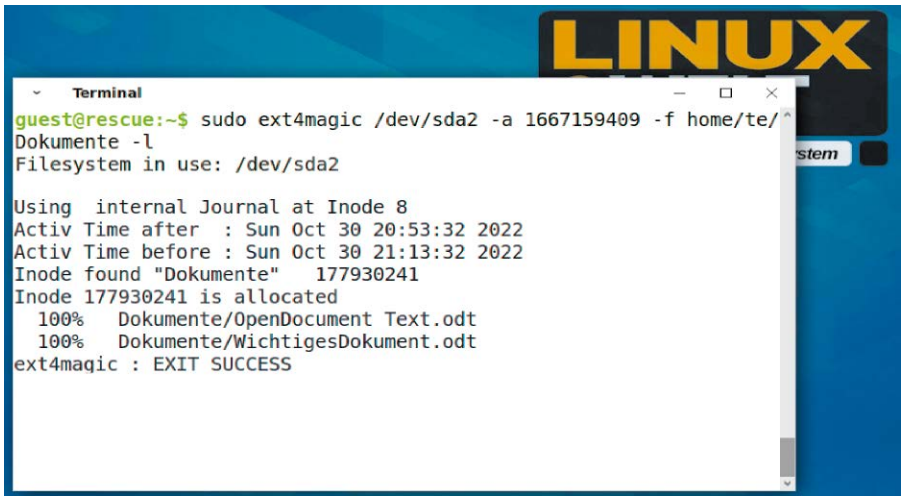
Es erscheint ein Dialog, wo Sie auf „Im abgesicherten Modus fortfahren“ klicken. Läuft jetzt alles ohne Absturz, rufen Sie das Programm erneut im abgesicherten Modus auf, wählen eine der angebotenen Optionen, etwa „Alle Benutzer-Extensions deaktivieren“, und klicken auf „Änderungen übernehmen und neu starten“. Wiederholen Sie das mit anderen Optionen. Bei der Radikalkur „Gesamtes Benutzerprofil zurücksetzen“ gehen alle bisherigen Einstellungen verloren.

Firefox und Thunderbird kennen die Option „--safe-mode“ ebenfalls, womit sich Erweiterungen deaktivieren lassen. Nutzer von Chromium oder Google Chrome verwenden für den gleichen Zweck „--incognito“. ■

Zerstörte Dateien retten

Wurden Dateien unter Linux versehentlich aus dem Papierkorb oder über das Terminal gelöscht, heißt es schnell handeln. Es besteht dann noch die Chance, die Dateien wiederzufinden.

VON THORSTEN EGGELING



Dateien wiederherstellen: Das Tool Ext4magic findet Verweise auf Dateien im Journal des Dateisystems. Sind noch Kopien vorhanden, lassen sich die Dateien oft rekonstruieren.

Bei einem Systemabsturz können Dateien verlorengehen oder beschädigt werden, und auch der Nutzer kann versehentlich wichtige Dateien löschen. Ist kein Backup vorhanden, lassen sich Dateien oft wiederherstellen. Das gelingt jedoch nicht immer verlustfrei und manchmal lassen sich Inhalte nur teilweise rekonstruieren. Die wichtigste Maßnahme zuerst: Wurden Dateien versehentlich gelöscht, schalten Sie den PC sofort aus. Ansonsten besteht die Gefahr, dass der jetzt als nicht belegt gekennzeichnete Speicherplatz umgehend mit neuen Daten überschrieben wird.

Gelöschte Dateien wiederherstellen

Wenn Sie Dateien über den Dateimanager löschen, landet diese erst einmal im Papierkorb und lassen sich problemlos wiederherstellen. Wurde der Papierkorb geleert oder eine Datei im Terminal gelöscht, bietet Linux standardmäßig keine Funktion für die Wiederherstellung. Mit dem Tool Ext4magic (*https://sourceforge.net/projects/ext4magic*) lassen sich Dateien jedoch ganz oder wenigstens teilweise wiederherstellen. Eine Garantie dafür gibt es allerdings nicht.

Booten Sie den PC mit dem LinuxWelt-Rettungssystem (auf der Heft-DVD, siehe auch den Beitrag ab Seite 8). Sie benötigen außerdem eine zweite Festplatte (intern oder extern). Die Partition mit den verlorenen Daten darf nicht über den Dateimanager eingebunden werden.

Schritt 1: Binden Sie über den Dateimanager nur die Zielpartition per Mausklick unter „Geräte“ ein. Im Terminal lassen Sie sich mit dem Kommando

```
lsblk
```

die Partitionen anzeigen. Für unser Beispiel gehen wir davon aus, dass „/dev/sda2“ die Partition mit den gelöschten Dateien ist und „/dev/sdb1“ das Backuplaufwerk, das unter „/mnt/sdb1“ in das Dateisystem eingehängt ist.

Schritt 2: Ext4magic benötigt den ungefähren Zeitpunkt, an dem eine Datei gelöscht wurde. Der lässt sich aus dem Journal des Dateisystems ermitteln:

```
sudo ext4magic /dev/sda2 -H -a
 $(date-d "-20minutes" +%s) -f
 home/[user]/Dokumente
```

Dieser Befehl zeigt ein Histogramm der Änderungen der letzten 20 Minuten an. Für einen anderen Zeitraum verwenden Sie beispielsweise „-60minutes“ oder „-2days“. Den (relativen) Pfad hinter „-f“ passen Sie an, je nachdem, wo sich die gelöschten Dateien befanden.

Schritt 3: Ext4magic zeigt im Histogramm unterhalb von „d_time“ die Zeit und die Löschungen an. Sollten alle Werte „0“ enthalten, hat das Tool keine gelöschten Dateien gefunden. Vergrößern Sie den Zeitraum, bis wenigstens in einer Zeile der Wert „1“ oder größer erscheint. Für Ext4magic benötigen Sie den Zeitstempel direkt vor dieser Zeile, also kurz vor dem Löschvorgang, beispielsweise „1667159409“.

Die Befehlszeile lautet dann

```
sudo ext4magic /dev/sda2 -a
 1667159409 -f home/[user]/
 Dokumente -l
```

Durch „-l“ (kleines „L“) zeigt das Tool die Dateien an, die sich wiederherstellen lassen. Die Wiederherstellung geschieht dann so:

```
sudo ext4magic /dev/sda2 -a
 1667159409 -f home/[user]/
 Dokumente -r -d /mnt/sdb1
```

Hinter „-d“ steht das Zielverzeichnis. Danach bleibt noch die Aufgabe, die gesicherten Dateien in den angelegten Ordnern manuell zu überprüfen, um das Gesuchte zu finden.

Dateien mit Photorec und Testdisk retten

Sollte Ext4magic keine brauchbaren Ergebnisse liefern, probieren Sie Photorec aus (*www.cgsecurity.org*). Das Tool ist ebenfalls im LinuxWelt-Rettungssystem zu finden und lässt sich im Terminal mit

```
sudo photorec
```

starten. Es bietet eine einfache Menüführung, in der Sie mit den Pfeiltasten navigieren und mit der Eingabetaste bestätigen. Die Partition mit den gelöschten Dateien darf nicht eingehängt sein, die Zielfestplatte muss eingebunden sein.

Schritt 1: Wählen Sie in Photorec die Festplatte aus, auf der sich die gelöschten Dateien befinden. Identifizieren Sie die Festplatte anhand von Bezeichnung und Größe. Bestätigen Sie mit „Proceed“. Über „File Opt“ lässt sich die Suche auf bestimmte Dateitypen einschränken. Aktivieren Sie die Option „zip“, um auch Libre-Office-Dateien wiederherzustellen.

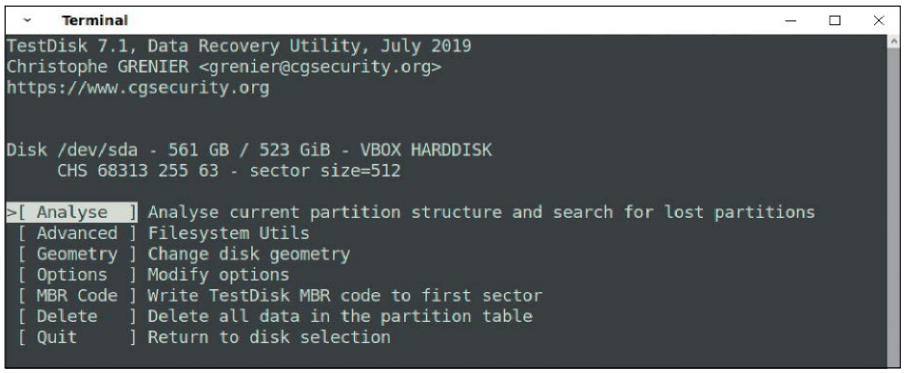
Schritt 2: Wählen Sie die gewünschte Partition und gehen Sie auf „Search“. Geben Sie bei einer Linux-Partition das Dateisystem mit „ext2/ext3“ an und bestätigen Sie mit der Eingabetaste. Ext4 wird dabei ebenfalls berücksichtigt.

Schritt 3: Wählen Sie das Zielverzeichnis. Durch den Verzeichnisbaum navigieren Sie mit den Tasten Cursor-links, Cursor-rechts und der Eingabetaste. Wählen Sie einen Ordner auf einem externen Laufwerk oder einer zweiten Festplatte. Mit der Taste C bestätigen Sie das Verzeichnis. Nachdem Photorec die Wiederherstellung beendet hat, finden Sie die wiederhergestellten Dateien im Zielverzeichnis in mehreren Ordnern. Die ursprünglichen Dateinamen kann Photorec oft nicht mehr rekonstruieren. Durchsuchen Sie die Verzeichnisse, um die gewünschten Inhalte zu finden.

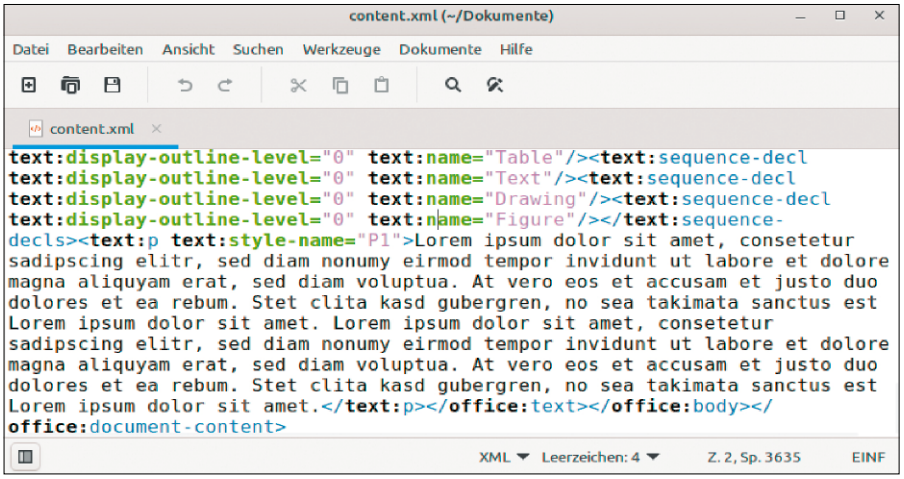
Testdisk (im LinuxWelt-Rettungssystem enthalten) ist ein Spezialist zur Wiederherstellung versehentlich gelöschter Partitionen oder defekter Partitionstabellen. Das Programm wird mit

```
sudo testdisk
```

gestartet und lässt sich ähnlich steuern wie Photorec. Nach dem Start wählen Sie „No Log“ und anschließend die Festplatte, auf der Sie eine Partition wiederherstellen möchten. Weiter geht es mit „Proceed“, „Intel“ (alle PC-Partitionen), „Analyse“ und „Quick Search“. Wählen Sie dann die Linux-Partition. Mit „p“ lassen Sie sich die enthaltenen Dateien anzeigen, mit „q“ geht es wieder zurück. Drücken Sie die Eingabetaste, um die Partition zur Wiederherstellung auszuwählen. Abschließend legen Sie die Partitionstabelle über „Write“ neu an, was Sie mit der Taste Y bestätigen. Fahren Sie das Rettungssystem dann herunter.



Partitionen zurückholen: Auch wenn eine Partition versehentlich gelöscht wurde, sind die Dateien in der Regel noch vorhanden. Testdisk kann die Partition dann wiederherstellen.



Defekte Office Dateien: Dateien, die sich in Libre Office nicht öffnen lassen, kann man manchmal noch entpacken. Der Inhalt ist in der Datei „content.xml“ zu finden.

Bei Ubuntu 22.04 und Linux Mint 21 berücksichtigt Testdisk die Bios-Boot-Partition nicht, die deshalb verlorengeht. Bei einem Bios/MBR-System stellen Sie Grub über Rescatux wieder her, wie im Artikel ab Seite 182 im Punkt 4 beschrieben.

Defekte Office-Dateien rekonstruieren

Libre-Office-Dateien, die gerade im Programm geöffnet sind, können beim Absturz des Systems oder durch andere Unfälle beschädigt werden. Bei einer teilweise defekten, aber noch lesbaren Festplatte kopieren Sie – soweit möglich – alle wichtigen Dateien über den Dateimanager des LinuxWelt-Rettungssystems auf ein Sicherungslaufwerk. Sollte sich eine Datei nicht mehr öffnen lassen, versuchen Sie die Reparatur im Terminal, bei einer Writer-Datei beispielsweise so:

```
zip -F [Datei.odt] --out
  [Repariert.odt]
```

Ersetzen Sie „-F“ durch „-FF“, wenn sich die Datei weiterhin nicht in Libre Office öffnen lässt. Die Platzhalter in eckigen Klammern ersetzen Sie jeweils durch den Dateinamen oder Pfad plus Namen. Das Verfahren lässt sich auch auf Microsoft-Office-Dateien (.docx oder .xslx) anwenden, da es sich bei allen diesen Formaten um ZIP-Archive handelt. Sollte die Reparatur nicht erfolgreich sein, lässt sich die Datei vielleicht mit

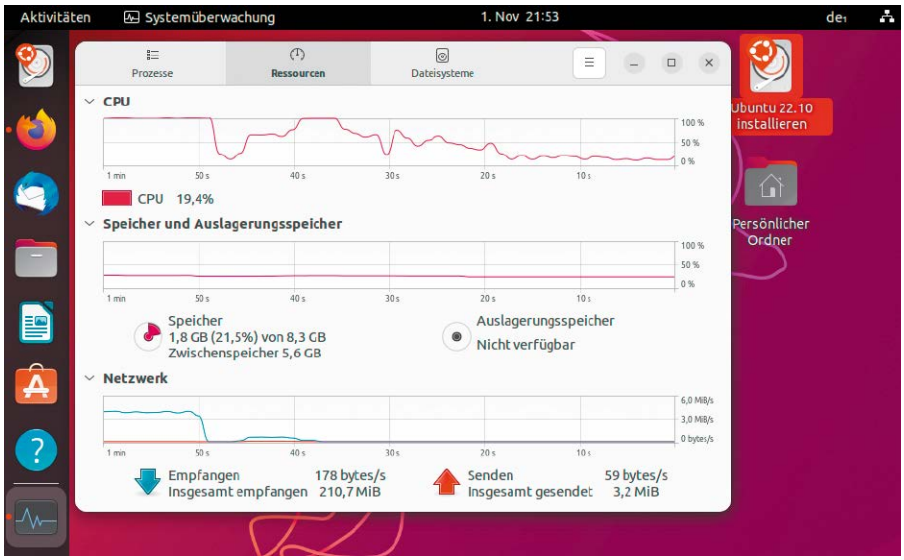
```
unzip [Repariert.odt]
```

entpacken. Bei Libre-Office-Dateien ist der Textinhalt dann in der Datei „content.xml“ zu finden, die Sie in einem Texteditor öffnen können. Kopieren Sie die relevanten Inhalte in eine neue Office-Datei. Microsoft Word speichert die Inhalte im Ordner „word“ in der Datei „document.xml“. ■

Wenn der Desktop streikt

Probleme mit der grafischen Oberfläche werden meist durch eine defekte Konfiguration oder fehlerhafte Treiber verursacht. Analyse und Reparatur sind etwas aufwendig, aber nicht wirklich kompliziert.

VON THORSTEN EGGELING



Test im Livesystem: Das Ubuntu-Installationsmedium verwendet nur Standardtreiber. Wenn es über einen längeren Zeitraum stabil läuft, sind Hardwaredefekte unwahrscheinlich.

Die grafische Oberfläche von Linux-Systemen läuft nur einwandfrei, wenn alle Komponenten mitspielen. Auf der Hardwareseite ist der Treiber für den Grafikchip dafür zuständig, dass überhaupt etwas auf dem Bildschirm erscheint. Bei der Software steuert der Displayserver (Xorg oder Wayland) den Monitor an, der Windowmanager zeichnet die Programmfenster und Desktopumgebungen wie Gnome, Cinnamon oder KDE liefern wesentliche Bestandteile wie Menüs, Systemleisten und Fensterelemente. Alles muss zusammenpassen und für alles gibt es Konfigurationsdateien – Raum genug für ausreichend Fehlerquellen. In der Praxis läuft der Linux-Desktop dennoch meist sehr stabil. Wie sich einige grundsätzliche Probleme untersuchen und beheben lassen, ist Gegenstand dieses Artikels.

Desktopprobleme untersuchen

Wenn bei der Linux-Neuinstallation Grafikprobleme auftauchen, helfen meist Kernel-Optionen weiter (siehe ab Seite 178). Bei einem System, das bereits einige Zeit ohne Auffälligkeiten lief, gehören Hardwaredefekte oder defekte Konfigurationsdateien zum Kreis der Verdächtigen. Es kann beispielsweise sein, dass der Desktop gar nicht mehr erscheint, nach einiger Zeit komplett einfriert oder sich nur zögerlich mit der Maus bedienen lässt. Um den Fehler einzugrenzen, booten Sie den PC mit einem beliebigen Livesystem. Auf der Heft-DVD dieser LinuxWelt finden Sie etwa Linux Mint 21.1. Starten Sie den Webbrowser, arbeiten Sie mit Libre Office, spielen Sie Videos ab und lassen Sie das Livesystem eine Zeitlang laufen. Wenn der Desktop auch hier einfriert oder Fehler zeigt, kann die Hardware das Problem sein. Prüfen Sie die Lüfter, installieren Sie ein Firmwareupdate oder lassen Sie den Hersteller oder Verkäufer das Gerät testen.

Fehler nach der Anmeldung: Ein anderer Fehlertyp liegt vor, wenn die grafische Oberfläche mit dem Anmeldebildschirm erscheint, die Anmeldung jedoch nicht zur gewohnten Oberfläche führt. Man landet entweder wieder bei der Anmeldung, der Desktop ist leer oder nicht benutzbar. Bei derartigen Symptomen ist wahrscheinlich die Konfiguration defekt. Legen Sie testweise einen neuen Benutzer an, da dieser mit einer frischen Konfiguration startet. Treten hier keine Fehler auf, muss es an einer der Konfigurationsdateien liegen. Wenn Sie es vorziehen, verwenden Sie einfach das neue Benutzerkonto weiter und kopieren persönliche Dateien vom alten in das neue Home-Verzeichnis.

Benutzerprofil umbenennen: Wer sich genauer mit dem Problem beschäftigen möchte, geht einen anderen Weg. Beenden Sie alle Programme und wechseln Sie zu einer virtuellen Textkonsole. Bei Linux Mint 21 verwenden Sie die Tastenkombination Strg-Alt-F1, bei Ubuntu 20.04 oder 22.04 drücken Sie Strg-Alt-F3. Melden Sie sich in der Konsole an. Bei Linux Mint stoppen Sie dann den Displaymanager (Anmeldebildschirm) mit

```
sudo service lightdm stop
```

und Ubuntu-Nutzer verwenden dazu diesen Befehl:

```
sudo service gdm3 stop
```

Benennen Sie Ihr Home-Verzeichnis um, erstellen Sie ein neues Home-Verzeichnis

und setzen Sie die Zugriffsrechte:

```
sudo mv /home/[user] /home/[user].bak
sudo mkdir /home/[user]
sudo chown [user]:[user] /home/[user]
```

Den Platzhalter „[user]“ ersetzen Sie jeweils durch die Bezeichnung Ihres Benutzerkontos. Danach starten Sie den Displaymanager mit

```
sudo service lightdm start
```

oder so:

```
sudo service gdm3 start
```

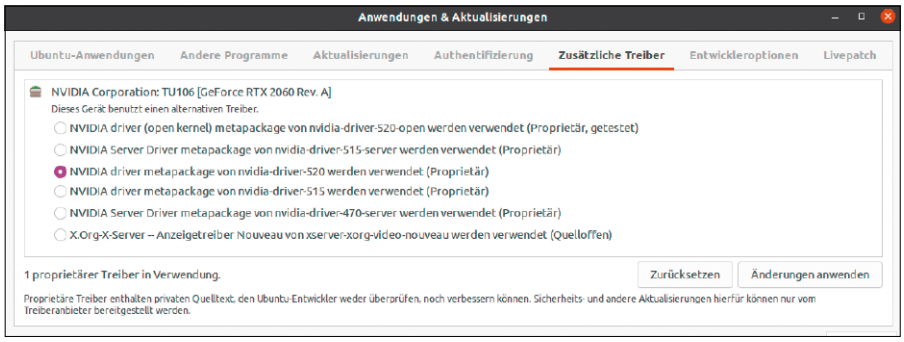
Melden Sie sich an und testen Sie die Funktionen des Systems. Wenn keine Probleme mehr auftauchen, liegt der Fehler in einer der Konfigurationsdateien. Damit beginnt der mühsame Teil der Analyse. Sie kopieren einzelne Ordner oder Unterordner nach und nach aus der Sicherungskopie („/home/[user].bak“) in das Home-Verzeichnis, melden sich ab und wieder an und warten auf mögliche Fehler. Beachten Sie, dass Konfigurationsverzeichnisse und -dateien mit einem Punkt beginnen und erst sichtbar werden, wenn Sie im Dateimanager die Tastenkombination Strg-H drücken.

Wenn der Fehler wieder auftritt, machen Sie die letzte Kopieraktion rückgängig. Danach kopieren oder verschieben Sie alle anderen Verzeichnisse und Dateien – außer den fehlerhaften – aus „/home/[user].bak“ nach „/home/[user]“.

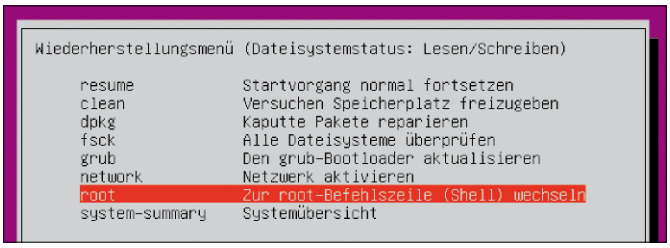
Probleme mit Treibern beheben

Nach der Installation verwenden Ubuntu und Linux Mint den Open-Source-Standardtreiber für den jeweiligen Grafikchip. Dessen Leistung ist für typische Desktopaufgaben ausreichend. Für anspruchsvollere Aufgaben installieren Sie optimierte Treiber für Grafikadapter von Nvidia oder AMD. Ubuntu-Nutzer suchen über „Aktivitäten“ nach „Treiber“ und klicken auf „Zusätzliche Treiber“. Bei Linux Mint führt der Weg über das Menü „Systemverwaltung → Treiberverwaltung“.

Treiberauswahl: Wenn ein Treiber verfügbar ist, werden meist mehrere Optionen angezeigt. Bisher galt die Regel, dass der Nvidia-Treiber mit der höchsten Versionsnummer und dem Zusatz „Proprietär, getestet“ die beste Wahl ist. Bei Treibern mit dem Zusatz „open kernel“ gilt das aber zur Zeit nicht. Unter *https://github.com/NVIDIA/open-gpu-kernel-modules* ist der Hinweis zu finden, dass bei Geforce-Modellen nur



Bessere Treiber? Die proprietären Treiber bieten zwar mehr Leistung, sind aber auch eine Fehlerquelle. Bei Problemen aktivieren Sie zumindest vorübergehend den Standardtreiber.



Notfallstart: Wenn die grafische Oberfläche nicht startet, booten Sie in das Wiederherstellungssystem. In der „root-Befehlszeile“ lassen sich defekte Treiber deinstallieren.

„Alpha-Qualität“ zu erwarten ist, der Treiber also mehr als unfertig ist. Im Moment ist daher ein Treiber ohne den Zusatz „open kernel“ zu empfehlen.

Zurück zum Standardtreiber

Bei Problemen mit dem proprietären Treiber stellen Sie den Standard „X.Org-X-Server“ wieder her. Sollte das über „Zusätzliche Treiber“ nicht möglich sein, weil der Desktop schwarz bliebt, starten Sie das System im Recoverymodus. Wenn bei Ihrer Installation das Grub-Bootmenü nicht automatisch erscheint, halten Sie bei Start des PCs die Umschalt-Taste gedrückt. Im Bootmenü gehen Sie dann auf den Eintrag mit dem Zusatz „Advanced options“ und danach auf den ersten Eintrag, der „(recovery mode)“ enthält. Im Menü wählen Sie „network“ und bestätigen mit „Ja“. Danach wählen Sie „root“ und drücken die Eingabetaste. Entfernen Sie den proprietären Nvidia-Treiber

```
sudo apt purge nvidia*
```

oder den AMD/ATI-Treiber:

```
sudo apt purge fglrx*
```

Fehlt der proprietäre Treiber, verwendet Linux wieder den Standardtreiber. Mit *reboot* verlassen Sie das Rettungssystem und starten Linux neu.

Die grafische Oberfläche sollte jetzt wieder nutzbar sein. ■

ZUSATZOPTIONEN FÜR NVIDIA-TREIBER

Bei der Installation neuer Nvidia-Treiber auf einem Desktopsystem vermeiden Sie besser Treiber mit dem Zusatz „Server“. Diesem Paket fehlen einige Tools für Desktopnutzer, beispielsweise nvidia-settings. Damit kann man sich Infos zum Grafikchip anzeigen lassen und auf Notebooks unter „PRIME profiles“ Stromsparfunktionen aktivieren: Standard ist „NVIDIA On-Demand“, womit der Nvidia-Chip nur bei Bedarf aktiviert wird. „NVIDIA (Performance Mode)“ schaltet den Chip dauerhaft ein, was den Akku schnell leert. „Intel (Power Saving Mode)“ belastet den Akku am wenigsten. Bei einigen Treiberversionen ist diese Option aber ausgegraut und daher nicht wählbar. Verwenden Sie dann im Terminal diesen Befehl:

```
sudo prime-select intel
```

Mit der Zeile

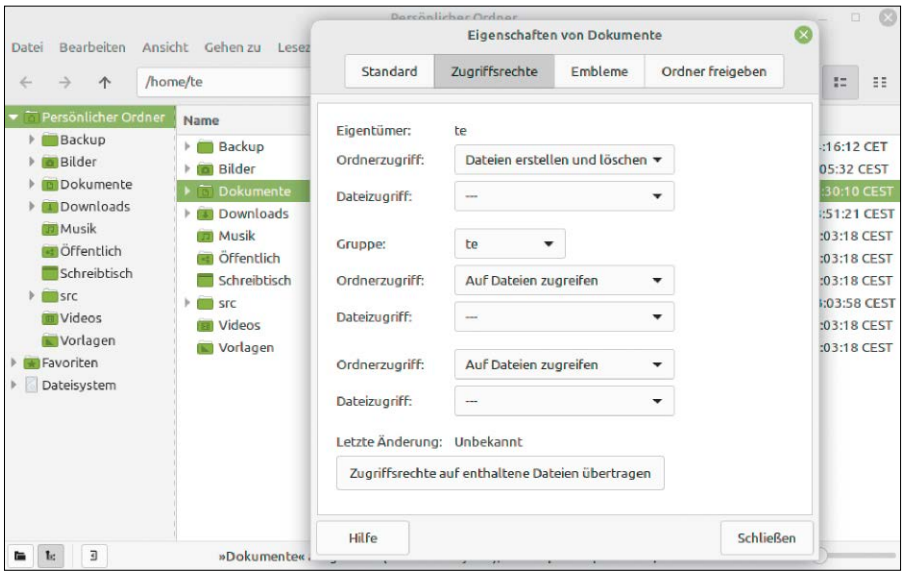
```
sudo prime-select on-demand
```

aktivieren Sie wieder den Standardmodus.

Zugriffsrechte anpassen

Wenn sich Ordner nicht öffnen oder Programme nicht starten lassen, kann das an den Zugriffsrechten liegen. Die lassen sich aber über den Dateimanager oder im Terminal schnell anpassen.

VON THORSTEN EGGELING



Zugriffsrechte prüfen und ändern: Im Dateimanager sehen Sie die geltenden Berechtigungen in den Eigenschaften von Ordnern und Dateien auf der Registerkarte „Zugriffsrechte“.

Linux ist ein Mehrbenutzersystem. Deshalb darf ein Standardnutzer nicht in alle Ordner hineinsehen und auch nicht alle Dateien beliebig öffnen oder ändern. Für die Sicherheit ist das gut, weil sich Systemdateien nicht ohne Weiteres löschen oder manipulieren lassen – weder vom Nutzer noch von Schadsoftware. Zugriffsrechte im Dateisystem bilden jedoch eine zusätzliche Ebene der Komplexität, mit der man sich zwar nicht ständig befassen muss, aber in einigen Fällen eben doch. Falsch gesetzte Rechte können den Zugang versperren oder einige Programme arbeiten nicht wie erwartet.

Grundlagen der Rechtevergabe

Unter Linux gehören alle Elemente im Dateisystem einem Benutzer („Besitzer“) und einer Gruppe. Die eigenen Dateien unter „/home/[User]“ gehören dem Benutzer „[User]“ und der gleichnamigen Gruppe. Der Platzhalter „[User]“ entspricht dem von Ihnen gewählten Benutzernamen.

Für Ordner und Dateien lassen sich Lese- und Schreibrechte vergeben, getrennt nach Besitzer und Gruppe. Zudem gibt es das Recht „Ausführen“. Ist es bei einer Datei gesetzt, darf ein Benutzer sie als Programm starten. Bei Ordnern gewährt es die Berechtigung, ihn zu öffnen beziehungsweise den Inhalt anzusehen. Außerdem lassen sich Rechte für „Andere“ festlegen. Damit sind Zugriffe von Benutzern gemeint, die weder Eigentümer sind noch zu der Gruppe gehören.

Rechte und erhöhte Rechte im Dateimanager

Welche Rechte für einen Ordner oder eine Datei gelten, lässt sich über den Dateimanager ermitteln und ändern. Klicken Sie unter Ubuntu & Co. ein Element im Dateisystem mit der rechten Maustaste an und wählen Sie „Eigenschaften“. Auf der Registerkarte „Zugriffsrechte“ sehen Sie die geltenden Rechte, die Sie auch ändern können. Bei Programmen oder Scripts aus dem Internet setzen Sie ein Häkchen vor „Datei als Programm ausführen“, damit sich die Anwendung starten lässt. Das ist auch bei Containern im Appimage-Format erforderlich.

Über die Schaltfläche „Zugriffsrechte der enthaltenen Dateien ändern“ lassen sich unter Ubuntu bei Ordnern die Rechte rekursiv für alle enthaltenen Elemente in einem eigenen Dialog setzen – für „Besitzer“, „Gruppe“ und „Andere“ jeweils getrennt für die enthaltenen Dateien und Ordner.

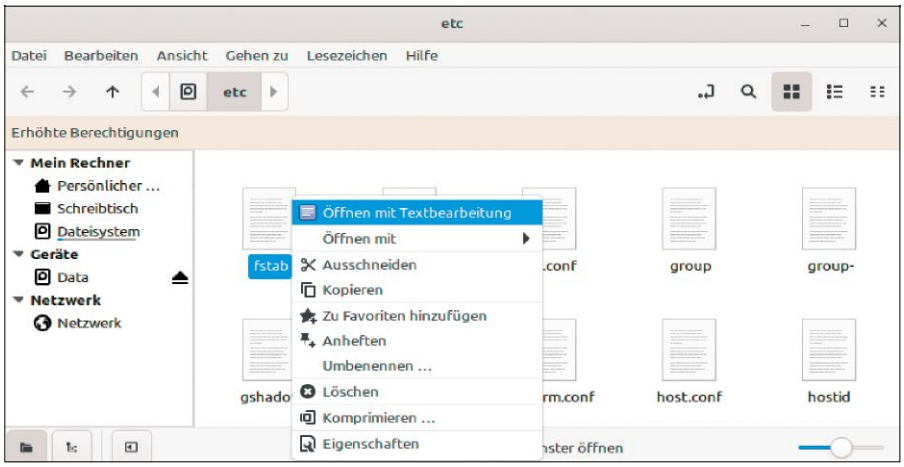
Bei Linux Mint funktioniert die Rechtevergabe im Dateimanager Nemo ähnlich. Es gibt die Rubriken „Eigentümer“, „Gruppe“ und „Andere“, bei der letzten fehlt allerdings die Beschriftung. Hinter „Ordnerzugriff“ stellen Sie die Zugriffsrechte ein. Zusätzlich gibt es Auswahlfelder hinter „Dateizugriff“. Die Einstellungen gelten für alle Unterordner und Dateien, wenn Sie auf „Zugriffsrechte auf enthaltene Dateien übertragen“ klicken.

Mehr Rechte anfordern: Beim Versuch einen Ordner zu öffnen, für den Sie kein Leserecht besitzen, erscheint bei Ubuntu und Linux Mint ein Fenster, in dem Sie den Vorgang mit Ihrem root-Passwort bestätigen. Dem Pfad in der Adressleiste (einblenden

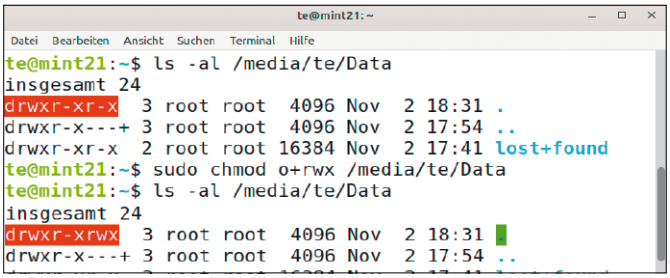
mit Strg-L) wird dann ein „admin://“ vorangestellt. Sie arbeiten im Dateimanager jetzt mit root-Rechten und dürfen die Zugriffsrechte der enthaltenen Elemente ändern.

Unter Ubuntu ist es nun möglich, neue Ordner anzulegen oder Dateien in das Verzeichnis zu kopieren. Über den Kontextmenüpunkt „Mit Textverarbeitung öffnen“ lassen sich Dateien mit erhöhten Rechten bearbeiten, wobei das Passwort erneut abgefragt wird. Mehr Komfort bietet die Installation des Pakets „nautilus-admin“. Das Kontextmenü von Ordnern wird damit um die Option „Als Systemverwalter öffnen“ erweitert und bei Dateien erscheint „Als Systemverwalter bearbeiten“.

Linux Mint verhält sich anders. Ist ein Ordner mit dem Präfix „admin://“ geöffnet, lassen sich keine neuen Ordner anlegen. Über „Öffnen mit Textverarbeitung“ kann man eine Datei zum Bearbeiten öffnen, das Passwort wird erneut abgefragt. Linux Mint bietet den Kontextmenüpunkt „Als Systemverwalter öffnen“ bereits standardmäßig. Anders als bei Ubuntu öffnet sich damit aber ein neues Fenster des Dateimanagers, in dem der Hinweis „Erhöhte Berechtigungen“ zu sehen ist. Sie arbeiten hier mit root-Rechten ohne Einschränkungen. In diesem Modus sollten Sie besonders vorsichtig sein, damit wichtige Systemdateien nicht versehentlich gelöscht werden.



Dateimanager als „root“: Linux-Mint-Nutzer verwenden den Kontextmenüpunkt „Als Systemverwalter öffnen“, um mit höheren Rechten Systemdateien zu bearbeiten.



Rechte im Terminal ansehen und setzen: Bei zusätzlichen Ext4-Laufwerke erlaubt man mit „chmod o+rwx“ allen Benutzern den Schreibzugriff auf das Verzeichnis unter „/media/[user]“.

Rechtevergabe im Terminal

Im Terminal lassen sich die Zugriffsrechte mit dem Befehl chmod ändern:

```
chmod o+rx /home/[User]
```

„Andere“ („o“ – „others“), also alle Benutzerkonten des Systems, dürfen dann auf das Home-Verzeichnis von „[User]“ zugreifen und Dateien lesen. Mit

```
chmod o-rx /home/[User]
```

entziehen Sie „Andere“ die Zugriffsrechte. Die anderen Benutzer des PCs können das Home-Verzeichnis von „[User]“ nicht mehr öffnen. Entsprechend setzen Sie statt „o“ die Buchstaben „u“ für einzelne Benutzer und „g“ für Gruppe ein. Will man die Berechtigungen für Ordner ändern, die einem nicht gehören, muss „sudo“ vorangestellt werden.

Zur Kontrolle lässt man sich die Zugriffsrechte mit

```
ls -al /home/[User]
```

anzeigen. In der ersten Spalte sind die Rechte mit „r“, „w“ und „x“ (lesen, schreiben, ausführen) zu finden, in der Reihenfolge „Besitzer“, „Gruppe“ und „Andere“. Ist der erste Buchstabe ein „d“, handelt es sich um einen Ordner.

Rechte rekursiv setzen: Ein typisches Beispiel ist das Verzeichnis des Apache-Webservers „/var/www“. Ist hier ein Content-Management-System wie Wordpress installiert, benötigt der Webserver Schreibrechte, damit er Dateien ändern oder erstellen kann. Mit der Zeile

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

wird zunächst der Besitzer und die Gruppe für das Benutzerkonto des Webservers geändert. Die Option „-R“ (rekursiv) bearbeitet alle Dateien und Ordner unter „/var/www“. Die tatsächlichen Rechte setzen Sie dann mit diesen zwei Befehlen:

```
sudo find /var/www -type d -exec
  chmod ug+rwx,o+rx {} +
sudo find /var/www -type f -exec
  chmod ug+rw,o+r {} +
```

Der erste Befehl wirkt sich rekursiv auf Ordner („d“ für „directory“) aus und erlaubt Eigentümer und Gruppe den Vollzugriff. „Andere“ dürfen den Inhalt der Verzeichnisse lesen. Die zweite Zeile ändert die Rechte von Dateien („f“ für „file“). Eigentümer und Gruppe erhalten Lese- und Schreibrechte, „Andere“ nur die Leseberechtigung.

Besonderheiten bei zusätzlichen Laufwerken

USB-Sticks, SD-Karten oder USB-Laufwerke sind meist mit den Dateisystemen FAT32, ExFAT oder NTFS formatiert. Ubuntu und Linux Mint binden externe Laufwerke automatisch in das Dateisystem ein und man kann über den Dateimanager darauf zugreifen. Die Linux-Zugriffsrechte gelten bei den genannten Dateisystemen nicht und der Benutzer erhält Vollzugriff.

Wird ein externes Laufwerk oder eine zweite Festplatte im PC mit einem Linux-Dateisystem wie Ext4 formatiert, berücksichtigt Linux die Benutzerrechte. Wenn es unter „/media/[User]/[Name]“ eingehängt ist, hat nur der Eigentümer „root“ Schreibzugriff. Um das zu ändern, starten Sie im Terminal

```
sudo chmod o+rwx /media/[User]/
  [Name]
```

„[User]“ ersetzen Sie durch Ihren Benutzernamen, „[Name]“ durch die Bezeichnung des Ordners, in den das Laufwerk eingehängt ist. Sind bereits Dateien und Ordner vorhanden, ändern Sie die Rechte rekursiv mit „find“ wie oben beschrieben. ■

Verlag

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, Stephan Lamprecht, 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 Stahl

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:
fotomek, Fajar, vectorlady, Thomas, hywards – AdobeStock; 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 2570-4362







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.

Digital Life

Windows & Linux



Jetzt am Kiosk!

Für nur 5,90 €

Gratis: Komplett-Paket auf Heft-DVD!

Bestellen unter
www.idgshop.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 3/23 Windows & Linux 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

Linux Installation

Mit unserer WebFAI richten wir Ihre Linux-Installation vollautomatisiert und exakt so vollständig funktionsfähig ein, wie dies in unserer Fertigung bei TUXEDO Computers vorgenommen wird!

Linux Distribution

Zur Auswahl stehen alle Linux Distributionen, die wir auch in unserem Onlineshop-Konfigurator zur Auswahl anbieten. Je nach Distribution haben Sie die Wahl zwischen verschiedenen Desktopoberflächen.

immer aktuell

Durch unsere WebFAI erhalten Sie zudem von unseren Servern immer unsere aktuellsten von uns getesteten Linux Betriebssystemsversionen.



TUXEDO **Web**FAI

Fully Automated Installation

100% Linux

5 Jahre Garantie

Lifetime Support

Gefertigt in Deutschland

Deutscher Datenschutz

Support vor Ort

TUXEDO

tuxedocomputers.com