LINUX WELT XXL



LINUX WELT XXL

4 190702 312900 02

+++ Aus für Windows 7! Jetzt auf Linux wechseln! +++

SONDERHEFT XXL
2/2020 Juli – September
€ 12,90 Schweiz 25,80 sfr
Österreich, Benelux € 14,40

NEU!
196 Seiten!

Linux statt Windows

Gratis! Sicher! Einfach!

Das Umsteiger-Handbuch 2020

Einfach auf Linux wechseln
Linux direkt von der Heft-DVD starten und ausprobieren · System parallel zu Windows installieren · Programme für Office, Internet & Co. nutzen

Linux optimal nutzen
Das beste Linux finden · Jede Hardware nutzen · System richtig einstellen · Neue Software laden · Sicher im Internet surfen u.v.m.

Tipps und Tricks für Profis
Linux schneller starten · Mehr Funktionen für Firefox, Libre Office & Co. · Systemaufgaben automatisieren u.v.m.



Exklusiv auf DVD!

LinuxWelt Toolbox

Die besten Programme für System, Netzwerk, Office und Sicherheit



Linux-Komplett-Paket mit 8 GB!

9 Top-Systeme auf der Multiboot-DVD

PLUS: 50 Linux-Handbücher mit 8000 Seiten

PLUS: Rettungs-DVD mit 10 Notfall-Tools

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

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

BEZAHLEN

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 macht gute Laune!

Linux ist kostenlos, läuft auf fast allen Rechnern und bietet eine unfassbar große Zahl an nützlichen und ebenfalls kostenlosen Programmen. Einsteiger und Fortgeschrittene greifen bei Fragen auf eine riesige und hilfsbereite Community in Foren und sozialen Netzen zu. Und schließlich bereitet das reine Ausprobieren von neuer Software den meisten Nutzern großen Spaß. So macht Linux einfach gute Laune – und die können wir in Zeiten von Corona gut gebrauchen. Ein schöner Zeitvertreib ist es zudem, wenn man Linux perfekt auf dem eigenen Rechner einrichtet.

In diesem Linux-Handbuch 2020 finden Linux-Neulinge einen rund 50 Seiten umfassenden Einsteiger-Guide, der alle wichtigen Punkte für den reibungslosen Linux-Erstkontakt erklärt. Von der Auswahl des besten Desktops und des passenden Linux-Systems über die richtige Systempflege bis hin zur Auswahl und Aktualisierung von Programmen. Fortgeschrittene Anwender und Profis finden in den weiteren Ratgebern neue und nützliche Hinweise für ihr Linux. Auf der Heft-DVD schließlich warten neun Linux-Systeme zum Ausprobieren und Installieren – darunter das für Windows-Umsteiger geeignete Linux Mint 19.3. Die meisten Systeme auf der DVD können Sie direkt von dort aus starten und völlig gefahrlos für Ihr eigentliches System testen.

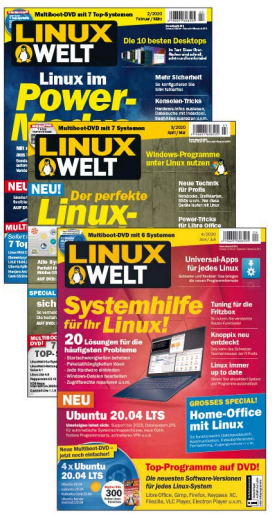
Viel Spaß mit Linux!



Arne Arnold
Redakteur
aarnold@it-media.de

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

Wenn Ihnen die LinuxWelt gefällt, können Sie sich das Heft für sechs Monate per Mini-Abo einfach ins Haus schicken lassen. Sie sparen damit satte 33 Prozent und erhalten noch einen Gutschein dazu.
Gratis-Versand: Mit dem Mini-Abo der LinuxWelt bekommen Sie drei Ausgaben der LinuxWelt ohne Versandkosten direkt nach Hause geliefert. In der Regel treffen sie noch vor dem offiziellen Verkaufsstart bei Ihnen ein.
Digitaler Zugriff: Als Ergänzung zum Mini-Abo der gedruckten Hefte bekommen Sie Ihre Ausgaben auch digital auf Ihr Mobilgerät.
33 Prozent sparen plus Gutschein: Mit dem Mini-Abo zahlen Sie nur 17 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.

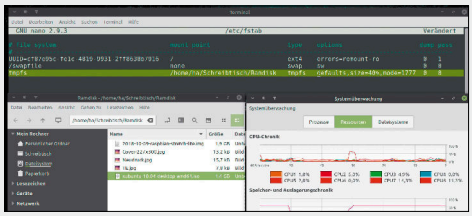




Linux für jeden Zweck!

In diesem Heftschwerpunkt verraten wir nicht nur, welches Linux sich für welchen Anwender eignet, sondern zeigen auch, welches System gut zu den verschiedenen Einsatzgebieten passt.

S. 90



Die 30 besten Systemtipps

So läuft Ihr Linux stabil, sicher und absolut zuverlässig.

S. 38



Sicher surfen!

Linux ist das wohl beste System zum sicheren Surfen.

S. 118

Grundlagen

6 **Das große LinuxWelt-Handbuch 2020**
In dieser XXL-Ausgabe stecken besonders viele Ratgeber und Tricks sowie eine randvolle DVD

8 **Linux-Systeme auf DVD**
Sie finden 9 Top-Systeme auf der Heft-DVD, etwa Linux Mint Cinnamon 19.3 und Ubuntu Mate

12 **Linux-Desktops 2020**
Für Linux gibt es viele Desktops mit großen Unterschieden. Die 10 interessantesten stellen wir vor

14 **Der Schlichte:** Gnome 3
15 **Der Umfangreiche:** KDE Plasma
16 **Für Umsteiger:** Cinnamon
17 **Der Klassische:** Mate
18 **Der Sparsame:** XFCE
19 **Die leichten L-Desktops**
20 **Der Reduzierte:** Deepin
21 **Der Einfache:** Budgie
22 **Der Schöne:** Pantheon
23 **Der Schnelle:** Moksha

Für Ein- und Umsteiger

24 **Der Umgang mit ISO- und IMG-Dateien**
So machen Sie aus Imagedateien bootfähige DVDs und USB-Sticks für die Linux-Installation

28 **Ubuntu-Installationen**
Das müssen Sie wissen, wenn Sie Ubuntu installieren möchten

32 **Grundlagen der Systemverwaltung**
Nach der Linux-Installation sollten Sie dringend diese Systemeinstellungen ändern

38 **Die 30 besten Systemtipps**
Wenn Linux läuft, lässt sich noch einiges tunen. Die 30 besten Systemtipps finden Sie hier

46 **Crashkurs zur Netzwerkhardware**
Für kleine Heimnetze genügt es oft, den Router gut einzustellen

50 **Linux und die Datenträger**
Mit diesen Tools partitionieren und formatieren Sie Festplatten, SSDs und USB-Sticks richtig

58 **Linux/Windows: Austausch & Kompatibilität**
Windows-Umsteiger können mit diesen Tools und Tricks ihre vorhandenen Dateien weiter nutzen

62 **Programme für Umsteiger**
Das sind die besten Umsteiger-Anwendungen für Office, Internet, Video, Audio & Co.

66 **Viren finden und beseitigen**
Es gibt nur wenige Viren, die Linux gefährlich werden können. Doch auch diese muss man abwehren

68 **Windows-7-System virtualisieren**
Windows 7 lässt sich einfach in einer Virtualbox weiter nutzen

Hardware & Netzwerk

72 **Die beste Linux-Hardware 2020**
Nicht jede Hardware arbeitet mit Linux gut zusammen. Wir zeigen, worauf Sie achten müssen

78 **Hardwarekontrolle mit Sensoren**
So nutzen Sie die Sensoren von Hauptplatine & Co.

82 **Rechner automatisch abschalten & starten**
Sie sparen Strom und die Hardware hält länger, wenn Sie Rechner auch mal ausschalten

84 **Fritzbox: Tipps & Tuning**
Diese Fritzbox-Tipps sollten Sie für Ihr Netzwerk beachten

88 **Raspberry Pi 4 als Desktop**
Der neue Raspberry Pi 4 hat genug Power für einen Desktop-PC

Software

150 Software und Paketverwaltung
Neue Anwendungen beziehen Sie aus dem Software-Repository

154 Container statt Pakete
Wer neuere Programmversionen nutzen möchte, verwendet Software im Container

156 Zusätzliche Paketquellen verwenden
Es gibt mehr als die Standard-Paketquellen von Ubuntu & Co.

158 Toolbox für Ubuntu & Mint
Die LinuxWelt-Toolbox liefert Ihnen als komfortables Werkzeug viele nützliche Anwendungen

162 Programme & Tools fürs Netzwerk
Linux fühlt sich im Netzwerk traditionell zu Hause. Mit diesen Tools tun Sie das auch

166 Tools für Audio, Video & Foto
Linux-Nutzer können mehrere Mediaplayer verwenden, je nach gewünschtem Funktionsumfang

168 Office-Pakete und Produktivität
Das sind die wichtigsten Zusatztools für Libre Office & Co.

170 Software für Platinenrechner
Der Raspberry Pi als Dateiserver, Mediacenter und mehr

172 Tools für die Linux-Automatisierung
Regelmäßige Aufgaben wie Backups lassen sich unter Linux automatisch durchführen

174 Service- & Mobilsysteme
Linux-Systeme sind flexibel und starten von jeder Art Datenträger

Tipps & Tricks

176 Programme und Schalter
Startparameter für viele Tools

180 Webbrowser und ihre Schalter
Firefox und Co. besser starten

182 Schaltergigant VLC
Der VLC lässt sich gut steuern

184 Veracrypt: Alles im Terminal
So verschlüsseln Sie schneller

185 Virtualbox via Terminal
Profitricks für Virtualbox

186 Office & Produktivität
Parameter für Libre Office & Co.

188 Systemtools & Zubehör
Wertvolle Automatisierung

192 Parameter des Linux-Kernels
Linux besser starten



Die Highlights der Heft-DVD lesen Sie auf der nächsten Seite

Standards

3 Editorial
194 Impressum

Linux für jeden Zweck

90 Was Sie über Ubuntu wissen müssen
Ubuntu ist das einfache Standardsystem für zuverlässige Desktoprechner

94 Neu: Linux Mint 19.3
Für Windows-Umsteiger ist das neue Linux Mint 19.3 ideal

100 Re- und Upcyling mit Linux
Alte Notebooks und Netbooks können mit Linux noch viele Jahre gute Dienste verrichten

102 Preiswerte Server dank Linux
Linux macht Minirechner, alte Hardware oder NAS-Systeme zu kostengünstigen Servern

104 Große und kleine Serverrollen
Mit diesen Tricks und Tools nutzen Sie Linux als Server

106 Linux auf USB: Die Werkzeuge
Mit diesen Tools bringen Sie Linux-Systeme auf USB-Sticks

110 Tools & Distris für USB
Linux live auf USB erledigt Reparaturen und Notfallkopien u. v. m.

114 Sicherer USB-Tresor
Ein richtig verschlüsselter USB-Stick verwahrt Dateien sicher

116 USB-Ideen: Medien, Systeme & Infos
Linux lässt sich auf USB-Medien auch ganz normal installieren



Sicherheit

118 Sicher surfen mit Linux
Linux ist sicher, zumindest sicherer als Windows. Davon sind Linux-Nutzer überzeugt

122 Sicher surfen – live oder virtuell!
Linux surft sicher! Noch sicherer wird Linux live oder virtuell

126 Sichere Browser
Kein Chrome oder Firefox kennt alle Minenfelder des Internets. Darum helfen diese Tipps

130 Mit VPN sicher durchs Netz
Mit VPN surfen Sie auch in fremden Netzen sicher und verschlüsselt

134 Mehr Schutz dank Sicherheitsschlüssel
Allein mit einem Passwort sind Onlinedienste nicht optimal geschützt

138 Firefox-Sicherheit
Dieser Beitrag erklärt die Techniken für Sicherheit und Datenschutz in Firefox

140 Thunderbird-Sicherheit
Mails an sich sind nicht gefährlich. Aber sie sollten Mails bleiben, nicht ins Web gehen …

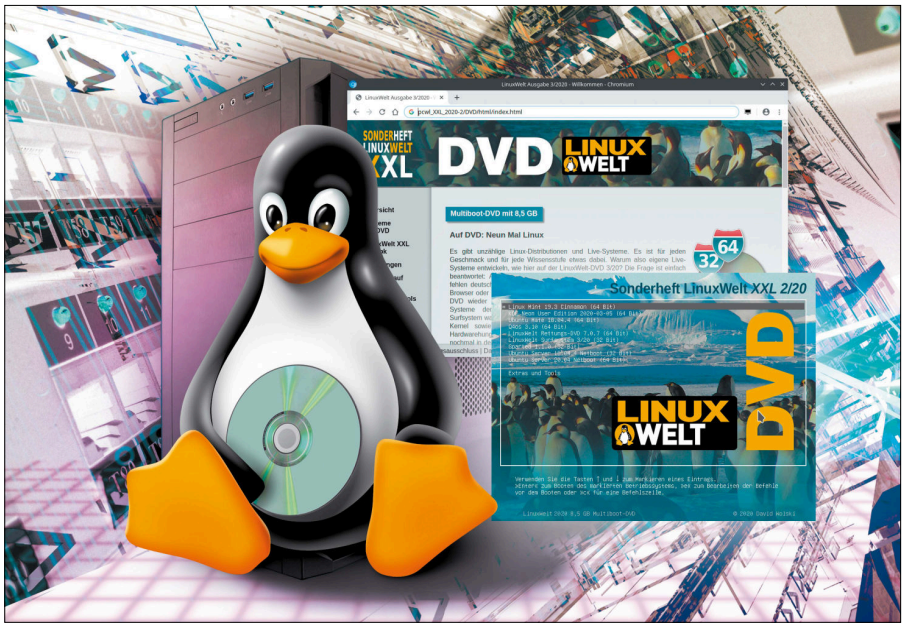
142 Datenverschlüsselung mit Linux
Wer sich den alleinigen Zugriff auf bestimmte Daten sichern will, muss diese richtig verschlüsseln

144 Veracrypt-Container
Veracrypt ist die beste Wahl, wenn Daten auf mehreren Systemen genutzt werden

148 Die besten Systemschutzmaßnahmen
Diese Einstellungen sollten Sie in Ihrem Linux vornehmen

Das große LinuxWelt-Handbuch 2020

Diese LinuxWelt präsentiert sich im XXL-Format mit extra vielen Ratgebern und Tipps. Und auch die beiliegende DVD ist randvoll mit neun Linux-Systemen und Distributionen. Zudem gibt es eine umfangreiche Bibliothek an freien Handbüchern für den Linux-Einstieg.



VON DAVID WOLSKI

Linux ist als Betriebssystem auf Servern, in der Cloud und auf Embedded-Geräten wie dem Raspberry Pi längst etabliert. Es hat traditionelle Unix-Systeme ab den späten 90er-Jahren aufgrund seiner freien Verfügbarkeit auf Servern bis heute nahezu völlig verdrängt. Auf Mobilgeräten hat der von Android genutzte Linux-Kernel die Entwicklung von Smartphones mitgeprägt und erschwingliche Geräte möglich gemacht. Ist Linux in seinen Ausprägungen, wir sprechen hier nicht nur vom Kernel allein, ein universelles Betriebssystem für jeden Einsatzzweck?

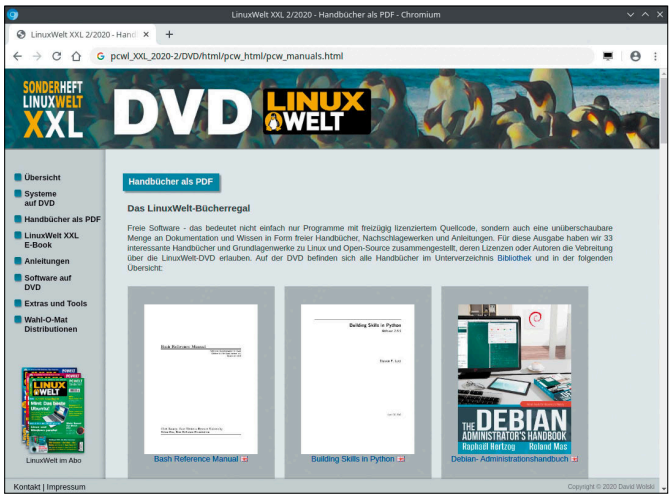
Schwerpunkt: Linux auf dem Desktop

Das ist heute immer noch nicht der Fall, denn die globale IT-Landschaft besteht eben auch aus Desktops. Die große Linux-Revolution auf dem Desktop, auf klassischen PCs als Anwendersystem ist ausgeblieben. In diesem Einsatzbereich ist Linux mit seinen tonangebenden, auf Heft-DVD vertretenen Distributionen, die durchaus einsteigerfreundlich sind, ein Exot geblieben. Neben Windows und Mac-OS X ist der Linux-Pinguin seltener anzutreffen und bleibt auch bei optimistischen Hochrechnungen bei einem weltweiten Marktanteil von lediglich drei Prozent. Dieser Prozentsatz bedeutet aber zumindest eine hohe absolute Zahl an Linux-Desktops, die sich hauptsächlich bei IT-Professionals wie Entwicklern und Administratoren finden, die jene Vorzüge einer ausgewachsenen Linux-Distribution schon seit deren Anfängen zu schätzen wissen: Sicherheit, Stabilität, aktuelle sowie spezialisierte Software und ein hohes Maß an Anpassungsfähigkeit.

Linux brilliert mit diesen Eigenschaften auch als Desktopsystem, Ubuntu und Linux Mint machen es vor (beide auf Heft-DVD). Aber es blieb bislang ein Betriebssystem für fortgeschrittene Anwender, die sich mit alternativen Softwarepaketen wie Libre Office zu helfen wissen oder mit der Hilfe von Wine vereinzelte Windows-Programme unter Linux einrichten können. In einer Umgebung wie im derzeit wichtigen Home-Office ist Linux als Desktop einem Windows durchaus ebenbürtig, mit seiner soliden, sicheren Entwicklung sogar überlegen, weil es mehrere Rollen übernehmen kann. Es bleibt eine Lernkurve für Umsteiger, die in diesem Sonderheft einen Schatz an sorgfältig zusammengetragenem Know-how aus dem LinuxWelt-Magazin finden, überarbeitet und neu nach Rubriken geordnet.

Ratgeber und Praxiswissen

Nach der Vorstellung der Distributionen auf Heft-DVD im nächsten Beitrag geht es auch gleich zu einer Übersicht der wichtigen Linux-Desktops. Denn es gibt eine überwältigend große Vielfalt von Distributionen und Desktopumgebungen. Nicht jeder Desktop passt in jedes Umfeld, zu jedem Wissensstand und zu allen Geschmäckern. Ausge-



Die LinuxWelt-Bibliothek: 50 freie Handbücher zu Linux und Open-Source-Software haben als PDF auf DVD Platz gefunden. Einige der PDFs liegen in Englisch vor, viele aber auf Deutsch.

rechnet die tonangebenden Desktops, Gnome und KDE, sind oft erst mal gar nicht die richtigen Einstiegspunkte für Umsteiger aus der Windows-Welt. Mit einem Einsteig geht es auch gleich weiter, denn in der ersten Rubrik geht es um Grundlagen, die einen erfolgreichen Start mit Linux auf dem Laptop oder PC mit diesem Magazin und den Distributionen auf Heft-DVD möglich machen. Auch wenn der Zielrechner selbst kein optisches Laufwerk hat, sind die Systeme nützlich, denn diese liegen auch als originalgetreue ISO-Datei auf DVD vor. Mit den ISO-Dateien lassen sich bootfähige USB-Sticks erzeugen, wie ein Beitrag in der Einsteiger-Rubrik Schritt für Schritt zeigt. Außerdem geht es dort um die Installation von Ubuntu-Systemen, die ersten Schritte in der Administration und um den Aufbau eines heimischen Netzwerks mit Linux im Mittelpunkt.

Sicherheit und Software

In einem Magazin, das Linux von seinen besten Seiten zeigen will, darf das Thema Sicherheit natürlich nicht fehlen, das hier aber keineswegs unkritisch betrachtet wird. Es ist richtig, dass ein Linux-System weit sicherer als Windows sein kann und aufgrund des Entwicklungsprozesses des Kernels und seiner wichtigen Komponenten bessere Voraussetzungen mitbringt. Eine korrekte Konfiguration und ein sicherheitsorientiertes Anwenderverhalten sind dabei jedoch ausschlaggebend. Eine Rubrik zum Thema Sicherheit beschäftigt sich mit den Vorzügen von Linux als sicheres Surfsystem, da zu diesem Zweck auch unsere aktualisierte Eigenentwicklung auf Heft-DVD ist. Es geht dazu aber auch um die Absicherung des eigenen installierten Linux-Systems, um die revolutionäre VPN-Technologie „Wireguard“ und um Verschlüsselung von Datenträgern.

Wer gerade erst zu Linux stößt, bekommt mit Distributionen wie Ubuntu Mate 18.04.4 (auf Heft-DVD) bereits einige Hilfestellung bei der Ausstattung des Systems mit alltagstauglicher Software. Dieses Konzept übernimmt die LinuxWelt Toolbox 1.8, die ebenfalls etliche nützliche Linux-Programme kurz in Kategorien vorstellt und eine Installation unter Debian, Ubuntu und seinen Varianten mit wenigen Klicks erlaubt.

Handbücher auf DVD: 50 PDF-Dateien

Einsteiger mussten vor einigen Jahren noch hohe Hürden nehmen, um sich mit Linux und Open Source vertraut zu machen. Dokumentation und Handbücher lagen meist in Form von anspruchsvoll geschriebenen, englischsprachigen How-to-Dateien vor oder auch als teure Wälzer von Fachverlagen. Generell war die Dokumentation zur Open-Source-Software aber immer ein wunder Punkt dieser freien Projekte und oft wenig mehr als ein Nachgedanke. Diese Situation hat sich deutlich verbessert und wer sich mit Fachbüchern und Dokumentationen weiterbilden will, findet auch zu beinahe jedem Thema der IT einen Einstieg in freien Anleitungen.

Zu dieser Ausgabe haben wir 50 interessante Handbücher sowie Grundlagenwerke zu Linux und Open Source gesammelt und auf der LinuxWelt-Heft-DVD untergebracht. Dieses Bücherregal liegt auf der DVD im Unterverzeichnis „Bibliothek“ und deckt recht unterschiedliche Bereiche von Linux-Desktops, Distributionen, Serveradministration bis Libre Office ab.

Es ist also für jeden Wissensstand und für jedes populäre Anwendungsgebiet etwas dabei. ■



AUF DVD – HIGHLIGHTS

Distributionen

- Linux Mint Cinnamon 19.3 (64 Bit)
- Ubuntu Mate 18.04.4 (64 Bit)
- KDE Neon User Edition (64 Bit)
- Q4-OS 3.10 (64 Bit)
- LinuxWelt-Surfsystem XXL (32 Bit)
- LinuxWelt-Rettungs-DVD 7.0.7 (64 Bit)
- Gparted Live 1.1.0 (32 Bit)
- Ubuntu Server Netboot 18.04.4 (32 Bit)
- Ubuntu Server Netboot 20.04 (64 Bit)

Bootfähige Extras und Tools

- Hilfen & Tools: Super Grub Disk, Memtest, HDT, DBAN, Plop Bootmanager
- LinuxWelt Toolbox 1.8
- Der Softwareinstaller der LinuxWelt in neuer Version. Empfehlungen und Ein-Klick-Installation
- LinuxWelt Digital XXL
- Gesammelte, zeitlose Artikel der LinuxWelt auf über 300 Seiten
- Die LinuxWelt-Bibliothek
- 50 freie Handbücher zu Linux und Open Source, jeweils als PDF

Linux-Systeme auf DVD

Das freie Betriebssystem kommt hier groß raus: Die Heft-DVD ist randvoll mit nützlichen Linux-Distributionen und mit cleveren Livesystemen abgerundet. Alle Systeme sind hier kurz sowie ausführlicher auf der HTML-Oberfläche der DVD vorgestellt.



VON DAVID WOLSKI

Diese DVD dreht sich um Distributionen und Livesysteme, die Linux von seiner besten Seite zeigen. Deshalb sind nicht nur Desktopsysteme vertreten und jene mit den bekannten Namen. Auch die Serverausgabe von Ubuntu sowie ein neues Rettungs- und Surfsystem der LinuxWelt-Redaktion sind in neuen Versionen mit dabei. Es gibt unzählige Linux-Distributionen und Livesysteme. Es ist für jeden Geschmack und für jede Wissensstufe etwas dabei. Warum also eigene Livesysteme entwickeln, wie hier für das Sonderheft XXL? Die Frage ist einfach beantwortet: Auf fertigen Systemen passt immer etwas nicht, beispielsweise fehlen deutschsprachige Übersetzungen, ein deutsches Tastaturlayout, aktuelle Browser oder ein besonders frischer Linux-Kernel. Von den Eigenentwicklungen abgesehen, geht es diesmal um starke Desktops: Linux Mint 19.3, Ubuntu Mate 18.04.4 und Q4-OS 3.10 erlauben auch Neueinsteigern einen schnellen Start mit dem eigenen Linux-System.

Multibootmenü: Alle Systeme von DVD starten

Der Weg zum laufenden System ist kurz: Um eine der Linux-Varianten von der DVD zu starten, legen Sie den Datenträger in das optische Laufwerk und starten den Rechner neu. Booten Sie dabei nicht von der Festplatte, sondern von der DVD. Dazu rufen Sie entweder beim Start per Tastendruck das Bootmenü der Firmware oder des Bios auf, was meist mit der Taste F8 oder F12 gelingt. Oder Sie ändern die Bootreihenfolge im Bios. Welche Taste Sie drücken müssen, verraten die Meldungen am Bildschirm. Die DVD startet nur im Bios-Modus und die Option „CSM/Legacy-Modus“ muss dazu in den Uefi-Einstellungen moderner PCs und Notebooks aktiviert sein. Der Uefi-Boot und Secure Boot wird von der Heft-DVD nicht unterstützt. Ein übersichtliches Multibootmenü stellt alle startfähigen Linux-Systeme zur Auswahl und hat für alle Einträge jeweils noch Untermenüs für die wichtige Startoptionen in petto.

Was tun ohne optisches Laufwerk? Auch in diesem Fall ist die Heft-DVD nicht wertlos. Denn alle sieben Systeme und die Installer zu Ubuntu Server 18.04.4 und 20.04 sind auch als ISO-Datei auf der DVD. Somit können Sie auf einem anderen PC ein System auf eigene Faust auf eine DVD beziehungsweise DVD brennen oder auch gleich auf einen schnellen USB-Stick schreiben. Auch dazu finden sich Hilfsprogramme auf DVD: Für Windows ist zum Brennen der ISO-Dateien, die sich auf der DVD im gleichnamigen Verzeichnis befinden, das Open-Source-Programm Infrarecorder 0.53 bestens geeignet. Zur Übertragung einer ISO-Datei auf USB-Stick dient das Windows-Programm Win 32 Disk Imager 1.0. Linux hat mit dd übrigens schon von Haus aus ein Tool zur Übertragung von Imagedateien auf Sticks an Bord.

Für alte und neue Hardware

Die meisten Livesysteme und Distributionen auf dieser DVD liegen jetzt in 64 Bit vor, denn 32-Bit-Systeme sind definitiv auf dem Weg auf das Abstellgleis. Allerdings sind Linux-Systeme für 64 Bit nicht enorm anspruchsvoll: Sie verlangen auch nur einen Prozessor der letzte 13 Jahre, angefangen mit dem AMD Athlon 64 und dem Intel 4 Prescott, denn diese CPUs boten bereits 64-Bit-Unterstützung. Nun gibt es natürlich dennoch ältere und richtig alte Geräte, die keine 64-Bit-Systeme starten können. Dazu zählen beispielsweise Intel-Atom-PCs, die eine 32-Bit-Distribution wegen ihres Bootloaders verlangen. Es gibt deshalb auch bei uns keine komplette Absage an 32 Bit: Lubuntu 18.10, das LinuxWelt-Surfsystem und Ubuntu Server 18.04.1 sind in ihrer 32-Bit-Ausgabe auf DVD vorhanden. Denn sie sind generell nützlich und sollen deshalb möglichst zu jeder PC-Hardware kompatibel sein. Außerdem zeigt Lubuntu 18.10 mit seinem geringen Ressourcenbedarf, dass auch ältere Rechner noch nicht zwangsläufig zum alten Eisen gehören. ■

Linux Mint 19.3 Cinnamon

Zweifelsohne ist Linux Mint mit seinem Cinnamon-Desktop eines der populärsten Linux-Systeme für Einsteiger. Es liegt als einfach zu installierendes Livesystem vor und basiert auf Ubuntu 18.04.3, das den Betriebssystemunterbau auf den Stand von Ubuntu mit Langzeitsupport bringt. Dies bedeutet, dass die Softwareausstattung von Linux Mint 19.3 (in 64 Bit auf DVD) inzwischen nicht mehr die neusten, dafür aber ausgereiften Programme umfasst. 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 und Xviewer ist ein Bildbetrachter. Der Videoplayer wurde aber gegen das Programm Celluloid ersetzt, da es auf MPV aufbaut und damit sehr performant arbeitet. Das hier verwendete Cinnamon hat ein Update auf 4.4 mit angenehmen Änderungen bekommen. Mint 19.3 erhält Updates bis April 2023. ■



Perfekter Einstieg: Linux Mint hat als Ubuntu-Ableger und durch seine Hilfestellungen sowie dem traditionellen Desktop Cinnamon viele Freunde gewonnen.

Ubuntu Mate 18.04.4

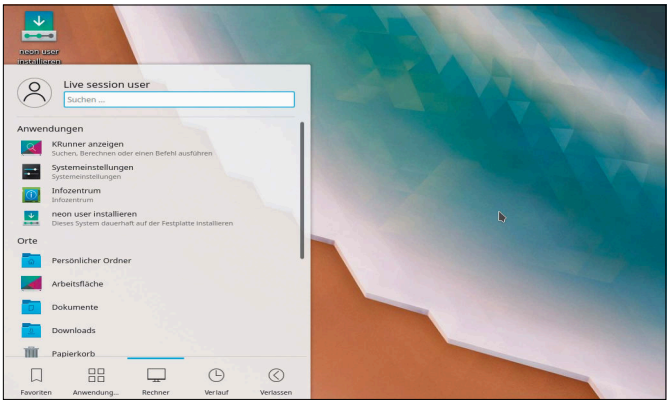
Der heimliche Star unter den offiziellen Ubuntu-Ausgaben ist das einsteigerfreundliche Ubuntu Mate. Es bringt Tugenden früherer Ubuntu-Versionen zurück und füllt damit eine Lücke, die zwischenzeitlich nur Linux Mint füllen konnte. Mate folgt als Desktopumgebung dem Bedienkonzept von Gnome 2, ist aber als Abspaltung so weit entwickelt, dass sich jetzt ab Mate 1.20 auch aktuelle Anwendungen gut in den Desktop einfügen. Die Arbeitsumgebung ist sehr anpassungsfähig und der Menüpunkt „System → Einstellungen → Darstellung → Mate Tweak“ erlaubt unter „Leisten“ die bequeme Auswahl verschiedener Desktoplayouts. Unter anderem gibt es hier die Einstellung „Mutiny“, die eine Leiste am Bildschirmrand im Stil von Unity nachbildet. Ubuntu Mate (in 64 Bit auf DVD) bringt eine Softwareausstattung, die für den Gnome-Desktop typisch ist, mit Firefox, Libre Office 6.0, Thunderbird 60 und VLC 3.0.4. Als grafische Paketverwaltung dient die „Software Boutique“ im Menü „System → Systemverwaltung“. ■



Aufgefrischt: Ubuntu Mate 18.04.4 liefert alle Updates, die bisher für Ubuntu 18.04 erschienen sind. Ein Upgrade auf die nächste Ubuntu-Version ist möglich.

KDE Neon User Edition

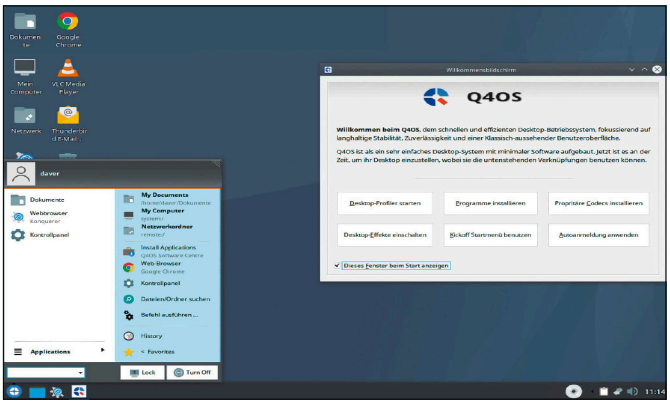
KDE Plasma ist der perfekte Desktop für fortgeschrittene Anwender, die gut mit einem opulenten Funktionsumfang zurechtkommen und die Arbeitsumgebung gerne bis ins Detail selbst konfigurieren. KDE Neon ist das laufend aktualisierte Vorzeigesystem für KDE Plasma und hat einige Vorteile gegenüber anderen Distributionen. Denn KDE Plasma 5 entwickelt sich schnell weiter. Eine Distribution wie Kubuntu oder Open Suse Leap kann dabei nicht immer Schritt halten. Und ein Arch Linux und dessen Abkömmlinge wie Manjaro oder Endeavour-OS sind dagegen oft zu aktuell und liefern zwischenzeitlich keinen robusten Desktop für die tägliche Arbeit. Diese Lücke füllt KDE Neon, denn die User Edition hat KDE-Pakete an Bord, die zwar frisch, aber nicht ungetestet sind. In der vorliegenden Ausgabe der KDE Neon User Edition (64 Bit) mit Langzeitsupport ist KDE Plasma 5.18 enthalten. Die KDE-Komponenten werden auch in der vorliegenden User Edition teilweise als Rolling Release gepflegt. ■



Das offizielle System der KDE-Entwickler: Die KDE Neon User Edition präsentiert als Aushängeschild der KDE-Arbeitsumgebung einen gut gestalteten Desktop.

Q4-OS 3.10

Diese Distribution ist für den Einsatz auf älteren Windows-PCs interessant, die kein Windows 10 mehr stemmen können. Das schlanke Linux-System mit einer soliden Debian-Basis läuft auf diesen PCs der letzten zehn Jahre noch richtig flott. Ein System für ältere Rechner: In Q4-OS steht der Desktop Trinity im Mittelpunkt, der KDE 3.5 als schlanke, ansehnliche Desktopumgebung im Stil von Windows am Leben erhält. Dieser Desktop dürfte vielen erfahrenen Anwendern ein alter Bekannter sein und Linux-Einsteigern eine vertraute Arbeitsumgebung bieten. Bei Programmen für den Alltag setzt Q4-OS (in 64 Bit auf Heft-DVD) auf die Debian-Paketquellen und erleichtert Einsteigern die Einrichtung des Systems nach der Installation mit der Auswahl fertiger Softwaresets. Optional stehen so Libre Office 5, Chromium als Browser, VLC und Thunderbird zur Verfügung. Unter Debian immer gerne gesehen sind die per Klick ladbaren Mediacodecs. Die Paketverwaltung geht mit Synaptic. ■



Q4-OS mit Desktop Trinity: Die Arbeitsumgebung lässt das genügsame KDE 3.5 als Abspaltung weiterleben und setzt die Ähnlichkeit zu alten Windows-Versionen.

LinuxWelt-Surfsystem XXL

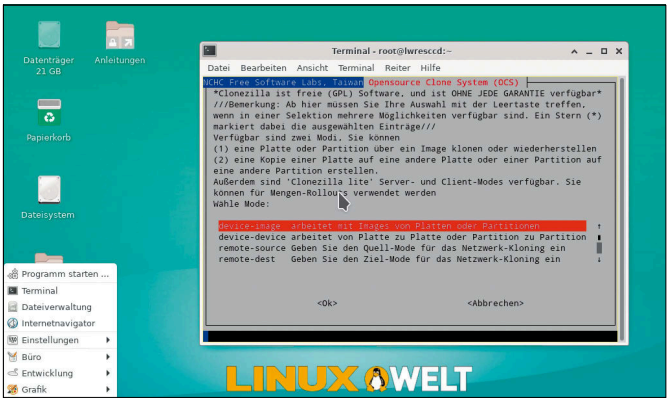
Neue Browser und ein neuer Linux-Kernel für das Surfsystem aus der LinuxWelt-Redaktion – bei diesem System auf der Basis von Porteus 4.0 geht es um gute Browser und eine kompakte, komfortable, deutschsprachige Desktopumgebung mit dem schlanken Mate-Desktop. Während ausgewachsene Livesysteme eine möglichst komplette Linux-Arbeitsumgebung mit etlichen Programmen einpacken möchten, zielt Porteus auf einen kleinen Satz nützlicher Programme ab. Der Name von Porteus, das als Basis dient, 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 individuell zusammengestellte Porteus-Ausgaben. Um genau das handelt es sich beim LinuxWelt-Surfsystem. Es liegt in 32 Bit und mit Kernel 5.5.4 vor, womit es mit aktueller sowie älterer Hardware kompatibel ist. Die WLAN-Verbindung richten Sie über den Network-Manager ein. ■



Besonders genügsames Livesystem: Das Surfsystem der LinuxWelt-Redaktion mit Firefox und Chromium läuft auch auf älteren Rechnern und liegt in 32 Bit vor.

LinuxWelt-Rettungs-DVD 7.0.7

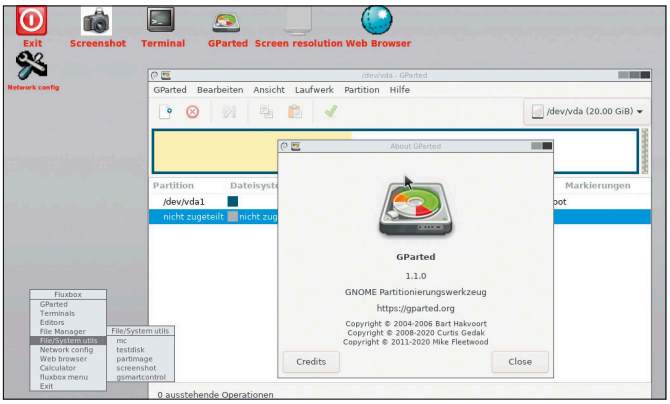
Dies ist ein Livesystem in 64 Bit, das sich zur Reparatur von liegengebliebenen Linux-Systemen und zur Datenrettung eignet – auch auf Windows-Rechnern. Das Livesystem ist jetzt aus Arch-Linux-Paketen aufgebaut und bringt alles mit, was ein PC-Experte braucht, um Daten von einem defekten Computer zu kratzen. Wie bei anderen Rettungssystemen liegt der Großteil der Werkzeuge in Form von Kommandozeilenprogrammen vor: Da es sich aber auf einer grafischen Oberfläche angenehmer arbeiten lässt, dient hier XFCE 4.14 als Desktop, der nach dem Boot startet. Um Daten von beschädigten oder gelöschten Partitionen zu retten, ist Testdisk und Photorec auf der Kommandozeile verfügbar. Auch das bewährte Imagingtool Clonezilla zum Spiegeln und Wiederherstellen von Partitionen und ganzen Festplatten läuft im Terminal. Als Front-End für den Portscanner Nmap ist Zenmap im Menü „Internet“ enthalten. Die WLAN-Verbindung konfiguriert man über den Network-Manager. ■



Grafische Programme runden die LinuxWelt Rettungs-DVD ab: Für Dateien ist der Dateimanager Thunar enthalten und als Browser steht Firefox ESR 68.4 bereit.

Gparted Live 1.1.0

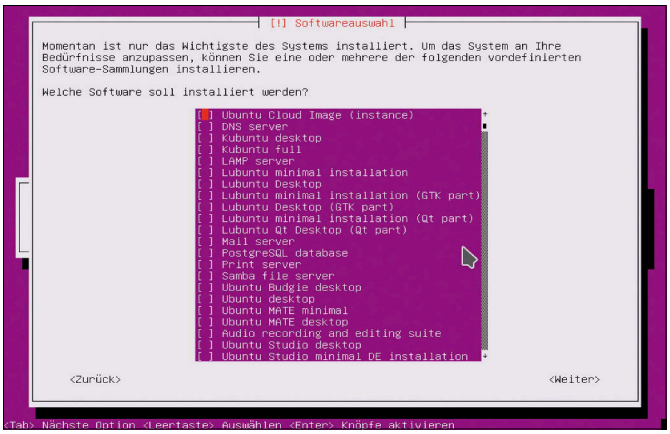
In Gparted Live dreht sich alles um den Partitionierer Gparted 1.1.0, also um die aktuelle Version des bewährten Tools, das über ein eigenständiges Livesystem startet. Deshalb die Entscheidung, Gparted Live auch nochmal einzeln in 32 Bit mitzunehmen. Diese Version gewährleistet die beste Kompatibilität, auch mit wirklich sehr alten PCs. Ein weiterer Vorteil dieses Livesystems: Der Partitionierer startet automatisch, ohne dass man ihn lange suchen muss. Gparted 1.1.0 hat wieder wichtige Fehlerbehebungen erhalten und erweitert die Unterstützung für FAT/FAT32 und das Flash-Friendly-Filesystem. Wie gewohnt geht der Partitionierer souverän mit allen Linux-Dateisystemen, aber auch mit Linux-fremden Dateisystemen wie NTFS (Windows) und HFS/HFS+ (Mac) um. Nach dem Boot zeigt Gparted Live mit „Configure console-data“ erst einen Dialog zur Wahl des Tastaturlayouts an. Die Standardoption „Don’t touch keymap“ lädt eine deutsche Tastenbelegung. ■



Der Partitionierer Gparted in Aktion: Das Tool erkennt, verschiebt und verkleinert oder vergrößert Partitionen und die enthaltenen Dateisysteme ohne Datenverlust.

Ubuntu Server Netboot 18.04.4

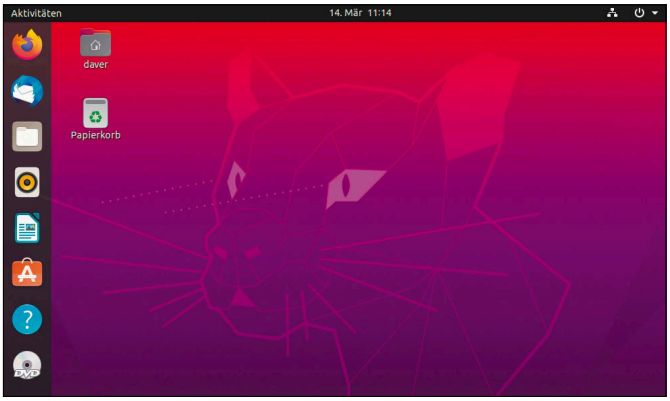
Ausnahmsweise sind diese Installationsmedien von Ubuntu kein Livesystem, sondern die Serverausgabe von Ubuntu mit textbasiertem Installer. Serversysteme brauchen üblicherweise keinen grafischen Desktop und konsequenterweise verzichtet man bei dieser offiziellen Ubuntu-Ausgabe auch darauf. Im Gegensatz zu den üblichen Ubuntu-Varianten, die als Livesystem vorliegen, weist dieses System ein Installationsprogramm im Stil von Debian auf, das direkt im 64-Bit- oder 32-Bit-Modus von der Heft-DVD startet. Auf Wunsch kann das Installationsprogramm auch gleich auf Deutsch umgeschaltet werden. Es gibt einen Partitionierer, der die Funktionen des grafischen Installationsprogramms von Ubuntu 18.04 abbildet. Hier können auch verschlüsselte Partitionen über den Logical Volume Manager (LVM) eingerichtet werden, genau wie im grafischen Pendant. Eine Paketauswahl nach Gruppen erlaubt die individuelle Zusammenstellung des Ubuntu-Systems. Eine individuelle Paketauswahl bleibt dem Anwender überlassen. ■



Der textbasierte Installer von Ubuntu Server (32 Bit und 64 Bit): Dieses Einrichtungsprogramm bildet die Schritte des grafischen Installers ab.

Ubuntu Server Netboot 20.04

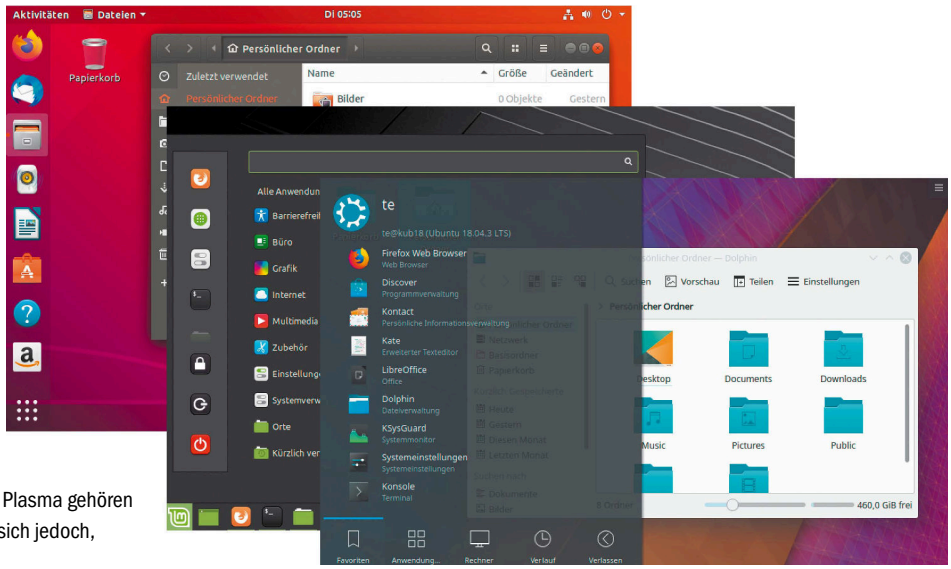
Zur Fertigstellung dieser Heft-DVD war Ubuntu 20.04 noch nicht fertig. Trotzdem ist schon der textbasierte Installer des nächsten Ubuntus mit von der Partie. Dieses Kunststück gelingt, weil dieses bootfähige Installationsmedium selbst keine Pakete mitbringt, sondern alles direkt aus den Online-Paketquellen von Ubuntu 20.04 „Focal Fossa“ bezieht. Und auf den Servern liegen alle Pakete dieser neuen Ubuntu-Ausgabe stets in frischen Versionen vor. Die offensichtliche Kehrseite soll natürlich nicht unerwähnt bleiben: Ganz so komfortabel wie aus einem Livesystem ist dieser Installer nicht. Der Installer ist identisch mit jenem der Vorgängerausgabe (siehe oben), liegt nun aber nur mehr in 64 Bit vor. Der interessante Punkt für Desktopanwender kommt auch hier fast am Ende der Installationsprozedur: Nach der „Installation des Grundsystems“ und der Frage nach automatischer Aktualisierung erscheint dann das Auswahlmenü von Paketgruppen und Desktopumgebungen. ■



Netboot-Installer: Während Ubuntu 20.04 „Focal Fossa“ auf seine Fertigstellung wartete, war das textbasierte Installationsprogramm bereits verfügbar.

Linux-Desktops 2020

Für Linux gibt es eine Vielfalt von Desktopumgebungen. Die Unterschiede bei der Ausstattung und Bedienung sind zum Teil erheblich. Daher eignet sich auch nicht jeder Desktop für jedermann.



Bekannte Desktops: Gnome 3, Cinnamon und KDE Plasma gehören zu den verbreiteten Desktopumgebungen. Es lohnt sich jedoch, einen Blick auf Alternativen zu werfen.

VON THORSTEN EGGELING

Die Auswahl der Desktopumgebung ist größtenteils Sache des Geschmacks oder der Gewohnheiten und auch nicht zwingend an eine Linux-Distribution gebunden. Es kann jedoch auch technische Gründe für die Entscheidung geben. Manche Desktopumgebungen eignen sich besonders für ältere oder weniger leistungsfähige Rechner. Auf den nächsten Seiten stellen wir die wichtigsten Linux-Desktops vor und erläutern deren Vorzüge und Nachteile. Dabei geht es um das Bedienkonzept, die Ansprüche an die Hardware und den Komfort bei der Konfiguration.

Distributionen und Desktopumgebungen

Die grafische Oberfläche eines Linux-Systems ist eine installierbare Software wie jede andere auch – und damit beliebig austauschbar. Im Prinzip lässt sich jede Desktopumgebung in jeder Distribution installieren, wenn die nötigen Programmpakete zur Verfügung stehen.

Der Desktopwechsel gelingt jedoch nicht immer ohne Schwierigkeiten. Manchmal fehlen Pakete oder die Konfigurationsdateien sind nicht optimal angepasst oder es gibt unerwünschte Nebenwirkungen auf den ursprünglichen Desktop. Wir erwähnen die manuelle Installation dennoch auf den nächsten Seiten, weil erfahrene Nutzer die Probleme mit etwas Internetrecherche beheben können.

Bei produktiv genutzten PCs raten wir vom manuellen Wechsel der Desktopumgebung ab. Es ist einfacher, sich gleich für eine Distribution mit dem gewünschten Desktop zu entscheiden. Wer den Ubuntu-Unterbau sympathisch findet, hat die größte Desktopauswahl. Ubuntu verwendet Gnome 3, außerdem gibt es Kubuntu (KDE Plasma), Xubuntu (XFCE), Lubuntu (LXQT), Ubuntu Budgie und Ubuntu Mate.

Das Ubuntu-basierte Linux Mint gibt es mit Cinnamon, Mate und XFCE. Bei Fedora heißen die Varianten „Spins“ (*https://spins.fedoraproject.org*). Neben dem Standarddesktop Gnome 3 stehen KDE, XFCE, LXQT, Mate, Cinnamon und LXDE in installierbaren Livesystemen zur Verfügung.

Auch Manjaro (*https://manjaro.org*) ist sehr flexibel, wenn es um den Desktop geht. Offizielle Ausgaben zeigen die Oberflächen Gnome 3, KDE oder XFCE. Communityeditionen gibt es mit Cinnamon, LXDE, LXQT, Mate, Openbox und Budgie. Der Installer Manjaro Architect bietet etwas Besonderes: Bei der Einrichtung bietet er sämtliche Desktops zur Auswahl.

Welcher Desktop für wen?

Bei Windows gibt es nur einen (offiziellen) Desktop. Bei Linux sind es etwa zehn verbreitete, dazu kommen mindestens noch einmal so viele exotische. Das ist verwirrend und trägt zur Verbreitung von Linux sicher nicht bei. Andererseits kann aber jeder die Distribution und Desktopumgebung wählen, die den persönlichen Bedürfnissen am nächsten kommt.

Das ist zugleich auch die Ursache der Diversifizierung. Die Entwickler sehen unterschiedliche Funktionen und Bedienkonzepte als wichtig an. Der Ressourcenbedarf ist ebenfalls zu berücksichtigen. Damit eine Desktopumgebung auf älterer Hardware geschmeidig läuft, sollte sie auf hübsche 3D-Effekte verzichten. Schlichtheit gefällt jedoch nicht allen, weshalb einige Desktopumgebungen Fenster beim Öffnen, Schließen oder Bewegen animieren, transparent darstellen oder beim Verschieben abdunkeln. Das ist hübsch, kostet aber CPU- und GPU-Leistung. Allerdings schaltet etwa KDE Plasma die Effekte automatisch ab, wenn der Grafikadapter kein Open GL für die Beschleunigung bie-

tet. Der Benutzer kann ebenfalls einzelne oder alle Effekte deaktivieren.
Die Desktopumgebungen lassen sich grob in folgende Kategorien einordnen:

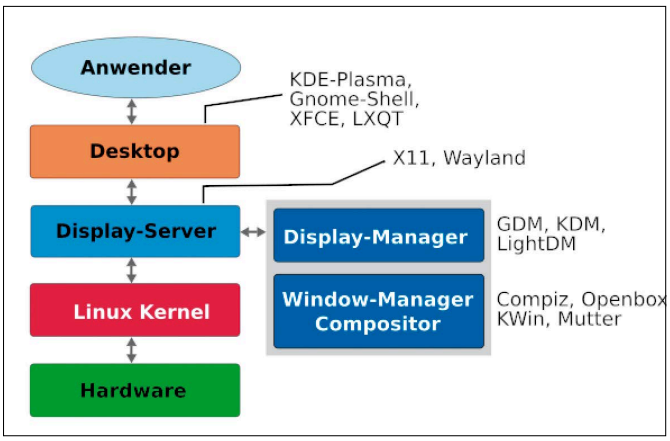
- ähnlich wie Windows, gut für Umsteiger
- schlicht und einfach, wenige Konfigurationsoptionen
- individuell bis ins Detail konfigurierbar und daher komplex
- geringer oder hoher Ressourcenbedarf
- erweiterbar über Plug-ins, Applets oder Miniprogramme
- alternativ oder experimentell: für Nutzer, die alternative Bedienkonzepte schätzen

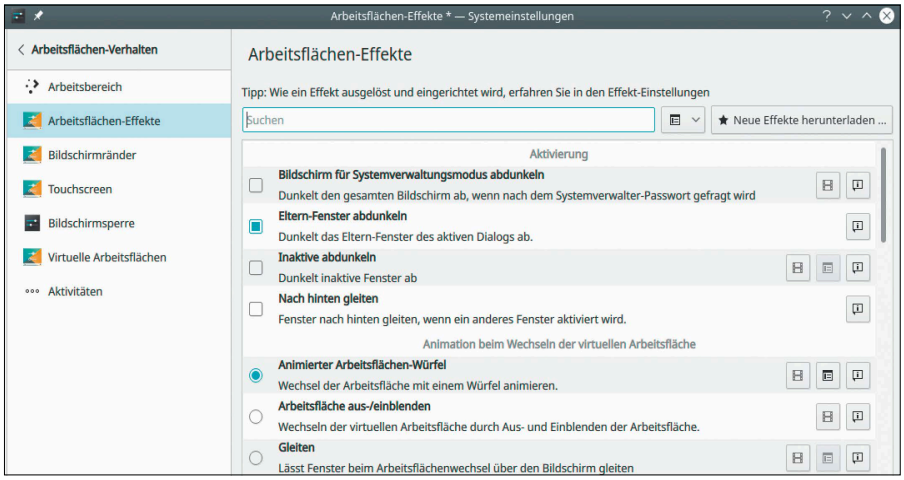
Ohne an dieser Stelle ins Detail zu gehen, ergeben sich daraus Empfehlungen für unterschiedliche Ansprüche.
Windows-ähnlich: Cinnamon, Mate oder KDE Plasma
Einfache Bedienung: Gnome 3, XFCE oder LXDE/LXQT
Flexibel und anpassungsfähig: KDE Plasma, Cinnamon, XFCE
Geringe Hardwareansprüche: LXQT, XFCE

Desktops, Software und Konfiguration

KDE, Gnome 3, Cinnamon & Co. sind nicht nur einfach so etwas wie Designs oder Themes, die den Desktop farbig gestalten. Bei Linux ist die grafische Oberfläche modular aufgebaut: Der Displayserver sorgt dafür, dass überhaupt eine grafische Darstellung erfolgt (GUI, Graphical User Interface). Der Displaymanager ermöglicht die Anmeldung des Benutzers und die Sitzungsauswahl. Die startet dann einen Windowmanager, der Fenster auf dem Bildschirm darstellt, wozu auch Panels, Menüs oder Taskleisten zählen. Eng damit verbunden ist der optionale Compositor. Er sorgt beispielsweise für Animationseffekte. Erst danach kommt die grafische Benutzeroberfläche ins Spiel, die mit Hintergrundgrafik, Icons, Fensterdekorationen und Menüs dem Benutzer direkt ins Auge fällt.
Zu den Oberflächen gehören in der Regel auch eigene Programme wie beispielsweise der Dateimanager. Diese Software ist so gestaltet, dass sie optisch zur grafischen Oberfläche passt. Es gibt auch jeweils spezielle Tools für die Konfiguration der Oberfläche mit mehr oder weniger Funktionen.
Ein weiteres wichtiges Element ist das GUI-Toolkit. KDE/LXQT-Programmierer verwenden Qt, Gnome, Cinnamon und Mate sind auf GTK aufgebaut. Die zugehörigen Programmbibliotheken sorgen für die Darstellung der Steuerelemente wie Schaltflächen, Scrollboxen und Eingabefelder. KDE/Qt-Programme sehen daher anders aus als Gnome/GTK. Es lassen sich jedoch alle Programme unter jeder Oberfläche starten, wenn die nötigen Bibliotheken vorhanden sind. ■

Fenstersystem: Für die grafische Oberfläche sind bei Linux mehrere Komponenten zuständig. Je nach System und Desktop kommen unterschiedliche Programme zum Einsatz.





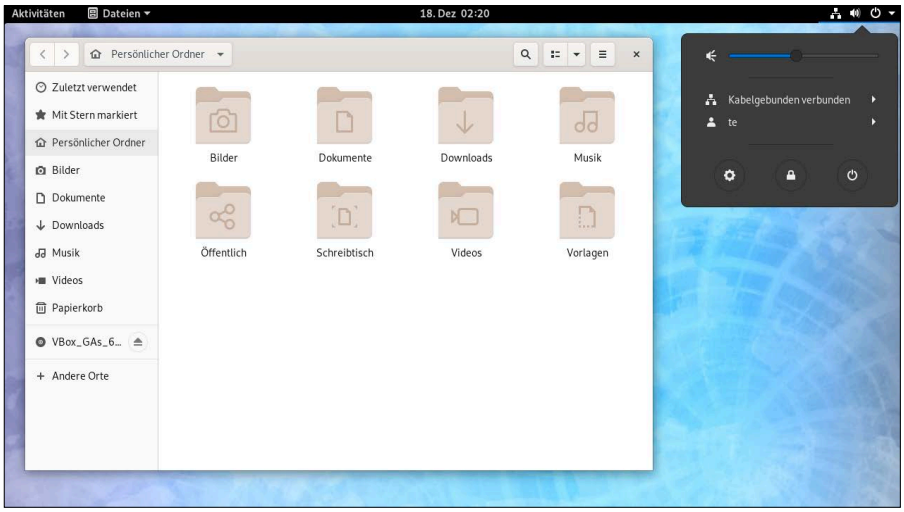
Spiel und Spaß: KDE-Nutzer können zahlreiche Arbeitsflächeneffekte konfigurieren, wenn die Hardware genügend Leistung bietet. Wenn nicht, lassen sich die Effekte auch abschalten.

EXOTISCHE DESKTOPUMGEBUNGEN

Abseits des Üblichen gibt es Ansätze für Experimentierfreudige. i3 (*https://i3wm.org*) ist ein Tiling Window Manager, bei dem sich Fenster nicht frei verschieben lassen, sondern in einem Raster angeordnet sind. Eine herkömmliche Desktopoberfläche oder ein Startmenü gibt es nicht. Ähnliche Funktionen bieten **Ratpoison** (*www.nongnu.org/ratpoison*) und **Wmii** (*https://wiki.archlinux.org/index.php/wmii*), deren Bedienung ebenfalls hauptsächlich per Tastatur erfolgt. Alle diese Desktops lassen sich bei Ubuntu/Mint aus den Standard-Paketquellen installieren.
Die **Moksha**-Oberfläche gibt es nur bei Bodhi Linux (Ubuntu-Basis, *www.bodhilinux.com*). Es handelt sich um eine Weiterentwicklung von **Enlightenment,** auf das wir auf Seite 23 ausführlicher eingehen. Die Bedienung orientiert sich mit Startmenü und Taskleiste an herkömmlichen Desktops. Das System ist schlank und besonders schnell und die Oberfläche lässt sich minutiös konfigurieren. Letzteres ist aber zugleich ein Nachteil, weil die Einstellungen kleinteilig und unübersichtlich sind. Außerdem fehlt eine globale Konfigurationszentrale. Eine Hilfestellung gibt der Artikel auf *www.pcwelt.de/2300744*.

Der Schlichte: Gnome 3

Den Gnome-3-Desktop nutzen viele bekannte Linux-Distributionen, darunter Fedora und Ubuntu. Die Oberfläche sieht jedoch nicht überall identisch aus, weil die meisten Distributoren kleine Anpassungen vornehmen.



VON THORSTEN EGGELING

Bei Gnome 3, auch Gnome-Shell genannt, liegt der Fokus auf Einfachheit und Schlichtheit. Verspielte Effekte sucht man vergebens. Ehemalige Windows-Nutzer müssen sich etwas umgewöhnen, weil Elemente wie ein klassisches Startmenü fehlen. Wo die Anwendungen und nicht das Betriebssystem im Mittelpunkt des Interesses stehen, kann Gnome 3 die richtige Wahl sein.

Konzept und Funktionsumfang

Bei einer Standardinstallation, beispielsweise in Fedora 31, sind eine Leiste mit Datum und Uhrzeit sowie einige Icons am oberen Bildschirmrand zu sehen, die zum Lautstärkeregler den Netzwerkeinstellungen und zum Dialog „Ausschalten“ führen. Ein Klick auf „Aktivitäten“ links oben blendet den Programmstarter („Dash“) ein. Die Ansicht dient gleichzeitig als Taskmanager, der Vorschaubilder der laufenden Anwendungen zeigt. Um Programme zu finden, verwenden Sie die Suchfunktion. Die unterste Schaltfläche im Dash führt zu einer großflächigen Übersicht mit häufig genutzten oder allen Programmen.

Fedora 31 ist so reduziert, dass es bei Fenstern nur die „X“-Schaltfläche zum Schließen vorhanden ist. „Minimieren“ ist im Kontextmenü zu finden. Der Desktop dient nur als Herberge für das Hintergrundbild und bleibt ansonsten ungenutzt. Es lassen sich auch keine Ordner oder Verknüpfungen darauf ablegen. Ubuntu 18.04 bringt Gnome dem gewohnten Bedienkonzept etwas näher. Fenster sind mit Schaltflächen für Minimieren, Maximieren und Schließen ausgestattet. Das Dash befindet sich immer im Vordergrund, zeigt Icons der laufenden Programme und erleichtert damit den Taskwechsel. Auf dem Desktop lassen sich immerhin Ordner anlegen.

Hardwareansprüche und Leistungsbedarf

Gnome galt lange als träge und speicherhungrig. Das hat sich bei den neueren Versionen zumindest teilweise geändert. Auf aktuellen PCs reagieren Gnome-3-Systeme ausreichend schnell. In Ubuntu 18.04 genehmigt sich das Betriebssystem ungefähr ein GB RAM, bei Fedora 31 ist es mit 730 MB etwas weniger (alle Messungen mit ps_mem, *https://github.com/pixelb/ps_mem*). Davon gehen gut 300 MB alleine auf das Konto der Gnome-Shell. Für ältere PCs mit wenig RAM ist Gnome 3 nur eingeschränkt zu empfehlen.

Konfiguration und Anpassungen

Die „Einstellungen“ bei Fedora und Ubuntu mit Gnome-Desktop bieten fast nichts für die Desktopgestaltung. Aushelfen kann das Tool Gnome-Tweaks (Paket: gnome-tweaks), das sich in einem deutschsprachigen Linux über eine Suche nach Optimierungen starten lässt. Darüber lassen sich beispielsweise Schriftbild, Fensterverhalten und Themes konfigurieren. Die Gnome-Shell lässt sich auch über Erweiterungen mit neuen Funktionen ausstatten. Mehr dazu lesen Sie bei *https://extensions.gnome.org*.

Die manuelle Installation

Wer den Gnome-3-Desktop beispielsweise unter Linux Mint oder Kubuntu installieren möchte, führt diese Befehlszeile aus:

```
sudo apt install ubuntu-gnome-
  desktop language-pack-gnome-de
```

Dieser Befehl

```
sudo dnf install @gnome-desktop
```

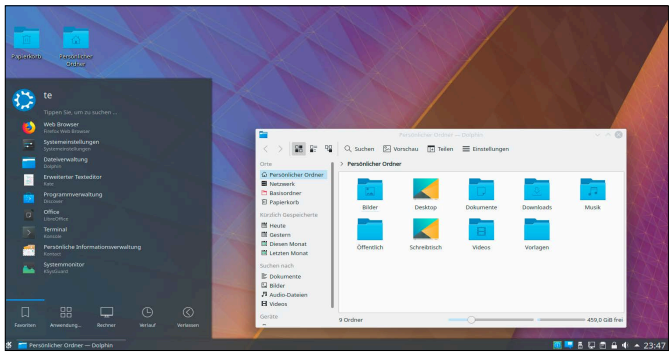
führt in Fedora ans Ziel. ■

STECKBRIEF GNOME 3

Webseite: *www.gnome.org*
Aktuelle Version:
Gnome 3.34 (12. September 2019)
Zielgruppe: Einsteiger, individuelle Anpassungen nur für Fortgeschrittene
Ressourcenbedarf: moderat bis hoch, der Open-GL-Desktop läuft am besten auf einem 3D-fähigen Grafikchip
Anpassungsfähigkeit: gering
Repräsentative Distributionen:
Ubuntu 18.04 (*https://ubuntu.com*), Fedora 31 (*https://getfedora.org*)

Der Umfangreiche: KDE Plasma

KDE ist eine der populärsten Desktopumgebungen. Einsteiger finden sich dank gewohnter Elemente schnell zurecht, Fortgeschrittenen bietet KDE umfassende und detaillierte Anpassungsmöglichkeiten.



VON THORSTEN EGGELING

KDE ist der Gegenentwurf zu Gnome 3. Wo bei Gnome nichts ist, ist bei KDE alles. Weder an Funktionen noch Einstellungen wurde gespart, sodass es an einigen Stellen auch unübersichtlich werden kann.

Konzept und Funktionsumfang

Es gibt ein Startmenü („K-Menü“) mit Suchfunktion, bei dem KDE aber eigene Wege geht. Es zeigt mehrere Schaltflächen, der Standard ist „Favoriten“. Nach einem Klick auf „Anwendungen“ sehen Sie Kategorien wie „Büroprogramme“ oder „Internet“. Weitere Klicks führen zu den Programmen. Unter „Verlassen“ gibt es Optionen wie „Abmelden“ oder „Neustarten“. Neben dem K-Menü liegen die Taskleiste und die Kontrollleiste mit diversen als Icons dargestellten Miniprogrammen (Lautstärkeregler, Netzwerke, Zwischenablage und mehr).
Der Desktop zeigt bereits die Icons „Papierkorb“ und „Persönlicher Ordner“. Über das Desktop-Kontextmenü „Neu erstellen“ lassen sich weitere Ordner, Dokumente oder Programmverknüpfungen hinzufügen. Drag & Drop zwischen Dateimanager und Desktop funktioniert ebenfalls. KDE ist nicht nur eine Desktopumgebung. Enthalten sind auch zahlreiche Anwendungen, die fast alle mit einem „K“ beginnen oder eins enthalten, beispielsweise Krita, Digikam, Konqueror, Kmail oder Kdenlive. Die Programme basieren auf den gleichen Bibliotheken und passen optisch perfekt zum Desktop.

Hardwareansprüche und Leistungsbedarf

Die umfangreiche Ausstattung wirkt sich erfreulich moderat auf den Speicherbedarf aus. Bei Kubuntu 18.04 belegt das System 760 MB RAM, bei Open Suse 15.1 nur 580 MB. Damit liegt KDE etwa in der Mitte zwischen Gnome 3 und XFCE. Auf nicht allzu alten PCs sollte KDE flüssig laufen.

Konfiguration und Anpassungen

In den „Systemeinstellungen“ finden sich unter „Erscheinungsbild“ und „Arbeitsbereich“ fast alle Optionen, die die Desktopoberfläche betreffen. Sie können eines der vorhandenen Designs für den Arbeitsbereich aktivieren und weitere herunterladen. Farben, Schriften, Bedienelemente und die Fensterdekoration – alles lässt sich individuell anpassen.
Darüber hinaus gibt es Optionen für einzelne Bedienelemente. Klicken Sie etwa auf das K-Menü mit rechter Maustaste und wählen Sie „Alternativen“. Voreingestellt ist „Anwendungs-Starter“. Wählen Sie „Anwendungsmenü“ für ein Menü, das dem Windows-7-Stil ähnelt. „Anwendungsübersicht“ zeigt einen Starter im Vollbildmodus. Die Einstellungsmöglichkeiten sind kleinteilig und nicht immer intuitiv. Die Symbole für Lautstärkeregelung, Zwischenablage und Netzwerk sind in einer eigenen Kontrollleiste neben der Uhr untergebracht. Wenn man den richtigen Punkt links neben der Uhr mit der rechten Maustaste anklickt, erscheint das Menü „Einstellungen für Systemabschnitt der Kontrollleiste“. Es öffnet sich ein Dialog, über den man Einträge entfernen oder hinzufügen kann.

Die manuelle Installation

In Ubuntu steht KDE über ein Metapaket zur Installation bereit:

```
sudo apt-get install kubuntu-
  desktop kde-l10n-de
```

Dieser Befehl

```
sudo dnf install @kde-desktop-
  environment
```

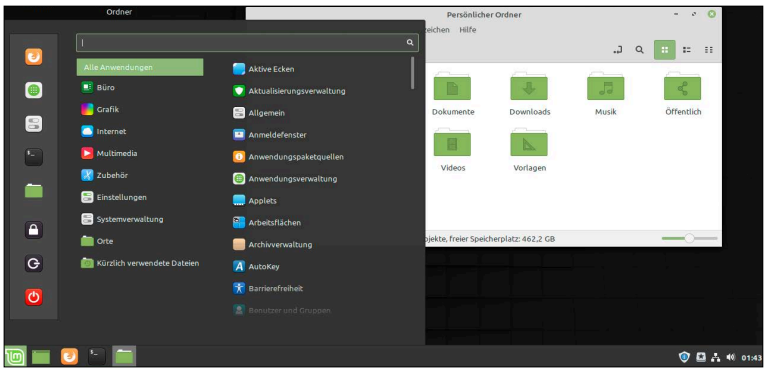
führt in Fedora ans Ziel. ■

STECKBRIEF KDE

Webseite: *http://kde.org*
Aktuelle Version:
KDE Plasma 5.17 (3. Dezember 2019)
Zielgruppe: fortgeschrittene Nutzer und Einsteiger
Ressourcenbedarf: moderat, die optionalen Effekte benötigen einen OpenGL-fähigen Grafikchip
Anpassungsfähigkeit: sehr hoch
Repräsentative Distributionen:
Kubuntu 18.04 (*www.kubuntu.org*), Open Suse 15.1 Leap (*http://de.opensuse.org*), Fedora 31 (*https://spins.fedoraproject.org*)

Für Umsteiger: Cinnamon

Cinnamon erfreut sich vor allem bei Windows-Umsteigern wachsender Beliebtheit. Die Ähnlichkeiten mit Windows sind beabsichtigt, auf individuelle Konfigurationsmöglichkeiten muss man aber nicht verzichten.



VON THORSTEN EGGELING

Cinnamon ist als Desktopoberfläche von Linux Mint (Version 19.3 auf Heft-DVD) bekannt geworden. Das System selbst basiert auf Ubuntu, die Mint-Entwickler haben aber neben Cinnamon beispielsweise einen eigenen Texteditor, Mediaplayer und Bildbetrachter beigesteuert. Der Desktop präsentiert sich schlicht, aber optisch ansprechend, lässt sich sehr gut anpassen sowie mit neuen Elementen erweitern.

Konzept und Funktionsumfang

Cinnamon orientiert sich an klassischen Desktops wie Gnome 2, Windows XP und Windows 7. Es gibt ein Startmenü mit Suchfunktion, das Kategorien wie „Büro“, „Grafik“ und „Multimedia“ zeigt. Es genügt, mit der Maus über die Kategorien zu navigieren, der Inhalt der Kategorie zeigt sich dann in der rechten Hälfte des Fensters. Ganz links gibt es einige Schaltflächen, die zu häufig benötigten Programmen und Tools wie Firefox, Anwendungsverwaltung, Systemverwaltung oder zum Dateimanager führen.

Die Leiste am unteren Bildschirmrand (flexibel änderbar) dient als Taskleiste und zeigt laufende Programme als Icon an. Per rechtem Mausklick und „An der Leiste anheften“ lässt es sich dauerhaft in der Leiste unterbringen, die damit auch als Schnellstarter dient. Im rechten Bereich der Leiste neben der Uhr sind die Icons für Lautstärkeregelung und Netzwerk untergebracht, wenn vorhanden, erscheinen hier auch Updatebenachrichtigungen. Der Desktop lässt sich standardmäßig als Dateiablage verwenden. Sie können Ordner, Dokumente oder Programmverknüpfungen darauf ablegen.

Hardwareansprüche und Leistungsbedarf

Cinnamon ist nicht besonders anspruchsvoll. Linux Mint 19.3 mit Cinnamon 4.4.5 belegt insgesamt um die 650 MB RAM. Damit ist es auch für ältere Hardware mit zwei oder vier GB RAM geeignet, wenn nicht zu viele Programme gleichzeitig laufen.

Konfiguration und Anpassungen

Alle Optionen sind bequem über die „Systemeinstellungen“ erreichbar, die Sie über das Icon auf der linken Seite im Startmenü aufrufen. Themen und Hintergrundbilder für die Arbeitsfläche sind mit wenigen Mausklicks geändert. Zusätzliche Themes lassen sich auf der Registerkarte „Hinzufügen/Entfernen“ herunterladen.

Wer gerne mit der Tastatur arbeitet, sollte unter „Geräte“ auf „Tastatur“ klicken. Auf der Registerkarte „Tastenkombinationen“ finden Sie die vordefinierten, aber anpassbaren Hotkeys.

Wer Wert auf ein sehr individuelles System legt, findet unter „Systemeinstellungen → Erweiterungen“ funktionale und optische Ergänzungen. Das geht dann aber oft zu Lasten der Hardwareressourcen. Die Installation der Erweiterungen besteht aus einem zweistufigen Prozess. Nach dem Download (Registerkarte „Herunterladen“) müssen die Erweiterungen zusätzlich noch manuell aktiviert werden. Bei den Applets für den Systembereich in der Hauptleiste ist der Ablauf analog. Zusätzlich zu Applets und Erweiterungen gibt es auch noch eine Handvoll zum Teil noch etwas instabiler „Desklets“, die sich am Desktop frei positionieren lassen.

Die manuelle Installation

Ubuntu-Nutzer verwenden für die Installation diesen Befehl:

```
sudo apt install cinnamon
```

Das Kommando

```
sudo dnf install @kde-desktop-
  environment
```

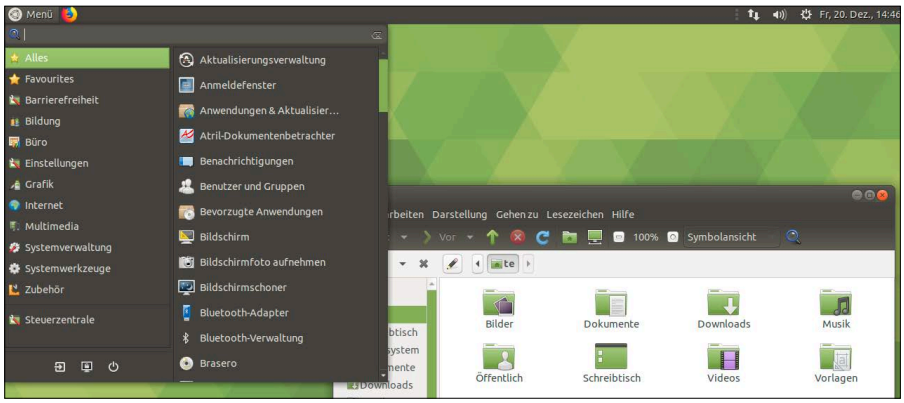
führt in Fedora ans Ziel. ■

STECKBRIEF CINNAMON

Webseite: *https://github.com/linuxmint/cinnamon*
Aktuelle Version:
Cinnamon 4.4.5 (12. Dezember 2019)
Zielgruppe: Nutzer, die einen klassischen Desktop suchen, ohne viel basteln zu müssen. Etwas Experimentierfreude ist nötig, um alle Feinheiten zu erkunden.
Ressourcenbedarf: moderat bis durchschnittlich, 3D-fähiger Grafikchip ist hilfreich, aber nicht erforderlich
Anpassungsfähigkeit: hoch, mit breitem Angebot an Themes, internen Appletfunktionen sowie Erweiterungen und Desklets
Repräsentative Distribution:
Linux Mint Cinnamon 19.3
(https://linuxmint.com)

Der Klassische: Mate

Mate ist eine weitere Variante des klassischen Linux-Desktops, setzt aber eigene Akzente. Zwischen den Distributionen gibt es kleine Unterschiede, auf die man achten sollte.



VON THORSTEN EGGELING

Der Mate-Desktop ist eine Weiterentwicklung des ursprünglichen Gnome-2-Desktops. Inzwischen liefern aktuelle GTK3-Komponenten die Basis, sodass sich auch neuere Gnome-Anwendungen gut in den Desktop integrieren. Mate bietet einen klassischen, aber individuell konfigurierbaren Desktop, der sich auch für ältere Hardware eignet.

Konzept und Funktionsumfang

Fedora 31 bietet einen weitgehend unveränderten Mate-Desktop. Für Desktopeffekte wird Compiz nebst zugehöriger Tools für die Einstellungen installiert. In der Leiste am oberen Bildschirmrand ist das Menü „Anwendungen“ untergebracht, in dem man über Kategorien wie „Büro“ und „Internet“ zu den gewünschten Programmen gelangt. Rechts daneben kann man über „Orte“ den Dateimanager Caja gleich mit einer Ordneransicht öffnen, beispielsweise „Dokumente“ oder „Downloads“. Die Einstellungen sind im eigenen Menü „System“ untergebracht, hier findet man auch „Abmelden“ und „Herunterfahren“. In der Leiste gibt es außerdem Icons, über die sich etwa der Dateimanager oder Firefox mit einem Mausklick starten lassen. Der rechte Teil der Leiste zeigt Icons für den Lautstärkeregler und das Netzwerk sowie Datum und Uhrzeit. Die Leiste am unteren Bildschirmrand dient als Taskleiste und als Arbeitsflächenumschalter.

Ubuntu Mate 18.04 ist auf der Basis Grün etwas farbenfroher konfiguriert (siehe Abbildung). Das einfache Mate-Menü gefiel den Entwicklern wohl nicht, weshalb das „Brisk Menü“ Einsatz kommt, das auch eine Suchfunktion bietet. Ansonsten entspricht Mate dem bei Fedora beschriebenen Konzept.

Hardwareansprüche und Leistungsbedarf

Der Hautspeicherbedarf liegt bei Ubuntu 18.04 und Fedora 31 mit gut 500 MB in etwa gleichauf. Wie KDE und Cinnamon qualifiziert sich diese Desktopumgebung damit auch für leistungsschwächere Hardware. Animationen über Compiz sollte man nur aktivieren, wenn der Grafikchip das unterstützt.

Konfiguration und Anpassungen

Die Einstellungen lassen sich gezielt über das Startmenü und in den „Einstellungen“ aufrufen (Fedora: Menü „System → Einstellungen“). Wer alle Bereiche im Blick haben möchte, startet die „Steuerzentrale“ (Fedora: „Kontrollzentrum“). Unter „Erscheinungsbild“ wählt man das Desktopthema, das sich auch individuell anpassen lässt. Fedora installiert zusätzlich den Emerald Motiv Manager, der sehr detaillierte Einstellungen erlaubt.

Bei Ubuntu 18.04 starten Sie in der Steuerzentrale unter „Darstellung“ das Tool „MATE Tweak“. Darüber legen Sie beispielsweise fest, welche Icons auf dem Schreibtisch auftauchen oder wie die Leisten aussehen sollen. Nach einem Klick auf Fenster lässt sich für mehr Effekte auch Compiz als alternativer Window-Manager wählen. Sie sollten dann auch das Paket „compizconfig-settings-manager“ installieren, damit Sie die Effekte konfigurieren können. Bei Fedora ist das Tool bereits dabei.

Die manuelle Installation

Mate ist in den offiziellen Paketquellen enthalten und lässt sich neben Gnome 3 unter Ubuntu installieren:

```
sudo apt install ubuntu-mate-
  desktop
```

Diese Befehlszeile

```
sudo dnf install @mate-desktop-
  environment
```

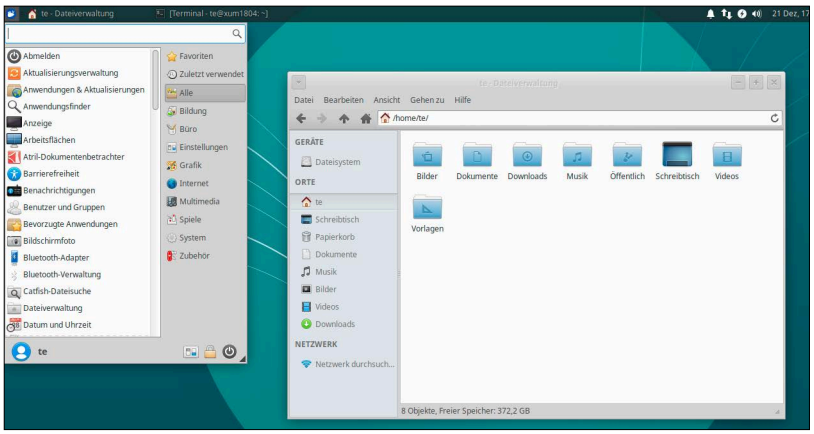
führt in Fedora ans Ziel. ■

STECKBRIEF MATE

Webseite: *http://mate-desktop.org*
Aktuelle Version:
Mate 1.22 (18. März 2019)
Zielgruppe: Einsteiger und konservative Anwender
Ressourcenbedarf: gering bis moderat, läuft auch ohne 3D-fähigen Grafikchip, braucht wenig RAM und Rechenleistung
Anpassungsfähigkeit: hoch
Repräsentative Distributionen:
Ubuntu Mate 18.04 (*https://ubuntu-mate.org*), Fedora 31 (*https://spins.fedoraproject.org*)

Der Sparsame: XFCE

XFCE ist eine sparsame und schlichte Desktopumgebung. Es gibt dennoch zahlreiche und durchdachte Komfortfunktionen, über die sich die Arbeitsumgebung komfortabel anpassen lässt.



VON THORSTEN EGGELING

XFCE gehört zu den ältesten Desktopumgebungen und seine Entwicklung verläuft sehr langsam. Nur alle paar Jahre gibt es eine neue Version – nach mehr als vier Jahren Pause zuletzt im August 2019. Die Oberfläche wird jedoch weiterhin gerne genutzt, weil sie wenig Ressourcen verlangt und trotzdem anpassungsfähig ist.

Konzept und Funktionsumfang

Bei Xubuntu enthält die Leiste am oberen Bildschirmrand ein Startmenü mit Suchfunktion und die Fensterknöpfe (Taskleiste). Im rechten Bereich sind die Uhr, Lautstärkeregler und Statusbenachrichtigungen zu Netzwerk und Updates untergebracht. Fedora mit XFCE ist ähnlich konfiguriert, zeigt aber ein einfacheres Startmenü ohne Suchfunktion.

Drag & Drop vom Dateimanager auf den Desktop bewirkt beim gleichen Laufwerk die Standardaktion „Verschieben“, andernfalls „Kopieren“. Wenn Sie mit der rechten Maustaste klicken und ziehen, öffnet sich ein Menü mit den Optionen „Hierher kopieren“, „Hierher verschieben“ und „Verknüpfung hier erstellen“. Das entspricht dem Verhalten von Windows, was Umsteigern die Bedienung erleichtert. Über das Kontextmenü des Desktops lassen sich neue Ordner, Dokumente oder Programmstarter erstellen.

Hardwareansprüche und Leistungsbedarf

XFCE benötigt wenig Hauptspeicher und eignet sich daher besonders gut für weniger leistungsstarke Hardware. Xubuntu beansprucht bei einer Standardinstallation ungefähr 380 MB RAM, wovon die Prozesse der Desktopumgebung etwa 100 MB belegen. XFCE liegt damit beim Ressourcenbedarf im unteren Bereich und wird nur noch von Enlightenment/Moksha unterboten.

Konfiguration und Anpassungen

Obwohl es sich bei XFCE um eine sehr schlanke Desktopumgebung handelt, sind die Anpassungsmöglichkeiten zahlreich und übersichtlich. Ein rechter Mausklick auf einen freien Bereich in der Leiste am oberen Bildschirmrand führt zum Menü „Leiste → Leisteneinstellungen“. Auf der Registerkarte „Objekte“ sind die vorhandenen Elemente aufgelistet, die Position lässt sich über die Pfeil-Schaltflächen ändern. Über die „+“-Schaltfläche fügen Sie neue Elemente hinzu. Die können Sie auch mit der Maus direkt vom Dialog auf die gewünschte Stelle in der Leiste ziehen.

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

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

Die manuelle Installation

Nutzer von Ubuntu oder Linux Mint können XFCE nachträglich installieren:

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

Dieser Befehl

```
sudo dnf install @xfce-desktop-
  environment
```

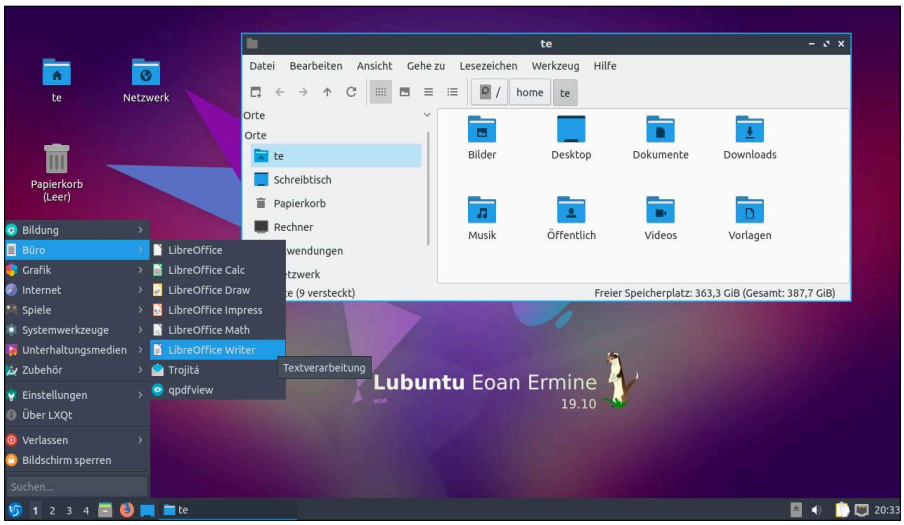
führt unter Fedora ans Ziel. ■

STECKBRIEF XFCE

Webseite: *www.xfce.org*
Aktuelle Version: XFCE 4.14 (12. August 2019)
Zielgruppe: Einsteiger und erfahrene, konservative Nutzer
Ressourcenbedarf: sehr moderat, läuft auch mit älteren CPUs und ohne 3D-Chip
Anpassungsfähigkeit: sehr gut
Repräsentative Distribution: Xubuntu 18.04 (*http://xubuntu.org*)

Die leichten L-Desktops

Die beiden L-Desktops stammen vom selben Anbieter und unterscheiden sich bei der Bedienung nur in Details. LXDE ist aber deutlich sparsamer mit den Systemressourcen als das jüngere LXQT.



VON THORSTEN EGGELING

Das „L“ in LXDE/LXQT steht für leichtgewichtig („Lightweight X11 Desktop Environment“). Das Ziel der Entwickler ist ein besonders schlanker Desktop, der sich auch auf leistungsschwacher Hardware gut verwenden lässt. LXDE basiert auf Gnome 2 und soll auch nicht auf Gnome 3 umgestellt werden. Der LXDE-Desktop wird trotzdem weiterentwickelt, obwohl mit LXQT, das wie KDE auf den Qt-Bibliotheken basiert, bereits der Nachfolger feststeht.

Konzept und Funktionsumfang

Lubuntu 18.04 verwendet noch LXDE, seit Lubuntu 19.10 kommt dort LXQT zum Einsatz. Im direkten Vergleich wirkt LXQT aufgrund der farbenfrohen Gestaltung sowie kontrastreicher Icons neuer und frischer (siehe Abbildung). Dabei handelt es sich jedoch um Anpassungen des Lubuntu-Teams. Vergleicht man die Fedora-Spins von LXDE und LXQT, ist kaum ein Unterschied zu entdecken.

Auch das jüngere LXQT bleibt beim bewährten Konzept: Eine Leiste am unteren Bildschirmrand bietet ein aufgeräumtes Startmenü, Schnellstarter, Taskleiste und Symbole etwa für Netzwerk und Lautstärkeregelung. Einige Verbesserungen zeigen sich in Details. Drag & Drop vom Webbrowser oder Dateimanager auf den Schreibtisch öffnen jetzt Menüs mit „Hierhin kopieren“ oder „Hier eine symbolische Verknüpfung erstellen“. Bei LXDE funktionierte das nicht so einfach.

Hardwareansprüche und Leistungsbedarf

Mit LXQT ist der Ressourcenbedarf gestiegen. Bei Fedora 31 belegt das LXDE-System 350 MB RAM, bei LXQT sind es 450 MB. Lubuntu 18.04 mit LXDE eignet sich mit 260 MB am besten für Rechner mit wenig Hauptspeicher. Lubuntu 19.10 mit LXQT benötigt dagegen 680 MB, was aber an den zusätzlich geladenen Komponenten liegt. Trotzdem benötigen die LXQT-Prozesse durchweg mehr RAM als die vergleichbaren LXDE-Prozesse.

Konfiguration und Anpassungen

Lubuntu mit LXQT folgt dem Trend und bietet unter „Einstellungen → LXQT-Systemeinstellungen“ ein „Konfigurationszentrum“, das etwa zu „Bildschirmeinstellungen“ oder „Erscheinungsbild“ führt. Man muss sich dann nicht jedes Mal durchs Menü hangeln, wenn man hintereinander mehrere Optionen anpassen möchte. Bei Fedora LXQT fehlt dieses „Konfigurationszentrum“ bisher noch.

Etwas verwirrend ist, dass es für einige Einstellungen mehrere Tools gibt. Über „Erscheinungsbild“ lassen sich beispielsweise die Bereiche „Icons Theme“ und LXQt Theme“ anpassen. Über den „Openbox Konfiguration Manager“ kann man ebenfalls das Theme einstellen, aber auch die Fensterdekoration gestalten. Es ist vieles konfigurierbar, aber man muss es erst finden.

Die manuelle Installation

Nutzer von Ubuntu 18.04 installieren LXDE mit dem Befehl

```
sudo apt install lubuntu-desktop
```

und LXQT mit

```
sudo apt install lubuntu-qt-desktop
```

Diese Kommandos

```
sudo dnf install @lxde-desktop-
  environment
sudo dnf install @lxqt-desktop-
  environment
```

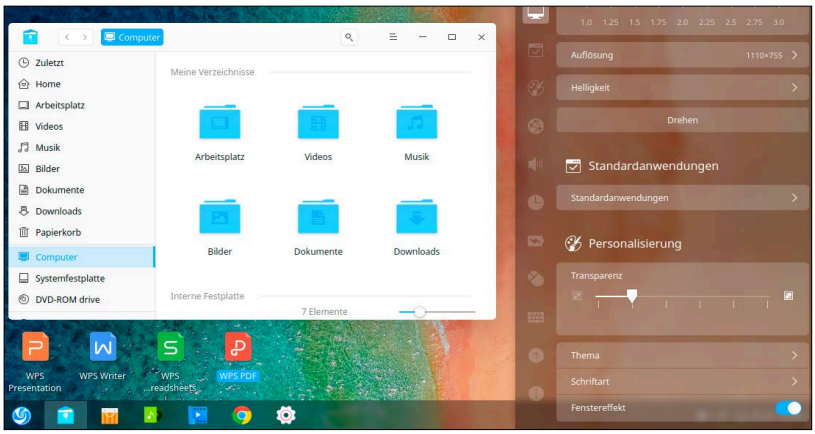
führen bei Fedora ans Ziel. ■

STECKBRIEF LXDE/LXQT

Webseite:
http://lxde.org, *https://lxqt.org*
Aktuelle Version:
LXDE 0.99.2 (25. Januar 2017), LXQT 0.14.1 (26. Februar 2019)
Zielgruppe:
Einsteiger bis Fortgeschrittene
Ressourcenbedarf: sehr gering bis durchschnittlich (je nach Version)
Anpassungsfähigkeit:
durchschnittlich bis hoch
Repräsentative Distributionen:
Lubuntu 18.04 (LXDE, *https://lubuntu.net*), Lubuntu 19.10 (LXQT, *https://lubuntu.net*),
Fedora 31 (*https://spins.fedoraproject.org*) mit LXDE oder LXQT

Der Reduzierte: Deepin

Deepin erfindet den Desktop nicht neu, setzt aber bei den Einstellungen eigene Akzente. Anpassungen sind nur begrenzt möglich, was typischen Desktopnutzern jedoch ausreichen dürfte.



VON THORSTEN EGGELING

Der Deepin-Desktop stammt aus der gleichnamigen chinesischen Distribution Deepin Linux. Das Deepin Desktop Environment (DDE) verwendet zwar Qt5, gilt aber als übersichtlicher, einfacher und platzsparender als KDE. Der Deepin-Desktop ist inzwischen in mehreren bekannten Distributionen verfügbar, darunter Ubuntu, Fedora, Open Suse und Manjaro.

Konzept und Funktionsumfang

Die chinesische Distribution Deepin Linux basiert auf Debian. Der Unterbau ist daher Nutzern von Ubuntu und Linux Mint nicht fremd. Deepin Linux lässt sich mit deutschen Spracheinstellungen installieren und ist weitestgehend gut übersetzt. Es sind jedoch einige Programme vorinstalliert, die es bisher nur in englischer Sprache gibt, beispielsweise WPS-Office. Der App Store bietet vorrangig chinesische Anwendungen. Als Paketverwaltung lässt sich jedoch Synaptic installieren und als Office-Paket Libre Office. Eine Alternative ist, Deepin in einer anderen Linux-Distribution zu installieren. Am einfachsten geht das mit Manjaro Architekt, das die Auswahl des gewünschten Desktops während der Installation erlaubt.

Deepin ist reduzierter Desktop, ähnlich wie Ubuntu mit Gnome 3. Die Farbgebung wirkt mit kontrastreichen Icons modern, insgesamt jedoch uneinheitlich. Dateimanager und Audioplayer sind standardmäßig mit weißem Theme konfiguriert, Videoplayer und Webbrowser Chrome erscheinen hingegen in tiefem Schwarz.

Die Leiste („Dock“) am unteren Bildschirmrand funktioniert auf den ersten Blick ähnlich wie das Ubuntu-Dash. Das erste Icon öffnet die Anwendungsübersicht mit einem Suchfeld im Vollbild. Über das unscheinbare Icon links oben kann man in eine Kategorienansicht umschalten. Das Icon rechts oben verkleinert das Menü auf ein Fenster mit Suchfunktion, das alle Programme oder Kategorien („Alle Kategorien“) zeigt. Außerdem sind Menüpunkte enthalten, die beispielsweise Ordner wie „Videos“ oder „Dokumente“ im Dateimanager öffnen.

Das Dock dient auch als Taskleiste, in der die Icons der laufenden Programme erscheinen. Per rechtem Mausklick und „Dock“ lässt sich ein Starter für das Programm erstellen.

Hardwareansprüche und Leistungsbedarf

Deepin liegt beim Ressourcenbedarf im Mittelfeld. Deepin Linux belegt etwa 640 MB RAM. Manjaro Architekt mit Deepin-Desktop kommt aufgrund zusätzlicher Autostartprogramme auf annähernd ein GB.

Konfiguration und Anpassungen

Die Einstellungen rufen Sie über das Zahnrad-Icon im Dock auf. Deepin blendet dann das „Kontrollzentrum“ im rechten Bereich des Bildschirms ein. Die Desktopeinstellungen öffnen sich nach einem Klick auf „Personalisieren“. Sie können die Transparenz des Einstellungsbereichs ändern und zwischen einem hellen und dunklen Fensterthema wählen, ferner Symbol- und Zeigerthema einstellen und die Schriftart ändern. Hintergrundbild und Bildschirmschoner lassen sich über das Kontextmenü des Desktop anpassen. Hier gibt es außerdem den Menüpunkt „Eckeneinstellungen“, die Aktionen auslösen kann, wenn Sie mit dem Mauszeiger in eine Ecke fahren (beispielsweise „Bildschirm schnell aus“ oder „Control Center“).

Die manuelle Installation

Für Ubuntu-Nutzer gibt es das PPA *https://launchpad.net/~leaeasy/+archive/ubuntu/dde* (zurzeit nur für 18.04). Unter Fedora lässt sich der Deepin-Desktop mit

```
sudo dnf install @deepin-desktop-environment
```

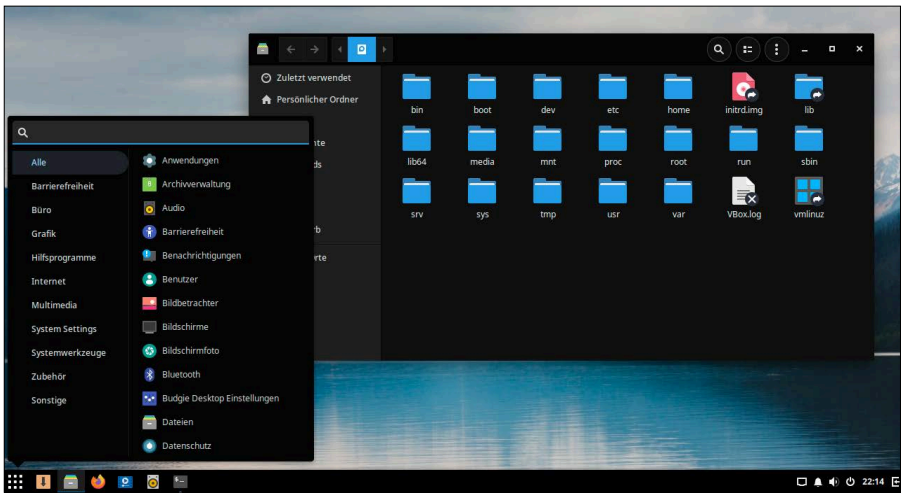
installieren. ■

STECKBRIEF DEEPIN

Webseite: *www.deepin.org*
Aktuelle Version: 2019.07.10 (19. Juli 2019)
Zielgruppe: Einsteiger und fortgeschrittene Nutzer
Ressourcenbedarf: durchschnittlich bis hoch
Anpassungsfähigkeit: gering
Repräsentative Distributionen: Deepin Linux (*www.deepin.org*), Manjaro Architekt (*https://manjaro.org*), Fedora (*https://getfedora.org*)

Der Einfache: Budgie

Budgie ähnelt LXQT, benötigt aber mehr Systemleistung. Der Desktop ist übersichtlich und besonders einfach bedienbar. Detaillierte Anpassungen sind hingegen eher mühsam.



VON THORSTEN EGGELING

Budgie ist eines der jüngsten Mitglieder im Ubuntu-Universum. Die Desktopumgebung stammt von der bisher weniger bekannten Distribution Solus (*https://getsol.us*) und lässt sich auch in Manjaro Linux Architekt installieren.
Budgie ist auch für Einsteiger geeignet, gehört aber nicht zu den Desktops mit geringen Anforderungen.

Konzept und Funktionsumfang

Bei Solus zeigt der Budgie-Desktop eine Leiste am unteren Bildschirmrand (siehe Abbildung). Diese enthält ein Startmenü mit Suchfunktion und Kategorien wie „Büro“ und „Grafik“. Ein Klick darauf öffnet die Liste der enthalten Anwendungen. In der Leiste sind außerdem einige Schnellstarter enthalten, etwa für den Dateimanager und Firefox. Am rechten Rand sind die üblichen Applets für Netzwerk, Lautstärkeregler und Herunterfahren untergebracht. Bei Solus sind Leiste und Fenster im modernen Schwarz gehalten, dazu passend ein Desktopmotiv in Dunkelblau, Schwarz und Grau.
Bei Ubuntu Budgie wandert die Leiste an den oberen Bildschirmrand, zwar ohne Schnellstarter, dafür aber mit ein paar zusätzlichen Applets (Quick Note, Night Lite, Orte). Der Desktophintergrund ist pink und blau, die Leiste halb transparent. Bunt geht es auch im Plank-Dock am unteren Bildschirmrand zu. Das Dock bietet Starter etwa für Rhythmbox, Libre Office Writer und Firefox. Der Desktop selbst ist weitestgehend funktionslos: Ordner, Dokumente oder Programmstarter lassen sich darauf nicht ablegen.

Hardwareansprüche und Leistungsbedarf

Mit Speicher geht Budgie nicht sparsam um. Solus belegt gut ein GB RAM, Ubuntu Budgie hält mit annähernd 1,4 GB den Rekord im Desktopvergleich. Schuld daran ist aber nicht nur die Desktopumgebung, sondern eine Reihe mitgestarteter Tools (was man ändern könnte).

Konfiguration und Anpassungen

Anpassungen (etwa von Systemleisten) über intuitive Kontextmenüs sind den Budgie-Entwicklern fremd. Für alle wichtigsten Optionen sind zentrale Systemwerkzeuge zuständig. Über „Budgie Themes“ installieren Sie neue Themes, in den „Budgie Desktop Einstellungen“ (beide im Menü unter „Systemwerkzeuge“) finden Sie die meisten Einstellungen, beispielsweise „Leiste oben“. Wenn man sich an das Fehlen intuitiver Kontextmenüs gewöhnt hat, sind die Budgie-Einstellungen durchaus übersichtlich. „Start“, „Zentrieren“ und „Ende“ bezeichnet die Position auf der Leiste. Man kann die Einstellungen der Elemente ändern oder weitere Applets hinzufügen.

Die manuelle Installation

Da Budgie noch eine recht neue und weniger getestete Desktopumgebung ist, empfehlen wir die Installation einer Distribution wie Solus oder Ubuntu Budgie zusammen mit diesem Desktop.
Eine Installation in Ubuntu 18.04 (Gnome 3) kann mit dem Befehl

```
sud apt install ubuntu-bungie-
  desktop
```

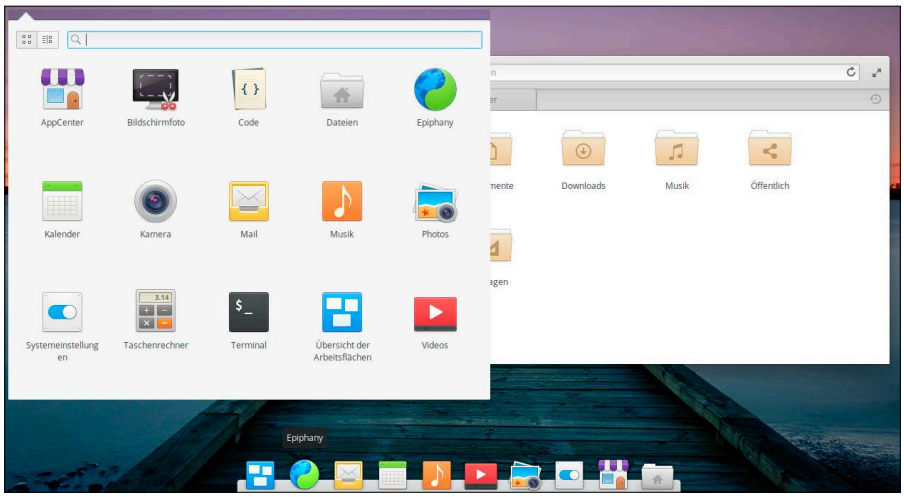
erfolgen.
Bei der Installation von Manjaro Architekt finden Sie bei der Desktopauswahl auch die Budgie-Oberfläche. ■

STECKBRIEF BUDGIE

Webseite: *https://github.com/solus-project/budgie-desktop*
Aktuelle Version: Budgie 10.5.1
Zielgruppe: Einsteiger, die einen klassischen Desktop bevorzugen und auf Anpassungen keinen Wert legen. Diese erfordern intensivere Beschäftigung und Vertrautheit.
Ressourcenbedarf: hoch
Anpassungsfähigkeit: durchschnittlich
Repräsentative Distributionen: Solus Budgie 4.0 (*https://getsol.us*), Ubuntu Budgie 19.10 (*https://ubuntubudgie.org/downloads*), Manjaro Architekt (*https://manjaro.org*)

Der Schöne: Pantheon

Der Pantheon-Desktop orientiert sich ein wenig an Mac-OS und übernimmt einige Ideen von anderen Desktopumgebungen. Die Einstellungsmöglichkeiten für persönliche Anpassungen sind allerdings rar.



VON THORSTEN EGGELING

Pantheon ist eine Entwicklung für die Distribution Elementary OS, die aktuell auf Ubuntu 18.04 basiert. Die Entwickler möchten einen Obulus für den Download der Distribution, akzeptieren aber auch die Zahlung von „0" Euro. Elementary OS ist ein sehr reduziertes System, das sich eigentlich für Linux-Einsteiger eignen würde. Dafür fehlen aber zu viele gewohnte Funktionen.

Konzept und Funktionsumfang

Das Dock am unteren Bildschirmrand erinnert an Mac-OS und dient als Programmstarter und Taskleiste. Für laufende Programme lässt sich über den Kontextmenüpunkt „Im Dock behalten" ein Starter hinzufügen. In der oberen Leiste öffnet sich nach einem Klick auf „Apps" das Anwendungsmenü mit Suchfunktion. Das zweite Icon links oben aktiviert eine Kategorienansicht. In Elementary OS ist kaum Software vorinstalliert. Libre Office fehlt, als Browser dient Epiphany. Über das „AppCenter" oder auf der Kommandozeile lassen sich jedoch alle Programme installieren, die es auch für Ubuntu gibt. Am rechten Rand zeigt die Leiste Icons für Lautstärke, Netzwerk, Benachrichtigungen. Der Klick auf das letzte Icon öffnet ein Menü mit Optionen zum „Abmelden" und „Herunterfahren".

Der Desktop ist funktionslos. Es gibt kein Kontextmenü und es lassen sich auch keine Dateien oder Verknüpfungen ablegen. In der Titelleiste der Fenster gibt es nur Knöpfe für „Schließen" und „Maximieren" beziehungsweise „Wiederherstellen". Im Kontextmenü gibt es auch „Minimieren".

Hardwareansprüche und Leistungsbedarf

Elementary OS 5.1 belegt ungefähr 630 MB RAM, bei einem Ubuntu 18.04 mit nachträglich installiertem Pantheon-Desktop gut 700 MB. Damit liegt der Desktop im Mittelfeld und sollte mit vier GB flüssig laufen.

Konfiguration und Anpassungen

In den „Systemeinstellungen" gelangt man über „Arbeitsfläche" zu einigen Desktopoptionen. Unter „Hintergrund" lässt sich ein Hintergrundbild festlegen, unter „Erscheinungsbild" die Paneltransparenz und Textgröße, unter „Dock" die Symbolgröße der Dockicons. Außerdem gibt es „Aktive Ecken" für Aktionen, die der Mauszeiger in den Bildschirmecken auslösen soll. Elementary-Tweaks erweitert die Möglichkeiten. So installieren Sie das Tool im Terminal:

```
sudo apt install software-
  properties-common
sudo add-apt-repository ppa: philip
  . scott/elementary-tweaks
sudo apt install elementary-tweaks
```

In den „Systemeinstellungen" klicken Sie danach auf das neue Icon „Tweaks". Unter „Fensterbedienung" stellen Sie hinter „Aussehen" etwa „Windows" ein. Dann erscheinen in den Titelleisten Schaltflächen für „Minimieren", „Maximieren" und „Schließen". Es gibt außerdem kleine Theme-Anpassungen für Fenster, Symbole und Mauszeiger.

Die manuelle Installation

Unter Ubuntu erhalten Sie die Dateien des Desktops aus einem PPA (vier Zeilen):

```
sudo add-apt-repository
  ppa:elementary-os/daily
sudo add-apt-repository
  ppa:elementary-os/os-patches
sudo apt dist-upgrade
sudo apt install elementary-theme
  elementary-icon-theme elementary-
  default-settings elementary-
  desktop
```

Mit folgendem Befehl

```
sudo dnf group install "pantheon
  desktop"
```

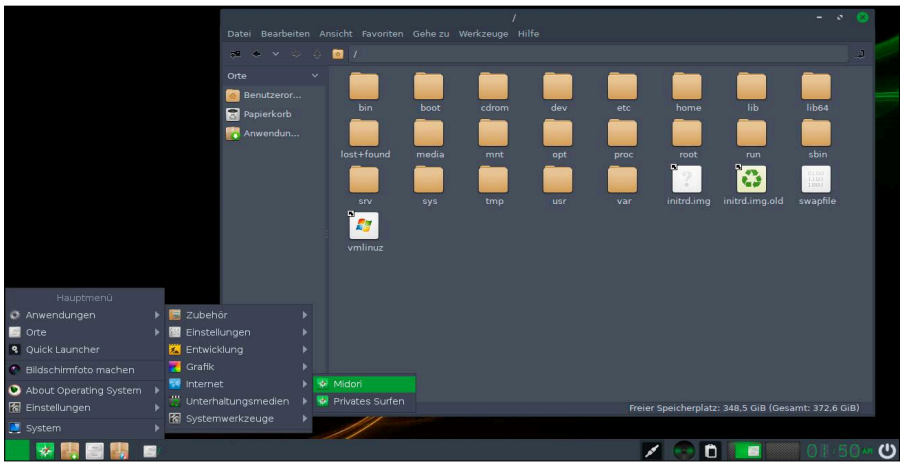
kommen Sie unter Fedora ans Ziel. ■

STECKBRIEF PANTHEON

Webseite: *https://elementary.io*
Aktuelle Version: Elementary OS 5.1
Zielgruppe: Einsteiger, die ein reduziertes Bedienkonzept schätzen
Ressourcenbedarf: durchschnittlich
Anpassungsfähigkeit: sehr gering
Repräsentative Distribution: Elementary OS 5.1 (*https://elementary.io*)

Der Schnelle: Moksha

Bodhi Linux mit Moksha-Desktop gehört in die High-Speed-Liga. Von einer SSD gebootet, ist das System nach etwa zehn Sekunden einsatzbereit. Trotzdem ist der Desktop nicht unzureichend ausgestattet.



VON THORSTEN EGGELING

Moksha ist ein Nachfolger des Enlightenment-Desktops. Nachdem die Entwicklung von Enlightenment stagnierte, startete das Moksha-Projekt, um Enlightenment weiterzuentwickeln. Das Ergebnis ist in der Linux-Distribution Bodhi Linux zu bewundern, das auf Ubuntu basiert. Enlightenment und Moksha lassen sich auch in Ubuntu installieren, das stabilere Moksha ist zu bevorzugen, weshalb wir hier nur darauf eingehen.

Konzept und Funktionsumfang

Bodhi Linux mit Moksha-Desktop zeigt auf den ersten Blick keine aufregenden Neuigkeiten. Am unteren Bildschirmrand ist eine Leiste untergebracht, deren erstes Icon zu einem schlichten Startmenü führt. Rechts daneben sind Schnellstarter etwa für den Browser Midori, das Bodhi App Center und den Dateimanager untergebracht. Auf der rechten Seite erscheint ein Systray-ähnlicher Bereich.

Der Desktop lässt sich bei Bodhi Linux nicht als Dateiablage nutzen. Nach einem linken Mausklick zeigt er das gleiche Menü wie das Startmenü in der Leiste. Von der sehr begrenzten Softwareauswahl abgesehen, würde sich Bodhi Linux auch für Einsteiger eignen. Der Fokus des Systems liegt jedoch auf dem sehr schnellen Start und maximaler Anpassbarkeit. Dank des Ubuntu-Unterbaus lassen sich aber alle für die Distribution verfügbaren Programmpakete einfach installieren.

Hardwareansprüche und Leistungsbedarf

Bodhi Linux belegt bei einer Standardinstallation etwa 250 MB Hauptspeicher. Auch bei einer nachträglichen Installation in Ubuntu 18.04 meldet ps_mem nur eine RAM-Belegung von 310 MB – deutlich weniger als bei den anderen nachinstallierten Desktopumgebungen. Damit ist Bodhi Linux ein Favorit für leistungsschwächere PCs, die zudem noch schnell starten sollen.

Konfiguration und Anpassungen

Die Konfigurationszentrale des Desktops ist im Menü über „Einstellungen → Einstellungskonsole“ („Settings → Settings Panel“) zu erreichen. Die grafische Zentrale ziehen Sie am besten so breit, dass Sie oben alle Kategorien im Blick haben und damit einen ersten Überblick erhalten. Auch wenn Sie bei der Installation als Sprache „Deutsch“ gewählt haben, ist die Oberfläche zunächst englischsprachig. Zuerst laden Sie das Modul für die Spracheinstellungen unter „Extensions → Modules“ und im neuen Fenster gehen Sie auf „Settings“. Klicken Sie auf „Language“ und dann auf „Load“. Dies erweitert die Einstellungskonsole um den neuen Punkt „Language“, wo Sie die Oberfläche auf Deutsch umstellen.

Unter „Aussehen“ finden Sie die meisten Optionen für die Darstellung des Desktops. „Thema“ betrifft die Moksha-eigenen Dialoge und die Fenstertitel, „Anwendungsthema“ das Aussehen von Programmen, die auf GTK basieren. Der Desktop Moksha selbst ist anpassungsfähig, aber er bietet keine grafische Zentrale für Hardwareeinstellungen oder Benutzerkonten.

Die manuelle Installation

Nutzer von Ubuntu 18.04 verwenden diese drei Zeilen in einem Terminalfenster:

```
echo deb [trusted=yes] http://
  packages.bodhilinux.com/bodhi/
  bionic b5main | sudo tee /etc/apt/
  sources.list.d/bodhi.list
sudo apt update
sudo apt install bodhi-desktop
```

Sie sollten die Installation wegen möglicher Nebenwirkungen jedoch nicht auf einem produktiv eingesetzten Arbeitsrechner durchführen. ■

STECKBRIEF MOKSHA

Webseite: *www.enlightenment.org, www.bodhilinux.com*
Aktuelle Version: Enlightenment 0.23.1, Moksha 0.3.1
Zielgruppe: fortschrittliche, experimentierfreudige Nutzer
Ressourcenbedarf: erstaunlich sparsam und schnell, läuft auch mit älteren CPUs und ohne 3D-Grafikchip
Anpassungsfähigkeit: sehr groß
Repräsentative Distribution: Bodhi Linux 5.0 (*www.bodhilinux.com*)

Der Umgang mit ISO- und IMG-Dateien

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

VON THORSTEN EGGELING



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

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

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

1. Dateisysteme auf DVDs und in ISO-Dateien

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

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

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

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

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

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

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

2. Dateisysteme in Laufwerksabbildern

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

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

3. Was steckt in der Abbilddatei?

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

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

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

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

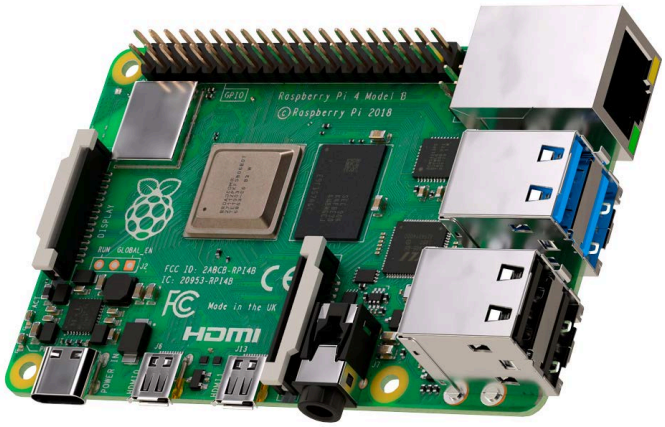
Dieses Abbild enthält also einen DOS/MBR-Bootsektor und eine Partition mit der Nummer „2“. Genauere Auskunft über die Partitionen gibt fdisk:

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

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



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



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

BACKUP: SD-KARTE UNTER LINUX SICHERN

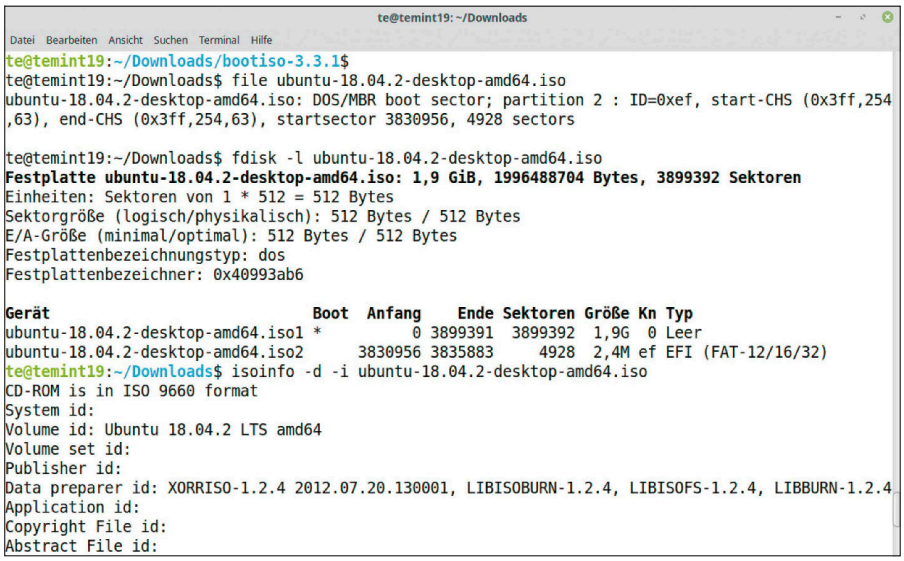
SD-Karten arbeiten im Raspberry Pi nicht immer zuverlässig. Manchmal kommt es zu Fehlern und das System startet nicht mehr. Es ist daher ratsam, ab und zu Backups zu erstellen. Fahren Sie den Raspberry Pi herunter, entnehmen Sie die SD-Karte und stecken Sie diese in den Kartenleser von PC oder Notebook.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

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

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

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

können Sie die Sicherung später wiederherstellen.



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

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

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

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

```
sudo apt install xorriso
```

nach und analysieren dann ein ISO-Abbild:

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

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

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

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

Dann bauen Sie den Bootsektor mit

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

ein.

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

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

4. Installationsmedium aus ISO-Datei erstellen

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

5. USB-Stick für die Installation erstellen

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

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

```
lsblk -p
```

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

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

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

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

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

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

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

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

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

Führen Sie diese drei Befehlszeilen im Downloadverzeichnis aus:

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

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

6. USB-Stick per Bash-Script befüllen

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

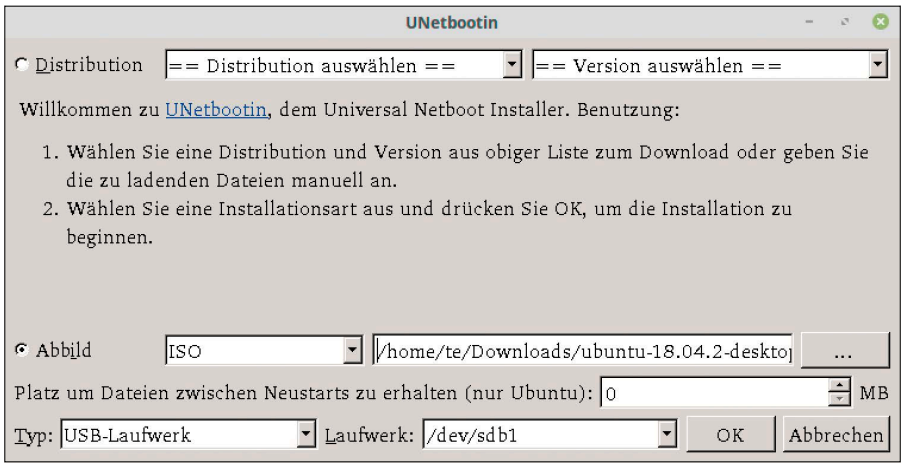
```
sudo apt install curl wimtools
 extlinux
```

Starten Sie das Script mit

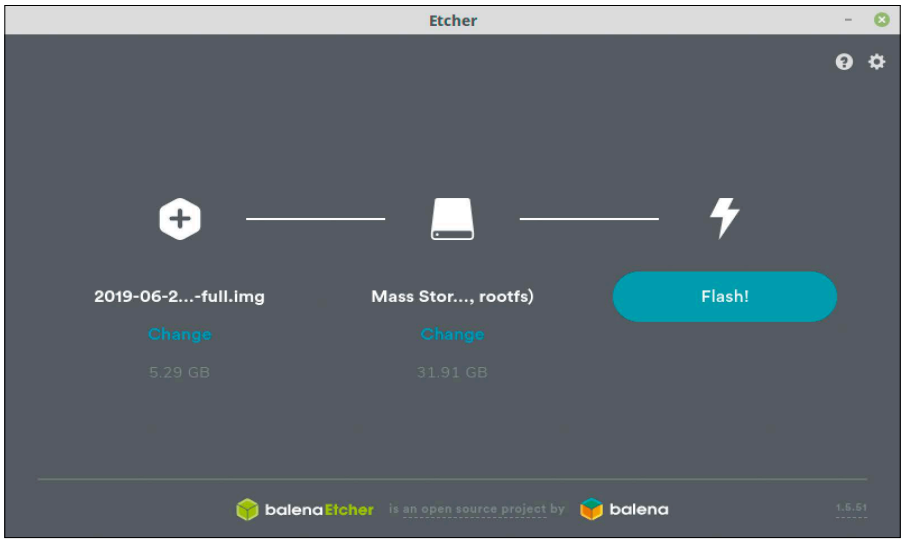
```
./bootiso -p [Boot-DVD.iso]
```

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

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



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



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

7. Images für Platinen-PCs kopieren

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

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

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

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

Ubuntu-Installationen

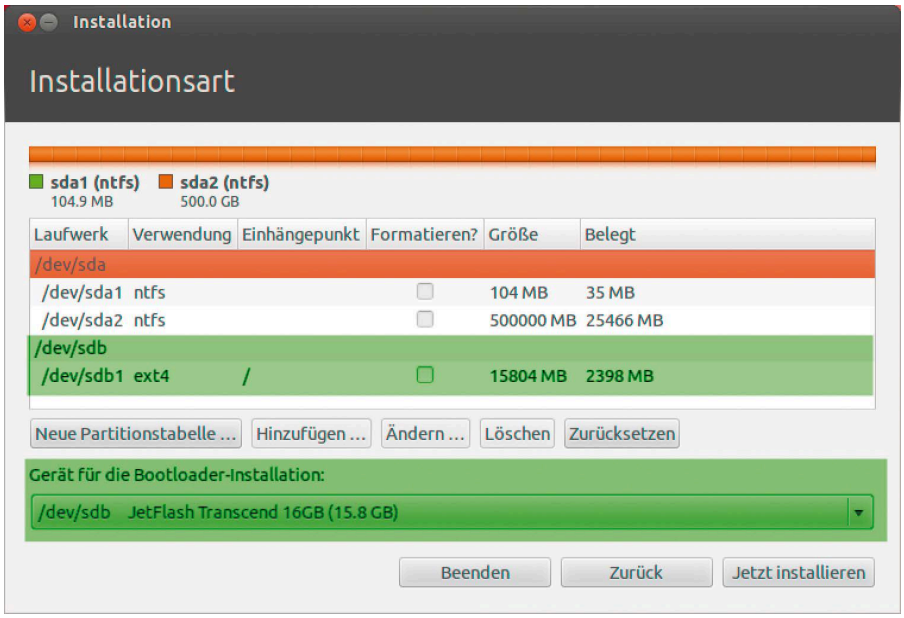
Dieser Beitrag erklärt alle Varianten der Ubuntu-Einrichtung und hat eine Reichweite, die weit über offizielles Ubuntu hinausgeht: Fast alle namhaften Desktopdistributionen verwenden beim Setup das Installationsprogramm von Ubuntu.

VON HERMANN APFELBÖCK

Installationen erfolgen über das (Ubuntu-) Livesystem, mit dem Sie Ihr Zielgerät booten und – im Normalfall – mit der Desktopverknüpfung „Ubuntu … installieren“ die Einrichtung starten. Bis zur Version 18.04 LTS verwenden alle Ubuntus denselben grafischen Installer Ubiquity. Auf diesen beziehen sich die meisten der folgenden Infos. Wo nötig, benennen wir Unterschiede beim Installer Calamares, der inzwischen in den Versionen von Kubuntu und Lubuntu ab 19.04 benutzt wird. Funktional bestehen zwischen Ubiquity und Calamares kaum Unterschiede.

Installation als alleiniges System

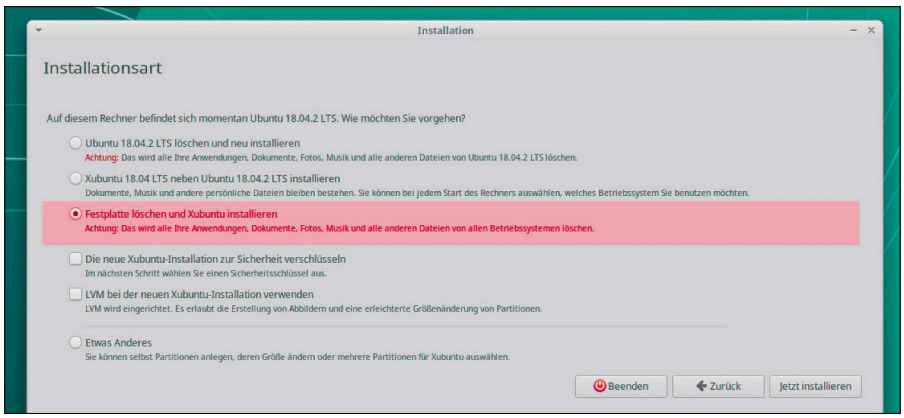
Zur Installation booten Sie den gewünschten Zielrechner mit dem System Ihrer Wahl. Dessen ISO-Abbild muss dazu vorher auf DVD oder auf USB-Stick geschrieben werden. Auf diese Aktion gehen wir im vorherigen Artikel ab Seite 24 ein sowie auf der Heft-DVD im PDF „LinuxWelt XXL“, in dem Sie viele weitere Grundlagenartikel finden. Standardmäßig sind PCs und Notebooks so eingestellt, dass sie automatisch von CD/DVD booten. Sollte dies anders konfiguriert sein, müssen Sie nach Einschalten das Bootmenü des Bios aufrufen. Dies erledigt in der Regel eine Funktionstaste, häufig F2, F8 oder F12, gelegentlich auch die Esc-Taste. Im Bootmenü wählen Sie dann das DVD-Laufwerk, das Sie an Kennzeichnungen wie „Internal CD/DVD“ oder „Atapi“ erkennen. Wenn Sie Ubuntu von USB booten, verwenden Sie ebenfalls das Bootmenü.
Beim gestarteten System handelt es um ein Livesystem, das den Installer mitbringt und auf dem Desktop als Verknüpfung anbietet. Für eine Ubuntu-Installation als alleiniges System sind keine weiteren Vorbereitungen nötig. Nach dem Start der Verknüpfung



Installation auf externe USB-Medien: Hier müssen Sie das richtige Laufwerk manuell orten und partitionieren. Auch der Bootloader muss auf das USB-Laufwerk.

wählen Sie die Sprache, Tastatur und die „Installation von Drittanbieter-Software“. Nach diesen einfachen Abfragen erscheint eventuell die Frage „Aktive Partitionen aushängen?“. Um sich alle Möglichkeiten offenzuhalten, antworten Sie hier mit „Ja“, um Zugriff auf alle Partitionen zu erhalten. Im nächsten Schritt erscheint der entscheidende Dialog „Installationsart“ mit zwei möglichen Szenarien:

1. Wenn die primäre Festplatte des Rechners kein System enthält, lautet die oberste

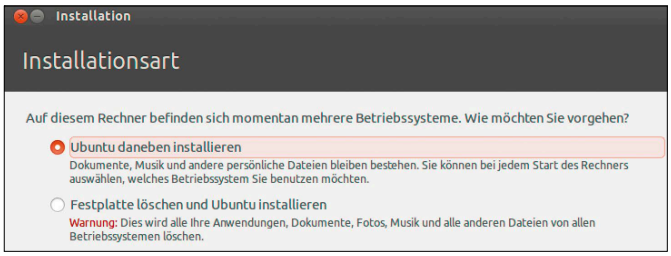


Einfachster Fall mit „tabula rasa“: Zum Einrichten als alleiniges System wählen Sie „Festplatte löschen …“. Der Installer erledigt Partitionierung und Auslagerung automatisch.

und vormarkierte Option „Festplatte löschen und Ubuntu installieren“.
2. Hat der Installer auf der primären Festplatte ein System gefunden, dann erscheint als oberste und markierte Option „Ubuntu neben [...] installieren“ und erst als zweite Option „Festplatte löschen [...]“.
Für die Einrichtung von Ubuntu als alleiniges System verwenden Sie in beiden Situationen „Festplatte löschen [...]“. Die übrigen Optionen des Dialogs lassen Sie ungenutzt und beginnen mit „Jetzt installieren“ den Vorgang, der danach nur noch die Angaben für das erste Benutzerkonto verlangt. Die Festplatte wird formatiert, der Datenbestand (und ein eventuelles System) gelöscht und Ubuntu eingerichtet.
Installer Calamares: Falls Sie aktuelles Kubuntu oder Lubuntu 19.04 oder später installieren, lautet der maßgebliche Schritt „Einrichtung der Festplatten“ oder „Partitionen“. Hier aktivieren Sie die Option „Geführt – vollständige Festplatte verwenden“, um das System als alleiniges System auf der primären Festplatte einzurichten.

Installation auf USB

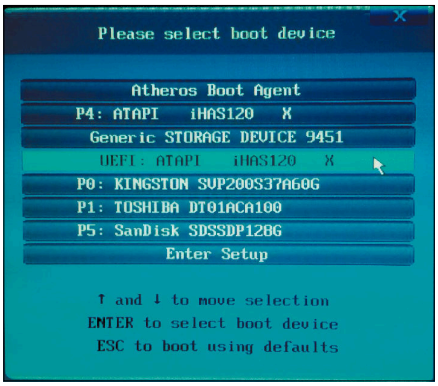
Ubuntu lässt sich auch ganz regulär auf USB oder auf eine sekundäre interne Platte installieren. Da der Installer stets die erste interne Festplatte „/dev/sda“ als Ziel vorschlägt, müssen Sie bei der Einrichtung auf ein USB-Gerät manuell die richtige Zielpartition festlegen. Daher wählen Sie im Fenster „Installationsart“ die Option „Etwas Anderes“. Das Laufwerk muss neu partitioniert und formatiert werden, alle darauf befindlichen Daten gehen verloren. Klicken Sie zunächst auf die „-“-Schaltfläche, um vorhandene Partitionen zu entfernen. Erstellen Sie dann auf dem „freien Speicherplatz“ mit der „+“-Schaltfläche eine neue primäre Partition mit dem kompletten Speicherplatz und dem Dateisystem Ext4. Hinter „Einbindungspunkt“ wählen Sie den Eintrag „/“ aus der Liste. Unter „Gerät für die Bootloader-Installation“ wählen Sie dasselbe USB-Laufwerk aus, auf dem Sie installieren – etwa „/dev/sdb“. Es ist wichtig, auch den Bootloader auf USB zu schreiben, andernfalls startet das System nur auf dem Rechner, mit dem Sie installiert haben. Bei Installation auf eine sekundäre interne Platte verwenden Sie hingegen „/dev/sda“ für den Bootloader.
Calamares: Bei diesem Installer (ab Kubuntu oder Lubuntu 19.04) lautet der maßgebliche Schritt „Einrichtung der Festplatten“ bzw. „Partitionen“. Hier benötigen Sie für USB-Installation den Unterpunkt „Manuell“. Nach „Weiter“ erhalten Sie eine Laufwerkliste, können dort ein USB-Medium wie „/dev/sdb1“ löschen und neu anlegen – mit den gleichen Einstellungen wie oben bei Ubiquity beschrieben.



Hier wurden mehrere vorhandene Systeme erkannt. Wenn Sie „daneben“ installieren, entsteht durch Verkleinern einer bestehenden Partition eine neue für Ubuntu.

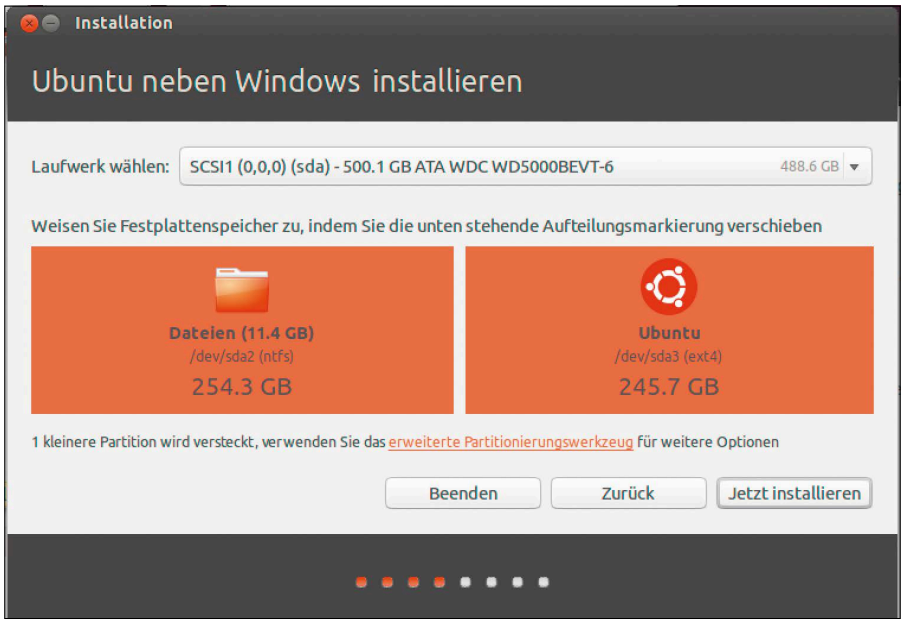
Multiboot mit Ubuntu

Der Ubuntu-Installer erkennt und respektiert vorhandenes Windows oder Linux. Etwas knifflig ist jedoch die Unterscheidung zwischen Bios- und Uefi-Partitionsschema. Bei der oben beschriebenen Soloinstallation spielt der Partitionsstil keine Rolle. Sobald aber zwei oder mehr Systeme parallel installiert werden sollen, dann wird der richtige Partitionsstil – Bios/MBR versus Uefi/GPT – entscheidend. Die Parallelinstallation kann nur gelingen, wenn das Livesystem in jenem Modus gestartet wird, in dem das bereits installierte System läuft. Andernfalls kann der Installer das vorhandene System nicht erkennen und wird dieses, sofern der Benutzer das Problem nicht bemerkt, bei der Ubuntu-Installation überschreiben.
Auf PCs mit Windows 8 oder 10 herrscht der moderne Uefi-Modus mit GPT-Partitionsstil. Weitere Systeme müssen auf die gleiche Weise eingerichtet werden. Da der Parallelbetrieb von Windows und Linux eines der verbreitetsten Multiboot-Szenarien ist, fokussieren wir uns nachfolgend auf die Parallelinstallation neben Windows im Uefi-Modus. Den aktuellen Partitionsstil des existierenden Systems können alle einschlägigen Tools ermitteln – unter Windows die „Datenträgerverwaltung“, unter Ubuntu Gparted, Gnome-Disks oder der KDE-Partitionsmanager. GPT erscheint hier als „gpt“, der MBR-Modus als „msdos“.
Uefi und GPT: Uefi/GPT ist bei Linux-Nutzern unbeliebt, weil es Komplikationen mit sich bringt. Allerdings ist GPT (GUID Partition Table) eine technisch notwendige Antwort auf die Tatsache, dass der alte MBR-Partitionsstil nur maximal zwei TB pro Partition adressiert – eine Grenze, die aktuelle Festplatten längst überschreiten. Für die Installation neben Windows 8/10 gelten folgende Regeln:



Uefi-Bootmenü: Die eingelegte DVD mit dem Livesystem erscheint zweimal – als „P4: ATAPI“ und als „Uefi: ATAPI“. Für eine Uefi-Installation muss diese zweite Bootoption gewählt werden.

1. Nur 64-Bit-Linux beherrscht GPT. Auch 32-Bit-Systeme können natürlich im Multiboot-Betrieb arbeiten, jedoch nur im Bios-/MBR-Partitionsstil. Ein Multiboot mit Windows 8/10 ist damit nicht möglich.
2. Die Heft-DVD der LinuxWelt bootet nur im Bios-Modus und eignet sich nicht für eine Uefi/GPT-Parallelinstallation. Sie müssen das gewünschte ISO-Abbild auf ein eigenes Medium transferieren (DVD oder USB) und Ubuntu damit installieren. Die ISO-Abbilder der Heft-DVD (unter „/Image-Dateien“) können Sie aber sehr wohl verwenden und sich den Download sparen.
3. Wenn das passende Installationsmedium vorliegt, müssen Sie damit den Zielrechner über das Bootmenü des Uefi-Bios starten. Das Bootmenü ist meistens durch frühzeitiges Drücken der Taste F2, F8, F12 oder Esc zu erreichen. Dort erscheinen dann die Laufwerke zwei Mal – einmal mit, einmal ohne den Vorsatz „UEFI“. Für Uefi-Parallelinstallation wählen Sie den „UEFI“-Eintrag. Einen eindeutigen Hinweis, dass Sie im richtigen Modus sind, liefert danach der Ubuntu-Installer, sofern er das vorhandene



Parallelinstallation: Der Installer verkleinert automatisch die bestehende Partition (links), um Platz für Ubuntu (rechts) zu schaffen. Mit der Maus verändern Sie die Kapazitäten nach Bedarf.

System anzeigt und die Option „Ubuntu neben [XXX] installieren“ anbietet oder auch allgemein „Ubuntu daneben installieren“, wenn mehrere Systeme vorliegen.

Hinweis „Secure Boot“: Uefi-Installationen haben einen weiteren Fallstrick. Die Uefi-Funktion „Secure Boot“ verhindert das Booten nicht signierter Systeme, was den Start von Schadsoftware verhindern soll. Im Unterschied zu Ubuntu-Derivaten besitzen aber offizielle Ubuntu-Editionen eine „Secure Boot“-Signatur. Nur wer selbst kompilierte Kernel oder Treiber einsetzen will, muss „Secure Boot“ im Uefi-Bios deaktivieren („Bios Features → Security“ oder ähnlich).

Starten Sie im Livesystem das Setup über das Desktopicon. Was das Fenster „Installationsart“ dann anbietet, hängt von der Situation ab. Wir gehen hier von einer Parallelinstallation neben Windows aus, jedoch gelten diese Infos auch für ein bereits bestehendes Linux-System im Uefi-Modus:

A. Gibt es nur eine Festplatte, die derzeit von Windows belegt ist, sehen Sie die Option „Ubuntu neben Windows Boot Manager installieren“. Nach einem Klick auf „Weiter“ schlägt der Assistent eine neue Aufteilung der Partitionen vor, indem er die Windows-Partition verkleinert und Platz für Ubuntu schafft. Die Partitionsgröße lässt sich ändern, indem Sie die Aufteilungsmarkierung mit der Maus verschieben.

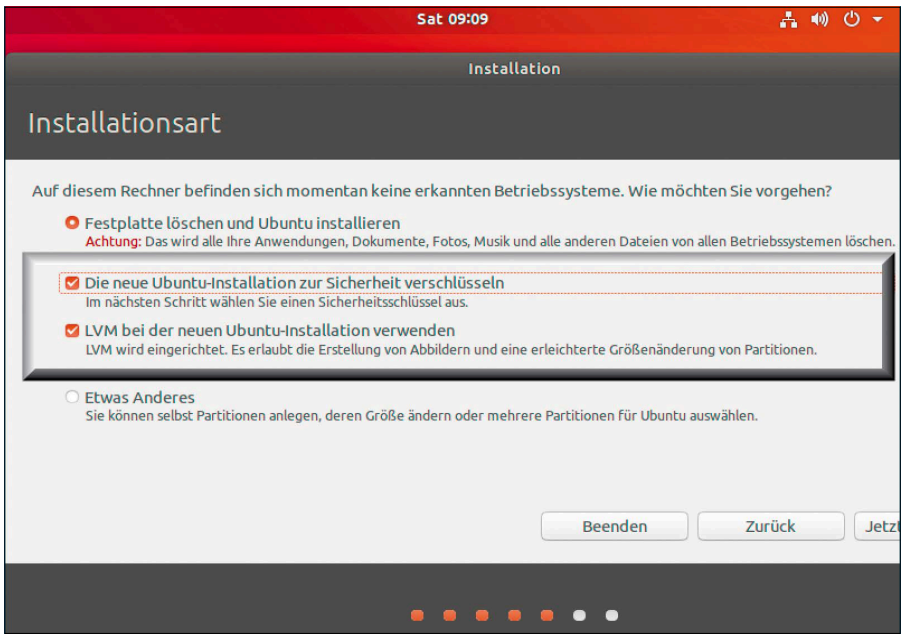
B. Ist neben einem installierten Windows oder Linux eine freie Partition vorhanden, erkennt der Installer das automatisch. Auch in diesem Fall wählen Sie die Option „Ubuntu neben Windows Boot Manager installieren“.

C. Sind zwei oder mehr Systeme vorhanden, dann führt das Angebot, „Ubuntu neben [XXX]“ zu installieren, zu einer weiteren Aufteilung und Partitionierung wie unter Variante A. Wenn Sie das neue System nicht zusätzlich installieren, sondern vielmehr eines der bestehenden Systeme durch das neue ersetzen möchten, gehen Sie anders vor und wählen „Etwas Anderes“. Die weiteren Schritte sind so wie oben für die Installation auf USB beschrieben: Sie löschen in der Laufwerkliste mit der „-“-Schaltfläche die Partition des obsoleten Systems und erstellen dann im „Freien Speicherplatz“ mit der „+“-Schaltfläche eine neue Ext4-Partition mit dem Mountpunkt „/“.

Die verschlüsselte Systempartition

Luks-verschlüsselte Systempartitionen sind der beste Schutz für Notebooks. Der Datenträger lässt auch beim Booten durch Fremdsysteme keinen Einblick in die Daten zu. Luks-Verschlüsselung (des Systems) ist nur bei der Installation möglich – nicht nachträglich. Die Ubuntu-Installer Ubiquity und Calamares bieten diese Option per einfachen Klick an. Der entscheidende Dialog im Installationsprogramm lautet „Installationsart“ (oder „Partitionen“). Beachten Sie, dass Sie für die Verschlüsselung dem Installer die gesamte primäre Festplatte überlassen müssen. Die Festplatte sollte leer sein oder nur noch Daten enthalten, die Sie nicht mehr benötigen.

Für Luks-Verschlüsselung wählen Sie „Festplatte löschen und Ubuntu installieren“. Darunter aktivieren Sie „Die neue Ubuntu-Installation ... verschlüsseln“ (Calamares: „Verschlüssele System“). Sobald Sie dies tun, wird der Punkt „LVM [...] verwenden“



Luks-Datenträgerverschlüsselung: Diese Option ist in allen Ubuntus einfach einzurichten, sofern das neue System die komplette primäre Festplatte übernehmen darf.

aktiv. Der Logical Volume Manager (LVM) ist notwendig, um neben der kleinen Bootpartition die Luks-formatierte Partition und die virtuelle LVM-Partition unterzubringen, die bei korrekter Kennworteingabe unverschlüsselt ins Dateisystem geladen wird.
Wenn Sie dann auf „Weiter“ klicken, folgt die Abfrage des Sicherheitsschlüssels (Kennwort). Dieser sollte eine gewisse Mindestkomplexität haben, aber für tägliche Eingabe zumutbar sein, denn das System startet später nur noch nach Kennworteingabe. Der Rest der Installation verläuft wie gewohnt. Wenn Sie später das System booten, erscheint stets die Abfrage „Please unlock disk [...]“. Dort geben Sie das Kennwort ein, um den Systemstart fortzusetzen.
Hinweis: Neben der Luks-Verschlüsselung gibt es für Desktopbenutzer keinen Anlass, bei der Installation „LVM“ zu aktivieren. Der Logical Volume Manager ist eine Abstraktionsschicht für Serversysteme mit flexiblen Kapazitätsansprüchen, um Festplatten zusammenzufassen und dynamisch zu erweitern.

Ubuntu Server: Netinstaller mit Highlights

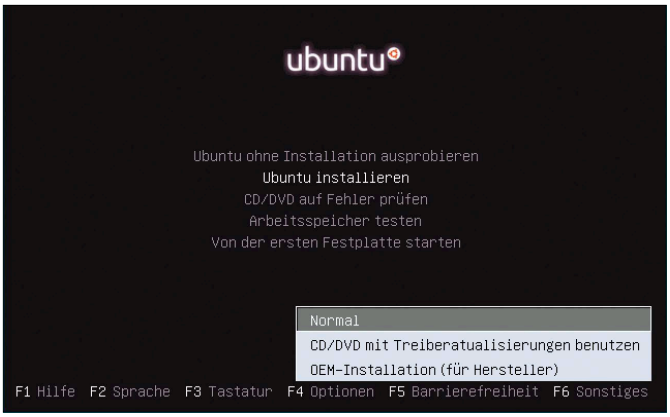
Wer Ubuntu auf PC oder Notebook einrichten will, wird den Ubuntu Server kaum auf der Rechnung haben. Der kann aber auch ein Desktopsystem installieren und bietet dabei interessante Vorteile. Vom Ubuntu Server gibt es zwei unterschiedliche Installer: ein großes Installationsmedium, das die meisten Pakete mitbringt, und einen winzigen Netinstaller, der alles aus dem Internet bezieht. Die angesprochenen Vorteile bringt nur der kleine Netinstaller (65 bis 75 MB), den Sie von *http://cdimage.ubuntu.com/netboot/* beziehen können. Empfohlene Version ist 18.04 LTS. Ethernet ist technische Voraussetzung für diese Installationsmethode, WLAN wird nicht unterstützt. Nun zu den Vorteilen:
1. Den Ubuntu Server gibt es bis hin zu den jüngsten Versionen auch noch in 32-Bit-Ausführung. 32-Bit-Systeme gehen sparsamer mit dem Arbeitsspeicher um und sind daher erste Wahl für ältere Hardware mit bis zu vier GB RAM, auch wenn eine 64-Bit-CPU vorliegt.
2. LTS-Versionen von Ubuntu Server erhalten wie die Ubuntu-Hauptversion (Gnome) volle fünf Jahre Updatesupport. Für alle anderen offiziellen Editionen (Kubuntu, Xubuntu, Mate etc.) gilt dies bekanntlich nicht: Sie erhalten nur drei Jahre Unterstützung. Da der Netinstaller am Ende eine Auswahl des Desktops vorsieht, können Sie sich ein Kubuntu (KDE), Xubuntu (XFCE) et cetera nach Belieben einrichten – mit fünf Jahren Support.
Das kleine Abbild (mini.iso) des Netinstallers bietet nur einen einfachen textbasierten Installer. Der Ablauf ist aber analog dem grafischen Ubiquity und unterstützt auch Verschlüsselung und Parallelinstallation. Für unseren Tipp entscheidend ist der abschließende Dialog „Softwareauswahl“, der nicht nur Serverpakete wie Samba, Open SSH oder Lamp anbietet, sondern auch sämtliche Oberflächen, die Sie von offiziellen Ubuntu-Editionen kennen.



Netinstaller für Ubuntu Server: Diese Setupmethode eignet sich auch für Desktopinstallationen und hat dabei zwei Vorteile (maximale Supportdauer und 32 Bit).

Die Installationsvariante „OEM install“

Wer Ubuntu für sich selbst installiert, hat mit der OEM-Variante keinerlei Vorteile. Aber die OEM-Installation bietet sich an für eine saubere Installation für Freunde oder Familienmitglieder. „Sauber“ deshalb, weil Sie das System mit einem temporären Konto „oem“ konfigurieren und der künftige Besitzer später unabhängig über sein eigenes Konto entscheidet (Name, Kennwort).
An den OEM-Installer kommen Sie nur, wenn Sie den Bootvorgang des Livesystems mit der Umschalt-Taste ausbremsen. Dann erscheint eine Auswahl mit fünf Optionen: Taste F4 blendet die „OEM Installation (für Hersteller)“ ein. Der Ablauf unterscheidet sich zunächst kaum von einer normalen Installation.
Ein wichtiger Unterschied ergibt sich beim Anlegen des Erstbenutzers („Wer sind Sie?). Dieser ist unveränderbar als „oem“ vorgegeben.
Der erste Start des so installierten Systems geht ohne Anmeldung zum Desktop. Nun können Sie im temporären Konto „oem“ das System optimieren. Nur systemweite Aktionen sind sinnvoll (Aktualisierung, Installationen, Netzwerk), benutzerspezifische Anpassungen nicht. Danach kann am Desktop der Link „Vorbereitung zur Auslieferung...“ geklickt und der Rechner dem Endbenutzer übergeben werden. Diesem wird dann der bekannte Dialog „Wer sind Sie?“ erneut angeboten, um nun den endgültigen Erstbenutzer anzulegen. ■

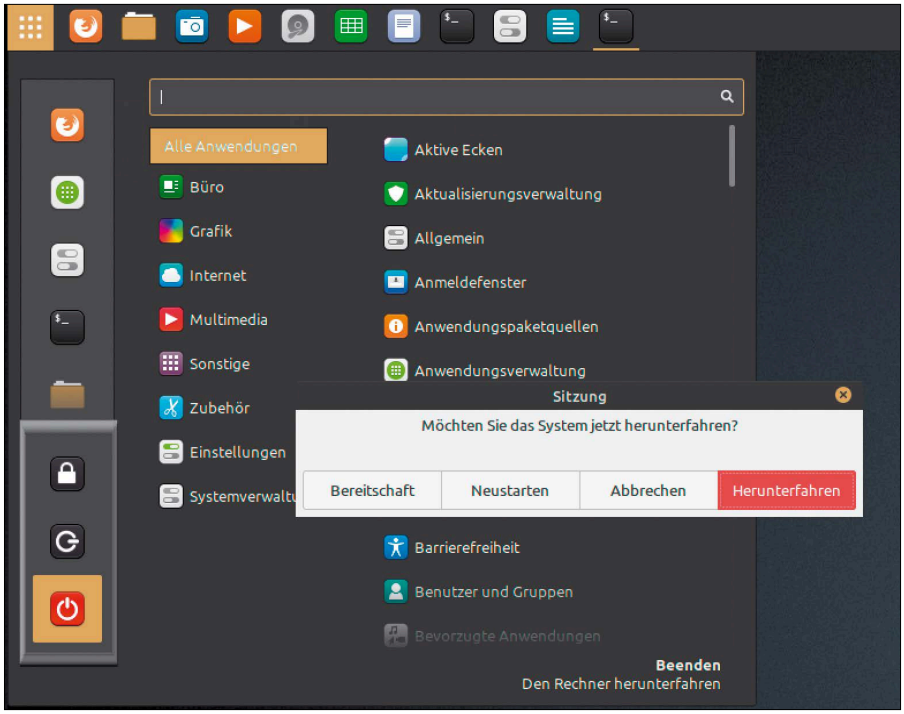


Nicht nur für Händler: Die OEM-Installation ermöglicht eine „saubere“ Systemeinrichtung für Freunde und Bekannte.

Grundlagen der Systemverwaltung

Nach der Installation sind Desktopsysteme wie Ubuntu und Linux Mint einsatzbereit. Das heißt aber nicht, dass die Systeme bereits optimal eingestellt sind. Wie bei jedem Betriebssystem gibt es Aufgaben der Systempflege, Fehlersuche und Optimierung.

VON HERMANN APFELBÖCK



Linux Mint zeigt seine Shutdown-Funktionen im Startmenü. Ubuntus mit Gnome & Co. bieten dafür ein Symbol in der Systemleiste.

Der nachfolgende Artikel erklärt die wichtigsten Aufgaben der Verwaltung und Wartung einer Ubuntu-Hauptedition (Gnome) und eines Linux Mint (Cinnamon). Dabei werden eindeutig die grafischen Werkzeuge im Vordergrund stehen und das Terminal nur eine Nebenrolle spielen. Die prominenten „Systemeinstellungen", die Gnome und Cinnamon bereitstellen, legen nur die Basis und sind nur zum geringeren Teil wirklich systemnah. Wichtige Aspekte wie Herunterfahren, Systemaktualisierung, Rechteverwaltung, Taskkontrolle, Autostarts und Cronjobs, Informationsmöglichkeiten über Hardware und Systemereignisse sind in den „Systemeinstellungen" nicht oder nicht ausreichend berücksichtigt.

1. Anmelden – Abmelden – Herunterfahren

Ubuntu und Mint zeigen nach dem Systemstart einen Anmeldebildschirm. Sie sehen den Benutzernamen, den Sie bei der Installation festgelegt haben. Klicken Sie diesen an, tippen Sie das Kennwort ein und bestätigen Sie mit „OK" oder Eingabetaste. Wenn Sie bei der Installation die Option „Automatisch anmelden" gewählt haben, entfällt die Anmeldung.

Das Beenden des Systems ist unterschiedlich geregelt: Bei Gnome und seinen Verwandten sehen Sie in der Systemleiste ganz rechts eine Schaltfläche mit dem Sitzungsmenü. Nach einem Klick können Sie hier zwischen „Abmelden", „Bereitschaft" (Suspend to RAM) und „Herunterfahren" wählen. In der Ubuntu-Hauptedition mit Gnome muss die stromsparende „Bereitschaft" durch Druck der Alt-Taste aktiviert werden. Auch das „Abmelden" – also die Benutzersitzung beenden – erscheint bei Gnome nicht direkt, sondern als Option unterhalb des angezeigten Kontonamens.

In Linux Mint sind alle Beenden-Funktionen im Hauptmenü untergebracht. Wer hier zusätzlich ein Sitzungsmenü à la Gnome in der Systemleiste haben will, kann dort das Leistenapplet „Benutzeranzeige" aktivieren.

2. Systemverwaltung und sudo-Recht

Aufgaben wie Installieren, Aktualisieren, Konfigurationsarbeiten setzen root-Recht voraus. Um dieses einzuräumen, ist „Substitute user do" (kurz „sudo") fester Bestandteil jeder Ubuntu/Mint-Distribution. Sudo erlaubt normalen Benutzerkonten, Befehle im Rechtekontext eines anderen Kontos auszuführen – in der Regel als root:

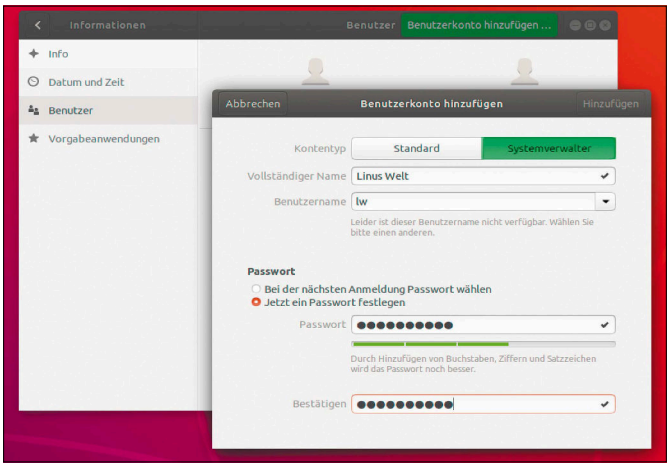
```
sudo gedit /etc/fstab
```

Ohne explizite Angabe eines Kontos (Schalter „-u") geht sudo automatisch vom Wechsel zum root-Konto aus. Im Beispiel wird die Datei „fstab" im Editor gedit geladen. Unter Linux Mint wäre Xed der passende Editor. Root-Recht ist nötig, weil normale

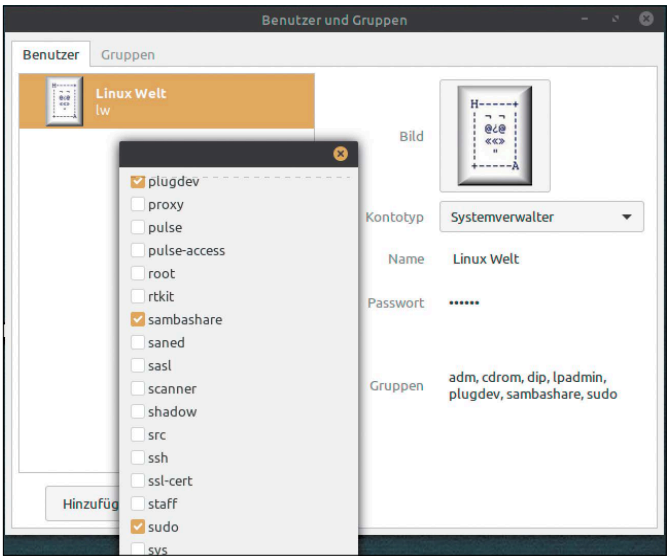
Benutzerkonten im Verzeichnis „/etc/“ kein Schreibrecht haben.
Sudo sorgt also dafür, dass zur vollständigen Systempflege ein gewöhnliches Benutzerkonto genügt. Das bei der Installation eingerichtete Erstkonto erhält diese sudo-Erlaubnis automatisch. Wenn Sie in den Systemeinstellungen unter „Benutzer und Gruppen“ ein neues Konto vom Typ „Systemverwalter“ anlegen, erhält auch dieses neue Konto sudo-Erlaubnis. Die Notwendigkeit, die verantwortliche Konfigurationsdatei „/etc/sudoers“ manuell zu bearbeiten, ergibt sich unter Ubuntu und Mint praktisch nie. Mit sudo und nachfolgendem Programmnamen

```
sudo nemo
```

lässt sich root-Recht erzwingen, das dann auch für alle nachfolgenden Aktionen im aufgerufenen Programm weiter gilt – hier im Dateimanager Nemo. Wer den Terminalaufruf vermeiden möchte, kann das root-Recht auch direkt im Dateimanager anfordern. Dazu verhilft die Eingabe *admin:///etc/* in der Adresszeile, die das Wurzelverzeichnis startet. Nemo in Linux Mint bietet überdies im Kontextmenü den Punkt „Als Systemverwalter öffnen“, der ebenfalls root-Recht eröffnet.



Systemverwaltung benötigt sudo-Recht: Wenn ein Konto als „Systemverwalter“ eingerichtet wird, erhält es automatisch sudo-Berechtigung, ebenso das bei der Installation erstellte Erstkonto.



Mint hat das umfassende Applet „Benutzer und Gruppen“ in den „Systemeinstellungen“. Ubuntu (Gnome) vereinfacht hier stark, kann das Applet aber nachrüsten (Paket „gnome-system-tools“).

3. 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 schlichte Anlegen von Standard- und Systemverwalterkonten ohne Gruppenzugehörigkeiten. Auf den meisten Desktopsystemen ist dies aber völlig ausreichend. Bei höheren Ansprüchen sollten Sie das Paket „gnome-system-tools“ nachinstallieren, was das frühere Tool „Benutzer und Gruppen“ wieder auf das System bringt. Linux Mint hat das standardmäßig, zeigt unter „Benutzer und Gruppen“ für jedes Konto die zugehörigen Gruppen und kann die Mitgliedschaft nach Klick auf „Gruppen“ detailliert justieren. Unter dem weniger auskunftsfreudigen Ubuntu bietet

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

eine gut lesbare Kontrolle über die Gruppenzugehörigkeit eines bestimmten Kontos.

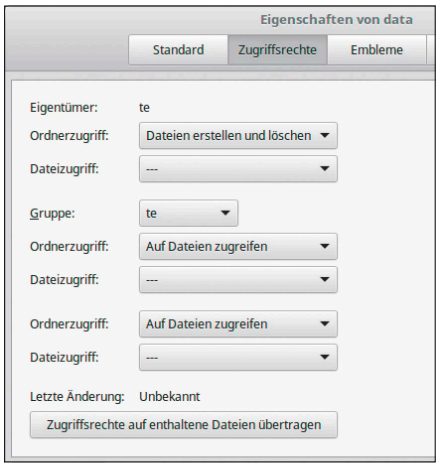
Für uneingeschränkte Systemnutzung – auch für Verwaltungsaufgaben – genügt aber in der Regel Zugehörigkeit zu den Gruppen „sudo“, „plugdev“, „audio“, „cdrom“ und „adm“. Streng genommen reicht allein „sudo“, um sich bei Bedarf jedes fehlende Recht zu verschaffen.
2. Konten vom Typ „Systemverwalter“ erhalten automatisch die wichtige sudo-Berechtigung. Nachträgliches sudo-Recht kann durch Ändern des Kontotyps, in Linux Mint auch über die detaillierten Gruppeneigenschaften zugeteilt werden.
3. Der Netzwerkdienst Samba benutzt eigene Passwörter. Jeder Benutzer, der auf die Freigaben zugreifen darf, benötigt daher, unabhängig vom Systemkonto, ein Samba-Passwort. Dazu verwenden Sie das Tool System-Config-Samba („Einstellungen → Samba-Benutzer“) oder diesen Befehl im Terminal:

```
sudo smbpasswd -a sepp
```

Am einfachsten ist es, als Samba-Kennwort erneut das Systemkennwort zu verwenden.

4. Zugriffsrechte für Dateiobjekte

Egal ob direkt am System oder beim Zugriff via Samba oder SSH – ohne lokale Zugriffsrechte ist Lesen und Schreiben nicht möglich. Gerade bei Zugriffsproblemen via Samba liegt es seltener an fehlenden Samba-Rechten als vielmehr an fehlenden lokalen Dateirechten.
Welche Rechte für einen Ordner gelten, ermitteln Sie unter Ubuntu im Dateimanager Nautilus im Kontextmenü unter „Eigenschaften → Zugriffsrechte“. Unter „Zugriff“ können Sie die Rechte für „Besitzer“, „Gruppe“ und „Andere“ festlegen. Per Klick auf die Schaltfläche „Zugriffsrechte der enthaltenen Dateien ändern“ lassen sich dann bei Ordnern die Rechte rekursiv für alle enthaltenen Dateiobjekte setzen. Um Ordnerinhalte für alle Konten erreichbar zu machen,



Zugriffsrechte in Linux Mint: Der dritte unterste Block bezieht sich auf alle anderen Systemkonten (neben „Besitzer“ oben und „Gruppe“ in der Mitte). Der entsprechende Hinweis fehlt diesem Dialog.

muss unter „Andere“ mindestens die Option „Auf Dateien zugreifen“ eingestellt sein (Lesezugriff). Für vollen Schreibzugriff ist die Option „Dateien erstellen und löschen“ zuständig.

Unter Linux Mint und Dateimanager Nemo sind die Verhältnisse analog, allerdings fehlt dem Rechtedialog der Zuordnungshinweis „Andere“. Während „Eigentümer“ und „Gruppe“ angezeigt sind, hat der dritte und unterste Block keine Zuordnung. Er bezieht sich aber genau wie bei Ubuntu auf alle anderen Konten, die hier Lese- und Schreibrecht erhalten können.

Achtung: Dateirechte lassen sich im Dateimanager nur ändern, wenn Sie der „Eigentümer“ sind. Für Rechteänderung an anderen Dateiobjekten müssen Sie den Dateimanager daher mit root-Recht starten (*sudo nautilus* im Terminal).

Den bequemeren Weg, nämlich einen Menüpunkt „Als Administrator öffnen“ wie in Mint und Nemo, können Sie bei häufigem Bedarf auch für Nautilus mit dem kleinen Paket „nautilus-admin“ nachrüsten. Ungeachtet der möglichen Rechteänderungen im Dateimanager ist für umfangreiche Aktionen das Terminal immer noch erste Wahl:

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

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

5. Hardware einrichten und optimieren

Standardperipherie wie SATA, Monitor, Ethernet, Tastatur, Maus, Touchpad, Audiochip kann in den „Systemeinstellungen“ näher konfiguriert werden, erfordert aber hardwaretechnisch wenig Aufmerksamkeit. Bei Grafikkarten, Druckern und WLAN-Adaptern 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 → Hinzufügen“ problemlos einzurichten. Taucht das Gerät 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).

Externe USB-WLAN-Adapter erkennt Linux größtenteils, aber nicht lückenlos. Eine Übersicht zu WLAN-Chipsätzen für Ubuntu und Mint 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).

6. Automount und statisches Mounten

Der Umgang mit internen Festplatten und Hotplug-Medien wie USB-Festplatten und Sticks ist unter Ubuntu und Linux Mint einfach. Sie schließen den Datenträger an und es erscheint umgehend ein Dateimanager-Fenster, das den Inhalt anzeigt, oder ein Dialog, der Zugriffsoptionen anbietet. Unter der Haube muss jeder Datenträger in das Dateisystem eingehängt werden (Automount) – in der Regel unter „/media/[user]“. Die Datenträger erscheinen in der Navigationsspalte des Dateimanagers unter „Mein Rechner“ oder „Geräte“. Wenn eingebundene Laufwerke nach dem ersten Hotplug erneut benötigt werden, empfiehlt sich daher der Gang zum Dateimanager.

Statisch eingehängt ist nur die Systemfestplatte, die schon bei der Installation in die Datei „/etc/fstab“ eingetragen wird. Alle anderen Datenträger, interne wie externe, werden beim Klick auf das gewünschte Gerät eingehängt. Auf Desktopsystemen ist solches Verhalten in Ordnung, auf Servern, die interne und externe Laufwerke bereitstellen sollen, hingegen nicht. Hier ist es notwendig, alle diese Laufwerke manuell in die „fstab“ einzutragen. Die hierfür notwendigen Informationen sind die eindeutige UUID des Laufwerks, dessen Dateisystem (Ext4, NTFS …) und der Mountordner. UUID und Dateisystem liefert dieser Befehl:

```
lsblk -f
```

Ein Eintrag für die „fstab „sieht dann im Prinzip so aus

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

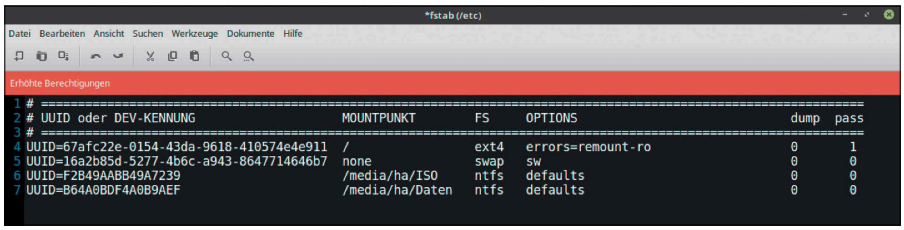
und in einem konkreten Beispiel etwa so:

```
UUID=BE43818F4A8138A3 /srv/data
 ext4 defaults 0 0
```

Die Festplatte mit dieser UUID wird dann beim Systemstart immer im Ordner „/srv/data“ bereitgestellt. Diemit Komma getrennten „Optionen“ enthalten im einfachsten Fall nur den Wert „defaults“, können aber auch komplex ausfallen (Fehlertoleranz, Dateirechte).

7. Das Tool „Laufwerke“ (Gnome-Disks)

Das Tool Gnome-Disks, auf deutschem System „Laufwerke“, ist der Standard unter Ubuntu und Linux Mint zur Datenträgerverwaltung. Links erscheint die Liste aller Datenträger, ein Klick auf einen Eintrag visua-



Sauber formatierte Datei „/etc/fstab“: Sorgen Sie in dieser Konfigurationsdatei mit Tabulatoren oder Leerzeichen für eine gut lesbare Tabellenform.

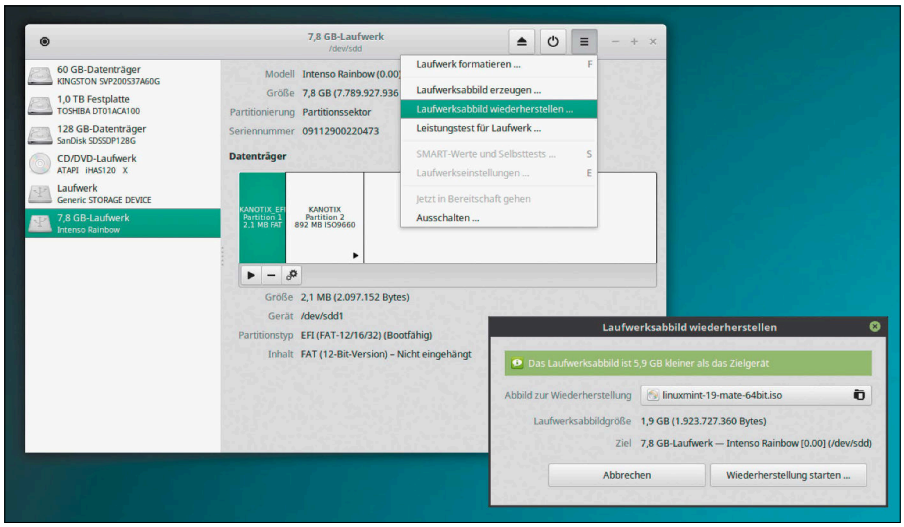
lisiert dessen Partitionierung, zeigt Gerätenamen („/dev/“...), Partitionsgrößen, Dateisystem und den Mountpunkt als Link, der auf Wunsch sofort den Dateimanager öffnet. Die Bearbeitungsmöglichkeiten sind gewöhnungsbedürftig, aber durchaus logisch aufgeteilt:

Laufwerksoptionen: Die Schaltflächen rechts oben bieten laufwerksbezogene Aufgaben. Ob nur eine, zwei oder drei Schaltflächen erscheinen, hängt vom markierten Laufwerkstyp ab. So lassen sich zum Beispiel interne Festplatten nicht aushängen oder abschalten, sodass in diesem Fall diese Schaltflächen fehlen.

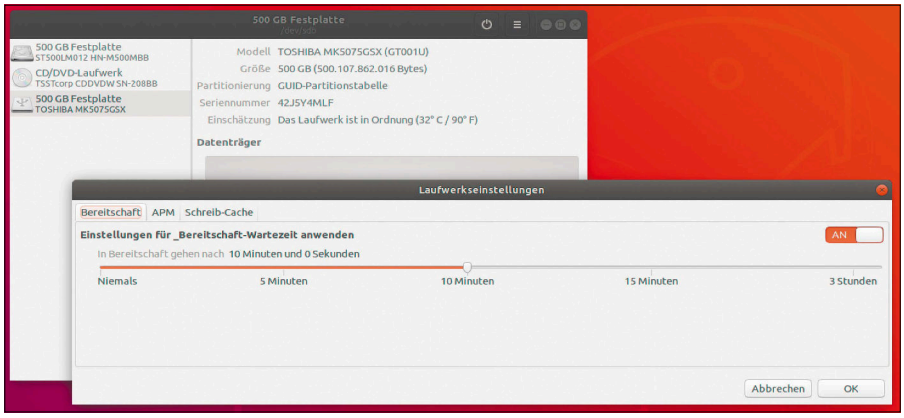
Immer vorhanden ist die Hauptschaltfläche mit den drei horizontalen Strichen („Hamburger-Menü“), die das Formatieren, das Arbeiten mit Images („Laufwerksabbild erzeugen/wiederherstellen“), ferner Tests und SMART-Analysen vorsieht. Die Option dieses Standardtools, Images vom markierten Datenträger in eine IMG-Datei zu schreiben („erzeugen“) oder eine IMG-Datei wieder zurück auf einen Datenträger („wiederherstellen“), machen manches andere Tool überflüssig.

Das „Hamburger-Menü“ ermöglicht über den Unterpunkt „Laufwerkseinstellungen“ auch einen Bereitschaftsmodus für Festplatten. Auf der Registerkarte „Bereitschaft“ setzen Sie den Schalter auf „An“ und stellen dann die Zeit ein, nach der sich die Festplatte abschalten soll. Die Zeitspanne reicht von „Niemals“ bis „3 Stunden“. Das funktioniert auch mit externen USB-Laufwerken. Zu empfehlen ist solches Abschalten nur bei reinen Datenplatten, wo Sie beim Zugriff eine kurze Anlaufzeit und damit eine Wartezeit von zwei, drei Sekunden tolerieren können.

Partitionsoptionen: Was Sie mit einzelnen Partitionen anstellen können, ist in den Schaltflächen unterhalb des Partitionsschemas untergebracht. Sie müssen erst das Rechteck der gewünschten Partition markieren und dann die gewünschte Schaltfläche anklicken. Sie können Partitionen aus- und einhängen, löschen (Minus-Schaltfläche), formatieren, Größen ändern, als Image sichern („Partitionsabbild erstellen“) oder ein Image auf die Partition zurückschreiben. Der Menüpunkt „Dateisystem bearbeiten“ vergibt ein Label für die Partition (Datenträgerbezeichnung), das eine hilfreiche Orientierung in den Mount-Verzeichnissen bietet.



Mächtiges Gnome-Disks („Laufwerke“): Das Standardtool beherrscht fast alle datenträgerrelevanten Aufgaben, unter anderem auch das Schreiben von Systemabbildern.



Datenfestplatten in den Ruhemodus schicken: Das Standardtool Gnome-Disks beherrscht auch diese Aufgabe.

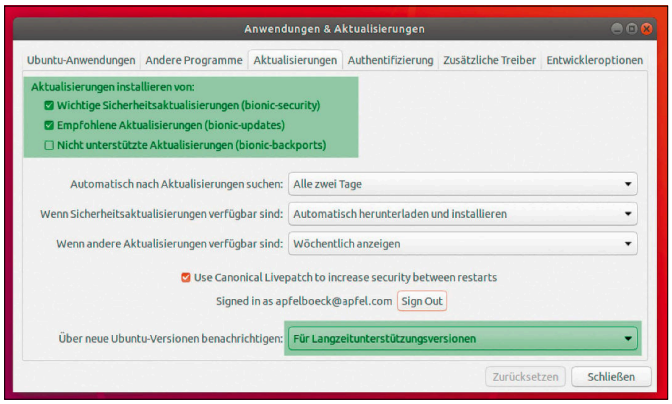
8. Software und Aktualisierung

In Ubuntu/Mint brauchen Sie drei verschiedene Werkzeuge für die Systemaktualisierung und die Softwareinstallation.

1. Unter „Anwendungspaketquellen“ sind die Paketquellen der Distribution einsehbar und erweiterbar. Solange Sie keine externen Quellen hinzufügen wollen, müssen Sie hier nichts ändern. Jedoch hat das Tool für jeden Nutzer eine wichtige Einstellung: Im Punkt „Ubuntu-Anwendungen“ oder „Offizielle Paketquellen“ (Mint) sind die Server eingestellt, woher Sie Updates und Programme beziehen. Der für Ihren Standort ideale „Spiegelserver“ lässt sich an dieser Stelle durch Klick und Warten auf den Übertragungstest eventuell optimieren.

2. Updates erledigt die „Aktualisierungsverwaltung“. Dieser Dienst läuft standardmäßig im Hintergrund und meldet über sein Symbol in der Systemleiste anstehende Updates. Klicken Sie dann einfach auf „Aktualisierungen installieren“, um die Updates anzuwenden. Ubuntu wie Mint können den Vorgang weiter vereinfachen: Linux Mint bietet in der „Aktualisierungsverwaltung“ unter „Bearbeiten → Einstellungen“ die vollautomatische Option „Automatisierung“. Unter Ubuntu stellen Sie unter „Anwendungen & Aktualisierungen“ nach Wunsch ein, welche Updates wie häufig gesucht werden sollen und ob diese automatisch installiert werden. Unentbehrlich ist die oberste Option „Wichtige Sicherheitsaktualisierungen“.

3. Für die Installation von Software ist das grafische Softwarecenter verantwortlich („Softwareverwaltung“ oder „Anwendungsverwaltung“ unter Mint). Das in Kategorien unterteilte Softwarecenter eignet sich zum Stöbern, repräsentiert aber nur eine Teilmenge aller verfügbaren Programme. Zum Deinstallieren gibt es in Ubuntu eine Übersicht der vorhandenen Software („Instal-



Vorgaben für automatische Updates: Die Ubuntu-Spezialität der Livepatches ist für Desktoprechner nicht relevant. Sie verschiebt nach Kernelpatches den fälligen Systemneustart (von Servern).

liert"), jeweils mit der Schaltfläche „Entfernen". Linux Mint hat keinen Filter für die installierte Software, signalisiert vorhandene Programme aber durch ein grünes Häkchen. Beachten Sie beim Entfernen stets Hinweise auf abhängige Pakete und stoppen Sie den Vorgang mit „Abbrechen", falls Pakete genannt werden, deren Relevanz Sie nicht beurteilen können.

Viele Nutzer werden die genannten grafischen Anlaufstellen dem Terminal vorziehen. Das Terminal bietet allerdings mit apt ein Tool, das sämtliche Aufgaben erledigt – *apt update* (Aktualisieren der Paketquellen), *apt upgrade* (Updates installieren), *apt install [Paket]* (Software installieren), *apt remove [Paket]* (Software löschen). Apt liefert außerdem, anders als die grafische Zentrale, sämtliche Software aus den Paketquellen.

Tipp: Eine komplette Liste aller installierten Softwarepakete liefert der folgende Terminalbefehl:

```
dpkg -l
```

Mit einem grep-Filter wie

```
dpkg -l | grep "office"
```

grenzen Sie die Liste auf Wunsch ein.

9. Die Systemeinstellungen

Die „Systemeinstellungen" in Ubuntu und Linux Mint sind größtenteils nicht so „systemnah", wie der Name suggeriert: Diese Zentrale bietet viele Optionen, die nur den angemeldeten Benutzer und dessen Desktop betreffen. Diejenigen Punkte der „Systemeinstellungen", die wirklich in die globale Systemverwaltung eingreifen, benötigen immer root-Recht. Die „Systemeinstellungen" in Linux Mint versammeln diese globalen Punkte unter der Überschrift „Systemverwaltung". Zu dieser Kategorie gehören unter anderem die Benutzerverwaltung („Benutzer und Gruppen"), die Desktopfirewall und die Treiberverwaltung.

Es gibt aber weitere Punkte, die gegebenenfalls systemweit greifen und dann root-Recht fordern: So ist etwa das Komplettieren der deutschen Sprachunterstützung unter „Region und Sprache" oder „Sprachen" (Linux Mint) ein globaler Systemeingriff, sobald Sprachpakete nachinstalliert werden müssen. Analog gilt das für das Einrichten von Geräten wie etwa einem Drucker: Wenn ein offener Treiber für den Drucker vorliegt und dieser für den Betrieb ausreicht, können Sie einen systemweit geltenden Drucker mit normalen Benutzerrechten anmelden, sobald aber ein zusätzlicher Herstellertreiber installiert werden soll, ist sudo-Recht erforderlich.

10. Die Taskverwaltung

Welche Programme laufen, wie viel Speicher belegt ist und wie es um die CPU-Auslastung bestellt ist, zeigt die „Systemüberwachung" (Gnome-System-Monitor). Ein Klick auf einen Spaltentitel in der Prozessliste sortiert die Prozesse nach Speicher- oder CPU-Bedarf und zeigt nach Rechtsklick auf den Spaltenkopf weitere Spalten (wichtig etwa „CPU-Zeit" oder „Befehlszeile").

Eine gute Alternative als Taskmanager ist htop im Terminal. Htop bietet einen vergleichbar präzisen Überblick und beherrscht den Abschuss von Tasks, die aus dem Ruder laufen (F9).

Die Autostarts: Bei der Anmeldung automatisch startende Programme gehören zum Repertoire jedes Desktopsystems. Zur Verwaltung dient in den „Systemeinstellungen" das Applet „Startprogramme". 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.

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.

CRONTAB: GENERELLES FORMAT

Minute	Stunde	Tag	Monat	Wochentag*	Kommando
0–59	0–23	1–31	1–12	0–6	Script | Programm
Crontab: 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=G3H3lM http://server.de/dl/my.php
0	09–18	*	*	*	wget --user=ha --password=G3H3lM 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 Cronjobs: Die crontab ist flexibler, als selbst erfahrene Linux-User wissen. Komplexere Zeitangaben sind allerdings eine Herausforderung.

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

```
sudo crontab -e
```

Jede Aufgabe erhält genau eine Zeile in der Crontab. Die ersten fünf Spalten 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.

11. Systemprotokolle für Fehlersuche

Systemprotokolle sind eine wichtige Informationsquelle, wenn System oder Software fehlerhaft arbeiten. Alle Protokolldateien sind unter „/var/log“ zu finden und liegen größtenteils als einfache Textdateien vor, die mit den üblichen Tools gelesen werden (gedit/xed oder cat/less/tail im Terminal). Eine gute Gesamtübersicht der wichtigsten Protokolle bietet unter Ubuntu wie Linux Mint das Standardprogramm „Protokolle“ (gnome-logs). Es fasst die Protokolldateien „auth.log“, „syslog“, „dpkg.log“, „Xorg.0.log“ in einem Fenster zusammen – chronologisch sortiert und außerdem filterbar nach Zeitraum und Prozessen.

- **auth.log** protokolliert die Systemanmeldungen.
- **syslog** ist das Systemlogbuch und zeigt Kernel-, Hardware- und Cron-Ereignisse.
- **dpkp.log** vermerkt alle manuellen (De-) installationen und automatischen Updates. Ergänzend und in mancher Hinsicht übersichtlicher ist ein Blick in die Datei „/var/log/apt/history.log“.
- **Xorg.0.log** liefert alle Meldungen des Anzeigeservers.

Eine besonders wichtige Info bei Hardwareproblemen sind die Kernel-Meldungen ab Systemstart, die das Tool dmesg chronologisch sammelt. Der Befehl



Mehr Spalten – mehr Infos: Die „Systemüberwachung“ (gnome-system-monitor) ist ein Taskmanager für höchste Ansprüche. Er kann alles und zeigt alles.

```
dmesg -T
```

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

12. Konfigurationsdateien im Griff

Die meisten Konfigurationsdateien mit globaler Geltung liegen im Pfad „/etc“. Folglich erfordert ihre Bearbeitung root-Recht. Die Dateien erscheinen dort als Einzeldatei wie etwa „/etc/fstab“ oder in einem Unterverzeichnis wie „/etc/samba/smb.conf“ (Samba-Konfiguration und Freigaben) oder „/etc/ssh/sshd_config“ (SSH-Server). Für die benutzerspezifische Konfiguration gibt es den Sammelordner unter „~/.config“ im Home-Verzeichnis.

Das übliche Zeichen für Kommentare ist die Raute „#“. Es ist dringend zu empfehlen, eigene Änderungen so zu kommentieren, dass sich diese Einträge von den Standardkommentaren unterscheiden – etwa so:

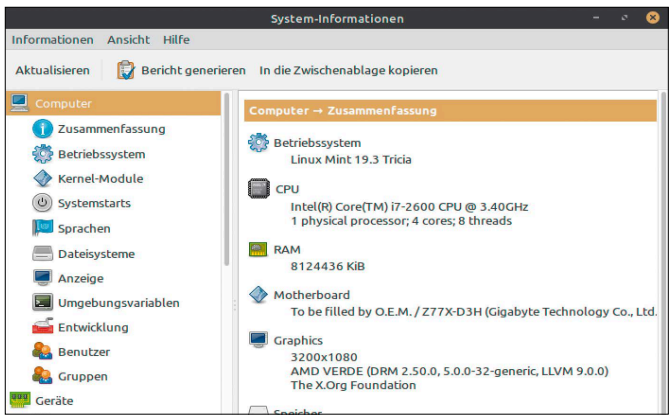
```
#sepp# SSH-Standardport 22
  geändert...
```

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

13. System- und Hardwareinfos

Was Ubuntu und Linux Mint unter „Systemeinstellungen → Informationen“ oder „Systeminformation“ (Mint) anzeigen, kommt über Gesamtspeicher, CPU, Architektur und die Angabe der Distribution nicht hinaus.

Wer ein grafisches Übersichtsprogramm vermisst, kann das Paket „hardinfo“ nachinstallieren. Eine puristische, aber sehr brauchbare Alternative für das Terminal ist das Tool inxi (Paket „inxi“). 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. ■



Standardkandidat zur Systemergänzung: Unter dem Paketnamen „hardinfo“ erhalten Sie ein ideales Desktoptool zur Recherche von System- und Hardwareeigenschaften.

Die 30 besten Systemtipps

Wenn Ubuntu oder Linux Mint auf halbwegs aktuelle Hardware trifft, sind diese Systeme bereits nach der Standardinstallation schnell und benutzbar. Mit den folgenden 30 Systemtipps gewinnen Sie aber Leistung, Kontrolle und Bedienkomfort hinzu.

VON HERMANN APFELBÖCK

Die folgenden 30 Systemtipps beziehen sich auf Standards und Standardprogramme unter Debian-basierten Distributionen und insbesondere Ubuntu und Linux Mint. Sie dürften aber im Prinzip auch für andere Distributionen gelten, wobei aber die praktische Umsetzung und Programmbezeichnungen abweichen können.

1. Der Zustand von Festplatten (SMART)

Moderne Festplatten folgen dem SMART-Standard (Self Monitoring, Analysis and Reporting Technology) und können Auskunft über ihren Gesundheitszustand geben. Die einschlägigen grafischen Werkzeuge Gnome-Disks („Laufwerke“) und der KDE-Partitionmanager zeigen die SMART-Werte interner Festplatten an. Das KDE-Tool äußert sich unter „Gerät → Status“ recht knapp, jedoch ist eine positive „Gesamtbewertung: Healthy“ sowie die Angabe der fehlerhaften Sektoren im Prinzip ausreichend. Gnome-Disks sollte hinter „Allgemeine Einschätzung“ die Aussage zeigen: „Das Laufwerk ist in Ordnung“. Bei SSDs steht hinter „wear-leveling-count“ in der Spalte „Normalisiert“ ein wichtiger Wert: Neue SSDs starten bei „100“ und der Wert reduziert sich mit der Zeit. Nähert er sich der „0“, müssen Sie das Laufwerk umgehend ersetzen.

Per USB angeschlossene Festplatten berücksichtigt das KDE-Tool ebenfalls, Gnome-Disks allerdings nicht. Hier benötigen Sie das Paket „smartmontools“ (*sudo apt install smartmontools*) und dann folgenden Terminalbefehl:

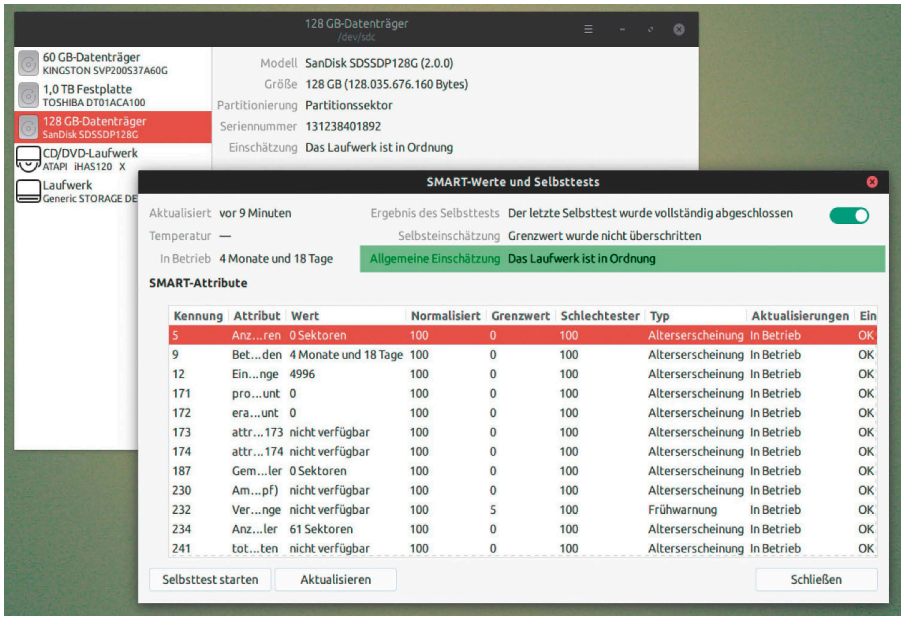
```
sudo smartctl -H /dev/sd[x]
```

Wenn der Health-Test mit „PASSED“ beantwortet wird, ist die Tauglichkeit des Laufwerks schon erwiesen. Weitere Details gibt es nach der Eingabe von

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

und noch ausführlicher mit dem Parameter „-a“. Ein wichtiger Wert ist „ Reallocated_Sectors_Ct“, der die Zahl defekter Sektoren anzeigt und im Optimalfall eine „0“ bieten sollte.

Gleiches gilt für „Spin_Retry_Count“, weil die hier gezählten gescheiterten Anlaufversuche auf mechanische Mängel deuten. Messwerte wie Seek- und Read Errors sind kaum relevant.



Diese SSD ist neuwertig und darf weitermachen: Gnome-Disks und die KDE-Partitionsverwaltung lesen die SMART-Werte von Datenträgern aus.

2. Der Zustand des Notebookakkus

Der Akku ist Verschleißteil Nummer eins im Notebook. Wie es um die Komponente steht, können viele Linux-Desktops recht detailliert mit dem Tool „Energiestatistiken“ ermitteln (gnome-power-statistics, mate-power-statistics etc.). Meist führt das unscheinbare Applet in der Systemleiste direkt zu diesem Tool. Neben irrelevanten Infos zeigt „Laptop-Akku → Details“ die Werte „Energie (Design/Entwurf)“ und „Energie wenn vollständig geladen“. Der erste ist ein idealer Referenzwert, der zweite zeigt die reale Akku-Ladekapazität. Ist die Differenz gravierend, sollten Sie den Nachkauf eines neuen Akkus erwägen.

Falls ein Desktop das grafische Statistiktool nicht mitbringt, lassen sich diese Werte auch auf der Kommandozeile mit

```
upower --monitor-detail
```

erfragen. Upower ist meistens Standard oder mit gleichnamigem Paketnamen schnell nachinstalliert.

3. Swapdatei komplett abschalten

Die Beobachtung der RAM-Auslastung im Taskmanager zeigt auf neuerer Hardware (und auch auf älterer Hardware mit einem dafür angemessenen Linux) praktisch immer, dass keine RAM-Auslagerung auf Festplatte stattfindet. Bei Rechnern mit acht oder 16 GB ist das Dauerzustand. Folglich können Sie dort die Swapdatei komplett abschalten. Das ist mit wenigen Handgriffen erledigt: Im laufenden System beenden diese beiden Terminalbefehle

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

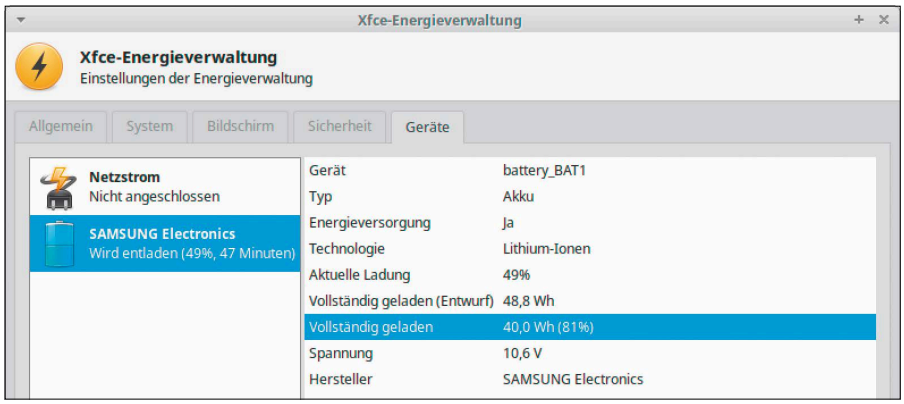
die Auslagerung und löschen die Auslagerungsdatei. Zuletzt deaktivieren Sie in der Datei „/etc/fstab“ die Zeile

```
/swapfile …
```

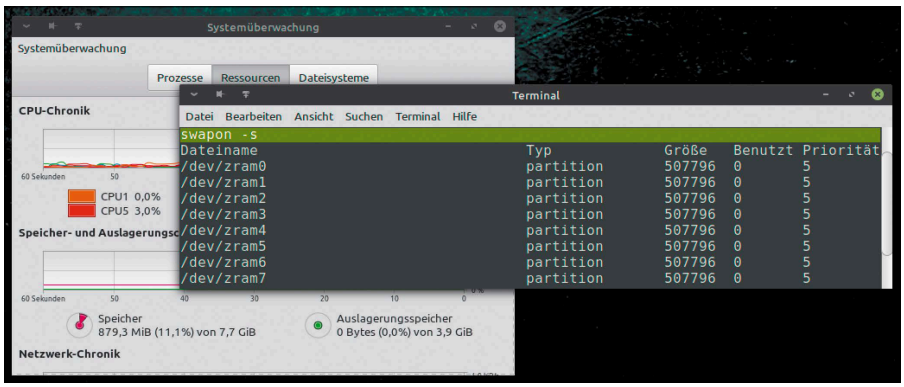
durch das Kommentarzeichen „#“.
Beachten Sie, dass der Ruhezustand „Bereitschaft“ (Suspend to RAM) weiterhin funktioniert. „Hibernation“ (Suspend to Disk) ist derzeit in den aktuellen Ubuntu-Varianten ohnehin nicht mehr vorgesehen, seit Ubuntu von der Swappartition auf die Swapdatei umgestellt hat.

4. Komprimierte Auslagerung mit Zram

Zram ist eine interessante Alternative zur Auslagerung auf Festplatte. Das Kernel-



Zustand des Akkus ermitteln: Die Energistatistiken zeigen den Referenzwert „Energie (Design)“ oder „Energie (Entwurf)“, der von „vollständiger Ladung“ nicht zu weit abweichen sollte.



Zram reserviert je nach RAM und CPU erhebliche Speicheranteile. Wie Sie im Bild sehen (0 Bytes von 3,9 GB), wird aber kein RAM abgezweigt, solange dies nicht erforderlich ist.

Modul reserviert einen Teil des Arbeitsspeichers, um dort mehrere RAM-Disks anzulegen, die als komprimierter Auslagerungsspeicher bei Engpässen dienen. In den Standardeinstellungen reserviert Zram die Hälfte des verfügbaren Arbeitsspeichers, teilt diesen durch die Anzahl der verfügbaren CPU-Kerne und richtet pro Kern ein Blockgerät ein. Bei einer CPU mit vier Kernen, entstehen vier Swapgeräte mit der Bezeichnung „/dev/zram0“, /“dev/zram1“ etc. Der Speicher wird aber dynamisch vergeben: Solange nichts auszulagern ist, nimmt Zram nichts in Anspruch. Erst wenn Auslagerung benötigt wird, geht RAM nach Bedarf vom physikalisch vorhandenen RAM

POWERTIPP 1: STANDBY-MODUS FÜR DATENLAUFWERKE

Bei Laufwerken, die nur Daten enthalten, können Sie Stromverbrauch und Lebensdauer durch Standby-Abschaltung deutlich verbessern. Für interne Datenfestplatten kann das Systemtool Gnome-Disks („Laufwerke“) über „Laufwerkseinstellungen → Bereitschaft“ den Timer für den Ruhezustand festlegen. Dort gibt es einen Schieberegler, ab welcher Frist der Inaktivität das Gerät in den Standby-Modus geschaltet werden soll.
Bei USB-Festplatten kommt man nur manuell mit dem Tool hdparm ans Ziel. Ermitteln Sie im Terminal zunächst mit

```
blkid
```

die Laufwerke, Bezeichnungen und UUID-Kennungen. Ist die gewünschte Festplatte beispielsweise „/dev/sdb“, dann aktivieren Sie mit folgendem Befehl den Ruhezustand:

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

Wenn das prinzipiell funktioniert, können Sie eine automatische Abschaltung festlegen:

```
sudo hdparm -S 180 /dev/sdb
```

Der Wert hinter „-S“ steht für „180 x 5 Sekunden“, also 15 Minuten. Diese Konfiguration wirkt allerdings nur bis zum nächsten Neustart des Systems. Für eine dauerhafte Änderung bearbeiten Sie die „hdparm“-Konfigurationsdatei:

```
sudo gedit /etc/hdparm.conf
```

Fügen Sie im Editor folgende Zeile am Ende der Datei an:

```
/dev/disk/by-uuid/[UUID] { spindown_time = 180 }
```

Den Platzhalter [UUID] ersetzen Sie – ohne die Klammern – durch die zuvor mit blkid ermittelte UUID.

ab. Zram befindet sich in den Paketquellen von Ubuntu und lässt sich mit minimalen Aufwand einrichten:

```
sudo apt install zram-config
```

Damit ist das Modul sofort aktiv, wie Sie mit

```
swapon -s
```

leicht kontrollieren können.

Wir empfehlen Zram als Ersatz für die Auslagerungsdatei auf Rechnern mit guter RAM-Ausstattung. Zram soll aber auch auf Rechnern mit geringem Speicher (Raspberry & Co.) Vorteile bringen, da die Auslagerung ins RAM wesentlich schneller ist und effiziente Komprimierung für minimalen Verbrauch sorgt. Zram lässt sich durch Deinstallieren von zram-config wieder abschalten.

5. Auslagerungsaktivität anpassen (Swappiness)

Wer die Auslagerung nicht abschalten möchte, kann über den „Swappiness"-Wert das Verhalten steuern. Der Wert darf zwischen zehn und 100 liegen. Je höher der Wert, desto aktiver schreibt der Kernel Speicherseiten aus dem RAM in die Swapdatei. Der voreingestellte Standard liegt bei 60.

Ein niedriger Wert kann bei guter RAM-Ausstattung, aber langsamer mechanischer Platte vorteilhaft sein. Umgekehrt kann ein hoher Wert die Systemleistung bei wenig RAM verbessern, sofern die Swapdatei auf einer schnellen SSD liegt. Mit diesem Befehl

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

ändern Sie den Wert temporär. Um einen Wert dauerhaft festzulegen, müssen Sie folgende Konfigurationsdatei bearbeiten:

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

Suchen Sie in der Datei nach „vm.swappiness" und ändern Sie den Wert:

```
vm.swappiness=90
```

Falls die betreffende Zeile fehlt, fügen Sie sie am Ende der Datei hinzu:

6. Einfacheres Systempasswort

Wer über sudo das System verwaltet, muss sein Systempasswort sehr häufig eingeben. Komplexe und lange Kennwörter sind eher lästig – und auf einem Desktopsystem auch nicht notwendig. Abgesehen vom Erstbenutzer, der bei der Installation eingerichtet wird, haben Ubuntu & Co. allerdings erhöhte Komplexitätsanforderungen an das Passwort für alle weiteren Konten. Das gilt auch bei Passwortänderungen für das Erstbenutzerkonto.

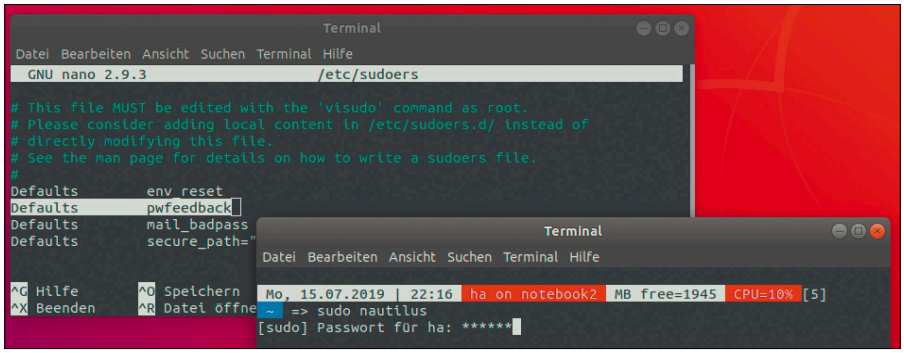
Wie immer unter Linux gibt es eine Stelle, um auch die Standards zu steuern: Öffnen Sie die folgende Datei

```
sudo nano /etc/pam.d/common-
 password
```

mit root-Recht, so finden Sie in der ersten „password"-Zeile die Anweisung „obscure". Das erzwingt eine Mindestkomplexität des Passworts (Sonderzeichen) und kann einfach gelöscht werden. Durch die Ergänzung „minlen=6" (Beispiel) am Ende derselben Zeile können Sie außerdem die Mindestlänge auf den gewünschten Wert herabsetzen.

7. Sudo-Passworteingabe mit Kontrolle

Standardmäßig schreibt man im Terminal das sudo-Kennwort ohne Rückmeldung im



Das Tool sudo nach der Konfigurationsänderung: Sternchen bei der Passworteingabe dienen als Rückmeldung der bereits getätigten Tastatureingaben.

POWERTIPP 2: RAMDISK ALS ZWISCHENDEPOT

16 GB RAM sind auf heutigen Notebooks keine Ausnahme mehr. Für den typischen Einsatz mit Office und Mediaplayer ist solche Ausstattung purer Luxus, mit dem sich aber Sinnvolles anfangen lässt. Wenn Sie einen zentralen Ordner, über den Sie den ganzen Datenaustausch inklusive Downloads abwickeln, in eine schnelle Ramdisk verlegen, entstehen mehrere Vorteile: mehr Leistung, automatische Entsorgung beim Herunterfahren, Schonung von SSD/Festplatte, Nutzung der brachliegenden RAM-Ressourcen.

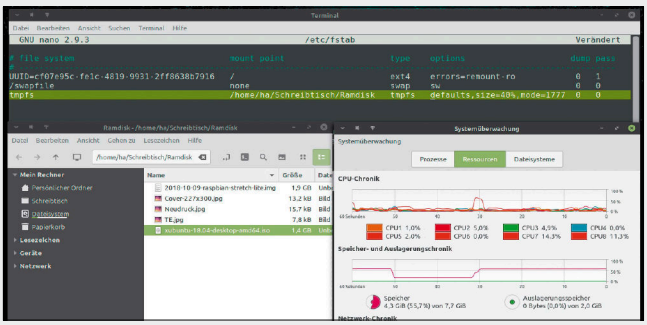
Eine Ramdisk ist über die Datei „fstab" schnell erstellt:

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

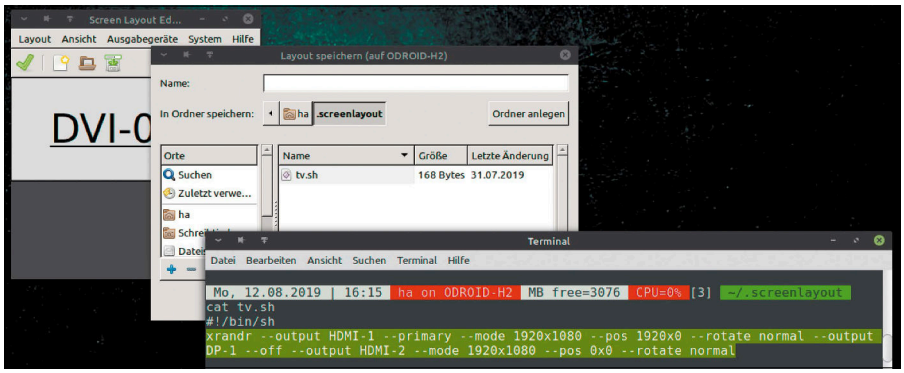
Hier fügen Sie die weitere Zeile

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

hinzu (der Mountpfad des Beispiels muss angepasst werden). Nach dem Speichern starten Sie Linux neu. Die angegebene Kapazität (hier 40 Prozent des Speichers) wird nicht statisch abgezweigt. Bleibt der Mountpunkt ungenutzt, verbraucht die Ramdisk auch keinen Speicher, wovon Sie sich mit einem Taskmanager wie etwa dem Gnome-System-Monitor leicht überzeugen können. Der Umgang mit Ramdisk-Daten erfordert etwas Disziplin und Gewöhnung, weil die Daten beim Shutdown gelöscht werden.



Ein Tipp für brachliegendes RAM: Die in der „fstab" eingetragene Ramdisk dient hier als temporäres Datendepot in einem Desktopordner.



Multimonitor-Layout mit xrandr-Script: Den komplexen Befehl kann das grafische xrandr als Shell-Script ablegen, das dann als Autostart dauerhaft für das gewünschte Layout sorgt.

Blindflug – eine auf Desktopsystemen eher paranoide Sicherheitseinstellung, um die Länge des Passworts zu verbergen. Es ist aber kein Problem, sich die bereits getippten Buchstaben mit Stellvertreterzeichen „*“ anzeigen zu lassen. Der Aufruf

```
sudo visudo
```

öffnet die Datei „/etc/sudoers“ im voreingestellten Editor. Unter

```
Defaults env_reset
```

fügen Sie die zusätzliche Zeile

```
Defaults pwfeedback
```

ein. Nach dem Speichern (Strg-O) und Beenden des Editors (Strg-X) zeigt die sudo-Abfrage ein Sternchen pro eingegebenem Zeichen. Unter Linux Mint ist dies inzwischen bereits Standard.

8. Deutsche Systemanmeldung

Wer für sein Systempasswort keine Sonderzeichen benutzt, wird das Problem gar nicht bemerken: Es gibt Fälle, wo zwar das komplette System auf Deutsch eingestellt ist, der Anmeldebildschirm jedoch englisches Tastaturlayout benutzt. Das führt dann bei Zeichen wie „z“, „y“, „ß“, „-“, „=“ zu Anmeldeproblemen. Lösung ist der Eingriff in die Datei „/etc/default/keyboard“. Die Datei enthält nur wenige Zeilen, die maßgebliche sollte

```
XKBLAYOUT="de"
```

lauten.

9. Multimonitorbetrieb mit Xrandr-Autostart

Bei Multimonitorbetrieb lässt sich über die Systemeinstellungen die Konfiguration und Position der Bildschirme exakt festlegen. Es gibt aber Fälle, wo Systeme diese Einstellung nicht permanent speichern und die Einrichtung bei jedem Start erneut erfolgen müsste – und das wäre unzumutbar.

Unter der Haube nutzen die grafischen Werkzeuge das Tool xrandr, daher kann der passende xrandr-Befehl als Autostart das Problem lösen. Und noch besser: Die Syntax der komplexen xrandr-Kommandos müssen Sie nicht selbst ermitteln. Das kann Ihnen das grafische Tool arandr abnehmen (*sudo apt install arandr*). Damit arrangieren Sie die Bildschirme mit der Maus nach Wunsch und gehen dann auf „Layout → Speichern unter“. Das auf diesem Weg gespeicherte Shell-Script legen Sie dann als zusätzlichen Eintrag unter „Startprogramme“ ab.

10. Schriftgrößen optimieren (DPI)

Bei Standardeinstellungen ist die Bildschirmdarstellung je nach Monitorgröße und Auflösung nicht immer optimal. Viele Programme haben eigene Zoomfunktionen, aber es gibt auch systemweite Methoden. Die Auflösung herabzusetzen ist möglich, geht aber immer mit Qualitätsverlust einher. Bessere Ergebnisse erzielt eine Anpassung der Schriften.

• Der Gnome-Desktop kann über das Tool Gnome-Tweaks die Schriftgrößen stufenlos skalieren. Die Einstellung lautet dort „Schriften → Skalierungsfaktor“.

• Cinnamon unter Linux Mint zeigt in den normalen Systemeinstellungen unter „Schriften“ die allgemeine Option „Skalierungsfaktor der Schrift“. Sie können an gleicher Stelle aber auch die Schrittgrößen für einzelne Objekte im Detail anpassen.

POWERTIPP 3: RECHNER ABSCHALTEN UND AUFWECKEN

Wenn ein PC oder Server zwischen 22:00 Uhr abends und 8:00 Uhr morgens garantiert nicht gebraucht wird, liegt es nahe, ihn für diese zehn Stunden abzuschalten. Das spart Strom und verlängert die Lebenszeit der Hardwarekomponenten. Das Tool Rtcwake, Bestandteil des meist vorinstallierten Standardpakets „util-linux“, kann Rechner sowohl abschalten wie zeitgesteuert wieder einschalten. Im einfachsten Fall sieht ein Kommando so aus:

```
sudo rtcwake -m off -s 300
```

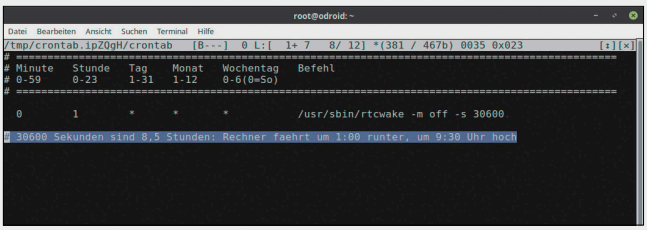
Der Befehl ist gut geeignet, um zu testen, ob die Hardware prinzipiell mitspielt. Der Schalter „-m“ bestimmt den Abschaltmodus „standby“, „mem“, „disk“, „off“ oder „no“. Das im Beispiel gewählte „off“ fährt das System komplett herunter und Parameter „-s“ gibt in Sekunden an, wann der Rechner wieder starten soll. Um rtcwake als Cronjob abzulegen, muss der Befehl in der Crontab von root untergebracht werden:

```
sudo crontab -e -u root
```

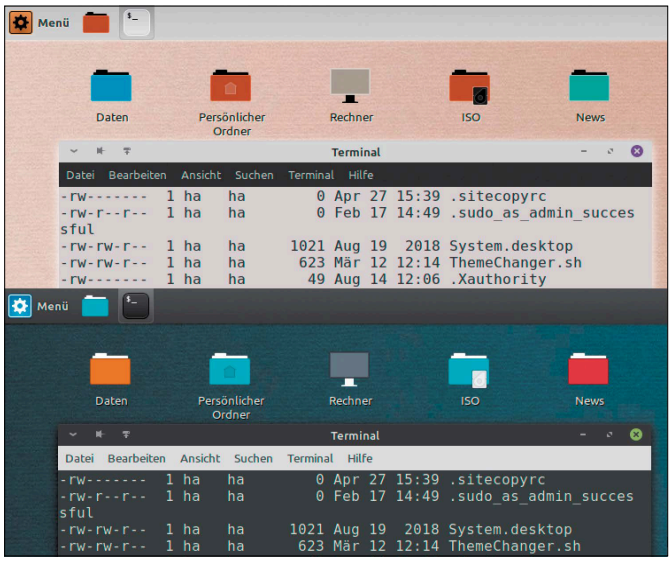
Folgender Cronjob

```
0       22      *       *       *       /usr/sbin/
 rtcwake -m off -s 36000
```

schaltet den Rechner um 22:00 Uhr ab und startet ihn wieder nach 36 000 Sekunden um 8:00 Uhr.



Ein Cronjob für Rtcwake: Dieser Rechner wird um 1:00 Uhr beendet und hat ab 9:30 Uhr wieder Dienst.



Einfache Farbumstellung mit Xcalib: Das hilft bei ungünstigen Lichtverhältnissen und funktioniert auf jedem Linux.

• KDE zeigt in den Systemeinstellungen unter „Schriftarten“ den Punkt „DPI für Schriften erzwingen“ und daneben das Eingabefeld für den gewünschten Wert.
• Der Budgie-Desktop skaliert in den „Budgie Desktop Einstellungen“ unter dem Punkt „Schriftarten“.
• LXQT zeigt den maßgeblichen Punkt unter „Erscheinungsbild → Schriften“.
• Bei Mate gehen Sie in den Systemeinstellungen auf „Erscheinungsbild → Schriften“ und auf „Details“. Ganz oben lässt sich der DPI-Wert exakt einstellen, sofern Sie vorher die automatische Erkennung abschalten.
• Unter XFCE finden Sie in den Systemeinstellungen den Punkt „Einstellungsbearbeitung“. Hier geht es ganz nach unten zur Kategorie „xsettings“. Im Wertefenster finden Sie dann erneut ganz unten den Eintrag „Xft“ mit dem Unterpunkt „DPI“. Den aktuellen Wert können Sie hier durch einen eigenen ersetzen.

11. Bildschirmfarben invertieren

Bei sehr ungünstigen (hellen) Lichtverhältnissen wird Text besser lesbar, wenn die typischen Farbverhältnisse (dunkel auf hell) umgekehrt werden. Ad hoc und auf Webseiten mit miserablen Kontrasten kann es genügen, mit Strg-A alles zu markieren und damit die Farbverhältnisse umzuschalten. Ein praktisches Tool, das den kompletten Desktop invertieren kann, ist das Programm Xcalib. Xcalib ist unter Ubuntu und Mint mit

```
sudo apt install xcalib
```

schnell nachinstalliert. Zum Invertieren der Bildschirmfarben genügt dann dieser Befehl („-i“ für „inverse“, „-a“ für „alter“):

```
xcalib -i -a
```

Mit demselben Befehl kehren Sie wieder auf die normale Einstellung zurück. Wirklich elegant wird dieses Tool, wenn Sie ihm unter „Einstellungen → Tastatur → Tastaturkürzel“ noch einen einprägsamen Hotkey spendieren.
Theoretisch lassen sich ähnliche Bildschirmoptimierungen durch einen Wechsel zu einem „HighContrast“-Theme erzielen. Xcalib hat aber den enormen Vorzug, auf jedem Desktop und ohne Recherche der verfügbaren Themen zu funktionieren.

12. Shutdown mit Zeitangabe

Nicht selten ergibt sich die Situation, dass man bei Arbeitsende das System beenden möchte, aber nicht beenden kann, weil ein Kopiervorgang oder ein Download noch einige Zeit läuft. Abzuwarten wäre lästig und auch unnötig, denn das Shutdown-Kommando beherrscht sowohl Uhrzeiten als auch Fristen:

```
sudo shutdown -P 23:00
sudo shutdown -P 60
```

Der erste Befehl beendet das System exakt um 23:00 Uhr, der zweite nach 60 Minuten. Das sudo-Kennwort wird sofort abgefragt, sodass Sie anschließend den Rechner verlassen können.

13. Maßnahme gegen Desktophänger

Die Reparaturmethoden der Linux-Desktops bei hängender Oberfläche sind nicht einheitlich.
Die Hotkeys Strg-Alt-Esc und Strg-Alt-Rücktaste sind relativ verbreitet, aber keineswegs überall gültig. Folgender Trick sollte auf den meisten Distributionen funktionieren, indem er den Display-Manager neu startet (sudo-Recht ist erforderlich). Der jeweils verwendete Display-Manager lässt sich wiederum vorher aus einer Konfigurationsdatei ermitteln:

```
dm=$(basename "$(cat /etc/X11/
  default-display-manager)")
sudo service $dm restart
```

Als knappes Alias „redesk“ ersparen Sie sich den Tippaufwand:

POWERTIPP 4: GRAFISCHE OBERFLÄCHE AUS- UND EINSCHALTEN

Die Linux-Option, die grafische Oberfläche einfach aus- und (bei Bedarf) wieder einzuschalten, ist vor allem für Platinenrechner interessant. Besonders wichtig wird dieser Trick bei Mini-PCs mit geringer Systemauswahl – wenn beispielsweise nur ein Ubuntu Mate zur Verfügung steht, dessen Desktop aber praktisch nicht benötigt wird. Typisch ist aber auch, dass die Oberfläche zur Einrichtung willkommen ist, danach aber nicht mehr. Wenn Sie nur noch die Serverdienste brauchen (Samba, SSH, Apache), dann lässt sich auf allen Ubuntu-basierten Systemen die Oberfläche mit

```
sudo systemctl set-default multi-user.target
```

abschalten. Die Maßnahme gilt ab dem nächsten Neustart. Je nach verwendeter Oberfläche werden dadurch einige Hundert MB RAM sowie CPU-Ressourcen frei. Mittels des Kommandos

```
sudo systemctl set-default graphical.target
```

ist der Desktop bei Bedarf auch wieder dauerhaft einzuschalten. Die abgeschaltete Oberfläche können Sie auf der Konsole außerdem jederzeit manuell mit

```
startx
```

starten.

```
alias redesk='DM=$(basename "$(cat
 /etc/X11/default-display-
 manager)");sudo service $DM
 restart'
```

Nach dieser Aktion erscheint der Anmeldebildschirm für eine neue Desktopsitzung. Die Methode funktioniert auch in einer virtuellen Konsole (Strg-Alt-F1), falls die grafische Oberfläche nicht mehr reagiert.

14. Fensterkiller Xkill optimal nutzen

Xkill ist praktisch überall vorinstalliert. Es beendet grafische Programme, deren Fenster nicht mehr reagieren, ohne dass Sie Programmname, Fenstername oder PID kennen müssen. Beim Aufruf von xkill verwandelt sich der Mauszeiger in ein Kreuz, mit dem Sie das Programm mit linker Maustaste anklicken und damit beenden. Die rechte Maustaste beendet xkill ohne Aktion.

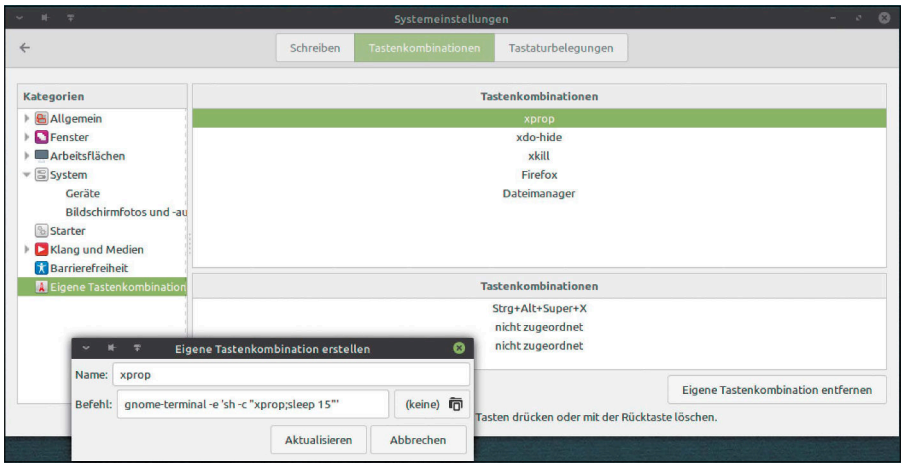
Mit dem lästigen manuellen Terminalaufruf *xkill* ist das Tool aber kaum die Hälfte wert. Einige Distributionen verwenden den Hotkey Strg-Alt-Esc, doch meistens ist kein globaler Hotkey eingestellt. Das sollten Sie unter „Systemeinstellungen → Tastatur → Tastaturkürzel“ ändern (oder ähnlich lautend), indem Sie xkill unter „Eigene Tastaturkürzel“ eintragen und dem Programm durch Drücken der Tastenkombination Strg-Alt-Esc, Strg-Alt-K oder wie gewünscht zuweisen.

15. Programminfo Xprop optimal nutzen

Für xprop gilt Ähnliches wie für xkill. Es ist überall Standard, benötigt aber einen manuellen Aufruf im Terminal. Das häufigste Motiv, xprop zu verwenden, ist die Frage nach dem Programmnamen eines Fensters. Also etwa die Frage: Wie lautet der Name des Dateimanagers, den ich gerade benutze? Nach dem Start von xprop verwandelt sich der Mauszeiger in ein Kreuz, mit dem Sie auf das gewünschte Fenster klicken. Im Terminal erscheint dann der zugehörige Programmname. Wer xprop oft benutzt, sollte sich einen Hotkey zurechtlegen.

Da für die Infoausgabe ein Terminal benötigt wird, ist der Befehl für den xprop-Hotkey schwieriger als bei xkill. Folgende Variante funktioniert auf Ubuntu und Linux Mint mit Gnome-Terminal:

```
gnome-terminal -e 'sh -c
 "xprop;sleep 10"'
```



Cleverer Hotkey: Zum Abfragen von xprop-Infos genügt die eingestellte Tastenkombination. Das Terminal zur Ausgabe der xprop-Infos startet gleich mit.

Die Anzeigedauer der xprop-Information, hier zehn Sekunden, ist beliebig einstellbar.

16. Wartezeit des Grub-Bootloaders

In Dual- oder Multiboot-Umgebungen wartet der Grub-Bootloader standardmäßig zehn Sekunden auf eine Auswahl, 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 dem Kommando

```
sudo update-grub
```

die Bootumgebung neu zu initialisieren.

17. Der Programmturbo Preload

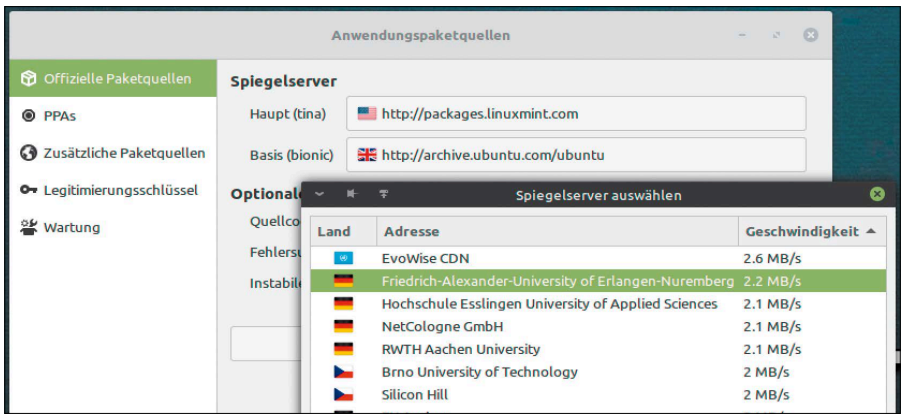
Das Tool Preload beschleunigt häufig oder über „Startprogramme“ immer gestartete Anwendungen. Der einfache Dienst protokolliert Ihre Programmvorlieben und lädt die Favoriten vorab in den Arbeitsspeicher. Der eigentliche Programmstart verläuft dadurch deutlich schneller. Preload ist in den Paketquellen verfügbar und in Ubuntu und Co. mit

```
sudo apt install preload
```

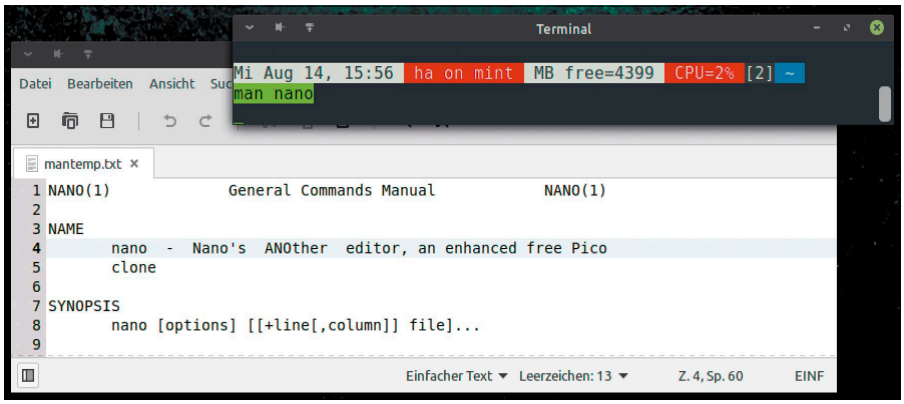
schnell nachinstalliert. Theoretisch können Sie in die Konfiguration des einfachen Tools manuell eingreifen („/etc/preload.conf“), dies ist jedoch weder erforderlich noch inhaltlich ergiebig.

18. Schnellen Spiegelserver einstellen

Für Installationen und Updates benötigen Sie einen Server, der die Paketquellen bereitstellt und möglichst schnell ausliefern soll. Je schneller Ihre Internetverbindung ist, desto mehr profitieren Sie von einem schnellen Spiegelserver. Ubuntu und Linux Mint können den geeignetsten deutschen Server selbst ermitteln: Dazu gehen Sie in



Lokaler und schneller Server für Updates und Installationen: Ubuntu und Linux Mint zeigen durch Schnelltests die geeignetsten Kandidaten für den Softwarebezug.



Man-Hilfeseiten in den grafischen Editor umleiten: Das vereinfacht Navigation und Suche in den unbeliebten, aber unvermeidlichen Manpages.

Ubuntu auf „Anwendungen & Aktualisierungen“, in Linux Mint zu den „Anwendungspaketquellen““. Dort finden Sie den aktuell eingestellten Spiegelserver. Diesen können Sie anklicken und erhalten unter Linux Mint direkt eine Liste der schnellsten Server, unter Ubuntu gehen Sie auf „Andere“, wonach Sie im Unterfenster die Option „Besten Server auswählen“ antreffen. Auch Ubuntu macht dann einige Verbindungstests und schlägt dann einen Server vor. Für Deutschland immer eine gute Wahl ist *netcologne.de*, das Sie auch direkt manuell auswählen können.

19. Bash-History mit Schlüsselwörtern

Ein einfacher Trick, um interessante Terminalbefehle bei Bedarf schnell wiederzufinden, besteht in der Kommentierung der Kommandos durch Schlüsselwörter.
Ein Beispiel:

```
lsblk -o name,fstype,uuid,size,typ
 e,mountpoint,label # Festplatte
 Disk
```

Der so eingegebene Befehl funktioniert wie gewohnt; alles ab dem Kommentarzeichen „#“ wird ignoriert. Der Befehl landet aber inklusive Kommentar in der Datei „~/.bash_history“. Folglich können Sie später in der Historysuche (Strg-R) ein Schlüsselwort wie „Festplatte“ eingeben und die Suche wird Ihnen die Befehle mit diesem Kommentar anbieten.

20. Besser lesbare Manpages

Manpages sind eine doppelte Zumutung: erstens inhaltlich, weil sie niemals anschauliche Beispiele enthalten, zweitens technisch aufgrund des antiken Standardviewers. Immerhin dieser zweite Mangel lässt sich ohne großen Aufwand beheben, indem Sie den Text an den Editor Ihrer Wahl schicken (hier gedit):

```
function man ()
{
/usr/bin/man $* > ~/mantemp.txt
 if [ -s ~/mantemp.txt ]; then
  gedit ~/mantemp.txt & disown
 fi
}
```

Wenn Sie diese Funktion in die Datei „~/.bashrc“ eintragen, erhalten Sie angeforderte Hilfeseiten künftig im grafischen Editor angezeigt.

21. Reduzieren von Systemmüll

Die Paketverwaltung von Debian, Ubuntu, Mint speichert die heruntergeladenen Pakete bei Installation und Aktualisierung in einem Zwischenspeicher unter „/var/cache/apt/archives“. Diesen Cache, der über Monate und Jahre erheblich anwachsen kann, leeren Sie mit

```
sudo apt-get clean
```

am besten regelmäßig.
Eine weitere Halde von Systemdaten kann sich durch deinstallierte Software ergeben, deren abhängigen Pakete weiter auf dem System verbleiben. Der Befehl

```
sudo apt-get autoclean
```

kann solche Pakete ermitteln und löschen.
Das Dateisystem Ext4 reserviert auf jeder Partition einen Speicherbereich für das Konto root. Das soll gewährleisten, dass sich root auch auf voller Systempartition noch anmelden kann. Aus historischen Gründen liegt der reservierte Platz bei fünf Prozent, das sind bei einer 240-GB-SSD immerhin 12 GB. Die Reserve können Sie mit dem Tool tune2fs gefahrlos verringern:

```
sudo tune2fs -m 3 /dev/sda1
```

Dies verringert die Anzahl der reservierten Blöcke auf „/dev/sda1“ auf drei Prozent.

22. Benutzerdateien komprimieren

Für effiziente Komprimierung ist Tar 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
```

Das Beispiel geht davon aus, dass sich tar im richtigen Verzeichnis befindet.
Die Nutzung gepackter „tar.gz“-Archive ist unter Ubuntu und Mint mit dem Archivmanager praktisch genauso komfortabel wie der Umgang mit unkomprimierten Daten im Dateimanager. Es ist also nicht nötig, die Daten für jede Nutzung auszupacken.

23. Samba versus SSH

Aufräumarbeiten beim Dateibestand von Linux-Servern lassen sich auf Netzfreigaben über Samba erledigen. Der effiziente Weg ist das aber definitiv nicht, vor allem wenn diese Arbeiten viele Löschaktionen beinhalten.
Verschieben, Löschen, Aufräumen ist über das SSH-Terminal und damit direkt am Server weitaus schneller als mit der Vermittlung über Samba. Aufräumen sollten Sie daher immer mit dem SSH-Terminal – und hier am bequemsten mit dem Midnight Commander!

24. Hostname (Rechnername) ändern

Bei der Installation eines Desktopsystems bestimmen Sie den Hostnamen des künftigen Systems selbst. Bei den komplett ausgelieferten Systemimages für Platinenrechner ist der Hostname hingegen vorgegeben und wenig aussagekräftig („raspberry“, „odroid“). Und auch bei der Installation von Desktopsystemen kann sich ein achtlos vergebener Hostname später als ungünstig herausstellen: Hostnamen erscheinen in der Routerübersicht und werden als Browseradressen und in Netzkommandos genutzt. Eine nachträgliche Änderung ist aber kein Problem. Sie öffnen mit root-Recht folgende Datei

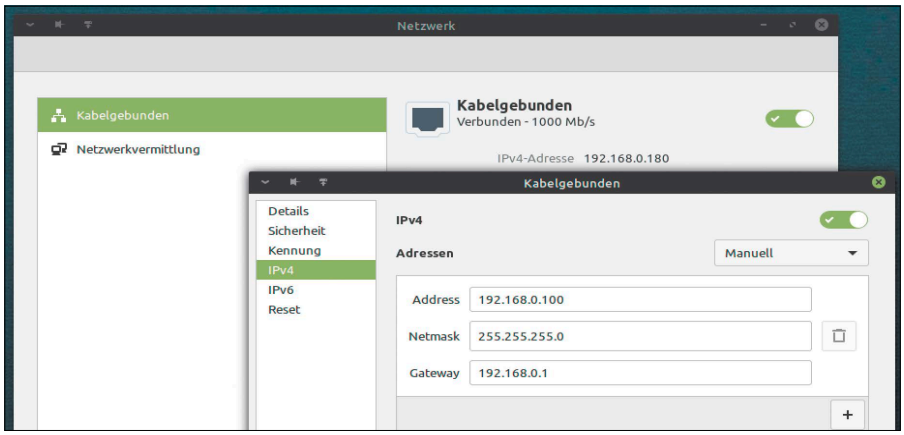
```
sudo gedit /etc/hostname
```

und tragen statt des bisherigen Namens den neuen ein. Danach starten Sie den Rechner neu.

25. Feste IP für Linux-Geräte

Server sowieso, aber letztlich jeder Linux-Rechner, der in irgendeiner Weise etwa per SSH oder Samba erreichbar ist, benötigt eine feste IPv4-Adresse im lokalen Netz. Nur so ist der Rechner via SSH, Samba im Dateimanager oder Apache im Browser zuverlässig erreichbar. Die gewünschte IP können Sie über das Netzwerkapplet in den Systemeinstellungen anfordern, indem Sie unter „IPv4“ die automatische DHCP-Vergabe abschalten und die Methode „Manuell“ einstellen. Darunter geben Sie die Wunsch-IP im lokalen Adressraum ein, darunter „255.255.255.0“ als Netzmaske und die Router-IP als „Gateway“. Nach dem nächsten Neustart gilt die neue IP-Adresse, sofern sie nicht anderweitig vergeben ist.

Alternativ funktioniert das auch über die Konfigurationsoberfläche des Routers. In der Fritzbox (*http://fritz.box*) finden Sie unter „Heimnetz → Netzwerkverbindungen“ ganz unten die Schaltfläche „Gerät hinzufügen“. Hier geben Sie „Name“ (Hostname) und „MAC-Adresse“ des Geräts ein (siehe unten), darunter die Wunsch-IP. Die Fritzbox wird nun melden, dass das Gerät bereits unter einer anderen IP bekannt ist, und Sie müssen mit „OK“ bestätigen, dass Sie die bisherige Einstellung überschreiben wollen. Danach starten Sie das Gerät neu. Hostname und die physikalische MAC-Adresse eines Rechners erfahren Sie mit den Terminalbefehlen *hostname* und *ip adress* auf dem jeweiligen Gerät. ■



Feste IPv4-Adresse für Server aller Art: Der Rechner kann eine bestimmte IP über seine Netzwerkeinstellungen anfordern. Alternativ ist die direkte IP-Vergabe in der Routerkonfiguration.

POWERTIPP 5: PLATZSPARENDE STARTERICONS

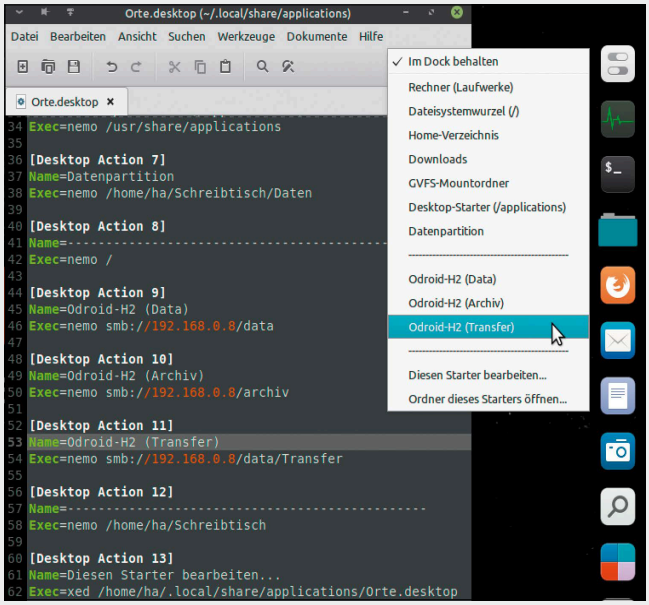
Starterverknüpfungen für Programme sind einfache Textdateien unter „/usr/share/applications“ mit der Endung „.desktop“ und einem Standardsatz von Direktiven wie „Name=…“, „Exec=[Programmaufruf]“ oder „Icon=[Icondatei]“. Das Format solcher Desktopdateien erlaubt aber nicht nur einen Programmaufruf, sondern eine beliebige Anzahl von Startern. Diese bietet das Startericon nach Rechtsklick im Kontextmenü an, sofern es in eine Starterleiste eingebaut ist. Ideal ist das Dock Plank (Paketname „plank“), aber auch das Starterdock von Ubuntu ist möglich.

Der Einbau des Icons in das Plank-Dock ist besonders einfach: Es genügt, die Desktopdatei irgendwo ins Home-Verzeichnis, etwa nach „~/.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.xx/19.xx muss das Script nach „~/.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 Script-Änderungen immer erst nach einer Neuanmeldung aktiv werden, während das Plank-Dock Änderungen im laufenden Betrieb einliest.

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 Programmaufruf benötigen. Der Einfachheit halber nummerieren Sie dabei die „Actions“ einfach durch.

Drei Beispiele auf *https://paste.ubuntu.com/p/2Tkrp8tH8b/* liefern Ihnen Vorlagen für solche Desktopdateien, um die einfache, aber doch lästige Tipparbeit auf ein Minimum zu reduzieren.



Das Dateimanager-Icon im Plank-Dock zeigt und lädt nach Rechtsklick eine ganze Reihe wichtiger Ordner. Die Abbildung zeigt auch einen Teil der dafür verantwortlichen Desktopdatei.

Crashkurs zur Netzwerkhardware

Für kleine Heimnetze genügt es oft, die Fähigkeiten des Routers konsequent zu nutzen und die Endgeräte an optimaler Stelle zu betreiben – verkabelt oder per Funknetz. Letzteres geht nicht? Auch kein Problem: WLAN und Ethernet lassen sich verlängern.



VON HERMANN APFELBÖCK

Wer von seinem Netzwerk nicht viel mehr erwartet als einen Zugang ins Internet für verkabelte und funktechnisch verbundene Endgeräte und eventuell noch eine zentrale Datenablage, benötigt kaum Netzwerk-Know-how auf Softwareebene. Es genügen Basiseinstellungen im Router und die Kenntnis geeigneter Hardware, um überall eine optimale Netzversorgung herzustellen. Diese Grundlagen sind Gegenstand dieses Netzwerk-Crashkurses. Auf pcwelt.de finden Sie unter *www.pcwelt.de/2086323* Netzwerkgrundlagen zum Einrichten eigener Linux-Server und zu Analyse und Problembehandlung im Heimnetz.

1. Netzadapter am Endgerät

Aufbau und Ausbau eines Netzwerks sind weitestgehend unabhängig vom System. Einzige Ausnahme sind die Netzadapter am Endgerät selbst (Notebook, PC). Diese benötigen einen passenden Betriebssystemtreiber. Mit Ethernet-Kabel gehen Sie eventuellen Treiberproblemen von vornherein aus dem Weg: Linux ist mit einer Kabelverbindung immer sofort im Netz und im Internet. Ebenfalls unproblematisch sind die allermeisten in Notebooks integrierten WLAN-Chips, während externe USB-WLAN-Adapter nicht immer Linux-kompatibel sind. Wie die Übersicht auf *https://wiki.ubuntuusers.de/WLAN/Karten* zeigt, werden die allermeisten USB-Adapter von Asus, AVM, D-Link, TP-Link direkt unterstützt. Durch praktischen Einsatz verifiziert haben wir die Tauglichkeit bei folgenden preisgünstigen Geräten (circa zehn bis 20 Euro):

- Asus N10 Nano WLAN-Stick
- TP-Link TL-WN823N N300 Mini WLAN
- CSL 300 Mbit/s USB 2.0 WLAN Stick
- Fritz!Wlan USB Stick-N v2.4

2. Der Heimrouter

Moderne Router vereinen eine Reihe von Funktionen – Switch für mehrere Ethernet-Anschlüsse, Funknetz, Telefonie, Druckerserver, NAS, Webfilter, Zeitbudget, Portfreigaben. Alle Funktionen lassen sich in der Konfigurationsoberfläche über jeden Browser steuern. Unerlässlich ist

1. das Einrichten des Funknetzes (Fritzbox: Netzname unter „WLAN → Funknetz“, Passwort unter „WLAN → Sicherheit“) und

2. das Festlegen der Ethernet-Leistung (Fritzbox: „Heimnetz → Heimnetzübersicht → Netzwerkeinstellungen“).

Router wie die Fritzbox sind im Browser über Standard-Hostnamen wie „fritz.box“ erreichbar, in jedem Fall aber mit der lokalen IP-Adresse. Die IP lautet oft 192.168.178.1 oder 192.168.0.1. Die Router-IP ermitteln Sie bei Bedarf mit dem folgenden Befehl:

```
ip route show
```

Im Prinzip genügt auch *ifconfig* oder *ip address*, wenn Sie im vierten und letzten Block der IPv4-Adresse statt der angezeigten Ziffer (die IP des aktuellen Geräts) die „1“ einsetzen.

Um mit dem Browser an die Konfigurationsoberfläche heranzukommen, muss zumindest ein Gerät im Netz angemeldet sein. Jeder kabelgebundene PC sollte per Voreinstellung sofort Zugang zum Netz fin-



WLAN per USB-Dongle: Nicht alle Billiggeräte werden von Linux unterstützt, die meisten Markengeräte wie hier von AVM jedoch schon.

© Quelle: amazon.de

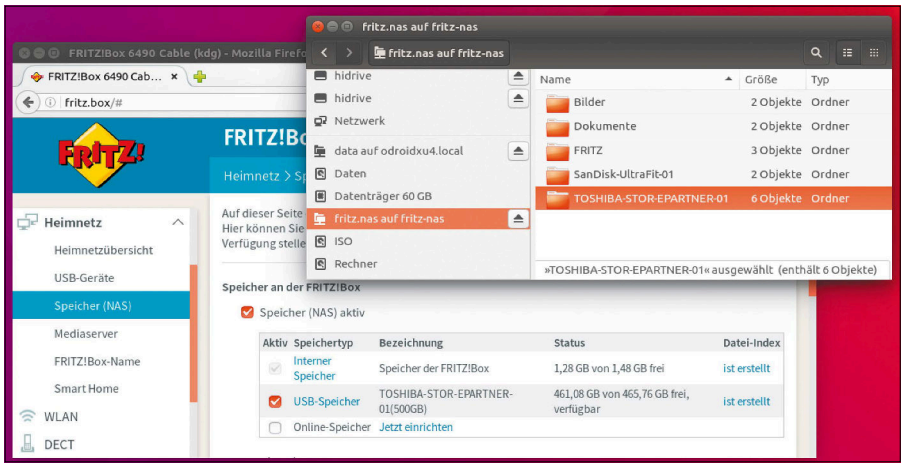
den. Voraussetzung dafür ist die aktivierte DHCP-Server-Funktion im Router (Dynamic Host Configuration Protocol), die automatisch IP-Adressen an alle Netzgeräte verteilt. Diese Einstellung ist aber überall Auslieferungsstandard.

Aufgrund seiner zentralen Rolle wäre es optimal, wenn der Router auch einen zentralen Standort einnimmt, wo Sie etwa einen PC oder ein Smart TV direkt per Kabel verbinden können. Die meisten Router besitzen vier Anschlüsse für Ethernet-Kabel – je mehr Sie davon für Geräte in unmittelbarer Nähe nutzen können, desto besser. Für die optimale Reichweite des Funknetzes wäre eine zentrale Lage im Wortsinn ebenfalls wünschenswert. Tatsache ist aber, dass Router oft ungünstig stehen, erzwungen durch die Nähe zum Splitter oder zum Kabelanschluss. Je nach Gegebenheiten in Wohnung oder Haus bieten sich dann die unter Punkt 3 bis 6 beschriebenen Techniken an.

Router als Datenserver: Wer einen zentralen Datenserver braucht, muss nicht notwendig einen „Server“ oder Platinenrechner einrichten. Viele Heimrouter bieten einen Datenserver mit einfachster Einrichtung – vorbildlich in der verbreiteten Fritzbox: Wenn Sie hier unter „Heimnetz → Speicher (NAS)“ die NAS-Funktion über „Speicher (NAS) aktiv“ einschalten, ist sofort der interne Speicher im Netz verfügbar. Der reicht natürlich nicht für einen Datenserver. Sobald Sie dann aber an einem der USB-Ports eine USB-Festplatte anschließen, wird dieser unter „Heimnetz → Speicher (NAS)“ angezeigt und kann dort durch die Klickbox aktiviert werden. Fritz-NAS arbeitet wie eine Linux-Samba-Freigabe: Der Standard-Hostname „fritz.nas“ (Standard-IP ist xxx.xxx.xxx.254) erscheint unter „Netzwerk“ im Dateimanager von Linux- und Windows-PCs und die Daten lassen sich nutzen, sofern sich der Netzteilnehmer ausweisen kann. Die dafür nötige Einrichtung der Benutzerkonten erledigen Sie unter „System → Fritz!Box-Benutzer“. Sofern nicht anders definiert, gibt die Fritzbox „Alle...verfügbaren Speicher“ großzügig mit Schreibrecht frei.

3. Ethernet-Kabel: Schnell und problemlos

Ethernet-Verbindungen sind unter Linux frei von jeder Treiberproblematik und gewährleisten einen störungsfreien Datendurchsatz. Anders als bei Funknetz und Power-LAN sind Übertragungsraten nahe dem theoretischen Wert auch im Alltag zu erreichen – bei Fast Ethernet mehr als zehn MB/s, bei Gigabit-Ethernet 100 MB/s. Wer neu verkabeln will, sollte Gigabit-Komponenten wählen. Netzgeräte mit langsameren Adaptern sind kein Hindernis, können aber nur mit ihrer langsameren Übertragungsrate mitspielen.



Fritz-Datenserver auf der Konfigurationsoberfläche und im Dateimanager: Die Freigabe eines USB-Datenträgers im Fritz-NAS ist einfacher als jede Serverlösung.

Netzwerkkabel sind in verschiedenen Kategorien erhältlich. Sie sind oft durch einen Aufdruck von „CAT“ und der nachfolgenden Kennziffer qualifiziert. Für 100 MBit wird ein CAT.5-Kabel benötigt; dieses funktioniert auch im Gigabit-LAN, besser sind dort Kabel mit der Kennzeichnung CAT.5e. Bei der Verkabelung sparen lohnt nicht, denn CAT.5e-Kabel mit zehn Metern kosten kaum fünf Euro.

Netzverkehr hinter Switch: Der komplette Datenverkehr vom und ins Internet muss durch den Router. Aber der Datenverkehr zwischen lokalen Geräten kann auch ohne Routervermittlung stattfinden, wenn diese Geräte an einem Netzwerkswitch hängen (Fast Ethernet oder Gigabit). Dabei spielt es keine Rolle, mit welchem Tempo die Daten von außerhalb zum Switch gelangen oder nach dort weiterfließen. Die mit dem Switch verbundenen Geräte kommunizieren untereinander im Bestfall im Gigabit-Tempo, selbst wenn der Durchsatz zum Router (etwa über das Funknetz) nur einen Bruchteil dieser Geschwindigkeit erreicht. Kleinere, für die Heimvernetzung meist ausreichende Switches haben fünf oder acht Anschlüsse und kosten etwa 15 Euro aufwärts.

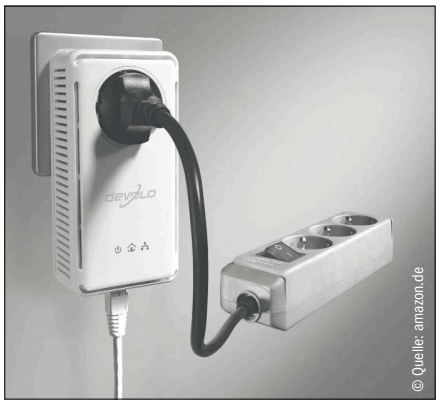


Viele Ethernet-Ports und volles Tempo: Alle verkabelten Endgeräte am Switch unterhalten sich unabhängig von der sonstigen Netzleistung mit Gigabit-Tempo.

4. Ethernet via Power-LAN

Wo direkte Verkabelung nicht in Frage kommt, ist eine Brücke über das Stromnetz eine gute Alternative. Power-LAN (auch Powerline oder DLAN) ist eine Kabelvernetzung, die für die Hauptdistanz die Stromleitung nutzt. Die kurzen Restwege übernehmen Ethernet-Kabel. Für Endgeräte spielt die Power-LAN-Brücke keine Rolle: Für Linux, Windows oder Mac-OS handelt es sich um normales Ethernet. Spezielle Treiber sind daher nicht notwendig, lediglich optionales Softwarezubehör (wie etwa das „Devolo Cockpit“ des Marktführers Devolo) ist in der Regel für Windows optimiert oder nur für Windows verfügbar.

Power-LAN ist relativ schnell, der theoretische Durchsatz von 500 oder 1200 MBit/s wird in der Praxis allerdings nicht annähernd erreicht. Im Idealfall und bei kürzeren Distanzen erreichen die Adapter 40 Prozent der theoretischen Bruttoleistung (also 200 bis 500 MBit/s), in ungünstigen Fällen aber auch nur 20 Prozent. Neben der Distanz der Adapter und der Qualität der Stromleitung können auch andere Stromverbraucher den Durchsatz beeinträchtigen. Trotzdem ist Power-LAN eine ideale Ergänzungslösung.



Power-LAN-Stecker: Die Netzwerkdaten laufen über die Stromleitung, die Restwege via Ethernet-Kabel zum Endgerät und Router. Die Weiterleitungssteckdose ist praktisch, wenn Wandsteckdosen knapp sind.

Es empfiehlt sich, die Adapter direkt in eine Wandsteckdose einzustecken und nicht in einer Steckerleiste zu verwenden. Immer zu empfehlen sind daher die etwas teureren Adapter mit integrierter Steckdose: Diese Steckdose kann somit weiter für andere Stromverbraucher oder für eine Steckerleiste genutzt werden. Ein schnelles Power-LAN-Starterkit mit zwei Adaptern kostet circa 80 Euro. Achten Sie beim Kauf auf die nützliche Weiterleitungssteckdose sowie auf die Anzahl der Ethernet-Ports, falls Sie mehrere Endgeräte direkt und ohne Switch anschließen wollen. Bei einem späteren Ausbau sollten Sie beim selben Hersteller bleiben, weil hier Adapter unterschiedlicher Geschwindigkeiten (500, 1200 MBit/s …) kompatibel sind.

Bei der Ersteinrichtung verbinden Sie den ersten Adapter per Ethernet-Kabel mit dem DSL-Router, den zweiten Adapter mit dem Endgerät (PC oder Switch). Drücken Sie innerhalb von zwei Minuten den Verschlüsselungsknopf am Gehäuse (bei älteren Devolo-Adaptern auf der Unterseite neben dem Ethernet-Port, bei neueren an der rechten Seite unten). Die Geräte handeln dann einen Code aus, über den sie sich künftig automatisch verbinden. Bei einem späteren Ausbau stecken Sie den neuen Adapter an, drücken dann erst den Verschlüsselungsknopf auf einem der älteren Adapter und danach den Knopf auf dem neuen.

WLAN über Power-LAN: Power-LAN-Adapter können auch als Access Point (siehe unten) das Funknetz ausbauen. Ein Ergänzungsadapter wie der Devolo DLAN 550 Wifi für etwa 65 Euro eignet sich vor allem dort, wo eine Power-LAN-Basis bereits vorliegt, mit der sich der Wi-Fi-Adapter dann umstandslos per Verschlüsselungsknopf verbinden kann. Die weitere Konfiguration im Browser (über die Geräte-IP) gleicht der eines Access Points.



Power-LAN-Ergänzungsadapter mit WLAN: Diese elegante Variante eines Access Points bietet umstandslos Funknetz, sofern bereits Power-LAN vorliegt. Leistungstechnisch sind klassische Access Points besser.

5. Access Point: Optimale Sendestation

WLAN (oder Wi-Fi) ist unverzichtbar, wenn mobile Geräte zum Haushalt gehören. Notebooks, Netbooks, Tablets und Smartphones bringen den nötigen WLAN-Chip standardmäßig mit. Ethernet ist dort entweder nicht vorhanden oder aus Mobilitätsgründen unerwünscht. Wenn das Router-Funknetz einen wichtigen Raum nicht abdeckt, dort aber ein Kabelnetz (direkt oder via Power-LAN) besteht, verwenden Sie an diesem Standort am besten einen Access Point. Das ist schneller und stabiler als ein Funknetz-Repeater – und eventuell sogar preisgünstiger (circa 30 bis 100 Euro). Der Access Point wird über seinen Ethernet-Anschluss zum Kabelnetz verbunden. Sobald angeschlossen, lässt er sich über seine IP-Adresse konfigurieren. Access Points nehmen sich per Werkseinstellung eine bestimmte IP, die das Handbuch verrät, die aber auch in der Geräteliste des Routers leicht zu finden ist. Ab Werk bringt Sie eventuell der Benutzer „admin“ und leeres Kennwort in die Konfiguration. Im Zweifel sind die Zugangsdaten im Handbuch vermerkt. Sorgen Sie dann dafür, dass der „admin“ ein echtes Kennwort erhält.

Das Einrichten des neuen Funknetzes geschieht unter „WLAN“, „Wireless“ oder „Drahtlos“ und erfordert die üblichen WLAN-Infos – also einen Netzwerknamen (SSID), den Verschlüsselungstyp sowie das Zugangskennwort. Danach können sich mobile Geräte zum neuen Funknetz verbinden oder je nach Standort zur Basisstation. Verwenden Sie besser klar unterscheidbare SSID-Namen für das Router-Funknetz und für dasjenige des Access Points. Mehr Konfigurationsarbeit ist für eine neue Funkstation nicht erforderlich. Jedoch bieten fast alle Access Points (und ähnlich die Power-LAN-Wi-Fi-Stecker) diverse zusätzliche Komfortoptionen wie Gastnetz, Kindersicherung, Zeitschaltung.

Altgeräte als Access Point: Oft liegt noch ein alter Router eines früheren Providers im Keller, der diese Aufgabe übernehmen kann. In diesem Gerät, dessen Konfiguration Sie wieder über seine IP-Adresse im Browser erreichen, müssen Sie unbedingt DHCP abstellen und auch sonst am besten alle Funktionen außer WLAN. Im Übrigen verfahren Sie wie bei einem Neugerät, definieren also SSID und Zugangskennwort. Einige Altrouter zeigen in der Konfiguration eine Option „Internetzugang über LAN“ oder ähnlich, die Sie aktivieren müssen.

6. Repeater: WLAN-Reichweite erweitern

Repeater vergrößern die Reichweite des Funksignals. Die je nach Ausstattung und Sendeleistung zwischen 20 und 100 Euro teuren Geräte sind die einfachste Methode, mangelhaftes WLAN zu verbessern, sind aber Power-LAN leistungstechnisch unterlegen. Falls es für die Repeater-Ersteinrichtung keine WPS-Option gibt (Wi-Fi Protected Setup per Taste), können Sie das Gerät auch manuell einrichten. Dazu stecken Sie das Gerät in der Nähe eines PCs in eine Steckdose. Danach klicken Sie unter Linux auf den Network-Manager in der System-



Repeater sind effiziente WLAN-Signalverstärker, erreichen aber nicht die Sendeleistung von Access Points oder von Power-LAN-Adaptern.

leiste. Hier sollte ein zusätzliches Netz mit dem Namen des Repeaters erscheinen, mit dem Sie sich „Verbinden“. Der Sicherheitsschlüssel lautet oft „00000000“, ein eventuell abweichendes Standardkennwort verrät die Dokumentation.

Danach laden Sie die Repeater-Konfigurationsoberfläche im Browser. Da Hostnamen wie „fritz.repeater“ nicht immer funktionieren, verwenden Sie am besten IP-Adresse des Repeaters, die Sie im Router herausfinden. Einzige fundamentale Einstellung in der Konfiguration ist die Wahl des Funknetzes, das der Repeater verstärken soll. Aktivieren Sie in dieser Liste den Namen Ihres Netzes und geben Sie das Kennwort für dieses Funknetz ein.

Bei der automatischen Ersteinrichtung übernehmen Repeater den Netznamen (SSID) der Basisstation. Klarer ist es, dem Funknetz des Repeaters einen eigenen Namen zu geben. Dies lässt sich in der Konfigurationsoberfläche einstellen, etwa beim Fritz Repeater unter „WLAN → Funkeinstellungen“. Bei eingerichteten Repeater (oder Access Points) besteht wenig Tuningbedarf, aber es ist immer besser, wenn Sie die Konfigurationsoberfläche über eine feste IP erreichen. Wenn die Konfiguration diese Möglichkeit nicht anbietet, können Sie die feste IP zentral im Router definieren.

Repeater als Brücke zum Kabel: Trotz eindeutiger Vorzüge von Verkabelung (und Power-LAN) können Sie im Heimnetz WLAN priorisieren. Das ist etwa dann notwendig, wenn Sie einen LAN-Drucker an einem Standort verwenden möchten, wo kein Ethernet zur Verfügung steht. Ein weiteres praktisches Beispiel für eine solche WLAN-Brücke zum Kabel wäre ein Linux-Rechner, der Ethernet nutzen soll, um der Treiberproblematik aus dem Weg zu gehen.

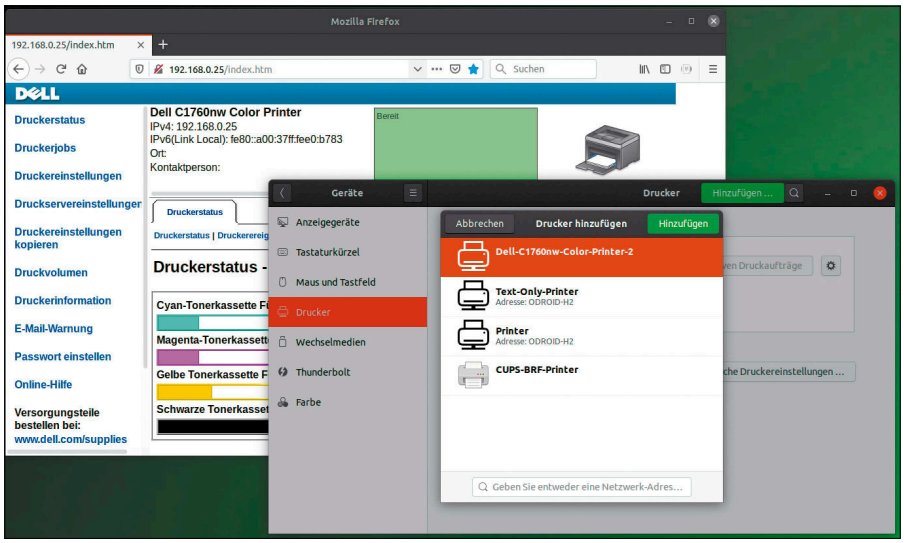
Sofern das Funksignal des WLAN-Routers den gewünschten Standort befriedigend abdeckt, können Sie dafür einen WLAN-Repeater mit Ethernet-Port einsetzen. So bietet etwa AVM seinen Fritz WLAN Repeater in mehreren Leistungsvarianten mit Ethernet-Anschluss. Sie stecken den Repeater einfach am gewünschten Ort in die Steckdose und verbinden damit den LAN-Drucker oder den Linux-PC mit einem Netzkabel. WLAN-Repeater mit Ethernet-Port kosten je nach Funkleistung etwa 30 bis 80 Euro. Eine leistungsstärkere und kaum teurere Alternative ist der Einsatz zweier Power-LAN-Adapter.



Access Point und seine Konfigurationsoberfläche: Ethernet-Kabel in die Buchse und in der Konfiguration ein neues WLAN anlegen – schon funkt das Gerät an gewünschter Stelle.

7. Netzwerkdrucker unter Linux

Anders als Drucker am USB-Port gehören Drucker mit Netzwerkadapter zu den unkomplizierten Peripheriegeräten. Viele Modelle benutzen standardisiertes PCL (Printer Command Language) oder Postscript. Damit ist der Druck ohne genau passenden Druckertreiber möglich. Netzwerkdrucker melden Sie in den Desktopdistributionen Ubuntu/Mint unter „Systemeinstellungen → Geräte → Drucker → Hinzufügen“ am System an. Unter „Neuer Drucker“ gehen Sie auf „Netzwerkdrucker“ und warten dann ab. Taucht der Drucker nicht automatisch auf, geben Sie die IP-Adresse des Netzwerkdruckers manuell an (die ist im Zweifel wie immer im Router zu ermitteln). Wird der Drucker gefunden, versucht Linux das Modell zu ermitteln und installiert den passenden oder einen generischen Druckertreiber, der mindestens die Standardfunktionen des Druckermodells abdeckt. ■



Anmelden eines Netzwerkdruckers: Das Linux-System wie hier Ubuntu findet den Drucker – sofern online – automatisch im Netzwerk und installiert einen passenden Treiber.

Linux und die Datenträger

Um Festplatten, SSDs und USB-Datenträger zu bearbeiten und zu kontrollieren, bringt der Linux-Desktop alles mit. Der Installer sorgt für die Einrichtung der Systempartition, Gnome-Disks & Co. arbeiten als Allrounder im Alltag und Gparted ist der Partitionierer für alle Fälle.



VON HERMANN APFELBÖCK

Hardwareseitig arbeiten Festplatten, SSDs und USB-Laufwerke unter Linux wie unter allen anderen Betriebssystemen. Einmal partitioniert, formatiert und eingebunden, benötigen Datenträger nur noch gelegentliche Kontrollen der aktuellen Belegung und SMART-Checks auf eventuelle Fehler. Optimales Partitionieren, Formatieren und Mounten erforderten aber schon immer einiges Basiswissen und diese Anforderungen an den PC-Nutzer sind in der aktuellen Übergangsphase mit fundamental unterschiedlichen Partitionsmethoden noch einmal gewachsen. Dieser Grundlagenbeitrag komprimiert die wesentlichen theoretischen und praktischen Probleme.

1. Partitionieren und Partitionsstil

Grundlegendste Aktion bei der Festplattenverwaltung ist das Anlegen der Partitionstabelle mit dem Partitionsstil, ferner der optionalen Einteilung in mehrere Teile (Partitionen) sowie der optionalen Festlegung der Partitionsgrößen. Viele PC-Nutzer bekommen von der Partitionierung (zumindest auf der primären Systemfestplatte) gar nichts mit, weil diese das Installationsprogramm automatisch erledigt. Liegt dabei nur eine interne Festplatte vor, die nicht weiter unterteilt werden soll, entfallen alle Entscheidungen zum Partitionsstil und zur Aufteilung. Die Installer aller Ubuntu-basierten Systeme entscheiden dann selbständig anhand der Datenträgerkapazität über den Partitionsstil: Auf großen Laufwerken über zwei TB Kapazität kommt modernes GPT (GUID Partition Table) zum Einsatz, auf kleineren Laufwerken der alte MBR-Stil. Der alte MBR-Partitionsstil (Master Boot Record, auch „msdos"-Partitionstabelle) kann Partitionen bis zu maximal 2,2 TB Größe verwalten. Für die mittlerweile gebräuchlichen Größen von vier bis 12 TB ist der GPT-Partitionsstil erforderlich, sofern solche Festplatten als Ganzes genutzt und nicht in mehrere Partitionen aufgeteilt werden. Bei Festplatten mit mehr als zwei TB sollten Sie besser immer GPT verwenden. Bei kleineren Laufwerken ist GPT zur Nutzung der kompletten Kapazität nicht erforderlich, aber eventuell trotzdem sinnvoll, wenn der PC mit Uefi-Firmware (Unified Extensible Firmware Interface) ausgestattet ist und Sie vielleicht auch Windows parallel installieren wollen (siehe Punkt 3).

Werkzeuge: Die grafischen Systemtools Gnome-Disks („Laufwerke") oder die KDE-Partitionsverwaltung können den Partitionsstil einer Festplatte kontrollieren und ändern. Die Umstellung des bestehenden Partitionsstils geht allerdings immer mit komplettem Datenverlust einher. Wir beschreiben den Vorgang nicht mit den desktopspezifischen Werkzeugen, sondern mit dem bekannten Partitionierungswerkzeug Gparted. Gparted ist zwar nicht überall Standard, aber bei Bedarf schnell nachinstalliert (*sudo apt install gparted* in Debian/Ubuntu/Mint). In Gparted sehen Sie über „Ansicht → Geräteinformationen" in der Zeile „Partitionsstil" den aktuellen Partitionsstil der gewählten Festplatte – meistens „msdos" (MBR) oder „gpt" (GPT). Über das Menü „Gerät → Partitionstabelle erstellen" können Sie den bisherigen Stil ändern.

Nach einem Klick auf „Anwenden“ erzeugt Gparted eine neue Partitionstabelle. Über „Partition → Neu“ erstellen Sie danach eine neue Partition.

Hinweis 1: Partitionen lassen sich, egal ob mit Gparted oder einem anderen Werkzeug, nur bearbeiten, wenn sie vorher aus dem Dateisystem ausgehängt wurden. Gparted erledigt dies nach Rechtsklick auf die Partition mit „Aushängen“. Falls das Aushängen scheitert, schließen Sie alle Programme inklusive Dateimanager, die den Vorgang durch ihren Zugriff verhindern könnten. Auch Netzwerkdienste wie Samba können die Bearbeitung blockieren. Wer Unmount-Blockaden ausschließen will, bootet am besten ein unabhängiges Livesystem mit Gparted.

Hinweis 2: Gparted sammelt Aufträge wie das Löschen, Erstellen oder Formatieren von Partitionen zunächst, ohne sie auszuführen. Erst „Bearbeiten → Alle Vorgänge ausführen“ startet die eigentliche Aktion.

Unter Windows zeigt die „Datenträgerverwaltung“ („diskmgmt.msc“) nach Rechtsklick auf „Datenträger [x]“ und „Eigenschaften“ auf der Registerkarte „Volumes“ den Partitionsstil an („MBR“ oder „GPT“).

Wenn keine grafische Oberfläche zur Verfügung steht, gibt es auch Terminaltools für die Festplattenverwaltung. Der Befehl

```
sudo fdisk -l
```

zeigt für die Laufwerke auch den aktuellen Partitionsstil an – hier neben „Festplattenbezeichnungstyp“ als „dos“ oder „gpt“. Für das Schreiben einer anderen Partitionstabelle, also zum Ändern des bisherigen Partitionsstils, verwenden Sie

```
sudo sgdisk -g /dev/sd[X]
```

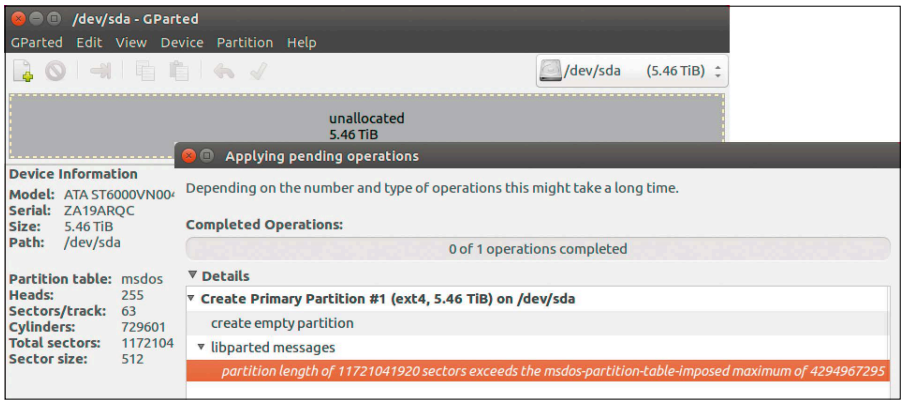
nach GPT oder

```
sudo sgdisk -m /dev/sd[X]
```

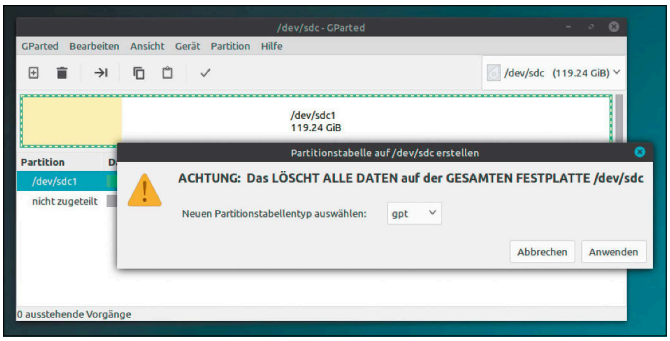
zum Schreiben einer MBR-Partitionstabelle. Ersetzen Sie dabei „[X]“ jeweils durch die richtige Kennung des Laufwerks. Bei reinen Datenpartitionen (nur Benutzerdaten) kann mit diesen Befehlen sogar eine Umwandlung des Partitionsstils ohne Datenverlust gelingen. Wir raten aber davon ab, sich darauf ohne Sicherung zu verlassen.

2. Partitionen löschen und anlegen

Das Löschen von Partitionen und Einrichten neuer Partitionen erledigen die typischen Gnome- und KDE-Tools ebenso wie Gparted. Gparted zeigt nach Rechtsklick auf die symbolische Partitionsfläche die Option „Löschen“. Dies impliziert in der Regel (und mit Gewissheit nach anschließenden Größenänderungen und Formatierung) den kompletten Datenverlust auf dieser Partition. Die Option „Neu“ zum Erstellen einer neuen Partition ist im Kontextmenü nur



Auch große Festplatten lassen sich im MBR-Stil durch Partitionierung komplett nutzen. Jedoch scheitert der Versuch, große Festplatten (hier mehr als fünf TB) als eine Partition anzulegen.



Ändern des Partitionsstils nach GPT: Dies schreibt die Partitionstabelle neu und bedeutet in der Regel einen kompletten Datenverlust auf dieser Festplatte.

AHCI-MODUS IM BIOS

Datenträger an der SATA-Schnittstelle arbeiten nur im vollen Tempo, wenn der SATA-Controller auf AHCI (Advanced Host Controller Interface) eingestellt ist – nicht IDE oder ATA. Normalerweise sollte AHCI auf neueren Rechnern die Standardeinstellung sein. Zweifel kann eine Kontrolle der Bios-/Uefi-Einstellungen beseitigen: Wenn dort unter „SATA-Konfiguration“, „OnChip SATA Type“, „SATA Operation“ (oder ähnlich lautend) die Option „Enhanced“ oder „AHCI“ eingestellt ist, dann nutzen angeschlossene Festplatte schnelles AHCI. Steht dort hingegen „ATA“, „Disabled“, „Legacy“, „Native IDE“ oder „Compatibility Mode“, dann laufen die an SATA angeschlossenen Laufwerke mit geringerer Leistung. Bei aktuellen Linux-Distributionen ist es im laufenden Betrieb möglich, den Modus im Bios auf AHCI umzuschalten. Der Kernel wird dann die enthaltenen AHCI-Treiber automatisch laden.



Bios-Setup: Damit Festplatten am SATA-Adapter mit optimaler Geschwindigkeit arbeiten, muss der AHCI-Modus aktiviert sein.

aktiv, wenn ein freier, nicht genutzter Bereich angeklickt wurde. Es muss also erst eine Partition gelöscht werden, um deren Platz („nicht zugeteilt“) dann neu zu nutzen. Mit dem anschließend angezeigten Schieberegler bestimmen Sie dann, ob die neue Partition den kompletten Platz erhalten oder eine Aufteilung in mehrere Partitionen erfolgen soll. Wenn Sie nur einen Teil der Kapazität verwenden, verbleibt danach „nicht zugeteilter“ Platz, den Sie danach mit „Neu“ auf analoge Weise partitionieren.

3. Partitionsstil (MBR/GPT) und Multiboot

Der Partitionsstil (GPT) ist nicht nur wichtig für große Datenträger jenseits der 2,2-TB-Grenze, sondern spielt auch eine entscheidende Rolle, wenn mehrere Systeme parallel installiert werden sollen – oft Linux neben Windows. Das Thema ist komplex, weil hier auch das Rechner-Bios mitspielt – Uefi (Unified Extensible Firmware Interface) oder Bios (Basic Input Output System). Theoretisch gibt es jede Kombination: Typisch ist Bios/MBR sowie Uefi/GPT, jedoch ist auch Bios/GPT und Uefi/MBR möglich. Das heißt, dass auch ein altes Bios Systeme von GPT-Partitionen oder ein modernes Uefi vom alten MBR booten kann. Ein Multiboot mit Windows funktioniert aber nur auf Bios/MBR oder Uefi/GPT.

Der theoretisch anspruchsvolle Knoten ist aber in der Praxis leicht zu lösen: Sie orientieren sich bei einer Parallelinstallationen einfach daran, was schon vorliegt, und installieren dann im selben Modus.

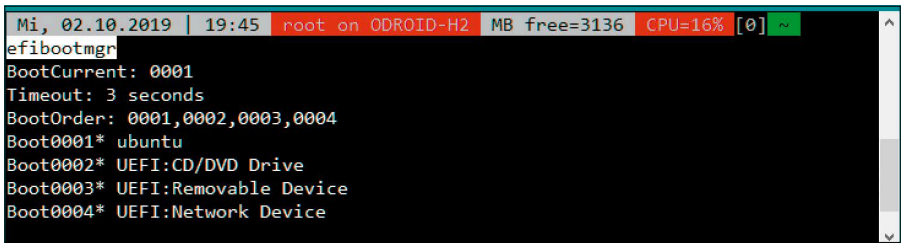
Ob das schon vorhandene System den Bios- oder Uefi-Modus verwendet, erfahren Sie unter Linux im Terminal durch Aufruf dieses Tools:

```
efibootmgr
```

Ist das Tool nicht vorhanden oder lautet dessen Ausgabe „EFI variables are not supported on this system“, dann läuft das System im Bios-Modus.

Unter Windows informiert das Systemtool Msinfo32. Hinter „BIOS-Modus“ steht bei Systemen im Bios-Modus „Vorgängerversion“, andernfalls „UEFI“. Letzteres ist bei allen neueren PCs mit vorinstalliertem OEM-Windows die Regel.

A. Liegt ein altes Bios und ein im MBR-Stil installiertes Erstsystem vor, ist die Lage eindeutig und es kann jedes 32- oder 64-Bit-System (Linux oder Windows) parallel installiert werden.



System im Bios- oder Uefi-Modus? Unter Linux beantwortet der Befehl efibootmgr diese Frage. Unter Windows hilft das Standardprogramm Msinfo32.



Friedliche Koexistenz: Ubuntu & Co. installieren sich im Uefi-Modus neben dem Windows-Bootmanager und integrieren den Windows-Bootloader in das Grub-Menü.

B. Liegt ein altes Bios, aber GPT-Partitionierung vor, kann nur ein 64-Bit-Linux installiert werden.

C. Liegt neues Uefi mit altem MBR-Stil vor (das geht vorläufig noch via Compatibility Support Module), kann jedes 32- oder 64-Bit-System (Linux oder Windows) parallel installiert werden. Dabei muss man den Rechner über das Bootmenü des Uefi-Bios starten (frühzeitiges Drücken der Taste F8, F12 oder Esc). Dort erscheinen dann die Laufwerke zwei Mal – einmal mit, einmal ohne den Vorsatz „UEFI“. Für MBR-Parallelinstallation wählen Sie Eintrag des betreffenden Installationslaufwerks ohne „UEFI“.

D. Liegt Uefi mit GPT-Stil vor, kann ein 64-Bit-System (Linux oder Windows) parallel installiert werden. Dabei muss man den Rechner über das Bootmenü des Uefi-Bios starten (frühzeitiges Drücken der Taste F8, F12 oder Esc). Für GPT-Parallelinstallation wählen Sie Eintrag des betreffenden Installationslaufwerks mit der Angabe „UEFI“.

Tipp: Trotz dieser relativ einfachen Fallunterscheidung kann man etwas falsch machen, was sich dann aber während der Installation des zweiten Systems schnell zeigt: Wenn kein Erstsystem erkannt wird und das neue System die gesamte Festplatte in Anspruch nehmen will, müssen Sie die Installation abbrechen.

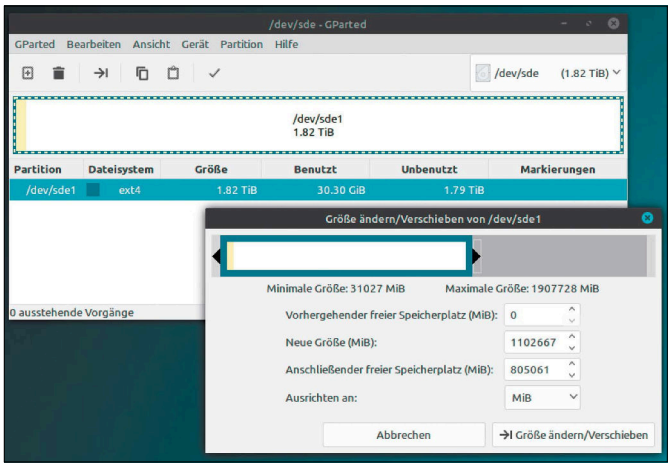
4. Partitionsgrößen nachträglich ändern

Die Einteilung (oder Nicht-Einteilung) eines Datenträgers kann sich nachträglich als ungünstig herausstellen. In diesem Fall besteht die Möglichkeit, eine bestehende Partition ohne Datenverlust zu verkleinern und auf dem frei werdenden Speicherplatz eine neue Partition anzulegen. Wirklich notwendig ist dieses Vorgehen aber nur in dem Fall, dass Sie ein weiteres Betriebssystem installieren wollen.

Werkzeuge: Erfreulicherweise sind die Installationsprogramme aller Ubuntu-Desktopsysteme auf die Situation vorbereitet, dass die Partition eines bestehenden Betriebssystems verkleinert werden muss. Mit der Option „Ubuntu neben [XXX] installieren“ schlägt der Installer eine neue Aufteilung der Partitionen vor, indem er die Partition des bestehenden Systems verkleinert und Platz für das neue System schafft. Die

gewünschten Partitionsgrößen lassen sich einfach mit der Maus über die Aufteilungsmarkierung einstellen.

Im Falle einer gewünschten Größenänderung ohne Installation oder ohne einen Installer, der solche Größenänderungen beherrscht, hilft wieder Gparted. Beachten Sie, dass Gparted nur ausgehängte Partitionen bearbeiten kann und folglich die Systempartition eines laufenden Systems tabu bleibt. Zugriff auf alle Festplatten hat Gparted nur, wenn es auf einem unabhängigen Livesystem läuft. In Gparted wählen Sie zunächst rechts oben Sie den gewünschten Datenträger. Klicken Sie dann 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):“ manuell ein. Danach klicken Sie auf „Größe ändern“. Gparted erledigt diesen wie alle Aufträge erst nach „Bearbeiten → Alle Vorgänge ausführen“.



Gparted verkleinert Partitionen ohne Datenverlust: Das können inzwischen auch andere Partitionsmanager, aber keiner so zuverlässig wie der Altmeister.

Unter Windows gibt es die Datenträgerverwaltung („diskmgmt.msc“), die nach Rechtsklick auf einer Partition die Option „Volume verkleinern“ anbietet. Die Größe der neuen Partition definieren Sie dann mit dem Wert neben „Zu verkleinernder Speicherplatz“. Dies ist eine weitere Möglichkeit, um eine Parallelinstallation eines Linux vorzubereiten, das kein ausreichendes Partitionierwerkzeug mitbringt.

FESTPLATTEN ZUSAMMENLEGEN

Der Logical Volume Manager (LVM) erlaubt das Anlegen einer „Volume Group“, in welche mehrere physische Laufwerke und Partitionen zu einem logischen Laufwerk zusammengefasst werden. Der angelegte Verbund ist dynamisch erweiterbar, enthaltene Datenträger können also wieder entnommen oder durch andere ersetzt werden. Das ist sehr flexibel, erhöht aber die Komplexität, zumal der Ausfall eines Datenträgers den ganzen Verbund gefährdet. LVM hat seinen Platz eindeutig auf Serversystemen mit flexiblen Kapazitätsansprüchen und ist nur erfahrenen Admins zu empfehlen.

In Ubuntu & Co. kann LVM bereits bei der Installation gewählt werden. Damit wird die Systempartition zum ersten Volume der LVM-Gruppe. Notwendig ist dies nicht, da sich LVM auch nachträglich einrichten lässt – unabhängig von der Systempartition und ausschließlich für Datensammlungen. Mit dem standardmäßig installierten Terminaltool lvm ist die Einrichtung von LVM-Pools allerdings eine mühsame Angelegenheit. Ein grafisches Tool gibt es aktuell nur für KDE – den „KDE-Manager für Laufwerkspartitionen“ (KVPM), der durch das gleichnamige Paket installiert werden kann:

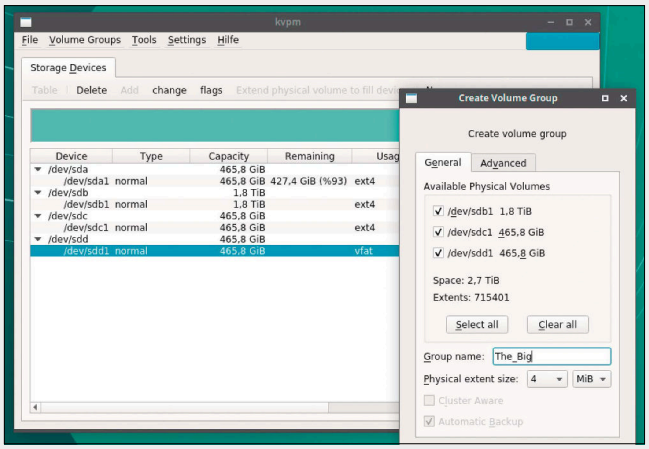
```
sudo apt install kvpm
```

Die Installation von kvpm ist auch unter Gnome-affinen Oberflächen (Gnome, Cinnamon, XFCE) möglich.

Mit KVPM ist der Ablauf dann recht bequem. Nachdem alle Laufwerke für den künftigen Datenpool angeschlossen sind, starten Sie den Manager mit root-Recht:

```
sudo kvpm
```

Klicken Sie in der Übersicht nacheinander mit rechter Maustaste auf alle Laufwerke und Partitionen, die zum neuen Pool gehören sollen, und wählen Sie „Filesystem operations → Unmount filesystem“. Danach verwenden Sie das Menü „Volume Groups → Create Volume Group“, markieren die Datenträger mit Kreuzchen und vergeben einen Gruppennamen. Nach „OK“ finden Sie im Register „Group: [Name]“ den zusammengelegten Speicher, den Sie nun – am einfachsten nach Rechtsklick auf den grünen Balken – mit „Create logical volume“ als ein logisches Volume definieren. Nutzen Sie mit dem Schieberegler den maximalen Platz und vergeben Sie einen Volumenamen. Der Speicherbalken ändert nun seine Farbe und nach Rechtsklick darauf können Sie den Speicherplatz in das Dateisystem mounten. Dabei ist noch ein beliebiges Dateisystem zu wählen und der gewünschte Mountpunkt.



KDE-Manager für Laufwerkspartitionen (KVPM): Hier werden drei Laufwerke unter dem Namen „The_Big“ zusammengefasst. Das Gesamtvolume muss dann noch formatiert werden.

5. Formatieren: Die Dateisysteme

Partitionieren und Formatieren erscheinen in grafischen Tools in einem Dialog wie eine Tateinheit. Tatsächlich bedeutet Partitionieren das Aufteilen von Festplattenbereichen, während Formatieren bereits weitaus betriebssystemnäher das Dateisystem für die jeweilige Partition bestimmt. Dateisysteme wie FAT32 beschränken sich auf eine relativ simple Verweisbibliothek zum Auffinden der Daten, Dateisysteme wie Ext4 oder NTFS erweitern diese Basisfunktion um Rechteattribute und Wiederherstellungsprotokolle (Journaling), Dateisysteme wie BTRFS erlauben sogar Snapshots des Partitionszustands und die Rückkehr zu einem früheren Zustand.

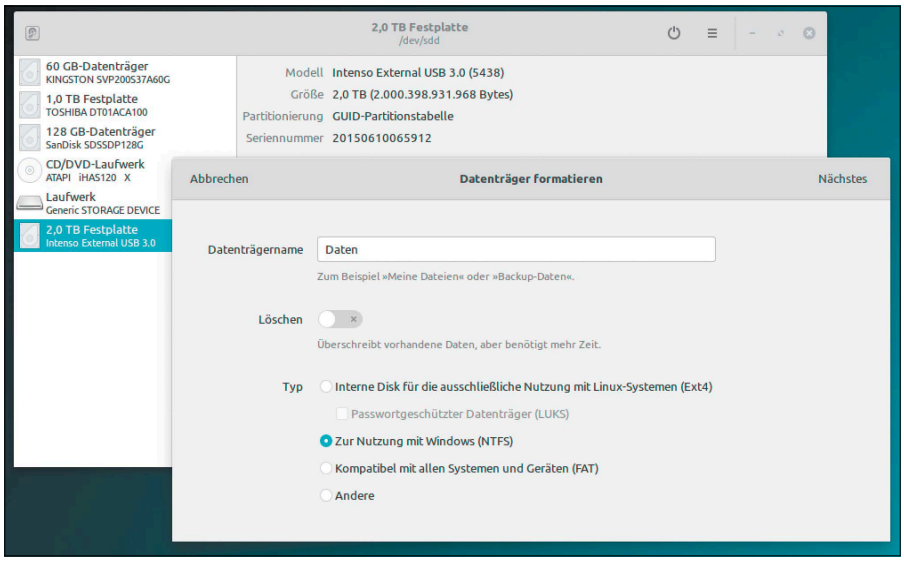
Trotz zahlreicher weiterer Dateisysteme wie F2FS, JFS, ZFS, ReiserFS, XFS ist die Wahl auf einem Desktopsystem nicht schwer: Für die Systempartition, aber auch für alle sonstigen Datenträger, die nur am Linux-System genutzt werden, ist Ext4 die solideste Wahl. Das gilt auch für Laufwerke, die Netzfreigaben leisten sollen.

Dateisysteme sind allerdings nicht beliebig kompatibel. So kann (oder will) Windows mit Ext4-formatieren Datenträgern nichts anfangen. Wenn Datenträger wie also interne Festplatten (bei Multiboot) oder mobile USB-Datenträger für den Datenaustausch zwischen Linux und Windows genutzt werden, sind andere Dateisysteme zu erwägen:

• Für kleinere interne oder externe Laufwerke (USB-Sticks), die für unkomplizierten Datenaustausch dienen sollen, eignet sich im einfachsten Fall eine Formatierung mit dem FAT32, das alle Betriebssystem ohne Hilfsmittel beherrschen und auch selbst formatieren können. Auf FAT32 ist allerdings die maximale Dateigröße auf vier GB limitiert. Wenn diese Grenze stört, kommt eventuell das Microsoft-Dateisystem exFAT in Betracht. Linux beherrscht exFAT demnächst standardmäßig, vorläufig ist noch die Nachinstallation des kleinen exFAT-Treibers ist mit

```
sudo apt install exfat-fuse exfat-utils
```

erforderlich. Danach können Sie exFAT-Datenträger sofort mit Linux-Dateimanagern nutzen und mit Werkzeugen wie Gnome-Disks („Laufwerke“) auch mit exFAT formatieren („Partition formatieren → Andere → exFAT“). Gparted hat exFAT zwar in seiner Dateisystemliste, will aber bislang nicht mit exFAT formatieren (inaktiv).



Formatieren mit Gnome-Disks: Das Tool „Laufwerke“ beschränkt sich auf die populärsten Dateisysteme, hilft aber bei der Auswahl. Gparted ist mächtiger, setzt aber Kompetenz voraus.

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

```
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
    -z, --mft-zone-multiplier NUM   Set the MFT zone multiplier
    -T, --zero-time                 Fake the time to be 00:00 UTC, Jan 1, 1970
    -F, --force                     Force execution despite errors
```

• Sind nur Linux- und Windows-Rechner im Spiel, ist das Microsoft-Dateisystem NTFS erste Wahl. Linux wie Windows haben dort Lese- und Schreibzugriff, Linux wie Windows können mit NTFS formatieren. Mac-OS X kann NTFS standardmäßig nur lesen.

Werkzeuge: Gparted erledigt die Formatierung einer Partition nach Rechtsklick und „Formatieren als“, wonach die Liste der unterstützten Dateisysteme angeboten wird. Standardprogramme wie Gnome-Disks beherrschen diese Pflichtaufgabe natürlich ebenso („Partition / Laufwerk formatieren“), bieten dabei zwar weniger Dateisysteme, leisten aber Anfängerunterstützung, indem sie die Kompatibilität der Dateisysteme skizzieren – etwa „Zur Nutzung mit Windows (NTFS)“.

Wenn Sie die Kommandozeile benutzen müssen, verwenden Sie den Befehl mkfs („make filesystem“):

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

Nach „mkfs.“ folgt die Angabe des Dateisystems „ext4“, hinter „-L“ („Label“) geben Sie optional eine Bezeichnung an, 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“. Für andere Dateisysteme gibt es entsprechende Tools, beispielsweise mkfs.ntfs oder mkfs.vfat (FAT32).

6. Mounten: Statisch und dynamisch

Mounten ist Pflicht: Jede Partition muss an definierter Stelle (Mountpunkt) in das Dateisystem eingebunden werden. Die einzige Partition, die in jedem Fall statisch beim Systemstart eingebunden wird, ist die Systempartition. Dies wird schon bei der Installation festgelegt, wenn Sie den Installationsort bestimmen und als Mountpunkt („Einbindungspunkt“) das Wurzel-

verzeichnis „/“ angeben. Resultat dieser Aktion ist ein Eintrag in der Datei „/etc/fstab“, die für alle statischen Mountaufträge zuständig ist (Beispiel):

```
UUID=[xxxxxxx]  /  ext4  errors=
 remount-ro  0  1
```

Manuelles Bearbeiten der „/etc/fstab“ für weitere statische Mountaktionen kann sinnvoll oder notwendig sein: Auf Servern, die Laufwerke automatisch bereitstellen sollen, ist es unbedingt notwendig, diese Laufwerke in die fstab einzutragen. Auf Desktoprechnern übernimmt der Dateimanager durch dynamisches Mounten (siehe unten) viele Mountaufgaben. Dennoch kann es komfortabel sein, interne Laufwerke mit Benutzerdaten via „/etc/fstab“ in einen klicknahen Ordner zu mounten. Unbedingt notwendig ist ein fstab-Eintrag auf Desktop-PCs, wenn Sie ein zusätzliches Laufwerk exakt an einer bestimmten Stelle des Dateisystems einhängen wollen.

Die für die „/etc/fstab“ notwendigen Informationen sind die eindeutige UUID des Laufwerks (eine hexadezimale Ziffern- und Buchstabenfolge), der Mountpunkt und dessen Dateisystem (Ext4, NTFS ...). Alle diese Angaben liefert der Befehl

```
lsblk -f
```

Ein Eintrag für die fstab sieht dann im Prinzip so aus

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

und im konkreten Beispiel etwa so:

```
UUID=BE43818F4A8138A3  /srv/data
 ext4  defaults  0  0
```

Die Partition/Festplatte mit dieser UUID wird dann automatisch im Ordner „/srv/data“ bereitgestellt. Der angegebene Mountordner muss existieren und sollte leer sein.

Die mit Komma getrennten „Optionen“ enthalten im einfachsten Fall nur den Wert „defaults“, können aber auch komplex ausfallen (Fehlertoleranz, Dateirechte). Die Mountoptionen sind schon deshalb eine Wissenschaft für sich, weil manche Dateisysteme ganz spezielle Eigenschaften besitzen, die mit den Optionen abgerufen werden können. Mit „defaults“, das eine Zusammenfassung von mehreren typischen Optionen ist, kommen Sie aber in den meisten Fällen ans Ziel.

Bevor Sie einen Rechner mit geänderter Datei „/etc/fstab“ neu starten, lohnt sich immer ein manueller Test:

```
sudo mount -a
```

Dies lädt alle Geräte, die in der Datei „/etc/fstab“ eingetragen sind.

Dynamisches Mounten: Auf dem Linux-Desktop erledigt der grafische Dateimanager den Großteil des Mountgeschäfts. Wenn Sie ein USB-Laufwerk anschließen oder ein neues Laufwerk gerade neu formatiert haben, taucht dieses sofort in der Navigationsspalte des Dateimanagers auf. Nach einem Mausklick darauf erledigt der Dateimanager das Mounten in das Dateisystem, und zwar unter „/media/[Benutzername]/[Volume-Label]“. Bei Ubuntu verhält sich der Dateimanager abhängig von Benutzerrechten, Dateisystem und Laufwerkstyp unterschiedlich:

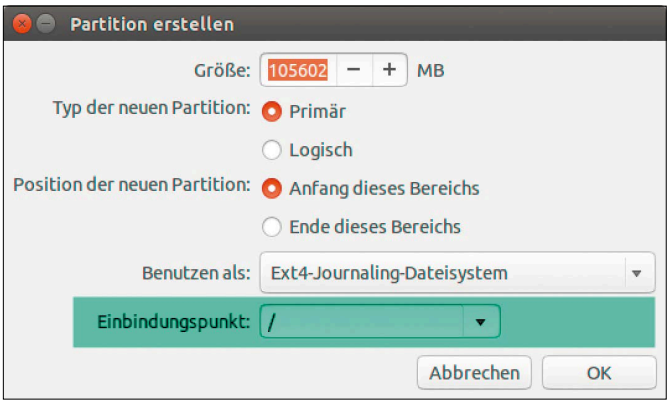
• Benutzer mit administrativen Rechten (Systemverwalter) dürfen interne und externe Laufwerke über den Dateimanager ein- und aushängen.

• Auch Systemverwalter erhalten bei Linux-Dateisystemen wie Ext4, BTRFS und XFS nur Lesezugriff, Schreibzugriff gibt es auf FAT32- und NTFS-Partitionen..

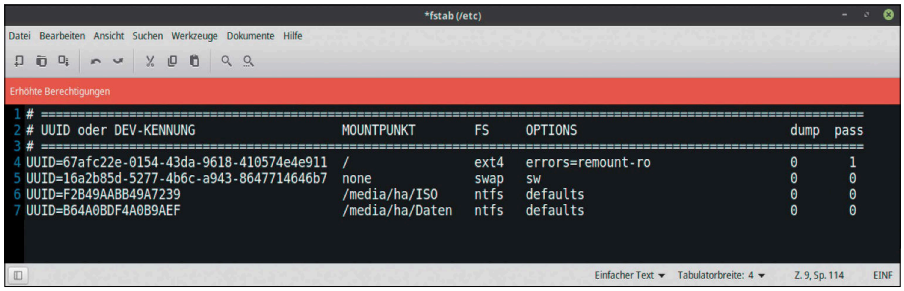
• Standardbenutzer dürfen über den Dateimanager nur externe Geräte (USB-Sticks und Festplatten) ein- und aushängen. Auf FAT32- und NTFS-Partitionen gibt es Lese- und Schreibzugriff.

• 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.

Zusammengefasst gibt es beim dynamischen Mounten von USB-Laufwerken mit FAT32 und NTFS die wenigsten Rechteprobleme. Wenn USB-Laufwerke ein Linux-Dateisystem besitzen, müssen Sie die Rechte wie bei internen Laufwerken setzen, um Schreibrecht zu erreichen.



Mountpunkt ab Installation: Das Wurzelverzeichnis („/“) für die Systempartition wird schon bei der Installation festgelegt.



Statisches Mounten mit „/etc/fstab“: Alle Partitionen, die hier eingetragen sind, lädt Linux beim Systemstart automatisch in den angegebenen Mountpunkt.

7. Zugriffsrechte im Dateisystem setzen

Bei neu in das Dateisystem eingebundenen Ext4-Partitionen (ebenso XFS oder BTRFS) hat nur „root“ Schreibzugriff, andere Benutzer erhalten nur Lesezugriff. Wenn Sie der einzige Benutzer des Systems sind, können Sie es sich einfach machen. Mit

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

setzen Sie im betreffenden Mountpunkt (hier „/mnt/Data“) maximale Zugriffsrechte. Bei Mehrbenutzersystemen ist die Rechtevergabe komplizierter. Hier steuern Sie den Zugriff über die Gruppenzugehörigkeit und Access Control Lists (ACL) mit dem Tool setfacl. Führen Sie im Terminalfenster folgende Befehle aus:

```
sudo chgrp plugdev /mnt/Data
```

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

Diese Befehlszeilen erstellen ein Verzeichnis „/mnt/Data“ für den Datenaustausch. Es gehört der Gruppe „plugdev“, die Vollzugriff erhält. „chmod g+s“ bewirkt, dass das Gruppenattribut 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 Gruppe „plugdev“ gehören unter Ubuntu/Mint standardmäßig alle Benutzer.

8. Kapazitäten einfach erweitern

Das Verzeichnis „/home“ mit den Benutzerdateien erfordert in aller Regel den meisten Plattenplatz. Sollte der Platz knapp werden, können Sie die Daten auf eine zweite Festplatte mit mehr Kapazität verlagern. Wichtig ist, dass gerade keine Dateien geöffnet sind, welche die Aktion blockieren.

Das Beispiel geht davon aus, dass eine zusätzliche Festplatte unter „/mnt/data“ eingebunden ist. Schließen Sie alle Programme und wechseln Sie mit Strg-Alt-F1 in die erste virtuelle Konsole. Dort kopieren Sie alle Verzeichnisse unter „/home“ auf das zusätzliche Laufwerk und benennen das bisherige Home-Verzeichnis um:

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

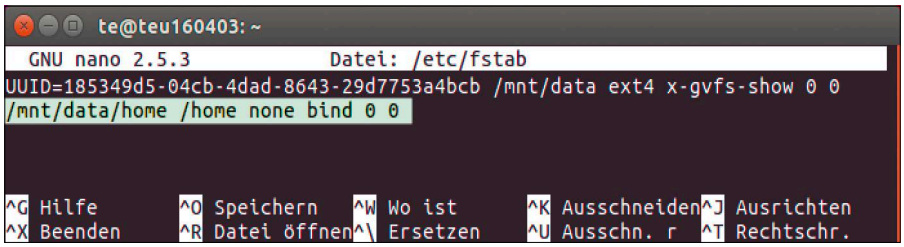
Beachten Sie beim rsync-Befehl den abschließenden Slash hinter „/home/“. Mit folgenden Befehlen erstellen Sie einen neuen Ordner „/home“ und hängen das Verzeichnis des neuen Laufwerks an dieser Stelle ein:

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

Funktioniert alles problemlos, dann sorgen Sie dafür, dass Linux den Ordner beim Systemstart automatisch vom primären Mountordner nach „/home“ abbildet. Dazu genügt eine zusätzliche Zeile der Datei „/etc/fstab“:

```
/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 – aber mit mehr Platz.



Mounttrick in der Datei „/etc/fstab“: Das unter „/mnt/data“ eingehängte Laufwerk wird über eine zweite Zeile mit der Option „bind“ einfach ins Home-Verzeichnis verschoben.

Tipp: Als alleiniger Systembenutzer lassen sich Plattenplatznöte unter „/home/[user]“ noch einfacher beheben. Im Beispiel nehmen wir an, dass der Ordner „~/Videos“ zu viel Platz benötigt. Auch hier schließen Sie alle Programme und mounten im Terminal nach der Eingabe von

```
mv ~/Videos ~/Videos.old
mkdir ~/Videos
```

den neuen Datenträger direkt in das betreffende Verzeichnis:

```
sudo mount /dev/sd[xy] ~/Videos
```

Danach verschieben Sie alle Inhalte aus „Videos.old“ nach „Videos“, was auch im Dateimanager geschehen kann. Eventuelle Rechteprobleme beheben Sie so:

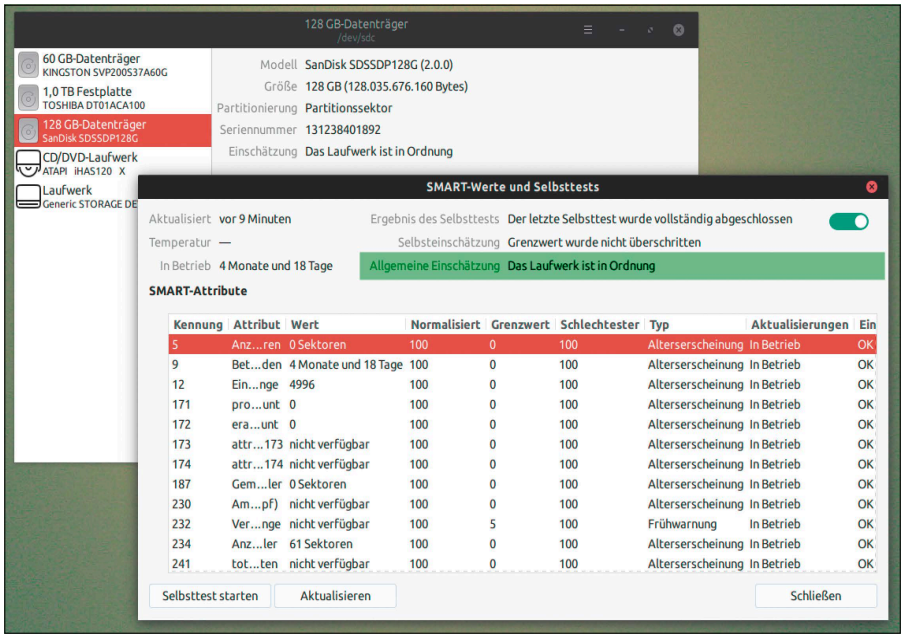
```
sudo chmod -cR 777 ~/Videos
```

Hat dies alles geklappt, tragen Sie den Datenträger mit seiner UUID und Mountpunkt „/home/[user]/Videos“ in die Datei „/etc/fstab“ ein.

9. Kontrolle des Datenträgerzustands (SMART)

Festplatten und SSDs protokollieren Statusinformationen (SMART-Werte), die Hinweise auf Fehler und Defekte geben. Die Werkzeuge Gnome-Disks und KDE-Partitionmanager zeigen die SMART-Werte interner Festplatten an. Das KDE-Tool äußert sich unter „Gerät → Status“ relativ knapp, jedoch sollte eine positive „Gesamtbewertung: Healthy“ für einen Gesamteindruck ausreichen.

Das Gnome-Tool ist unter „SMART-Werte und Selbsttests“ recht gesprächig, sollte aber vor allem hinter „Allgemeine Einschätzung“ die Aussage zeigen: „Das Laufwerk ist in Ordnung“. Bei SSDs steht hinter „wear-leveling-count“ in der Spalte „Normalisiert“ ein wichtiger Wert: Neue SSDs starten bei „100“ und der Wert reduziert sich mit der Zeit. Nähert er sich der „0“, müssen Sie das Laufwerk ersetzen. Per USB angeschlossene Festplatten berück-



Gnome-Disks und die KDE-Partitionsverwaltung lesen die SMART-Werte von Datenträgern aus: Die angezeigte SSD ist neuwertig und darf weitermachen.

sichtigt das KDE-Tool ebenfalls, Gnome-Disks allerdings nicht. Hier benötigen Sie das zusätzliche Paket „smartmontools“ und folgenden Terminalbefehl:

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

Wenn der Health-Test mit „PASSED“ beantwortet wird, ist die Tauglichkeit des Laufwerks schon erwiesen. Weitere Details gibt es nach der Eingabe von

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

und noch ausführlicher mit dem Parameter „-a“. Ein wichtiger Wert ist „Reallocated_Sectors_Ct“, der die Zahl defekter Sektoren anzeigt und im Optimalfall eine „0“ bieten sollte. Gleiches gilt für „Spin_Retry_Count“, weil die hier gezählten gescheiterten Anlaufversuche auf mechanische Mängel deuten. Seek- und Read-Errors sind hingegen kaum relevant.

10. Kontrolle der Festplattenbelegung

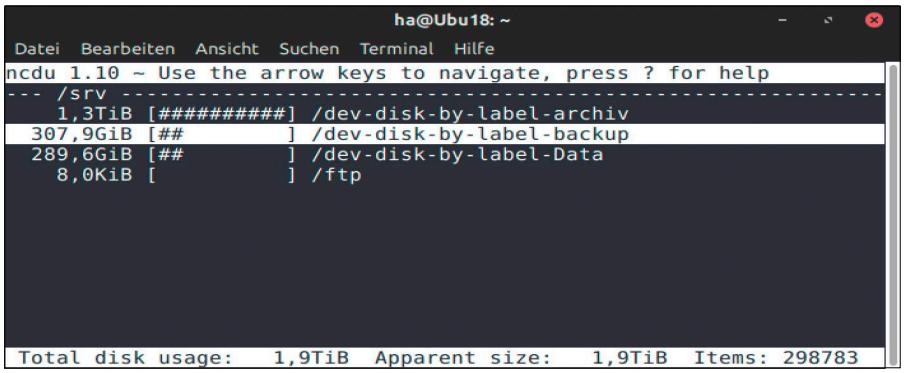
Auf Gnome-Desktops finden Sie das Tool Baobab („Festplattenbelegung“) im Hauptmenü. Es zeigt die Gesamtkapazität und den Füllstand von Datenträgern. Nach Klick auf den Pfeil ganz rechts startet Baobab eine Ordneranalyse, die es nach kurzer Wartezeit als Kreis- oder Kacheldiagramm visualisiert. Das sieht hübsch aus, doch der Erkenntniswert hält sich in Grenzen. Viele Nutzer werden sich von

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

im Terminal schneller und besser informiert fühlen. Vor allem die Prozentzahl („Verw%“) bietet gute Orientierung. Wer eine Größenanalyse der Verzeichnisse benötigt, ist mit einem weiteren Terminalwerkzeug

```
du -h
```

übersichtlich beraten. Wer es genauer wissen muss, kann auch das Tool Ncdu nachinstallieren. Das Terminalprogramm sortiert die Verzeichnisse nach der enthaltenen Datenmenge und kann auch aktiv löschen. Um das komplette Dateisystem zu durchforsten, muss man Ncdu auf der obersten Ebene starten („ncdu /“). ■



Verzeichnisgrößen mit Ncdu ermitteln: Auf SSH-verwalteten Servern ist Ncdu unverzichtbar und selbst auf dem Desktop eine Empfehlung.

DATENTRÄGER IM BEREITSCHAFTSMODUS

Festplatten lassen sich in den Ruhemodus schicken. Die Gnome-affinen Ubuntus inklusive Mint können mit Gnome-Disks („Laufwerke“) einstellen, wann sich eine Festplatte abschalten soll. Wählen Sie dort die gewünschte Festplatte aus und gehen Sie im Menü auf „Laufwerkseinstellungen“. Auf der Registerkarte „Bereitschaft“ setzen Sie den Schalter auf „An“ und stellen die Zeit ein, nach der die Festplatte sich abschalten soll. Die Zeitspanne reicht von „Niemals“ bis „3 Stunden“. Das funktioniert neuerdings auch mit externen USB-Laufwerken.

Wenn Gnome-Disks fehlt, kann auch hdparm im Terminal den Bereitschaftsmodus konfigurieren. Ermitteln Sie zuerst mit

```
blkid
```

die Laufwerke, Bezeichnungen und UUID-Kennungen. Ist die gewünschte Festplatte beispielsweise „/dev/sdb“, dann aktivieren Sie mit diesem Befehl den Ruhezustand:

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

Wenn das funktioniert, können Sie eine automatische Abschaltung festlegen:

```
sudo hdparm -S 180 /dev/sdb
```

Der Wert hinter „-S“ steht für 180 mal fünf Sekunden, also 900 Sekunden oder 15 Minuten. Verwenden Sie „-S 0“, wenn sich eine bestimmte Festplatte niemals abschalten soll (siehe auch: man hdparm). Diese Maßnahme wirkt allerdings nur bis zum nächsten Neustart. Für eine dauerhafte Änderung bearbeiten Sie die hdparm-Konfigurationsdatei:

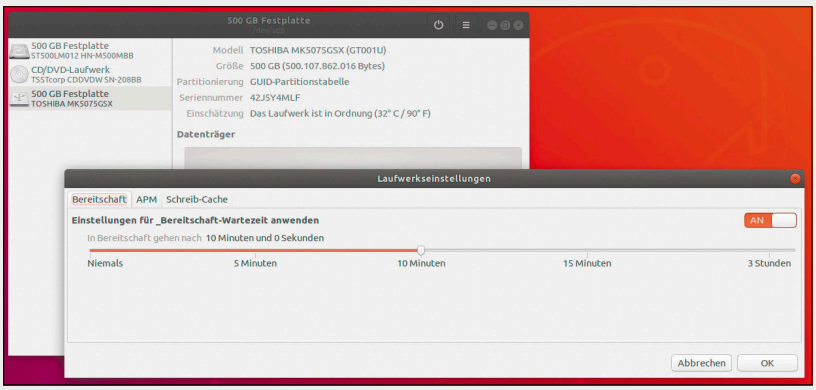
```
sudo nano /etc/hdparm.conf
```

Fügen Sie im Editor folgende Zeile am Ende der Datei an:

```
/dev/disk/by-uuid/[UUID] { spindown_time = 180 }
```

Die UUID-Kennungen ermittelt das Kommando blkid.

Hinweis: Der Bereitschaftsmodus ist nur bei Daten- oder Backupplatten sinnvoll. Auf der Festplatte mit der Systempartition finden ständig Laufwerkszugriffe statt – die Festplatte würde also nach dem Abschalten sofort wieder anlaufen. Die Folge wäre mehr Verschleiß statt weniger.

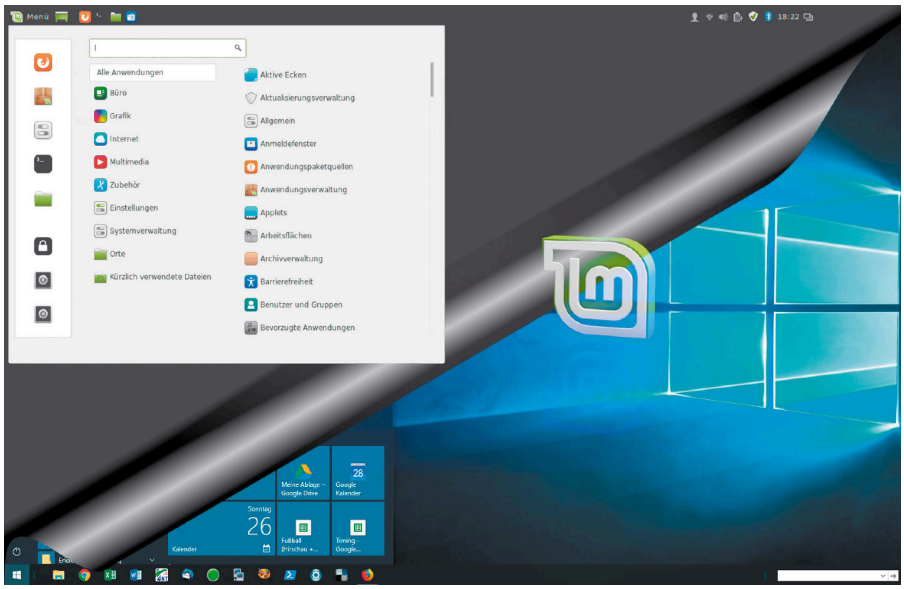


Datenfestplatten in den Ruhemodus schicken: Gnome-Disks beherrscht diese Aufgabe, notfalls ist dies aber auch über hdparm im Terminal zu steuern.

Linux/Windows: Austausch & Kompatibilität

Installation und Einrichtung von Linux-Systemen fallen auch Windows-Umsteigern leicht. Doch wie steht es danach um die vorhandenen Benutzerdaten und Medien, um die Softwareausstattung und den Datenaustausch?

VON HERMANN APFELBÖCK



Dieser Grundlagenbeitrag dreht sich um die beiden Aspekte des „Wie“ und „Was“ beim Datenaustausch zwischen Linux und Windows. Wie tauschen Sie Dateien problemlos zwischen beiden Betriebssystemen? Welche Formate und Formatinterpreter (Programme) eignen sich für plattformübergreifendes Arbeiten?

Dabei konzentrieren wir uns in diesem ersten Beitrag auf verbreitete Standardaufgaben, die allenfalls Planung und Detailkorrekturen fordern, aber keine fundamentalen Probleme stellen. Wie Sie unter Linux proprietäre Formate bearbeiten und Windows-Spezialsoftware nutzen, ist Gegenstand eines Artikels auf *www.pcwelt.de/2057577*, der sich mit Wine und Virtualisierung befasst.

Netzwerkgespräche zwischen Linux und Windows

Für den heimischen Datenaustausch zwischen Linux und Windows ist das Netzwerk der eleganteste Weg. Jedes Linux mit installiertem Samba-Client (Standard) kann die Freigaben von Windows-Rechnern nutzen. Umgekehrt greift Windows umstandslos auf die Samba-Freigaben eines Linux-Rechners zu (Samba-Server). In beiden Richtungen gelten die üblichen Regeln, dass ein zugreifender Benutzer sowohl die nötige Netzwerkerlaubnis als auch die nötigen lokalen Dateirechte besitzen muss.

Samba (SMB/CIFS) ist aber nicht der einzige Kommunikationsweg: Auf den meisten Linux-Rechnern läuft ein SSH-Server (oder ist schnell eingerichtet mit *apt install openssh-server*) und somit das Transferprotokoll SFTP. Dies lässt sich mit dem plattformübergreifenden Filezilla auch unter Windows nutzen (*www.filezilla-project.org*). Sie können dort einen Linux-Rechner mit IP, SSH-Authentifizierungsdaten („Verbindungsart: Normal“) und SFTP-Protokoll in den Servermanager eintragen, sich verbinden und Dateien übertragen.

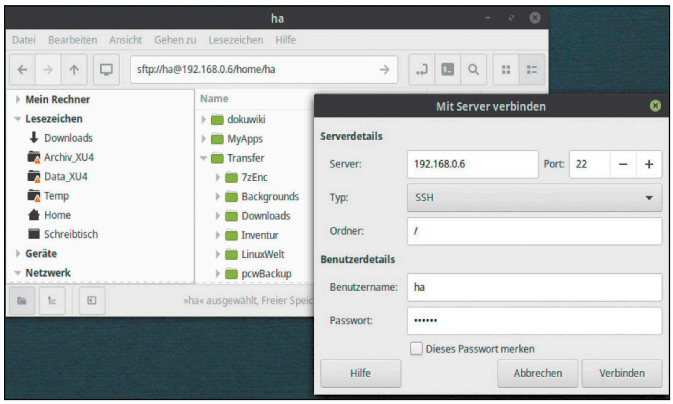
Eine bequeme Transfermethode – ebenfalls über SSH – eröffnet ferner die „Bash on Ubuntu on Windows“ (BUW). Das optionale BUW kann in Windows unter „Systemsteuerung → Programme und Features“ nachgerüstet werden („Windows Subsystem für Linux“) und stellt ein vollwertiges Terminal-Ubuntu bereit.

Mit einem wiederum hier nachinstallierten Midnight Commander (*sudo apt-get install mc*) ist die bekannte „Shell-Verbindung“ (SSH) möglich und Sie haben die Dateisysteme des Linux-Rechners und des Windows-Systems vor sich (Windows unter „/mnt/c“).

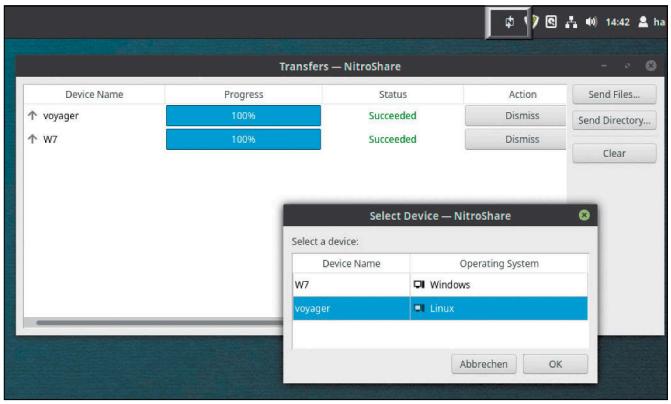
Wer es sich beim Datenaustausch besonders einfach machen will, kann unter Linux (*apt install nitroshare*) und Windows (*https://nitroshare.net/*) das Peer-to-Peer-Tool Nitroshare einrichten. Wo immer dieses läuft, kann es mit „Send Files“ und „Send Folder“ Daten zu einem beliebigen Empfänger im lokalen Netzwerk schicken, wo Nitroshare ebenfalls läuft.

Datenträger für Linux & Windows

Sollen physische Datenträger, also interne Festplatten (bei Multiboot) oder mobile USB-Datenträger, für den Datenaustausch zwischen Linux und Windows genutzt werden, gibt es etliche Einschränkungen, die sich aber durch Planung vermeiden lassen:



Datenaustausch mit SSH (SFTP): Die Linux-Dateimanager beherrschen SFTP von Haus aus. Auf Windows-Systemen kann Filezilla aushelfen.



Datenaustausch mit Nitroshare: Das plattformunabhängige Tool ist eine simple Alternative für Heimnetze, wo kein Konfigurationsaufwand anfallen soll.

Linux-Dateisysteme (meist Ext4) sind für Windows nicht lesbar. Trotz mancher Linux-Umarmung zeigt Microsoft bis dato kein Interesse, Linux-Datenträger unter Windows zu unterstützen. Dass das technisch kein Problem wäre, zeigt die externe Software Ext FS for Windows (*www.paragon-software.com*), die man aber längst nicht überall voraussetzen kann.

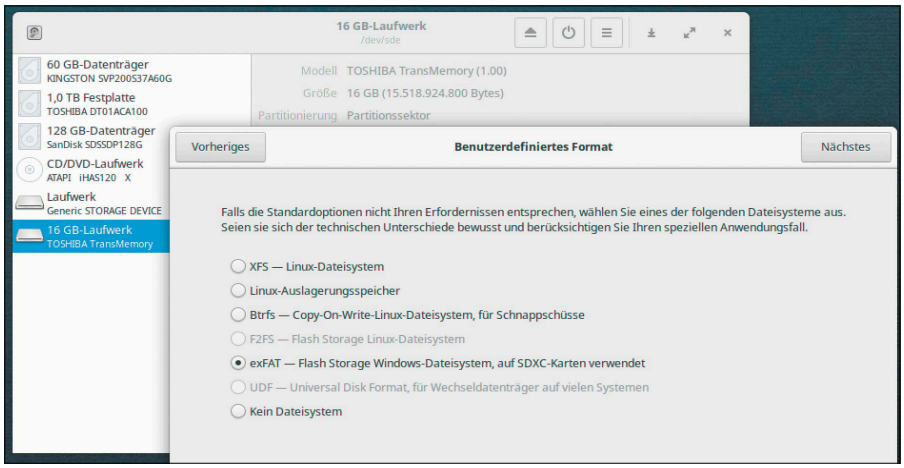
• Für interne oder externe Laufwerke, die für den unkomplizierten Datenaustausch dienen sollen, eignet sich im einfachsten Fall eine Formatierung mit dem alten FAT32, das alle Systeme ohne Hilfsmittel beherrschen und auch selbst formatieren können.

• Wer ISO-Images und Filme austauschen will, sollte die maximale Dateigröße von nur vier GB unter FAT32 bedenken. In diesem Fall kommt das Microsoft-Dateisystem exFAT in Betracht. Linux beherrscht exFAT zwar nicht standardmäßig, aber die Nachinstallation des kleinen exFAT-Treibers ist mittels des Kommandos

```
sudo apt install exfat-fuse exfat-
  utils
```

im Handumdrehen erledigt. Danach können Sie exFAT-Datenträger sofort mit Linux-Dateimanagern nutzen und mit Werkzeugen wie Gnome-Disks („Laufwerke“) auch mit exFAT formatieren („Partition formatieren → Andere → exFAT“). Gparted hat exFAT zwar in seiner Dateisystemliste, will aber bislang nicht mit exFAT formatieren (inaktiv).

• Sind nur Linux- und Windows-Rechner im Spiel, ist das Microsoft-Standarddateisystem NTFS erste Wahl. Linux wie Windows haben dort Lese- und Schreibzugriff, Linux wie Windows können mit NTFS formatieren. Mac-OS X kann darauf standardmäßig nur lesen.



exFAT unter Linux: Das einfache Microsoft-Dateisystem (ohne Dateirechte) überwindet das Vier-GB-Limit von FAT32 für einzelne Dateien und ist unter Linux umstandslos nachzurüsten.

Kontinuität beim Mailprogramm

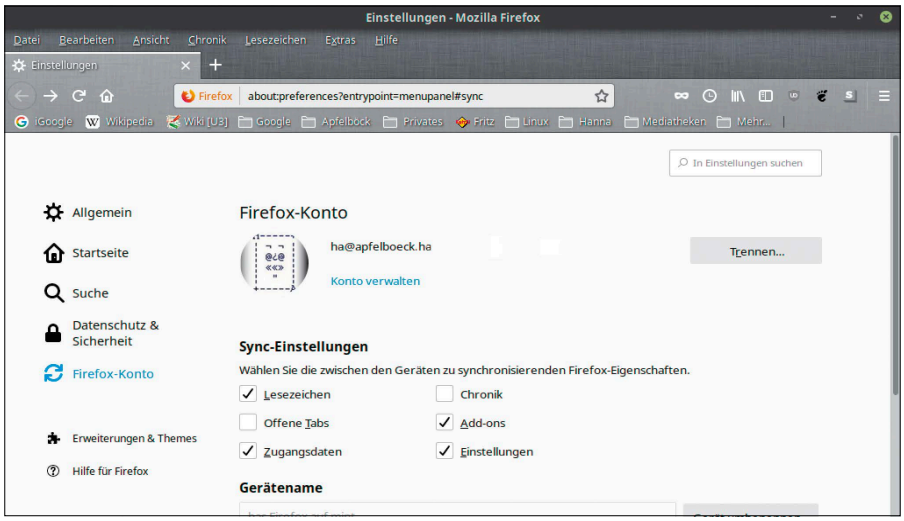
Wer seine Mails im Browser liest und schreibt (Webmailer), muss sich nicht umstellen. Nicht viel anders liegt der Fall, wenn Sie zwar ein lokales Mailprogramm, dort aber statt POP3 das IMAP-Protokoll verwenden. Dann liegen alle Mails auf dem Server und es genügt im jeweiligen Betriebssystem das Einrichten des IMAP-Kontos.

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

Thunderbird kann auch aushelfen, um die Daten zunächst aus Microsoft Outlook zu importieren. Diese Option bietet das Mailprogramm beim Setup automatisch an. Danach können Sie das Thunderbird-Profil – wie oben beschrieben – nach Linux transportieren.

Uneingeschränkte Kontinuität im Browser

Die unter Windows wie Linux populären Browser Chrome/Chromium und Firefox sind praktisch funktionsgleich. Außerdem machen sie es dem Nutzer einfach, Browsereinstellungen, Webkennwörter, Themes und Lesezeichen automatisch von Windows



Auf jedem Rechner derselbe Browser mit denselben Einstellungen: Firefox und Chrome bieten plattformübergreifend identische Funktionalität und Einstellungen via Sync-Service.

nach Linux zu übernehmen. Voraussetzung ist nur, dass Sie zunächst unter Windows die Browsersynchronisierung aktivieren und dies dann unter Linux mit demselben Browser wiederholen:

Für **Google Chrome / Chromium** brauchen Sie nur ein Google-Konto. Über das Menü „Einstellungen“ oder die Adresse „chrome://settings/“ können Sie sich „In Chrome anmelden“ und dann den Umfang der Synchronisierung bestimmen. Alles zu synchronisieren ist am bequemsten. Danach erhält jeder Browser Chrome/Chromium, den Sie unter Windows oder Linux auf diese Weise einstellen, dieselben Lesezeichen, Erweiterungen, Designs.

Firefox bietet die Synchronisierung unter „Firefox → Einstellungen → Sync“. Sie benötigen ein Konto auf dem Mozilla-Server und wählen daher „Firefox-Sync einrichten“, anschließend „Neues Benutzerkonto anlegen“. Beim Firefox am Linux-Rechner wählen Sie unter „Einstellungen → Sync → Firefox-Sync einrichten“ die Optionen „Ich habe ein Benutzerkonto“ und „Ich habe das Gerät nicht bei mir“. Dann geben Sie die Firefox-Sync-Kontodaten ein.

Word, Excel und Libre Office

Das auf größeren Distributionen standardmäßig installierte Libre Office (Paketname „libreoffice“) lädt und bearbeitet mit Ausnahme von Access-Datenbanken im Prinzip alle Dateien, die mit altem und neuem Microsoft Office erstellt wurden (97 bis 2019). Wo diese Suite noch nicht vorliegt, sollte das mittels

```
sudo apt install libreoffice
  libreoffice-l10n-de libreoffice-
  help-de
```

auf jedem Desktop-Linux unbedingt korrigiert werden (im Beispiel gleich mit deutscher Oberfläche und Hilfe). Hundertprozentige Kompatibilität mit Microsoft Office ist aber nicht erreichbar. Word, Excel und Powerpoint bieten etliche Formate, mathematische Funktionen, Diagrammtypen oder Übergangseffekte, die Libre Office nicht kennt. Korrigierbare kleinere Probleme gibt es bei Tabellen und Bildern, ferner bei Inhaltsverzeichnissen in der Textverarbeitung. Pivot-Tabellen in der Tabellenkalkulation und neuere Videofunktionen von Powerpoint sind ebenfalls nicht voll kompatibel. Bei nur lesender Nutzung sind diese kleinen Inkompatibilitäten kein Problem, bei der Weiterbearbeitung müssen Sie aber gegebenenfalls nachbessern.

Einige generelle Maßnahmen können den Korrekturaufwand verringern: Libre Office kommt mit den älteren Binärformaten (DOC, XLS, PPT) besser zurecht als mit dem jüngeren Office Open XML (OOXML) von Microsoft Office ab Version 2007.

Daher ist es klug, Austauschdateien in Microsoft Office im älteren „97-2003“-Format zu speichern und so an Libre Office weiterzugeben. Um die Kompatibilität zwischen den Office-Suiten zu erhöhen, gibt es in Libre Office unter „Extras → Optionen“ eine Reihe von Einstellungen: Standardmäßig sollten alle Optionen unter „Laden/Speichern → Microsoft Office“ aktiviert sein. Dasselbe gilt für alle Optionen unter „Laden/Speichern → VBA-Eigenschaften“: VBA-Makros sind zwar nicht kompatibel, aber diese Einstellungen bewahren immerhin eventuelle Makros in MS-Office-Dokumenten. Ferner finden Sie noch den Punkt „LibreOffice Writer → Kompatibilität“: Die hier angebotenen Optionen eignen sich zum Experimentieren, wenn der Austausch von Textdokumenten Probleme verursacht.

Jüngeres Microsoft Word, Excel und Powerpoint liest und bearbeitet seinerseits die von Libre Office erstellten Formate ODT, ODS, ODP praktisch klaglos. Es ist also durchaus praktikabel, diese Linux-Formate ohne Konvertierung direkt an Windows-Nutzer weiterzugeben.

Multimedia-Dateien unter Linux

Populäre Bildformate, Musikformate und Videos sind plattformunabhängig und verursachen keine Probleme beim Austausch zwischen Windows und Linux.

Bildformate: Pixelgrafiken wie JPG- oder PNG-Fotos sind generell problemlos. Vorinstallierte Bildviewer wie eog (Eye of Gnome, „Bildbetrachter“) oder gthumb kennen alle gängigen Formate.

Diese reinen Viewer genügen für Alltagsansprüche mit Thumbnailübersicht, Diashow und einfachsten Darstellungsfunktionen wie Drehen der Bilder. Zusätzliche Bearbeitungsfunktionen und eine Datenbank zur Bildverwaltung bietet Shotwell (so auch der Paketname), das unter Ubuntu zum Standard gehört.

Das SVG-Format, das insbesondere für Diagramme genutzt wird, können die Programme Libre Office Draw, Inkscape und Gimp öffnen und bearbeiten. Bei proprietären Formaten von Adobe Photoshop, Adobe Illustrator, Corel Draw ist hingegen unter Linux mit Gimp und Inkscape mit gelegentlichen Detailfehlern zu rechnen.

Gimp – mit gleichlautendem Paketnamen – ist bei einigen Desktopdistributionen Standard. Die anspruchsvolle Bildbearbeitung beherrscht sämtliche verbreiteten Bildformate, auch PSD-Photoshop oder Postscript (PS und EPS).

Wenn Sie bearbeitete Gimp-Bilder nicht im eigenen XCF-Format, sondern etwa im Photoshop-Format weitergeben möchten, müssen Sie in Gimp das Menü „Datei → Exportieren“ verwenden.

Eine Ergänzungssoftware ist der Bildviewer Xnview MP, der auch exotische Bildformate (insgesamt 500) beherrscht und unter Win-

dows wie unter Linux zu Hause ist. Das deb-Installationspaket für Debian-basierte Systeme (Ubuntu, Mint & Co.) muss über die Herstellerseite (*www.xnview.com*) heruntergeladen und dann installiert werden.

Musikformate: Ob MP3, WMA, FLAC, AAC, WAV oder OGG – die Standardplayer der einzelnen Linux-Distributionen spielen alles ab. Die Frage ist daher eher, ob der Umfang des Standardplayers genügt: Ein Multitalent ist Banshee (gleichnamiger Paketname), der alle Audioformate abspielt und eine Medienverwaltung mitbringt. Wer gleichzeitig Windows nutzt, kann den plattformübergreifenden Player auch dort verwenden. Dasselbe gilt auch für den multifunktionalen VLC, der neben Video und Film auch alle gängigen Musikformate abspielt.

Midi-Dateien sind praktisch nur für Musikproduzierende relevant. Zum Abspielen bestehender Midi-Daten genügt das Tool Timidity (mit gleichnamigem Paketnamen), für die Midi-Erzeugung sind unter Linux die Programme Musescore und Rosegarden erste Wahl (mit gleichnamigen Paketnamen).

Videos und DVDs: Wo immer Videos und Filme genutzt werden und die Allzweckwaffe VLC nicht vorinstalliert ist, sollten Sie dies mit *sudo apt install vlc* nachholen. Kein anderer Player besitzt die Fehlertoleranz und den Funktionsumfang des plattformübergreifenden VLC. Mit aktiviertem libdvd spielt der VLC-Player auch DVDs ab. Die DVD-Komponente laden Sie mit

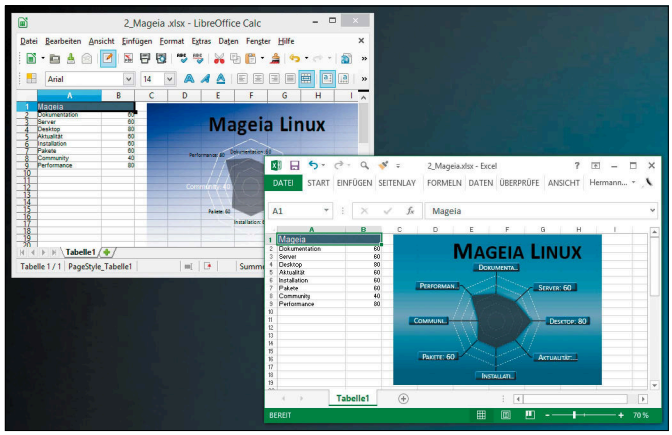
```
sudo apt install libdvd-pkg
```

nach und erledigen d die eigentliche Installation mit diesem Befehl

```
sudo dpkg-reconfigure libdvd-pkg
```

unter Debian-basierten Systemen wie Ubuntu und Linux Mint.

Vollständige Office-Kompatibilität ist nicht erreichbar: Bei etlichen Funktionen, Diagrammen, Verweisfunktionen oder Formatierungen muss Libre Office nachbearbeiten oder vereinfachen.



PDF, RTF, Text, Epub und Packerarchive

Für PDF-Dateien ist in vielen Distributionen ein standardmäßig installierter „Dokument-Betrachter" wie Evince (Gnome) oder Okular (KDE) zuständig. Die pure PDF-Anzeige beherrscht heute außerdem jeder Browser wie Firefox oder Chrome.

Beachten Sie, dass PDF-Dateien mit Libre Office Draw auch bearbeitet werden können. Dessen Möglichkeiten sind zwar weit entfernt vom kostenpflichtigen Windows-Programm Adobe Acrobat, genügen aber für Textkorrekturen. Außerdem können alle Libre-Office-Komponenten standardkonforme PDFs exportieren („Datei → Exportieren als → Als PDF...").

Während für das RTF-Format Libre Office (Writer) zuständig ist, lesen und bearbeiten Sie puren Text, Codedateien oder HTML mit dem jeweiligen Editor der Linux-Distribution (Gedit, Xed, Leafpad u. a.).

Für das elektronische Buchformat Epub, das unter Windows standardmäßig der Browser Edge wiedergibt, ist unter Linux in der Regel kein Standardprogramm installiert: Hier hilft als große Lösung die Nachinstallation des Programms Calibre (mit gleichnamigen Paketnamen), für gelegentliches Lesen eines Epub-Textes reicht aber auch die Browsererweiterung „ePubReader" (Sevina), die für Firefox und Chrome/Chromium identisch vorliegt.

ZIP, RAR, CAB: Für gepackte Archive aller Art gibt es die „Archivverwaltung" – unter Gnome-affinen Desktops der „File-Roller", unter KDE das Tool „Ark". Diese Tools beherrschen die Linux-typischen Archive wie TAR und GZ ebenso wie die unter Windows verbreiteten Formate ZIP und RAR, können darüber hinaus auch ISO-Images und Windows-CAB-Dateien verarbeiten. Das ebenfalls populäre Packerformat 7-Zip ist allerdings nicht standardmäßig an Bord, obwohl es für Imagedateien und den Archivaustausch mit Windows eine wichtige Rolle spielt. Mit dem Befehl

```
sudo apt install p7zip-full
```

rüsten Sie die Komponente schnell nach. Der Packer wird bei der Installation automatisch in die grafische Archivverwaltung integriert. ■

GROSS-/KLEINSCHREIBUNG UND SONDERZEICHEN

Unter Windows spielt die Schreibung weder bei Dateinamen noch bei Befehlen eine Rolle. „DIR" ist dasselbe wie „dir" oder „diR". Unter Linux ist genaue Schreibung zwingend: Den Befehl „LSBLK" gibt es nicht und ein Schalter „-X" bedeutet etwas anderes als „-x". Folgerichtig können in einem Ordner auf einem Linux-Dateisystem Dateiobjekte wie „Musik", „musik" und „MUSIK" nebeneinander existieren. Windows wird in solchen Fällen nur ein inhaltliches Ziel finden, egal, welches der drei Objekte Sie anklicken. Das Problem kann nur bei einem Samba-Server auftreten, weil auf einem Austauschdatenträger mit FAT32, exFAT oder NTFS das Dateisystem solche Namensgleichheit verbietet – auch für Linux. Weitere Unterschiede betreffen Sonderzeichen im Dateinamen: Windows-Umsteiger, die Dateien via Samba zwischen Linux und Windows austauschen wollen, werden früher oder später auf „Fehler beim Kopieren" treffen. Das kann ein Rechteproblem sein, kann aber auch die viel trivialere Ursache haben, dass der Dateiname nicht Windows-konform ist. Doppelpunkt (:), Längsstrich (|) Anführungszeichen („), Fragezeichen (?) und Backslash (\) sind in Dateinamen unter Linux erlaubt, unter Windows nicht – und führen zu besagten Fehlern. Einfach die Datei unter Linux umbenennen und das Problem ist gelöst.

Programme für Umsteiger

Wer unter Windows Firefox und Libre Office nutzt, muss sich beim Wechsel auf Linux kaum umgewöhnen. Trotzdem ist einiges anders und nicht für jede bisher genutzte Anwendung gibt es eine gleichwertige Alternative.

VON THORSTEN EGGELING



Schlüsselfertiges Betriebssystem: Linux-Distributionen richten die wichtigsten Anwendungen bereits bei der Erstinstallation ein. Textverarbeitung und Bildverwaltung sind schon dabei.

Wie gut der Umstieg von Windows auf Linux gelingen kann, hängt auch von der bisher genutzten Software ab. Das Spektrum beginnt beim gelegentlichen PC-Nutzer, der hauptsächlich den Browser und ab und zu eine Bildbearbeitung für die Urlaubsfotos verwendet. Auf dem typischen Büro-PC wird ausgiebig von Textverarbeitung und Tabellenkalkulation Gebrauch gemacht, hinzu kommen eventuell noch Buchhaltungsprogramme oder Software für die Steuererklärung. Der Poweruser bearbeitet Bilder mit Adobe Photoshop, schneidet Videos mit Adobe Premiere und installiert Unmengen von Software, die sich für Windows aus dem Internet herunterladen lässt.

Windows hat für alle genannten Nutzergruppen etwas Passendes zu bieten, Linux nur teilweise. Außerdem sind die Zielgruppen andere. Linux eignet sich eher für Personen, die auch ohne spezielle Software auskommen, die bereit sind, sich umzugewöhnen, oder die sich einfach gerne mit Linux beschäftigen möchten. Auf der anderen Seite stehen Benutzer, die Serverdienste (SSH, Apache, Samba) benötigen, und die dann bei Linux besser aufgehoben sind als bei Windows.

Wer unter Windows vor allem Open-Source-Software einsetzt, sollte auch mit Linux keine Probleme haben. Die unterschiedlichen Softwareangebote für Linux und Windows sind ansonsten nur schwer vergleichbar. Am einfachsten ist es, die Linux-Anwendungen einfach auszuprobieren und sich dann zu entscheiden.

1. Programme für alle Benutzer

Linux-Distributionen wie Ubuntu oder Linux Mint bieten direkt nach der Installation die wichtigsten Anwendungen für die meisten Benutzer. Als Office-Paket ist Libre Office vorhanden (siehe Punkt 2), Firefox ist der Standard-Webbrowser und für E-Mail gibt es Thunderbird.

Umsteiger von Windows auf Ubuntu 18.04 oder später haben unter Umständen Probleme, die installierten Anwendungen überhaupt zu finden. Die Starterleiste am linken Bildschirmrand zeigt nur Icons beispielsweise für Firefox, Libre Office Writer, Rhythmbox und den Dateimanager. Ein Klick auf „Aktivitäten“ ermöglicht die Suche nach Anwendungen und Tools, deren Namen man kennt. Das unscheinbare Symbol in der Starterleiste ganz unten hilft weiter. Nach einem Klick darauf zeigt Ubuntu die Icons der häufig genutzten Programme und nach einem Klick auf „Alle“ jede installierte Anwendung für die grafische Oberfläche. Es lassen sich dann beispielsweise die Tabellenkalkulation Libre Office Calc, die Fotoverwaltung und Fotobearbeitung Shotwell (siehe Punkt 3) oder der Player Videos starten. Ist ein Programm aktiv, sehen Sie sein Icon in der Starterleiste. Nach einem rechten Mausklick erscheint ein Menü, in dem Sie auf „Zu Favoriten hinzufügen“ gehen können. Das Programmsymbol bleibt dann in der Leiste und die Anwendung lässt sich darüber später schneller starten.

Linux Mint 19 bietet eine ähnliche Ausstattung. Das Startmenü erinnert an Windows 7 und führt Umsteiger wie gewohnt zu den gewünschten Programmen. Firefox, Thunderbird und Libre Office sind vorinstalliert. Unter „Zubehör“ finden Sie Taschenrechner, Screenshottool und Textbearbeitung.

2. Programme für den Büro-PC

Libre Office bietet einen großen Funktionsumfang, der für die meisten privaten Anwender ausreicht. Die Suite enthält die Textverarbeitung Writer, die Tabellenkalkulation Calc, das Präsentationsprogramm Impress und das Zeichenprogramm Draw. Das Datenbankmodul Base lässt sich über die Paketverwaltung nachinstallieren.

Die Bedienung über Menüs und der Funktionsumfang erinnern an Microsoft Office 2003. Microsoft Office 365 sieht im Vergleich moderner aus, auch wenn die Bedienung über das Menüband nicht nach jedermanns Geschmack ist. Komfortfunktionen wie „Designs“ mit Livevorschau im aktuellen Dokument gibt es beispielsweise in Libre Office Writer nicht und der Tabellenkalkulation fehlen etliche Rechenoptionen von Excel.

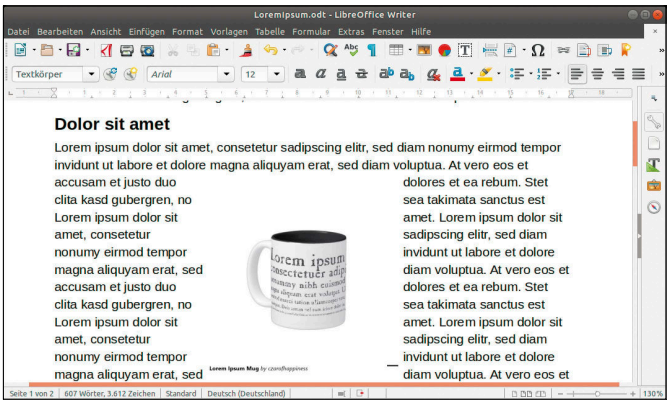
Wer gelegentlich einen Brief schreibt oder Finanzberechnungen macht, wird in Libre Office kaum etwas vermissen. Probleme sind zu erwarten, wenn Sie häufig Dokumente mit Nutzern von Microsoft Office austauschen müssen. Die Import- und Exportfilter werden zwar ständig verbessert, die Übernahme aller Formatierungen ist vor allem bei komplexeren Dokumenten jedoch nicht garantiert.

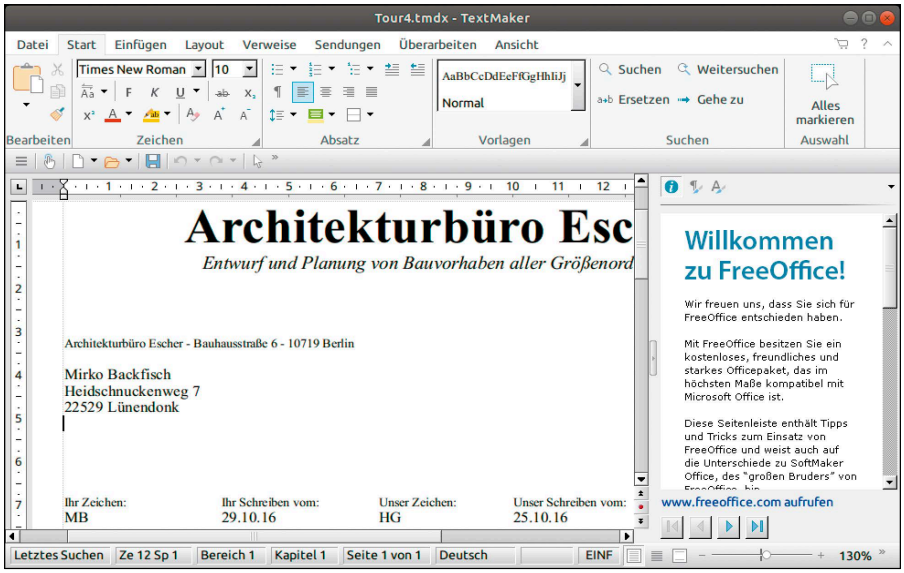
Mehr Kompatibilität zu Microsoft-Produkten verspricht Softmaker Office (*www.softmaker.de*). Die Importfilter sind besser als jene von Libre Office, wenn auch nicht perfekt. Wer das ausprobieren möchte, kann sich bei Softmaker eine kostenlose 30-Tage-Demo herunterladen. Die Vollversion Softmaker Office Standard 2018 kostet 79,95 Euro. Für 99,95 Euro gibt es Softmaker Office Professional 2018, das mit dem Duden Korrektor eine besonders leistungsfähige Rechtschreibprüfung enthält.

Außerdem können Sie die Gratisversion Free Office nutzen, die aber keine Microsoft-XML-Formate speichern kann (*www.freeoffice.com*). Die Speicherformate „.doc“ und „.xls“ stehen jedoch für den Datenaustausch zur Verfügung.

Wer Broschüren oder Zeitschriften layouten möchten, greift unter Windows zu Adobe Indesign oder Quark Xpress. Vergleichbare Desktop-Publishing-Programme gibt es für Linux nicht. Für den Hobbylayouter genügt aber Scribus (*www.scribus.net*), das sich über die Paketverwaltung installieren lässt. Das Programm beherrscht den professionellen Textsatz und kann Dokumente so für den Druck vorbereiten, dass auch die Farben stimmen (CMYK-Farbseparation).

Office-Paket: Libre Office Writer kann zwar nicht ganz mit Microsoft Word mithalten, bietet aber für die meisten privaten Nutzer ausreichende Funktionen.





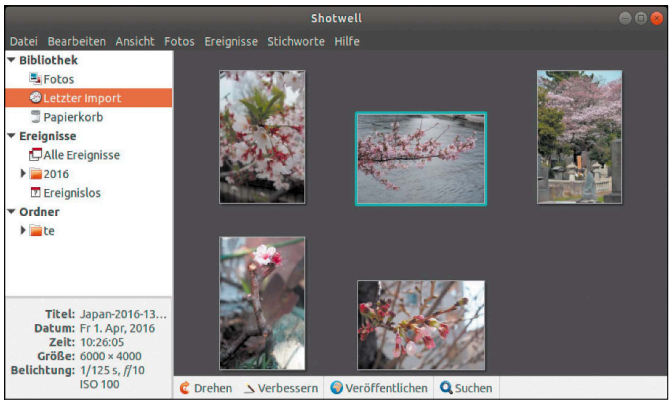
Textmaker: Softmaker Office gibt es auch in einer kostenlosen Version. Leistungsfähige Importfilter für die Microsoft-XML-Formate bietet aber nur die Bezahlversion des Programms.

3. Fotoverwaltung und Bildbearbeitung

Das bei Ubuntu standardmäßig installierte Shotwell ist eine einfache Fotoverwaltung. Bilder lassen sich mit Stichwörtern versehen und bewerten, was die Basis für die schnelle Anzeige von Bildern aus der gleichen Kategorie und für Ansichtsfilter bildet. Shotwell bietet einfache Bearbeitungsfunktionen wie „Zuschneiden“ oder „Rote-Augen-Effekt“.

WINDOWS-PROGRAMME UNTER LINUX NUTZEN

Wer spezielle Windows-Programme benötigt, kann eine Windows-Installation im Dualboot neben Linux auf dem gleichen PC verwenden. Eine bessere Lösung bietet jedoch Virtualisierungssoftware wie Virtualbox. Windows-Programme stehen damit jederzeit zur Verfügung, ohne dass Sie den PC neu starten müssen. Der Nachteil: Auch für ein virtualisiertes Windows benötigen Sie einen Lizenzschlüssel von Microsoft. Wer Windows nur gelegentlich startet, verwendet die Enterprise-Version von Windows 10 kostenlos für einen 90-Tage-Test(*www.pcwelt.de/k2mNT9*). Welche Voraussetzungen Ihr PC erfüllen muss, wie Sie die aktuelle Virtualbox-Version unter Linux installieren und Windows 10 darin einrichten, lesen Sie unter *www.pcwelt.de/2111217*.



Fotos verwalten: Shotwell bietet ausreichende Funktionen für die Organisation von Urlaubsbildern. Mit Tools wie „Drehen“ oder „Anpassen“ lassen sich die Fotos auch bearbeiten.

Mit Digikam lassen sich Fotos (*www.digikam.org*) nach Alben, Tags oder Stichwörtern sortieren beziehungsweise kategorisieren. Es stehen zahlreiche Tools für die Fotobearbeitung zur Verfügung, etwa Tonwertkorrektur, Rote-Augen-Korrektur oder Rahmenbearbeitung. Auch eine Unterstützung von Fotos in RAW-Formaten ist vorhanden: Digikam kann nicht nur die eingebettete Vorschau anzeigen, sondern RAW-Dateien in der Vorschau öffnen. Wer Fotos im RAW-Format bearbeiten möchte, greift zu Darktable oder Rawtherapee. Alle genannten Programme lassen sich über die Paketverwaltung installieren.

Die Zielgruppe von Gimp (*www.gimp.org*) sind Benutzer, die unter Windows Photoshop einsetzen. Das Programm bietet Malwerkzeuge, Ebenen, Masken, Automatikverbesserung und etliche Filter. Sie können damit Fotos retuschieren, Bilder freistellen oder verfremden. Wie bei Photoshop erschließen sich die meisten Funktionen nicht auf Anhieb. Bestimmte Effekte sind nur durch eine geeignete Kombination von Masken und Ebenen zu erreichen.

Da Gimp jedoch weit verbreitet ist und viel genutzt wird, finden Sie im Internet ausreichend Unterstützung.

Ein guter Startpunkt ist die Dokumentation unter *www.gimp.org/docs*. Gimp ist in den Standard-Repositorien von Ubuntu und Linux Mint enthalten. Neuere Versionen lassen sich unter Ubuntu als Snap-App installieren.

4. Player für Audio & Video

Bei Ubuntu heißt der Videoplayer „Videos“ (Totem Video Player), bei Linux Mint „Medienwiedergabe“ (Xplayer). Den Programmen ist gemeinsam, dass sie das Multimedia-Framework Gstreamer benutzen. Gstreamer stellt eine Infrastruktur zur Verfügung, über die sich Audio- und Videodateien abspielen beziehungsweise codieren und decodieren lassen.

Anwender müssen sich um die Details in der Regel nicht kümmern. Sobald Sie eine Multimedia-Datei über den Dateimanager öffnen, startet der passende Player. Wenn Ubuntu oder Linux Mint das Dateiformat bisher unbekannt ist, fordert der Player die Installation der nötigen Gstreamer-Module (Codecs) automatisch an.

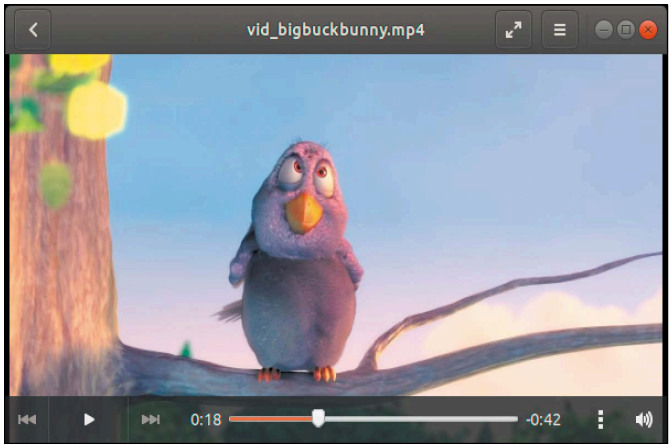
Wenn Ihnen diese Standardplayer nicht gefallen oder der Funktionsumfang nicht ausreicht, installieren Sie den verbreiteten VLC Media Player (*www.videolan.org*). Das Programm bringt eigene Codecs mit und spielt alle gängigen Medienformate ab. Eine weitere Alternative ist Smplayer (*http://smplayer.sourceforge.net*). Dieses grafische Front-End für Mplayer hält den gesamten Funktionsumfang von Mplayer bereit. Wichtige Audio- und Videocodecs hat Smplayer ebenfalls bereits mit an Bord. Beide Programme sind in den Standard-Repositorien von Ubuntu und Linux Mint zu finden.

5. Videoeditoren für Linux

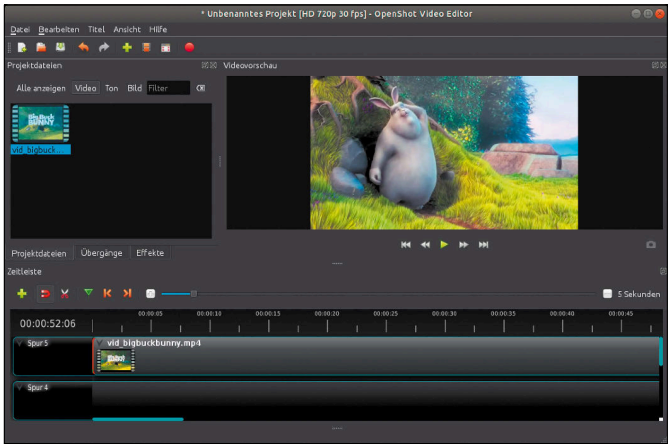
Openshot ist ein funktionsreicher und trotzdem für Einsteiger verständlicher Videoeditor (*www.openshot.org*). Sie importieren das ungeschnittene Rohmaterial zunächst in eine Projektdatei. Aus der Liste der Projektelemente ziehen Sie dann die einzelnen Bestandteile auf die Zeitleiste. Das Schneiden und Trimmen ist intuitiv gelöst. Sie zerteilen einen Clip und können dann nach Rechtsklick auf den jeweiligen Teil über das Kontextmenü den Abschnitt löschen oder verschieben.

Neben den Schnittfunktionen stehen eine Reihe von Übergängen zur Verfügung. Sie wählen den gewünschten Effekt aus der Liste und ziehen ihn auf die entsprechende Spur. Über das Kommando „Datei → Video exportieren“ und die Auswahl eines Profils geben Sie die geschnittene Fassung in eine neue Datei aus.

Weitere Videoeditoren für Linux sind Pitivi und Kdenlive. Pitivi (*www.pitivi.org*) ähnelt in



Filme ansehen: Die Standardplayer von Ubuntu und Linux Mint bieten nur Basisfunktionen. Wer mehr will, greift zum VLC Media Player oder Smplayer.



Videos bearbeiten: Openshot schneidet Videos. Es gibt mehrere Spuren und Sie können Videotitel und Übergänge erzeugen sowie Effekte einbauen.

Bedienung und Funktionsumfang Openshot. Kdenlive (*https://kdenlive.org*) bietet mehr Funktionen, benötigt dafür aber auch mehr Einarbeitungszeit.

Alle genannten Programme lassen sich über die Paketverwaltung in Ubuntu und Linux Mint installieren. Auf den Seiten der Hersteller gibt es auch neuere Versionen – in der Regel als Appimage, Snap-App oder Flatpak. Wer Videos nur in andere Formate umwandeln möchte, verwendet dafür Handbrake oder Avidemux. Ausführliche Infos dazu finden unter *www.pcwelt.de/1802166*.

6. Software für das Internet

Firefox ist einer der beliebtesten Browser und glänzt vor allem durch seine Erweiterbarkeit über Add-ons. Das Programm geht jedoch nicht besonders sparsam mit dem Hauptspeicher um, was vor allem bei vielen geöffneten Tabs das System ausbremsen kann. Der Browser schneidet bei Geschwindigkeitstests gut ab, aber andere können es noch besser – beispielsweise Chromium (*www.chromium.org*), der Open-Source-Ableger von Google Chrome. Der Ressourcenverbrauch ist geringer als bei Firefox, die Geschwindigkeit in einigen Bereichen höher. Die Unterschiede von Chromium im Vergleich zu Google Chrome sind gering. Sie



Schlanker Browser: Wer auf Firefox-Add-ons verzichten kann, findet in Chromium einen schnellen Webbrowser, der sparsamer mit den Systemressourcen umgeht.

betreffen einige Einstellungen, Codecs sowie die Erweiterungen für Adobe Flash und PDF. Chromium ist in den Standard-Paketquellen von Ubuntu und Linux MInt enthalten. Es gibt jedoch auch Gründe, Google Chrome zu installieren (*www.google.de/chrome*). Einer davon ist das Angebot von Amazon Video, das HTML5-Videos nur in Google Chrome, aber nicht in Chromium anzeigt. Google bietet ein eigenes Repository für Ubuntu an. Infos zu dem Thema finden Sie unter *www.pcwelt.deZ2174471*.

Wer gerne per Chat kommuniziert oder ein bewegtes Bild des Gegenüber sehen will, kann auch unter Linux Skype installieren. Aktuelle „deb"- und RPM-Pakete sowie eine Snap-App gibt es bei Microsoft zum kostenlosen Download (*www.pcwelt.de/P3BHbX*). Wenn Sie Open-Source-Software bevorzugen, installieren Sie die Messenger Pidgin oder KDE-Telepathy. Beide unterstützen Netzwerkprotokolle wie ICQ, MSN, Jabber und Google Talk und lassen sich direkt über die Paketverwaltung installieren. ■

SOFTWARE AUS DEM QUELLTEXT KOMPILIEREN

Ein Kompilat aus dem Quelltext ist nur erforderlich, wenn es kein PPA oder eine andere Downloadquelle für die gewünschte Software gibt.

Dank App-Image, Snap-Apps und Flatpak ist das inzwischen nur noch selten erforderlich. Ein eigener Build kann jedoch weiterhin aus Sicherheitsgründen wünschenswert sein. Nur so stellen Sie sicher, dass eine Software tatsächlich dem Quelltext entspricht und nicht manipuliert wurde.

Sie benötigen keine Programmierkenntnisse, aber den souveränen Umgang mit der Kommandozeile und unter Umständen ausreichende Englischkenntnisse für die Lektüre der Dokumentation.

Ein allgemeines Rezept für die Erzeugung von Binärdateien aus dem Quellcode gibt es nicht, unser Beispiel für Ubuntu 18.04 zeigt jedoch einige grundsätzlichen Schritte.

Wer die Verschlüsselungssoftware Veracrypt (*www.veracrypt.fr*) selbst kompilieren möchte, installiert zuerst die nötigen Entwicklertools

```
sudo apt install git build-essential yasm libfuse-dev
  pkg-config libgtk2.0-dev libcppunit-dev
  libwxgtk3.0-dev makeself
```

Welche Entwicklerpakete („*-dev") erforderlich sind, ermitteln Sie in der Beschreibung der jeweiligen Software. Danach erstellen Sie ein Arbeitsverzeichnis, laden den Quellcode herunter und starten den Buildvorgang (sechs Zeilen):

```
mkdir ~/src
cd ~/src
wget -q -O - https://github.com/wxWidgets/wxWidgets/
  releases/download/v3.0.4/wxWidgets-3.0.4.tar.bz2
  | tar xvjf -
git clone https://github.com/veracrypt/VeraCrypt.git
cd ~/src/VeraCrypt/src/Build
sudo ./build_veracrypt_linux.sh
```

Nach Abschluss des Buildvorgangs liegen die Installerpakete im Ordner „~/src/VeraCrypt/src/Setup/Linux". Zur Installation starten Sie in diesem Verzeichnis diesen Befehl:

```
sudo ./veracrypt--CustomEFI-setup-gui-x64
```

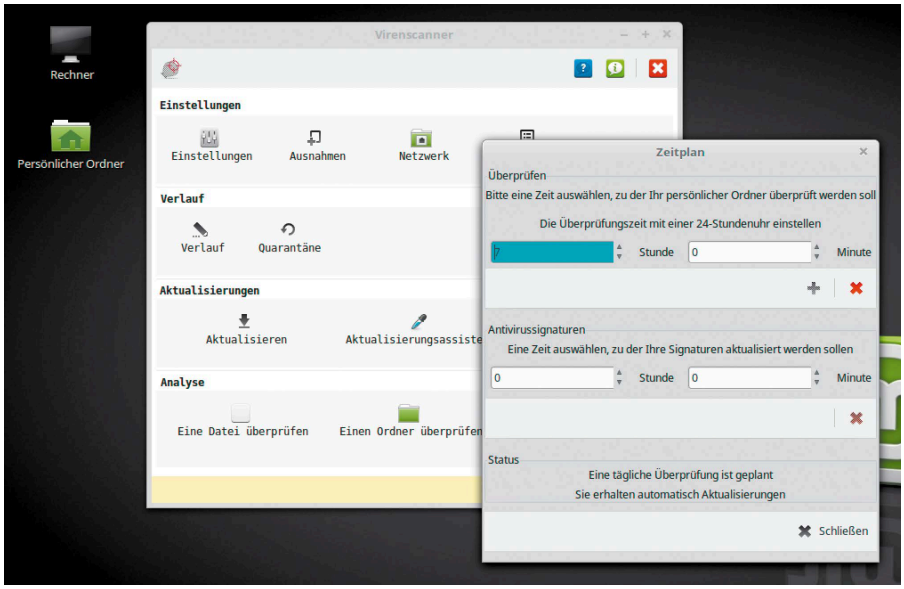
Ganz typisch ist die Vorgehensweise bei Veracrypt nicht. Die meisten Entwickler bieten kein spezielles Build-Script an. Meist gibt es das Script „configure", das die Voraussetzungen prüft. Mit *make* wird das Programm kompiliert und danach mit *sudo make install* installiert.

Viren finden und beseitigen

Die Bedrohungslage ist bei Linux mehr als entspannt. Aufgrund der Architektur und seiner deutlich geringeren Verbreitung haben Virenentwickler mit dem System ihre Mühe. Das bedeutet aber nicht, dass Viren für Linux-Anwender gar keine Rolle spielen.

VON STEPHAN LAMPRECHT

Windows-Schädlinge können Linux nichts anhaben oder nicht beschädigen. Aber natürlich können sie auch unter Linux vorkommen. Auf einem Linux-NAS in einer gemischten Netzwerkumgebung können früher oder später auch Windows-Viren liegen, die sich beim Abruf der infizierten Datei auch auf andere Clients verbreiten. Deswegen ist es ratsam, Linux-Server regelmäßig auf Viren zu überprüfen, sofern dort auch Windows-Rechner zugreifen.



Das Open-Source-Programm Clam-AV, für das es auch grafische Oberflächen gibt, ist der meistverbreitete Virenscanner unter Linux.

Das Linux-System regelmäßig scannen

Der Klassiker für diese Aufgabe ist Clam-AV. Der Scanner wird auch für Linux angeboten. Das Programm ist in den Paketquellen aller bekannten Distributionen vorhanden und mit wenigen Klicks installiert. Wie bei allen Virenscannern gilt auch hier, dass die Signaturdateien regelmäßig aktualisiert werden müssen. Das übernimmt ein spezielles Programm, das Sie in einem Terminal mittels des Befehls

```
sudo freshclam
```

manuell aufrufen. Üblicherweise wird aber ein Daemon installiert und gestartet, der in regelmäßigen Abständen automatisch nach neuen Signaturdateien Ausschau hält. Clam-AV ist so flexibel, dass es eine ganze Reihe von Möglichkeiten gibt, das Scannen zu automatisieren und zu steuern. Auch die Einbindung in eigene Anwendungen ist möglich. Hier hilft ein Blick in die umfangreiche Dokumentation des Projekts, die auch die zahlreichen Optionen beim Funktionsaufruf erklärt. Denn das Programm kann wahlweise den Nutzer nur über gefundene Viren informieren oder betroffene Dateien auch verschieben.

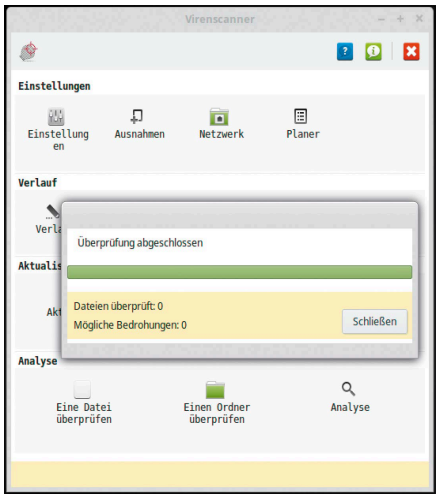
Ein einfacher und schneller Weg, den Prozess zu automatisieren, besteht im Anlegen eines Shell-Scripts, das lediglich aus dem Funktionsaufruf des Programms besteht. Dieses Script können Sie dann in die Crontabelle des Systems im gewünschten Intervall eintragen. Der Aufruf selbst könnte dann so aussehen:

```
sudo clamscan -r --move=VERZEICHNIS0
  VERZEICHNIS1 VERZEICHNIS2
```

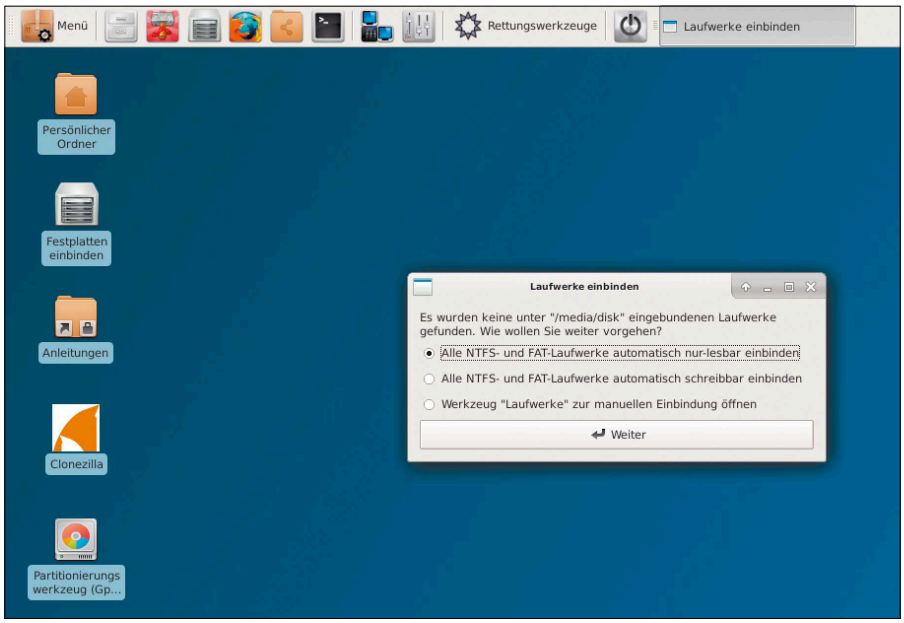
In diesem Fall untersucht die Software die Ordner „Verzeichnis1“ und „Verzeichnis2“ rekursiv (Schalter „-r“), also inklusive aller Unterordner. Jede verdächtige Datei wird in das Verzeichnis verschoben, das Sie hinter „--move=“ angeben. Es gibt auch einen Schalter, um eine Datei automatisch zu löschen. Damit sollten Sie aber vorsichtig sein, da ja Fehlalarme nicht immer auszuschließen sind.

Linux als Windows-Helfer

Linux ist auch die perfekte Unterstützung, wenn es darum geht, Windows-Systeme zu untersuchen und im Notfall erste Maßnahmen zu ergreifen. Spätestens wenn Clam-AV einen Virus auf dem Linux-Dateiserver findet, ist es Pflicht, sämtliche Windows-Clients genauer unter die Lupe zu nehmen. Hier greifen Sie am besten auf ein Rettungssystem zurück, wie sie viele Hersteller von Sicherheitslösungen zum Download anbieten.



Die Prüfung mit Clam-AV lässt sich automatisieren und ist empfehlenswert, wenn das System etwa als Dateiserver für Windows-Clients genutzt wird.



PC-Welt-Rettungs-DVD: Unser Linux-Spezialsystem für Windows-Pannen kann nach Viren scannen und Benutzerdateien retten oder das Windows-Passwort zurücksetzen.

Die LinuxWelt-Redaktion bietet ebenfalls ein solches Rettungssystem, das Sie kostenlos nutzen können (*www.pcwelt.de/downloads/PC-WELT-Notfall-DVD-3890747.html*). Der Unterbau solcher Systeme und auch dieses Rettungssystems ist ein Linux, das im Livebetrieb ausgeführt wird. Mit dem unabhängigen Notfallsystem können Sie den Windows-Rechner aus unkompromittierter Quelle nach Viren durchsuchen, Benutzerdateien auf andere Datenträger retten oder Reparaturen erledigen, falls ein Windows-System nicht mehr startet.

Die Vorgehensweise ist bei allen Datenrettern ähnlich. Sie starten den Computer über DVD- oder USB-Medium. Dazu müssen Sie im Bios meist die Reihenfolge beim Systemstart verändern oder Secure Boot abschalten. Das Livesystem wird Sie dann dazu auffordern, ein WLAN auszuwählen, falls der Computer nicht per Ethernet mit dem Internet verbunden ist. Meist erfolgt anschließend die Aktualisierung der Programme und der Virensignaturen.

Unter Linux können Sie nur auf Datenträger zugreifen, die in das Linux-Dateisystem eingehängt sind. Das gilt auch für Rettungssysteme. Um also gezielt die interne Festplatte oder besser eine Partition zu untersuchen oder zu bearbeiten, müssen Sie die Platte des Windows-Rechners erst anmelden. Im Notfallsystem der LinuxWelt/PC-Welt gibt es dafür das Leistensymbol „Festplatten einbinden“. Über die weitere Schaltfläche „Rettungswerkzeuge“ erreichen Sie dann mehrere Antivirenprogramme – neben Clam-AV auch Avira oder Sophos.

„Reparatur“ ist selten erfolgreich

Und wenn ein Virus gefunden wird? Die meisten am Markt befindlichen Schutzprogramme versprechen, einen Virenbefall reparieren zu können. Was unter dieser Reparatur zu verstehen ist, definieren die Hersteller aber sehr verschieden. Häufig wird die entsprechende Datei nur lokalisiert und automatisch in ein besonderes Verzeichnis verbannt („Quarantäne“). Wenn es sich um die ausführbare Datei eines Windows-Programms handelt, lässt sich dieses dann nicht mehr starten.

Nach unserer Einschätzung sind die Versuche, einen Virus tatsächlich physikalisch aus einer befallenen Binärdatei zu entfernen, selten von Erfolg gekrönt. Bevor Sie sich auf zweifelhafte Rettungsaktionen einlassen, ist es sicherer, den befallenen Rechner vollständig neu aufzusetzen. Dazu gehören die vollständige Formatierung der Speichermedien, die Installation des Betriebssystems aus einer vertrauenswürdigen Quelle und die Wiederherstellung der gespeicherten Benutzerdateien aus einem Backup.

Wichtige Benutzerdateien können Sie mit dem Rettungssystem aber auch vom infizierten System auf einen anderen Datenträger kopieren und dadurch retten. Die Gefahr, dass Office-, Text- und Mediendateien Schadsoftware enthalten und diese durch einen Software-Interpreter wie Excel, Adobe Reader oder VLC ausgelöst werden, ist nicht völlig auszuschließen, aber sehr gering.

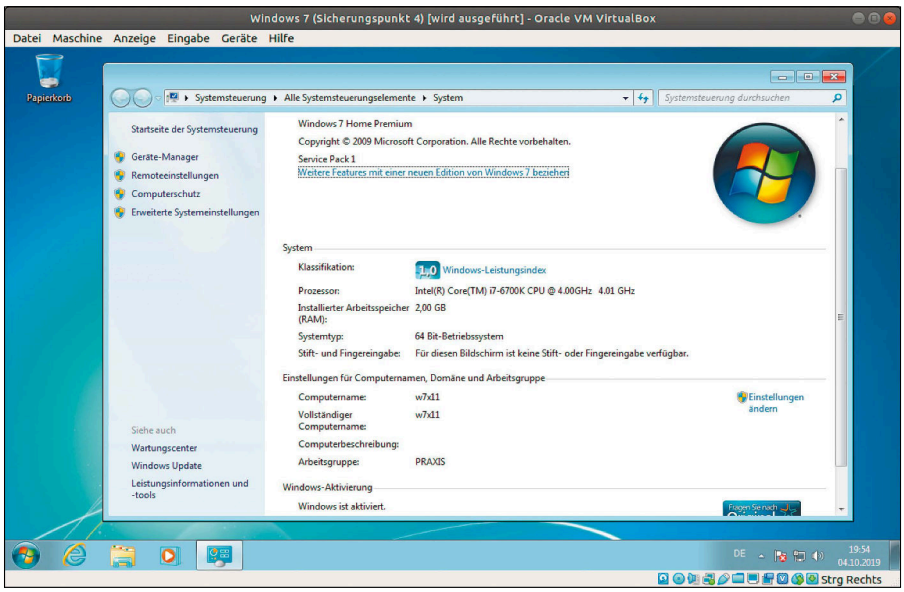
Rootkits sind für Linux gefährlich

Es gibt durchaus ein Bedrohungsszenario für Linux-Systeme, das Sie ernst nehmen sollten. Das Konto root darf unter Linux alles und Rootkits, deren Namen sich inzwischen auch für ähnliche Schädlinge für andere Systeme eingebürgert hat, sind Werkzeugsammlungen eines Angreifers, die sich erfolgreich vor der Entdeckung von Virenscannern tarnen. Ein solches Rootkit eröffnet dem Angreifer die Option, sich auf dem kompromittierten System anzumelden, Netzwerkverkehr zu überwachen oder Programme zu starten. Häufig werden solche erfolgreich auf verschiedenen Systemen installierten Kits für konzertierte Attacken genutzt.

Ein Programmpaket, das beim Aufspüren solcher Rootkits hilft, ist „chkrootkit“, das in den Paketquellen aller Distribution zu finden ist. Es wird in einem Terminal mit root-Recht gestartet (*sudo chkrootkit*), um das System zu untersuchen. Um sicher zu sein, dass das eigene System und damit das Programm chkrootkit nicht seinerseits kompromittiert ist, ist es ratsam, chkrootkit von einer unabhängigen Live-CD zu verwenden. Möglicherweise hat der Angreifer sein Rootkit gegenüber der Software getarnt, deswegen kann es nicht schaden, eine zweite Meinung etwa mit dem Programm rkhunter einzuholen. Auch dieses Tool ist in allen Distributionen über die Paketquellen zu beziehen. ■

Windows-7-System virtualisieren

Seit Januar 2020 ist Schluss mit Windows 7. Wer nun auf Linux umsteigen möchte, kann aber Windows 7 bei Bedarf in einer sicheren virtuellen Umgebung noch länger nutzen.



Windows unter Linux: In einer virtuellen Maschine lässt sich Windows 7 relativ sicher weiternutzen. Da es sich um einen Wechsel der Hardware handelt, muss Windows neu aktiviert werden.

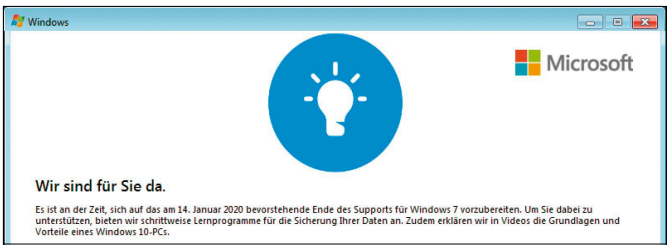
VON THORSTEN EGGELING

Am 14. Januar 2020 beendete Microsoft den erweiterten Support für Windows 7. Seitdem gibt es für die meisten Nutzer keine Sicherheitsupdates mehr. Ohne regelmäßige Sicherheitsupdates wird Windows 7 jedoch zu einem gefährdeten System. Trotzdem lässt sich das System weiterhin verwenden. Der komfortabelste Weg führt über eine Virtualisierungssoftware unter Linux. Kopieren Sie die Windows-Installation einfach in eine virtuelle Maschine (Physical to Virtual, P2V). Wer dabei ein paar Regeln beachtet, kann danach Windows 7 auch ohne Updates relativ sicher betreiben. Wir gehen in diesem Artikel davon aus, dass Ubuntu oder Linux Mint sowie Virtualbox 6.x bereits installiert sind. Informationen zur Ubuntu-Installation gibt es unter *www.pcwelt.de/1939429* und zu Virtualbox unter *www.pcwelt.de/2111217*.

Service: Alle Befehlszeilen aus diesem Artikel können Sie über *www.pcwelt.de/8z9r5n* herunterladen.

1. Was das Ende des Supports bedeutet

Seitdem Microsoft die Sicherheitsupdates einstellt hat, ist das System durch neu entdeckte Sicherheitslücken bedroht. Windows 7, 8 und 10 basieren teilweise auf demselben Quellcode, weshalb einige Sicherheitslücken wahrscheinlich in allen Systemen zu finden sind, bei Windows 7 jedoch nicht mehr behoben werden. Daher ist damit zu rechnen, dass Windows 7 seit Januar das bevorzugte Ziel von einigen Hackern ist. Das von Microsoft festgelegte



Bevorstehendes Ende: Nutzer von Windows 7 erhalten bereits seit einiger Zeit einen Hinweis, der zum Umstieg auf Windows 10 bewegen soll.



Windows 7 ohne Updates: Noch funktioniert die Aktualisierung. Ab Mitte Januar gibt es jedoch keine Updates mehr, Sicherheitslücken werden nicht mehr geschlossen.

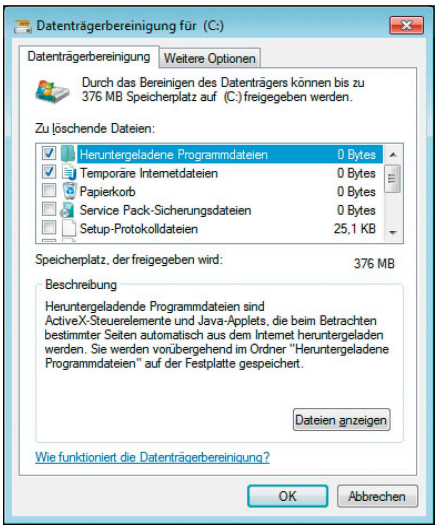
Ende der Nutzungsdauer bedeutet jedoch nicht das Ende der Nutzbarkeit. Windows 7 lässt sich auch nach dem 14. Januar 2020 starten, neu installieren und mit einem gültigen Produktschlüssel aktivieren.
Wenn Windows 7 ohne Verbindung zum Internet genutzt wird, darf dies als weitestgehend sicher gelten. Neu installierte Software muss allerdings sorgfältig geprüft werden und sollte nur aus vertrauenswürdigen Quellen stammen. Das Gleiche gilt für jede Art von Dateien, die Anwendungen unter Windows 7 öffnen und verarbeiten sollen. Programme wie PDF-Reader oder Office-Pakete sollte man solange wie möglich aktualisieren. Es ist jedoch damit zu rechnen, dass die meisten Softwarehersteller den Support für Windows 7 ebenfalls zeitnah einstellen werden.

2. Eingeschränkter Schutz durch Virtualisierung

Virtualisierungssoftware stellt einen virtuellen PC (virtuelle Maschine, VM) bereit, in dem sich ein weiteres Betriebssystem starten lässt. Sie können beispielsweise das installierte Linux nutzen (Hostsystem) und gleichzeitig bei Bedarf Windows 7 (Gastsystem) in einem Fenster oder auch im Vollbild starten.
Virtualisierungssoftware erlaubt keinen direkten Zugriff auf die PC-Hardware, mit Ausnahme von USB-Geräten. Die Gesamtleistung liegt daher etwas unterhalb eines herkömmlich installierten Systems auf dem gleichen PC und die virtuelle Grafikkarte eignet sich nur für Desktopanwendungen, aber nicht für aufwendige 3D-Spiele.
Ein mit Schadsoftware belastetes Windows kann jedoch eine Gefahr für das lokale Netzwerk darstellen. Über Freigaben können Viren andere Windows-PCs im Netzwerk infizieren. Das lässt sich vermeiden, indem Sie dem virtuellen PC nur Zugang zu schreibgeschützten Freigaben erlauben oder Daten auf einem anderen Weg austauschen (siehe Punkt 6).

3. Vorbereitungen für die Systemkopie

Der Transfer eines bestehenden Windows-Systems in eine virtuelle Maschine lässt sich deutlich beschleunigen, wenn Sie Windows vorher gründlich aufräumen. Löschen und deinstallieren Sie daher alles, was Sie nicht benötigen. Große Dateien verschieben Sie beispielsweise auf eine externe Festplatte. Nutzen Sie die Datenträgerbereinigung („cleanmgr.exe“), um überflüssige Dateien zu löschen.
Das Dateisystem sollte fehlerfrei und defragmentiert sein. Klicken Sie die Systemfestplatte im Windows-Explorer mit der rechten Maustaste an, wählen Sie „Eigenschaften“ und gehen Sie auf die Registerkarte „Tools“. Starten Sie die Fehlerüberprüfung und danach die Defragmentierung.
Windows-Tools: Damit Windows 7 in einer virtuellen Maschine startet, muss die Bootumgebung neu erstellt werden. Dafür benötigen Sie die ISO-Datei oder DVD des Installationsmediums von Windows 7. Ein Systemreparatur-Datenträger (Win-R, recdisc) funktioniert auch, muss aber unter einer Bios/MBR-Installation erstellt worden sein.



Windows aufräumen: Vor dem Umzug in eine virtuelle Maschine sollten Sie überflüssige Dateien löschen. Dabei hilft die Datenträgerbereinigung.

4. Windows-Partition mit Gparted kopieren

Die Festplatte mit der Windows-Partition muss in Virtualbox eingebunden werden. Das funktioniert jedoch nicht, wenn Linux von dieser Festplatte startet. In diesem Fall lesen Sie ab Punkt 5 weiter.
Schritt 1: Führen Sie die folgenden beiden Befehlszeilen aus:

```
sudo usermod -a -G vboxusers [User]
sudo usermod -a -G disk [User]
```

Den Platzhalter „[User]“ ersetzen Sie durch Ihren Benutzernamen. Die Gruppenzugehörigkeiten ermöglichen den Zugriff auf Festplatten ohne administrative Rechte und auf USB-Geräte in Virtualbox. Danach starten Sie Linux neu.
Schritt 2: Öffnen Sie ein Terminal (Strg-Alt-T) und starten Sie

```
sudo parted -l
```

Parted zeigt an, unter welchem Gerätepfad die Windows-Partition zu finden ist, beispielsweise auf der ersten Partition „/dev/sdb1“ der Festplatte „/dev/sdb“. Verwenden Sie dann diesen Befehl:

```
vboxmanage internalcommands
  createrawvmdk -filename ~/
  WinDisk.vmdk -rawdisk /dev/sdb
```

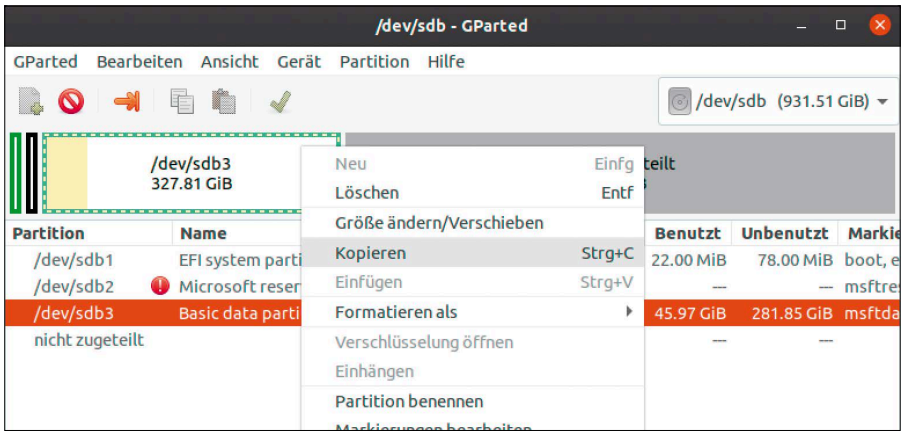
„/dev/sdb“ ersetzen Sie durch den zuvor ermittelten Laufwerkspfad. Sie erzeugen damit die virtuelle Festplatte „~/WinDisk.vmdk“, die auf das physikalische Laufwerk verweist.
Der Schritt kann entfallen, wenn Sie die Windows-Festplatte über einen SATA-USB-Adapter anschließen. Dafür muss das Oracle VM Virtualbox Extension Pack installiert sein (*www.virtualbox.org/wiki/Downloads*).
Schritt 3: Starten Sie Virtualbox und erstellen Sie eine neue VM für Windows 7. Erzeugen Sie über den Einrichtungsassistenten eine virtuelle Festplatte mit der

WINDOWS-BOOTUMGEBUNG REPARIEREN

Oft genügen die Computerreparatur-Optionen, um die Startumgebung von Windows 7 zu erzeugen. In manchen Fällen reicht das aber nicht aus. Booten Sie dann die virtuelle Maschine vom Windows-Installationsmedium und drücken Sie die Tastenkombination Umschalt-F10. In der Eingabeaufforderung geben Sie die folgenden vier Befehle ein:

```
bootrec /fixmbr
bootrec /fixboot
bootrec /rebuildbcd
bootsect /nt60 C: /mbr
```

Damit reparieren Sie die Bootumgebung und Windows 7 lässt sich danach in der virtuellen Maschine starten.



Windows umziehen: In einem Linux-Livesystem kopieren Sie mit Gparted die bisherige Windows-Partition und fügen diese in die virtuelle Festplatte ein.

Größe der bisherigen Windows-7-Partition oder größer.

Schritt 4: In den Einstellungen der virtuellem Maschine („Ändern“) gehen Sie auf „Massenspeicher“. Binden Sie als DVD-Laufwerk die ISO-Datei des Installationsmediums von Ubuntu 18.04 (auf Heft-DVD) oder 19.10 ein.

SATA-Festplatte: Klicken Sie „Controller: SATA“ mit der rechten Maustaste an, gehen Sie auf „Festplatte hinzufügen“ und klicken Sie auf „Vorhandene Festplatte auswählen“. Dann klicken Sie auf „Hinzufügen“, wählen die in Schritt 2 erstellte „vmdk“-Datei aus und bestätigen mit „Auswählen“ und „OK“.

USB-Festplatte: Bei einem USB-Laufwerk gehen Sie in der Navigation auf der linken Seite auf „USB“. Wählen Sie „USB-2.0-Controller (EHCI)“ oder „USB-3.0-Controller (xHCI), je nachdem, mit welchem USB-Port das Laufwerk verbunden ist. Klicken Sie auf die Schaltfläche mit dem „+“-Zeichen und wählen Sie das USB-Laufwerk. Klicken Sie auf „OK“, um die Änderungen zu speichern.

Schritt 5: Starten Sie die VM und darin das Ubuntu-Livesystem. Über „Aktivitäten“ suchen und starten Sie das Partitionierungstool Gparted. Das Auswahlfeld rechts oben zeigt zwei Festplatten: „/dev/sda“ ist die bisher leere virtuelle Festplatte und „/dev/sdb“ die bisherige Systemfestplatte.

Schritt 6: Wählen Sie „/dev/sda“, und gehen Sie im Menü auf „Gerät → Partitionstabelle erstellen“. Hinter „Neuen Partitionstabellentyp auswählen“ stellen Sie „msdos“ (MBR-Partitionstyp) ein und klicken auf „Anwenden“.

Es spielt keine Rolle, ob Windows 7 bisher auf einer Festplatte mit MBR-Partitionstyp installiert war oder GPT/Uefi verwendet. Da die Kombination Uefi/Windows 7 mit Virtualbox nicht funktioniert, muss Windows 7 in der VM im klassischen Bios/MBR-Modus starten.

Schritt 7: Wählen Sie „/dev/sdb“, klicken Sie die Windows-Partition mit der rechten Maustaste an und gehen Sie auf „Aushängen“. Danach wählen Sie im Kontextmenü „Kopieren“. Wechseln Sie zu „/dev/sda“, klicken Sie mit der rechten Maustaste in das Fenster, gehen Sie auf „Einfügen“ und klicken Sie auf die Schaltfläche „Einfügen“. Gehen Sie im Menü auf „Bearbeiten → Alle Vorgänge ausführen“ und bestätigen Sie mit „Anwenden“.

Nach Abschluss des Kopiervorgangs wählen Sie im Kontextmenü der eingefügten Partition „Markierung bearbeiten“, setzen ein Häkchen vor „boot“ und klicken auf „Schließen“. Fahren Sie das virtuelle System herunter.

Schritt 8: Im Hauptfenster „Oracle VM Virtualbox Manager“ klicken Sie auf „Ändern“ und ersetzen unter „Massenspeicher“ die ISO-Datei des Linux-Livesystems durch die ISO-Datei des Windows-7-Installationsmediums oder des Systemreparatur-Datenträgers. Über das CD/DVD-Icon lässt sich auch eine DVD im Laufwerk auswählen. Die in Schritt 4 hinzugefügte „vmdk“-Datei entfernen Sie aus der Konfiguration oder Sie deaktivieren unter „USB“ den Filter für USB-Geräte.

Schritt 9: Booten Sie das Windows-Installationssystem in der virtuellen Maschine. Klicken Sie auf „Weiter“ und dann auf „Computerreparaturoptionen“. Sobald Windows die Installation gefunden hat, klicken Sie auf „Reparieren und neu starten“. Sollte Windows 7 danach nicht booten, rufen Sie erneut die „Computerreparaturoptionen“ auf. Diesmal klicken Sie auf „Weiter“, dann auf „Systemstartreparatur“, „Fertig stellen“ und „Neu starten“. In einigen Fällen reicht das nicht aus, um Windows 7 zum Start zu überreden. Was Sie dann unternehmen müssen, lesen Sie im Kasten „Windows-Bootumgebung reparieren“.

5. P2V von Windows 7 über ein Backup

Sollten sich Windows 7 und Linux zusammen auf einer Festplatte befinden, erstellen Sie unter Linux ein Windows-Backup auf Dateisystemebene, das Sie danach auf die virtuelle Festplatte zurücksichern.

Installieren Sie unter Linux folgendermaßen zwei zusätzliche Pakete:

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

Der SSH-Server ermöglicht dem Gastsystem den Zugriff über das Netzwerk auf den Host und das Paket „wimtools“ enthält Programme, die sich für ein Windows-Backup unter Linux nutzen lassen.

Schritt 1: Ermitteln Sie über

```
sudo parted -l
```

den Gerätepfad der Windows-Installation, beispielsweise „/dev/sda3“. Sollte die Partition eingehängt sein, hängen Sie sie mit

```
te@Z77X: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
te@Z77X:~$ mkdir ~/Backup
te@Z77X:~$ wimcapture /dev/sda3 ~/Backup/windows7.wim "Windows 7"

Capturing WIM image from NTFS filesystem on "/dev/sda3"
Scanning "/dev/sda3"
171 MiB scanned (773 files, 123 directories)
Excluding "/$Recycle.Bin" from capture

Excluding "/hiberfil.sys" from capture

Excluding "/pagefile.sys" from capture
1244 MiB scanned (2954 files, 502 directories)
Excluding "/System Volume Information" from capture
15 GiB scanned (107668 files, 19681 directories)
Using LZX compression with 8 threads
Archiving file data: 5 GiB of 15 GiB (34%) done
```

Windows kopieren: Wimcapture erstellt ein platzsparendes Windows-Backup in einer WIM-Datei. In der virtuellen Maschine sichern Sie es dann auf die virtuelle Festplatte zurück.

```
sudo umount /dev/sda3
```

aus.

Schritt 2: Um das Backup zu erstellen, führen Sie die folgenden zwei Befehlszeilen aus:

```
mkdir ~/Backup
wimcapture /dev/sda3 ~/Backup/
  windows7.wim "Windows 7"
```

Im Ordner „Backup“ liegt danach die „wim“-Datei mit dem kompletten Systemabbild.

Schritt 3: Bereiten Sie eine virtuelle Maschine für Windows 7 vor. Erzeugen Sie über den Einrichtungsassistenten eine virtuelle Festplatte mit der Größe der bisherigen Windows-7-Partition oder größer. Binden Sie unter „Massenspeicher“ das ISO-Abbild einer Linux-Live-DVD ein, so etwa Ubuntu 19.10.

Unter „Netzwerk“ wählen Sie hinter „Angeschlossen an:“ den Eintrag „Netzwerkbrücke“, damit das Gastsystem Zugang zum lokalen Netzwerk erhält.

Schritt 4: Booten Sie das Linux-Livesystem in der virtuellen Maschine. Mit Hilfe von Gparted erstellen Sie auf „/dev/sda“ eine MS-DOS-Partition (siehe Punkt 4), die Sie mit dem Dateisystem NTFS formatieren. Setzen Sie über „Markierung bearbeiten“ die Option „boot“, damit die Partition aktiv und bootfähig ist.

Schritt 5: Führen Sie im Livesystem im Terminal die folgenden zwei Befehle aus:

```
sudo add-apt-repository universe
sudo apt install wimtools sshfs
```

Mit der Zeile

```
sudo sshfs -o allow_other [User]@
  [IP]:/home/[User]/Backup /mnt
```

hängen Sie den Backupordner aus Schritt 2 unter „/mnt“ in das Dateisystem ein. Den Platzhalter „[User]“ ersetzen Sie jeweils durch Ihren Benutzernamen, „[IP]“ ist die IP-Adresse oder der Name des Hostsystems.

Schritt 6: Kopieren Sie den Inhalt der „wim“-Datei auf die virtuelle Festplatte:

```
sudo wimapply /mnt/install.wim 1 /
  dev/sda1
```

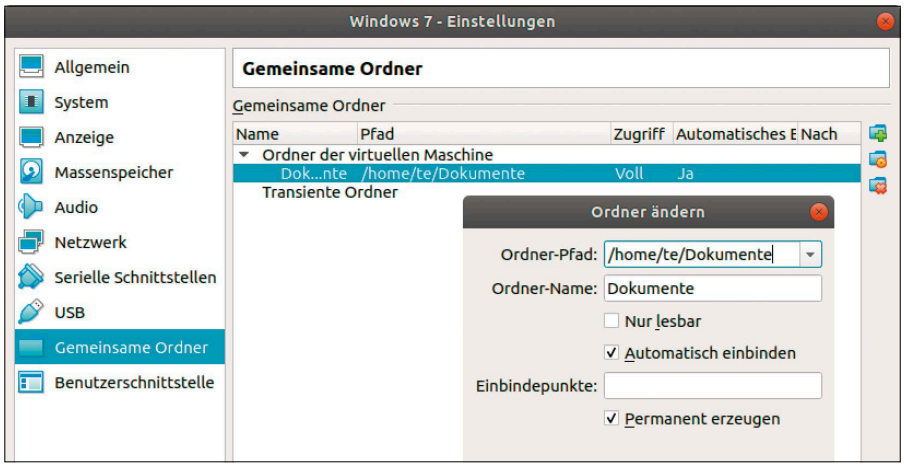
Danach erstellen Sie die Windows-Bootumgebung, wie in Punkt 4 in den Schritten 8 und 9 beschrieben.

6. Windows 7 optimieren und absichern

Die Leistung eines virtuellen PCs lässt sich über die Gasterweiterungen verbessern, die Treiber etwa für die Maus und den virtuellen Grafikadapter enthalten. Zur Installation gehen Sie auf „Geräte → Gasterweiterungen einlegen“, öffnen im virtualisierten System das DVD-Laufwerk im Windows-Explorer und rufen das Programm

```
VBoxWindowsAdditions.exe
```

Auf. Folgen Sie den Anweisungen des Installationsassistenten und starten Sie Windows danach neu. Im Gastsystem stehen jetzt weitere Funktionen zur Verfügung. Der Windows-Desktop wird automatisch an die Größe des Fensters angepasst und der Mauszeiger löst sich automatisch, wenn Sie ihn aus dem Fenster ziehen.



Datenaustausch: Verwenden Sie im virtualisierten Windows 7 einen gemeinsamen Ordner mit dem Hostsystem. Das ist sicherer als der Zugang zu Netzwerkfreigaben.

Netzwerk und Datenaustausch: Eine virtuelle Maschine ist bei der Standardkonfiguration „NAT“ vom lokalen Netzwerk getrennt, hat aber Zugang zum Internet. Wenn Sie den virtuellen Netzwerkadapter als „Netzwerkbrücke“ konfigurieren, erscheint die VM auch im lokalen Netzwerk – das ist aus Sicherheitsgründen für Windows 7 nicht zu empfehlen.

Zur Datenübertragung zwischen Host- und Gastsystem verwenden Sie besser einen gemeinsamen Ordner. Gehen Sie im Fenster der virtuellen Maschine auf „Geräte → Gemeinsame Ordner → Gemeinsame Ordner“. Über die „+“-Schaltfläche bestimmen Sie einen Ordner für den Datenaustausch auf dem Hostsystem. Setzen Sie Häkchen vor „Automatisch einbinden“ und „Permanent erzeugen“. Unter Windows 7 erreichen Sie den Ordner im Windows-Explorer über „Netzwerk“ und „Vboxsrv“ oder den Laufwerksbuchstaben „Z:“.

Im Fenster der virtuellen Maschine können Sie zwei weitere Optionen für den Datenaustausch aktivieren: „Geräte → Gemeinsame Zwischenablage → bidirektional“ und „Geräte → Drag und Drop → bidirektional“. Wenn Sie im Hostsystem beispielsweise einen Textabschnitt mit Strg-C kopieren, lässt er sich im Gastsystem in einem Editor mit Strg-V einfügen. Drag & Drop funktioniert bei Windows 7 nur in eine Richtung, etwa vom Linux-Dateimanager auf den Windows-Desktop. ■

WINDOWS IN DER VM AKTIVIEREN

Nach dem Umzug oder einer Neuinstallation in einer virtuellen Maschine läuft Windows 7 auf neuer Hardware. Die Aktivierung stellt in der Regel kein Problem dar und kann in der Systemsteuerung über „System → Windows aktivieren“ umstandslos erfolgen. Nach unseren Erfahrungen funktioniert die Aktivierung mit Produktschlüsseln der Vollversion sowie mit OEM/SB-Schlüsseln. Sollte das fehlschlagen, nutzen Sie die telefonische Aktivierung.

VMs lassen sich klonen oder auf andere Rechner kopieren. Solange die virtuelle Hardware sich nicht wesentlich verändert, bleibt die Aktivierung unabhängig vom jeweils genutzten PC erhalten. Wenn Sie nur eine Windows-7-Lizenz besitzen, dürfen Sie das System aber nur in der virtuellen Maschine starten und das bisher auf der Festplatte installierte System nicht gleichzeitig verwenden.

Die beste Linux-Hardware 2020

Linux-Nutzer müssen Hardware besonders sorgfältig auswählen, denn die Installation gelingt nicht immer reibungslos. Lesen Sie, was aktuelle Hardware leisten muss und worauf Sie bei Linux achten sollten.

VON THORSTEN EGGELING, VERENA OTTMANN, THOMAS RAU, INES WALKE-CHOMJAKOV



Intel-NUC: Mini-PCs liefern je nach CPU und RAM eine ähnliche Leistung wie ausgewachsene Desktop-PCs. Die Intel-Hardware ermöglicht die Installation beliebiger Betriebssysteme.

Viele PCs und Notebooks sind fast unkaputtbar, aber irgendwann ist doch ein Austausch ratsam. Neuere Modelle versprechen mehr Geschwindigkeit, längere Akku-Laufzeiten und ein besseres Display. Bei älteren Geräten bewirkt der Wechsel von einer Festplatte zur SSD einen deutlichen Leistungsschub. Die Anschaffung neuer Geräte ist immer eine schwere Entscheidung. Bei PC-Systemen und Notebooks haben Sie die Wahl zwischen vielen Modellen mit unterschiedlichster Ausstattung. Je nach gewünschtem Einsatzgebiet kann ein preisgünstiges Notebook mit einem langsamen Prozessor reichen. Wer unter Linux regelmäßig einen Kernel kompiliert, Videos umwandelt oder PC-Spiele verwendet, braucht hingegen ein leistungsfähigeres Modell. Das Gleiche gilt für Grafikkarten und Monitore.

Eines ist in jedem Fall vor dem Kauf empfehlenswert: Verschaffen Sie sich zunächst einen Überblick, was sich technisch getan hat und worauf Sie achten sollten. Blättern Sie dazu einfach zur gewünschten Gerätekategorie. Hier finden Sie alles Wichtige kompakt zusammengefasst.

Hardware für Linux

Bei einem Marktanteil von annähernd 90 Prozent kümmern sich fast alle Hersteller vor allem darum, dass Windows reibungslos auf PCs und Notebooks läuft. Geräte mit vorinstalliertem Linux gibt es nur wenige, etwa bei Dell (*www.dell.com*) und Tuxedo (*www.tuxedocomputers.com*). Trotzdem lässt sich der größte Teil der Hardware auch unter Linux problemlos nutzen. In den PCs stecken meist Standardkomponenten von nur wenigen Herstellern, die genauso oder ähnlich auch in den Servern zu finden sind, die in Rechenzentren stehen – und hier dominiert Linux. Von der Intel-Chipsatzgrafik abgesehen gibt es bei Grafikadaptern nur zwei Hersteller: Nvida und AMD. Beide stellen Treiber und Know-how für Linux zur Verfügung, die Unterstützung ist daher gut bis sehr gut.

Bei Notebooks ist die Situation häufig anders. Im Bios beziehungsweise der Firmware lässt sich nicht viel einstellen und es gibt zahlreiche Spezialfunktionen beispielsweise für die Stromsparmodi und die Steuerung der Hintergrundbeleuchtung. Unter Windows sorgen Treiber und Zusatzprogramme für die korrekten Funktionen, bei Linux ist das nicht sichergestellt. Mal lassen sich WLAN oder Bluetooth nicht zur Zusammenarbeit bewegen, die Tastaturbeleuchtung bliebt dunkel oder der Akku hält weniger lange durch als unter Windows.

Auch bei Peripheriegeräten wie Druckern, Scannern und Multifunktionsgeräten ist die Situation nicht eindeutig. Aktuelle Geräte namhafter Anbieter wie HP, Epson oder Canon funktionieren fast immer. Der volle Funktionsumfang lässt sich mit Treibern und Software vom Hersteller nutzen. Bei Geräten, die der Discounter um die Ecke gerade anbietet, ist die Linux-Unterstützung dagegen fraglich.

Fazit: Computer mit Standardausstattung arbeiten unter Linux fast immer problemlos. Bei Notebooks und Peripheriegeräten sollte man im Internet vor dem Kauf nach der Linux-Unterstützung suchen. Sie finden häufig Erfahrungsberichte andere Nutzer, denen Sie entnehmen können, was funktioniert und was nicht.

Das klassische PC-System

Den Standard-PC für Multimedia- und Office-Anwendungen im großen Gehäuse, mit vielen Anschlüssen und Erweiterungsmöglichkeiten finden Sie nur noch selten im Handel. Ein Beispiel ist der Medion Akoya P66072, den Sie mit einem Core i5-9400, acht GB RAM sowie einer Speicherkombi aus einer 256 GB großen SSD und einer Ein-TB-Festplatte für rund 600 Euro bekommen. Größer ist das Angebot an Rechnern in dieser Größe, wenn Sie auch eine einigermaßen spieletaugliche Grafikkarte wünschen: Meist kommt eine Geforce GTX 1050 zum Einsatz, die für viele Spiele in Full-HD

genügt. Entsprechende Modellvarianten des HP Pavilion 590 oder des Acer Aspire TC-885 kosten 700 bis 800 Euro.

Kompakt-PCs: Für alltägliche Rechenaufgaben genügt auch ein kleinerer PC mit einem kompakten Acht-Liter-Gehäuse wie der Lenovo Ideacentre 510S oder der Acer Aspire XC-885. Die Preise beginnen ab rund 400 Euro, zum Beispiel mit einem Core i3-8100 und einer Ein-TB-Festplatte. Etwas teurer sind kompakte Businessrechner wie der Dell Optiplex 3060 oder der HP 290 G1: In einer empfehlenswerten Ausstattung mit Core i5, aht GB RAM und 256 GB SSD kosten sie ab rund 650 Euro.

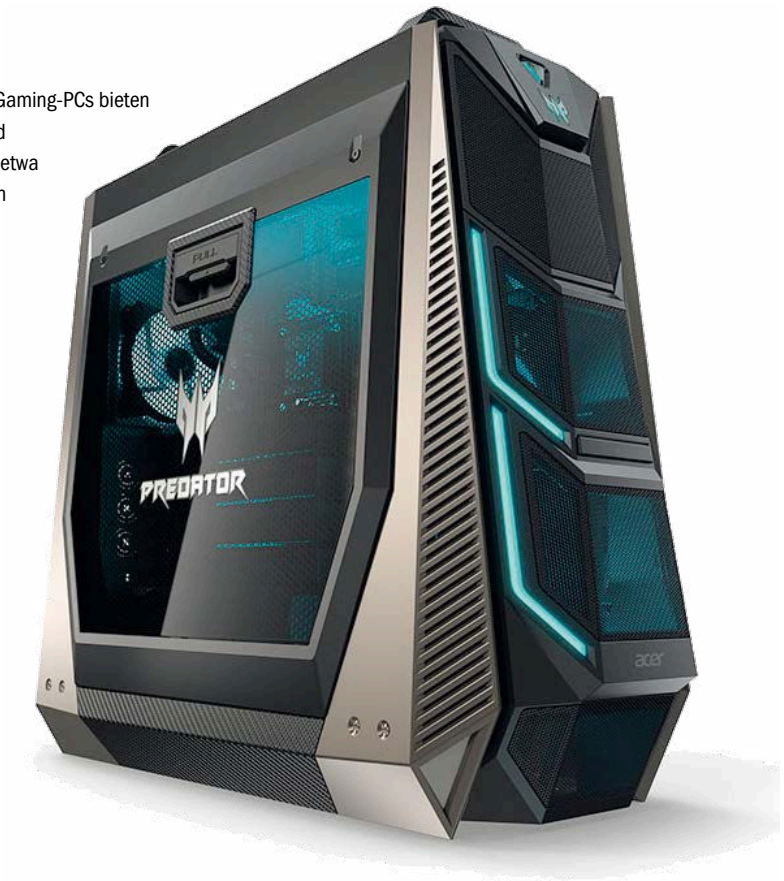
Noch weniger Platz beanspruchen Mini-PCs wie der Trekstor WBX5005, mit Abmessungen von 11 x 12 x 4,6 cm. Die Preise starten ab rund 300 Euro mit einem Core i3-5005U, acht GB RAM und einer 128 GB großen SSD. Die Intel NUC-Kits sind Minirechner, die lediglich mit einer auf der Platine gelöteten CPU bestückt sind. Sie ergänzen RAM und Festplatte im 2,5-Zoll oder M.2-Format. Die Preise starten ab 140 Euro. Da hier nur Intel-Hardware verbaut ist, stellt der Betrieb der Intel-NUCs mit Linux keine Herausforderung dar.

Gaming-PCs: Wer einen Rechner für aktuelle Spiele in bester Qualität sucht, muss mindestens rund 1100 Euro anlegen, etwa für den Asus ROG Huracan G21 im kompakten Gehäuse mit Core i7-9700K und Geforce RTX 2070. Größere Gehäuse versprechen mehr Platz für Erweiterungen und Kühlung und kosten mit entsprechend leistungsfähigen Komponenten rund 1600 Euro, wie der Lenovo Legion T530 oder der HP Omen 875. Nach oben sind den Preisen und der Ausstattung kaum Grenzen gesetzt: Die Top-Konfiguration des Acer Predator Orion 9000 mit Core i9, Geforce RTX 2080 Ti und 128 GB RAM kostet satte 10 000 Euro.

Relativ neue Grafikkarten wir die Nvidia RTX 2060 oder 2070 werden von den Standardtreibern einiger Linux-Distributionen bisher nicht unterstützt. Bei der Neuinstallation bleibt der Bildschirm schwarz. Wie sich das Problem beheben lässt, lesen Sie im Kasten „Grafikkarten und Linux-Treiber".

Notebooks für jede Rolle

Schon ab rund 400 Euro bekommen Sie derzeit 15-Zoll-Notebooks mit einer 256 GB großen SSD – etwa aus der Modellreihe Aspire 3 von Acer oder der E-Serie des Medion Akoya. Wer's ein bisschen schlanker, schicker und vollkommen lautlos schätzt, der greift zum Trekstor Primebook P15 mit einer 128 GB großen SSD und Passivkühlung. Den günstigen Notebooks ist gemeinsam, dass sie mit einem eher schwachbrüstigen Prozessor arbeiten – wie Pentium N4200, N5000 oder Athlon 3000U. Damit laufen selbst einfache Aufgaben wie Websurfen und Texterstellung langsamer. Ab 500 Euro gibt es Modelle mit einem schnelleren Core i3 aus der siebten oder achten Coregeneration und für rund 50 Euro mehr auch schon Angebote mit einem Core i5.

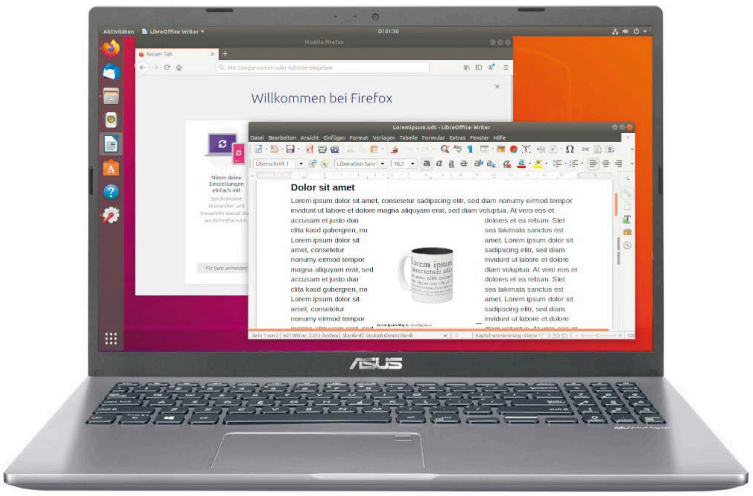


Hochpreisig: Aktuelle Gaming-PCs bieten auffällige Gehäuse und Top-Komponenten, so etwa der Acer Predator Orion 9000 – zu Preisen im fünfstelligen Bereich.

UEFI, SECURE BOOT & PARALLELINSTALLATION

Auf neuen PCs und Notebooks ist Windows 10 im Uefi-Modus vorinstalliert. Außerdem ist Secure Boot aktiv, was die Bootumgebung vor Schadsoftware schützen soll. Die Installation von Ubuntu oder Linux Mint als alleiniges System oder parallel zu Windows stellt eigentlich kein Problem dar. Bei beiden Systemen sind die Dateien des Bootmanagers und der Kernel digital signiert. Die Systeme starten daher auch bei aktiviertem Secure Boot. Trotzdem sollte man die Funktion im Firmwaresetup deaktivieren, weil später installierte Treiber wahrscheinlich nicht signiert sind und der Kernel sie nicht laden kann.

Bei einigen Notebooks funktioniert die Linux-Installation nicht reibungslos. Wenn man Windows löschen und nur Linux installieren möchte, sollte man in der Firmware die Bios-Emulation CSM (Compatibility Support Module) oder „Legacy" aktivieren und die Installation im Bios-Modus mit dem MBR-Partitionsschema erledigen. Bei einer Parallelinstallation muss der Uefi-Modus aktiviert bleiben. Sollte das Linux-Installationssystem nicht starten, gibt es dafür keine allgemeingültige Lösung. Manchmal sind spezielle Firmwareeinstellungen nötig oder man muss den Grub-Bootloader auf dem USB-Stick als vertrauenswürdig für den Uefi-Start festlegen. Bei Problemen hilft nur eine Recherche im Internet. Klüger ist es jedoch, schon vor dem Kauf nach Problemen beim Linux-Betrieb zu suchen und gegebenenfalls ein anderes Modell zu wählen.



Notebook-Allrounder: Das beste Preis-Leistungs-Verhältnis bieten derzeit Notebooks zwischen 600 und 700 Euro – beispielsweise das Asus Vivobook 15.



Teuer, aber gut: Das Lenovo Thinkpad X1 Extreme kostet um die 2500 Euro. Dafür bietet das Notebook Rechen- und Grafikleistung auf höchstem Niveau.

Allrounder ab 600 Euro: Zwischen 600 und 700 Euro finden Sie die meisten Notebooks, deren Ausstattung voll alltagstauglich ist: Sie bieten typischerweise einen Core i5 und acht GB oder sogar 16 GB RAM sowie eine 512 GB große SSD. Entsprechende Modelle gibt es von HP in der 15er-Serie und von Asus beim Vivobook 15. Gelegentlich finden Sie sogar schon Laptops mit einer Ein-TB-SSD wie das Lenovo Ideapad S340.

Die AMD-Prozessoren Ryzen 5 und 7 aus der 3000er-Serie halten mit entsprechenden Intel-Core-CPUs aus der achten Generation problemlos mit und sind bei einigen Anwendungen sogar schneller. Sie können also bedenkenlos zugreifen, wenn Ihr Wunsch-Laptop in einer bestimmten Ausstattung nur mit Ryzen statt mit Intel-CPU zu haben ist.

Notebooks zum Spielen: Fürs Gaming in Full-HD eignet sich beispielsweise der Acer Nitro 5 mit einem Coreprozessor aus der leistungsstarken H-Serie und einer Geforce GTX 1650 (rund 1000 Euro). Soll das Spiele-Notebook flach und leicht sein, achten Sie auf eine GPU im Max-Q-Design: Die entsprechenden Geforce-Chips sind nicht ganz so leistungsstark, produzieren aber weniger Abwärme. Wer es sich leisten kann, muss mit einem Notebook wie dem Lenovo Thinkpad X1 Extreme ab rund 2500 Euro keine Kompromisse mehr eingehen: Es bietet hohe Rechen- und Grafikleistung, 4K-Auflösung, viele Schnittstellen und ein leichtes Gehäuse.

Dedizierte Grafikkarten

Obwohl Intel die Leistung der im Hauptprozessor integrierten Grafik mit jeder Coregeneration steigert, benötigen Sie in vielen Fällen unbedingt eine zusätzliche Grafikkarte im PC – für Spiele sowieso, aber auch, wenn Sie häufig Fotos und Videos bearbeiten oder mit Renderingprogrammen arbeiten. Eine Grafikkarte sorgt außerdem

GRAFIKKARTEN UND LINUX-TREIBER

Neueste Grafikchips werden von den Linux-Distributionen mit den Standardtreibern teilweise noch nicht unterstützt.

Im schlimmsten Fall bleibt der Bildschirm bei der Linux-Installation oder nach Umbau der Grafikkarte schwarz. Es kann helfen, eine neuere Linux-Distribution zu verwenden, beispielsweise Ubuntu 19.10 statt 18.04 (oder demnächst Ubuntu 20.04).

In der Regel lässt sich das Problem bei der Neuinstallation mit zusätzlichen Startparametern umgehen. Wenn Sie beispielsweise Ubuntu 18.04 im Bios-Modus von DVD oder USB-Stick booten, drücken Sie eine beliebige Taste und wählen als Sprache „Deutsch“. Dann drücken Sie die Taste F6 und aktivieren mit der Eingabetaste die Optionen „acpi=off“, „noapic“, „nolapic“ und „nomodset“. Drücken Sie die Esc-Taste und gehen Sie auf „Ubuntu ohne Installation ausprobieren“. Der Desktop des Livesystems sollte dann erscheinen, wenn auch mit geringer Auflösung. Führen Sie die Installation wie gewohnt durch.

Beim Booten im Uefi-Modus drücken Sie im Grub-Menü die Taste „E“. Tragen Sie die genannten Kernel-Parameter getrennt durch Leerzeichen hinter den beiden Bindestrichen („--“) in die Zeile ein, die mit „linux“ beginnt. Drücken Sie F10, um das System zu booten.

Nach Abschluss der Installation startet Ubuntu und verwendet weiterhin die angegebenen Kernel-Optionen. Dann suchen Sie über „Aktivitäten“ nach „Treiber“, klicken auf „Anwendungen & Aktualisierungen“ und gehen zur Registerkarte „Zusätzliche Treiber“. Ubuntu 18.04 bietet Ihnen Nvidia-Treiber ab Version 430 an, die Grafikkarten der Produktserien RTX 2060 bis 2080 unterstützen.

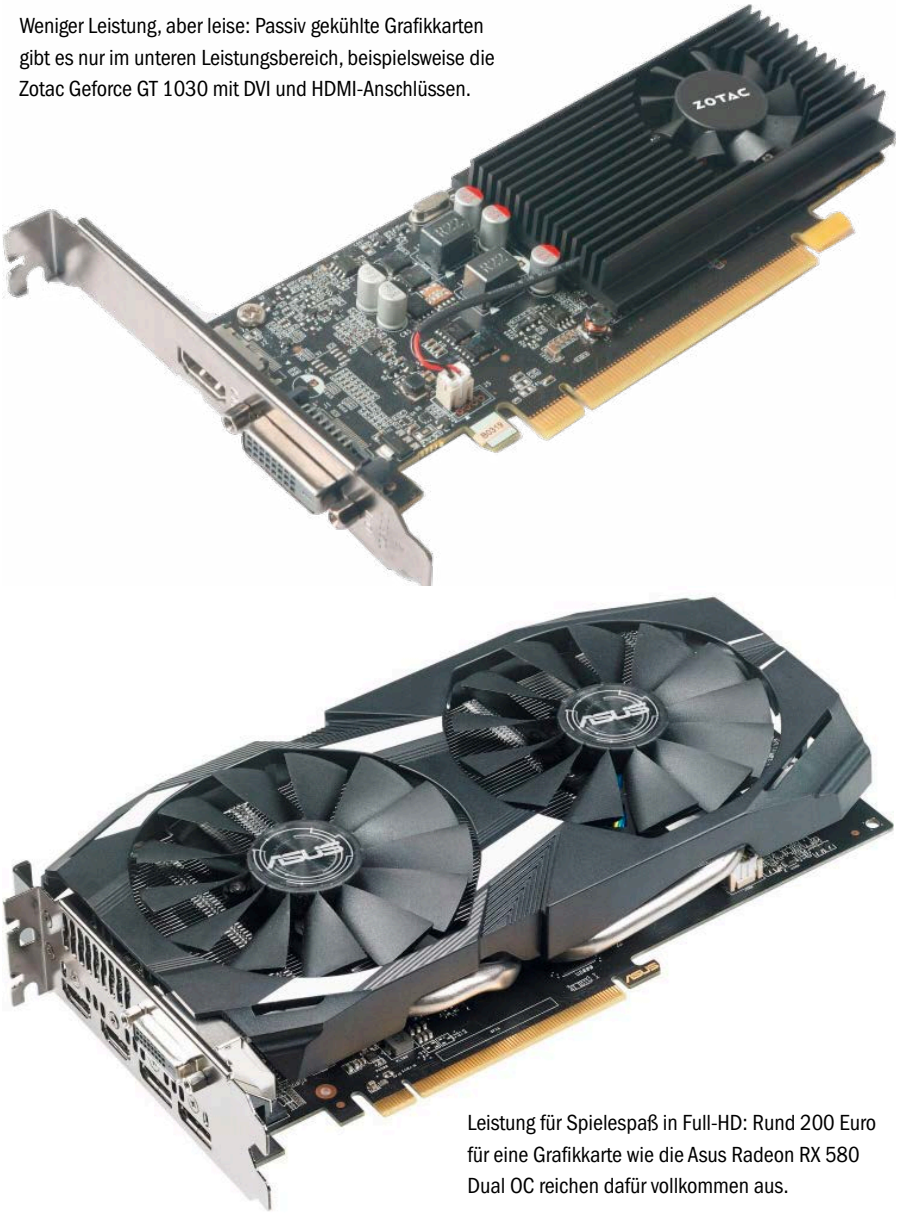
Vor dem Neustart entfernen Sie die Kernel-Parameter aus der Datei „/etc/default/grub“ und aktualisieren die Grub-Konfiguration mit

```
sudo update-grub
```

Mit dem aktuellen Nvidia-Treiber startet das System problemlos und bietet dann auch die maximale Leistung des Grafikchips.

für mehr und bessere Displayanschlüsse, um zum Beispiel ein Multi-Display-Setup mit hohen Auflösungen einzusetzen.
Dabei sollten Sie zu einer Grafikkarte für unter 100 Euro greifen, wenn Sie dem PC nur mehr Anschlüsse verschaffen wollen. Diese Karten arbeiten mit dem AMD-Chip Radeon R5 230 oder dem Nvidia-Geforce GT 710. Für rund 80 Euro gibt es passiv gekühlte Karten mit einem Geforce GT 1030, die sich auch für einen leisen Wohnzimmer-PC eignen.
Wieviel Sie als PC-Spieler in eine Grafikkarte investieren müssen, hängt vor allem von der Auflösung ab, in der Sie spielen. Für Full-HD mit guten Grafikdetails ist derzeit die AMD-GPU RX 580 erste Wahl, am besten auf einer Grafikkarte mit acht GB Speicher, wie bei der MSI RX 580 Armor oder der Asus Radeon RX 580 Dual OC, die beide etwa 180 Euro kosten. Oder Sie greifen zu einer Karte mit Nvidia Geforce GTX 1650 für knapp unter 180 Euro oder dem etwas schnelleren GTX 1660 für knapp über 200 Euro. Der kleinere Grafikspeicher von sechs GB ist beim Spielen in Full-HD in der Regel kein Nachteil.
Um beim Spielen in Full-HD auch in aktuellen Games maximale Details flüssig darzustellen, sollten Sie bis rund 300 Euro ausgeben. Auch in diesem Segment bietet AMD mit dem RX Vega 56 eine leistungsfähigere, aber auch etwas lautere Lösung als Nvidia: Für die Asus Radeon RX Vega 56 RO Strix OC bezahlen Sie rund 270 Euro. Karten mit dem Konkurrenzchip von Nvidia, dem Geforce GTX 1660 Ti, kosten knapp über 300 Euro.
Karten bis rund 500 Euro eignen sich zum Spielen in der WQHD-Auflösung (2560 x 1440). Für knapp unter 400 Euro bekommen Sie Karten mit dem Radeon RX 5700, knapp über 400 Euro kosten Modelle mit dem schnelleren RX 5700 XT. Auch bei diesem AMD-Chip empfehlen sich Karten mit einer angepassten leiseren Kühllösung wie die Sapphire Radeon Pulse RX 5700 XT für rund 440 Euro. Je nach Leistungsanforderungen können Sie rund 550 Euro für eine Karte mit Geforce RTX 2070 wie die Gigabyte RTX 2070 Super Gaming OC, etwa 700 Euro für die Asus Geforce RTX 2080 ROG Strix Gaming Advanced oder sogar über 1200 Euro ausgeben: Dafür bekommen Sie die derzeit schnellste Gaming-GPU RTX 2080 Ti, zum Beispiel auf der MSI Geforce RTX 2080 Ti Gaming X Trio.

Weniger Leistung, aber leise: Passiv gekühlte Grafikkarten gibt es nur im unteren Leistungsbereich, beispielsweise die Zotac Geforce GT 1030 mit DVI und HDMI-Anschlüssen.



Leistung für Spielespaß in Full-HD: Rund 200 Euro für eine Grafikkarte wie die Asus Radeon RX 580 Dual OC reichen dafür vollkommen aus.

Solid State Disks (SSDs)

SSDs bringen den Rechnern mehr Tempo als ein neuer Prozessor oder mehr RAM. Da Solid State Disks keine beweglichen Teile haben, arbeiten sie vollkommen geräuschlos und sind robuster als Magnetfestplatten. Unter Linux ist wie unter Windows bei der Installation auf SSD nichts Besonderes zu beachten. Das System erkennt den Typ des Datenträgers automatisch und setzt regelmäßig den Trimbefehl ab, um gelöschte Speicherbereiche wieder verfügbar zu machen.
Bei internen SSDs sind Sie mit unterschiedlichen Anschlüssen und Formfaktoren konfrontiert. Welche für Sie geeignet sind, gibt das Mainboard vor. Flashspeicher im 2,5-Zoll-Format wird inzwischen nur noch per SATA angeschlossen. Hier erreichen Sie beim aktuellen SATA III einen theoretischen Maximaldurchsatz von 600 MB/s. 2,5-Zoll-SSDs bieten mit bis zu vier TB reichlich Platz und sind auch preislich erschwinglich geworden: Eine günstige SATA-SSD mit einem TB Kapazität erhalten Sie für rund 100 Euro – so etwa die Crucial MX500. Damit steht einem PC-Upgrade von HDD auf SSD nichts mehr im Wege.
M.2 erlebt seinen Durchbruch, seit sich die Flashspeicher in die PCI-Express-Schnittstelle stecken lassen und das NVMe-Protokoll verwenden. Denn über PCIe erreichen die Flashmodule weitaus höhere Datenraten. Maximal angebunden, klettert das Tempo auf theoretische 4000 MB/s. Welcher Typ genau in Ihr System passt, verrät



Crucial MX500 1 TB: Die SATA-SSD ist mit rund 100 Euro bereits so günstig, dass Sie die Magnetfestplatte ersetzen können, ohne sich in Unkosten zu stürzen.



Mehr Sicherheit: Damit Ihre Daten nicht in falsche Hände geraten, sollten Sie externe Festplatten verschlüsseln. Die Diskashur 2 wird durch Eingabe einer PIN entsperrt.

Ihnen das Handbuch zum Mainboard. Weit verbreitet sind die Formate 2242 und 2280. Preisunterschiede ergeben sich innerhalb einer Kapazitätsklasse durch den verwendeten Flashspeicher und Controller. NVMe-SSDs bieten momentan eine maximale Kapazität von zwei TB.

Externe Festplatten und SSDs

Externe Festplatten im 2,5-Zoll-Format sind besonders mobil, arbeiten leise und meist energiebewusst. Es gibt sie mit Kapazitäten von bis zu fünf TB – beispielsweise bei Seagate ab 120 Euro. Externe 3,5-Zoll-Platten eignen sich dagegen bestens für den stationären Gebrauch und bieten höhere Kapazitäten – derzeit bis zu 14 TB wie das G-Drive Thunderbolt 3 für etwa 700 Euro. Allerdings benötigen 3,5-Zoll-Platten eine eigene Stromversorgung und sind leistungshungriger und lauter.

Wer im mobilen Betrieb auf Sicherheit Wert legt, sollte zu einem Modell mit Verschlüsselung greifen. Die Diskashur 2 von iStorage beispielsweise ist eine Sicherheitsfestplatte mit Zahlenfeld, über das Sie Ihren Zugangscode eingeben. Sie kostet circa 300 Euro für ein TB. Oder Sie setzen gleich auf einen sicheren Zugang per Fingerabdruck, wie ihn die Verbatim Fingerprint Secure Festplatte für 125 Euro bietet (ein TB). Die Ersteinrichtung muss unter Windows oder am Mac erfolgen. Danach lässt sich die Festplatte jedoch auch unter Linux entsperren.

Externe SSDs verwenden oft einen SATA-USB-Adapter, wobei das verbaute Modul entweder das 2,5-Zoll- oder auch das längliche M.2-Format haben kann (etwa bei der Verbatim Vx500 mit 480 GB für 120 Euro). Teurere externe SSDs wie das G-Drive mobile Pro SSD von G-Technology (ab 300 Euro) basieren auf dem schnelleren PCI-Express-Standard. Die Größe einer externen SSD entspricht in der Regel der einer externen 2,5-Zoll-Festplatte.

Deutlich kleiner fallen dagegen etwa die Seagate One Touch SSD für 170 Euro aus (ein TB) sowie die Elite Portable SSD oder die Pro Elite Portable SSD (ab 150 Euro für ein TB) von PNY. Alle drei haben etwa Kreditkartenformat. Was die Tempoangaben angeht, so schaffen externe SSDs laut Hersteller im Schnitt 540 MB/s beim sequenziellen Lesen und Schreiben.

Teurere Modelle wie das G-Drive mobile Pro SSD von G-Technology liegen laut Hersteller bei 900 bis 1000 MB/s. Preislich beginnen externe SSDs mit einem TB und USB 3.0 bei 50 bis 70 Euro. Für USB 3.1 und NVMe-Anbindung müssen Sie mit 150 Euro aufwärts rechnen.

Monitore mit TN- und IPS-Technik

Suchen Sie einen Allrounder, mit dem Sie mehrere Jahre gut auskommen, sehen Sie sich einen UHD-Monitor an. Hier liegt der Einstieg inzwischen bei rund 200 Euro – etwa für den Samsung U28E590D. Schirme dieser Klasse haben die hohe Auflösung von 3840 x 2160 Pixeln, eine Diagonale von 27 oder mehr Zoll, verwenden aber oft noch die TN-Panel-Technik, die Schwächen in der Abdeckung von Farbräumen und in den Blickwinkeln nach sich zieht; gleichzeitig aber schnell schaltet und zumindest eine der adaptiven Synchronisierungstechniken – meist Freesync – beherrscht.

Bessere Qualität bieten Monitore mit IPS-Panel. Dieser Paneltyp hat sich dank seiner Farben, Kontraste und Blickwinkelstabilität durchgesetzt. In der Kombination mit UHD und 27 Zoll investieren Sie rund 50 Euro mehr – etwa für den Philips 276E8VJSB/00. Ist der Hochkontrast für Sie äußerst wichtig, müssen Sie in derselben Monitorklasse mit gut 420 Euro rechnen – etwa für den LG 27UL600-W.

Für Gamer bringen es auch IPS-Panels inzwischen auf eine Reaktionszeit von einer Millisekunde und 240 Hertz, wie der topaktuelle LG Ultragear 27GN750, der dazu noch mit HDR 10 und Nvidia-G-Sync-Kompatibilität punktet, aber mit 429 Euro (UVP) ins Geld geht, sich dabei auf Full-HD-Auflösung (1920 x 1080 Pixel) beschränkt und wahrscheinlich erst im Laufe des Jahres 2020 erhältlich sein wird.

Drucker & Multifunktionsgeräte

Wenn Sie auf Farbe verzichten können, ist ein Schwarzweiß-Laserdrucker oft die beste Lösung. Er verträgt auch längere Ruhezeiten, ohne dass Sie Kompromisse in der Druckqualität eingehen müssen. Seine Stärke liegt im Textdruck dank scharfer Buchstaben und guter Deckung. Der HP Laser 107w für rund 120 Euro beispielsweise ist eine kompakte A4-Lösung für den Hausgebrauch. Möchten Sie für einen Tin-

tenstrahldrucker nicht mehr als 50 bis 60 Euro investieren, sollte es für das Gerät Tintenpatronen mit mehr Inhalt geben. So drücken Sie die Seitenpreise wenigstens ein wenig – wie etwa beim Canon Pixma TR4550 für rund 50 Euro.

Die höchste Ersparnis bei Tinte erreichen Sie, wenn Sie einen Drucker mit Tanksystem kaufen. Die Drucker und Multifunktionsgeräte haben eingebaute Behälter, die sich mit Tinte aus Flaschen nachfüllen lassen. Damit erreichen Sie Seitenpreise weit unter einem Cent. Allerdings liegen die Gerätepreise deutlich über Patronendruckern. Aktuell müssen Sie mit rund 180 Euro rechnen – etwa für den Epson Ecotank ET-2600. Zur Nutzung des vollen Funktionsumfangs müssen Sie unter Linux in der Regel zusätzliche Treiberpakete installieren. Die Downloads finden Sie über die Support-Webseite des jeweiligen Herstellers.



UHD-Bildschirm zum günstigen Preis: Der Monitor Philips 276E8VJSB/00 kostet rund 250 Euro, sieht schick aus und zeigt natürliche Farben bei guter Helligkeit.

WLAN und Router

Beim Wechsel der Anschlussart oder Anschlussgeschwindigkeit denken viele Anwender auch an den Neukauf eines WLAN-Routers. Zukunftssicherheit für einen schnellen DSL-Anschluss bietet die Fritzbox 7590 von AVM mit Super-Vectoring mit bis zu 300 MBit/s, die derzeit rund 200 Euro kostet. Das Pendant für schnelle Kabelanschlüsse mit bis zu einem GBit/s Downloadtempo ist die Fritzbox 6591 für 250 Euro. Beide bringen 11ac-WLAN mit und liefern darüber maximal 1733 MBit/s über fünf GHz plus 800 MBit/s über 2,4 GHz.

Neuer Standard Wi-Fi 6: Einige Hersteller haben bereits Router für den neuen WLAN-Standard Wi-Fi 6 (alias 11ax) auf den Markt gebracht. Sie bieten noch höheres WLAN-Tempo mit maximal drei bis sechs GBit/s. Aktuell gibt es noch wenige WLAN-Geräte mit diesem Funkstandard, doch wird deren Zahl 2020 zunehmen. Der Einstieg in die WLAN-Zukunft beginnt bei knapp unter 200 Euro, zum Beispiel mit dem Netgear Nighthawk AX4 oder dem Asus RT-AX58U.

Eines der wenigen verfügbaren WLAN-Funkmodule für Notebooks stammt von Intel und kostet um die 20 Euro. Das Notebook muss für die AX200-Karte einen M2-Stecksockel besitzen. Linux-Treiber sind ab Kernel-Version 5.1 standardmäßig vorhanden – Ubuntu 18.04.4 verwendet zurzeit bereits Kernel 5.3. Weitere Informationen finden Sie bei Intel über *www.pcwelt.de/u6q_Wd*. ■



Samsung U28E590D: Solche Bildschirme mit TN-Panel-Technik sind besonders günstig, erreichen aber nicht die satten Farben und Kontraste der Monitore mit IPS-Panel.

© amazon



Canon Pixma TR4550: Für rund 50 Euro bekommen Sie einen kompakten Kombidrucker, der ein Fax, einen Vorlageneinzug und eine Duplexeinheit mitbringt.

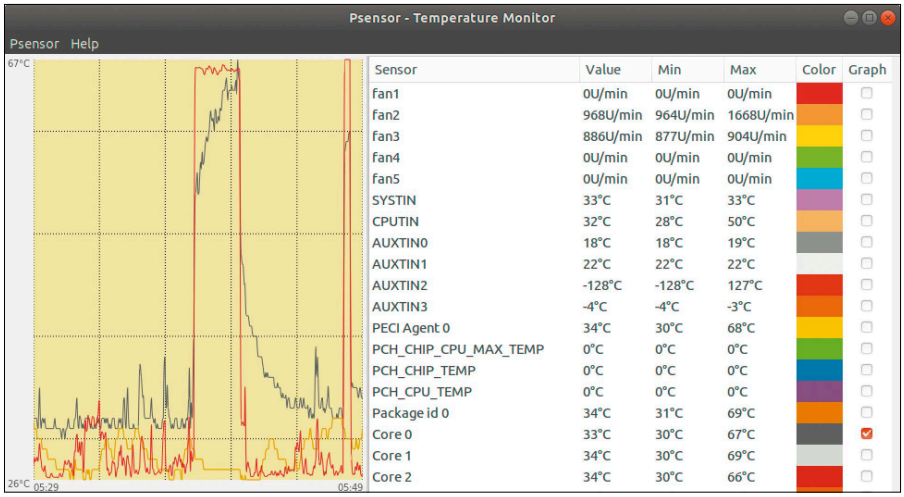
Hardwarekontrolle mit Sensoren

Wie heiß der Prozessor wird oder ob sich der CPU-Lüfter noch dreht, lässt sich per Software herausfinden. Um alle verfügbaren Sensoren abzufragen, ist jedoch etwas Konfigurationsarbeit nötig.

VON THORSTEN EGGELING

Ein defekter oder verschmutzter Lüfter kann die Temperatur von Prozessor oder Grafikkarte so weit in die Höhe treiben, dass das System instabil wird. Die CPU taktet dann herunter, der Rechner reagiert nur noch zögerlich oder stürzt häufig ab. Dauerhaft zu hohe Temperaturen schaden außerdem den elektronischen Bauteilen, was nach einiger Zeit zu einem Komplettausfall führen kann. In PCs ist das Netzteil eine weitere Fehlerquelle. Defekte Kondensatoren beispielsweise halten die Spannungen nicht mehr stabil, was zu zahlreichen Fehlfunktionen führen kann.

Ob sich alle Werte im Normbereich befinden oder ob es Auffälligkeiten gibt, erfahren Sie unter Linux mit Tools, die die Sensordaten auslesen. Weitere Tools informieren Sie über Gesundheit und Temperatur der Festplatten. Wie das funktioniert, zeigen wir am Beispiel Ubuntu 18.04, bei anderen Systemen kann das Vorgehen teilweise abweichen.



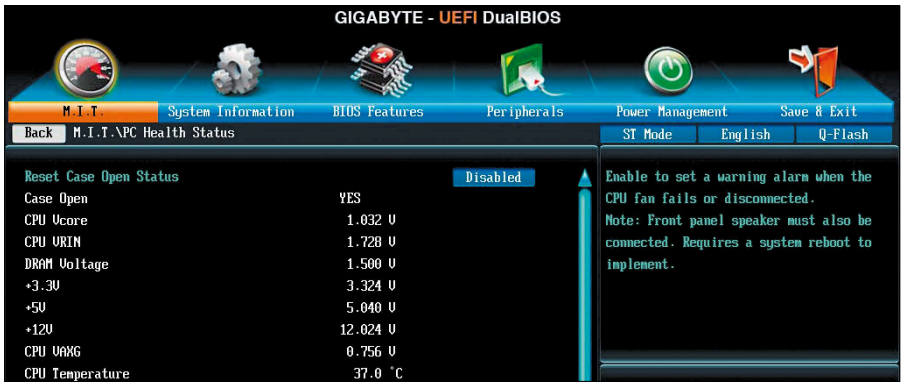
Sensoren auf der Hauptplatine messen Temperaturen und die Umdrehungszahlen der Lüfter. Einige Werte sind nicht plausibel, weil nicht alle Pins des Sensorchips belegt sind.

Messwerte über Bios/Firmware ermitteln

Nicht jede Hauptplatine ist mit Sensoren für Temperaturen und Spannungswerte ausgestattet. Vor allem bei Notebooks sind in der Regel keine Sensorchips verbaut. Was die Hardware kann, lässt sich im Bios/Firmwaresetup ermitteln. Bei Notebooks gibt es oft nur wenige Angaben, etwa zur Taktfrequenz und Temperatur der CPU. Bei Desktop-PCs finden Sie dagegen meist in einem Menü wie „PC Health“ oder ähnlich ausführlichere Informationen zu Spannungen, Temperaturen und den Umdrehungszahlen der Lüfter. Sind diese vorhanden, ist die Hauptplatine mit einem Sensorchip ausgestattet, der sich unter Linux wahrscheinlich auch per Software auslesen lässt.

Treiber für Sensoren einrichten

Der Linux-Kernel bietet Module, über die sich Hardwaredaten auslesen lassen, die aber nicht alle automatisch geladen werden. Um den passenden Treiber zu finden, installieren Sie das Paket „lm-sensors“ mit



Gesundheitsstatus: Ist ein Sensorchip vorhanden, finden Sie im Bios/Firmwaresetup meist Angaben zu den Versorgungsspannungen und der Lüfterdrehzahl.



Sensorchip auf dem Mainboard: Im Zweifelsfall suchen Sie den Chip auf der Hauptplatine. Die Hersteller sind oft Nuvoton, Winbond oder ITE.

diesem Terminalbefehl:

```
sudo apt install lm-sensors
```

Danach starten Sie das eigentliche Tool:

```
sensors
```

Auf den meisten PCs erhalten Sie nur Infos zur Temperatur der Prozessorkerne. Dafür ist ein Modul zuständig, das der Kernel standardmäßig lädt. Um weitere Sensoren zu finden, verwenden Sie diesen Befehl:

```
sudo sensors-detect --auto
```

Die Option „--auto“ sorgt dafür, dass alle Fragen automatisch mit dem vorgegebenen Wert beantwortet werden. Am Ende sehen Sie eine Liste der erforderlichen Kernel-Module. Im optimalen Fall hat sensors-detect den Sensorchip erkannt, beispielsweise „it87“ oder „nct6775“. Sollte nur „cortemp“ (Intel), „k10temp“ oder „k8temp“ (AMD) auftauchen, scrollen Sie im Terminal zum Beginn der Informationen und dann wieder nach unten. Achten Sie auf die Angabe „yes“ am Ende der Zeilen. Bei einem Test-PC mit der Hauptplatine MSI B250M PRO-VDH tauchte hier

```
Trying family 'VIA/Winbond/
  Nuvoton/Fintek'... Yes
Found unknown chip with ID 0xd352
```

auf. Sensors-detect hat zwar einen Sensor-Baustein gefunden, den Treiber aber nicht geladen, weil dieser offiziell die Version des Chips nicht unterstützt. In diesem Fall kann es helfen, das Laden des Treibers zu erzwingen, für unser Beispiel etwa mit dieser Befehlszeile:

```
sudo modprobe nct6775 force_
  id=0xd352
```

Sensors sollte dann deutlich mehr Informationen liefern, wenn der Treiber geladen wurde. Mit dem Terminalbefehl

```
dmesg
```

lassen Sie sich die letzten Kernel-Meldungen ausgeben. Bei Erfolg sehen Sie eine Info wie die folgende:

```
nct6775: Found NCT6795D or
  compatible chip at 0x4e:0xa20
```

Es gibt allerdings keine Gewähr dafür, dass das bei jeder Hauptplatine ähnlich funktioniert. Die Suche im Internet nach der gemeldeten ID in Verbindung mit „sensors“ liefert meist Ergebnisse mit den Erfahrungen anderer Benutzer.

Wenn sensors-detect nichts findet, obwohl ein Sensorchip vorhanden ist, versuchen Sie dessen Typ mit einem Blick auf die Hauptplatine herauszufinden. Es handelt sich meist um Bausteine mit der Aufschrift „Nuvoton“, „Winbond“ oder „ITE“ mit Abmessungen von circa 1 x 1 cm. Manchmal sind diese Informationen auch im Handbuch zu finden. Über eine Internetsuche ermitteln Sie, ob und wie dieser Chip sich unter Linux ansprechen lässt.

Treiber beim Systemstart laden: Damit die Sensorinformationen direkt nach einem Linux-Neustart zur Verfügung stehen, erstellen Sie eine Konfigurationsdatei:

```
sudo gedit /etc/modules-load.d/
  sensoren.conf
```

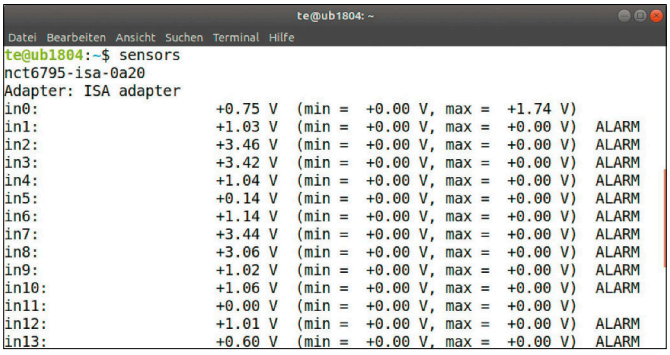
Tragen Sie die Namen der Treiber jeweils in einer eigenen Zeile ein. „cortemp“, „k10temp“ oder „k8temp“ müssen Sie nicht eintragen, weil der Kernel diese Module automatisch lädt. Wenn zusätzliche Optionen erforderlich sind, erstellen Sie zusätzlich die Datei „/etc/modprobe.d/sensoren.conf“. Hier tragen Sie beispielsweise diese Zeile

```
options nct6775 force_id=0xd352
```

ein.

Formatierung der Sensorwerte anpassen

Sensors gibt zahlreiche Werte aus, die sich nur teilweise von selbst erklären und auch nicht immer plausibel sind. Die Angaben zu den Umdrehungszahlen der Lüfter, beispielsweise hinter „fan2“ und „fan3“, stimmen meistens. Bei den Spannungsangaben, etwa hinter „in0“ bis „in14“, ist jedoch nichts von 12 oder fünf Volt zu sehen, son-



Unklare Ausgabe: Ohne passende Konfiguration zeigt sensors nur die Rohdaten. Welche Spannung sich hinter „in0“ oder „in1“ verbirgt, muss man erst herausfinden.

TEMPERATURENTWICKLUNG UNTER BELASTUNG

Probleme der Hardware zeigen sich oft erst, wenn die Temperatur unter höherer Last ansteigt. Das kleine Tool s-tui hilft Ihnen dabei, die CPU-Auslastung in die Höhe zu treiben, die Temperatur zu kontrollieren und damit die Wirksamkeit der Lüftung zu testen. s-tui ist mit einer einfachen grafischen Oberfläche für das Terminalfenster ausgestattet. Zur Installation verwenden Sie diese beiden Befehlszeilen:

```
sudo apt-get install gcc python-dev python-pip stress
sudo pip install s-tui
```

Danach starten Sie das Tool mit

```
s-tui
```

Das Programm zeigt die Taktfrequenz, Auslastung, Temperatur und Leistungsaufnahme des Prozessors an. Klicken Sie auf „Stress“, um den Belastungstest zu starten. Die Temperatur sollte dabei nicht über das für die CPU zulässige Maximum steigen und das Betriebssystem sollte weiter stabil laufen. Andernfalls reinigen Sie die Lüfter oder tauschen sie aus.

dern deutlich geringere Werte. Die Ursache dafür liegt im geringen Messbereich der Sensoren, meist 0 bis 4,08, 3,06 oder 2,048 Volt. Die Register liefern 256 Messwerte, sodass sich etwa bei 2,048 Volt acht Millivolt-Schritte ergeben. Höhere Spannungen werden durch vorgeschaltete Widerstände reduziert und müssen erst in die tatsächlichen Werte umgerechnet werden. Das erfolgt zusammen mit der Beschriftung der Einträge über die Datei „/etc/sensors3.conf", die Daten für einige meist ältere Sensorchips enthält. Ist ein unterstützter Chip enthalten, sehen Sie in der sensors-Ausgabe beispielsweise statt „in2" die Beschreibung „+3.3V". „sensors3.conf" wird bei einem Paketupdate überschrieben, daher sollten Sie in der Datei nichts ändern. Für eigene Anpassungen werden Konfigurationsdateien mit der Endung „.conf" im Ordner „/etc/sensors.d" berücksichtigt.

Vorbereitete Konfigurationsdateien finden Sie im Github-Projekt von lm-sensors (*www.pcwelt.de/lmsens*). Eventuell gibt es hier eine Datei, die genau zu Ihrem Mainboard passt. Kopieren Sie diese in den Ordner „/etc/sensors.d" und lesen Sie die Konfiguration mittels

```
sudo sensors -s
```

ein. Sensors zeigt dann Beschreibungen und die korrigierten Messwerte.

Korrekturwerte für Spannungen ermitteln

Wenn bei Github keine Konfigurationsdatei für Ihren PC zu finden ist, suchen Sie im Internet danach. Sollten Sie nichts finden, erstellen Sie die Datei selber. Als Vorlage kann eine der Github-Dateien für eine ähnliche Hauptplatine mit dem gleichen Sensorchip dienen.

Welche Versorgungsspannungen sich genau hinter den Ausgaben von sensors verbergen, lässt sich nicht ohne Weiteres herausfinden und ohne Dokumentation vom Mainboardhersteller nur erraten. Erste Hinweise gibt eine Beobachtung der Werte mittels des Befehls

```
watch -d sensors
```

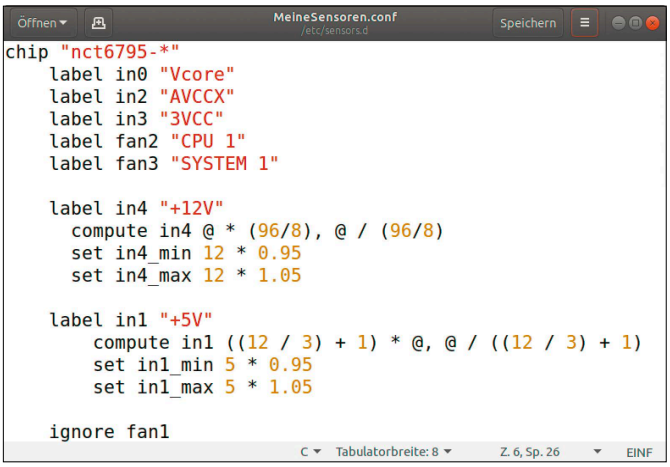
Durch „-d" werden die Änderungen hervorgehoben. Erzeugen Sie eine höhere Prozessorlast, beispielsweise über das Tool s-tui (siehe Kasten). Bei aktuellen CPUs verändert sich wenigstens ein Wert deutlich unter Last, etwa von 0,75 auf 1,08 Volt. Das ist typisch für die CPU-Kernspannung („Vcore"). Da sich die Spannung im Messwertbereich des Sensors bewegt, ist sie nicht skaliert und kann ohne Umrechnung verwendet werden.

Die Spannungen fünf und 12 Volt sind nur schwer zu identifizieren, da diese auf jeden Fall umgerechnet werden müssen. Eine allgemeine Anleitung dafür ist über *www.pcwelt.de/senso* zu finden. Es handelt sich um eine archivierte Seite des Wikis von lm-sensors.org, da die Website nicht mehr online ist.

Zur Berechnung benötigt man mehrere Messungen der Versorgung mit fünf und 12 Volt. Die findet man entweder über Bios-Screenshots im Internet, man beobachtet Schwankungen der Werte im Bios-Setup oder verwendet ein vom Boardhersteller geliefertes Tool unter Windows. Aus den Spannungsdifferenzen ergeben sich dann die skalierten Millivolt-Schritte, beispielsweise von 50 Millivolt. Wenn der Chip in 12-mV-Schritten misst und das Bios eine Spannung von 12,072 anzeigt, lautet die Rechnung: 12,072 V/ (50/12)=2,897 V. Wenn in der Ausgabe von sensors ein Wert um die 2,897 Volt auftaucht, handelt es sich wahrscheinlich um den Messwert für die 12-Volt-Spannungsversorgung.

Bei Sensorchips mit einem kleinen Messbereich von 2,048 Volt, wie dem NCT6795D in unserem Test-PC, liegen die Werte oft dicht beieinander. Man kann sich damit behelfen, den Skalierungsfaktor herauszufinden. Angenommen, das Bios zeigt 12,48 Volt an und Sensors liefert 1,02, 1,03, 1,04 Volt, dann ergibt sich bei Acht-mV-Schritten: 12,48/1,04*8=96. Die anderen Voltzahlen ergeben keine ganzzahligen Werte und scheiden daher wahrscheinlich aus, jedenfalls, wenn sich die Spannung inzwischen nicht geändert hat. Der Skalierungsfaktor ist in diesem Fall 96/8, also 12: 12,48 V / (96/8) = 1,04 V. Bei 5,5 und 3,3 Volt gehen Sie entsprechend vor. Die Skalierungsfaktoren können jedoch andere sein und aufgrund von Rundungsfehlern ergeben sich auch nicht immer ganzzahlige Faktoren.

Ausgabe anpassen: Über eine Konfigurationsdatei ändern Sie die Beschriftung der Sensoren und rechnen Spannungsangaben mit Korrekturfaktoren um.



Individuelle Konfiguration erstellen

Erzeugen Sie die eigene Konfigurationsdatei mit einem beliebigen Texteditor:

```
sudo gedit etc/sensors.d/
  MeineSensoren.conf
```

In der ersten Zeile muss „chip" gefolgt von der Typbezeichnung stehen. Wenn sensors „nct6795-isa-0a20" ausgibt, genügt „nct6795-*". Danach folgen Abschnitte für die einzelnen Sensoren, die jeweils mit „label" beginnen:

```
label in4 "+12V"
```

Dies weist dem Sensor „in4" einen aussagekräftigen Namen zu. In den „label"-Abschnitten lässt sich mit „compute" ein Spannungs- oder Temperaturwert umrechnen und mit „set" ein Minimal- und Maximalwert setzen. Mit „ignore" blenden Sie einen dahinter angegebenen Wert aus. Eine Beispielkonfiguration sehen Sie in der Abbildung oben.

Die Berechnung mit „compute" verwendet den jeweiligen Wert („@") und besteht aus zwei Teilen. Vor dem Komma wird die aktuelle Spannung mit dem zuvor ermittelten Korrekturfaktor multipliziert. Die Formel nach dem Komma wird für die Anpassung der Minimal- und Maximalwerte eingesetzt. Nachdem Sie die Konfigurationsdatei gespeichert haben, führen Sie

```
sudo sensors -s
```

aus und lassen sich die geänderten Werte dann mit sensors anzeigen.

```
te@ub1804: ~/Apps/DocFetcher-1.1.22
Datei  Bearbeiten  Ansicht  Suchen  Terminal  Hilfe
nct6795-isa-0a20
Adapter: ISA adapter
Vcore:                  +0.91 V  (min =  +0.75 V, max =  +1.35 V)
+5V:                    +5.16 V  (min =  +4.76 V, max =  +5.24 V)
AVCCX:                  +3.46 V  (min =  +2.98 V, max =  +3.63 V)
3VCC:                   +3.42 V  (min =  +3.14 V, max =  +3.47 V)
+12V:                  +12.48 V  (min = +11.42 V, max = +12.58 V)
in5:                    +0.15 V  (min =  +0.00 V, max =  +0.00 V)  ALARM
in6:                    +1.14 V  (min =  +0.00 V, max =  +0.00 V)  ALARM
in7:                    +3.44 V  (min =  +2.98 V, max =  +3.63 V)
in8:                    +3.06 V  (min =  +2.70 V, max =  +3.63 V)
in9:                    +1.02 V  (min =  +0.00 V, max =  +0.00 V)  ALARM
in10:                   +1.06 V  (min =  +0.00 V, max =  +0.00 V)  ALARM
in11:                   +0.00 V  (min =  +0.00 V, max =  +0.00 V)
in12:                   +1.00 V  (min =  +0.00 V, max =  +0.00 V)  ALARM
in13:                   +0.60 V  (min =  +0.00 V, max =  +0.00 V)  ALARM
in14:                   +1.55 V  (min =  +1.42 V, max =  +1.58 V)
CPU 1:                   976 RPM  (min =    0 RPM)
SYSTEM 1:                892 RPM  (min =    0 RPM)
```

Ohne Gewähr: Mit der geeigneten Konfiguration zeigt sensors sinnvolle Werte an. Ob die Berechnungen tatsächlich stimmen, zeigt erst eine längere Beobachtung.



Messdaten auf dem Desktop: Die Gnome-Shell-Erweiterung Freon zeigt die Temperaturen von Festplatten, der Grafikkarte sowie die Versorgungsspannungen an.

Grafische Oberfläche für Sensoren

Sobald lm-sensors konfiguriert ist, können Sie psensor für eine grafische Darstellung verwenden. Das Programm lässt sich unter Ubuntu über das gleichnamige Paket installieren. Psensor zeigt die gleichen Werte an wie sensors, allerdings keine Spannungen. Setzen Sie Häkchen in der Spalte „Graph“, um sich den Verlauf eines Wertes im Diagramm anzeigen zu lassen.

Über „Einstellungen“ im Menü legen Sie auf der Registerkarte „Providers“ fest, welche Sensoranbieter berücksichtigt werden sollen. Neben „lm-sensors“ gibt es auch Unterstützung für Sensoren auf Nvidia-Grafikkarten, wenn der proprietäre Nvidia-Treiber installiert ist. Unter „Hard disk drive“ aktivieren Sie „Enable support of udisks2“. Psensor liefert dann auch die Temperaturen der Festplatten. Soll Psensor automatisch starten, setzen Sie auf der Registerkarte „Startup“ ein Häkchen vor „Launch on session startup“. Das Tool zeigt sich auch über ein Symbol im Panel, das nach einem Klick darauf eine Übersicht mit den Sensordaten liefert.

Ein weiteres Tool ist die Erweiterung Freon für die Gnome-Shell, die sich ebenfalls als Symbol im Panel zeigt und bei Bedarf auch Infos zu den Versorgungsspannungen liefert. Für die Installation gehen Sie auf *https://extensions.gnome.org*. Hier richten Sie über den Link „Click here to install browser extension“ zuerst eine Firefox-Erweiterung ein. Nutzer von Ubuntu 18.04 müssen außerdem das Paket „chrome-gnome-shell“ installieren. Starten Sie Firefox neu, suchen Sie auf der Webseite nach „Freon“ und klicken Sie auf „Freon by UshakovVasilii“. Setzen Sie den Schalter rechts oben auf „On“ und bestätigen Sie per Klick auf „Installieren“. Nach kurzer Zeit meldet sich die Erweiterung mit den Temperaturangaben für Maximal- und Durchschnittswerte im Panel. Per Mausklick klappen Sie ein Menü mit weiteren Werten auf. Was angezeigt werden soll, legen Sie über „Sensoreinstellungen“ fest. Setzen Sie beispielsweise den Schalter hinter „Versorgungsspannung anzeigen“ auf „An“. Hinter „HDD/SSD-Temperaturdienst“ wählen Sie in der Regel „UDisks2“ und hinter „Grafikkartendienst“ einen Anbieter wie „Nvidia“ oder „Catalyst“ (AMD).

Zustand der Laufwerke prüfen

Festplatten und SSDs protokollieren Statusinformationen automatisch. Diese SMART-Werte (Self-Monitoring, Analysis and Reporting Technology) lassen sich auslesen und geben Hinweise auf Defekte. Starten Sie das Tool gnome-disks per Suche nach „Laufwerke“, bei Ubuntu 18.04 über „Aktivitäten“. Klicken Sie das gewünschte Laufwerk auf der linken Seite des Fensters an und drücken Sie die S-Taste.

Das Fenster zeigt die Temperatur des Laufwerks und die Betriebsstunden. Hinter „Allgemeine Einschätzung“ sollte „Das Laufwerk ist in Ordnung“ stehen – wenn nicht, sollten Sie an einen Austausch denken. Bei SSDs steht in der Tabelle hinter „wear-leveling-count“ in der Spalte „Normalisiert“ ein aussagekräftiger Wert. Neue SSDs starten mit „100“ und der Wert reduziert sich mit der Zeit. Sobald er nahe „0“ ist, sollten Sie das Laufwerk ersetzen.

Gnome-disks zeigt bei externen Laufwerken keine SMART-Werte und auch keine Temperatur an. Dafür benötigen Sie das Tool gsmartcontrol, das Sie über das gleichnamige Paket installieren. Per Doppelklick auf das gewünschte Laufwerk öffnen Sie das Infofenster. Auf der Registerkarte „Attributes“ sehen Sie die SMART-Werte und unter „Temperature Log“ die Temperatur.

Hinweis: Auch bei unauffälligen SMART-Werten kann ein Laufwerk jederzeit ausfallen. Vor Datenverlust schützen nur regelmäßige Backups. ■

SMART-Attribute

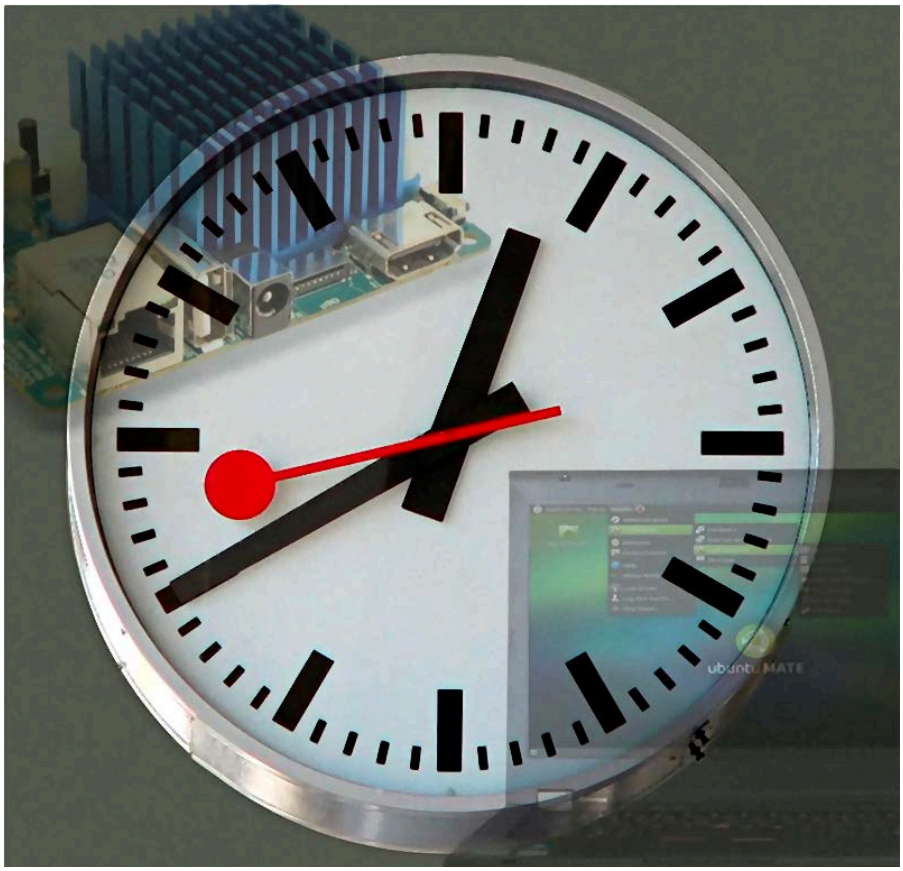
Kennung	Attribut	Wert	Normalisiert	Grenzwert	Schlechtester	Typ	Aktualisierungen	Einschätzung
5	Anzahl neu… Sektoren	0 Sektoren	100	10	100	Frühwarnung	In Betrieb	OK
9	Betriebsstunden	1 Jahr, 9 Monate und 1 Tag	96	0	96	Alterserscheinung	In Betrieb	OK
12	Einschaltvorgänge	811	99	0	99	Alterserscheinung	In Betrieb	OK
177	wear-leveling-count	19	99	0	99	Frühwarnung	In Betrieb	OK
179	used-reser…ocks-total	0	100	10	100	Frühwarnung	In Betrieb	OK
181	program-f…ount-total	0	100	10	100	Alterserscheinung	In Betrieb	OK
182	erase-fail-count-total	0	100	10	100	Alterserscheinung	In Betrieb	OK
183	runtime-b…lock-total	0	100	10	100	Frühwarnung	In Betrieb	OK
187	Gemeldet…are Fehler	0 Sektoren	100	0	100	Alterserscheinung	In Betrieb	OK
190	Temperatur der Luft	27° C / 81° F	73	0	51	Alterserscheinung	In Betrieb	OK
195	Durch Har…e Bitfehler	0	200	0	200	Alterserscheinung	In Betrieb	OK
199	UDMA-CRC-Fehlerrate	0	100	0	100	Alterserscheinung	In Betrieb	OK
235	Rate der f…ien Blöcke	nicht verfügbar	99	0	99	Alterserscheinung	In Betrieb	OK
241	total-lbas-written	nicht verfügbar	99	0	99	Alterserscheinung	In Betrieb	OK

Festplatten-Selbsttest: Das Systemtool gnome-disks kann die SMART-Werte interner Laufwerke auslesen. „wear-leveling-count“ kann bei alten SSDs in Richtung „0“ gehen.

Rechner automatisch abschalten & starten

Weder Desktop-PCs noch Serverdienste müssen permanent laufen, wenn es eindeutige Zeiten gibt, wo keiner sie nutzt. Manuelles Abschalten ist die übliche Lösung, komfortabler aber sind der automatische Shutdown und ein zeitgesteuerter Neustart.

VON HERMANN APFELBÖCK



© conrad.de / avm.de

Wenn ein Datenserver zwischen 22:00 Uhr abends und 8:00 Uhr morgens garantiert nicht gebraucht wird, liegt es nahe, ihn für diese zehn Stunden abzuschalten. Das spart nicht nur Strom, sondern verlängert auch die Lebenszeit der Hardwarekomponenten. Das zeitgesteuerte Ausschalten ist per Cronjob eine leichte Übung, aber optimal wird der Hardwareschlaf erst, wenn auch das Aufwachen ohne manuellen Eingriff des (Home-)Administrators gelingt.

Rtcwake: Unterschätztes Standardwerkzeug

Das einschlägige Tool, um einen Rechner komplett auszuschalten (oder – falls unterstützt – in einen ACPI-Ruhezustand zu versetzen) und ihn zur gewünschten Zeit wieder zu starten, ist auf praktisch jedem Linux-System vorinstalliert. Rtcwake ist Bestandteil des Standardpakets „util-linux". Das „rtc" im Toolnamen steht für Real Time Clock und bezieht sich auf die physikalische Hardwareuhr.

Diese läuft auch, wenn die Hardware in einem Ruhezustand oder komplett ausgeschaltet ist und kann den Neustart auslösen, wenn ein definierter Zeitpunkt erreicht ist. Unter Linux ist dieser Zeitpunkt standardmäßig in der Datei „/sys/class/rtc/rtc0/wakealarm" abgelegt und das Tool rtcwake ist das Werkzeug, diesen Zeitpunkt vorzugeben.

Im einfachsten Fall sieht ein Kommando folgendermaßen aus:

```
sudo rtcwake -m off -s 180
```

Der Befehl ist gut geeignet, um zu testen, ob die Hardware prinzipiell mitspielt. sudo oder root-Recht ist immer erforderlich. Der Schalter „-m" bestimmt den ACPI-Modus. Mögliche Werte sind „standby", „mem", „disk", „off" und „no". Letzteres „no" kann dazu dienen, einen Aufwachzeitpunkt festzulegen, ohne den Rechner in irgendeiner Weise zu beenden. „standby", „mem", „disk" sind Suspendvarianten unterschiedlicher Schlaftiefe. Für unsere Zwecke einschlägig ist „off", welches das System komplett herunterfährt.

Als zweiter Parameter ist hier „-s" („seconds") mit einer nachfolgenden Zeitangabe in Sekunden angegeben. Der Befehl wird also, wenn die Hardware mitspielt, das System komplett beenden und dann nach drei Minuten neu starten (180 Sekunden). Wir empfehlen, den geplanten Neustart immer mit diesem Parameter „-s [...]" anzugeben,

selbst wenn es sich um viele Stunden handelt. Es ist wenig Mühe, etwa neun Stunden in Sekunden umzurechnen (9*3600=32 400). Mit dem Schalter „-t“ („time“) ist auch eine exakte Zeitangabe möglich. Da diese Zeitangabe immer in Linux-Sekunden seit dem 1.1.1970 zu berechnen ist, muss in der Regel eine Date-Variable aushelfen:

```
sudo rtcwake -m off -t $(date +%s -d
 'tomorrow 08:00')
```

Dies würde den Rechner ausschalten und am nächsten Tag um 8:00 Uhr wieder einschalten. Achten Sie beim Hantieren mit Schalter „-t“ darauf, dass bei einem Herunterfahren nach Mitternacht „today“ statt „tomorrow“ gewählt werden muss. Aber wie schon angesprochen: Eine Zeitangabe in Sekunden mit Schalter „-s“ ist stets der einfachere Weg.

Rtcwake als Cronjob

Da rtcwake root-Recht erfordert, müssen solche Befehle in der Crontab von root untergebracht werden (in einer User-Crontab würde der Befehl einfach ignoriert). Die Crontab von root bearbeiten Sie mit folgendem Kommando:

```
sudo crontab -e -u root
```

Wenn in der crontab keine PATH-Anweisung steht, ist die volle Pfadangabe zum benötigten Kommando erforderlich:

```
0   1   *   *   *  /usr/sbin/rtcwake
 -m off -s 30600
```

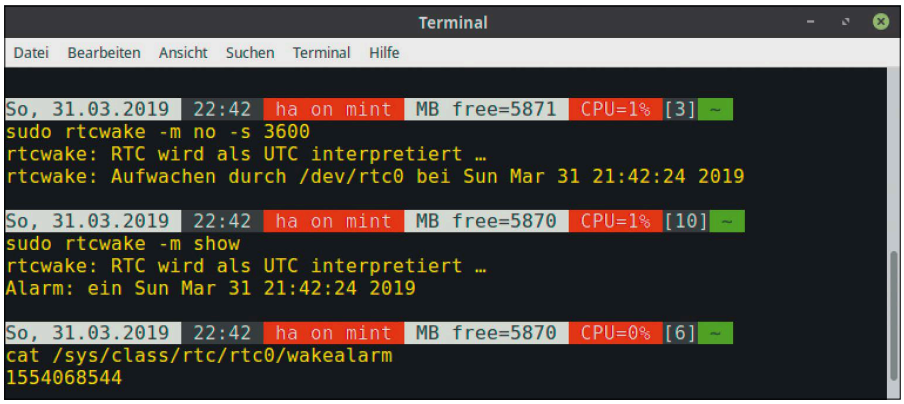
Dieser Befehl schaltet den Rechner um 1:00 Uhr nachts ab und startet ihn wieder nach 30 600 Sekunden, das sind 8,5 Stunden und somit exakt um 9:30 Uhr. Die Pfadangabe „/usr/sbin/rtcwake“ sollte auf jedem Linux zutreffen, kann aber mit

```
which rtcwake
```

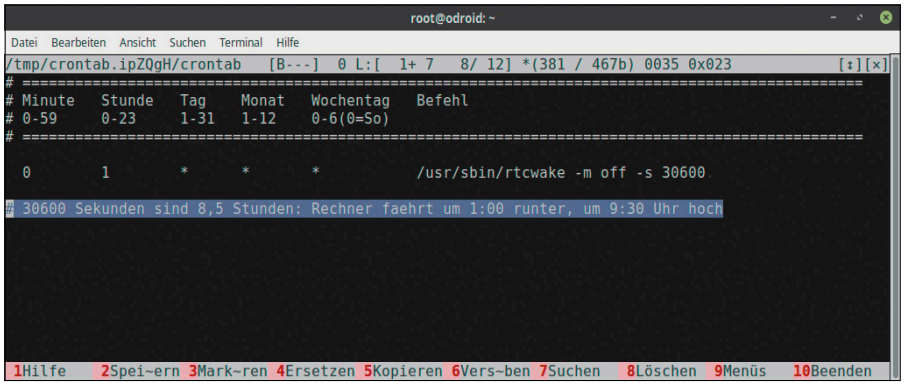
vorsichtshalber vorab geprüft werden.

Rtcwake funktioniert nicht mit jeder Hardware

Während PCs, Notebooks und auch Platinenrechner wie der Odroid XU4 den beschriebenen Einschlaf-Aufwach-Automatismus zuverlässig mitspielen, ist die Methode leider nicht überall tauglich. So beantwortet etwa der Raspberry 3 rtcwake generell mit einer Fehlermeldung, während ein Odroid U3 zwar herunterfährt, aber nicht planmäßig startet. Letztlich hilft nur Ausprobieren. Was per root-Crontab in jedem Fall funktioniert (*sudo crontab -e -u root*), ist der zeitgesteuerte Shutdown – im folgenden Beispiel wieder um 1:00 Uhr nachts:



Der Aufwachzeitpunkt: Die Arbeitsweise von rtcwake ist eigentlich simpel, insofern es nur eine einzige Linux-Sekunden-Angabe in eine Datei schreibt (wakealarm). Durch die UTC-Zeitverschiebungen ist die Analyse aber knifflig. Ausprobieren hilft.



Ein Befehl mit zwei Aufgaben: Rtcwake fährt den Rechner herunter und legt den Zeitpunkt des Neustarts fest. Den Zeitpunkt des Shutdowns bestimmt die Crontab.

```
0   1   *   *   *  /sbin/shutdown
 now
```

Da Platinenrechner typischerweise booten, wenn die Stromzufuhr zunächst unterbrochen und zur passenden Zeit wieder eingeschaltet wird, kann man sich für den zeitgesteuerten Neustart mit einer einfachen mechanischen oder digitalen Zeitschaltuhr behelfen (ab fünf Euro).

Wer die Aufgabe ganz schick lösen will, kann auch eine intelligente Funksteckdose verwenden. Fritzbox-Besitzer erhalten für 40 Euro den flexiblen Stecker Fritz Dect 200, der sich über die Fritzbox-Konfiguration („Heimnetz → Smart Home“) komfortabel einstellen lässt.

Egal, ob primitive mechanische Zeitschaltuhr oder vergleichsweise edle Funksteckdose: Beachten Sie immer, den Zeitpunkt des ordentlichen Systemshutdowns über die Crontab einige Minuten früher zu legen als das Abschalten der Stromversorgung. ■



Wenn die Rechnerhardware den Start mit rtcwake nicht mitmacht, können Zeitschaltstecker aushelfen: Zubehör wie die Funksteckdose Fritz Dect 200 ist eine anspruchsvolle Lösung (40 Euro), die mechanische Brennenstuhl-Zeitschaltuhr links kostet kaum sechs Euro.

Fritzbox: Tipps & Tuning

Router sind die zentralen Schaltstellen im Heimnetzwerk. Wer die umfangreichen Optionen des Routers und namentlich der AVM Fritzbox ignoriert, verschenkt erhebliches Potenzial. Dieser Beitrag liefert Tipps für den optimalen Einsatz des AVM-Routers.

VON HERMANN APFELBÖCK

Es gibt tatsächlich den Typus PC-Nutzer, der mit Begeisterung am System und am Desktop bastelt, aber das fundamentale Gerät seines Netzwerkes schlicht vergisst. DSL- und Kabelrouter verrichten in dunklen Ecken der Wohnung oft unbeachtet ihre Arbeit. Es lohnt sich aber, dem Gerät mehr Aufmerksamkeit zu schenken, dies umso mehr, wenn es sich um eine Fritzbox handelt. Die Konfiguration des Routers ist mit *http://fritz.box* oder mit *http://192.168.178.1* (so der Standard) mit jedem Browser zu erreichen.

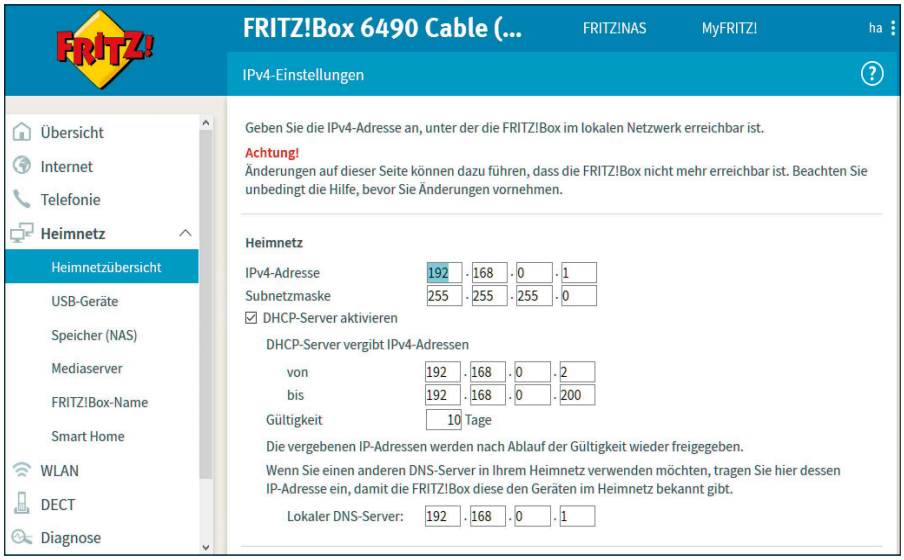
1. Fast Ethernet oder Gigabit-LAN

Wer überwiegend Netzgeräte mit Gigabit-Ethernet besitzt, sollte unbedingt unter „Heimnetz → Heimnetzübersicht" die „Netzwerkeinstellungen" kontrollieren. Die vier LAN-Ports der Fritzbox, LAN 1 ausgenommen, sind nämlich im Auslieferungszustand in der Regel gedrosselt. Sie laufen im stromsparenden „Green Mode" mit Fast-Ethernet-Leistung, also mit 100 MBit/s. Setzen Sie auf „Power Mode", wenn der angeschlossene Client oder Switch das unterstützt.

2. IP und Adressraum des Routers

Heimanwendern ist es oft egal, ob der Router mit der IP 192.168.178.1 oder 192.168.1.1 vorkonfiguriert ist und damit für alle lokalen Geräte den Adressraum 192.168.178.[1–255] oder 192.168.1.[1–255] vorgibt. Anders steht es, wenn ein neuer Router in ein sorgfältig konfiguriertes Netz kommt, wo Serverdienste mit fester IP eingerichtet sind und Scripts oder Browser-Lesezeichen bestimmte IP-Adressen erwarten.

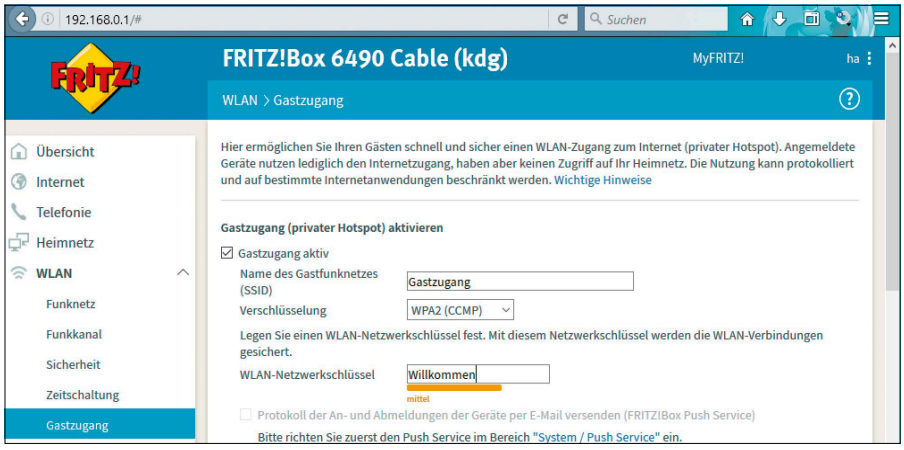
Hier wäre die Umstellung aller Details auf einen neuen Adressraum eine zeitraubende Aufgabe. Alle Router erlauben daher die manuelle Einstellung der eigenen IP. In der Fritzbox gehen Sie auf „Heimnetz → Heimnetzübersicht → Netzwerkeinstellungen". In der erweiterten Ansicht finden Sie die Schaltfläche „IPv4-Adressen". Hier können Sie ganz oben die gewünschte IP-Adresse festlegen.



IP-Adresse einer neuen Fritzbox ändern: Dies ist eine wichtige Einstellung, wenn ein neuer Router in ein sorgfältig eingerichtetes Netzwerk Einzug hält.

3. Gastzugang: WLAN und LAN4

Mit dem Gastzugang unter „WLAN → Gastzugang → Gastzugang aktiv" kann die Fritzbox für Gäste einen separaten Internetzugang bereitstellen, der vom übrigen Netzwerk getrennt ist. Das Gast-WLAN erhält eine eigene Netzwerkkennung (SSID) und



Vorkonfigurierter Gastzugang für Besucher: Sie müssen das primäre WLAN-Kennwort nicht preisgeben und halten Gäste vom lokalen Netzwerk fern (Client Isolation).

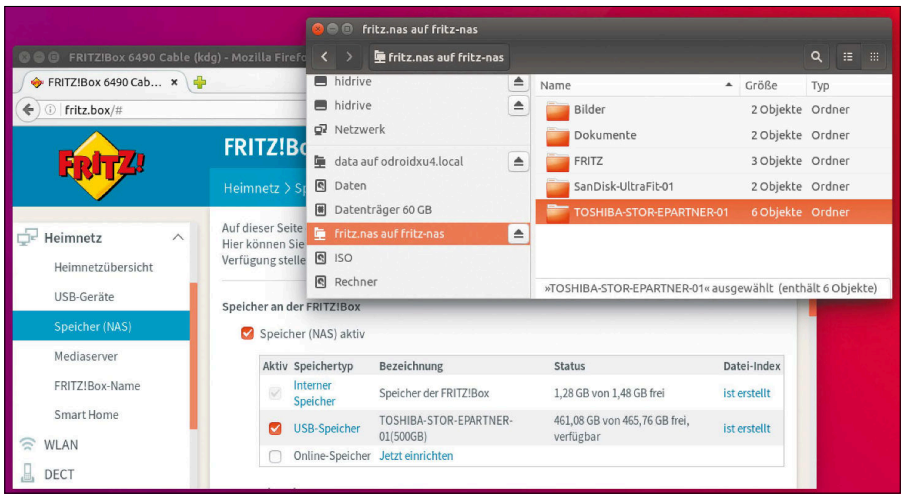
ein eigenes Passwort. Sie müssen also nicht das primäre WLAN-Passwort an Gäste weitergeben. Außerdem hat das Gast-WLAN keinen Zugriff auf das lokale Netzwerk und dessen Samba- oder SSH-Freigaben (Client Isolation). Wenn Sie die zusätzliche Option „Internetanwendungen beschränken: Nur Surfen und Mailen erlaubt“ aktivieren, dann sind im Gastnetz auch alle Ports geschlossen, die für FTP oder Bittorrent zuständig sind. Um etwa Fotos oder Musik über das WLAN auszutauschen, können Sie den Gastgeräten aber erlauben, miteinander zu sprechen. Dazu markieren Sie die Option „WLAN-Geräte dürfen kommunizieren“.

Die Fritzbox sieht neben dem Gast-WLAN auch einen verkabelten Gastzugang am LAN-Port 4 vor. Der lässt sich unter „Heimnetz → Heimnetzübersicht → Netzwerkeinstellungen“ mit einem Mausklick aktivieren. Weitere Einstellungen gibt es hier nicht: Für das angeschlossene Gerät gilt erneut die Client Isolation, die keine Kommunikation mit dem lokalen Netz zulässt.

4. Kindersicherung für das Internet

Jeder Home-Admin mit Verantwortung für Heranwachsende sollte sich die Zeit nehmen, die „Kindersicherung“ der Fritzbox zu bearbeiten. Kinder und Jugendliche lassen sich zeitlich wie inhaltlich durch die technische Autorität des Routers reglementieren, ohne sie ständig selbst kontrollieren zu müssen. Die Regeln sind für jedes einzelne Netzgerät unter „Internet → Filter → Kindersicherung“ zu aktivieren. Voraussetzung sind Zugangsprofile („Standard“, „Unbeschränkt“), dem Sie dann das jeweilige Gerät zuweisen. Dabei gibt es Zeitbeschränkungen, Protokollverbote sowie die Möglichkeit, eine erlaubte Whitelist (sehr restriktiv) oder eine verbotene Blacklist anzulegen. Die Blacklist kann man manuell ergänzen, aber das vorgegebene BPJM-Modul (Bundesprüfstelle für jugendgefährdende Medien) kann die Hauptarbeit leisten. Das Modul lässt sich unter „Internet → Filter“ einfach per Häkchen aktivieren. Die Beschränkungen für den oben erklärten „Gast“-Zugang basieren übrigens ebenfalls auf einem „Zugangsprofil“.

Haben Sie unter „Internet → Filter → Zugangsprofile“ etwa das neue Profil „Kids“ angelegt, weisen Sie unter „Kindersicherung“ dem Rechner oder Smartphone des Kindes ganz rechts per Klickbox dieses „Zugangsprofil“ zu.



Fritz-Datenserver auf der Konfigurationsoberfläche und im Dateimanager: Die Einrichtung eines USB-Datenträgers im Fritz-NAS ist einfacher als jede Serverlösung.

5. USB-Laufwerke im Netzwerk

Einfacher als mit dem eingebauten Fritz-NAS kommen Sie nicht an einen zentralen Netzwerkspeicher. Sie können die Inhalte von USB-Datenträgern dauerhaft und auch jederzeit ad hoc im ganzen Heimnetz bereitstellen: Stecken Sie das USB-Laufwerk einfach an einen der USB-Ports der Fritzbox. Fritz-OS kann mit Linux- (Ext) und Windows-Dateisystemen (NTFS, FAT) umgehen. Der angeschlossene Datenträger ist im Browser über *http://fritz-nas/* für Uploads und Downloads erreichbar, aber natürlich auch als Samba-Freigabe unter „Netzwerk“ in Linux- oder Windows-Dateimanagern.

Damit dies jederzeit funktioniert, muss lediglich einmal und damit dauerhaft die NAS-Funktion aktiviert werden. Das erfolgt unter „Heimnetz → Speicher (NAS) → Speicher (NAS) aktiv“. Für den Zutritt ist außerdem ein Benutzerkonto mit Kennwort erforderlich, das Sie unter „System → Fritz!Box-Benutzer“ einrichten.

Wenn Sie einen USB-Datenträger wieder entfernen möchten, sollten Sie ihn nicht einfach abziehen, sondern vorher im Fritzbox-Konfigurationsfenster „Heimnetz → USB-Geräte“ aushängen, indem Sie den Auswurf-Button anklicken oder die Schaltfläche „Alle sicher entfernen“.

Die Leistung des Fritz-NAS hängt vom Netzwerk (Gigabit oder Fast Ethernet) und von den USB-Ports ab. Ältere Fritzboxen bieten nur USB 2.0 und auch in relativ neuen Modellen 6490 (das Kabelmodell, das weitgehend 7490 entspricht) ließ Vodafone USB 2.0 verbauen.

6. MAC-Filter fürs Funknetz

MAC-Filterung ist eine verschärfende Maßnahme, die nur noch definierte Geräte ins WLAN lässt. Skeptiker werden einwenden, dass die dazu abgefragte MAC-Adresse des WLAN-Clients so eindeutig nicht ist, weil jedes Linux eine beliebige MAC-Adresse vorgaukeln kann („MAC-Spoofing“ etwa mit ifconfig). Das ist richtig, jedoch müsste der Einbrecher wissen, welche MAC-Adressen der Router erlaubt, oder aber unzählige Adressen ausprobieren. 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 Geräte zugelassen. Die Option „WLAN-Zugang auf die bekannten WLAN-Geräte beschränken“ aktiviert den MAC-Filter. Dieser Schutz ist nicht ganz bequem: Jedes hinzukommende Gerät im Haushalt oder jedes Besuchergerät muss hier später explizit mit seiner MAC-Adresse aufgenommen werden („WLAN-Gerät hinzufügen“). Es empfiehlt sich daher, vor dem Aktivieren des MAC-Filters alle benötigten Geräte anzumelden, sodass 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“) und in Windows über „Netzwerk und Internet → Verbindungseigenschaften“, in Android unter „Einstellungen → Allgemein → Geräteinformationen → Status“.

7. WLAN-Netzwerknamen unterdrücken

Die SSID (WLAN-Name) muss nicht für alle Nachbarn sichtbar sein. In der Fritzbox lässt sich dies 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. Allerdings zeigen Wi-Fi-Scanner den Netznamen auch dann an, wenn er unterdrückt wird. Die Maßnahme hilft also nur gegen technisch unbedarfte Nachbarn.

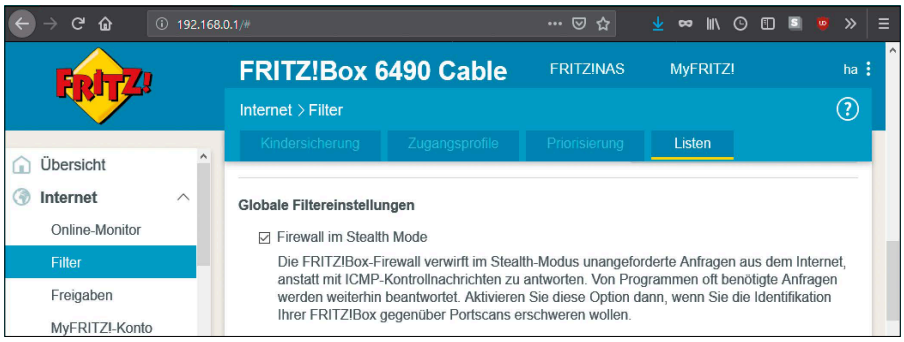
8. Router im „Stealth-Modus“

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 Portscan ein allgemeiner Ping-Befehl vorausgeht, ob die IP-Adresse überhaupt erreichbar ist, dann wird das Script in der Tat weiterreisen, weil die Fritzbox nicht antwortet.

Der Nutzwert ist aber relativ: Wenn der Angriffsversuch mit einem zeitaufwendigeren „nmap -Pn“ erfolgt, wird die Fritzbox trotz Stealth-Modus antworten. Es hängt also davon ab, welche Genauigkeit und welchen Zeitaufwand ein Portscan ansetzt. Wenn Hacker Tausende Adressbereiche möglichst schnell scannen wollen, nehmen sie unter Umständen nur einfachste Mittel. Diese einfachen Abfragen wehrt der Stealth-Modus ab. Relevant ist die Maßnahme nur, wenn Sie über Portfreigaben (→ Tipp 13) Serverdienste im Internet anbieten.

9. Priorisierung von Geräten

Das Heimnetz ist ohne manuellen Eingriff basisdemokratisch: Jedes Gerät darf die volle Bandbreite beanspruchen. Das ist überall, wo es konfliktfrei funktioniert, der einfachste Zustand. Wenn aber der Office-PC bei ernsthaften Recherchen gebremst wird, weil an anderer Stelle weniger ernsthafte Youtube-Videos laufen, kann die Fritzbox helfen: Der Punkt lautet „Internet → Filter → Priorisierung“. Über „Neue Regel“ unter „Priorisierte Anwendungen“ geben Sie das Gerät an, das ungebremst arbeiten soll. Der Vorrang kann auf eine bestimmte Anwendung wie etwa SSH beschränkt werden oder für den privilegierten Rechner global gelten („alle“ unter „Netzwerkanwendungen“).



Der Stealth-Modus kann nicht schaden: Genauere Portscans werden Ihr Netzwerk trotzdem finden, aber auf einfache Ping-Anfragen antwortet die Fritzbox nicht.

10. Fritzbox als Druckerserver

Die Fritzbox bringt ältere Drucker ohne LAN und WLAN per USB ins Heimnetz. Schließen Sie den Drucker an einen USB-Port des Routers an und schalten Sie ihn ein. Die Fritzbox wird jetzt den Drucker unter „Heimnetz → USB-Geräte → Geräteübersicht“ melden. Nun gehen Sie auf einem Linux-PC in den Systemeinstellungen auf „Drucker“ und „Hinzufügen“. In der Geräteliste wählen Sie „AppSocket/HP JetDirect“ und geben rechts oben als „Rechner“ die IP-Adresse der Fritzbox an. Unter Windows nutzen Sie unter „Geräte und Drucker → Drucker hinzufügen“ die Option „Drucker unter Verwendung einer TCP/IP-Adresse oder eines Hostnamens hinzufügen“.

11. Fritzbox als Faxgerät

Die Fritzbox zeigt unter „Telefonie → Fax“ die Option „Faxfunktion einrichten“. Hier tragen Sie Ihre Mailadresse ein, ferner das Kennwort und den SMTP-Server. Die Daten können Sie im Zweifel etwa Ihrem Thunderbird-Mailclient entnehmen (Servereinstellungen und Postausgangsserver). An diese Mailadresse werden die Faxe dann weitergeleitet und auf Wunsch auch noch im Fritzbox-NAS abgelegt. Bei mehreren Telefonanschlüssen können Sie die gewünschte Rufnummer für den Faxempfang auswählen.

12. Feste IP für einen Server

Server benötigen eine feste IP-Adresse. Wenn Sie unter „Heimnetz → Heimnetzübersicht“ in der Zeile des gewünschten Geräts „Details“ anklicken, sehen Sie dort die Option „Diesem Netzwerkgerät immer die gleiche Ipv4-Adresse zuweisen“. Allerdings können Sie hier keine Wunsch-IP vergeben, sondern müssten die gerade aktuelle IP des Geräts akzeptieren. Ist diese IP nicht erwünscht, geht es auch anders: Unter „Heimnetz → Netzwerkverbindungen“ gibt es ganz unten die Schaltfläche „Gerät hinzufügen“. Hier geben Sie „Name“ (Hostname) und „MAC-Adresse“ des Geräts ein, darunter die Wunsch-IP. Der Router wird nun melden, dass ihm das Gerät unter einer anderen IP bekannt ist, und Sie müssen mit „OK“ bestätigen, dass Sie die Einstellung überschreiben wollen. Danach starten



Feste IP-Nummer: Server sollten im Netzwerk immer über dieselbe Adresse erreichbar sein. In der Fritzbox-Konfiguration lässt sich das für jedes einzelne Gerät festlegen.

Sie das Gerät neu. Hostname und die physikalische MAC-Adresse erfahren Sie mit den Terminalbefehlen „hostname“ und „ifconfig“ auf dem jeweiligen Gerät. Unter Windows heißt der Befehl „ipconfig“.

13. Webfreigaben für Serverdienste

Wer einen heimischen Daten- oder Webserver über das Internet erreichen will, muss einen Port nach außen öffnen. Dies geschieht in der Fritzbox unter „Internet → Freigaben → Portfreigaben“. Die Vorgehensweise nach „Neue Portfreigabe“ ist einfach und am globalsten über „Andere Anwendungen“ zu erreichen: Entscheidend ist „von Port“ und „bis Port“. Meistens ist nur ein Port erforderlich und dann steht hier in beiden Feldern dieselbe Zahl. Sie können einen beliebigen Phantasieport wie etwa „22222“ angeben, den Sie sich aber einprägen müssen. Ein beliebig gewählter Außenport erhöht die Sicherheit, weil Angreifer oft ohne Portanalyse nur Standardports wie 80 (HTTP) oder 22 (SSH) abfragen.
Entscheidend ist dann die Zielangabe „an Computer“. Das muss der lokale Server sein, der den Dienst anbietet. Die Angabe „an IP-Adresse“ trägt die Fritzbox nach Auswahl des Rechners aus der Liste automatisch ein. Der Server muss unbedingt eine feste IP verwenden, damit die Webanfragen richtig ankommen. Ganz unten tragen Sie „an Port“ ein – das ist nun der reale Port, über welchen der Dienst läuft, also etwa 80 (HTTP) oder 22 (SSH). Von außen kommen Sie ab sofort über Ihre öffentliche IP-Adresse plus Angabe der Portnummer an Ihren Serverdienst. Anstatt eines Aufrufs im lokalen Netz der Form (Beispiel)

```
http://192.168.178.10/dokuwiki
```

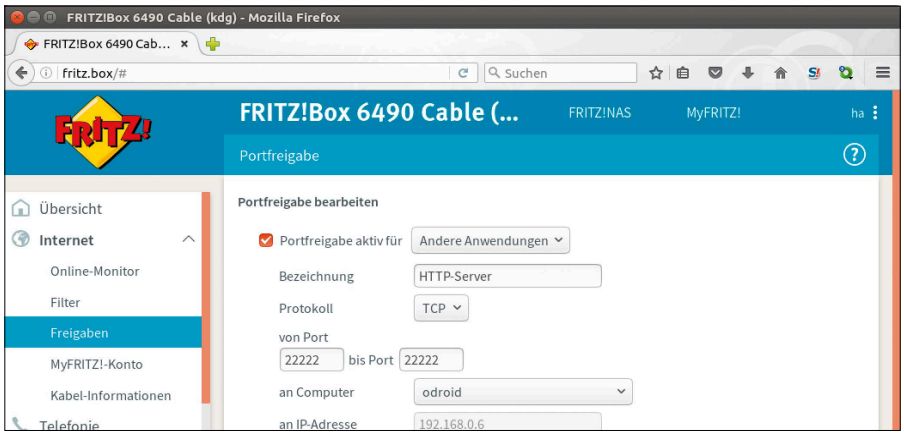
könnte der Aufruf aus der Ferne dann etwa

```
http://178.27.56.125:22222/
  dokuwiki
```

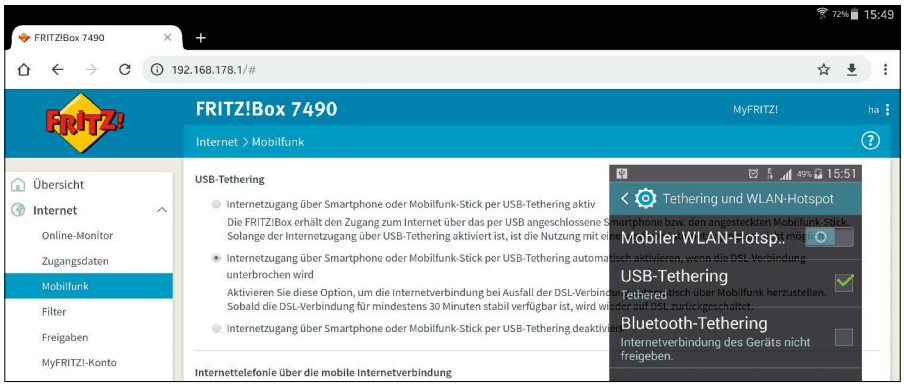
lauten. Dazu müssen Sie die öffentliche und täglich wechselnde IP kennen (oder einen Dyn-DNS-Dienst benutzen).

14. Notfallwerkzeuge der Fritzbox

Sollte eine Fritzbox über *http://fritz.box* oder die Standard-IP *http://192.168.178.1* nicht mehr erreichbar sein, etwa weil Sie für den Router eine falsche IP-Adresse eingestellt haben, dann hilft der eingebaute Notzugang. Die Konfiguration des Routers lässt sich immer auch über die IP-Adresse



Portfreigabe für den Webzugriff: Der öffentliche Port („von Port“) kann willkürlich gewählt werden, der Zielport („an Port“) muss genau stimmen und zur richtigen (lokalen) IP-Adresse führen.



Notmaßnahme: Ein per USB an die Fritzbox angeschlossenes Smartphone kann über den Mobilfunk das Heimnetz versorgen – mit unvermeidlichen Geschwindigkeitseinbußen.

http://169.254.1.1 aufrufen. Hier können Sie im Bestfall Konfigurationsfehler manuell beheben – fundamental etwa unter „Heimnetz → Heimnetzübersicht → Netzwerkeinstellungen“ sowie „Internet → Freigaben“ und „Internet → Filter“. Schlimmstenfalls kann die Fritzbox unter „System → Sicherung → Werkseinstellungen“ auch komplett zurückgesetzt werden. Besser ist es, wenn eine Sicherung der Konfiguration vorliegt, die Sie mit „System → Sicherung → Wiederherstellen“ importieren können. Diese Vorsorge sollten Sie treffen, wenn der Router optimal eingerichtet ist: Nach „System → Sicherung → Sichern“ fordert die Fritzbox ein Kennwort für die Sicherungsdatei, danach sogar noch einen Druck auf eine Fritzbox-Taste. Die Datei bewahren Sie an gut erreichbarer Stelle auf, eventuell inklusive Kennwort im Dateinamen (in einem privaten Netzwerk).

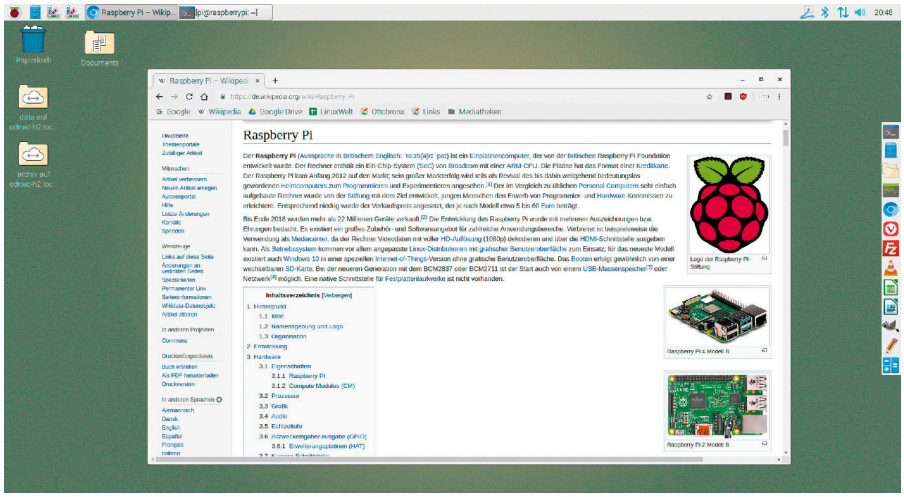
15. Mobilfunk bei Providerstörung

Die Fritzbox bietet über USB die Möglichkeit, einen LTE-Stick anzuschließen, um darüber online zu gehen. Unter „Internet → Mobilfunk“ gibt es dann die zusätzliche Option „Mobilfunkverbindung automatisch aktivieren, wenn die DSL-Verbindung unterbrochen wird“. Der Mobilfunk springt dann automatisch ein, wenn DSL ausfällt. Beachten Sie, dass die Fritzbox den Eintrag „Mobilfunk“ nur anzeigt, wenn tatsächlich ein LTE-Stick angeschlossen ist.
Auch Smartphones können dabei aushelfen. Verbinden Sie das Handy per USB-Kabel mit der Fritzbox. Auf dem (Android-) Smartphone gehen Sie unter „Einstellungen“ auf „Drahtlos & Netzwerke → Tethering & mobiler Hotspot“ und aktivieren „USB-Tethering“.
Auch jetzt zeigt die Konfigurationsoberfläche der Fritzbox unter „Internet” zusätzlich den Eintrag „Mobilfunk“. Aktivieren Sie dort den Eintrag „Internetzugang über Smartphone oder USB-Tethering“. Danach können alle Geräte wieder über die Fritzbox online gehen, dies allerdings mit der vermutlich geringeren Bandbreite der mobilen Datenübertragung. ■

Raspberry Pi 4 als Desktop

Schon älteren Modellen des Raspberry Pi wurde Desktoptauglichkeit angedichtet. Dass der deutlich leistungsstärkere Pi 4 diese Rollendiskussion neu anheizt, war zu erwarten. Und in der Tat: Bei richtiger Konfiguration taugt der Pi 4 allemal als Zweitdesktop.

VON HERMANN APFELBÖCK



Eigentlich sollte es selbstverständlich sein, dass von einer kleinen Platine zum Preis von 50 oder 60 Euro keine echte PC-Leistung zu erwarten ist. Der Raspberry Pi wurde als Bastelplatine geboren und kann sich inzwischen uneingeschränkt als Dateiserver, Mediencenter oder HDMI-Zuspieler für das TV-Gerät bewähren. Nachdem der Pi 4 nun aber bis zu vier GB RAM und eine Quadcore-CPU mit 1,5 GHz mitbringt, wird er gerne mit älteren Notebooks und PCs ähnlicher Ausstattung verglichen, die ja ihrerseits als Hardware für den Desktopbetrieb konzipiert waren. Das verkennt aber die Tatsache, dass ARM-CPUs mit vergleichbarer Kernzahl und Taktung nicht annähernd die Leistung der x86-CPUs (von Intel und AMD) erreichen. Trotzdem ist der Einsatz des Raspberry 4 als Desktopsystem realistisch, sofern man diese Rolle eindeutig festlegt, seine Multitaskinganspruche nicht übertreibt – und vor allem das Betriebssystem auf eine schnelle SD-Karte schreibt.

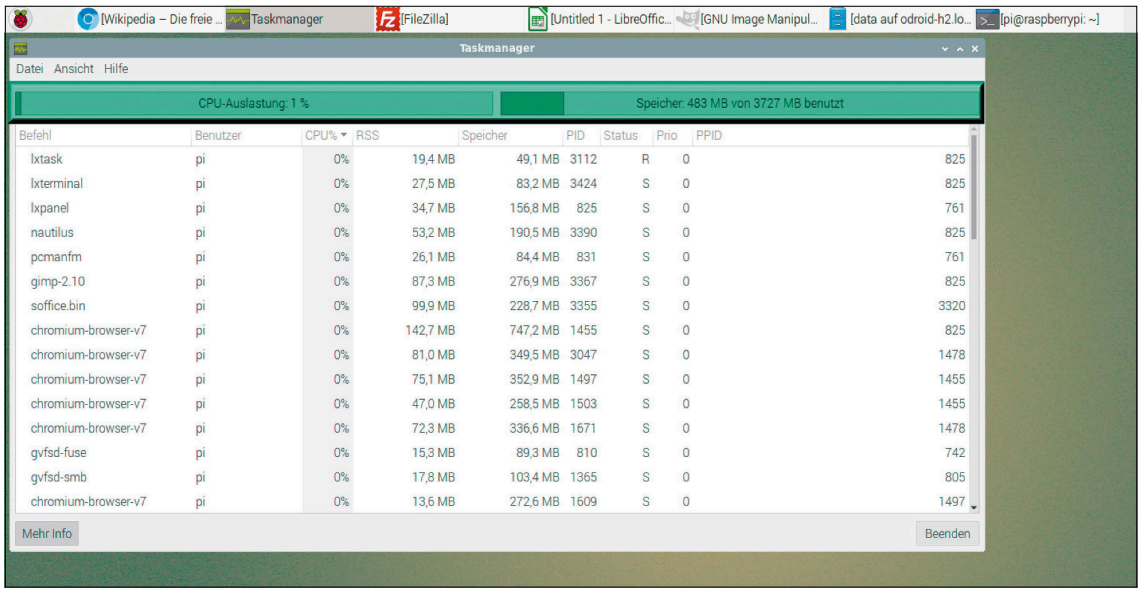
SD-Karte und Betriebssystem

Die eindeutig wichtigste Maßnahme für einen flüssigen Raspberry-Desktop ist eine richtig schnelle Micro-SD-Karte, die Lesegeschwindigkeiten von etwa 100 MB/s erreicht. Eingefrorene Fenster, langsamer Bootvorgang, zähe Installationen, für die man schnell den kleinen Raspberry Pi 4 verantwortlich machen könnte, sind allesamt Folgen einer unzureichenden SD-Karte. Der Leistungsunterschied des Pi 4 mit einem Raspbian auf einer Class-10-Karte (Class 10 ohne weitere Attribute bedeutet lediglich zehn MB/s) und einer Class-10-UHS-Karte (100 MB/s und mehr – UHS I, II und III) ist dramatisch. Die schnellsten SD-Karten beginnen mit Kapazitäten von 32 GB und tragen den Zusatz „SDXC“, „UHS“ oder „Ultra“. Eine Empfehlung sind etwa Sandisk-SDXC-Karten mit der Bezeichnung „Extreme“. Der Preis solcher SD-Karten kann je nach Kapazität dann allerdings den Preis der Raspberry-Platine erreichen.

Beim Betriebssystem gibt es derzeit noch kaum Alternativen: Das Raspbian „Buster“ (*www.raspberrypi.org/downloads*) mit seinem bescheidenen Desktop „Pixel“ dürfte aber so und so die angemessene Wahl bleiben, selbst wenn früher oder später Alternativen wie Ubuntu Mate bereitstehen. Wem der Pixel-Desktop zu karg ist, kann sich über Metapakete wie „mate-desktop-environment“ oder „lxqt“ auch in Raspbian immer noch einen anderen Desktop nachrüsten. Von den drei Raspbian-Varianten empfehlen wir „Raspbian Buster with desktop“, das mit Browser Chromium und VLC-Mediaplayer nicht viel, aber doch die wesentlichste Software mitbringt. Gezielte Nachinstallation sind jederzeit im Terminal über „apt install“ möglich, während das grafische Tool „Recommended Software“ (rp-prefapps) mit seinem sehr begrenztem Angebot eher überflüssig erscheint.

Mit einer flotten SD-Karte erzielt der Raspberry Pi 4 mit Raspbian respektable Bootzeiten: In 17 Sekunden sind wir beim Anmeldebildschirm und bei gewählter Auto-Anmeldung („Raspberry-Pi-Konfiguration → System → Automatisch Anmeldung“) dauert der Start bis zum vollständigen Desktop ganze 21 Sekunden.

Beim Desktopbetrieb mit Raspbian „Buster“ und typischer Anwendungssoftware wie Browser, VLC, Gimp, Libre Office ist es unwahrscheinlich, dass das System jemals mehr als ein GB RAM benötigt. Die Maximalausstattung des neuen Platinenmodells mit vier GB RAM ist daher definitiv nicht



Multitasking: Der neue Raspberry bedient mehrere aktive Prozesse flüssig und ohne Desktopaussetzer. Speicherengpässe sind auf dem sparsamen Raspbian-System generell kein Thema.

notwendig, schon die mittlere Variante mit zwei GB RAM bietet genügend Reserven.
Um den Desktopbetrieb zu optimieren, lohnen sich etliche Optionen und Kontrollen in der Systemkonfiguration: Unter „Einstellungen → Raspberry-Pi-Konfiguration“ muss unter „System“ der „Boot“ zum „Desktop“ erfolgen. Unter „Schnittstellen“ sollten, soweit möglich, alle Dienste deaktiviert sein und unter „Leistung“ können Sie den „GPU-Speicher“ auf 128 (MB) erhöhen. Wer die Platine konsequent auf den Desktopeinsatz fokussiert, wird außerdem auf die Installation von Serverdiensten wie Samba, Open SSH oder Apache verzichten.

Software und Desktop

Besondere Softwarediät müssen Sie dem Raspberry Pi 4 nicht auferlegen. Auch anspruchsvollere Software wie Libre Office oder Gimp ist in wenigen Sekunden gestartet. Der in Raspbian vorinstallierte Browser Chromium ist gegenüber dem etwas trägeren Firefox die vermutlich beste Wahl für den Raspberry. Nach dem Browserstart ist das Verhalten auch mit etlichen geöffneten Tabs jederzeit flüssig. Eine noch etwas flinkere Alternative wäre der Browser Vivaldi, von dem es auf *https://vivaldi.com/de/* auch ein DEB-Paket für die ARM-Architektur gibt. Das bleibt aber eher Geschmackssache ohne Not. Ein Ausweichen auf wirklich minimalistische Browser wie Midori hat der Raspberry Pi 4 definitiv nicht nötig, zumal solche Alternativen in der Regel nur RAM sparen, aber beim Seitenaufbau eher langsamer sind. Raspbians schlichter Pixel-Desktop bietet durchaus mehr Anpassungsmöglichkeiten als das Hauptmenü unter „Einstelllungen“ standardmäßig preisgibt. Es lohnt sich, dies mit dem „Main Menu Editor“ zu korrigieren. Hier finden Sie in der Kategorie „Einstellungen“ weitere Tools wie „Erscheinungsbild anpassen“ oder „Openbox Konfiguration Manager“, die standardmäßig deaktiviert sind, aber nach Klick auf das Kästchen „Anzeigen“ im Hauptmenü erscheinen.

Pi 4 als Desktop-PC: Das Fazit

Eben Upton, Gründer und Leiter der Raspberry Pi Foundation, hat die Frage, ob der neue Raspberry Pi 4 desktoptauglich sei, klipp und klar folgendermaßen beantwortet: „Yes, it is suitable for use as a general-purpose desktop PC“.
Der Raspberry Pi 4 als Allzweck-PC? Wir hatten erhebliche Zweifel, doch beim aktuellen Raspberry ist solche Nutzung in der Tat realistisch, vorausgesetzt, man spart weder bei der SD-Karte noch beim Gehäuse. Als Surfstation, als Zweitdesktop oder als Übungsrechner für Schulen ist die Platine uneingeschränkt zu empfehlen und absolviert sogar Multitasking mit Installationen oder Datentransfers neben laufendem Browser ohne Murren. ■

FLIRC LÖST DIE HITZEPROBLEME LAUTLOS

Neben allem Jubel über den Raspberry Pi 4 stand schnell die Sorge über eine allzu heiße neue Himbeere. Mit dem Kommando „vcgencmd measure_temp“ gemessene 70 Grad und darüber sind im Desktopbetrieb keine Ausnahme, sondern eher die Regel. Doch das Hitzeproblem ist mit kleiner Investition zu beheben – und zwar lautlos ohne lästige Lüfter: Das in der letzten LinuxWelt als Newsmeldung vorgestellte Aluminiumgehäuse „Flirc Raspberry Pi 4 Case“ (*www.welectron.com/Metallgehaeuse*, 20 Euro) konnten wir mittlerweile im Dauerbetrieb testen. Es sorgt dafür, dass der Raspberry Pi 4 auch bei Hochlast keine 70 Grad mehr erreicht und im Normalbetrieb bei etwa 55 bis 60 Grad bleibt. Das ist immer noch hübsch warm, aber tolerierbar. Das auch optisch ansprechende Gehäuse führt eine quadratische Einbuchtung im Deckel exakt auf SOC und CPU der Platine und kann damit die Abwärme großzügig auf die gesamte Deckelfläche ableiten. Diese einfache Maßnahme wirkt erwiesenermaßen effizienter als die kleinen Kühlkörper für das SOC, wie sie ebenfalls im Elektronikfachhandel angeboten werden.



Quelle: amazon.de

Was Sie über Ubuntu wissen müssen

Ubuntu passt immer! Egal, welche Hardware Sie antreiben wollen und welches Bedienkonzept Sie bevorzugen – EIN passendes Ubuntu gibt es allemal. Dieser Beitrag liefert grundlegende Infos über Status quo, Erscheinungsweise und Varianten.

VON HERMANN APFELBÖCK

2004 gründete der Südafrikaner Mark Shuttleworth die Firma Canonical und entwickelte auf Basis von Debian die Linux-Distribution Ubuntu. Das vieldeutige Zulu-Wort „Ubuntu“ können Sie sich auf *https://de.wikipedia.org/wiki/Ubuntu_(Philosophie)* von Nelson Mandela erklären lassen, wenn Sie möchten. „Humanismus“ übersetzt es vielleicht passend vieldeutig.

Die Distribution Ubuntu dominiert seit etwa 2006 den Linux-Desktop eindeutig: Linux auf PCs und Notebooks ist seither fast immer Ubuntu oder ein Ubuntu-Derivat wie Linux Mint. Von der soliden Debian-Basis übernimmt Ubuntu nicht den Stablezweig, sondern zugunsten höherer Aktualität eine Mischung aus „Testing“ und „Unstable“. Systemkomponenten und Programme in Ubuntu sind dadurch immer um Monate aktueller als bei der erzkonservativen Debian-Mutter.

Ungeachtet mancher gescheiterten Pläne mit der eigenen Oberfläche (Unity) oder dem hausgemachten Fenstermanager (Mir) ist Canonical mit Ubuntu ein nachhaltiger Fels im volatilen Biotop der Linux-Systeme. Open-Source-Ideologen kritisieren manche Ubuntu-Sonderwege wie Unity, Mir oder das Containerformat Snap zur Softwareverteilung. Auch manche Partnerschaft mit Microsoft (Ubuntu-Subsystem für Windows, Secure-Boot-Signatur bei Parallelinstallation) gefällt nicht jedem Linux-Freak. Aus pragmatischer Sicht dürfte aber kein Zweifel bestehen, dass die freien und verlässlichen Ubuntu-Systeme ein Glücksfall für Linux-Anwender sind.



Die Ubuntu-Hauptedition mit Gnome-Desktop: Wie die abgebildete Anwendungsübersicht ist hier alles groß und plakativ. Das Konzept versteht aber jeder nach fünf Minuten.

Die Erscheinungsweise von Ubuntu

Erscheinungsweise und Lebenszyklen von Ubuntu-Distributionen sind durchaus kompliziert, jedoch wird der Ubuntu-Benutzer von Ablaufterminen und Upgradepflichten kaum behelligt, am wenigsten, wenn er sich auf Langzeitversionen (LTS) konzentriert. Der seit Jahren pünktliche Ubuntu-Erscheinungszyklus sieht wie folgt aus:

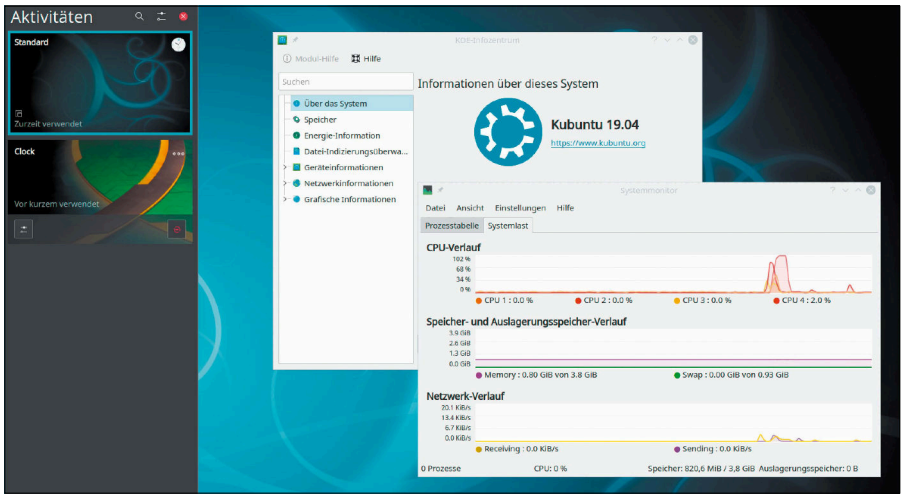
• Es gibt halbjährliche Zwischenversionen im April und im Oktober. Diese erhalten als Versionsnummer die jeweilige Jahreszahl mit Monat – also etwa 19.10 für die zu Redaktionsschluss aktuellste Version (vom Oktober 2019). Solche Interimsversionen bieten den neuesten Stand von Linux-Kernel, Desktop- und Softwareentwicklung, haben aber mit jeweils neun Monaten Support nur relativ kurze Gültigkeit (STS-Versionen: Short Term Support). Wer diesen flotten Zyklus mitmachen will, muss halbjährlich (mit jeweils dreimonatiger Schonfrist) das Upgrade auf die nächstfolgende Version erledigen. Das ist über die systemeigene „Aktualisierungsverwaltung“ weitgehend automatisierbar, darf aber nicht vergessen werden.

• Im April aller geradzahligen Jahre erscheinen die wichtigen LTS-Versionen (Long Term Support, Langzeitunterstützung). Dies sind die Meilensteine für die Ubuntu-Gemeinde, da diese Versionen bis zu maximal fünf Jahre mit Updates versorgt werden. Achtung: Die oft betonten fünf Jahre gelten nur für die Hauptedition mit Gnome. Alle anderen Editionen erhalten drei Jahre Support.

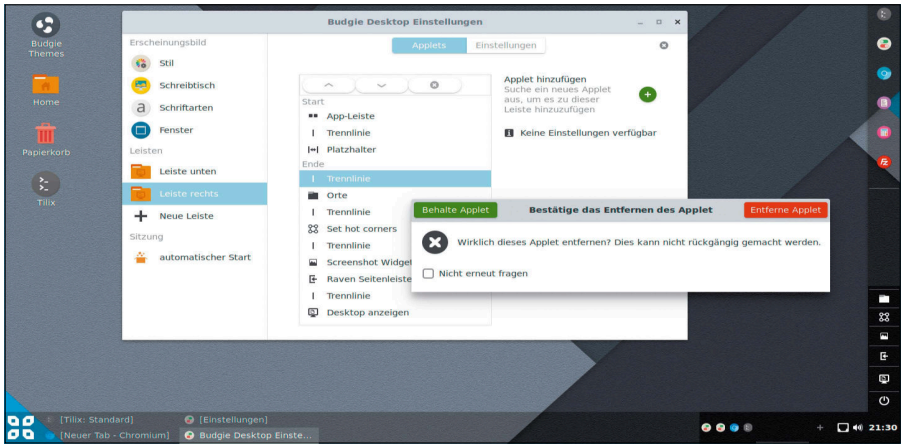
Einmal installiert, muss man sich als Nutzer einer LTS-Version jahrelang um nichts mehr kümmern. Die meisten Ubuntu-Nutzer, erst recht Serveradministratoren, warten grundsätzlich diese LTS-Versionen ab und

lassen die Zwischenversionen links liegen. Die zu Redaktionsschluss aktuellste LTS-Version erschien im April 2018 und trägt folglich die Versionsnummer 18.04. Erst mit Erscheinen dieses Heftes springt die aktuelle LTS-Version auf 20.04. Die momentan vorletzte LTS-Version 16.04 ist nach wie vor gültig. Die auf Heft-DVD vorliegenden LTS-Versionen 18.04 sind daher keineswegs „veraltet", sondern repräsentieren den fast aktuellen Stand der bevorzugten LTS-Ausgabe. Auch zahlreiche Ubuntu-Derivate wie Linux Mint konzentrieren sich auf die LTS-Versionen und erneuern ihre Systembasis im Turnus von Ubuntu LTS.

• LTS-Versionen erhalten nach einiger Laufzeit eine zusätzliche Versionsziffer wie etwa 18.04.4. Dies signalisiert das Point Release 4. Die sogenannten „Point Releases" erscheinen etwa halbjährlich – nicht ganz so termingenau wie LTS-Ausgaben und Zwischenversionen. Sie entsprechen den „Service Packs" von Windows und versammeln auf erneuerten ISO-Installationsmedien alles, was eine LTS-Version bislang an Updates erhalten hat. Sinn dieser Maßnahme ist es, bei Neuinstallationen unnötige Downloads zu vermeiden. Es ist zwar technisch problemlos möglich, heute ein originales Ubuntu 18.04 zu installieren, jedoch erspart das Installationsmedium 18.04.4 Downloadwartezeiten beim Anwender sowie Ressourcen beim Spiegelserver. Im laufenden Betrieb spielen die Release Points keine Rolle, da Updates automatisch installiert werden.



Kubuntu für Anspruchsvolle und Bastler: Der KDE-Desktop ist durchdacht, aber komplex. Linux-Nutzer, die von Gnome & Co. kommen, müssen sich vielfach umstellen – auch bei der Software.



Von der Demokratie nach oben gespült: Das hübsche, aber kernlose Ubuntu Budgie halten wir für relativ überflüssig, es hat sich aber durch Beliebtheit als offizielles Ubuntu etabliert.

LTS versus STS und Upgradepfade

Die Priorität von Ubuntu LTS ist unbestritten und wird auch durch Verbreitungszahlen eindeutig bestätigt. Trotzdem ist LTS nicht generell besser als STS. Auf Basis der drei STS-Interimsversionen wird die nachhaltige LTS-Version entwickelt. Ein Ubuntu LTS ist quasi das Resultat aus den einzelnen Entwicklungsstufen der drei Vorgänger. Bei der ersten STS-Version nach einer LTS-Version liegt der Fokus auf Innovation (18.10), bei der nächstfolgenden steht Leistungsoptimierung im Vordergrund (19.04), während die dritte STS-Version (19.10) mit Blick auf die nachfolgende LTS-Version (demnächst 20.04) vor allem auf Stabilität setzt.

Vorteile und Nachteile von LTS: Mit der Installation eines Ubuntu LTS (verschiedenen Varianten auf Heft-DVD) besitzen Sie mehrere Jahre sorgenfreien und vollautomatischen Updatesupport. Kernel und Software bleiben aber auf dem ursprünglichen Stand, solange Sie kein Upgrade anstoßen. Softwareausnahmen sind die sicherheitskritischen Programme Browser und Mailclient: Firefox und Thunderbird werden auch unter LTS-Versionen permanent aktualisiert.

Vorteile und Nachteile von STS: Der Support eines Ubuntu STS ist auf neun Monate begrenzt, was etwa halbjährlich zum Upgrade auf die nächsthöhere Version verpflichtet. STS-Versionen unterliegen geringeren Stabilitätsansprüchen als LTS-Versionen und können auch mal den einen oder anderen Bug enthalten. Andererseits sind hier der Kernel mit Treiber und Hardwareunterstützung, ferner Software und Desktop auf dem aktuellen Stand. Wenn Sie aus Aktualitätsgründen eine neue STS-Version bevorzugen, ist die zentrale Anlaufstelle die Seite *https://ubuntu.com/download* (Ubuntu-Hauptedition), die mit der Unterseite *https://ubuntu.com/download/flavours* auch zu Kubuntu, Xubuntu & Co. führt.

Upgradeoptionen: Kein Ubuntu ist eine Sackgasse. LTS-Langzeitversionen sind völlig offen und können jederzeit auf eine STS-Interimsversion umsteigen, falls Softwareneuheiten oder Kernel-Treiber für aktuelle Hardware dies nahelegen. Das typische LTS-Upgrade ist aber dasjenige zur nächsthöheren LTS-Version – konkret das Upgrade von 18.04 auf 20.04 in diesem Frühjahr.

STS-Ubuntu kann immer nur jeweils zur nächsten Zwischenversion upgraden und muss dabei jeden Schritt konsequent mitmachen. Ein installiertes Ubuntu 19.04 musste also im Herbst auf 19.10 upgraden und im jetzt auf 20.04. Dabei wird es dann automatisch zur LTS-Version.

Was hat sich getan seit 18.04?

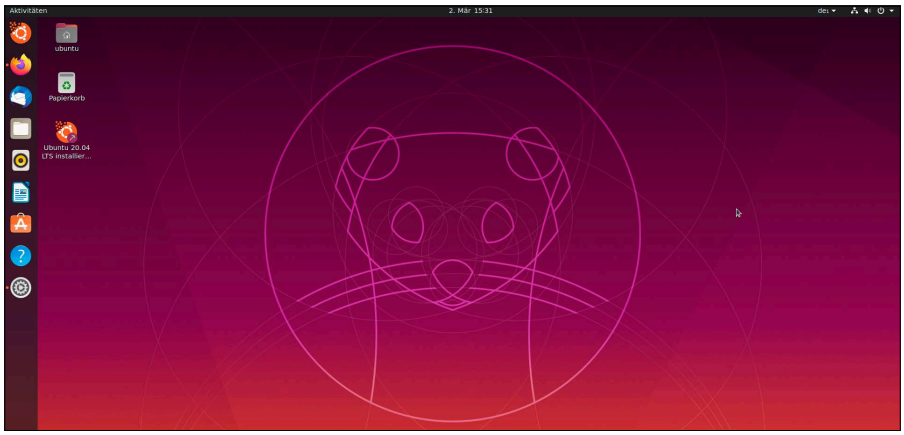
Um Ihnen die Entscheidung zwischen der LTS-Version und den STS-Versionen zu vereinfachen, resümieren wir kurz die Entwicklung seit 18.04. Generell bringen die Zwischenversionen kein Feuerwerk krachender Innovationen, sondern behutsame Anpassungen der jeweiligen Oberflächen, neuere Software und natürlich einen frischen Linux-Kernel mit aktualisierten Treibern. So bietet Ubuntu 19.04 mit Kernel 5.0 Unterstützung für die damals neue AMD-Prozessorgeneration Ryzen 2 und Epyc 2. Ab Version 18.10 wurde mit Kernel 4.18 an den Stromsparmaßnahmen gefeilt, um die Akkulaufzeiten von Notebooks zu verlängern. Im empirischen Test messen wir knapp zehn Prozent längere Laufzeiten gegenüber der LTS-Version 18.04.

Durch die Kompression von Bootmodulen starten die Versionen 19.04 etwas schneller als die LTS-Version, allerdings nur, wenn ein moderner Prozessor vorliegt. Auf älteren Rechnern wirkt die Kompression hingegen kontraproduktiv, weil die langsame CPU, welche die Module erst entpacken muss, zum Flaschenhals wird: Auf älteren Geräten booten ältere LTS-Versionen schneller.

Der Service der „Livepatches“ hat ab Version 18.10 Eingang in die grafische Oberfläche unter „Anwendungen & Aktualisierungen“ gefunden. Dies ist als frühe Vorbereitung für die nächste LTS-Version 20.04 zu interpretieren, denn Zwischenversionen wie 18.10 und 19.04 erhalten keine Livepatches. Motiv für diese Technik sind sicherheitsrelevante Kernel-Patches, die eigentlich einen Neustart benötigten. Livepatches stopfen die Sicherheitslücken vorläufig im laufenden Betrieb, sodass störende Neustarts verschoben werden können. Es handelt sich um einen Service für Server im Dauerbetrieb. Auf PCs und Notebooks, die jeden Tag neu gestartet werden, sind Livepatches irrelevant.

Ubuntu 19.10: Was kommt als Nächstes?

Die Zwischenversion 19.10 ist am 17.10.2019 erschienen, die nächste LTS-Version 20.04 kommt im April 2020. Ab Version 19.10 wird Ubuntu mit allen offiziellen Varianten den proprietären Nvidia-Grafiktreiber bereits als Paket auf den Installationsmedien anbieten. Der Anwender kann also schon bei der Installation entscheiden, ob er den Herstellertreiber einbinden möchte. Mehr noch: Der Treiber lässt sich auch schon im Livesystem aktivieren. Mit dem aktualisierten Gnome-Desktop 3.34 werden auch Gnome-Komponenten wie der Dateimanager („Nautilus“) und der Gnome Display Manager (für bessere Multimonitor-Unterstützung) überarbeitet. Alphaversionen in Form von Daily Builds sind von der Version 20.04 zu Redaktionsschluss bereits verfügbar (*http://cdimage.ubuntu.com/daily-live/current/*), allerdings nur von der Hauptedition mit Gnome-Desktop. Unser Kurztest Anfang März 2020 offenbarte jedoch weder bei der Installation noch im Betrieb nennenswerte Änderungen gegenüber dem Vorgänger. Wir entdeckten „nur“ Kernel 5.4 und noch nicht Kernel 5.5.



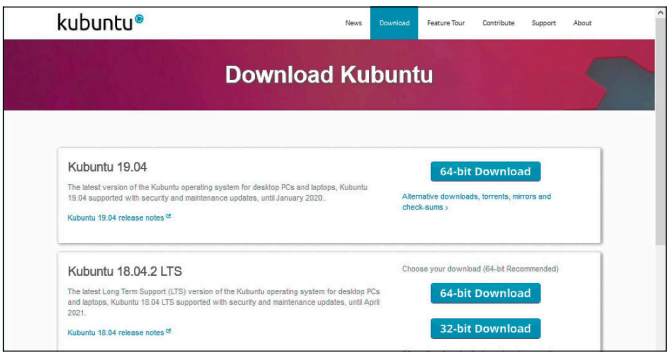
Ubuntu 20.20 soll im April 2020 erscheinen, allerdings erst nach Redaktionsschluss. Hier ist eine frühe Vorabversion zu sehen. Es wird sich um eine der wichtigen LTS-Versionen handeln.

32 Bit und 64 Bit

Der Ubuntu-Abschied von 32 Bit ist praktisch vollzogen: Seit Version 19.04 verzichten auch die kleinen Editionen Xubuntu und Lubuntu auf 32 Bit. Für die Version 18.04 gilt dies allerdings noch nicht: Hier sind noch sämtliche Ubuntus, ausgenommen die Gnome-Hauptedition, in 32 Bit zu finden. Auf Heft-DVD können wir Ihnen allerdings nur Ubuntu Server 18.04 in 32 Bit anbieten, während wir sonst 64-Bit-Varianten von Ubuntu bevorzugten. 32-Bit-Ausgaben von 18.04 erreichen Sie auf Wunsch unter *https://ubuntu.com/download*. Mit 32 Bit kommt auch das LinuxWelt-Surfsystem.

32 Bit ist ökonomischer im Speicherverbrauch. Eine technische Notwendigkeit für ein 32-Bit-System besteht allerdings auch auf älteren Rechnern so gut wie nie. Im Zweifel können Sie sich die CPU-Architektur Ihres Rechners unter Linux mit dem Terminalbefehl *lscpu* oder in den Systemeinstellungen anzeigen lassen, unter Windows mit dem Hotkey Win-Pause.

64-Bit-Systeme haben unbestrittene Vorteile: Sie beherrschen Uefi/GPT (wichtig für Parallelinstallation neben Windows), überwinden das Zwei-TB-Limit bei Festplatten und adressieren nativ (deutlich) mehr als vier GB RAM. 64-Bit-Systeme starten übrigens sowohl 64-Bit- wie 32-Bit-Software. Eine Ankündigung Canonicals, 32-Bit-Programme künftig (ab Version 19.10) nicht mehr zu unterstützen, wurde nach heftigen Protesten aus der Gaming-Ecke (Steam) wieder zurückgenommen.



32 Bit stirbt aus: Die LTS-Version 18.04 bietet alles (außer der Hauptedition) noch für beide CPU-Architekturen an. Die aktuellen und künftigen Ubuntus gibt es aber nur noch mit 64 Bit.

Die offiziellen Ubuntus

Neben den Desktopeditionen Ubuntu, Kubuntu, Xubuntu, Lubuntu, Ubuntu Budgie und Ubuntu Mate gibt es auch noch ein Ubuntu Kylin und Ubuntu Studio (Sondereditionen für chinesische Nutzer und für Audio-/Videoproduktion), die wir in diesem Heft nicht berücksichtigen. Die sechs nachfolgend charakterisierten Ubuntus unterscheiden sich in der Bedienung deutlich, aber aufgrund aktueller Entwicklungen nicht mehr so deutlich wie früher: Insbesondere die Entscheidung zwischen Xubuntu, Lubuntu und Mate ist bei der LTS-Version 18.04 durch unterschiedliche Hardwareansprüche noch recht klar, gerät aber in den jüngsten Versionen zur Geschmacksfrage.

Ubuntu sollte relativ aktuelle Hardware ab Dualcore-CPU, 3D-Grafikchip und vier GB RAM vorfinden. Die Oberfläche Gnome ist modern, schick und absolut einsteigertauglich. Canonical stattet Gnome abweichend zum Original mit positionierbarer Favoritensleiste („Dock“) und einem Desktop als Dateiablage aus.

Für tiefere Gnome-Anpassungen sind traditionell das Tool Gnome-Tweaks („Optimierungen“) und die Gnome-Extensions zuständig.

Kubuntu mit dem anspruchsvollen KDE Plasma galt ehemals als besonders ressourcenhungrig, hat sich aber mittlerweile auf dem Niveau der Hauptedition eingependelt. Aktuellere Hardware und vier GB RAM sind auch hier zu empfehlen. KDE Plasma ist minutiös und umfassend einstellbar und bietet mit Workspace-„Aktivitäten“, KDE Connect (für Smartphone-Verbindungen) oder verschlüsselten Vaults-Containern zahlreiche Spezialitäten. Kubuntu ist das Ubuntu für KDE-Fans und Desktopbastler.

Ubuntu Budgie liefert einen aufgeräumten, kontrastreichen und attraktiven Desktop mit (noch) mittleren Hardwareansprüchen (800 MB RAM). Für Einsteiger, Ästheten und Notebooknutzer lohnt sich der Blick allemal, allerdings nicht für Desktopbastler. Der tendenziell hermetische Budgie lässt intuitive Einladungen zur Anpassung per Kontextmenü vermissen, die man von anderen Oberflächen gewöhnt ist.

Ubuntu Mate ist mit mittlerweile 500 bis 700 MB RAM (18.04/19.04) Eigenbedarf kein echtes Leichtgewicht mehr. Zwei GB RAM sind zu empfehlen. Der Desktop bedient Nutzer, die ein klassisches Bedienkonzept jenseits von Gnome 3.x oder KDE Plasma bevorzugen und es hübscher wollen als das etwas altbackene Xubuntu. Ubuntu Mate bietet einen ansehnlichen, aber unprätentiösen Allzweckdesktop, mit dem Einsteiger, Umsteiger und Pragmatiker klarkommen.

Xubuntu mit dem XFCE-Desktop ist neuerdings das sparsamste Ubuntu und bedient auch schwächere Hardware wie etwa Netbooks mit einem GB RAM. Xubuntu eignet sich auch für Einsteiger, profitiert aber von etwas Anpassungsarbeit.

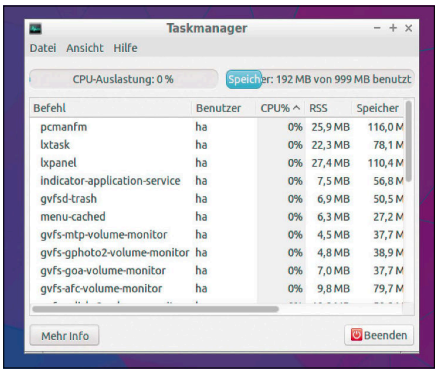
XFCE ist eine konservative, aber absolut ausgereifte Oberfläche mit klassischem Startmenü und gut konfigurierbaren Systemleisten.

Lubuntu ist in der LTS-Version 18.04 die kleinste Variante der Ubuntu-Familie – noch deutlich anspruchsloser als Xubuntu. Mit dem einfachen, aber funktionalen LXDE-Desktop hat es nur 200 MB Eigenbedarf und ist ein Kandidat für betagte Rechner. Lubuntu hat aber seit Version 18.10 den Desktop gewechselt: Mit dem deutlich hübscheren LXQT-Desktop liegt es heute mit annähernd 500 MB RAM über einem Xubuntu.

Ubuntu-Derivate und Linux Mint

Über die offiziellen Flavours hinaus sind aus der grundsoliden Ubuntu-Basis zahlreiche Derivate erwachsen: Bodhi Linux, Chromium-OS, Elementary-OS, Linux Mint, Peppermint-OS, Voyager-OS, Zorin-OS – um nur die bekanntesten zu nennen. Sie alle nutzen als Unterbau zumeist das aktuelle Ubuntu LTS, zum Teil auch die Ubuntu-STS-Versionen. Der Hauptanspruch solcher Derivate liegt zumeist in einer eigenen oder individuell arrangierten Benutzeroberfläche. Darüber hinaus übernehmen inoffizielle Derivate den Ubuntu-Unterbau nicht komplett wie die offiziellen Varianten, sondern mischen ihn mit selbst angepassten oder aus externen Quellen stammenden Softwarepaketen.

Über das Alleinstellungspotenzial manches Ubuntu-Derivats kann man geteilter Meinung sein. Unbestritten hat aber Linux Mint mit Cinnamon mit die freundlichste Oberfläche für Windows-Umsteiger (die auch Linux-Fans goutieren) und ein Bodhi Linux hat zwar eine sehr gewöhnungsbedürftige Oberfläche, frisiert aber den Ubuntu-Unterbau zum schnellsten uns bekannten Betriebssystem. ■



Ein GB RAM ist für Lubuntu 18.04 eine Menge Speicher: Das pure System inklusive LXDE-Desktop fordert – je nach Treiberausstattung – nur 150 bis 250 MB.

DIE UBUNTUS: OFFIZIELLE FLAVOURS UND INOFFIZIELLE DERIVATE (AUSWAHL)

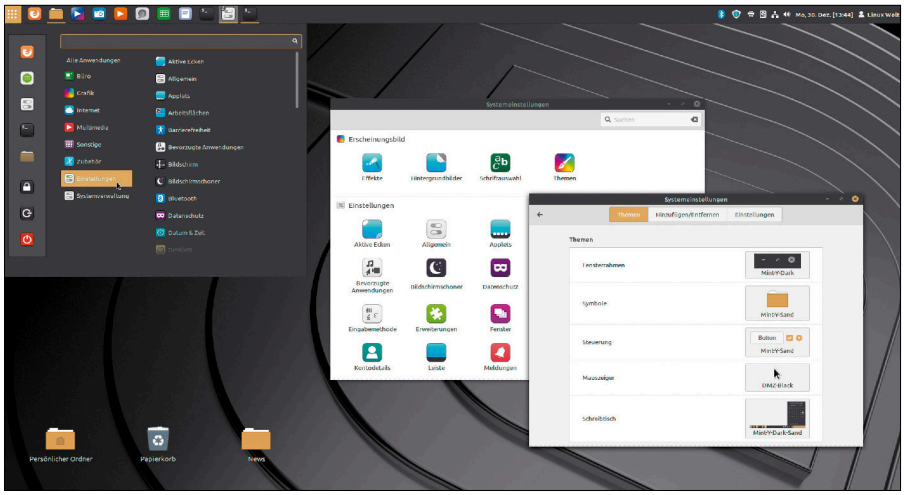
Distribution	aktuelle Version**	Desktop	Webseite
Bodhi Linux	5.0	Moksha (E17)	*www.bodhilinux.com*
Elementary-OS	5.1.2	Pantheon	*https://elementary.io/de/*
Kubuntu*	18.04.3 LTS	KDE	*www.kubuntu.org*
Linux Mint	19.3	Cinnamon	*www.linuxmint.com*
Lubuntu*	18.04.4 LTS	LXDE	*https://lubuntu.me/*
Peppermint-OS	10	XFCE/LXDE	*http://peppermintos.com*
Ubuntu*	18.04.4 LTS	Gnome	*www.ubuntu.com*
Ubuntu Budgie*	18.04.4 LTS	Budgie	*https://ubuntubudgie.org*
Ubuntu KDE Neon	02-2020	KDE	*http://neon.kde.org*
Ubuntu Mate*	18.04.4 LTS	Mate	*https://ubuntu-mate.org*
Voyager-OS	18.04	XFCE	*https://voyagerlive.org/*
Xubuntu*	18.04 LTS	XFCE	*https://xubuntu.org/*
Zorin-OS	15.1	Gnome	*https://zorinos.com*

* offizielles Ubuntu ** Redaktionsschluss war vor der Ubuntu Version 20.04, Zwischenversionen hatten den Stand 19.10

Linux Mint 19.3

Linux Mint 19.3 erneuert seine Systembasis, indem es seinen Unterbau auf das dritte Point Release 18.04.3 LTS seines Ubuntu-Vorbilds umstellt. Darüber hinaus gibt es dezente Neuerungen beim Desktop Cinnamon und beim Softwarezubehör.

VON HERMANN APFELBÖCK



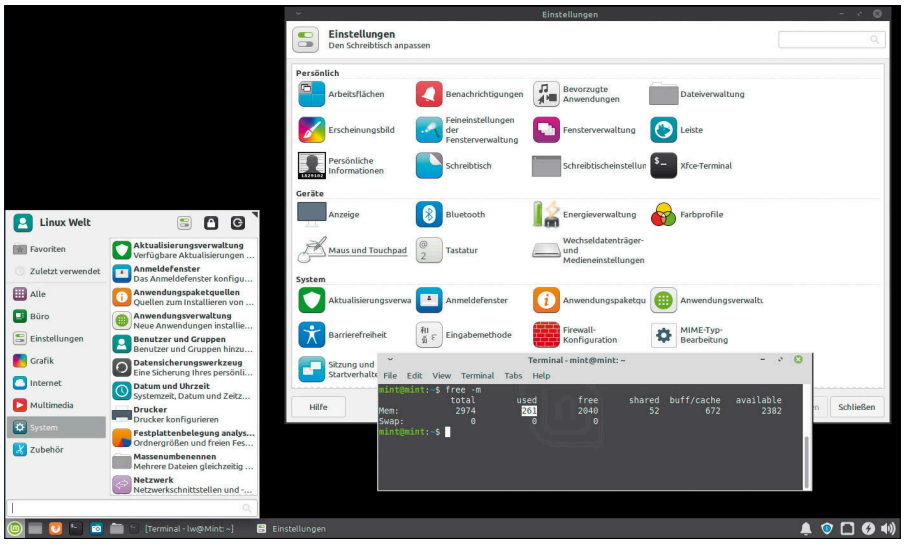
Das beliebte Desktopsystem erhält turnusgemäß sein nächstes Update: Linux Mint 19.3 trägt den Namen „Tricia“ und garniert seine Systemaktualisierung wieder mit etlichen, aber bescheidenen Verbesserungen und Änderungen. Linux Mint 19.3 ist wie sein Ubuntu-Unterbau eine Langzeitversion, die bis 2023 unterstützt wird. Aufgrund seiner Produktionsweise als Ubuntu-Derivat kann Linux Mint bei Kernel, Unterbau und Softwareversionen niemals Trendsetter sein, zumal schon seine Systembasis Ubuntu dies nicht leistet. Version 19.3 hat daher den nicht mehr taufrischen Kernel 5.0 an Bord (vom März 2019). Manche mitgelieferte Software wie Libre Office (6.0.7.3) datiert sogar noch auf das Ende des Jahres 2018 zurück.

Zum Nachteil gerät dies aber nur dann, wenn der Nutzer ganz bestimmte und allerneueste Softwarefunktionen unbedingt benötigt oder wenn allerneueste Hardware die jüngsten Treiber im Linux-Kernel voraussetzt.

Linux Mint 19.3: Die Varianten

Linux Mint 19.3 erscheint mehr oder weniger zeitgleich zum Supportende von Windows 7. Für Umsteiger von Windows ist Linux Mint Cinnamon die klügste Wahl aus der Menge der Linux-Distributionen. Die Hauptvariante orientiert sich an vielen Windows-Standards und ist eine Linux-Distribution, die im Benutzeralltag eine vollständig grafische Bedienung erlaubt. Linux Mint fokussiert auf Umsteiger und Einsteiger, hat aber auch Linux-Freaks auf seiner Seite. Dafür sorgt die Cinnamon-Oberfläche, die nicht nervt, sondern dient und dabei attraktiv ist. Diese Oberfläche ist das Aushängeschild von Linux Mint und gleichzeitig dessen wichtigste Eigenentwicklung. Cinnamon liegt in neuester Version 4.4.5 vor.

Plädoyer für Cinnamon: Die nachfolgende Vorstellung bezieht sich in erster Linie auf die Cinnamon-Hauptvariante. Neben dieser Ausgabe pflegt das Mint-Team eine Ausgabe mit dem Desktop Mate sowie die ressourcensparendste Ausgabe mit XFCE-Oberfläche. Die Mate-Variante (Mate-Version 1.22) hat neben dem attraktiveren Cinnamon schwache Argumente, zumal sie kaum schlanker ausfällt. Das bekannt sparsame XFCE (XFCE-Version 4.14) ist immer zu rechtfertigen, wenn ältere Zielhardware vorliegt.



XFCE-Edition: Die sparsamste Variante ist immer eine gute Wahl für ältere Hardware. Wirklich anspruchsvoll ist aber auch die Cinnamon-Hauptedition nicht.

Im Vergleich zu Cinnamon und Mate, die etwa 600 bis 700 MB beziehungsweise 500 bis 600 MB fordern, kommt die XFCE-Variante schon mit etwa 300 bis 400 MB aus. Allerdings hat Linux Mint mit XFCE kaum nennenswerte Vorteile gegenüber einem Ubuntu mit XFCE (Xubuntu), das seinerseits stets einige Monate aktueller ist als das Mint-Derivat. Gleiches gilt auch für Mint Mate neben dem offiziellen Ubuntu Mate.

Alles in 32 und 64 Bit: Alle drei Ausgaben gibt es neben der 64-Bit-Architektur auch in 32 Bit. Letzteres ist heutzutage nicht mehr selbstverständlich und die sparsameren 32-Bit-Ausgaben sind die bevorzugte Wahl, wenn der Zielrechner weniger oder bis maximal vier GB RAM mitbringt und Linux Mint als alleiniges System installiert werden soll. Als 32-Bit-Ausgabe bleibt sogar die Cinnamon-Edition bei einem RAM-Bedarf unter 400 MB. 32-Bit-Varianten können nativ nur etwa 3,7 GB RAM verwalten und beherrschen keine Uefi-Multiboot-Installation (mit GPT-Partitionsschema). Ansonsten bestehen keine nennenswerten Einschränkungen gegenüber 64 Bit.

Systemvoraussetzungen: Keine Mint-Edition stellt hohe Hardwareansprüche. Als Minimalanforderung nennt das Mint-Team für alle drei Ausgaben ein GB RAM und 15 GB auf Festplatte, was selbst für die XFCE-Edition knapp ausfällt. Wir empfehlen zwei GB RAM für XFCE, zwei bis vier GB RAM für Mate und Cinnamon. Für ein Linux im Dauerbetrieb sollten für System, Updates, Timeshift-Snapshots und Softwareinstallation wenigstens 50 GB bereitstehen – für Benutzerdateien entsprechend mehr. Eine ältere Dualcore-CPU ist für XFCE ausreichend, für Cinnamon und Mate darf es auch etwas moderner sein.

Download und ISO: Anlaufstelle für alle (dreimal je zwei) Editionen ist die Seite *https://linuxmint.com/download.php*, die dann zu deutschen und internationalen Spiegelservern verlinkt. Der für alle Varianten knapp zwei GB umfassende Download ist kostenlos. Das ISO-Image muss dann mit den üblichen Mitteln (wahlweise dd, Etcher, Win 32 Disk Imager, Gnome-Disks oder KDE-Partitionmanager) bootfähig auf USB kopiert werden, um es danach am Zielrechner zu booten und das System aus dem Livemedium zu installieren.

LinuxWelt-Leser, die sich für die Hauptedition entscheiden, sparen sich den Download, weil das Installationsmedium von Linux Mint 19.3 Cinnamon von der Heft-DVD startet. Ein Kopieren auf USB (aus dem Heft-DVD-Verzeichnis („Image-Dateien“) kann unter Umständen trotzdem notwendig werden, nämlich wenn Linux Mint im Uefi-Multiboot neben Windows installiert werden soll. Die Heft-DVD bootet und installiert im Bios-Modus.



HDT-Tool im Livesystem: Die Mint-Live- und Installationsmedien bieten das Hardware Detection Tool als neue Bootoption.

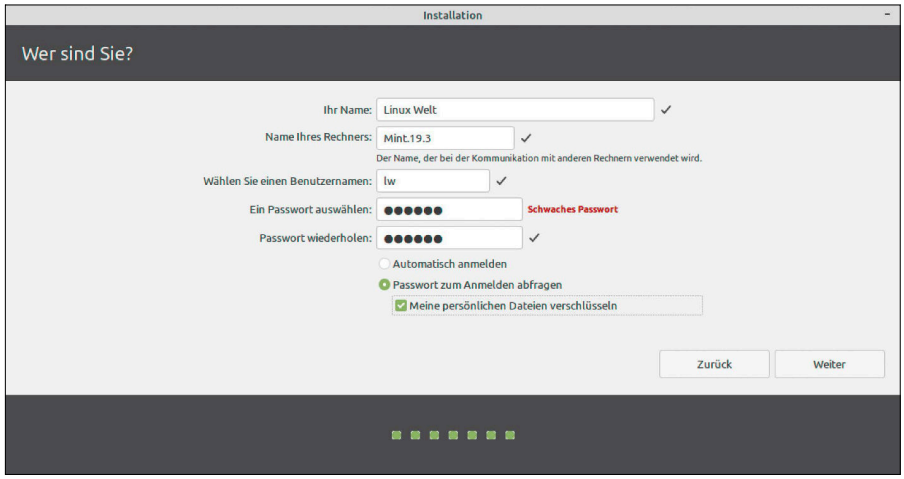
Im Linux-Mint-Livesystem

Im Live- und Installationsmedium gibt es in Version 19.3 als neue Bootoption das nützliche HDT-Tool. HDT erscheint mit dem Eintrag „Hardware Detection“ im Bootmenü des Livesystems und leistet eine umfassende und detaillierte Analyse der Rechnerhardware. Das zusätzliche Servicesystem ist als Entscheidungshilfe gedacht, um vor einer Installation etwa CPU (64 Bit?) oder RAM (mehr als vier GB?) abzufragen. Im späteren installierten Linux Mint fehlt HDT.

Wird das Livesystem mit dem Standardeintrag „Start Linux Mint“ gestartet, gibt es am Desktop den üblichen Link für den Start der Installation. Im Menü des Livesystems findet sich auch wieder das schon in der letzten Version 19.2 eingeführte „Boot Repair“, das verbreitete Grub-Probleme beheben kann. Boot Repair ist – wie HDT – dem Livesystem vorbehalten und fehlt im installiertem Linux Mint.

Für die Installation, die der Desktoplink „Install Linux Mint“ auslöst, dient unverändert der bekannte Ubuntu-Installer („Ubiquity“), dessen wesentlichster Dialog „Installationsart“ über die Partitionierung entscheidet. Im einfachsten Fall für ein alleiniges System auf dem Zielrechner ist „Festplatte löschen und Linux Mint installieren“ die richtige Wahl.

Die Vorgehensweise im Ubuntu-Installer für andere Varianten wie Multiboot, Instal-

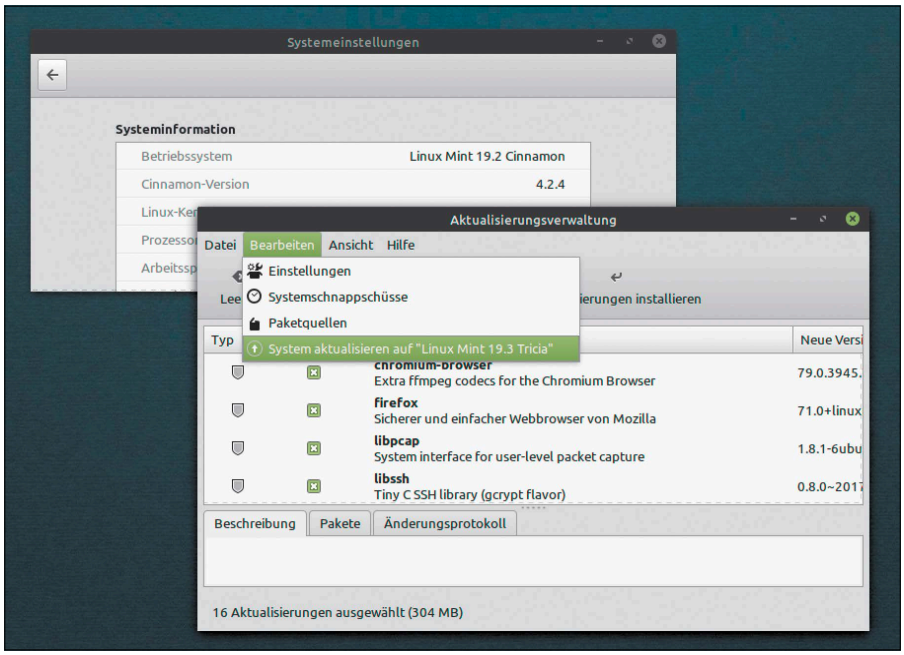


Home-Verschlüsselung: Linux Mint 19.3 hält unverdrossen an dieser Installationsoption fest, die Ubuntu schon längst nicht mehr anbietet.

lation auf USB oder Einsatz der Datenträgerverschlüsselung Luks wurde vielfach erklärt, so auch im E-Book „LinuxWelt XXL 2020-02“ auf der Heft-DVD unter „Grundlagen → Ubuntu-Installationen“.
Nicht neu, aber als weiterhin vorhandene Option positiv anzumerken ist im späteren Installationsdialog „Wer sind Sie?“ die Option „Meine persönlichen Daten verschlüsseln“. Diese Verschlüsselung mit dem Programm Ecrypt FS erfasst das Home-Verzeichnis des Erstbenutzers, den Sie in diesem Dialog anlegen. Bemerkenswert ist dies insofern, als Ubuntu diese Verschlüsselung aus dem Installer längst ersatzlos gestrichen hat.

Das Upgrade von 19.x auf 19.3

Wer ein Linux Mint 19.x laufen hat, benötigt das Installations- und Livesystem natürlich nicht, sondern kann über das Internet auf Version 19.3 upgraden. Das funktioniert genauso wie bei den früheren Versionen:
1. Sie starten über das Menü die Aktualisierungsverwaltung und gehen auf „Auffrischen“. Das Systemprogramm wird dann melden, dass es eine „neue Version der Aktualisierungsverwaltung“ gibt, die Sie mit Klick auf „Die Aktualisierung anwenden“ auf das System laden.



Upgrade eines älteren Mint 19.x: Der Aufstieg zur aktuellen Version 19.3 erfolgt online über die Aktualisierungsverwaltung. Kernel und Anwendungssoftware bleiben unverändert.

2. Die Aktualisierungsverwaltung wird installiert, die alte Version automatisch geschlossen und die neue Version geladen.

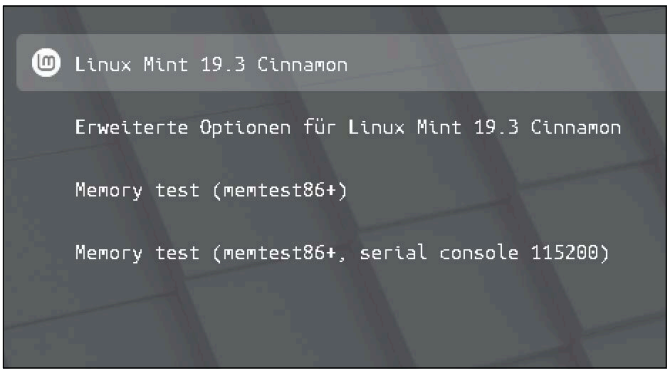
ERSTEINRICHTUNG UND ANPASSUNG

Neu installiertes Linux Mint ist noch nicht komplett eingerichtet. Die wichtigsten Pflichten zeigt der „Willkommen“-Bildschirm unter „Erste Schritte“.
Aktualisierungsverwaltung: Das Wichtigste ist ein Besuch in den Paketquellen, da es seit Erscheinen von Version 19.3 schon wieder neue Updates gibt. Gehen Sie in der „Aktualisierungsverwaltung“ auf „Auffrischen“, danach auf „Aktualisierungen installieren“. Eine weitere Aktion an dieser Stelle („Bearbeiten → Paketquellen“) ist die Auswahl optimaler „Spiegelserver“: Spiegelserver sind die beiden Server mit Mint- und Ubuntu-Paketen, woher das System die Software bezieht. Beim Klick auf die voreingestellten Server startet ein Geschwindigkeitstest, der die schnellsten Server nach oben sortiert.
Treiberverwaltung: Unter „Systemverwaltung → Treiberverwaltung“ installieren Sie proprietäre Herstellertreiber – in der Regel Grafiktreiber. Die Treibersuche erfolgt automatisch.
Timeshift: Nach dem Start („Systemverwaltung → Timeshift“) wird der „Schnappschusstyp“ abgefragt. Übernehmen Sie das voreingestellte „RSYNC“. Im nächsten Schritt geht es um den Zieldatenträger der Sicherung. Timeshift bietet nur Partitionen mit Linux-Dateisystem an. Standardziel, wenn nur eine Festplatte vorliegt, ist das Wurzelverzeichnis, wo der zusätzliche Ordner „timeshift“ entsteht. Im letzten Schritt definieren Sie einen Zeitplan und die Menge der Systempunkte. Automatische Sicherung ist aber nicht zwingend, da sich Schnappschüsse jederzeit manuell über „Erstellen“ auslösen lassen.
Monitoreinstellungen: Linux Mint erkennt die optimale Auflösung automatisch. Nur bei Dual-Monitor-Betrieb ist es notwendig, den primären Bildschirm und die Anordnung der Monitore unter „Systemeinstellungen → Bildschirm“ festzulegen. Hier arrangieren Sie die Monitore einfach mit der Maus. Lohnend für optimale Darstellung ist ferner der Punkt „Systemeinstellungen → Schriftauswahl → Skalierungsfaktor der Schrift“. Der steht standardmäßig auf „1,0“ und lässt sich verkleinern oder vergrößern.
Netzwerkadapter: Mit WLAN-Adaptern besteht die übliche Pflicht, sich am Funknetz anzumelden. Dies funktioniert über das Netzwerksymbol in der Systemleiste. Wenn der WLAN-Adapter hardwaretechnisch nicht erkannt wird, fehlen dort die Option „Funknetzwerk aktivieren“ sowie die Anzeige der nahen Funknetze. Dann hilft eventuell eine vorübergehende Kabelverbindung und das Nachladen des proprietären Treibers über „Systemeinstellungen → Treiberverwaltung“).
Benutzer und Konten: Nach der Installation gibt es nur das Konto, das Sie beim Setup angelegt haben. Dieses Erstbenutzerkonto ist „Systemverwalter“ mit sudo-Recht. Unter „Systemeinstellungen → Benutzer und Gruppen“ können Sie Benutzerkonten einsehen, Kennwörter und Kontotyp ändern und neue Konten anlegen. Konten vom Typ „Systemverwalter“ erhalten automa-

Das erkennen Sie daran, dass nun unter „Bearbeiten“ ein neuer Punkt auftaucht: „System aktualisieren auf [...] Tricia“. Bevor Sie die Schaltfläche klicken, bringen Sie Linux Mint mit „Aktualisierungen installieren“ erst noch auf den neuesten Stand.

3. Nach dem Klick auf „Bearbeiten → System aktualisieren [...]“ folgt noch die vom Mint-Team bekannte Umstandskrämerei mit allerlei Versionsinformationen und einer letzten Bestätigung, dass man das Upgrade trotz theoretischer Probleme installieren will („Ich verstehe das Risiko...“).

Das Upgrade – in unserem Fall von 19.2 auf 19.3 – ist dann eine durchaus überschaubare Angelegenheit, sowohl zeitlich als auch bei der Downloadmenge. Die größten Datenmengen betreffen das Artwork mit neuen Icons und Hintergrundbildern. Der Kernel wird beim Upgrade nicht erneuert. Wer einen jüngeren Kernel installieren will, muss dies in der Aktualisierungsverwaltung unter „Ansicht → Linux-Kernel“ manuell nachholen. Gleiches gilt auch für die Änderungen bei der Softwareausstattung: Auch hier bleibt Linux Mint auf dem Stand der Vorgängerversion.



Booten via Grub: Der Bootmanager ist aufgehübscht und zeigt mit Mint-Hintergrund schon vorab, wohin die Bootreise geht.

Das Onlineupgrade ist im Wesentlichen ein Desktopupgrade auf die Cinnamon-Version 4.4.6 (beziehungsweise Mate 1.22 oder XFCE 4.14).

Erster Blick auf Mint 19.3

Nach der Installation der neuen Version zeigt der Start neuen grafischen Feinschliff: Der Grub-Bootloader ist mit einem Mint-typischen Hintergrund unterlegt. Ist Linux Mint als einziges System auf dem jeweiligen Rechner, bekommt man Grub allerdings nur zu Gesicht, wenn der Bootvorgang mit Umschalttaste gebremst wird. Dies ist nur nötig in Problemfällen, um unter „Erweiterte Optionen“ spezielle Notschalter zu verwenden. In Multiboot-Umgebungen erscheint das Grub-Menü mit dem Mint-Hintergrund hingegen standardmäßig.

Den Startvorgang verziert jetzt das erneuerte runde Mint-Logo, das später auch als Menülogo auftaucht. Das neue Logo ist schicker, jedoch gibt es beim Systemstart keine Fortschrittsanzeige mehr unter dem Logo, die signalisiert, dass das System arbeitet. Alle drei Mint-Editionen laden beim Start den bekannten Einsteigerdialog „Willkommen“ (mintwelcome). Das Abar-

tisch sudo-Recht. Beachten Sie, dass die Home-Verzeichnisse unabhängig vom Kontotyp gegenseitig offenstehen für lesenden Zugriff aller Systembenutzer. Um dies abzustellen, gehen Sie mit dem Dateimanager in das übergeordnete Verzeichnis „/home“ und markieren Ihren eigenen Ordner. Nach Rechtsklick und „Eigenschaften → Zugriffsrechte“ setzen Sie an der dritten und untersten Stelle von „Ordnerzugriff“ die Rechte auf „Keine“.

Cinnamon-Anpassung: Über „Systemeinstellungen → Themen“ bestimmen Sie das Aussehen entscheidend. Wichtigster Unterpunkt ist „Schreibtisch“, weil dieser die Farben des Hauptmenüs und der Hauptleiste festlegt. Bei der Auswahl des „Fensterrahmens“ für die Titelleisten aller Programmfenster ist „Mint-Y-Dark“ (oder vergleichbar) zu empfehlen, damit die wichtige Titelleiste kontrastreich ausfällt.

Der Punkt „Fenster → Titelleiste“ steuert Aussehen und Verhalten der Titelleiste: Die Funktion der Kontrollelemente (Minimieren, Schließen, Maximieren) kann individuell eingestellt werden. Die Registerkarte „Fenster → Verhalten“ bietet die wichtige Option „Fokussierungsverhalten“: Normalerweise erhält ein Fenster durch Mausklick den Eingabefokus; mit der Option „Maus“ genügt ein Mouseover ohne Klick, um es eingabebereit in den Vordergrund zu bringen.

Den Desktophintergrund ändern Sie über „Systemeinstellungen → Hintergrundbilder“. Der kürzeste Weg hierzu ist ein Rechtsklick am Desktop und „Hintergrundbild [...] ändern“. Abgesehen von den voreingestellten Bildern können Sie mit dem kleinen Plus-Symbol auch einen Ordner mit eigenen Bildern verwenden.

Der weitere Punkt „Schreibtisch“ ist insofern wichtig, weil Cinnamon hier die Standardsymbole am Desktop wie „Papierkorb“ oder „Eingehängte Datenträger“ anbietet. Hier können Sie einzeln festlegen, welche Symbole der Desktop zeigen soll.

Die „Systemeinstellungen“ bieten ferner „Desklets“ (Desktopgadgets), „Erweiterungen“ (Erweiterungen für Cinnamon) und „Applets“ (Elemente für die Systemleiste). Wirklich ergiebig sind nur die Leistenapplets: Die Kontextoption „Applets“ bietet eine Übersicht der derzeit aktiven (Häkchen) und der sonstigen Applets. Die Minus-Schaltfläche deaktiviert ein Element, die Plus-Schaltfläche aktiviert ein Applet. Die meisten Leistenapplets bieten außerdem eine eigene Konfiguration über das Zahnradsymbol, die sich mindestens bei so wichtigen Applets wie dem Hauptmenü oder der „Gruppierten Fensterliste“ lohnt.

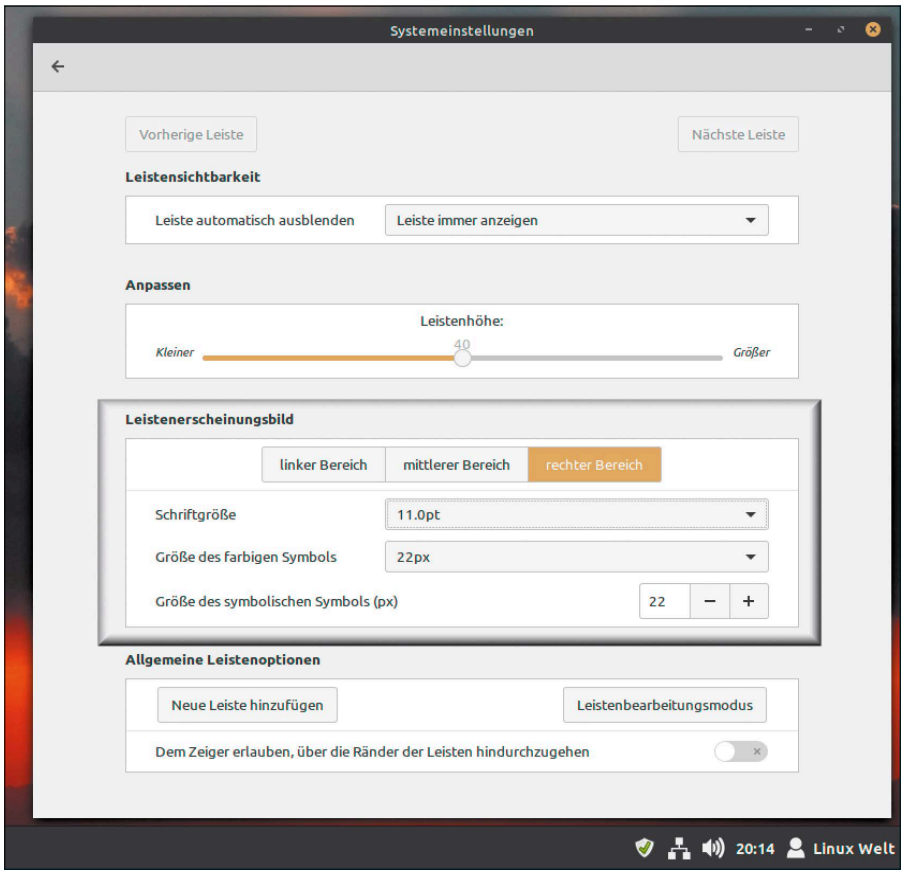
Die Position der Leistenelemente kann der Applets-Dialog nicht ändern. Dazu ist nach Rechtsklick auf der Systemleiste der „Leistenbearbeitungsmodus“ nötig. Danach lassen sich einzelne Applets mit der Maus an die gewünschte Stelle ziehen. Beachten Sie, dass im Leistenbearbeitungsmodus sämtliche Applets inaktiv sind.

beiten des Punktes „Erste Schritte“ mit Systemschnappschüssen, Treiberverwaltung und Aktualisierungsverwaltung ist zur Ersteinrichtung jedem Nutzer zu empfehlen. Änderungen gegenüber den Vorgängerversionen gibt es hier nicht. Die wenigen, alle drei Editionen betreffenden Neuerungen sind folgende:

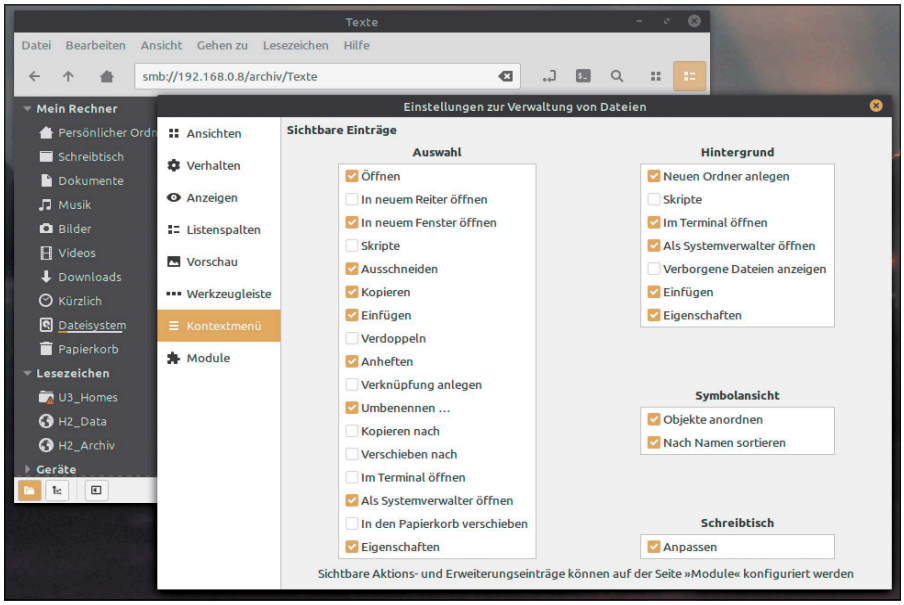
1. Der Punkt „Systemeinstellungen → Sprachen“ wurde um das regionale Zeitformat erweitert. Bislang umfasste der Punkt die Systemsprache und die regionsspezifischen Zahl- und Währungsformate. Zeitzone und Datums- und Zeitformate mussten an anderer Stelle definiert werden.

2. Die Hauptleiste präsentiert mit einem Warndreieck Systemmeldungen, die eine Benutzeraktion erfordern. Wenn das Symbol erscheint, sieht das Mint-System Veranlassung, den Benutzer zu warnen. Typische Meldungen vor einer Ersteinrichtung, die jeder Benutzer sehen wird, betreffen noch nicht konfigurierte Timeshift-Schnappschüsse oder ein fehlendes Passwort für das – eigentlich inaktive – root-Konto, das aber im Falle eines defekten Benutzerkontos einen Notzugriff erlaubt. Das neue Warndreieck wird aber auch anschlagen, wenn künftig eine neue Mint-Version vorliegt oder das Supportende naht.

3. Die Unterstützung für hochauflösende (HiDPI-)Monitore ist zwar nicht abgeschlossen, aber mit Version 19.3 weiter verbessert. Dabei geht es nicht zuletzt um kosmetische Anpassungen, um grafische Elemente wie Icons auf bei sehr hoher Bildschirmauflösung scharf darzustellen.



Noch detailliertere Cinnamon-Leistenoptik: Jetzt kann jeder der drei Bereiche in der Systemleiste hinsichtlich Symbol- und Schriftgröße exakt eingestellt werden.



Der Dateimanager unter Cinnamon ist ein Vorbild für Anpassungsfähigkeit. In der neuesten Version sind alle Kontextmenüs optional deaktivierbar, um die Übersicht zu verbessern.

Neues bei Cinnamon

Am Mint-Desktop Cinnamon wird weiter gefeilt, aber die Luft für Innovationen wird zusehends dünner:

1. Die vom Mint-Team an erster Stelle genannte Verbesserung (*www.linuxmint.com/rel_tricia_cinnamon_whatsnew.php*) ist eine kosmetische Marginalie. Sie betrifft die Schriftgrößen in der Systemleiste und ist unter „Systemeinstellungen → Leiste → Leistenerscheinungsbild“ zu finden. Die drei verschiedenen, individuell einstellbaren Leistenbereiche gibt es schon länger, auch unterschiedliche Symbolgrößen für Programmstarter oder Icons in der „Gruppierten Fensterliste“. Nun lassen sich aber auch die Symbolgröße der Systemicons anpassen sowie die Schriftgröße der Systemelemente. Die Schriftgröße betrifft nicht allzu viele Leistenapplets, aber etwa die Datumsanzeige kommt in Betracht, eventuell auch die „Benutzeranzeige“ (falls mit textlicher Namensangabe eingestellt) oder der „Arbeitsflächenwechsel“ (falls mit Ziffernnummerierung eingestellt).

2. Das Leistenapplet „Blueberry“ zur Kontrolle von Bluetooth-Geräten wurde überar-

beitet. Es unterstützt laut Mint-Team mehr Bluetooth-Geräte und bietet daher verbesserte Erkennung.

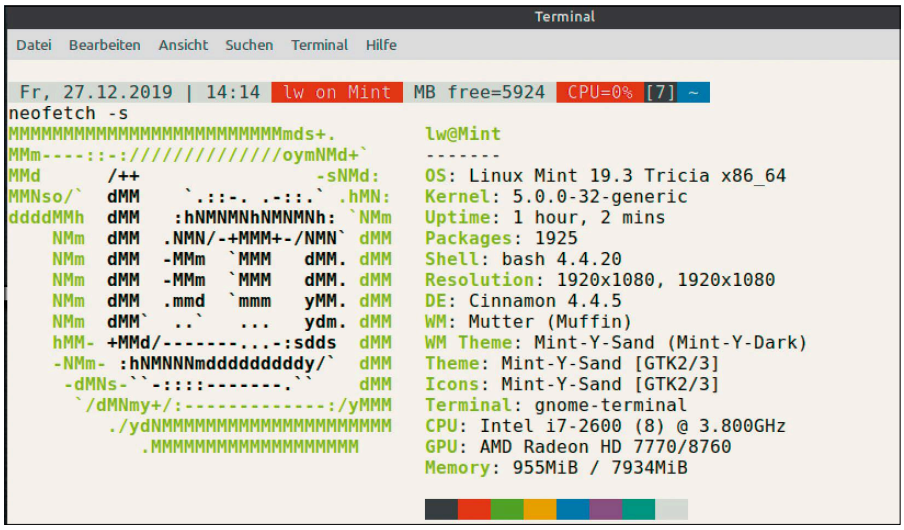
3. Die Cinnamon-typischen X-Apps erhalten marginale Verbesserungen. So erkennt der Standardeditor Xed jetzt „Wörter" mit beginnendem „http:" und „www." als Webadressen und bietet nach Rechtsklick auf solche „Wörter" den zusätzlichen dynamischen Kontext „[URL] öffnen", was dann den Standardbrowser aufruft.

4. Der Cinnamon-Dateimanager Nemo gehört seit Jahren zum Besten, was in dieser Kategorie zu haben ist. In der jüngsten Version führt das Menü „Bearbeiten → Einstellungen → Kontextmenüs" zu einer detaillierten Liste der verfügbaren Kontextmenüs und erlaubt das Aktivieren und Deaktivieren der Aktionen. Auf diese Weise entschlacken Sie das Angebot auf genau die Funktionen, die Sie wirklich benötigen. Das gilt analog auch für unnötige „Module" oder Symbole in der „Werkzeugleiste" – ein Angebot, das der Dateimanager aber schon länger kennt.

Nicht behoben ist weiterhin das Samba-Problem, dass der Klick auf „Netzwerk → Windows-Netzwerk" keine Freigaben auflistet. Dafür kann Nemo nichts, denn dieses Problem sitzt tiefer und muss von Canonical/Ubuntu oder durch das Samba-Protokoll gelöst werden. Weiterhin gilt aber als praktikable Abhilfe, eine Freigabe über „Datei → Mit Server verbinden" manuell und mit den notwendigen Angaben (IP, Domäne, Benutzer, Passwort) zu verbinden, dabei die Option „Das Passwort merken" zu aktivieren und danach die im Dateimanager geöffnete Freigabe dauerhaft als Lesezeichen zu speichern („Lesezeichen → Lesezeichen hinzufügen").

Änderungen bei der Anwendungssoftware

Die Softwareausstattung von Linux-Distributionen wird gerne kommentiert, kritisiert oder gelobt. Ein ernstes Kriterium für die Wahl einer Distribution sollte die mitgelieferte Software niemals sein, weil Überflüssiges ebenso schnell entsorgt wie Fehlendes bei Bedarf nachinstalliert ist. Trotzdem ist es interessant, die Motive der Distributionsmacher für oder gegen eine bestimmte Anwendungssoftware zu hinterfragen. Die vorinstallierte Software ist in allen drei Editionen identisch. Wichtige Standards sind seit jeher der Browser Firefox, das Mailprogramm Thunderbird sowie Libre Office. Beim weiteren Zubehör gibt es immer wieder mal neue Entscheidungen, so auch wieder in Version 19.3.



Neues Infotool im Terminal: Neofetch ist eine hübsche Ergänzung in Mint 19.3, steht aber im Prinzip jeder Linux-Distribution über die Paketquellen zur Verfügung.

Filmwiedergabe mit Celluloid: Das ist wohl eine arbeitsökonomische Entscheidung. Den bisherigen Xplayer hat das Mint-Team selbst gepflegt (auf Basis des Totem-Players), ohne damit die Leistung von Playern zu erreichen, welche die Hardwarebeschleunigung des Grafikchips nutzen. Gnome MVP, neuerdings „Celluloid", beherrscht dies und unterstützt höhere Auflösungen als der bisherige Xplayer. Als positiver Nebeneffekt soll Celluloid bei der Filmwiedergabe die CPU-Last und den Stromverbrauch senken (wichtig bei Notebooks). Im direkten Vergleich mit dem von uns bevorzugten VLC Player liegt Celluloid bei der CPU-Last gleichauf, zudem ist der RAM-Bedarf des VLC deutlich geringer.

Unterm Strich ist der VLC der bessere Player, entspricht aber offenbar nicht dem Trend der Mint-Macher zu möglichst einfacher Einsteigersoftware.

Pixelbearbeitung mit Drawing: Bei „Drawing" (auf deutschsprachigem System „Zeichnung") vermeiden wir die Bezeichnung „Bildbearbeitung", denn solchen Anspruch erfüllt das Programm nicht. Mit Drawing, das statt des komplexen Gimp Einzug findet, kann man geometrische Muster zeichnen oder Bildausschnitte mit farbigen Rahmen hervorheben. Es handelt sich um einfaches Pixelzeichnen ohne Zeichenobjekte oder gar Ebenen. Immerhin bleibt das brauchbare Pix an Bord, das sowohl als schneller Bildviewer arbeitet als auch (über das Symbol „Bearbeiten") typische Fotonachbearbeitung wie Schärfen, Farbkorrektur oder Zuschneiden vorsieht.

Notizen mit Gnote: Die Notwendigkeit einer lokalen Notizen-App darf bezweifelt werden, da Webdienste von Google, Microsoft oder Evernote zentrale Lösungen anbieten. Und wer dies aus Datenschutzgründen ablehnt, hat als Linux-Nutzer wenig Mühe, sich im Heimnetz eine zentrale Webserver-Lösung für Notizen einzurichten. Falsch ist es dennoch nicht, wenn das Mint-Team bei der aussterbenden Gattung der lokalen Notizprogramme mit Gnote weitermacht und das bisherige Tomboy ersetzt. Damit verschwindet nämlich das letzte Mono-basierte Programm aus der Mint-Standardausstattung. Mono ist eine Übersetzungsschicht für Microsoft-.NET-Software und sollte aufgrund sehr hoher RAM-Ansprüche nur bei unentbehrlicher Software zum Einsatz kommen.

Systeminfo mit Neofetch: Im Terminal gibt es ab Version 19.3 das Infotool Neofetch, das eine Anzahl von Optionen mitbringt und nach dem einfachen Aufruf mit

```
neofetch
```

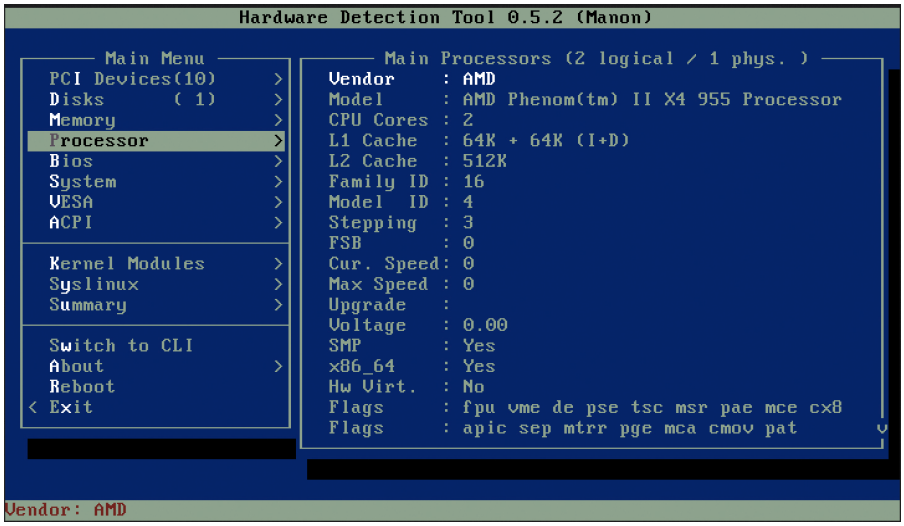
die wichtigsten Systeminformationen ausgibt (System, Kernel, CPU, GPU, RAM, Uptime, Desktop, Desktopthema und mehr). Neofetch informiert vollständiger als der Punkt „Systeminformation" in der grafischen Zentrale. Wer allerdings auch Infos über Datenträger und Netzwerk erwartet, wird ohne ein zusätzliches Tool wie inxi nicht auskommen. ■

Re- und Upcyling mit Linux

Der Heftschwerpunkt „Linux für jeden Zweck“ startet mit einem Thema mit wirtschaftlicher Brisanz: Muss man grundsolide ältere Hardware tatsächlich entsorgen, weil sie heutigen Standards nicht mehr entspricht oder weil das bisherige System ausläuft?

VON HERMANN APFELBÖCK

Die Frage „Was tun mit alter Hardware“ dürfte zu Beginn diesen Jahres Millionen Endanwender beschäftigt haben: Denn Windows 7 lief am 14. Januar 2020 aus – und dies oft auf Hardware, die für ein Upgrade auf Windows 10 technisch nicht ausreicht. Die LinuxWelt liefert auf diese Frage konkrete Antworten und Empfehlungen. Ungeachtet des nahenden Endes von Windows 7 besitzt fast jeder PC-Nutzer ausgemusterte Geräte, die unter Linux noch einen guten Job machen könnten. Darum geht es in diesem Beitrag. Jedoch fassen wir uns bei den technischen Details zu passender Hardware und Systemsoftware kurz.



Ältlicher, aber brauchbarer Prozessor: Das bootfähige HDT-Tool auf Heft-DVD informiert über alle Hardwarekomponenten eines Rechners inklusive aller CPU-Eigenschaften.

Der Hardwarecheck

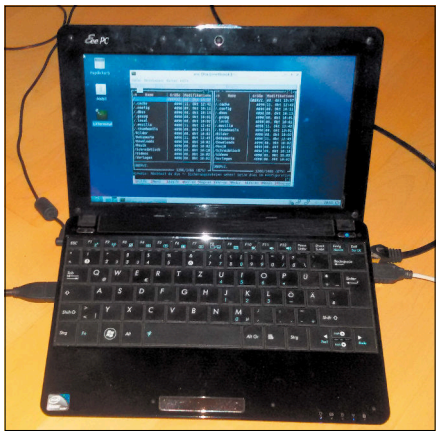
Die Mindestanforderungen für ein Gerät, das sich mit Linux und mit einigem Spaß wiederbeleben lässt, liegen etwa auf dem Niveau der kleinen Platinenrechner Raspberry & Co:

- Eine Dualcore-CPU ab ein GHz sowie mindestens ein GB RAM sollte das Altgerät mitbringen. Diese etwa für Netbooks typische Ausstattung reicht bestens für kleine Serverrollen, kann aber auch noch als Zweitdesktop und zum Surfen genügen.
- Das Thema PAE – eine CPU-Eigenschaft, um mit 32-Bit-CPUs mehr als 3,2 GB RAM zu adressieren – sollten wir ad acta legen. Hardware ohne PAE-fähige CPU ist ein Fall für den Elektronikschrott, wenngleich manche Linux-Spezialdistributionen solche CPUs immer noch unterstützen (Varianten mit dem Stichwort „nonpae“, „legacy“).
- Generell sind 32-Bit-Prozessoren so veraltet (15 Jahre und älter), dass Recyclingversuche wenig Freude versprechen. Jedoch kann es sinnvoll und ressourcenschonend sein, auf alter 64-Bit-Hardware ein 32-Bit-Linux zu installieren, wie es etwa Debian (*www.debian.org*), älteres Lubuntu (*https://lubuntu.net/*), Antix (*https://antixlinux.com*), Q4-OS (https://q4os.org/) oder Bodhi Linux (*www.bodhilinux.com*) nach wie vor anbieten.
- Ältere Netbooks/Notebooks bieten in der Regel Fast Ethernet (100 MBit/s). Das ist für einen Zweitdesktop oder kleinen Heimserver ausreichend; überzeugend servertauglich ist dieses Tempo allerdings nicht, was insbesondere bei großen Film- und Imagedateien unangenehm auffällt.
- USB 2.0 genügt für jeden Zweitdesktop und auch noch für einen Heimserver mit moderaten Ansprüchen. Geräte mit altem USB 1.x sind nicht mehr alltagstauglich.

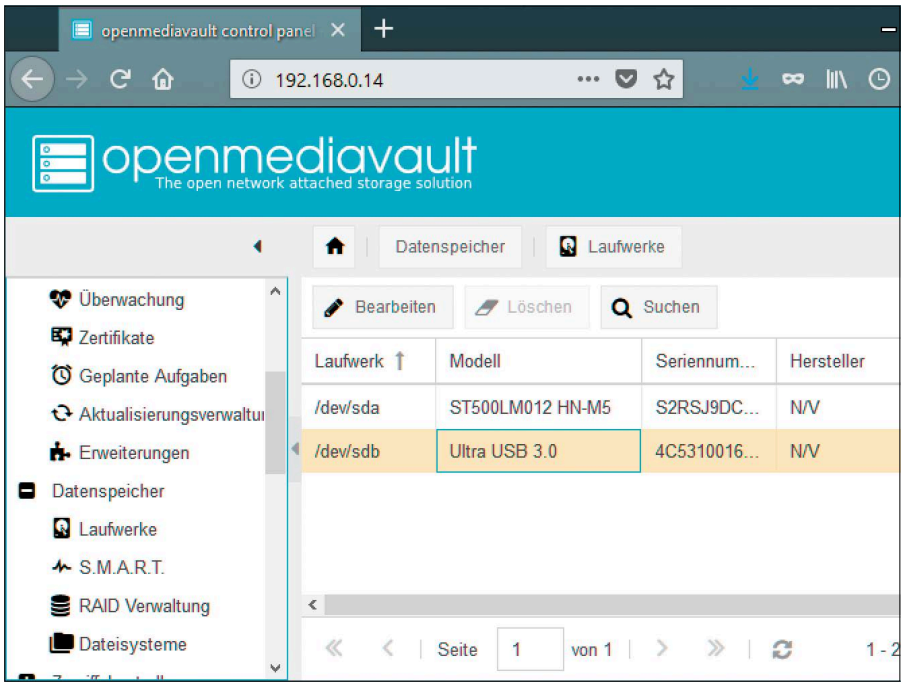
Welche Hardware konkret in einem Altgerät steckt, können Sie eventuell mit dem System ermitteln, das auf dem Gerät aktuell noch läuft. Meistens einfacher ist aber der Griff zum unabhängigen Hardware Detection Tool (HDT), das Sie bootfähig auf der Heft-DVD finden (unter „Extras und Tools“). HDT liefert alle relevanten Infos zu CPU, RAM, Ethernet, WLAN. Lediglich die Recherche der USB-Version ist mühsam und eventuell schneller durch einen empirischen Test zu erledigen, wobei ein Kopiertempo von 15 bis 30 MB/s taugliches USB 2.0 indiziert.

Altrechner als Zweitdesktop

Für den Desktopeinsatz älterer Notebooks und Netbooks sind die kleineren Ubuntu-



Nicht vorschnell zum Elektronikschrott! Solche Netbooks erreichen locker die Leistung eines Raspberry 3 und arbeiten klaglos als Datenserver oder wie hier als Desktop (Lubuntu).



Hübsche Oberfläche für Datenserver: Open Media Vault zeigt hier eine größere Datenfestplatte und den (überdimensionierten) USB-Stick für das System. Acht GB reichen dem sparsamen NAS-System.

Editionen Lubuntu und Xubuntu eine zumutbare Last. Diesen Distributionen sollten insbesondere solche Nutzer den Vorzug geben, die mit wenig Linux-Erfahrung ein unkompliziertes Allzwecksystem suchen. Kandidaten wie Antix, Bodhi, Bunsenlabs oder Kanotix sind zwar noch schlanker und schneller, erfordern aber auch mehr Einrichtungsaufwand.

So können etwa nach der Standardinstallation wichtige Netzwerkkomponenten fehlen, die für den Zugriff auf Freigaben notwendig sind (Pakete wie „libsmbclient“, „smbclient“, „openssh-client“, „gvfs-backends“). Im Unterschied zu Ubuntu-Varianten verwenden exotischere Distributionen statt Netzwerkmanager und Automount im Dateimanager gewöhnungsbedürftige Tools wie Gigolo oder Wicd. Nicht zuletzt muss der Einsatz von Minimalisten mit Abstrichen am Desktop bezahlt werden: Das Einrichten eines Bodhi Linux oder Bunsenlabs kostet einige Zeit der Einarbeitung, sofern Sie das System nicht bereits intim kennen.

Eine Anmerkung zum Browser: Browser wie Firefox und Chrome sind Schwergewichte. Altgeräte danken den Einsatz möglichst schlanker Linux-Browser wie Epiphany oder Midori mit schnelleren Start- und Reaktionszeiten. Diese Alternativen haben reduzierte Funktionen und Anpassungsmöglichkeiten, reichen aber völlig für den Surfalltag.

Altgeräte als Heimserver

Während Altgeräte als Desktop oder als Surfsystem über den Status eines Zweit- und Notsystems selten hinauskommen, können ältere Notebooks und Netbooks als Heimserver voll überzeugen. Die meistgenutzte Serverrolle ist die eines Samba-Datenservers. CPU und RAM sind für diese Aufgabe unkritisch, und mit Fast Ethernet und an USB 2.0 angeschlossenen Laufwerken ist ein heimischer Datenserver kein Turbo, aber ein solides Arbeitstier.

Wer es dabei klickfreundlich haben will, kann das NAS-System Open Media Vault (OMV) in seiner x86-Ausführung installieren (*https://sourceforge.net/projects/openmediavault/files/*). OMV, aktuell Version 4.1.22, bringt typische Serverdienste wie Samba, FTP, SSH standardmäßig mit. Das Download-ISO ist ein textbasierter Installer, der die wenigen Schritte gut erklärt. Als „Primäre Netzwerk-Schnittstelle“ sollte kabelgebundenes Ethernet gewählt werden („eth0“). Der Rechnername ist frei wählbar, „Domain-Name“ belassen Sie auf der Vorgabe „local“. Das „Root-Passwort“ brauchen Sie für den Systemzugriff via SSH.

Der Punkt „Festplatten partitionieren“ erscheint, wenn für das System mehrere Zieldatenträger in Betracht kommen. Dies ist praktisch immer der Fall, wenn Sie das Setup über ein externes Medium ausführen und das Altgerät noch eine interne Festplatte enthält. Installieren Sie nicht auf die interne Festplatte, weil das System grundsätzlich den kompletten Datenträger übernimmt und der restliche Platz verschwendet wäre. Für das kleine System genügt ein USB-Stick mit acht oder 16 GB.

Die spätere Konfiguration verläuft in einer Weboberfläche, die über die IP-Adresse des Servers mit jedem Browser im lokalen Netz zu erreichen ist. Angeschlossene Datenträger (Ext, FAT, NTFS) mountet OMV automatisch ins Dateisystem und zeigt sie unter „Datenspeicher → Reale Festplatten“. Wesentliche Einstellungen finden Sie unter „Dienste“, wo Sie für Netzfreigaben „SMB/CIFS“ aktivieren. Danach kann im Register „Freigaben“ ein Datenträger oder Ordner freigegeben werden. Die zugriffsberechtigten Konten richten Sie unter „Zugriffskontrolle → Benutzer“ ein.

Noch ökonomischer als OMV arbeitet ein Datenserver ohne Weboberfläche (und ohne grafischen Desktop), der komplett im Terminal per SSH eingerichtet und gewartet wird. Kandidaten für solchen Einsatz sind Debian (Netinstaller unter *www.debian.org/distrib/netinst*) oder der Ubuntu-Server (*www.ubuntu.com/download/server*). Terminalkundige erstellen Samba-Freigaben für etliche Benutzer mit einer Handvoll Befehlen in wenigen Minuten. Beispiele für Samba im Terminal dafür finden Sie im angesprochenen PDF „LinuxWelt XXL“ auf der Heft-DVD. ■

Preiswerte Server dank Linux

Der freie und anpassungsfähige Linux-Kernel kann jede Hardware antreiben. Tatsächlich gibt es vom Kleinstgerät bis hin zum Supercomputer keine Skalierung, die Linux auslässt. Endanwender profitieren insbesondere vom unteren Segment.

VON HERMANN APFELBÖCK



Ob Router, NAS, Kamera, Navigationsgerät, Flugzeugentertainment oder CERN-Großrechner – ein spezialisiertes Linux kann es klein oder groß. Die bei Privatnutzern verbreitetsten Linux-Anpassungen sind Fritz-OS für die Fritzbox-Router und natürlich Android für Mobilgeräte, das Google 2008 in Rekordzeit als Antwort auf das 2007 erschienene iPhone entwickelte. Viele kreative Ideen und Konzepte für neue und preisgünstige Endanwender-Hardware wären ohne den offenen Linux-Kernel schnell begraben oder nie geboren. Außerdem müssten Geräte wie Router oder NAS ohne Linux anders kalkuliert werden und wären entsprechend teurer (Lizenzgebühren).

Eine überraschend erfolgreiche Allianz zwischen innovativem Hardwarekonzept und Linux ist die Geräteklasse der Ein-Platinen-Rechner mit dem Raspberry Pi als Initiator, dem inzwischen zahlreiche Konkurrenten gefolgt sind. Die als Entwicklerboards und Programmiereinstieg geplanten Winzlinge haben sich zu preisgünstigen Heimservern weiterentwickelt und als attraktive Alternativen zu kommerziellen NAS-Geräten etabliert.

„Embedded“ versus „offene“ Systeme

In NAS-Homeservern von Asus, Buffalo, D-Link, QNAP, Synology u. a. arbeitet fast immer ein angepasstes Linux (ganz selten Windows) – bei dieser Geräteklasse regelmäßig mit Apache- oder Nginx-Server, der die Konfigurationsoberfläche im Netz anbietet. Ähnliches gilt für Router, Access Points, Repeater und Heimnetzgeräte aller Art wie etwa IP-Kameras. Es handelt sich stets um ein Embedded Linux, das zwar oft modulare Erweiterungen und Systemupdates erlaubt, aber im Prinzip hermetisch bleibt. Ein Austausch des Systems ist regulär nicht vorgesehen. Die Platinenrechner Raspberry & Co. haben demgegenüber gleich drei entscheidende Vorteile:

1. Die Systemsoftware kann frei gewählt werden. Mindestens eine Handvoll von Systemen unterschiedlicher Ausrichtung ist für jeden Platinenrechner zu finden, am meisten für den Raspberry Pi. Die primäre Strategie bei der Systemsuche wird beim Hardwarehersteller ansetzen:

Raspberry Pi: *www.raspberrypi.org*
Odroid: *www.hardkernel.com*
Banana Pi: *www.lemaker.org*
Cubieboard: *http://cubieboard.org*
Cubox/Hummingboard: *http://solid-run.com*

Aber es gibt auch Distributionen wie **Dietpi**, das unter *https://dietpi.com/* zentral für jede denkbare Hardware angeboten wird.

2. Auf Platinen installieren Sie ein offenes Linux-System. Ein Betriebssystem wie Raspbian oder Dietpi kann beliebige Software und Komponenten nachrüsten, aber auch Unnötiges entsorgen. Ob der Server, nur mit SSH verwaltet, als minimaler Datenserver läuft oder mit Webdiensten, einem Open Media Vault, mit Kodi, Plex oder einem anderen Medienserver, das bestimmt der Benutzer.

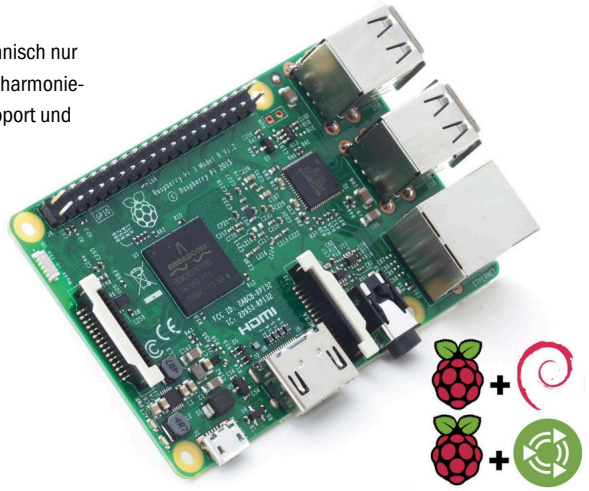
3. Da das System einfach auf SD-Karte geschrieben und in den Platinenslot gesteckt wird, kann es durch eine Imagesicherung der SD-Karte leicht kopiert und jederzeit wiederhergestellt werden. Außerdem ist bei einem Hardwaredefekt ein sorgfältig eingerichtetes System auf einer baugleichen Platine durch Einsatz der SD-Karte sofort wieder einsatzfähig.

NAS versus Platinenhardware

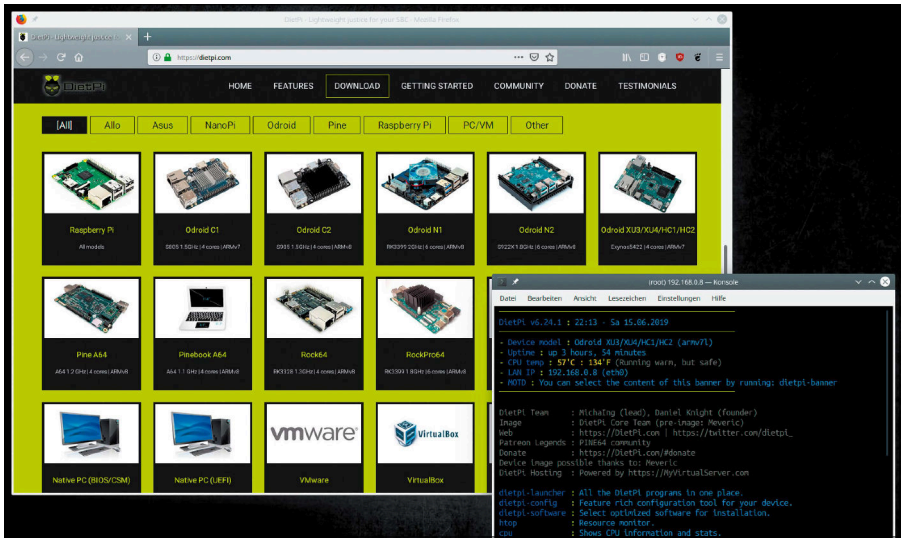
Es gibt NAS-Geräte für mehrere Tausend Euro mit acht oder 16 Festplatten, mehreren Ethernet-Ports und üppigen weiteren Anschlüssen. Es wäre unfair, solche Profigeräte neben Hundert-Euro-Platinen wie Cubieboard 6, Odroid XU4 oder Odroid N2 zu stellen. Vielmehr geht es hier um typische Home-NAS-Geräte mit bis zu vier Einschüben und Preisen bis maximal 500 Euro. Hinsichtlich CPU und RAM sind teurere Platinenrechner mit ARM-Quadcore-CPU (zwei GHz) und zwei bis vier GB RAM den typischen Home-NAS-Geräten überlegen. Die ARM-Marvell-CPUs günstiger NAS-Geräte können da eindeutig nicht mithalten, die leistungsstärkeren Intel-Celeron-CPUs sind erst in der NAS-Preisklasse ab 300 Euro aufwärts verbaut.

Die wichtigeren Kriterien sind allerdings die Netzwerkleistung und die Übertragungsleistung auf angeschlossene Datenträger. Beim Raspberry Pi 3 ist das Gigabit-LAN durch USB 2.0 auf etwa 300 MBit/s gedrosselt. Wer aber mit einem kommerziellen NAS mithalten will, muss Gigabit-LAN mit USB 3.0 oder SATA kombinieren. Beim Raspberry Pi 4 ist sind die LAN-Einschränkungen des Pi 3 beseitigt, er liefert USB 3.0 und volles Gigabit-LAN. Weitere Kandidaten sind Odroid XU4 (circa 70 Euro bei *pollin.de*), Odroid N2 (circa 95 Euro bei *pollin.de*), Cubieboard 6 (aktuell nicht lieferbar) und Banana Pi M3 (circa 80 Euro bei *amazon.de*). Zu diesen Preisen sind jeweils 15 bis 20 Euro für Gehäuse und Netzteil zu addieren.

Eine detaillierte Gegenüberstellung aller bekannten Ein-Platinen-Rechner finden Sie auf der englischsprachigen Wikipedia unter *https://en.wikipedia.org/wiki/Comparison_of_single-board_computers*.



Das Original: Der Raspberry 3 ist technisch nur Durchschnitt, aber die Komponenten harmonieren und zudem überzeugen Preis, Support und Systemauswahl.



Dietpi gibt es für jede Platine (*https://dietpi.com*). Das schlanke Serversystem bietet hervorragende Konfigurationszentralen, will aber per SSH im Terminal administriert werden.

Typische Linux-Systeme für Platinen

Der Installer Noobs (*www.raspberrypi.org/downloads/noobs*) ist für Raspberry-Einsteiger der einfachste Weg für die Systeminstallation. Entpacken Sie Noobs (etwa 1,5 GB mit Raspbian im Gepäck) oder Noobs Lite (32 MB für Onlineinstallation) auf eine FAT-formatierte SD-Karte mit mindestens acht GB. Anschließend legen Sie diese Karte in den Raspberry ein und befolgen die Anweisungen. Systemauswahl und Installation erfolgen direkt auf dem Raspberry. Im großen Noobs-Image ist Raspbian enthalten, außerdem lassen sich unter anderem Libre Elec (Kodi), Raspbian Lite, Lakka oder Recalbox-OS via Internet installieren.

Noobs ist ein Installer und nicht der typische Weg zum Platinensystem. Der sieht vielmehr so aus, dass Sie das Systemimage beim Hersteller herunterladen und einfach auf SD schreiben (egal ob mit dd, Win 32 Disk Imager oder Etcher). Damit ist es – ohne Installation – auf der passenden Hardware sofort lauffähig.

Eine besonders schlanke „Diät"-Distribution, die es unter *https://dietpi.com/* für praktisch alle Platinenrechner gibt, ist der Minimalserver Dietpi – ein System standardmäßig ohne grafischen Desktop, aber mit exzellenten Konfigurationszentralen, das sich für alle SSH-affine Nutzer eignet. Die Zentralen zeigt Dietpi bei jedem Systemstart und jeder SSH-Anmeldung an. Der „dietpi-launcher" ist die übergeordnete Instanz, die sämtliche Dietpi-Programme anbietet, inklusive Paketmanager, Updater, Backup und Cronjob-Manager. Die Zentrale „dietpi-config" enthält die fundamentale CPU-, Hardware- und Netzwerkkonfiguration. „dietpi-software" ist der Paketmanager zum Installieren und Deinstallieren.

Einem kommerziellen NAS-System am nächsten kommen Sie mit dem einfach bedienbaren und mit Plug-ins erweiterbaren System Open Media Vault. Auch OMV haben praktisch alle Platinenhersteller in ihrem Systemrepertoire.

Ähnliches gilt für das Mediencenter Kodi, das es in mehreren Distributionen gibt (Libre Elec, Open Elec, OSM, Xbian). Mindestens eine dieser Kodi-Distributionen hat jede populäre Platine im Angebot. Anders als bei anderen Distributionen ist bei Kodi eine Ersteinrichtung über direkt angeschlossene Peripherie erforderlich (Maus, Tastatur, Monitor). ■

Große und kleine Serverrollen

Der Linux-Desktop bleibt in der Nische, doch als Server ist Linux ganz groß und dominiert als Lamp-Server (Linux – Apache – My SQL – PHP) das Internet. Zahlreiche kleine und große Linux-Serverlösungen machen aber auch das Heimnetz attraktiver.

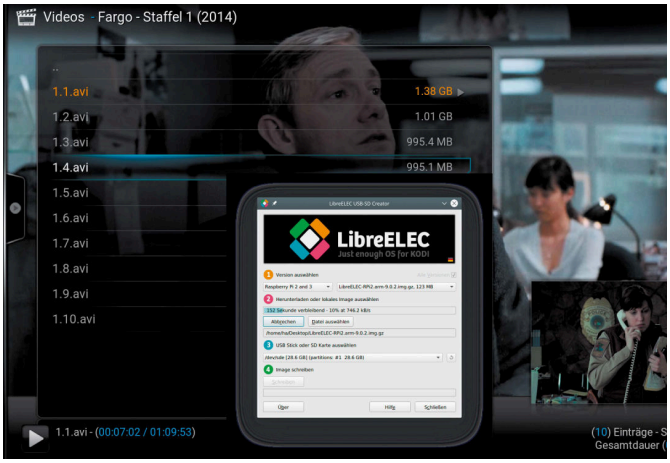
VON HERMANN APFELBÖCK

Während sich Mac-OS von Serverambitionen weitgehend verabschiedet hat und praktisch nur noch als Dateiserver dienen kann, behauptet Windows weiterhin seinen Platz neben Linux. Typische Serverdienste mit und ohne Apache/Nginx sind plattformunabhängig und laufen auch unter Windows – etwa Wordpress, Drupal, Joomla, Mediawiki, Dokuwiki. Programmpakete wie XAMPP vereinfachen die Einrichtung einer Lamp-Umgebung unter Windows und Mac-OS X und erlauben viele Serverprojekte auch auf diesen Plattformen. Selbstverständlich verzichten auch Medienserver wie Kodi oder Plex nicht auf die verbreitete Windows-Plattform.

Die meisten dieser Serverdienste haben ihre Heimat aber im Open-Source- und Linux-Umfeld. Das zeigt sich nicht nur in der deutlich größeren Anzahl kleiner und spezialisierter Dienste, sondern auch im Variantenreichtum: So gibt es etwa für das Kodi-Mediencenter mit Libre Elec, Geexbox, OSMC, Xbian unter anderem eine ganze Anzahl von Spezialdistributionen für PCs und Platinenrechner. Und zahlreiche kleinere, vor allem für das Heimnetz interessante Dienste laufen ausschließlich unter Linux. Dieser Artikel kann nur einige wenige Beispiele ansprechen.

Nextcloud: Cloud für Web und Intranet

Die flexible Kollaborations-Suite Nextcloud (*https://nextcloud.com/*) eignet sich als Datenzentrale, Terminkalender, Fotogalerie, Adressverwaltung und vieles mehr – und auf Wunsch auch weniger: Denn der Umfang ist modular über „App-Pakete" zu verwalten. Der Vorgänger Owncloud war unter einer XAMPP-Umgebung auch noch unter Windows zu installieren, die Nextcloud hat sich davon distanziert. Unter Windows sind nur noch Umwege über einen Docker-Container oder eine Linux-VM realisierbar.



Serversoftware wie das Kodi-Mediencenter findet unter Linux beste Unterstützung. Dazu gehören spezielle Distributionen wie hier Libre Elec für Platinenrechner.

Unter Linux ist das Projekt zu Hause und hier gibt es inzwischen besonders komfortable Installationsvarianten, die das Produkt im Handumdrehen startklar machen:

Nextcloud als Snap-Paket: Die Installation als Snap-App ist ideal für Nutzer, die aktuell keinen Apache-Server laufen haben und sich mit dessen Konfiguration auch nicht befassen wollen. Im Snap-Paket wird inklusive Apache alles eingerichtet, was Nextcloud benötigt. In Ubuntu ist die Snap-Verwaltung Standard, wo nicht (etwa bei Raspbian), ist das mit

```
sudo apt install snapd
```

schnell nachgeholt. Damit ist die Nextcloud mit dem schlichten Befehl

```
sudo snap install nextcloud
```

installiert, sofort startklar und unter *http://localhost* am Rechner selbst, über dessen IP-Adresse mit jedem Browser im Netz erreichbar. Da heutige Browser auch im lokalen Netz HTTPS erwarten, verwenden Sie für SSL-Verschlüsselung ein selbst signiertes Zertifikat:

```
sudo nextcloud.enable-https self-
  signed
```

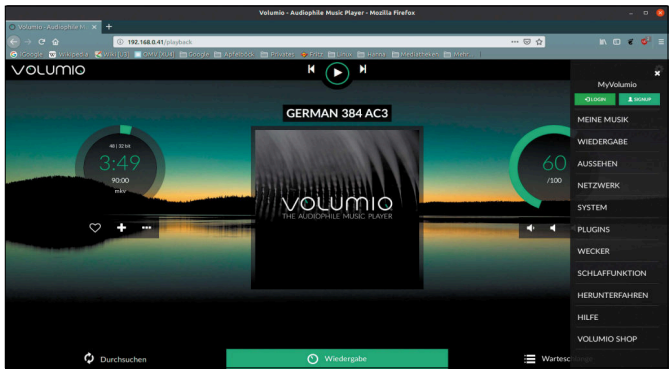
Für den Zugriff muss dann jeder Browser im lokalen Netz eine Ausnahmeregel festlegen (Firefox: „Risiko akzeptieren und fortfahren"). Die weitere Konfiguration der Nextcloud ist keineswegs trivial, eine laufende Instanz ist aber mit dieser Snap-Variante in Minuten erreicht.

Nextcloud für Platinen: Nextcloud Pi (*https://ownyourbits.com/nextcloudpi/*) ist ein Sorglospaket für Odroid XU4, Rock64, Banana Pi, aber auch für PCs (x86), indem es das Betriebssystem Raspbian gleich mit einer eingebauten Nextcloud kombiniert. Das Image schreiben Sie nach dem Entpa-

cken mit den üblichen Mitteln auf eine SD-Karte. Im Prinzip ist die Nextcloud nach Einlegen der SD-Karte in die Platine sofort lauffähig und konfigurationsbereit.

Die Soundstation Volumio

Volumio ist ausschließlich als Linux-System verfügbar. Ursprünglich für den Raspberry konzipiert, ist es inzwischen auch für Odroid, Asus Tinker Board und x86 (PC) portiert. Funktional handelt es sich um eine Musikstation, die am lokalen Gerät Musik abspielt, aber über einen Webserver von jedem Netzwerkgerät zu steuern ist (*http://volumio.local*). Der ZIP-Download kann nach dem Entpacken mit den üblichen Werkzeugen (Etcher, dd, Win 32 Disk Imager, letzteres auf Heft-DVD) auf USB transferiert werden. Mit schicker und äußerst einfacher Oberfläche kann Volumio auch große Musikbibliotheken performant verwalten und überzeugend präsentieren.



Hübsche Musikstation: Volumio ist eine spezialisierte Distribution, deren einfache Oberfläche am Gerät selbst und übers Netzwerk identisch zu bedienen ist.

Readymedia: Kleiner Medienserver

Streamingserver, die Audio und Video an Netzwerkgeräte ausliefern, bietet Linux in Fülle. Kodi, Gerbera, Mopidy sind allesamt Streaminglösungen mit unterschiedlicher Ausrichtung. Fokus bei Readymedia (Mini DLNA) ist Minimalismus und der Verzicht auf jede Oberfläche. Der Server erscheint einfach auf allen DLNA/UPnP-konformen Endgeräten (TV, Smartphone, VLC, Windows Media Player) und erlaubt den Abruf der Medien. Das Programm liegt noch unter seinem alten Namen „minidlna“ in den Paketquellen und ist mit

```
sudo apt install minidlna
```

schnell installiert. Konfiguriert wird der Purist über die Textdatei „/etc/minidlna.conf“ mit Einträgen wie:

```
media_dir=A,/home/ha/Musik
```

Das „A,“ steht für Audio („V“ für Videos und „P“ für Bilder) und weist Readymedia an, den Ordner inhaltstypisch zu analysieren (Metainfos). Nach Konfigurationsänderungen ist ein Neustart des Dienstes mit

```
sudo service minidlna restart
```

erforderlich.

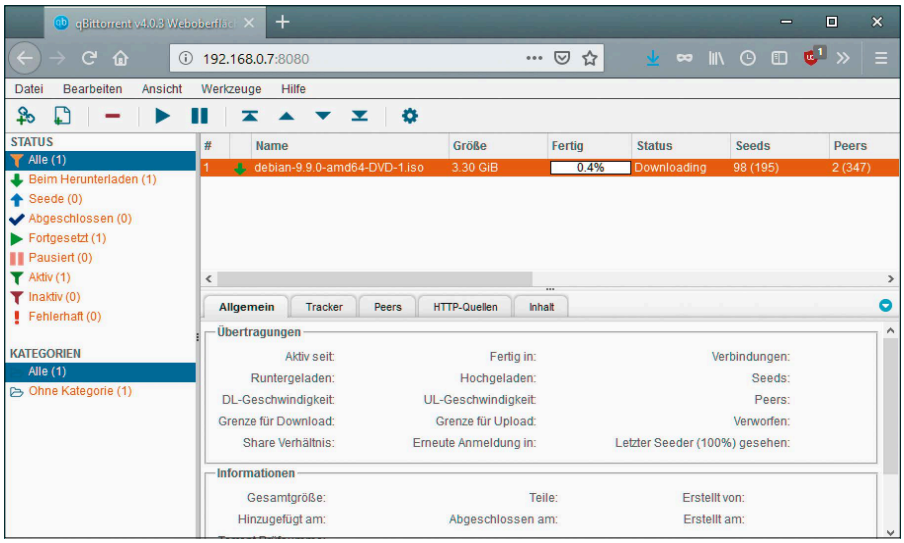
Qbittorrent-Client mit Weboberfläche

Ein Beispiel für eine spezialisierte Serverrolle ist ein zentraler Bittorrent-Empfänger, den alle Netzteilnehmer über seine IP-Adresse nutzen. Das erspart lokale Bittorrent-Programme auf allen anderen Rechnern. Das Tool installieren Sie auf dem Server mit

```
sudo apt install qbittorrent-nox
```

aus den Paketquellen. Als Serverhardware genügt ein Raspberry vollauf. Nach dem Start (*qbittorrent-nox*) ist der Server über „[IP]:8080“ mit jedem Browser erreichbar. Der Zugang erfolgt als Benutzer „admin“ mit Kennwort „adminadmin“ (was Sie über „Werkzeuge → Optionen → Weboberfläche“ ändern können). Jeder Rechner im Netz kann Torrent-Dateien zum Server hochladen und somit dort den Download auslösen. Idealerweise ist umgekehrt das – in Qbittorrent-nox einstellbare – Downloadverzeichnis per Samba freigegeben.

Wenn Qbittorrent immer laufen soll, braucht es einen Aufruf mit vollem Pfad „/usr/bin/qbittorrent-nox“ in der Crontab. Oder Sie starten es bei Bedarf über SSH, wobei dann auf dem Server zusätzlich ein SSH-Server laufen müsste (nie verkehrt). ■



Der zentrale Qbittorrent lässt sich über das Netzwerk im Browser bedienen. Diese Aufgabe stemmt auch ein kleiner Platinenrechner der Sorte Raspberry Pi.

SERVERDIENST FÜR SERVER

Kein Linux-Server ohne Open-SSH-Server! Es gibt keinen verbreiteteren Serverdienst unter Linux und keinen, der eine schnörkellosere Serveradministration ermöglicht. Ein Benutzerkonto auf dem Server und ein SSH-Befehl genügen, um über das Netz den kompletten Server im Terminal unter sich zu haben. Mit dem zugehörigen Datenprotokoll SFTP steht das komplette Dateisystem auch grafischen Dateimanagern zu Diensten. SSH beherrscht auch das unixoide Mac-OS X, während Windows sich lange Zeit auf native Remotefähigkeiten zurückzog (Win RM) und erst neuerdings an einem SSH-Server arbeitet (als SSH-Client dient seit Ewigkeiten das Tool Putty).

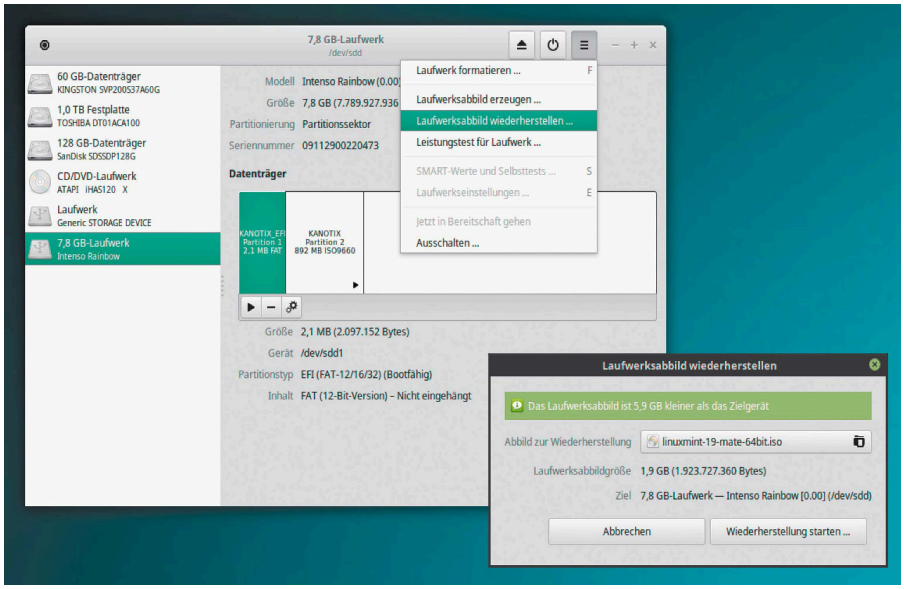
Linux auf USB: Die Werkzeuge

Linux läuft ohne Einschränkung auf USB-Datenträgern – mit USB 3.x fast wie auf Festplatte oder SSD. Dieser und die folgenden Artikel beschreiben Kopierwerkzeuge, Installationsvarianten, einschlägige Distributionen und Szenarien.

VON HERMANN APFELBÖCK

Für Linux auf USB gibt es gute Gründe: Einer der dringendsten ist der Einsatz einer unabhängigen Rettungsumgebung, wenn Windows oder Linux nicht mehr startet oder der Start aus Sicherheitsbedenken nicht mehr ratsam ist. Oder man benötigt ein sicheres Livesystem zum Surfen oder ein Testsystem für riskante Webbesuche, ohne sein reguläres Linux oder Windows zu gefährden. Doch auch der Einsatz als mobiler Desktop auf USB-Stick ist denkbar.

Dieser Beitrag erklärt das „Wie“, also die technischen Werkzeuge, mit welchen Sie die gewünschten Systeme startklar auf USB befördern. Die nachfolgenden Artikel thematisieren dann das „Was“, also die geeigneten Tools und Distributionen für den USB-Einsatz sowie speziellere Szenarien für sicher verschlüsselte Daten auf mobilen Sticks und USB-Festplatten.



Rohkopie eines ISO-Abbilds auf USB-Stick: Auf Desktop-Linux erledigt Standardzubehör wie hier Gnome-Disks diesen Job. Tools wie Etcher oder dd-Kommandos sind hier nicht notwendig.

1. Bootfähige ISOs kopieren

An Kopierwerkzeugen für ISO-Abbilder auf USB besteht kein Mangel. Wer nur ein einziges Livesystem ohne „Persistenz“-Option (siehe unten) auf USB übertragen will, kann einen der nachfolgend beschriebenen Rohkopierer verwenden. Eine solche Rohkopie setzt immer voraus, dass das kopierte ISO-Image eine hybride Bootumgebung mitbringt, also nicht nur ISO-konform von CD/DVD bootet, sondern auch von USB. Dies ist aber heute bei den allermeisten Livesystemen Standard.

Der einschlägige Rohkopierer dd unter Linux ist das Kommandozeilentool dd mit dieser Syntax:

```
sudo dd if=[Name].iso of=/dev/sd[x]
```

Nach „if=“ (Inputfile) folgt der Name, gegebenenfalls der komplette Pfad der ISO-Datei, nach „of=“ (Outputfile) das Zielgerät. Das altehrwürdige dd (Diskdump) behält vor allem dadurch seine Berechtigung, dass es unter allen Linux-Distributionen funktioniert.

Alternative und bequemere Rohkopierer sind grafische Tools wie der Partitionsmanager unter KDE oder Gnome-Disks („Laufwerke“) unter Gnome, Cinnamon & Co.: Hier markieren Sie links das gewünschte Ziellaufwerk und wählen über das Zahnradsymbol die Option „Partitionsabbild wiederherstellen“. Sie erhalten dann ein Navigationsfenster, um das zu kopierende ISO-Image auszuwählen.

Der einschlägige Rohkopierer unter Windows heißt Win 32 Disk Imager (auf Heft-DVD, Download unter *http://sourceforge.net/projects/win32diskimager*).

Hier genügt es, die Quelldatei („Image File“) und das Zielgerät („Device“) anzugeben. Da das Werkzeug standardmäßig nur IMG-Dateien anzeigt, wählen Sie als Dateifilter „*.*“, um eine ISO-Quelldatei auszuwählen. Die Schaltfläche „Write“ startet den Kopiervorgang.

Ein zunehmend populärer Rohkopierer ist Etcher. Das grafische Werkzeug gibt es für Linux, Windows und Mac-OS (*https://www.balena.io/etcher/*), ist überall identisch und einfach zu nutzen, fällt aber für seine schmale Funktionalität viel zu wuchtig aus (100 bis 130 MB).

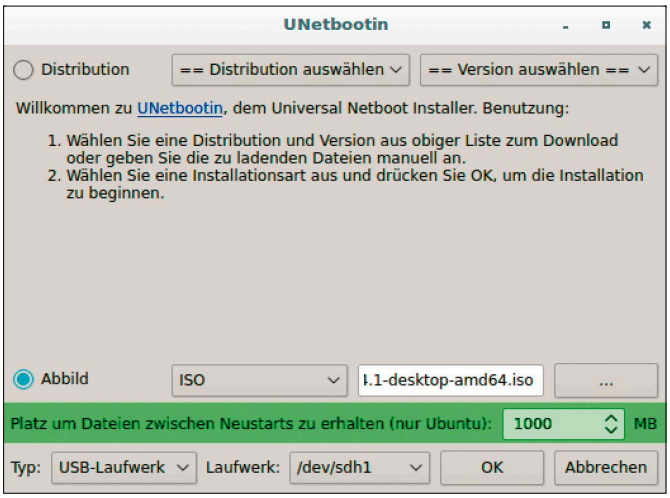
2. Unetbootin unter Linux und Windows

Unetbootin transportiert wie die Rohkopierer genau ein Livesystem (ISO-Image) auf den Zieldatenträger Ihrer Wahl. Das langbewährte Tool gibt es für Linux, Windows und Mac-OS X (auf Heft-DVD, Download unter *https://unetbootin.github.io/*). Um ein ISO-Image bootfähig auf USB-Stick zu befördern, wählen Sie im Dialog unten die Option „Abbild“ und navigieren dann mit der Schaltfläche „...“ zur gewünschten Datei. Nach Klick auf „Öffnen“ erscheint der komplette Pfadname im Eingabefeld. Danach wählen Sie neben „Typ“ die Option „USB-Laufwerk“ und neben „Laufwerk“ geben Sie die Kennung des USB-Sticks an. Der Klick auf „OK“ startet den Kopiervorgang. Kontrollieren Sie die Laufwerkskennung des USB-Sticks ganz genau, denn Unetbootin wird das Medium komplett überschreiben also alle Daten löschen.

Das ISO-Abbild muss nicht unbedingt bereits lokal vorliegen. Unetbootin kennt nämlich die allermeisten populären Distributionen und kann diese auf Wunsch auch selbst aus dem Web herunterladen. Dazu dient die Drop-down-Liste „Distribution auswählen“ ganz oben. Ob dies in allen Fällen funktioniert, haben wir nicht getestet, da wir den eigenhändigen Download vorziehen.

Persistenzoption: Gegenüber einer einfachen Rohkopie bietet Unetbootin den wesentlichen Vorzug des optionalen Persistenzspeichers, der alle Ubuntu-Livesysteme wesentlich aufwertet. Wenn Sie eine offizielle Ubuntu-Variante oder ein Ubuntu-Derivat wie Linux Mint oder Elementary OS auf USB kopieren, erscheint im Programmfenster automatisch eine zusätzliche Option: Neben „Platz um Dateien zwischen Neustarts zu erhalten“ können Sie eine Speichergröße festlegen, beispielsweise „500 MB“. Dies ermöglicht es, im späteren Livesystem weitere Programme zu installieren oder das System individuell einzurichten. Systemeinstellungen und nachinstallierte Programme bleiben dann erhalten. Das ist untypisch für ein Livesystem und erweitert den Komfort erheblich. Für ein paar individuelle Einstellungen genügt ein Persistenzspeicher von 50 bis 100 MB, für geplante Nachinstallationen sollte es mit 200 bis 500 MB etwas mehr Platz sein. Solche Persistenzoption für Ubuntu-Verwandte bieten auch die nachfolgend beschriebenen Multiboot-Tools (Multiboot-USB, Yumi).

Nutzen Sie in Unetbootin & Co. das Angebot der Persistenz. Dann kann das (Ubuntu-) Livesystem Einstellungen speichern und zusätzliche Software installieren.



3. Multiboot-USB: Livesystem-Sammlung auf USB

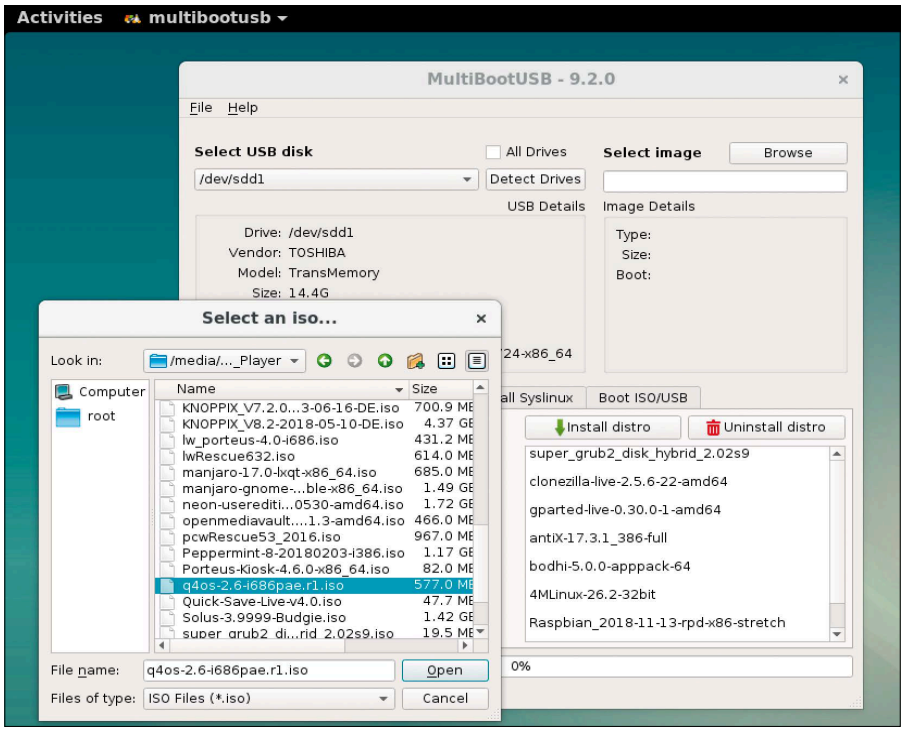
Wer auf USB-Sticks oder USB-Festplatten eine ganze Sammlung an Livesystemen unterbringen will, hat unter Linux die Wahl zwischen Multisystem und Multiboot-USB. Beide Tools funktionieren, aber aufgrund der einfacheren Bedienung und der funktional identischen Windows-Variante empfehlen wir Multiboot-USB (aktuelle Version 9.2.0 unter *http://multibootusb.org/page_download/*).

Eventuell finden Sie es auch in den Paketquellen, also im grafischen Softwarecenter, oder als Paketname „python3-multibootusb“ für die Terminalinstallation

```
sudo apt install python3-
  multibootusb
```

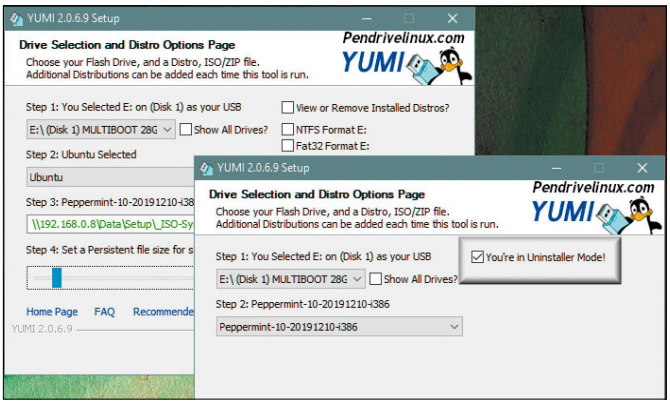
unter Debian, Ubuntu & Co.

Beim eingelegten Stick muss unter „Select USB disk“ die Partition /dev/sd[x]1“ gewählt werden (nicht das Gerät „/dev/sd[x]“), unter „Select image“ und „Browse“ geht es dann von ISO-Image zu ISO-Image, das jeweils mit „Install distro“ (Fenster unten rechts) auf das Laufwerk geschrieben wird. Bei Debian/Ubuntu-Systemen können Sie im Fenster links optional einen persistenten Speicher-



Multiboot-USB macht die Zusammenstellung von bootfähigen Livesystemen einfach. Das Tool läuft mit identischer Bedienung unter Linux und Windows.

bereich festlegen. Wo immer das angeboten wird, sollten Sie das annehmen (aus den bereits unter Punkt 2 genannten Gründen). Die Fortschrittsanzeige hat eine Macke, insofern sie rasch auf 70, 80 oder 99 Prozent wächst, dann aber relativ lange stagniert. Warten Sie in jedem Fall ab, bis das Tool die finale Bestätigung zeigt. Der spätere Bootscreen zeigt alle Livesysteme in der Reihenfolge der Einrichtung. Nicht alle Systeme booten zuverlässig, Debian/Ubuntu-basierte jedoch immer.



Yumi im Installer- (oben) und im Uninstaller-Modus (unten): Das Tool leistet unter Windows ähnliche Arbeit wie Multiboot-USB, ist aber noch einfacher zu bedienen.

4. Yumi: Multiboot-Stick unter Windows

Trotz des genannten Multiboot-USB bleibt unter Windows das englischsprachige Yumi (Your Universal Multiboot Installer) erste Wahl, um mehrere Linux-Livesysteme auf einen USB-Stick zu befördern. Größter Vorzug von Yumi ist die Tatsache, dass dieses Tool unschlagbar einfach in der Benutzung ist – quasi ein Unetbootin mit Wiederholschleife. Yumi liegt auf Heft-DVD (den Download gibt es unter *https://www.pendrivelinux.com/yumi-multiboot-usb-creator/*).

Yumi benötigt unter Windows keine Installation – einfach herunterladen und die ausführbare Datei starten. Die wenigen Schritte sind ähnlich wie bei Unetbootin: Sie wählen in „Step 1" das gewünschte 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 zum Distributionsnamen passen, den 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 beliebige 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 dem Livesystem einen persistenten Speicher und damit begrenzte Anpassungsfähigkeit spendieren können (siehe auch Punkt 2).

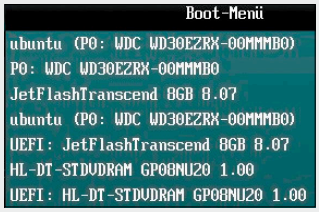
Yumi kann auch noch fehlende ISO-Images aus dem Internet laden. Dazu wählen Sie mit „Step 2" die Distribution und aktivieren dann das Kästchen „Download Link". Nach absolvierter Kopie fragt Yumi jedes Mal automatisch nach: „Would you like to add more ISOs...". Mit „Ja" oder „Yes" können Sie dann nach demselben Strickmuster weitere Systeme aufnehmen, solange der Platz des Datenträgers reicht. Beim Booten des Datenträgers erscheint der Yumi-Bootloader: Der bietet das normale Booten von der Festplatte an sowie unter „Linux Distributions" die eingerichteten Systeme auf USB. Yumi kann auf einem früher erstellten Multiboot-Stick nachträglich Systeme hinzufügen oder entfernen. Beim Erweitern gehen Sie einfach so vor wie oben beschrieben. Sie erhalten 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.

Einschränkungen von Yumi: Yumi kopiert den Inhalt eines ISO-Abbilds auf den Stick

TIPPS FÜR DEN OPTIMALEN USB-STICK

Grundlegende Bootprobleme mit USB-Sticks oder USB-Festplatten, für welche das Rechner-Bios verantwortlich ist, sind sehr unwahrscheinlich, da der USB-Boot seit zwei Jahrzehnten zum PC-Alltag gehört. Jedoch ist es durchaus wahrscheinlich, dass ein Rechner nicht einfach automatisch von einem angeschlossenen Stick startet. Standardmäßig priorisiert das Bios die interne Festplatte sowie DVD-Laufwerke als Boot-Datenträger.

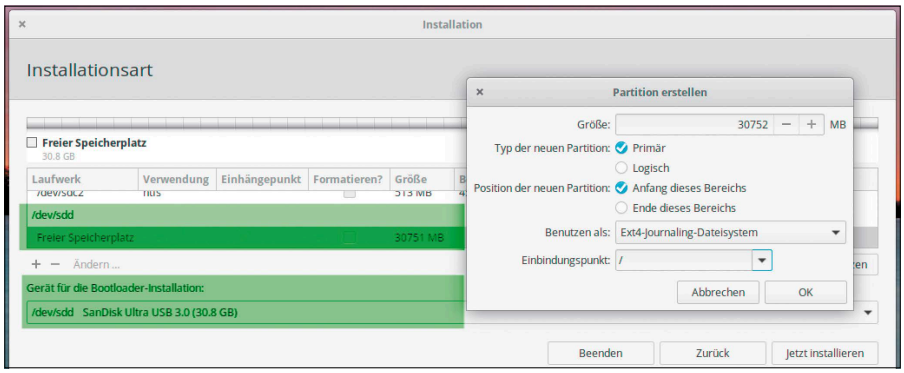
1. Das Bios-Bootmenü: Die Bootreihenfolge lässt sich im Bios-Setup zwar generell umstellen, das ist aber für gelegentliche Starts von Linux-Livesystemen auf USB nicht nötig: Es genügt, das Bootmenü des Bios abzurufen, indem Sie nach dem Einschalten des Geräts frühzeitig eine bestimmte Taste drücken. Das Bootmenü zeigt dann die möglichen Bootquellen an und erlaubt die Auswahl des Sticks. Die Taste für das Bootmenü ist leider nicht standardisiert – oft hilft Esc, F8, F9, seltener F10, F11, F12. Das Bios-Bootmenü zeigt dann alle angeschlossenen Geräte an und Sie können das gewünschte USB-Medium manuell auswählen.



2. Der „saubere" USB-Stick: Ein zweites mögliches Bootproblem entsteht durch USB-Datenträger, die mit Altlasten (Partitionstabelle, Partitionierung) daherkommen und nun mit Livesystemen oder Linux-Installationen ausgestattet werden sollen. Die einschlägigen Tools für das Einrichten von Livesystemen (Unetbootin, Multiboot-USB, Yumi ...) erkennen solche Altlasten in der Regel nicht, kopieren munter und scheitern später beim Bootvorgang. Verwenden Sie am besten einen mit FAT32 oder NTFS formatierten Stick, der vorher unter Linux oder Windows komplett gesäubert wurde. Unter Linux verwenden Sie dafür am besten das Tool Gparted und dessen Menü „Gerät → Partitions-

und erstellt einen Bootloader. Letzteres ist streng genommen nur dann zuverlässig, wenn das System bekannt ist. Yumi lässt daher den Schritt 3 mit der Auswahl der ISO-Datei erst zu, wenn vorher die Distribution ausgewählt wurde.

Beachten Sie, dass Yumi ein angeschlossenes USB-Gerät nur dann als Installationsmedium anbieten, wenn dessen erste Partition erreichbar ist. Unter Windows ist das Medium nicht verfügbar, wenn auf der ersten Partition des Sticks bereits ein Linux vorliegt. Am besten verwenden Sie für den Multiboot-Stick einen leeren und mit FAT32 formatierten USB-Stick.



Reguläre Installation auf USB: Hier wird gerade die Systempartition eingerichtet (später „/dev/sdd1“). Der Bootloader muss ebenfalls auf den USB-Datenträger („/dev/sdd“).

5. (Multiboot-)Installation auf USB

Die genannten Werkzeuge wie Unetbootin, Multiboot-USB oder Yumi schreiben im Handumdrehen eine Linux-Distribution oder eine ganze mobile Sammlung startklar auf USB. Es handelt sich aber ausschließlich um Livesysteme – eingefrorene Systeme, die keine Anpassungen zulassen. Durch Persistenz werden Livesysteme flexibler, Livesysteme bleiben sie aber dennoch. Wer ein uneingeschränktes, individuell eingerichtetes Desktopsystem auf USB-Medium transportieren will, kann jedes Linux ganz regulär auf USB-Stick installieren. Für die Installation benötigen Sie aber erst einmal ein laufendes Livesystem (mit Installer). Der unter Punkt 1 beschriebene Schritt und das gestartete Livesystem sind also Voraussetzung für die reguläre Installation auf USB. Der Installer wird stets die erste interne Festplatte „/dev/sda“ als Ziel vorschlagen. Für die Installation auf ein USB-Gerät müssen Sie daher manuell die richtige Zielpartition festlegen.

Im Ubuntu-Installer wählen Sie dazu im Fenster „Installationsart“ die Option „Etwas Anderes“. Bei anderen Installationsprogrammen lautet der einschlägige Punkt „Manuell“ oder ähnlich. Das Laufwerk muss neu partitioniert und formatiert werden, alle darauf befindliche Daten gehen verloren. Klicken Sie zunächst auf die „-“-Schaltfläche, um vorhandene Partitionen zu entfernen. Erstellen Sie dann auf „Freier Speicherplatz“ mit der „+“-Schaltfläche eine neue primäre Partition mit dem kompletten Speicherplatz (dazu unten mehr) und dem Dateisystem Ext4.

Hinter „Einbindungspunkt“ wählen Sie den Eintrag „/“ aus der Liste. Unter „Gerät für die Bootloader-Installation“ wählen Sie dasselbe USB-Laufwerk aus, auf dem Sie installieren – etwa „/dev/sdb“. Es ist entscheidend, auch den Bootloader auf das USB-Laufwerk zu schreiben (andernfalls startet das System nur auf dem Rechner, mit dem Sie installiert haben).

Multiboot: Wenn der USB-Datenträger groß genug ist, kann auch ein zweites oder drittes System regulär installiert werden. Dies sollten Sie am besten schon bei der Einrichtung des ersten Systems planen: Dann verwenden Sie nämlich bei der Partitionierung des ersten Systems nicht die komplette Größe, sondern nur einen angemessenen Teil. Der verbleibende Rest steht dann bei der Installation eines zweiten Systems als „Freier Speicherplatz“ zur Verfügung und kann dann – wie oben beschrieben – für das nächste Linux partitioniert werden. ■

tabelle erstellen“ und hier den Typ „msdos“. Achten Sie penibel darauf, hierbei das richtige Medium zu adressieren. Unter Windows ist die Datenträgerverwaltung gelegentlich nicht in der Lage, existierende Linux-Partitionen (etwa mit LVM und Luks-Verschlüsselung) zu beseitigen. Was aber praktisch immer hilft, ist eine Eingabeaufforderung mit Administratorrecht und das Tool diskpart. Mit

```
diskpart
list disk
select disk [x]
clean
```

ist der Datenträger bereinigt und kann dann im Explorer frisch formatiert werden. Achten Sie auch hier penibel auf die richtige Kennziffer („x“).

3. Das Dateisystem: Beginnend mit dem einfachen Dateisystem FAT32 kommen alle Tools unter Linux wie Windows problemlos klar. Wenn Sie Linux auf dem USB-Datenträger ordentlich installieren, wird der Installer automatisch nach Ext4 umformatieren. Tools wie Unetbootin werden die bestehende Formatierung hingegen so belassen. Zum Problem kann das nur dann werden, wenn der USB-Datenträger große Dateien (größer vier GB) aufnehmen soll.

Das ist ein Limit für FAT32. Für einfache Abhilfe sorgt eine Formatierung mit NTFS (wenn auch Windows zugreifen soll) oder mit Ext4.

4. Die Kapazität: Livesysteme fordern nicht viel Platz. Selbst mit größeren Kandidaten plus optionalem Persistenzspeicher sind pro System allerhöchstens drei GB belegt. Davon bekommen Sie selbst auf kleineren Sticks eine Handvoll im Multiboot-Betrieb unter.

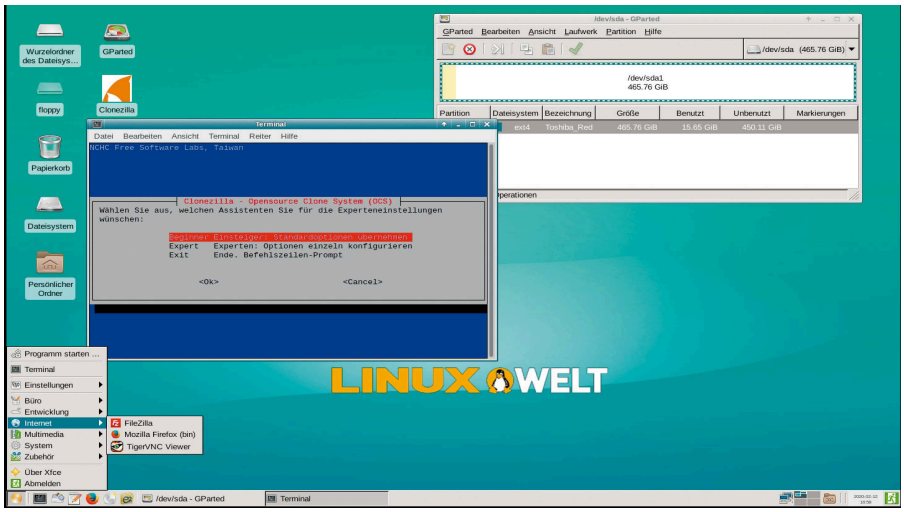
Bei ordnungsgemäßer Installation eines Linux-Systems sollten Sie hingegen mindestens 20 GB pro System einplanen.

Tools & Distris für USB

Linux live auf USB erledigt Reparaturen und Notfallkopien, kann aber auch produktivere Rollen übernehmen: Einem Einsatz als unabhängiges Zweitsystem, als Surfsystem oder als portable Softwaresammlung steht nichts im Wege.

VON HERMANN APFELBÖCK

Der vorherige Beitrag hat die Werkzeuge thematisiert, um eines oder mehrere Livesysteme auf USB zu kopieren oder Linux regulär auf den USB-Datenträger zu installieren. Hier geht es um die inhaltliche Umsetzung dieser Möglichkeiten, also um die geeigneten Linux-Systeme. Unentbehrlich sind Nothelfer und spezialisierte Dienstleister, die hier im Vordergrund stehen. Aber auch unabhängige Surfsysteme und alltagstaugliche Zweitsysteme auf USB sorgen für mehr Sicherheit und Mobilität. Da solche Zweitsysteme eine dienende Rolle haben, steht der Desktop-Glanz hier hintenan.



Topkandidat für USB-Sticks: Die LinuxWelt-Rettungs-DVD hat einschlägige Spezialisten wie Clonezilla oder Gparted an Bord und taugt mit Browser, Filezilla und mehr auch als Zweitsystem.

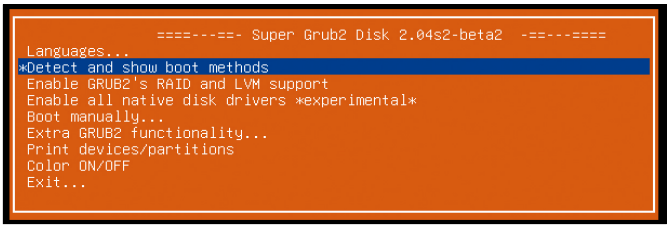
Spezialisierte Livewerkzeuge

Alle unter diesem ersten Punkt vorgestellten Werkzeuge sind reine Livesysteme ohne Installationsoption, die man nur im Notfall ad hoc benutzt. Die zum Teil recht kleinen Tools sind ein Fall für eine Multiboot-Sammlung, die Sie mit Multiboot-USB oder Yumi zusammenstellen.

Super Grub Disk: Der Grub-Bootmanager kann nach fehlerhafter Partitionierung bei der Installation schon mal an falscher Stelle landen, wonach das System nicht booten will. Regelmäßig entsorgt wird Grub auch durch Windows-Installationen. Das ist aber kein ernstes Problem, wenn Super Grub2 Disk zur Hand ist. Mit der Option „Detect and show boot methods“ durchforstet das Hilfsprogramm alle Datenträger nach Systemen, zeigt diese an und startet das ausgewählte System. Die tatsächliche Reparatur der Grub-Umgebung findet dann mit

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

im laufenden System statt. Der unverzichtbare Helfer startet auch von der Heft-DVD (siehe „Extras und Tools“).



Boothilfe nach Windows-Installation: Super Grub2 Disk findet Linux-Systeme auch ohne Bootmanager, zeigt sie anschließend an und startet das gewünschte.

Rescatux: Das neueste Rescatux bietet unter einem ansehnlichen LXQT-Desktop Browser, Dateimanager, Terminal und Zubehör und kann damit auch als allgemeines Notfallsystem dienen.

Im Zentrum steht aber die grafisch organisierte und somit klickbare Script-Sammlung Rescapp. Deren Bedienung ist gruselig, der Nutzwert dennoch unbestritten. Während Super Grub Disk installierte Systeme nur sucht und startet, aber die Bootumgebung nicht repariert, kann Rescatux defekte Grub-Bootloader wiederherstellen. Im Menüpunkt „Grub“ kann die Reparaturoption „Restore Grub“ einen neuen Grub-Bootloader schreiben.

Die Funktion „Update Grub Menus“ greift zur Restaurierung der Bootmenüs auf die Konfigurationsdateien des installierten Linux-Systems zurück.

Für Ubuntu-Systeme ist unter „Expert Tools“ das Werkzeug „Boot-Repair“ vorhanden, das den Bootloader eines Ubuntu-Systems wiederherstellen kann. Nebenbei gibt es auch Windows-Unterstützung: Die betreffende Rubrik enthält Reparatur-Tools für MBR- und Uefi-Umgebungen, zudem eine Option, das Windows-Kennwort „leer“ zu setzen.

Im Bootmenü des Hilfssystems steht eine Version für 64 Bit und für 32 Bit zur Auswahl. Diese muss passend zum installierten System ausgewählt werden.

Hardware Detection Tool: Das winzige HDT ist selbsterklärend, verschafft einen kompletten Überblick zur Hardware eines Computers und befindet sich standardmäßig auf der Heft-DVD unter „Extras und

Tools“. Die IMG-Datei von *http://hdt-project.org* transportieren Sie mit jedem Rohkopierer auf USB, jedoch können die Multiboot-Werkzeuge Multiboot-USB und Yumi nicht damit umgehen. Trotzdem bekommen Sie HDT erfolgreich in eine Multiboot-Sammlung, wenn Sie die funktionsgleiche ISO-Variante Core3 HDT von *www.serverelements.com* verwenden. In Yumi müssen Sie diese unter Schritt 3 als „Unlisted ISO“ klassifizieren und mit der Bootoption „GRUB“ auf USB-Stick kopieren.

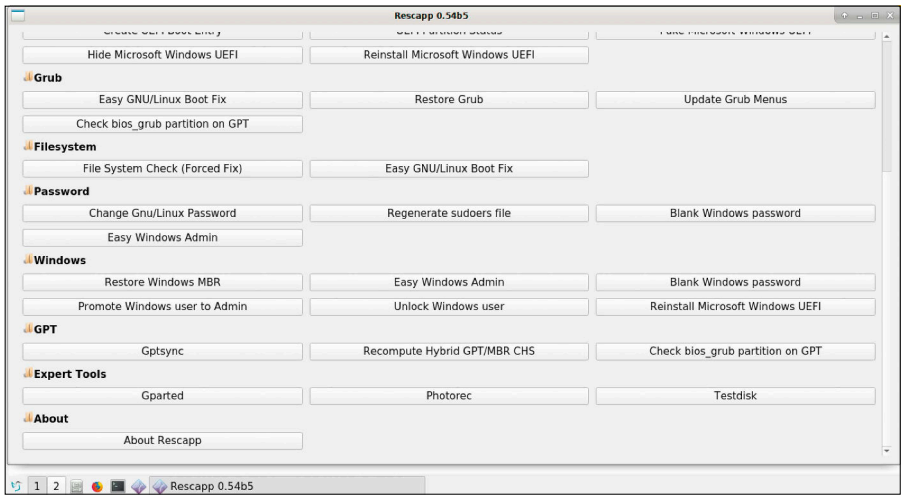
Darik's Boot and Nuke (DBAN): Soll eine alte Festplatte den Besitzer wechseln oder im Elektronikschrott landen, ist DBAN das geeignete Werkzeug. Das winzige Livesystem überschreibt und löscht mechanische Festplatten so, dass sich keine Daten mehr rekonstruieren lassen. Der Anwender kann die Anzahl der Überschreibvorgänge frei bestimmen. Das Tool startet auch von der Heft-DVD (siehe dort „Extras und Tools“).

Gparted Live ist das sehr reduzierte und anspruchslose Livesystem der Gparted-Entwickler, welches das Partitionierungsprogramm Gparted auf jeder Hardware lauffähig macht. Das 32-Bit-System (in Version 1.1.0 auf Heft-DVD) läuft ohne Einschränkungen auch auf 64-Bit-Rechnern. Zwar ist Gparted auf den meisten Linux-Systemen vorinstalliert oder zumindest über den Paketmanager erhältlich, aber in Notsituationen ist Gparted Live die schnelle Alternative, um Festplatten und Partitionen zu löschen, erstellen, vergrößern und verkleinern. Größenänderungen an der Systemfestplatte sind generell nur über ein unabhängiges Livesystem möglich. Das Tool bearbeitet auch NTFS-Datenträger von Windows-Installationen. Neben Gparted bietet das Livesystem kaum Software und nur einen spartanischen Browser. Ein Menü fehlt, alles Verfügbare liegt als Desktopverknüpfung vor.

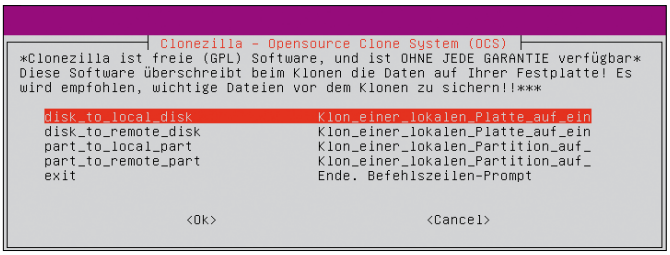
Clonezilla erledigt das Backup und Restore kompletter Datenträger oder Partitionen. Die Images können lokal und auf Netzwerkfreigaben gespeichert werden. Clonezilla beherrscht neben den verbreiteten Linux- und Windows-Dateisystemen auch BTFS, Reiser FS, HFS+, exFAT und spricht alle Netzwerkprotokolle (Samba, SSH, NFS, Webdav). Für Direktkopien von einer Festplatte auf eine zweite wählen Sie im gebooteten Clonezilla „device-device“, danach „Beginner“ und „disk_to_local_disk“. Bestimmen Sie dann die Festplatte, die Sie kopieren möchten. Bei der Systemfestplatte handelt es sich in der Regel um „sda“. Nach „OK“ wählen Sie die Zielfestplatte. Wenn sich nur zwei Festplatten im PC befinden, ist dies „sdb“. Prüfen Sie die Angaben genau, um ja nicht Quelle und Ziel zu verwechseln. Bei startfähigen Festplatten fragt Clonezilla automatisch, ob Sie auch die Startumgebung („boot loader“) kopieren möchten. Bestätigen Sie dies mit „y“ und Eingabetaste.

Zur Sicherung eines Plattenimages wählen Sie wählen Sie die Option „device-image“ und danach „local_dev“. Geben Sie die Festplatte an und danach das Verzeichnis, wohin Sie das Abbild speichern wollen. Wählen Sie „Beginner“ und „savedisk“ und geben Sie einen Dateinamen für das Image an. Die spätere Wiederherstellung eines Abbilds läuft entsprechend ab. Nach „Beginner“ wählen Sie „restoredisk“, danach die Abbilddatei und die Zielfestplatte.

Virenscanner sind eine eigene Kategorie Linux-basierter Notfallsysteme, die es von praktisch allen AV-Herstellern gibt (Avira, Bitdefender, Kaspersky & Co.). Das Livesystem sorgt für einen unkompromittierten Scannerbetrieb. Allen Livesystemen dieser Art ist gemein, dass der Scanner zunächst ein Update der Virendefinitionen über das Internet einfordert. Vorhandene Partitionen werden in der Regel automatisch erkannt und vor dem Scan eingehängt. Ein Livewerkzeug dieser Kategorie empfiehlt sich vor allem für Windows-Anwender, aber auch für Linux-Server, die von Windows-Clients mitgenutzt werden.



Rescatux stammt vom Entwickler der Super Grub Disk. Es repariert – ohne Garantie – defekte Grub-Bootloader sowie auch Windows-Bootumgebungen.



Klonprogramm Clonezilla: Die Textmenüs sind nicht hübsch, aber gut erklärt. Sie arbeiten entweder mit Imagesicherung oder – wie hier – mit Direktkopien zwischen lokalen Datenträgern.

Reparatursysteme für Linux und Windows

Reparatursysteme müssen ihren Job machen und dafür die richtigen Werkzeuge mitbringen. Desktopästhetik und Anpassungsfähigkeit stehen hingegen hinten an, wenn wichtige Dateien vom bootunfähigen Hauptsystem gekratzt werden müssen. Wer es trotzdem halbwegs schick haben will, kann sich das kostenpflichtige (elf US-Dollar) Parted Magic auf USB kopieren. Hingegen kann System Rescue CD gegenüber den nachfolgend beschriebenen redaktionseigenen Livesystemen kaum bestehen. Deren Größen (< 1 GB) legen eigentlich den Einsatz auf einem Multiboot-Stick nahe, jedoch booten die Systeme unter den im vorangehenden Artikel beschriebenen Werkzeugen nicht zuverlässig. Wir empfehlen ihren Soloeinsatz auf kleineren USB-Sticks.



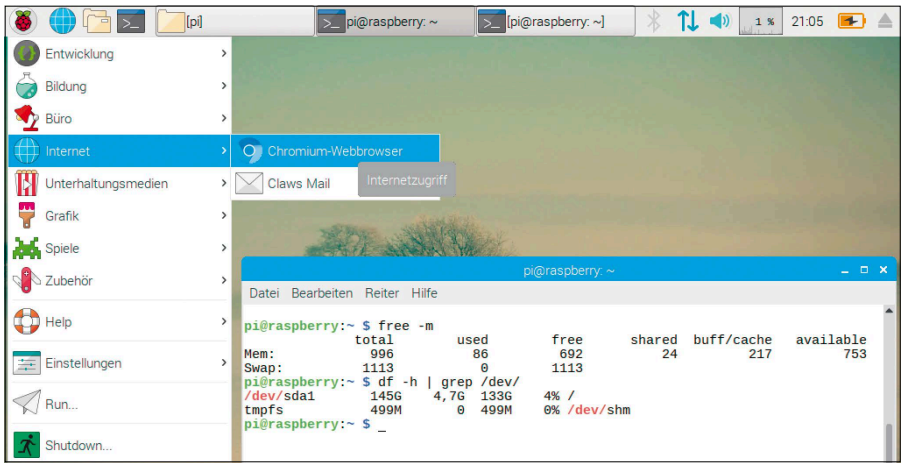
Bootmenü: Wenn Sie das System von einem USB-Stick booten, erscheint dieses Menü.

PC-Welt-Rettungs-DVD: Dieser Nothelfer ist auf Windows-Pannen spezialisiert und enthält Virenscanner, Rettungstools für gelöschte Dateien, Kennwortlöschung, Kopier- und Klonspezialisten, den Gparted-Partitionierer und sogar einen Editor für die Windows-Registry. Auf USB-Stick kopiert, bietet das System ein verschlüsseltes Home-Verzeichnis für mobile Daten. Am einfachsten kopieren Sie aus dem laufenden Notfallsystem auf den Stick (Menü „Zubehör → Installation auf USB-Laufwerk“). Hier wählen Sie den USB-Stick als Ziel, legen die Größe für das verschlüsselte Home-Verzeichnis fest und klicken auf „Installation starten“. Im Prinzip erledigt aber auch jeder Rohkopierer diesen Job.

LinuxWelt-Rettungs-DVD: Dieses Livesystem finden Sie in frisch aktualisierter Version auf der Heft-DVD. Es dient als Werkzeugkasten für Linux-Pannen, kann mit XFCE-Oberfläche, Browser, Gparted, Dateimanager, Terminal, Clonezilla, Filezilla, Brennprogramm aber auch als allgemeines Zweitsystem arbeiten. Für den Transport des ISO-Abbilds („lwRescue707.iso“) auf USB verwenden Sie einen Rohkopierer wie dd, Gnome-Disks oder Win 32 Disk Imager. Im System arbeiten Sie grundsätzlich mit root-Recht. Ein Passwort für den Benutzer „root“ ist nicht gesetzt und Terminalbefehle benötigen kein „sudo“. 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“. Danach binden Sie diese Partition über das Terminal ein (Beispiel):

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

Zu Dateibearbeitung verwenden Sie dann am besten den Dateimanager Thunar, wo Sie die eingehängten Partitionen unter „/mnt“ antreffen. Per Klick auf „Netzwerke durchsuchen“ erhalten Sie Zugriff auf Netzwerkfreigaben, die Sie etwa für die Datensicherung verwenden.



Raspbian x86 als Zweitsystem: Das kleine Debian für den Raspberry ist eine echte Empfehlung für die USB-Installation – schnell, einfach und anspruchslos.

Surf- und Zweitsysteme

Die Gewissheit, trotz streikendem System schnell ins Internet zu kommen, ist heutzutage fast eine Notwendigkeit. Von Minimalisten wie Slitaz (*www.slitaz.org*) Tiny Core (*http://tinycorelinux.net*) oder Puppy Linux (*http://puppylinux.com/*) raten wir eher ab: Auch die bringen Sie zwar ins Web, dies aber weder optisch ansprechend noch technisch genügend.

Peppermint-OS bietet auf Ubuntu-Basis deutlich mehr Internet als nur den Browser: Google Drive, Google Mail, Dropbox sind allesamt vorbildlich integriert. Außerdem setzt die Distribution den XFCE-Desktop auf Diät, um das System gegenüber einem Xubuntu deutlich zu verschlanken. Ungeachtet seines Webfokus lässt sich Peppermint mit weiteren Programmen zu einem Allzweckdesktop erweitern, wenn das System aus dem Livebetrieb auf einen USB-Datenträger installiert wird.

Porteus Desktop sowie das darauf basierende **LinuxWelt-Surfsystem** (auf Heft-DVD) sind auf den schnellen Internetzugang spezialisiert. Porteus arbeitet selbst auf optischen Medien wie der Heft-DVD flott. Ideal ist sein Einsatz aber, wenn es aus dem Livebetrieb über „Systemwerkzeuge → Porteus Installer“ auf USB übertragen wird. 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 ist Porteus deutschsprachig mit deutschem Tastaturlayout. Als Browser stehen Firefox, Chromium und Vivaldi zur Auswahl.

Slax Linux ist ein pures Livesystem und an Reduktion schwer zu überbieten. Es gibt nur Chromium, VLC, Editor, Rechner, Dateimanager und Terminal. Das schmale Angebot ist aber hübsch aufbereitet wie bei einem Smartphone-Homescreen. Für Anwender, die nur Browser und VLC brauchen, ist Slax eine schnelle und attraktive Lösung.

Knoppix wird nur noch in der DVD-Ausgabe gepflegt, die CD-Ausgabe (700 MB) ist veraltet. Das System versteht sich als schlanker Programmstarter für jegliche Open-Source-Prominenz. Folglich finden sich diverse Browser, Mailclients, Dateimanager, Bildviewer und Mediaplayer. Libre Office, Tools, Spiele – alles ist dabei. Das macht Knoppix unübersichtlich bis konzeptlos. Aber wer bei einem Zweitsystem sichergehen will, alles an Bord zu haben, ist mit Knoppix gut versorgt. Das System selbst ist anspruchslos und läuft auf jedem Altrechner.

Kleine Allzwecksysteme auf USB

Für eine mobile Arbeitsumgebung sind Livesysteme kaum geeignet: Die eine oder andere Desktopeinstellung vermisst man auf Dauer schmerzlich und bei der mitgelieferten Software fehlen wesentliche Programme. Eventuell genügt ein Livesystem mit Persistenz, doch auf der sicheren Seite ist man nur mit einem regulär installierten System. Kandidaten wie **Lubuntu, Xubuntu, LXLE, Sparky Linux**, ferner auch die etwas antiquierten **Kanotix, Antix** oder **Bunsenlabs** nehmen sich hinsichtlich Bedienerführung und Ressourcenverbrauch nicht viel. Das sehr schlanke **Trisquel Mini** und das für diese Gewichtsklasse eher anspruchsvolle **Linux Lite** fallen etwas aus

der Reihe. Explizit erwähnen wir hier Kandidaten, die nicht jeder auf dem Zettel hat: **Q4-OS** mit dem Desktop Trinity ist schnell und anspruchslos. Das System startet auf USB-3.0-Stick in 13 Sekunden zum Log-in. Der Desktop Trinity wirkt altbacken, ist aber anpassungsfähig und bietet einen klassischen Desktop mit Dateiablage und einem Menü im Stil alter Windows-Versionen. Die Installation aus dem Livesystem über den Desktop-ink „Install Q4OS" erledigt der Debian-Installer, wobei für die Installation auf USB unter „Festplatten partitionieren" der Eintrag „Manuell" und dann der Zielstick gewählt werden muss. Mit **Raspbian x86** wurde das Raspberry-System auf die PC-Architektur umgeschrieben. Das System startet auf USB-3.0-Stick in 17 Sekunden zum pragmatischen LXDE-Desktop. Die Bedienung ist klassisch und die mitgelieferte Software genügt für produktives Arbeiten. Optisch kann Raspbian locker mit Knoppix oder Lubuntu mithalten.

Bodhi Linux ist Ubuntu-basiert, aber ungleich schneller. Das System 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 Desktop Moksha ist allerdings gewöhnungsbedürftig. Die entscheidende Zentrale 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", über den Sie dann die Oberfläche komplett nach Deutsch umstellen. ■

LINUX AUF USB

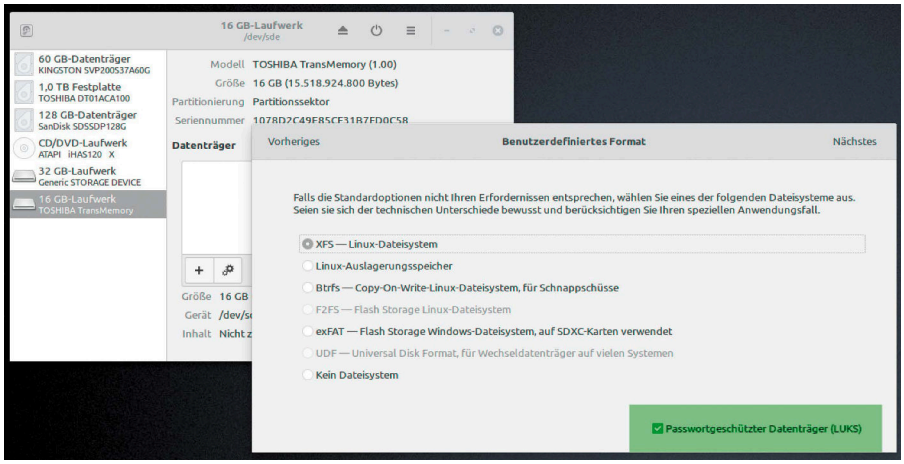
Name	Version	Projekt & Download	Download (MB)	Beschreibung	Installierbar	auf DVD
USB-taugliche Allzwecksysteme						
Antix	19	*https://antixlinux.com*	800	schlankes, pragmatisches Allzwecksystem mit Fokus auf älterer Hardware	ja	–
Bodhi Linux	5.0	*www.bodhilinux.com*	1400	sehr schnell und sparsam, allzwecktauglich, eigenwilliger Moksha-Desktop	ja	–
Bunsenlabs	„Helium"	*www.bunsenlabs.org*	1100	puristisches, schnelles Allzwecksystem, Anpassungen für Fortgeschrittene	ja	-
Kanotix	„Steelfire"	*www.kanotix.org*	1200	anspruchsloses, schnelles, klassisches Allzwecksystem mit LXDE-Desktop	ja	–
Knoppix	8.6.1	*www.knoppix.org*	4400	Livesystem mit einfachem LXDE-Desktop und umfassender Software	ja	–
Linux Lite	4.8	*www.linuxliteos.com*	1400	noch schlankes Allzwecksystem mit XFCE-Desktop (ähnlich Xubuntu)	ja	ja
Lubuntu	18.04.4 LTS	*http://lubuntu.net*	1000	anspruchsloses Allzwecksystem mit LXDE-Desktop	ja	–
Q4-OS	„Centaurus"	*https://q4os.org*	680	sparsames, anpassungsfähiges System mit altmodischer Trinity-Oberfläche	ja	–
Raspbian x86	2020-02-30	*www.raspberrypi.org*	2900	pragmatisches Allzwecksystem (x86-Variante des Raspberry-Desktops)	ja	–
Sparky Linux	5.10.1	*https://sparkylinux.org*	1300	solides, schlankes Allzweck-Debian ohne Spezialisierung	ja	–
Trisquel Mini	8.0	*https://trisquel.info/de*	950	sehr schlankes Ubuntu, „Mini"-Variante benötigt Ausbau der Software	ja	–
Xubuntu	18.04.4 LTS	*http://xubuntu.org*	1400	noch schlankes Allzwecksystem mit XFCE-Desktop und ausreichender Software	ja	–
Surfsysteme						
LinuxWelt-Surfsystem	3.20	–	480	Porteus-basiertes Surfsystem, deutsch lokalisiert plus Browserauswahl	nein	ja
Peppermint-OS	10	*http://peppermintos.com*	1500	Ubuntu-Derivat mit XFCE und Webspezialisierung, aber auch allzwecktauglich	ja	ja
Porteus Desktop	4.0	*http://www.porteus.org*	280	reines Live- und Surfsystem mit Persistenzoption, schnell, klein, ausbaufähig	nein	–
Porteus Kiosk	4.9.0	*http://porteus-kiosk.org*	100	Browser pur, keinerlei Systemzugriff, Einrichtung über Installerimage	nein	–
Slax	9.11.0	*www.slax.org*	270	hübscher Minimalist mit sehr wenig Software (Browser, VLC, Dateimanager)	nein	–
Tails	4.3	*https://tails.boum.org*	1100	Surfsystem mit TOR-Browser für anonymisierten Webzugang	ja	–
Reparatursysteme						
PC-WELT-Rettungs-DVD	6.1	*www.pcwelt.de/1168242*	960	Reparatursystem mit Fokus auf Windows-Nothilfe	nein	–
Parted Magic	2019_12_24	*https://partedmagic.com*	570	schickes und funktionales Reparatursystem, Download für 11 US-Dollar	nein	–
System Rescue CD	6.0.7	*www.system-rescue-cd.org*	690	Reparatursystem mit Fokus auf Linux-Nothilfe	ja	–
LinuxWelt-Rettungs-DVD	7.0.7	*https://goo.gl/aWjaKt*	680	Reparatursystem mit Fokus auf Linux-Nothilfe, auch als Zweitsystem tauglich	nein	ja
Spezialisierte Livewerkzeuge						
Clonezilla	2.6.4-10	*https://clonezilla.org*	280	Klonen von Partitionen und Festplatten in Abbilder oder Disk-to-Disk	nein	–
Darik's Boot & Nuke (DBAN)	2.3.0	*https://goo.gl/khsq2d*	16	löscht mechanische Festplatten nachhaltig	nein	ja
Gparted Live	1.1.0	*http://gparted.org*	340	spartanisches Reparatursystem mit Fokus auf Datenträger und Partitionierung	ja	ja
Hardware Detection Tool (HDT)	0.5.2	*www.serverelements.com*	1	Hardwareanalyse (CPU, RAM, PCI)	nein	ja
Memtest86	5.01	*www.memtest.org*	2	gründlicher Speichertest	nein	ja
Rescatux	0.72-beta7	*www.supergrubdisk.org*	690	diverse Bootreparaturen für Linux und Windows	nein	–
Super Grub Disk	2.04s2	*www.supergrubdisk.org*	15	eng spezialisierter Bootnothelfer, startet Linux/Windows ohne Bootmanager	nein	ja

Sicherer USB-Tresor

Da USB-Sticks oft vergessen oder verloren werden, ist Verschlüsselung für solche Datenträger ein besonders kritisches Thema. Auf sicher verschlüsselten USB-Sticks können Sie auch sensible Daten ohne Bedenken mitnehmen.

VON HERMANN APFELBÖCK

Für verschlüsselte Daten auf USB gibt es zahlreiche Software- und Hardwarelösungen. Diese unterscheiden sich weniger hinsichtlich ihrer Sicherheit, sondern vor allem hinsichtlich Komfort und Plattformunabhängigkeit. Die Notwendigkeit, in eine besonders sichere, aber teure Hardwarelösung wie etwa den Kingston Ironkey zu investieren (ab circa 100 Euro aufwärts), stellt sich für private Nutzung und für Firmennutzung auf unterer und mittlerer Ebene eher nicht. Die hier vorgestellten Varianten konzentrieren sich auf sichere Standardsoftware und einfache Bedienung.



Luks für USB: Diese Verschlüsselungmethode ist für mobile Datenträger optimal, wenn das Medium ausschließlich unter Linux genutzt wird.

Luks-verschlüsselte USB-Medien

Luks (Linux Unified Key Setup) ist eine einbruchssichere Partitionsverschlüsselung. Sie ist ohne Zweifel die einfachste Lösung für USB-Medien, sofern Sie dort keinen Windows-Zugriff benötigen (oder Mac-OS). Ohne Zugangskennwort gestatten Luks-Datenträger keinerlei Einblick in die Verzeichnisstruktur und in die Daten.

Mit Standardzubehör wie Gnome-Disks („Laufwerke“ unter Ubuntu und Linux Mint) oder dem KDE Partition Manager ist die Einrichtung unter Linux denkbar einfach: Sie schließen den USB-Stick an, hängen das Laufwerk mit Gnome-Disks aus und löschen mit dem Laufwerkstool eventuell bestehende Partitionen mit dem Minus-Symbol unterhalb der Partitionsanzeige. Mit dem Plus-Symbol erstellen Sie dann auf dem freien Speicherplatz eine neue Partition mit Größenangabe (im Normalfall die Gesamtgröße). Mit „Nächstes“ geht es zum Folgedialog, wo Sie den „Datenträgernamen“ vergeben und als „Typ“ die Option „Andere“ wählen. Mit „Nächstes“ kommt dann der Dialog mit der Dateisystemwahl, der – abseits der übrigen Optionen – unten rechts das Angebot „Passwortgeschützter Datenträger (Luks)“ anzeigt. Nach zweimaliger Kennwortvergabe ist das Laufwerk präpariert.

Bei späterer Verwendung verlangen Linux-Dateimanager automatisch das Kennwort und mounten den Datenträger nur bei korrekter Eingabe. Wenn Sie dabei nicht am heimischen PC sitzen, ist es ratsam, bei der Passwortabfrage die Option „sofort vergessen“ zu wählen – andernfalls ist der Stick künftig ohne Passwort zu öffnen.

Auf größeren USB-Festplatten lässt sich Luks auch dosieren. Sie können den geschützten Bereich so klein oder groß definieren, wie Sie möchten. Wenn Sie etwa auf einer Zwei-TB-Platte eine Luks-Partition mit 500 GB einrichten, dann eine zweite unverschlüsselte Partition mit den restlichen 1500 GB, dann verhält sich diese zweite Partition unter Linux wie Windows standardmäßig: Beim Anstecken des Datenträgers wird die Partition im Dateimanager geladen. Die Luks-Partition sieht hingegen nur Linux und fragt nach dessen Kennwort. Bei korrekter Eingabe lädt Linux dann auch diese Partition. Die Reihenfolge der Partitionen – Luks-Partition am Anfang oder am Ende – spielt keine Rolle.

Veracrypt-Container für Linux und Windows

Wenn außer Linux auch Windows und Mac-OS Zugriff auf die verschlüsselten USB-Daten haben sollen, ist Luks nicht geeignet. Dann brauchen Sie eine andere Lösung. Wir empfehlen die Software Veracrypt, die für alle drei Plattformen zur Verfügung steht. Das heißt: Mit einem Betriebssystem A (etwa Linux) erstellte verschlüsselte Container lassen sich auch mit dem System B (etwa Windows) lesen und ändern. Die Situation ist aber etwas komplizierter als beim Linux-Standard Luks:

1. Sie sind darauf angewiesen, auf jedem System, wo Sie Veracrypt-Container nutzen wollen, diese Software vorzufinden. Veracrypt-Installationspakete für alle Plattformen gibt es unter *www.veracrypt.fr*. In Ubuntu und Co. ist Veracrypt auch über ein PPA in der aktuellsten Version schnell eingerichtet:

```
sudo add-apt-repository
  ppa:unit193/encryption
```

```
sudo apt update
sudo apt install veracrypt
```

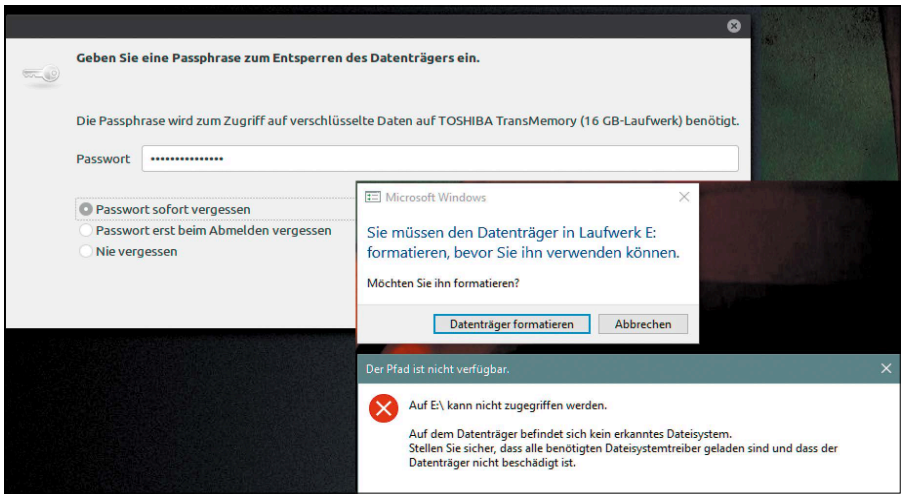
2. Das Dateisystem des USB-Datenträgers muss für alle Betriebssysteme nutzbar sein. Daher kommen bei der Formatierung des USB-Mediums FAT32 und besser NTFS in Betracht. NTFS ist deshalb besser, weil der USB-Stick dann auch Dateien (und Veracrypt-Container) größer als vier GB aufnehmen kann.

3. Beim Anlegen von Verycrypt-Containern müssen Sie beim internen Containerformat erneut darauf achten, ein allgemein kompatibles Dateisystem einzurichten, am besten NTFS. Wir beschreiben in aller Kürze den Vorgang mit Fokus auf diesen Aspekt des Dateisystems:

Sie klicken im Veracrypt-Hauptfenster auf „Create Volume“, dann auf „Create an encrypted file container“ und „Standard VeraCrypt volume“. Hier geben Sie Pfad und Namen einer bisher nicht existierenden Datei auf dem USB-Datenträger an. Unter „Encryption Options“ belassen Sie alles auf den Vorgaben. Die anschließende Angabe der Containergröße sollte großzügig ausfallen, weil die Kapazität nicht mehr zu ändern ist. Nach der Passwortvergabe sind die „Format Options“ für das innere Dateisystem des Containers wichtig: Wählen Sie NTFS, wenn Sie die Daten auch unter Windows brauchen.

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“).

Um später – egal mit welchem Betriebssystem – den verschlüsselten Container zu laden, navigieren Sie im Hauptfenster von Veracrypt mit „Select File“ zur Containerdatei. Mit Klick auf „Mount“ wird diese entschlüsselt im Linux-Dateimanager oder Windows-Explorer geöffnet und der Inhalt kann bearbeitet werden.



Luks-USB unter Linux und Windows: Linux (oben) fragt nach dem Kennwort, Windows (unten) kann mit dem Stick definitiv nichts anfangen.



Dateisysteme: Sollen Veracrypt-Daten unter Linux wie Windows funktionieren, ist ein kompatibles Dateisystem wichtig – einmal für den USB-Datenträger selbst, zum andern für den Container.

Veracrypt-Software auf USB

Die beiden voranstehenden Szenarien sollten für reine Linux-User ebenso ausreichen wie für Linux/Windows-User, die sichere USB-Daten zwischen Bürorechner und privatem PC transportieren.

Wenn man allerdings nicht weiß, auf welchen Rechner man seine Veracrypt-Daten lesen muss, folglich auch nicht weiß, ob dort Veracrypt installiert ist, lässt sich die USB-Ausstattung noch perfektionieren. USB-Stick oder -Platte können sowohl die Linux-Version als auch die Windows-Variante mitbringen.

- Für Windows gibt es eine portable Veracrypt-Variante (auf *https://portableapps.com* oder *www.veracrypt.fr*), die nach Doppelklick der Downloaddatei nur auf den Stick entpackt werden muss.
- Der USB-Stick kann auch die Linux-Version von Veracrypt mitbringen, sofern dort ein Linux regulär installiert und durch Veracrypt ergänzt wird. Der USB-Stick muss für dieses Szenario in zwei Teile partitioniert werden, da Linux seine eigene Ext4-Partition benötigt, während die portable Veracrypt-Software für Windows sowie der Veracrypt-Container auf einer NTFS-Partition liegen müssen. Die konkrete Vorgehensweise sieht wie folgt aus:

1. Sie partitionieren den USB-Datenträger vorab oder während der Linux-Installation in zwei Teile: Dabei setzen Sie die NTFS-Partition an den Anfang des USB-Sticks („/dev/sd[x]1“). Das heißt, Sie beginnen die Partitionierung des Speicherplatzes mit einer primären Partition mit NTFS-Dateisystem. Das verhindert später lästige Windows-Fehlermeldungen über nicht erkannte Partitionen.

2. Sie installieren Linux auf die zweite Partition des Sticks („/dev/sd[x]2“). Versäumen Sie dabei nicht, den Bootmanager auf den Stick zu legen („/dev/sd[x]“).

3. Sie installieren danach auf dem mobilen Linux die Software Veracrypt.

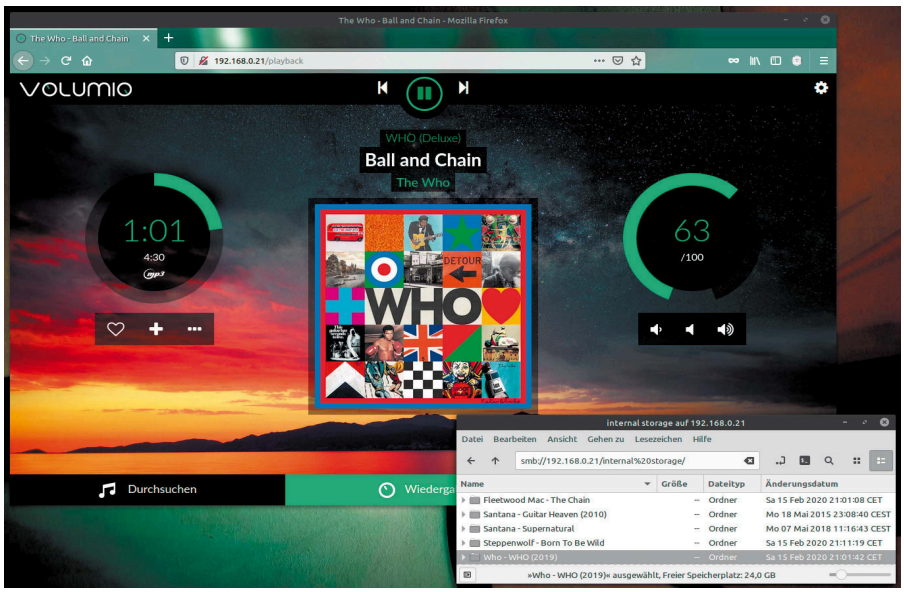
4. Sie kopieren unter Windows das portable Veracrypt auf den Stick.

5. Den verschlüsselten Veracrypt-Container erstellen Sie unter Linux oder Windows auf der NTFS-Partition des Sticks. ■

USB-Ideen: Medien, Systeme & Infos

Da Linux als Livesystem wie auch regulär installiert auf USB-Medien läuft, gibt es keine Denkverbote hinsichtlich Ihrer Mobilausstattung. Dieser Beitrag liefert weitere Ideen und zeigt, dass manche USB-Lösung etwas mehr Planung benötigt.

VON HERMANN APFELBÖCK



Lokale Medien hat Volumio standardmäßig nicht vorgesehen. Die Quelle „INTERNAL“ muss man sich erst schaffen und hat dann die ideale Kombination von Musikarchiv plus System auf USB.

Mobile Soundstation Volumio

Volumio ist eine schicke und einfach zu bedienende Musikstation. Das System ist kein Medienserver, sondern spielt Musik am lokalen Rechner. Allerdings enthält es Serverkomponenten und ist über seinen Webserver von jedem Netzwerkgerät zu steuern (Standardadresse: *http://volumio.local*) und über seinen Samba-Server zu erreichen und zu bestücken (smb://volumio.local).

Das ursprünglich für den Raspberry entwickelte System benötigt keine echte Installation. Sie besuchen die Projektseite *https://volumio.org*, laden dort die PC-Variante „X68/X64“ herunter (komprimierte 650 MB) und übertragen diese Datei mit einem Rohkopierer auf das USB-Medium. Dort entstehen drei Partition mit insgesamt etwa vier GB – eine kleine Bootpartition, die Systempartition und eine zunächst kleine dritte Datenpartition.

Die Ersteinrichtung nach dem ersten Start nehmen Sie am besten am lokalen Rechner vor, kann aber auch bereits im lokalen Netzwerk mit jedem Browser erledigt werden – über die Standardadresse „http://volumio.local“. Beim ersten Start werden einige Standards wie Spracheinstellungen und Rechnername abgefragt. Da der USB-Datenträger im Idealfall neben dem Volumio-System auch die eigentliche Musiksammlung gleich mitbringen sollte, ist hier eine USB-Festplatte die ideale Hardware. Das steht nicht im Widerspruch zur relativ platzsparenden Primärpartitionierung, denn beim ersten Booten wird die dritte Datenpartition automatisch zur Gesamtkapazität erweitert.

Das Problem ist dann nur, diesen Platz für Musikdateien zu nutzen. An der Oberfläche finden Sie nur Optionen, um externe Quellen wie Netzlaufwerke oder andere USB-Medien einzubinden. Hier kommt der Samba-Server von Volumio ins Spiel: Es gibt eine Standardfreigabe „Internal Storage“, die Sie ohne Authentifizierung unter Linux (*smb://volumio.local*) wie Windows (*\\volumio.local*) erreichen. Wenn Sie dort über das Netz einige Musikmedien ablegen, entsteht im Dateisystem auf der Datenpartition der Ordner „/volumio_data/dyn/data/INTERNAL“. Natürlich steht es Ihnen frei, alle Musikmedien via Samba abzulegen. Mit dem Wissen über diesen lokalen Ordner bestücken Sie die Musiksammlung aber vermutlich deutlich schneller, wenn Sie die USB-Festplatte als Datenfestplatte in einem anderen Linux einhängen und dann in den Ordner „/dyn/data/INTERNAL“ kopieren.

Im später wieder laufenden Volumio klicken Sie auf das Zahnradsymbol und dann auf „QUELLEN“, um dann mit „Neu einlesen“ die von außen kopierten Medien in die Musikbibliothek zu integrieren. Die Quelle „INTERNAL“ wird dann beim „Durchsuchen“ (links unten) und „Musikbibliothek“ als auch bei der direkten Titelsuche (rechts oben) angezeigt beziehungsweise berücksichtigt.

Portables Linux unter Windows

Für Windows-Nutzer, die gelegentlich ein Linux-Zweitsystem benötigen (zum Beispiel ein Surfsystem), ist Virtualbox Portable ein besonders attraktives Angebot. Die portable Variante des Virtualisierers kann auf dem

USB-Stick einfach neben dem gewünschten Linux transportiert werden. Damit starten Sie den Virtualisierer auf jedem Windows-System und damit wiederum die Linux-VM. Portable Virtualbox erhalten Sie über einen Installer auf *www.vbox.me*, der aus dem normalen Installationspaket von Virtualbox die portable Variante baut.

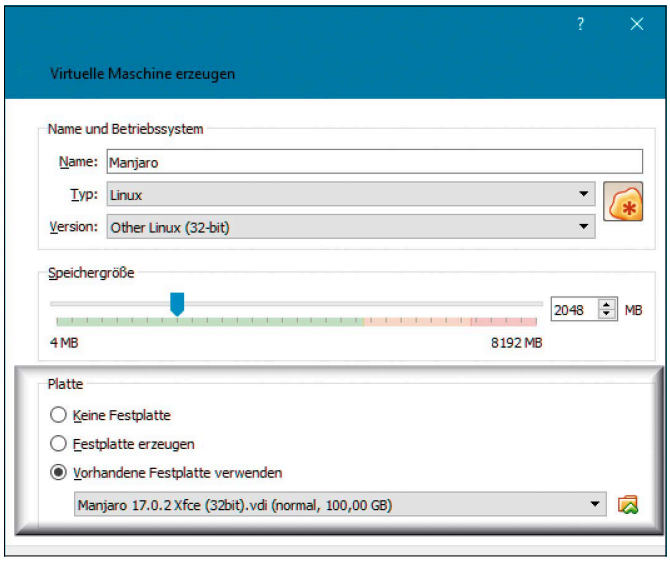
Nach dessen Aufruf klicken Sie auf „Search“ und „german.ini“, um auf Deutsch umzustellen. Danach beziehen Sie über die große Schaltfläche „Installationsdateien von VirtualBox herunterladen“ das Originalpaket. Nach dem Download wählen Sie über die Klickbox des Dialogs zwischen der 32- oder 64-Bit-Version (vorzugsweise 64 Bit). Nach „OK“ entsteht dann der Ordner „Portable-VirtualBox“ mit allen nötigen Komponenten. Diesen können Sie dann auf USB verschieben.

Das portable Virtualbox hat keine Einschränkungen und kann jegliche virtuelle Systeme auf Basis von Linux-ISO-Dateien einrichten. Einfacher ist aber der Rückgriff auf bestehende virtuelle Festplatten, die bereits alles enthalten. Anlaufstelle ist die Webseite *www.osboxes.org*. Über das Dropdown-Feld „VM IMAGES → VirtualBox Images“ kommen Sie zu den passenden VDI-Downloads. Diese sind mit 7-Zip gepackt, daher brauchen Sie diese Freeware unter Windows zum Entpacken (*www.7-zip.de*, auch auf Heft-DVD).

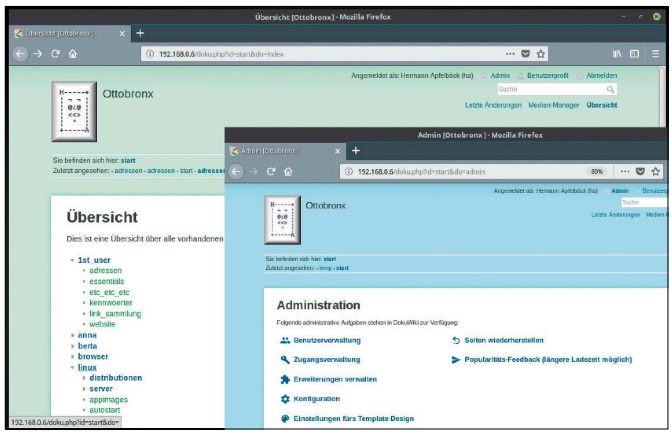
Die resultierende VDI-Datei muss natürlich mit auf den USB-Datenträger, am einfachsten in das Hauptverzeichnis der Virtualbox-Software unter „Portable VirtualBox“. Zum Einrichten eines neuen Systems auf Basis der VDI-Datei starten Sie „Portable-VirtualBox.exe“, klicken auf „Neu“ und geben die Basisdaten ein. Nach der Vergabe der RAM-Größe wählen Sie unter „Platte“ die Option „Vorhandene Festplatte verwenden“ und navigieren zur gewünschten VDI-Datei auf dem USB-Stick.

Das war’s schon: Mit „Starten“ laden Sie das neue virtuelle System. Das Standardkonto aller virtuellen VDIs auf osboxes.org lautet „oxboxes“ mit Kennwort „osboxes.org“. Damit melden Sie sich an. Danach haben Sie alle Möglichkeiten, das Linux-System individuell einzurichten.

Ein kleines Ärgernis sind die Laufwerkskennungen: Wenn ein virtuelles System auf USB-Stick mit der Kennung „E:“ eingerichtet wurde, funktioniert es nicht, wenn der Stick auf dem nächsten Rechner zufällig die Kennung „F:“ oder „G:“ erhält. Für Abhilfe sorgt ein Eintrag in die zugehörige „vbox“-Datei unter „\data\.VirtualBox\Machines\[Name]“, indem man hier die Kennung an die Gegebenheiten anpasst. Noch einfacher ist es, dem USB-Medium grundsätzlich den Buchstaben „A:“ zu verpassen. Das ist in der Windows-Datenträgerverwaltung („diskmgmt.msc“) mit wenigen Klicks erledigt („Laufwerksbuchstaben und -pfade ändern“).



Virtuelle Festplatte auf USB kopieren und dann im portablen Virtualbox einrichten: Auf diesem Weg ist das virtuelle Linux nach wenigen Mausklicks startklar.



Mehr als nur eine Notizensammlung: Ein portables Dokuwiki bietet hierarchische Strukturen, Textauszeichung, Medienintegration und ansprechende Optik.

Das Wiki in der Hosentasche

Wer seine Notizen, Adressen, Infosammlungen in einem Wiki auf Apache- oder Nginx-Basis abruft, bearbeitet und erweitert, kann dieses Wiki natürlich auch auf USB-Stick transportieren. Voraussetzung ist ein ordentlich auf USB installiertes Linux-System mit Apache/Nginx, Wiki-Software und mindestens PHP. Eine Datenbank benötigt das hier empfohlene Dokuwiki (*www.dokuwiki.org*) nicht. Das Dokuwiki ist ein guter Mobilbegleiter, weil Daten und Konfiguration streng getrennt sind und damit der Datenabgleich mit der heimischen Wiki-Installation besonders leicht fällt: Nur das Unterverzeichnis „/data“ enthält die Inhalte enthält und ist mit rsync leicht zu synchronisieren.

Sie können die Inhalte eines Dokuwiki auf USB sogar zusätzlich von Windows-PCs abrufen, da es eine portable Windows-Version des Dokuwiki gibt (siehe *https://download.dokuwiki.org/* und dort links unten „MicroApache“). Um das Wiki sowohl unter dem Linux-System als auch als Windows-App auf einem einzigen USB-Stick zu realisieren, benötigt der Stick allerdings neben der Ext4-Partition mit der Linux-Installation eine zusätzliche Partition mit FAT32 oder NTFS.

Einrichtung und Benutzung des Dokuwiki werden an dieser Stelle nicht erläutert. Eine kleine Anleitung finden Sie im PDF „LinuxWelt XXL“ auf der Heft-DVD unter „Linux als Server → Linux als Infoserver“. ■

Sicher surfen mit Linux

Linux ist sicher, zumindest sicherer als Windows. Davon sind Linux-Nutzer und auch dieses Magazin überzeugt. Tatsächlich ist Linux eine ideale Grundlage für Anwender mit erhöhtem Sicherheitsbedarf, wie die folgenden Tipps zeigen.

VON DAVID WOLSKI



Wie alle dogmatischen Behauptungen ruft auch ein Satz wie „Linux ist sicher(er)“ mit gutem Grund Skeptiker auf den Plan. Linux, so das Gegenargument, sei nicht mehr oder weniger sicher als ein gut gepflegtes Windows 10. Lediglich die geringe Verbreitung bei gleichzeitigem Variantenreichtum von Linux-Distributionen erziele ein gewisses Maß an Sicherheit durch Obskurität. Der Einwand ist nicht ganz falsch, wie das Beispiel Mac-OS zeigt, das in den letzten Monaten verstärkt ins Visier von Schadsoftware geriet, obwohl Mac-OS X als Unix-System ähnliche Grundlagen der System- und Prozesssicherheit besitzt wie Linux. Die Firma Malwarebytes sieht in einer aktuellen Studie Schadsoftware für Macs im Aufschwung.

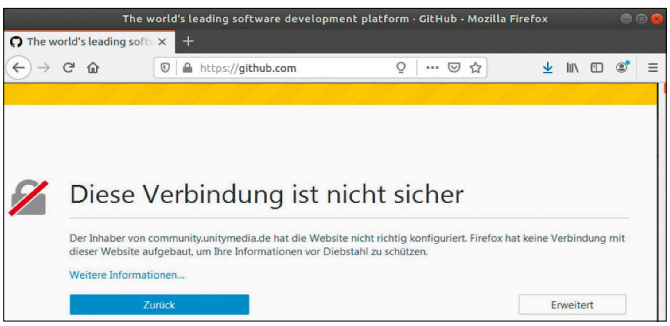
Ein genauerer Blick auf die Ergebnisse zeigt, dass es sich dabei meist um bösartige Browser-Plug-ins handelt, die Anwendern unter Vorspiegelung falscher Tatsachen zur Installation untergeschoben werden. Das zeigt exemplarisch, dass das Nutzungsverhalten einen erheblichen Einfluss darauf hat, wie sicher ein Computersystem im Internet ist.

Dieser Einstieg in die Rubrik „Sicherheit“ zeigt die Grundlagen, wie sich Anwender mit einem Linux-System sicher im Internet bewegen. Aber wir ziehen hier auch einige Tricks für Vielreisende und Außendienstmitarbeiter aus dem Hut, die mit Linux auf dem Notebook und einem kleinen Linux-Gateway in der Firma oder zu Hause deutlich sicherer unterwegs sind, wenig Spuren im öffentlichen Netzwerk hinterlassen oder auf ortsgebundene Streamingdienste zugreifen.

Tabu: unverschlüsselte Protokolle

Das sicherste System, die längsten Passwörter und die stringenteste Konfiguration nützen wenig, wenn Passwörter im Klartext übertragen werden. Es ist ein großes Tabu, im Internet mit unverschlüsselten Anmeldedaten zu arbeiten. Klar, darunter fallen Webseiten aller Art, die eine Anmeldung verlangen.

Es fallen aber auch einige ehemals weit verbreitete Protokolle zur Datenübertragung in dieses Tabu: Die für den Zugriff auf eigene Server eingesetzten Protokolle



Seltsam, eben ging es noch? Bei selbst signierten Zertifikaten ist dieser Warnhinweis harmlos, ansonsten ist Vorsicht geboten, denn der Traffic könnte umgeleitet werden.

HTTP, FTP und Webdav haben alle das gleiche Problem: Die Zugangsdateien für die Anmeldung an Servern werden unverschlüsselt übertragen.

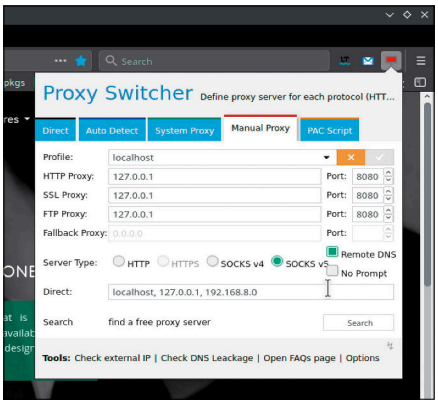
Unterwegs, beim Zugriff auf das heimische Netzwerk über öffentliche WLAN-Verbindungen, ist die Anmeldung über diese Protokolle deshalb tabu. Hüten muss man sich vor der unvermittelten Browsermeldung „Dies ist keine sichere Verbindung (Chrome/Chromium) oder „Dieser Verbindung wird nicht vertraut" (Firefox) bei Webseite, die zuvor noch tadellos funktionierten. Denn dies weist auf ein ungültiges SSL-Zertifikat hin, auf eine Man-in-the-Middle-Attacke oder auf eine Umleitung des Traffics zu einem anderen Webserver.

Getunnelt: SSH als Proxy

Eine SSH-Verbindung zum eigenen Server kann unterwegs auch als Proxyserver dienen, um den Netzwerkverkehr eines Browsers sicher verschlüsselt über den SSH-Server zu Hause zu schicken. Der Browser geht dann über den heimischen Anschluss ins Internet und der eigentliche Verkehr bleibt in unsicheren WLANs verborgen. Dazu verbindet sich der SSH-Client im Terminal mit dem Befehl

```
ssh -ND 8080 [User]@[Hostname]
```

zum gewünschten Server. Danach geht man in die Browsereinstellungen und trägt dort als „SOCKS Host" beziehungsweise „SOCKS Proxy" einfach „localhost" ein und als Port „8080". Ab jetzt gehen die Browser-



Socks-Proxy zum Surfen: Die Erweiterung „Proxy Switcher and Manager" vereinfacht in Firefox, Chrome und Chromium die Konfiguration von Proxyverbindungen.

FRAGEN UND ANTWORTEN

Braucht Linux eine Firewall?

Eine Softwarefirewall ist ein Paketfilter und auch unter Linux sinnvoll, wenn ein Server im Internet erreichbar ist und seine Dienste nach außen anbietet. Auf Desktopsystemen ist dies nicht der Fall. Linux-Distributionen wie Ubuntu oder Mint installieren deshalb keine Firewallregeln mit. Kommt ein Linux-System sowohl als Desktop als auch als Server zum Einsatz, so bieten stringente Regeln für eingehenden Verkehr zusätzliche Sicherheit vor Angriffen und Portscans von außen gegen den eigenen Rechner und auch einen Schutz vor einer fehlerhaften Serverkonfiguration, die versehentlich weitere Ports öffnet.

Braucht Linux einen Virenscanner?

Für ein aktuelles, mit Updates versorgtes Linux-System werden Viren nicht gefährlich, weil es praktisch keine Linux-Viren gibt. Gefährlicher sind Würmer, die sich über Sicherheitslücken von Serverkomponenten fortpflanzen. Zeitige Updates sind das adäquate Mittel dagegen und im Firmenumfeld eine stringentes, überwachtes Patchmanagement. Eine Gefahr ist aber auch die versehentliche Verbreitung von Malware in Netzwerken, die dem Linux-System nichts ausmacht, aber nur darauf wartet, einen Windows-PC zu befallen. Verdächtige Dateien sollten auch Linux-Anwender deshalb zum Check auf den von Google betriebenen Onlinedienst Virustotal hochladen (*https://www.virustotal.com*).

Sind Livesysteme zum Surfen sicherer?

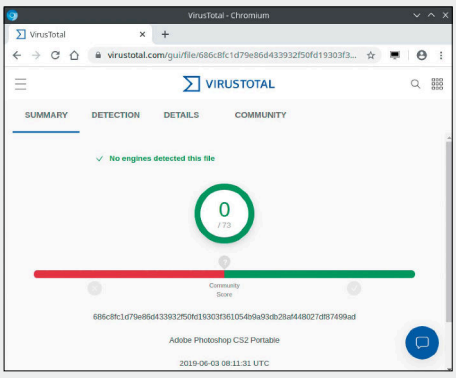
Der Vorteil eines stets frisch von einem unbeschreibbaren Datenträger gestarteten Linux-Systems ist dessen Immunität gegen Manipulationen durch Malware, die eventuelle Browserlücken ausnutzt. Es ist aber auch hier darauf zu achten, möglichst keine veralteten Browser einzusetzen, selbst wenn die Konsequenzen gering wären. Das LinuxWelt-Surfsystem (auf Heft-DVD) aktualisieren wir deshalb immer wieder mit neuen Browsern.

Brauche ich ein VPN zum Surfen?

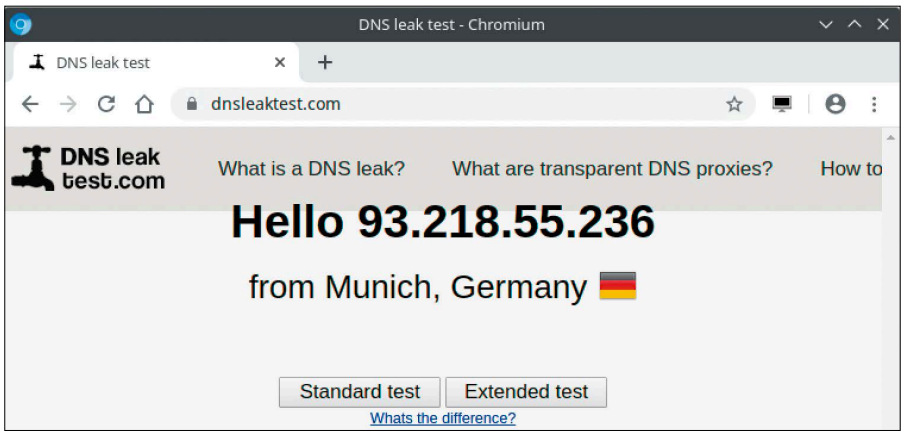
Ein Virtual Private Network ist vor allem für zertifikatsbewehrte, verschlüsselte Zugriffe von außen auf Firmennetzwerke sinnvoll, um von unterwegs aus über eine wenig vertrauenswürdige Internetverbindung in einem LAN teilnehmen zu können. Zum Surfen im öffentlichen Web ist ein VPN keine Lösung mit einem erheblichen Plus an Sicherheit, zumal einige VPN-Anbieter mit Kundendaten nicht sorgsam umgehen oder sogar gehackt wurden. Für den Zugriff auf ortsabhängige Streamingdienste ist ein VPN aber auch beim Surfen nützlich.

Ist das Surfen im TOR-Netzwerk sicherer?

Nicht per se. TOR ist ein Anonymisierungsnetzwerk und erfüllt nicht die gleichen Aufgaben wie ein VPN. Die aufwendige Anonymisierung in TOR über mehrere, wechselnde, vertrauenswürdige Zwischenstationen bedeutet, dass niemand den Netzwerkverkehr und die IP-Adresse von Besuchern zurückverfolgen kann. Von der besuchten Website aus ist nur die IP-Adresse des TOR-Endpunkts (Exit-Node) aus dem TOR-Netzwerk sichtbar. TOR ist allerdings kein Ersatz für durchgängige Verschlüsslung, da die letzte Verbindung von TOR zum Zielserver nicht standardmäßig verschlüsselt ist. Auch gibt es keine Garantie, dass ein unbemerkt kompromittierter Node nicht doch den Netzwerktraffic aufzeichnet. Bei Webseiten, die Benutzeranmeldung und Passwort verlangen, ist deshalb auch bei TOR die Verbindung über HTTPS Pflicht.



Auf Nummer sicher: Damit das Linux-System nicht zur Virenschleuder wird, sollten verdächtige Dateien vor der Weitergabe an Windows-Rechner auf Virustotal überprüft werden.



DNS-Server überprüfen: Die Seite *https://www.dnsleaktest.com* zeigt, welchen DNS-Server der Browser nutzt. Abfragen an lokale DNS-Server verraten dem Netzwerkbetreiber die besuchten URLs.

anfragen per SSH durch den angegebenen Server, der die Webseiten als Proxy abruft und verschlüsselt zurück zum SSH-Client und dann zum Browser schickt. Das Terminalfenster muss dazu geöffnet bleiben.

Socks-Proxy im Browser bequem aktivieren: Es wäre sehr umständlich, die Browsereinstellungen zum Socks-Proxy immer manuell vorzunehmen. Browsererweiterungen helfen dabei, schnell zu einer vorkonfigurierten Proxyverbindung umzuschalten. Für Firefox gibt es dazu den „Proxy Switcher und Manager" als Add-on unter *https://addons.mozilla.org/de/firefox/addon/proxy-switcher-and-manager* und für Chrome/Chromium unter *http://bit.ly/2TnwCqj*. Die Erweiterung platziert ein neues Symbol in der Menüleiste. Einen Socks-Proxy trägt man unter „Manual Proxy" ein und das Symbol färbt sich dann bei aktiver Proxyverbindung rot.

DNS-Leaks vermeiden

Während der Netwerktraffic bei der Nutzung einer VPN- oder SSH-Verbindung zum Surfen verschlüsselt über den Gatewayserver geht, bleiben DNS-Abfragen üblicherweise unverschlüsselt. DNS-Abfragen hinterlassen Spuren im genutzten Netzwerk und erlauben Rückschlüsse, welche Seiten ein Anwender besucht. Die Seite *https://www.dnsleaktest.com* zeigt, welche DNS-Server der Browser nutzt. Sicherer ist es, die DNS-Abfragen ebenfalls über das VPN oder den Socks-Proxy umzuleiten. Der „Proxy Switcher und Manager" bietet dazu in Firefox die Option „Remote DNS" unter „Manual Proxy".

Opensnitch: Anwendungen überwachen

Von Mac-OS X ist das Tool Little Snitch bekannt, das die angeforderten Netzwerkverbindungen von Programmen überwacht. Das grafische Python-Tool Opensnitch überträgt das Konzept auf den Linux-Desktop und erlaubt einen Blick darauf, was Anwendungen ins Netzwerk senden und von dort empfangen.

Das englischsprachige Tool für Fortgeschrittene liegt unter *https://github.com/gustavo-iniguez-goya/opensnitch/releases* auf der Github-Webseite des Entwicklers. Die Installation unter Ubuntu und Linux Mint erfolgt über die angebotenen DEB-Dateien „opensnitch_[Version]_amd64.deb" sowie „python3-opensnitch-[Version]_all.deb", die man in ein leeres Verzeichnis herunterlädt und dort dann im Terminal mit

```
sudo dpkg -i *.deb
sudo apt -f install
```

installiert. Der zweite hier angegebene Befehl löst die weiteren Abhängigkeiten auf und Opensnitch wird noch einige Python-Pakete automatisch nachinstallieren. Auf dem Linux-System startet Opensnitch einen Systemd-Dienst und legt auf dem Desktop ein Symbol im Infobereich ab. Damit starten Sie die Programmoberfläche, die alle Netzwerkverbindungen nach Prozessen aufschlüsselt. Außerdem schlägt Opensnitch immer Alarm, wenn eine Anwendung zum ersten Mal eine Netzwerkverbindung öffnet, und zeigt die Verbindungsdetails an. Die Verbindung kann der Button „Allow connection" erlauben oder mit „Block connection" verbieten.

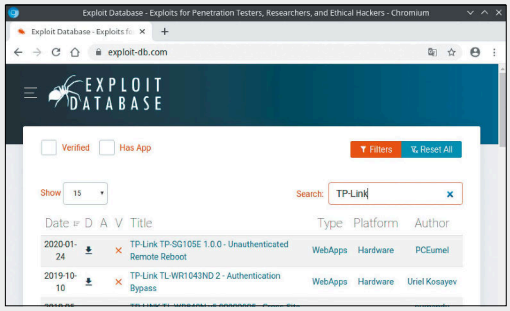
Browser: Aktuell und vertrauenswürdig

Veraltete Browser mit Sicherheitslücken stellen auch unter Linux ein Risiko dar. Linux-Distributionen machen Updates über

ROUTER UND ACCESS POINTS: SCHWACHSTELLE FIRMWARE

Eine oft übersehenes Risiko sind die Router und Access Points selbst, die das WLAN aufspannen oder 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 Geräte Sicherheitslücken, die Einbrüche von außen, von der Internetverbindung aus ermöglichen. Aktuell sind auch Lücken in der Firmware von Cypress- und Broadcom-Chipsätzen bekannt, die ein Belauschen des Netzwerktraffics über eine Schwachstelle in der WPA2-Verschlüsselung erlauben.

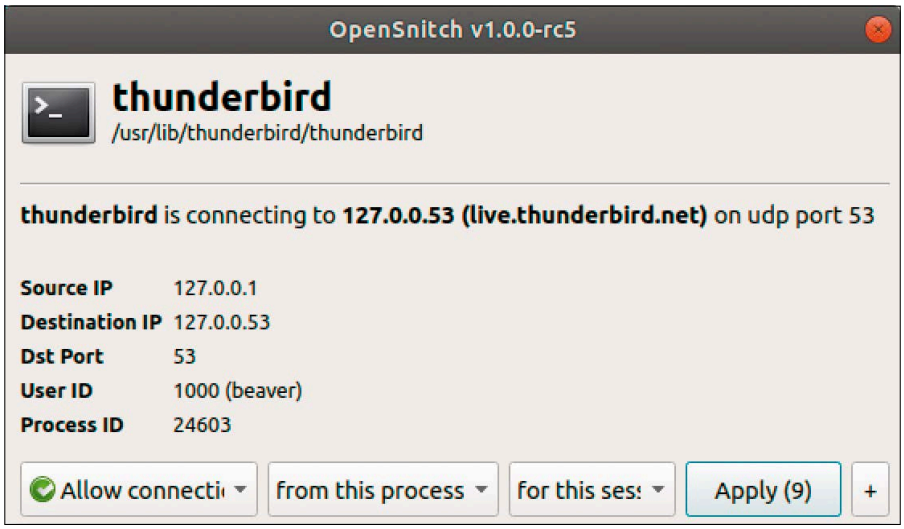
Aufschlussreich ist auch immer eine Suche im Web nach bekannten Lücken. Eine umfangreiche Datenbank bekannter Schwachstellen bietet die englischsprachige Exploit-DB (*https://www.exploit-db.com*). Bei Routern und Access Points mit bekannten Sicherheitslücken, gegen die es kein Firmwareupdate mehr gibt, sollte ernsthaft in Betracht gezogen werden, die Geräte auszumustern.



Firmware-Sicherheitslücken: Die Datenbank auf *www.exploit-db.com* erlaubt eine Volltextsuche nach Sicherheitslücken von Routern und Access Points.

den Paketmanager beziehungsweise die Aktualisierungshinweise auf dem Linux-Desktop zu einer der leichteren Aufgaben, das System aktuell zu halten. Browser sind dabei jene Pakete, die vergleichsweise häufig Updates erhalten, und es empfiehlt sich, solche Updates nicht aufzuschieben. Besonders wichtig ist gerade bei Browsern die Herkunft der Pakete aus vertrauenswürdigen Quellen wie offizielle Repositories von Distributionen.

Neben den verbreiteten Browsern Firefox, Chrome und Chromium gibt es Abspaltungen (Forks), die auch auf Entwicklerwebseiten zum Download bereitstehen. Diese Seiten können nicht als vertrauenswürdig genug gelten, wie der Hack des Archivservers des Palemoon-Projekts im letzten Jahr zeigt. Palemoon ist eine Firefox-Abspaltung mit ansehnlichen Benutzerzahlen. Die Entwickler mussten eingestehen, dass nach dem Hack des Archivservers die dort angebotenen Binärdateien des Palemoon-Browsers Malware enthielten, und zwar schon seit Dezember 2019. Betroffen waren laut Entwicklern nur die Windows-Dateien, aber es hätte auch Linux-Pakete treffen können. Pakete aus offiziellen Quellen sind von der Linux-Distribution dagegen kryptografisch signiert, um eine Manipulation auszuschließen. Generell besteht dieses Risiko auch bei Projekten bei Github und Gitlab, allerdings sind die Sicherheitsstandards dieser Codeverwaltungssysteme von Haus aus hoch. ■



Eingehende und ausgehende Verbindung: Opensnitch ist eine junge Desktopfirewall für Linux, die Programmen den Netzwerkzugriff verweigern kann.

FIREWALL FÜR LINUX IN MEHREREN ROLLEN

Oft dient ein Linux-System als Desktop- oder Entwicklersystem und erfüllt nebenbei im Hintergrund auch noch Serveraufgaben. Mit leistungsfähiger Hardware für wenig Geld ist dies kein Problem, verlangt dann aber einen anderen Ansatz für eine sichere Konfiguration: Es sind Firewalltechniken gefragt, die auf einem purem Desktopsystem nicht nötig wären, da es dort keine Serverdienste zu schützen gilt.

1. SSH-Port absichern: Dieser Punkt ist für die meisten Linux-Systeme relevant, nicht nur für Server im Internet. Denn einen SSH-Server mit Open SSH starten viele fortgeschrittene Anwender auf ihrem Rechner. Ein Schutzmechanismus für den SSH-Port bietet das Tool Sshguard. Es überprüft im Hintergrund Log-in-Versuche und blockt die IP-Adresse dieser Versuche nach einer definierbaren Zahl von fehlgeschlagenen Anmeldungen für zehn Minuten. In Debian/Ubuntu ist das Paket mit

```
sudo apt install sshguard
```

schnell installiert und dann sofort aktiv.

2. Firewallregeln erstellen: Überflüssige Serverdienste mit offenen Ports sollten auf keinem System laufen. Trotzdem kann es vorkommen, dass eine versehentlich installierte oder noch nicht fertig eingerichtete Serverkomponente unerwünscht Ports öffnet. Dagegen hilft der Paketfilter von Linux, der sehr detaillierte Regeln für Netzwerkpakete erlaubt. Debian und Ubuntu machen es mit dem Tool UFW (Uncomplicated Firewall) vergleichsweise einfach, Regeln für den Paketfilter des Linux-Kernels zu erstellen. Mit dem Kommando

```
sudo apt install ufw
```

ist UFW bei Bedarf nachinstalliert. Die Syntax ist einfach gehalten und erstellt im Hintergrund die komplexen iptables-Regeln. Um beispielsweise die Ports 22 (SSH), 80 (HTTP) und 443 (HTTPS) zu erlauben und alles andere zu verbieten, genügen diese drei Befehle:

```
sudo ufw allow 22
sudo ufw allow 80
sudo ufw allow 443
```

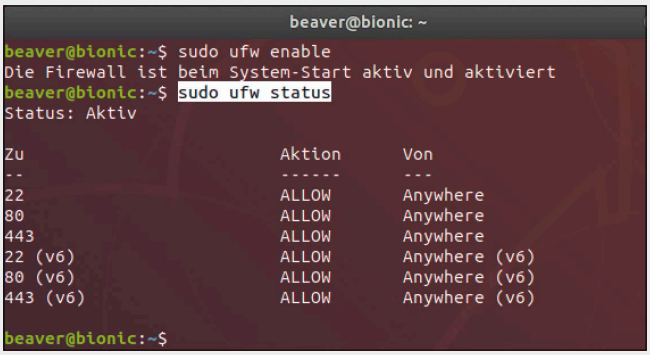
Anschließend wird die Firewall mit

```
sudo ufw enable
```

gestartet. Der Befehl

```
sudo ufw status
```

überprüft die aktuellen Regeln.



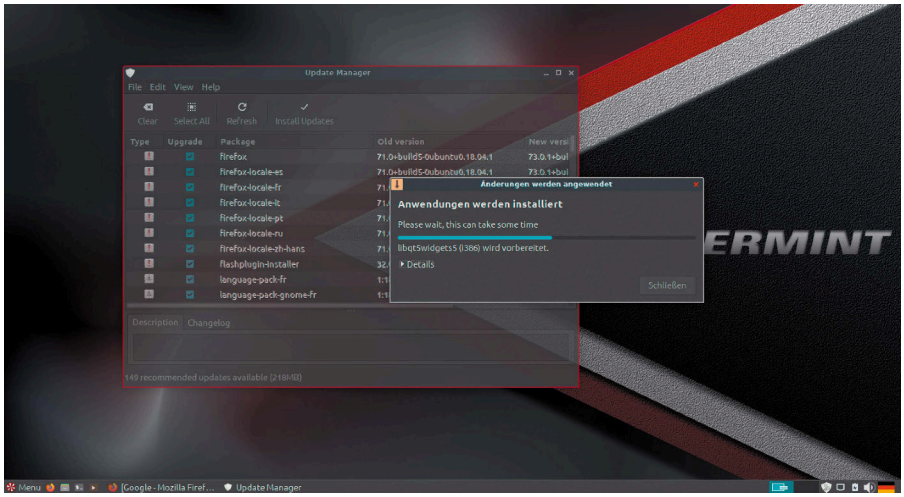
Vereinfachte Firewall für Debian/Ubuntu: UFW (Uncomplicated Firewall) ist ein unkompliziertes Werkzeug zur Definition von Firewallregeln.

Sicher surfen – live oder virtuell!

Linux surft sicher! Noch sicherer wird Linux live oder virtuell. Es gibt für wirklich jeden Anspruch eine maßgeschneiderte Lösung. Wählen Sie aus den hier vorgestellten Szenarien, was sich für Sie am besten eignet.

VON HERMANN APFELBÖCK

Geringe Verbreitung, zahlreiche Varianten, kompetente Nutzer: Linux ist kein lohnendes Angriffsziel für digitale Schädlinge. Livesysteme und Virtualisierung können das Linux-Bollwerk weiter härten – ein Angebot, das auch Windows-Anwender recht komfortabel in den sicheren Linux-Hafen einfahren ließe. Doch fehlen dort oft das Bewusstsein und Know-how, und stattdessen rüstet man lieber seine Abwehrraketen und Quarantänestationen auf. Ein großer Irrweg: Wie leicht es ist, sich praktisch sorgenfrei als Linux- wie als Windows-Nutzer im Web zu bewegen, zeigt dieser Beitrag.



Peppermint-OS – ein Surfsystem für alle Fälle: Diese Distribution mit Webfokus ist virtuell und live (mit Persistenz), unkompliziert zu aktualisieren und taugt damit längerfristig als Zweitsystem.

1. Zweitsysteme zum Surfen auf USB

Egal ob Linux- oder Windows-User – ein unabhängiges Surfsystem ist eine Rückversicherung für den Fall, dass das primäre System ausfällt. Unabhängig vom Pannenfall hilft aber ein Livesystem auch dann, wenn der Internetausflug keine Spuren auf dem Rechner hinterlassen oder das Hauptsystem geschützt werden soll. Für den gelegentlichen Liveeinsatz als Surfsystem eignet sich praktisch jedes schlanke Linux. Anwendern mit Sicherheitsanspruch beim Homebanking oder allgemein beim Surfen kann ein kleines Ubuntu völlig ausreichen (Lubuntu, Xubuntu). Es genügt, das heruntergeladene ISO-Image der gewählten Distribution mit dd, Gnome-Disks oder dem Win 32 Disk Imager auf USB-Stick zu kopieren.

Bei häufiger Nutzung wird ein Livesystem aber nicht alle Wünsche erfüllen. Der Browser bleibt unkonfiguriert, Lesezeichen fehlen und das Mailkonto muss stets neu eingerichtet werden. Für komfortableres Surfen empfiehlt sich daher ein Livesystem, das durch Persistenz zumindest die wichtigsten Anpassungen erlaubt. Die Heft-DVD liefert ein spezialisiertes Surfsystem mit, das solche Anpassungsfähigkeit bietet – es ist der Porteus-Desktop, exklusiv angepasst als „LinuxWelt-Surfsystem“.

2. Peppermint-OS mit Webfokus

Peppermint 10 kombiniert auf Ubuntu-Basis ein ansehnliches XFCE mit einem wilden, aber gelungenen Mix aus XFCE-, Mate- und Mint-Komponenten. Die als Live- und Surfsystem spezialisierte Distribution ist genügsam und auf USB jederzeit flott unterwegs. Der Download des Live- und Installimages von *https://peppermintos.com* beträgt etwa 1,5 GB (32 und 64 Bit). Das heruntergeladene ISO-Image lässt sich leicht auf USB-Sticks und -Festplatten transportieren (siehe unten).

Peppermints Fokus liegt auf der Internet- und Cloudanbindung und bietet mehr als nur den Browser. Google Drive, Google Mail, Microsoft Office Online, Dropbox, Pixlr, Bittorrent sind allesamt vorbildlich integriert. Die Dienste von Microsoft und Google erscheinen wie lokal installierte Anwendungen.

Peppermint auf USB: Verwenden Sie das Tool Unetbootin (auf Heft-DVD) und dessen Persistenzoption mit einer Kapazität von mindestens 1000 MB, um das Peppermint-ISO von auf USB zu kopieren. Danach sind dauerhafte Anpassungen und Nachinstallationen möglich.

Empfehlung: Peppermint ist nicht so schlank und schnell wie Porteus (LinuxWelt-Surfsystem), aber viel unkomplizierter. Die Ubuntu-Basis garantiert ein pflegeleichtes

Surfsystem, das Sie mit Persistenzspeicher leicht erweitern („Anwendungsverwaltung“, apt im Terminal) und längerfristig aktuell halten („Aktualisierungsverwaltung“ oder apt).

3. Porteus: Das LinuxWelt-Surfsystem

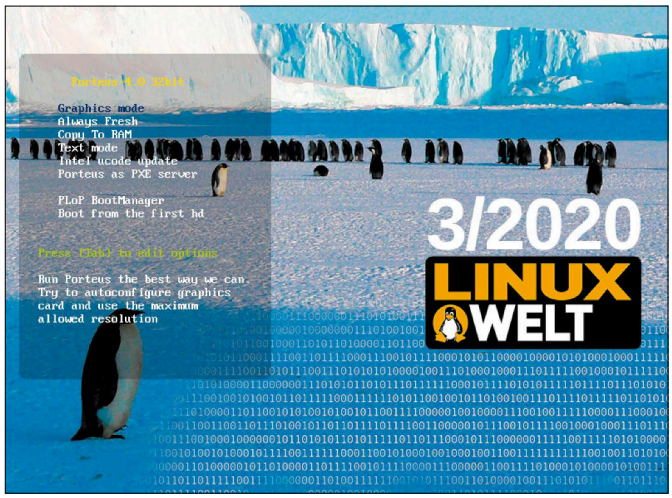
Porteus (*www.porteus.org*) ist das Surfsystem schlechthin. Das Slackwareprojekt ist klein, schnell und anpassungsfähig. Es läuft auch auf älteren PCs mit einem GHz-CPU und einem GB RAM und benötigt ohne laufende Programme kaum 250 MB RAM. Dabei wirkt es überhaupt nicht spartanisch, sondern wie ein komfortables System. In der LinuxWelt-Edition stehen die Browser Firefox und Chromium zur Auswahl. Der Mate-Desktop samt Anwendungen ist deutschsprachig, nur die – allerdings nicht unwichtigen – Porteus-eigenen Tools bleiben in Englisch.

LinuxWelt-Surfsystem auf USB: Bei regelmäßiger Nutzung empfiehlt sich die Übertragung auf USB-Stick. Auf USB 3.x ist Porteus richtig schnell mit Bootzeiten unter 20 Sekunden und Browserstarts von zwei, drei Sekunden. Außerdem eröffnet der USB-Betrieb persistente Anpassungen der Oberfläche oder des Browsers. Porteus läuft auf jedem Dateisystem, auch auf NTFS oder FAT32. Da dies jedoch später zu Persistenzeinschränkungen führt, formatieren Sie den USB-Stick besser vorab mit Ext4 oder auch im laufenden Porteus mit Gparted.

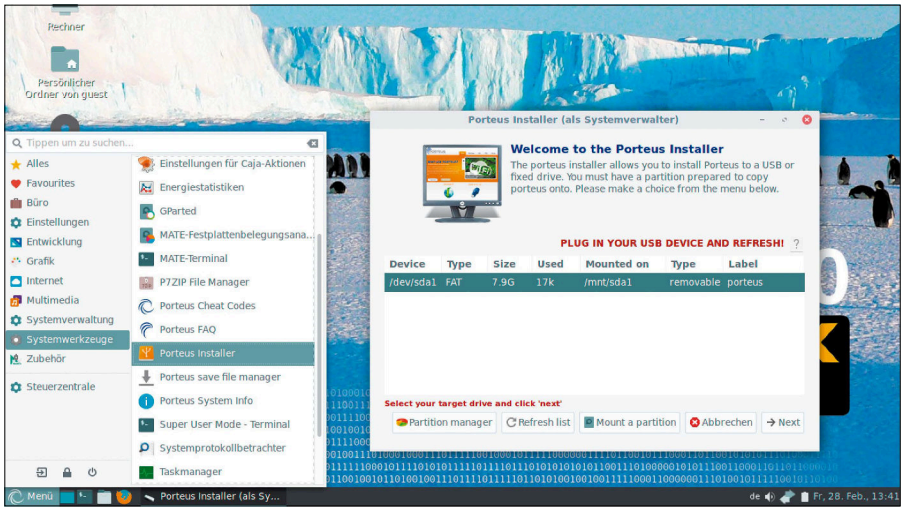
Booten Sie Porteus mit unserer Heft-DVD und wählen Sie im Menü unter „Systemwerkzeuge“ den Eintrag „Porteus Installer“. Dabei wird das root-Kennwort abgefragt („toor“). Unter den angezeigten Partitionen wählen Sie dann den eingelegten USB-Stick und erledigen mit „Next“ und der Option „Install bootloader“ (wichtig!) die Übertragung.

Benutzung und Anpassung: Im Bootmenü von Porteus entscheiden Sie, ob das System im „Graphics mode“ laufen soll oder in den Betriebsarten „Always fresh“ sowie „Copy To RAM“. Die letzten beiden Modi verwerfen alle Systemanpassungen grundsätzlich. Auf USB-Stick ist in der Regel „Graphics mode“ zu empfehlen, denn dann bietet das Livesystem die Option für dauerhafte Änderungen. Erledigen Sie dazu die gewünschten Änderungen wie etwa das Aktivieren der Browsersynchronisierung. Danach gehen Sie unter „Systemverwaltung → Porteus Settings Centre“ 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 angebotenen Optionen wählen Sie „Save to module“ und navigieren bei der nachfolgenden Ordnerauswahl im Dateisystem nach „/mnt/sd[xn]/porteus/base“. Damit speichern Sie ein neues (XZM-)Modul, das Porteus künftig standardmäßig lädt.

Empfehlung: Hinsichtlich Geschwindigkeit, Anspruchslosigkeit und Anpassungsfähigkeit sind Porteus und das LinuxWelt-Surfsystem nicht zu schlagen. Das Slackwaresystem, dessen modulare Technik hier nur angedeutet wurde, ist aber deutlich komplizierter als ein Ubuntu-Derivat.



Start des LinuxWelt-Surfsystems: Sie haben die Wahl zwischen dem unveränderlichen Basissystem („Always Fresh“, „Copy To RAM“) oder einem anpassbarem System (nur auf USB).

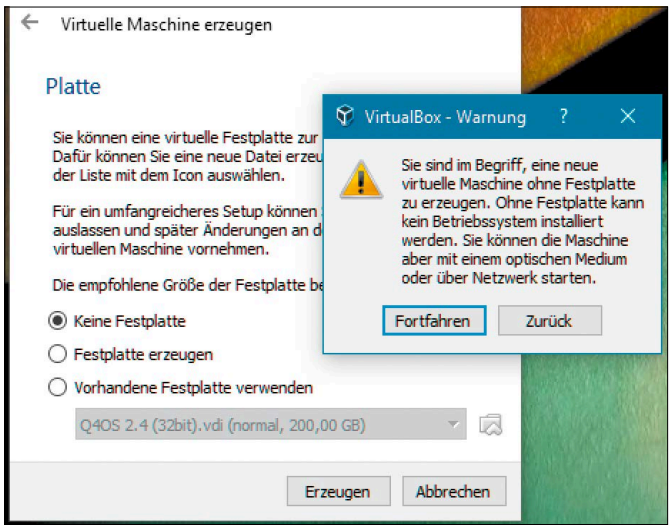


Das LinuxWelt-Surfsystem (Porteus) gehört auf USB-Sticks: Aus dem Livesystem von der Heft-DVD kopieren Sie mit dem Porteus Installer zum Stick.

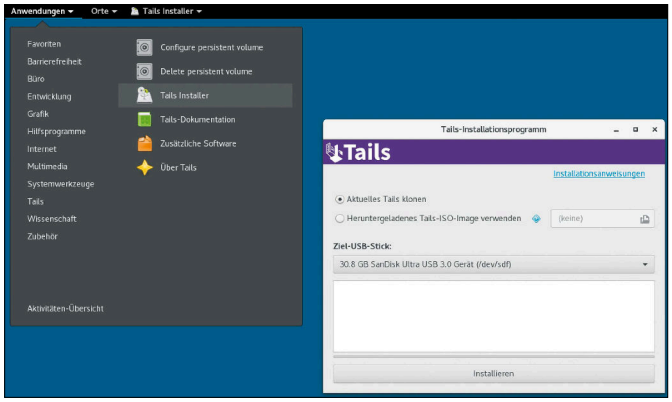
4. Virtuelles Linux unter Windows/Linux

Eine virtuelle Surf-VM mit Linux kann unter Linux wie Windows eingerichtet werden, ist aber eher das klassische Szenario für sicherheitsbewusste Windows-Nutzer. Das Linux-System in der virtuellen Maschine verbindet Sicherheit mit Bedienkomfort: Der Windows-Nutzer muss sein System nicht verlassen und den Austausch von Daten zwischen Windows-Host und Linux-Gast kann man sich so komfortabel wie gewünscht einrichten. Dass Schadprogramme aus dem Linux-Gastsystem ausbrechen, ist extrem unwahrscheinlich. Natürlich müssen aber auch die Grenzen deutlich sein: Ein virenverseuchtes Windows-Programm bleibt auch beim Download in der Linux-VM ein Schädling und behält bei der Weitergabe an das Windows-System sein ganzes Schadpotenzial.

Die Voraussetzungen für ein virtuelles Linux sind für heutige Notebooks oder PCs keine Hürde: Acht GB RAM sind völlig ausreichend, vier GB RAM etwas knapp, aber für Windows plus ein sparsame Linux-VM



Livesystem im Virtualisierer: Dieser einfachste Fall kommt ohne virtuelle Festplatte aus. Sie müssen nur unter „Massenspeicher“ für das optische Laufwerk den Pfad zur ISO-Datei angeben.



Tails mit Persistenz: Über das Livesystem auf einem ersten USB-Stick schreiben Sie mit dem Tails Installer das System auf einen zweiten USB-Stick. Nur so wird Tails anpassungsfähig.

noch so eben ausreichend. Als Prozessor sollte mindestens eine Dualcore-CPU mit zwei GHz vorliegen, die Virtualisierung nativ unterstützt – mit den Techniken Intel VT-X (Virtualization Technology) oder AMD-V (AMD Virtualization). Ob dies zutrifft, kann zum Beispiel das Hardware Detection Tool (auf Heft-DVD, „Extras und Tools“) ermitteln – als CPU-Flag „vmx“ bzw. „svm“. Nicht zuletzt sollten Sie für ein ordentlich installiertes virtuelles Linux einen Plattenplatz von 15 bis 20 GB entbehren können.

Je nachdem, was Sie von Ihrer Surf-VM erwarten, gibt es Varianten mit unterschiedlichem Einrichtungsaufwand.

1. Livesystem als VM: Dazu brauchen Sie das heruntergeladene ISO-Image der gewünschten Distribution. Da es in erster Linie um den Browser geht, genügt jedes schlanke Ubuntu wie etwa Peppermint. In Virtualbox klicken Sie dann auf „Neu“, geben einen Namen an, als Typ „Linux“ und als Version in diesem Beispiel „Ubuntu (64 Bit)“. Als „Speichergröße“ genügen 2048 MB oder weniger. Nach „Weiter“ benötigen Sie bei einem Livesystem unter „Platte“ keine virtuelle Festplatte und wählen „Keine Festplatte“. Der VM müssen Sie dann noch mit „Ändern“ unter „Massenspeicher“ das ISO-Abbild mitteilen. Dies geschieht unter „Controller: IDE“ auf dem CD-Symbol. Aktivieren Sie das Kästchen „Live-CD/DVD“ und klicken Sie auf das CD-Symbol ganz links oben. Hier können Sie als „Datei für optisches Medium“ das ISO-Image des gewünschten Livesystems wählen. Damit ist die Surf-VM startklar.

2. Appliance als VM: Für Virtualbox gibt es zahlreiche sofort lauffähige Linux-Systeme zum Download. Es handelt sich – im Unterschied zu Livesystemen – um vollwertige Installationen, die Sie anschließend beliebig anpassen können. Eine Anlaufstelle für solche virtuellen Festplatten ist *www.osboxes.org*. Nach dem Download einer Virtualbox-VDI starten Sie Virtualbox. Die ersten Schritte nach Klick auf „Neu“ entsprechen dem Vorgehen wie oben („Livesystem als VM“). 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.

Ein weiteres Beispiel für eine VM-Appliance, die sich sogar noch einfacher über die Importfunktion von Virtualbox anlegen lässt, ist das Anonymisierungssystem Whonix (siehe Punkt 6).

3. Reguläre VM-Installation: Hier durchlaufen Sie den Virtualbox-Assistenten und wählen im Dialog „Platte“ die Option „Festplatte erzeugen“, anschließend den Dateityp VDI. Wie oben angesprochen, sollten Sie bei der Größe nicht geizen. Genau wie bei Variante 1 müssen Sie der eingerichteten VM anschließend mit „Ändern“ unter „Massenspeicher“ das ISO-Abbild der Distribution mitteilen. Wenn Sie das virtuelle System danach „Starten“, lädt das Livesystem, mit dem Sie dann auf die virtuelle Festplatte installieren. Wählen Sie eine sparsame, möglichst vertraute Distribution mit komfortablem Installer. Dann fallen das Setup sowie die spätere Systempflege (Aktualisierung, Anpassung) umso leichter. Komfortfunktionen wie eine gemeinsame Zwischenablage von Host- und Gastsystem erfordern die sogenannten „Gasterweiterungen“. Dafür wählen Sie unter Virtualbox das Menü „Geräte → Gasterweiterungen einlegen“. Damit wird ein virtuelles ISO-Image im virtuellen Linux eingehängt und erscheint im Dateimanager als CD-Medium unter „Geräte“. Dort starten Sie dann das Script „VboxLinuxAdditions.run“. Der Dateiaustausch zwischen Host und Gast kann über das Virtualbox-Angebot „Gemeinsame Ordner“ organisiert werden. Oft genügt aber auch eine Samba-Freigabe im lokalen Netzwerk oder ein USB-Medium, das Virtualbox über „Geräte → USB“ für die VM bereitstellen kann.

5. Tails: Anonym im Internet

Tails (*https://tails.boum.org*) liefert ein Komplettpaket zum Surfen, das auf der benutzten Hardware keinerlei Spuren hinterlässt und im Web keine persönlichen Spuren. Damit ist das Debian-System „out of the box“ eine Anonymisierungswaffe. Tails bietet automatischen Zugang zum anonymisierenden TOR-Netzwerk. Der TOR-Browser schickt Webanfragen verschlüsselt durch drei zufällige Stationen des TOR-Netzwerks.

Der Zielserver erfährt folglich nur die IP-Adresse des letzten TOR-Knotens, aber nicht diejenige des Rechners, von dem die Anfrage ursprünglich stammt. Solche Anonymisierung funktioniert im gesamten öffentlichen Internet, für das Darknet und dessen Sites (*.onion) ist der TOR-Browser die technische Voraussetzung.

Tails auf USB: Das Tails-Image sollte auf USB kopiert werden (unter Virtualbox läuft das System zäh). Die Projektseite *https://tails.boum.org* betreibt relativ viel Umstand um die Installation, tatsächlich genügen aber der Download des ISO-Abbilds und die Rohkopie auf USB-Stick – mit dd oder Gnome-Disks unter Linux oder mit dem Win 32 Disk Imager unter Windows. Damit ist Tails als pures Livesystem bereits einsatzbereit. Wer die Option des persistenten Speichers nutzen will, muss Tails aus dem Livesystem über „Tails → Tails Installer → Aktuelles Tails klonen“ nochmal auf einen zweiten und endgültigen USB-Stick weitertransportieren. Die Einrichtung der Persistenz erfolgt dann über das Menü „Tails → Configure persistent volume“. Persistenz macht dauerhafte Softwarenachinstallationen möglich („Install Every Time“ wählen!), auch das dauerhafte Anlegen von Browserlesezeichen gelingt. Wer Tails oder ähnliche TOR-Systeme benutzt, muss jedoch Nachteile in Kauf nehmen:

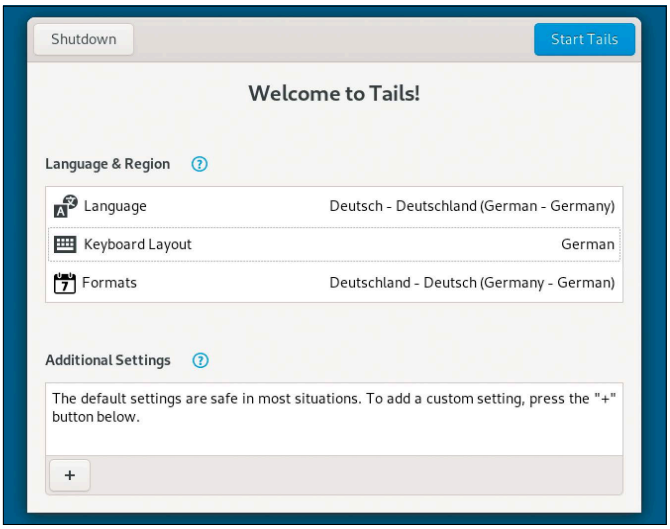
- Das TOR-Netzwerk ist langsam. Statt zweier Sendungen (Anfrage und Antwort) handelt es sich hier um insgesamt acht Sendungen über eventuell langsame Zwischenknoten.
- Personalisierte Aktionen sind zu meiden. So wird etwa Google eine Anmeldung sofort als Fremdzugriff von einem unbekannten Gerät monieren und das Konto eventuell sperren.
- Benutzern, die nur der penetranten Werbeverfolgung entrinnen möchten, muss klar sein, dass sie sich im TOR-Netzwerk in Nachbarschaft zum Darknet und inmitten einer überwiegend kriminellen Gesellschaft bewegen. Wie viele TOR-Knoten inzwischen von Geheimdiensten und Polizei betrieben werden, weiß niemand.

6. Whonix: Virtueller Anonymisierer

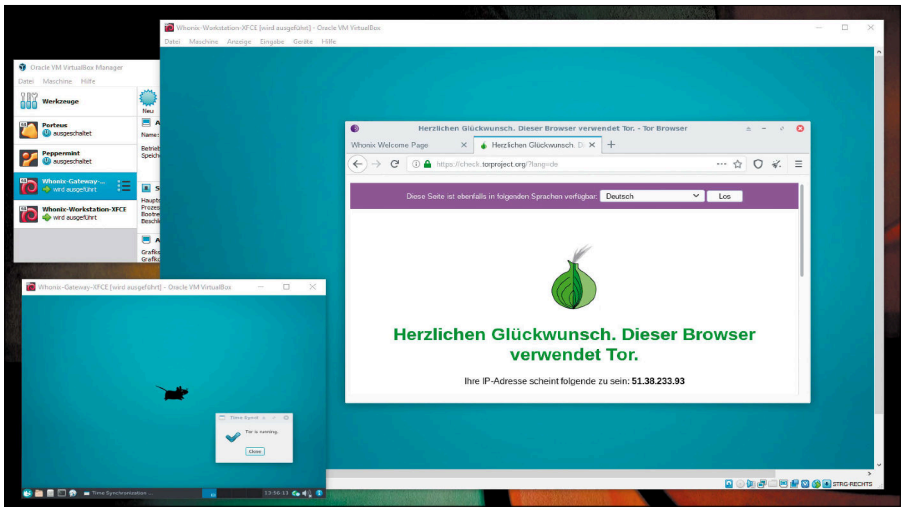
Die Linux-Distribution Whonix (*www.whonix.org*) ist mit Tails vergleichbar: Im Zentrum steht auch hier die anonymisierte Internetnutzung über das TOR-Netzwerk. Ein erster Unterschied besteht darin, dass Whonix als Virtualbox-Appliance auf den virtualisierten Einsatz spezialisiert ist, während Tails den Liveeinsatz auf USB bevorzugt. Der technische Ansatz von Whonix geht jedoch ein ganzes Stück weiter als Tails. Whonix besteht nämlich aus zwei getrennten Betriebssystemen: Im „Whonix-Gateway“ läuft die TOR-Instanz, die den Datenverkehr über das TOR-Netz abwickelt. Das zweite System (Whonix-Workstation) kann nur über das Whonix-Gateway ins Internet und enthält die Anwendungen (Browser, Mail mit PGP-Verschlüsselung). Was eigentlich zwei getrennte Rechner benötigt, kann durch Virtualisierung auf einem PC unter Virtualbox realisiert werden.

Beide Whonix-Systeme wurden 2019 in einer Appliance zusammengefasst, was die Installation deutlich vereinfacht: Unter *www.whonix.org/wiki/Download* klicken Sie hinter „Linux“ auf den Link „VirtualBox“. Der Download dieser OVA-Datei enthält beide VMs, die Sie unter Virtualbox mit „Datei → Appliance importieren“ einrichten. Danach erscheinen in Virtualbox zwei neue VMs, wovon Sie immer erst das Gateway, danach die Workstation starten. Die getrennten Systeme sollen sicherstellen, dass selbst ein gehackter Browser der Workstation die öffentliche IP-Adresse (und damit Lokalität und Person) nicht preisgeben kann, da er sie selbst nicht kennt.

Das Konstrukt mit zwei VMs unter Virtualbox erscheint aufwendig, läuft aber auf jedem durchschnittlichen Rechner mühelos. Für Nachinstallationen und Konfigurationsänderungen verwenden Sie das Standardkonto „user“ mit sudo-Recht und Kennwort „changeme“. ■



Startdialog in Tails: Sprachauswahl und Tastaturbelegung sind bei jedem Systemstart zu absolvieren – auch auf USB und Persistenzspeicher.



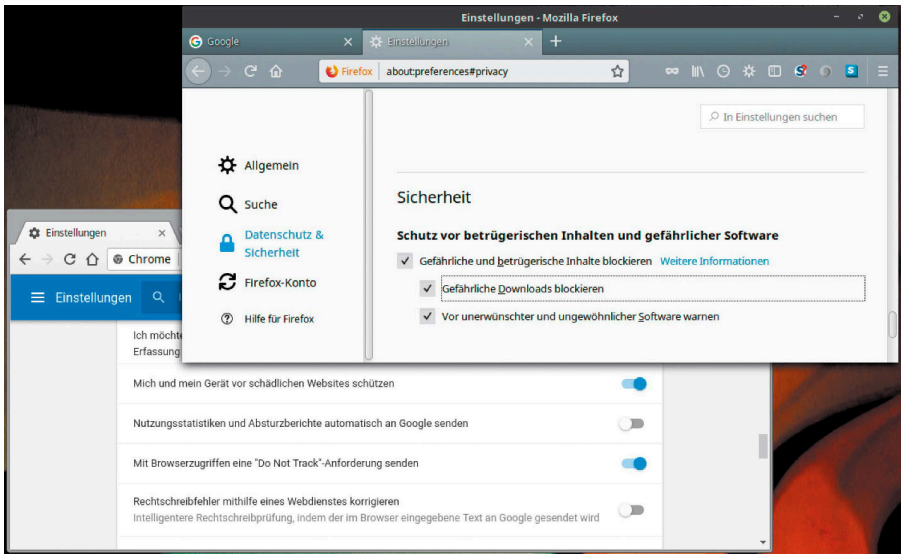
Whonix im anonymen TOR-Netz: Whonix besteht aus zwei VMs. Der komplexe Aufbau ist erstaunlich leichtfüßig und bietet – zumindest theoretisch – ein Sicherheitsplus gegenüber Tails.

Sichere Browser

Die Sicherheitstechniken der Webbrowser werden immer besser. Aber kein Chrome oder Firefox kennt alle Minenfelder des Internets und jedes Fehlverhalten des Benutzers. Unsere „Fragen und Antworten“ zur Browsersicherheit sollen vor allem sensibilisieren.

VON HERMANN APFELBÖCK

Browser haben Sicherheitslücken, Hacker sind einfallsreich und Benutzer machen Fehler. Sicherheit im Internet wird immer relativ bleiben – man kann sie graduell optimieren, mehr aber auch nicht. Was auf der Seite des Browsers wirklich wichtig ist, lesen Sie auf folgenden Seiten. Die wichtigste Maßnahme haben Sie als LinuxWelt-Leser aber bereits erledigt: Sie benutzen Linux und damit das virenresistenteste Betriebssystem.



Sicherheit und Datenschutz in Firefox und Chrome: Die Browsereinstellungen ähneln sich äußerlich und technisch (Safe Browsing API) bis in die Details.

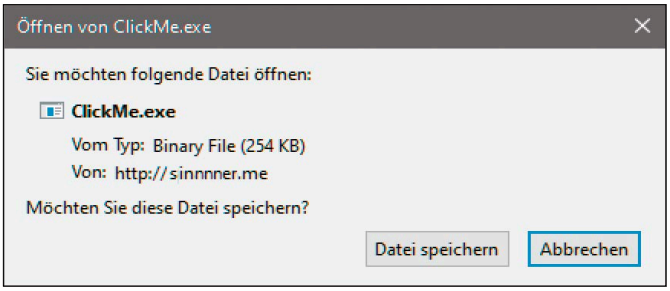
Der sicherste Browser

Chrome/Chromium und Firefox sind die Standardbrowser unter Linux. Daneben gibt es eine ganze Reihe weiterer Browser. Welcher ist der beste Kandidat, wenn man das Kriterium Sicherheit an erste Stelle setzt?

Die Anzahl der verfügbaren Browser schrumpft sofort erheblich, wenn man auf den Unterbau sieht: Browser wie Vivaldi, Opera, Midori sowie spezielle „Sicherheitsbrowser“ vor allem für Windows (Avast Secure, Avira Scout, Commodo Dragon, Epic, TOR) verwenden unter der Haube allesamt einen Chromium oder Firefox (einzige Ausnahme der spartanische Midori). Selbst Microsoft baut Edge inzwischen auf Basis von Chromium. „Sicherheitsbrowser“ erhalten höhere Sicherheit daher nicht von der Basis her, sondern nur durch Browsererweiterungen, durch Virtualisierung oder durch ein Linux-Livesystem. Die Frage nach dem sichersten Browser reduziert sich letztlich auf eine Entscheidung zwischen Firefox und Chrome.

Chrome/Chromium: Nach Ausweis gemeldeter Sicherheitslücken ist Chrome sicherheitstechnisch spitze – mit den wenigsten Lücken 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 → Datenschutz und Sicherheit → Synchronisierung und Google-Dienste“ als „Mich und mein Gerät vor schädlichen Websites schützen“. Sie ist standardmäßig aktiv, blockiert den Zugang auf gefährliche Sites und warnt vor viralen Downloads. Chrome hat zusätzlich eine relativ simple Heuristik, die vor „ungewöhnlichen“ Downloads warnt. Die Kriterien für diese Heuristik sind allerdings nicht offengelegt (Name, Hashwert, Größe, Herkunft des Downloads?). Über die interne Chrome-URL *chrome://flags/* lässt sich die zusätzliche Sicherheitsoption „Strict-Origin-Isolation“ aktivieren. Diese lädt jede Website als separaten Prozess, was zwar den Speicherbedarf erhöht, aber den Datenzugriff über Sitegrenzen hinweg unterbindet.

Firefox: Auch Firefox benutzt die Safe Browsing API von Google Chrome und damit eine Blacklist schädlicher Websites. Die einschlägigen Optionen zeigt der Browser unter „Einstellungen → Datenschutz & Sicherheit“ ganz unten unter „Schutz vor be-



Schädliche Downloads: Firefox warnt nicht vor Downloads, wenn die betreffende Website bislang nicht als bösartig gemeldet wurde.

trügerischen Inhalten…“. Hier sollten alle drei Kästchen aktiviert sein, um gefährliche Webseiten und Downloads zu blockieren. Dieser Grundschutz wird auf Basis einer Blacklist alle 30 Minuten aktualisiert. Eine weitergehende Heuristik wie Chrome besitzt Firefox nicht. Das heißt: Firefox blockiert zwar Downloads von bekannten betrügerischen Seiten, lässt aber einen Virendownload von einer bisher unbescholtenen Webseite ohne Kommentar zu.

Sicherheit versus Datenschutz

„Sicher surfen“ will jeder, doch versteht darunter nicht jeder dasselbe: Die zwei völlig verschiedenen Aspekte der Systemsicherheit und des Datenschutzes werden dabei gerne vermengt. Was bedeutet „Sicher surfen“ eigentlich?

Im engeren Sinn heißt „Sicheres Surfen“, dass das System technisch vor Schadsoftware geschützt ist und nicht durch Schädlinge übernommen werden kann. Mit Datenschutz, informationeller Selbstbestimmung und Abwehr von Werbetracking hat dies nichts zu tun.

Der technische Schutz vor Schadsoftware hat eindeutig Priorität vor dem Datenschutz, zumal ein gekapertes System auch alle persönlichen Daten freilegt – und dies nicht für Google und Werbeindustrie, sondern für kriminelle Hacker.

Voraussetzungen für (relative) Sicherheit

Welchen technischen Schutz bieten Browser gegen die Schädlinge im Internet und wie kann der Nutzer diesen Schutz verbessern?

Angesichts von Abermillionen Websites, unvermeidlichen Sicherheitslücken und zunehmend dynamischen Webinhalten mit zahlreichen Script-Aktivitäten kann die Browsertechnik nur eindämmend wirken. Folgende Maßnahmen sorgen für relativ sicheres Surfen – mit den genannten Einschränkungen:

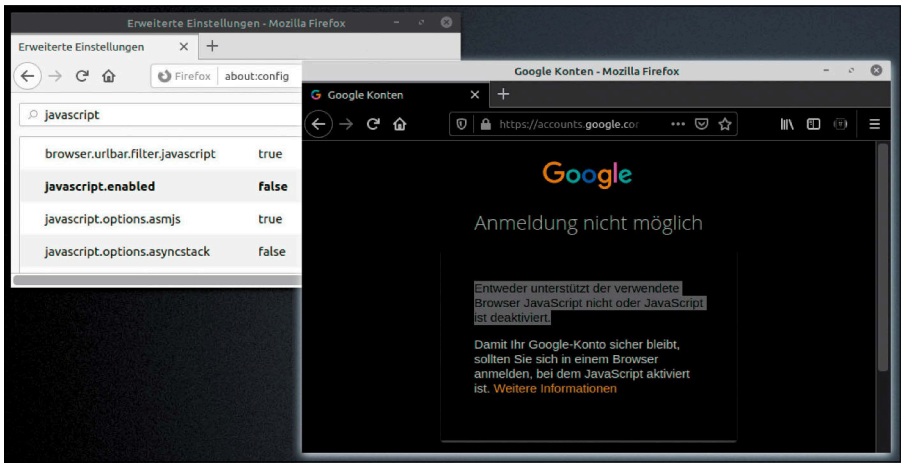
• Durch die Sandboxtechnik aller modernen Browser werden die Webinhalte zumindest theoretisch vom Betriebssystem abgeschottet.

• Um bekannt gewordene Sicherheitslücken zeitnah zu schließen, wird der Browser ständig aktualisiert. Dafür sorgen Chrome und Firefox durch interne Updatedienste automatisch. Der Nutzer sollte dem Updateangebot aber möglichst immer ohne Aufschub folgen. Vor bislang unbekannten Lücken schützen die Updates nicht.

•Browser wie Chrome und Firefox kennen schädliche Websites und warnen den Nutzer vor dem Zutritt. Solche Blacklists können allerdings niemals vollständig sein.

• Browser wie Chrome und Firefox warnen vor bekannten schädlichen Downloads. Auch dieser Schutz kann niemals umfassend und lückenlos gelten.

• Script-Aktivitäten im Web lassen sich theoretisch abschalten (Firefox, „about:config“, „javascript.enabled“ oder Chrome, „Einstellungen → Erweitert → Datenschutz und Sicherheit → Website-Einstellungen → JavaScript“). Das ist aber kaum praktikabel, da es dann Fehlermeldungen hagelt. Ein nicht bequemer, aber gangbarer Kompromiss ist das Add-on Noscript (siehe unten).



Das Web ohne Javascript: Sicherer wäre das, praktikabel allerdings nicht. Ein auch nicht ganz bequemer Kompromiss ist das Add-on Noscript.

Das Add-on Noscript

Welche Maßnahmen bieten besonders sicherheitsbewussten Anwendern den größten Schutz?

Surfen mit Chrome oder Firefox unter Linux – und noch sicherer unter einem Linux-Livesystem – bietet per se maximalen Schutz, da die Schädlinge primär auf Windows zielen. Wer dennoch über alle Script-Aktivitäten im Web die volle Kontrolle haben will, kann das Add-on Noscript einbauen (für Chrome und Firefox). Das Add-on blockiert Javascript, Java und andere ausführbare Inhalte. Damit ist Noscript der Schädlingsstop schlechthin, aber zweifellos unbequem, weil fast jede Webseite Script-Code verwendet.

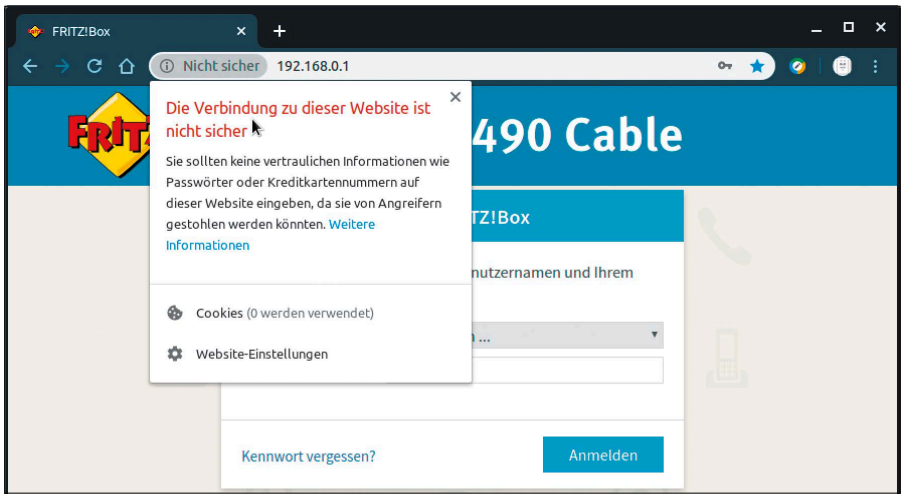
Immerhin landen einmal erlaubte Sites in der Whitelist des Tools und müssen später nicht mehr bestätigt werden, aber zunächst müssen Sie auf vielen interaktiven Seiten die Scripts manuell erlauben. Dies geschieht über das Noscript-Symbol mit Klick auf das blaue „S“ mit kleiner Uhr (temporär) oder mit dem zweiten „S“-Symbol (dauerhaft). Falls eine als „Trusted“ bewertete Seite rot markiert bleibt, dann ist die Verbindung nicht HTTPS-verschlüsselt. Wenn dort nur 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“ HTTPS voraussetzt.

Add-ons: Weniger ist besser

Noscript ist nicht jedermanns Sache: Gibt es empfehlenswerte Sicherheitserweiterungen für weniger erfahrene Nutzer?

Auch für Add-ons gilt: Es handelt sich um Software, welche die Browserkomplexität erhöht und auch selbst fehlerhaft oder gar schädlich sein kann. Ein prominentes Beispiel ist das Add-on WOT (Web of Trust), das vor betrügerischen Websites warnt, aber mit den Benutzerdaten seinerseits skandalösen Datenhandel betrieb. Das Add-on ist zwar immer noch ein Sicherheitsgewinn, hat aber in puncto Datenschutz seinen Kredit verspielt und dürfte außerdem durch die Safe Browsing API von Chrome/Firefox weitgehend obsolet sein.

Das einzige sicherheitsrelevante Add-on neben Noscript, das auch normalen Nutzern zu empfehlen ist, ist HTTPS Everywhere (siehe unten). Deutlicher in Richtung Datenschutz und Werbeabwehr geht das Add-on Ublock Origin, das Werbetracker und Werbung blockiert. Theoretisch kann



„Nicht sicher“, weil nur HTTP? Browser sollten zumindest bei lokalen Adressen (hier der lokale Router) von dieser Warnung absehen.



Diese Erweiterung verschlüsselt zwar nicht das Internet, erzwingt aber die verschlüsselte HTTPS-Version, wo immer ein Server dies anbietet.

Ublock auch die Sicherheit erhöhen, weil auch Werbung Schadsoftware transportieren kann.

Verbindung ist „Nicht sicher“

Was bedeutet es, wenn Chrome neben einer Adresse „Nicht sicher“ anzeigt oder – gleichbedeutend – Firefox ein durchgestrichenes Schloss-Symbol?
Der Browserhinweis „Nicht sicher“ ist kein Signal für betrügerische oder schädliche Seiten. Er bedeutet nur, dass die Interaktion zwischen Server und Benutzer unverschlüsselt verläuft – mit HTTP (Hypertext Transfer Protocol). Websites, die nur Daten ausliefern, aber keine Anmeldung, Abfrage oder sonstige Interaktion des Lesers vorsehen, können im Prinzip auf ein SSL/TSL-Zertifikat und HTTPS (Hypertext Transfer Protocol Secure) ohne Nachteil verzichten. Allerdings wird es auch dort zunehmend zum „Schönheitsfehler“, nur HTTP anzubieten. Unverzichtbar ist verschlüsseltes HTTPS hingegen überall, wo der Seitenbenutzer Anmeldekennwörter oder personenbezogene Daten wie Mail- oder Postadresse übermittelt – insbesondere bei Bankgeschäften und Einkäufen über Paypal und Kreditkarte.
Achtung: Verschlüsseltes HTTPS ist kein Garant für vertrauenswürdige Seiten. Auch betrügerische Seiten können verschlüsselte Verbindungen anbieten.

Das Add-on HTTPS Everywhere

Das Add-on HTTPS Everywhere gibt es für Firefox wie Chrome und behauptet etwa im Chrome Web Store, „das Internet zu verschlüsseln“. Garantiert das Add-on verschlüsseltes HTTPS?
Die Ansage, das Internet zu verschlüsseln, ist natürlich Unsinn. Ein kleines Add-on auf Clientseite kann keine verschlüsselte Verbindung herstellen, wenn der ausliefernde Server nur HTTP anbietet. Richtig ist, dass das Tool – wo immer verfügbar – zu verschlüsseltem HTTPS wechselt, falls die Adresseingabe oder ein Link eine unverschlüsselte HTTP-Adresse enthält. Sie können das Tool sogar dahingehend verschärfen, dass der Zugang zu unverschlüsselten Seiten generell verboten wird („Unverschlüsselte Anfragen sind derzeit blockiert“). Auch dann ist es noch möglich, diese Seite zu öffnen, aber dazu muss explizit die Schaltfläche „Unsichere Seite öffnen“ gewählt werden.

„Incognito“ oder „Privates Fenster“

Ist es sicherer, generell im „Incognito-“ (Chrome) beziehungsweise „privaten“ Modus ins Internet zu gehen?
Mit dem Thema „Sicherheit“ hat diese Datenschutzoption nichts zu tun. „Privates Surfen“ bietet keinerlei zusätzlichen Schutz vor Schädlingen oder betrügerischen Seiten. Es anonymisiert weder die IP noch verschleiert es strafbare Handlungen. Der Sinn dieser Einstellung ist es, die kommerzielle Trackingschnüffelei der Werbeindustrie zu verhindern und außerdem die Surfspuren (Verlauf, Cache, Cookies) auf dem Rechner zu beseitigen.
Übrigens: Noch weniger sicherheitsrelevant ist die „Do Not Track“-Option aller modernen Browser. Die Bitte „Do Not Track“ im Header der Browseranfrage sollte es der Gegenstelle verbieten, Nutzungsprofile über den Besucher anzulegen. Der Effekt ist aber fraglich, weil Websites nicht verpflichtet sind, der Bitte nachzukommen.

Cookies: Lästig, aber bequem

Erhöht es die Sicherheit, dem Browser das Speichern von Cookies zu verbieten?
Cookies haben keinen Einfluss auf die Internetsicherheit, sondern gehören zum Thema Datenschutz. Die kleinen Cookie-Textdateien, die praktisch alle Websites ablegen, notieren IP-Adresse, Datum und Uhrzeit des Besuchs sowie eventuelle Zugangsdaten.
Das Auswerten von Cookies ergibt ein Nutzungsprofil, das Google & Co. dann für gezielte Werbeplatzierung nutzen. Radikales Blockieren oder Löschen von Cookies (etwa in Firefox unter „Datenschutz & Sicherheit → Cookies […] löschen“) ist aber in der Praxis eher zu unbequem: Auf vielen Seiten ist dann eine explizite Anmeldung erforderlich. Die Daten wird dann zwar der Autofill-Mechanismus des Browsers eintragen, aber trotzdem sind stets zusätzliche Klicks erforderlich. ■

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

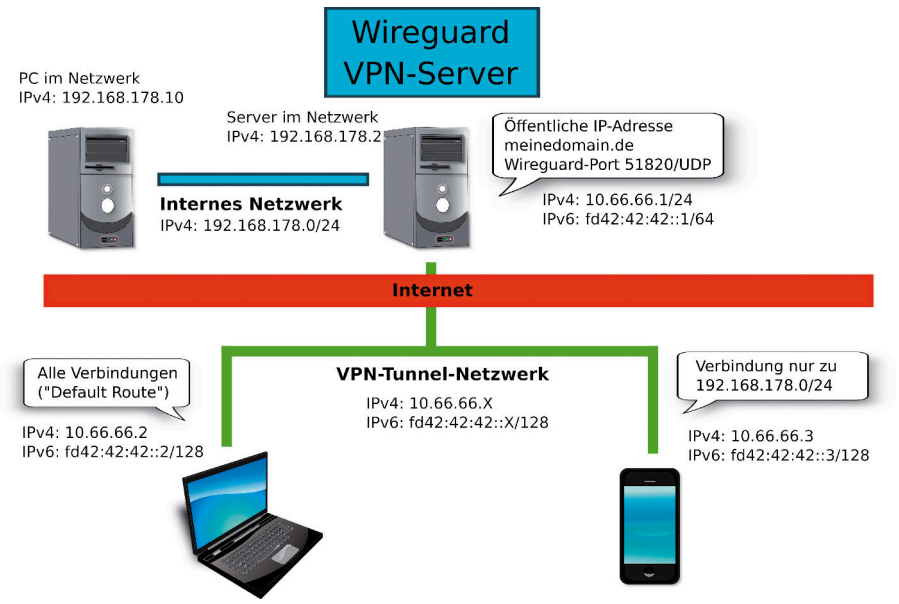
AWPNA14143

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

Mit VPN sicher durchs Netz

Mit VPN surfen Sie auch in fremden Netzen sicher, weil die Verschlüsselung Sie vor Datenspionen schützt. Einen VPN-Zugang können Sie mieten, aber auch ein eigener VPN-Server ist schnell konfiguriert.

VON THORSTEN EGGELING



Tunnel durchs Internet: Eine mit Wireguard verschlüsselte VPN-Verbindung bietet Schutz, wenn Sie sich in öffentliche WLANs einwählen.

Die meisten Verbindungen zu Web-, Mail- oder Chatservern erfolgen mittlerweile verschlüsselt über HTTPS/SSL. Im eigenen WLAN ist der Datentransfer zum Router zudem noch per WPA2 verschlüsselt. Gefahr droht jedoch in fremden WLAN-Netzen, wenn der Zugriff ohne Anmeldung erfolgt und damit keine Verschlüsselung stattfindet. Personen, die im gleichen WLAN unterwegs sind, können den unverschlüsselten Datenverkehr belauschen und bei HTTPS-Verbindungen zumindest die Adressen der Server herausfinden, die Sie besuchen. Es ist auch möglich, Ihnen gefälschte SSL-Zertifikate unterzuschieben oder Seitenaufrufe an Phishing-Server umzuleiten.

Das sicherste Mittel dagegen ist ein VPN-Tunnel (Virtual Private Network). Der verschlüsselt die komplette Internetverbindung und Spione im Netzwerk kommen nicht an Ihre Daten. Eine VPN-Verbindung stellen Sie über einen VPN-Anbieter her, was nur einige Euro im Monat kostet (siehe Kasten „VPN-Anbieter"). Oder Sie richten Ihren eigenen VPN-Server zu Hause oder in einem Rechenzentrum ein.

VPN dient nicht zum anonymen Surfen im Internet. Dafür ist andere Software erforderlich (siehe Artikel ab Seite 122). Mit VPN können Sie aber Ihren tatsächlichen Standort verbergen. Dadurch lässt sich im Ausland Geoblocking austricksen, das den Zugang beispielsweise zu einigen Streamingangeboten verwehrt.

Service: Alle (hier im Magazin durch Zeilenumbrüche teilweise schwer lesbaren) Befehlszeilen sowie eine Wireguard-Beispielkonfiguration können Sie über *www.pcwelt.de/wguard* abrufen.

1. VPN-Server einrichten

Wir beschreiben die Installation für Ubuntu 18.04 oder Linux Mint 19.3 auf einem Server im eigenen Netzwerk. Vorab ist zu bedenken, dass die Leistung durch die geringe Uploadgeschwindigkeit vieler DSL-Anschlüsse begrenzt ist. Wenn Tarif und Leitung den Upload mit 50 oder 100 MBit/s bieten, ist das ideal. Noch schneller geht es nur mit einem Server bei einem Webhosting-Anbieter, den man schon für unter zehn Euro pro Monat mieten kann. Als VPN-Software empfehlen wir Wireguard (*www.wireguard.com*). Die noch recht junge Software lässt sich im Vergleich zu anderen VPN-Lösungen einfach konfigurieren und der Aufbau der Verbindungen erfolgt relativ schnell. Zudem bleibt die Verbindung zuverlässiger bestehen, wenn man den Netzwerkzugang wechselt, beispielsweise von WLAN zu Mobilfunk.

Wireguard ist bei Ubuntu 18.04 nicht im Standard-Repository enthalten. Die Installation erfolgt daher im Terminal über ein PPA:

```
sudo add-apt-repository
  ppa:wireguard/wireguard
sudo apt update
sudo apt install wireguard qrencode
```

Starten Sie Linux danach neu.

2. Wireguard-Server konfigurieren

Der Server muss als Router IPv4- und IPv6-Pakete weiterleiten. Um die Funktion zu aktivieren, editieren Sie zunächst die Datei „sysctl.conf":

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

Entfernen Sie dort die Kommentarzeichen („#“) vor „net.ipv4.ip_forward=1“ und „net.ipv6.conf.all.forwarding=1“. Mit

```
sysctl -p
```

aktivieren Sie die Änderungen ohne Neustart.

Schritt 1: Führen Sie auf dem Server die folgenden drei Befehle aus:

```
sudo mkdir /etc/wireguard
(umask 077 && printf "[Interface]\
 nPrivateKey = " | sudo tee /etc/
 wireguard/wg0.conf > /dev/null)
wg genkey | sudo tee -a /etc/
 wireguard/wg0.conf | wg pubkey |
 sudo tee /etc/wireguard/publickey
```

Damit erzeugen Sie (erste Zeile) die Datei „/etc/wireguard/wg0.conf“ mit dem Konfigurationsabschnitt

```
[Interface]
PrivateKey =
```

Die zweite Zeile erzeugt den für die Authentifizierung nötigen privaten Schlüssel, baut ihn in die „conf“-Datei ein und erstellt den öffentlichen Schlüssel in der Datei „/etc/wireguard/publickey“.

Schritt 2: Öffnen Sie die Wireguard-Konfigurationsdatei in einem Editor:

```
sudo gedit /etc/wireguard/wg0.conf &
```

Ergänzen Sie die Zeilen, wie es in der Abbildung rechts oben zu sehen ist (Download: *www.pcwelt.de/wguard*).

Die Bezeichnung der Netzwerkschnittstelle, in unserem Beispiel „enp0s3“, passen Sie für Ihr System an. Wie diese heißt, erfahren Sie über den Befehl

```
ip addr
```

Die iptables-Regeln sorgen dafür, dass die Datenpakete von den Clients weitergeleitet und für die öffentliche IP des VPN-Servers umgeschrieben werden (NAT, Network Address Translation).

Alle IP-Adressen müssen bei Wireguard im CIDR-Format (Classless Inter-Domain Routing) angegeben werden. Einen Umrechner dafür finden Sie unter *www.ipaddressguide.com/cidr*.

Die IP-Adresse ist frei wählbar, sollte aber – wie in unserem Beispiel – aus einem privaten Adressbereich nach RFC 1918 stammen. Allerdings besteht die Gefahr von Adresskonflikten, wenn derselbe Bereich zufällig auch im gerade genutzten WLAN zum Einsatz kommt. Eine Alternative ist eine IP-Adresse gemäß RFC 6596, beispielsweise „100.64.0.1/10“, die ebenfalls nicht über das Internet geroutet wird und damit als sicher gelten kann.



Serverkonfiguration: Unter „[Interface]“ stehen die Daten für den Server. Der „[Peer]“-Abschnitt enthält die Schlüssel (hier noch nicht eingetragen) und IP-Adressen der Clients.

3. Die Konfigurationsdatei für VPN-Clients

Erzeugen Sie eine Konfigurationsdatei für den VPN-Client im Home-Verzeichnis auf Ihrem Server (vier Zeilen):

```
printf "[Interface]\nPrivateKey = "
 | tee ~/wg0-client1.conf > /dev/
 null
wg genkey | tee -a ~/wg0-client1.
 conf | wg pubkey | tee ~/client1_
 publickey
printf "[Peer]\nPresharedKey = " |
 tee -a ~/wg0-client1.conf > /dev/
 null
wg genpsk | tee -a ~/wg0-client1.
 conf
```

Die letzte Zeile erzeugt einen Presharedkey, der für zusätzliche Sicherheit sorgt. Ergänzen Sie in der Datei „wg0-client1.conf“die Zeilen, wie in der Abbildung unten zu sehen ist.

Die IP-Adresse hinter „DNS=“ teilt dem Client mit, welchen DNS-Server er verwenden soll. „8.8.8.8“ ist ein öffentlicher Google-DNS-Server. Ohne diese Angabe verwendet der Client die DNS-Adresse des jeweiligen WLANs und die Abfragen lassen sich abfangen beziehungsweise manipulieren.

Im Abschnitt „[Peer]“ tragen Sie hinter „PublicKey =“ den Schlüssel aus der Datei „/etc/wireguard/publickey“ des Wireguard-Servers ein. Hinter „Endpoint=“ bringen Sie die



Clientkonfiguration: Hinter „Endpoint=“ steht die öffentliche IP-Adresse oder der Domainname des Servers sowie der Port, den Sie beim VPN-Server festgelegt haben.

VPN-ANBIETER MIT WIREGUARD

Wer keinen eigenen VPN-Server betreiben möchte, findet im Internet mehrere VPN-Anbieter, die auch Wireguard unterstützen.

Ein kostenloses Angebot gibt es bei *https://tunsafe.com/vpn*. Eine Registrierung ist nicht nötig, Klicks auf „Create New Account“ und „Generate and Download“ genügen. Tunesafe bietet allerdings kein IPv6.

Mullvad VPN (*https://mullvad.net*) und Azirevpn (*www.azirevpn.com*) sind beide in Schweden beheimatet und bieten VPN ab fünf Euro pro Monat. Es werden IPv4 sowie IPv6 unterstützt und es gibt Serverstandorte beispielsweise in Kanada, Spanien und den USA. Von allen Anbietern erhält man eine „conf“-Datei und einen QR-Code, die sich wie in Punkt 4 beschrieben verwenden lassen.

aus dem Internet erreichbare öffentliche IP-Adresse des Servers oder seinen Domainnamen unter. Wenn Ihr Internetanbieter keine feste IP-Adresse bereitstellt, verwenden Sie einen Anbieter für dynamische IP-Adressen. Im Router muss außerdem eine Weiterleitungsregel („Port forwarding“) für den Port „51820“ auf dem Server-PC eingerichtet sein (siehe *www.pcwelt.de/1745578*).

„AllowedIPs = 0.0.0.0/0“ bewirkt, dass der gesamte Internetverkehr durch den VPN-Tunnel über Ihr heimisches Netzwerk läuft und Sie auf das lokale Netzwerk sowie den Server zugreifen können.

Die Zeile

```
AllowedIPs = 10.66.66.1/32,
  192.168.178.0/24
```

erlaubt den Zugang zum Server und das heimische Netzwerk, alle anderen Zugriffe laufen über die aktuelle Internetverbindung des Clients. Wenn mehrere Clients das VPN verwenden sollen, erzeugen Sie nach dem gleichen Muster eine entsprechende Anzahl anders benannter Konfigurationsdateien und mit jeweils anderen IP-Adressen.

Serverkonfiguration ändern: Ergänzen Sie auf dem Server in der Datei „/etc/wireguard/wg0.conf“ unter „[Peer]“ hinter „Public Key=“ den öffentlichen Schlüssel des Clients aus der Datei „~/client1_publickey“ sowie den „PresharedKey“ aus der Datei „~/wg0-client1.conf“.

Bei mehreren Clients vervielfältigen Sie den Abschnitt „[Peer]“ und tragen den öffentlichen Schlüssel des jeweiligen Clients ein. Hinter „AllowedIPs=“ passen Sie die IP-Adresse mit „10.66.66.3/32“, „10.66.66.3/32“ und so weiter an.

4. VPN-Verbindung aufbauen

Installieren Sie Wireguard auf einem Client-PC unter Linux wie in Punkt 1 beschrieben. Kopieren Sie dann die Clientkonfigurationsdatei „wg0-client1.conf“ in den Ordner „/etc/wireguard“.

Starten Sie Wireguard auf dem Server

```
sudo wg-quick up wg0
```

und auf dem Client mit

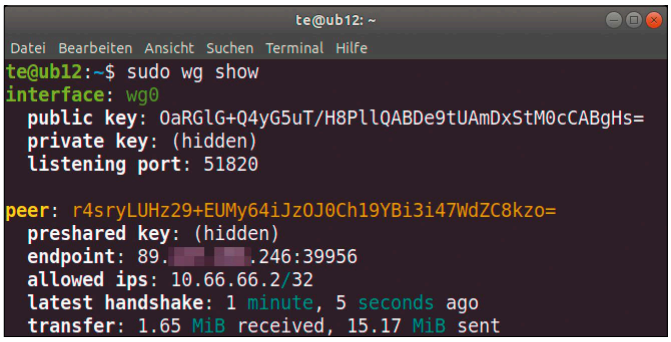
```
sudo wg-quick up wg0-client1
```

Um eine Verbindung wieder zu beenden, ersetzen Sie „up“ durch „down“.

Auf dem Server erhalten Sie mit

```
sudo wg show
```

Informationen zur Verbindung. Hinter „latest handshake:“ steht die Zeit seit Beginn der Verbindung und hinter „transfer:“, wie viele Daten empfangen beziehungsweise gesendet wurden.



Verbindungsinfos: Mit „sudo wg show“ lässt sich auf dem Server abfragen, welche Clients gerade verbunden sind und welche Datenmengen übertragen wurden.

Windows und Smartphones: Wireguard-Software für andere Betriebssysteme laden Sie über *www.wireguard.com/install* herunter. Beim Windows-Client laden Sie einfach die unter Linux erstellte Clientkonfiguration über „Import tunnel(s) from file“ und klicken dann auf „Activate“, um die Verbindung herzustellen. Die Apps für Android- und iOS-Smartphones können die Konfiguration bequem über einen QR-Code einlesen. Den erstellen Sie unter Linux mit dieser Befehlszeile:

```
qrencode -t ansiutf8 -l L < wg0-
  client1.conf
```

In der Smartphone-App scannen Sie den QR-Code ein und aktiveren danach die VPN-Verbindung.

Hinweis: Zum Testen können sich Server und Client auch im selben Netzwerk befinden. Für einen aussagekräftigen Test müssen Client-PC oder Smartphone die Internetverbindung jedoch auf einem anderen Weg herstellen, beispielsweise über das Mobilfunknetz. Rufen Sie im Browser *https://ipv6-test.com* auf. Wenn alles richtig konfiguriert ist, zeigt Ihnen die Webseite die öffentlichen IPs des Wireguard-Servers an. Ohne VPN sehen Sie die IPs des jeweiligen Internetproviders.

VPN-Server automatisch starten: Der folgende Befehl

```
systemctl enable wg-quick@wg0
```

sorgt dafür, dass der VPN-Dienst auf dem Server automatisch startet.

5. Alternatives Open VPN

Eine Alternative zu Wireguard ist das zwar bewährte, aber nicht besonders schnelle Open VPN.

Tipps zur manuellen Einrichtung lesen Sie unter *www.pcwelt.de/40450*. Deutlich schneller und einfacher geht es jedoch mit dem Script Pi VPN (*www.pivpn.io*). Es wurde ursprünglich für den Raspberry Pi entwickelt, funktioniert aber auch auf einem Ubuntu- oder Debian-Rechner. Neben Open VPN kann das Script auch einen Wireguard-Server konfigurieren.

Laden Sie das Script herunter und starten Sie es folgendermaßen:

```
wget -O pivpn https://install.
  pivpn.io
bash pivpn
```

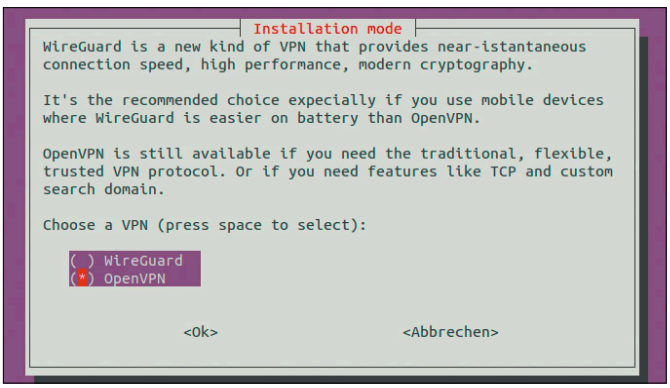
Folgen Sie den Anweisungen des Assistenten. Nach Abschluss der Installation lässt sich mittels

```
pivpn add
```

eine „ovpn“-Konfigurationsdatei erstellen. Auf dem Client sorgt dann der Aufruf

```
sudo openvpn --config [ovpn-Datei]
```

für den Start der Verbindung. ■



Open VPN einrichten: Das Script Pi VPN unterstützt Sie mit einem Assistenten bei der Konfiguration von Open VPN. Es kann aber auch Wireguard installieren.

PC-WELT PLUS

GRATIS! Eine Ausgabe gedruckt & digital



Jetzt kostenlos die gedruckte & digitale Ausgabe bestellen!

Jetzt bestellen unter
www.pcwelt.de/gratis 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 die PC-WELT gratis.

Möchten Sie die PC-WELT Plus anschließend weiter lesen, brauchen Sie nichts zu tun. Sie erhalten die PC-WELT Plus für weitere 12 Ausgaben zum aktuellen Jahresabopreis von z.Zt. 87,60 EUR. Danach ist eine Kündigung zur übernächsten Ausgabe jederzeit möglich.

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

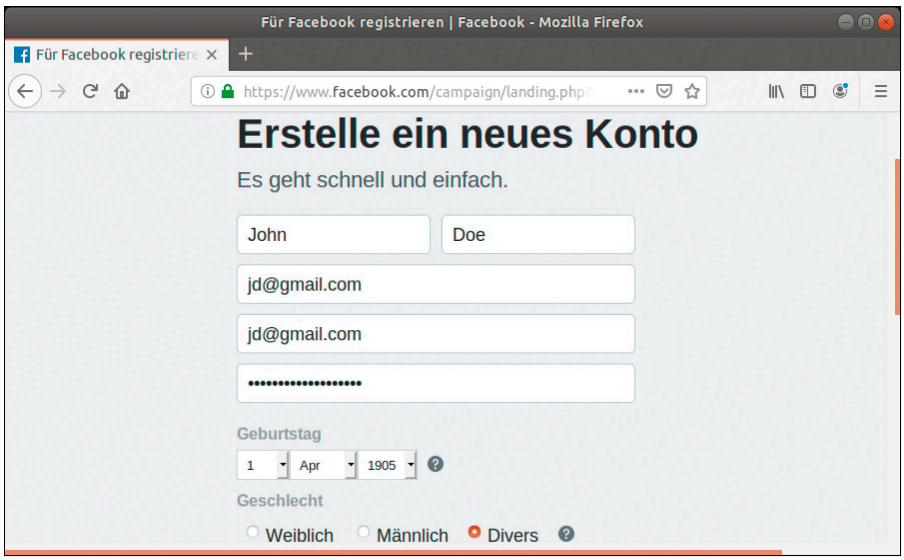
PWPNA14140

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

Mehr Schutz dank Sicherheitsschlüssel

Alleine mit einem Passwort sind Onlinedienste nicht optimal geschützt. Ein USB-Sicherheitsschlüssel verbessert den Schutz und kann auch die Linux-Anmeldung absichern.

VON THORSTEN EGGELING



Gefahr für Onlinekonten: Die Absicherung nur mit Benutzernamen und Passwort bedroht Ihre Online-Identität. Sicher ist eine Zwei-Wege-Authentifizierung.

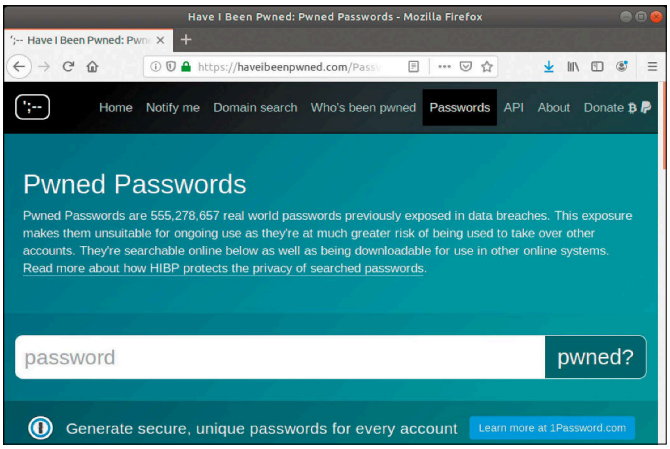
Die Anmeldung mit Benutzername und Passwort gilt seit langem als die größte Schwachstelle bei jeder Art von Authentifizierung. Einfache Passwörter lassen sich erraten oder ausprobieren und komplexe Passwörter überfordern den Benutzer. Zudem bietet auch das beste Passwort keinen Schutz, wenn es nach dem Einbruch in den Server eines Onlinedienstes in falsche Hände gerät. Onlinekonten und PCs lassen sich jedoch über eine Zwei-Wege-Authentifizierung effektiv absichern. Die Idee dahinter ist einfach: Bei der Anmeldung muss neben Benutzernamen und Passwort ein weiterer Faktor hinzukommen. Dafür gibt es unterschiedliche Verfahren. Die Identität lässt sich beispielsweise über einen Code prüfen, den Sie sich per SMS zusenden lassen, über eine App auf dem Smartphone oder mit Hilfe zusätzlicher Hardware. Nicht alle Methoden bieten die gleiche Sicherheit.

Service: Die Befehlszeilen, Scripts und Beispielkonfigurationen dieses Artikels sowie weitere Information zum Thema finden Sie über *www.pcwelt.de/5Wk1MZ*.

1. Das Problem mit den Passwörtern

Die Authentifizierung nur mit dem Benutzernamen und Passwort ist aus mehreren Gründen problematisch. Zu einfache Passwörter stellen eine Gefahr dar, weil Onlinekonten einfach durch Ausprobieren gekapert werden können. Aber auch bei komplexen Passwörtern gibt es keine vollständige Sicherheit.

Passwort und Benutzername sind beim Anbieter in einer Datenbank gespeichert. Gerät die Benutzerdatenbank nach einem Servereinbruch in falsche Hände, können Sie nicht sicher sein, ob fremde Personen Zugriff auf Ihr Konto haben. Die Anbieter informieren meist – aber nicht immer – per E-Mail und fordern Sie dazu auf, das Passwort zu ändern. Oft wird der Einbruch aber nicht sofort bemerkt. Deshalb gilt die Empfehlung, bei den diversen Onlinediensten stets unterschiedliche Passwörter zu verwenden. Das erhöht für Sie als Benutzer allerdings den Aufwand bei der Passwortverwaltung.



Datendiebstahl: Mailadressen und Passwörter können bei Servereinbrüchen in falsche Hände geraten. Ob Ihre Daten gestohlen wurden, lässt sich unter *https://haveibeenpwned.com* ermitteln.

Tipp: Ob Ihre E-Mail-Adresse oder das Passwort bei einem Servereinbruch kopiert worden sind, können Sie übrigens unter *https://haveibeenpwned.com* herausfinden.

2. Die Lösung: Zwei-Faktor-Authentifizierung

Mehr Sicherheit lässt sich durch die Kombination von Benutzernamen und Passwort mit einer weiteren Information erreichen. Der zusätzliche Faktor stammt im optimalen Fall von einem anderen Gerät oder Medium. Der Vorteil: Das Passwort muss dann nicht besonders kompliziert sein und wenn es in falsche Hände geraten sollte, dann spielt das keine Rolle. Der Zugang zum Konto wird erst gewährt, wenn Sie sich mit einem zusätzlichen Schlüssel ausweisen. Bei der Anmeldung sollten mindestens zwei der drei folgenden Elemente zum Einsatz kommen:

- Wissen: etwas, das nur der Nutzer weiß (Passwort, PIN)
- Besitz: etwas, das nur der Nutzer besitzt (Mobiltelefon, Sicherheitsschlüssel)
- Inhärenz: etwas, das zum Nutzer gehört (Fingerabdruck, Gesichtserkennung)

„Besitz" kann beispielsweise eine ausgedruckte Liste, SMS, Smartphone-App oder ein Nummerngenerator sein. Die Kombination aus „Wissen" und „Besitz" ist am leichtesten umzusetzen, weil dafür meist bereits vorhandene Hardware wie ein Smartphone genutzt werden kann.

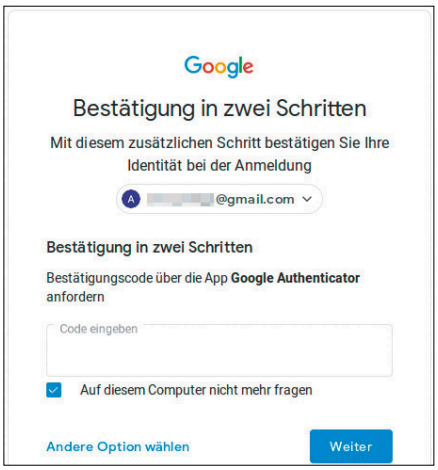
Je nach Konfiguration wird neben dem Passwort der Sicherheitsschlüssel bei jeder Anmeldung oder sicherheitsrelevanten Aktion angefordert oder er gilt dauerhaft für ein bestimmtes Gerät beziehungsweise den verwendeten Browser. Unbefugte Personen, die Ihr Passwort in Erfahrung gebracht haben, benötigen daher in jedem Fall zusätzlich den Sicherheitsschlüssel, wenn sie sich auf einem anderen PC anmelden.

3. Sicherheit von Einmalpasswörtern

Vor allem Banken haben in der Vergangenheit bei der Zwei-Wege-Authentifizierung auf Einmalpasswörter in Form einer TAN gesetzt (OTP: One Time Password). Die gab es zuerst als ausgedruckte Listen und dann per SMS. Im Prinzip wäre das sicher, wenn Bankingteilnehmer nicht immer wieder TANs über Phishingseiten preisgegeben hätten. SMS lassen sich durch Trojaner auf dem Smartphone abfangen oder beim Mobilfunkanbieter mitlesen. Banken sind aufgrund gesetzlicher Vorgaben dazu verpflichtet, die möglichen Risiken zu reduzieren. Beim Onlinebanking beispielsweise wurden Sie mit den geänderten Anforderungen wahrscheinlich schon konfrontiert. Die meisten Banken fordern inzwischen die zusätzliche Authentifizierung über eine Banking-App oder einen Chip-TAN/Smart-TAN-Generator an. Banking-Apps können als sicher gelten, solange PC und Smartphone nicht durch Schadsoftware kompromittiert sind oder Benutzername, Passwort und Smartphone nicht in falsche Hände geraten.

TAN-Generatoren arbeiten offline und sind daher vor Hackerangriffen geschützt. Zudem benötigen Sie Ihre Bankkarte, um eine TAN zu erzeugen. Diese gilt nur für einen bestimmten Auftrag, dessen Daten Sie auf dem Display des TAN-Generators prüfen sollten. Die Auftragsdaten lassen sich bei Geräten mit optischen Sensoren von einem Flickerbild auf dem PC-Monitor einlesen. Das Verfahren kann als sicher gelten, solange unbefugte Personen nicht in den Besitz von Bankkarte und Zugangsdaten gelangen. Wenn Sie den Verlust bemerken und die Karte sperren lassen, erzeugt der Generator keine gültigen TANs mehr.

Eine weitere Variante sind Passwörter, die nur eine Zeitlang gültig sind (TOTP: Time-based One Time Password). Weit verbreitet ist die Smartphone-App Google Authenticator, die von Google, Amazon, Paypal und weiteren Diensten unterstützt wird. Bei der Initialisierung, also bei der Einrichtung der Zwei-Faktor-Authentifizierung, wird ein geheimer Schlüssel erzeugt und auf dem Smartphone und auf dem Server gespeichert. Der Google Authenticator erstellt auf Basis dieses Schlüssels und der aktuellen Uhrzeit das Einmalpasswort, das aus sechs Ziffern besteht und für 30 Sekunden gilt. Die Uhren von Server und Client müssen ungefähr synchron sein, damit das Passwort akzeptiert wird. Die Schwachstelle von TOTP: Client und Server verwenden identi-



Zweiter Faktor: Viele Konten lassen sich über einen zusätzlichen Code sichern, der beispielsweise vom Google Authenticator auf dem Smartphone erzeugt wird.

ZUSÄTZLICHE TOOLS FÜR DEN YUBIKEY

Die im Artikel erwähnten Kommandozeilentools für den Yubikey sind allesamt in den Paketquellen aktueller Linux-Systeme enthalten. Wer möchte, kann sich aber auch Verwaltungstools für die grafische Oberfläche installieren. Führen Sie im Terminal diese zwei Befehlszeilen aus, um das Yubico-PPA hinzuzufügen:

```
sudo add-apt-repository ppa:yubico/stable
sudo apt-get update
```

Danach lassen sich per „sudo apt install [Paketname]" drei zusätzlich Pakete installieren.

yubikey-manager-qt: Das Programm bietet eine einfache grafische Oberfläche für die Konfiguration von FIDO2, OTP und PIV. Außerdem lassen sich damit einzelne Funktionen deaktivieren und wieder aktivieren.

yubikey-personalization-gui: Das Yubikey Personalization Tool dient ebenfalls zur Konfiguration des Yubikeys, bietet aber erweiterte Funktionen. Sie verwenden es vor allem, wenn Sie in einem Unternehmen mehrere Yubikeys konfigurieren möchten.

yubioath-desktop: Der Yubikey-Authenticator arbeitet ähnlich wie der Google Authenticator. Er generiert jedoch Einmalpasswörter, die über den Yubikey abgesichert sind.

sche Schlüssel. Sollte der Schlüssel in falsche Hände geraten, könnten ihn auch Phishingseiten verwenden.

4. Beste Absicherung über Hardwareschlüssel

Maximale Sicherheit versprechen Hardwaretokens für den USB-Port, auf denen ein privater Schlüssel gespeichert ist. Dieser Schlüssel lässt sich nicht auslesen und wird auch nicht an einen Onlinedienst übertragen. Bei der Einrichtung der Zwei-Wege-Authentifizierung übermittelt der USB-Token seinen öffentlichen Schlüssel an den Server des Onlineanbieters. Die Aktion muss der Nutzer am USB-Token per Knopfdruck bestätigen. Damit ist sichergestellt, dass die Information tatsächlich von der Hardware stammt und nicht per Software simuliert wird. Der weitere Datenaustausch wird dann über den USB-Token mit dem privaten Schlüssel signiert, was einer digitalen Unterschrift entspricht. Der Server prüft die Signatur mit dem ihm inzwischen bekannten öffentlichen Schlüssel. Passen Daten und Signatur zusammen, ist die Identität bestätigt.

Da der private Schlüssel sich beim USB-Token nicht auslesen lässt und der öffentliche Schlüssel nur dem Onlinedienst bekannt ist, gibt es hier kaum Angriffsflächen. Zudem speichern die USB-Token die URL der ursprünglichen Website und die Anmeldung funktioniert nur hier. Ein Angreifer müsste daher den Webserver des Onlinedienstes komplett unter seine Kontrolle bringen, damit ein Angriff Erfolg hat.

5. Hardwareschlüssel für Google & Co.

USB-Tokens für die Onlineauthentifizierung gibt es schon ab zehn Euro. Ein Beispiel ist Key-ID Fido U2F (*www.key-id.com*) für etwa 12 Euro. Der USB-Sicherheitsschlüssel ist nach Fido (Fast Identity Online, *https://fidoalliance.org*), zertifiziert und bietet daher Kompatibilität mit vielen Webdiensten. „U2F“ steht für Universal Second Factor, also Zwei-Wege-Authentifizierung. Zur Zeit werden unter anderem Google, Dropbox, Facebook und Wordpress.org unterstützt.

Mit gut 50 Euro ist der Yubikey 5 NFC deutlich teurer (*www.yubico.com*). Der Sicherheitsschlüssel bietet dafür aber auch zahlreiche Funktionen, unter anderem Fido, Fido2, Webauthn, Smart Card (PIV-kompatibel), OTP, TOTP und Open PGP. Entsprechend lang ist die Liste der unterstützten Onlinedienste, die Sie unter *https://www.yubico.com/works-with-yubikey/catalog/* finden. Mit Fido2 sind Sie auch für die Zukunft gerüstet. Bisher gibt es für den noch recht neuen Standard jedoch nur wenige Einsatzbereiche, etwa bei Microsoft für die Windows-10-Anmeldung ohne Passwort.

Unter Linux lässt sich der Yubikey für die Zwei-Wege-Authentifizierung in den Webbrowsern Firefox und Google Chrome nutzen. Dafür ist keine zusätzliche Software erforderlich. Es ist aber auch möglich, die Linux-Anmeldung mit dem Sicherheitsschlüssel zu schützen.



Sicherheitsschlüssel: Der Yubikey (50 Euro) unterstützt auch aktuelle Standards wie FIDO2. Key-ID (12 Euro) bietet den U2F-Standard, was für die meisten Onlinedienste ausreicht.

6. Zwei-Wege-Authentifizierung per USB-Token

Wir erläutern am Beispiel Google, wie sich eine Zwei-Wege-Authentifizierung mit einem Sicherheitsschlüssel einrichten lässt. Bei den meisten Onlinediensten läuft es ähnlich ab.

Schritt 1: Melden Sie sich auf dem PC bei Google an, öffnen Sie die Webseite *https://myaccount.google.com/security*, klicken Sie auf „Bestätigung in zwei Schritten“ und auf „Jetzt starten“. Geben Sie das Google-Passwort ein und klicken Sie auf „Weiter“.

Schritt 2: Es ist sinnvoll, die Benachrichtigung per SMS zu aktivieren. Sollte der Sicherheitsschlüssel gerade nicht verfügbar sein, können Sie sich über die alternative Methode anmelden. Wenn Sie das nicht wünschen, klicken Sie auf „Andere Option auswählen“ und „Sicherheitsschlüssel“ und fahren bei Schritt 4 fort. Andernfalls tippen Sie Ihre Telefonnummer ein und wählen die Option „Telefonanruf“ (Festnetz) oder „SMS“. Nach einem Klick auf „Weiter“ geben Sie den Code aus der SMS ein, klicken auf „Weiter“ und dann auf „Aktivieren“.

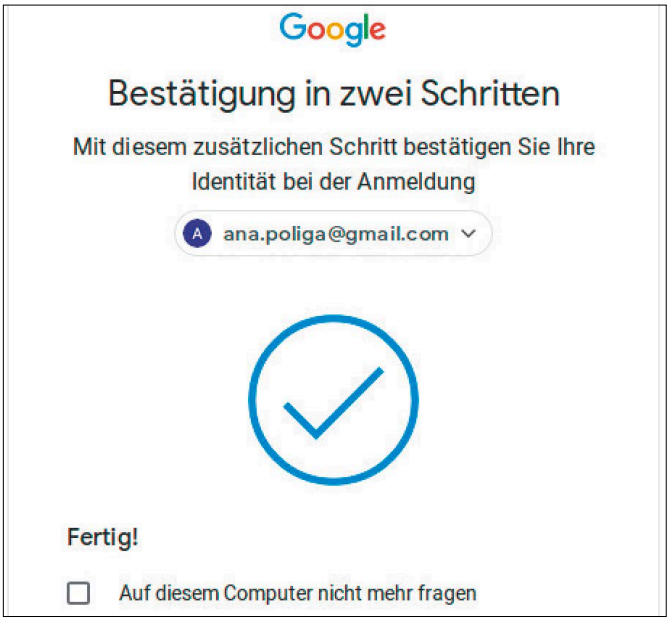
Schritt 3: Klicken Sie unter „Alternativen zweiten Schritt einrichten“ auf „Sicherheitsschlüssel“ hinzufügen und dann auf „Weiter“.



Key mit dem Konto verknüpfen: Aktivieren Sie in den Google-Einstellungen die „Bestätigung in zwei Schritten“. Danach registrieren Sie den Sicherheitsschlüssel.

Schritt 4: Danach verbinden Sie den Yubikey oder Key-ID-Schlüssel mit dem PC. Berühren Sie die Scheibe auf dem Yubikey oder drücken Sie bei Key-ID den Taster. Tippen Sie eine aussagekräftige Bezeichnung für den Schlüssel ein und klicken Sie auf „Fertig“.

Schritt 5: Melden Sie sich bei Google ab und mit Ihrem Passwort wieder an. Danach bestätigen Sie die Anmeldung am Sicherheitsschlüssel wie in Schritt 4. Auf der folgenden Seite ist standardmäßig ein Häkchen vor „Auf diesem Computer nicht mehr fragen“ gesetzt. Das ist zwar bequem, macht aber den zusätzlichen Schutz durch den Sicherheitsschlüssel zunichte, etwa wenn das Notebook verloren geht. Daher sollten Sie das Häkchen entfernen, bevor Sie auf „Weiter“ klicken.



Unsicherheitseinstellung: Bei Google ist standardmäßig „Auf diesem Computer nicht mehr fragen“ aktiviert. Für maximale Sicherheit sollten Sie das Häkchen entfernen.

7. Über den Yubikey bei Linux anmelden

Der Yubikey wird von Linux standardmäßig wie eine Tastatur behandelt und als „Human Interface Device“ erkannt. Die Konfiguration als Hardwaretoken für die Linux-Anmeldung erfordert jedoch höhere Rechte, die Sie über Udev-Regeln anfordern.

Schritt 1: Die erforderlichen „rules“-Dateien „69-yubikey.rules“ und „70-u2f.rules“ finden Sie unter *www.pcwelt.de/5Wk1MZ* im Ordner „yubikey“. Kopieren Sie beide Dateien in den Ordner „/etc/udev/rules.d“. Danach führen Sie die folgenden zwei Befehle in einem Terminalfenster aus.

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

Starten Sie Linux neu.

Schritt 2: Installieren Sie die erforderliche Software:

```
sudo apt-get install libpam-yubico
 yubikey-personalization
```

Führen Sie danach diese drei Befehlszeilen aus:

```
ykpersonalize -2 -ochal-resp
 -ochal-hmac -ohmac-lt64 -oserial-
 api-visible
mkdir $HOME/.yubico
ykpamcfg -2 -v
```

Das erste Kommando konfiguriert den Yubikey für das Challenge-Response-Verfahren. Der Key besitzt zwei Konfigurationsspeicher. „Slot 1“ ist vom Werk aus für Yubico-OTP eingerichtet und liefert das Einmalpasswort für Onlineanmeldungen, wenn Sie die Schaltfläche kurz berühren. „Slot 2“ ist nicht belegt, was Sie über die Option „-2“ und das Tool ykpersonalize ändern. ykpamcfg sendet eine zufällige Zeichenfolge (Challenge) an den Yubikey, der einen mit seinem privaten Schlüssel erzeugten Hashwert zurückgibt (Response). Das Ergebnis wird in einer Datei im Ordner „$HOME/.yubico“ gespeichert. Bei der Authentifizierung wird erneut eine Challenge an den Yubikey gesendet. Wenn er korrekt antwortet, handelt es sich um denselben Schlüssel, der bei der Initialisierung mit dem PC verbunden war, und die Anmeldung ist erfolgreich.

Schritt 3: Jetzt müssen Sie die Anmeldung über den Yubikey noch in die Linux-Anmeldung einbauen. Erstellen Sie (als root) die Textdatei „/etc/pam.d/inc_yubikey“ mit diesen vier Zeilen:

```
auth required pam_yubico.so
 mode=challenge-response
auth [success=1 default=ignore]
 pam_unix.so    try_first_pass
auth requisite pam_deny.so
auth required pam_permit.so
```

Schritt 4: Probieren Sie die Konfiguration zuerst für „sudo“ aus:

```
sudo gedit /etc/pam.d/sudo
```

Mint-Nutzer verwenden „xed“ statt „gedit“. Setzen Sie ein Kommentarzeichen (‚#‘) vor die Zeile „@include common-auth“ und fügen Sie darunter die Zeile

```
@include inc_yubikey
```

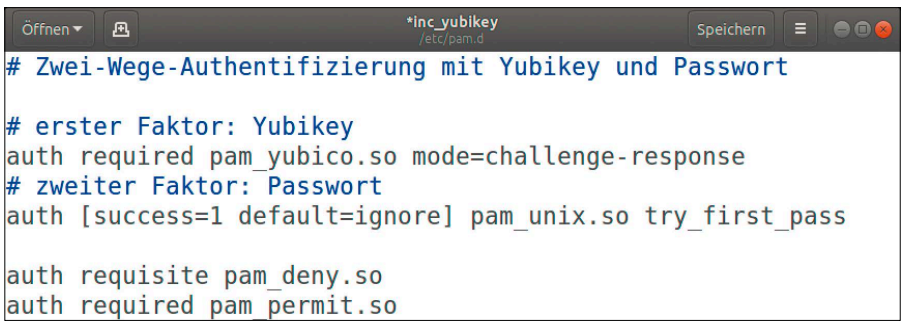
ein. Öffnen Sie dann ein weiteres Terminal, wo Sie diesen Befehl eingeben:

```
sudo -i
```

Der Wechsel zum Systemverwalterkonto funktioniert jetzt nur mit eingesteckten Yubikey und Passwort.

Schritt 5: Bauen Sie „@include inc_yubikey“ entsprechend in die Dateien „/etc/pam.d/gdm-password“ (Linux Mint 19: „/etc/pam.d/lightdm“) sowie „/etc/pam.d/polkit-1“ ein.

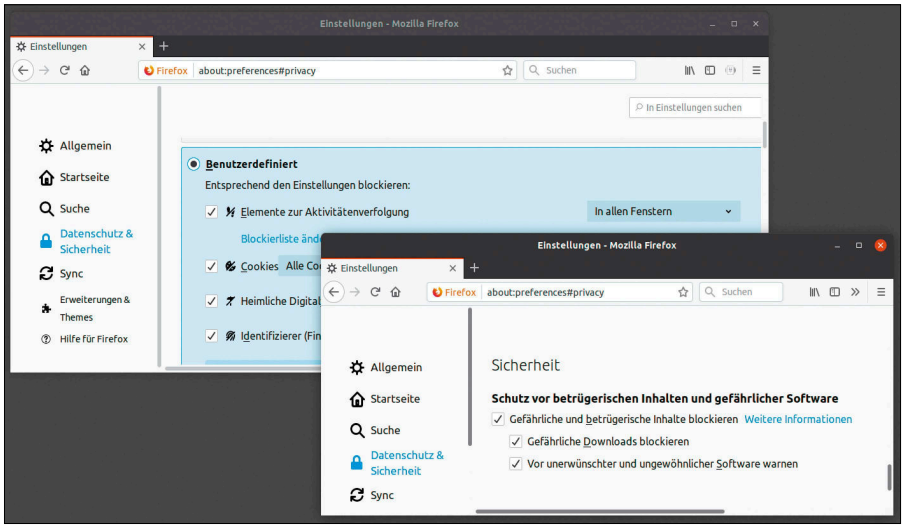
Damit sichern Sie die Anmeldung an der grafischen Oberfläche zusätzlich über den Yubikey ab. ■



Linux-Log-in absichern: Diese PAM-Konfiguration erlaubt die Linux-Anmeldung nur, wenn der Yubikey mit dem PC verbunden ist und Sie das richtige Passwort eingeben.

Firefox-Sicherheit

Moderne Browser filtern das Web und schützen vor gefährlichen Webseiten und Downloads. Dieser Beitrag erklärt die Techniken für Sicherheit und Datenschutz im Mozilla-Browser Firefox.



VON HERMANN APFELBÖCK

Sicherheit im Browser hat zwei Aspekte: Das Wichtigste ist der Schutz vor betrügerischen Seiten und Schadsoftware. An zweiter Stelle steht der Datenschutz für Surfaktivitäten, Lesezeichen und Kennwörter. Der Artikel erklärt die Sicherheitsfunktionen von Firefox, der unter Linux mit Masterpasswort und besserem Script-Schutz (mit Noscript) weiter erste Wahl bleibt.

Das Masterpasswort

Firefox fragt bei einer neuen Webanmeldung, ob das Passwort gespeichert werden soll. Solches Speichern ist bequem, weil Sie sich das Passwort dann nicht länger merken müssen. Andererseits bedeutet das, dass jeder, der Zugriff auf Ihr Gerät hat, auch Ihre persönlichen Zugänge nutzen kann. Unter „Einstellungen → Sicherheit → Gespeicherte Zugangsdaten“ lassen sich alle Kennwörter sogar in Gesamtschau bequem auslesen. Dagegen hilft das Masterpasswort, das Sie unter „Einstellungen →Datenschutz & Sicherheit → Master-Passwort verwenden“ einrichten und das die Kennwörter verschlüsselt. Der Komfortverlust ist vertretbar: Das Masterpasswort wird pro Firefox-Sitzung nur einmal abgefragt, eventuell auch gar nicht, falls Sie keinen Zugriff auf die Kennwörter benötigen.

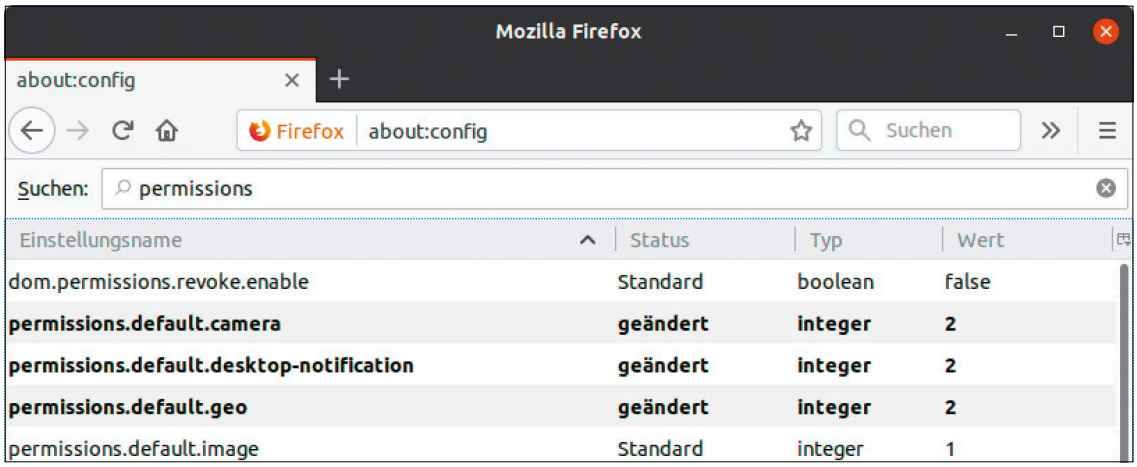
Die Firefox-Schutzmechanismen

Anlaufstelle ist der Punkt „Einstellungen → Datenschutz & Sicherheit“. Die wichtigsten Einstellungen zeigt Firefox ganz unten auf dieser Seite unter **„Schutz vor betrügerischen Inhalten…“.** Hier sollten alle drei Kästchen aktiviert sein, um gefährliche Webseiten und Downloads zu blockieren. Es handelt sich um einen Grundschutz, der auf der Basis einer Blacklist funktioniert, die ständig aktualisiert wird (alle 30 Minuten). Eine weitergehende Heuristik wie Chrome besitzt Firefox nicht. Das heißt: Firefox blockiert Downloads von bekannten betrügerischen Seiten. Den Virendownload von einer bisher unbescholtenen Webseite wird Firefox hingegen ohne Kommentar zulassen, während Chrome in gleicher Situation vor einem „ungewöhnlichen Download“ warnt. Allerdings ist dieser Chrome-Mechanismus relativ primitiv: Er schlägt dann an, wenn Dateiname und Signatur unbekannt sind und eine ausführbare Extension vorliegt (wie EXE oder DEB). Unter Linux ist solche Unterstützung kaum relevant.

Berechtigungen für Kamera und Mikro: Eine Webseite sollte niemals ungefragt Kamera oder Mikrofon Ihres Rechners benutzen dürfen. Auch der geografische Standort ist ein personenbezogener Fakt, der nicht ungefragt berichtet werden muss. Solche „Berechtigungen“ regelt der gleichnamige Punkt unter „Datenschutz & Sicherheit“. Mit der Schaltfläche „Einstellungen“ bestimmen Sie für Standort, Kamera, Mikrofon und Benachrichtigungen je einzeln, dass alle Webseiten (die nicht in der Liste stehen) nichts automatisch dürfen: Der Punkt lautet „Neue Anfragen […] blockieren“.

Ganz oben auf der Konfigurationsseite „Datenschutz & Sicherheit“ steht der Punkt **„Seitenelemente blockieren“.** Hier steht der Datenschutzaspekt im Vordergrund. Die Stufe „Standard“ genügt für den Schutz vor der Aktivitätenverfolgung von Trackern, die Surfdaten, Cookies und Fingerprints (errechnet aus Browser, Computer, Betriebssystem, Bildschirmauflösung u. a.) über mehrere Websites hinweg sammeln, sowie vor Krypto-Minern und schädlichen Scripts. Die Einstellung „Streng“ erzielt praktisch einen permanenten „Privaten Surfmodus“ (siehe unten). „Benutzerdefiniert“ ermöglicht gegenüber „Standard“ und „Streng“ kaum genauere Abstufungen, nur die Cookieakzeptanz können Sie hier noch restriktiver (als „Streng“) oder noch toleranter (als „Standard“) setzen.

Bei „strenger“ oder „benutzerdefiniert“ strenger Konfiguration ist es immer noch möglich, die Verbote für vertrauenswürdige Websites aufzuheben. Dies geschieht im Abschnitt „Seitenelemente blockieren“ ganz oben mit der Schaltfläche „Ausnahmen verwalten“.



Alternative Konfiguration: Einstellungen wie „Permissions“ (Berechtigungen) sind in der Firefox-Konsole „about:config“ leichter zu filtern als in den grafischen Einstellungen.

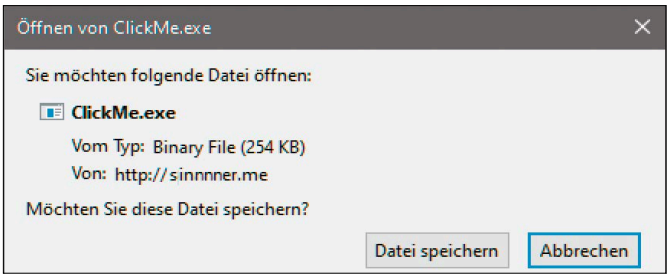
Das Surfen im „Privaten Fenster“

„Privates Surfen“ bietet keinen Schutz vor Schädlingen oder betrügerischen Seiten. Es anonymisiert weder die IP noch verschleiert es strafbaren Handlungen. Trotzdem sind „Private Fenster“ nützlich: Sie unterbinden den Großteil kommerzieller Trackingschnüffelei. Ein wichtiger Nebenaspekt ist ferner, dass Sie ohne Cookies und Webprotokolle unterwegs sind und neutrale Ergebnisse erhalten (gelegentlich wichtig bei Suchmaschinen und Onlineshops). In Firefox ist der Hotkey Strg-Umschalt-P der schnellste Weg zum privaten Fenster.

Neben dem privaten Modus bietet Firefox eine „Do Not Track“-Option. Dieser Info-Tag im Header der Browseranfrage sollte es der Gegenstelle verbieten, Nutzungsprofile über den Besucher anzulegen. Der Effekt ist aber fraglich, weil Websites nicht verpflichtet sind, der Bitte nachzukommen. „Do Not Track“ ist nicht standardmäßig aktiv. Sie finden die Option „Websites eine „Do Not Track“-Information senden“ unter „Einstellungen → Datenschutz & Sicherheit“.

Die Firefox-Synchronisierung

Browsersynchronisierung bedeutet für Nutzer mehrerer Geräte einen unschätzbaren Komfort. Sie benötigt allerdings ein kostenloses Konto auf *https://accounts.firefox.com* und hat den Nebenaspekt, dass viele persönliche Daten auf dem Mozilla-Server hinterlegt werden müssen – aus Bequemlichkeit meist auch die Passwörter („Zugangsdaten“). Der Umfang der Synchronisierung ist unter „Einstellungen → Sync“ im Detail einstellbar. Firefox verschlüsselt aber standardmäßig alle Daten, wobei der Schlüssel auf dem Gerät des Benutzers verbleibt. Die Mozilla Foundation ist grundsätzlich vertrauenswürdig und macht keine Geschäfte mit Benutzerdaten.



Schädliche Downloads: Firefox warnt nicht vor Downloads, wenn die betreffende Website bislang nicht als bösartig gemeldet wurde.

Sicherheitsrelevante Erweiterungen

Firefox hat seine Stärken bei der Erweiterbarkeit und dies gilt auch für den Sicherheitsaspekt: Firefox-Erweiterungen suchen und installieren Sie über „Add-ons → Erweiterungen“.

Noscript: Das Add-on verhindert, dass Firefox Javascript, Java oder andere ausführbare Inhalte automatisch startet. Noscript ist unbequem, aber der Schädlingsstop schlechthin. Einmal erlaubte Sites landen in der Whitelist und müssen später nicht mehr einzeln bestätigt werden, aber zunächst müssen Sie auf vielen interaktiven Seiten diverse Scripts manuell erlauben. Dies geschieht über das Noscript-Symbol mit Klick auf das blaue „S“ mit kleiner Uhr (temporär) oder mit dem zweiten „S“-Symbol (dauerhaft). Falls eine als „Trusted“ bewertete Seite rot markiert bleibt, dann ist die Verbindung nicht HTTPS-verschlüsselt. Wenn dort nur 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“ HTTPS voraussetzt.

HTTPS Everywhere: Verschlüsseltes HTTPS ist bei allen Webanmeldungen, vor allem bei Bankgeschäften und Einkäufen unverzichtbar.

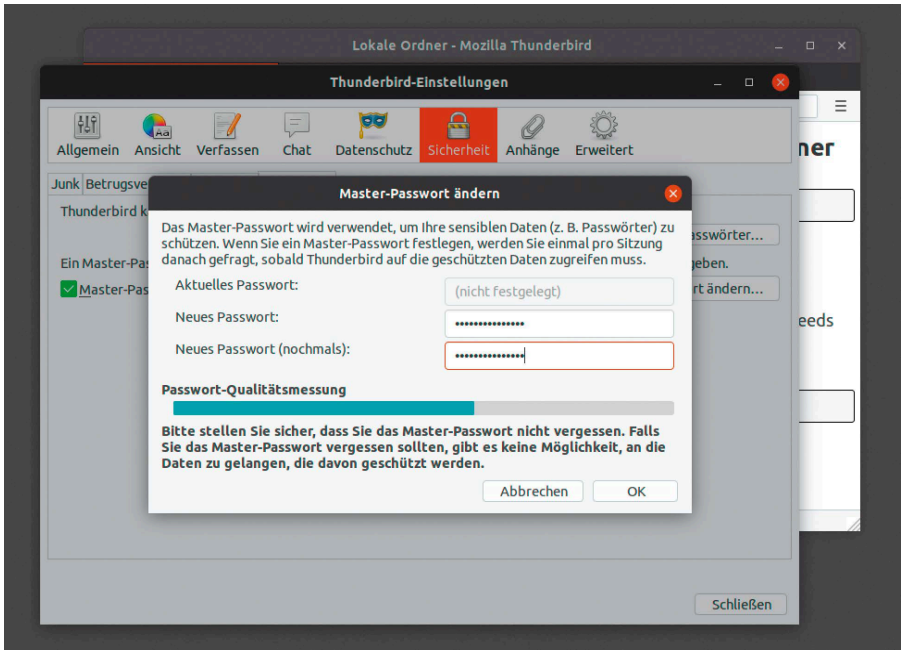
Der Browser zeigt verschlüsselte Verbindungen in der Adresszeile grün gefärbt. HTTPS Everywhere wählt, wo immer verfügbar, eine verschlüsselte HTTPS-Verbindung zu einer Website, auch wenn die Adresseingabe oder ein Link eine unverschlüsselte HTTP-Adresse anfordert. Die Bedeutung des Add-ons nimmt aber ab, je mehr HTTPS zum Standard wird. Beachten Sie außerdem, dass „grünes“ HTTPS zwar den Datenverkehr verschlüsselt, aber keine vertrauenswürdige Seite garantiert. Auch betrügerische Seiten nutzen heutzutage oft verschlüsselte Verbindungen.

Lastpass & Co.? Als Ersatz für den eingebauten Passwortmanager gibt es Alternativen wie das Add-on Lastpass. Dieser Manager benötigt ein Konto bei Lastpass und verspricht auf seinen Servern AES-Verschlüsselung aller Daten. Der Einsatz solcher Alternativen ist aber nicht recht nachvollziehbar: Das native Firefox Sync bietet neben der Synchronisierung der Kennwörter auch noch die von Lesezeichen und Einstellungen. Aus unserer Sicht gibt es kein Motiv, einen externen Passwortmanager zu verwenden. ■

Thunderbird-Sicherheit

Mails an sich sind nicht gefährlich. Aber sie sollten Mails bleiben, nicht ins Web gehen – und Mailanhänge von Fremden haben auf dem Rechner gar nichts verloren. Wenn Sie dann noch Ihre Zugangsdaten schützen, sind Sie auf der sicheren Seite.

VON HERMANN APFELBÖCK



Jüngst hatte ein Windows-Schädling Erfolg, der als Mailanhang in Form einer Word-Datei verschickt wurde. Die Nachricht forderte zum Lesen der Word-Datei auf, mit dem Hinweis, doch bitte beim Öffnen der Datei den Makrovirenschutz von Word zu deaktivieren. Dass viele Anwender dieser Aufforderung gehorcht haben, ist dümmer, als Windows und Word erlauben, beweist aber die Manipulierbarkeit und Naivität der meisten Internetnutzer. Gesundes Misstrauen ist unerlässlich und beginnt mit misstrauischen Softwareeinstellungen.

Die Notwendigkeit des Masterpassworts

Ein „gehacktes" oder den falschen Personen bekanntes Mailkonto (Benutzername und Kennwort) legt nicht nur die Korrespondenz offen, sondern ermöglicht den Zugriff auf weitere Log-ins: Denn bei den meisten Diensten genügt die Mailadresse, um sich („Kennwort vergessen?") einfach ein neues Passwort zu beschaffen. Trotzdem werden sich die meisten Nutzer den Komfort erlauben, die Zugangsdaten in der Thunderbird-Konfiguration zu hinterlegen. Thunderbird speichert dann die Daten im Profilordner in der Datei „logins.json", was die automatische Anmeldung am Mailserver ermöglicht. Dadurch ergeben sich folgende Datenschutzlücken:

1. Wer auf das laufende System mit Ihrem Benutzerkonto Zugriff hat, kann die Zugangsdaten in Thunderbird unter „Einstellungen → Sicherheit → Passwörter → Gespeicherte Passwörter → Passwörter anzeigen" auslesen. Das ist kein großes Problem, sofern Sie in einer Büroumgebung vor Verlassen des Arbeitsplatzes den Desktop sperren.

2. Kritisch sind verlorene Notebooks oder der Fremdzugriff auf PCs, auf denen Thunderbird die Zugangsdaten verwaltet. Auf den ersten Blick scheint das unproblematisch, denn die Zugangsdaten in der Datei „logins.json" sind verschlüsselt. Diese Verschlüsselung ist jedoch nicht mehr als Sichtschutz, um die Passwörter nicht im Klartext abzulegen. Es gibt Tools, um diese Zugangsdaten zu entschlüsseln. Noch umfassender ist der schlichte Umzug des Thunderbird-Profils mit Copy & Paste: Wer nach dem Boot mit einem Fremdsystem einfach den Profilordner („/home/[user]/.thunderbird/[xxxxxxxx]") auf USB-Stick kopiert und dann auf einem anderen Rechner in ein neu angelegtes Thunderbird-Profil einfügt, hat Zugangsdaten, Kennwörter und die komplette Mailkorrespondenz vorliegen.

Angesichts dieser Bedrohung gibt es für Notebooks, Mehrbenutzersysteme und leicht zugängliche Bürorechner nur zwei angemessene Antworten: Entweder man verzichtet auf das Thunderbird-Angebot, die Zugangsdaten zu speichern, oder man benutzt das Masterpasswort. Die Vergabe des Masterpassworts erledigen Sie unter „Bearbeiten → Einstellungen → Sicherheit → Passwörter → Master-Passwort verwenden". Dadurch werden die Zugangsdaten individuell verschlüsselt, sodass der Fremdzugriff auf Dateiebene erfolglos ist.

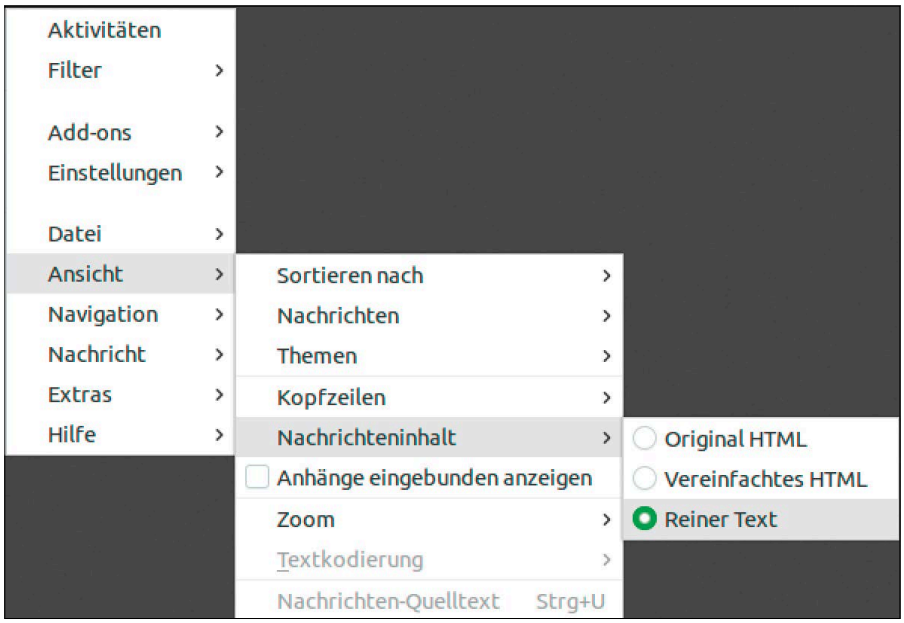
HTML-Format und externe Inhalte

HTML erlaubt hübsche Kommunikation mit Bildern, Links, Farben, Schriften. In Geschäftsmails mit Logos und Signaturen sind solche Formatierungen oft alternativlos. Auf der anderen Seite bietet HTML eine Plattform für Scripts und Tracking aller Art. Standardmäßig blockiert Thunderbird immerhin alle externen Inhalte, die nicht in der Nachricht selbst enthalten sind. Dafür sorgt die deaktivierte Option „Einstellungen → Datenschutz → Externe Inhalte in Nachrichten erlauben".

Schon das Anzeigen externer Elemente genügt, dem externen Webserver mitzuteilen, erstens dass überhaupt, zweitens wann und wo der Mailempfänger die Mail erhalten und gelesen hat. Das harmloseste Resultat ist daher der Nachweis, dass die Mailadresse existiert und genutzt wird. Beim Klick auf externe Inhalte kann aber darüber hinaus bereits ein Script ausgelöst werden, das Schadsoftware installieren will.

Externe Inhalte sollten deaktiviert bleiben. Man kann aber noch einen Schritt weitergehen und alle Nachrichten als reinen Text öffnen: Dazu genügt die globale Einstellung „Ansicht → Nachrichteninhalt → Reiner Text". Ein ästhetischer Kompromiss, der zumindest aktives Scripting aushebelt, ist die Einstellung „Vereinfachtes HTML". Ergänzend zu dieser Option sollte der Punkt „Ansicht → Anhänge eingebunden anzeigen" abgeschaltet werden. Dies unterbindet die Gefahr, dass ein Anhang schon beim Öffnen der Nachricht ein Script aktiviert.

Wer auf Formatierung und Bilder keinen Wert legt, kann seine eigenen Nachrichten als Reintext verschicken. Dies lässt sich unter „Einstellungen → Konten-Einstellungen" für jedes Konto mit „Verfassen & Adressieren" einzeln festlegen, indem Sie die Option „Nachrichten im HTML-Format verfassen" deaktivieren.



Nicht hübsch, aber hübsch sicher: Das Abschalten der HTML-Anzeige entschärft Links auf externe Websites und entzaubert manipulative Tarnoptik.

Maßnahmen gegen Phishing und Spam

Thunderbird kann betrügerisches Phishing und lästiges Spam („Junk") erkennen. Ob der Anti-Phishing-Filter aktiv ist (Standard), kontrollieren Sie unter „Einstellungen → Sicherheit → Betrugsversuche". Die Thunderbird-Regeln, gefälschte Nachrichten zu erkennen, sind hart codiert und nicht zu beeinflussen. Fundamentale Mechanismen erkennen falsche Web-URLs, die auf andere als die angezeigten Seiten führen, ferner gefälschte Bildverweise, die anders lauten als die URL der tatsächlichen Bildquelle. In solchen Fällen warnt Thunderbird: „Diese Nachricht könnte ein Betrugsversuch (Phishing) sein".

Beachten Sie, dass Sie der Gefahr, per unbedachten Klick auf eine gefälschte URL zu gelangen, kategorisch aus dem Weg gehen, wenn Sie Mails als „Reiner Text" anzeigen (siehe oben). Anderen Aufforderungen von Phishingbetrügern kann aber keine Technik, sondern nur der Verstand widerstehen: Die Abfrage von Bank- oder Kreditkartendaten macht kein Kreditinstitut per Mail und das Laden eines Anhangs unbekannter Absender verbietet sich von selbst.

Spam („Junk") ist in der Regel nur lästig, kann aber auch Stufe 1 zur Verifizierung des Mailkontos sein, dem dann Schlimmeres nachfolgt.

In den Einstellungen unter „Sicherheit → Junk" können Sie global bestimmen, ob Junknachrichten in den Junkordner verschoben werden sollen. Die Option, Spam automatisch zu löschen, ist meistens zu radikal, da Thunderbird wie jede Software gelegentlich irrt.

Anders als den Phishingfilter können Sie Thunderbird bei Spam individuell trainieren. Dazu markieren Sie jede Nachricht als Junk, die Sie als solche einstufen. ■

DER THUNDERBIRD-CHECK

- **„Ansicht → Nachrichteninhalt → Reiner Text":** Diese Einstellung ist nicht schön, denn sie unterbindet die Anzeige von HTML-Format, damit aber auch trügerische Tarnoptik und fatale Klicks auf Weblinks.
- **„Einstellungen → Sicherheit → Betrugsversuche":** Die einzige Option an dieser Stelle muss aktiviert sein, damit der Phishingfilter arbeitet.
- **„Einstellungen → Sicherheit → Passwörter":** Hier vergeben Sie das Masterpasswort. Wo und warum sich ein Masterpasswort empfiehlt, erklärt der Haupttext. Unter „Einstellungen → Sicherheit → Passwörter → Gespeicherte Passwörter" zeigt Thunderbird alle hinterlegten Zugangsdaten.
- **„Einstellungen → Datenschutz":** Folgende Option sollte aktiviert sein: „Websites mitteilen, meine Aktivitäten nicht zu verfolgen".
- **„Einstellungen → Datenschutz":** Folgende Option sollte auf keinen Fall aktiviert sein: „Externe Inhalte in Nachrichten erlauben".
- **„Einstellungen → Erweitert → Allgemein → Konfiguration bearbeiten":** Die Low-Level-Konfiguration zeigt Expertenoptionen, die über die Einstellungen der grafischen Oberfläche hinausreichen. Die meisten Direktiven sind allerdings nicht oder unzureichend dokumentiert. Das nicht risikolose Javascript können Sie durch Doppelklick beim Eintrag
  `javascript.enabled`
  auf „false" setzen und damit ausschalten.

Datenverschlüsselung mit Linux

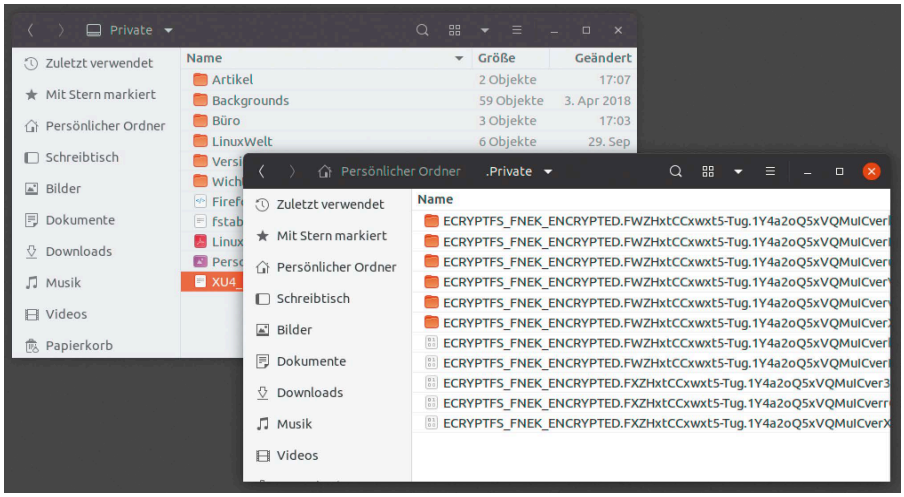
Wer sich den alleinigen Zugriff auf bestimmte Daten sichern will, muss diese verschlüsseln. Dabei stehen Geräte im Fokus, die besonders leicht in fremde Hände geraten, nämlich Notebooks und USB-Medien.

VON HERMANN APFELBÖCK

Verschlüsseln ist ein beeindruckender Vorgang: Aus standardisierten Tabellen-, Text- oder Bilddateien, die Milliarden Geräte und Personen lesen könnten, wird ein Binärcode, den nur noch Sie selbst lesbar machen. Die Motive, dies genau so zu wollen, müssen weder paranoid noch staatstragend noch kriminell oder schmuddelig sein: Ein verlorener USB-Stick kann unglaublich viel über Identität, Status, Arbeitgeber, Kontakte und Interessen verraten.

Linux-Werkzeuge zur Verschlüsselung

Wenn verschlüsselte Daten ausschließlich unter Linux genutzt werden, stehen zwei Methoden im Zentrum: Luks ist erste Wahl, zumal damit die Datenmenge dosierbarer ist, als es der Name „Datenträgerverschlüsselung“ nahelegt. Dazu unten mehr. Kleinere Lösungen bieten die sehr ähnlichen Werkzeuge Ecrypt FS und Enc FS. Aus Gründen der besseren Integration sehen wir hier klare Vorteile für Ecrypt FS, dessen Arbeitsweise wir unten kurz beschreiben. Andere Techniken können allenfalls als Ad-hoc-Lösung dienen, um schnell einen Dateianhang oder eine Clouddatei zu schützen. Ein Zukunftsversprechen, aber aktuell nicht praktikabel, ist die dateisystemeigene Ext4-Verschlüsselung. Diese von Google für Android entwickelte Ext4-Erweiterung hat unter Linux noch keinerlei Desktopintegration und bleibt auch im Terminal eine Zumutung. Da ist es komfortabler, etwa zum Packer 7-Zip zugreifen, der seine Archive mit Passwort verschlüsseln kann. Wenn Sie



Die kleine Ecrypt-FS-Lösung: Das Kryptotool richtet sehr bequem einen Ordner „~/Private“ ein, der bei der Systemanmeldung die Daten aus „~/.Private“ entschlüsselt.

nach Rechtsklick auf einer Datei „Komprimieren“ und das Format „7z“ wählen, gibt es unter „Erweiterte Einstellungen“ die Passwortoption. Mit

```
sudo apt install p7zip-full
```

rüsten Sie 7-Zip bei Bedarf nach.

Ecrypt FS: Einfach und komfortabel

Ecrypt FS bietet transparente Verschlüsselung eines Ordners inklusive aller Unterordner. Wer mit den beiden vorgegebenen Standardordnern klarkommt („/home/[user]“ oder Untermenge „/home/[user]/Private“), kann sich über komfortabelste Bedienung freuen. Die Einrichtung ist einfach und Sie benötigen kein Extrakennwort, da Ecrypt FS durch die Systemanmeldung entschlüsselt. Die Sicherheit hängt daher vom Systempasswort ab.

1. Verschlüsseltes „Home“ des Erstbenutzers: Linux Mint 19.x bringt diese Möglichkeit nach wie vor im Installer mit. Mit der Option „Meine persönlichen Dateien verschlüsseln“ wird Ecrypt FS automatisch für das Home-Verzeichnis des Erstbenutzers eingerichtet. Bei Fremdzugriff auf das Gerät ist zwar der Großteil des Dateisystems lesbar, nicht aber der Inhalt von „/home/[user]“. Dieser liegt verschlüsselt unter „/home/.ecryptfs/[user]/.Private“. Die Dateien werden automatisch unverschlüsselt nach „/home/[user]“ geladen, sobald sich der Benutzer anmeldet. Aus Anwendersicht ändert sich nichts beim Umgang mit den Dateien.

2. Verschlüsseltes „Home“ für weitere Konten: Unter Ubuntu, Linux Mint & Co. ist es sehr einfach, weitere Konten mit Home-Verschlüsselung einzurichten. Falls Ecrypt FS nicht installiert ist, holen Sie dies zunächst mit

```
sudo apt install ecryptfs-utils
```

nach. Danach legt dieser Terminalbefehl

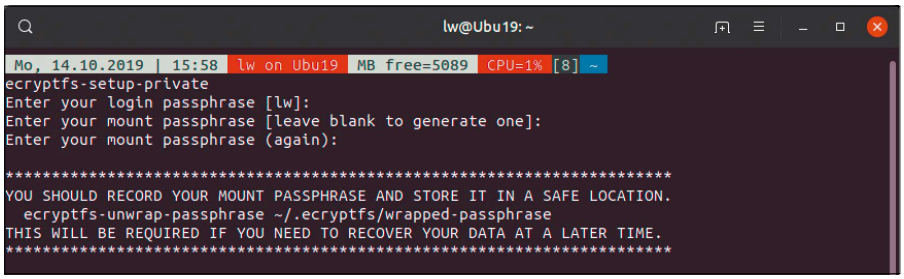
```
sudo adduser --encrypt-home [Konto]
```

einen neuen Benutzer an. Das Passwort für den neuen Benutzer wird mit „Geben Sie ein neues UNIX-Passwort ein:“ abgefragt. Danach kann sich der neue Benutzer anmelden und das verschlüsselte Home-Verzeichnis nutzen. Das Mounten der verschlüsselten Daten erfolgt auch hier automatisch mit der Systemanmeldung.

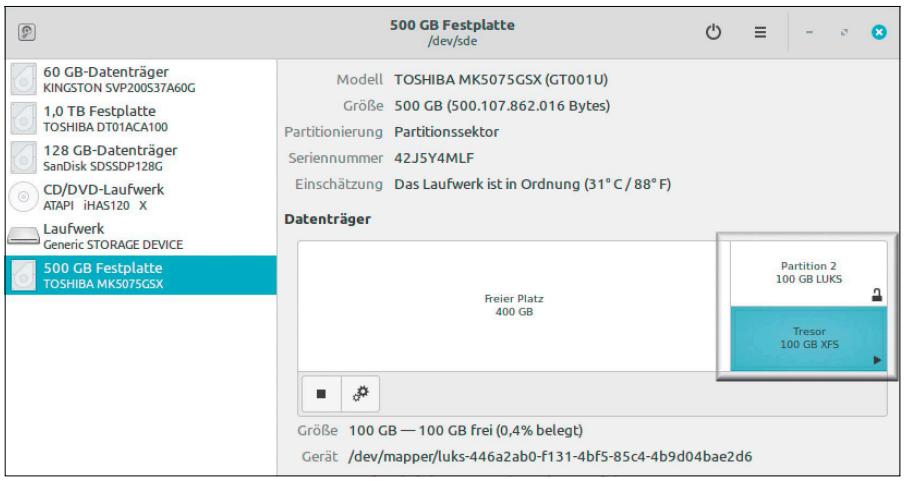
3. Nur den Unterordner „~/Private“ verschlüsseln: Ecrypt FS kann jederzeit genutzt werden, um im eigenen „Home“ einen geschützten Unterordner anzulegen, der standardmäßig den Namen „Private“ erhält:

```
ecryptfs-setup-private
```

Das Kommando fordert zunächst die Eingabe des normalen Systemkennworts („loginpassphrase“). Danach erwartet das Werkzeug mit der „mount-passphrase“ den Schlüssel, mit dem die Daten codiert werden. Die „mount-passphrase“ müssen Sie bei der späteren Benutzung niemals interaktiv eingeben und sollte zur höheren Sicherheit komplex ausfallen. Nach der nächsten Anmeldung erscheint im Home-Verzeichnis der neue Ordner „~/Private“. Alle Dateien darin werden bei der Anmeldung automatisch aus dem versteckten Ordner „~/.private“ entschlüsselt und bei der Abmeldung dorthin verschlüsselt.



Gut integriertes Ecrypt FS: Ein knapper Befehl aktiviert den verschlüsselten „Private“-Unterordner. Ein komplett verschlüsseltes „Home“ kann ein adduser-Befehl einrichten – aber nur für neue Konten.



Luks auf kleiner Partition: Die Verschlüsselung muss nicht mehr Platz einnehmen, als Sie für sensible Daten tatsächlich brauchen. Die übrige Laufwerkskapazität bleibt normal nutzbar.

Luks-Verschlüsselung: Transparent und flexibel

Luks (Linux Unified Key Setup) ist eine Datenträgerverschlüsselung ähnlich Bitlocker unter Windows. Gut organisiert leistet Luks aber mehr als die typische Komplettverschlüsselung des Systems.

1. Vollverschlüsselung ab Installation: Ubuntu-Distributionen bieten Luks bei der Systeminstallation. Im Dialog „Installationsart“ erscheint die Option „Die neue [...] Installation zur Sicherheit verschlüsseln“. Sobald Sie diese aktivieren, wird der weitere Punkt „LVM [...] verwenden“ aktiv. Der Logical Volume Manager ist notwendig, um neben der unverschlüsselten Bootpartition die Luks-formatierte Partition und die virtuelle LVM-Partition unterzubringen, die später – bei korrekter Kennworteingabe – unverschlüsselt ins Dateisystem geladen wird. Das Kennwort wird im nächsten Installerschritt abgefragt: Es sollte komplex, aber für tägliche Eingabe zumutbar sein: Das System startet später nur noch nach Kennworteingabe.

2. Luks auf USB: Luks kann auch USB-Laufwerke schützen. Mit dem Standardtool Gnome-Disks („Laufwerke“ unter Ubuntu und Linux Mint) ist das besonders einfach (ähnlich der „KDE Partition Manager“): Sie schließen das USB-Laufwerk an, hängen es im Dateimanager oder mit Gnome-Disks aus und löschen mit dem Laufwerkstool bestehende Partitionen mit dem Minus-Symbol unterhalb der Partitionsanzeige. Mit dem Plus-Symbol erstellen Sie auf dem freien Speicherplatz eine neue Partition mit Größenangabe. Mit „Nächstes“ geht es zum Folgedialog, wo Sie den „Datenträgernamen“ vergeben und als „Typ“ die Option „Andere“ wählen. Mit „Nächstes“ kommt dann der Dialog mit der Dateisystemwahl, der unten rechts den Eintrag „Passwortgeschützter Datenträger (LUKS)“ anzeigt. Nach Kennwortvergabe und Formatieren ist das Laufwerk präpariert. Bei späterer Verwendung verlangen Linux-Dateimanager automatisch das Kennwort und mounten den Datenträger bei korrekter Eingabe.

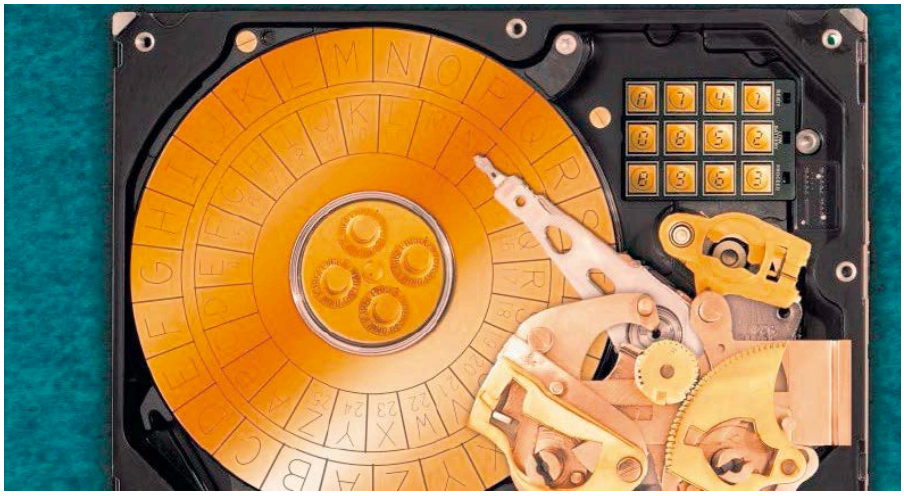
3. Partitionierungstipps: Luks-Verschlüsselung auf USB fordert keineswegs den kompletten Datenträger. Sie können den geschützten Bereich so klein oder groß definieren, wie Sie möchten. Wenn Sie etwa ein Zwei-TB-Medium mit einer Luks-Partition mit 400 GB einrichten, eine zweite unverschlüsselte Partition mit den restlichen 1600 GB, dann verhält sich diese zweite Partition unter Linux wie Windows standardmäßig: Beim Anstecken des Datenträgers wird die Partition im Dateimanager geladen (sofern ein kompatibles Dateisystem vorliegt). Die Luks-Partition sieht hingegen nur Linux und fragt nach dessen Kennwort. Bei korrekter Eingabe lädt Linux dann auch diese Partition. Die Reihenfolge der Partitionen – Luks-Partition am Anfang oder am Ende – spielt keine Rolle.

Was für USB-Laufwerke gilt, gilt auch für interne Festplatten. Durch Aufteilung der Systemfestplatte in System- und Luks-Partition erhalten Sie einen geschützten Bereich, den Sie im Dateimanager unter „Geräte“ per Klick bequem ein- und aushängen. Wer diese Konstellation nachträglich einrichten möchte, muss die Systempartition mit einem Livesystem und Gparted verkleinern, um im freien Platz eine Luks-Partition zu schaffen. ■

Verschlüsselte Veracrypt-Container

Veracrypt ist die beste Wahl, wenn verschlüsselte Daten auf unterschiedlichen Betriebssystemen genutzt werden. Die Software ist unter Linux, Windows und Mac-OS zwar nicht völlig funktionsgleich, aber die verschlüsselten Daten sind kompatibel.

VON HERMANN APFELBÖCK



Quelle: David Wolski

Veracrypt ist Open-Source-Software und kann keine geheimen Hintertüren für Geheimdienste verbergen. Es eignet sich für große Datenmengen auf Festplatten und mobilen USB-Datenträgern, weniger für den Transfer in die Cloud, da auch bei geringen Datenänderungen der Transport des gesamten Volumes („Container") notwendig wäre. Der technische Anspruch von Veracrypt geht deutlich über so einfache Motive hinaus, Mitarbeiteradressen oder Gehaltstabellen zugriffssicher zu verschlüsseln. Mit versteckten Volumes, diversen Verschlüsselungsalgorithmen, Zugangsmethoden über Passwort, PIM und Schlüsseldateien taugt das Werkzeug für politisch Verfolgte, vermutlich auch für strafrechtliche Verfolgte. Veracrypt ist komplex, wer sich jedoch auf das Wesentliche konzentriert, ist mit den Handgriffen zum Erstellen und Mounten von verschlüsselten Containern schnell vertraut.

Plattformen und Installation

Veracrypt gibt es auf der Projektseite *www.veracrypt.fr/en/Downloads.html* für Linux, Windows und Mac-OS. Generell ist Veracrypt auf Windows fokussiert und dort nochmal deutlich komplexer, da es auch Systempartitionen verschlüsselt und für externe Datenträger eine In-Place-Verschlüsselung bestehender Datenträger ohne Datenverlust anbietet. Unter Mac-OS ist neben Veracrypt das zusätzliche OSXFUSE erforderlich, um Veracrypt-Container laden zu können. Wenn Sie Veracrypt von der Projektseite auf Linux Mint installieren wollen, wählen Sie derzeit das DEB-Paket für Ubuntu 18.04. Alternativ funktioniert auf allen Ubuntu-basierten Distributionen auch die Einrichtung über ein PPA:

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

Im Unterschied zur Windows-Version ist Veracrypt unter Linux nicht Deutsch lokalisiert, weswegen wir uns bei den Menübezeichnungen an die englischsprachigen halten.

Die Datenträgerverschlüsselung

Da Veracrypt unter Linux einen Datenträger oder eine Partition komplett löschen und neu formatieren muss, um ihn zu verschlüsseln, gibt es nur einen nennenswerten Grund für die Komplettverschlüsselung: Der Datenträger soll sich wie ein unformatiertes Laufwerk verhalten. Ein Veracrypt-Laufwerk präsentiert sich unter Linux als unbekanntes Dateisystem und Windows will es umstandslos sofort formatieren. Nur Veracrypt kann das Laufwerk laden.

Ist dies tatsächlich so 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 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 dafür, dass keine oder nur eine Partition vorliegt. Alle weiteren Optionen der Einrichtung unterscheiden sich nicht vom Anlegen eines einfacheren Containers, das nachfol-

gend genauer beschrieben ist. Für das Mounten verschlüsselter Datenträger verwenden Sie die Schaltfläche „Select Device“.

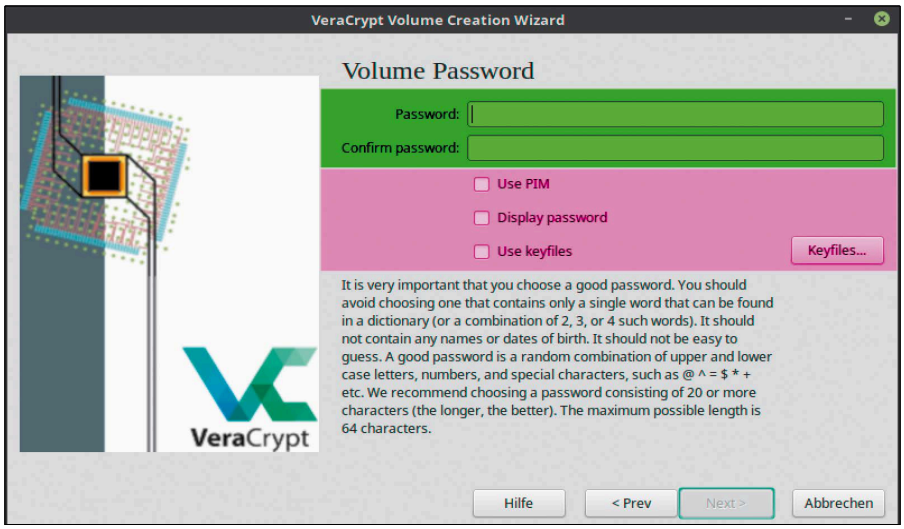
Die Containerverschlüsselung

Die Containerverschlüsselung ist technisch einfacher und die von uns wie auch vom Veracrypt-Assistenten empfohlene. Um eine 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 Vorgaben. Danach geben Sie die Größe der Containerdatei an. Die sollte großzügig ausfallen, weil die Kapazität nicht mehr zu ändern ist.

Danach kommt die Passwortvergabe. Speziellere Optionen sind im nächsten Punkt beschrieben. Für die meisten Szenarien ist ein Passwort völlig ausreichend. Die anschließenden „Format Options“ gelten für das innere Dateisystem des Containers und sind wichtig: Wählen Sie NTFS, wenn Sie die Daten auch unter Windows brauchen. Ein USB-Medium, das Sie unter allen Systemen nutzen möchten, muss nicht nur selbst ein allgemein kompatibles Dateisystem haben, sondern auch der Veracrypt-Container muss mit einem solchen formatiert sein. Im Allgemeinen kann man wenig falsch machen, sowohl als Datenträgerformat als auch beim internen Containerformat NTFS zu wählen. FAT genügt nur, wenn 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 oder das Dateisystem des Containers nicht kompatibel sind.

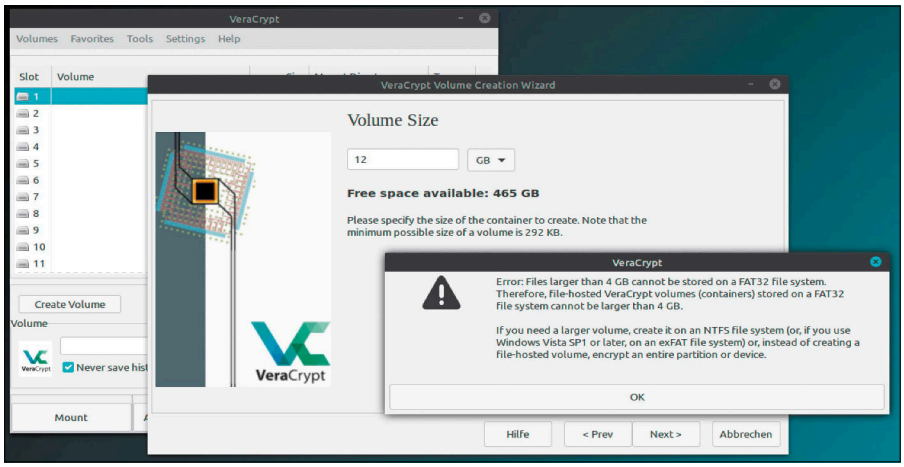
Zur Schlüsselerstellung auf Basis des Passworts erwartet Veracrypt Mausbewegungen im eigenen Fenster. Schließen Sie den Vorgang am Ende mit „Format“ ab. Damit



Veracrypt-Einsteiger halten sich besser an die einfache Passwortoption. Die erweiterten Möglichkeiten erhöhen die Komplexität (PIM, Keyfiles, Default Keyfiles).

VERACRYPT: PLUS UND MINUS

+ Veracrypt verschlüsselt sicher und kann als Open-Source-Software keine heimlichen Hintertüren für Geheimdienste enthalten.
+ Veracrypt ist plattformunabhängig und bester gemeinsamer Nenner, wenn verschlüsselte Daten zwischen Linux und Windows (und Mac-OS) ausgetauscht werden. Insbesondere Daten auf USB-Laufwerken können zuverlässig geschützt und auf verschiedenen Betriebssystemen verwendet werden.
+ Veracrypt-Daten können – mit gewisser Vorbereitung – auf einem zentralen Netzwerkserver von allen Systemen genutzt werden.
+ Veracrypt-Container sind flexibel: Anders als bei einer kompletten Datenträgerverschlüsselung ist die Größe beliebig skalierbar und genau auf die Menge der zu verschlüsselnden Daten abstimmbar. Außerdem gibt es keine Beschränkung für die Menge solcher Container.
+ – Die Basisbedienung ist relativ einfach, die Kenntnis aller Optionen jedoch anspruchsvoll.
+ – Veracrypt ist eine Software für PCs und Notebooks. Smartphones und Tablets mit Android und iOS werden nicht direkt unterstützt. Apps wie EDS Lite (Android) und Disk Decipher (iOS) sind unbefriedigend und bieten allenfalls Lesezugriff.
– Mit der bis zur Unsichtbarkeit reichenden Transparenz von Luks (Linux) und Bitlocker (Windows) kann Veracrypt nicht konkurrieren. Im Unterschied zu diesen Verschlüsselungsmethoden führt an der aktiven Benutzung der externen Veracrypt-Software kein Weg vorbei.
– Der Einsatz von Veracrypt erfordert gelegentlich Geduld: Das Laden („Mount“) und Entladen („Dismount“) ist öfter mal zäh, sollte Sie aber keinesfalls veranlassen, den Vorgang durch „Auswerfen“ des Datenträgers oder durch Abziehen eines USB-Mediums zu unterbrechen.
– Beim Hantieren mit Veracrypt-Containern werden Sie zusätzlich zum Containerpasswort stets auch nach dem sudo-Kennwort gefragt werden, das mit dem Veracrypt-Passwort nichts zu tun hat und vermutlich anders lautet. Unter Windows geschieht mit der Abfrage der Benutzerkontensteuerung im Prinzip technisch dasselbe, kann aber dort zu keinen Irritationen führen, weil kein Passwort verlangt wird.



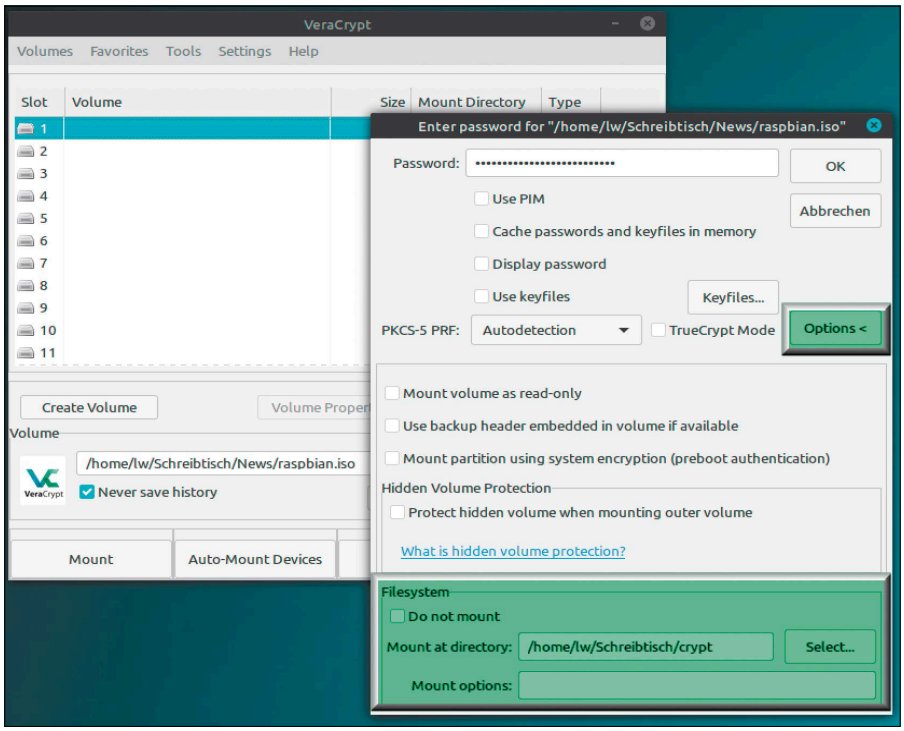
Im Zweifel NTFS: Die Auswahl eines kompatiblen Dateisystems ist zweimal wichtig – einmal für den Datenträger selbst (bei USB-Medien), zum andern für das interne Containerformat.

ist der Container einsatzbereit. Um den Container zu verwenden, navigieren Sie mit „Select File“ im Hauptdialog zur Containerdatei. Mit Klick auf „Mount“ wird diese im Dateimanager geöffnet. Linux mountet Container standardmäßig (aber nicht zwangsläufig) nach „/media/veracrypt [nummer]“, Windows auf freie Laufwerksbuchstaben. Auf diesen Datenträgern lesen und arbeiten Sie wie auf einem normalen Laufwerk. Die Schaltfläche „Dismount“ im Hauptdialog entlädt den Container, der somit wieder geschützt ist.

Optionen für erhöhte Sicherheit

Bei der Passwortvergabe haben wir bisher zwei Optionen übergangen. Interessant sind sie durchaus, aber sie erhöhen die Komplexität.

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 Kennwort zum Öffnen dieses Containers nicht mehr. Zusätzlich ist 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 beim Erreichen des genauen PIM-Werts den Entschlüsselungsheader generieren. Achtung: Ein hoher PIM-Wert (vier- und fünfstellig) verlangsamt den Mountvorgang deutlich.



Optionen ohne Ende: Manche interessante Veracrypt-Funktion erschließt sich erst beim zweiten Blick, so etwa, dass die Linux-Version einen Container in jeden beliebigen Pfad laden kann.

Container mit Passwort und Keyfile: Der Passwortdialog hält eine weitere Möglichkeit parat – nämlich die „Keyfiles“ (Schlüsseldateien). Dabei kann es sich um eine oder mehrere beliebige Datei(en) 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. Der Inhalt der Schlüsseldatei darf sich also keinesfalls ändern, das Verzeichnis oder der Dateiname jedoch durchaus. Ideale Kandidaten für Schlüsseldateien sind Binärdateien, PDFs oder ISO-Images, die normalerweise nie geändert werden.

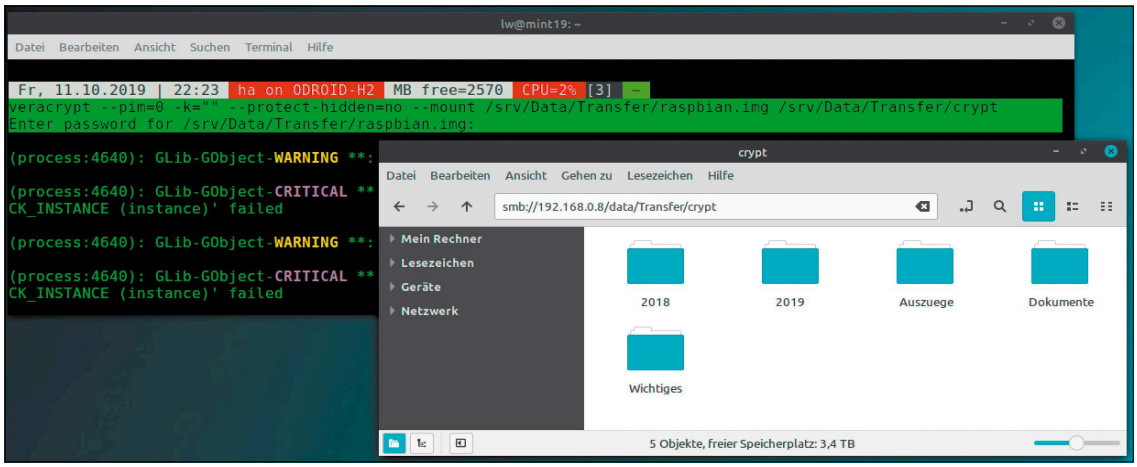
Ein Keyfile ist wie die PIM-Zahl additiv: Es ersetzt nicht das Passwort, sondern muss zusätzlich vorliegen. Das Keyfile kann ein schwächeres Kennwort rechtfertigen und die Kennworteingabe verkürzen.

Zum passenden Keyfile müssen Sie zum Öffnen eines Containers normalerweise über die Schaltfläche „Keyfiles“ manuell navigieren. Jedoch gibt es auch die Option, über „Settings → Default Keyfiles“ auf einem Rechner eine Standarddatei zu verwenden. Diese berücksichtigt Veracrypt dann automatisch – ohne manuelle Auswahl.

Schaltfläche „Volume Tools“: Für einen geladenen Container lassen sich alle bisherigen Einstellungen nachträglich ändern. Das erledigen Sie im Hauptfenster über „Volume Tools“. Sie können ein neues Passwort vergeben oder Keyfiles hinzufügen oder entfernen. Beachten Sie, dass die Aktion noch einmal eine korrekte Anmeldung mit den bisherigen Daten erfordert.

Container im Netzwerk

Verschlüsselte Daten im Netzwerk freizugeben, scheint paradox. Im privaten Heimnetz ist das aber nicht nur praktikabel, sondern auch komfortabel, weil die Veracrypt-Container dann an zentraler Stelle liegen und von Linux- wie Windows-Rechnern bearbeitet werden können. Im Prinzip gibt es zwei Möglichkeiten:



Veracrypt-Container im Netz: Wenn Veracrypt am Server läuft, kann dieser via SSH den Container auf eine Samba-Freigabe mounten. Im Heimnetz ist das sicher zu vertreten.

A. Der verschlüsselte Container liegt auf einer Samba- oder Windows-Freigabe des Servers und wird am Clientrechner mit Veracrypt gemountet.

Dies wäre die sicherste Möglichkeit, hat aber zu viele Einschränkungen. Unter Linux müsste dazu die komplette Samba-Freigabe vorher ordentlich ins Dateisystem gemountet werden. Und selbst wenn dabei alle Rechteprobleme ausgeräumt würden, könnte Veracrypt den Container nur für Lesezugriff laden.

B. Der verschlüsselte Container wird auf dem Server selbst mit Veracrypt gemountet, und zwar in einen Ordner auf einer bestehenden Samba-Freigabe. Diese zweite Möglichkeit ist unkomplizierter, hat keine Beschränkungen, ist aber auch unsicherer: Solange der Container auf die Freigabe gemountet ist, haben die Samba-Berechtigten auf die Daten Zugriff.

Es ist letztlich eine Frage der Netzwerkrechte und der Menge der Netzteilnehmer, ob diese Möglichkeit in Betracht kommt. Im Privatnetz sollte wenig dagegen sprechen. Die notwendigen Zutaten dieser Variante B sind folgende:

1. Als Server kommt nur Linux ernsthaft infrage: Sie benötigen nämlich SSH-Zugriff (also einen laufenden Open-SSH-Server) und eine Samba-Freigabe (Samba-Server). Das ließe sich mit Windows-Freigabe und Remotesteuerung auch realisieren, jedoch benötigt der Server außerdem ein installiertes Veracrypt. Und ungeachtet mancher Defizite der Linux-Variante hat Veracrypt unter Linux einen entscheidenden Vorteil: Es kann den Containerinhalt in jedes beliebige Verzeichnis mounten („Mount → Options → Mount at directory“ oder per Kommandozeile, siehe unten).

2. Den Veracrypt-Container erstellen Sie auf dem Server selbst oder kopieren einen existierenden auf den Server.

3. Sie mounten den Container bei Bedarf auf dem Server auf die Samba-Freigabe. Da sämtliche Veracrypt-Aktionen auch als Terminalkommando zu erledigen sind, geschieht das am einfachsten über SSH auf der Kommandozeile – im Prinzip:

```
ssh [server-ip]
veracrypt --mount [Containerdatei]
  [Mountpunkt_auf_Samba_Freigabe]
```

Achtung: Die Anmeldung am Server und das Mounten des Containers muss mit einem Systemkonto geschehen, das sowohl Zugriff auf die Samba-Freigabe besitzt als auch sudo-Berechtigung (notwendig zum Mounten von Veracrypt-Containern).

Der Befehl fragt allerdings auch weitere Zugangsmethoden wie PIM und Schlüsseldateien ab. Wenn nur ein Passwort genutzt wird, unterdrücken Sie alle weiteren Abfragen mit diesem Befehl (konkretes Beispiel):

```
ssh ha@192.168.0.8
veracrypt --pim=0 -k="" --protect-
  hidden=no --mount /srv/Data/
  crypt.iso /srv/Data/crypt
```

Nicht wundern: Während hier alle anderen Veracrypt-Schalter in der ausführlichen Form mit Doppelbindestrich geschrieben sind, benötigt der Keyfiles-Schalter offenbar die Kurzform „-k“. Der lange Befehl ist natürlich ein Kandidat für ein Bash-Alias, das die Sache abkürzt. Der Pfad „/srv/Data“ in diesem Beispiel wäre per Samba freigegeben und somit die Containerdaten anschließend im Unterverzeichnis „crypt“ für berechtigte Samba-Konten zugänglich.

4. Nach der Bearbeitung der verschlüsselten Daten entlädt der Befehl (wieder auf dem Server via SSH)

```
veracrypt --dismount
```

alle Veracrypt-Container. Ist ein Container gerade in aktiver Benutzung, erscheint womöglich eine Fehlermeldung. Dies können Sie mittels

```
veracrypt --force --dismount
```

zwar ignorieren, aber es empfiehlt sich, das betreffende zugreifende Programm (oft nur der Dateimanager auf einem Samba-Client) zu beenden und dann den normalen Entladebefehl aufzurufen. ■

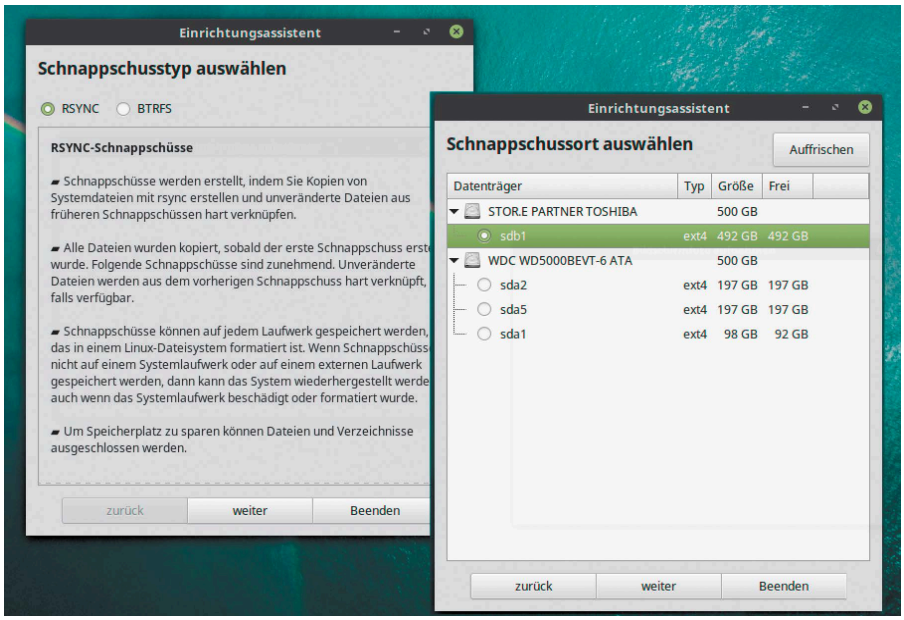
PARANOIA? VERSTECKTE VOLUMES!

Im Formatassistenten 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 anderes Kennwort erhält. Nutzt man beim späteren Mounten 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.

Die besten Systemschutzmaßnahmen

Datensicherung ist unbeliebt, aber ein notwendiges Übel jeder großen wie kleinen IT-Infrastruktur. Mit den richtigen Tools kostet aber nur die erste Einrichtung oder die Kommandorecherche Zeit. Danach läuft das Meiste automatisch ab.

VON HERMANN APFELBÖCK



Einrichten der Timeshift-Sicherung: Ein unabhängiger Datenträger ist als Backupziel ideal, der muss aber bei automatischer Sicherung nach Zeitplan immer verfügbar sein.

Mit Linux sind Sie gegen Schadsoftware so gut wie immun, doch mit Benutzerfehlern und Havarien müssen Sie auch hier rechnen. Versehentliches Löschen, Konfigurationsfehler, misslungene Upgrades oder Festplattendefekte verursachen Datenverluste. Dagegen hilft nur eine gesunde Redundanz: Sorgen Sie dafür, dass Sie alle wichtigen Dateien und Ordner ein zweites oder drittes Mal vorfinden.

Systemschutz (1): Timeshift

Das Sicherungswerkzeug Timeshift ist unter Linux Mint Standard. Es erstellt Momentaufnahmen des Dateisystems, die beim Zurückspielen einen früheren Zustand wiederherstellen. Unter Ubuntu ist es nicht Standard, aber eine empfehlenswerte Ergänzung. Timeshift liegt fast überall in den Standardpaketquellen und ist mit

```
sudo apt install timeshift
```

schnell nachinstalliert.

Der erste Sicherungspunkt ist ein komplettes Backup der Systemverzeichnisse. Weitere Wiederherstellungspunkte fallen dann viel kleiner aus, da Timeshift nur noch geänderte Dateien speichert. Der Rest wird per Hardlinks abgebildet. Folgesicherungen haben nur scheinbar den im Dateimanager angezeigten großen Speicherbedarf.

Die Einrichtung: Timeshift fordert beim Start immer das sudo-Kennwort, da es Zugriff auf alle Ordner benötigt. Beim ersten Start wird der „Schnappschusstyp“ abgefragt („RSYNC“). Im nächsten Schritt geht es um den „Schnappschussort“, also um den Zieldatenträger der Sicherung. Timeshift bietet alle Partitionen mit Linux-Dateisystem an (notwendig wegen der Hardlink-Technik). Besser als die Systempartition selbst ist ein unabhängiger zweiter Datenträger, der dann aber immer zur Verfügung stehen muss, wenn Sie einen automatisierten Timeshift-Plan verwenden. Im letzten Schritt definieren Sie einen Zeitplan („Schnappschussebenen“) und die Menge der gespeicherten Systempunkte. Auf einem normal genutzten Desktop sollten wöchentliche Sicherungen und drei bis fünf aufbewahrte Sicherungspunkte genügen, aber das lässt sich beliebig steigern. Getroffene Einstellungen können Sie später jederzeit ändern. Mit der Schaltfläche „Erstellen“ können Sie auch jederzeit einen Sicherungspunkt manuell auslösen.

Wiederherstellen: Die Backups bestehen aus unkomprimierten Ordnern und Dateien unter „/timeshift/snapshots“. Einzelne Dateiobjekte oder der komplette frühere Zustand lassen sich daher mit jedem Livesystem rekonstruieren, falls das primäre System nicht mehr funktioniert – im Prinzip auch ohne Timeshift. Noch bequemer geht's aber mit Timeshift selbst: Das Tool zeigt in seiner Liste alle Sicherungspunkte. Mit „Wiederherstellen“ schreiben Sie einen markierten Punkt zurück. Die Partitionsdaten werden im Fenster „Ziellaufwerk auswählen“ noch einmal explizit abgefragt.

Systemschutz (2): Clonezilla-Images

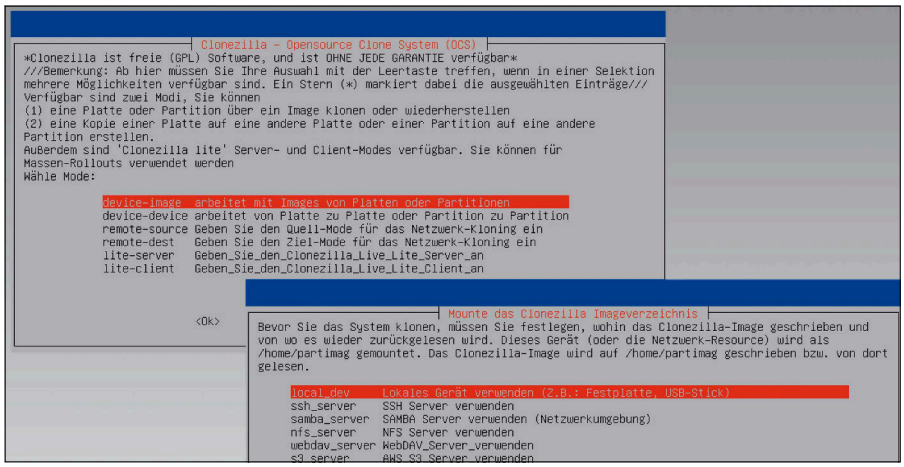
Mit Clonezilla erstellen Sie Abbilder von Festplatten oder klonen den Inhalt einer

Festplatte direkt auf eine zweite. Das Livesystem beziehen Sie über *http://clonezilla.org* (260 MB). Clonezilla ist textbasiert, hat aber eine pseudo-grafische Oberfläche. Mit den Pfeiltasten navigieren Sie im Menü und bestätigen die Auswahl mit Eingabetaste. Mit der Tabulator-Taste wechseln Sie zwischen Schaltflächen wie „OK“ und „Cancel“. Soll die Sicherung auf eine USB-Festplatte erfolgen, schließen Sie diese vorher an.

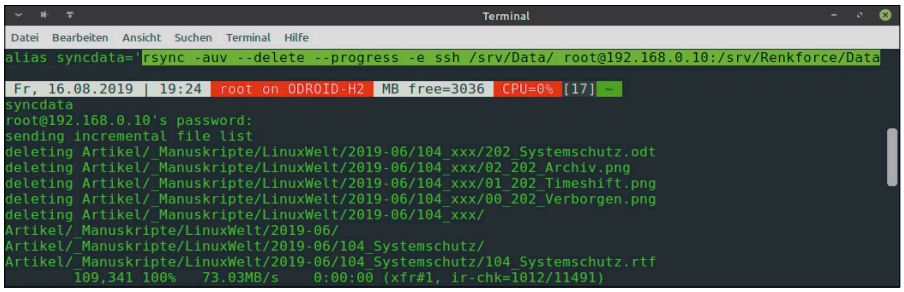
Abbildsicherung: Im gebooteten Clonezilla wählen Sie für ein Imagebackup die Option „device-image“ und danach „local_dev“. Geben Sie die Festplatte an und danach das Verzeichnis, wohin Sie das Abbild speichern wollen. Wählen Sie „Beginner“ und „savedisk“ und geben Sie einen Dateinamen für das Image an. Die spätere Wiederherstellung eines Abbilds läuft entsprechend ab. Nach „Beginner“ wählen Sie „restoredisk“, danach die gewünschte Abbilddatei und dann die Zielfestplatte.

Direktkopien: Für eine Direktkopie von einer Festplatte auf eine zweite wählen Sie „device-device“, danach „Beginner“ und „disk_to_local_disk“. Bestimmen Sie dann die Festplatte, die Sie kopieren möchten. Bei der Systemfestplatte handelt es sich in der Regel um „sda“. Nach „OK“ wählen Sie die Zielfestplatte. Wenn sich nur zwei Festplatten im PC befinden, ist dies „sdb“. Bestätigen Sie diese Auswahl und auch die nächsten beiden Meldungen mit der Eingabetaste. Sie erhalten dann eine zusammenfassende Meldung über die ausgewählten Festplatten. Prüfen Sie die Angaben genau, um ja nicht Quelle und Ziel zu verwechseln. Bei startfähigen Festplatten fragt Clonezilla automatisch, ob Sie auch die Startumgebung („boot loader“) kopieren möchten. Bestätigen Sie dies mit „y“ und Eingabetaste.

Hinweis: Bei einer Direktkopie muss die Zielfestplatte mindestens die Kapazität des Quelllaufwerks besitzen. Ist das Ziellaufwerk größer, sollten Sie nachträglich die Partitionsgröße ausdehnen, um die Festplatte komplett zu nutzen. Dies erledigen Sie am besten mit Gparted in einem Livesystem (etwa Linux Mint 19.3 auf Heft-DVD). Über „Größe ändern/verschieben“ lässt sich die Partition ausdehnen.



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



Spiegelsynchronisierung mit Rsync: Solche 1:1-Kopie mit Löschschalter ist nur zu empfehlen, wenn das Backupziel nie direkt bearbeitet wird (in der Abbildung eine Sicherung via SSH von Server zu Server).

Datenbackups mit Rsync

Theoretisch kann Timeshift auch zur Sicherung der Home-Verzeichnisse eingesetzt werden („Einstellungen → Benutzer“). Dies halten wir aber bei großen Datenbeständen unter „/home“ für keine gute Idee, weil es den Zeitaufwand und die Schnappschussgrößen für Timeshift erheblich aufbläht. Für Benutzerdateien sind Backups oder Synchronisierungen mit Rsync erste Wahl. Rsync sichert auf interne und externe Laufwerke, auf Freigabeordner, auf Netzwerk- oder Webserver, auf denen der SSH-Server läuft. Rsync hat reichlich Schalter zu bieten, doch fasst die Option „-a“ häufig benötigte Funktionen zusammen. Damit erreichen Sie rekursives Kopieren aller Unterverzeichnisse:

```
rsync -a /home/ha/ /media/ha/usb/
  backup
```

Das Beispiel geht davon aus, dass ein USB-Laufwerk mit dem Label „usb“ unter „/media/ha“ eingehängt ist. Dies ist das Ziellaufwerk der Sicherung. Das angegebene Verzeichnis („backup“) wird automatisch erstellt, sofern es noch nicht existiert. Das erste – nach den Schalteroptionen – angegebene Verzeichnis ist der Quellordner. Beachten Sie den abschließenden Slash (/). Nur so landen alle Sicherungsdaten direkt im Zielordner „backup“.

Von weiteren Rsync-Schaltern sind mindestens drei unentbehrlich: Mit

```
rsync -av --delete /home/ha/ /
  media/ha/usb/backup
```

erzeugen Sie bei periodischer Sicherung eine Mirror-Kopie. Was unter der Quelle „/home/ha“ seit dem letzten Kopiervorgang gelöscht wurde, wird auch auf dem Ziel gelöscht. Mit falschen Pfadangaben wäre das fatal. Ein Testlauf mit „--dry-run“

```
rsync -av --delete –dry-run /home/
  ha/ /media/ha/usb/backup
```

zeigt alle zu erwartenden Aktionen, ohne sie tatsächlich auszuführen. Schalter „-u“ spart bei periodischen Sicherungen Zeit (*rsync -auv …*), weil er bereits bestehende Dateien überspringt.

Sicherung via SSH: Rsync kann von jedem Rechner im Netzwerk Daten beziehen oder dorthin kopieren, wo ein SSH-Server läuft. Die Sicherung folgt diesem Schema

```
rsync -av -e ssh ha@192.168.0.66:/
  home/ha/Bilder/ /home/ha/Bilder
```

oder auch mit

```
rsync -auv --delete -e ssh /var/www/
  root@192.168.0.8:/var/www/
```

in die andere Richtung. ■

Software und Paketverwaltung

Neue Anwendungen und Updates beziehen Sie unter Linux in der Regel aus dem Softwarerepository der jeweiligen Distribution. Für die Verwaltung gibt es mehrere Tools mit unterschiedlichen Funktionen.

VON THORSTEN EGGELING



Fast alle Linux-Distributionen verwenden eine zentrale Paketverwaltung, über die Sie die gewünschte Software beziehen, installieren und aktualisieren. Die Vorteile: Sie erhalten geprüfte und virenfreie Programmpakete, die reibungslos mit dem Betriebssystem zusammenarbeiten. Sicherheitsupdates gibt es automatisch für jedes installierte Programm.

Es gibt aber auch Nachteile. Bei Distributionen wie Ubuntu, Linux Mint oder Debian sind Sie in der Regel auf die Programmversionen festgelegt, die zur jeweiligen Version des Betriebssystems gehören. Neuere Versionen gibt es erst beim nächsten Upgrade der Distribution. Ausnahmen sind beispielsweise Firefox und Thunderbird. Wer aktuellere Programme benötigt oder in der Paketverwaltung nicht fündig wird, kann jedoch zusätzliche Paketquellen einbinden oder Software auf anderen Wegen installieren (siehe Artikel ab Seite 154 und 156).

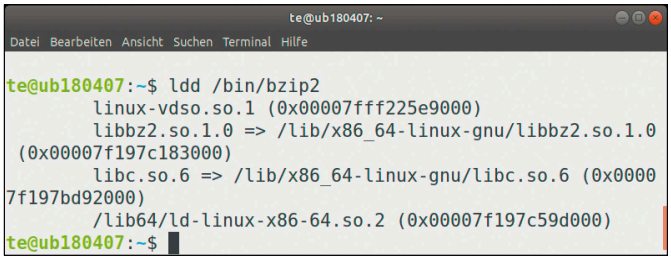
Für die Paketverwaltung bieten Ubuntu und verwandte Distributionen mehrere Tools für unterschiedliche Zielgruppen und mit unterschiedlichen Funktionen. Teilweise ist es Geschmackssache, welchem Programm der Vorzug zu geben ist. Es gibt aber auch Aufgaben, die sich nur mit einem bestimmten Tool erledigen lassen.

1. Programme und Bibliotheken

Ausführbare Programmdateien enthalten unter Linux in der Regel nicht alle nötigen Komponenten. Meist ist zusätzlich wenigstens eine Standardbibliothek erforderlich, die Funktionen für in der Programmiersprache C geschriebene Programme enthält. Genauere Informationen liefert beispielsweise diese Befehlszeile:

```
ldd /bin/bzip2
```

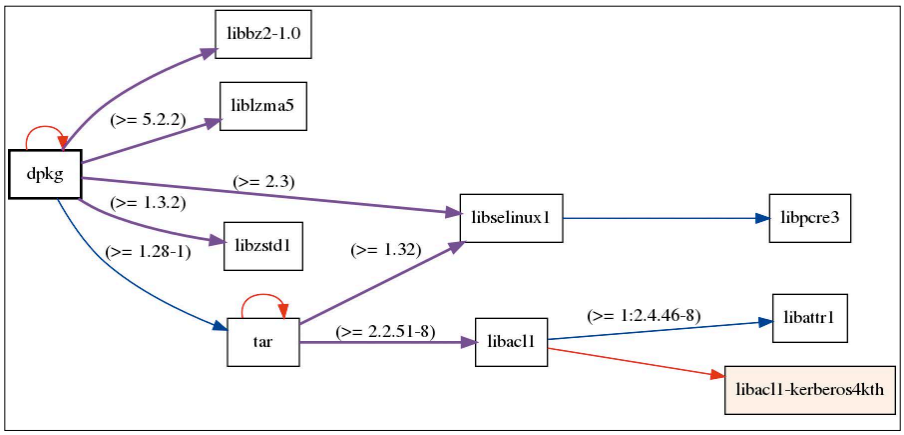
In der Ausgabe sehen Sie alle Programmbibliotheken, die das Komprimierungstool bzip2 benötigt. Darunter ist die Standardbibliothek „libc.so.6“ zu finden, „linux-vdso.so.1“ stellt einige Kernel-Funktionen bereit und „ld-linux-x86-64.so.2“ ermöglicht es, Bibliotheken bei Bedarf zu laden („dynamic shared“). Die Komprimierungsfunktion ist in der Bibliothek „libbz2.so.1.0“ zu finden, die auch andere Programme nutzen können. Programme benötigen genau die Bibliotheken, mit den denen sie erstellt wurden, oder eine höhere, abwärtskompatible Version. Das Konzept der dynamisch ladbaren, gemeinsam genutzten Bibliotheken verringert die Größe der Programmdateien und ermöglicht eine effiziente Hauptspeichernutzung.



Abhängigkeiten: Die meisten Programme benötigen zusätzliche Bibliotheken. Die Paketverwaltung sorgt für die automatische Installation der abhängigen Pakete.

2. Das Debian-Paketformat

Bei Installation oder Update lädt die Paketverwaltungssoftware bei Debian/Ubuntu-Systemen eine „deb“-Datei herunter. Es handelt sich um ein gepacktes Archiv, das ausführbare Dateien, Bibliotheken und Konfigurationsdateien enthalten kann, die bei der Installation in das Dateisystem kopiert werden. Ebenfalls enthalten sind meist einige Scripts, über die sich beim Setup beispielsweise Konfigurationsdateien anpassen oder Systembenutzer erstellen lassen. Ein weiterer Bestandteil ist eine Textdatei mit Informationen über die Abhängigkeiten von anderen Paketen sowie optionalen Empfehlungen für zusätzliche Pakete.



Dependency Tree: Damit ein Linux-Programm läuft, sind meist zusätzliche Tools und Bibliotheken ab einer bestimmten Version erforderlich. Welche das sind, lässt sich mit debtree ermitteln.

3. Die Paketverwaltung bei Ubuntu

Bei der Softwareinstallation muss die Paketverwaltung die ausführbaren Dateien auf die Festplatte kopieren und dafür sorgen, dass alle benötigten Bibliotheken und Tools vorhanden sind. Bei komplexeren Programmen ergibt sich ein verzweigter Baum von Abhängigkeiten („dependency tree“) und die Paketverwaltung installiert mehrere Pakete.

Wer es genauer wissen möchte, kann mit dem Befehl

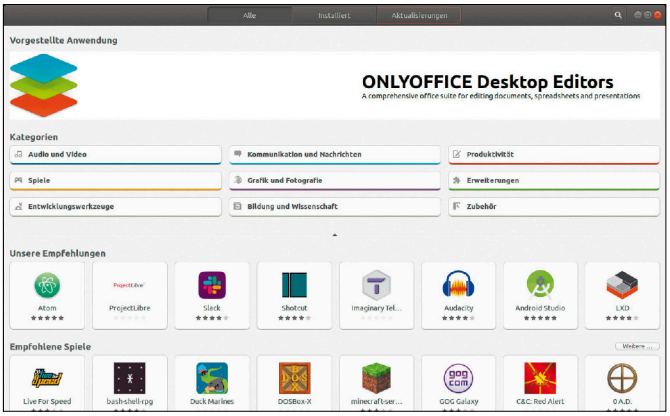
```
debtree [Paketname] | dot -Tpng >
 bild.png
```

eine grafische Darstellung der Abhängigkeiten eines Pakets erstellen. Die Pakete „debtree“ und „graphviz“ müssen dafür installiert sein.

Das zentrale Programm zur Paketverwaltung heißt unter Ubuntu und verwandten Systemen dpkg. Es verwendet Datenbanken, in denen verfügbare und installierte Pakete gespeichert sind. dpkg lädt jedoch keine Paketdateien herunter und prüft keine Abhängigkeiten. Deshalb werden Sie das Tool nur selten direkt nutzen (siehe auch ab Seite 154). Stattdessen verwenden Sie eines der Programme, die wir in den nächsten Punkten beschreiben.

4. Die Standard-Paketverwaltung von Ubuntu

Anwendungen für die grafische Oberfläche lassen sich in Ubuntu mit Ubuntu-Software installieren, entfernen und aktualisieren. Sie starten es über das Icon in der Starterleiste. Auf der Registerkarte „Alle“ zeigt das Tool Kategorien wie „Audio und Video“ und „Grafik und Fotografie“. Klicken Sie eine Kategorie an und stöbern Sie in der Liste nach für Sie interessanten Anwendungen. Wenn Sie den Namen eines Programms kennen, können Sie auch die Suchfunktion verwenden (Lupensymbol auf der Startseite). Empfehlenswert ist auch ein Blick in die



Programme installieren: Ubuntu-Software ermöglicht eine komfortable Programmauswahl. Das Angebot ist hier aber nicht vollständig und enthält beispielsweise keine Terminaltools.

PAKETVERWALTUNG IN ANDEREN DISTRIBUTIONEN

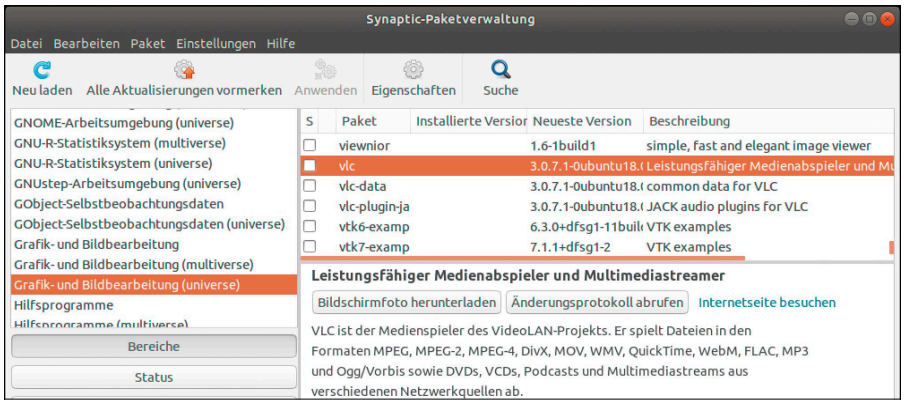
Bei allen verbreiteten Linux-Distributionen erfolgt die Paketverwaltung ähnlich wie bei Debian/Ubuntu. Es gibt jedoch andere Paketformate und Tools für deren Verwaltung. Bei Fedora dient Gnome-Software als Standardtool, das auch die Basis von Ubuntu-Software bildet. Nutzer des KDE-Desktops nutzen Plasma Discovery. Im Terminalfenster kommt hier dnf, der Nachfolger von yum, zum Einsatz. dnf ähnelt in der Bedienung apt. Für die Installation beispielsweise verwendet man

```
sudo dnf install [Paketname]
```

Als Paketformat verwendet Fedora RPM (RPM Package Manager, früher Red Hat Package Manager). RPM wird auch von Open Suse genutzt, zur Paketverwaltung dient hier Yast2 und auf der Kommandozeile Zypper.

Auch Gentoo Linux kennt eine Softwareverwaltung, die allerdings etwas anders funktioniert. Das Tool emerge greift auf einen täglich aktualisierbaren Portage-Tree zu, in dem Infos zu Quelltextarchiven und Abhängigkeiten hinterlegt sind. Bei der Installation werden die Binärdateien aus dem Quelltext erstellt. Das ermöglicht sehr aktuelle Softwareversionen, birgt aber auch ein hohes Fehlerpotenzial. Letztlich ist der Benutzer selbst dafür verantwortlich, dass alles reibungslos zusammenpasst.

Kategorie „Erweiterungen“. Hier finden Sie neue Schriftarten und nützliche Shell-Erweiterungen.
Ein Klick auf das Programmsymbol führt zu weiteren Informationen (häufig mit Screenshot), Beschreibungen und Rezensionen. Unter „Details“ erfahren Sie jeweils, um welchen Pakettyp es sich handelt. Wenn hinter „Quelle“ beispielsweise „ubuntu-bionic-universe“ oder ähnlich steht, handelt es sich um ein herkömmliches „deb“-Paket. Sollte die Angabe „Snap-Store“ lauten, dann handelt es sich um einen Snap-Container (siehe ab Seite 154).
Klicken Sie auf „Installieren“, um eine Software einzurichten. Sollte diese bereits vorhanden sein, sehen Sie die Schaltflächen „Starten“ und „Entfernen“. Die Registerkarte „Installiert“ (Startseite) zeigt Ihnen eine Liste der installierten Anwendungen, per Klick auf „Entfernen“ können Sie ein Programm deinstallieren. Auf der Registerkarte „Aktualisierungen“ sehen Sie die verfügbaren Updates. Klicken Sie auf die Schaltfläche links oben im Fenster, um die Paketdatenbank zu aktualisieren.



Alles installieren: Synaptic bietet eine schnelle Suche nach allen verfügbaren Anwendungen, Tools und Bibliotheken. Software lässt sich außerdem über „Bereiche“ auswählen.

5. Softwarepakete mit Synaptic verwalten

Synaptic ist bei Linux Mint 19 bereits vorinstalliert, Ubuntu-Nutzer können das Tool über Ubuntu-Software nachinstallieren. Synaptic bietet eine Suchfunktion und mehrere Filter, über die sich die Ansicht auf die gewünschte Software einschränken lässt. Das Tool ist im Vergleich zu Ubuntu-Software etwas unübersichtlicher, dafür liefert aber die Suche schnellere Ergebnisse. Anders als mit Ubuntu-Software lassen sich mit Synaptic alle verfügbaren Programme installieren, also auch Tools für die Kommandozeile, Bibliotheken und Entwicklerpakete.
Nach dem Start von Synaptic klicken Sie zuerst auf „Neu laden“, um die Paketdatenbank zu aktualisieren, und danach auf die Schaltfläche „Suche“. Tippen Sie einen Suchbegriff ein und klicken Sie auf „Suchen“. Sie können den Namen eines Programms verwenden oder einen Begriff, der in der Beschreibung vorkommen sollte. Synaptic kann auch alle verfügbaren Programme aus einer Kategorie anzeigen. Dazu klicken Sie auf „Bereich“ und wählen beispielsweise „Grafik- und Bildbearbeitung“. In der Regel ist alles aus dieser Kategorie bereits installiert. Weitere Software gibt es unter „Grafik- und Bildbearbeitung (universe)“ sowie „Grafik- und Bildbearbeitung (multiverse)“. Programme aus dem Bereich „multiverse“ unterliegen lizenzrechtlichen Einschränkungen, was beispielsweise für Multimedia-Codecs gelten kann. In der Kategorie „universe“ ist freie Software ohne solche Einschränkungen zu finden. Für Endanwender in Deutschland hat diese Unterscheidung jedoch keine Konsequenzen. Sie können alle installierbaren Programme uneingeschränkt und kostenlos nutzen. Es kann jedoch Länder oder Einsatzbereiche geben, die Programme aus dem Bereich „multiverse“ nicht erlauben.
Software installieren und entfernen: Wenn Sie fündig geworden sind, klicken Sie das gewünschte Paket mit der rechten Maustaste an und wählen „Zum Installieren vormerken“. In der Regel öffnet sich ein Fenster, das eine Liste mit weiteren erforderlichen Paketen anzeigt. Klicken Sie auf „Vormerken“ und danach in der Synaptic-Symbolleiste auf „Anwenden“. Das Fenster „Zusammenfassung“ zeigt ihnen die anstehenden Änderungen. Klicken Sie auf „Anwenden“, um die Installation anzustoßen.
Für die Deinstallation wählen Sie im Kontextmenü eines Pakets „Zum Entfernen vormerken“ und klicken danach auf „Anwenden“. Prüfen Sie im Fenster „Zusammenfassung“ die Angaben unter „Zu entfernen“. Hier sollten nur das gewählte Paket und wenige weitere Pakete aufgeführt sein.

PROBLEME BEI DER INSTALLATION BEHEBEN

Bei der Vielzahl der Softwarepakete ist nicht ausgeschlossen, dass es bei Installationen oder Updates zu Fehlern kommt. Meist sind nur Pakete betroffen, die selten installiert werden und nicht ausreichend gepflegt sind. Die Installation kann beispielsweise fehlschlagen, wenn eine Abhängigkeit besteht, die nicht erfüllt werden kann. Das Problem lässt sich meist mit

```
sudo apt-get -f install
```

lösen. Dabei wird das defekte Paket entfernt. Sollte das nicht funktionieren, verwenden Sie

```
sudo dpkg -r [Paketname]
```

Damit löschen Sie das Paket ohne Prüfung der Abhängigkeiten.
Bei Problemen mit Abhängigkeiten können Sie nur darauf warten, dass der Paketbetreuer den Fehler behebt. Oder Sie suchen nach einer alternativen Quelle für die Software (siehe ab Seite 154).
Eine häufige Fehlermeldung bei der Verwendung von apt ist „Konnte Sperre /var/lib/dpkg/lock-frontend nicht bekommen“ oder ähnlich. Ursache dafür ist meist ein automatisches Update im Hintergrund. Warten Sie einige Zeit, bis das Update abgeschlossen ist, und versuchen Sie es dann erneut. Die Meldung erscheint auch, wenn ein anderes Tool die Paketverwaltung gesperrt hat (beispielsweise Synaptic) oder wenn Sie apt ohne vorangestelltes „sudo“ starten.

Ist die Liste sehr lang, besteht die Gefahr, dass wichtige Pakete dabei sind, und die Deinstallation die Funktionen des Betriebssystems beeinträchtigt. In diesem Fall sollten Sie die Deinstallation besser abbrechen. Bei systemrelevanten Programmen gibt Synaptic ohnehin eine Warnmeldung aus. Die Frage „Sind Sie sicher, dass Sie das tun wollen?“ sollte Sie immer alarmieren und ist besser mit „Nein“ zu beantworten.

Im Kontextmenü gibt es außerdem den Punkt „Zum vollständigen Entfernen vormerken“. Damit entfernen Sie Programmdateien inklusive Konfiguration. Verwenden Sie diese Funktion, wenn Sie ein Programm auch in Zukunft nicht mehr verwenden wollen oder wenn Sie Fehler in der Konfiguration vermuten, die sich auch nach einer Neuinstallation auswirken können. Synaptic löscht jedoch nur die systemweite Konfiguration. Konfigurationsdateien in den Benutzerverzeichnissen unter „/home“ müssen Sie manuell entfernen.

6. Softwarepakete im Terminalfenster verwalten

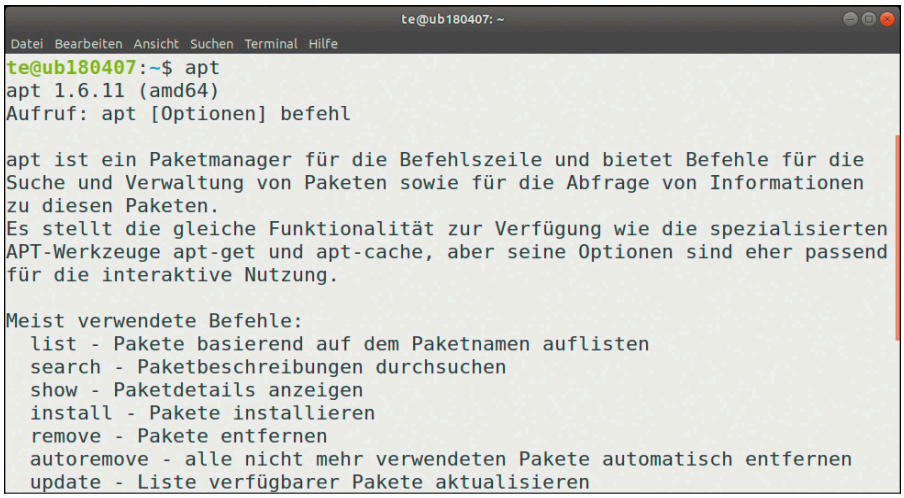
Bei der SSH-Fernwartung eines Servers im Netzwerk sind Sie auf Kommandozeilentools angewiesen. Diese leisten aber auch auf einem Arbeitsrechner gute Dienste, weil Installationen über die Kommandozeile schneller und bequemer ablaufen als über die Tools für die grafische Oberfläche. Meist werden Sie unter Ubuntu, Linux Mint oder Debian das Tool apt einsetzen. Starten Sie es in einem Terminalfenster ohne weitere Optionen, um einen kurzen Hilfetext zu erhalten. Für die Installation einer Software verwenden Sie

```
sudo apt update
sudo apt install [Paketname]
```

Die erste Zeile aktualisiert die Paketdatenbank, die zweite installiert das im Platzhalter „[Paketname]“ angegebene Paket. Sie können auch mehrere Paketnamen hintereinander verwenden – durch schlichtes Leerzeichen getrennt. Für die Deinstallation verwenden Sie

```
sudo apt remove [Paketname]
```

Auch hier sollten Sie vorsichtig sein, wenn apt mehr als ein Paket entfernen möchte. apt gibt jedoch eine deutliche Warnung aus, wenn Sie versuchen, systemrelevante Pakete zu entfernen. Wenn bei der Deinstallation unnötige Pakete zurückbleiben, gibt apt eine Liste unter „Die folgenden Pakete wurden automatisch installiert und



Schnelle Paketverwaltung: apt ist im Terminal einfach zu verwenden und bietet den meisten Komfort, wenn Sie mehrere Programme auf einmal einrichten wollen (apt install [Paketnamen]).

werden nicht mehr benötigt:“ aus. Diese Pakete lassen sich mit

```
sudo apt autoremove
```

entfernen. Diesen Befehl sollten Sie in regelmäßigen Abständen verwenden, besonders nach mehreren Kernel-Updates. Wenn der aktuelle Kernel stabil läuft, entfernen Sie damit alte Kernel-Pakete, was Platz auf der Festplatte einspart. Mit dem Befehl

```
apt list [Suchmuster]
```

können Sie nach Softwarepaketen suchen. Verwenden Sie für den Platzhalter „[Suchmuster]“ beispielsweise *gimp*. apt gibt dann alle Paketnamen aus, in denen „gimp“ an beliebiger Stelle vorkommt. Entsprechendes leistet

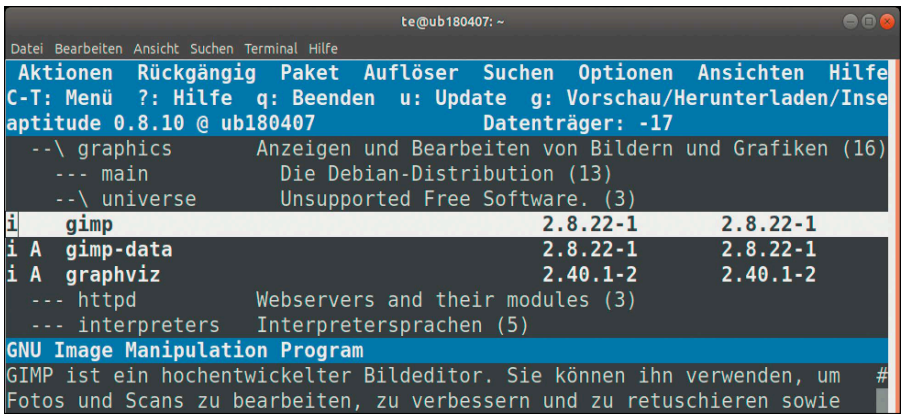
```
apt search [Suchmuster]
```

für die Suche in den Paketbeschreibungen. Das Kommandozeilentool apt-get bietet alle für apt beschriebenen Funktionen und noch ein paar mehr. Es gibt beispielsweise „purge“ für die vollständige Entfernung von Paketen und „download“, wenn Sie ein „deb“-Paket vorerst nicht installieren, sondern nur herunterladen wollen. Ebenfalls nützlich ist dieser apt-Befehl:

```
sudo apt-get clean
```

Dies löscht den Paketcache und räumt damit Festplattenplatz frei.

Wer eine Paketverwaltung mit Menüsteuerung im Terminal bevorzugt, kann aptitude installieren. Das Menü rufen Sie per Strg-T auf. Alternativ verwenden Sie Tastaturkürzel, die aptitude bei den einzelnen Menüpunkten anzeigt. Drücken Sie die Taste „/“, um nach Paketen zu suchen, und die Taste „N“ für „Weitersuchen“. Mit der Plus-Taste („+“) markieren Sie ein Paket für die Installation, dann drücken Sie die Taste „G“ für eine Vorschau der Änderungen und noch einmal die Taste „G“, um die Installation durchzuführen. Über die Minus-Taste („-“) lassen sich Pakete für die Deinstallation auswählen. ■



Alternative fürs Terminal: aptitude ist nicht besonders übersichtlich, bietet aber im Terminal eine menügeführte Paketverwaltung mit Programminfos und eine Suchfunktion.

Container statt Pakete

Wer neuere Programmversionen nutzen oder ausprobieren möchte, verwendet Software im Container. Seit Version 16.04 ist Ubuntu dafür standardmäßig vorbereitet. Linux Mint bevorzugt das Flatpak-Format.

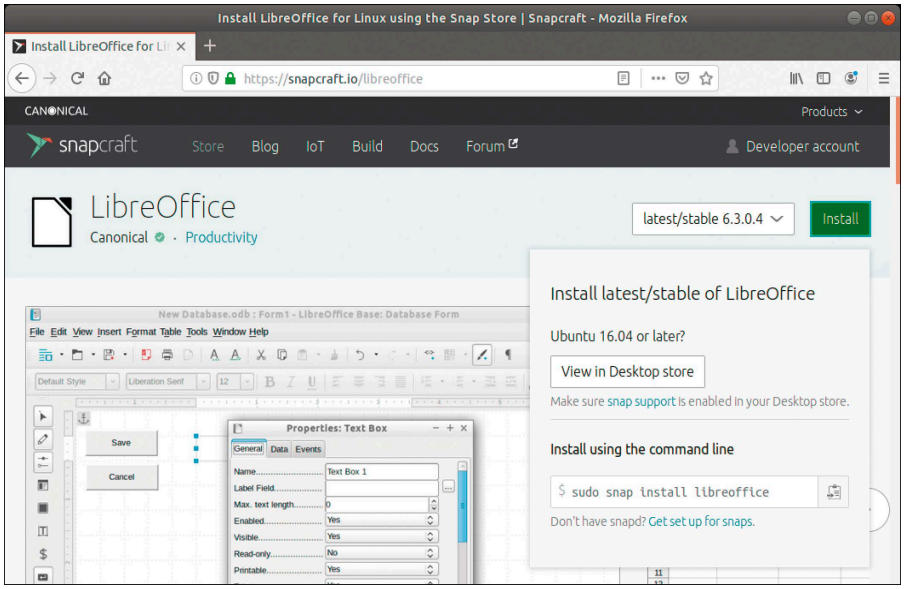
VON THORSTEN EGGELING

Linux-Programme laufen nur unter genau der Distribution problemlos, für die sie erstellt wurden. Das schränkt die Verbreitung aktueller Programmversionen stark ein und fortlaufende Anpassungen für andere Distributionen sowie Systemversionen erhöhen den Entwicklungsaufwand erheblich. Software lässt sich aber auch zusammen mit allen nötigen Komponenten in einen eigenständigen Container packen. Programme in Containern arbeiten weitestgehend unabhängig vom installierten Betriebssystem und können andere Anwendungen nicht beeinträchtigen. Es gibt aber auch Nachteile bei der Verwendung von Containerformaten.

Programme für alle Linux-Distributionen

Softwarecontainer enthalten neben dem eigentlichen Programm auch alle nötigen Bestandteile des Betriebssystems sowie Bibliotheken. Im Idealfall läuft eine Anwendung im Container unter jedem Linux-System. Auf diesem Weg können Sie neuere Versionen verwenden, auch parallel zu einem herkömmlich als „deb"-Paket installierten Programm.

Ubuntu setzt seit Version 16.04 das von Canonical entwickelte Format Snap-Apps (kurz: Snaps) ein. Seit Ubuntu 18.04 sind bereits einige Snap-Apps vorinstalliert, beispielsweise die Systemüberwachung und der Taschenrechner. Als Nutzer merken Sie davon nichts, außer dass die Programme eventuell etwas langsamer starten als gewöhnlich. Zentrale Anlaufstelle für die Suche nach Snap-Apps ist *https://snapcraft.io/store*. Hier finden Sie auch Informationen zur Installation der Snap-Software für alle unterstützten Distributionen, wenn diese auf Ihrem System noch nicht vorhanden ist.



Snap-Apps suchen: Über *https://snapcraft.io/store* finden Sie Programme schnell und bequem. Ein Klick auf „View in Desktop store" führt direkt zur Installation über Ubuntu-Software.

So funktionieren Snap-Apps

Lassen Sie sich in einem Terminalfenster mit dem Befehl

```
mount
```

die eingehängten Dateisysteme anzeigen. Sie sehen unter Ubuntu 18.04 etliche eingehängte Squashfs-Container, beispielsweise „/var/lib/snapd/snaps/gnome-calculator_406.snap". Snap-Apps sind Image-Dateien mit der Dateinamenserweiterung „.snap", die im Ordner „/var/lib/snapd/snaps" liegen und in das Dateisystem unterhalb des Ordners „/snap" eingehängt sind. Bei Squashfs-Containern handelt es sich um ein komprimiertes und schreibgeschütztes Format. Jeder Container enthält einen Verzeichnisbaum, in dem alle Dateien liegen, die ein Programm benötigt.

Alle Snap-Apps nutzen gemeinsam die Basissysteme Ubuntu Core und Base mit minimaler Ausstattung, die unter „/snap/core" beziehungsweise „/snap/core18" eingehängt sind. Laufzeitumgebungen wie Perl oder Java muss der Snap-Container selbst mitbringen. Es ist daher deutlich mehr Platz auf der Festplatte erforderlich als bei „deb"-Paketen – der Speicherbedarf steigt und die Programme starten langsamer. Angesichts großer Festplatten und schneller CPUs ist das auf aktuellen PCs jedoch zu tolerieren.

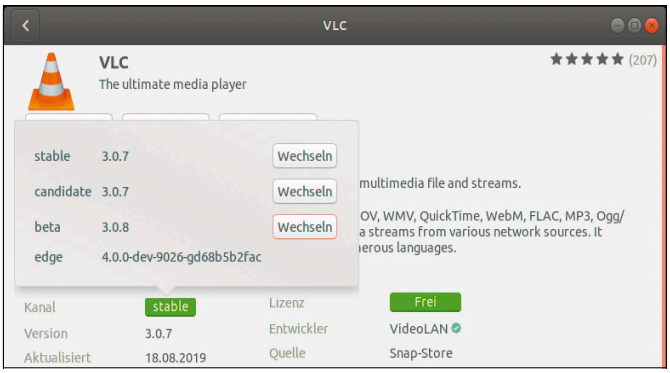
Snap-Apps in Ubuntu installieren

Nutzen Sie die Suchfunktion in Ubuntu-Software oder stöbern Sie in den Kategorien, um das gewünschte Programm zu finden. Wenn Sie beispielsweise nach dem Mediaplayer VLC suchen, taucht dieser im Ergebnis zweimal auf. Unter „Details" sehen Sie, um welche Version es sich handelt. Steht hinter „Quelle" die Angabe „Snap-Store", handelt es sich um eine Snap-App. Hinter „Kanal" klicken Sie auf „stable". Es öffnet sich ein Fenster, in dem Sie zwischen den Kanälen umschalten können. Bei „beta" oder „edge" finden Sie

meist höhere Versionsnummern. Die Software ist aber nicht ausreichend getestet und kann Fehler enthalten.

Klicken Sie beim gewünschten Programm auf „Installieren“ und danach auf „Starten“. Später verwenden Sie für den Programmstart eine Suche über die „Aktivitäten“. Sind unterschiedliche Versionen eines Programms installiert, beispielsweise VLC sowohl als „deb“-Paket als auch als Snap-Container, dann wird es unübersichtlich. Die Suche liefert für VLC zwei Ergebnisse, Beschriftung und Icon unterscheiden sich jedoch nicht. Hier hilft nur ausprobieren, welche Version sich hinter welchem Icon verbirgt.

Alternative: Suchen Sie ein Programm über *https://snapcraft.io/store*. Wählen Sie rechts oben im Fenster die gewünschte Version, klicken Sie auf „Install“, auf „View in Desktop store“ und dann auf „Link öffnen“. Installieren Sie die App in Ubuntu-Software wie oben beschrieben.



Mehrere Versionen: Über Ubuntu-Software können Sie auch Beta- oder Vorabversionen von Snap-Apps installieren. Sollten diese nicht gut funktionieren, kehren Sie zum Kanal „stable“ zurück.



Snap-Apps dürfen nicht alles. In Ubuntu-Software legen Sie bei der jeweiligen App nach einem Klick auf „Berechtigungen“ fest, was erlaubt ist und was nicht.

Snap-Apps verwalten

Ubuntu prüft viermal täglich, ob Updates für Snap-Apps verfügbar sind. Die Installation erfolgt automatisch. Im Terminalfenster lässt sich das Update auch folgendermaßen manuell einleiten:

```
sudo snap refresh
```

Mit dem weiteren Befehl

```
snap list --all
```

lassen Sie sich alle installierten Snap-Apps anzeigen. Um zu der vorherigen Version zurückzukehren, verwenden Sie den Parameter „revert“:

```
sudo snap revert gnome-calculator
```

Um etwa eine ältere Revision 260 von gnome-calculator (Taschenrechner) zu löschen, nutzen Sie diesen Befehl:

```
snap remove --revision 260 gnome-
  calculator
```

Dieser Schritt ist endgültig, weil sich ältere Versionen nicht aus dem Snap-Store installieren lassen.

Wenn Sie eine neuere Version ausprobieren möchten, wechseln Sie den Update-Kanal, für VLC beispielsweise so:

```
sudo snap switch --edge vlc && sudo
  snap refresh vlc
```

Zurück zur Version aus dem „stable“-Kanal geht es mit:

```
sudo snap switch --stable vlc &&
  sudo snap refresh vlc
```

Mit Hilfe des Tools snap können Sie auch nach Apps suchen (mit *snap find [Suchbegriff]*) und diese installieren (*snap install [snap-app]*).

Zugriffsrechte für Snap-Apps festlegen

Aus Sicherheitsgründen haben Snap-Apps nur Zugriff auf das Home-Verzeichnis. Das führt zu Irritationen, wenn Linux den Zugriff beispielsweise auf einen Wechseldatenträger verweigert. Deshalb sollten Sie direkt nach der Installation über Ubuntu-Software auf „Berechtigungen“ klicken. Aktivieren Sie „Lese/Schreibe Dateien auf mobilen Datenträger“, wenn die App auf USB-Geräte zugreifen soll, die unter „/media“ eingehängt sind. ■

WEITERE CONTAINERFORMATE NUTZEN

Nicht alle Programme sind als Snap-App verfügbar. Einige Entwickler bevorzugen Flatpak, wieder andere das Format Appimage. Flatpak-Container funktionieren ähnlich wie Snaps. Bei Linux Mint 19 ist Flatpak bereits vorinstalliert, Ubuntu-Nutzer installieren die Software mit

```
sudo apt install flatpak
```

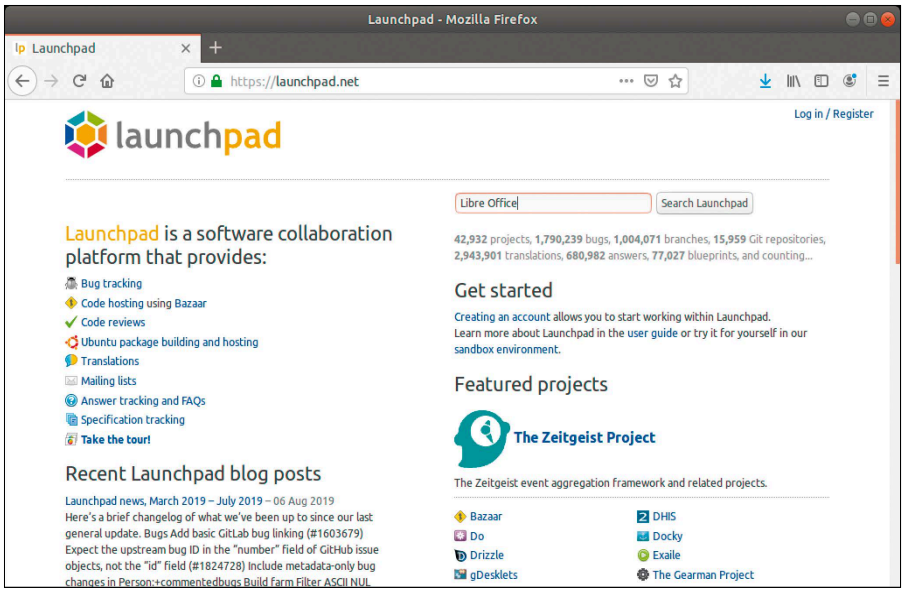
Flatpak-Apps finden Sie über *https://flathub.org/apps*, in Linux Mint auch über die „Anwendungsverwaltung“ in der Kategorie „Flatpak“.

Bei Appimage handelt es sich um portable Apps für Linux. Zusätzliche Software für die Verwaltung ist nicht erforderlich. Die heruntergeladene Datei enthält alles Nötige. Programme finden Sie beispielsweise über *https://appimage.github.io/apps*. Nach dem Download machen Sie die Datei ausführbar („Eigenschaften → Zugriffsrechte“ im Dateimanager). Das Programm lässt sich dann per Doppelklick starten.

Ein weiteres Containerformat ist Docker (*www.docker.com*). Es wird hauptsächlich für Serveranwendungen ohne grafische Oberfläche eingesetzt. Informationen zu den verfügbaren Programmen und Installationsanleitungen finden Sie unter *https://hub.docker.com*.

Zusätzliche Paketquellen verwenden

Die Standard-Paketquellen von Ubuntu stellen die wichtigsten Programme bereit. Sollten Sie hier etwas nicht finden, binden Sie weitere Paketquellen ein oder Sie installieren Pakete manuell.



Neue Softwarepakete: Was Sie in den Ubuntu-Paketquellen nicht finden, gibt es wahrscheinlich bei Launchpad. Binden Sie für Installation und Updates die gewünschte Paketquelle ein.

VON THORSTEN EGGELING

Die Softwareinstallation über die Ubuntu-Paketverwaltung aus den Standardrepositorien ist der bequemste und sicherste Weg. Manchmal fehlt jedoch das gewünschte Programm oder es gibt nur eine veraltete Version. Sie sind jedoch nicht auf das angewiesen, was der Distributor bereitstellt. Für neue Software lassen sich weitere Paketquellen konfigurieren oder deb-Pakete manuell installieren.

Service: Eine Textdatei mit allen Befehlszeilen aus diesem Artikel laden Sie über *http://www.pcwelt.de/mQYUqt* herunter.

Zusätzliche Paketquellen einbinden

Sie können jede Paketquelle einbinden, die ein Repository im Ubuntu/Debian-Format betreibt und für Ihre Systemversion passende Software bereitstellt. Beim Update der Paketdatenbank prüft die Paketverwaltung die Gültigkeit der GPG-Schlüssel von Paketquellen und Paketlisten. In den Paketlisten sind Hash-Werte der „deb"-Pakete hinterlegt, die ebenfalls berücksichtigt werden. Sollte der GPG-Schlüssel einer Softwarequelle nicht vorhanden oder ungültig sein, lässt sich die Paketquelle nicht verwenden und die darüber angebotene Software nicht installieren.

Am einfachsten ist die Installation von Fremdpaketen über ein Launchpad-PPA (Personal Package Archive). Die Website *https://launchpad.net* wird vom Ubuntu-Distributor Canonical betrieben und ist die bevorzugte Plattform für Entwickler, die Softwarepakete für Ubuntu und verwandte Distributionen bereitstellen möchten.

Verwenden Sie die Suchfunktion auf der Startseite, um herauszufinden, ob es ein PPA für die gewünschte Software gibt. Die Suche beispielsweise nach „Libre Office" und Klick auf den Link „LibreOffice Packaging in Launchpad" führt zu einer Übersichtsseite. Unter „Personal package archives" klicken Sie auf „LibreOffice 6.4.x", wenn Sie die zurzeit aktuellste (Beta)-Version von Libre Office installieren möchten. Unter „Overview of published packages" öffnen Sie hinter „Published in:" eine Liste mit den Ubuntu-Versionen, für die Pakete verfügbar sind. Bei diesem PPA ist die älteste Version „Bionic" (Ubuntu 18.04.1). „LibreOffice 6.2.x" gibt es dagegen auch für Xenial (Ubuntu 16.04). Wenn die Version passt, verwenden Sie im Terminalfenster die Befehlszeile unter „Adding this PPA to your system", beispielsweise

```
sudo add-apt-repository
  ppa:libreoffice/libreoffice-6-4
```

Bestätigen Sie mit Eingabetaste, dass Sie das PPA verwenden wollen. Es wird dann über die Textdatei „/etc/apt/sources.list.d/libreoffice-ubuntu-libreoffice-6-4-bionic.list" als neue Paketquelle eingebunden, der zugehörige GPG-Schlüssel ist unter „/etc/apt/trusted.gpg.d" zu finden. Abweichend von der Ubuntu-Dokumentation aktualisiert „add-apt-repository" bei Ubuntu 18.04 die Paketdatenbank automatisch. Sollte das bei Ihnen nicht der Fall sein (oder unter einer älteren Ubuntu-Version), dann verwenden Sie diesen Befehl:

```
sudo apt update
```

Da Libre Office wahrscheinlich bereits installiert ist, genügt dann

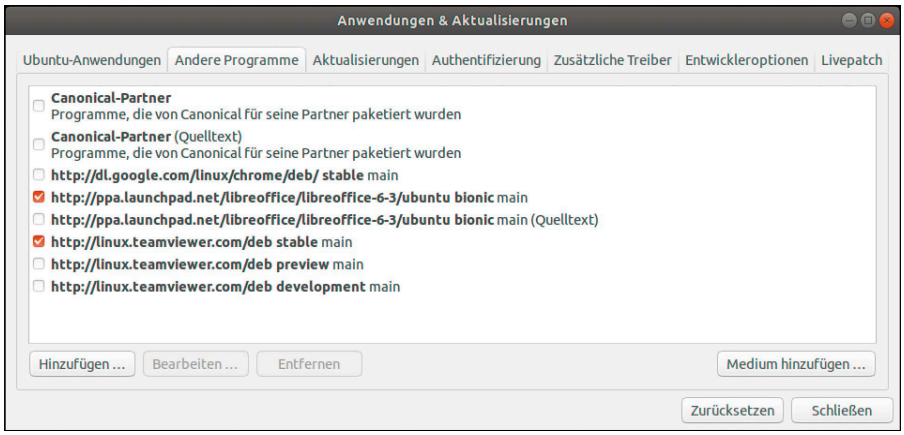
```
sudo apt upgrade
```
für das Upgrade. Andernfalls verwenden Sie folgende Zeile
```
sudo apt install libreoffice
```
für unser Beispiel.

Paketquellen manuell einbinden

Sollte es kein Launchpad-PPA für die gewünschte Software geben, finden Sie bei Anbietern von Linux-Software oft Adressen für deren eigene Repositorien. Der Ablauf ist immer der gleiche: Zuerst importieren Sie den GPG-Schlüssel und konfigurieren dann die neue Paketquelle.
Wer beispielsweise Google Chrome verwenden möchte (siehe auch den übernächsten Punkt), importiert zunächst den Schlüssel:
```
wget -q -O - https://dl-ssl.google.com/linux/linux_signing_key.pub | sudo apt-key add -
```
Mit folgendem Befehl erzeugen Sie eine Textdatei für die neue Paketquelle:
```
echo deb [arch=amd64] http://dl.google.com/linux/chrome/deb/ stable main | sudo tee /etc/apt/sources.list.d/google_chrome.list
```
Danach verwenden Sie
```
sudo apt update
sudo apt install google-chrome-stable
```
für die Installation der Software.

Paketquellen wieder entfernen

Paketquellen, die Sie nicht mehr benötigen, sollten Sie entfernen. Die darüber installierte Software bleibt erhalten und muss manuell deinstalliert werden (*apt remove [Paketname]*). Verwenden Sie diesen Befehl:
```
sudo add-apt-repository -r ppa:[Launchpad-Nutzername/PPA-Name]
```
Den Platzhalter ersetzen Sie durch die Angaben, die Sie auch bei der Installation verwendet haben. Sie können auch das grafische Tool „Anwendungen & Aktualisierungen“ nutzen, das Sie über „Aktivitäten“ finden. Gehen Sie dort auf die Registerkarte „Andere Programme“, entfernen Sie das Häkchen vor der Paketquelle und klicken Sie auf „Entfernen“.
Alternativ verwenden Sie das Tool ppa-purge, das Sie mit
```
sudo apt install ppa-purge
```
installieren.
Mit dem Befehl

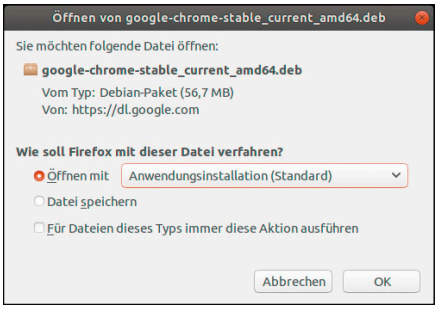


Paketquellen verwalten: Paketquellen lassen sich mit Hilfe von „Anwendungen & Aktualisierungen“ entfernen. Die installierte Software müssen Sie selbst deinstallieren.

```
sudo ppa-purge ppa:[Launchpad-Nutzername/PPA-Name]
```
deaktivieren Sie die PPA-Quelle. Sollte eine andere Version der Software in den offiziellen Quellen zu finden sein, wird diese automatisch als Ersatz installiert.
Das ist beispielsweise der Fall, wenn Sie Libre Office über das PPA auf die Version 6.4.x aktualisiert haben wie zuvor beschrieben. ppa-purge richtet dann erneut die Vorgängerversion ein. Ist das Paket über die Standard-Paketquellen nicht installierbar, bleibt es erhalten und Sie deinstallieren es manuell.

Heruntergeladene „deb“-Pakete installieren

Ubuntu-Software kann auch Pakete installieren, die Sie aus dem Internet herunterladen. Ein Beispiel ist Google Chrome (*www.google.de/chrome*). Beim Download über Firefox ist hinter „Öffnen mit“ standardmäßig „Anwendungsinstallation“ eingestellt. Nach einem Klick auf „OK“ öffnet sich Ubuntu-Software und Sie klicken auf „Installieren“. Das Chrome-Paket weist eine Besonderheit auf: Es richtet eine neue Paketquelle für den Google-Browser ein und installiert den Google-GPG-Schlüssel. Sie erhalten daher auch regelmäßig Updates für den Browser. Einige „deb“-Pakete aus dem Internet bieten diesen Komfort eventuell nicht. Für ein Update installieren Sie dann – wenn verfügbar – eine neue Version des „deb“-Pakets. ■



Pakete installieren: „deb“-Dateien, die Sie über den Browser herunterladen, öffnen Sie gleich mit Ubuntu-Software („Anwendungsinstallation“) und klicken auf „Installieren“.

FREMDPAKETE KÖNNEN DAS SYSTEM GEFÄHRDEN

Grundsätzlich ist jede Softwareinstallation immer Vertrauenssache. Die GPG-Schlüssel dürfen nicht kompromittiert und die Downloadserver müssen sicher sein. Bei den offiziellen Ubuntu-Servern können Sie von professioneller Wartung und umfangreichen Sicherungsmaßnahmen ausgehen. Launchpad (*https://launchpad.net*) wird zwar ebenfalls von Ubuntu-Distributor Canonical betrieben, Software kann hier jedoch jeder einstellen. Die Wahrscheinlichkeit, dass Schadsoftware frühzeitig entdeckt und gemeldet wird, ist aber sehr hoch. Launchpad darf daher als ausreichend sicher gelten. „deb“-Dateien aus dem Internet sollten Sie nur vertrauen, wenn diese von bekannten Anbietern stammen. Alles andere ist als unsicher anzusehen und das Risiko bei der Installation müssen Sie selbst verantworten.

Toolbox für Ubuntu & Mint

Linux-Systeme bieten direkt nach der Installation eine umfangreiche Softwareausstattung. Weitere nützliche Programme empfehlen die nachfolgenden Artikel und bieten dazu mit der LinuxWelt-Toolbox ein komfortables Werkzeug.

VON THORSTEN EGGELING

Software lässt sich unter Linux schnell und sicher aus dem Software-Repositorium der jeweiligen Distribution installieren. Wer eine aktuellere Version oder spezielle Programme benötigt, kann in Ubuntu oder Linux Mint auch PPAs (Personal Package Archive) einbinden. DEB-Pakete für die bequeme Installation gibt es bei Bedarf auch auf den Webseiten von Softwareherstellern. Eine bequeme Alternative sind Containerformate wie Snap-Apps, Flatpak und Appimage.

Es ist allerdings eine Herausforderung, im unüberschaubaren Angebot das passende Tool für einen bestimmten Zweck zu finden. Oft gibt es mehrere Programme für die jeweilige Aufgabe, aber nicht jedes davon kann auch alle Ansprüche erfüllen. Auf den folgenden Seiten finden Sie daher die Beschreibungen nützlicher Anwendungen und Tools sowie Tipps zu deren Verwendung. Für die komfortable Installation haben wir das Programm LinuxWelt-Toolbox (auf Heft-DVD) erstellt. Hier finden Sie ausführliche Anleitungen und Internetlinks sowie Befehlszeilen oder Schaltflächen für die schnelle Installation. Die meisten Einträge beziehen sich auf Ubuntu und Linux Mint und gelten größtenteils auch für verwandte Systeme wie Debian.



Bequeme Installationen: Die LinuxWelt-Toolbox zeigt Programmbeschreibungen und Infolinks. Für die Installation oder den Start der gewünschten Software genügt oft ein Mausklick.

1. Die LinuxWelt-Toolbox installieren

Die LinuxWelt-Toolbox erleichtert die Installation der in diesem und den sechs folgenden Artikeln genannten Programme. Entpacken Sie das Tool von der Heft-DVD aus dem Ordner „Software“ in das Home-Verzeichnis. Im Verzeichnis „LinuxWelt-Toolbox“ finden Sie die Datei „lwToolbox_x86_64“ für 64-Bit-Systeme, die Sie per Doppelklick starten. Nutzer eines 32-Bit-Systems verwenden „lwToolbox_i386“, für den Raspberry Pi eignet sich „lwToolbox_arm“.

Vorbereitungen: LinuxWelt-Toolbox läuft unter Ubuntu 16,04, 18.04 und 19.10, Linux Mint 18 und 19 sowie Raspbian Buster. Für den Download von Tooldatenbank und Updates muss libssl 1.0 oder libssl 1.1 installiert und die Dateien oder Symlinks „libssl.so“ und „libcrypto.so“ müssen vorhanden sein. Ob das der Fall ist, prüfen Sie in einem Terminalfenster mit den folgenden zwei Zeilen:

```
sudo ldconfig -v
ldconfig -pv | grep
 'libssl\.\|libcrypto\.'
```

Sollten in der Ausgabe beispielsweise nur „libssl.so.1.0.0“ und/oder „libssl.so.1.1“ auftauchen, aber nicht „libssl.so“, dann installieren Sie ein zusätzliches Paket:

```
sudo apt install libssl-dev
```

Nutzer von Ubuntu 19.10 müssen ein weiteres Paket installieren:

```
sudo apt install libgtk2.0-0
```

Für den Start von Programmen über die LinuxWelt-Toolbox ist außerdem bei allen Systemen xterm erforderlich und bei Ubuntu/Mint außerdem apturl für die Paketinstallation:

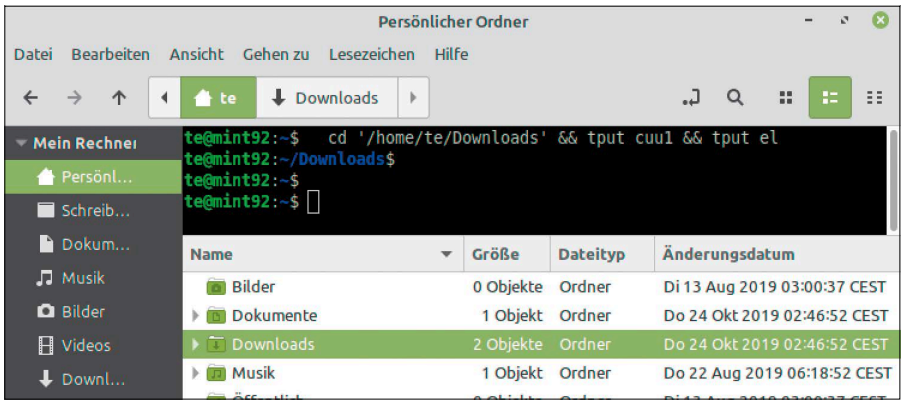
```
sudo apt install xterm apturl
```

Beim ersten Start der LinuxWelt-Toolbox erscheint ein Fenster, in dem Sie auf „Download“ klicken. Damit laden Sie die aktuelle Tooldatenbank herunter, die auf der Heft-DVD aus Aktualitätsgründen nicht mit dabei ist. Sie können das Programm

inklusive Tooldatenbank auch über *www.pcwelt.de/2Gtt1r* herunterladen.
Prüfen Sie auf der Registerkarte „Optionen“, ob die Toolbox das System richtig erkannt hat. Wichtig ist vor allem der Eintrag hinter „Codename“ (etwa „bionic“ für Ubuntu 18.04 LTS). Falls der falsche Codename auftaucht, tragen Sie den richtigen ein und klicken auf „Speichern“.
Eine Übersicht mit den Codenamen finden Sie auf *https://wiki.ubuntu.com/DevelopmentCodeNames*.

2. Softwarepakete suchen und installieren

Bei Ubuntu ist das Programm „Ubuntu Software“ die erste Anlaufstelle für die Suche nach neuer Software, Benutzer von Linux Mint nutzen die „Anwendungsverwaltung“. Fortgeschrittene Linux-Nutzer verwenden das Kommandozeilentool apt oder greifen zu Synaptic, das bei Linux Mint bereits vorinstalliert ist.
Sie finden Synaptic im Menü „Systemverwaltung → Synaptic-Paketverwaltung“. Das Tool ist schnell und ermöglicht vor allem eine gezieltere Paketauswahl. Meist genügt die Eingabe eines Suchbegriffs in das Eingabefeld unter „Schnellauswahl-Filter“. Oder Sie klicken auf die Schaltfläche „Suche“ und tippen den Suchbegriff ein. Über das Auswahlfeld darunter lässt sich der Bereich beispielsweise auf „Name“ oder „Beschreibung und Name“ eingrenzen. Per Klick auf „Einstellungen → Paketquellen“ gelangen Sie zum Fenster „Anwendungen & Aktualisierungen“. Auf der Registerkarte „Andere Programme“ lässt sich festlegen, welche Repositorien die Paketverwaltung berücksichtigt.
Installation: Wechseln Sie in der Linux-Welt-Toolbox über das Ausklappmenü in die Rubrik „Ubuntu/Mint“. Ubuntu-Nutzer installieren Synaptic nach Klicks auf die Schaltflächen „Paketverwaltung“ und „Synaptic installieren“.



Dateimanager erweitern: In Nemo können Sie unter Linux Mint ein Terminalfenster integrieren. Darüber lassen sich Befehle schnell im aktuellen Ordner absetzen.

3. Tools für die Dateiverwaltung

Dateien kopieren, löschen oder verschieben gehört zu den täglichen Handgriffen. Der Dateimanager ist daher eines der wichtigsten Tools. Bei Linux gibt es eine ganze Reihe: Je nachdem, welche Distribution und welcher Desktop installiert ist, zeigt sich standardmäßig etwa Nautilus (Ubuntu Unity), Dolphin (KDE) oder Nemo (Cinnamon/Linux Mint). Nautilus und Nemo bieten praktische Erweiterungen, etwa um die Größe von mehreren Bildern zu ändern oder Prüfsummen von Dateien zu berechnen. Außerdem lassen sich in beide Dateimanager Scripts einbinden und starten. Über das Kontextmenü können Sie dann etwa Ordner schnell packen oder Audiodateien konvertieren. Für Nemo gibt es eine Erweiterung, über die sich ein Terminalfenster im Dateimanager einblenden lässt, das automatisch in den jeweils geöffneten Ordner wechselt.
Installation: Nautilus, Nemo und Dolphin laufen unter allen Desktopumgebungen und Ubuntu-Varianten. Die nötigen Pakete sind in den Standardrepositorien enthalten. Über die LinuxWelt-Toolbox finden Sie alle relevanten Paketnamen und Funktionen für die schnelle Installation nach einem Klick auf „Dateimanager“. Weitere Alternativen gibt es in der Rubrik „Zwei-Fenster Dateimanager“.

DIE LINUXWELT-TOOLBOX NUTZEN

In der LinuxWelt-Toolbox sehen Sie links oben eine Auswahlliste, über die Sie die Rubrik einstellen.
Für diesen Artikel beispielsweise „Ubuntu/Mint“. Die Schaltflächen am linken Rand führen Sie jeweils zur Beschreibung eines oder mehrerer Tools. Die Programme sind teilweise in den Standardrepositorien von Ubuntu, Linux Mint oder Debian enthalten.
In diesem Fall gibt es blaue Schaltflächen am unteren Rand des Fensters, über die Sie ein Programm installieren und starten können. Teilweise sind auch im Text Schaltflächen für die Installation untergebracht.
Alternativ können Sie die Programme auf der Kommandozeile mit apt installieren. Die dafür nötige Befehlszeile kopieren Sie über die Schaltfläche „Kopieren (Strg-C)“ und fügen die Zeile in einem Terminalfenster mit Strg-Umschalt-V ein.

Bitte beachten Sie: Die Installationsanleitungen und Befehlszeilen beziehen sich auf den Stand der Entwicklung im Oktober 2019. Bei neuen Programmversionen kann es Abweichungen geben. Sollte ein Download oder eine Installation nicht funktionieren, informieren Sie sich auf der Webseite des Anbieters.
Die LinuxWelt-Toolbox verwendet XML-Dateien aus dem Unterverzeichnis „Tools“ als Datenbank. Über die Registerkarte „Datenbank“ können Sie die Inhalte bei Bedarf ändern und eigene Tools hinzufügen. Die Beschreibungstexte stammen aus den HTML-Dateien im Ordner „doc“. Diese lassen sich auch im Webbrowser aufrufen – eine Übersicht liefert die Datei „index.html“. Nach eigenen Anpassungen sichern Sie die Ordner „Tools“ und „doc“, damit diese bei einem Update nicht verloren gehen. Für Ihre individuelle Toolsammlung verwenden Sie die Rubrik „Benutzer“.

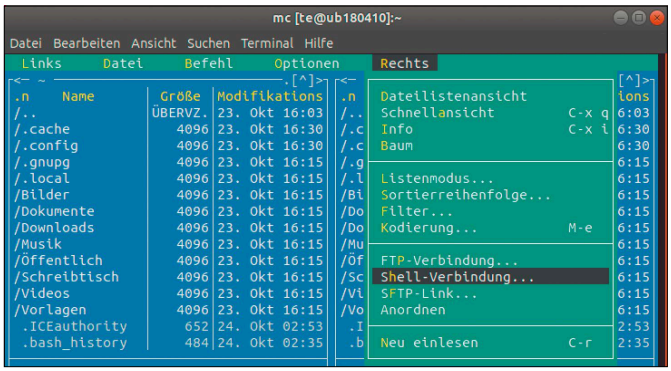
4. Dateimanager im Terminalfenster nutzen

Auch im Terminalfenster müssen Sie nicht auf einen komfortablen Dateimanager verzichten. Das bekannteste Tool heißt Midnight Commander und lässt sich mit dem Befehl „mc“ starten. Vor allem beim Fernzugriff über SSH auf Server oder PCs, wo kein Desktop zur Verfügung steht, zeigt dieses Tool seine Stärken.

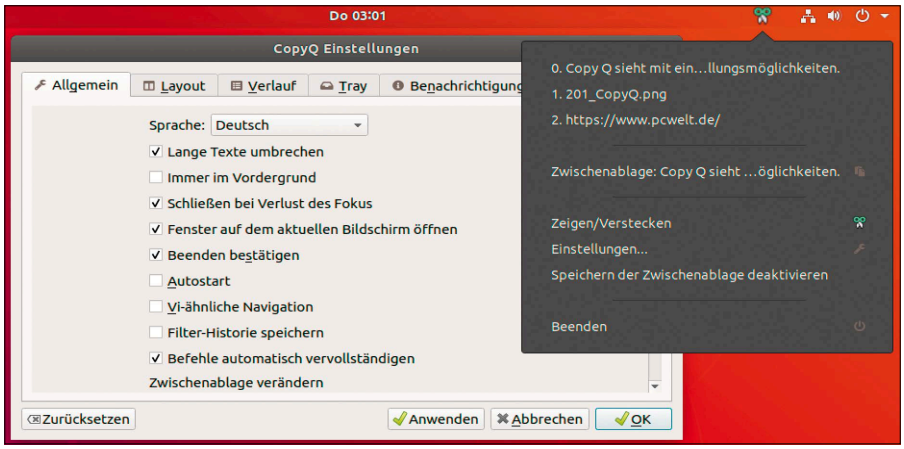
Die wichtigsten Operationen lassen sich über die F-Tasten steuern, deren Bedeutung in der unteren Leiste zu sehen ist. F5 beispielsweise kopiert das aktuell markierte Element in das Verzeichnis des anderen Panels. Über F3 rufen Sie einen Dateibetrachter auf und über F4 einen Editor. Taste Esc gefolgt von der Eingabetaste setzt den gerade markierten Ordner- oder Dateinamen in die Kommandozeile ein.

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 Servername oder IP-Adresse an, optional bereits mit dem gewünschten User (etwa „root@192.168.1.10“). Nach Eingabe des Kennworts zeigt der MC wieder seine beiden Fensterhälften und Sie kopieren bequem Dateien zwischen dem lokalen und dem entfernten System.

Installation: Der MC ist in allen Linux-Distributionen verfügbar. Die Installationsanleitung finden Sie in der LinuxWelt-Toolbox nach einem Klick auf „Dateimanager“.



Komfort im Terminal: Der Midnight Commander vereinfacht die Dateiverwaltung auf der Kommandozeile und ermöglicht auch den Datenaustausch über SSH und FTP.



Zwischenablage mit Copy Q: Das Programm hat einen großen Funktionsumfang und zeigt in seinem Verlauf auch Bilder an. Es steht auch für Windows und Mac-OS zur Verfügung.

5. Mehr Funktionen für die Zwischenablage

Einige Desktopumgebungen behandeln die Zwischenablage stiefmütterlich und überlassen deren Verwaltung dem X-Window-System. Dieses arbeitet mit einer empfindlichen Einschränkung: Kopiert man Inhalte aus einem Programm in das Clipboard und schließt dann das Programm, so verschwinden dessen Inhalte aus der Ablage.

Gpaste: Eine Zwischenablage mit lückenlosem Kurzzeitgedächtnis und einem permanenten Erinnerungsvermögen bietet das Gnome-Programm Gpaste. Es nimmt mehrere Bilder und Textausschnitte auf, die sich über das Symbol im Gnome-Panel auswählen lassen. Gpaste ist englischsprachig, aber einfach zu bedienen.

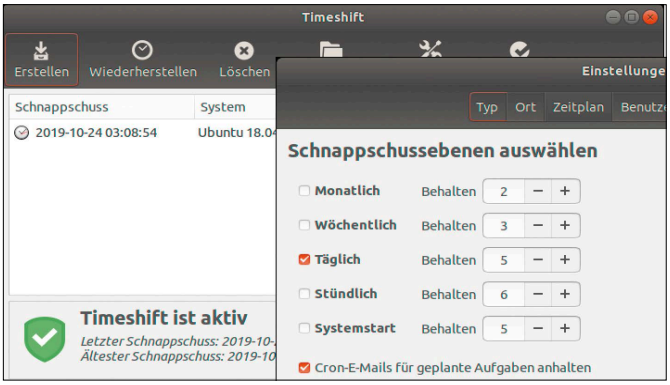
Gpaste ist in den Paketquellen der verbreiteten Linux-Distributionen mit Gnome-Desktop enthalten. Nach der Installation ist ein Neustart des Desktops nötig. Das Tool „Gnome-Tweaks“ (siehe Punkt 6) ist wichtig, um die Gnome-Shell-Erweiterung nach der Installation zu aktivieren.

Copy Q: Für Linux, Windows und Mac-OS gibt es das deutschsprachige Programm Copy Q. Es nimmt Bilder, Text und HTML-formatierten Text auf und kann diese auf Wunsch auch ohne Formatierungen einfügen. Die zwischengespeicherten Einträge lassen sich in einem Editor direkt bearbeiten und überstehen sogar einen Systemneustart.

Installation: Hinweise zu Installation und Benutzung von Gpaste und Copy Q finden Sie in der LinuxWelt-Toolbox nach einem Klick auf „Zwischenablage“.

6. Eigene Dateien und System sichern

Backups sind lästig, aber wichtig. Persönliche Dateien aus Ihrem Home-Verzeichnis sollten Sie regelmäßig sichern, das komplette System zumindest vor größeren Änderungen, etwa vor Distributionsupgrades. Für die persönlichen Daten ist bei Ubuntu standardmäßig ein Tool installiert, das Sie



Systembackup: Timeshift sichert das komplette Linux-System. Es eignet sich für regelmäßige und platzsparende Backups, weil nur geänderte oder neue Dateien berücksichtigt werden.

per Suche im Dash nach „Datensicherungen“ finden. Linux-Mint-Nutzer rufen ein ähnliches Tool über das Menü und „Systemverwaltung → Datensicherungswerkzeug“ auf. Für regelmäßige Backups empfehlen wir das Tool Timeshift (unter Linux Mint Standard). Es erstellt Momentaufnahmen des Dateisystems, die beim Zurückspielen einen vorherigen Zustand wiederherstellen. Home-Verzeichnisse sind standardmäßig ausgeschlossen, lassen sich aber über die „Einstellungen“ dem Backup hinzufügen. Der erste Sicherungspunkt ist immer ein komplettes Backup der Systemverzeichnisse und mit einigen Gigabyte recht groß. Weitere Wiederherstellungspunkte sind dann aber deutlich kleiner, da Timeshift nur noch die Unterschiede zum vorherigen Sicherungspunkt speichert.

Installation: Die Installationshinweise zu Timeshift finden Sie in der LinuxWelt-Toolbox nach einem Klick auf die Schaltfläche „Backup“.

7. Tuningtool für den Desktop

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 allerdings nicht. Mit gnome-tweaks ist es möglich, den Desktop als Dateiablage zu verwenden, ferner Arbeitsflächen, Schriftbild, Fensterverhalten, Fensterschaltflächen und Fensteroptik genauer zu justieren.

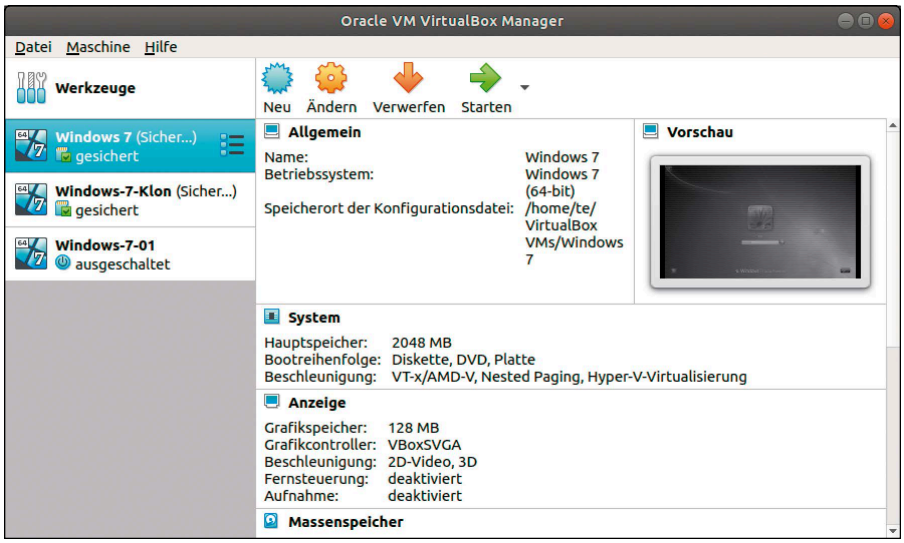
Installation: Eine ausführliche Funktionsbeschreibung und Installationsanleitung liefert LinuxWelt-Toolbox nach einem Klick auf „Tweak-Tools“.

8. Nützliche Systemtools

Wie viel Speicher steckt im Rechner? Wo ist die Konfigurationsdatei für den Samba-Server? Wie beende ich ein eingefrorenes Programmfenster? Und wo ist das Mountverzeichnis für das eingehängte Netzlaufwerk? Antworten auf diese und viele weitere Fragen geben wir in einem längeren Beitrag, den Sie in der LinuxWelt-Toolbox per Klick auf „Systemtools in der Praxis“ aufrufen. Dabei kommen prominente grafische Programme unter den Desktopsystemen Ubuntu und Linux Mint zu Wort, aber den größeren Anteil erhalten die typischen Terminalprogramme. Diese haben nämlich zwei entscheidende Vorteile: Erstens funktionieren sie auf allen Linux-Distributionen, zweitens sind sie alternativlos, wenn ein Server per SSH im Terminal administriert wird. Ein Teil der genannten Tools ist bei Ubuntu oder Linux Mint standardmäßig installiert. Wenn nicht, finden Sie in der LinuxWelt-Toolbox eine Installationsanleitung.

Anpassungen mit Gnome-Tweaks: Viele wichtige Detaileinstellungen zum Aussehen und Verhalten des Desktops sind nur über dieses zusätzliche Werkzeug zugänglich.





Virtualisierung: Installieren Sie Betriebssysteme in einer virtuellen Maschine. Darin lässt sich Software gefahrlos ausprobieren und Sie können Windows-Anwendungen unter Linux starten.

9. Virtualisierung und Windows-Programme

Nicht immer steht eine benötigte Software auch für Linux zur Verfügung. Es bietet sich dann an, Windows in einer virtuellen Maschine zu verwenden und hier die jeweils gewünschte Software zu nutzen. Die Virtualisierungssoftware Virtualbox ist in den Standard-Paketquellen enthalten. Darüber lässt sich die Open-Source-Variante installieren, die aber meist nicht ganz aktuell ist und einige Funktionen vermissen lässt, beispielsweise die Unterstützung von USB-Geräten. Der Hersteller Oracle (*www.virtualbox.org*) stellt jedoch eigene Linux-Repositorien bereit, über die sich die aktuelle Version einrichten lässt.

Installation: Klicken Sie in der LinuxWelt-Toolbox auf „Virtualisierung“. Sie finden hier eine Schaltfläche für den Import der Oracle-PGP-Schlüssel, mit dem die Pakete digital signiert sind. Danach klicken Sie auf „Virtualbox installieren“. Die Befehlszeilen für die manuelle Installation sind darunter zu finden.

Alternative: Für den Start von vielen Windows-Programmen unter Linux eignet sich auch Wine, das Windows-Funktionen unter Linux nachbildet. Am einfachsten gelingt die Installation von Windows-Software über Playonlinux. Die Softwareauswahl für Wine ist jedoch begrenzt. Oft funktionieren nur ältere Programmversionen problemlos. Sehen Sie auf *www.playonlinux.com* nach, ob und wie gut die benötigte Software unterstützt wird.

Installation: Für die Einrichtung von Playonlinux, die automatisch die passende Wine-Version anfordert, klicken Sie in LinuxWelt-Toolbox auf „Virtualisierung“ und dann auf „Playonlinux installieren“. ■

Programme & Tools fürs Netzwerk

Linux fühlt sich im Netzwerk traditionell zu Hause. Das System ist als Datei- oder Webserver schnell eingerichtet und auch die Fernwartung über das Netzwerk stellt kein Problem dar.

VON THORSTEN EGGELING



Über den Dateimanager nutzen Sie Freigaben im lokalen Netzwerk, die auf einem Linux- oder Windows-Server liegen. Die Zugangsdaten können Sie dauerhaft speichern.

Was Sie für das Internet benötigen, ist bei allen gängigen Linux-Distributionen bereits vorinstalliert. Als Browser dient meist Firefox und für E-Mails gibt es Thunderbird. Der Zugriff auf Netzwerkfreigaben erfolgt über den Dateimanager. Serverdienste für Dateifreigaben oder SSH/SFTP sind standardmäßig oft nicht vorhanden, lassen sich aber schnell aus den Paketquellen nachinstallieren. Die Kommandozeilen aus diesem Artikel, Tipps, Beschreibungen, Internetlinks zu weiteren Informationen und Downloadlinks finden Sie in der LinuxWelt-Toolbox (auf DVD) in der Rubrik „Netzwerk".

1. Zugriff auf Freigaben im Netzwerk

Linux, Windows und Mac-OS sprechen im Netzwerk eine gemeinsame Sprache: Das SMB/CIFS-Protokoll. Einen SMB-Client (für den Zugriff auf SMB-Freigaben) bringen alle Systeme mit: Mac-OS zeigt solche Windows-Freigaben im Dateimanager in einer eigenen Rubrik. Unter Linux Mint, Ubuntu & Co. finden Sie die Freigaben über „Andere Orte → Windows-Netzwerk" oder „Netzwerk" im Dateimanager – und ganz ähnlich auch im Windows-Explorer. Sofern es sich um eine Freigabe ohne den großzügigen „Gastzugriff" (Zugriff ohne Kontoinformationen) handelt, ist zum Öffnen eine Authentifizierung notwendig: Dazu benötigen Sie den Namen und das Kennwort eines Samba-Kontos. Diese Zugangsdaten kann sich jeder Client dauerhaft merken, sodass die spätere Nachfrage entfällt (Option „Nie vergessen" unter Ubuntu/Linux Mint).

Ab Ubuntu 18.04/Linux Mint 19 gibt es allerdings Probleme mit Windows-Freigaben. Diese werden im Dateimanager nicht angezeigt. Der Grund dafür: Aus Sicherheitsgründen ist das Protokoll SMB 1.1 deaktiviert, das aber für die Auflistung der Freigabenamen erforderlich ist. Bis die Distributoren diesen Fehler behoben haben, geben Sie den Pfad hinter „Mit Server verbinden" oder in der Adresszeile (Strg-L) in der Form

```
smb://Servername/Freigabename
```

ein. Für den künftigen schnelleren Zugriff legen Sie über das Hamburger-Menü (Icon mit den drei horizontalen Linien) ein Lesezeichen für die Freigabe an. Unter Mint verwenden Sie das Menü „Lesezeichen".

2. Freigaben für Windows- und Linux-PCs

Für die Freigabe persönlicher Ordner verwenden Sie im Ubuntu-Dateimanager den Kontextmenüpunkt „Freigabe im lokalen Netzwerk" eines Ordners. Setzen Sie ein Häkchen vor „Diesen Ordner freigeben". Ist der Freigabedienst Samba noch nicht installiert, klicken Sie auf „Freigabedienst einrichten" und danach auf „Installieren". Anschließend melden Sie sich bei Linux ab und wieder an.

In Linux Mint 19 Cinnamon heißt der Kontextmenüpunkt „Freigabeoptionen". Bevor Sie ihn nutzen können, müssen Sie Samba installieren. Dazu verwenden Sie im Terminal die folgenden zwei Befehle:

```
sudo apt update
sudo apt install samba
```

Im Fenster „Ordner freigeben" können Sie ein Häkchen vor „Gastzugriff (für Nutzer ohne Benutzerkonto)" setzen. Damit erlauben Sie anderen PCs im Netzwerk ohne Anmeldung Lesezugriff auf den freigegebenen Ordner. Ansonsten gibt es Lesezugriff nach vorheriger Anmeldung nur für Nutzer, die ein Konto auf dem PC mit der Freigabe besitzen. Schreibzugriff ist möglich, wenn Sie ein Häkchen vor „Anderen erlauben, Dateien in diesem Ordner zu erstellen oder zu löschen" setzen. Damit die Anmeldung funktioniert, müssen Sie aber vorher den gewünschten Benutzerkonten ein Samba-



Ordnerfreigabe: Eigene Ordner lassen sich über das Kontextmenü „Freigabe im lokalen Netzwerk“ (Ubuntu) für gemeinsame Nutzung im Netz bereitstellen.



Samba-Server konfigurieren: Mit dem grafischen Tool aus dem Paket „system-config-samba“ erstellen Sie Freigaben für angemeldete Benutzer und Gäste.

Passwort zuweisen, denn Samba verwendet eigene Passwörter, die vom Systemkonto unabhängig sind:

```
sudo smbpasswd -a [User]
```

Den Platzhalter „[User]“ ersetzen Sie durch die Bezeichnung des Benutzerkontos. Tippen Sie das Passwort ein und bestätigen Sie es. Das Passwort darf identisch mit dem Linux-Anmeldepasswort sein oder von diesem abweichen.

Es ist jedoch empfehlenswert, auf allen Linux- und Windows-PCs die gleiche Kombination von Benutzernamen und Passwörtern zu verwenden.

Samba konfigurieren: Für die Basiskonfiguration von Samba sowie systemweiter Freigaben empfiehlt sich bei Ubuntu 16.04, 18.04 sowie Linux Mint 18 und 19 die Installation des Pakets „system-config-samba“. Bei Ubuntu 19.10 ist es nicht mehr installierbar. Erstellen Sie zuerst eine Konfigurationsdatei:

```
sudo touch /etc/libuser.conf
```

Danach starten Sie das Tool mit

```
sudo -H system-config-samba
```

Über „Einstellungen → Server-Einstellungen“ legen Sie bei Bedarf die Arbeitsgruppe für den Samba-Server fest, wenn Sie in Ihrem Netzwerk etwas anderes als den Linux- und Windows-Standard „Workgroup“ verwenden.

Klicken Sie auf „Datei → Share hinzufügen“, um einen Ordner im Netzwerk freizugeben. Setzen Sie ein Häkchen vor „Sichtbar“ und auf der Registerkarte „Zugang“ wählen Sie die Option „Jedem Zugriff erlauben“. Alle Benutzer im Netzwerk haben dann über das Gastkonto anonymen Zugang zu dieser Freigabe. Ist auf der Registerkarte „Basis“ ein Häkchen vor „Beschreibbar“ gesetzt, ist auch anonymer Schreibzugriff möglich. Die Dateisystemrechte haben jedoch Priorität.

NETZWERKTOOLS FÜR DIE KOMMANDOZEILE

Im Terminalfenster lassen sich einige nützliche Tools starten, über die Sie die Netzwerkkonfiguration prüfen oder ändern können. Mit der Eingabe von

```
ip addr
```

ohne weitere Parameter erhalten Sie die physikalische MAC-Adresse des Netzwerkadapters, die lokale IP-Adresse und die Anzahl und Datenmenge der empfangenen (RX) und der gesendeten (TX) Datenpakete seit dem letzten Systemstart. Ethernet-Adapter tauchen mit Bezeichnungen wie „enp0s3“ auf, WLAN-Adapter etwa als „wlp5s0“. Bei der an erster Position angezeigten „lo“-Schnittstelle mit der IP-Adresse 127.0.0.1 handelt es sich um einen Loopback-Adapter, über den lokale Prozesse via TCP/IP miteinander kommunizieren. Gibt „ip addr“ eine IP-Adresse aus, die nicht im Bereich des Routers liegt, oder erscheint gar keine Adresse, ist die Netzwerkverbindung gestört. Mit Ping prüfen Sie Netzwerkverbindungen: *ping google.de* oder *ping 192.169.178.1* geben Zeilen mit Antworten aus, wenn das Netzwerk erreichbar ist. Andernfalls erscheint „Destination Host Unreachable“ oder ähnlich.

Das Programm Ethtool zeigt die Geschwindigkeit des Netzwerkadapters an. Sie rufen es beispielsweise mit folgender Befehlszeile auf:

```
ethtool enp0s3
```

Erscheint hinter „Speed“ der Wert „1000Mb/s“, nutzt der Adapter Gigabit-Ethernet. *ethtool -i enp0s3* gibt den Namen des Treibers aus, der für diese Schnittstelle verantwortlich ist.

Der Net-Befehl dient zur Kontrolle und Konfiguration eines Samba-Servers. Net ist vor allem praktisch, wenn Sie Samba-Freigaben auf einem Server ohne grafische Oberfläche oder aus der Ferne über SSH verwalten müssen. Folgende Befehlszeile gibt die vom aktuellen Benutzer erstellten Freigaben aus:

```
net usershare list
```

Eine neue Freigabe erstellen Sie mit dieser Zeile:

```
net usershare add sepp /home/sepp "" sepp:f
```

In diesem Fall wird „/home/sepp“ mit dem Freigabenamen „sepp“ für den gleichnamigen User im Netzwerk freigegeben. Über den Befehl *net usershare delete sepp* löschen Sie diese Freigabe.

Installation: Alle genannten Tools sind bei Ubuntu und Linux Mint standardmäßig vorhanden oder lassen sich nachinstallieren. Die Befehlszeile zur Installation finden Sie in der Linux-Welt-Toolbox nach einem Klick auf „Terminal-Tools“.

Ordner und Dateien im freigegebenen Verzeichnis müssen für den Gastzugriff mit Schreibrechten dem Benutzer „nobody“ und der Gruppe „nogroup“ gehören und ausführbar beziehungsweise beschreibbar sein. Das lässt sich in einem Terminalfenster beispielsweise durch folgenden Befehl erreichen:

```
sudo chown -R nobody:nogroup /
  freigegeben
sudo chmod -R 755 /freigegeben
```

Installation: In der LinuxWelt-Toolbox finden Sie nach einem Klick auf die Schaltfläche „Samba“ eine Schaltfläche für die Installation von „system-config-samba“. Folgen Sie den Links zu den weiterführenden Informationen. In der Rubrik „Raspberry Pi“ erfahren Sie nach einem Klick auf „Datenserver“, wie sich Samba über die Datei „/etc/samba/smb.conf“ konfigurieren lässt. Die Anleitung gilt nicht nur für Raspbian, sondern auch für andere Linux-Systeme wie Ubuntu 19.10.

3. Terminal und Dateitransfer über SSH

SSH (Secure Shell) ist ein Netzwerkprotokoll, über das Sie eine verschlüsselte Verbindung zu anderen Linux-PCs im Netzwerk herstellen. Es kommt vor allem bei der Fernwartung von Servern zum Einsatz. Der SSH-Client ist bei Ubuntu und Linux Mint Standard. Auf jedem Client-PC im Netzwerk können Sie über

```
ssh [User]@[Server] [:Port]
```

Verbindungen aufbauen. Den Platzhalter „[User]“ ersetzen Sie durch das Systemkonto auf dem Server, „[Server]“ durch Name oder IP-Adresse des Open-SSH-Servers. Die Portangabe kann entfallen, wenn der Standardport (22) verwendet wird. Danach können Sie im Terminal so arbeiten, als ob Sie direkt vor dem entfernten PC sitzen würden.

Installation: Wenn Sie auf allen Rechnern im Netzwerk den Open-SSH-Server installieren, funktioniert die Verbindung in alle Richtungen. Ein SFTP-Server für den Dateitransfer wird dabei automatisch mit installiert. In der LinuxWelt-Toolbox finden Sie nach einem Klick auf „OpenSSH“ die Befehlszeile für die Installation, zusätzliche Informationen zum Dateitransfer per SFTP sowie über die Anmeldung mit einem Sicherheitsschlüssel statt mit einem Passwort. Weitere Infos zu SSH erhalten Sie nach einem Klick auf „Netzwerk-Tools“.



Fernwartung: In der LinuxWelt-Toolbox finden Sie alle Informationen zur Einrichtung des Open-SSH-Servers und zur optimalen Nutzung der SSH-Clients.

4. Webserver auf dem PC einrichten

Im eigenen Netzwerk lässt sich ein Webserver für ein Intranetportal nutzen, etwa mit einem Wiki für die Ideensammlung oder mit einem Teamkalender. Sie können außerdem Webanwendungen wie Wordpress, Joomla oder Magento installieren und die Konfiguration sowie Gestaltung der Weboberfläche ausprobieren.

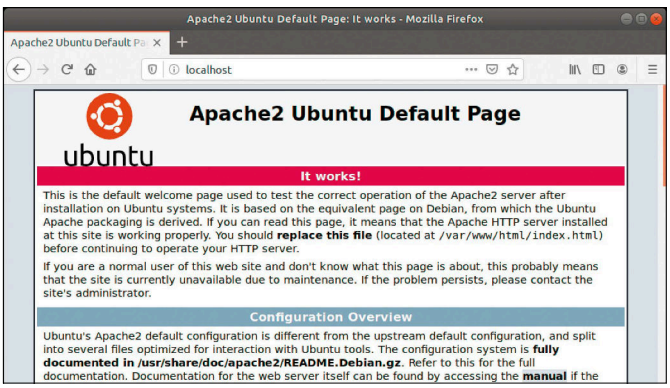
Der Webserver auf dem eigenen PC kann seine Dienste auch im Internet anbieten. Dazu müssen Sie in Ihrem DSL-Router die Portweiterleitung auf den Server-PC aktivieren. Wechselnde IP-Adressen, fehlende IPv4-Unterstützung durch den Internetprovider und eine geringe Uploadgeschwindigkeit lassen diese Lösung jedoch als wenig attraktiv erscheinen.

Für kleine Teams, die keinen Server im Internet mieten wollen, kann der heimische Webserver jedoch ausreichen. Sie sollten dann jedoch einen Dienst für dynamisches DNS nutzen, damit der Server stets über einen konstanten Domainnamen erreichbar ist. Wie sich dynamischem DNS einrichten lässt, lesen Sie in der LinuxWelt-Toolbox nach einem Klick auf „Nextcloud“ in der Rubrik „Raspberry Pi“.

Installation: In der LinuxWelt-Toolbox finden Sie nach einem Klick auf „Der eigene Webserver“ eine Installationsanleitung für den Apache Webserver zusammen mit Dokuwiki. Eine Alternative für Geräte mit limitierter Hardwareausstattung zeigen wir unter „Nginx-Webserver“.

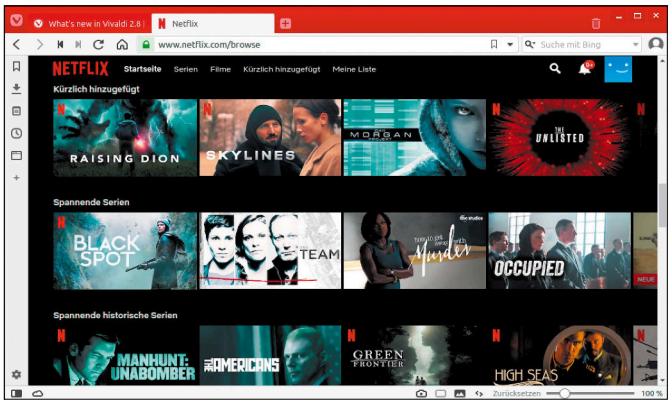
5. Tipps & Tools für das Heimnetzwerk

Netzwerke sind hardwareseitig unglaublich flexibel und ausbaufähig. Linux wiederum ist für das Netzwerk geschaffen und macht als Netzwerkclient wie als Server eine glänzende Figur. In der LinuxWelt-Toolbox finden Sie nach einem Klick auf „Netzwerk-Tools“ einen Beitrag, der Basiswissen und



Webserver: Nach der Apache-Installation zeigt „http://localhost“ im Browser die Standard-Website „index.html“ aus dem Verzeichnis „/var/www/html/“.

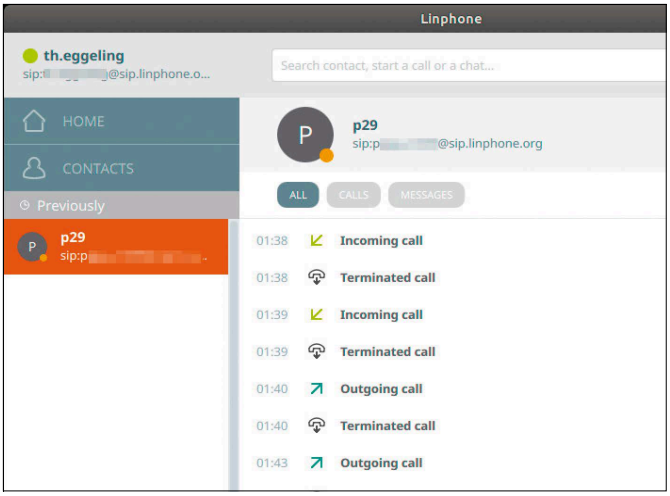
vertiefende Tipps für ein optimiertes Heimnetz liefert. Dabei geht es um das lokale LAN- und WLAN-Netz mit typischen Geräten, Kommunikationsprotokollen, Freigaben und Serververwaltung.
Alle genannten Tools wie ping, ifconfig, iwlist, arp oder nmap sind bei den meisten Linux-Systemen vorinstalliert oder sie lassen sich aus den Standardrepositorien nachinstallieren (siehe auch den Kasten „Netzwerktools“).



Schneller Browser: Vivaldi basiert auf Google Chrome und spielt auch Filme etwa von Amazon oder Netflix ab. Die Oberfläche lässt sich individuell anpassen.

6. Frische Browser fürs Internet

Firefox ist einer der beliebtesten Webbrowser und bei den meisten Linux-Distributionen bereits vorinstalliert. Der Browser glänzt vor allem durch seine Erweiterbarkeit über Add-ons. Firefox geht jedoch nicht besonders sparsam mit dem Hauptspeicher um, was vor allem bei vielen geöffneten Tabs das System ausbremsen kann. Chromium (*www.chromium.org*), ein Open-Source-Ableger von Google Chrome, hat einen geringeren Ressourcenverbrauch. Die Unterschiede von Chromium im Vergleich zu Google Chrome sind gering. Sie betreffen einige Einstellungen, Codecs sowie die Erweiterungen für Adobe Flash. Chromium ist in den Standard-Paketquellen von Ubuntu und Linux Mint enthalten. Streams von Amazon Video oder Netflix kann Chromium allerdings nicht wiedergeben. Dafür benötigen Sie Google Chrome (*www.google.de/chrome*) oder Firefox.
Eine weitere Alternative ist der Browser Vivaldi (*https://vivaldi.com*), der ebenfalls auf Chrome basiert und auch Videos von Amazon oder Netflix abspielen kann. Der Schwerpunkt bei Vivaldi liegt auf der Anpassungsfähigkeit. Tabs lassen sich in Tabgruppen organisieren, Sie können die Position von Tab- und Adressleiste festlegen, den Browser über konfigurierbare Kurzbefehle steuern und Notizen zu Webseiten erstellen.
Installation: In der LinuxWelt-Toolbox wählen Sie links oben die Rubrik „Netzwerk“ und klicken dann auf „Browser“. Sie finden hier Installationsanleitungen für alle genannten Webbrowser.



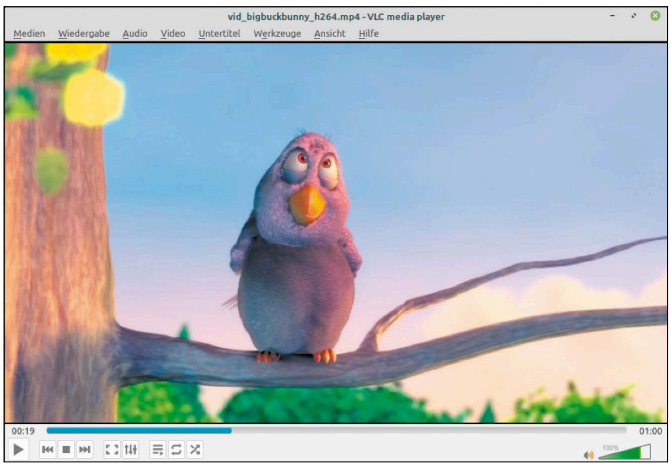
Telefonieren mit Linux: Für die aktuelle Linphone-Version verwenden Sie eine Flatpak-App. Das Programm beherrscht Sprach- und Videotelefonate sowie Chats.

7. E-Mail und Kommunikation

Das verbreitete E-Mail-Programm Thunderbird ist bei Ubuntu und Linux Mint bereits vorinstalliert. Wenn Sie mehr Funktionen benötigen, sollten Sie sich Evolution ansehen. Dabei handelt es sich um ein Groupwarepaket, das neben Mail auch Kalender, Adressbuch, Aufgabenlisten und Notizen bietet.
Eine weitere Alternative ist Kmail, vor allem für Nutzer des KDE-Desktops. Der Funktionsumfang von Kmail entspricht in etwa dem von Thunderbird. Für Groupwarefunktionen installieren Sie das Metapaket mit dem Namen „kdepim“. Darin sind neben Kmail unter anderen auch ein Adressbuch, Aufgaben- sowie Terminplaner enthalten. Das Programm Kontact („Persönliche Informationsverwaltung“) kann als Zentrale für diese Anwendungen genutzt werden.
Wer lieber per Chat kommuniziert oder ein bewegtes Bild des Gegenübers sehen will, kann Skype installieren. Aktuelle DEB- und RPM-Pakete gibt es bei Microsoft zum kostenlosen Download (*www.pcwelt.de/P3BHbX*). Wenn Sie Open-Source-Software bevorzugen, dann installieren Sie die Messenger Pidgin oder KDE-Telepathy. Beide unterstützen Netzwerkprotokolle wie ICQ, MSN, Jabber und Google Talk. Als Alternative zu Whatsapp gibt es auch für Linux eine Desktop-App von Telegram (*https://telegram.org*).
Als VoIP-Lösung für Sprach- und Videotelefonate sowie Chats lässt sich bei Ubuntu 18.04/19.10 und Linux Mint 19 Linphone installieren. In den Standardrepositorien finden sich allerdings nur ältere Versionen, weshalb Sie besser die Flatpak-App von der Webseite des Herstellers verwenden (*www.linphone.org*). Linphone gibt es auch für Windows, Mac-OS, Android und iOS.
Über das Programm oder direkt auf der Seite *https://www.linphone.org/freesip/* erstellen Sie ein Konto, das die kostenlose Kommunikation mit anderen Linphone-Nutzern ermöglicht. Wer einen Festnetzanschluss oder ein Mobiltelefon anrufen möchte, benötigt ein kostenpflichtiges Konto bei einem SIP-Anbieter, beispielsweise *www.sipgate.de*.
Installation: Klicken Sie in der LinuxWelt-Toolbox unter „Netzwerk“ auf „Kommunikation“. Hier finden Sie Schaltflächen oder Links zur Installation der genannten Programme sowie Befehlszeilen für die manuelle Einrichtung der Software. ■

Tools für Audio, Video & Foto

Linux-Nutzer können mehrere Mediaplayer verwenden, je nach gewünschtem Funktionsumfang. Außerdem stehen zahlreiche Tools bereit, mit denen sich Multimedia-Formate bearbeiten oder umwandeln lassen.



Filme abspielen: Der VLC Mediaplayer gibt alle verbreiteten Audio- und Videoformate wieder. Nur für kopiergeschützte DVDs benötigen Sie eine zusätzliche Programmbibliothek.

VON THORSTEN EGGELING

Im Bereich Multimedia müssen Linux-Nutzer auf nichts verzichten. Abspielprogramme für Musik und Filme sind vorinstalliert und es gibt Bildbetrachter und Programme für die Fotoverwaltung. Wem die Standardprogramme nicht reichen, sollte sich die Alternativen ansehen. Alle in diesem Artikel erwähnten Programme lassen sich über die LinuxWelt-Toolbox (auf Heft-DVD) installieren. Wählen Sie die Rubrik „Multimedia“ und steuern Sie mit der Schaltfläche darunter die gewünschten Tools an.

1. Mediaplayer für Linux

Bei Ubuntu taucht der Mediaplayer unter der Bezeichnung „Videos“ auf, Nutzer von Linux Mint finden im Menü unter „Multimedia“ die „Medienwiedergabe“. Ob die Player alle verbreiteten Audio- und Videoformate abspielen können, hängt davon ab, ob Sie bei der Installation die Option „Installation von Drittanbieterprogrammen“ aktiviert haben. Wenn nicht, installieren Sie diese Pakete nach:

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

Alternative Player: Der VLC-Player ist immer eine gute Wahl *(www.videolan.org)*, da er eigene Codecs mitbringt und alle gängigen Medienformate abspielt. Eine weitere Alternative ist Smplayer (*http://smplayer.sourceforge.net*). Dieses grafische Front-End für Mplayer hält den gesamten Funktionsumfang von Mplayer bereit. Wichtige Audio- und Videocodecs hat Smplayer ebenfalls an Bord.

Installation: In der LinuxWelt-Toolbox finden Sie Schaltflächen und Befehlszeilen für die Installation der Gstreamer-Plug-ins sowie von VLC und Smplayer per Klick auf „Mediaplayer“.

2. Videodateien bearbeiten und konvertieren

Mit Avidemux schneiden Sie Videodateien, recodieren in andere Formate oder verpacken Video- und Audiospuren ohne Qualitätsverlust neu (*http://fixounet.free.fr/avidemux*). In welchem Format das Ausgangsmaterial vorliegt, spielt keine Rolle, denn Avidemux kommt mit allen Formaten klar.

Videos konvertieren: Handbrake (*http://handbrake.fr*) wandelt Videos in das MKV- oder MP4-Container-Format mit h264- oder h265-Codec um. Eine umfangreiche Liste mit Konvertierungsprofilen für mobile Geräte und Internetplattformen erleichtert die Konfiguration. Bei Bedarf passen Sie auf den Registerkarten „Bild“ oder „Video“ die Einstellungen an. Mit Klick auf „Enkodierung starten“ beginnt die Konvertierung.

Installation: Avidemux gibt es als Appimage zum Download, das unter Ubuntu oder Linux Mint läuft. Handbrake ist im Standardrepositorium zu finden, neuere Versionen in einem PPA. Für die Installationen und weitere Infos klicken Sie in der LinuxWelt-Toolbox auf „Video bearbeiten“.

3. Videoeditoren für Ubuntu/Mint

Wer Videos nicht nur umwandeln, sondern bearbeiten möchte, kann das einsteigertaugliche Openshot verwenden (*www.openshot.org*). Schneiden und Trimmen sind intuitiv: Sie zerteilen einen Clip und löschen oder verschieben nach Rechtsklick auf den jeweiligen Teil den Abschnitt. Neben den Schnittfunktionen gibt es eine Reihe von Übergängen. Sie wählen den Effekt aus der Liste und ziehen ihn auf die entsprechende Spur. Über das Kommando „Datei → Video exportieren“ und Auswahl eines Profils schreiben Sie die geschnittene Fassung in eine neue Datei.

Weitere Videoeditoren für Linux sind Pitivi, Kdenlive und Cinelerra. Pitivi (*www.pitivi.*

org) ähnelt in Bedienung und Funktionsumfang Openshot. Kdenlive (*https://kdenlive.org*) und Cinelerra (*http://cinelerra.org*) bieten mehr Funktionen, benötigen aber Einarbeitungszeit.

Installation: Klicken Sie in der LinuxWelt-Toolbox auf „Videoeditoren“. Die Installation erfolgt über die zugehörige Schaltfläche meist aus den Standardrepositorien. Für neuere Versionen verwenden Sie die Downloadlinks oder Terminalbefehle.

4. Fotosammlungen verwalten

Für die Fotoverwaltung ist bei Ubuntu Shotwell vorinstalliert, bei Linux Mint Pix. Bilder lassen sich mit Stichwörtern versehen und es gibt einfache Bearbeitungsfunktionen. Wer mehr will, verwendet Digikam (*www.digikam.org*), das Fotos nach Alben, Tags, Stichwörtern sortieren und kategorisieren kann. Es enthält zahlreiche Tools für die Fotobearbeitung wie die Tonwert- oder Rote-Augen-Korrektur. Eine Unterstützung von RAW-Formaten ist vorhanden, jedoch ist Digikam kein Ersatz für Darktable und Rawtherapee.

Installation: Digikam, Darktable, Rawtherapee sind in den Paketquellen von Ubuntu und Mint enthalten. Zur Installation und für weitere Infos klicken Sie in der LinuxWelt-Toolbox auf „Fotos verwalten“.

5. Bilder unter Linux bearbeiten

Gimp (*www.gimp.org*) kann zwar auch Fotos bearbeiten, hat aber höhere Ansprüche – vergleichbar mit Photoshop. Gimp bietet Zeichenwerkzeuge, Ebenen, Masken, Automatikverbesserung und Filter. Sie können Fotos retuschieren, Bilder freistellen oder verfremden. Wie bei Photoshop erschließen sich die meisten Funktionen nicht auf Anhieb und bestimmte Effekte sind nur durch eine Kombination von Masken und Ebenen zu erreichen. Für Gimp gibt es aber viel Unterstützung – ein guter Einstieg ist die Dokumentation unter *www.gimp.org/docs*.

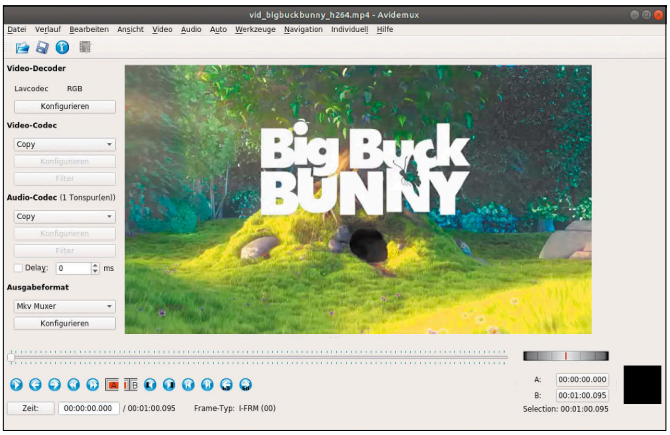
Installation: Gimp ist in den Standardrepositorien von Ubuntu und Linux Mint enthalten. Zur Installation und für weitere Infos klicken Sie in der LinuxWelt-Toolbox auf „Gimp“.

6. Tools für Audiodateien

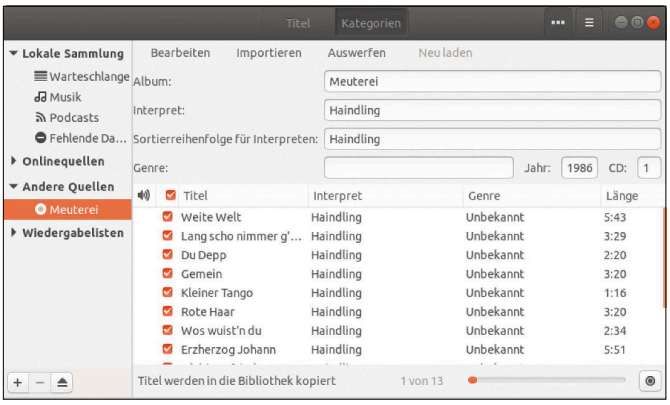
Rhythmbox – Standard unter Ubuntu und Linux Mint – kann Musikdateien wiedergeben und verwalten. Über „Importieren“ lassen sich Audio-CDs nach MP3 umwandeln. Über „Bearbeiten → Einstellungen“ legen Sie auf der Registerkarte „Musik“ das Ausgabeformat fest. Das Tool ermittelt über eine Internetabfrage Infos zur eingelegten CD und benennt die Audiodateien entsprechend.

Audacity ist das Tool der Wahl zum Bearbeiten und Aufnehmen von Audiodaten. Auf beliebig vielen Spuren lassen sich Audiodateien mischen, bearbeiten, mit Effekten versehen oder Hintergrundgeräusche entfernen. Audacity eignet sich zum Digitalisieren von Schallplatten oder zur Nachvertonung eigener Videos.

Installation: Klicken Sie in der LinuxWelt-Toolbox auf „Audio-Tools“. Installieren Sie Audacity über die zugehörige Schaltfläche.



Avidemux: Das Programm beherrscht den verlustlosen Schnitt fast beliebiger Videodateien. Das Tool arbeitet sehr schnell, wenn die Recodierung entfallen kann.



Musik verwalten und abspielen: Rhythmbox gibt Audiodateien wieder und kann auch Audio-CDs importieren. Die Tracks werden nach einer CDDB-Abfrage passend benannt.

DVD- UND BLU-RAY-WIEDERGABE

Um Video-DVDs abzuspielen, müssen Sie unter Ubuntu/Mint ein zusätzliches Paket installieren. Im Terminalfenster verwenden Sie diesen Befehl:

```
sudo apt-get install libdvd-pkg
```

Die angezeigten Meldungen bestätigen Sie mit „OK“ beziehungsweise „Ja“ und starten dann diesen Befehl:

```
sudo dpkg-reconfigure libdvd-pkg
```

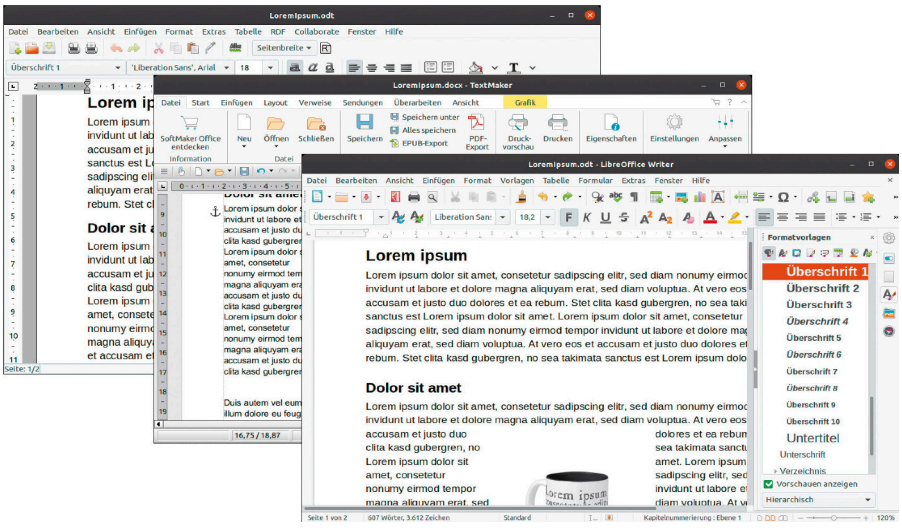
Beantworten Sie die Frage in der ersten Meldung mit „Ja“. Wenn Sie DVDs im Standardplayer abspielen möchten, installieren Sie zusätzlich das Paket „gstreamer1.0-plugins-bad“. Alternativ verwenden Sie den VLC Player.

Zur Zeit gibt es für Linux-Nutzer keine einfache Möglichkeit, verschlüsselte Blu-ray-Disks abzuspielen. Die Anleitung unter *https://wiki.archlinux.org/index.php/Blu-ray* ist eine Chance, aber keine Garantie, dass sich jede Blu-ray wiedergeben lässt. Eine Anleitung zur Installation der Bibliotheken für die Wiedergabe verschlüsselter DVDs lesen Sie in der LinuxWelt-Toolbox nach einem Klick auf „DVD/Blu-ray“.

Office-Pakete und Produktivität

Bei den meisten Desktopdistributionen steht direkt nach der Installation ein umfangreiches Office-Paket zu Verfügung. Mit zusätzlichen Programmen und Tools lässt sich die Arbeitsumgebung weiter ausbauen und effizienter nutzen.

VON THORSTEN EGGELING



Freie Wahl: Abiword, Textmaker Free und Libre Office Writer sind die beliebtesten Textprogramme unter Linux. Alle drei haben einen Funktionsumfang, der für die meisten Aufgaben ausreicht.

Libre Office bietet alles für typische Büroaufgaben: Textverarbeitung und Tabellenkalkulation, ein Präsentationsprogramm und ein Modul für Zeichnungen sind mit dabei. Ein Datenbankmodul lässt sich bei Bedarf ergänzen. Einige Distributionen, beispielsweise Lubuntu, setzen auf die leichtgewichtigere Kombination von Gnumeric (Tabellenkalkulation) und Abiword (Textverarbeitung). Welchen Funktionsumfang Sie tatsächlich benötigen, probieren Sie am besten selbst aus. Die meisten in diesem Artikel genannten Programme sind über die Paketverwaltung schnell installiert. Anleitungen und Links finden Sie in der LinuxWelt-Toolbox (auf Heft-DVD) unter „Office“.

1. Office-Pakete für Linux

Der Funktionsumfang von Libre Office (*www.libreoffice.org*) reicht wahrscheinlich für die meisten privaten Nutzer aus. In der Textverarbeitung lassen sich Briefe professionell formatieren und die Tabellenkalkulation hilft bei Berechnungen. Probleme sind zu erwarten, wenn Sie häufig Dokumente mit Nutzern von Microsoft Office austauschen müssen. Die vollständige Übernahme der Formatierungen ist vor allem bei komplexeren Dokumenten nicht garantiert. Wer darauf angewiesen ist, nutzt unter Linux Microsoft Office in einer virtuellen Maschine. Informationen dazu gibt es in der LinuxWelt-Toolbox in der Rubrik „Ubuntu/Mint“ nach einem Klick auf „Virtualisierung“.

Mehr Kompatibilität zu Microsoft-Produkten verspricht Softmaker Office (*www.softmaker.de*). Die Importfilter sind besser als die von Libre Office. Wer das ausprobieren möchte, kann sich bei Softmaker eine kostenlose 30-Tage-Demo herunterladen. Die Vollversion Softmaker Office Standard 2018 kostet 79,95 Euro. Für 99,95 Euro gibt es Softmaker Office Professional 2018, das mit dem Duden-Korrektor eine leistungsfähige Rechtschreibprüfung enthält. Außerdem können Sie die Gratisversion Free Office (*www.freeoffice.com*) nutzen, die sich nur in Kleinigkeiten von der Kaufversion unterscheidet (siehe *https://www.freeoffice.com/de/vergleich*).

Installation: Libre Office ist in der Regel standardmäßig eingerichtet und steht in den Standard-Paketquellen bereit. Wer eine aktuellere Version installieren möchte, verwendet die Anleitung aus der LinuxWelt-Toolbox in der Rubrik „Office“.

2. Erweiterungen für Libre Office

Über Erweiterungen (*http://extensions.libreoffice.org*) erhält Libre Office zusätzliche Funktionen. Empfehlenswert ist die verbesserte Rechtschreib- und Grammatikprüfung Language Tool (*www.languagetool.org*). Die Installationsanleitung liefern wir Ihnen in der LinuxWelt-Toolbox (Schaltfläche „Office-Pakete“).

Sie können selbst Makros für Libre Office erstellen, um häufig wiederkehrende Arbeitsschritte zu automatisieren. Komplexere Programme, sogar mit einer eigenen Benutzeroberfläche, sind ebenfalls möglich, erfordern jedoch Programmierkenntnisse. Den Einstieg in die Makroprogrammierung erleichtert der Makrorecorder, mit dem Sie Menüklicks sowie Tastatureingaben aufzeichnen und später wiedergeben. Informationen zu Makros und einige nütz-

liche Beispiele haben wir in der LinuxWelt-Toolbox untergebracht (Schaltfläche „Makros für Libre Office“).

3. Alternative Office-Programme

Wer ab und zu einen Brief schreibt, für den kann auch Abiword ausreichend sein (*www.abiword.org*). Die Bedienung ist einfach und orientiert sich an den Standards von Libre Office und Word 2003. Abiword benötigt kaum Systemressourcen und ist Standard bei leichtgewichtigen Linux-Distributionen. Das Gleiche gilt auch für die Tabellenkalkulation Gnumeric (*www.gnumeric.org*). Den Funktionsumfang von Excel erreicht das Programm nicht, dafür gibt es aber ausgefeilte finanzmathematische Funktionen und ein gut bedienbares Modul, mit dem sich Graphen erzeugen lassen.

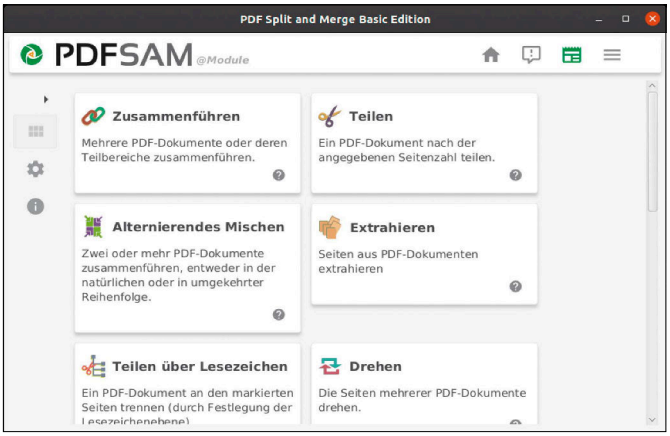
Mit Scribus layouten Sie Broschüren, Zeitschriften und mehr (*www.scribus.net*). Das Programm beherrscht professionellen Textsatz und kann Dokumente so für den Druck vorbereiten, dass auch die Farben stimmen (CMYK-Farbseparation).

Calibre ist ein plattformunabhängiges Programm zur Verwaltung und Konvertierung von E-Books (*http://calibre-ebook.com*). Es kennt alle gängigen Formate wie Epub, LRF, Mobi und PDF. Außerdem lassen sich die Inhalte auf E-Book-Readern übertragen.

Installation: Informationen zu den genannten Tools finden Sie in der LinuxWelt-Toolbox über die Schaltfläche „Office-Programme“.



Anspruchsvolle Broschüren: In Scribus arbeiten Sie mit Text- und Bildrahmen, was ein professionelles Layout beispielsweise für Flyer, Zeitschriften und andere Druckwerke erlaubt.



Tools für PDFs: PDF Split and Merge kann PDF-Dateien bearbeiten. Sie können beispielsweise PDFs neu aufteilen, zusammenführen oder einzelne Seiten entnehmen.

4. Produktive Desktoptools

Die Dateimanager unter Ubuntu und Linux Mint bieten eine Suchfunktion, mit der Sie Ordner und Dateien über ihren Namen finden. Wenn Sie auch Dateiinhalte finden wollen, benötigen Sie ein Tool wie Docfetcher (*http://docfetcher.sourceforge.net*). Das Programm leistet eine Volltextsuche für Libre und Microsoft Office, Abiword, PDF, Epub sowie Textdateien aller Art. Docfetcher arbeitet mit einem Index, den Sie zunächst für das gewünschte Verzeichnis erstellen. Die Volltextsuche arbeitet mit logischen Operatoren und zeigt eine Vorschau der Fundstellen.

Das Tool Recoll (*www.lesbonscomptes.com/recoll*) leistet Ähnliches, bietet aber eine fortgeschrittene Abfragesyntax. Sie können Suchabfragen formulieren, die das Suchergebnis auf Metadaten wie Autorenname oder Schlüsselwörter eingrenzen. Recoll bringt außerdem einen eigenen Webserver mit, mit dessen Hilfe Sie anderen PCs im Netzwerk die Suche im Browserfenster zur Verfügung stellen.

Installation: Docfetcher ist ein portables Tool für alle Betriebssysteme und benötigt eine Java-Runtime (Paket: „default-jre“). Sie müssen es nur herunterladen und entpacken. Recoll lässt sich unter Ubuntu und Linux Mint direkt installieren. Lesen Sie dazu die Anleitung in der LinuxWelt-Toolbox nach einem Klick auf „Desktop-Tools“.

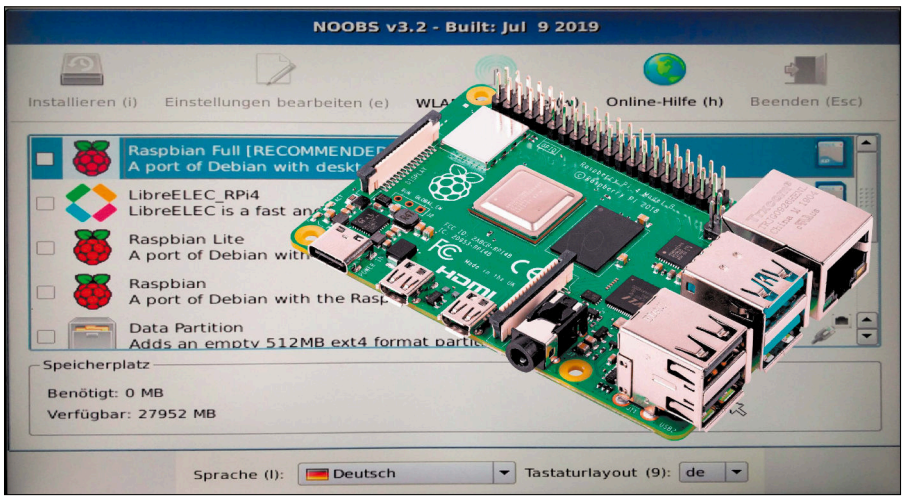
5. PDFs erstellen und bearbeiten

Mit den genannten Office-Paketen (siehe Punkt 1) lassen sich Dokumente im PDF-Format speichern. Libre Office kann PDFs auch öffnen und bearbeiten, mit Inkscape geht das ebenfalls, allerdings nur mit einzelnen Seiten. Da PDF ein Format für die Archivierung von Dokumenten und den Druck ist, sind der Nachbearbeitung Grenzen gesetzt. PDFs lassen sich jedoch ohne Problem aufteilen, Sie können einzelne Seiten extrahieren, hinzufügen, löschen oder drehen. Ein geeignetes Tool dafür ist PDF-Shuffler (Paket: „pdfshuffler“, Ubuntu 19.10: „pdfarranger“). Noch mehr Funktionen und eine ansprechende grafische Oberfläche bietet PDF Split and Merge (Paket: „pdfsam“). Es kann Dokumente zusammenfügen und zerteilen, Seiten drehen und umsortieren. Sie können Dokumente per Maus zusammenstellen und sehen dabei stets eine Vorschau des fertigen PDFs.

Installation: PDF-Shuffler ist in den Standardrepositorien enthalten. Aktuelle Versionen von PDF Split and Merge gibt es auf der Downloadseite des Herstellers. In der LinuxWelt-Toolbox finden Sie nach einem Klick auf „PDF-Tools“ eine Anleitung zu Installation und Downloadlinks. ■

Software für Platinenrechner

Der Erfolg des Raspberry Pi hat die Entwicklung von Mini-PCs vorangetrieben. Dank geringer Leistungsaufnahme eignen sich die Geräte hervorragend als Dateiserver oder Mediacenter am TV-Gerät.



Einfache Installation: Die Noobs-Dateien kopieren Sie auf eine FAT32-formatierte SD-Karte. Das gewünschte Betriebssystem wählen Sie dann direkt auf dem Raspberry Pi.

VON THORSTEN EGGELING

Mini-PCs gibt es in unterschiedlichen Preislagen und mit mehr oder weniger leistungsfähiger Hardware. Nicht jeder Platinenrechner eignet sich für beliebige Einsatzbereiche. Für Dateiserver sind Gigabit-Ethernet und USB 3.0 oder ein SATA-Adapter wünschenswert, für die Medienwiedergabe ein Grafikchip mit Hardwarebeschleunigung. Der Raspberry Pi 4 deckt die meisten Bereiche ab, weshalb wir uns hier auf dieses Gerät konzentrieren. Informationen zu anderen Mini-PCs, Downloadlinks und die Befehlszeilen aus diesem Artikel liefert die LinuxWelt-Toolbox (auf Heft-DVD) in der Rubrik „Platinenrechner".

1. Systeme für den Raspberry Pi

Der Installer Noobs (*www.raspberrypi.org/downloads/noobs*) – „New Out Of Box Software" – ist für Raspberry-Einsteiger der einfachste und schnellste Weg für die Systeminstallation. Die Standardversion (2,4 GB) enthält bereits das Desktopsystem Raspbian („Full"), das auf Debian basiert und die Multimedia-Zentrale Libre Elec mitbringt. Sie können während der Installation auch Raspbian Lite ohne Desktopumgebung herunterladen. Bei der Noobs-Lite-Variante (38 MB) laden Sie das gewünschte System immer während der Installation herunter.

Entpacken Sie Noobs auf eine FAT32-formatierte SD-Karte mit mindestens acht GB Kapazität. Anschließend legen Sie die Karte in den Raspberry ein. Im unteren Bereich des Fensters wählen Sie als Sprache „Deutsch" und stellen bei „Tastaturlayout" den Wert „de" ein. Setzen Sie ein Häkchen vor dem gewünschten Betriebssystem, klicken Sie auf „Installieren" und folgen Sie den weiteren Anweisungen des Assistenten.

Wenn Sie mehrere Systeme wählen, muss die SD-Karte genug Platz bieten. Den benötigten und verfügbaren SD-Speicher zeigt Noobs an. Planen Sie Reserven ein, damit Updates und zusätzliche Software auf die SD-Karte passen. Beim Start wählen Sie im Bootmenü das gewünschte System, das zuletzt verwendete startet nach kurzer Wartefrist automatisch. Drücken Sie beim Start die Shift-Taste, sobald die Aufforderung dazu erscheint, um wieder auf die Noobs-Oberfläche zu gelangen. Hier können Sie die Systemauswahl ändern oder ein weiteres System installieren. Dabei wird ein bereits vorhandenes System allerdings überschrieben, was einer Neuinstallation entspricht.

Hinweis: Noobs kommt manchmal nicht mit SD-Karten größer 32 GB zurecht, auch wenn diese mit FAT32 formatiert sind und zumindest ab Raspberry Pi 3 auch Karten mit mehr als 256 GB funktionieren sollten. In diesem Fall laden Sie das Abbild des gewünschten Systems herunter und kopieren es auf die SD-Karte, wie in der LinuxWelt-Toolbox unter „Systeme für den Pi" beschrieben.

Noch mehr Systeme: Über *www.raspberrypi.org/downloads* finden Sie weitere Betriebssysteme für den Raspberry Pi, beispielsweise Ubuntu Mate, Ubuntu Server, das Mediacenter OSMC und Windows 10 IoT Core. Der Inhalt der heruntergeladenen Abbilddatei muss auf die SD-Karte kopiert werden. Detaillierte Anleitungen dazu finden Sie in der LinuxWelt-Toolbox („Systeme für den Pi").

Installation: In der LinuxWelt-Toolbox finden Sie in der Rubrik „Platinenrechner“ Downloadlinks und Beschreibungen wichtiger Betriebssysteme für den Raspberry Pi.

2. Raspberry Pi als Dateiserver

Wenn Sie einen Raspberry Pi als Datenspeicher im Netzwerk bereitstellen wollen, installieren Sie unter Raspbian das Programmpaket „samba“. Da Samba eine eigene Benutzerdatenbank verwendet, benutzen Sie folgenden Befehl, um für den Standardbenutzer „pi“ ein Passwort festzulegen:

```
sudo smbpasswd -a pi
```

Das genügt, um über einen Dateimanager unter Linux oder Windows eine Verbindung herzustellen. Standardmäßig ist das Home-Verzeichnis schreibgeschützt freigegeben. In Nautilus oder Nemo tippen Sie beispielsweise folgende URL in die Adresszeile ein (einblenden mit Strg-L).

```
smb://[Raspberry]/pi/
```

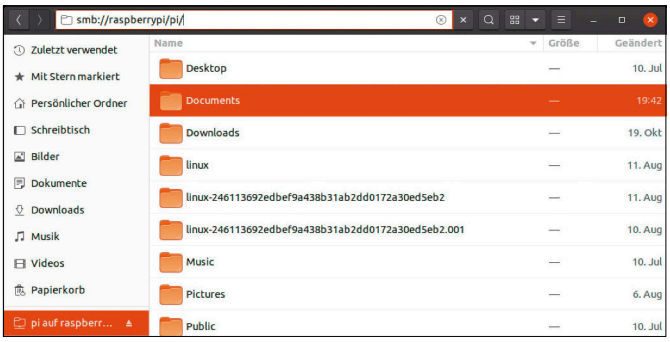
Den Platzhalter „[Raspberry]“ ersetzen Sie durch den Hostnamen oder die IP-Adresse des betreffenden Raspberry Pi. Sie haben dann Lesezugriff auf das Home-Verzeichnis des Benutzers „pi“.

Installation: Die Befehlszeilen zur Installation und Konfiguration des Samba-Servers finden Sie in der LinuxWelt-Toolbox nach einem Klick auf „Datenserver“. Hier erfahren Sie auch, wie Sie den Lesezugriff auf das Home-Verzeichnis aktivieren und andere Ordner freigeben.

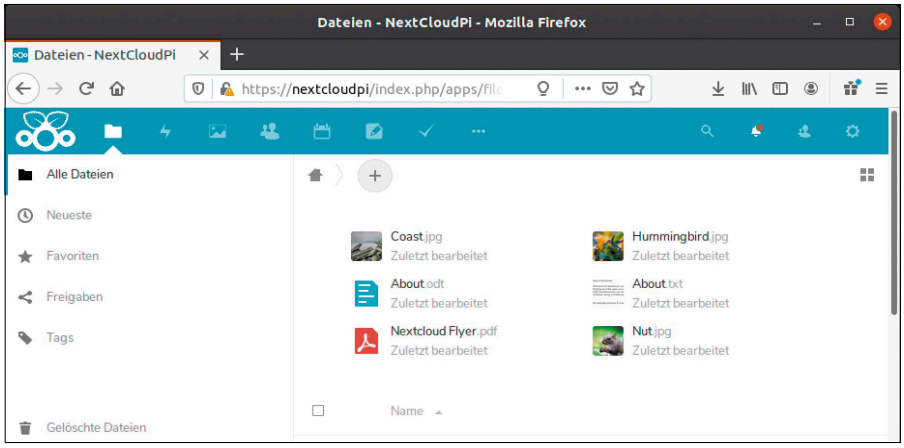
3. Raspberry Pi als Cloudserver

Nextcloud (*https://nextcloud.com*) bietet fast alles, was für den Datenaustausch über das lokale Netzwerk oder Internet erforderlich ist, beispielsweise Kalender, Adressbuch, Fotogalerie, Wiedergabe von und Musik und Videos sowie gemeinsames Arbeiten an Dokumenten. Über Plug-ins lassen sich die Funktionen noch erweitern. Der Zugriff erfolgt über eine Weboberfläche oder Sie verwenden eine Clientsoftware für Windows, Mac-OS, Linux, Android oder iOS, um einen lokalen Ordner mit dem Cloudserver zu synchronisieren.

Nextcloud lässt sich auf dem Raspberry Pi entweder als Neuinstallation fertig vorbereitet zusammen mit Raspbian oder nachträglich in einem laufenden Raspbian einrichten. Die erste Variante ist vorzuziehen, außer Sie betreiben bereits ein auch für andere Dienste konfiguriertes Raspbian. In der LinuxWelt-Toolbox finden Sie ausführliche Anleitungen für beide Wege. Soll der heimische Nextcloud-Server auch aus dem Internet erreichbar sein, richten Sie einen Dienst für dynamische IP-Adressen ein. Wie das geht, erfahren Sie in der LinuxWelt-Toolbox unter „Netzwerk → Portweiterleitung“. ■



Freigaben im Netzwerk: Samba verwandelt den Raspberry Pi in einen Dateiserver. Ohne weitere Konfiguration ist der Zugriff auf das Home-Verzeichnis des Benutzers „pi“ möglich.



Die eigene Cloud: Nextcloud vereinfacht den Datenaustausch über das lokale Netzwerk und das Internet. Der Funktionsumfang lässt sich über zusätzliche Apps erweitern.

BEISPIELPROJEKTE FÜR DEN RASPBERRY PI

In der LinuxWelt berichten wir regelmäßig über nützliche Raspberry-Pi-Projekte. Mit einem Stück Extrasoftware oder zusätzlicher Hardware lässt sich das Gerät vielfältig einsetzen. Ausführliche Anleitungen lesen Sie in der LinuxWelt-Toolbox in der Rubrik „Platinenrechner“.

Kontrolle per LCD: Oft verrichtet ein Raspberry Pi im Netzwerk ohne Monitor und Eingabegeräte seine Dienste – meist genügt ein gelegentlicher Besuch per SSH. Ein günstiges LCD zur Ausgabe von Systeminformationen macht die Platine aber gesprächiger.

Werbeblocker für das Netzwerk: Das Projekt Pi-Hole ist nicht nur ein schwarzes Loch für Werbung, sondern es blockiert auch Tracker, die Ihr Surfverhalten verfolgen und monetarisieren möchten. Die Software läuft auch auf dem Raspberry Pi, klinkt sich in Ihr Netzwerk ein und arbeitet auf DNS-Basis.

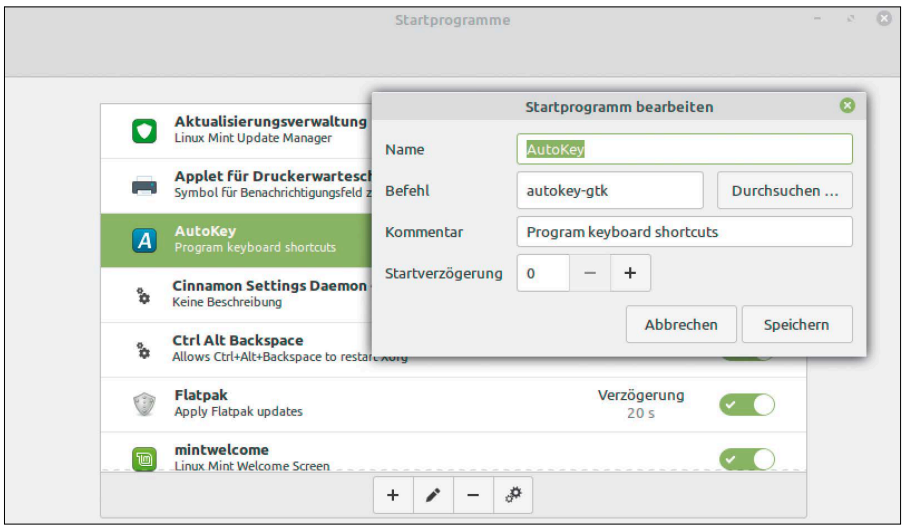
Pi als Webcam: Der Raspberry Pi lässt sich für etwa 30 Euro mit einer Kamera ausstatten. Per Script laden Sie Einzelbilder regelmäßig auf einen Webserver hoch. Wenn Sie Live-Videostreams bevorzugen, gibt es auch dafür eine Lösung. Das System lässt sich damit auch für die Raumüberwachung mit automatischer Bewegungserkennung einsetzen.

Streamingdienste einbinden: Um die Musiksammlung aus Streamingdiensten in den eigenen vier Wänden über Lautsprecher auszugeben, bietet sich der Raspberry Pi als einfache und preiswerte Lösung an.

Tools für die Linux-Automatisierung

Regelmäßige Aufgaben wie beispielsweise Backups lassen sich unter Linux automatisch durchführen. Mit Shell-Scripts und Zusatztools können Sie aber praktisch jedes Vorhaben automatisieren.

VON THORSTEN EGGELING



Programme automatisch starten: Soll ein Programm direkt nach der Anmeldung sofort zur Verfügung stehen, erstellen Sie dafür einen Eintrag mit „Startprogramme“.

Linux erledigt schon von Haus aus einige Aufgaben automatisch im Hintergrund. Das System erstellt beispielsweise Backups wichtiger Konfigurationsdateien, archiviert Logdateien und prüft auf Updates. Die Infrastruktur lässt sich für eigene Backup-Scripts oder andere regelmäßige Wartungsarbeiten nutzen. Automatisierung ist auch sinnvoll, wenn Sie mehrere Arbeitsschritte nacheinander häufig ausführen müssen. Dabei hilft ein einfaches Script für die Bash-Shell, das Sie manuell, zeitgesteuert oder per automatische Ordnerüberwachung starten. Hilfetexte und Befehlszeilen für die Installation von Automatisierungswerkzeugen finden Sie in der LinuxWelt-Toolbox (auf Heft-DVD) in der Rubrik „Automatisierung“.

1. Programme automatisch starten

Bei der Anmeldung automatisch startende Programme gehören zum Repertoire jedes Desktopsystems. Zur Verwaltung suchen Sie unter Ubuntu über „Aktivitäten“ nach „Startprogramme“, bei Linux Mint gehen Sie im Menü auf „Einstellungen → Startprogramme“. Über „Hinzufügen“ beziehungsweise die Plus-Schaltfläche lassen sich Programme in den Autostart aufnehmen. Das ist bei einigen Systemtools nützlich (siehe Punkt 2), es kann sich aber um beliebige Programme handeln. In der Regel genügt hinter „Befehl“ der Programmname ohne Pfad. Mint-Nutzer können eine Startverzögerung einstellen, damit das System unmittelbar nach der Anmeldung nicht zu sehr belastet wird.

2. Textbausteine und Scripts mit Autokey

Das englischsprachige Autokey ist ein vielseitiges Tool für systemweite Textbausteine bis hin zu raffinierten Scripts. Sie legen damit Textbausteine an, die Sie über ein Kürzel oder eine Tastenkombination in einen Editor, die Textverarbeitung, das E-Mail-Programm oder das Terminalfenster einfügen. Autokey beherrscht außerdem Scripts, um komplexere Aufgaben der Automatisierung zu erledigen.

Autokey ist in den Paketquellen von Ubuntu 16.04, 18.04 und 19.10 enthalten (Paket: „autokey-gtk“). Das Programm lässt sich standardmäßig über ein Panel-Icon steuern, was bei Ubuntu 18.04 und 19.10 jedoch nicht erscheint, bei Linux Mint 19 sehen Sie es in der Leiste am unteren Bildschirmrand. Wie Sie Ubuntu dazu bringen, Autokey automatisch zu starten und das Panel-Icon anzuzeigen, lesen Sie in der LinuxWelt-Toolbox nach einem Klick auf „Autokey“. Hier finden Sie neben der Installationsanleitung auch Tipps zur Konfiguration und Beispiel-Scripts.

3. Zeitgesteuerte Tasks mit Cron

Auf Linux-Systemen läuft ein Crondienst, der Aufgaben zeitgesteuert ausführt. Cron nutzt eine systemweite Datei „/etc/crontab“, die für alle Benutzer gilt und im Terminal mit root-Recht bearbeitet werden kann:

```
sudo crontab -e
```

Zusätzlich kann jeder Benutzer in einer eigenen Crontab Programme laden, indem er *crontab -e* ohne „sudo“ aufruft. Crontab-Einträge benötigen fünf Zeitangaben (Minute, Stunde, Tag, Monat, Wochentag) mit Leerzeichen oder Tabulatoren getrennt, danach den Programmbefehl. Ein Backup, das täglich um 22:00 Uhr laufen soll, kann dann so aussehen:

```
0  22  *  *  *  rsync -av /home/sepp/
  /media/sepp/USB/backup
```

Der Asterisk (*) bedeutet wie üblich „alle“ an der betreffenden Stelle – hier also „an jedem Tag, jedem Monat und jedem Wochentag“. Um Formatfehler bei relativ einfachen Zeitangaben zu vermeiden, gibt es simplifizierende Variablen, die Sie anstelle der fünf Zeitangaben verwenden können (@hourly, @daily, @weekly, @midnight). So ist etwa die Variable „@midnight“ identisch mit der ausgeschriebenen Schreibweise „0 0 * * *“. Einen ausführlichen Beitrag zu Cron finden Sie in der LinuxWelt-Toolbox nach einem Klick auf „Cronjobs“.

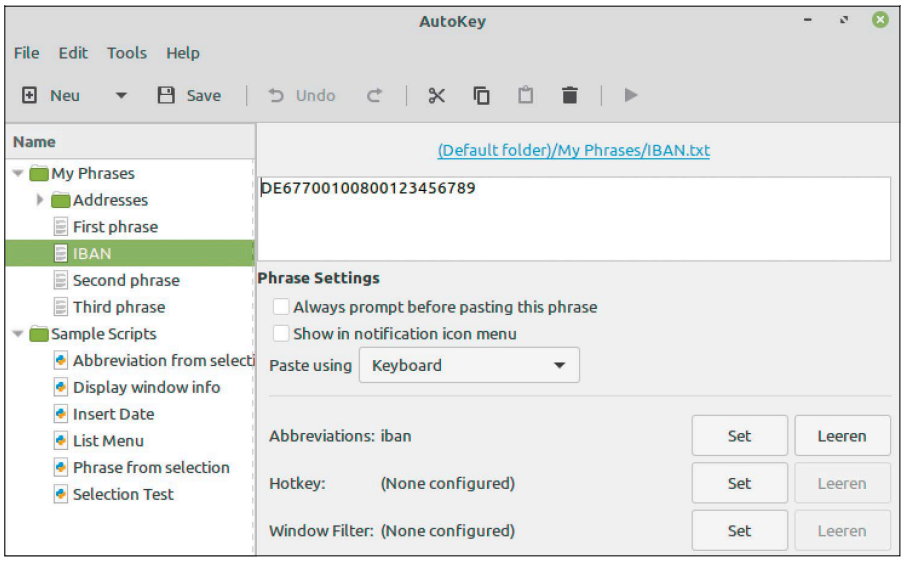
4. Crontab mit grafischen Tools bearbeiten

Bei Systemen mit KDE-Desktop (Kubuntu) installieren Sie das Paket „kde-config-cron“. In den „Systemeinstellungen“ lassen sich dann unter „Starten und Beenden → Aufgabenplaner“ Zeitpläne für den automatischen Start erstellen. Für Ubuntu und Linux Mint eignet sich das Tool Gnome-Schedule. Es ist jedoch nicht in den Paketquellen enthalten und es gibt auch kein PPA. Sie können das Tool aber selbst kompilieren. Die Anleitung dazu finden Sie in der LinuxWelt-Toolbox nach einem Klick auf „Aufgaben planen“.
Gnome-Schedule bietet auch eine Möglichkeit, definierte Aktionen über das Tool at einmalig zu einem bestimmten Zeitpunkt auszuführen. Die wichtigsten Intervalle wie „Jeden Tag“ finden Sie klickfertig vor und die „Vorschau“ bietet in der Form „An jedem Tag um 01:00“ eine gute Kontrolle.

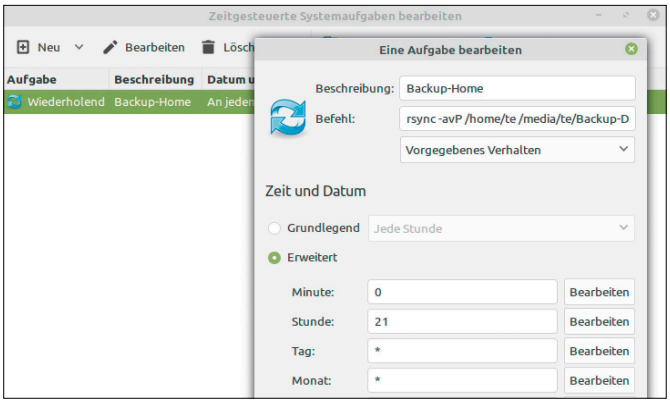
5. Automatische Datensicherung

Backups anzulegen ist unverzichtbar. Sie müssen die nötigen Vorkehrungen jedoch nur einmal treffen, den Rest übernimmt Linux automatisch. Das Kommandozeilentool rsync arbeitet zuverlässig und schnell und ist in allen verbreiteten Linux-Distributionen standardmäßig enthalten. Es lässt sich mit zahlreichen Schaltern und Optionen für jede Aufgabe anpassen, im Alltag genügen aber einige wenige.
Backups sollten immer auf unabhängige Datenträger erfolgen – etwa auf eine zweite interne Festplatte oder ein USB-Laufwerk. Für ein einfaches manuelles Backup des eigenen Home-Verzeichnisses auf eine USB-Festplatte genügt folgendes Kommando:

```
rsync -avP $HOME /media/$USER/
  [Laufwerks-ID]/backup
```



Textbausteine: Häufig genutzte Textabschnitte legen Sie in Autokey fest. Über ein Kürzel lässt sich der Text dann in jedem beliebigen Programm einfügen.



Automatisierte Aufgaben: In Gnome-Schedule erstellen Sie Cronjobs für einmalige oder wiederkehrende Aufträge. Das eignet sich etwa für regelmäßige Backups.

Die „Laufwerks-ID“ ist die Bezeichnung einer USB-Festplatte, die Linux automatisch unter „/media/$USER“ eingebunden hat. Ändern Sie den Pfad entsprechend Ihrer Systemkonfiguration. „$USER“ ist eine Standardvariable für den Namen des Benutzers, „$HOME“ für den Pfad zum Home-Verzeichnis. Das Ziel „backup“ erstellt rsync automatisch, wenn es noch nicht vorhanden ist.
Backup-Script für rsync: Klicken Sie in der LinuxWelt-Toolbox auf „Rsync“. Hier finden Sie ein Shell-Script für inkrementelle Backups und Infos zu erweiterten Funktionen sowie Backups über SSH. Über die Aufgabenplanung (siehe Punkt 3 und 4) erstellen Sie einen Zeitplan für regelmäßige Backups.

6. Scripts und Ordnerüberwachung

Shell-Scripts sind Textdateien, die interne Shell-Befehle und Programmaufrufe enthalten. Im einfachsten Fall bringen Sie in einem Script nur einen oder mehrere Programmnamen sowie die gewünschten Optionen oder Parameter unter. Variablen, Schleifen („for … do … done“) und Bedingungen („if … fi“) ermöglichen komplexere Programmstrukturen.
In der LinuxWelt-Toolbox finden Sie nach einem Klick auf „Shell-Scripts“ einige Beispiele. Diese zeigen, wie sich Audio- und Bilddateien konvertieren oder Screenshots erstellen lassen. Shell-Scripts rufen Sie bei Bedarf manuell auf oder zeitgesteuert über einen Cronjob.
Für einige Aufgaben ist auch der automatische Aufruf per Ordnerüberwachung sinnvoll. Wie Sie diese einrichten, erfahren Sie nach einem Klick auf „Incron“. Mit diesem eleganten, aber nicht ganz einfachen Mechanismus können Sie dann beispielsweise Audiodateien automatisch in ein anderes Format umwandeln, sobald diese in einem bestimmten Ordner landen. ■

Service- & Mobilsysteme

Linux-Systeme sind flexibel und starten von jeder Art Datenträger. Auf einem USB-Stick oder einer USB-Festplatte lässt sich schnell ein Zweit- oder Reparatursystem einrichten.



Aus der LinuxWelt-Redaktion stammen die LinuxWelt-Rettungs-DVD (Linux-Wartung), das LinuxWelt-Surfsystem und die PC-WELT-Rettungs-DVD (Windows-Tools).

VON THORSTEN EGGELING

Mit Linux-Livesystemen kommen Sie spätestens bei der Installation von Ubuntu oder Linux Mint in Kontakt. Beide lassen sich von einer DVD oder einem USB-Stick starten und bieten einen ersten Eindruck von der Gestaltung des Desktops. Enthalten sind viele Programme, die Sie später auch beim installierten Linux nutzen, beispielsweise Firefox und Libre Office. Sollte ein Tool fehlen, lässt es sich auch im Livesystem installieren. Der Datenträger ist jedoch schreibgeschützt, sodass zusätzliche Programme bei einem Neustart wieder verschwunden sind. Das ist in den meisten Fällen auch erwünscht, damit das System immer in einem definierten Zustand startet und nicht manipuliert werden kann. Livesysteme eignen sich daher gut als sichere Surfumgebung.

1. Livesysteme für jeden Zweck

Installations-DVDs etwa vom Ubuntu oder Linux Mint eignen sich für Reparaturen, wenn das Hauptsystem einmal streikt. Auf die Version kommt es nicht an. Mit neueren Linux-Versionen lassen sich auch ältere Systeme reparieren. Nur die Architektur sollte übereinstimmen (32 oder 64 Bit).
Sie können beispielsweise die Dateien aus Ihrem Home-Verzeichnis sichern oder die Bootumgebung reparieren. Livesysteme sind außerdem so konstruiert, dass sich temporär Reparaturtools oder Analysesoftware nachinstallieren lassen. Allerdings überdauern hinzugefügte Dateien keinen Neustart. Auf einem USB-Stick lässt sich Ubuntu/Mint jedoch so einrichten, dass Programme und Konfiguration erhalten bleiben.
In der LinuxWelt-Toolbox (auf Heft-DVD) bieten die ersten vier Einträge in der Rubrik „Service/Mobil-Systeme“ eine Übersicht mit den wichtigsten Livesystemen. Sie erfahren, was Sie beim Umgang mit den heruntergeladenen ISO-Dateien und beim Transfer auf einen USB-Stick beachten müssen.
Außerdem finden Sie Tipps zur Auswahl eines für Ihre Zwecke geeigneten Systems, ausführliche Installationsanleitungen und Downloadlinks.

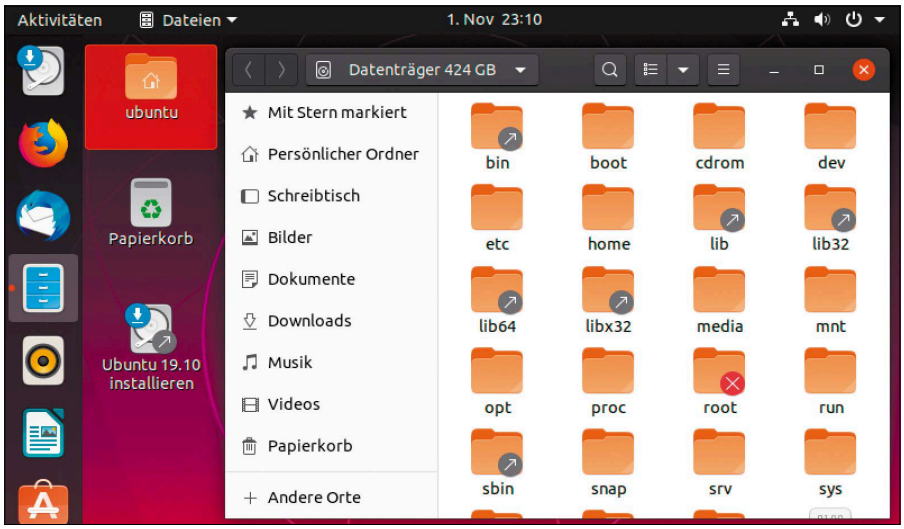
2. Linux mit Zweitsystem reparieren

Über ein Livesystem erhalten Sie Zugriff auf die Partitionen eines installierten Betriebssystems. Das lässt sich nutzen, wenn Sie das Passwort vergessen haben, die Konfigurationsdateien bearbeiten oder den Bootmanager reparieren müssen.
Die LinuxWelt-Rettungssystem (*www.pcwelt.de/uqtBiY*) startet schnell und ist auf die Wartung von Linux-Installationen spezialisiert. Das System startet standardmäßig mit der grafischen Oberfläche XFCE und deutscher Tastaturbelegung. Im LinuxWelt-Rettungssystem sind der Dateimanager Thunar, Firefox und Filezilla installiert. Festplattenabbilder lassen sich mit Clonezilla erstellen, Partitionen verwalten Sie mit Gparted. Nach dem Start zeigt der Desktop automatisch ein Terminal mit root-Recht, in dem Sie die üblichen Linux-Tools für die Kommandozeile verwenden und beispielsweise Partitionen per mount-Befehl einhängen können. Als bequemer Dateimanager für das Terminalfenster ist außerdem der Midnight Commander (mc) installiert. Eine Anleitung mit praktischen Tipps erreichen Sie in der LinuxWelt-Toolbox per Klick auf „LinuxWelt-Rettungs-DVD“.

3. Windows mit Linux retten

Einige Windows-Probleme lassen sich nur über ein Zweitsystem beheben. Das ist beispielsweise nötig, wenn Windows nicht mehr startet und Sie nur einige wichtige Dokumente sichern wollen.

Die PC-WELT-Rettungs-DVD (*www.pcwelt.de/pcwrescue*) enthält spezielle Tools für Windows-Systeme, kann aber auch für Linux wertvolle Dienste leisten. Sie können den Browser Firefox für die Recherche im Internet nutzen, außerdem sind Clonezilla und Gparted an Bord. Nach einem Klick auf „Rettungswerkzeuge“ sehen Sie die Menüeinträge für Tools, mit denen Sie das Windows-Passwort löschen, gelöschte Dateien („QPhotorec“) wiederherstellen oder nach Schadsoftware („ClamAV“) suchen können. Wenn möglich, sollten Sie das PC-WELT-Rettungssystem von einem USB-Stick booten. Es startet dann schneller. Wie Sie die PC-WELT Rettungs-DVD auf einem USB-Stick einrichten – auch mit permanentem und verschlüsseltem Speicher – erfahren Sie in der LinuxWelt-Toolbox unter „PC-WELT Rettungs-DVD“.



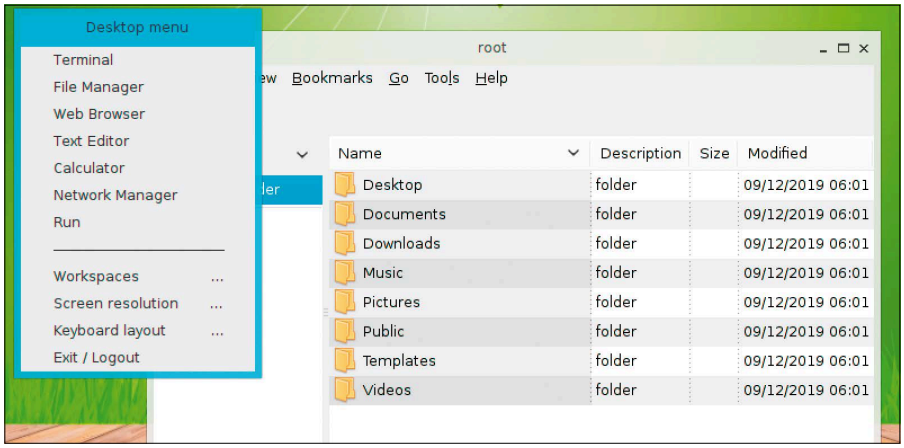
Das Ubuntu-Installationsmedium genügt für viele Reparaturen, Konfigurationsänderungen und die Datenrettung. Weitere Tools lassen sich nachinstallieren.

4. Mini-Linux- und Surfsysteme

Das LinuxWelt-Surfsystem bietet eine komfortable deutschsprachige Desktopumgebung. Es ist nur rund 500 MB groß und enthält die Browser Chromium, Firefox sowie Vivaldi. Außer den Browsern stehen im Livesystem der Partitionierer Gparted, der Mediaplayer Audacious sowie der Gnome Mplayer zur Verfügung. Zur Übertragung auf USB-Stick verwenden Sie im laufenden System das Tool unter „Applications → System Tools → create live USB“. Das dazu abgefragte root-Passwort lautet „toor“.

Slax gehört zu den wirklich kleinen und schnellen Livesystemen (264 MB): Viel mehr als ein Browser, Mediaplayer und ein rudimentärer Desktop ist nicht dabei. Über einen Rechtsklick auf den Desktophintergrund aktivieren Sie im Menü „Keyboard Layout → German“ das deutsche Tastaturlayout. Ein Klick auf das Starter-Symbol rechts unten blendet die verfügbaren Programme ein, inklusive dem „Net Manager“ zum Aufbau einer WLAN-Verbindung. Außerdem gibt es als grafischen Dateimanager den kleinen Pcmanfm von LXDE.

Neben dem Browser Chromium sind das Terminal, Texteditor und Taschenrechner dabei. Weitere Softwarepakete gibt es zum temporären Nachinstallieren über eine Internetverbindung mit apt-get im Terminal.



Minimales Livesystem: Slax ist klein und startet schnell. Es bietet eine einfache Oberfläche, über die sich beispielsweise Browser und Texteditor starten lassen.

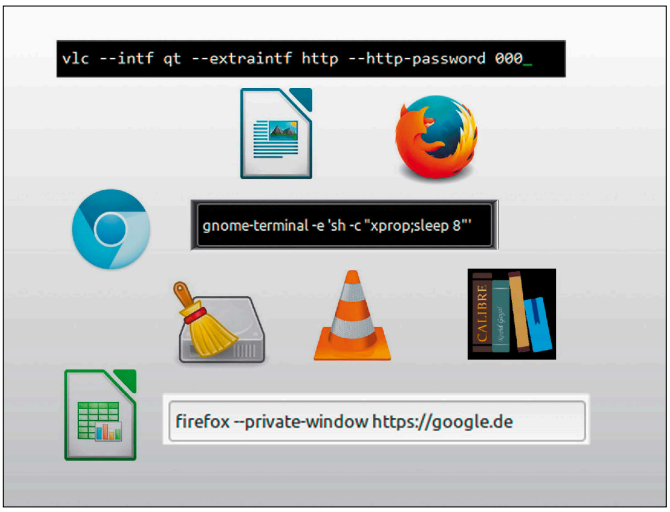
Das Livesystem Tails erfüllt nur einen Zweck: Den unkomplizierten Zugang zum TOR-Netzwerk. Hinter dem Kürzel TOR steht das Netzwerk „The Onion Router“ – eine Verkettung anonymisierender Proxyserver. Dieses Proxynetzwerk erlaubt auch in Zeiten von rigoroser Überwachung des Netzwerkverkehrs ein hohes Maß an Anonymität.

Informationen zu den genannten Systemen inklusive Downloadlinks finden Sie in der LinuxWelt-Toolbox in der Rubrik „Service/Mobil-Systeme“. ■

FIRMWAREEINSTELLUNGEN FÜR LIVESYSTEME

Die meisten Linux-Systeme starten problemlos auf jedem Rechner. Wenn nicht, prüfen Sie die Bios-/Firmwareeinstellungen. Suchen Sie nach Optionen wie „CSM“, „Uefi and CSM“ oder „Uefi and Legacy“, die meist unter Menüs wie „Boot“ oder „Boot Order“ zu finden sind. Die Bios-Emulation CSM (Compatibility Support Module) sollte aktiviert sein, damit der PC sowohl im Uefi- als auch im Bios-Modus booten kann. Deaktivieren Sie Secure Boot. Die Funktion verhindert den Start der meisten Livesysteme. Ändern Sie außerdem die Bootreihenfolge, damit der PC vom DVD-Laufwerk oder USB-Stick bootet.

Programme und Schalter



Startparameter für Browser, Office, VLC & mehr: Sie werden staunen, wie viel Potenzial in den meist kaum bekannten Startoptionen steckt. Der erste Artikel der Rubrik Tipps & Tricks zeigt erste Beispiele, beschreibt aber vor allem die technischen Einsatzmöglichkeiten.

VON HERMANN APFELBÖCK

Um bei Kommandozeilentools die Arbeitsweise zu steuern, ist es die einzige vorgesehene Möglichkeit, dem Befehl Schalter (Parameter) und Argumente mitzugeben. Schalter bestimmen die gewünschte Unterfunktion, Argumente die zu bearbeitenden Objekte wie Ordner, Datei, Laufwerk oder Gerät. Grafische Programme erwarten hingegen ihre Anweisungen durch Mausklicks auf Menüs. Trotzdem haben viele grafische Programme ein zum Teil schmales, zum Teil umfangreiches „Command Line Interface“ (CLI). Das gilt für Windows- wie für Linux-Software, ist aber unter Linux weitaus verbreiteter. Die Einsatzmöglichkeiten solcher Parameter haben die wenigsten Nutzer auf dem Radar. Dieser und die folgenden Artikel sollen zeigen, wie viel Potenzial in solchen Parametern steckt. Dabei konzentrieren wir uns auf populäre Software und auf produktive Startbefehle. Die zahlreichen Unterschiede zwischen den Desktopkomponenten – etwa bei Dateimanager, Editoren, Zubehör in Gnome, KDE, Mate, XFCE et cetera – kann das Special nicht abbilden.

Service: Die – zum Teil – komplexen Befehle finden Sie auch auf *https://paste.ubuntu.com/p/3fqWVy9JGM/*.

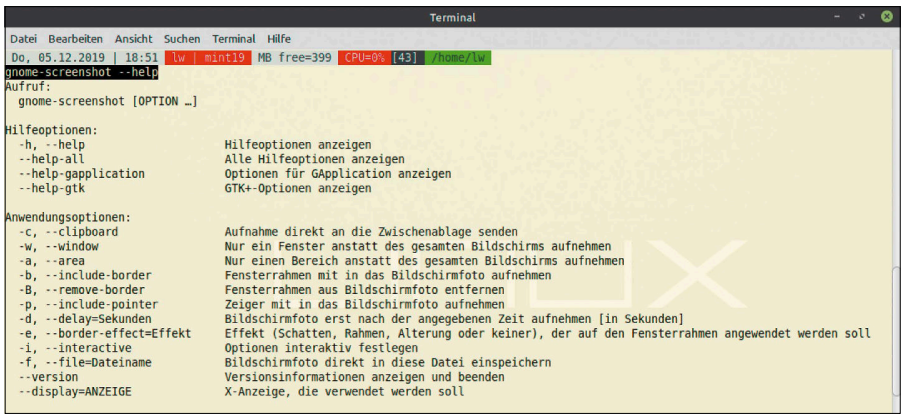
So finden Sie die Startparameter

Was die folgenden Seiten präsentieren, kann im Prinzip jeder experimentierfreudige Anwender selbst recherchieren. Es gibt grafische Software, die nur einige Standards wie etwa die Versionsanzeige anbietet (meist Schalter „--version“), ferner Kandidaten mit etlichen interessanten Funktionsaufrufen, schließlich Programme, die sich praktisch komplett über die Kommandozeile steuern lassen. Typischerweise zeigen grafische Programme, die über das Terminal mit dem Standardschalter „-h“ oder „--help“ gestartet werden, ihre Startparameter an:

```
vlc --help
```

Oft verweist die Schalterliste sogar auf noch eine umfangreichere Optionsliste („--help-all“). Das Beispiel des VLC Players dürfte die Notwendigkeit einer gewissen Experimentierfreudigkeit sofort deutlich machen: Bei grafischer Software mit einem umfangreichen Command Line Interface gibt es reichlich Schalter, deren Nutzen und Wirkung Sie dann einzeln ausprobieren müssten. Hinzu kommt die generelle Auswahl der Software, die sich für solchen Einsatz eignet.

Beides ist richtig Arbeit – und die wollen wir Ihnen abnehmen.



Die erste Recherche: Nach „--help“ und noch ausführlicher „--help-all“ offenbaren die allermeisten grafischen Linux-Programme eine Reihe von Aufrufparametern.

Tipp 1: Die Existenz einer mehr oder weniger umfangreichen Kommandozeilensteuerung sollten Sie bei keinem Linux-Programm unterschätzen: Es gibt Situationen, wo solche Steuerung sogar systemrettend sein kann. Ein sprechendes Beispiel ist das Systemtool Timeshift, das eine Systemsicherung auch dann wiederherstellen kann (per Kommando in der virtuellen Konsole), wenn die grafische Oberfläche nicht mehr funktioniert (dazu später mehr).
Tipp 2: Beachten Sie, dass unter Linux alle grafischen Programme standardmäßig Statusmeldungen ausgeben, wenn sie im Terminal gestartet werden. Der Aufruf „vlc“ (ohne Parameter) im Terminal berichtet daher über diverse Interna des Programms und kann in Problemfällen auf die Spur der Problemursache führen.

So nutzen Sie die Startparameter

Wenn sich der Start einer Software mit bestimmten Parametern als nützlich erweist, liegt es nahe, diesen Aufruf möglichst komfortabel einzurichten. Schalter oder komplizierte Schalterkombinationen sind lästig bei der Eingabe und außerdem schnell wieder vergessen. Mit welcher Methode Sie sich die Eingabe am besten erleichtern, hängt davon ab, wie die Programmfunktion genutzt wird – im Terminal oder an der grafischen Oberfläche. Als zweiter Aspekt kommt hinzu, welchen Aufwand der Schaltereinbau lohnt und wieviel Kompetenz Sie dafür mitbringen. Die vier nachfolgend beschriebenen Methoden gelten für praktisch jeden Linux-Desktop und für alle Parameter, die wir nachfolgend oder Sie selbst recherchieren.

Methode 1: Alias für das Terminal

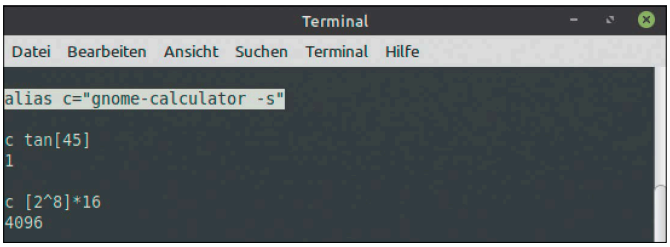
Wenn der Funktionsaufruf im Terminal erfolgen darf, ist eine Alias-Abkürzung die beste und einfachste Lösung.
Beispiel 1: Das Zubehörtool Gnome-Calculator schickt seine Rechenergebnisse ins Terminal, wenn der Parameter „-s“ mitgegeben wird:

```
gnome-calculator -s [2^8]/tan[40]
```

Das ermöglicht weit bequemeres Rechnen im Terminal als mit dessen eigenen Terminaltools, der gezeigte Aufruf wäre aber viel zu umständlich. Ein einfaches Bash-Alias wie

```
c="gnome-calculator -s"
```

vereinfacht dann das Rechnen im Terminal auf Kommandos dieser Art:



Taschenrechner im Terminal: Der grafische Gnome-Calculator kann Aufgaben und Ergebnisse auch im Terminal erledigen. Ein Alias sorgt für minimalen Schreibaufwand.

```
c 3,14*9
c [22^2]-[12*3,5]
```

Beispiel 2: Der Python-Interpreter enthält ein Modul „SimpleHTTPServer“, das im Handumdrehen Lese- und Downloadzugriff über das ganze Netzwerk ermöglicht:

```
python -m SimpleHTTPServer 8080
```

Die Schreibung ist wichtig, hingegen kann der Port (hier „8080“) beliebig gewählt werden. Jeder Browser im lokalen Netz kommt nun mit der IP- und Portangabe an diese Freigabe (also etwa mit 192.168.178.20:8080). Kenntnis der IP-Adresse (im Beispiel 192.168.178.12) und des Ports sind natürlich vorauszusetzen. Freigegeben wird ab dem Verzeichnis, in dem der Befehl erfolgt. Das Schöne an solchen Kommandoaufrufen ist, dass Sie über Terminal und Bash zusätzlich noch gewünschte Standards setzen können. Selbst in einem knappen Alias ist die Kombination mehrerer Befehle bekanntlich kein Problem (mit Semikolon):

```
alias miniserver="cd /; python -m
 SimpleHTTPServer 8080"
```

Das würde ab dem Wurzelverzeichnis „/“ das komplette Dateisystem freigeben.
Beispiel 3: Ein weiteres Beispiel, für das ein Bash-Alias vollkommen ausreicht, ist der Start einer Diashow mit dem Gnome-Bildbetrachter Eog (Eye of Gnome). Dazu genügt im gewünschten Verzeichnis ein Befehl wie dieser:

```
eog -s *.jpg *.png *.bmp
```

Die Angabe der gewünschten Bildformate ist fehlertoleranter, falls sich auch andere Dateien im Verzeichnis befinden, welche die Diashow unterbrechen würden. Ansonsten würde auch der allgemeine Stellvertreter „*“ ausreichen. Um das Ganze nach Wunsch anzupassen, könnten Sie dem obigen Grundbefehl etwa noch den Befehl

```
gsettings set org.gnome.eog.
 fullscreen seconds 8
```

vorausschicken, um die Bilder im Acht-Sekunden-Takt zu wechseln.

```
alias slide="gsettings set org.
 gnome.eog.fullscreen seconds
 8;eog -s *.jpg *.png *.bmp"
```

Methode 2: Angepasste Programmstarter

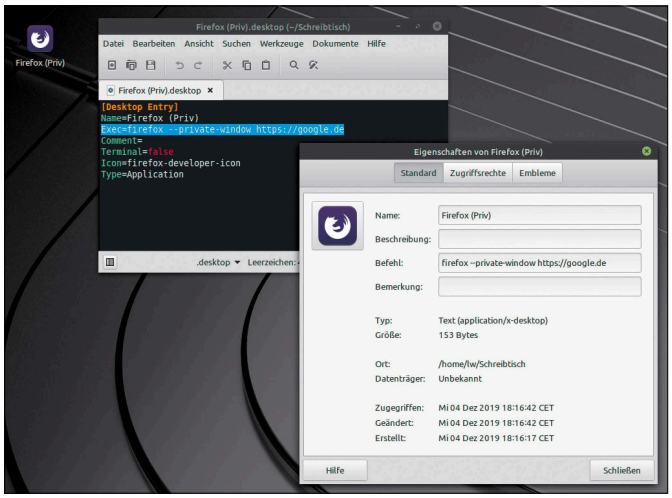
Die Standardverknüpfungen zu allen grafischen Programmen, die das Startmenü oder auch ein Starterdock anbietet, basieren auf Textdateien mit der Endung „.desktop“, die sich standardmäßig unter „/usr/share/applications“ befinden. Selbstverständlich lassen sich auch diese Dateien anpassen und in der maßgeblichen Zeile „exec=[Programmname]“ um einen oder mehrere Parameter erweitern. Allerdings sollten Sie dies nicht in den Originaldateien machen, sondern besser mit normalen Benutzerrechten im Home-Verzeichnis unter „~/.local/share/applications“, wobei Sie als Basis ein Original aus dem Pfad „/usr/share/applications“ verwenden können. Starter im Verzeichnis „~/.local/share/applications“ werden auch vom Hauptmenü berücksichtigt. Zusätzlich lassen sich natürlich auch auf dem Desktop solche Programmstarter einrichten, wobei aber nicht alle Desktopumgebungen so entgegenkommend sind wie etwa Linux Mint mit Cinnamon und dem Kontextmenü „Neuen Starter hier erstellen“. Eventuell müssen Sie die Starterdatei manuell erstellen und über „Eigenschaften → Zugriffsrechte“ ausführbar machen. In solchen Verknüpfungen, die oft weit mehr enthalten (siehe Standards unter „/usr/share/applications“), genügen im einfachsten Fall der Header „[Desktop Entry]“, der „Name“, der „Exec“-Befehl und die Zeile „Type=Application“.
Beispiel 1: Browser wie Firefox oder Chrome bieten den „privaten“ Modus ohne Cookies und ohne Webprotokolle per Startschalter. Ein Aufruf wie

```
firefox --private-window https://
 google.de
```

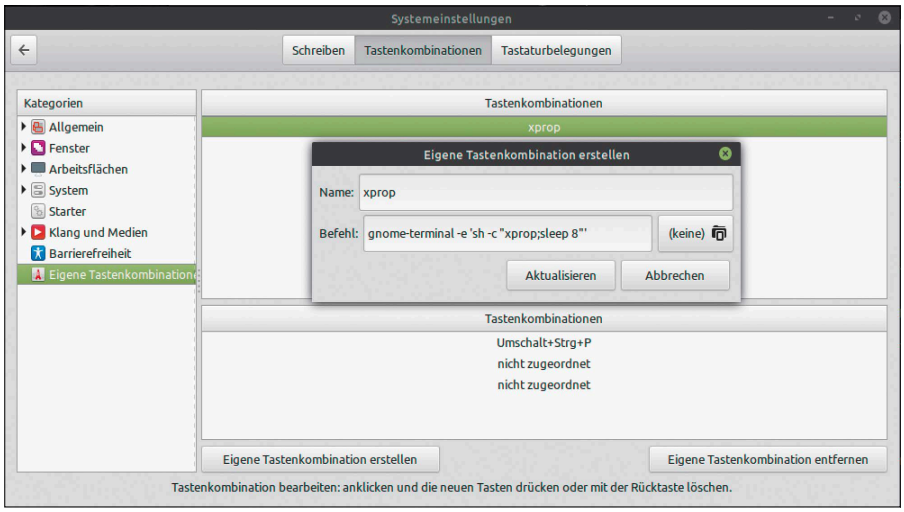
startet die deutsche Google-Suche in diesem Modus. Bei Chrome/Chromium würde der analoge Befehl so lauten:

```
chrome --incognito https://google.
 de
```

Eine zusätzliche Startverknüpfung mit diesem Befehl („exec=...“) ist über eine



Angepasste Starter: Wenn Programme in einem bestimmten Modus (auch Größe, Position) starten sollen, kann dies oft durch Schalter angefordert werden – hier für den „privaten" Firefox-Modus.



Systemhotkeys profitieren ebenfalls von Startschaltern: Dieses xprop-Beispiel ist relativ trickreich. Im Zweifel gelingt aber immer der Umweg über ein zwischengeschaltetes Shell-Script.

„.desktop"-Datei schnell angelegt und lädt dann den Browser standardmäßig im privaten Modus.

Beispiel 2: Dateimanager können durch mitgegebene Parameter so starten, dass sofort die meistgenutzten Ordner angezeigt werden. Das Beispiel bezieht sich auf Linux Mint mit Dateimanager Nemo, da dieser mehrere Ordner in Tabs präsentieren kann:

```
nemo --tabs /home /srv
  smb://192.168.
  178.8/Data/Transfer
```

Beispiel 3: Eine sehr häufig genutzte Benutzerdatei, etwa eine Buchhaltungstabelle, muss nicht im Dateimanager oder in der Kalkulationssoftware gesucht werden. Auch hierfür eignet sich ein eigener Starter, der zum Beispiel folgenden Befehl („exec=...") enthalten könnte:

```
soffice --calc --smb://192.168.
  178.8/Data/Büro/Buchhaltung.xlsx
```

Die Samba-Freigabe ist absichtlich gewählt, weil Libre Office bei einem solchen Aufruf die Netzfreigabe automatisch mountet. Das erspart einen Gang in den Dateimanager und macht den direkten Link zur Tabelle noch produktiver als bei einer lokalen Datei.

Methode 3: Benutzerdefinierte Hotkeys

Alle Beispiele wie die unter Methode 2 genannten sind auch als benutzerdefinierte Tastenkombinationen realisierbar. Hier muss nur der entscheidende Befehl unter den Systemeinstellungen („Tastatur" oder „Geräte → Tastatur") hinterlegt und dann der gewünschte Hotkey gewählt werden.

Beispiel 1: Das beliebte, zum Teil sogar zum Desktopstandard avancierte Starterdock Plank macht seine Einstellungen nicht mehr durch ein eigenes Dockicon verfügbar – um Platz zu sparen. Die Dockkonfiguration (Position, Verhalten) ist aber über den Befehl

```
plank --preferences
```

jederzeit erreichbar. Dieser Befehl ist mühelos als Hotkey realisierbar (dass die Konfiguration auch mit dem nicht ganz intuitiven Strg-Rechtsklick erreichbar ist, sei der Vollständigkeit halber erwähnt).

Beispiel 2: Die zahlreichen Hotkeys für Bildschirmfotos unter Ubuntu und Mint sind eher verwirrend. Im Prinzip genügen Vollbild, Fenster und Auswahlmarkierung. Das Zubehör Gnome-Screenshot („Bildschirmfoto") benötigt für Fenster-Screenshot den Schalter „--window", für Mausmarkierung „--area" und schalterlos für Vollbild. Diese Befehle wie etwa

```
gnome-screenshot --delay=8
  --window
```

als benutzerdefinierte Hotkeys abzulegen (und die Systemstandards zu deaktivieren), ist eine einfache Übung. Der zusätzliche „--delay"-Schalter ist bei Fenster-Screenshot zu empfehlen, um vorher das geeignete Fenster und eventuelle Dialoge aktivieren zu können.

Noch komfortabler wird es, wenn die Screenshot-Datei dann gleich zur Bearbeitung auf dem Desktop liegt:

```
gnome-screenshot --delay=8
  --window -f /home/[user]/
  Schreibtisch/temp.png
```

Komplizierter wird es sofort, wenn Variablen eingebaut werden sollen:

```
gnome-screenshot --area -f ~/
  Schreibtisch/$(date +%H_%m_%S).
  png
```

Dies kann das Terminal mühelos interpretieren, die Hotkeyverwaltung (oder ein „.desktop"-Starter) hingegen nicht. Dieses Beispiel ist nur über den Weg eines winzigen Shell-Scripts realisierbar, das genau diese eine Zeile enthält und dann in der Hotkeyverwaltung etwa mit

```
sh /home/[user]/area-screenshot.sh
```

eingetragen wird. Dieser Umweg befördert die Auflösung der Variablen wieder in die Terminal-Shell, die dies zuverlässig erledigt. Solcher Umweg über ein Shell-Script ist nicht nur für den Einsatz von Variablen notwendig, sondern auch dann, wenn Starter oder Hotkeys eine Aktion auslösen sollen, die mehrere Shell-Befehle erfordern.

Beispiel 3: Ein interessanter Kandidat für einen globalen Hotkey ist das kleine Systemtool xprop. Der Grund, xprop zu verwenden, ist in der Regel die Frage nach

dem Programmnamen eines Fensters. Also etwa die Frage: Wie lautet der Name des Dateimanagers, den ich gerade benutze? Nach dem Aufruf von xprop im Terminal verwandelt sich der Mauszeiger in ein Kreuz, mit dem Sie auf das gewünschte Fenster klicken. Im Terminal erscheint dann der zugehörige Programmname.
Bei diesem Beispiel interessieren uns nicht die Parameter, die das Programm selbst hat, sondern ein Schalter des grafischen Terminals, der eine komfortable Hotkey-Integration ermöglicht:

```
gnome-terminal -e 'sh -c
  "xprop;sleep 8"'
```

Dieser Befehl (und der zugeordnete Hotkey) startet auf Gnome-affinen Desktops ein Terminal mit den beiden Aufträgen „xprop“ und „sleep 8“. Xprop wartet auf Ihren Mausklick auf das gewünschte Objekt, die Eigenschaften werden dann acht Sekunden angezeigt.
Es ist tricky: Der Schalter „-e“ wird als eigentlich veraltet moniert – aber nur so funktioniert der Aufruf. Hinzu kommt der Trick, dem Terminal mit „sh“ zwei Befehle mitzugeben.

Methode 4: Ausbau des Dateimanagers

Datei- und ordnerbezogene Aktionen sind gut im Terminal aufgehoben, noch komfortabler allerdings als elegantes Kontextmenü im Dateimanager. Solchen Ausbau beherrschen praktisch alle grafischen Dateimanager, wobei aber zum Teil externe Tools notwendig sind (nautilus-actions, caja-actions). Am einfachsten, aber nicht ohne Bastelei, funktioniert es mit Nemo unter Linux Mint.
Beispiel 1: Libre Office bietet die stille Konvertierung von Dokumentformaten im Hintergrund, ausgelöst durch den passenden Parameter:

```
soffice --convert-to pdf Datei.rtf
soffice --convert-to "txt:Text
  (encoded):UTF8" Datei.odt
```

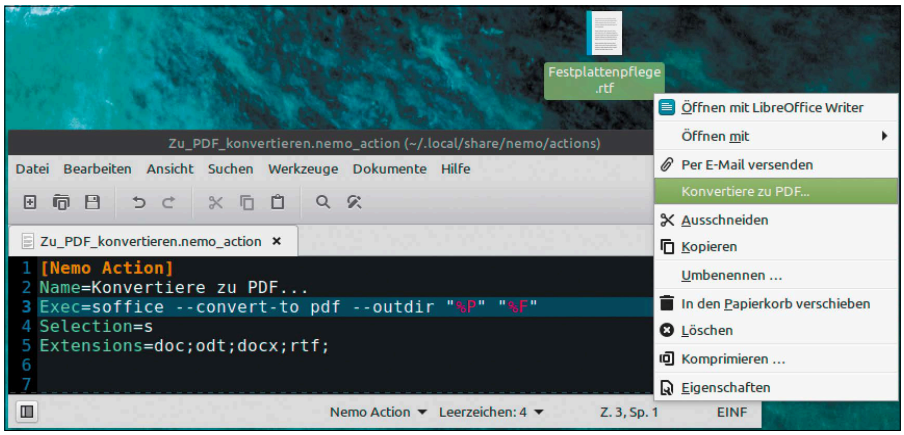
Die Ausgabedateien behalten die Originalnamen – nur mit neuer Extension. Soll die Ausgabe in ein anderes Verzeichnis erfolgen, ist dies durch den Schalter „--outdir [...]“ zu erzwingen. Mit einem Befehl wie

```
soffice --convert-to pdf *.docx
```

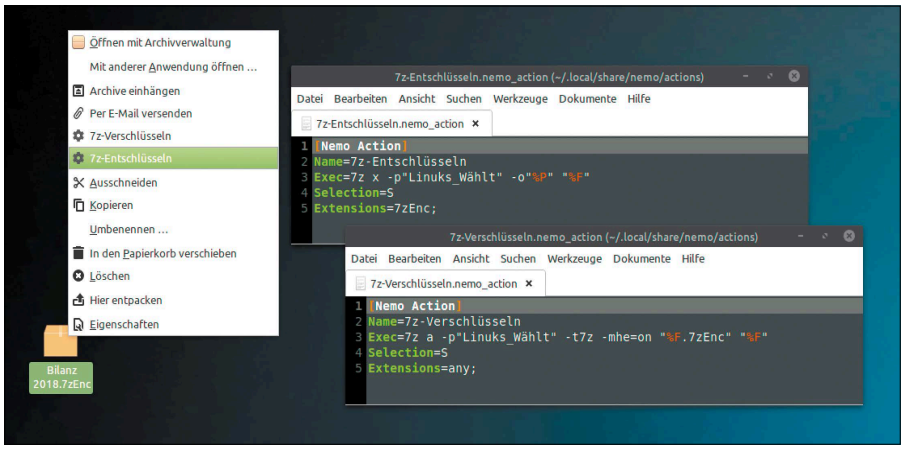
ist sogar eine Massenkonvertierung leicht möglich.
Um eine Konvertierung von Einzeldateien im Dateimanager Nemo einzubauen, müssen Sie mit Konfigurationsdateien unter „~/.local/share/nemo/actions/“ hantieren. Eine Action-Datei an dieser Stelle muss die Endung „.nemo_action“ besitzen und als erste Zeile den Header „[Nemo Action]“. Erste Orientierung bieten die Standards unter „/usr/share/nemo/actions/“. Entscheidend ist dann Anweisung „Exec=...“ mit dem Programmaufruf:

```
[Nemo Action]
Name=Konvertiere zu PDF…
Exec=soffice --convert-to pdf
  --outdir "%P" "%F"
Selection=s
Extensions=doc;odt;docx;rtf;
```

Der Parameter „--outdir“ ist hier für die Ausgabe in das aktuelle Verzeichnis („%P“) notwendig, weil Libre Office sonst immer nach „home/[user]“ exportiert. Die Zeile „selection=s“ bestimmt, dass die Aktion nur bei einem Rechtsklick auf einer einzelnen Datei aktiv wird. „Extensions= „ schränkt auf gewünschte Quelldateitypen ein.



Stilles Konvertieren: Libre Office kann im Hintergrund zu PDF, Text oder HTML konvertieren. Diese Aktion ist hier als Kontextmenü in den Dateimanager Nemo eingebaut.



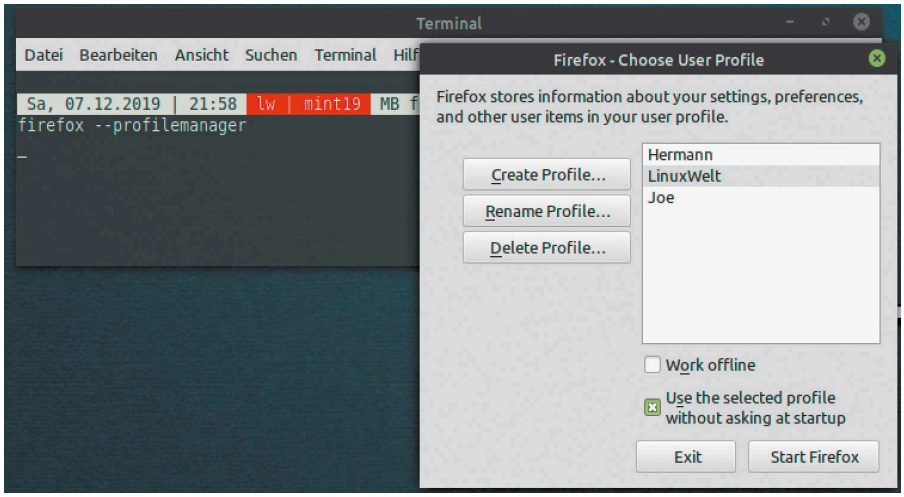
Geschützte 7-Zip-Archive im Kontext: Das Zusammenspiel der Packerschalter und der Übergabeparameter in den Nemo-Erweiterungen klappt so gut, dass kein Shell-Script notwendig ist.

Beispiel 2: Als sehr praktische Integration in den Dateimanager erweist sich eine Verschlüsselungsroutine mit dem Packer 7-Zip. Zwar ist 7z ein Terminaltool, für das wir aber an dieser Stelle eine Ausnahme machen, zumal das Funktionsangebot und das Resultat der grafische Dateimanager anbietet. Als Kandidat dient wieder das Mint-Zubehör Nemo.
Das Prinzip der Action-Scripts ist bereits im Beispiel 1 erklärt. Die wenigen Codezeilen für passwortgeschützte 7-Zip-Archive zeigt die Abbildung oben (siehe auch unter *https://paste.ubuntu.com/p/f7RZ8VzFWH/*). Das per Parameter „-p“ übergebene Passwort müssen Sie natürlich in beiden Dateien ändern, bei der Benutzung im Dateimanager wird es künftig automatisch übergeben. Beachten Sie, dass dieser Passwortschutz für mobile Dateien auf USB oder für den Transport in die Cloud gedacht ist. Am lokalen Rechner sind die Funktion sowie das Passwort im Klartext ersichtlich. ■

Webbrowser und ihre Schalter

Wer seinen Browser seit Jahren über eine schlichte Verknüpfung startet, wird kaum glauben, welches Arsenal an Optionen diese Software mitbringt. Hier ist nur Platz für die interessantesten Optionen von Firefox und Chrome/Chromium.

VON HERMANN APFELBÖCK



Alle Browser unterstützen Aufrufparameter, Chrome/Chromium deutlich mehr als Firefox, ohne dies aber nach Schalter „--help“ oder in der Manpage umfassend zu dokumentieren. Dasselbe gilt für Vivaldi und Opera, die zum Großteil auf Chromium basieren. Tatsächlich sind die meisten der Chrome-Schalter aber auch kaum für den Anwender relevant, sondern eher Testparameter für Entwickler. Die wichtigsten Parameter für Endanwender folgen hier. Den direkten Browserstart im „privaten“ Modus hat bereits der voranstehende Einstiegsartikel erklärt („--incognito“ für Chrome, „--private-window“ bei Firefox).

Browsereparaturen

Wenn Browser nicht mehr starten oder ständig hängen, liegt es fast immer am Benutzerprofil oder fehlerhaften Erweiterungen. Dann lässt sich der Browser in einem sicheren Modus ohne Add-ons starten. Bei Firefox ist das ganz einfach:

```
firefox -safe-mode
```

Über das Menü „Add-ons → Erweiterungen“ können Sie nun Schritt für Schritt Erweiterungen deaktivieren und den Browser dann normal starten, bis Sie die verantwortliche Erweiterung entdeckt haben und diese dann dauerhaft deinstallieren.

Für Chrome gibt es einen analogen Befehl:

```
google-chrome --disable-extensions
```

Das Problem ist hier, dass für Chrome nach diesem Start schlicht keine Erweiterungen mehr installiert sind. Anders als bei Firefox können Sie die Add-ons jetzt nicht gezielt deaktivieren. Ein jetzt störungsfreier Start hilft daher nur zu der Erkenntnis, dass der Fehler an einem der Add-ons liegen muss. Sie finden die Chrome-Erweiterungen unter „~/.config/google-chrome/Default/Extensions/“.

Der Firefox-„Profilmanager“

Firefox – und analog das Mailprogramm Thunderbird – haben mit dem Profilmanager ein mächtiges Werkzeug eingebaut, das über einen Startparameter zu erreichen ist:

```
firefox --ProfileManager
```

Der Nutzwert ist ein mehrfacher:

1. Wenn Sie bei Browserproblemen schnell eine funktionierende Software brauchen, ohne sich mit Reparaturen aufhalten zu wollen, wählen Sie dann einfach „Profil erstellen“. Mit dem neuen Profil werfen Sie den kompletten Ballast ab und starten einen jungfräulichen Firefox. Die alten Daten können Sie im Profilmanager auch komplett löschen („Profil löschen“ nach dem Aufruf von *firefox --ProfileManager*).

2. Mit Firefox-Profilen lässt sich unter einem Benutzerkonto ein deutlich unterschiedener Browser realisieren – etwa mit den Profilen „Arbeit“ und „Privat“ mit jeweils anderen Lesezeichen, Startadressen, Themes und Add-ons. Das kann auch für mehrere Personen auf einem Heimrechner genutzt werden, der nur ein Systemkonto verwendet. Für den Start des passenden Profils dient dieser Befehl:

```
firefox -p Sepp
```

Undokumentiert blieb dieser Schalter:

```
firefox --CreateProfile Sepp
```

Der erstellt ein neues Profil mit dem angegebenen Konto, ohne Firefox selbst zu starten.

Kioskmodus für Chrome und Firefox

Google Chrome und Chromium bieten unter Hunderten von größtenteils undokumentierten Startparametern auch einen für

den Kioskmodus. „Kiosk“ bedeutet, dass der Browser im Vollbild ohne Adresszeile, Menü, Navigationselemente und Lesezeichenleiste läuft, außerdem ohne Titelleiste (Beenden ist nur über Alt-F4 möglich):

```
google-chrome --kiosk https://
  google.de
```

Die Kioskansicht lässt sich im Unterschied zum normalen Vollbild, für das es ebenfalls einen Schalter gibt („--start-fullscreen“), mit der Taste F11 nicht abschalten.

Firefox hat den Kioskmodus in früheren Versionen Add-ons überlassen. Die neueste Version 71 ist unter Linux noch nicht überall verfügbar, bringt aber nun ebenfalls einen Kioskschalter mit:

```
firefox --kiosk https://google.de
```

Das Resultat entspricht jenem unter Chrome: Der Browser zeigt die angegebene Seite im Vollbild und blendet sowohl die eigenen Menü- und Navigationselemente aus als auch die Titelleiste. Für einen gewissen Schutz vor unkontrollierter Internetnutzung bietet Chrome eine weitere Option. Über das Menü „Weitere Tools → Verknüpfung erstellen“ legt Chrome Webseiten als Link am Desktop ab, die der Browser dann ohne Menü- und Navigationselemente und vor allem ohne Adresszeile darstellt. Solche Verknüpfungen etwa zu lokalen Intranetseiten, die nur interne Links verwenden, führen erst mal nicht darüber hinaus. Auf der Kommandozeile ist der Start im App-Modus mit diesem Befehl

```
google-chrome --app=http://192.
  168.0.8/dokuwiki/
```

möglich.

Allerlei nützliche Kleinigkeiten

Nach dem ersten Firefox-Start werden Sie nicht mehr aufgefordert, Einstellungen oder Lesezeichen von anderen installierten Browsern zu importieren. Wenn Sie diese Aktion versäumt haben und später nachholen wollen, hilft folgender Schalter:

```
firefox --migration
```

Dies öffnet den kleinen Dialog „Import Wizard“ („Import-Assistent“) mit einer Auswahl der Browser, deren Daten Firefox importieren kann.

Mit den Schaltern „--width“ und „--height“ lässt sich die gewünschte Größe des Firefox festlegen, sofern etwa folgender Befehl als Firefox-Starter abgelegt wird:

```
firefox --width 1200 --height 800
```

Ein weiterer einfacher Trick ist der Standardstart mit mehreren URLs. Die Browserkonfiguration sieht normalerweise nur eine Startseite vor, aber mit

```
firefox google.de wikipedia.de
  192.168.0.6
```

starten Sie problemlos mehrere wichtige Standard-URLs. Die erste angegebene Adresse ist dann jeweils die aktiv angezeigte. Chrome beherrscht das natürlich auch.

Den Nutzwert der annähernd 280 Chrome/Chromium-Schalter (siehe *http://tiny.cc/p1cehz*) können wir hier nur andeuten. Die meisten sind nur für Entwickler relevant. Aber natürlich kann auch Chrome etwa mit

```
google-chrome --window-size=1200,
  800 --window-position=0,0
```

zu exakter Größe und Position veranlasst werden.

Der interessante Schalter „--user-data-dir“ kann für den nächsten Chrome-Start ein beliebiges Verzeichnis festlegen, in das der Browser seine Daten schreibt:

```
google-chrome --user-data-dir=/
  home/sepp/Schreibtisch/temp
```

Das entspricht im Prinzip einem Profilmanager, weil damit ein jungfräulicher Chrome mit Standardeinstellungen startet. Nebenbei ist dadurch gut zu kontrollieren, was eine einzige Browsersitzung am Rechner an Daten hinterlässt. Wenn Sie das Verzeichnis danach wieder löschen, bleibt die Browsersitzung auf dem Rechner garantiert spurlos.

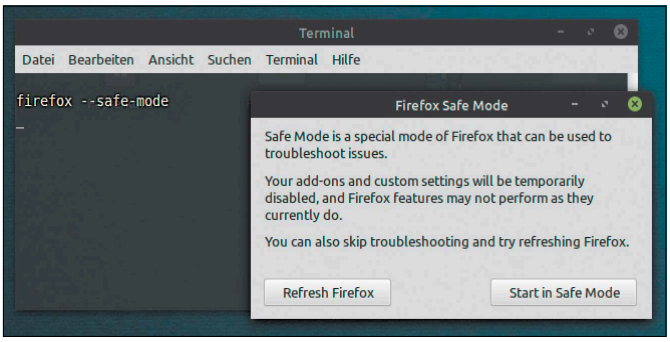
Um in Chrome einfach per Aufruf oder Verknüpfung die Sprache zu wechseln, gibt es den Startparameter „--lang=“:

```
google-chrome --lang=fr http://
  google.fr
```

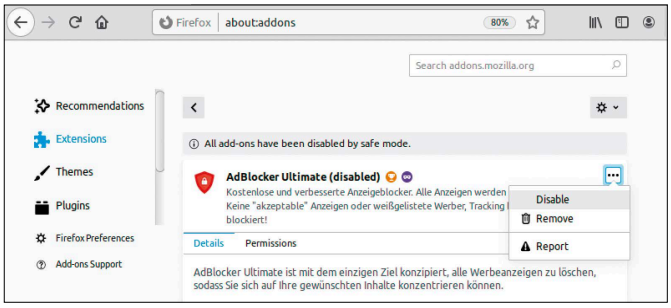
Zahlreiche „--enable-[...]“ und „--disable-[...]“ Anweisungen können die Funktionalität des Browser erweitern oder beschränken. Die „Enable“-Schalter betreffen aber fast ausschließlich experimentelle Funktionen. Der wichtigste Disable-Schalter („--disable-extensions“) wurde bereits erwähnt. Chrome-Parameter können aber darüber hinaus alles Mögliche abschalten:

```
google-chrome --disable-audio-
  output
google-chrome --disable-sync
```

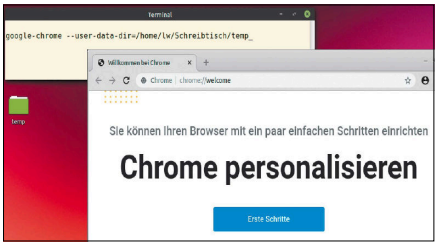
Nach dem ersten Schalter bleibt Chrome stumm, nach dem zweiten pausiert die Synchronisierung, obwohl sie im Browser aktiviert ist. Tiefergehende Schalternutzung setzt intime Kenntnis der Unterfunktionen und Flags voraus, die Chrome unter „chrome://about“ detailliert anzeigt. ■



Wichtiger Reparaturschalter: Firefox startet im „Safe Mode“ ohne Erweiterungen und lokale Sprachpakete.



Firefox im Safe Mode: Jetzt lassen sich unter „Add-ons“ (oder Adresse „about:addons“) verdächtige Add-ons abschalten oder löschen.



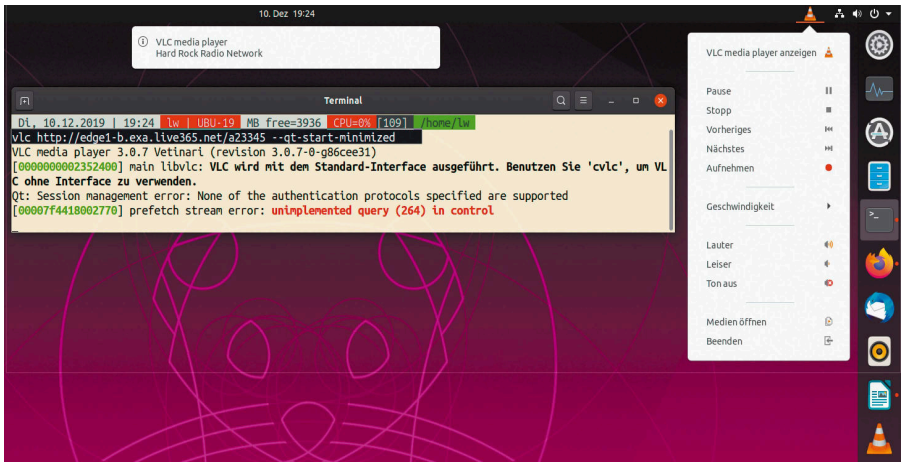
Neues Verzeichnis – neuer Browser: Chrome/Chromium haben zwar keinen Profilmanager, aber genügend andere Optionen, um den Browser neu einzurichten.

Schaltergigant VLC

Der Mediaplayer VLC ist als Film- und Musik-Alleskönner bekannt. Dass er auch bei der Steuerung durch Startparameter ein Gigant ist, dürfte der Mehrzahl der Nutzer entgehen. Solcher Einsatz ist aber auch kein Fall für typische Mausklicker.

VON HERMANN APFELBÖCK

Es wäre ein unsinniger Anspruch, die Parameter des VLC in diesem knappen Artikel erklären zu wollen. Da das Programm so ziemlich alles über sein Command Line Interface erledigen kann, ist genau dies die erste und wichtigste Information: Wenn Sie – irgendein – Multimedia-Anliegen haben, das ohne Klicks an der Oberfläche erledigt werden soll, dann geht das aller Voraussicht mit dem VLC (siehe *https://wiki.videolan.org/VLC_command-line_help*). Dieser Artikel kann nur Anregungen für einige interessante VLC-Starts bieten.



Abspielen eines Radiostreams: Wie sich der VLC-Player dabei präsentieren soll (oder gar nicht), ist durch Parameter zu steuern – hier minimiert in der Systemleiste.

Audio aus dem Web abspielen

Um schnell und ohne Öffnen der VLC-Oberfläche in den Stream Ihres bevorzugten Nachrichtensenders reinzuhören, brauchen Sie nur dessen Streamadresse. Die ist über Google schnell zu ermitteln – oft in unterschiedlichen Soundqualitäten. Für das Abspielen genügt dann folgender Aufruf (Alias oder Link):

```
vlc http://streams.br.de/b5aktuell_2.m3u --qt-start-minimized
```

Der Schalter „--qt-start-minimized“ minimiert den VLC in die Systemleiste (Systray-Symbol unter Windows). Soll der Sender immer laufen, kann sich der Player mit dem Interfaceschalter „--intf=dummy“

```
vlc http://streams.br.de/b5aktuell_2.m3u --intf=dummy
```

auch ganz unsichtbar machen.

Audio-Netzwerkstream aufnehmen

Anstatt einen Netzwerkstream abzuspielen, kann der VLC diesen auch in eine Ausgabedatei schreiben, also aufnehmen:

```
vlc http://edge1-b.exa.live365.net/a23345 --sout "#duplicate{dst=std{access=file,dst=aufnahme.mp3}"
```

Der Stream wird in diesem Beispiel im aktuellen Verzeichnis in die Datei „aufnahme.mp3“ geschrieben. Die Aufnahme läuft solange, bis der VLC manuell beendet wird. Auch hier kann sich der Player mit dem zusätzlichen Schalter „--qt-start-minimized“ dezent verkleinern. Das folgende Beispiel

```
vlc http://edge1-b.exa.live365.net/a23345 --sout "duplicate{dst=std{access=file,mux=raw,dst=aufnahme.mp3}" --stop-time 3600 vlc://quit
```

bestimmt vorab eine Aufnahmezeit von einer Stunde und beendet den VLC dann automatisch.

Bildschirmvideo aufnehmen (Screencast)

Der VLC kann Bildschirmvideos in jeder Qualität aufnehmen. Folgender Befehl produziert ein Video anspruchsloser Qualität:

```
vlc screen:// --screen-fps=30 --sout "#transcode{vcodec=h264,acodec=copy}:file{dst=aufnahme.mp4}"
```

Mit ergänzenden Schaltern wird die Aufnahme hochwertiger und ruckelfrei:

```
vlc screen:// --screen-fps=30 --sout-x264-preset fast --sout-x264-tune animation --sout "#transcode{vcodec=h264,acodec=copy}:file{dst=aufnahme.mp4}"
```

Die Aufnahme startet sofort und endet mit dem Beenden des Mediaplayers. Als Ausgabedatei ist im Beispiel „aufnahme.mp4“ angegeben, die – ohne nähere Pfadangabe – einfach im aktuellen Verzeichnis gespeichert wird.

Wahl der Oberfläche (Interface)

Standardoberfläche ist (auch unter Windows) „Qt“, also das verbreitete Grafiktoolkit. Wie schon in einem Beispiel gezeigt, kann der VLC über den Schalter „--intf=“ aber auch andere Bedienoberflächen benutzen oder auch gar keine („--intf=dummy“). Eine textbasierte Oberfläche wird sich niemand grundlos zumuten, kann aber beim SSH-Zugriff nützlich sein:

```
vlc --intf=ncurses
```

Neben weiteren, eher exotischen Interfaceoptionen ist vor allem der eingebaute HTTP-Server interessant, der die Steuerung des Players im Browser eines beliebigen Netzwerkclients ermöglicht (Tablet, Smartphone, PC). Remotesteuerung bedeutet,

dass der Rechner mit dem VLC weiterhin das Abspielgerät bleibt und der Client die Medienauswahl und Lautstärke erledigt. Der HTTP-Server bietet weder eine schicke Oberfläche noch nennenswerten Bedienkomfort, genügt aber zur fundamentalen Fernsteuerung:

```
vlc --intf=http --http-port=2222
  --http-password nix
```

Danach ist der VLC remote über jeden Browser mit der Adresse

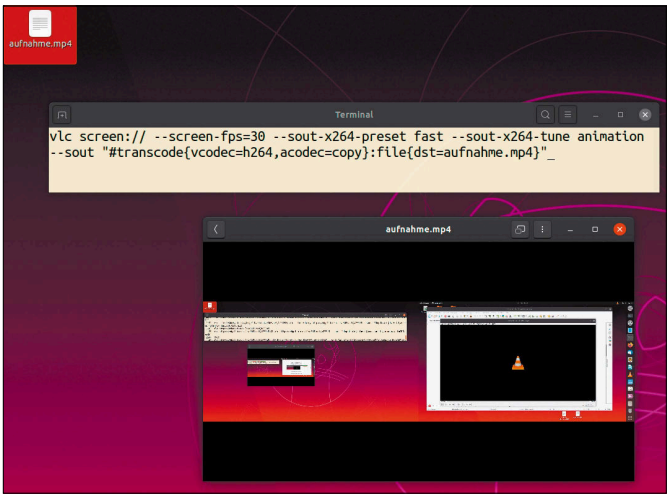
```
[IP-Adresse]:2222
```

erreichbar. Bei der Authentifizierungsabfrage lassen Sie das Feld „Benutzernamen“ leer und geben nur das Passwort ein. Statt des Stellvertreters „[IP-Adresse]“ verwenden Sie die tatsächliche lokale IP des Rechners, auf dem der VLC läuft – also beispielsweise „192.168.1.25:2222“.

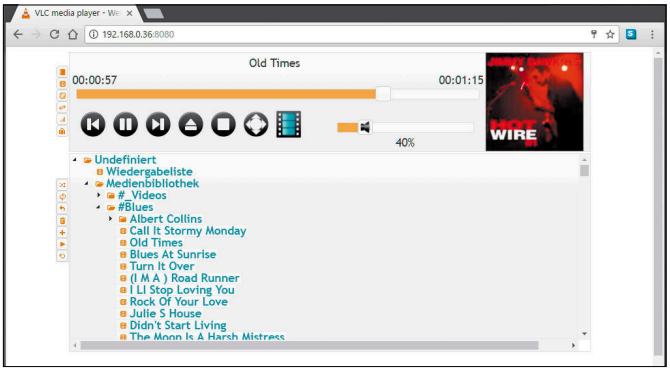
Nichts, was nicht ginge: Der VLC kann auch zwei Interfaces parallel starten. Soll der Player etwa neben dem HTTP-Server auch noch die normale Oberfläche am lokalen Rechner anzeigen, hilft der Schalter „--extraintf“ (Extra-Interface):

```
vlc --intf=qt --extraintf=http
  --http-password nix
```

Lediglich beim laufenden VLC ist es nicht möglich, nachträglich ein Extra-Interface nachzuladen.



Bildschirmvideos mit VLC: Ein komplexer Befehl startet einen qualitativen Screencast. Das Bild zeigt den Aufruf und unten die fertige Aufnahme.



HTTP-Server nach „vlc --intf=http“: Die VLC-Fernbedienung via Browser leistet fundamentale Netzwerksteuerung, ist aber im Klickkomfort noch ausbaufähig.

Genaues Filmfragment abspielen

Das nächste Beispiel scheint zunächst akademisch, ist es aber nicht. Mit

```
vlc [Dateiname] --start-time [x]
  --stop-time [y]
```

spielt der VLC ein exaktes Filmfragment von Sekunde „x“ bis Sekunde „y“. Damit können Sie sich für eine Präsentation oder ein Firmenvideo das Zuschneiden eines größeren Videos ersparen:

```
vlc demo.avi --start-time 124
  --stop-time 240 --repeat
  --fullscreen
```

Passender Einsprungpunkt und das Ende sind durch Ausprobieren schnell ermittelt. Durch den Schalter „--repeat“ wird die Sequenz endlos wiederholt. Eine derartige Endlospräsentation lässt sich mit folgenden Schaltern noch restriktiver gestalten:

```
vlc demo.avi --start-time 124
  --stop-time 240 --repeat --video-
  wallpaper --no-video-title-show
```

Jetzt zeigt der Player außerdem überhaupt keine Bedienelemente mehr an und lässt sich nur noch über einige Standard-Hotkeys beeinflussen und nur durch Alt-F4 beenden. Wenn die Soundspur stört, lässt sie sich mittels

```
vlc demo.avi [...] --noaudio
```

auch abschalten. Umgekehrt würde der Schalter „--novideo“ nur den Sound abspielen, nicht das Bild.

Konvertieren per Kommando

Selbstverständlich konvertiert der VLC auch per Schalterübergabe. Das bringt gegenüber der grafischen Oberfläche den Vorteil, dass sich Mediendateien ganzer Verzeichnisse bearbeiten lassen. Ohne gute Kenntnisse bei Codecs, Bitraten und Videocontainern dürfte ein Kommando wie dieses

```
vlc "LennyKravitz.vob"
  --sout=#transcode{vcodec=h264,vb
  =1024,acodec=mp4a,ab=192,channels
  =2}:standard{access=file,mux=
  ts,dst=LennyKravitz.mpg}
```

einigermaßen überfordern (obwohl noch relativ einfach gehalten und nur für eine Datei). Klar ist zunächst die Angabe der Quelldatei, nach „--sout“ folgt der Ausgangskanal, wobei „vcodec“ den gewünschten Videocodec, „acodec“ den Audiocodec angibt. Die Liste der insgesamt unterstützten Codecs ist unter *https://wiki.videolan.org/Codecs/* einsehbar und ziemlich umfangreich. „vb“ (Video-Bitrate) und „ab“ (Audio-Bitrate) bestimmen Abtastrate und Qualität für Bild und Ton, „channels“ nennt die Anzahl der Audiokanäle („2“ für Stereo). Nach „access“ geht es zum Ausgabeformat – hier eine Datei („file“) mit dem Multiplexing-Containerformat „ts“ („mux“) und dem angegebenen Dateinamen.

Resetkommando zur Standardoberfläche

Im Menü „Werkzeuge → Plugins und Erweiterungen“ lässt sich der Plug-in-Manager des VLC öffnen, um im Web verfügbare Erweiterungen und Skins nachzurüsten. Das Experimentieren mit Skins kann aber den Player außer Gefecht setzen. Vorübergehend hilft

```
vlc --ignore-config
```

und schlimmstenfalls setzt der Player nach diesem Startparameter

```
vlc --reset-config
```

auf seine Standardoberfläche zurück, Einstellungen wie etwa eine eingerichtete Medienbibliothek bleiben jedoch erhalten. ■

Veracrypt: Alles geht im Terminal

Die Verschlüsselungssoftware Veracrypt hat ein komplettes Command Line Interface (CLI) zur Benutzung im Terminal. Dies erlaubt zum einen die einfachere Bedienung am Desktop, zum anderen den Einsatz auf SSH-administrierten Servern.

VON HERMANN APFELBÖCK

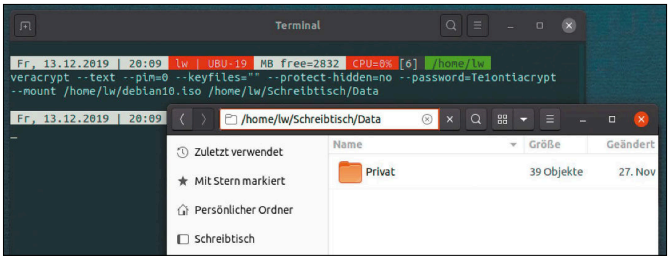
Ähnlich dem VLC-Player bilden die meisten Veracrypt-Schalter Funktionen ab, die auch über die Oberfläche zu erreichen sind. Dies aber komplett: Das vereinfacht das Mounten von Containern am Desktop erheblich und erlaubt es, Veracrypt per SSH-Netzzugriff auf entfernten Servern zu bedienen. Veracrypt gibt es auf der Projektseite *www.veracrypt.fr* für Linux, Windows und Mac-OS, für Ubuntu auch über das PPA *ppa:unit193/encryption*.

Container am Desktop-PC

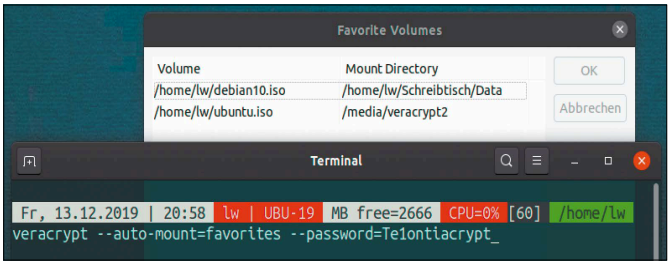
Das Anlegen neuer Container mit Schalter „--create“ und den zahlreichen notwendigen Optionen (Datei, Größe, Algorithmus, Passwort) ist möglich, aber nicht praxisnah: Neue Container braucht man nicht täglich und die Aktion ist an der grafischen Oberfläche bequem zu absolvieren. Ganz anders steht es um das Mounten bestehender Container: Das bedeutet Starten von Veracrypt, Navigieren zum Container („Select File“), Mounten („Mount“) und Eingabe des Kennworts. Der folgende Befehl erledigt das in einem Aufwasch (ein Fall für ein Alias):

```
veracrypt --text --pim=0
  --keyfiles="" --protect-hidden=no
  --mount /home/lw/debian10.iso /
  home/lw/Schreibtisch/Data
```

Container ist hier die Datei „debian10.iso“, die in den Desktopordner „Data“ geladen wird. Die Angaben, dass keine PIM, Keyfiles und versteckte innere Volumes verwendet werden, sind notwendig, weil sie sonst abgefragt werden. Eventuell kann auf einem Desktop-PC sogar das Kennwort direkt übergeben werden:



Mit einem Befehl die Daten im Zugriff: Das Mounten verschlüsselter Veracrypt-Container ist mit (gespeicherten) Befehlszeilen wesentlich komfortabler als mit der Oberfläche.



Noch einfacher mounten? Dieser knappe Befehl lädt alle Veracrypt-Container, die vorher als „Favoriten“ definiert wurden – sofern alle dasselbe angegebene Passwort verwenden.

```
veracrypt --text --pim=0
  --keyfiles="" --protect-hidden=no
  --password=GEH3IM --mount /home/
  lw/debian10.iso /home/lw/
  Schreibtisch/Data
```

Dann entfallen alle Rückfragen. Der Schalter „--text“ sorgt dafür, dass die Veracrypt-Oberfläche nicht starten muss und eventuelle Rückfragen im Terminal erfolgen. Andernfalls erscheint eine grafische Abfrage. Der Befehl *veracrypt --dismount* genügt, um alle Veracrypt-Container zu entladen.

Containerverwaltung per SSH

Für Container auf einem Headless-Server (etwa einem Raspberry) gilt dasselbe wie beim Desktop. Die Mühe, diese mit „--create“ einzurichten, scheint unnötig, da es einfacher ist, Container auf dem Desktop zu erstellen und dann zum Server zu verschieben. Danach lässt sich der Container über SSH genauso mounten wie oben für den Desktop beschrieben. Wenn der entschlüsselte Inhalt über Samba zugänglich sein soll (was sich nur im Heimnetz empfiehlt), dann müssen Sie den Container auf eine Samba-Freigabe mounten – und zwar mit einem Systemkonto (auf dem Server), das Zugriff auf die Samba-Freigabe besitzt und außerdem sudo-Rechte (notwendig zum Mounten von Veracrypt-Containern). Ein Beispiel: Bei einer angenommenen Samba-Freigabe von „/srv/data/“, wo auch der Container liegt, würde folgender Befehl genügen:

```
veracrypt --text --pim=0
  --keyfiles="" --protect-hidden=no
  --display-password --mount /srv/
  data/debian10.iso /srv/data/
  privat
```

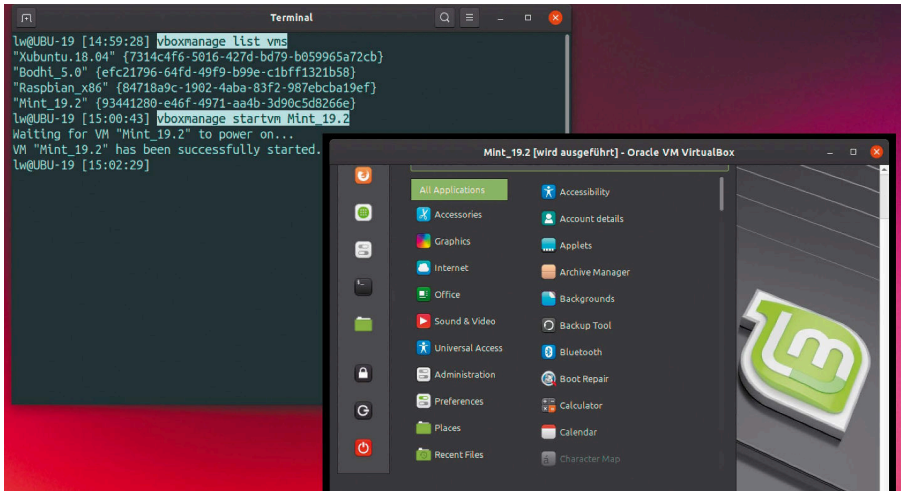
Der hier zusätzlich genutzte Schalter „--display-password“ zeigt das eingegebene Passwort im Klartext. ■

Virtualbox via Terminal

Beim Virtualisierer von Oracle gibt es eine Reihe von Spezialprogrammen, die in der Summe eine komplette Terminalsteuerung anbieten. Das wichtigste dieser Tools ist vboxmanage, dessen Möglichkeiten wir hier nur andeuten können.

VON HERMANN APFELBÖCK

Das CLI von Virtualbox umfänglich zu beschreiben, würde eine ganze LinuxWelt füllen. Das Thema ist noch komplexer als etwa beim VLC, weil es hier neben virtualbox, virtualboxvm, vboxmanage, vboxwebsrv, vboxheadless noch weitere Subprogramme gibt, die allesamt ein Arsenal an Schaltern mitbringen. Wir beschränken uns hier auf einige populäre Aktionen, die auf der Kommandozeile schneller und handlicher ablaufen als in der grafischen Bedienung.



Turbostart: Der Befehl „vboxmanage startvm ...“ ist der schnellste Weg zu einer laufenden Virtualbox-VM.

VMs anzeigen und starten

In gewisser Analogie zum voranstehenden Veracrypt lassen wir das Erstellen von virtuellen Maschinen außen vor. Das mächtige vboxmanage beherrscht dies zwar über zahlreiche Unterbefehle wie „create“, „modifyvm“, „createmedium“, „storagectl“, „storageattach“, jedoch besteht in der komfortablen Oberfläche wenig Leidensdruck, diese Aufgabe ins Terminal zu verlegen. Einziger Anlass, dies zu tun, wäre die Administration über SSH. Wie vboxmanage die virtuellen Maschinen adressiert haben will, erfahren Sie nach diesem Befehl:

```
vboxmanage list vms
```

Dies zeigt in Kürze die – von Ihnen angelegten – Bezeichnungen wie etwa „Xubuntu_18.04“ sowie die von Virtualbox vergebenen eindeutigen IDs. Beides kann wahlweise verwendet werden, um dann eine VM zu laden oder zu ändern. Der Befehl

```
vboxmanage startvm "Xubuntu_18.04"
```

startet folglich die genannte VM und diese Option bietet als Link oder Alias den eindeutig flotteren Weg zu einer virtuellen Maschine. Wenn eine VM nur Serverdienste anbieten soll oder nur zum Zweck der automatischen Systemaktualisierung geladen wird, gibt es dafür den speziellen Befehl „vboxheadless“ (der seine Schalter in gebräuchlicher Schreibweise mit führendem „--“ fordert):

```
vboxheadless --startvm
  "Xubuntu_18.04"
```

Der vboxmanage-Unterbefehl „controlvm“ greift auf eine laufende VM zu. Während

```
vboxmanage controlvm
  "Xubuntu_18.04" poweroff
```

umstandslos und radikal beendet, macht folgender Befehl

```
vboxmanage controlvm
  "Xubuntu_18.04" screenshotpng
  $(date +%H.%M.%S.png)
```

einen Screenshot von der VM – eine hübsche Option, die den Transport des Screenshots ins Hostsystem erspart. Wer nur einen Screenshot braucht, kann nach „screenshotpng“ einfach statisch „tmp.png“ verwenden.

Virtuelle Festplatten vergrößern und konvertieren

Das Tool vboxmanage ist unglaublich fix beim Vergrößern der virtuellen Festplatte. Diese Notwendigkeit stellt sich relativ häufig, wenn die zunächst gewählte Kapazität nicht mehr ausreicht. Es muss sich allerdings um eine native und als „dynamisch“ angelegte VDI von Virtualbox handeln. Beides ist Standardvorgabe und sollte aus eben diesem Grund beibehalten werden. Der ausführliche Infobefehl (hier gleich gefiltert nach „vdi“)

```
vboxmanage list vms --long | grep vdi
```

hilft, um die betreffende VDI zu identifizieren. Der Befehl

```
vboxmanage modifyhd "/home/lw/
  VirtualBox VMs/Bodhi_5.0/
  Bodhi_5.0.vdi" --resize 30000
```

vergrößert dann im Handumdrehen auf die hier gewünschten 30 GB. Die Festplatte muss dann aber noch mit Gparted auf die neue Partitionsgröße erweitert werden.

Wer Virtualbox und Vmware benutzt, hat VMs in verschiedenen Formaten vorliegen. Virtualbox beherrscht das VMDK-Format von Vmware, während Vmware mit den VDI-Dateien von Virtualbox nichts anfangen kann. Auch hier hilft das Werkzeug vboxmanage. Nach Ermittlung der gewünschten VDI

```
vboxmanage list vms --long | grep vdi
vboxmanage clonemedium [Name].vdi
  [Name].vmdk --format VMDK
```

konvertiert „clonemedium“ die angegebene VDI-Datei ins Vmware-Format. ■

Office & Produktivität

In diesem Artikel kommen neben Libre Office weitere Programme unter die Lupe, die im thematischen Umfeld von Büro und Produktivität stehen. Auch hier geht es um Schalteraktionen, welche die Möglichkeiten der grafischen Oberfläche erweitern.

VON HERMANN APFELBÖCK

Libre Office ist bei der CLI-Steuerung nicht so ergiebig, wie es die Abfrage mit „libreoffice --help“ zunächst erwarten lässt. Die diversen Hilfedokumente (etwa „--helpcalc“) sind ebenso wenig Kandidaten für die Kommandozeile wie der Start der einzelnen Komponenten wie etwa

```
libreoffice --calc
```

Das erledigen die vorgegebenen Starterlinks der Oberfläche ebenso. Dennoch verbleiben einige interessante Schalterkandidaten, insbesondere die Möglichkeit der Massenkonvertierung.

Die weiteren Beispiele mit Thunderbird, Fsearch und Keepass zeigen nützliche Tricks, die diese Programme noch effektiver machen. Die E-Book-Suite Calibre steht insofern für sich, als es sich um eine vollständig im Terminal administrierbare Programmsammlung handelt.

Libre Office: Konvertieren und mehr

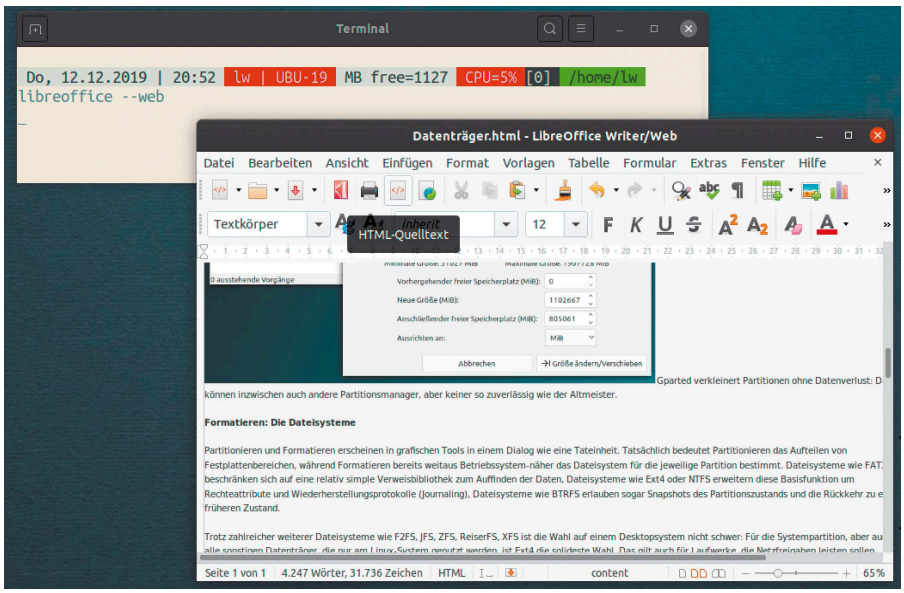
Auf die Schalteroption, Textdokumente (ODT, DOC, DOCX, HTML, TXT) in andere Formate wie PDF oder Epub zu konvertieren, hat bereits der Einstiegsartikel hingewiesen. Die Ausweitung zur globalen Massenkonvertierung ist kein großer Schritt: Der folgende Befehl konvertiert alle Dateien vom Typ DOCX (Microsoft Word) im aktuellen Verzeichnis und sämtlichen Unterverzeichnissen in das PDF-Format:

```
find . -type f -iname "*.docx" -exec
 libreoffice --convert-to pdf '{}'
 \;
```

Die Originale bleiben erhalten, die PDFs erhalten dabei den Originalnamen plus Extension „.pdf“.

Ein wichtiger Reparaturschalter ist dieser Befehl:

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



Libre Office Writer als HTML-Editor: Der Aufruf mit Parameter „--web“ ändert die Fensterdarstellung und liefert in der Standard-Symbolleiste spezielle Funktionen mit.

Die Office-Suite startet dabei mit einem Standardprofil und ignoriert dabei die Einstellungen des Benutzerkontos.

Der Aufruf

```
libreoffice --norestore
```

unterdrückt den Dialog „Dokumentwiederherstellung“ nach einem Beenden oder Crash mit nicht gespeicherten Dateien. Dies ist kein Befehl für den manuellen Gebrauch, sondern eher geeignet als Standardaufruf, wenn Sie das Wiederherstellungsangebot stört.

Mit dem Schalter

```
libreoffice --web
```

starten Sie die Komponente Writer als HTML-Editor.

Die Unterschiede zum Normalbetrieb sind nicht gravierend, aber doch deutlich: Die Symbolleiste bringt spezialisierte Funktionen mit wie „HTML-Quelltext“ und „Vorschau im Webbrowser“. Außerdem nutzt das Bearbeitungsfenster die gesamte Breite ohne Seitenformatierung.

Thunderbird: Safemode und Profile

Die wichtigsten Parameter beim Mozilla-Mailprogramm entsprechen jenen des Firefox-Bruders. Der Troubleshooting-Parameter

```
thunderbird -safe-mode
```

startet das Programm ohne Erweiterungen, wonach Sie eventuell problematische Addons entfernen oder deaktivieren können. Und genau 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. Mit

```
thunderbird --ProfileManager
```

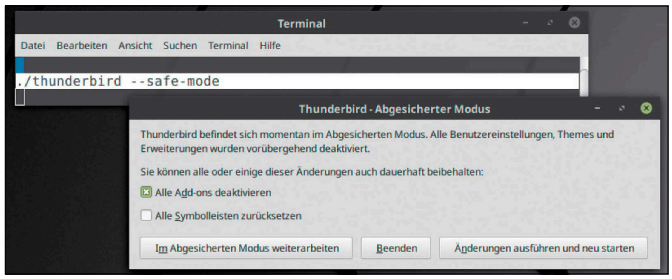
und „Profil erstellen“ entsteht ein neues Profil mit dem gewünschten Namen.
Um die Profile mit zwei Startern aufrufen zu können, benötigen Sie folgende Startparameter:

```
thunderbird -P Sepp
```

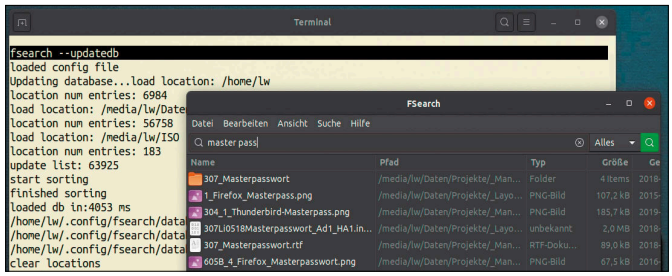
Noch besser: Sie können mit diesem Befehl sogar ein zweites Profil neben der bereits geöffneten Thunderbird-Instanz laden.
Mindestens zu erwähnen ist ferner der Schalter „--compose“, der per Kommandozeile sämtliche Maildetails übergeben kann, hier im Beispiel nur die drei wichtigsten (Empfänger, Betreff, Text):

```
thunderbird --compose "to=sepp@
 huber.de,subject=TEST,body=TEST"
```

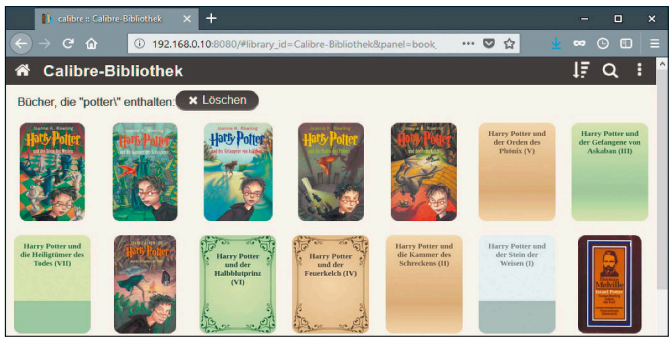
Wohl damit Thunderbird nicht als Spammaschine missbraucht wird, ist dann immer noch der manuelle Klick auf „Senden“ erforderlich (was theoretisch das xdotool übernehmen könnte). Ansonsten hat dieser Parameter praktischen Wert nur bei absolut standardisierten Nachrichten an immer gleiche Adressaten.



Thunderbird-Startparameter: Der hier angeforderte „Safe Mode“ ist ein Notschalter, um das Mailprogramm ohne Add-ons zu laden.



Tolle Dateisuche mit Datenbankupdate: Fsearch hat mittlerweile einen Schalter für die Datenbankaktualisierung, der einen automatischen Cronjob ermöglicht.



Calibre als E-Book-Server: Für solchen Servereinsatz bietet die E-Book-Suite ihren kompletten Funktionsumfang auch auf Kommandozeile.

Fsearch: Datenbankupdate für Suchtool

Das Tool Fsearch ist eine absolute Empfehlung für die schnelle Dateisuche in großen Datenbeständen und daher in neueren Distribution in den Paketquellen zu finden („fsearch-trunk“). Über sein PPA ist stets die neueste Version erreichbar:

```
sudo add-apt-repository
 ppa:christian-boxdoerfer/
 fsearch-daily
sudo apt update
sudo apt install fsearch-trunk
```

Fsearch hat einen früheren Mangel beseitigt und verdient genau deshalb seinen Platz an dieser Stelle. Die Datenliste lässt sich nämlich jetzt mit dem Befehl

```
fsearch --updatedb
```

„von außen“ aktualisieren. Solches Update erledigt Fsearch „headless“, also ohne Start der grafischen Oberfläche. Damit ist es nun möglich, die Datenbank automatisiert aktuell zu halten, etwa mit einem Cronjob alle vier Stunden.

Keepass-X: Synchrone Datenbank

Der Passwortmanager Keepass-X, der in allen verbreiteten Distributionen in den Paketquellen liegt (Paketname „keepassx“), arbeitet als rein lokale Software. Das Öffnen der lokalen KBD-Datenbankdatei erfordert die Eingabe des Keepass-Masterpasswort und ist daher auch bei physischem Fremdzugriff geschützt. Eine Synchronisierung des Keepass-Tresors (KBD-Datei) für mehrere Rechner ist allerdings nicht vorgesehen. Über den Keepass-Start mit der KBD-Datei als Parameter lässt sich dies aber dennoch realisieren, wenn die Keepass-Datei auf allen Rechnern im Synchronisierungsordner einer Cloud liegt – etwa bei Dropbox:

```
keepassx ~/Dropbox/[name].kbd
```

Weitere Sicherheitsmaßnahmen sind nicht erforderlich, weil Keepass-X selbst die KBD-Datei sicher verschlüsselt.

Calibre: E-Book-Verwaltung

Calibre ist eine spezialisierte Programmsammlung zur Verwaltung von E-Books und verdient aufgrund seiner lückenlosen CLI-Steuerung seinen Platz in dieser Artikelsammlung. Das Paket besteht aus einer Reihe von Einzelprogrammen wie calibre, calibre-server, calibredb, ebook-convert, ebook-viewer, die wiederum über ihre Manpage ihre Optionen preisgeben. Damit – und das ist sein Anspruch – lässt sich Calibre auf einem Server vollständig per SSH-Terminal verwalten (wobei allerdings zumindest die Ersteinrichtung mit grafischen Mitteln zu empfehlen ist). Der Befehl mit Angabe dees Bibliothekspfades

```
calibre-server /home/sepp/Calibre-
 Bibliothek/
```

startet die Serverkomponente und ist gleichbedeutend mit dem Menüpunkt „Verbinden/Teilen → Inhalteserver starten“ an der grafischen Oberfläche. Die Bibliothek ist danach mit jedem Browser über die IP-Adresse des Serverrechners zu erreichen und zu benutzen. Für den Ausbau und die Verwaltung der Bibliothek ist das Programm calibredb zuständig. Hier lautet wieder der wichtigste Schalter „add“, und der kann alles, was die grafische Oberfläche unter „Bücher hinzufügen“ anbietet. So importiert der Befehl

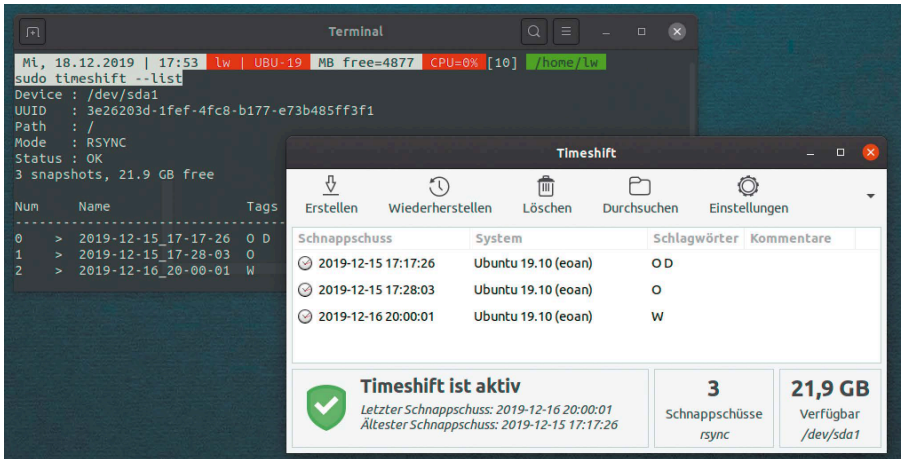
```
calibredb add --recurse /media/
 sepp/Data/PDFs
```

alle E-Book- und Textformate aus dem angegebenen Pfad in die Calibre-Bibliothek.

Systemtools & Zubehör

Kommandozeilenschalter von grafischen Systemtools und Zubehörprogrammen haben unterschiedliche Relevanz: Sie reicht von verspielten Nettigkeiten über wertvolle Automatisierungsoptionen bis hin zur schlichten Notwendigkeit.

VON HERMANN APFELBÖCK



Ein Tool wie die Timeshift-Systemsicherung wäre ohne Command Line Interface fast wertlos: Was helfen Ihnen Sicherungs-Snapshots, wenn Sie bei streikender Oberfläche nicht mehr darauf zugreifen können? Erst das CLI rüstet das Programm für alle Pannensituationen. Der Vorteil, statt Mausklicks auch Terminalschalter nutzen zu können, ist nicht überall so evident, aber lohnende Beispiele gibt es dennoch genügend.

Systemwiederherstellung mit Timeshift

Wie „timeshift --help" zeigt, hält dieses Tool zur Systemsicherung auch auf der Kommandozeile alle wesentlichen Funktionen bereit. Die allermeisten sind aber nur relevant, wenn Timeshift auf einem SSH-administrierten Server eingesetzt wird. Für das Erstellen eines Snapshots genügen dort zwei Befehle (Beispiel):

```
sudo timeshift --snapshot-device /
  dev/sdb1
sudo timeshift --create
```

Als Zielgerät (Snapshot-Device) kommt nur ein Datenträger mit Linux-Dateisystem in Frage.

Ein wichtiger Tipp führt zwar vom eigentlichen Schalterthema etwas weg, ist aber in diesem Zusammenhang unverzichtbar: Das CLI von Timeshift bietet nämlich keinen Exclude-Schalter, um Verzeichnisse von der Sicherung auszunehmen. Ohne solches Exclude kommt es auf einem Server typischerweise zur Situation, dass Timeshift eingehängte Datenpartitionen unter „/media", „/srv" oder „/mnt" sichern will. Das ist in der Regel nicht das, was man von einer Systemsicherung erwartet. Abhilfe schafft der Eingriff mit root-Recht in die Timeshift-Konfigurationsdatei „/etc/timeshift.json". Unter der Zeile „exclude" sind standardmäßig nur die Home-Verzeichnisse eingetragen. Darunter lassen sich weitere Verzeichnisse mit Benutzerdateien eintragen und damit von der Sicherung ausnehmen.

Auf einem Desktopsystem wird man die Sicherungspunkte lieber in der grafischen Oberfläche erledigen. Wenn im Zeitplan, den der Ersteinrichtungsassistent anbietet, eine periodische Sicherung (täglich oder wöchentlich) gewählt wird, übernimmt das sowieso ein automatischer Cronjob. Jedoch sollte jeder Desktopnutzer unbedingt wissen, dass die Wiederherstellung auch im Terminal und auch in der virtuellen Konsole möglich ist, falls die Oberfläche streikt. Die wahrscheinlich bequemste Methode, einen Snapshot wiederherzustellen, ist dieser Befehl:

```
sudo timeshift --restore
```

Dann zeigt Timeshift die Liste aller verfügbaren Snapshots automatisch an und der gewünschte kann mit der angegebenen Kennziffer ausgewählt werden. Etwas umständlicher und nur für eine automatisierte Wiederherstellung nötig ist die direkte Angabe des gewünschten Snapshots:

```
sudo timeshift --restore --snapshot
  '2019-12-12_18-23-08'
```

Die verfügbaren Snapshots zeigt Timeshift nach dem Befehl

```
sudo timeshift --list
```

an. Notwendig ist diese Verfahrensweise nur, wenn das System überhaupt nicht mehr läuft (auch nicht die virtuelle Konsole) und Timeshift auf einem externen Livesystem den angegebenen Snapshot zurückschreiben muss. Dabei ist zusätzlich die Angabe des Zielmediums erforderlich:

```
sudo timeshift --restore --snapshot
  '2019-12-12_18-23-08' --target /
  dev/sda1
```

Achtung: Nach einem „timeshift --restore“ folgt automatisch ein Systemneustart. Wenn man aus der grafischen Oberfläche wiederherstellt, sollten alle Dateien vorher gesichert werden.

Automatisierte Bleachbit-Löschaktionen

Das in den meisten Standard-Paketquellen erhältliche Bleachbit hat wirklich jede großräumige bis marginal-kosmetische Löschaktion im Repertoire und darf als klassischer Cleaner unter Linux gelten. Die meisten Löschaktionen finden im Home-Verzeichnis statt (Browser, Mail, Office), jedoch kann Bleachbit auch in der Paketverwaltung löschen, wenn es mit dem Menülink „BleachBit (as root)“ oder mit „sudo bleachbit“ im Terminal gestartet wird.

Bleachbit kann aber mehr, als in der grafischen Oberfläche angewählte Optionen abzuarbeiten. Alle Detailfunktionen sind auch als Terminalkommando abrufbar. Der Befehl

```
bleachbit --list-cleaners
```

zeigt alle Löschmodule an, annähernd 200 inzwischen, wovon aber die meisten nur Spezialroutinen für einzelne Programme sind (insbesondere für Browser). Jedes einzelne Modul kann mit dem Schalter „--clean“

```
bleachbit --clean system.cache
```

gestartet werden. Bei Löschzielen mit diversen Unterabteilungen (system, apt, firefox, chromium, google_chrome, thunderbird) funktioniert auch diese Variante:

```
bleachbit --clean apt.*
```

Damit können Sie Löschvorgänge durch ein Bash-Script automatisieren oder sogar als regelmäßigen Cronjob anlegen:

```
0 18 * * * bleachbit --clean
  firefox.*
```

Beachten Sie dabei aber, dass bestimmte Löschmodule (system, apt) nur mit root-Recht funktionieren.

Wer via SSH interaktiv auf die Terminalkommandos von Bleachbit ausweichen muss, hat hier alle Kontrollmöglichkeiten wie an der Oberfläche. Folgender Befehl

```
bleachbit --preview firefox.*
```

zeigt vorab ganz detailliert an, wie viele und welche Dateien der Clean-Befehl löschen würde.

Nachtlicht mit Redshift

Redshift ist in einigen Desktopdistributionen inzwischen vorinstallierter Standard, in jedem Fall aber über die Standard-Paketquellen zu erreichen. In Ubuntu hat der „Nachtmodus“ sogar Aufnahme in den allgemeinen Systemeinstellungen gefunden. Redshift arbeitet am Bildschirm als Blaufilter und erhöht den Rotanteil, was in den Nachtstunden augenschonend sein soll und besseren Schlaf verspricht. Um dem Anwender manuelle Einstellungen zu ersparen, ermittelt Redshift seit einigen Versionen automatisch den geografischen Standort des Anwenders und erhöht bei Einbruch der Nacht automatisch den Rotanteil. Wer solchen Automatismus nicht schätzt, kann auf die dauerhafte Aktivierung des Zubehörs verzichten und Redshift bei Bedarf interaktiv steuern:

```
redshift -O 4000
```

Dieser Schalter (großes „O“) stellt auf „warme“ 4000K mit deutlich verstärktem Rotanteil. Möglich sind Werte zwischen 1000 und 25000. Der Befehl

```
redshift -x
```

führt jederzeit zum Standard von 6500 K zurück.

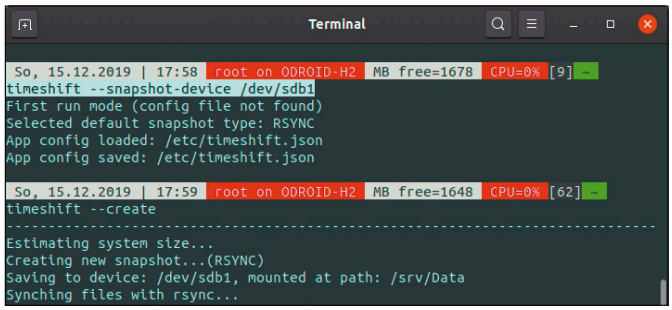
Die Dateimanager und der Punkt

Die Pfadangaben „.“ (Punkt) und „..“ (zwei Punkte) für das aktuelle beziehungsweise das nächsthöhere Verzeichnis sind lebende Fossile auf allen aktuellen Dateisystemen. Ein Alias wie

```
alias x='nautilus .'
```

mit dem ominösen Punkt gehört daher in jede „.bashrc“, um im Terminal auf schnellstem Weg den gerade aktuellen Ordner in

Timeshift im Terminal: Das Sicherungswerkzeug hat neben der grafischen Oberfläche ein (fast) vollständiges CLI und funktioniert daher auch per SSH oder in der virtuellen Konsole.





Bleachbit automatisieren: Der Allzweckcleaner kann solche Aufträge auch als Cronjob abarbeiten.

DESKTOPS NEU STARTEN

Gnome, Cinnamon, KDE & Co – alle Desktops bieten spezielle Schalter oder Kommandos, um die Oberfläche im Notfall zu beenden und neu zu laden, so etwa „gnome-shell --replace“ (Gnome), „cinnamon --replace“ (Cinnamon) oder „kquitapp5 plasmashell && plasmashell & disown“ (KDE). Wer dauerhaft mit einem Desktop arbeitet, kann sich wohl mit der jeweiligen Aktion anfreunden, allen anderen sei hingegen ein Vorgehen empfohlen, das überall unter dem Fenstersystem X11 funktioniert:

```
dm=$(basename "$(cat /etc/X11/default-display-manager)")
sudo service $dm restart
```

Hier wird einfach der aktive Displaymanager ermittelt und neu gestartet. Dies beendet den Desktop und startet ihn neu zum Anmeldefenster.

den grafischen Dateimanager zu laden. Die folgende Variante

```
alias x='xdg-open .'
```

ist gleichbedeutend, aber globaler, weil sie unabhängig vom Programmnamen des jeweiligen Dateimanagers funktioniert.

KDE-Dateimanager im Zwei-Fenster-Modus

„Orthodoxe" Dateimanager wie der Midnight Commander im Terminal oder der Gnome-Commander sind nach wie vor beliebt wegen ihres praktischen Zwei-Fenster-Modus. Das Prinzip beherrschen aber auch einige Standard-Dateimanager, wenn man den passenden Hotkey drückt oder schon beim Start den richtigen Parameter mitgibt. Der KDE-Dateimanager Dolphin ist ein Kandidat für diese Aufrufvariante

```
dolphin --split
```

oder gleich mit Angabe der gewünschten Startordner:

```
dolphin --split /home/sepp /media/
  sepp
```

Dies erzwingt zwei vertikal geteilte Fenster gleicher Größe. Dolphin kann solchen Zwei-Fenster-Start allerdings auch in den Einstellungen als Standard festlegen. Der Einsatz des Schalters ist also nur sinnvoll, wenn Sie sonst die normale Darstellung eines Ordners bevorzugen, für Kopieraufgaben aber den schnellen Link zum Zwei-Fenster-Modus schätzen.

Ein fester Platz für das Terminal

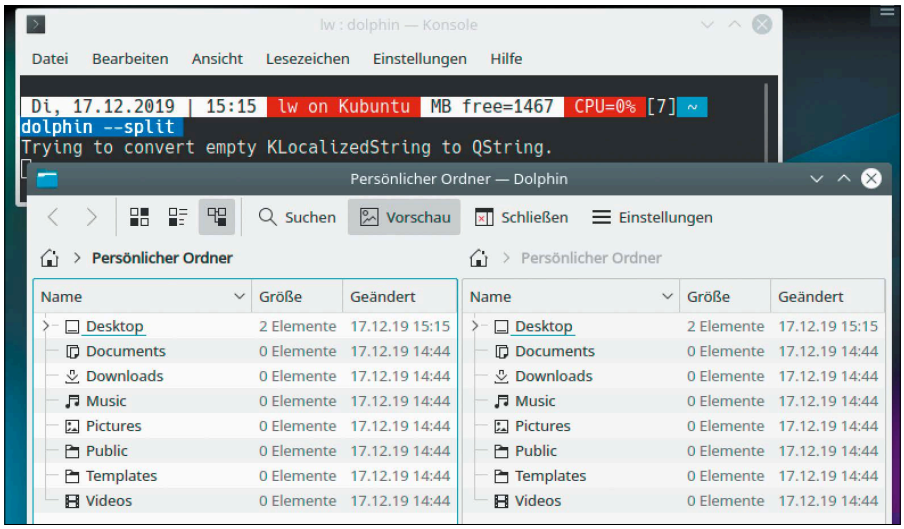
Wer das Terminal beim Start immer in gewünschter Größe und Position bereitstellt, erspart sich nachträgliches Verschieben und Größenänderungen. Die meisten Terminalemulatoren wie Gnome-Terminal oder Terminology können dies per Startparameter festlegen:

```
gnome-terminal
  --geometry=120x24+400+0
```

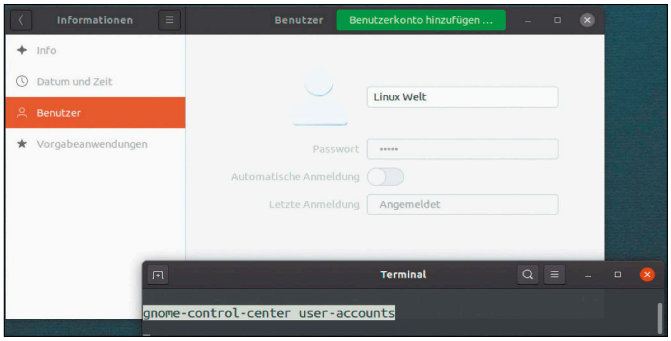
Dies würde ein Terminal mit 120 Zeichen Breite und 24 Zeilen Höhe oben und zentriert starten (letzteres ist abhängig von der Bildschirmauflösung). Diesen Aufruf definieren Sie am besten in einer eigenen „desktop"-Starterdatei und/oder als Befehl für den Terminal-Standardhotkey Strg-Alt-T.

Applets in den „Systemeinstellungen"

Die „Systemeinstellungen" von Gnome und Gnome-ähnlichen Desktops starten in der Regel mit dem Unterpunkt, wo sie zuletzt



Grafische Dateimanager akzeptieren in jedem Fall eine Ordnerangabe als Aufrufparameter. Dolphin unter KDE bietet außerdem den Zwei-Fenster-Modus mit Schalter „--split".



Direkter Sprung in ein Applet der „Systemeinstellungen": Das Gnome-Control-Center unter Ubuntu sowie das Pendant unter Linux Mint können per Schalter jeden Unterpunkt laden.

verlassen wurden. Die meisten Zentralen (nicht KDE) können aber auch jeden Punkt direkt per Startparameter ansprechen. Dieser Befehl

```
gnome-control-center -l
```

listet alle Bezeichnungen wie „network", „display", „info-overview", „user-accounts" auf, die das Systemprogramm direkt ansprechen kann. Ein Befehl wie

```
gnome-control-center user-accounts
```

startet dann die Zentrale gleich mit dem gewünschten Applet.

Die Zentrale Cinnamon-Settings von Linux Mint geht noch einen Schritt weiter. Die verfügbaren Applets sind in der Manpage (*man cinnamon-settings*) zu ermitteln – etwa „network" oder „display". Zusätzlich zum Start solcher Unterpunkte mit

```
cinnamon-settings network
```

gibt es aber etliche Punkte mit weiterführenden Registerkarten (Tabs). Diese lassen sich dann ganz präzise mit

```
cinnamon-settings applets -t 1
```

öffnen. Im Beispiel handelt es sich um die zweite Registerkarte „Download" zur Installation zusätzlicher Desktopapplets. Die Zählung der Tabs beginnt bei „0".

Das Screenshottool von KDE

Der Startbeitrag zu diesem Schwerpunkt nennt ein Beispiel, wie sich die zahlreichen Startparameter des Screenshottools von Gnome komfortabel in globalen Hotkeys verwenden lassen. Das unter KDE Plasma zuständige Tool Spectacle steht dem in nichts nach, sondern liefert eine noch umfassendere CLI-Steuerung (siehe *spectacle --help*). Folgender Befehl erledigt einen Vollbild-Screenshot

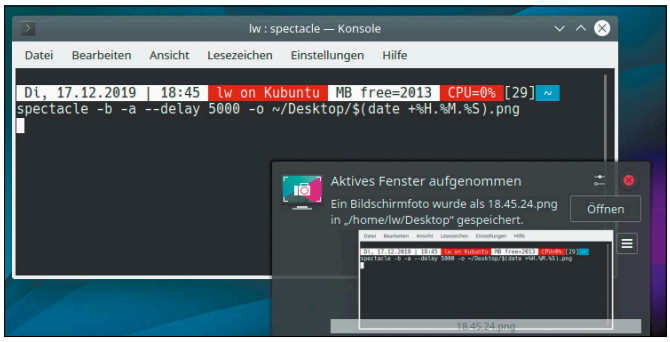
```
spectacle --fullscreen
  --background --output ~/
  Desktop/$(date +%H.%M.%S).png
```

und legt diesen mit Zeitstempel am Desktop ab. Der folgende Befehl

```
spectacle --activewindow --delay
  5000 --background --output ~/
  Desktop/$(date +%H.%M.%S).png
```

macht ein Bild vom aktiven Fenster und lässt dazu fünf Sekunden Wartezeit, um das gewünschte Fenster anzuklicken. Die Opti-

on „--background“ sorgt dafür, dass die in diesem Fall überflüssige grafische Oberfläche von Spectacle nicht erscheint.
Beachten Sie bei solchen und ähnlichen Befehlen, dass nur die Kommando-Shell Variablen wie „~“ und „$date“ korrekt auflöst. Für den Einsatz in einem Hotkey müssten Sie den Umweg über ein Shell-Script gehen, wie im Startbeitrag beschreiben.



Screenshots mit Spectacle (KDE): Mit solchen Befehlen als Alias oder Hotkey können Sie sich das Ablegen von Screenshot-Dateien vereinfachen.

Die Softwarezentrale in Gnome

Der grafische Paketmanager in der Ubuntu-Hauptedition und in anderen Gnome-ähnlichen Desktops hat einige Aufrufschalter mit eher geringer Relevanz für den Benutzeralltag, die überdies zum Teil unzuverlässig funktionieren (etwa „ gnome-software --details-pkg=[Paketname]“). Nützlich kann aber der direkte Sprung in einen bestimmten Übersichtsmodus sein:

```
gnome-software --mode=installed
```

Dies öffnet sofort die Liste der aktuell installierten Software. Weitere Modi sind „updates“ (ausstehende Aktualisierungen), „updated“ (aktualisierte Software) und „overview“ (die Standardübersicht).

Das xdotool steuert den Desktop

Wo es um Terminalkommandos geht, die grafische Programme beeinflussen und steuern, darf das spezialisierte xdotool nicht fehlen. Anders als die bisherigen programmeigenen Schalter ist das xdotool ein allgemeines Werkzeug für beliebige andere Programme und Aktionen an der grafischen Oberfläche.
Falls das kleine Zubehör nicht vorinstalliert ist, kann es mit gleichnamigem Paketnamen nachgerüstet werden. xdotool kann Mausaktionen oder Tastatureingaben per Terminalbefehl ausführen.
Folgender Befehl

```
xdotool key "super+d"
```

simuliert den Hotkey Windows-D, um den Desktop anzuzeigen. Ein weiteres einfaches Beispiel

```
xdotool mousemove 0 0;xdotool
  click 1
```

befördert den Mauszeiger in die linke obere Ecke (Position 0,0) und löst dort einen Mausklick aus. Um die exakte Mausposition eines Elements zu ermitteln, hilft dieser Befehl:

```
sleep 5;echo $(xdotool
  getmouselocation --shell)
```

Das Werkzeug kann aber weit mehr als Mausnavigation, Mausklicks oder Tastatureingaben („type“), weil es Herrschaft über alle Fensterfunktionen besitzt. Die folgende Befehlskombination

```
TMP=$(xdotool selectwindow);
  xdotool windowkill $TMP
```

wartet zunächst auf den Klick auf ein Programmfenster. Der Befehl „selectwindow“ ermittelt beim Klick das Fenster-Handle und mit dieser Kennziffer kann xdotool dann alle Fensteraktionen ausführen – hier gewaltsames Beenden. Ähnlich funktioniert das nächste Beispiel:

```
TMP=$(xdotool selectwindow)
xdotool windowunmap $TMP
zenity --calendar
xdotool windowmap $TMP
```

Hier macht das xdotool das geklickte Fenster unsichtbar. Der mit dem Tool zenity gestartete Minikalender hat nur den Tarnzweck, des neuerliche Sichtbarmachen mit „windowmap“ zu verzögern. Sobald der Kalender geschlossen wird, wird auch das versteckte Programmfenster wieder sichtbar. Auch hier gilt, dass solche Befehlsfolgen mit Variablen nur in der Shell funktionieren und daher der Umweg über ein Shell-Script notwendig ist.

Die Desktopsteuerung mit D-Bus

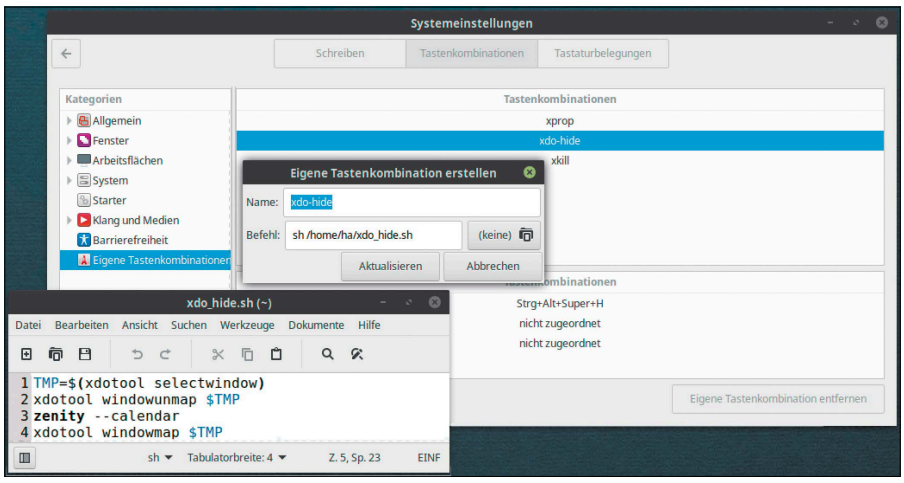
Praktisch alle Linux-Desktops verwenden die Schnittstelle D-Bus (Desktop-Bus) zur Prozesskommunikation. Die Interna dieser objektorientierten Schnittstelle führen schnell in Bereiche der Entwicklung und Programmierung, da die Objekte exakt benannt und die genauen Methodennamen verwendet werden müssen. Auch Groß- und Kleinschreibung ist exakt zu beachten. Trotzdem können zumindest einfachere Befehle mit *dbus-send* oder *gdbus* (etwas einfacher) auch vom Desktopbenutzer produktiv genutzt werden. Das folgende Beispiel adressiert das Objekt der Gnome-Shell und ruft dort die „Aktivitäten“-Übersicht auf:

```
dbus-send --session --type=method_
  call --dest=org.gnome.Shell /org/
  gnome/Shell org.gnome.Shell.Eval
  string:'Main.overview.show();'
```

Die Anwendungsübersicht in Gnome lässt sich mit diesem Befehl

```
gdbus call --session --dest org.
  gnome.Shell --object-path /org/
  gnome/Shell --method org.gnome.
  Shell.ShowApplications
```

auslösen. ■



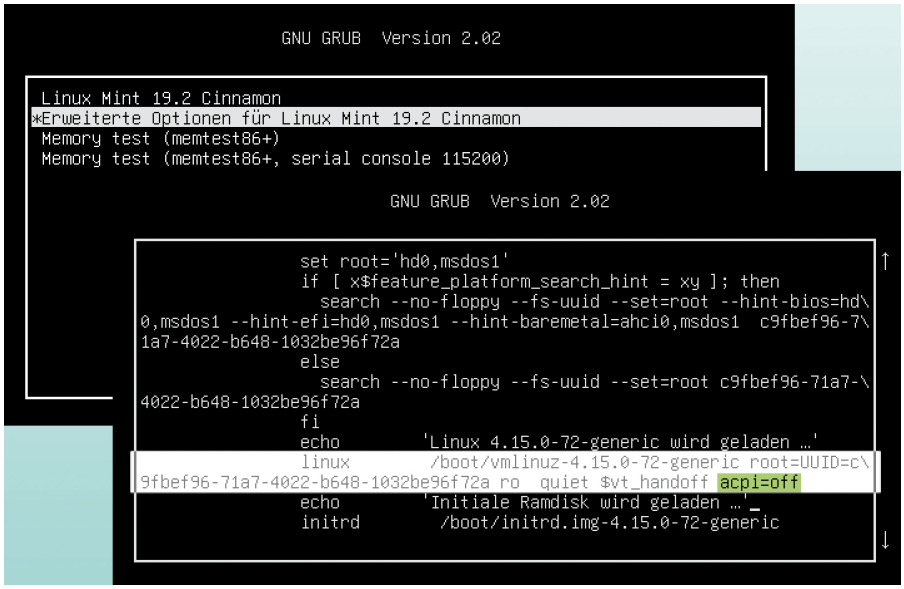
Desktopsteuerung mit xdotool: Hier dient das Werkzeug zum Verstecken von Fenstern. Als Auslöser wird der Hotkey Strg-Alt-Super-H angelegt.

Parameter des Linux-Kernels

Der Linux-Kernel ist kein grafisches Programm und fällt damit aus der Reihe der vorangegangenen Beiträge. Die Ausnahme ist aber durch ihr Gewicht zu rechtfertigen: Kernel-Parameter („Cheatcodes“) können fundamentale Startprobleme umschiffen.

VON DAVID WOLSKI UND HERMANN APFELBÖCK

Jedes Linux-System bietet eine stattliche Reihe von Kernel-Parametern. Diese steuern Kernel-Eigenschaften, Treiberoptionen und den Umgang mit Hardwarekomponenten. Die nachfolgend erklärten Parameter sind die wichtigsten Helfer für die häufigsten Startprobleme, es gibt aber noch mehr: Für Ubuntu und Co. liefert die englischsprachige Hilfeseite *https://help.ubuntu.com/community/BootOptions* eine Übersicht und eine komplette Liste bietet die offizielle Kernel-Dokumentation unter *www.kernel.org/doc/html/v4.10/admin-guide/kernel-parameters.html*.



Bootloader Grub: In Ubuntu oder Mint muss beim Start die Umschalt-Taste gedrückt werden, damit sich das Bootmenü mit seinen Bearbeitungsmöglichkeiten zeigt.

Cheatcodes setzen: Grub 2 oder Isolinux

Alle Kernel-Parameter werden als Optionen im jeweils verwendeten Bootloader angegeben, also entweder in Grub 2 oder in Isolinux. Die Vorgehensweise unterscheidet sich je nach Bootloader.

Grub 2: In den meisten Fällen erledigt Grub den Start von Livesystemen und Installationsmedien. Im Uefi-Modus ist Grub 2 so gut wie immer der verwendete Bootloader. Den Startdurchlauf können Sie mit früh gedrückter Umschalt-Taste bremsen, um an die erweiterten Optionen zu gelangen. Danach führt nach der Markierung eines Bootеintrags die Taste E zu einen rudimentären Texteditor. Der Editor ist mehrzeilig und bricht überlange Zeilen am Ende zur besseren Übersicht um. Die Navigation erfolgt mit Cursortasten. Grundsätzlich gehören Kernel-Parameter an das Ende jener Zeile, die mit „linux“ beginnt. Nach der Änderung der Zeile startet die Taste F10 den Bootеintrag mit den neuen Einstellungen.

Auch bei einem installierten Linux kommt fast immer Grub 2 zum Einsatz. Der temporäre Einsatz eines erforderlichen Kernel-Parameters gelingt analog wie für Livesysteme beschrieben, gilt aber nur für diesen einen Start. Um einen Parameter dauerhaft zu setzen, ist eine Bearbeitung der Konfigurationsdatei „/etc/gefault/grub“ mit root-Recht nötig:

```
sudo gedit /etc/gefault/grub
```

Dort definiert die Zeile

```
GRUB_CMDLINE_LINUX="[parameter]
 =[wert] …"
```

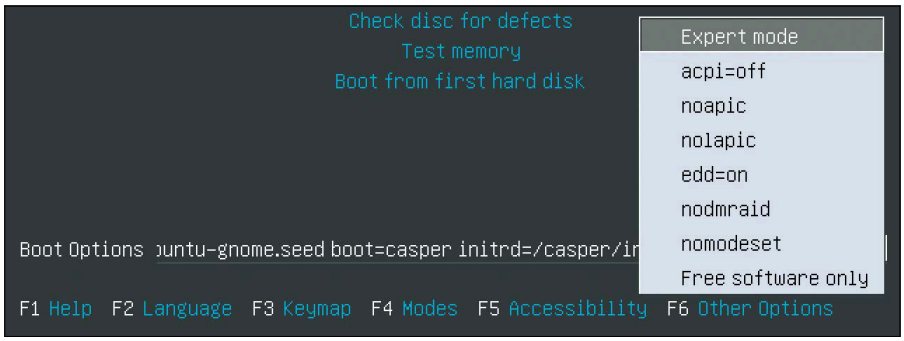
die manuell hinzugefügten Kernel-Parameter. Stehen hier schon Parameter, so ergänzen Sie die Zeile am Ende nach einem Leerzeichen. Generell sind Kernel-Parameter durch Leerzeichen voneinander abgetrennt und folgen entweder dem Schema „[Parameter]=[Wert]“ oder bestehen aus einem einzigen Schlüsselwort. Parameter sind frei kombinierbar, auch die Reihenfolge spielt keine Rolle. Nach dem Speichern der Konfigurationsdatei muss der Bootloader mit diesem Terminalbefehl über die neue Konfiguration informiert werden:

```
sudo update-grub
```

Isolinux: Bei einigen Livesystemen meldet sich Isolinux als Bootloader, falls das System im Bios-Modus und nicht über Uefi gestartet wird. Wird der Countdown angezeigt, so unterbricht der Druck auf eine beliebige Taste den Start. Isolinux zeigt

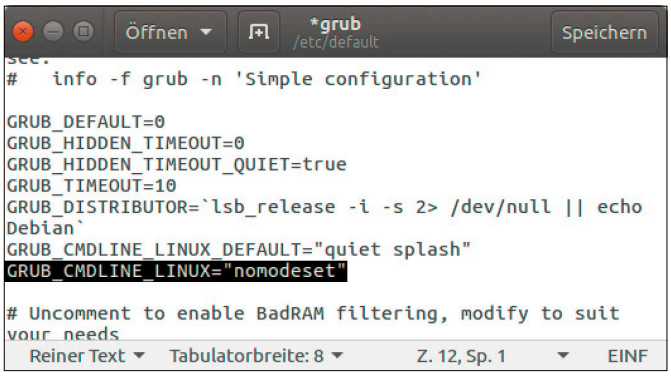
dann meist eine Oberfläche mit einigen Menüpunkten an, etwa zur Auswahl der Sprache. Die Tabulator-Taste verwandelt die untere Zeile in eine Eingabezeile und zeigt zum gerade ausgewählten Menüeintrag die Kernel-Parameter an. Am Ende der Zeile können Sie weitere Kernel-Parameter ergänzen und die Eingabetaste bootet dann das System mit den neuen Optionen.

Bei Ubuntu und Varianten vereinfacht Isolinux die Fehlerbehandlung über die Taste F6: Hier zeigt dann ein Untermenü die allerwichtigsten Kernel-Parameter wie „acpi=off“ und bietet diese per Mausklick an. Die Option „Expert mode“ führt zur manuellen Eingabezeile für die Kernel-Parameter.



Bootloader Isolinux: Dieser Bootloader wird immer seltener und brachte bei Ubuntu (Taste F6) ein Menü für die wichtigsten Cheatcodes mit. Der „Expert mode“ führt zur manuellen Bearbeitung.

Bootmenü von Grub 2 ergänzen: Kernel-Parameter, die auf installierten Systemen permanent gelten sollen, müssen in die Datei „/etc/gefault/grub“ eingetragen werden.



Wichtige Parameter bei ACPI-Problemen

Ein Dauerthema, das auf vielen Notebooks den Linux-Start verhindert, sind inkompatible Stromsparfunktionen im ACPI (Advanced Configuration and Power Interface), das ein Merkmal des Bios beziehungsweise Uefi ist. ACPI ist auf Windows zugeschnitten und es gibt zu viele Abweichungen, um von einem Standard sprechen zu können.

acpi=off zwingt Linux dazu, ACPI komplett zu ignorieren und damit ohne Stromsparfunktionen und Leistungsmanagement für CPU und GPU zu starten. Auch das Hyperthreading und die Lüfterregelung sind abgeschaltet.

acpi=ht erlaubt dem Linux-Kernel gerade mal noch so viele ACPI-Fähigkeiten der Hardware, dass das Hyperthreading der CPU funktioniert. Andere Stromsparfunktionen bleiben dagegen deaktiviert.

acpi=strict weist die ACPI-Unterstützung des Kernels an, nur ACPI-Merkmale der vorhandenen Hardware zu beachten, die exakt dem Standard folgen. Auf problematischen Notebooks ist diese Option immer einen Versuch wert.

acpi=noirq: Dieser Parameter lässt die ACPI-Unterstützung des Kernels intakt, weist das System aber an, die Verteilung von Hardwareinterrupts für PCI-Geräte nicht auch ACPI zu überlassen. Bei störrischen Notebooks oder bei spontanen Abstürzen während des Betriebs kann der Parameter oft weiterhelfen.

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.

Grafikprobleme und weitere Hürden

Bleibt der Bildschirm nach einem zunächst erfolgreichen Start dunkel, wenn eigentlich der Desktop des Livesystems oder der Anmeldebildschirm erscheinen sollte, so liegt dies meist an nicht ausreichend unterstützten Grafikchips. Folgende Parameter können in diesem Fall 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 Boots in einen grafischen Modus. Dies funktioniert nicht bei allen Grafikchips – etwa haben die meisten Modelle von Nvidia Probleme damit. Mit dem Parameter „nomodeset“ verzichtet der Kernel auf den Wechseln in den Grafikmodus und bleibt bei purem Text. Eine weitere Komponente APIC (Advanced Programmable Interrupt Controller) hat mit dem angesprochenen ACPI nichts zu tun, sondern steuert die Interruptanforderungen der Prozessorkerne. APIC kann aber ebenfalls Ärger verursachen. Der Parameter

nolapic löst Probleme mit heiklen Bios-Versionen, reduziert aber in jedem Fall die Zahl der vorhandenen CPU-Kerne auf einen. Der Schalter eignet sich nur als erste Hilfe, bis ein Bios-Update oder eine neue Kernel-Version 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 Chipset weiter. Eine häufig erfolgreiche Kombination bei besonders widerspenstigen Notebooks ist

```
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 auf 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. ■

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: 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.

LINUX WELT

Stellen Sie uns auf die Probe!

2x LinuxWelt zum Testpreis



Jetzt testen:
2x LinuxWelt
gedruckt & digital

11,90 €

Satte **30 %** gespart!

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

- ✓ **2x LinuxWelt als Heft frei Haus** mit Gratis-DVD
- ✓ **2x LinuxWelt direkt aufs Smartphone & Tablet** mit interaktivem Lesemodus

Jetzt bestellen unter
www.pcwelt.de/linuxtesten 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 Testabo für 11,90 €.

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

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

LWPMA14147

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



Sicher und Privat

Alle Systeme von TUXEDO Computers kommen startklar mit Linux. Sie bieten neben beeindruckender Leistung auch eine umfassende Absicherung Ihrer persönlichen Daten sowie starken Schutz Ihrer Privatsphäre.

Privatsphäre+
Intel ME, Webcam, Audio und WLAN abschaltbar

Vollverschlüsselung
System und Daten komplett geschützt vor Unbefugten

Frei von Spyware
Überprüfbare Sicherheit dank Open Source Software

Automatische Installation
Systemreset dank webbasierter, vollautomatischer Installation

100% Linux

5 Jahre Garantie

Lifetime Support

Gefertigt in Deutschland

Deutscher Datenschutz

Support vor Ort

TUXEDO COMPUTERS

tuxedocomputers.com