LINUX WELT XXL

SONDERHEFT XXL 2/2018 Mai – Juli
€ 12,90 CH 25,80 sfr · Österreich, Benelux 14,40

NEU!
196 Seiten!

Linux KOMPLETT!

Alle Infos zu Mint, Ubuntu & Co.

Das Handbuch 2018

Linux perfekt einrichten

Die besten neuen Systeme finden

Linux optimal installieren und konfigurieren

Mehrere Systeme auf einem PC einrichten

Drucker und Scanner anschließen

Nutzerrechte vergeben und verwalten



Linux optimal nutzen

Alle Routine-Aufgaben automatisch starten

Freigaben im Netzwerk festlegen und kontrollieren

Alle Dateiformate einfach für Linux konvertieren

Desktop und Terminal im Praxiseinsatz

Profi-Tricks und Troubleshooting

Linux als Server nutzen

Virtualisierungs-Software tunen

Bootprobleme lösen und Systemabstürze beseitigen



Sicher mit Linux!

Komplette Systemverschlüsselung · Daten und Datenträger sichern · Security-Einstellungen für Browser und Mailprogramm

PLUS: Rettungssystem auf DVD

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

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. 49,50 EUR. Danach ist eine Kündigung zur übernächsten Ausgabe jederzeit möglich.

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

Arne Arnold,
Redakteur
aarnold@it-media.de



Vielseitig, einfach und sicher: Linux

Vielseitig: Das freie Betriebssystem Linux hat ungemein viel zu bieten. Es läuft auf Ihrem Desktop-PC genauso gut wie auf einem Heimserver oder einem Mini-PC wie dem Raspberry Pi. Und in jedem Fall haben Sie die Wahl aus Dutzenden unterschiedlichen Systemen. Damit Sie bei der Vielfalt den Überblick behalten und das für Ihren Rechner optimale Linux finden, stellen wir Ihnen hier die interessantesten Systeme vor.

Einfach: Wenn Sie Linux nur ausprobieren möchten, geht das mit der Heft-DVD ganz einfach. Denn mit den sieben Livesystemen auf unserer Heft-DVD starten Sie – ohne Installation – Ihren Rechner mit Linux und haben innerhalb kürzester Zeit ein komplettes Ubuntu oder Mint laufen. Die Daten und das System auf Ihrem PC bleiben von dieser Aktion völlig unberührt.
Sollten Sie als Windows-Umsteiger beim Ausprobieren von Linux Fragen haben, finden Sie die Antworten sehr wahrscheinlich ab Seite 46 in unserem Umsteiger-Guide.

Sicher: Als Linux-Nutzer profitieren Sie von einem System, das kaum von PC-Viren bedroht ist und für das es sehr schnell Updates gegen neue Sicherheitslücken gibt. So waren Linux-Nutzer gegen Meltdown, eine der größten Sicherheitslücken der IT-Geschichte, als erste vor allen anderen Nutzern geschützt. Infos zur Sicherheit für Ihre Daten finden Sie ab Seite 150.

Komplett: Dieses Linux-Handbuch für das Jahr 2018 möchte Sie mit allem Wichtigen für Ihren Rechner und Ihren Heimserver versorgen. Zu den 196 Seiten dieses Hefts finden Sie deshalb noch 33 Handbücher auf der Heft-DVD mit einem Gesamtumfang von 5500 Seiten. Insgesamt also genügend Lesestoff für spannende Entdeckungen.

Viel Spaß beim Lesen!



Jetzt testen! Die Magazin-App von PC-WELT, LinuxWelt & Co.

Wir haben die Magazin-App der PC-WELT speziell für Sie entwickelt – und die Vorteile liegen direkt auf der Hand: Alle Hefte, alle Reihen und alle Sonderhefte stehen dort für Sie bereit. Die App läuft auf allen großen Mobil-Plattformen – iPhone, iPad, Android, Windows und Windows Mobile, allerdings noch nicht unter Linux.
Die erste Ausgabe, die Sie herunterladen, ist für Sie kostenlos. Um die App zu nutzen, installieren Sie die für Ihr Gerät passende Version einfach über die Download-Links unter *www.pcwelt.de/app*. Auf dieser Seite finden Sie auch alle Informationen zum schnellen Einstieg und zu neuen Funktionen. Als Abonnent – zum Beispiel der LinuxWelt – bekommen Sie die entsprechende digitale Ausgabe für Ihr Mobilgerät kostenlos dazu, auch mit speziell angepasstem Lesemodus und Vollzugriff auf die Heft-DVD.

Übrigens: Wenn Sie eine digitale Ausgabe gekauft haben, können Sie sie auf allen Ihren Geräten lesen.



www.pcwelt.de/app

Linux für jeden Zweck

Oft ist es keine leichte Aufgabe, die passende Linux-Distribution für die anvisierte Aufgbe zu finden. Hier hilft unser Überblick über die wichtigsten Systeme mit ihren Vor- und Nachteilen. Zum Glück gibt es für alle Aufgaben und für jede Hardware ein passendes System.

ab S. 54



Grundlagen

8 | Das komplette Linux-Handbuch 2018
Es lohnt sich, in diesem Jahr mal wieder Ihr Linux-System auf Vordermann zu bringen

10 | Distributionen auf Heft-DVD
Sieben Mal Linux zum Ausprobieren, Installieren und als Problemlöser

16 | Handbücher auf DVD
Dokumentation und Wissen in 33 wichtigen Handbüchern

18 | Linux-Distributionen: ein Überblick
Ein erster Richtungskompass im Linux-Distributionsdschungel

22 | Hauptstämme im Radarcheck
Arch, Debian, Gentoo & Co.: Was die Linux-Hauptlinien unterscheidet und wo Stärken und Schwächen liegen

26 | Die Linux-Desktops
KDE, Gnome, Cinnamon & Co.: Kurzvorstellungen und Zielgruppenbestimmung für 16 Linux-Oberflächen

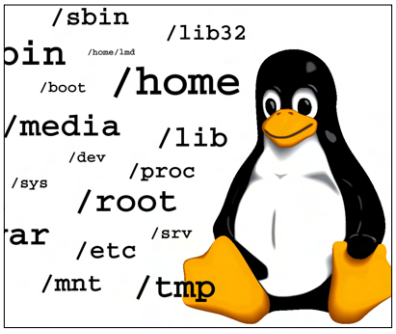
30 | Linux-Images & Livesysteme
Unentbehrliche Grundlagen zur variablen Nutzung und Verarbeitung von Linux-Systemabbildern

34 | Die Linux-Installation
Solo, Multiboot, Verschlüsselung, Uefi: Die Installationsgrundlagen am Beispiel des Ubuntu-Installers

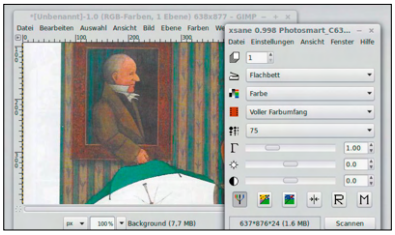
38 | Das Linux-Dateisystem
Organisation und Rechte im Dateisystem: Der Beitrag zeigt die Grundlagen und praktische Eingriffsszenarien

42 | Drucker & Scanner
Treiber – Konfiguration – Komfortfunktionen – Freigaben: So nutzen Sie Drucker, Scanner und Multifunktionsgeräte

46 | Linux für Umsteiger
Wer Windows kennt, kommt auch mit Linux zurecht: Die nötigen Tipps gibt's in diesem Beitrag



Seite 38: Laufwerksbuchstaben gibt es bei Linux nicht, sondern standardisierte Ordner.



Seite 42: Drucker installieren: Meist erkennt Linux USB- und Netzwerkdrucker.

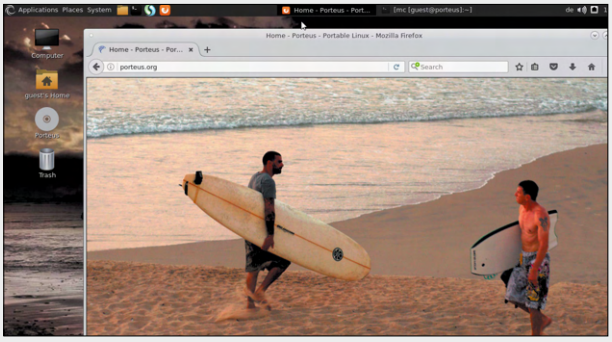


Linux ist anders als Windows: Das Wichtigste bespricht der Beitrag ab Seite 46.

Porteus: Elegantes Surfsystem

Zum Surfen ideal ist ein ballastfreies und flott startendes Minisystem wie Porteus.

ab S. 62

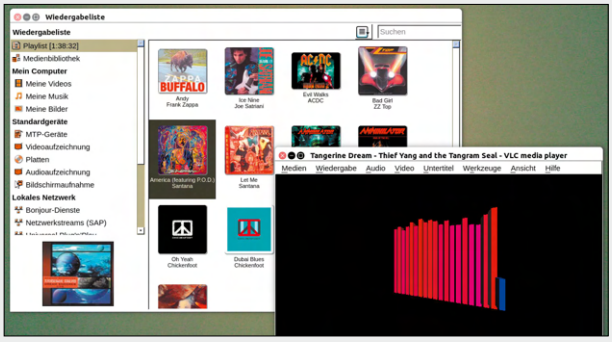


Alleskönner VLC

Für Video, Musik und mehr

Der Mediaplayer VLC darf auf keinem Linux- oder Windows-Rechner fehlen, weil er praktisch alle Video- und Musikformate abspielt.

ab S. 72



Linux für jeden Zweck

54 | Universalsystem Linux Mint 18.3
Neuestes Mint mit Service-Pack-Status „3“ und viel Feinschliff in System und Desktop

58 | Schwache Hardware: Lubuntu
Pragmatiker mit LXDE-Desktop: Das schlanke Lubuntu kann mehr, als der erste Anschein vermuten lässt

60 | Schwache Hardware: Bodhi Linux
Klein und exotisch: Bodhi Linux ist enorm schnell, präsentiert aber einen gewöhnungsbedürftigen Desktop

62 | Zweitsystem: Surfsystem Porteus
Schnell, portabel, sicher: portables Surfen im Fokus

64 | PC-WELT-Notfallsystem
Linux rettet Windows: Das Livesystem ist auf Windows-Pannen spezialisiert

66 | LinuxWelt-Rettungs-DVD
Linux rettet Linux: Das Livesystem liefert alle Tools für die Linux-Reparatur

68 | Server: Ubuntu Server
Die Serverversion von Ubuntu ist schnell installiert

70 | Multiboot-Umgebungen schaffen
Wir zeigen Ihnen, worauf Sie achten müssen

Software

72 | Alleskönner VLC
Durchblick im VLC: Nutzen Sie den ganzen Funktionsumfang

78 | Swiss File Knife (SFK)
Turbobefehle für die Shell: Das Swiss File Knife funktioniert unter Linux und Windows

80 | Zwei-Fenster-Dateimanager
Varianten eines Erfolgsrezepts: „Orthodoxe“ Dateimanager für Linux

82 | Fotos unter Digikam
Fotosammlungen verwalten: Digikam beherrscht Stichwörter und Metadaten

86 | Ubunsys für Server
Neues Admin-Tool mit interessanten Optionen, aber Reifemängeln

88 | Virtualisierungsgrundlagen
So funktionieren virtuelle Betriebssysteme

92 | Vmware in der Praxis
Installation – Erweiterungen – Gastsysteme

98 | Virtualbox in der Praxis
Grundlagen und Tipps für optimales Virtualbox

Dateien und Ordner im Griff

Hier finden Sie Grundlagen und raffinierte Tipps zum Umgang mit Dateien, Ordnern, Rechten und Dateiformaten.

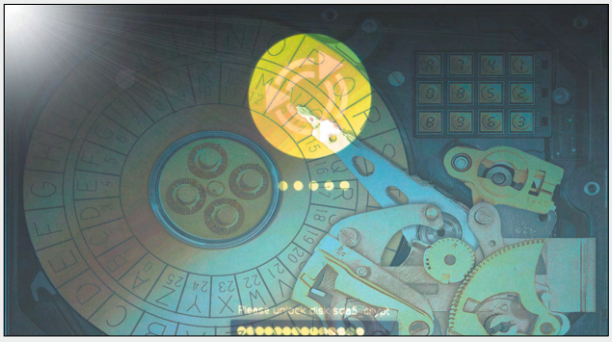
ab S. 112



Alles verschlüsselt!

Linux ist Verschlüsselungs-Weltmeister: Dieser Schwerpunkt erklärt alle prominenten Techniken und wofür sich diese jeweils am besten eignen.

ab S. 150



Tipps & Tricks für Linux

104 | Notfallknopf für Linux
So löschen Sie Benutzerordner während der Anmeldung am System

106 | Cronjobs ausgereizt
Basics und Geheimnisse der Crontab: Diese Optionen der Crontab sind längst nicht jedem Linux-User geläufig

108 | Websites einfach klonen
Die Werkzeuge Httrack und Wget: Damit gelingen komplette oder selektive Kopien von Websites

110 | Verspielte Terminaltools
Terminal und Scripts mit Charme: Textkunstwerke, sprechende Rechner, besonders kluge Kühe und mehr ...

112 | Dateibearbeitung
Großer Ratgeber zur Datei- und Ordnerbearbeitung unter Linux

Standards

3 | Editorial
194 | Impressum

Pannenhilfe für Linux & Hardware

124 | Defekte Hardware
Diagnose von Hardwarefehlern und Komponententausch

128 | Netzwerkprobleme lösen
Mit systematischer Suche grenzen Sie Fehler ein

132 | Bootprobleme (Grub)
Die Bootumgebung ist defekt oder von Windows überschrieben? Diese Reparaturvarianten sollten Sie kennen

136 | ISO-Dateien booten
Grub 2 kann Livesysteme auch direkt aus ihren ISO-Dateien heraus booten

138 | Starthilfe mit Kernel-Schalter
Spezielle Kernel-Cheatcodes machen den Linux-Start toleranter

142 | Instabile Systeme
Absturzanalyse: So unterscheiden Sie Softwarebugs von Hardwaredefekten

144 | Datenrettung nach Abstürzen
So retten Sie wichtige Daten und sichern defekte Partitionen

146 | Desktop- und X-Server-Fehler
Wenn die Oberfläche nicht startet oder hängt: Das hilft zuverlässig weiter

148 | Rechteprobleme lösen
Zugriff verboten? So korrigieren Sie Besitzer und Zugriffsrechte



Seite 132: Insbesondere nach Windows-Installationen muss Grub repariert werden.



Seite 136: Grub 2 kann Livesysteme auch direkt aus ihren ISO-Dateien heraus booten.

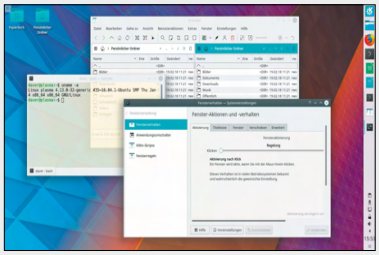
Die Highlights auf Heft-DVD



Sieben Mal Linux zum Ausprobieren, Installieren und als Problemlöser: Die Heft-DVD bietet eine sorgfältige Auswahl aktueller Systeme. Der Schwerpunkt liegt auf Distributionen, mit welchen Linux als Betriebssystem im Alltag glänzt.

ab S. 10

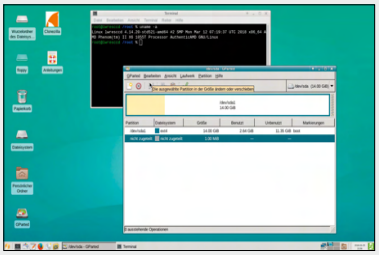
KDE Neon User Edition
Mit dieser Variante bekommt dieser Desktop ein neues Vorzeigesystem der KDE-Entwickler selbst



Ubuntu Mate 18.04-daily
Die einsteigerfreundliche Ubuntu-Variante zeigt sich mit interessanten Neuerungen



LinuxWelt-Rettungs-DVD
Reparieren, testen, sichern, wiederherstellen: Die wichtigsten Linux-Tools zur Datenrettung



Sicherheit

150 | Verschlüsselung
Der Artikel stellt alle Methoden vor, bewertet sie und bringt eine vollständige Praxisanleitung für die Einrichtung und Nutzung

160 | Verschlüsseln per Mausaktion
Incron-Grundlagen am Beispiel einer Veschlüsselungsroutine: Eine Mausaktion verschlüsselt Dateien

Raspberry-Projekte & Hardwaretricks

162 | Fritzbox & Co. ausgereizt
Neue und alte Router: Wie Sie das Potenzial ausschöpfen (Open WRT, Multi-WAN, Smarthome) und Altgeräte für neue Einsatzzwecke aufbereiten

172 | Privates Netz mit Pi VPN
VPN-Server ganz einfach: Pi-VPN erspart viel Einrichtungsaufwand

174 | Tipps zu Open Media Vault 3
Das NAS-System Open Media Vault Version 3 „Erasmus“ ist seit längerem verfügbar und läuft nun sehr stabil. Hier erfahren Sie, wie Sie das System installieren, einrichten und bedienen

Server & Netzwerk

176 | Der Samba-Server
Die verbreitetste und universellste Serverrolle: Linux als Datenserver mit Samba

178 | Multifunktionale Home-Cloud
Warum sich eine Nextcloud-Instanz auch im lokalen Netz lohnt

181 | Infos, Texte und Notizen
Notizen, Wikis und Suchserver: Diese Lösungen zentralisieren Ihre wichtigsten Infos

184 | Termine und Adressen
Ein Kalenderserver mit Radicale oder Baikal vereinfacht die Verwaltung Ihrer Termine

186 | E-Books im Netzwerk
Ein Server mit Calibre stellt die E-Book-Bibliothek für alle Netzgeräte via Browser bereit

188 | Der eigene Fotoserver
Bilderzentrale je nach Anspruch mit minimalistischem Single File PHP Gallery oder ausgewachsenem Piwigo

190 | Webserver Nginx
Schneller als Apache: Was Nginx besser und anders macht

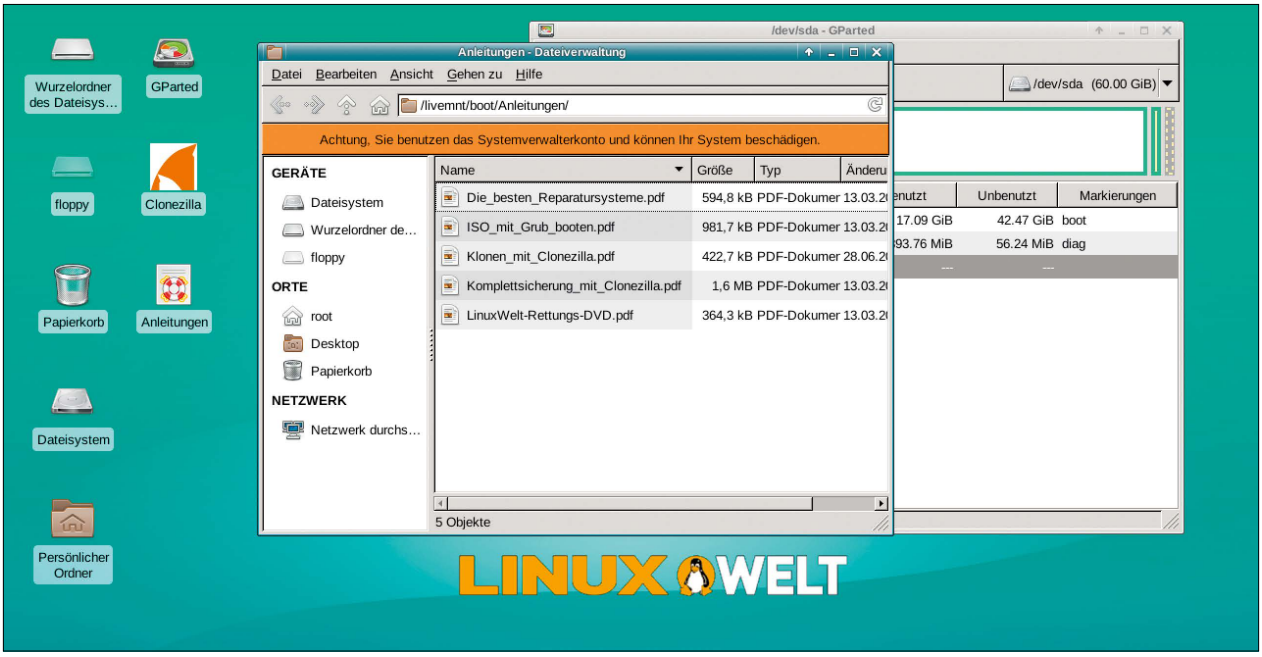
192 | VPN mit Sshuttle
Virtual Private Network über SSH – der einfachste Weg



Das komplette Linux-Handbuch 2018

In diesem Jahr gibt es wieder eine LTS-Version von Ubuntu. Für diese Long-Term-Support-Version (LTS) bekommen Sie fünf Jahre lang Updates. Es lohnt sich also, in diesem Jahr mal wieder Ihr Linux-System auf Vordermann zu bringen.

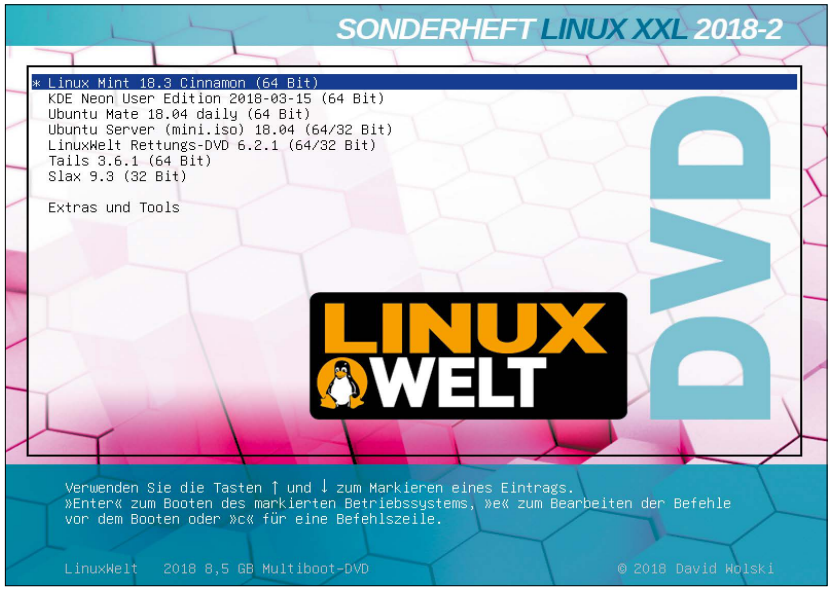
Von **Hermann Apfelböck, Arne Arnold und David Wolski**



Mit diesem Linux-Handbuch halten Sie alle wichtigen Infos zu Linux für das Jahr 2018 in Händen. Und es lohnt sich, dieses Jahr mal wieder eine gründliche Systempflege zu betreiben. Mit Ubuntu 18.04 gibt es seit dem 26. April 2018 eine neue LTS-Version. Auf der Heft-DVD dieser Ausgabe finden Sie eine Vorabversion von Ubuntu Mate 18.04-daily, die sich nach der Installation auf die aktuelle Final-Version aktualisiert. Nach Erscheinen der Hauptausgabe von Ubuntu 18.04 werden auch alle Nebenausgaben von Ubuntu wie Kubuntu, Ubuntu Budgie oder Xubuntu ebenfalls mit aktualisiertem Unterbau auf Basis von 18.04 bereitstehen.

Ein Update Ihres aktuellen Linux-Systems oder eine saubere Neuinstallation lohnt sich also, da die LTS-Version fünf Jahre mit Updates versorgt wird. Vielleicht probieren Sie aber auch einmal ein anderes Linux-System aus. In den Rubriken „Grundlagen“ und „Linux für jeden Zweck“ stellen wir viele verschiedene Distributionen vor.

Pannenhilfe: Die Freude an Updates und neuen Systemen kann allerdings auch schnell in Frust und Ärger umschlagen, wenn nach einem Systemwechsel oder -upgrade Linux nicht mehr starten möchte oder zumindest wichtige Hardwarekomponenten nicht mehr wie gewünscht funktionieren. Gegen solche Fälle finden Sie in der Rubrik „Pannenhilfe für Linux & Hardware“ Tipps und Tricks für den Notfall. Auf der Heft-DVD gibt’s dazu das exklusive LinuxWelt-Rettungssystem, mit dem sich PCs auch dann wieder flottmachen lassen, wenn der Bootmanager streikt. Die Abbildung oben zeigt übrigens die LinuxWelt-Rettungs-DVD, auf deren Desktop Sie zusätzlich



Das DVD-Bootmenü: Hier starten Sie sieben Livesysteme, die Sie auch installieren können, oder Sie nutzen unter „Extra und Tools“ wichtige Servicesysteme.

Überblick Auf DVD

KDE Neon User Edition 2018-03-25 (64 Bit)
Ubuntu-Variante der KDE-Entwickler 11

Ubuntu Mate 18.04-daily (64 Bit)
Einsteigerfreundliche Ubuntu-Variante 12

LinuxWelt-Rettungs-DVD 6.2.1
Repariert defekte Bootloader und Systeme 13

Linux Mint 18.3 Cinnamon
Beliebtes Linux-System für Einsteiger und Profis 14

Slax 9.3
Minimalistisches System zum Surfen 14

Tails 3.6.1
Anonym im Web surfen 15

Ubuntu Server (mini.iso) 18.04
Serverinstallation in der neuen Version 18.04 15

Handbücher für Linux
33 Nachschlagewerke zu allen wichtigen Linux-Themen

Extras und Tools
Boothelfer und Hardwareanalyse: Supergrub, Plop Bootmanager, Memtest, Hardware Detection Tool (HDT)

noch mehrere Anleitungen für den Notfall finden.

Sicherheit: Ein weiterer wichtiger Schwerpunkt in unserem Linux-Handbuch 2018 ist das Thema Sicherheit. In der entsprechenden Rubrik haben wir alle die Tools und Tipps zusammengetragen, die Sie für einen guten Datenschutz und hohe Datensicherheit benötigen. Das betrifft sowohl Ihre Daten auf dem Rechner als auch beim Surfen im Internet.

33 Handbücher auf Heft-DVD: Wenn Ihnen die Infos dieser LinuxWelt XXL mit ihren 196 Seiten noch nicht ausreichen, finden Sie über die Bedienerführung der Heft-DVD unter der Rubrik „Handbücher als PDF“ 33 Nachschlagewerke zum Thema Linux und Open-Source-Software. Für Einsteiger lohnt sich zum Beispiel ein Blick in die PDFs zu Ubuntu, Linux und Open Suse. Dort finden sich leicht nachvollziehbare Beschreibungen zu Installation, Einrichtung und Softwarenutzung. Das Distributionshandbuch zu Ubuntu geht auch detailliert auf die vorinstallierte Standardsoftware ein und ist somit auch ein Einsteigerleitfaden für Firefox, Thunderbird, Rhythmbox & Co. Die PDFs zu den verschiedenen Mint-Ausgaben fokussieren auf System und jeweilige Oberfläche.

Livesystem von der DVD booten: Die Benutzung der beiliegenden DVD ist einfach und im Heft nicht weiter erklärt. Um ein Livesystem zu starten, legen Sie die DVD ins Laufwerk und booten den Rechner von DVD. Dazu rufen Sie beim Rechnerstart per Tastendruck das Bios-Bootmenü auf und wählen das DVD-Laufwerk oder Sie ändern die Bootreihenfolge im Bios. Im Menü der Heft-DVD (siehe Bild und Tabelle rechts) wählen Sie dann eine Distribution aus.

In der Regel gelingt der Aufruf mit der Option „Normaler Start“. Beim Start eines Systems von der Heft-DVD bleibt Ihre Festplatte ebenso unberührt wie das dort installierte Betriebssystem. Dies gilt natürlich dann nicht mehr, wenn Sie aus dem Livesystem die Installation starten.

Die meisten der Systeme liegen auch als ISO-Image auf Heft-DVD (im Verzeichnis „/Image-Dateien“). Damit haben Sie die Möglichkeit, die Systeme bootfähig wahlweise auf eine eigene CD/DVD oder auf einen USB-Stick zu kopieren. Die dafür notwendigen Werkzeuge für Linux wie Windows finden Sie ebenso auf der Heft-DVD wie praktische Anleitungen hierzu.



33 Handbücher mit über 5500 Seiten geballtem Linux-Wissen finden Sie auf der Heft-DVD.

Heft-DVD: Eine Scheibe Linux

Sieben Mal Linux zum Ausprobieren, Installieren und als Problemlöser: Die Heft-DVD bietet eine sorgfältige Auswahl aktueller Systeme. Der Schwerpunkt liegt auf Distributionen, mit welchen Linux als Betriebssystem im Alltag glänzt.

Von **David Wolski**



Die Welt der Server und Embedded-Geräte ist durch Linux ein munteres, wachsendes Pinguin-Reservat geworden. Wo aber steht Linux auf dem Desktop, als Alltagssystem? Geht man nach den Markterhebungen verschiedener Onlinedienste, so steht Linux auch bei sehr optimistischen Schätzungen Anfang 2018 bei höchstens drei Prozent Marktanteil – eine krasse Diskrepanz zum ungebremsten Siegeszug des freien Betriebssystems auf Servern und Mobilgeräten. Sicher liegt es nicht an mangelnder Auswahl: Bei Linux und dessen Distributionen geht es, von spezialisierten Plattformen wie Android abgesehen, um die freie Auswahl freier Software und dementsprechend vielfältig ist das Angebot. Nicht nur Einsteiger stehen vor Qual der Wahl. Denn es gibt eine überwältigende XXL-Vielfalt an Distributionen und Desktopumgebungen. Nicht jeder Desktop passt in jedes Umfeld, zu jedem Wissensstand und zu allen Geschmäckern. Nutzerzahlen von Linux-Desktops zu quantifizieren, ist beinahe unmöglich.

Die DVD als Wegweiser

Fragt man nur ein Dutzend gestandene Linux-Anwenderinnen und -Anwender, so bekommt man ein Vielfaches dieser Zahl an Meinungen, Einwürfen und Empfehlungen zurück. Und eine Menge Kraftausdrücke, obskure Geek-Weisheiten und mit religiösem Eifer verfochtene Überzeugungen zu Usability, APIs und Desktopdesign. Deshalb bleibt der Linux-Desktop auch im Jahr 2018 eine sehr breit aufgestelltes Feld. Es gibt nicht „den“ perfekten Linux-Desktop – genauso wenig, wie plötzlich ein herausragendes Werk der Weltliteratur auf Wikipedia entstehen könnte. Was es gibt, sind glänzende Ideen, geniale Tüftler und individuelle Beiträge von Genies, die vielleicht genau die Lösung parat haben, die Sie oder Ihr Team gerade für ein Projekt braucht. Klar wäre es für die Situation und Chancen für Linux auf dem Desktop besser, wenn alle Hände an einem Strang zögen und eine Art Standardoptik à la Microsoft Windows entwickelten, die unsichere Anwender vor vollendete Tatsachen stellt und diese zudem als das Nonplusultra ausgibt. Aber so funktioniert Open Source nicht. Die Heft-DVD dieses Sonderhefts hat deshalb die Aufgabe, populäre Linux-Desktops sowie handverlesene Linux-Distributionen und damit dieses XXL-Betriebssystem von seiner besten Seite zu präsentieren.

Gut dokumentiert: Handbücher auf DVD

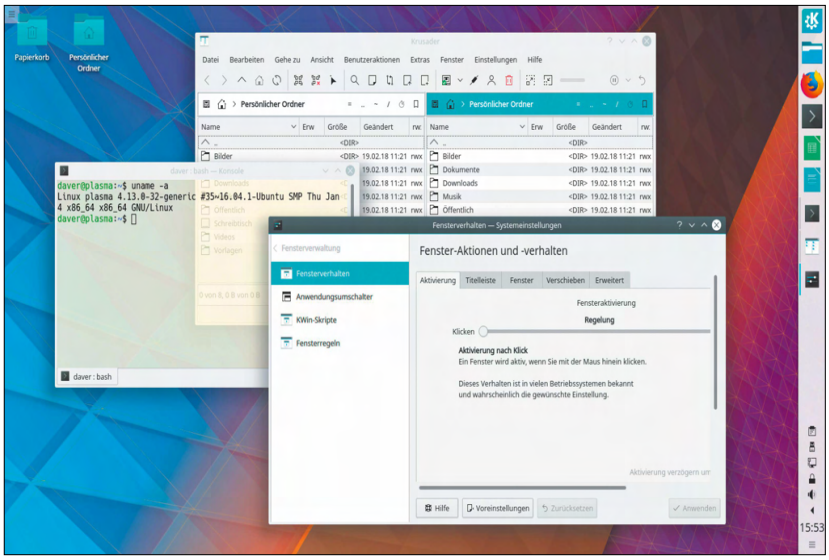
Freie Software umfasst nicht einfach nur Programme mit freizügig lizenziertem Quellcode, sondern auch eine unüberschaubare Menge an Dokumentation und Wissen in Form freier Handbücher, Nachschlagewerke und Anleitungen. Für diese Ausgabe haben wir 33 interessante Handbücher sowie Grundlagenwerke zu Linux und Open Source gesammelt und auf DVD untergebracht. Dieses Bücherregal liegt auf der DVD im Unterverzeichnis „Bibliothek“ und deckt recht unterschiedliche Bereiche von Linux-Desktops, Distributionen, Serveradministration und Softwareentwicklung ab.

Es ist also für jeden Wissensstand und für jedes populäre Anwendungsgebiet etwas dabei. Das Bücherregal auf DVD soll zum Stöbern einladen und ist zu umfangreich, um alles systematisch durchzugehen. Dazu sind die Themen auch zu unterschiedlich.

KDE Neon User Edition

Hier dreht sich alles um KDE Plasma 5, seit Jahren eine der populärsten Desktopumgebungen für Linux: Mit der KDE Neon User Edition (64-Bit-Version auf Heft-DVD) bekommt dieser Desktop ein neues Vorzeigesystem der KDE-Entwickler selbst.

Von **David Wolski**



Ein Aushängeschild für KDE Plasma: Die KDE Neon User Edition will ein stets aktuelles, aber stabiles KDE liefern, verlässt sich bei den Grundlagen aber auf Ubuntu.

Drei Kräfte haben sich für dieses laufend aktualisierte System zusammengetan: Jonathan Riddell als ehemaliger Kopf hinter Kubuntu, die KDE-Entwickler und deren Sponsoren. Diese prominente Aufstellung hat dafür gesorgt, dass KDE Neon nach einigen Startschwierigkeiten neben Open Suse und Kubuntu das wichtigste Vorzeigesystem für diese Desktopumgebung geworden ist. Als diese Distribution, die Ubuntu 16.04 als Betriebssystem-Basis nutzt, vor zwei Jahren mit einer großen Ankündigung zur Open-Source-Konferenz FOSDEM in Brüssel an den Start ging, waren KDE-Anwender und Entwickler anderer Linux-Desktopsysteme skeptisch: Noch eine KDE-Distribution, noch dazu eine auf der Basis Ubuntus? Die Befürchtungen: Eine eigene Distribution des KDE-Teams wird dem schon länger bestehenden Kubuntu schaden und dazu noch eine ineffiziente Verdoppelung gleicher Arbeiten bedeuten.

Neue Kadenz für KDE

Das aktuelle KDE Plasma 5.x entwickelt sich immer noch sehr schnell weiter. Die üblichen Linux-Distributionen, die in ihrem eigenen Rhythmus erscheinen, können dabei oft nicht Schritt halten. In so einer Umgebung ist es besser, mit möglichst frischen KDE-Paketen zu arbeiten. Eine Distribution wie Kubuntu oder Open Suse Leap kann hier aber nicht Schritt halten. Ein stets aktuelles Arch Linux und dessen Abkömmlinge wie Manjaro oder Netrunner sind dagegen oft zu experimentell und können zwischenzeitlich keinen stabilen Desktop für die tägliche Arbeit bieten. Diese Lücke soll nun KDE Neon füllen, denn die vorliegende User Edition hat KDE-Pakete an Bord, die zwar frisch, aber bereits getestet sind. So ist in der vorliegenden Ausgabe der KDE Neon User Edition KDE Plasma 5.12 enthalten. Unter anderem lässt sich hier KDE nach der Installation einiger Zusatzpakete auch schon unter Wayland ausprobieren.

Ubuntu darunter

Trotz dem Zerwürfnis zwischen einigen ehemaligen Kubuntu-Köpfen und der Ubuntu-Gemeinde samt Canonical ist KDE Neon kein Abschied von Ubuntu. Denn als Grundlage dient auch hier noch Ubuntu 16.04 LTS, von dem Kernel, wichtige Betriebssystemkomponenten und einige Anwendungen außerhalb des KDE-Umfelds stammen. KDE Neon wird auch in der User Edition teilweise als Rolling Release gepflegt. Das heißt, KDE-Komponenten bekommen laufende Updates, während der Ubuntu-Kern bei den erprobten Programmversionen der letzten LTS-Ausgabe bleibt.

Der Installer ist eine KDE-Version von Ubiquity, die auch im offiziellen Kubuntu die Einrichtung auf Festplatte übernimmt. Das Livesystem (in 64 Bit auf Heft-DVD) enthält deutsche Sprachpakete und bietet die gesamte Oberfläche auch in Deutsch an. Die Hardwareanforderungen fallen nicht anders als bei Kubuntu oder Open Suse aus: Eine 64-Bit-CPU und zwei GB RAM sollten es sein – besser mehr, denn KDE hat einen recht großen Speicherhunger.

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

Ubuntu Mate 18.04-daily

Mate ist nicht nur ein aufputschendes Heißgetränk aus den Anden, sondern auch der englische Begriff für einen guten Freund. Freundlich und aufgeputscht zeigt sich Ubuntu Mate 18.04-daily (in 64 Bit auf Heft-DVD) mit interessanten Neuerungen.

Von **David Wolski**



Sehr zuvorkommend: Der Willkommensbildschirm von Ubuntu Mate zeigt keine faden Infos, sondern führt gleich zur ersten Programmauswahl über die „Software Boutique".

Der heimliche Star unter den offiziellen Ubuntu-Ausgaben ist das besonders einsteigerfreundliche Ubuntu Mate. Es bringt Tugenden früherer Ubuntu-Versionen vor Unity 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 soweit entwickelt, dass sich jetzt ab Mate 1.20 auch die neuen Gnome-Anwendungen mit den Toolkits GTK3 (Gnome) und Qt5 (KDE) gut in den Desktop einfügen. Neu ist außerdem eine automatische Erkennung von Hi-DPI-Bildschirmen, auf welchen Mate jetzt automatisch seine Menüelemente hochskaliert.

Unity lässt grüßen

Nach dem ersten Start nach der Einrichtung mit dem gewohnten Ubuntu-Installer begrüßt den Anwender der aufgeräumte Mate-Desktop und der Willkommensbildschirm dieser Distribution, der über die „Software Boutique" gleich dabei hilft, populäre Programmpakete mit wenigen Klicks einzurichten. Wer in die Systemeinstellungen geht, findet bald neue Funktionen: 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. Neu sind in dieser Einstellung ein globales Menü in der oberen Leiste und ein „Head-up-Display" (HUD), das über die Alt-Taste aktiviert wird. Diese Funktion erlaubt die Suche nach Menüpunkten in der laufenden Anwendung per Tastatureingaben, so wie dies in Unity möglich war.

Nicht einfach eine Vorabversion

In kleineren Schritten ist der Mate-Desktop damit zu einer Arbeitsumgebung geworden, die sich gut anpassen lässt und sowohl Einsteiger als auch langjährige Linux-Anwender bedient. Ubuntu Mate bringt eine Softwareausstattung, die für den Gnome-Desktop typisch ist, mit Firefox 59, Libre Office 6.0.2, Thunderbird 52 inklusive der Kalenderanwendung Lightning, als Musikplayer Rhythmbox 3.4.2 und für Videos VLC 3.0.1. Viele ehemalige Gnome-Programme wie Texteditor, PDF-Betrachter und Dateimanager sind ebenfalls in ihrer Mate-Abspaltung vorhanden. Als grafische Paketverwaltung dient nun die „Software Boutique" im Menü „System -> Systemverwaltung". Hier können auch die traditionelleren Paketverwaltungen Synaptic und das Gnome Software Center nachinstalliert werden. Ubuntu Mate hat bereits einige Snap-Pakete vorinstalliert. Dabei handelt es sich um die Terminalanwendung „pulsemixer", die eine Lautstärkeregelung für Pulse Audio anzeigt, die einfache Paketverwaltung „Software Boutique" und die Begrüßungsanwendung. Bei Ubuntu Mate 18.04-daily handelt es sich um eine Vorabversion dieser Distribution vom 22. März 2018. Dieses bootfähige, installierbare Livesystem wird aber die Final installieren.

Nach der Installation ist dazu nur eine Systemaktualisierung über den Aktualisierungsmanager nötig beziehungsweise ein Update mit apt in der Kommandozeile. Ein Vorteil der modernisierten, aber weiterhin schlanken Desktopumgebung: Mit Ubuntu Mate 18.04 fühlt sich auch ein schwächerer PC der letzten zehn Jahre noch schnell genug zum Arbeiten an.

Website: *https://ubuntu-mate.org*
Dokumentation:
https://ubuntu-mate.org/about

LinuxWelt-Rettungs-DVD

Reparieren, testen, sichern, wiederherstellen: Die wichtigsten Linux-Tools zur Datenrettung, aber auch für Komplettbackups und zur Bearbeitung von Partitionen versammelt die LinuxWelt-Rettungs-DVD 6.2.1 aus eigener Entwicklung der Redaktion.

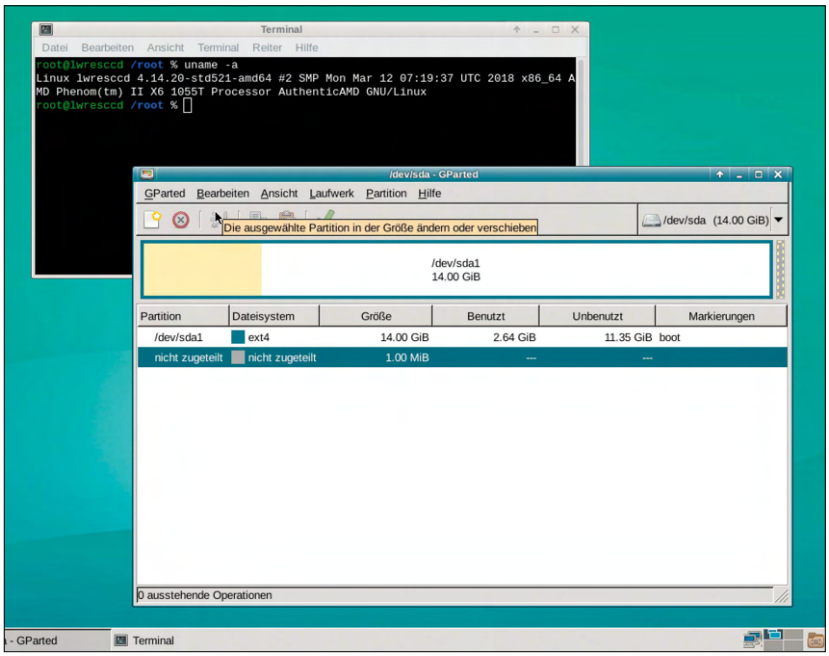
Von **David Wolski**

Es ist immer nützlich, einen gut sortierten Werkzeugkasten für Notfälle parat zu haben. Was genau in einen Werkzeugkasten für Linux-Systeme gehört, darüber haben erfahrene Linux-Aficionados und Betriebssystembastler unterschiedliche Vorstellungen. Es gibt aber jene unverzichtbaren Tools, die immer dabei sein sollten und im Mittelpunkt der LinuxWelt-Rettungs-DVD stehen.

Das Livesystem begann als persönliche Werkzeugsammlung von LinuxWelt-Redakteur Thorsten Eggeling zur Datenrettung, Partitionierung und für Komplettbackups. Als Grundlage dient die System Rescue CD – ein Livesystem, das vor allem wegen des enthaltenen Partitionierers Gparted auch schon öfter auf Heft-DVDs der LinuxWelt vertreten war. Die LinuxWelt-Rettungs-DVD ist um einige wichtige Programme erweitert und zudem weitgehend deutschsprachig. Für Rechner ohne DVD-Laufwerk liegt das Livesystem zur Übertragung auf USB-Stick auch als ISO-Datei auf Heft-DVD. Wie bei anderen Distributionen und Livesystemen dient unter Linux der Befehl dd dazu, die Datei auf einen USB-Stick zu schreiben.

Programme im Überblick

Nach dem Start des Systems, das in 32 und 64 Bit auf Heft-DVD vorliegt, präsentiert sich die schlichte, aber recht komfortable Oberfläche mit einer geöffneten Eingabeaufforderung. Der angemeldete Benutzer ist bereits root. In der unteren Leiste gibt es Links zu den häufig benötigten Programmen wie



Gut gefüllter Werkzeugkasten: Die LinuxWelt-Rettungs-DVD ist eine modifizierte Ausgabe der System Rescue CD, weitgehend deutschsprachig und um viele Tools ergänzt.

Firefox, dem Dateimanager, Terminalfenster, Texteditor und dem Partitionierer Gparted. Der Partitionierer liegt in der aktualisierten Version 0.30 vor und eignet sich vortrefflich zur Änderung des Partitionsschemas von bestehenden Partitionen ohne Datenverlust sowie zur neuen Aufteilung und Formatierung von Datenträgern.

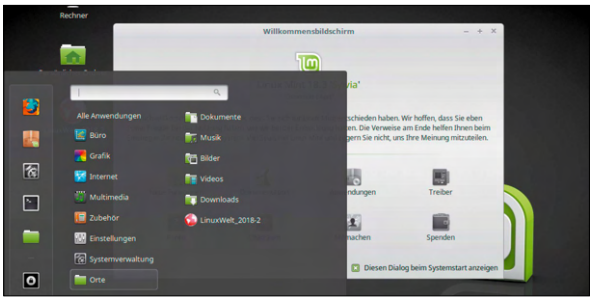
Im Anwendungsmenü findet sich unter „System -> Clonezilla“ das bewährte Backuptool. Clonezilla kann ganze Datenträger oder auch nur einzelne Partitionen sichern, auf andere Laufwerke übertragen und Abbilder in komprimierte Imagedateien schreiben. Das Backupmedium kann eine lokale Festplatte sein, ein externes USB-Laufwerk oder sogar eine Netzwerkfreigabe. Clonezilla spricht mit Windows-freigaben, mit SSH-Servern und sogar mit NFS-Freigaben.

Tools zur Datenrettung

Zwei wichtige Tools zur Datenrettung sind Photorec und Testdisk: Ersteres eignet sich zum Wiederherstellen gelöschter Dateien und läuft im Terminal, wo es mit dem Aufruf *photorec* gestartet wird. Das verwandte Programm testdisk kümmert sich um gelöschte Partitionen. Beide Tools nehmen dazu eine Datenträgeranalyse vor, die eine Weile dauern kann, aber viele verloren geglaubte Dateien wiederherstellt.

Website: *http://www.sysresccd.org*
Dokumentation: *http://www.sysresccd.org/Online-Manual-DE*

Linux Mint 18.3 Cinnamon

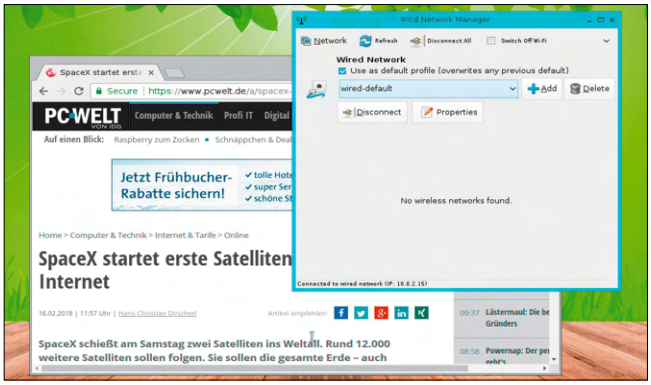


Das Aroma frische Minze: Die neue Version des populären Desktop-Linux-Systems basiert auf Ubuntu 16.04.3 und bringt den Betriebssystemunterbau mit dem neuen Kernel 4.10 auf den Stand des letzten Ubuntus mit Langzeitsupport. Mint (64-Bit-Ausgabe auf Heft-DVD) bleibt nun stets bei den LTS-Versionen von Ubuntu mit Langzeitsupport. Zwischenversionen wie Ubuntu 17.04/17.10 lässt Linux Mint aus, damit im Entwicklungsprozess mehr Zeit für die eigenen Ergänzungen bleibt. Und diese umfassen nicht nur kleine Projekte wie die einzelnen Mint-Tools, sondern die Desktopoberfläche Cinnamon.

Das hier verwendete Cinnamon hat ein Update auf 3.6.6 bekommen, das einen Monat vor Mint erschien. Eine der wichtigsten Neuerungen ist ein neuer Softwaremanager zur bequemen Installation populärer Programmpakete. Anders als Ubuntu, von dem die Distribution abstammt, gibt Linux Mint dem App-Containerformat „Flatpak“ der Gnome-Foundation den Vorzug. Flatpaks tauchen auch im neuen Softwaremanager auf. Im Abschnitt „Details“ ist angegeben, ob es sich beim ausgewählten Programmpaket um einen Flatpak-Container handelt, der seine eigenen Systembibliotheken mitbringt, um Konflikte zu vermeiden. Das hat den Vorteil, dass Linux Mint 18.3 nun jetzt auch neuere Gnome-Programme installieren kann, die mit den älteren Bibliotheken des Cinnamon-Desktops nicht kompatibel wären. Der Cinnamon-Desktop 3.6.6 kann sich nun, wie Gnome, mit Cloudkonten verbinden und bindet dazu auf Wunsch die Dienste von Google, Owncloud, Microsoft, Facebook und anderen ein.

Website: *https://linuxmint.com*
Dokumentation: *https://linuxmint.com/rel_sylvia.php*

Slax 9.3

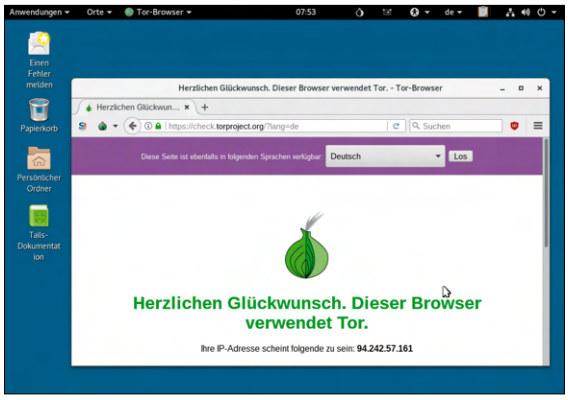


Ein ansehnliches Minisystem zum Surfen mit dem Browser Chromium bringt das schlanke und flotte Livesystem Slax auf den Desktop. Es fühlt sich auch auf richtig alten Rechnern noch wohl und bootet deshalb in seiner 32-Bit-Ausgabe von Heft-DVD. Anders als seine Vorgängerversionen basiert Slax jetzt auf Debian GNU/Linux und nicht mehr auf dem viel exotischeren Slackware. Das erlaubt dem Entwickler, wieder häufiger neue Slax-Ausgaben zu bauen. Von Debian stammen außerdem das Init-System Systemd und der Paketmanager apt in der Kommandozeile. Von DVD bootet das Livesystem blitzschnell und zeigt eine schlichte, ansprechende, englischsprachige Oberfläche. Zunächst ist auch noch das US-Tastaturlayout aktiv, was ein Rechtsklick auf den Desktop und „Keyboard Layout -> German“ ändert.

Ein Klick auf das Starter-Symbol rechts unten blendet die verfügbaren Programme ein, inklusive dem neu hinzugefügten „Net Manager“. Dabei handelt es sich nicht um den üblichen Network Manager von Gnome, sondern um das Python-Programm Wicd. Es erlaubt eine genauere Kontrolle über die verfügbaren Netzwerkschnittstellen, aber auch mehrere Schritte: Für das gewünschte WLAN müssen in den Verbindungsinformationen noch die verwendete Verschlüsselung, WPA2 in den meisten Fällen, sowie das Passwort eingetragen werden. Außerdem gibt es einen grafischen Dateimanager, ein Terminal, Browser Chromium 63, Texteditor und Taschenrechner. Weitere Softwarepakete gibt es zum Nachinstallieren über eine Internetverbindung mittels apt-get im Terminal.

Website: *http://www.slax.org*
Dokumentation: *http://www.slax.org/de/documentation.php*

Tails 3.6.1

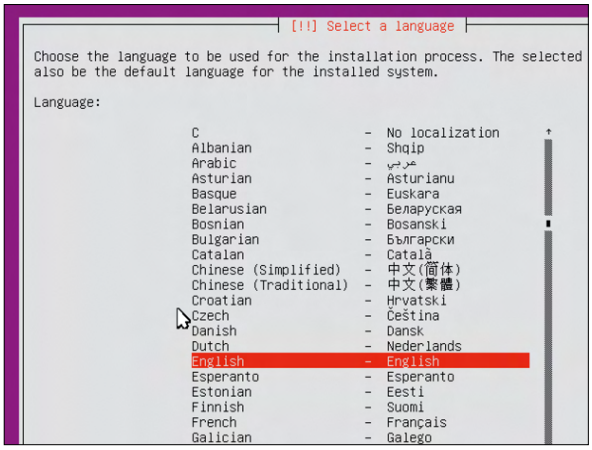


Bei diesem Livesystem geht es um eine gewisse Anonymität im Web: Der Name „Tails“ ist eine Abkürzung und steht für „The Amnesic Incognito Live System“. Dies ist ein Livesystem mit einem fertig eingerichteten TOR-Client, der ohne weitere Konfiguration sofort einsatzbereit ist. Die Verbindung zum TOR-Netzwerk, das Anonymität über eine Verkettung von mehreren vergesslichen Proxyservern erreicht, steht nach dem Start des Desktops nach einigen Momenten automatisch. Diesen können Sie auf dem vorgeschalteten Willkommensbildschirm gleich nach Deutsch umschalten. Der Desktop ist ein Gnome 3 im Classic Mode mit Taskleiste. Als Browser ist eine Variante von Firefox 52.7.2 (TOR-Browser) vorhanden, außerdem gibt es den Instant Messenger Pidgin 2.12 und für E-Mail das Programm Thunderbird 52. Weitere Anwendungen wie Libre Office 5.2.7, Gimp 2.8.18, PDF-Betrachter und der Audioplayer Audacious runden das Livesystem ab, das aus den Quellen von Debian 9 „Stretch“ aufgebaut ist. Damit läuft Tails dank dem Kernel 4.15 auch auf neueren Chipgenerationen von Intel und AMD. Wichtige Patches gegen die CPU-Sicherheitslücken „Meltdown“ und „Spectre“ sind ebenfalls vorhanden. Das Livesystem erkennt dank mitgelieferter Firmware verbreitete WLAN-Chips auf Anhieb.

Für den unkomplizierten Aufbau einer Netzwerkverbindung in WLAN und Ethernet ist der Network Manager von Gnome mitgeliefert. Es gibt einen englischsprachigen Installer im Anwendungsmenü unter „Tails“ , der das Livesystem über den Punkt „Install by cloning“ auf einem USB-Stick einrichtet.

Website: *https://tails.boum.org*
Dokumentation: *https://tails.boum.org/about/index.de.html*

Ubuntu Server



Ubuntu ist auch in den minimalen Installationsmedien für Server wieder in der brandneuen Version 18.04 LTS erschienen. Diese aufgefrischten ISO-Dateien installieren das brandneue Ubuntu mit fünf Jahren Langzeitsupport. Ubuntu 18.04 LTS wird von Anfang an sicher gegen die CPU-Sicherheitslücken „Meltdown“ und „Spectre“ sein. Dafür sorgt unter anderem der Kernel 4.15, der im Laufe des Supportzeitraums schrittweise mit Point Releases aktualisiert wird. Ausnahmsweise sind diese Installationsmedien von Ubuntu kein Livesystem, sondern die Serverausgabe von Ubuntu mit textbasiertem Installer. Serversysteme brauchen meist keinen grafischen Desktop und konsequenterweise verzichtet diese offiziellen Ubuntu-Installationart darauf. Stattdessen gibt es nach dem Start von der Heft-DVD in 64 Bit oder 32 Bit ein Installationsprogramm im Stil von Debian. Es gibt sogar einen textbasierten Partitionierer, der die Funktionen des grafischen Installationsprogramms von Ubuntu 18.04 abbildet. Eine Paketauswahl nach Gruppen erlaubt die individuelle Zusammenstellung des Ubuntu-Systems. Wer möchte, kann auch bereits zusammengestellte Paketgruppen für bestimmte Serveraufgaben installieren, um beispielsweise in wenigen Schritten einen kompletten LAMP-Stack (Linux, Apache, My SQL, PHP) aufzusetzen. Man kann hier aber auch ein grafisches System mit den üblichen Ubuntu-Desktops über auswählbare Paketgruppen einrichten. Da alle Pakete bei der Installation heruntergeladen werden, ist eine flotte Internetverbindung über Ethernet Pflicht.

Website: *http://ubuntu.com*
Dokumentation: *https://wiki.ubuntuusers.de/Server_Installation/*

Auf DVD: Handbücher zu Linux und Open Source

Freie Software bringt nicht nur Programme mit freizügig lizenziertem Quellcode, sondern auch eine enorme Menge an Dokumentation und Wissen in Form freier Handbücher. Nicht weniger als 33 wichtiger Handbücher finden sich auf Heft-DVD.



Von **David Wolski**

Für Einsteiger in das Thema Linux galt es bis vor einigen Jahren hohe Hürden zu nehmen, um ein System einzurichten, zu nutzen und zu administrieren. Open-Source-Entwicklung folgt keinem strengen Kanon von Entwicklung, Freigabe und Dokumentation. Gerade der Mangel an Dokumentation schreckte stets viele Linux-Einsteiger ab. Inzwischen gibt es jedoch eine große Zahl von Handbüchern zum Thema Linux und Linux-Software. Eine spannende Auswahl finden Sie auf der Heft-DVD.

Zahlreiche Handbücher auf DVD

Ausgereifte Linux-Distributionen mit schicken Oberflächen und ein Schatz an sorgfältig erstellter Dokumentation beseitigen alte Berührungsängste. Denn freie Software umfasst nicht einfach nur Programme mit freizügig lizenziertem Quellcode, sondern auch eine unüberschaubare Menge an Dokumentation und Wissen in Form freier Handbücher, Nachschlagewerke und Anleitungen. Für diese Ausgabe haben wir 33 interessante Handbücher sowie Grundlagenwerke zu Linux und Open Source gesammelt und auf DVD untergebracht. Dieses Bücherregal liegt auf der DVD im Unterverzeichnis „PDFs“ und deckt recht unterschiedliche Bereiche von Linux-Desktops, Distributionen, Serveradministration und Softwareentwicklung ab. Es ist also für jeden Wissensstand und für jedes Anwendungsgebiet etwas dabei.

Das Bücherregal auf DVD soll zum Stöbern einladen und ist zu umfangreich, um alles systematisch durchzugehen. Dazu sind die Themen auch zu unterschiedlich. Lesen Sie dort rein, wo Ihre aktuellen Interessen liegen, und heben Sie den Rest für später auf.

Zwar decken diese Nachschlagewerke nicht alle Funktionen aktueller Softwareversionen oder Distributionen ab. Bei Handbüchern zur Serveradministration, zu Scripting und der Befehlszeile Bash geht es sowieso um zeitloses Wissen, das über Jahre aktuell bleibt. Etwa die Hälfte der PDFs ist deutschsprachig, die andere Hälfte ist englischsprachig. Viele fundamentale Aktionen finden jedoch unter Linux im Terminal statt und die Terminalbeispiele sprechen meistens für sich und haben selbst dann ihren Wert, wenn Ihnen die Übersetzung der englischsprachigen Kommentierung zu mühsam ist. Das gilt auch für die Programmierhandbücher zu Python und Perl.

Einsteiger und Fortgeschrittene

Eher leicht verdauliche Infos für Anwender bieten die Einsteigerbücher zu Ubuntu, Linux und Open Suse. Hier geht es um solide deskriptive Beschreibungen zu Installation, Einrichtung und Softwarenutzung aus erster Hand. Das Distributionshandbuch zu Ubuntu geht auch detailliert auf die vorinstallierte Standardsoftware ein und ist somit auch ein Einsteigerleitfaden für Firefox, Thunderbird, Rhythmbox & Co. Die PDFs zu den verschiedenen Mint-Ausgaben fokussieren klarer auf System und jeweilige Oberfläche. Ebenfalls klar den Desktopanwender im Auge haben die Anleitungen zu Open Office und Gimp, während die Suse-Bücher in verschiedene Richtung zielen: Die Titel zu Gnome und seinen

Standardprogrammen, ferner zum Schnelleinstieg, eventuell auch noch der „Tuning Guide“ sind anwenderorientiert, während sich die weiteren Suse-Bücher an Administratoren und Deploymentprofis richten.

In einigen PDFs wie „Linux für Fortgeschrittene“ geht es vor allem um die Verwaltung des Systems im Terminal und über Shell-Scripts. Das „Debian Administrationshandbuch“ geht ebenfalls ins Detail und gilt größtenteils auch für Ubuntu, Mint und viele weitere Linux-Distributionen. Mit „Building Skills in Python“ und „Essential Perl“ gibt es zwei englischsprachige Programmierhandbücher. Das erstere ist ein umfassendes Nachschlagewerk, das zweite ein knapper, komprimierter Abriss mit vielen Codebeispielen, der sich auch für Perl-Einsteiger eignet.

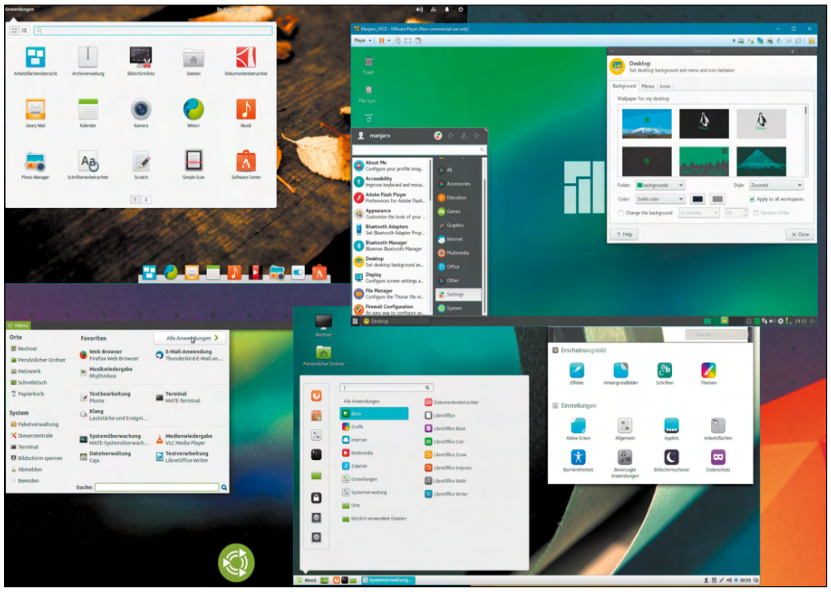
Praktisch alle allgemeineren Bücher beschäftigen sich mal mehr, mal weniger ausführlich auch mit der Kommando-Shell. Da es bei ernsterer Benutzung von Linux ohne Terminal nun mal nicht geht, ist zumindest der interaktive Einsatz der Shell auch für Desktopanwender relevant. Hierzu gibt es gleich drei spezielle PDFs unterschiedlicher Tiefe: Ein umfassender Titel ist „The Linux Command Line“. Ebenfalls ausführlich ist das „Bash Reference Manual“, während „Linux Shell for Beginners“ nur die allerwichtigsten Grundlagen erläutert.

Übersicht: Linux-Handbücher auf DVD

Titel	PDF-Datei	Sprache	Seiten
Bash Reference Manual	bash.pdf	englisch	172
Building Skills in Python	BuildingSkillsinPython.pdf	englisch	564
Debian-Administrationshandbuch	debian-handbook.pdf	englisch	509
Essential Perl	EssentialPerl.pdf	englisch	25
Getting Started with Ubuntu 16.04	Getting%20Started%20with%20Ubuntu%2016.04.pdf	englisch	139
Gimp Kurzreferenz	gimp-keys-de.pdf	deutsch	1
Introduction to the Linux Command Shell	ShellIntro.pdf	englisch	13
Lawrence Lessig: Freie Kultur	OSP_lessig_freiekultur.pdf	deutsch	297
Einführung Libre Office	01ES_01LibreOfficeEinfuehrung_V35.pdf	deutsch	27
Linux Administration II	Linux_adm2-de-manual.pdf	deutsch	233
Linux für Fortgeschrittene	Linux_grd2-de-manual.pdf	deutsch	230
Linux Mint 18.1 Cinnamon	Mint_18.1_Cinnamon.pdf	deutsch	44
Linux Mint 18.1 Mate	Mint_18.1_Mate.pdf	deutsch	48
Linux Mint 18.0 XFCE	Mint_XFCE_german_18.0.pdf	deutsch	47
Linux Newbie Administrator Guide	LinuxNewbieAdministratorGuide.pdf	englisch	45
Linux Scripting Tutorial	Linux_Shell_Scripting_Tutorial_2.pdf	englisch	301
Linux-Administration I	Linux_adm1-de-manual.pdf	deutsch	258
Linux-Grundlagen	Linux_Grundlagen_de-manual.pdf	deutsch	211
Linux-Infrastrukturdienste	Linux_infs-de-manual.pdf	deutsch	160
Linux-Netzadministration	Linux_nadm-de-manual.pdf	deutsch	169
Pro Git	progit.pdf	englisch	514
Producing Open Source Software	producingoss.pdf	englisch	198
Snort, Acid & Co.	OSP_heinlein-bechtold_snort.pdf	deutsch	258
Suse Linux: Administrationshandbuch	suse_book_sle_admin.pdf	deutsch	472
Suse Linux: Deployment	suse_book_sle_deployment.pdf	deutsch	288
Suse Linux: Gnome-Benutzerhandbuch	suse_book_gnomeuser.pdf	deutsch	218
Suse Linux: Schnelleinführung zur Installation	suse_book_quickstarts.pdf	deutsch	19
Suse Linux: Security-Guide	suse_book_security.pdf	englisch	351
Suse Linux: Tuning-Guide	suse_book_sle_tuning.pdf	englisch	215
The Linux Command Line	TLCL-17.10.pdf	englisch	537
Ubuntu Server Guide	Ubuntu_Serverguide.pdf	englisch	378
Unix Toolbox	unixtoolbox.book.pdf	englisch	30
Vim Recipes	vim-recipes.pdf	englisch	178

Linux-Distributionen: Eine Vorsortierung

Ubuntu, Debian, Mint? Knoppix, Tails, Parted Magic? KDE, Gnome, Cinnamon? Wer sich mit Linux beschäftigt, muss Dutzende von Namen verarbeiten und einordnen. Einige feste Claims helfen als Wegmarken.



Von **Hermann Apfelböck**

Alles, was auf dem Linux-Kernel aufbaut, heißt Linux (oder auch Android). Das sind dann etwa 300 für Endanwender offen verfügbare Distributionen und noch weitaus mehr Embedded-Linux/Android-Systems, die in elektronischen Geräten aller Art arbeiten. Angesichts einer aktuellen Kernel-Größe von etwa 90 MB wird sofort deutlich, dass das Verbindende aller Linux-Distributionen viel kleiner ausfällt als die Unterschiede. Es soll Aufgabe dieses Beitrags sein, diese Unterschiede zu erklären und zu begründen – so jedenfalls für die verfügbaren Endanwender-Systeme.

Für die Vielfalt der Linux-Varianten gibt es triftige und weniger triftige Gründe: Höchst verdienstvoll ist die breite und facettenreiche Linux-Unterstützung für unterschiedlichste Hardware vom protzigen Gaming-PC bis hinunter zu kleinen ARM-Platinenrechnern und scheinbar obsoleten Altgeräten. Höchst willkommen ist auch die großzügige Wahlfreiheit einer opulenten, avantgardistischen, klassischen, möglichst simplen oder auch puristischen Bedienoberfläche. Darüber hinaus wird es aber auch gerne geschmäcklerisch: Manche Distribution rechtfertigt sich durch Details oder Softwarepakete, die auch auf zehn anderen Distributionen vorhanden oder realisierbar sind.

Debian, Arch & Co: Hauptlinien

Angesichts von Hunderten lebender Distributionen, die auf dem Linux-Kernel basieren, scheint die Auswahl der neun Systeme im nachfolgenden und grundlegenden Radar-Check ab Seite 22 willkürlich und unzureichend. Tatsächlich gehen aber praktisch alle existierenden Distributionen auf diese Hauptstämme zurück und sind letztlich ein Debian/Ubuntu-, Arch-, Gentoo-, Slackware- oder Red-Hat-Linux.

Hier folgen einige grundlegende Überlegungen zur Einordnung. Auf die Gefahr hin zu pauschalisieren, sind die meisten Gentoo-, Slackware-, Red-Hat- und Arch-basierten Systeme nicht mehrheitsfähig, sondern Inseln für Linux-Kenner und für spezialisierte Einsatzgebiete. Jedoch gibt es auch hier Ausnahmen:

1. Red Hat: Hier lassen sich zwei Distributionen herausheben, die in erster Linie für technisch versiertere Anwender in Betracht kommen:

- **Fedora Linux** (*https://fedoraproject.org/de*) ist in fast jeder neuen Version ein Hingucker mit innovativen Funktionen. Aktuell ist die Fedora 27. Im Mai 2018 kommt Version 28 Standardoberfläche ist Gnome. Die Installation mit „Anaconda“ ist aber durchaus eine Hürde, die Linux-Erfahrung erfordert.
- **Cent-OS** (*http://centos.org*, aktuelle Version 7.4) ist ein freier Klon des



Arch Linux für den Desktop: Das als System für Kenner bekannte Arch findet durch leicht installierbare Derivate (Manjaro und Antergos) vermehrt den Weg zum normalen Anwender.

Serversystems Red Hat Enterprise mit dem außergewöhnlichen Supportzeitraum von zehn Jahren. Statt auf experimentelle Neuentwicklungen wie Fedora zielt Cent-OS ausschließlich auf Stabilität. Dies ist ideal für Server, aber auch für Linux-Desktops, die möglichst lange laufen sollen.

2. Slackware: Hier sind zwei sehr populäre Distributionen zu nennen:

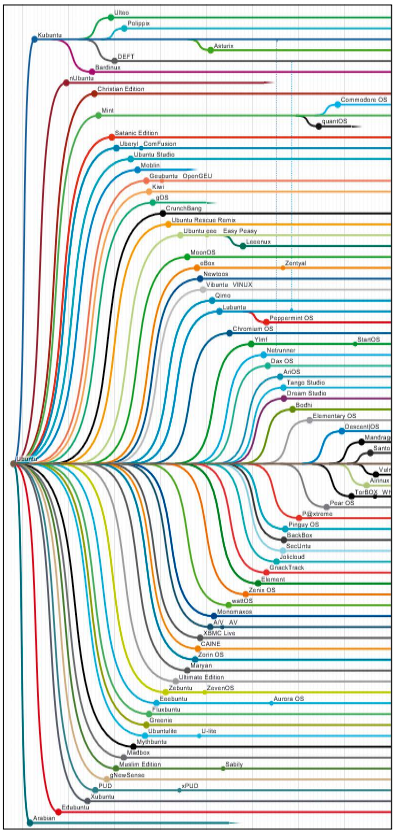
- **Open Suse Leap** (*www.opensuse.org/de*) liegt aktuell in Version 42.3 vor, ab Mail 2018 wird eine neue Version erwartet. Suse war mehr als ein Jahrzehnt fast das einzige Linux, das mit grafischer Bedienung und Konfigurierbarkeit auf den PC-Desktop zielte. Die grundsolide Distribution hat in den letzten Jahren in Konkurrenz zu Ubuntu-Familie an Bedeutung eingebüßt und tendiert neuerdings eher Richtung Innovation und Experimentierfreude, weniger Richtung Einsteigerfreundlichkeit. Die (noch) aktuelle Versionsnummer 42 bezieht sich auf die Zahl 42 aus dem Roman „Per Anhalter durch die Galaxis“.
- **Porteus** (*www.porteus.org*) ist als Livesystem konzipiert (keine Installation) und erste Wahl für ein mobiles, dabei überragend schnelles und anpassungsfähiges Surfsystem. Ein spezieller Kioskmodus eignet sich für unbeaufsichtigte öffentliche Geräte.

3. Arch Linux: Hier gibt es drei besonders populäre Distributionen:

- **Archbang** (*www.archbang.org*) ist ein Rolling Release ohne Versionsangabe, das sich über das Paketmanagement ständig aktuell hält. Das besonders schnelle und kleine System mit der puristischen Openbox-Oberfläche erfordert bei der Einrichtung gründliche Linux-Kenntnisse. Die laufenden Updates per Rolling Release können auch mal Probleme verursachen. Dann muss man sich selber zu helfen wissen.
- **Manjaro** (*http://manjaro.github.io*), in aktueller Version 17.1.5 ermöglicht durch den grafischen Installer und grafischen Paketmanager einen vereinfachten Zugang zu Arch Linux, wird dadurch aber nicht zum Einsteigersystem. Dasselbe gilt für den Arch-Ableger **Antergos** 17.10 mit den gleichen grafischen Werkzeugen.

4. Gentoo: Namhafte Gentoo-Distributionen sind:

- **Sabayon** (*www.sabayon.org*, aktuell 17.12) und das bewährte Notfallsystem
- **System Rescue CD** (*www.system-rescue-cd.org, aktuell 5.2.1*). Beide,



Quelle: Andreas Lundqvist, Donjan Rodic

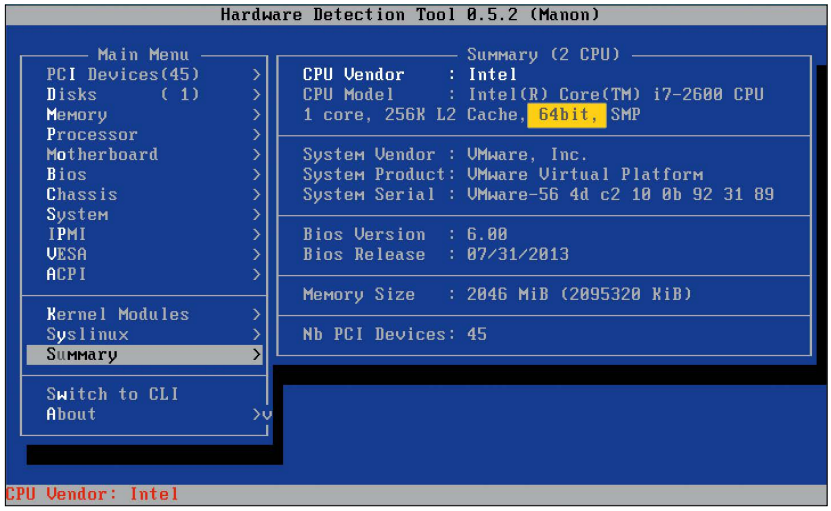
Viele Ubuntus: Dieses Bild kann nur die Mengen vermitteln. Um die Ubuntu-Derivate lesbar einzusehen, gehen Sie auf *https://de.wikipedia.org/wiki/Liste_von_Linux-Distributionen*.

das schnelle Desktopsystem Sabayon wie das Notfallsystem, richten sich an erfahrene Linux-Anwender, wobei Sabayon im Vergleich zum purem Gentoo immerhin einen grafischen Installationsassistenten und einen grafischen Paketmanager mitbringt.

Die Dominanz der Debian-Familie

Der Debian-Stammbaum zählt etwa 150 aktive Distributionen (u. a. Debian selbst sowie zahlreiche Ubuntu-Derivate inklusive Linux Mint). Damit hat Debian deutlich mehr Nachfolger als alle anderen Linux-Stämme zusammen:

- **Arch Linux:** circa elf aktive Distributionen (u. a. Manjaro, Archbang)
- **Gentoo-Linux:** circa 13 aktive Distributionen (u. a. Sabayon, System Rescue CD)
- **Slackware:** circa 45 aktive Distri-



Hardwareinfos mit HDT: Das Hardware Detection Tool liegt bootfähig auf der Heft-DVD und zeigt unter „Summary“ oder „Processor“ die Prozessorarchitektur (32 oder 64 Bit).

butionen (u. a. Open Suse, Porteus, Salix)

- **Red Hat:** circa 65 aktive Distributionen (u. a. Fedora, Red Hat Enterprise, Cent-OS)

Allein die annähernd 70 Ubuntu-Derivate summieren sich auf mehr Systeme, als jeder andere Linux-Hauptstamm aufweist. Hauptgründe für die Debian-Verbreitung sind Kompaktheit, Flexibilität und Stabilität (beim meist genutzten „Stable“-Zweig) und die zuverlässige Paketverwaltung mit enorm großer Auswahl an Software. Viele Derivate wie Linux Mint, Netrunner, Elementary OS, Bodhi Linux, Zorin-OS oder Bunsenlabs geben ihre Debian/Ubuntu-Abstammung im Namen nicht preis. Auch Knoppix, Raspbian für Raspberry Pi, Steam-OS für Spielerechner oder das NAS-System Open Media Vault – sie alle basieren auf Debian.

Den Anwender- und Desktopbereich dominieren komfortable Debian-Systeme wie Ubuntu, Mint oder Elementary OS eindeutig, lediglich Open Suse und Fedora haben hier noch einen (halben) Fuß in der Tür. Auch als Serversystem im Home- oder Home-Office-Bereich sind Debian selbst und seine Derivate Ubuntu Server und Open Media Vault führend, lediglich Cent-OS ist hier eine Nicht-Debian-Alternative. Unterm Strich sind Debian-Systeme für Einsteiger, aber auch für viele pragmatische Linux-Kenner erste Wahl.

Zur Debian/Ubuntu-Familie liefert dieses Heft eine ganze Reihe von genaueren Vorstellungen, u. a. zu Debian, Kubuntu, Linux Mint, Xubuntu, Lubuntu, Ubuntu Server, Elementary OS, Bunsenlabs und Ubuntu Server.

Einziger nennenswerter Nachteil von Debian, Ubuntu & Co. sind etwas angestaubte Softwarepakete: Wer stets frischeste Versionen von VLC, Libre Office et cetera möchte, ist am besten bei einem Arch-Linux aufgehoben.

Die Architektur: 32 oder 64 Bit?

Die meisten Linux-Distributionen bieten je eine Ausführung in 32- oder 64-Bit-Architektur an, manche aber auch nur noch ein 64-Bit-Variante. 32-Bit-Systeme benötigen generell weniger Arbeitsspeicher.

Für Geräte bis vier GB RAM empfehlen wir daher ein Linux in 32-Bit-Ausführung, ab vier GB hingegen ein 64-Bit-System. Zwar können 32-Bit-

Infoquellen zu Linux-Distributionen

Die deutschsprachige Wikipedia-Seite „Liste_Linux_Distributionen“ (*https://de.wikipedia.org/wiki/Liste_von_Linux-Distributionen*) leistet einen knappen Gesamtüberblick über die Derivate aller Linux-Hauptzweige. Neben hübsch visualisierten Stammbäumen zu Arch, Debian & Co., die allerdings nur bis 2013 reichen, gibt es eine Kurzcharakterisierung des Hauptstamms und einen zwei bis dreizeiligen Ministeckbrief zu den einzelnen Derivaten. Für eine praxisnahe, technische Entscheidungshilfe fallen diese Infos zu dünn aus und müssten dringend aktualisiert werden, aber für eine Erstorientierung oder eine historische Gesamtschau ist dieser Überblick genau richtig.

Die englischsprachige Wikipedia-Seite „Comparison_of_Linux_distributions“ (*https://en.wikipedia.org/wiki/Comparison_of_Linux_distributions*) zeigt auf sechs anspruchsvollen Tabellen fundierte Infos zu allen wichtigen Distributionen. Hier ist etwa die Existenz eines installierbaren Livesystems oder eines grafischen Installers, die allgemeine Ausrichtung, das Gründungsjahr, das Standard-Dateisystem, der Standarddesktop oder die Menge der Softwarepakete für jede Distribution schnell recherchierbar. Diese Tabellen sind mit die besten Entscheidungshilfen für eine strategische Distributionssuche, sofern ein kompetenter Leser die richtigen Kriterien anlegt. Einfach ist das Zusammenfassen relevanter Infos aus verschiedenen Tabellen allerdings nicht. Außerdem löst auch diese Seite das allgemeine Dilemma nicht konsequent, ab wann man technisch von einer selbständigen Distribution sprechen kann: Während Dutzende Ubuntu-Derivate unter „Ubuntu“ subsummiert sind, erscheinen dann etwa die Ubuntu-Derivate Linux Mint oder Bodhi Linux doch wieder als eigenständige Distribution.

Die Website Distrowatch (*https://distrowatch.com*) liefert seit mehr als 15 Jahren Infomaterial zu allen Linux-Distributionen. Neben Basisdaten über Herkunft und Ausrichtung gibt es immer eine knackig-knappe (wenn auch selten tiefschürfende) Systemcharakteri-

Systeme über eine CPU-Erweiterung (PAE) auch mehr als vier GB RAM nutzen, dies ist jedoch nicht empfehlenswert und führt zu Leistungseinbußen. Unumgänglich ist ein 32-Bit-System nur dort, wo noch ein sehr alter 32-Bit-Prozessor arbeitet.

Das ist bei allen Rechnern, die jünger als etwa 12 Jahre sind, sehr unwahrscheinlich. Lediglich auf einigen Netbook-Produktreihen trifft man noch bis 2010 auf 32-Bit-Prozessoren. Wenn Sie sich unsicher sind, kann Sie unabhängig vom Betriebssystem ein Tool der Heft-DVD informieren: Die DVD zeigt unter „Extras und Tools" das nützliche „Hardware Detection Tool", das umfassende Auskunft zu CPU und Speicher liefert.

Ein 64-Bit-System ist in zwei Fällen erforderlich – erstens, wenn das Zielgerät mehr als vier GB Speicher besitzt, der nur durch 64-Bit-Architektur nativ adressiert wird, zweitens, wenn eine Installation im Uefi-Modus geplant ist. Letzteres ist typischerweise dort notwendig, wo bereits ein Windows oder Linux im Uefi-Modus vorliegt und nun ein weiteres Linux im Dual- oder Multibootbetrieb parallel installiert werden soll. Nur 64-Bit-Systeme unterstützen den Uefi-Modus mit seinem neuen Partitionsschema. Weitere Informationen zu Multiboot im Uefi-Modus lesen Sie ab Seite 70.

Paketformate und Paketmanager

Linux-Systeme beziehen Software und Updates standardmäßig aus den Paketquellen des Distributionsherstellers. Das dafür genutzte Paketformat und der dafür vorgesehene Paketmanager unterscheiden sich zwischen den großen Linux-Familien Debian, Arch & Co. Daher bestimmt der erste Einstieg in Linux oft jahrelang die weitere Systemwahl. Für das Resultat einer installierten Software spielt es zwar eigentlich keine Rolle, welches Format zugrunde liegt, aber die Gewöhnung an ein Werkzeug baut doch Hürden gegenüber anderen: Wer einmal das Paketformat DEB (Debian, Ubuntu, Mint) und das hier zuständige Terminaltool Apt gewöhnt ist, erlebt die Umstellung auf RPM (Slackware, Red Hat), Tar.xz (Arch) oder Portage (Gentoo) als deutliche Hürde.

Das Paketmanagement unterscheidet sich nicht nur technisch hinsichtlich der Erkennung von Paketabhängigkeiten, sondern auch deutlich in der Bedienung. Als einsteigerfreundlich in dieser Hinsicht dürfen Debian/Ubuntu-basierte Systeme mit Apt und Open Suse mit Zypper gelten. Natürlich liefern Desktopdistributionen in aller Regel auch grafische Softwarezentralen mit, die eine Einarbeitung in die Syntax des Terminal-Paketmanagers für den Installationsalltag weitgehend überflüssig machen. Dennoch sind fundamentale Kenntnisse im Terminal oft nützlich für schnelle Systemupdates und für Notfälle.

Ranking der Seitenaufrufe

Zeitraum: Last 6 months [Los]

Rang	Distribution	HPD*
1	Mint	2897
2	Debian	1991
3	Manjaro	1855
4	Ubuntu	1529
5	openSUSE	1170
6	deepin	1028
7	Zorin	1019
8	Fedora	1011
9	Antergos	986
10	elementary	844
11	Solus	802
12	CentOS	795

Rangliste der Distributionen auf distrowatch.com: Einige Systeme verlassen niemals die Top 10 oder Top 20. Die Rangliste ist aber kein objektiver Gradmesser für die Verbreitung.

sierung, ferner weiterführende Links, einen Screenshot und einen Versionsvergleich mit genauen Paketlisten. Außerdem ist die Rangliste auf der Distrowatch-Startseite ein vielbeachtetes Bewertungssystem für die aktuelle Popularität der Distributionen, wenngleich sie über die tatsächliche Verbreitung nichts aussagt: Sie misst nur das Interesse der Distrowatch-Besucher an den dortigen Beschreibungen. Die Aussagekraft kann man daher mit Recht in Frage stellen, andererseits ist aber Fakt, dass es schlicht keine validere Quelle zur Beliebtheit einzelner Linux-Distributionen gibt. Die Verbreitung von Linux insgesamt ist besser analysierbar, weil Webserver das Betriebssystem des Besuchers identifizieren können.

Die Top 10, Top 20 oder auch Top 100 bei Distrowatch wechseln in ständigem Auf und Ab ihre Plätze, jedoch gibt es Platzhirsche, die seit Jahren konstant in der Top 10 residieren. Linux Mint ist als Tabellenführer wie festgenagelt, Ubuntu, Debian, Fedora und Open Suse verlassen die Top 10 nie. Bemerkenswert ist, dass sich mit Manjaro und Antergos seit Monaten zwei Ableger von Arch Linux oben etablieren, da Arch gemeinhin als System für Linux-Kenner gilt.

Es handelt sich bei den Spitzenreitern fast ausschließlich um Desktopsysteme für PCs und Notebooks. Auch dies ist ein warnendes Indiz, dass die Rangliste nicht die tatsächliche Verbreitung wiedergibt. Am Server spielen Linux-Systeme die führende Rolle, jedoch hat ein typischer Debian- oder Red-Hat-Admin kein Motiv, sich auf Distrowatch über Debian, Cent-OS oder Red Hat Enterprise zu informieren.

Unterm Strich ist Distrowatch eine hervorragende Quelle, um sich schnell über die generelle Ausrichtung und den aktuellen Trend einer bestimmten Distribution zu informieren. Auch Exoten und begrabene Projekte sind anzutreffen. Zur strategischen Suche ist die Seite weniger geeignet. Die Rangliste hat begrenzte Aussagekraft, ist aber bei extremen Ausschlägen (Absturz, Turboaufstieg) immerhin ein Indiz für den aktuellen Trend einer Distribution.

Distributionen im Check

Für Windows-Umsteiger ist es keine leichte Aufgabe, die passende Linux-Distribution für die anvisierte Aufgabe zu finden. Die folgende Übersicht klassifiziert wichtige tonangebende Systeme anhand ihrer Besonderheiten und Stärken.

Von **David Wolski**



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

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

Orientierungshilfe und Bewertung

Die Landkarte der Linux-Distributionen zeigt einige große bekannte Kontinente und unzählige kleinere Provinzen. Der folgende Distributions-Check nimmt sich die tonangebenden Systeme vor. Mancher Linux-Kenner mag hier sein eigenes Lieblingssystem vermissen, denn der Überblick erhebt keinen Anspruch auf Vollständigkeit. Umgekehrt sind einige Distributionen aufgeführt, die technisch keinen Platz als selbständiges Linux verdienten, aber einfach zu populär sind, um sie hier wegzulassen.

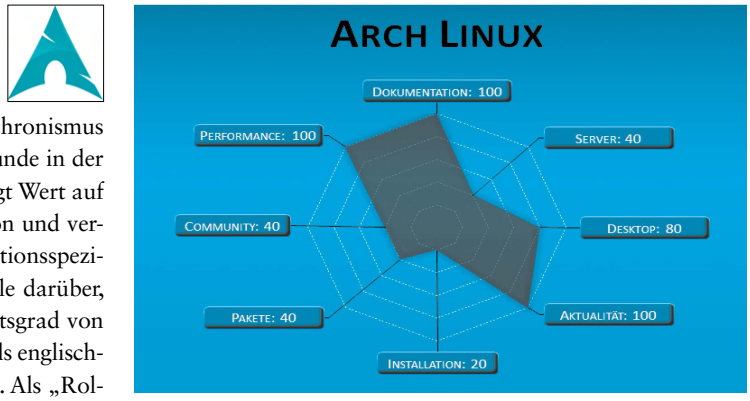
Die jeweiligen Stärken und Schwächen der Distributionen zeigt jeweils ein Radardiagramm mit den Bewertungskriterien, wie sie die Legende auf dieser Seite auflistet. Drei der acht Punkte verdienen eine kurze zusätzliche Kommentierung: „Performance“ gibt den Erfahrungswert wieder, wie schnell und leistungsfähig ein System in der Standardkonfiguration ist. Die Menge der „Pakete“ ist ein wichtiges Kriterium für Desktopnutzer, da Linux-Systeme Software immer aus den Paketquellen der Distribution beziehen. „Aktualität“ spielt nicht nur für neueste Softwareversionen eine Rolle, sondern auch für die genutzte Hardware. Denn nur ein aktueller Kernel liefert die Treiber für allerneueste Hardwareentwicklungen.

Ausschlaggebend ist in der Wertung der Zustand einer Distribution, wie sie sich im Jahr 2017 präsentiert hat. Da die hier ausgewählten Systeme aber keinen umfangreichen Änderungen im Quartalsrhythmus unterliegen, wird die Bewertung und Einschätzung einige Jahre Bestand haben.

Legende zu den Radargrafiken

Server	Servertauglichkeit (bei Ubuntu Unterscheidung LTS-Version)
Desktop	Desktoptauglichkeit (Einsatz auf PC und Notebook)
Installation	Komfort bei der Systemeinrichtung
Performance	Leistung als Server und Desktop
Pakete	Umfang der angebotenen Softwarepakete
Aktualität	Stand der Programmversionen in den Standard-Paketquellen
Dokumentation	Ausführlichkeit / Einsteigerfreundlichkeit der Dokumentation (dt./engl.)
Community	Unterstützung durch Wikis und Foren

Arch Linux

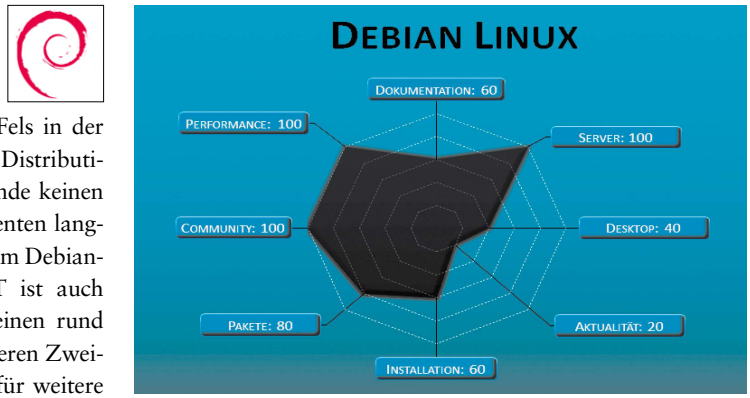


Obwohl Arch mit hohem Do-it-Yourself-Faktor, der schon bei der Installation beginnt, als Anachronismus erscheint, hat sich die Distribution enorm viele Freunde in der fortgeschrittenen Anwenderschaft gemacht: Arch legt Wert auf einen schlanken Aufbau und manuelle Konfiguration und versteckt die Innereien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

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

Offizielle Webseite: *www.archlinux.de*

Debian GNU/Linux

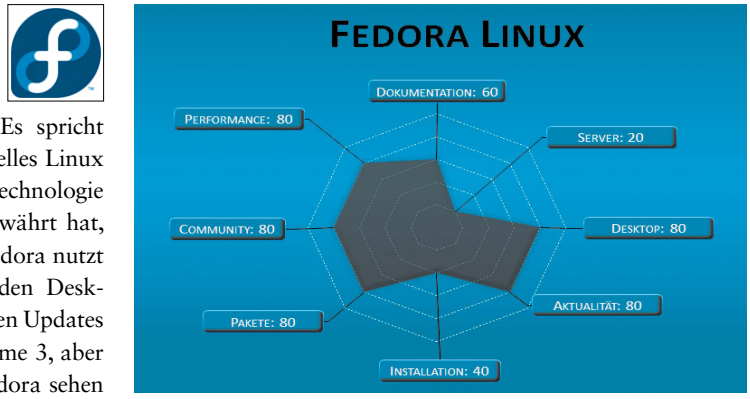


Das System für höchste Ansprüche an Stabilität ist in der turbulenten Linux-Entwicklung der Fels in der Brandung und mit 23 Jahren eine der dienstältesten Distributionen. Auf neueste Pakete legt die Entwicklergemeinde keinen Wert. Deswegen werden Programme und Komponenten langsamer aufgenommen als bei der Konkurrenz. Auf dem Debian-Paketformat DEB und der Paketverwaltung APT ist auch Ubuntu aufgebaut. Neue Debian-Ausgaben erscheinen rund alle zwei Jahre und die Entwicklung erfolgt in mehreren Zweigen: Debian Unstable bietet neueste Software, die für weitere Tests in Debian Testing aufgenommen wird, das wiederum die Vorstufe zu Debian Stable ist.

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

Offizielle Webseite: *www.debian.org*

Fedora



Das von Red Hat gesponserte Fedora ist ein Trendsetter mit topaktueller Programmauswahl. Es spricht ambitionierte Anwender an, die ein möglichst aktuelles Linux für den Desktop-Einsatz suchen. Wenn sich eine Technologie wie der neue Init-Daemon Systemd bei Fedora bewährt hat, wandert sie später zu Red Hat Enterprise Linux. Fedora nutzt das RPM-Paketformat und ist vornehmlich für den Desktopeinsatz geschaffen, da sich das System mit häufigen Updates oft ändert. Die typische Desktopumgebung ist Gnome 3, aber auch Mate, LXDE und KDE können sich unter Fedora sehen lassen. Die Installation erfolgt über Livesysteme oder mit der universellen DVD-Ausgabe. Der Installer ist eher umständlich.

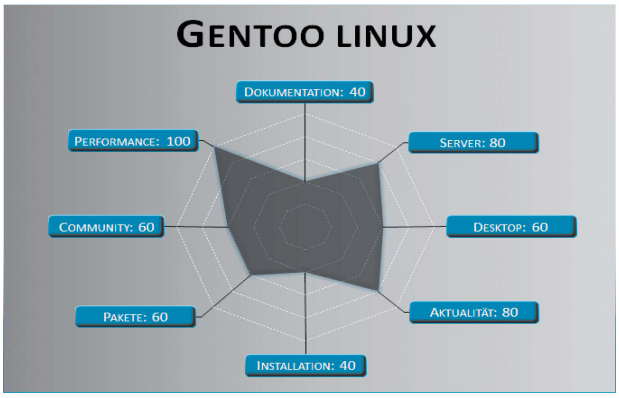
Der typische Fedora-Anwender hat beruflich oft mit Red Hat Enterprise Linux oder Cent-OS zu tun oder ist sogar Administrator, will aber zu Hause lieber ein aktuelleres Fedora, das schon mal eine Vorschau auf das nächste Red Hat bietet.

Offizielle Webseite: *http://fedoraproject.org*

Gentoo Linux



Auch wenn der Stern Gentoos langsam sinkt, ist diese Distribution kein Fall für die Geschichtsbücher. Das liegt auch an Google Chrome-OS, das seit 2010 auf das anpassungsfähige Gentoo als Basis setzt. Gentoo zeichnet sich wie Arch durch ein eigenes Paketformat aus, das mit dem Paketmanager Portage an die „Ports“ von Free BSD erinnert. Dies erlaubt die Kompilierung von Programmen nach Bedarf aus einem Repository mit mehr als 10 000 Quellpaketen. Dies ist eindeutig ein Fall für Fortgeschrittene, die sich um jedes Detail und die Konfiguration selbst kümmern. Gentoo ist ein „Rolling Release“, das sich über den Paketmanager auf dem neuesten Stand halten lässt.



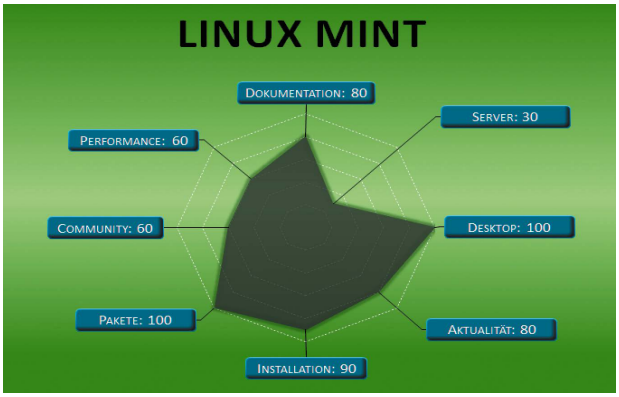
Der typische Gentoo-Anwender scheut keine hohen technischen Ansprüche, weil er die Anpassungsfähigkeit und Quelltextpakete schätzt, die Gentoo zu einem besonders schnellen System machen. Die Installation erfolgt per Scripts.

Offizielle Webseite: *www.gentoo.org*

Linux Mint



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



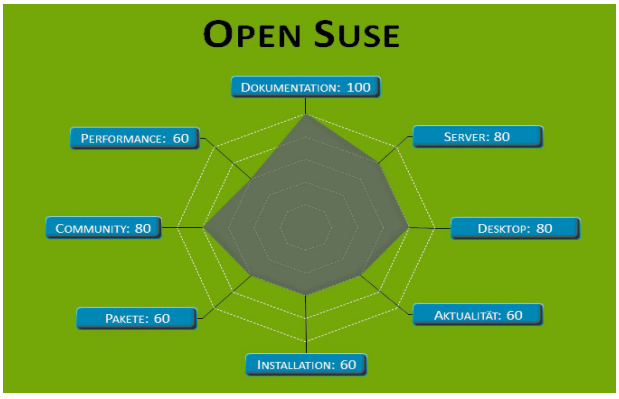
Der typische Mint-Anwender sucht ein anwenderfreundliches Desktop-Linux. Zudem ebnen viele Analogien zu Windows dem Windows-Umsteiger den Weg zu Linux.

Offizielle Webseite: *www.linuxmint.com*

Open Suse



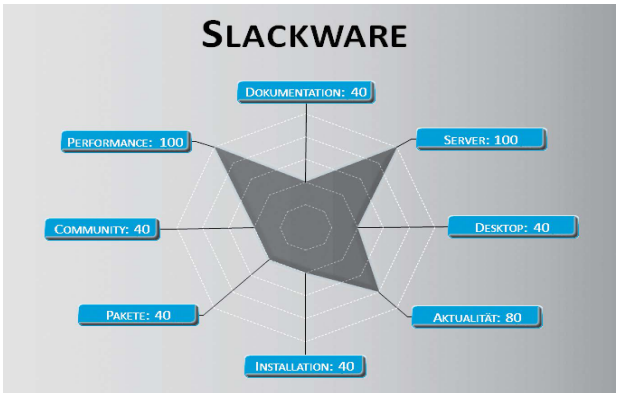
Einen langen gewundenen Weg hat Open Suse hinter sich, das bereits 1992 in Deutschland entstand und auf dem RPM-Paketformat basiert. Das System war über lange Jahre die einzige namhafte Distribution, die ein benutzerfreundliches, grafisches Desktop-Linux anbot und erfreute sich insbesondere in Deutschland größter Beliebtheit. Mittlerweile musste Open Suse den Pokal für Einsteigerfreundlichkeit an Ubuntu und Linux Mint abgeben, punktet aber immer noch mit exzellentem KDE-Desktop und grafischen Konfigurationshilfen. Seit der Übernahme durch Novell 2005 ist es wie Fedora ein von der Community entwickeltes Projekt. Die Paketauswahl ist nicht brandaktuell, lässt sich aber durch inoffizielle Paketquellen des Build Service erweitern.



Der typische Suse-Anwender setzt auf das grafische Menüsystem von Yast zur Administration oder ist ein Traditionalist, der mit Suse zu Linux kam und ihm bis heute treu bleibt.

Offizielle Webseite: *http://de.opensuse.org*

Slackware

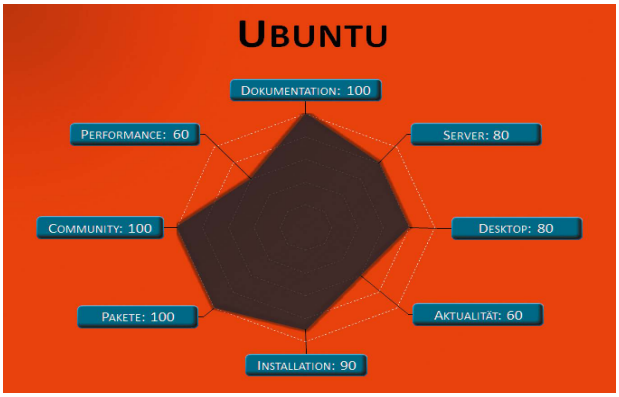


Als Fossil hat sich Slackware in eine Nische zurückgezogen, in der hauptsächlich Entwickler und Administratoren zu Hause sind. Die älteste aktive Distribution war anfangs die Basis für Suse Linux. Slackware vertritt bis heute die reine Lehre der Linux-Administration: Es gibt bis auf den Installer kaum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

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

Offizielle Webseite: *www.slackware.com*

Ubuntu

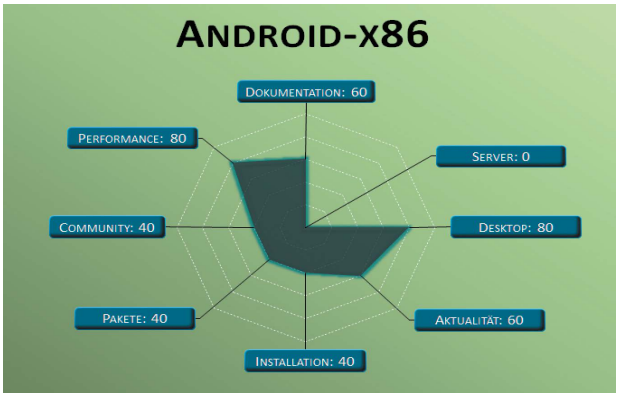


Die Distribution mit ungebrochener Popularität auf dem Desktop verfolgt den Anspruch, ein universelles System für PCs, Server und Mobilgeräte zu sein. Das Kernsystem basiert auf Debian. Auf dem klassischen Desktop-PC genießen offizielle Varianten mit Mate, XFCE und LXDE seit der Einführung der kontroversen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

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

Offizielle Webseite: *www.ubuntu.com*

Android-x86



Android ist keine herkömmliche Linux-Distribution. Von Google wurde Android ursprünglich parallel zu Chrome-OS für Smartphones geschaffen; Kernkomponenten wie die Android Runtime für Java-Apps und die touchorientierte Oberfläche sind dafür maßgeschneidert. Trotzdem ist das System so anpassungsfähig, dass OEMs und Entwicklergemeinden eigene Ausgaben bauen. Android-x86 und Remix-OS sind Vertreter dieser Gattung und werden wie Linux-Distributionen als installierbare Livesysteme ausgeliefert – aufgrund lizenzrechtlicher Beschränkungen allerdings ohne Google-Apps, zu welchen auch der App Store Google Play gehört. Wer Android-x86 auf PCs einsetzen will, muss APKs manuell installieren oder mit dem App-Store-F-Droid vorlieb nehmen.

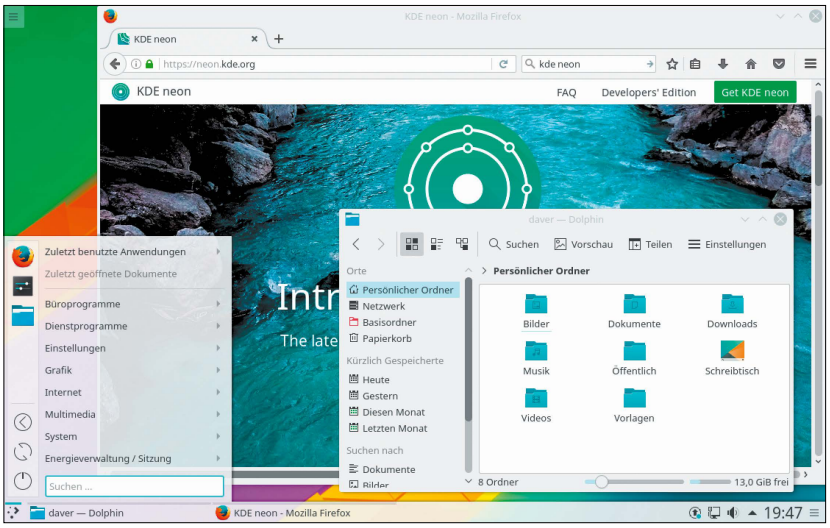
Der typische Android-X86-Anwender will eine simple Oberfläche auf einem Zweit- oder Drittrechner, muss aber für die Einrichtung Experimentierbereitschaft mitbringen.

Offizielle Webseite: *www.android-x86.org*

Die Linux-Desktops

Die Linux-Vielfalt hat zwei Ebenen: Neben der Auswahl des Systemunterbaus steht auch noch die Entscheidung für eine bestimmte Oberfläche. Derselbe Unterbau kann viele Desktopgesichter haben, derselbe Desktop verschiedenen Systemen dienen.

Von **Hermann Apfelböck**



Für anspruchsvolle Linux-Anwender: Das komplexe KDE bietet maximale Anpassungsfähigkeit und hat mit KDE Plasma 5 ein geradliniges Gewand bekommen.

Eine saubere Grenzziehung zwischen Distributions- und Desktopvielfalt ist schwierig bis unmöglich. Ubuntu hat sich je nach Standarddesktop unterschiedliche „Distributionsnamen“ wie Kubuntu oder Xubuntu gegeben, obwohl dabei nur ein anderer Desktop (KDE und XFCE) auf demselben Ubuntu arbeitet.

Wenn sich eine Linux-Mint-Variante als „Linux Mint XFCE Edition“ bezeichnet, darf man die Frage stellen, wieviel „Mint“ noch drinsteckt, da doch ein Ubuntu bei Mint den Systemunterbau legt und Linux Mint sich primär durch seinen Stammdesktop Cinnamon definiert. Und wie Mint definieren sich auch andere Distributionen wie Elementary OS, Solus oder Bodhi Linux hauptsächlich durch ihren Desktop. Die Entscheidung für einen Desktop gibt aber nicht nur die Systembedienung vor: Sie bestimmt maßgeblich die Hardwareansprüche an RAM, CPU, GPU sowie Reaktions- und Startgeschwindigkeiten.

Ein nackter Ubuntu Server ohne Desktop konsumiert etwa 50 MB RAM, während ein Ubuntu mit KDE-Oberfläche (Kubuntu) schon ab Start das 15-fache fordert (750 MB). Die richtige Einschätzung, was ein Desktop kann und für welche Hardware er taugt, ist daher für die Wahl des richtigen Systems unverzichtbar.

Desktops und Distributionen

Ein Linux-System kann bekanntlich mehrere Desktops aufnehmen. Folglich sollte es möglich sein, Desktops wie einen Mediaplayer oder eine Office-Suite als unabhängige Software zu beschreiben. Tatsächlich ist aber die Verzahnung zwischen Systembasis und Desktop dann doch komplexer als bei einer beliebigen Anwendungssoftware:

1. Die Parallelinstallation von Desktopumgebungen ist ein erheblicher Systemeingriff und längst nicht alle Desktops vertragen sich überall problemlos nebeneinander.

2. Eine Desktopumgebung ist mehr als der Desktop: Sie bringt ein mehr oder weniger umfangreiches Softwarepaket mit, mindestens mit Dateimanager und Editor, oft mit Audio-und Videoplayer sowie PDF- und Textviewer.

3. Der mit der Distribution ausgelieferte Desktop ist in der Regel sorgfältig vorkonfiguriert und unterscheidet sich von einem nachinstallierten Desktop. Diese Vorkonfiguration erspart oft erheblichen Anpassungsaufwand.

Einsteiger, Anfänger, Pragmatiker fahren daher am besten, wenn sie eine Linux-Distribution mit ihrer angestammten und mitgelieferten Standardoberfläche wählen.

Die Tabelle nennt 16 populäre bis exotische Linux-Desktops in alphabetischer Abfolge. Die nachfolgenden Kurzbeschreibungen orientieren sich hingegen an der Verbreitung und beginnen mit der Prominenz.

1. KDE: Anpassungsfähig bis detailverliebt

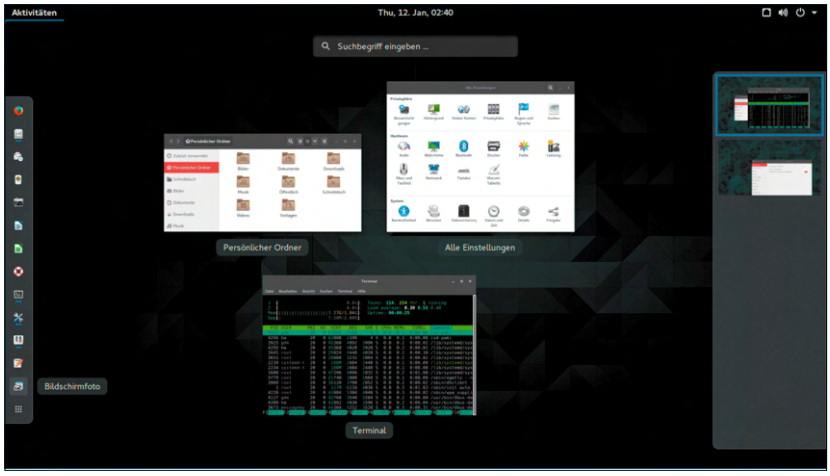
Eine der dienstältesten (seit 1996) und populärsten Desktopumgebungen ist KDE, das sich mit Version 4 erfolgreich neu erfand. KDE ist eine opulente Oberfläche für aktuellere Rechner mit Mehrkern-CPU, Open-GL-fähigem Grafikchip und vier GB RAM. Der Desktop ist ideal für fortgeschrittene Nutzer, die detaillierte Anpassungsoptionen zu schätzen wissen.

Der Plasma-Desktop stellt die Arbeitsoberfläche bereit mit Minipro-

grammen (Plasma-Widgets) und dem Window-Manager Kwin, der für Fensterdarstellung und Effekte sorgt. Standardmäßig befinden sich die KDE-Bedienelemente am unteren Bildschirmrand. Ganz links gibt es in der Standardkonfiguration das K-Menü mit Kategorien und Suchfeld. Neben dem K-Menü liegen die Taskleiste und daneben die Kontrollleiste mit Miniprogrammen (Lautstärke, Network-Manager, Zwischenablage). Eine aufgeräumte Übersicht aller Optionen bieten die „Systemeinstellungen“ im KDE-Menü. Daneben enthält die KDE-Umgebung herausragende Software wie den Dateimanager Dolphin, den Bildbetrachter Gwenview oder die Bildverwaltung Digikam. Gute KDE-Distributionen sind Kubuntu, Ubuntu KDE Neon und Open Suse Leap.

2. Gnome 3: Der moderne Desktop

Gemessen an der Zahl der Gnome-affinen Nachfolger (Unity, Mate, Cinnamon, Pantheon, implizit auch XFCE, LXDE, LXQT) ist Gnome der produktivste Linux-Desktop. Mit dem fast 20 Jahre alten Ur-Gnome hat heutiges Gnome 3 freilich nicht mehr viel gemein. Version 3 war ein radikaler Neuanfang, der bewährte Elemente über Bord warf. Das neue Gnome-Bedienkonzept ist modern, schick, funktional, aber reduziert. An den Grundfunktionen lässt Gnome kaum Eingriffe zu. Flexibilität erhält Gnome hauptsächlich durch externe Erweiterungen (*https://extensions.gnome.org*). Gnome ist ein Desktop für aktuellere Hardware mit Mehrkern-CPU, 3D-Grafik und vier GB RAM.

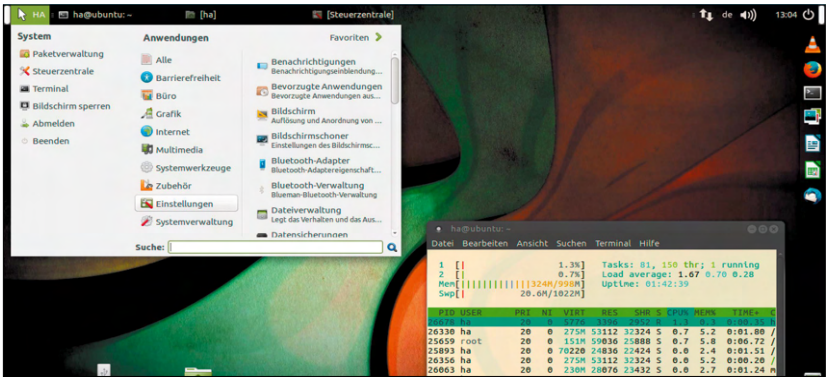


Elegant und modern: Gnome 3 zeigt auf Windows-Taste oder aktive Ecke links oben diese Übersicht mit Fenster- und Arbeitsflächenansicht sowie dem Suchfeld.

Obwohl Gnome auf Elemente wie das Startmenü verzichtet, findet sich jeder Einsteiger schnell zurecht. Als Umschalter und Programmstarter dient die Übersichtsseite „Aktivitäten“, die über die Windows-Taste oder über die linke obere Ecke erreichbar ist. Dort gibt es Schnellstarticons und das wichtige Suchfeld. Die „Einstellungen“ liefern ein aufgeräumtes Menü für allgemeine Optionen wie Sprache, Hintergrundbild und Hardwarekonfiguration. Weitere Optionen sind in der Extraanwendung Gnome-Tweak-Tool untergebracht. Empfohlene Gnome-Distributionen sind Ubuntu Gnome, Fedora, Manjaro Gnome.

Die Linux-Oberflächen

	Stammdesktop unter	Hardwareanspruch	Flexibilität	Merkmale
Budgie	Ubuntu Budgie/Solus	noch moderat	mittel	relativ einfach, gewöhnungsbedürftige Seitenleiste
Cinnamon	Linux Mint	moderat	hoch	einfache, klassische Basisbedienung und sehr flexibel
Fvwm	(nur optional, z. B. in Debian)	minimal	mittel	minimalistisch
Gnome	Ubuntu Gnome/Fedora	hoch	gering	elegant, modern, einfach, aber gewöhnungsbedürftig
KDE	Kubuntu/Open Suse	hoch	exzellent	komplexes, aber gereiftes Konzept
LXDE	Lubuntu/Knoppix	gering	mittel	einfach, klassisch, funktional, altmodische Optik
LXQT (LXDE-Nachfolger)	(nur optional, z. B. in Manjaro)	gering	mittel	einfach, klassisch, funktional
Mate	Ubuntu Mate	moderat	hoch	einfache, klassische Basisbedienung und flexibel
Moksha (E17)	Bodhi Linux	sehr gering	hoch	exotisch bis konfus, aber klein und schnell
Openbox	Bunsenlabs	minimal	mittel	minimalistisch, Anpassung anspruchsvoll
Pantheon	Elementary OS	mittel	gering	sehr einfach, elegant, aber puristisch
Pixel	Raspbian (Raspberry Pi)	gering	mittel	relativ einfach und klassisch
Trinity	Q4os	sehr gering	hoch	komplexer KDE-3-Fork, altmodische Optik
Unity	Ubuntu	noch moderat	gering	sehr einfach, intuitiv
Wmii	(nur optional, z. B. in Debian)	minimal	gering	minimalistisch und exotisch – ohne Mausunterstützung
XFCE	Xubuntu	gering bis moderat	hoch	klassisch, ausgereift, flexibel, etwas altmodisch



Klassisch und anpassungsfreudig: Mit dem Mate-Desktop lebt die Oberfläche von Gnome 2 in einer modernisierten Variante weiter.

3. Ubuntus Unity: Gnome und wieder Gnome

Unity ist die Standardoberfläche von Ubuntu. Sie setzte von 2011 bis 2017 auf ein stark angepasstes Gnome. Die Entwicklung lief aber von der Gnome-Community komplett getrennt. Mit Ubuntu Version 17.10 wechselte die Distribution technisch zurück auf das Standard-Gnome 3, behielt aber seine Optik und das sehr einfache Bedienkonzept von Unity bei. Rein äußerlich war der Wechsel des Desktop bei 17.10 kaum bzw. nur für langjährige Nutzer bemerkbar.

Das Bedienkonzept versteht jeder Nutzer auf Anhieb, allerdings bezahlt der Unity-Anwender den intuitiven Bedienkomfort mit dem Preis geringer Anpassungsmöglichkeiten.

Die Bedienung erfolgt über zwei Standardleisten, die Starterleiste links und das Hauptpanel oben. Die Starterleiste ist eine Kombination aus Taskleiste und Favoritenleiste: Sie zeigt die aktuell laufenden Programme und zusätzlich die Programmfavoriten. Das oberste Symbol mit dem Ubuntu-Logo öffnet das Dash – die Suchzentrale für Programme und Dateien. Das Hauptpanel am oberen Rand bietet das Sitzungsmenü sowie Indikatoren wie Zeitanzeige und Netzwerk-Manager. Im Gnome-Control-Center („Systemeinstellungen“) gibt es fundamentale Funktionen der Hardware- und Desktopanpassung. Zusätzliche Möglichkeiten bietet das Unity Tweak Tool, das nachinstalliert werden muss. Die einzige Distribution mit Desktop im Unity-Look ist Ubuntu.

4. Cinnamon: Der Mint-Desktop

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

Die Systemleiste enthält ein klassisches und anpassungsfreudiges Startmenü und typische Elemente wie Fensterliste, Netzwerkmanager und Arbeitsflächenwechsler. Großzügig sind auch die Optionen, um die Optik an eigene Wünsche anzupassen. Moderne Fensterthemen und Hintergründe für die Arbeitsfläche sind mit wenigen Mausklicks geändert. Generell ist das Angebot der zentralen „Systemeinstellungen“ breiter als das der reduzierenden Gnome/Unity-Desktops. Cinnamon ist Standard unter Linux Mint.

5. Mate: Klassisch und flexibel

Mit Mate entstand ebenfalls 2011 (siehe -> Punkt 4) in Ablehnung des modernen Gnome 3 ein weiterer Fork von Gnome 2. Mate ist seither eine weitere Alternative für Anwender, die einen traditionellen Desktop bevorzugen. Die Oberfläche erhielt trotz althergebrachter Bedienkonzepte ein modernisiertes Äußeres und reicht an die Anpassungsfähigkeit von Cinnamon heran. Dabei gehört Mate zu den sparsamen Desktops und kommt notfalls ohne 3D-Grafikchip und schon mit einem GB RAM aus.

Die wesentlichen Elemente der Arbeitsfläche sind die Leisten, die sich mit diversen Applets füllen und per Rechtsklick im Detail konfigurieren lassen. Die Systemeinstellungen heißen hier „Kontrollzentrum“, das alle Optionen zu Aussehen, Verhalten, Hardwareeinstellungen, Autostart-Programmen in einer aufgeräumten Übersicht zusammenfasst. Bekannteste Distribution mit Mate ist Ubuntu Mate, jedoch gibt es inzwischen von fast allen namhaften Distributionen eine Mate-Edition (Linux Mint, Debian, Fedora u. a.).

6. XFCE: Linientreuer Klassiker

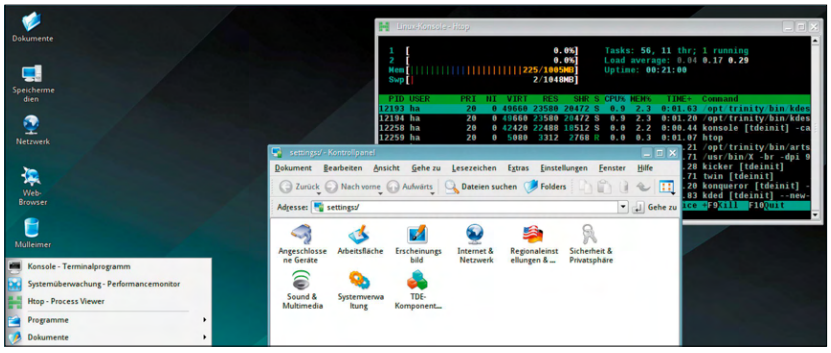
XFCE („X-Face“) gehört seit 1996 mit KDE und Gnome zu den Urgesteinen der Linux-Desktops, hat sich aber im Gegensatz zu diesen stets geradlinig entwickelt und nie revolutioniert. XFCE ist etwas angestaubt, aber perfekt für Nutzer, die klassische Elemente schätzen und selbst Hand anlegen mögen. Die Möglichkeiten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

Mit dem Dateimanager Thunar hat XFCE einen der wenigen seiner Art an Bord, die ein Drag & Drop von Dateien mit rechter Maustaste mit Kontextmenü beantworten. Im Konfigurationszentrum („Einstellungen“) sind alle Basics wie Monitoreinstellung, Benutzerverwaltung, Themes, Fensteroptik oder Treibersuche. Hauptmenü („Whisker“) und Symbolleisten von XFCE sind eine lohnende Spielwiese:

Es gibt diverse vorgegebene Elemente wie Arbeitsflächenumschalter, Sitzungsmenü („Aktionsknöpfe“) oder eine Minikommandozeile. Auch bei Aussehen, Größe, Farbe, Transparenz oder Ausblendverhalten lassen XFCE-Panels keine Wünsche offen. Praktisch alle Distributionen bieten eine Variante dieses Klassikers. Ein sorgfältig konfiguriertes XFCE liefert etwa Xubuntu.

7./8. LXDE/LXQT: Schlank und komplett

LXDE zeigt seit über zehn Jahren, dass ein kompletter Desktop keine Gigahertz-CPU braucht und dass 512 MB eine Menge Speicher sein können. Die funktionale Oberfläche benötigt nur gut 150 MB. LXDE kombiniert für das Ziel einer möglichst sparsamen Lösung heterogene Elemente wie den Window-Manager Openbox und eigene Komponenten wie Lxpanels (Leisten) oder Lxappearance (Optikkonfiguration). Die per Voreinstellung oft unnötig spröde Optik ist durch individuelle Anpassung deutlich optimierbar. LXQT ist der Nachfolger von LXDE, der die Integration von Software mit jüngeren QT-Bibliotheken leistet. Bei LXDE folgen solche Programme nicht der systemweit eingestellten Fensteroptik. Einfachster Weg zu einem sorgfältig vorkonfigurierten LXDE ist die Distribution Lubuntu.



Der Trinity-Desktop zeigt ein altes KDE 3.5, das als Abspaltung (Fork) mit kleinen Verbesserungen weiterlebt und von Kubuntu-Entwicklern nebenher gepflegt wird.

9. Moksha (E17): Schneller Exot

Enlightenment („E“, aktuelle Version ist E19) vereint minimale Hardwareansprüche mit ansprechender Ästhetik und Flexibilität. Verwirrende bis konfuse Optionen erschweren allerdings den Zugang. Moksha, Standarddesktop unter Bodhi Linux, hat als Fork von E17 etwas aufgeräumt, bleibt aber ein Abenteuer. Die schnelle Oberfläche läuft auf älterer Hardware ohne 3D-Grafik und 512 MB bis 1 GB RAM.

10. Trinity: Sparsames und schlankes Retro-KDE

Trinity führt die längst eingestellte KDE-Version 3.5 als Fork weiter. Das Ergebnis ist eine schlanke Oberfläche im allerdings im altbackenen Retrodesign daher kommt.

Die Ansprüche des Desktops liegen etwa zwischen LXDE und XFCE. Hauptargument für Trinity ist die Tatsache, dass der KDE-Fork auch auf angestaubter Hardware die detaillierten Anpassungsoptionen eines KDE mitbringt. Unter den prominenten Distributionen ist Trinity rar. Der einfachste Weg ist der Einsatz der Distribution Q4os mit Trinity als Standard.

Schönlinge – Puristen – Spezialisten

11. Pantheon: Dieser Desktop ist Standard der Distribution Elementary OS. Der aufgeräumte und ästhetische Desktop mit Mac-OS-Optik zeigt nur Starterdock und Systemleiste und bietet nur fundamentale Einstellungsoptionen. Zielgruppe sind softwareorientierte Desktopnutzer, die eine hübsche Oberfläche suchen.

12. Budgie: Technisch ambitionierter als Pantheon liefert diese Oberfläche auch eine multifunktionale Seitenleiste. Das Konzept ist innovativ, aber gewöhnungsbedürftig. Entwickelt wird Budgie für die Distribution Solus, hat aber als Ubuntu Budgie Remix Einzug in die offiziellen Ubuntu-Varianten gefunden.

13. Openbox: Eigentlich ist Openbox nur ein altehrwürdiger Window-Manager, ist aber über diese Rolle hinausgewachsen. Pures Openbox liefert am Desktop nicht mehr als ein simples Startmenü per Mausklick, mit Ergänzungen und Konfigurationstools wird daraus aber eine Arbeitsumgebung, die kaum mehr als 100 MB Speicher beansprucht. Die manuelle Einrichtung von purem Openbox ist mühsam. Ein sorgfältig vorkonfiguriertes Openbox liefert die Distribution Bunsenlabs „Hydrogen“.

14. Fvwm-Crystal: Einer der ältesten Fenstermanager für Linux ist der „F Virtual Window-Manager“ (Fvwm). Dem originalen Fvwm von 1993 sieht man sein Alter deutlich an. Viel getan hat sich aber bei der Variante Fvwm-Crystal mit Taskleiste, Menü und virtuellen Arbeitsflächen. Trotz minimaler Ansprüche (unter 100 MB RAM) sieht Fvwm-Crystal mit Transparenzeffekten schick aus. Eine fertige Distribution mit diesem Fenstermanager gibt es nicht, jedoch ist das Fossil noch als Paket unter Debian und Ubuntu erhältlich (fvwm-crystal).

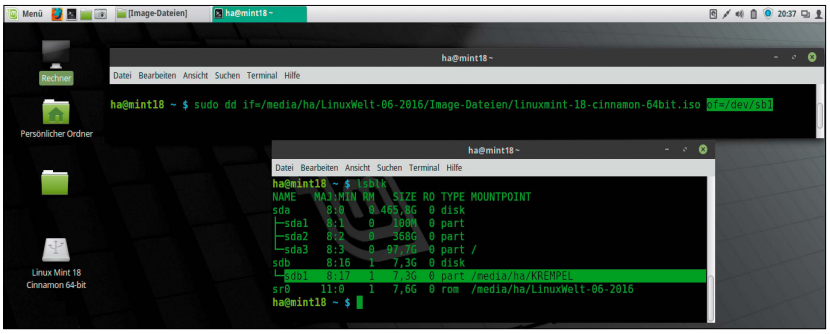
15. Wmii: Wmii (Window-Manager Improved) geht grenzwertig noch als Fenstermanager durch: Alle Aktionen zum Öffnen und Anordnen von Fenstern erfolgen per Tastatur. Der Hotkey Windows-Taste plus Eingabetaste öffnet ein neues Terminal, Windows-P einen Ausführen-Dialog. Fenster arrangiert Wmii nebeneinander oder in Spalten. Dieser Ansatz ist sinnvoll, wo ein Linux-Rechner nur einige wenige Programmfenster anzeigen soll. Wmii ist bei vielen Distributionen unter gleichnamigem Paketnamen zu erreichen.

16. Pixel: Dieser Desktop ist eine junge Entwicklung der Raspberry Pi Foundation. Er dient als verbesserter Ersatz für das bisher genutzte LXDE auf dem Raspberry-System Raspbian. Die Änderungen sind vorwiegend kosmetischer Natur.

Linux-Images & Livesysteme

Linux gibt es im Internet in vielen Varianten zumeist kostenlos in Form von ISO-Dateien zum Download. Der erste Schritt ist der Start solcher Livesysteme auf USB oder DVD. Eine Installation auf Festplatte oder USB folgt erst im zweiten Schritt.

Von **Hermann Apfelböck**



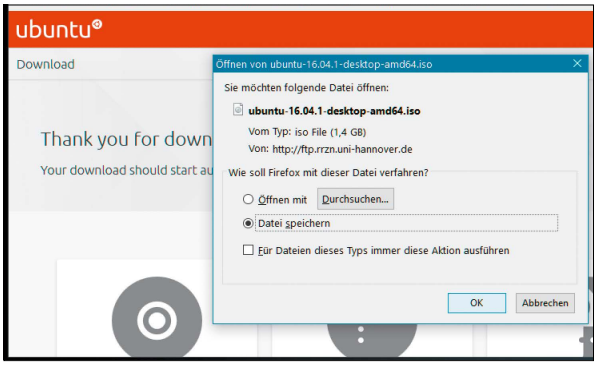
Der Umgang mit Linux-Abbildern im ISO-Format gehört zum Alltag jedes Linux-Nutzers. Selbst wenn Sie nicht zu den Experimentierfreudigen gehören, die immer wieder mal gerne eine neue Linux-Distribution ausprobieren, kommen Sie an der Herstellung bootfähiger Linux-Datenträger nicht vorbei. Dank einschlägiger Werkzeuge ist dies ein einfacher und zuverlässiger Vorgang.

Dieser Artikel erklärt, wie Sie nach dem Download eines Linux-ISO-Images zu einem bootfähigen und lauffähigen Linux-Livesystem auf USB oder DVD kommen. Dieser Vorgang ist grundlegend und auch dann notwendig, wenn Sie ein Linux eigentlich auf die Festplatte installieren möchten. Der Artikel zeigt ferner, dass bereits solche (eigentlich unveränderbare) Livesysteme interessante Möglichkeiten und Varianten bieten. Dieser Beitrag zeigt hingegen noch nicht die reguläre Installation – diese ist Gegenstand des nachfolgenden Artikels.

Suche nach dem gewünschten ISO-Image

Wo gibt es Linux? Die einfachste Antwort: auf der beiliegenden Heft-DVD. Wenn Sie sich für die dort enthaltene Systemauswahl interessieren, dann können Sie sich den Download aus dem Internet sparen: Die dort enthaltenen Distributionen starten umstandslos, bieten aus dem Livesystem die Installation auf Festplatte und liegen außerdem als ISO-Dateien im Ordner „/Image-Dateien“, falls Sie ein Livesystem auf eine eigene DVD oder einen USB-Stick übertragen möchten. Mittelfristig kommen Sie aber am Download und an der eigenen Bearbeitung von ISO-Abbildern nicht vorbei: Dazu suchen Sie einfach über Google & Co. nach dem Namen des gewünschten Systems – also etwa nach „xubuntu download“. Die einschlägige Projektwebseite, in diesem Beispiel *https://xubuntu.org*, wird dann an erster Stelle oder jedenfalls weit oben rangieren. Dort gibt es dann einen Eintrag „Download“, der Sie ans Ziel bringt. Meist ist noch zu entscheiden, ob es ein 32- oder 64-Bit-System sein soll. Im Linux-Umfeld steht hier meist „i386“ für 32 Bit und „amd64“ für 64 Bit, wobei „amd“ keine Einschränkung auf den Hersteller AMD bedeutet. Die schlankere 32-Bit-Architektur eignet sich besser für ältere Hardware, 64-Bit-Systeme für aktuelle Rechner mit mehr als vier GB RAM. 64 Bit ist Voraussetzung für eine Installation im Uefi-Modus (siehe den nachfolgenden Artikel).

Kleinere Linux-Distributionen haben keinen eigenen Downloadserver, sondern nutzen die Downloadplattform *https://sourceforge.net*. Auch Universitäten helfen oft als Spiegelserver mit, um die Downloadlasten zu verteilen. Es ist also in Ordnung, wenn Sie von einer Linux-Projektseite nach sourceforge.net oder an einen Uniserver geschickt werden. Wer sichergehen will, dass ihn seine Recherche und sein Download nicht in dunkle Ecken führen, kann auch auf der Übersichtsplattform *http://distrowatch.com/* nach Linux-Distributionen suchen.



Download eines ISO-Abbilds: Ubuntu wird in diesem Fall von einem deutschen Uniserver bereitgestellt. „amd64“ ist die unter Linux gebräuchliche Bezeichnung für 64-Bit-Systeme.

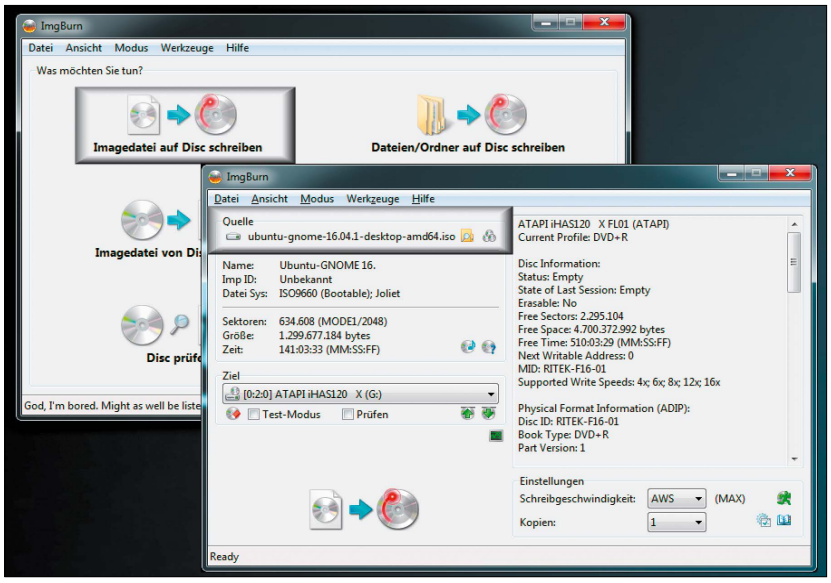
Die Kopierwerkzeuge für ISO-Abbilder

Um aus dem Internet geladene ISO-Abbilder bootfähig auf CD/DVD/USB/SD zu kopieren, gibt es einschlägige Tools, die Sie zum Großteil auf der Heft-DVD vorfinden. Beim Schreiben von Abbildern müssen Sie das Zielmedium sorgfältig kontrollieren, damit Sie nicht statt eines geplanten USB-Sticks als Ziel eine große USB-Festplatte überschreiben.

Unter Linux auf CD/DVD kopieren: Viele Linux-Distributionen bringen standardmäßig das Programm Brasero mit. Wo es fehlt, ist es über die Paketquellen der Repositories gegebenenfalls schnell nachinstalliert. Mit Brasero brennen Sie unter Linux am bequemsten bootfähige CDs (ISOs bis 700 MB) oder DVDs (ISOs größer als 700 MB). Ähnlich wie bei Imgburn unter Windows genügen im Brasero-Startmenü die Wahl „Abbild brennen“ und die nachfolgende Auswahl der ISO-Datei.

Unter Windows auf CD/DVD kopieren: Unter Windows empfehlen wir das Tool Imgburn (Windows-Version auf Heft-DVD, Download unter *http://imgburn.com*), um je nach Imagegröße bootfähige CDs (ISOs bis 700 MB) oder DVDs (ISOs größer als 700 MB) zu brennen. Natürlich beherrschen auch große Brennprogramme wie Nero diesen Job. Unter Imgburn wählen Sie nach dem Start die Option „Imagedatei auf Disc schreiben“. Der wichtigste Punkt des Folgedialogs ist links oben „Quelle“ mit dem kleinen Ordnersymbol, über das Sie dann zur ISO-Quelldatei navigieren. Bei eingelegtem Rohling wird dann die große Schaltfläche links unten aktiv, mit der Sie den Schreibvorgang auslösen.

Unter Linux und Windows „roh“ auf USB und SD-Karten kopieren: In aller Regel enthalten die ISO-Abbilder von Linux-Distributionen alle notwendigen Informationen einschließlich der Bootumgebung. Daher ist eine 1:1-Rohkopie auf USB oder auf SD-Karte völlig ausreichend. Der einschlägige Rohkopierer dd unter Linux ist das Kommandozeilentool dd mit



Linux-Abbild auf DVD-Rohling brennen: Unter Windows leistet das kostenlose Imgburn (auf Heft-DVD) zuverlässige Arbeit und benötigt dafür nur wenige Klicks.

der folgenden 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.

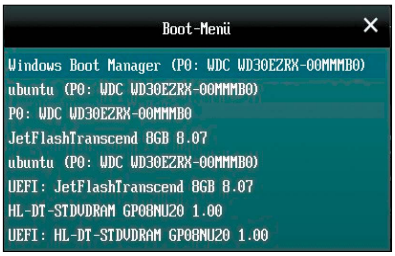
Der Rohkopierer Win 32 Disk Imager macht dasselbe unter Windows (auf Heft-DVD, Download unter *http://sourceforge.net/projects/win32diskimager*). Hier genügt es, die Quelldatei („Image File“) und das Zielgerät („Device“) anzugeben. Die Schaltfläche „Write“ startet den Kopiervorgang.

Unter Linux und Windows mit Unetbootin auf USB oder SD-Karte kopieren: Unetbootin schreibt seine eigene Bootumgebung auf das Zielmedium und eignet sich für alle Ubuntu-basierten Systeme einschließlich Linux Mint. Für Distributionen, die nicht Ubuntu-basiert sind, verwenden Sie die oben beschriebenen Rohwerkzeuge. Unetbootin ist jedoch ideal, wenn Sie ein Ubuntu-Livesystem anpassungsfähig halten wollen (siehe unten „Persistenz“).

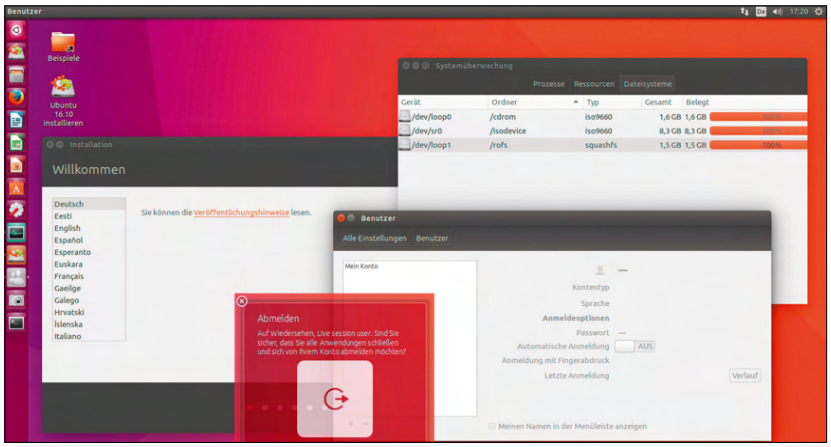
Unetbootin gibt es für Linux, Windows und Mac-OS X (Windows-Version auf Heft-DVD und Download unter *http://unetbootin.sourceforge.net*). Um ein ISO-Image bootfähig auf USB-Stick zu befördern, wählen Sie im Dialog unten die Option „Abbild“ und navigieren dann mit der Schaltfläche „...“ zur gewünschten 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. Mit „OK“ starten Sie den Kopiervorgang. Kontrollieren Sie die Laufwerkskennung des USB-Sticks ganz genau, denn Unetbootin wird das Medium komplett überschreiben. Unter Windows erscheint das Laufwerk mit Laufwerksbuchstaben, unter Linux mit der Gerätebezeichnung „/dev/sd[x]“. Nach „OK“ startet der Kopiervorgang.

Der Start eines Linux-Livesystems

Um einen Rechner von einer eingelegten CD/DVD zu booten, sind meistens keine Vorbereitungen erforderlich. Ob ein PC oder Notebook automatisch von einem USB-Medium bootet, ist hingegen nicht gewiss und hängt von den Bios/Uefi-Einstellungen ab. Die Reihenfolge, mit der das Bios die Datenträger abfragt, lässt sich natürlich im Bios-Setup ändern, aber das ist selten nötig: Jedes Bios/Uefi ermög-



Bootauswahl beim Gerätestart: Je nach Bios/Uefi führt eine Taste wie Esc, F9, F10, F11, F12 zu einer solchen Liste, auf der Sie den Datenträger mit dem Linux-System auswählen.



Typisches Livesystem zum Arbeiten, Testen, Installieren: Dass es sich „nur" um ein Livesystem handelt, zeigen das Read-only-Dateisystem („/rofs") und fehlende Benutzerkonten.

licht beim Rechnerstart per Tastendruck eine Bootauswahl, die alle Datenträger anzeigt. Dort wählen Sie dann einfach mit der Cursortaste die CD/DVD („ATAPI…") oder das meist eindeutig benannte USB-Laufwerk. Leider können wir Ihnen nicht verbindlich sagen, welche Taste bei Ihrem Gerät diese Bootauswahl auslöst. Die Tasten Esc, F9, F10, F11, F12 sind häufige Kandidaten. Sollte die Bootauswahl das DVD-Laufwerk oder den USB-Stick nicht anzeigen, müssen Sie im Uefi noch die Option „Secure Boot" deaktivieren.

Livesysteme starten in der Regel mit einem Standardbenutzer „Live User" (oder ähnlich einfach) ohne Anmeldung zum Desktop. Zugangskennwörter brauchen Sie nicht, es sei denn, Sie melden sich absichtlich oder versehentlich ab. In diesem Fall ist das Standardkennwort des „Live Users" leicht zu googlen oder auf der Projektseite der Distribution zu erfahren.

Möglichkeiten und Grenzen von Livesystemen

Das Kopieren eines ISO-Abbilds auf CD/DVD/USB und Starten des Livesystems ist in vielen Fällen nur der notwendige Zwischenschritt, um dann die Distribution aus dem laufenden Livesystem auf die Festplatte zu installieren (siehe dazu den folgenden Beitrag). Livesysteme sind keine vollwertigen Betriebssysteme, denn Systemveränderungen überleben keinen Neustart: Ein Livesystem, selbst wenn es sich auf einem beschreibbaren Medium befindet, speichert Änderungen nicht dauerhaft. Das Dateisystem wird in den Arbeitsspeicher geladen und die in der Sitzung durchaus möglichen Änderungen gehen beim Herunterfahren wieder verloren. Typischerweise erkennen Sie laufende Livesysteme mit dem mount-Befehl im Terminal, der ein „loop0"-Device, ein „cloop"-Device (komprimiert), ein „squashfs" (komprimiert) oder auch ein „aufs"-Dateisystem (Another Union File System) anzeigt. Dennoch sollten Sie den Wert von Livesystemen nicht unterschätzen:

1. Sie können sich ein Linux unverbindlich ansehen und bis ins Detail prüfen, ob es zu Ihnen passt. Livesysteme machen dabei keinerlei Eingriffe auf Datenträger und lassen bestehende Systeme völlig unberührt.

2. Ein Livesystem ist ein zuverlässiger Test für die Hardware. Wenn Sie im Livesystem keine Probleme mit Grafik, Netzwerk, Drucker und sonstiger Peripherie haben, dann trifft das auch auf das installierte System zu. Der Umkehrschluss, dass Probleme im Livesystem auch dauerhaft beim installierten System bestehen werden, ist hingegen nicht immer zutreffend: Im endgültigen System besteht ja die Möglichkeit, Hardwaretreiber nachzurüsten. Beachten Sie außerdem, dass jedes Livesystem Startparameter für Problemsituationen vorsieht, die zumindest einen Notfallstart ermöglichen.

3. Breit ausgestattete Livesysteme wie jenes von Ubuntu eignen sich hervorragend als Notfall-, Zweit- oder Mobilsystem. Sie können damit sofort produktiv arbeiten, wenn das Hauptsystem, sei es Windows, Linux oder Mac-OS, einmal streikt. Dabei haben Sie Zugriff auf alle Datenträger, können von dort Benutzerdaten kopieren oder auch Reparaturen ausführen. Linux-Livesysteme sind ferner prädestiniert für die Rolle als Surfsysteme für sicheres Onlinebanking oder riskante Webbesuche. Auch der Einsatz einer portablen Arbeitsumgebung oder eines einbruchssicheren Datenspeichers ist einschlägig: Ein Linux aus der Hosentasche kann an jedem PC genutzt werden.

Anpassung und Aufwertung von Livesystemen

Ein Linux-Livesystem bleibt Livesystem. Es gibt jedoch bei Livesystemen auf beschreibbaren Medien wie USB-Sticks durchaus Optionen für funktionale Aufwertung. Die nachfolgend beschriebenen, sehr unterschiedlichen Techniken beschränken sich auf Ubuntu-Varianten inklusive Linux Mint.

1. Unetbootin mit „Persistenz": Das bereits beschriebene Tool Unetbootin zeigt die Option „Platz um Dateien zwischen Neustarts zu erhalten". Als Speichergröße tragen Sie hier beispielsweise „1000 MB" ein. Dies ermöglicht es, im späteren Livesystem weitere Programme zu installieren, das

System individuell einzurichten oder Benutzerdateien abzulegen. Systemeinstellungen und nachinstallierte Programme bleiben dann erhalten. Das ist untypisch für ein Livesystem und erweitert dessen Komfort erheblich. Einige Livesysteme wie Tails (*https://tails.boum.org*) oder Puppy Linux (*http://puppylinux.org*) bieten diese Option auch unabhängig von Unetbootin an – unter dem Namen „Persistenz".

Beachten Sie aber, dass auch ein Livesystem mit Persistenz im Vergleich zu einem vollwertig installierten Linux limitiert bleibt. Umfangreiche Installationen, langfristige Systemupdates, unbegrenzte Mengen von Benutzerdateien setzen zwingend eine Installation voraus. Erst hier gibt es dann auch einen oder mehrere Benutzer und eine entsprechende Zugangskontrolle.

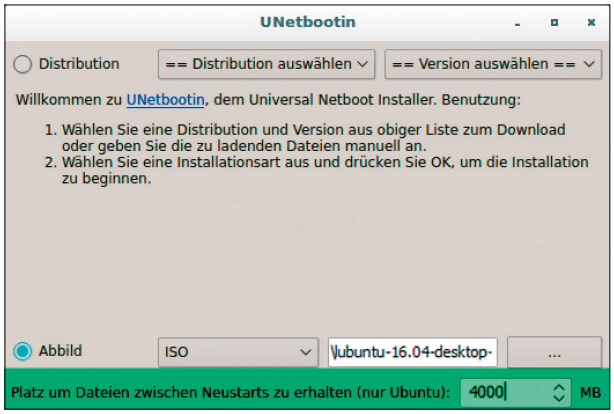
2. Angepasstes Livesystem mit Systemback: Dies ist ein völlig anderer Ansatz als bei Unetbootin. Das Livesystem bleibt typisch eingefroren und unveränderlich, jedoch können Sie es vorab minutiös nach Ihren Vorstellungen einrichten: Statt eines Livesystems von der Stange nutzen Sie hier ein Livesystem mit individuell eingerichtetem Desktop und genau der Software, die Sie brauchen. Die technisch unkomplizierte Möglichkeit mit dem Tool Systemback eignet sich auch für weniger erfahrene Linux-Nutzer.

Aufwendiger als der Einsatz des komfortablen Tools ist aber zunächst die optimale Einrichtung des Systems. Sie benötigen ein normal installiertes Ubuntu oder Linux Mint. Bei den Anpassungen gibt es einige triviale, aber leicht zu übersehende Fallen:

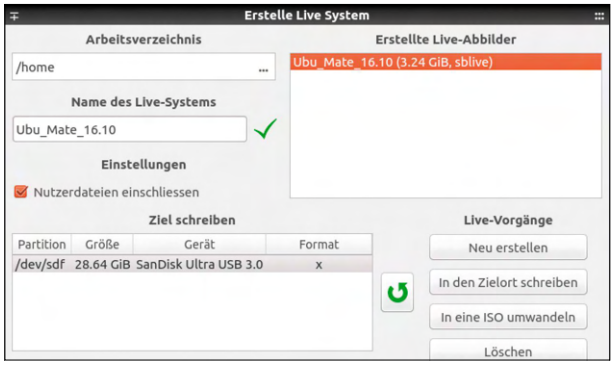
- Richten Sie vor allen Einstellungen einen Benutzer ein („Systemeinstellungen -> Benutzer"), mit dem sich die künftigen Systembenutzer identifizieren können, und erledigen Sie dann die komplette Konfiguration ebenfalls in diesem Konto.
- Verwenden Sie keine proprietären Treiber und verzichten Sie auf die Sparoptionen der „Energieverwaltung", wenn das Livesystem auf anderer Hardware als dem Basissystem zuverlässig laufen soll.
- Das Einrichten und Speichern von WLAN- und Freigabekennwörtern ist nur dann sinnvoll, wenn das Livesystem künftig auch im gleichen Umfeld genutzt wird.
- Machen Sie mit Ihrem Basissystem nach allen Maßnahmen mindestens einen Neustart und probieren Sie alle wesentliche Software durch: Nichts ist lästiger als ein Livesystem, das Sie später standardmäßig mit einer Fehlermeldung begrüßt, oder eine Software, die bei jedem Start nachfragt, ob es als Standardprogramm genutzt werden soll. Jede solche Bremse ist im Basissystem mühelos zu lösen, im späteren Livesystem nicht mehr. Ist alles korrekt eingerichtet, können Sie Systemback auf Ubuntu-basierten Systemen über ein externes PPA beziehen:

```
sudo add-apt-repository ppa:nemh/
  systemback
sudo apt-get update
sudo apt-get install systemback
```

Der Aufruf erfordert root-Rechte. Als wesentliche Voreinstellung definieren Sie bei Bedarf zunächst das „Speicherverzeichnis" („Storage directory") rechts oben. Standardmäßig nutzt Systemback das Home-Verzeichnis – und zwar nicht das des angemeldeten Benutzers, sondern den Hauptordner „/home". Die einschlägige Schaltfläche lautet „Erstellung Live System" („Live system create"). Dieses öffnet einen gleichnamigen Unterdialog („Erstellung Live System"), wo Sie mit „Neu erstellen" („Create new") zunächst ein Image des laufenden Basissystems anlegen – dieses landet mit der Endung „.sblive" standardmäßig im Verzeichnis„/home". Ist der Vorgang abgeschlossen, erscheint das Image unter „Erstellte Live-Abbilder" („Created Live images"). Danach stecken Sie einen USB-Stick an, sorgen mit dem Refreshknopf neben „Ziel schreiben" („Write target") dafür, dass der Stick auftaucht, und markieren dort den Datenträger. Ferner klicken Sie unter „Erstellte Live-Abbilder" auf das Image. Sind Quelle und Zieldatenträger markiert, wird die Schaltfläche „In den Zielort schreiben" („Write to target") aktiviert, die Sie nunmehr auslösen. ●



Permanentspeicher: Geben Sie in Unetbootin die Größe der Persistenzdatei an. Dann kann das (Ubuntu-)Livesystem zusätzlich installierte Software dauerhaft anbieten.



Livesystem aus einem laufenden Ubuntu/Mint erstellen: Das vorher erzeugte Liveabbild und der Zieldatenträger müssen markiert sein, damit die Schaltfläche „In den Zielort schreiben" aktiv wird.

Die optimale Ubuntu-Installation

Bei der Installation bieten Ubuntu-basierte Distributionen den größten Komfort. Das System lässt sich solo, neben Windows oder Linux oder auch auf externen USB-Datenträgern einrichten. Dieser Artikel erklärt alle Varianten unter Bios wie Uefi.

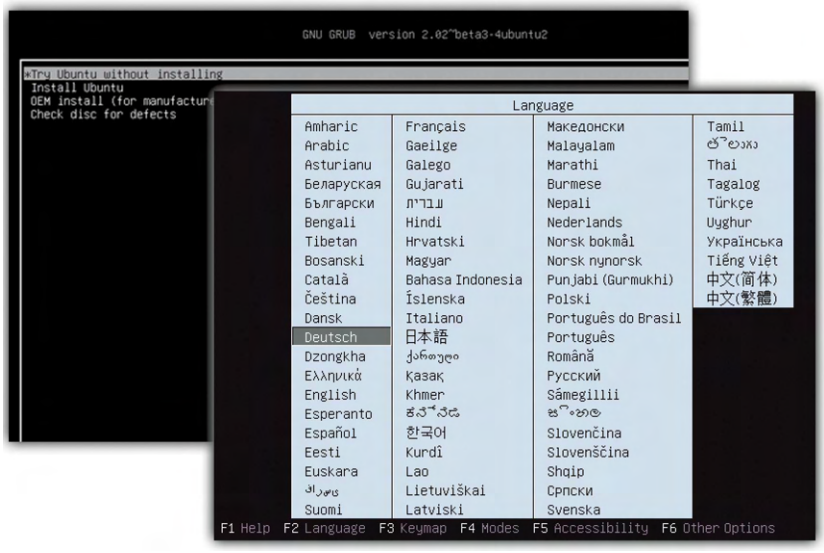
Von **Thorsten Eggeling**

Der Ubuntu-Installer Ubiquity ist übersichtlich und zuverlässig. Er erkennt vorhandene Linux- und Windows-Systeme automatisch und bietet dann die Parallelinstallation an. Andere Linux-Installer können da nicht ganz mithalten, wenngleich auch ein Debian-Installer oder jener von Manjaro durchaus informativ und logisch arbeitet.

Generell ist es mit keinem Installer ein Problem, ein Linux solo auf einen Datenträger zu befördern. Grundregeln sind hierbei, dass das System erstens seine eigene Systempartition benötigt, zweitens – aber nicht zwingend – eine kleine Swappartition zur Speicherauslagerung. Der Bootloader ist bei Installation auf PCs und Notebooks auf der standardmäßig vorgeschlagenen ersten internen Platte („dev/sda“) am richtigen Ort, bei Installation auf externe USB-Datenträger muss er hingegen ebenfalls auf das USB-Medium geschrieben werden.

Bei sorgfältiger Beachtung dieser Grundregeln werden Sie mit keinem Linux Mühe haben, es als alleiniges System zu installieren.

Der nachfolgende Installationsratgeber fällt trotz des komfortablen Ubuntu-Tools deutlich komplizierter aus. Grund hierfür ist, dass wir hier systematisch alle Multiboot-Szenarien berücksichtigen (inklusive Bios/Uefi-Problematik) und außerdem die Verschlüsselungsoptionen für Systempartition und Home-Verzeichnis.



Ubuntu-Livesystem: Beim Start vom Installationsmedium zeigt Ubuntu im Bios-Modus eine Sprachauswahl. Im Uefi-Modus gibt es nur ein englischsprachiges Menü.

1. Ubuntu-Installation vorbereiten

Ubuntu lässt sich auf allen PCs und Notebooks unabhängig vom Alter installieren. Vor einigen Jahren gab es jedoch einen Technologiewechsel, der sich auf die Linux-Installation auswirkt. PCs aus der Ära Windows XP und 7 starten von Festplatten mit einem MBR-Partitionsschema (Master Boot Record). Ist auf einem Gerät Windows 8 oder 10 vorinstalliert, kommt eine Uefi-Firmware zum Einsatz und auf der Festplatte ist eine GPT-Partition zu finden (GUID Partition Table). Sehen Sie im Firmwaresetup nach, welche Einstellungen für Uefi oder EFI es gibt. Rufen Sie diese kurz nach dem Einschalten des PCs über Tasten wie Esc, Entf (Del), F2, F8 oder F10 auf. Unter Windows 8 oder 10 gelangen Sie so in das Bios-Setup: Klicken Sie im Windows-Anmeldebildschirm rechts unten die „Herunterfahren“-Schaltfläche an. Halten Sie die Shift-Taste gedrückt und klicken Sie im Menü der Schaltfläche auf „Neu starten“. Gehen Sie auf „Problembehandlung -> Erweiterte Optionen -> UEFI-Firmwareeinstellungen“ und dann auf „Neu starten“.

Suchen Sie nach Optionen wie „Uefi only“, „CSM“, „Uefi and CSM“, „Uefi and Legacy“ oder „Legacy Boot“, die meist unter Menüs mit Namen wie „Boot“ oder „Boot Order“ zu finden sind. Wenn Sie Linux neben Windows installieren möchten, lassen Sie diese

Einstellung unverändert oder Sie wählen etwas wie „Uefi and CSM“. Die Bios-Emulation CSM (Compatibility Support Module) sorgt dafür, dass der PC sowohl im Uefi als auch im Bios-Modus booten kann. Die Parallelinstallation von Linux muss jedoch immer im Uefi-Modus erfolgen, wenn auch Windows in diesem Modus installiert ist. Soll auf dem Gerät nur Ubuntu Platz finden, spielt es keine Rolle, ob Sie den Bios- oder Uefi-Modus verwenden. Daraus ergeben sich keine besonderen Vor- oder Nachteile.

Im Firmwaresetup sollten Sie außerdem Secure Boot deaktivieren. Secure Boot soll die Bootumgebung vor Schadsoftware schützen. Ubuntu ist dafür zwar vorbereitet, aber die Funktion kann unter bestimmten Umständen zu Problemen führen. Die Einstellungen für Secure Boot finden Sie meist unter einem Menü wie „Bios Features“, „Security“ oder ähnlich. Setzen Sie die Option auf „Disabled“. Windows wird nicht beeinträchtigt, wenn Sie CSM aktivieren und Secure Boot abschalten.

Installation im Bios-Modus: Sie können den Rechner von der Heft-DVD booten und das gewünschte Linux-System auswählen. Ist kein DVD-Laufwerk vorhanden, erstellen Sie einen Setupstick für die Installation. Auf der Heft-DVD finden Sie dafür das Tool Unetbootin, das sich unter Linux oder Windows starten lässt.

Installation im Uefi-Modus: Auf der Heft-DVD liegen die ISO-Dateien der Linux-Distributionen im Verzeichnis „Image-Dateien“. Brennen Sie aus der ISO-Datei eines 64-Bit-Systems eine DVD oder erstellen Sie mit Unetbootin einen Setupstick. Nur 64-Bit-Systeme beherrschen Uefi-Boot.

Livesystem booten: Sollte der Computer nicht von der DVD oder dem USB-Stick booten, ändern Sie im Bios/Firmwaresetup die Bootreihenfolge. Viele PCs zeigen auch ein Bootmenü, wenn Sie kurz nach dem Einschalten eine Taste wie Esc, F9 oder F10 drücken. Für den Uefi-Modus wählen Sie das Bootlaufwerk mit dem vorangestellten Hinweis „Uefi“. Das Ubuntu-Auswahlmenü erscheint dann nur in englischer Sprache und Sie wählen „Try Ubuntu without installing“. Im Bios-Modus drücken Sie kurz nach dem Start des Livesystems eine beliebige Taste, wählen als Sprache „Deutsch“ und dann den Menüeintrag „Ubuntu ohne Installation ausprobieren.



Firmwareeinstellungen: Wenn Sie Ubuntu auf einem Uefi-PC im Bios-Modus installieren wollen, dann muss die CSM-Unterstützung aktiviert sein.



Ubuntu alleine: Ist kein weiteres System auf dem PC installiert, gibt es im Fenster „Installationsart“ nur die Option „Festplatte löschen und Ubuntu installieren“.

2. Ubuntu-Installation durchführen

Nach dem Start des Livesystems von DVD oder USB-Stick sehen Sie den Ubuntu-Desktop. Sie haben jetzt Gelegenheit, das System auszuprobieren und sich mit dem Desktop vertraut zu machen. Die Installation starten Sie per Doppelklick auf das Icon „Ubuntu 17.04 installieren“ beziehungsweise „Install Ubuntu 17.04“. Folgen Sie den Anweisungen des Setupassistenten. Zuerst wählen Sie als Sprache „Deutsch“ aus.

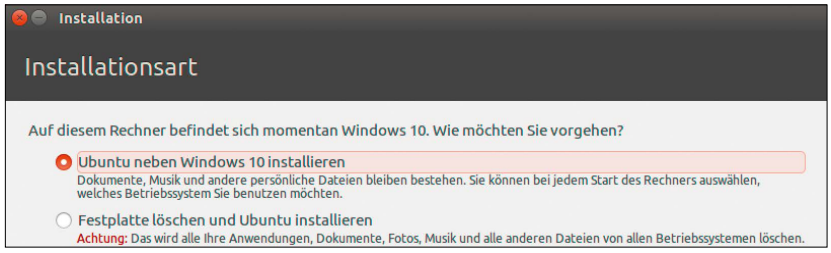
Danach sollten Sie Häkchen vor den beiden angebotenen Optionen setzen. Die eine betrifft den Download von Updates während der Installation, die andere die Installation von „Drittanbieter-Software“ etwa für die MP3-Wiedergabe, WLAN-Geräte und den Flash-Player. Dafür ist eine Internetverbindung erforderlich.

Nach Klick auf „Weiter“ erscheint das Fenster „Installationsart“. Was dieser Dialog anbietet, hängt von den Verhältnissen auf Ihrem PC ab, also davon, was der Installer auf der Festplatte vorfindet:

A. Ganze Festplatte für Ubuntu: Ist die Festplatte leer, können Sie nichts falsch machen. Der Installer bietet mit der Option „Festplatte löschen und Ubuntu installieren“ an, die ganze Platte für Ubuntu zu verwenden, und Sie können das einfach bestätigen.

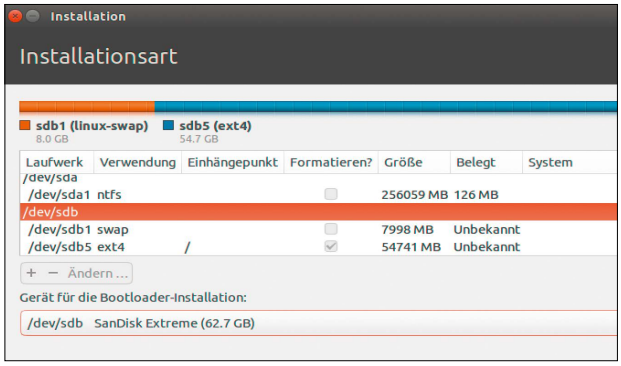
B. Bisheriges Betriebssystem ersetzen: Ist auf der Festplatte ein Betriebssystem installiert, das Sie durch Ubuntu ersetzen wollen, wählen Sie ebenfalls „Festplatte löschen und Ubuntu installieren“. Dann wird die Partition gelöscht, neu formatiert und Ubuntu darauf installiert.

C. Ubuntu neben Windows: Genug Platz auf der Festplatte vorausgesetzt, können Sie Ubuntu auch neben Windows installieren und beim Rechnerstart über einem Bootmanager auswählen, welches System starten soll.



Multiboot: Befindet sich Windows auf der Festplatte, bietet Ubuntu die Parallelinstallation an. Per Bootmanager wählen Sie später das gewünschte System.

USB-Installation: Der Grub-Bootloader muss auf dem USB-Laufwerk landen. Liegt er auf der Festplatte, lassen sich die hier installierten Systeme nicht mehr starten.



Der Installer erkennt bereits vorhandene Systeme und bietet Ihnen an, Ubuntu parallel dazu zu installieren. Die Option heißt dann „Ubuntu neben Windows 10 installieren“ (Bios) oder „Ubuntu neben Windows Bootmanager installieren“ (Uefi). Aktivieren Sie diese und klicken Sie auf „Weiter“. Im nächsten Schritt können Sie dann die Windows-Partition per Schieberegler verkleinern und dadurch Platz für Ubuntu schaffen.

Ist eine zweite Festplatte vorhanden, die Sie für Linux nutzen wollen, können Sie diese hinter „Laufwerk wählen“ angeben.

D. Manuelle Partitionierung: Möchten Sie selbst die verwendeten Partitionen anlegen und zuweisen, wählen Sie „Etwas Anderes“. Die Option bringt Sie zum erweiterten Partitionierungswerkzeug. Hier können Sie unter „Gerät für die Bootloader-Installation“ auswählen, wo der Bootloader Grub 2 installiert werden soll. In Punkt 3 erfahren Sie mehr darüber.

Der weitere Ablauf ist immer derselbe, unabhängig von dem, was Sie bei „Installationsart“ gewählt haben. Sie legen die Zeitzone, Tastaturbelegung, Erstkonto und Passwort fest. Außerdem gibt es die Wahl zwischen der automatischen Anmeldung und der Anmeldung nach Passworteingabe. Zusätzlich ist eine Option vorhanden, über die Sie die Verschlüsselung Ihrer persönlichen Dateien aktivieren können (siehe Punkt 3). Das Passwort des Erstkontos dient nicht nur zur Anmeldung beim System. Es ist sudo-berechtigt und auch für administrative Aufgaben erforderlich, etwa für die Installation neuer Software.

Nach Abschluss der Installation klicken Sie auf „Jetzt neu starten“. Nach dem Neustart begrüßt Sie das frisch Installierte Ubuntu-System.

3. Installation auf einem USB-Gerät

Für die Installation auf einem USB-Stick oder einer USB-Festplatte wählen Sie im Fenster „Installationsart“ immer die Option „Etwas Anderes“. In der Regel wird sich auf einer USB-Festplatte oder einem USB-Stick nur eine Partition befinden. Löschen Sie diese über die kleine Minus-Schaltfläche („-“). Alle darauf befindlichen Daten gehen verloren.

Erstellen Sie über die „+“-Schaltfläche eine kleine Partition für die Auslagerungsdatei („Swap“). Der Swapspeicher sollte etwa 20 bis 30 Prozent größer sein als der Hauptspeicher (RAM). Dieser Schritt ist bei PCs mit vier GB RAM oder mehr jedoch nicht unbedingt erforderlich.

Auf die gleiche Weise legen Sie eine große Partition für das Linux-System an. Hier wählen Sie hinter „Einbindungspunkt“ den Eintrag „/“ aus der Liste. Unter „Gerät für die Bootloader-Installation“ wählen Sie das USB-Gerät aus, typischerweise „/dev/sdb“. Kontrollieren Sie diese Angabe genau. Wenn Sie den Bootloader auf die Festplatte schreiben, startet das System der Festplatte ohne das angeschlossene USB-Gerät nicht mehr. Klicken Sie zum Abschluss auf „Jetzt installieren“ und folgen Sie den weiteren Anweisungen des Setupprogramms. Bei Bedarf aktivieren Sie die Verschlüsselung Ihrer persönlichen Daten (siehe -> Punkt 5).

4. Ubuntu-Partition verschlüsseln

Wenn Sie die komplette Systempartition verschlüsseln wollen, wählen Sie im Fenster „Installationsart“ die Option „Die neue Ubuntu-Installation zur Sicherheit verschlüsseln“. Dabei wird automatisch auch ein Häkchen vor „LVM bei der neuen Ubuntu-Installation verwenden“ gesetzt.

Das Verfahren bietet bei mobilen Geräten hohe Sicherheit, denn persönliche Daten liegen nicht nur im Home-Verzeichnis. Nach einem Klick auf „Weiter“ geben Sie den Sicherheitsschlüssel ein. Dieser sollte möglichst lang und kompliziert sein, damit die Verschlüsselung vor Hackerangriffen geschützt ist. Fahren Sie mit „Jetzt installieren“ fort.

Auch wenn Ubuntu nicht mehr startet, können Sie trotzdem auf die verschlüsselte Partition zugreifen. Booten Sie den PC einfach vom Installationsmedium und starten Sie den Dateimanager. Klicken Sie auf „Andere Orte“. Sie sehen eine Übersicht mit den vorhandenen Partitionen, eine davon mit dem Zusatz „verschlüsselt“. Klicken Sie diese an, tippen Sie das Passwort

zum Entsperren des Datenträgers ein und klicken Sie auf „Verbinden“. Danach können Sie auf die Inhalte wie gewohnt zugreifen.

Zweitschlüssel: Ohne das richtige Passwort kommen auch Sie selbst nicht mehr an die Daten heran. Es empfiehlt sich daher, ein Zweitpasswort zu erstellen, das ebenfalls ausreichend kompliziert sein muss. Öffnen Sie ein Terminalfenster (Strg-Alt-T) und holen Sie über den Befehl

```
blkid
```

Informationen zu den Partitionen ein. Hier taucht die root-Partition beispielsweise in einer Zeile mit den Angaben „/dev/sda5“ und „TYPE=crypto_LUKS“ auf. Tippen Sie dann folgende Befehlszeile ein:

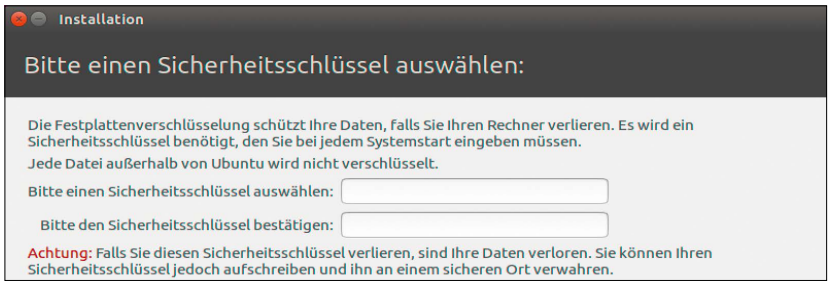
```
sudo cryptsetup luksAddKey /dev/
  sd[xx]
```

Bestätigen Sie mit dem bei der Ubuntu-Installation vergebenen Passwort. „/dev/sd[xx]“ ersetzen Sie durch die Bezeichnung der root-Partition. Tippen Sie den bisherigen und danach den neuen Sicherheitsschlüssel ein. Beim Systemstart können Sie jetzt beide Schlüssel verwenden, um die Partition zu entsperren.

5. Nur persönliche Daten verschlüsseln

Für stationäre PCs reicht es in der Regel aus, nur das Home-Verzeichnis zu verschlüsseln. Das empfiehlt sich vor allem bei Mehrbenutzer-PCs. Die Komplettverschlüsselung hat hier wenig Sinn, weil kein anderer Benutzer das System ohne Sicherheitsschlüssel entsperren könnte. Wer besonders sicherheitskritische Daten besitzt, kann jedoch die Installation verschlüsseln (Punkt 4) und zusätzlich auch noch das Home-Verzeichnis.

Um die Verschlüsselung zu aktivieren, setzen Sie bei der Ubuntu-Installation im Fenster „Wer sind Sie?“ ein Häkchen vor „Meine persönlichen Daten verschlüsseln“. Nach der ersten Anmeldung beim neu installierten System erscheint ein Fenster mit dem Hinweis „Ihre Verschlüsselungspassphrase notieren“. Klicken Sie auf „Diese Aktion ausführen“. Danach geben Sie das Anmeldepasswort ein und bestätigen mit der Eingabetaste. Sie sehen dann das von Ubuntu zufällig generierte Passwort für die Verschlüsselung. Notieren Sie dieses, denn Sie benötigen es im Problemfall vielleicht später einmal für die Wiederherstellung eines defekten Dateisystems.



Installation verschlüsseln: Mit dem selbst gewählten Sicherheitsschlüssel lässt sich die Ubuntu-Partition entsperren. Der Schlüssel sollte ausreichend komplex sein.

Für den Zugriff auf Ihr Home-Verzeichnis genügt die Anmeldung bei Ubuntu mit dem bei der Installation vergebenen Passwort. Die Entschlüsselung erfolgt dabei automatisch. Vor anderen Benutzern ist das verschlüsselte Home-Verzeichnis sicher. Diese erhalten beim Zugriff eine Fehlermeldung, die auf fehlende Rechte hinweist.

6. Erste Schritte nach der Installation

Auch für Linux gibt es häufig Updates, die Sicherheitslücken und Fehler im System sowie der installierten Software beseitigen. Meist meldet sich schon kurz nach der Installation die Aktualisierungsverwaltung und weist Sie auf verfügbare Updates hin. Klicken Sie einfach auf „Jetzt installieren“ und bestätigen Sie mit Ihrem Passwort. Zur Installation neuer Programme dient „Ubuntu Software“, das Sie über das Icon in der Menüleiste am linken Bildschirmrand erreichen. Sie können in Kategorien stöbern oder sich durch die Empfehlungen inspirieren lassen. Erfahrene Nutzer bevorzugen meist die Kommandozeile, weil sich darüber Software schneller aktualisieren oder neu installieren lässt.

In einem Terminalfenster genügen diese beiden Zeilen, um erst die Softwarelisten neu zu laden und dann das System mit Updates zu versorgen:

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

Die Installation eines neuen Programms erfolgt beispielsweise über *apt install synaptic*.

Bei Synaptic handelt es sich um eine alternative und übersichtliche Paketverwaltung, die vor allem bei der Suche in Paketbeschreibungen und nach Paketnamen nützlich ist.

Weitere Home-Verzeichnisse verschlüsseln

Sollen bei einem Mehrbenutzersystem auch die Daten anderer Benutzer verschlüsselt werden, dann erledigen Sie das über die Kommandozeile. Öffnen Sie ein Terminal und tippen Sie folgende Zeile ein:

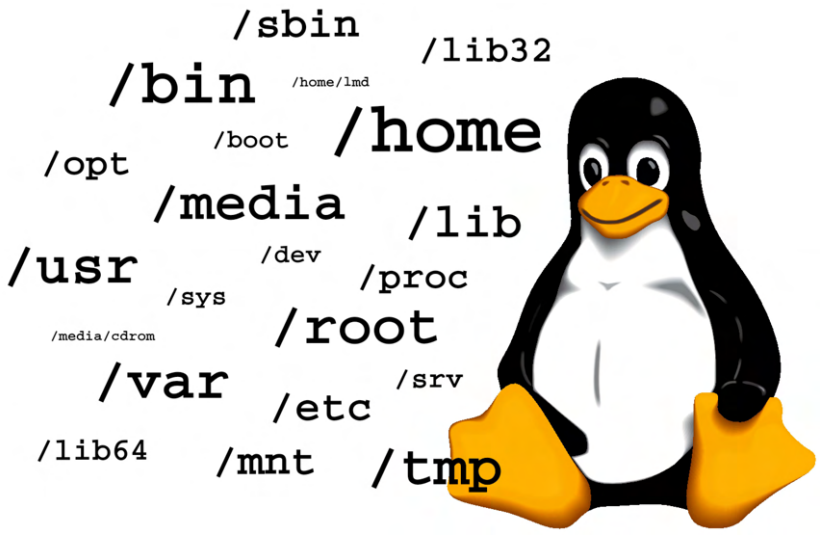
```
sudo adduser --encrypt-home [Benut
  zername]
```

„[Benutzername]“ ersetzen Sie durch den Kontonamen des Benutzers, den Sie neu erstellen möchten. Anschließend vergeben Sie das Passwort für den neuen Benutzer nach „Geben Sie ein neues UNIX-Passwort ein“: Geben Sie die Benutzerinformationen ein oder lassen Sie die Zeilen leer, indem Sie die Eingabetaste betätigen. Danach kann sich der neu angelegte Benutzer mit dem von Ihnen festgelegten Passwort anmelden und das verschlüsselte Home-Verzeichnis nutzen. Auch er erhält einen Hinweis, sich die Verschlüsselungspassphrase zu notieren.

Das Linux-Dateisystem

Laufwerksbuchstaben gibt es bei Linux nicht, dafür aber standardisierte Ordner in einem einzigen Verzeichnisbaum. Der grundlegende Aufbau ist bei allen Linux-Distributionen im Wesentlichen identisch.

Von **Thorsten Eggeling**



Für die Systemkonfiguration und die Fehlersuche sind Kenntnisse der Struktur des Linux-Dateisystems und der Rechteverwaltung hilfreich bis unentbehrlich. Es gibt Situationen, in denen Sie sich intensiver mit Ordnern und Zugriffsrechten befassen müssen, etwa wenn Sie eine weitere Festplatte einbinden und Dateien darauf auslagern möchten.

Die wichtigsten Verzeichnisse

Bei Linux liegen alle Verzeichnisse unterhalb von „/“, auch das Wurzel- oder root-Verzeichnis genannt. „root“ (englisch für „Wurzel“) ist hier nicht zu verwechseln mit dem administrativem Benutzer „root“, dessen Home-Verzeichnis unter „/root“ liegt.

Sie sehen alle vorhandenen Ordner, wenn Sie im Dateimanager etwa unter Ubuntu auf „Rechner“ klicken. Bei einer Standard- Linux-Installation liegen alle Ordner auf einer einzigen Partition, die in „/“ eingehängt ist (Mountpunkt).

„/bin“ und **„/sbin“** enthalten ausführbare Dateien (Binaries), die das System benötigt und die schon nach dem Start verfügbar sein müssen. Programme in „/sbin“ dienen zur Systemverwaltung und erfordern administrative Rechte.

„/boot“ enthält Dateien, mit welchen Linux zunächst bootet, also mindestens den Bootloader und den Kernel. Außerdem ist eine Ramdisk namens „initramrd“ vorhanden, die Dateien und Treiber für die Initialisierung des Systems enthält.

„/dev“ ist das Systemverzeichnis für Gerätedateien. Diese sind eine Besonderheit von Linux, denn sämtliche erkannten Geräte und deren Eigenschaften sind, strikt nach Unix-Philosophie, immer als Datei abgebildet.

„/etc“ beherbergt als zentrales Verzeichnis alle systemweiten Konfigurationsdateien. Hier liegen in weiteren Unterverzeichnissen und Einzeldateien die Einstellungen der Systemkomponenten und Serverdienste sowie diverse Voreinstellungen für Benutzer. Mit Dateien unter „/etc“ hat man bei der Administration eines Systems ständig zu tun.

„/home“ ist der Ordner, in dem man sich bei der täglichen Arbeit aufhält. Jeder Benutzer erhält unter „/home“ sein eigenes Verzeichnis, in dem er sämtliche Zugriffsrechte hat. Hier liegen sowohl die persönlichen Dateien und Dokumente als auch die persönlichen Konfigurationsdateien. Außer dem Besitzer und root hat niemand Schreibzugriff auf die Verzeichnisse unterhalb von „/home“.

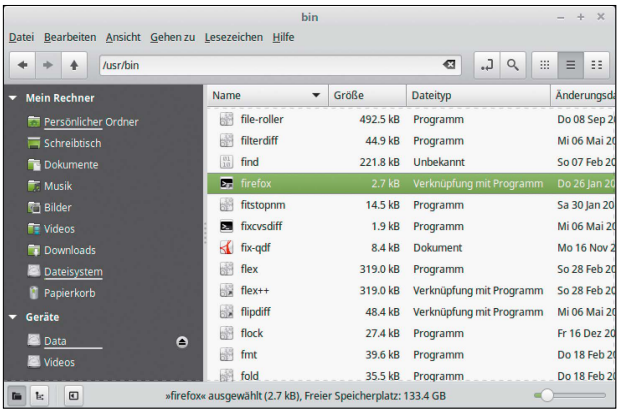
„/lib“ sowie **„/lib32“** und **„/lib64“** sind für Anwender kaum von Bedeutung. Hier lagert das System gemeinsam genutzte Programmbibliotheken.

„/media“ enthält Unterverzeichnisse mit automatisch eingehängten externen Datenträger – beispielsweise eingelegte DVDs oder angeschlossene USB-Sticks. „/mnt“ ist für den gleichen Zweck vorgesehen, wird aber von aktuellen Linux-Systemen nicht mehr verwendet.

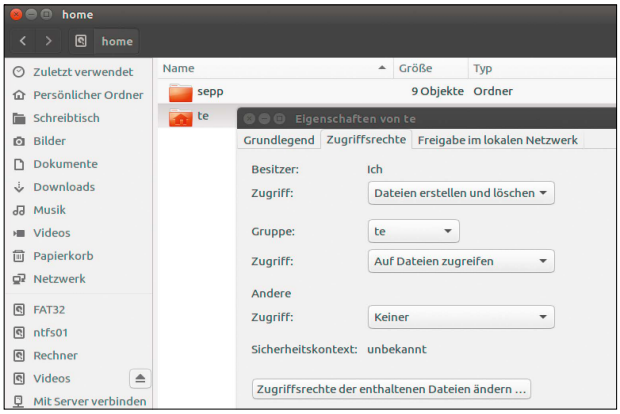
„/opt“ steht für „optional“ und ist der richtige Ort für nachträglich installierte Programme, die nicht zum Standardrepertoire einer Linux-Distribution in deren Paketquellen gehören.

„/proc“ und **„sys“** sind Verzeichnisse für spezielle Dateien, die das System selbst pflegt und aktive Prozesse abbilden. Jedes ausgeführte Programm legt hier eine Datei mit dem aktuellen Zustand ab. Zudem verbucht der Kernel in Einzeldateien wichtige Systeminfos.

„/tmp“ enthält nur temporäre Dateien, die während des Betriebs von Anwendungen entstehen und die anschließend verworfen werden können.



Programme: Unter „/usr/bin“ liegen die meisten Anwendungen. Standardbenutzer haben nur Leserechte, können also keine Dateien löschen oder ändern.



Nautilus unter Ubuntu: Sie können Berechtigungen für Ordner ändern und nach Klick auf „Zugriffsrechte der enthaltenen Dateien ändern“ auch für alle Dateien und Unterordner.

„/usr“ steht für „User System Resources“. Hier liegen vor allem unter „/usr/bin“ ausführbare Programme für das Terminalfenster und die grafische Oberfläche. Eine besondere Rolle spielen die Ordner unterhalb von „/usr/local“, in denen selbst kompilierte oder heruntergeladene Programme landen können. Anwendungen in „/usr/local/bin“ haben Vorrang vor denen in „/usr/bin“. Dadurch ist es möglich, aktualisierte Tools zu installieren und ohne Einfluss auf die Paketverwaltung zu verwenden.

„/var“ versammelt alle Dateien, die von Serverdiensten oder vom System selbst im laufenden Betrieb erstellt, beschrieben und eventuell auch wieder gelöscht werden, jedoch nicht nur temporär sind. Hier finden sich beispielsweise wichtige Logdateien, der Druckerspooler und die Arbeitsverzeichnisse eines Mailservers.

Zugriffrechte im Dateisystem

Als Standardbenutzer haben Sie nur Schreibrechte im Ihrem eigenen Home-Verzeichnis und im Ordner „/tmp“. In den meisten anderen Verzeichnissen besitzen Sie nur Leserechte, die auch nötig sind, um Programme etwa aus „/usr/bin/“ zu starten.

Unter Linux gehören Ordner und Dateien einem Benutzer („Eigentümer“) und einer Gruppe. Die eigenen Dateien unter „/home/sepp“ beispielsweise gehören dem Benutzer „sepp“ und der gleichnamigen Gruppe. Für jedes Element im Dateisystem lassen sich Lese- und Schreibrechte vergeben, getrennt nach Eigentümer und Gruppe. Zudem gibt es das Recht „Ausführen“. Ist es bei einer Datei gesetzt, darf ein Benutzer sie als Programm starten. Bei Ordnern gewährt es die Berechtigung, ihn zu öffnen beziehungsweise den Inhalt anzusehen.

Außerdem lassen sich Rechte für „Andere“ festlegen. Damit sind Zugriffe von Benutzern gemeint, die weder Eigentümer sind noch zu der festgelegten Gruppe gehören.

Rechte über den Dateimanager ändern

Welche Rechte für einen Ordner oder eine Datei gelten, lässt sich über einen Dateimanager ermitteln – unter Ubuntu etwa mit Nautilus.

Nutzer von Linux Mint können den Dateimanager Nemo per Doppelklick auf das Desktopsymbol „Persönlicher Ordner“ öffnen. Gehen Sie auf „Rechner“ (Ubuntu) beziehungsweise „Dateisystem“ (Linux Mint) und dann in den Ordner „home“. Klicken Sie Ihr Home-Verzeichnis mit der rechten Maustaste an, wählen Sie „Eigenschaften“ und dann die Registerkarte „Zugriffsrechte“.

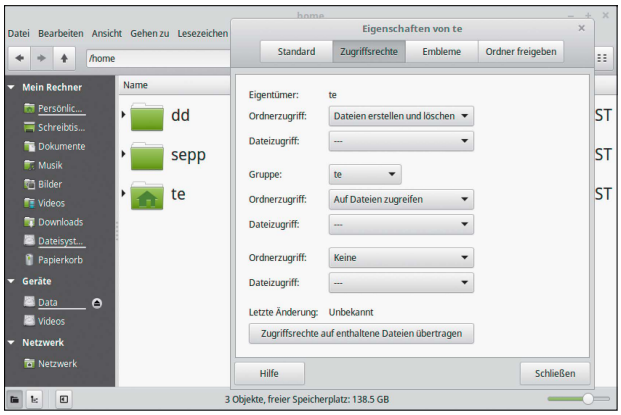
In Nautilus können Sie hinter „Zugriff“ die Rechte für „Besitzer“, „Gruppe“ und „Andere“ festlegen. Sie haben die Wahl zwischen „Dateien nur auflisten“ (lesen), „Auf Dateien zugreifen“ (ausführen/suchen) und „Dateien erstellen und löschen“ (schreiben). Bei „Gruppe“ und „Andere“ gibt es zudem „Keiner“, was den Zugriff für beide unterbindet. Das Recht „Dateien nur auflisten“ führt bei Ordnern effektiv ebenfalls dazu, dass ein Zugriff auf den Inhalt nicht möglich ist.

Sie werden bemerken, dass bei den Zugriffsrechten für „Andere“ der Wert „Auf Dateien zugreifen“ eingestellt ist. Andere Benutzer können daher den Inhalt fremder Home-Verzeichnisse einsehen und Dateien öffnen, aber nicht verändern. Wenn Sie das nicht möchten, setzen Sie für Ihr Benutzerverzeichnis die Rechte für „Andere“ hinter „Zugriff“ auf „Keiner“.

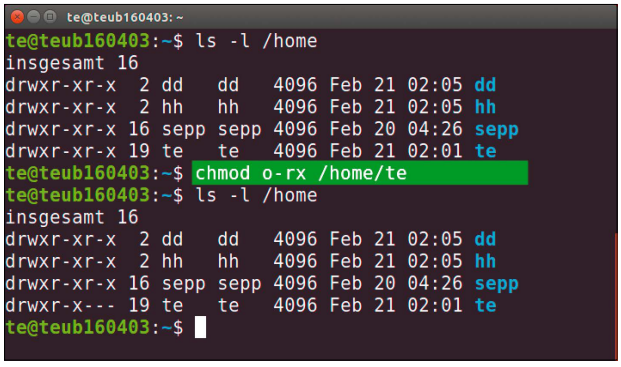
Über die Schaltfläche „Zugriffsrechte der enthaltenen Dateien ändern“ lassen sich bei Ordnern in einem eigenen Dialog die Rechte auch rekursiv für alle enthaltenen Elemente setzen – für „Besitzer“, „Gruppe“ und „Andere“ jeweils getrennt für die enthaltenen Dateien und Ordner.

Bei Linux Mint funktioniert die Rechtevergabe über den Dateimanager Nemo ähnlich, das Fenster „Eigenschaften -> Zugriffsrechte“ sieht nur etwas anders aus.

Es gibt die drei Rubriken „Eigentümer“, „Gruppe“ und „Andere“, bei der letzten fehlt allerdings die Beschriftung. Hinter „Ordnerzugriff“ stellen Sie wie bei Ubuntu die Zugriffsrechte



Nemo unter Linux Mint: Die Registerkarte „Zugriffsrechte“ zeigt mehr Optionen als bei Ubuntu, weil Sie hier auch die Rechte für die enthaltenen Elemente festlegen können.



Kommandozeile: Mit Hilfe des Tools chmod legen Sie die Zugriffsrechte für Dateien und Ordner fest. Mit ls -l kontrollieren Sie die geltenden Rechte.

ein. Zusätzlich gibt es Auswahlfelder hinter „Dateizugriff“. Einstellungen, die Sie hier vornehmen, gelten zusammen mit denen hinter „Ordnerzugriff“ für alle Unterordner und Dateien, wenn Sie die Option „Zugriffsrechte auf enthaltene Dateien übertragen“ verwenden.

Rechte auf der Kommandozeile festlegen

Das Terminal kann die Zugriffsrechte schneller festlegen als grafische Dateimanager. Mit dem Befehl

```
ls -l /home
```

lassen Sie sich die Zugriffsrechte, Besitzer und Gruppen anzeigen.

In der ersten Spalte symbolisiert das vorangestellte „d“ Verzeichnisse („directory“). Direkt dahinter folgen die Rechte für „Benutzer“, „Gruppe“ und „Andere“. Eine Ausgabe wie „drwxr-x---“ bedeutet Lesen („r“), Schreiben („w“) und Ausführen/Suchen („x“) für den Benutzer.

Die Gruppe darf lesen sowie ausführen/suchen („r-x“), „Andere“ haben keinen Zugriff („---“).

Mit dem Befehl chmod ändern Sie die Rechte:

```
chmod o+rx /home/sepp
```

„Andere“ („o“) dürfen dann auf das Verzeichnis zugreifen und Dateien lesen. Wenn Sie die Rechte für Dateien/Ordner ändern möchten, die nicht Ihnen gehören, stellen Sie diesem und allen folgenden Befehlen ein „sudo“ voran. Mit

```
chmod o-rx /home/sepp
```

entfernen Sie die Berechtigungen wieder. Entsprechend setzen Sie „u“ für Benutzer und „g“ für Gruppe ein.

```
chmod g+rw /home/sepp/Datei.txt
```

gibt der Gruppe Lese- und Schreibzugriff für eine Datei.

Der Besitzer einer Datei lässt sich mit dem Befehl chown ändern. Die allgemeine Form lautet

```
sudo chown [User] [Datei/Ordner]
```

Die Befehle chmod, chgrp und chown verarbeiten die zusätzliche Option „-R“. Der Befehl

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

ändert bei allen Elemente unterhalb des angegeben Pfades den Eigentümer auf den Benutzer „sepp“.

Zusätzliche Festplatten und Rechte

Externe USB-Laufwerke, die mit dem Dateisystem NTFS oder FAT32 formatiert sind, erscheinen automatisch im Dateimanager. Jeder Benutzer hat darauf Lese- und Schreibzugriff. Wenn Sie jedoch mehr Speicherplatz für Dateien benötigen, eine neue Festplatte in den PC einbauen und diese mit dem Linux-Dateisystem Ext4 formatieren, erhalten Sie standardmäßig nur Lesezugriff. Das Problem lässt sich lösen, indem Sie das Tool gnome-disks verwenden. Damit können Sie Festplatten formatieren und die Art der Einbindung in das Dateisystem ändern.

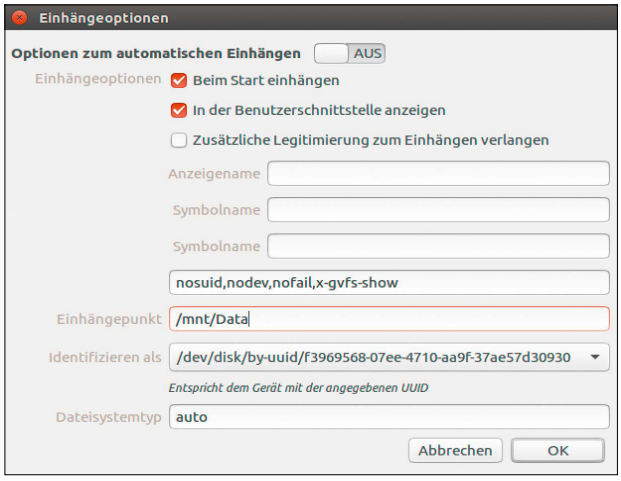
Nutzer von Linux Mint starten das Tool über „Zubehör -> Laufwerke“, unter Ubuntu suchen Sie im Dash nach „Laufwerke“. Auf der linken Seite des Fensters wählen Sie die neue Festplatte aus, klicken dann im rechten Bereich des Fensters auf die Schaltfläche mit dem Zahnradsymbol und wählen im Menü „Partition formatieren“. Hinter „Typ“ wählen Sie „Kompatibel mit Linux-Dateisystem (Ext4)“ und hinter „Name“ geben Sie eine aussagekräftige Bezeichnung ein, beispielsweise „Data“. Klicken Sie auf „Formatieren“, danach erneut auf „Formatieren“ und bestätigen Sie den Vorgang mit Ihrem Passwort. Über die „Play“-Schaltfläche neben dem Zahnradsymbol lässt sich die neue Partition in das Dateisystem unterhalb von „/media/[User]/Data“ einbinden. Wenn Sie sich die Zugriffsrechte über den Dateimanager ansehen, stellen Sie fest, dass der Ordner danach Ihnen gehört und nur Sie Vollzugriff haben.

Mehrbenutzersystem: Damit auch andere Nutzerkonten das Laufwerk nutzen können, hängen Sie die Partition über die „Stop“-Schaltfläche wieder aus. Klicken Sie auf das Zahnradsymbol und auf „Einhängeoptionen bearbeiten“. Setzen Sie den Schalter hinter „Optionen zum automatischen Einhängen“ auf „Aus“. Hinter „Einhängepunkt“ geben Sie das gewünschte Verzeichnis an, beispielsweise „/mnt/Data“. Das Verzeichnis muss nicht exi-

stieren, es wird automatisch angelegt. Klicken Sie auf die „Play“-Schaltfläche, um das Laufwerk in das Dateisystem einzubinden.

Das alleine genügt jedoch noch nicht, denn das Verzeichnis „/mnt/Data“ gehört auch jetzt dem Benutzer, der es angelegt hat. Damit auch andere Benutzer des PCs auf die Dateien zugreifen können, gehen Sie im Dateimanager auf „/mnt/Data“. Wählen im Kontextmenü „Eigenschaften“ und gehen auf die Registerkarte „Zugriffsrechte“. Ändern Sie für „Andere“ hinter „Zugriff“ die Einstellung in „Auf Dateien zugreifen“.

Soll auch der Schreibzugriff möglich sein, könnten Sie im Prinzip „Dateien erstellen und löschen“ wählen. Das hat jedoch einen gravierenden Nachteil: Legt ein Benutzer Ordner oder Dateien an, dann gehören diese ihm – allen anderen Benutzern fehlt dann der Schreibzugriff. Um das zu ändern, steuern Sie den Zugriff über die Gruppenzugehörigkeit und Access Control Lists (kurz ACL). Das dafür nötige Tool setfacl ist unter Ubuntu 16.04 und Linux Mint 18.x standardmäßig installiert. Führen Sie im Terminal folgende fünf Befehlszeilen aus:



Festplatten verwalten: In den „Einhängeoptionen“ von gnome-disks („Laufwerke“) legen Sie fest, über welchen Ordner im Dateisystem Sie auf das Laufwerk zugreifen können.

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

Damit erstellen Sie das Verzeichnis „/mnt/Data/Projekte“ für den Datenaustausch.

Es gehört der Gruppe „plugdev“, die Vollzugriff erhält. „chmod g+s“ bewirkt, dass die Gruppe erhalten bleibt, wenn ein Benutzer neue Dateien oder Ordner anlegt. Mit setfacl setzten Sie die Standardzugriffsrechte, die auf alle enthaltenen und zukünftigen Elemente vererbt werden.

Im Ergebnis erhalten alle Mitglieder der Gruppe „plugdev“ Lese- und Schreibzugriff, andere Benutzer nur eine Leseberechtigung.

Nun müssen Sie nur noch alle Benutzer, die Schreibzugriff erhalten sollen, zur Gruppe hinzufügen:

```
sudo usermod -aG plugdev [User]
```

Den Platzhalter „[User]“ ersetzen Sie durch den gewünschten Benutzer.

Ordner auf eine andere Festplatte auslagern

Unter Linux spielt es keine Rolle, auf welcher Festplatte oder Partition ein Verzeichnis tatsächlich liegt. Wenn der Platz knapp wird, können Sie einen Ordner wie „/home“ jederzeit von einem anderen Laufwerk einbinden. Voraussetzung dafür ist, dass Sie bereits eine zweite Festplatte wie im Punkt „Zusätzliche Festplatten und Rechte“ beschrieben unter „/mnt/Data“ eingebunden haben. Es genügt, dass Sie für „Andere“ hinter „Zugriff“ das Recht „Auf Dateien zugreifen“ eingestellt haben. ACLs verwenden Sie hier nicht, weil unter „/home“ jeder Benutzer in der Regel nur auf seine eigenen Dateien zugreifen muss.

Beenden Sie alle Programme und öffnen Sie ein Terminal. Unter Linux Mint beenden Sie mit

```
sudo service mdm stop
```

die grafische Oberfläche, unter Ubuntu-Nutzer mit diesem Befehl:

```
sudo service lightdm stop
```

Sie befinden sich jetzt auf einer Textkonsole, bei der Sie sich mit Ihrem Benutzernamen anmelden. Das Passwort tippen Sie blind ein, es wird nicht angezeigt. Sollte die Konsole nicht zu sehen sein, drücken Sie Alt-F1.

Als Erstes kopieren Sie die Home-Verzeichnisse auf die zweite Festplatte:

```
sudo rsync -aXS /home/ /mnt/Data/home/
```

Dann benennen Sie das Verzeichnis „/home“ um und legen ein neues Verzeichnis an:

```
mv /home /home.bak
mkdir /home
```

Laden Sie dann die Filesystem-Tabelle in den Editor nano:

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

Im Editor fügen Sie die Zeile

```
/mnt/Data/home /home bind defaults,bind 0 0
```

ein. Damit konfigurieren Sie die Verbindung von „/mnt/Data/home“ auf der neuen Festplatte mit dem Ordner „/home“ auf der Systemfestplatte.

Drücken Sie Strg-X und bestätigen Sie mit „j“ und Eingabetaste. Mit dem Befehl

```
sudo mount -a
```

hängen Sie den Ordner in das Dateisystem ein. Danach führen Sie mit *sudo reboot* einen Neustart durch.

Drucker und Scanner

Die meisten Drucker, Scanner und Multifunktionsgeräte lassen sich auch unter Linux problemlos verwenden. Mehrere Hersteller bieten für die optimale Nutzung aller Funktionen auch eigene Software an.

Von **Thorsten Eggeling**



Vor allem bei weitverbreiteten Geräten der Marktführer HP, Canon und Epson stehen die Chancen gut, dass sich ein Drucker oder Multifunktionsgerät auch unter Linux ohne Aufwand in Betrieb nehmen lässt. Mit den Standardtreibern gibt es teilweise Einschränkungen, die sich aber meist durch die Installation eines Treibers vom Hersteller beheben lassen. Allerdings bieten nicht alle Hersteller eine optimale Unterstützung für Linux an. Bevor Sie ein neues Gerät kaufen, sollten Sie im Internet nach den Erfahrungen anderer Linux-Nutzer suchen.

1. Das Linux-Drucksystem Cups

Unter Linux kommt standardmäßig das Drucksystem Cups zum Einsatz (Common Unix Printing System, *www.cups.org*). Es enthält Druckertreiber und Software für die Konfiguration. Cups ist in einer Client-Server-Architektur aufgebaut. Der Druckclient schickt die Druckaufträge, ein Druckserver erledigt das Drucken auf dem Rechner, an dem der Drucker angeschlossen ist. Seit 2007 gehört Cups zu Apple, denn das Drucksystem wird auch unter Mac-OS verwendet.

Im November 2017 hat Apple beschlossen, die Software mit Erscheinen der Version 2.3 unter die Apache-Lizenz zu stellen.

2. Drucker mit Standardtools einrichten

Linux erkennt viele Drucker am USB-Anschluss und im Netzwerk automatisch und der passende Treiber wird ebenfalls automatisch eingerichtet. Zur Konfiguration suchen Sie bei Ubuntu 16.04 im Dash oder bei Linux Mint 18 im Startmenü nach „Drucker“. Wurde der USB-Drucker automatisch erkannt, taucht er im Fenster „Drucker - localhost“ auf. Andernfalls klicken Sie auf „Hinzufügen“. Ein USB-Drucker sollte in der Liste unter „Geräte“ erscheinen. Wenn nicht, prüfen Sie die USB-Verbindung. Klicken Sie den Eintrag für den Drucker an und dann auf „Weiter“ und „Anwenden“. Sollte kein Treiber für das Druckermodell vorinstalliert, aber ein Herstellertreiber verfügbar sein, bietet Ihnen der Assistent teilweise Download und Installation an. Auf der linken Seite des Fensters tauchen unter „Netzwerkdrucker“ alle Geräte automatisch auf, die über eine eigene Netzwerkschnittstelle verfügen. Auch hier hilft Ihnen der Assistent bei der Treibereinrichtung, wenn diese nicht schon automatisch erfolgt ist.

Ist der Drucker an einem Linux- oder Windows-PC über Samba freigegeben, gehen Sie auf „Windows-Drucker via SAMBA“ und klicken auf „Auswählen“. Im Fenster „SMB-Browser“ wählen Sie den gewünschten Server und Drucker aus.

Wenn die Freigabe mit einem Passwort gesichert ist, müssen Sie Benutzername und Passwort eingeben, bevor Sie den Drucker auswählen können. Klicken Sie auf „OK“ und dann auf „Weiter“. Der Rest läuft wie bei der Installation eines lokal angeschlossenen Druckers ab.

Drucker konfigurieren: Sobald Drucker installiert sind, können Sie im Fenster „Drucker - localhost“ beim gewünschten Gerät im Kontextmenü auf „Einstellungen“ gehen. Unter „Einstel-

Linux-Treiber:
Downloads & Infos

Hersteller	Internetadresse
Brother	*www.pcwelt.de/AOve2K*
Canon	*www.canon.de/support*
Epson	*www.pcwelt.de/po1lvX*
HP	*www.pcwelt.de/Zli0pr*
Samsung	*www.pcwelt.de/k8FAyA*
Lexmark	*http://goo.gl/mUwc6e*

lungen“ lassen sich bei Bedarf die Beschreibung und die Geräteadresse ändern. Sehen Sie sich den Eintrag hinter „Marke und Modell“ an. Wenn hier bei einem HP-Drucker in der Zeile „requires proprietary plugin“ auftaucht, müssen Sie ein zusätzliches Plug-in installieren (siehe -> Punkt 4).

Bei „Zugriffskontrolle“ bestimmen Sie, welche Benutzer den Drucker verwenden dürfen. Standardmäßig ist der Zugriff für alle Benutzerkonten erlaubt. Was unter „Druckeroptionen“ erscheint, hängt vom Typ des Druckers und vom Treiber ab. Meist können Sie wenigstens die Papiergröße und die Druckqualität einstellen. Die Rubrik „Tinten-/Tonerfüllstand“ liefert Informationen zum Verbrauchsmaterial, sofern der Treiber das unterstützt. Hier finden Sie unter „Statusmeldungen“ aber auch Hinweise zu möglichen Fehlern beim Ausdruck.

Tipp: Drucker lassen sich auch über die Cups-Weboberfläche hinzufügen und konfigurieren. Dazu rufen Sie im Browser die URL „http://localhost:631“ auf. Wie Sie den Zugriff für andere Rechner im eigenen Netzwerk erlauben, lesen Sie in -> Punkt 5.

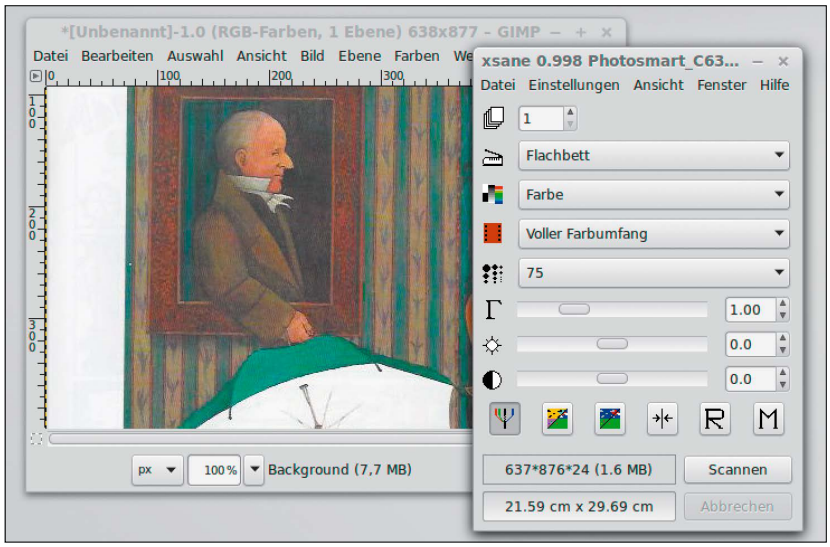
3. Scanner einrichten und nutzen

Scanner funktionieren unter Linux oft ohne spezielle Treiber. Bei Ubuntu und Linux Mint sind die nötigen Pakete „libsane“ und „simple-scan“ bereits vorinstalliert. Beim Start erkennt das Programm Simple Scan den Scanner automatisch.

Eine Liste mit Geräten, die Sane standardmäßig unterstützt, finden Sie unter *http://www.sane-project.org/sane-mfgs.html*. Wenn Sie ein Multifunktionsgerät oder einen Scanner von HP oder Epson besitzen, installieren Sie die Treiber wie in -> Punkt 4 beschrieben. Simple Scan ist ein sehr einfaches Basisprogramm. Es genügt für das gelegentliche Einlesen von Belegen oder Bildern. Deutlich mehr Optionen bietet die Alternative Xsane, die Sie im Terminal mit

```
sudo apt install xsane
```

nachinstallieren.



Drucker installieren: Meist erkennt Linux USB- und Netzwerkdrucker automatisch. Wenn nicht, wählen Sie das gewünschte Gerät nach einem Klick auf „Hinzufügen“ aus.

4. Herstellertreiber installieren

Wenn sich Drucker oder Scanner nicht ansprechen lassen, benötigen Sie einen Treiber vom Gerätehersteller. Diesen finden Sie über eine Suche im Downloadbereich des Herstellers (siehe Tabelle „Linux-Treiber“).

Wir zeigen in diesem Artikel beispielhaft, wie Sie Treiber und Software für Geräte von Epson und HP installieren. Ausführliche Anleitungen für Geräte anderer Hersteller finden Sie unter *https://wiki.ubuntuusers.de/Drucker* und *https://wiki.ubuntuusers.de/Scanner*.

Epson-Geräte einrichten: Epson-Treiber finden Sie über *www.pcwelt.de/po1lvX*. Tippen Sie dort den Produktnamen des Epson-Druckers, Scanners oder Multifunktionsgerätes ein. Wir verwenden als Beispiel „XP-225“ (Drucker/Scanner-Kombi). Unter Betriebssystem wählen Sie „Linux“. Nach einem Klick auf die Schaltfläche mit dem Lupensymbol sehen Sie eine Seite, die drei Downloads anbietet. Klicken Sie bei „ESC/P-R Driver (generic driver)“ und „Epson Printer Utility“ jeweils auf „Download“ und dann unten auf der Seite auf „Accept“. Sie se-

Linux-Druckerfreigabe unter Windows

Windows erkennt über Cups freigegebene Drucker in der Regel nicht automatisch. Unter Windows 8.1 gehen Sie in der Systemsteuerung auf „Geräte und Drucker“. Klicken Sie auf „Drucker hinzufügen“ und dann auf „Der gesuchte Drucker ist nicht aufgeführt“. Wählen Sie die Option „Freigegebenen Drucker über den Namen auswählen“ und geben Sie darunter eine Adresse in der folgenden Form

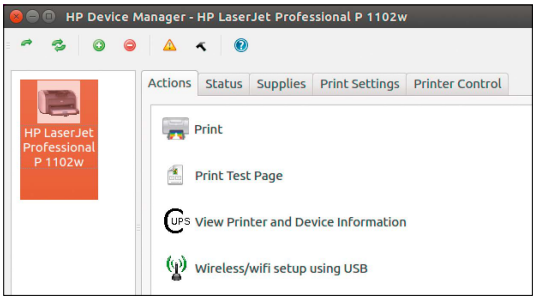
```
http://[Server]/printers/[Druckerna
me]
```

ein. Ersetzen Sie den Platzhalter „[Server]“ durch den Namen oder die IP-Adresse des Linux-Druckservers. Für „[Druckername]“ setzen Sie die Bezeichnung ein, die in der Linux-Konfiguration vergeben ist. Windows fragt dann nach dem Treiber für den Drucker. Sollte dieser in der Liste nicht erscheinen, installieren Sie den Windows-Treiber des Herstellers.

Unter Windows 10 rufen Sie die „Einstellungen“ auf (Win-I), klicken auf „Geräte“ und dann auf „Drucker & Scanner“. Klicken Sie auf „Drucker oder Scanner hinzufügen“ und danach auf „Der gewünschte Drucker ist nicht aufgelistet“. Danach geht es weiter wie unter Windows 8.1 (siehe Anfang des Kastens).



Software für Epson-Scanner: Image Scan for Linux können Sie kostenlos bei Epson herunterladen. Über das Programm lässt sich der Scanner bequem konfigurieren.



HP-Drucker verwalten: HP liefert mit dem Device Manager ein umfangreiches Tool, über das Sie Drucker einrichten und fast alle Optionen des Druckers einstellen können.

hen dann Downloadlinks für RPM-Pakete (Fedora, Open Suse) und DEB-Pakete (Ubuntu, Linux Mint). Für unser 64-Bit-Ubuntu-System laden wir die Dateien „epson-inkjet-printer-escpr_1.6.17-1lsb3.2_amd64.deb“ und „epson-printer-utility_1.0.2-1lsb 3.2_amd64.deb“ herunter. Auf der Downloadseite für den Scannertreiber finden Sie nach einem Klick auf „Accept“ zunächst nur eine englischsprachige Anleitung im PDF-Format. Klicken Sie auf „Package Download Page“ und laden Sie das Treiber- und Softwarepaket herunter, für Ubuntu beispielsweise die Datei „iscan-bundle-1.0.4.x64.deb.tar.gz“.

Die beiden DEB-Dateien installieren Sie einfach per Doppelklick im Dateimanager. „iscan-bundle-1.0.4.x64.deb.tar.gz“ entpacken Sie über den Kontextmenüpunkt „Hier entpacken“. Dann öffnen Sie ein Terminalfenster und wechseln mit dem Befehl cd in das Verzeichnis, in das Sie die Datei entpackt haben. Tippen Sie folgende Befehlszeile ein, um die Software Image Scan for Linux zu installieren:

```
sudo ./install.sh
```

Richten Sie anschließend den Drucker wie in Punkt 2 beschrieben ein. Für den Scanner verwenden Sie das Programm Simple Scan oder für mehr Funktionen das Epson-Tool Image Scan for Linux.

Wenn Sie das Epson-Gerät nicht per USB, sondern über das Netzwerk ansprechen, findet Image Scan for Linux den Scanner nicht. Um das zu ändern, öffnen Sie die Konfigurationsdatei in einem Editor:

```
sudo nano /etc/sane.d/epkowa.conf
```

In der Datei gibt es einen Beispielabschnitt für die Netzwerkkonfiguration. Hier fügen Sie folgende Zeile ein:

```
net [IP-Adresse]
```

Den Platzhalter „[IP-Adresse]“ ersetzen Sie hier durch die tatsächliche IP Ihres Epson-Gerätes.

HP-Geräte einrichten: Die Software Linux Imaging and Printing (HPLIP) ist unter Ubuntu/Mint standardmäßig installiert und deckt einen Großteil der HP-Geräte ab. Über *www.pcwelt.de/wrAkL4* können Sie eine Geräteliste abrufen. In der Spalte „Min. HPLIP“ erfahren Sie, welche HPLIP-Version mindestens für ein Gerät erforderlich ist. Sollte in der Spalte „Driver Plug-in“ der Vermerk „Required“ stehen, müssen Sie ein zusätzliches Plug-in installieren, damit der Drucker funktioniert. Bei „Optional“ trägt das Plug-in zur Funktionsverbesserung bei. Ermitteln Sie in einem Terminalfenster, welche HPLIP-Version installiert ist:

```
dpkg -l hplip
```

HPLIP aktualisieren: Sollte für Ihr Druckermodell ein Update nötig sein, gehen Sie auf *https://developers.hp.com/hp-linux-imaging-and-printing* und klicken auf „Download HPLIP“. Wählen Sie die Linux-Distribution, für unser Beispiel „Ubuntu“, und klicken Sie auf „Download HPLIP“. Im Terminalfenster starten Sie dann die Installation mit

```
sh ~/Downloads/hplip-3.17.11.run
```

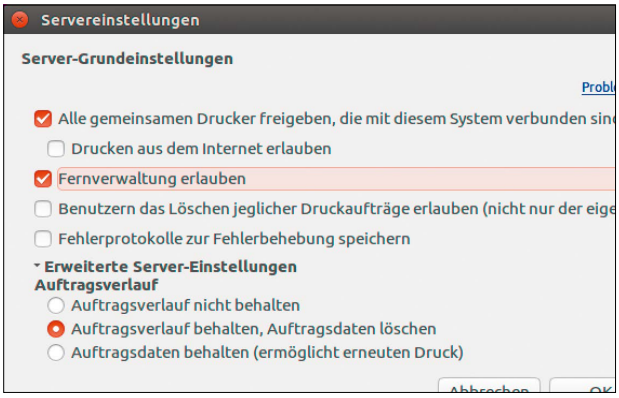
Passen Sie den Pfad und Dateinamen an. Folgen Sie dann den Anweisungen des Assistenten. Er lädt die nötigen Abhängigkeiten herunter, entfernt die vorinstallierte HPLIP-Version und richtet die neue Version ein. Im letzten Schritt werden Sie aufgefordert, Linux neu zu starten.

Klicken Sie auf das HP-Icon in der Leiste am oberen Bildschirmrand und gehen Sie auf „HP Device Manager“. Über das Tool können Sie eine Testseite ausdrucken und den Drucker konfigurieren.Sollte ein Plug-in erforderlich sein, erscheint nach der Linux-Anmeldung, wenn Sie den Drucker verbinden oder spätestens, wenn Sie die Testseite ausdrucken, eine Nachricht des Plug-in-Installers. Klicken Sie auf „Next“ und folgen Sie den Anweisungen des Assistenten. Danach ist der Drucker einsatzbereit.

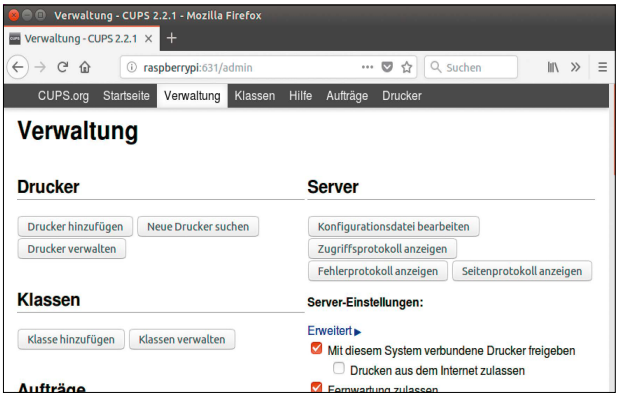
Vorinstalliertes HPLIP verwenden: Wenn die vorhandene HPLIP-Version für Ihr Gerät ausreicht, genügt in der Regel die Druckerinstallation wie in -> Punkt 2 beschrieben. Sollte ein benötigtes HP-Plug-in fehlen, ist es am einfachsten, die Verwaltungsoberfläche zu installieren:

```
sudo apt install hplip-gui
```

Starten Sie Linux neu und richten Sie das Zusatz-Plug-in ein wie oben beschrieben.



Druckerfreigabe: In den „Server-Grundeinstellungen“ aktivieren Sie die Freigabe der Drucker und die „Fernverwaltung“ .



Cups konfigurieren: Der Druckserver lässt sich über eine Weboberfläche verwalten. Sie können hier auch neue Drucker hinzufügen.

5. Drucker im Netzwerk freigeben

Um einen Drucker für andere Linux- oder Windows-PCs über das Netzwerk bereitzustellen, gehen Sie in den Systemeinstellungen auf „Drucker“. Im Hauptmenü, bei Ubuntu 16.04 am oberen Bildschirmrand, gehen Sie auf „Server -> Einstellungen“. Setzen Sie ein Häkchen vor „Alle gemeinsamen Drucker freigeben, die mit dem System verbunden sind“. Setzen Sie bei Bedarf außerdem ein Häkchen vor „Fernwartung erlauben“, damit andere PCs im Netzwerk die Cups-Weboberfläche aufrufen können. In den Eigenschaften der einzelnen Drucker gibt es unter „Richtlinien“ die standardmäßig aktivierte Option „Freigegeben“. Entfernen Sie das Häkchen, um einen Drucker von der Freigabe auszuschließen. Die Freigaben gelten für alle Drucker unabhängig von der Art des Anschlusses (USB- und Netzwerkdrucker).

Unter Linux erscheinen über Cups freigegebene Drucker in der Regel automatisch in den Systemeinstellungen unter „Drucker“. Wenn nicht, richten Sie ihn ein wie in -> Punkt 2 beschrieben.

6. Raspberry Pi als Druckserver nutzen

Wer einen Raspberry Pi im Netzwerk unter Raspbian oder OSMC als Datei- oder Medienserver betreibt, kann auch einen Druckserver darauf einrichten. Für diese Aufgabe ist sogar ein Raspberry Pi Zero ausreichend. Die nachstehende Beispielkonfiguration ist aber nicht auf Raspbian beschränkt, sondern funktioniert so sinngemäß auch bei anderen Linux-Systemen.

Für HP-Drucker ist unter Raspbian Jessie allerdings kein Drucker-Plug-in für die ARM-Architektur verfügbar. Sollten Sie darauf angewiesen sein, müssen Sie das aktuellere Raspbian Stretch installieren (*www.raspberrypi.org/downloads/raspbian*). Einen Überblick über Strech liefert der Beitrag unter *http://bit.ly/2FICCBv.*

Installieren Sie zuerst Cups in einem Terminalfenster und geben Sie dann dem Standardbenutzer „pi“ die Zugriffsrechte:

```
sudo apt install cups
sudo usermod -a -G lpadmin pi
```

Wenn Sie OSMC verwenden, ersetzen Sie den Benutzernamen „pi“ durch „osmc“. Öffnen Sie die Cups-Konfigurationsdatei mittels des Befehls

```
sudo nano /etc/cups/cupsd.conf
```

im Editor. Tragen Sie am Anfang der Datei diese zwei Zeilen ein:

```
DefaultEncryption Never
DefaultAuthType None
```

Bei den drei „<Location...>“-Blöcken ergänzen Sie jeweils die Konfiguration mit der folgenden Zeile

```
Allow @LOCAL
```

In der Zeile

```
Listen localhost:631
```

ersetzen Sie „localhost“ durch „0.0.0.0.“. Starten Sie Cups danach neu:

```
service cups restart
```

Rufen Sie nun im Webbrowser auf einem beliebigen PC im Netzwerk die Adresse

```
http://[Raspi]:631
```

auf. Den Platzhalter „[Raspi]“ ersetzen Sie durch den Namen oder die IP-Adresse Ihres Raspberry Pi. Gehen Sie auf „Verwaltung“ oder „Administration“ (je nachdem, was angezeigt wird). Setzen Sie ein Häkchen vor „Mit diesem System verbundene Drucker freigeben“ und klicken Sie auf „Einstellungen ändern“. Klicken Sie dann auf „Drucker hinzufügen“. Wenn Sie zur Anmeldung aufgefordert werden, verwenden Sie den Namen des Pi-Standardbenutzers („pi“ oder „osmc“) und sein Passwort.

Die weitere Konfiguration entspricht in etwa der unter Ubuntu (siehe -> Punkt 2). Wählen Sie einen per USB angeschlossenen oder einen Netzwerkdrucker und klicken Sie auf „Weiter“. Vergeben Sie eine Bezeichnung für den Drucker oder übernehmen Sie die Vorgabe. Setzen Sie ein Häkchen vor „Diesen Drucker im Netz freigeben“ und nach Klick auf „Weiter“ wählen Sie das Druckermodell. Klicken Sie auf „Drucker hinzufügen“, ändern Sie bei Bedarf die Werte hinter „Media Size“ und „Print Quality“. Danach klicken Sie auf „Standardeinstellungen festlegen“. Für HP-Drucker sollten Sie auch in Raspbian HPLIP nutzen. Zur Installation führen Sie diese Befehlszeile aus:

```
sudo apt install hplip
```

Das fehlende Drucker-Plug-in installieren Sie ab HPLIP-Version 3.15.4 bei Bedarf mit

```
sudo hp-plugin -i
```

nach. ●

Linux-Hürden für Umsteiger überwinden

Linux ist anders als Windows. Wer bisherigen Windows-Nutzern allein mit der Wahl des richtigen Linux ein Quasi-Windows verspricht, unterschlägt strategische und technische Hürden. Das Wichtigste bespricht dieser Beitrag.

Von **Hermann Apfelböck**



Ubuntu mit Gnome: Der innovative Desktop ist auf einfache Bedienung mit wenigen Mausklicks ausgelegt. Beste konservative Alternative ist Linux Mint mit Cinnamon.

Da es hier um Linux für Windows-Umsteiger geht, geht es logischerweise um Desktopsysteme für PCs und Notebooks. Die großartigen Möglichkeiten, die Linux (und zwar nur Linux) auf kleinen Servern eröffnet, bleiben komplett außen vor. Klipp und klar: Linux kann Windows auf dem Desktop ersetzen – aber nicht überall und nicht immer ohne Hindernisse.

1. Die Vielfalt der Distributionen

Für Windows-Umsteiger ist der artenreiche Linux-Zoo undurchsichtig: Es gibt eine dreistellige Anzahl von Linux-Varianten (*http://distrowatch.com*). Empfehlungen mit dem Motto „Das beste Linux für Windows-Umsteiger" sind nicht verkehrt, aber zu relativieren. Solche Aussagen insinuieren, dass die Wahl des richtigen Systems alle Umstiegsprobleme aus dem Weg räume. Richtig ist, dass manche Distributionen für Einsteiger überhaupt nicht in Betracht kommen, weil Installation, Konfiguration, Oberfläche oder alles zusammen unzumutbare Anforderungen stellen würden. Richtig ist ferner, dass Windows-Umsteiger sich nicht auf Linux-Exoten einlassen sollten: Die Nachhaltigkeit solcher Projekte ist ungewiss und eine heute hochgelobte Neuerscheinung kann zwei Jahre später eingestellt sein.

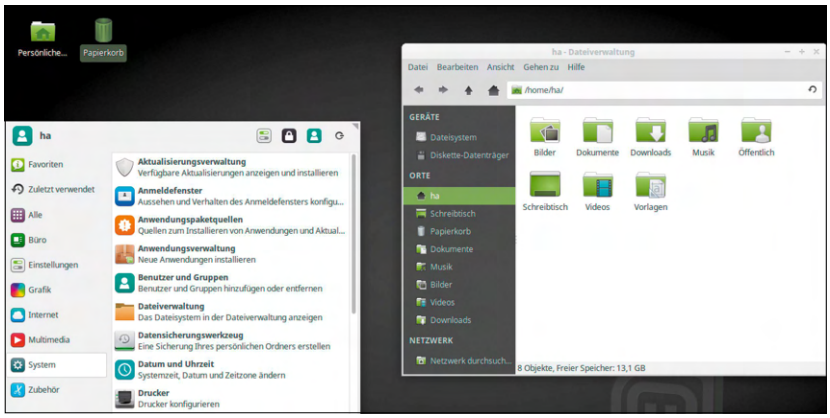
Dieser Artikel ist keine Distributionsberatung. Wir begnügen uns hier mit der pauschalen Empfehlung für Debian/Ubuntu-basierte Distributionen (Debian, Ubuntu, Kubuntu, Ubuntu Mate, Xubuntu, Lubuntu, Linux Mint). Diese garantieren Nachhaltigkeit und lange Supportzeiträume. Der Installer aller Ubuntu-Varianten inklusive Linux Mint ist das Komfortabelste, was unter Linux anzutreffen ist, und auch der Debian-Installer ist einsteigertauglich. Unter den Bedienkonzepten dieser Systeme kommt Linux Mint mit dem Cinnamon-Desktop den Gewohnheiten eines Windows-Nutzers am meisten entgegen. Die Ubuntu-Spielarten Ubuntu und Kubuntu erfordern mehr Gewöhnung, sind aber wie Ubuntu Mate, Xubuntu und Lubuntu schnell „habituiert".

2. Die Vielfalt der Oberflächen

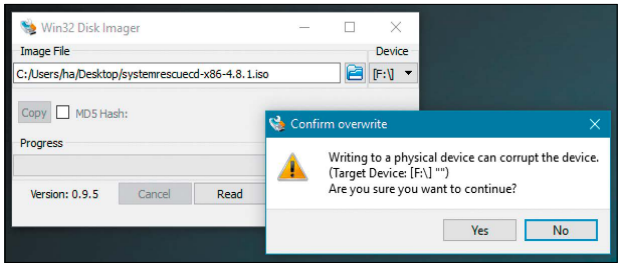
Punkt 1 hat es schon angesprochen: Zur Vielzahl der Linux-Distributionen kommt eine weitere, für Windows-Nutzer verwirrende Diversifizierung: Populäre Systeme wie Debian, Ubuntu und Linux Mint bieten für denselben Systemunterbau mehrere Desktopumgebungen an (Oberflächen) und die Wahl der Oberfläche ist mehr als nur eine Geschmacksfrage: Sie bestimmt maßgeblich die Konfigurierbarkeit und Anpassungsfähigkeit des Systems, die mitgelieferte Standardsoftware und den Ressourcenverbrauch.

Die wichtigsten Desktops sind die Schwergewichte KDE und Gnome 3 sowie die Leichtgewichte XFCE und LXDE (ideal für ältere Rechner). Cinnamon, Standardoberfläche von Linux

Mint, und Mate sind wichtige Abspaltungen der älteren Gnome-2-Basis und führen dessen klassisches Bedienkonzept mit Systemleisten und Hauptmenü fort. Mate und Cinnamon, ebenso die sparsamen Oberflächen XFCE und LXDE für schwächere Hardware sind für Umsteiger leicht nachvollziehbar. KDE ist extrem anpassungsfreudig, aber auch relativ komplex, während Gnome 3 mit gewissen Parallelen zu Windows 10 ungewöhnlich, aber klar und simpel ausfällt. Es gibt neben den genannten eine Reihe weiterer Linux-Oberflächen mit exotischem Charme oder verblüffender Anspruchslosigkeit. Windows-Nutzer sollten davon besser Abstand halten. Beachten Sie, dass einige Ubuntu-Distributionsnamen den benutzten Desktop anzeigen: Der Name „Kubuntu“ ist zu lesen als „Ubuntu mit KDE“, während Xubuntu“ und „Lubuntu“ als „Ubuntu mit XFCE beziehungsweise LXDE“ aufzulösen ist. Das „Ubuntu“ ohne Zusatz meint die Hauptvariante mit Gnome-Desktop.



Sparsame Desktops: Distributionen mit XFCE und LXDE (im Bild Mint mit XFCE) laufen auch auf älterer Hardware mit wenig Speicher. Die Optik ist konservativ.



Win 32 Disk Imager für 1:1-Kopien von ISO-Abbildern: Das Hilfsprogramm ist das technische Windows-Äquivalent des Linux-Tools dd.

3. Das Kriterium „Homogenität“

Windows ist Windows, und alles, was das System mitbringt, trägt die Microsoft-Handschrift. Linux ist der Systemkern – der Rest jedoch ist modular. Für Umsteiger ist es ein oft unterschätztes Problem, dass Oberfläche, Systemzubehör, Software nicht aus einer Hand sind. Der Nutzer muss mit unterschiedlicher Fehlertoleranz und Qualität rechnen: Die eine Komponente ist einsteigerfreundlich und warnt vor Fehlgriffen, die nächste erwartet hingegen einen Benutzer, der genau weiß, was er tut.

Wer als Umsteiger solches Gefälle vermeiden will, nimmt am besten ein Ubuntu oder Linux Mint und nutzt für die Systemverwaltung ausschließlich die Systemwerkzeuge, welche die Distribution mitbringt. Die vorinstallierten Systemtools populärer Distributionen sind hinsichtlich Zielgruppe und Qualität homogen und ausgereift.

4. Handarbeit mit ISO-Abbildern

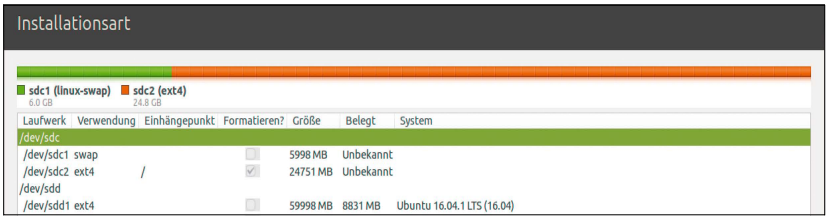
Suche und Download einer Distribution sind kein Abenteuer, da eine Websuche nach einem populären System wie etwa „Kubuntu“ mühelos zur Projektseite und von dort zum ISO-Download führt. Das ISO-Abbild muss dann aber bootfähig auf DVD oder USB kopiert werden. Diese für Linux-User vertraute Prozedur ist für Windows-Nutzer keineswegs selbstverständlich. Das einschlägige Windows-Werkzeug, um ISO-Abbilder auf CDs (ISO bis 700 MB) oder DVDs (ISO größer als 700 MB) zu brennen, ist das Tool Imgburn (auf Heft-DVD, Download unter *http://imgburn.com*).

Wählen Sie hier die Option „Image-datei auf Disc schreiben“. Der wichtigste Punkt des Folgedialogs ist links oben „Quelle“ mit dem kleinen Ordnersymbol, über das Sie dann zur ISO-Quelldatei navigieren. Bei eingelegtem Rohling wird dann die bunte Schaltfläche links unten aktiv, mit der Sie den Schreibvorgang auslösen.

Das beste Werkzeug, um unter Windows ISO-Abbilder auf USB oder SD-Karten zu kopieren, ist der 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. Die Schaltfläche „Write“ startet den Kopiervorgang. Der Win 32 Disk Imager schreibt eine bitgenaue Rohkopie auf das Zielgerät und wird nur dann ein bootfähiges Medium erstellen, wenn das ISO-Abbild eine Bootumgebung enthält. Dies ist aber bei allen uns bekannten Abbildern der Fall.

Eine Alternative, um unter Windows ISO-Abbilder auf USB oder SD-Karten zu kopieren, ist Unetbootin (auf Heft-DVD, Download unter *http://unetbootin.sourceforge.net*). Hier wählen Sie im Dialog unten die Option „Abbild“ und navigieren 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 den Laufwerksbuchstaben des USB-Sticks an. „OK“ startet den Kopiervorgang. Anders als der Win 32 Disk Imager schreibt Unetbootin seine eigene Bootumgebung auf das Zielmedium. Das



Ubuntu-Installer: Bei USB-Installationen müssen Sie Partitionen und Bootloader manuell einrichten (hier auf „/dev/sdc“). Die Einrichtung auf interne Festplatten verläuft vollautomatisch, sofern die vom Installer analysierte Situation zutrifft.



Stromsparfunktionen: Die Akkulaufzeiten von Notebooks sind unter Linux kürzer. Die Basiseinstellungen des Systems können aber durch externe Tools ergänzt werden.

Medium wird somit auch bootfähig, wenn das ISO-Abbild keine Bootumgebung enthält. Andererseits funktioniert diese Bootumgebung aber nur für Ubuntu-basierte Distributionen.

5. Livesystem und Installationsmedium

Windows-Nutzer kennen eine Setup-DVD zur Systeminstallation, aber keine Livesysteme. Die ISO-Abbilder aller populären Linux-Desktopdistributionen sind aber beides – Livesystem inklusive Installer. Das ist ein großzügiger Service, weil er das Ausprobieren eines Systems erlaubt und die tatsächliche Installation direkt aus dem laufenden Livesystem. Die weitreichenden Möglichkeiten, die ein Livesystem bietet, sind aber auch Anlass zu Missverständnissen: Ist ein ISO-Livesystem, das auf ein beschreibbares Medium (USB) kopiert wird, nicht genau dasselbe wie ein auf USB installiertes Linux? Nein! Livesysteme bleiben auch auf einem beschreibbaren Laufwerk unveränderlich, alle Änderungen gehen beim nächsten Shutdown wieder verloren. Wer Linux auf USB installieren will, muss die Installation genauso durchlaufen wie bei der Einrichtung auf interner Festplatte.

6. Hürden bei der Installation

Ein Linux-Setup fordert mehr Angaben als ein Windows-Setup, das im Kern nur die Zielpartition (sofern eine Auswahl besteht) und den Erstbenutzer abfragt. Erste Ursache dafür ist, dass Linux kein kommerzielles Lizenzmodell und keine Bindung an die Hardware kennt, daher beliebig oft und auch auf USB-Datenträger installiert werden kann. Ein zweiter Grund ist die Tatsache, dass der Bootloader auf einem beliebigen Datenträger gespeichert werden kann. Diese großzügigen Möglichkeiten sind komplexer als bei Windows und äußern sich notgedrungen auch in technischer Weise.

Wenn die Partitionierung im Linux-Installer manuell erfolgt, gibt es eine weitere technische Hürde: Die meisten Distributionen wollen für die Speicherauslagerung eine extra Swappartition.

Ohne auf die unterschiedlichen Installer einzeln einzugehen, unter denen der Ubuntu/Mint-Installer Ubiquity Komfortmaßstäbe setzt, gelten überall folgende Prinzipien:

1. Linux benötigt wie Windows nicht unbedingt eine komplette Festplatte, aber eine eigene Partition. Verfügbare Partitionen wird der Installer in der Form „/dev/sd[x][n]“ anzeigen – etwa „/dev/sda1“. Es muss absolute Sicherheit herrschen, hier das richtige Laufwerk „[x]“ und die richtige Partition „[n]“ anzugeben, weil diese Partition komplett überschrieben wird. Wichtigste Orientierung bieten die Größenangaben für die Partitionen. Weitere Abfragen für eine Linux-Systempartition gelten dem Dateisystem („ext4“ empfohlen) und dem Einhängepunkt („/“ für das Wurzelverzeichnis).

2. Für den Bootloader ist im Normalfall „/dev/sda“ vorgegeben. Das ist die erste interne Festplatte, so wie es auch Windows automatisch festlegt, und das ist in Ordnung, wenn Sie Linux auf eine interne Festplatte installieren. Bei Installation auf USB-Laufwerke müssen Sie hingegen als Bootloader-Ziel das Laufwerk angeben, wohin Sie auch das System installieren: Ist die Systempartition etwa „/dev/sdc1“, dann gehört der Bootloader auf das Gerät „/dev/sdc“. Wird dies übersehen, ist der USB-Stick nicht bootfähig.

3. Je nach Installer kann das Einrichten der zusätzlichen Swappartition lästig bis unrealisierbar sein, da nicht jeder Installer ein Partitionierungswerkzeug anbietet. Einfachste Lösung ist es, auf die Swappartition zu verzichten. Jedoch lässt sich eine Festplatte auch vorab mit Gparted unter Linux oder mit der Windows-Datenträgerverwaltung so aufteilen, dass eine große Partition für das System und eine kleine (etwa acht GB) für die Auslagerung entsteht. Die richtigen Dateisysteme – „ext4“ für das System, „swap“ für die Auslagerung, kann dann später der Linux-Installer einrichten. Bei Verwendung des Ubuntu-Installers werden Sie mit diesen technischen Fragen nur belästigt, wenn Sie unter „Installationsart“ die manuelle Einrichtung „Etwas Anderes“ wählen (etwa für ein Setup auf USB). Bei anderen Optionen – In-

stallation auf primäre Festplatte oder Dualboot neben Windows – übernimmt das Setup alles automatisch.

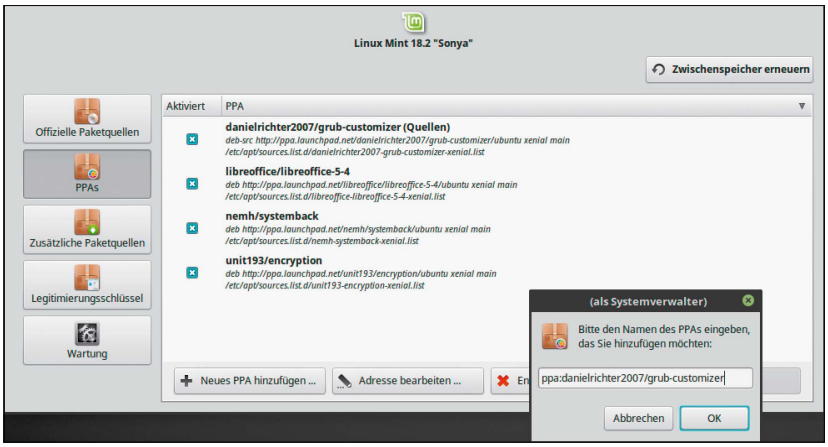
7. Unter Linux funktioniert nicht jede Hardware

Nicht jeder Hersteller hält es für nötig, Linux-Treiber für seine Hardware zu entwickeln. Resultat ist, dass dann dieses Gerät unter Linux schlicht nicht funktioniert. Kernkomponenten wie SATA, Ethernet, Grafikarte, Monitor, Maus, Tastatur sind nicht betroffen, wohl aber USB-Drucker, Scanner, WLAN-Adapter, TV-Sticks insbesondere von Billiganbietern. Die Chancen, anhand exakter Gerätekennungen und Chiprevisionen doch noch Abhilfe im Web zu finden, sind begrenzt und gegebenenfalls für Umsteiger zu knifflig.

Keine Abhilfe, aber präventive Problemerkennung bieten die Livesysteme der Linux-Distributionen. Alles, was im Livesystem problemlos funktioniert, wird im selben System auch nach Installation auf Festplatte funktionieren. Ein Sonderfall sind brandneue Rechner mit aktuellsten Prozessoren: Hier ist es wichtig, ein Linux mit möglichst aktuellem Kernel zu verwenden, der den neuesten CPU-Entwicklungen bereits Rechnung trägt. Am Beispiel Ubuntu wäre in solchen Fällen die jüngste Version 17.10 (Kernel 4.13) der Langzeitversion 16.04.3 (Kernel 4.10) vorzuziehen.

8. Energiesparfunktionen unter Linux

Windows-Umsteiger müssen damit rechnen, dass sich der Akku desselben Notebooks unter Linux schneller entleert als unter Windows. Standardmäßig bietet Linux (Ubuntu: „Systemeinstellungen -> Leistung“, Mint: „Energieverwaltung“) fundamentale Stromspartechniken mit Time-outs für Bildschirm und Bereitschaftsmodus, jedoch bietet Windows hier in enger Absprache mit den Hardwareherstellern filigranere Regeln. Immerhin ist eine Näherung an Windows-Verhältnisse mit spezialisierten Tools wie Linux Advanced Power Management (TLP) zu erreichen.



Jenseits der offiziellen Softwarequellen: PPAs (Personal Package Archives) für Ubuntu und Mint erweitern oder aktualisieren den Softwarebestand der Distributions-Paketquellen.

9. Fehlende Software und Spiele

Anpassungsfähige Windows-Umsteiger werden unter Linux für jedes Einsatzgebiet geeignete Software vorfinden. Wenn es aber statt Gimp oder Libre Office ganz bestimmte Microsoft- oder Adobe-Software sein muss, kann Linux nicht dienen. Wer aus beruflichen Gründen uneingeschränkte Kompatibilität mit Excel, Word, Indesign oder Photoshop benötigt, wird mit Linux mittelfristig nicht froh: Der durchaus realisierbare Austausch der Formate erfordert immer wieder lästige Korrekturen am Detail.

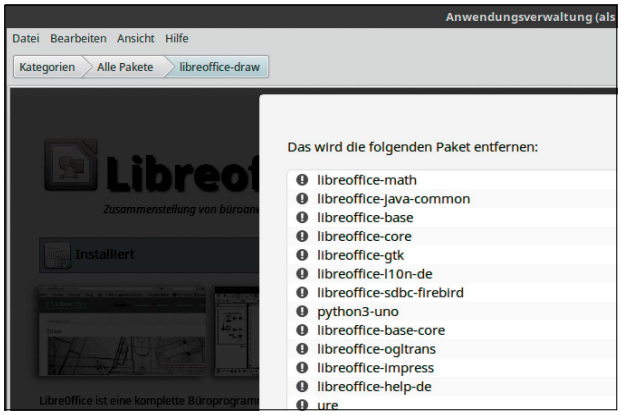
Auch die Erfolge, die das Projekt Wine mit dem Nachbau der Windows-API vorweisen kann (*https://appdb.winehq.org/*), fallen qualitativ sehr unterschiedlich aus: Dass hier genau die benötigte Version einer Windows-Software einen störungsfreien „Platinum“- oder „Gold“-Status erreicht, bleibt ein Glücksfall. Ferner bedeutet die Benutzung von Wine eine weitere Hürde: Die Einrichtung ist einfach, der produktive Umgang damit aber keineswegs trivial. PC-Spiele? Trotz Anbindung an die Spielplattform Steam ist Linux in Konkurrenz zu Windows keine Gamingplattform.

Das Angebot bleibt gegenüber Windows reduziert und leistungstechnisch kann selbst das dedizierte Gaming-Linux Steam-OS (*http://store.steampowered.com/steamos/*) ein Windows nicht schlagen.

10. Die Installation von Software (Paketmanagement)

Der Bezug von Software bedeutet für Umsteiger eine große Umstellung. Linux bezieht seine Software aus den Paketquellen der jeweiligen Linux-Distribution. Die Softwarepakete sind signiert und garantiert virenfrei – ein unschätzbarer Vorteil gegenüber Windows. Ein weiterer Vorteil ist die Möglichkeit, ein komplettes System einschließlich Software mit einem einzigen Befehl zu aktualisieren (*sudo apt dist-upgrade*). Auf der anderen Seite sehen Windows-Nutzer, die es gewöhnt sind, sich aus dem gesamten Web zu bedienen, auch Nachteile: Was die Distributions-Paketquellen bereitstellen, ist hinsichtlich Umfang und Aktualität begrenzt. Die Debian/Ubuntu-Repositories sind quantitativ zwar sehr gut gefüllt, doch stagnieren hier oft die Programmversionen während des Lebenszyklus einer Distribution. Wer nicht selbst den Quellcode kompilieren will, bleibt oft auf ältere Versionen beschränkt.

Dieses strikte Softwaredeployment ist allerdings schon längst aufgeweicht. Programmentwickler können ihre Software auf einem PPA (Personal Package Archive) anbieten. Wenn der Anwender solche PPAs etwa mit *apt-add-repository ppa:libreoffice/ppa* (Beispiel für Libre Office) in seine Standardpaketquellen aufnimmt, kann er das Softwareangebot erwei-



Vorsicht mit abhängigen Paketen beim Deinstallieren: Das Beispiel zeigt Libre Office Draw, das sich nicht deinstallieren lässt, ohne das komplette Office-Paket mitzuziehen.

tern oder aktueller halten. Zusätzlich zu den PPAs kommen zunehmend Programme in Containerpaketen in Mode (Snap, Flatpak, Appimage). Solche Pakete bringen alle benötigten Systembibliotheken mit und sind somit distributionsunabhängig, ohne Installation lauffähig und portabel.

11. Softwareverwaltung: Grafische Tools oder Terminal

Der Komplex der Paketverwaltung unter Ubuntu (und ähnlich Linux Mint) ist für Umsteiger gewöhnungsbedürftig, da er sich auf drei grafische Werkzeuge aufteilt. Was Ubuntu als Softwarequellen nutzt, ist unter „Systemeinstellungen -> Anwendungen & Aktualisierungen“ einstellbar. Aktives Aktualisieren findet aber nicht in diesem Tool statt, sondern in der „Aktualisierungsverwaltung“. Für Neu- oder Deinstallationen ist wiederum das Tool „Ubuntu Software“ zuständig, das allerdings nur einen Bruchteil der etwa 40 000 Pakete der Ubuntu-Repositories anbietet.

Umsteiger, die mit der Kommandozeile nicht gänzlich auf Kriegsfuß stehen, sind mit apt-Befehlen im Terminal oft besser beraten, wo sich alles zentral an einem Ort erledigen lässt. Eine Handvoll Kommandos genügt für fundamentale Aufgaben (weitere Optionen zeigt der Kasten „Software, Updates, Upgrades“). Der Befehl

```
sudo apt install vlc
```

installiert eine Software, dessen Paketnamen Sie kennen (im Beispiel der VLC-Player). Wenn Sie einen Paketnamen nicht kennen, hilft apt-cache, das auch nach Beschreibungen filtern kann:

```
apt-cache search  dateimanager
```

Für das Deinstallieren genügt ein remove-Kommando:

```
sudo apt remove vlc
```

Die wichtigsten Befehle für Updates und Upgrades lesen Sie weiter unten unter -> Punkt 12.

Achtung: Das Deinstallieren von Programmen ist unter Linux vollständiger als vom Windows-Nutzer gewohnt. Wenn Sie im jeweiligen Softwarecenter oder im Terminal mit *sudo apt remove […]* ein Programmpaket entfernen, berücksichtigt Linux alle verzeichneten abhängigen Pakete. Im Extremfall kann eine kleine Desktopkomponente, die aber integraler Teil der grafischen Oberfläche ist, den kompletten Desktop deinstallieren. Dies geschieht aber nach Anzeige der entsprechenden Paketliste und einer Rückfrage. Wenn der Löschauftrag eine Liste von abhängigen Paketen meldet, sollten Sie den Auftrag abbrechen.

12. Updates & Upgrades

Windows hat seinen monatlichen Patchday, an dem es optional auch Microsoft-Anwendungssoftware aktualisiert (Office). Die komplette restliche Software benötigt allerdings ihre je eigenen Updates. Bei Linux genügt hingegen ein Befehl (*sudo apt dist-upgrade*) oder ein Klick auf die automatisch erscheinende Meldung der „Aktualisierungsverwaltung“ für ein Komplettupdate inklusive Software.

Heikler als Updates sind Upgrades. Bei Ubuntu sind Upgrades auf die jeweils nächste Version vorgesehen. Sie können also von 17.04. auf 17.10 wechseln oder von der LTS-Version 16.04 auf 18.04 LTS. Sobald ein Upgrade verfügbar ist, meldet sich die Aktualisierungsverwaltung automatisch. Sie müssen dann nur auf „System aktu-

Software – Updates – Upgrades

Aus Gründen, die der Haupttext darlegt, ist der Komplex der Paketverwaltung im Terminal am besten aufgehoben. Das Tool apt (Advanced Package Tool) ist das Terminalwerkzeug unter Debian/Ubuntu/Mint für alle Aufgaben der Paketverwaltung (Softwarequellen, Aktualisierung, Neu- und Deinstallation). Alle Befehle außer *apt-cache search* benötigen root-Recht (vorangestelltes *sudo*):

apt update	Software-Paketquellen aktualisieren (fundamental)
apt upgrade [Paket]	komplettes System [oder bestimmte Software] aktualisieren
apt full-upgrade	komplette Aktualisierung des Systems (inkl. Löschen alter Pakete)
apt install [Paket]	Programm installieren
apt remove [Paket]	Programm deinstallieren
apt purge [Paket]	Programm komplett löschen
apt autoremove	nach Deinstallationen überflüssige gewordene Pakete löschen
apt-add-repository [Quelle]	externe Software-Paketquelle erlauben
apt-cache search [Name]	sucht nach Paketnamen und Beschreibungen
do-release-upgrade	Upgrade auf nächsthöhere Version

alisieren“ klicken und den weiteren Anweisungen folgen. Wenn Sie das Angebot aus Zeitmangel zunächst ablehnen, können Sie die Option später über die „Aktualisierungsverwaltung“ nachholen.

Der Terminalbefehl für ein Upgrade lautet folgendermaßen

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

und sollte durch eine normale Systemaktualisierung mit

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

vorbereitet werden.

Linux Mint zeigt in der „Aktualisierungsverwaltung“ im Menü „Bearbeiten“ die Option „System aktualisieren auf Linux Mint xx.x“, sobald ein jüngere Version erhältlich ist. Bevor man das tut, ist es ratsam, das System erst auf den neuesten Stand zu bringen (wie bei Ubuntu).

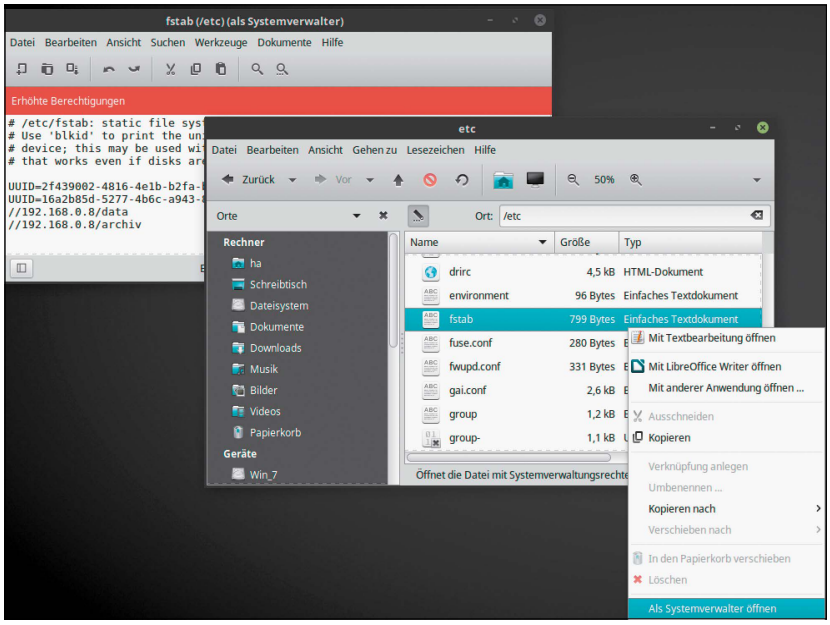
Sollte ein Upgrade wegen eines Abhängigkeitsfehlers abbrechen, nutzen Sie diese beiden Befehle:

```
sudo apt -f install
sudo apt dist-upgrade
```

Achtung: Systemupgrades sind ein langwieriger und kritischer Vorgang. Viele Distributionen bieten das Upgrade daher gar nicht erst an. Ubuntu und Linux Mint haben den Vorgang aber nach unserer Erfahrung gut im Griff. Ärgerlich sind Upgradeangebote, die überwiegend scheitern und am Ende doch eine Neuinstallation erfordern (wie etwa beim NAS-System Open Media Vault).

13. „sudo“ und Administratorrechte

Die Verhältnisse zwischen Standard- und Administrator/root-Konto sind unter Linux und Windows ähnlich, aber der bedarfsweise Wechsel von eingeschränkten Benutzerrechten zu uneingeschränkten root-Rechten folgt anderen Regeln. Möglich ist dieser Wechsel bei Windows wie Linux nur Systemkonten, die zur Gruppe der Administratoren gehören. Während Windows nur einen „Ja“-Klick auf die Abfrage der „Benutzerkontensteuerung“ verlangt, fordert Linux die Eingabe des



Kontextmenü für Administratorrechte: Die Dateimanager von Ubuntu und Mint machen es einfach, Ordner oder Dateien zu bearbeiten, die den Wechsel zu root-Rechten erfordern.

Benutzerkennworts. Diese Abfrage an der grafischen Oberfläche erscheint bei allen systemnahen Aktionen (Installation, Paketquellen, Benutzerkonten, Aktualisierungsverwaltung). Im Terminal kann dem eigentlichen Befehl sudo vorangestellt werden, um dem Befehl root-Recht zu verleihen. Auch hier fordert Linux die Eingabe des Benutzerkennworts.

Die Erlaubnis, mit *sudo* den Rechtekontext zu wechseln, erhält normalerweise jedes Benutzerkonto vom Typ „Administrator“ automatisch. Es ist aber darüber hinaus möglich, sudo-Erlaubnis über die Konfigurationsdatei „/etc/sudoers“ manuell und individuell einzurichten.

Im grafischen Dateimanager sind alle Schreibaktionen wie „Ordner anlegen“ oder „Löschen“ inaktiv, wenn man sich jenseits von „/home“, „/tmp“ oder „/media“ aufhält. Jedoch bieten Desktopsysteme wie Ubuntu und Mint das Kontextmenü „Als Systemverwalter öffnen“, um im Dateimanager uneingeschränkt mit root-Recht zu arbeiten. Wenn ein Dateimanager diese Option nicht selbst anbietet, können Sie ihn im Terminal mit vorangestellten *sudo* starten – also etwa *sudo nautilus*, um root-Recht zu erzwingen.

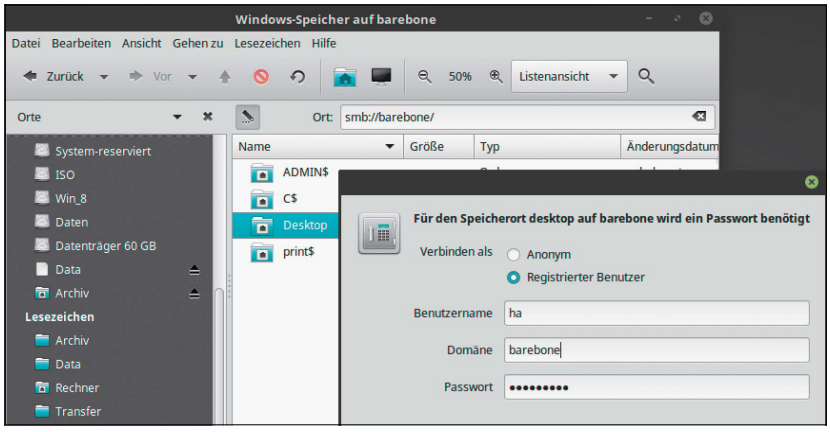
14. Die lokalen Dateirechte

Das Thema Dateibesitz und Dateirechte ist unter Windows wie Linux kompliziert und Ursache für manche Zugriffsprobleme, zumal auch Netzfreigaben für einen User „xyz“ mindestens auch lokale Leserechte für „xyz“ voraussetzen. Linux-Einsteiger können nichts Klügeres machen, als manuelle Rechteänderungen möglichst zu vermeiden. Dabei helfen Ubuntu-Systeme inklusive Linux Mint mit Dateimanagern, die lokale Datenträger und Netzwerklaufwerke automatisch (Automount) so ins Dateisystem mounten, dass keine Rechtekonflikte entstehen. Die typische Nutzung von Netzressourcen über „Netzwerk durchsuchen“, Klick auf den gewünschten Server und dessen Freigabe lädt die Netzfreigabe automatisch in einen Mountpunkt, der keine lokalen root-Rechte benötigt. Im Hintergrund arbeitet bei allen Gnome-affinen Desktops das Tool gvfs-mount, das auch im Terminal benutzt werden kann und stets in den Pfad „/run/user/[user-id]/gvfs/“ mountet.

Dieses Automount geht Rechteproblemen aus dem Weg und hat nur den Nachteil, dass es nicht dauerhaft gilt: Es muss einmal in der laufenden Li-



Ausführen-Bit setzen: Scripts werden erst ausführbar, wenn das Execute-Bit gesetzt ist. Das erledigt der Dateimanager oder auch chmod +x [name] im Terminal.



Netzwerkauthentifizierung mit „Domäne“: Diese Abfrage beantworten Sie am einfachsten mit dem Rechnernamen des Servers, der die Freigabe bereitstellt.

nux-Sitzung geschehen und gilt bis zur Abmeldung.

Bei typischen Zugriffsproblemen, wo statt dem normalen User nur root die nötigen Dateirechte besitzt, ist daher die richtige Antwort eine andere Mountmethode – und nicht das rekursive Ändern massenhafter Dateirechte. Dennoch ist das im Notfall natürlich möglich. Dateimanager eignen sich über „Eigenschaften -> Zugriffsrechte“ nur für einzelne Ordner und Dateien. Der Terminalbefehl chown („change ownership“) ändert den Besitzer und arbeitet sich mit Schalter „-R“ auch rekursiv durch ganze Ordnerebenen:

```
sudo chown -R [Benutzer] [Pfad]
```

Zum Ändern der Rechte dient der Befehl chmod – mit leider zwei Beschränkungen. Er arbeitet nicht rekursiv, was sich mit Hilfe des find-Befehls kompensieren lässt. Chmod unterscheidet aber auch nicht zwischen Dateien und Ordnern. Wenn man Dateien und Ordnern dieselben Zugriffsrechte zuteilt, führt das zu dem Dilemma, dass sich entweder Ordner nicht öffnen lassen oder Dateien allesamt das „Ausführen“-Recht erhalten. Beides wäre fehlerhaft. Daher sind zwei Befehle notwendig:

```
find . -type f -exec chmod 664 {}
 \;
find . -type d -exec chmod 775 {}
 \;
```

„type f“ bearbeitet nur Dateien, „type d“ nur Ordner. Die Beispielbefehle würden ab dem aktuellen Verzeichnis (Punkt „.“) alle Unterordner verarbeiten. Eine Rechteänderung, die jeder Linux-Nutzer kennen muss, betrifft das „Ausführen“-Bit von Scripts, das sich über „Eigenschaften -> Zugriffsrechte“ oder mit

```
chmod +x [Dateiname]
```

setzen lässt. Ohne dieses Bit gelten Scripts als Textdatei und werden nur angezeigt statt ausgeführt.

15. Automount von Netzwerkressourcen

Beim erstmaligen Mounten von Samba-Freigaben im Dateimanager (siehe -> Punkt 14) muss sich der zugreifende Benutzer ausweisen und Samba-Kontonamen und -Kennwort eingeben. Diese Zugangsdaten können auf Wunsch dauerhaft hinterlegt werden („Nie vergessen“). Zusätzlich – und für Windows-Umsteiger ungewohnt – wird hier die „Domäne“ abgefragt. Im lokalen Netzwerk verwenden Sie hier wahlweise den Rechnernamen des Servers wie „rasp-berry“ oder „fritz-nas“ oder die Arbeitsgruppe, typischerweise „workgroup“, sofern keine explizit angelegt wurde.

Eine weitere Hürde für Windows-Nutzer ist der relativ abgelegene Automount-Pfad von Netzwerkfreigaben unter „/run/user/[…]/gvfs/“. Im Dateimanager, wo eingehängte Ressourcen unter „Geräte“ mit einem Klick erreichbar sind, spielt dieser Mountpunkt keine Rolle, bei der Nutzung anderer Tools oder des Terminals hingegen schon. Wird nun versucht, mit einem manuellen mount-Befehl ein Netzlaufwerk in einen angenehmeren Userpfad einzubinden, dann stellt sich das Problem, dass der mount-Befehl root-Rechte erfordert, was dann unweigerlich zu Rechteproblemen im Mountordner führt. Hier hilft nur ein Eingriff in eine Konfigurationsdatei, hier in die „/etc/fstab“ (Beispiel):

```
//192.168.178.20/archiv   /home/
 ha/Archiv   cifs   user=ha,passwo
 rd=0815,domain=raspi,users
 0       0
```

Die Freigabe wird dann automatisch bei der Systemanmeldung eingehängt. Die Option „users“ sorgt dafür, dass man die Freigabe außerdem mit Userrechten ein- und aushängen darf. Die beiden Befehle

```
mount /home/ha/Archiv
umount /home/ha/Archiv
```

funktionieren dann ohne root-Recht und benötigen lediglich den Mountpunkt als Parameter.

16. Netzprotokolle und Anwendungssoftware

Die Dateimanager Nautilus, Nemo, Dolphin, Caja prominenter Desktopsysteme beherrschen den Umgang mit diversen Netzwerkprotokollen – neben Samba („smb://“) und FTP („ftp://“) auch SSH („sftp://“) oder Webdav („webdav://“). Solche Netzadressen zeigt der Dateimanager, wenn Sie über „Netzwerk durchsuchen“ einen Datenserver anklicken, Adressen wie „smb://

raspberry/“ können Sie aber auch direkt in die Adresszeile des Dateimanagers eingeben. Für Einsteiger irritierend ist die Tatsache, dass ein solcher Netzwerkpfad zwar im Dateimanager ans Ziel führt, im Terminal oder einer Anwendungssoftware jedoch scheitert. Einfacher Grund ist, dass diese Programme die Protokolle nicht beherrschen: Sie erwarten, dass solche Netzressourcen in das lokale Dateisystem eingehängt wurden, und arbeiten nur über diesen lokalen Mountpfad. Also – zunächst im Dateimanager mounten, erst danach in der Software nutzen!

17. Übersicht über sämtliche Laufwerke

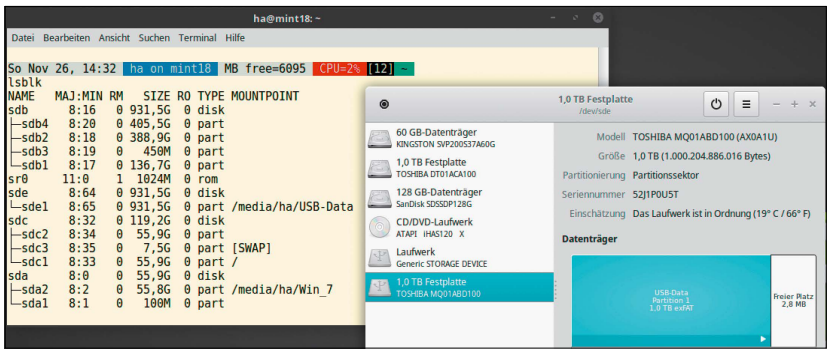
Der Windows-Explorer zeigt interne und externe Laufwerke mit allen Partitionen auf oberster Ebene an. Viele Linux-Umsteiger vermissen diese Ebene, die von dort ein Herabsteigen in die Verzeichnisebenen gestattet.

Der Einstieg über das Wurzelverzeichnis („/“) des Dateisystems ermöglicht dies nicht, da Laufwerke oder Netzfreigaben in beliebigen Verzeichnissen eingehängt sein können. Jedoch bietet die Navigationsleiste in den Dateimanagern eine solche Übersicht: Unter „Geräte“ sind dort üblicherweise alle Partitionen aufgelistet. Wer zusätzlich eine Übersicht der Laufwerke im Hauptfenster sehen will, kann in das Adressfeld des Dateimanagers „computer:///“ eingeben und diese Laufwerkübersicht mit Strg-D („Lesezeichen -> Lesezeichen hinzufügen“) dauerhaft in der Navigationsspalte ablegen. Bei manchen Dateimanagern ist dieser Eintrag namens „Rechner“ standardmäßig vorhanden.

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

Unter Windows dienen aufsteigende Buchstaben als Kennung für Datenträger. Aus historischen Gründen beginnt das Alphabet bei „C“, da „A“ und „B“ ungenutzt weiterbestehen (ehemals Diskettenlaufwerke).

Linux ist hier eigentlich klarer, dennoch sind die Kennungen ein häufiges



Wichtig vor Installationen oder Kopieren von ISO-Abbildern: lsblk im Terminal liefert einen Überblick über alle Partitionen – rechts das Systemtool gnome-disks („Laufwerke“).

Problem für Umsteiger. Laufwerke und Partitionen eindeutig zu bestimmen, ist aber fundamental bei der Installation oder beim Schreiben von ISO-Abbildern.

Eine Kennung wie „/dev/sda1“ beginnt mit „/dev/“ für „Device“, „sd“ kennzeichnet die Schnittstelle „Sata Device“ (seltener sind „sc“ für SCSI-Device oder „m“ für Raid). Wichtig wird es danach: „a“ bedeutet die erste interne Festplatte, „b“ die zweite oder – falls nicht vorhanden – bereits das erste externe USB-Laufwerk. Die abschließende Zahl ist die Partitionsangabe. Die Kennungen sind über grafische Werkzeuge wie „Laufwerke“ (gnome-disks) oder Gparted zu ermitteln. Eine schnelle Übersicht bietet der Terminalbefehl lsblk, der sich optional mit Outputparametern („-o“)

```
lsblk -o name,type,label,size,moun
  tpoint,fstype
```

gesprächiger schalten lässt.

19. Groß-Klein-Schreibung und Sonderzeichen

Unter Windows spielt die Schreibung weder bei Dateinamen noch bei Befehlen und Schaltern eine Rolle. „DIR“ ist dasselbe wie „dir“ oder „diR“. Unter Linux ist genaue Schreibung hingegen zwingend: Den Befehl „LSBLK“ gibt es nicht, und ein Schalter „-X“ bedeutet etwas anderes als „-x“. Folgerichtig können auch Dateiobjekte wie „Musik“, „musik“ und „MUSIK“ nebeneinander existieren.

Nonchalant verhält sich Linux hingegen bei Sonderzeichen in Datei- und Ordnernamen. Die Sortierung von Ordnern und Dateien im Dateimanager wie im Terminal fällt bei Verwendung von Sonderzeichen deutlich anders aus. Während Windows einen Ordner „_Start“ vor allen Ordner mit alphanumerischen Startzeichen einsortiert, ignoriert Linux das Sonderzeichen und ordnet ihn unter „S“ ein.

Zum echten Problem beim Datenaustausch zwischen Linux und Windows können Sonderzeichen in Dateinamen werden, da Linux mehr Sonderzeichen erlaubt als Windows. So können Linux-Dateinamen auch Doppelpunkt, Fragezeichen, Asterisk (*) oder Backslash enthalten.

20. Abmelden – Shutdown – Bereitschaft

Unter Windows 10 führt ein Rechtsklick auf das Hauptmenü zum Punkt „Herunterfahren oder abmelden“. Der Klickweg ist nicht intuitiv, aber immerhin ist hier alles an Ort und Stelle. Unter Linux handhaben die Desktopoberflächen das jeweils eigen: Unter Linux Mint sind alle Abschaltfunktionen wie Abmelden, Ausschalten, Neustart oder Bereitschaft im Hauptmenü versammelt – übersichtlich und leicht zu finden. Andere Linux-Desktops wie etwa Gnome folgen der technischen Logik und trennen die echten Abschaltfunktionen von jenen der Benutzersession. Hinter dem typischen Abschaltsymbol gibt es daher nur Shutdown und Neustart, während die Abmeldung oder die Bildschirmsperre unter dem Kontonamen zu finden sind. ●

Linux Mint 18.3 mit Flatpak und Timeshift

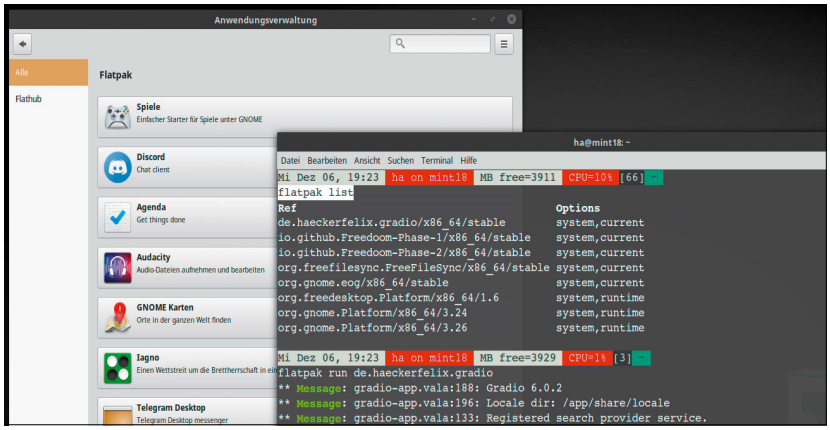
Linux Mint 18.3 ist eine einfach bedienbare und stabile Distribution. Ihre Systembasis basiert auf dem Point Release 16.04.3 LTS des Ubuntu-Vorbilds. Dieser Release enthält viele Updates, aber noch nicht die Patches gegen Meltdown und Spectre.

Von **Hermann Apfelböck**

Linux Mint basiert bekanntlich auf der LTS-Version von Ubuntu und folgt dieser stets mit einigen Monaten Verzögerung. Das letzte Point Release 16.04.3 von Ubuntu fand im August 2017 statt und Linux Mint vollzog Anfang Dezember den analogen Schritt zu 18.3. Damit ist Linux Mint wieder auf dem Stand der Dinge mit aktuellerem Linux-Kernel 4.10 inklusive frischen Hardwaretreibern. Das nächste große Update auf Mint 19 wird für Mai oder Juni 2018 erwartet. Es basiert dann auf Ubuntu 18.04.

Der Platzhirsch unter den Linux-Desktops war zwischen August und Dezember nicht faul: Linux Mint 18.3 erhält nämlich nicht nur den neuen Ubuntu-Unterbau, sondern eine Reihe beachtlicher Verbesserungen, die sämtliche Mint-Varianten betreffen (Cinnamon, Mate, XFCE, KDE), sowie einige Neuheiten beim Standarddesktop Cinnamon (Version 3.6). Die Hauptvariante mit dem Cinnamon-Desktop finden Sie bootfähig auf Heft-DVD.

Mit Version 18.3 fiel übrigens auch noch eine mutige strategische Entscheidung: Linux Mint verabschiedet sich vom KDE-Desktop – Version 18.3 ist das letzte Mint mit KDE-Edition. Das ist aus unserer Sicht ein vernünftiger Schritt, da sich Linux Mint in erster Linie durch seinen Stammdesktop Cinnamon definiert, für dessen Weiterentwicklung nun mehr Ressourcen freiwerden.



Integriertes Flatpak: Die grafische Anwendungsverwaltung bietet Flatpak-Container neben normaler Software. Unter der Haube arbeitet das Kommandozeilentool flatpak.

Infos zu Linux Mint 18.3 „Sylvia“
Webseite und Downloadlinks: *www.linuxmint.com*
Dokumentation: *www.linuxmint.com/documentation.php*
Release Notes für Version 18.3: *www.linuxmint.com/rel_sylvia.php*

Anwendungsverwaltung mit Flatpak-Integration

Für das Mint-Team ist der grafische Paketmanager mintinstall („Anwendungsverwaltung“ auf deutschem System) der eindeutige Star der neuen Version 18.3. Die Anwendungsverwaltung wurde grundlegend überarbeitet und präsentiert sich in der Tat schnörkellos mit einem Abschnitt „Empfehlungen“ und einem Register mit „Kategorien“. Wer von vornherein weiß, was er will, nutzt rechts oben das Suchfeld. Die Ladegeschwindigkeit des Programms sowie die Reaktionszeiten beim Klick auf „Kategorien“ sind deutlich verbessert. Die Anwendungsverwaltung bleibt aber weiterhin ein opulenter Task mit erheblichen Speicherbedarf. Wichtiger als die Leistungsverbesserung scheinen uns daher zwei weitere grundlegende Neuheiten:

1. Das Tool läuft im Usermodus. Zum Suchen und Stöbern ist daher keine Passworteingabe erforderlich. Diese wird erst dann notwendig, wenn tatsächlich eine Software installiert oder entfernt werden soll. Das einmal eingegebene Passwort merkt sich das Programm während der Laufzeit, sodass die Eingabe nur ein einziges Mal erfolgen muss.

2. Unter den „Kategorien“ gibt es auch eine Schaltfläche „Flatpak“. Das ist nicht ganz logisch, da es sich bei Flatpak um keine inhaltliche Kategorie wie „Film und Klang“ handelt, sondern um eine Technik, Software in distribu-

tionsunabhängige Container zu verpacken. Trotz unlogischer Stelle ist es grundsätzlich verdienstvoll, dass die Anwendungsverwaltung die auf Flathub (*https://flathub.org/*) angebotene Software hier an zentraler Stelle anbietet. Die Integration von Flatpak-Containern setzt voraus, dass das Kommandozeilenwerkzeug für Flatpaks installiert ist. Dies ist in Mint 18.3 der Fall, wie Sie sich anhand folgender Terminalbefehle überzeugen können:

```
flatpak --help
flatpak list
```

Die Anwendungsverwaltung dient nur als klickfreundliches Front-End für dieses Werkzeug. Flatpak-„Installationen“ werden aber darüber hinaus wie echte Installationen ordnungsgemäß in das Mint-Menü eingetragen.

Datenbackup und Timeshift

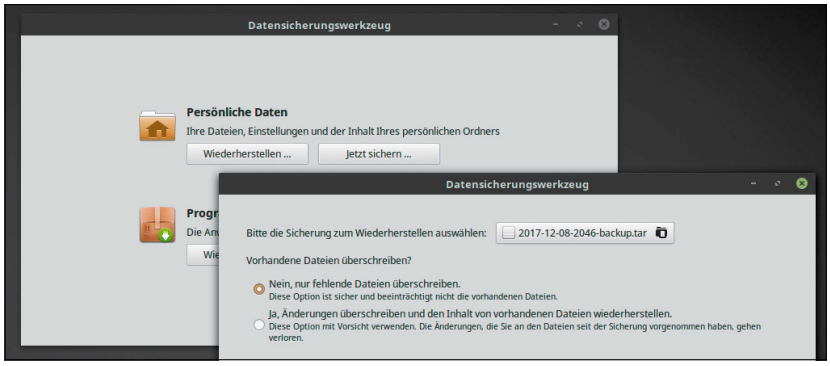
Die Mint-Eigenentwicklung mintbackup („Datensicherungswerkzeug“ auf deutschem System) wurde für Version 18.3 umgeschrieben und vereinfacht. Das Tool sichert jetzt nur noch im Home-Verzeichnis und kann daher ohne root-Recht laufen. Die Beschränkung auf das Home-Verzeichnis kompensiert Mint 18.3 durch die Standardbeigabe des Tools Timeshift, das seinerseits die Sicherung von Systemverzeichnissen übernimmt (siehe unten). Das Datensicherungswerkzeug bietet nur die Optionen „Wiederherstellen“ und „Jetzt sichern“. Beim Sichern kopiert es einfach alle angegebenen Ordner und Dateien mit Pfad, Zeitstempel und Rechte in ein „tar“-Archiv. Dabei kann der Benutzer Ordner und Dateien explizit ausschließen und einschließen, und die einmal getroffene Auswahl merkt sich mintbackup dauerhaft. Beim „Wiederherstellen“ müssen Sie nur den Pfad zum „tar“-Archiv angeben.

Das renovierte mintbackup ist weder funktionsreich noch raffiniert, aber als simples Tar-Front-End eine hübsche Anfängerhilfe. Das Standardziel des Backups unter „~/Dokumente/Sicherungen“ ist aber sicher suboptimal und sollte durch einen Zielpfad auf einem anderen Datenträger ersetzt werden. Eine zweite Funktion von mintbackup, welche nachinstallierte Programme protokolliert und im Falle des Falles in einem Aufwasch auf das System holt, ist eher eine Marginalie und außerdem eingeschränkt auf die Aktionen in der Anwendungsverwaltung.

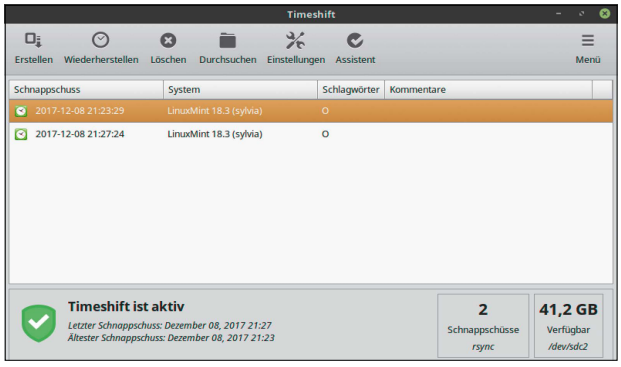
Timeshift: Für die Systemsicherung holt sich Linux Mint 18.3 das bekannte Werkzeug Timeshift an Bord, das platzsparende, differentielle Schnappschüsse des Systems anfertigt. Timeshift kümmert sich nur um Systemdateien und ist somit der ideale Gegenpart zum Mint-eigenen Datensicherungswerkzeug. Die Schnappschüsse erledigt im Normalfall das Backupwerkzeug rsync. Ist Linux Mint auf dem Dateisystem BTRFS installiert, kann man alternativ die Option „BTRFS“ anwählen, da dieses Dateisystem solche Schnappschüsse selbst beherrscht. Zurückliegende Systemsicherungen können im Timeshift-Fenster mit „Wiederherstellen“ komplett restauriert werden. Es ist aber auch möglich, über die Schaltfläche „Durchsuchen“ gezielt einzelne Dateien aus einer Sicherung in das aktuelle System zu kopieren.

Neues in Cinnamon

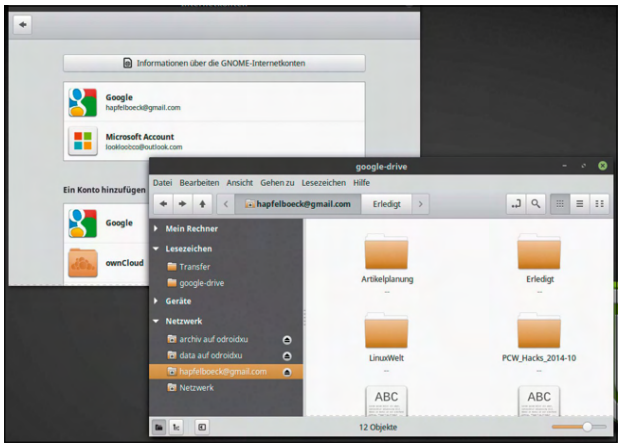
Cinnamon 3.6 zeigt in den „Systemeinstellungen“ das Applet „Internetkonten“. Damit integriert die Oberfläche das Tool gnome-online-accounts, das prominente Clouddienste direkt für Gnome-Programme zugänglich macht. Bemerkenswert ist die Verbindung zu Google Drive und zu Owncoud-/Nextcloud-Servern, die dann mit dem Dateimanager Nemo besucht werden können. Bei anderen Clouddiensten sind speziellere Programme wie Evolution oder Gnome Calendar für den Zugriff vorgesehen. Das Einbinden eines Internetkontos ist einfach: Im Applet „Internetkonten“ genügt unter „Konto hinzufügen“ ein Klick auf das gewünschte Konto – etwa „Google“. Danach fordert das Tool die Authentifizierungsdaten. Sobald diese korrekt eingegeben sind und die Anmeldung mit einem anderen Gerät (Smartphone) bestätigt wurde, ist der Clouddienst integriert.



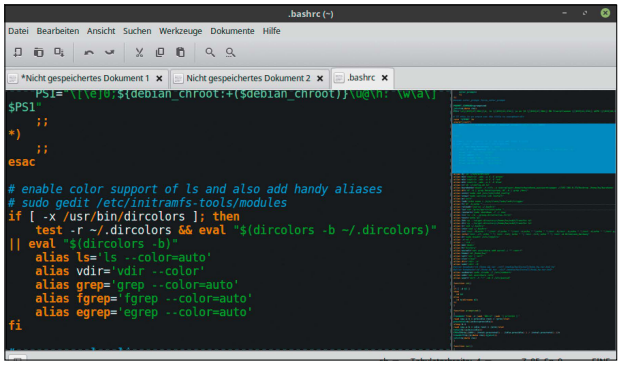
Simples Mintbackup: Das Tool wurde weiter vereinfacht – es verzichtet auf root-Rechte und sichert nur noch unter „/home“.



Timeshift als neuer Standard unter Linux Mint: Das Werkzeug sichert den aktuellen Systemstatus in differentiellen Schnappschüssen und kann manuell oder per Cron ausgelöst werden.



Google Drive im Dateimanager: Nach der Integration in den Systemeinstellungen ist die Google-Cloud für Nemo sofort zugänglich.



Marginal, aber praktisch: Der Texteditor Xed erhält eine optionale Übersichtsspalte, in der es sich besonders flott blättern lässt.

So erscheint dann etwa Google Drive als Server in der Navigationsspalte des Dateimanagers Nemo und ist wie eine lokale Ressource benutzbar.

Diverse weitere Detailverbesserungen in Cinnamon 3.6 bleiben zum Teil schwer überprüfbar und wie die verbesserte Hi-DPI-Unterstützung zum Teil marginal: So beherrschen Cinnamon-Eingabefelder (etwa das Suchfeld im Hauptmenü) den Maus-Mittelklick als Einfügekommando aus der Zwischenablage. Und der Netzwerkmanager in der Systemleiste hat einen zusätzlichen Eintrag erhalten, um bei Bedarf eine erneute Suche nach Funknetzwerken auszulösen.

Neue und verbesserte Tools

Das Mint-Team legt seit Jahren Wert auf objektive Debugmöglichkeiten im Falle von Systemproblemen. Der Rechtsklick auf die Cinnamon-Systemleiste mit den Optionen „Fehler suchen“ und „Looking Glass“ sind hauptsächlich für Entwickler und das Mint-Team selbst von Belang, die Option „Cinnamon neustarten“ an dieser Stelle ist auch für Endanwender ein nützlicher Nothelfer. Jetzt kommt noch ein neues Mint-Tool hinzu:

Mintreport, auf deutschem System „Systemberichte“, kann Abstürze protokollieren und an die Mint-Entwickler schicken. Nach dem Start des Programms erscheinen im oberen Fenster die „Absturzberichte“. Über die Schaltflächen „Fehlerverfolgungssystem“ und „Pastebin“ werden deren Informationen online veröffentlicht. Die Schaltfläche „Lokale Dateien“ führt zum Archiv „crash.tar.gz“, das erfahrenen Nutzern profunde Infos über das betroffene Programm, System, Zeitpunkt, Speicher und Systemvariablen vermittelt.

Die **Systemanmeldung** ist unter „Systemeinstellungen -> Anmeldefenster“ individueller konfigurierbar denn je: So kann die Anmeldung Infos wie Rechnername, Uhrzeit oder Akkustand je nach Wunsch anzeigen oder eben nicht. Neu ist ebenfalls die Option, die Liste der Systembenutzer auszublenden und eine manuelle Anmeldung zu erzwingen.

Xed, der Editor auf Basis von Gedit (deutsch: „Textbearbeitung“), erhält eine unscheinbare, aber praktische neue Funktion unter „Ansicht -> Übersichtskarte“. Dies blendet am rechten Fensterrand eine Miniaturansicht ein, die zwar nicht mehr lesbar ist, aber mit der Maus sehr schnelles Navigieren in größeren Texten oder Scripts ermöglicht.

Xreader („Dokumentenbetrachter“) und Xplayer („Videos“) erhalten marginale Änderungen: Der Xreader, der hauptsächlich zur Anzeige von PDF-Dateien dient, erhält neue Navigationspfeile zum Vor- und Zurückblättern. Im Xplayer wurde die Bilddarstellung im Vollbildmodus optimiert.

Linux Mint 18.3: Neuinstallation und Upgrade

Das auf DVD vorliegende Livesystem von Linux Mint 18.3 eignet sich zum Ausprobieren und für Neuinstallationen (zum Upgrade älterer Versionen siehe unten). Für eine Neuinstallation wählen Sie im gestarteten Livesystem einfach den Desktoplink „Linux Mint installieren“. Beachten Sie aber, dass die Heft-DVD ausschließlich im Bios-Modus bootet. Für eine Uefi-Parallelinstallation neben einem bereits existierenden Windows oder Linux im Uefi-Modus benötigen Sie einen USB-Stick oder eine eigene DVD mit dem Mint-Livesystem. Da dieses auch als originalgetreue ISO-Datei im Verzeichnis „/Image-Dateien“ der Heft-DVD vorliegt, können Sie das Abbild mit den üblichen Mitteln (dd, Brasero, Win 32 Disk Imager, Imgburn) von der Heft-DVD auf Ihr eigenes Medium übertragen. Secure Boot, typisch bei parallelem Windows, wird von Linux Mint nicht unterstützt und muss daher im Bios abgeschaltet werden.

Linux Mint mit Cinnamon in 64-Bit-Ausführung ist kein ausgesprochenes Leichtgewicht, hat aber noch moderate Mindestanforderungen: Eine Dualcore-CPU ab etwa 1,5 GHz Taktfre-

quenz ist empfehlenswert sowie mindestens zwei GB RAM, da System und Desktop alleine schon mal circa 600 MB belegen. Eine etwas leichtgewichtigere 32-Bit-Version steht unter *www.linuxmint.com/download.php* zum Download bereit. Für den standardmäßigen Cinnamon-Desktop ist eine 3D-fähige Grafikkarte/Grafikchip von Vorteil, damit die Oberfläche inklusive dezenter Animationen ansprechend flott läuft.

Als Installationsprogramm nutzt Linux Mint seit je den komfortablen Installer Ubiquity von Ubuntu. Der beherrscht automatische Solo- und Dualboot-Szenarien und erkennt bereits installierte Systeme. Für kompliziertere Szenarien gibt es im Dialog „Installationsart“ die manuelle Option „Etwas Anderes“, die einen kompletten Partitionsmanager mitbringt. Notwendig ist diese manuelle Methode in jedem Fall bei Installationen auf externe USB-Datenträger.

Upgrade der Version 18.x: Ein bereits vorliegendes Linux Mint 18, 18.1 oder 18.2 kann via Internet, also ohne Installationsmedium, ein Upgrade auf die aktuelle Version 18.3 erhalten. Mit anderen Worten: In diesem Fall brauchen Sie keinen Download des ISO-Images. Folgende Vorgehensweise ist notwendig: Zunächst bringen Sie die bestehende Version 18.2 auf den neuesten Stand:

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

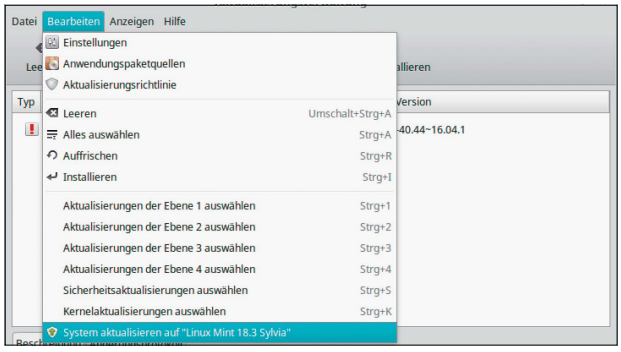
Danach starten Sie über das Menü die „Aktualisierungsverwaltung“. Ist diese auf dem aktuellen Stand (wofür die obigen Befehle gesorgt haben), dann erscheint unter „Bearbeiten“ der zusätzliche Punkt „System aktualisieren auf…18.3…“. Damit lösen Sie das Upgrade auf die neueste Version aus und müssen nur noch dem Assistenten folgen. Bei eventuellen Nachfragen, ob Konfigurationsdateien erhalten oder ersetzt werden sollen, entscheiden Sie sich für das „Ersetzen“.

Bei einem Upgrade kann auch schon mal etwas schief gehen: Upgradeskeptische und besonders vorsichtige Anwender können vorbereitend folgende Maßnahmen vornehmen:

1. Sicherung aller Benutzerdateien unter „/home“

2. Deaktivieren des Bildschirmschoners während der Laufzeit des Upgrades: „Systemeinstellungen -> Bildschirmschoner -> Einstellungen“ und dort Verzögerungsintervall „Nie“

3. Deaktivieren eventueller externer „Cinnamon Spices“ (Applets, Desklets, Erweiterungen und Themen unter „Systemeinstellungen -> Einstellungen“).



Upgrade übers Internet: Der Wechsel eines Mint 18, 18.1 oder 18.2 auf aktuelles 18.3 erfolgt über die „Aktualisierungsverwaltung“ – nicht über das Installationsmedium.

Optimierung nach Neuinstallation oder Upgrade

Nach einer Neuinstallation suchen Sie „Systemverwaltung -> Treiberverwaltung“ auf, um auf proprietäre Grafiktreiber umzustellen. Unter „Einstellungen -> Bildschirm“ stellen Sie – falls nötig – die optimale Auflösung ein. Der Gang zu diesem Applet ist fast nur bei Multimonitor-Betrieb notwendig.

Da es seit Erscheinen von Version 18.3 schon wieder eine Reihe neuer Updates gibt, empfiehlt sich eine sofortige Systemaktualisierung. Das ist vor allem wegen der Bugs Meltdown und Spectre in Intel-CPUs wichtig:

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

Für die laufende Aktualisierung sorgt die „Aktualisierungsverwaltung“ mit ihren Levels „1“ bis „5“. Alles, was nicht vom Mint-Team getestet wurde, sondern etwa aus den Ubuntu-Repositories stammt, wird mit Stufe 4 oder 5 bewertet und nicht berücksichtigt. Das können Sie ändern, indem Sie unter „Bearbeiten -> Einstellungen -> Ebenen“ auch die Stufen 4 und 5 als „sicher“ und „sichtbar“ markieren.

Cinnamon bietet zahlreiche individuelle Anpassungsmöglichkeiten über die „Systemeinstellungen“, zum Beispiel:

„Themen“ bestimmen das Aussehen des Mint-Desktops entscheidend. Der wichtigste Unterpunkt ist „Schreibtisch“, weil dieser die Farben des Hauptmenüs und der Hauptleiste festlegt. Die Auswahl des „Fensterrahmens“ für die Titelleisten aller Taskfenster und der „Symbole“ (im Dateimanager und am Desktop) verändert die Optik ebenfalls deutlich.

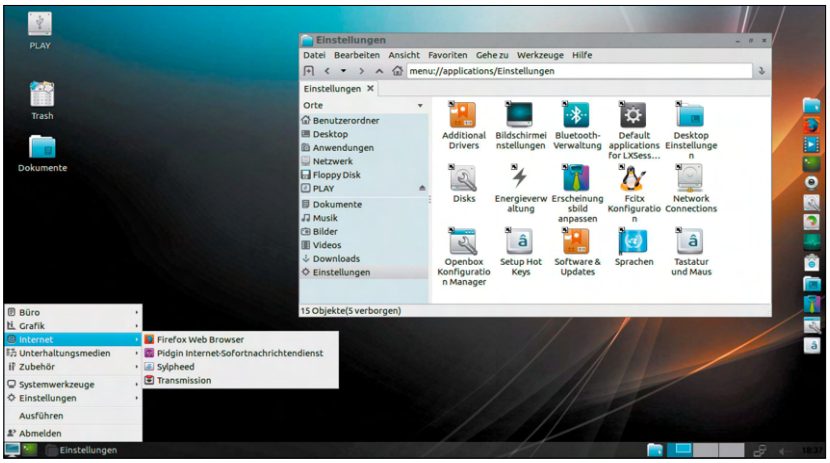
Unter **„Fenster -> Titelleiste“** bestimmen Sie das Verhalten der Titelleiste: Die Funktion der Kontrollelemente in der Titelleiste kann ebenso individuell eingestellt werden wie das Verhalten beim Doppelklick oder Rechtsklick auf der Titelleiste. So kann etwa das Mausrad auf der Titelleiste das Fenster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

„Effekte“ betreffen Fensteraktionen wie Verkleinern oder Schließen. Sie lassen sich komplett deaktivieren, was aus Hardware- wie Nutzersicht die schnellste und ökonomischste Lösung ist. Wer möchte, kann die Effekte aber unter „Anpassen“ differenziert einstellen sowohl hinsichtlich des Effekttyps wie auch der Effektdauer. ●

Lubuntu mit LXDE

Die kleinste Variante der Ubuntu-Familie ist noch anspruchsloser als Xubuntu. Lubuntu ist mit seinem einfachen, aber funktionalen LXDE-Desktop ein Kandidat für betagte Rechner, kann aber Pragmatikern auch auf moderner Hardware genügen.

Von **Hermann Apfelböck**



Wie bei allen Ubuntu-Varianten fordert der Lubuntu-Kernel eine CPU mit PAE. Das ist aber auch schon die einzige Einschränkung. Lubuntu kommt auf allen Altrechnern zurecht, die wenigstens eine CPU der Sorte Pentium III oder AMD Athlon mitbringen. Beim Arbeitsspeicher genügen theoretisch schon 512 MB, da das System samt Desktop nur etwa 150 MB belegt. Die Oberfläche LXDE ist in doppelter Hinsicht ein pragmatischer Desktop: Er setzt erstens sichtlich auf schlanke und unverzichtbare Komponenten und kombiniert dafür zweitens unter der Haube eine Mixtur aus verschiedenen Bestandteilen. LXDE wird aktuell überarbeitet, um Kompatibilität mit modernen Programmiertoolkits herzustellen. Eventuell werden die folgenden Lubuntu-Versionen den LXDE-Nachfolger LXQT enthalten. Der längst geplante Umstieg verzögert sich seit mehreren Versionen, da Lubuntu mit LXQT den bisherigen LXDE-Fokus beibehalten muss: Das Motto „sehr klein, sehr schnell“ soll bleiben.

Lubuntu liegt wie alle Ubuntu-Varianten derzeit als aktuelle Version 17.10.1 und als LTS-Version 16.04.3 vor (Stand: März 2018). Der Support für die LTS-Langzeitversion reicht im Unterschied zu anderen Ubuntus nur bis April 2019 (statt 2021).

Ein extraschlankes Ubuntu

Die LXDE-Oberfläche bietet einen reduzierten Desktop mit Systemleiste inklusive Applets für Sound, Netzwerk und Uhrzeit sowie ein einfaches Startmenü. Alle anderen Desktopkomponenten und Programme leiht sich LXDE von anderen Desktopumgebungen, wobei Lubuntu schlanken Alternativen stets den Vortritt gibt: Window-Manager ist Openbox, zur Dateiverwaltung steht der einfache Pcmanfm bereit. Weitere mitgebrachte Anwendungsprogramme sind vom XFCE- und Gnome-Desktop übernommen, wobei es auch ganz beliebige Programme aus dem Ubuntu-Fundus zum Installieren gibt. Die Arbeitsumgebung ist flexibel genug, auch Qt-Anwendungen aus dem KDE-Umfeld zu beherbergen. Die nötigen Bibliotheken werden dazu bei der Ausführung solcher Programme automatisch nachgeladen. Dies klingt nach Stückwerk und Flickenteppich, aber Lubuntu bietet insgesamt einen konsistenten und ansehnlichen Desktop.

Die Systemleiste (lxpanel) ist nach Rechtsklick mit grafischer Hilfe optisch wie inhaltlich gut anpassbar und beliebig zu positionieren („Leisteneinstellungen -> Geometrie“). Dabei gelingen Leistenanpassungen im Vergleich zu Xubuntu und Ubuntu Mate sogar einfacher, insbesondere bei vertikaler Anordnung. Für das Erscheinungsbild der Fenster und Schriftgrößen gibt es im Tool obconf („Einstellungen -> Openbox Konfiguration Manager“) diverse Themen und Optionen. Das Aufmacherbild zu diesem Artikel zeigt, dass Lubuntu nach einigen Anpassungen einen konservativen, aber durchaus attraktiven Desktop bieten kann.

Die Standardausstattung liefert ein stattliches Rundumpaket an Systemwerkzeugen. Unter anderem sind Terminal, Gparted, System Profiler, Taskmanager, Laufwerksverwaltung, Synaptic und das grafische Softwarecenter gnome-software an Bord. Bei der Anwendungssoftware bringt Lubuntu hingegen außer dem Browser Firefox nur das Nötigste mit. Die gewünschte Office- und Multimedia-Ausrüstung muss sich der Benutzer daher selbst nach Bedarf ergänzen. Auch der angestammte Dateimanager pcmanfm ver-

dient eventuell eine Ergänzung durch Nautilus oder Nemo, da pcmanfm keine Netzlaufwerke mounten kann.

Anpassungen am LXDE-Desktop

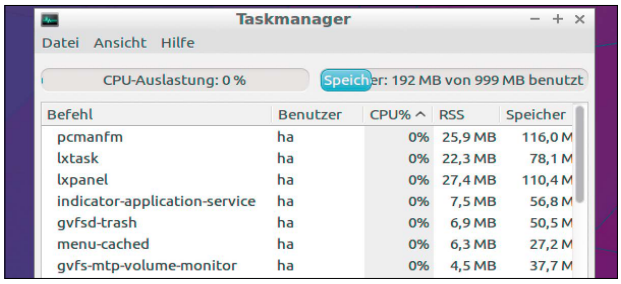
Im klassisch-einfachen Hauptmenü gibt es unter „Einstellungen“ die typischen Applets, um Sprachunterstützung, Energieverwaltung, Netzwerk, Bildschirm und Peripheriegeräte zu konfigurieren. Hier geht es bei bunt gemischten Tools aus LXDE selbst sowie XFCE und Gnome (gnome-language-selector, xfce4-power-manager-settings, lxrandr, lxinput, network-admin) optisch größtenteils etwas schlichter zu als bei großen Desktopdistributionen. Funktional erfüllen diese grafischen Werkzeuge aber Aufgaben völlig zufriedenstellend.

Für die Desktopkonfiguration sind im Wesentlichen die folgenden Anlaufstellen zuständig:

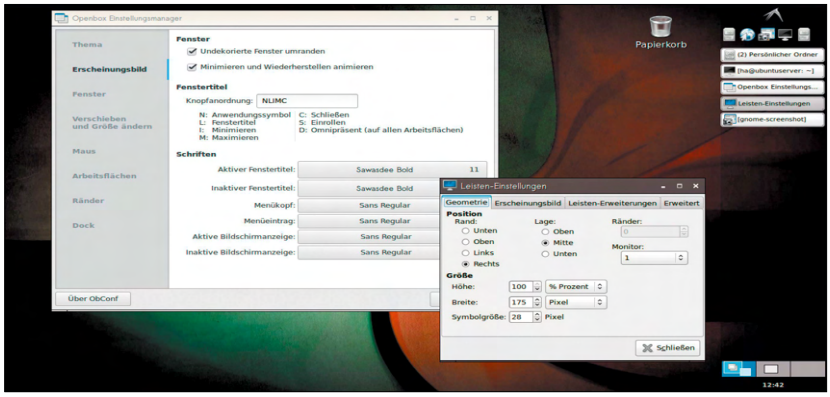
„Einstellungen -> Openbox Konfiguration Manager“ lädt das Tool obconf, das die Fensteroptik, die Fenstertitel, das Mausverhalten und die Anzahl der Arbeitsflächen vorgibt. Beachten Sie, dass sich moderne Gnome- oder KDE-Software nicht an diese Vorgaben der Fensterdekoration hält. Das gilt etwa auch für das standardmäßig installierte Softwarecenter (gnome-software). Solche Integrationsmängel nimmt Lubuntu pragmatisch in Kauf.

„Einstellungen -> Erscheinungsbild anpassen“ startet das Tool lxappearance mit weiteren Feineinstellungen zu Fenster, Fensterrahmen, Icon- und Mauszeiger-Themen und Schriftgrößen.

„Einstellungen -> Desktop Einstellungen“ ist ein Job des Dateimanagers pcmanfm, der dazu mit dem Parameter „pcmanfm --desktop-pref“ aufgerufen wird. Hier ist es vorgesehen, ein Hintergrundbild für den Desktop festzulegen. Interessant ist auch die Registerkarte „Erweitert“ mit der Option, beim (Rechts-)Klick auf den Desktop das Anwendungsmenü des Openbox-Fenstermanagers anzuzeigen. Ist diese Option aktiviert, geht allerdings das normale Rechtsklickmenü am Desktop verloren. Die Entscheidung ist Ermessenssache und nur durch Ausprobieren zu klären.



Ein GB RAM sind für Lubuntu eine Menge Speicher: Das pure System inklusive LXDE-Desktop fordert nur 150 bis 250 MB.



Lubuntu hübsch gemacht: LXDE muss nicht minimalistisch ausfallen. Durch Leistenanpassungen und Optikeinstellungen wird aus dem Ökosystem ein ansehnlicher PC-Desktop.

Die ausbaufähige(n) Systemleisten können Sie durch Rechtsklick auf eine freie Stelle einer Leiste optisch und funktional konfigurieren. Unter „Geometrie“ ist jede vertikale und horizontale Anordnung, Größe und Ausdehnung einstellbar. Die Registerkarte „Erscheinungsbild“ bestimmt die Optik, die über „Durchgehende Farbe…“ auch transparent ausfallen darf.

Funktional entscheidend ist die Registerkarte „Leisten-Erweiterungen“. Hier können Sie mit „Add“ und „Remove“ Leistenapplets einfügen oder entfernen und die gewünschte Position festlegen („Up“, „Down“). Viele Applets sind in diesem Dialog nach dem Markieren außerdem individuell konfigurierbar.

Unbedingt notwendig ist das etwa bei der „Anwendungsstartleiste“, um die dort angehefteten Programmfavoriten individuell einzurichten. Die einzelnen Leistenelemente lassen sich allerdings auch jederzeit nach Rechtsklick auf das Element anpassen.

Der Desktop selbst ist über den Dateimanager pcmanfm ein normaler Ordner und kann als Datei- und Ordnerablage genutzt werden. LXDE fördert dies, indem es beim Rechtsklick auf einen Eintrag im Hauptmenü die Option „Der Arbeitsfläche hinzufügen“ anbietet.

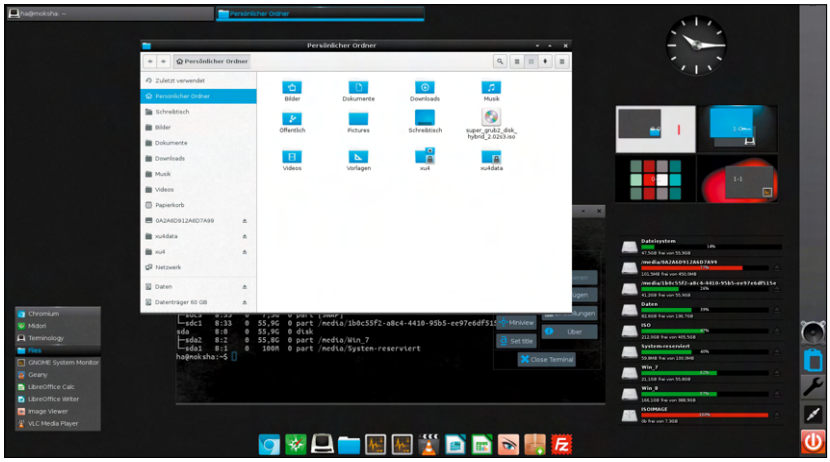
Lubuntu 16.04.3 oder 17.10.1

Systembasis:	Ubuntu 16.04.3 oder 17.10.1
Einsatzzweck:	Desktop für ältere PCs und Notebooks
Zielgruppe:	alle, auch Einsteiger
Hardwareansprüche:	sehr anspruchslos
Projektseite:	*http://lubuntu.net/*
Merkmale:	einfache, aber funktionale und anpassungsfähige Oberfläche, spartanische Software-Standardausstattung

Bodhi Linux für Experimentierfreudige

Bodhi Linux mit Moksha-Desktop ist exotisch. Wer mit konservativen Erwartungen herangeht, wird sich verirren oder kapitulieren. Bodhi lohnt aber eine Investition: Das System ist frappierend schnell, anpassungsfähig und sparsam.

Von **Hermann Apfelböck**



Bodhi ist keine Distribution für Pragmatiker. Wer sein System schnell eingerichtet haben will, wird sich mit den minutiösen bis verwirrenden Einstellungen dieser Oberfläche nicht anfreunden. Auch enthält die mitgelieferte Software nur das Allernotwendigste und macht Nachinstallationen unerlässlich – vorzugsweise über apt im Terminal. Zielgruppe sind Nutzer, die Wert auf einen individuellen Desktop legen und bereit sind, dafür auch einige Zeit zu investieren. Bodhi basiert auf Ubuntu, sein eigenwilliger Desktop Moksha ist eine Abspaltung von Enlightenment (oder schlicht „E“).

Bodhi Linux: Ein Speed-Ubuntu

Bodhi spielt in der Ökoliga der Linux-Distributionen und liefert für sehr alte Hardware sogar noch eine Non-PAE-Variante aus (siehe unter *www.bodhilinux.com/download* „Legacy“-Variante für sehr alte Rechner). Das entscheidende Motiv für Bodhi sollte das aber nicht mehr sein: Für schwache Hardware gibt es einfachere und solidere Distributionen (Antix, Bunsenlabs). Außerdem ist Moksha modular aufgebaut: Bei größter Sparsamkeit kommt das System nach Anmeldung mit 150 MB RAM aus, sind aber alle Module aktiviert und einige Desktopelemente eingerichtet, liegt der Speicherbedarf schnell bei 250 MB und mehr. Hauptmotive für Bodhi Linux sind daher eher andere Aspekte:

1. Bodhi ist ein frappierendes Speed-Ubuntu: Beim Systemstart zur Anmeldung zählen wir auf schneller Hardware (mit SSD) neun Sekunden. Mittelschwere Programme sind schneller eingabebereit, als der Mausfinger von der Auslösetaste zurückkommt.

2. Moksha ist eine komplett grafisch konfigurierbare Oberfläche. Wirklich jedes Detail ist über grafische Anpassungsdialoge per Maus zu erreichen. Das gelingt nicht überall konsistent, führt zu unzähligen kleingliedrigen Einstellungsfenstern, erspart aber jedes Editieren von Konfigurationsdateien.

3. Moksha ist ein extravaganter und liberaler Desktop. Der Nutzer kann über jedes Modul selbst entscheiden, ob er es benötigt und wie sich ein gewähltes Element verhalten soll. Dieser Desktop ist ein Gegenentwurf zu den simplifizierenden Oberflächen Gnome oder Unity.

Erste Orientierung in Bodhi Linux

Da Bodhi auf Ubuntu basiert, erledigt die Installation der zuverlässige Ubuntu-Installer Ubiquity (siehe Seite 34). Standardmäßig präsentiert Bodhi eine Systemleiste („Shelf“ oder deutsch „Modulablage“). Die ist ab Start durchaus konservativ bestückt mit Startmenü, Favoritenbereich, Taskübersicht und einem Infobereich. Im Grunde handelt es bei den „Shelves“ um Modulcontainer, die an beliebigen Bildschirmrändern beliebig mit „Modulen“ befüllt werden können.

Das Startmenü ist nicht nur über die Leiste, sondern auch mit normalem (Links-)Klick auf eine freie Desktopstelle zu erreichen, während ein Rechtsklick am Desktop eine Auswahl von Programmfavoriten anbietet, die Sie allerdings erst definieren müssen.

Die entscheidende Konfigurationszentrale ist im Menü über „Einstel-

lungen -> Einstellungskonsole“ zu erreichen („Settings -> Settings Panel“).

Ein erster wesentlicher Gang führt nach „Language“. Sehr wahrscheinlich fehlt diese Kategorie noch und dies ist erste Gelegenheit, den modularen Aufbau von Moksha kennenzulernen: Unter „Extensions -> Modules“ („Erweiterungen -> Module“) finden Sie die komplette Sammlung der verfügbaren Module, geordnet nach Kategorien. Das Sprachmodul findet sich unter „Settings“ und lässt sich mit Klick auf „Load“ aktivieren. Dies erweitert die Einstellungskonsole dann um den neuen Punkt „Language“, wo Sie die Oberfläche nach Deutsch umstellen.

Ein wichtiger Verwaltungspunkt in der Einstellungskonsole sind die „Einstellungen“ mit dem Unterpunkt „Profile“. Hier ist es nämlich möglich, den aktuellen Zustand über „Hinzufügen“ als Profil zu speichern. Außerdem liegen die Standardprofile „Bodhi Linux“ und „Default“ vor, auf die Sie durch Markieren und „Übernehmen“ jederzeit zurückkehren können.

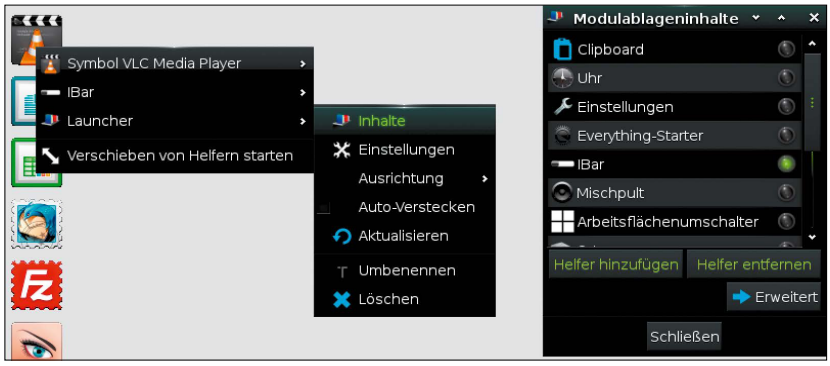
Fundamente der Optik richten Sie in der ersten Kategorie „Aussehen“ ein. Während „Thema“ die Moksha-eigenen Dialoge und die Fenstertitel betrifft, ändert „Anwendungsthema“ das Aussehen von Programmen, die auf GTK basieren. Ein wichtiger Unterpunkt ist hier ferner die „Skalierung“, die alle Moksha-Fenster stufenlos in der gewünschten Größe einstellt.

In der zweiten Kategorie „Anwendungen“ lohnt es sich, „Bevorzugte Anwendungen“ zu definieren, sofern Sie am Desktop das Rechtsklick-Menü verwenden wollen. Dazu markieren Sie in Liste das betreffende Programm und klicken auf „Hinzufügen“.

Der nachfolgende Punkt „iBar-Anwendungen“ (unter „Anwendungen“) ist nur dann relevant, wenn Sie in einer Systemleiste („Shelf“) das Modul iBar tatsächlich verwenden – es handelt sich ebenfalls um einen Favoritenstarter. Das Modul iBar ist ein Beispiel für die zum Teil konfuse Komplexität des Desktops: Das Modul muss unter „Erweiterungen -> Module“ aktiviert sein, und es muss unter „Erweiterungen -> Modulablagen -> Inhalte“ in eine Modulablage (Shelf) integriert werden. Konfiguriert und bestückt wird es aber unter „Anwendungen -> iBar-Anwendungen“.



Schaltzentrale: Die Einstellungskonsole ist der Dreh- und Angelpunkt der Desktopkonfiguration. Der Umfang lässt sich unter „Erweiterungen -> Module“ festlegen.



Komplexe Leistenanpassung: Um die Modulablage selbst und nicht etwa nur ein Modul anzupassen, müssen Sie nach Rechtsklick den blau-roten Eintrag wählen.

Leisten und „Helfer“ einrichten

Neben dem Hauptmenü sind Leisten („Modulablagen“) und Desktopgadgets („Helfer“) die prägenden Elemente. Eine Leiste kann viele Module aufnehmen, ein „Helfer“ ist ein einzelnes Modul am Desktop. Die Module sind aber hier und dort dieselben.

„Modulablagen“ (Leisten): Wenn Sie eine bestehende Leiste rechts anklicken, erscheint unter anderem die Option „Shelf…“. Hier kommen Sie dann über „Inhalte“ an die Module und können aktuell enthaltene (farbiges Symbol) entfernen oder inaktive (graues Symbol) hinzufügen. Wenn eine Modulablage mehrere Module enthält, gibt es nach Rechtsklick außerdem die Möglichkeit, die Einzelteile innerhalb der Leiste zu verschieben.

„Helfer“ (Gadgets): Ein einzelnes Modul am Desktop definieren Sie in der Einstellungskonsole unter „Erweiterungen -> Helfer -> Ebenen -> Hintergrund“. Das neue Modul kann dann verschoben und skaliert werden. Dies funktioniert auch nach Rechtsklick auf das Modul, Klick auf den Modulnamen und „Einstellungen“.

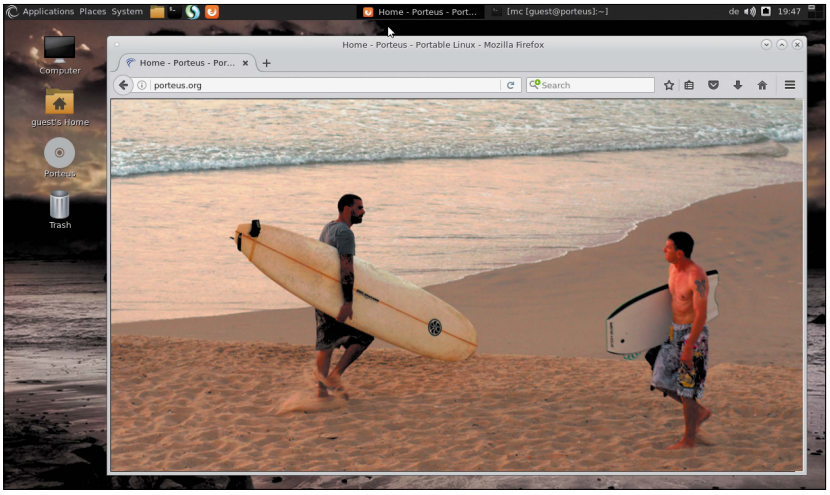
Bodhi Linux 4.5.0

Systembasis:	Ubuntu 16.04 LTS
Einsatzzweck:	Zweitsystem, Desktop für ältere Geräte (auch ohne PAE)
Zielgruppe:	Experimentierfreudige
Hardwareansprüche:	sehr gering
Projektseite:	*www.bodhilinux.com*
Merkmale:	klein, extrem schnell, eigenwilliger Desktop Moksha (E17)

Porteus: Elegantes Surfsystem

Ausgewachsene Livesysteme haben den Anspruch, eine möglichst komplett eingerichtete Arbeitsumgebung zu starten, meist auch mit Tools für den Notfall. Zum Surfen ideal ist aber ein ballastfreies und flott startendes Minisystem wie Porteus.

Von **Hermann Apfelböck und David Wolski**



In einem ausgewachsenen Livesystem wie Knoppix und Kanotix ist der Browser ein Programm unter vielen anderen. Bei Minisystemen zum Surfen stehen dagegen die Webbrowser im Mittelpunkt und neben grafischer Oberfläche, Netzwerkchip-Treibern und Konfigurationstools sind nur wenige Werkzeuge mit an Bord. Porteus ist in seiner Basisvariante ohne Extras ein besonders kleiner, erweiterbarer Vertreter dieser Klasse von Linux-Systemen. Der Name setzt sich aus „Portabilität“ und dem Namen Proteus aus der griechischen Mythologie zusammen, der seine Daseinsform nach Belieben ändern konnte. Porteus ist ein schnelles, ansehnliches sorgfältig zusammengestelltes Livesystem mit mehreren Desktops zur Auswahl, das einen Rechner schnell und unkompliziert zu einer Surfstation macht. Das installierte Betriebssystem auf der Festplatte wird dabei nicht angetastet.

Livesysteme Porteus Linux ohne Installation

Livesysteme brachten Linux in den frühen Zeiten des freien Betriebssystems einem größeren Benutzerkreis näher, da die Linux-Installation mit textbasierten Installern und manueller Hardwarekonfiguration noch bis vor 15 Jahren ein Thema für Spezialisten war. Knoppix war das erste brauchbare Linux-Livesystem und nahm Anwendern mit seinen automatisierten Konfigurations-Scripts zur Hardwareerkennung eine Menge Arbeit ab. Knoppix setzt auf Debian auf, liefert mit seinen Start-Scripts aber das technische Vorbild für nahezu alle heute populären Livesysteme: Nach dem Boot des Kernels liefert ein kleines Ramdisk-Abbild, das in den Speicher entpackt wird, alle nötigen Binaries (Programme) und Scripts für den weiteren Startprozess. Das eigentliche Livesystem liegt in einem ebenfalls gepackten umfangreichen Dateisystemabbild, das alle Software sowie Desktopumgebung platzsparend auf dem Startmedium unterbringt.

Porteus nutzt Slackwaretechnik: Porteus folgt diesem allgemeinen Prinzip, hat aber andere Wurzeln und baut auf Slackware Linux auf, einer weniger bekannten, aber besonders flexiblen Distribution. Eine überschaubare Schar von Experten schwört nach wie vor auf die Vorzüge von Slackware, mit dem sich sehr kompakte, spezialisierte Linux-Systeme bauen lassen. Für Slackware gibt es ein eigenes vorbereitetes Set an Scripts für die Erstellung von Livesystemen, die „Linux Live Scripts“ (*https://www.linux-live.org*). In modifizierter Variante kommen diese auch bei Porteus zum Einsatz.

Im Gegensatz zu anderen Livesystemen, die ein komplett vorbereitetes Linux starten, ist Porteus modular aufgebaut. Neben den Basismodulen für Kernel, Systemtools und der grafischen Oberfläche Xorg können weitere Module das Livesystem ergänzen. Diese Module stammen von Slackwarepaketen ab und fügen sich beim Laden in die vorhandene Verzeichnisstruktur des Livesystems ein.

Software nachrüsten

Der modulare Aufbau macht Porteus wandlungsfähig. In der Desktopedition steht Porteus deshalb wahlweise mit Cinnamon, Mate, KDE oder XFCE als Desktop zum Download bereit (*http://linux.rz.rub.de/porteus/i586*).

In seiner Basisausführung hat Porteus seit Version 3.2 keine Browser mehr vorinstalliert und die ISO-Dateien des Livesystems liefern nur das Grundsystem mit dem jeweiligen Desktop. In dieser Form ist Porteus kein schlüsselfertiges Livesystem, denn bevor es einen Nutzen erfüllen kann, muss noch Software nachgerüstet werden. Dazu enthält Porteus einen Paketmanager im Anwendungsmenü unter „Applications -> System Tools -> USM (Unified Slackware Package Manager)“. Die Installation eines Pakets erfolgt in mehreren Schritten: Zuerst wird über „Updates -> Update All“ die Paketdatenbank aufgefrischt. Nach der Suche des gewünschten Pakets lädt es ein Klick auf die Option „Convert to modules“ und „Download“ herunter.

Anschließend zeigt die Schaltfläche „Yes“ den Ordner des Pakets an, das jetzt als Porteus-Modul vorliegt. Ein Rechtsklick auf die Moduldatei mit der Endung „xzm“ bindet das Programm mit „Open with activate“ in das laufende System ein.

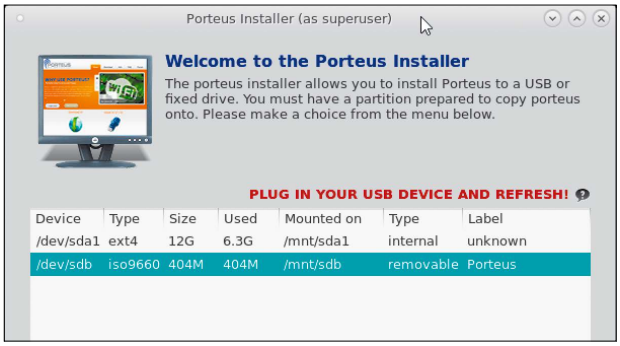
Kiosk-Variane

Die Kiosk-Variante von Porteus ist besonders einfach: Hier startet ausschließlich Firefox. Es gibt keinerlei Zugriff auf das System, und auch Firefox speichert keine Infos wie Verlauf oder Kennwörter. Beendet wird das System durch Abschalten des Geräts.

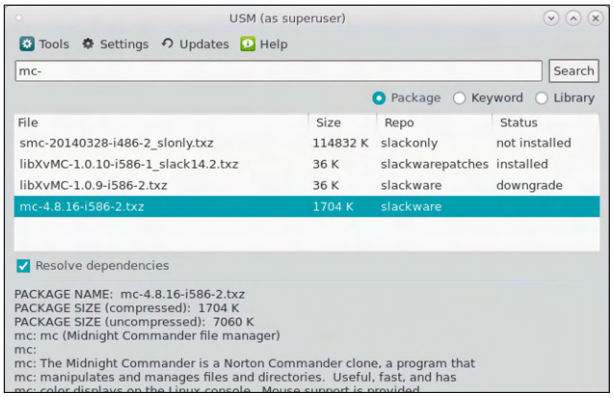
Erhältlich ist die Kiosk-Variante Porteus 4.6.0 unter http://porteus-kiosk.org/ als ISO-Image. Sie schreiben es zum Beispiel mit folgendem Befehl auf einen USB-Stick, um dann Porteus von diesem Stick aus zu installieren:

dd if=Porteus-Kiosk-4.6.0-x86_64.iso of=/dev/sdb

Die Kennung „sdc“ ist ein Beispiel – bitte passen Sie das unbedingt auf Ihr System an. Booten sie mit dem USB-Stick einen Rechner. Er startet ein Installer-Image, denn erst damit erfolgt nun der Zusammenbau des endgültigen Porteus-Systems. Sie wählen zunächst die Netzverbindung (Kabel oder WLAN), ferner den Browser (Firefox oder Chrome) und danach diverse Detaileinstellungen. Wir zählen insgesamt knapp 50 Einstellungen, die Sie treffen können und die ganz brauchbar englischsprachig erklärt werden. Lassen Sie sich hier Zeit, denn die Konfiguration ist dann endgültig und muss im Fehlerfall mit dem Installer-ISO wiederholt werden: Die Vorgaben sind zwar allesamt sinnvoll, aber einige manuelle Änderungen sollten Sie in jedem Fall vornehmen.



Schnellster Weg auf einen USB-Stick: Der Installer im Anwendungsmenü richtet das laufende Livesystem in wenigen Schritten auf USB-Stick ein.



Porteus ergänzen: Das System auf Heft-DVD liefert Firefox und Chromium bereits mit. Der Paketmanager installiert bei Bedarf weitere Programme als Modul im Livesystem.

Mindestens eine Suchmaschine als Startpage sollte eingestellt werden. Ob Sie die Voreinstellung des generellen „Private Mode“ haben möchten, ist ebenfalls zu überlegen. Auf Wunsch können Navigations-Buttons aktiviert werden. Deutsches Keyboard als primäres Layout ist wichtig, ferner am Ende die Optionen, das System per SSH oder VNC fernwarten zu können. Wenn Sie durch alle Optionen durch sind, können Sie diese Konfiguration entweder als ISO-Image ablegen („Save ISO“) oder gleich direkt auf den Zieldatenträger schreiben („Install ISO“). Ideal sind USB-Sticks oder eine SD-Karte, weil das System kaum 100 MB beansprucht.

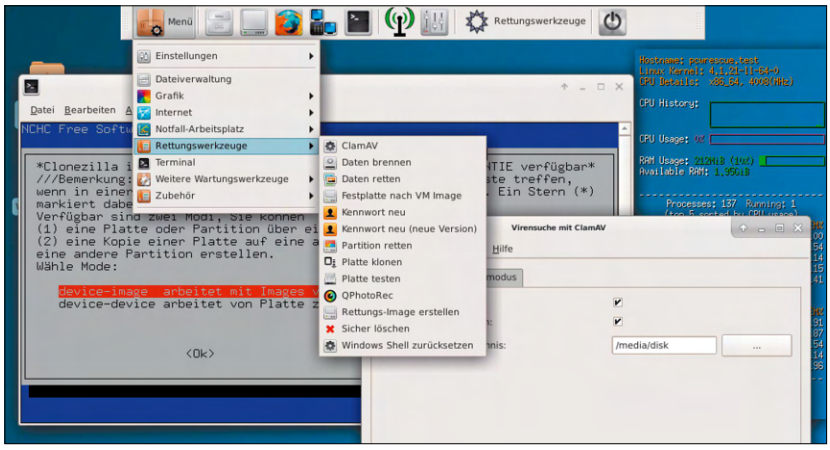
Porteus 3.2.2

Systembasis:	Slackware Linux.
Einsatzzweck:	kompaktes, elegantes Surfsystem
Zielgruppe:	Einsteiger, gelegentliche Linux-Anwender
Hardwareansprüche:	gering
Projektseite:	*www.porteus.org (Downlaod: http://linux.rz.rub.de/porteus/i586)*
Merkmale:	Der enthaltene Paketmanager kann Porteus zur Laufzeit um weitere Programme ergänzen.

Linux rettet Windows

Ein bootbares Zweitsystem auf Linux-Basis kann bei vielen Windows-Problemen helfen. Die PC-WELT-Rettungs-DVD bietet Tools, die auf havarierte Windows-Systeme spezialisiert sind.

Von **Thorsten Eggeling**



Hilfe für Windows: Die Rettungs-DVD enthält Tools, mit denen Sie Festplatten klonen, nach Schadsoftware suchen und ein vergessenes Windows-Kennwort zurücksetzen.

Einige Windows-Probleme lassen sich nur über ein Zweitsystem beheben. Das ist beispielsweise dann nötig, wenn Windows nicht mehr startet und Sie akut einige wichtige Dateien des defekten Systems benötigen. Das Rettungssystem hilft aber auch, wenn ein vergessenes Anmeldepasswort oder Schadsoftware die normale Windows-Nutzung verhindern.

Die PC-WELT-Rettungs-DVD starten

Laden Sie die ISO-Datei der PC-WELT Rettungs-DVD über *www.pcwelt.de/1168242* herunter und brennen Sie damit eine DVD. Unter Linux verwenden Sie dazu das Kontextmenü des Dateimanagers, in dem ein passendes Brennprogramm zu finden sein sollte. Noch besser ist es, das System auf einen USB-Stick zu kopieren. Es startet dann schneller. Am einfachsten geht das mit dem Tool dd wie auf *www.pcwelt.de/2261312* beschrieben. Unter Windows verwenden Sie den Win 32 Disk Imager (auf Heft-DVD).

Der USB-Stick lässt sich auch aus dem laufenden Livesystem heraus erstellen. Dazu gehen Sie im „Menü“ auf „Zubehör -> Installation auf USB-Laufwerk“, wählen das Ziellaufwerk, setzen optional ein Häkchen vor „Verschlüsseltes /home erstellen“ und ändern dahinter bei Bedarf die Größe. Danach klicken Sie auf „Installation starten“. Sie werden dann beim ersten Start des Systems aufgefordert, ein Passwort für das verschlüsselte Verzeichnis zu vergeben.

Wenn Sie einen PC mit der PC-WELT-Rettungs-DVD booten, sehen Sie ein Menü, in dem Sie in der Regel den ersten Eintrag wählen. Sollte das nicht funktionieren, finden Sie unter „Sicherer Start“ weitere Optionen. Wählen Sie beispielsweise „VESA graphics auto“, wenn der Bildschirm schwarz bleibt.

Netzwerkverbindung herstellen: Wenn der PC per Kabel mit dem Netzwerk verbunden ist, sollte die Konfiguration automatisch erfolgen. Mit einem Klick auf die Menüschaltfläche links oben und „Internet -> Wicd Network Manager“ starten Sie ein Programm, über das Sie die Netzwerkkonfiguration prüfen und bei Bedarf ändern können. Hier wählen Sie auch Drahtlosnetze aus und geben den WLAN-Schlüssel ein.

Das funktioniert jedoch nur, wenn ein von Linux unterstützter WLAN-Adapter im PC steckt.

Nach Schadsoftware suchen

Kommt es bei Windows zu Abstürzen, unerklärlichem Verhalten oder ungewöhnlichen Netzwerkzugriffen, kann ein Virus dahinterstecken. Für die Diagnose starten Sie den Virenscanner von der PC-WELT-Rettungs-DVD. Klicken Sie auf die Menüschaltfläche und dann auf „Rettungswerkzeuge -> ClamAV“. Wählen Sie die Option „Alle NTFS- und FAT-Laufwerke automatisch nur lesbar einbinden“. Klicken Sie auf „Weiter“. Im Fenster „Virensuche mit ClamAV“ gehen Sie auf „Informationen -> Aktualisieren“, um die aktuellen Virendefinitionen herunterzuladen. Schließen Sie das Fenster per Klick auf „OK“ und klicken Sie auf „Durchsuchen starten“. Der Vorgang kann – je nach Datenmenge – sehr lange dauern. Der Virenscanner zeigt in der Standardkonfiguration die Funde nur an, ändert aber nichts auf der Festplatte.

Sollte der Virenscanner fündig werden, müssen Sie entscheiden, wie Sie weiter vorgehen. Zuerst informieren Sie sich im Internet über die Funktion der Schadsoftware. Im Rettungssystem verwenden Sie dafür den Browser Firefox. In einigen Fällen kann es sinnvoll sein, die betroffene Partition mit Schreibzugriff einzubinden (siehe

nächster Punkt) und dem Virenscanner die Bereinigung zu überlassen. Die Optionen dafür setzen Sie auf der Registerkarte „Expertenmodus“.

Meist lässt sich jedoch nicht sicherstellen, dass tatsächlich alle Bedrohungen restlos entfernt wurden. Zudem können wahrscheinlich nur Sicherheitsexperten ermitteln, auf welchem Weg ein Virus auf den PC gelangt ist und über welche Methoden er sich automatisch reaktiviert. Deshalb hilft oft nur die Radikalkur: Sichern Sie alle persönlichen Benutzerdaten, formatieren Sie die Festplatte und installieren Sie dann Windows neu.

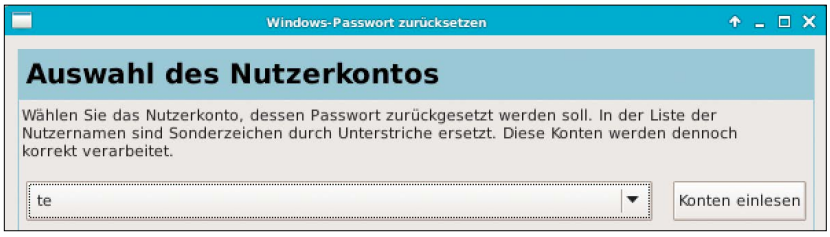
Dateien von der Festplatte retten

Wenn Windows nicht mehr startet oder ständig abstürzt, ist nicht immer Zeit, sich sofort um die Reparatur zu kümmern. Sie wollen vielleicht nur eine Excel-Datei von der Festplatte retten und an einem anderen PC weiterarbeiten. Sollte ein Virenbefall das Problem sein, können Sie über die PC-WELT-Rettungs-DVD Ihre persönlichen Dateien vor der Neuinstallation auf ein anderes Laufwerk kopieren.

Verbinden Sie das USB-Gerät mit dem PC und binden Sie die Partitionen ein. Klicken Sie dazu in der Symbolleiste auf das dritte Icon „Festplatten einbinden“. Sie sehen eine Liste mit den gefundenen Partitionen, in der Sie beispielsweise auf „Partition 2 (sda2, ntfs) einbinden“ klicken. Die zweite Partition ist in der Regel die Windows-Systempartition, die erste die Bootpartition. Der USB-Stick taucht dann etwa als „sdb1“ auf. Setzen Sie beim USB-Stick und bei anderen Partitionen, für die Sie Schreibzugriff benötigen, ein Häkchen vor „schreibbar?“. Das ist bei der Systempartition jedoch nur möglich, wenn Sie Windows zuvor vollständig heruntergefahren haben. Andernfalls erhalten Sie eine Fehlermeldung, die sich nur über ein noch funktionierendes Windows beheben ließe, indem Sie Windows 8.1/10 mit „Neu starten“ beenden (nicht über „Herunterfahren“). Beim Einbinden öffnet sich automatisch der Dateimanager „Thunar“. Gehen Sie in das Verzeichnis, aus dem Sie Daten kopieren möchten. Das Kopieren funktioniert mit dem Linux-Dateimanager wie unter Windows gewohnt etwa mit den Tastenkombinationen Strg-C und Strg-V.



WLAN-Zugriff: Gehen Sie auf „Internet -> Wicd Network Manager“. Klicken Sie beim gewünschten Funknetz auf „Verbinden“ und geben Sie den WPA-Schlüssel ein.



Windows-Kennwort vergessen? Die Windows-Partition findet das Tool in der Regel automatisch. Sie müssen nur den Benutzer auswählen, dessen Kennwort Sie löschen möchten.

Weitere Rettungswerkzeuge nutzen

Mit Clonezilla, das Sie über das Icon auf dem Desktop starten, erstellen Sie Sicherungskopien von Festplatten und Partitionen oder ziehen das System auf eine neue Festplatte oder SSD um. Das Programm bietet viele Optionen, weshalb wir hier auf eine ausführliche Beschreibung verzichten müssen und auf *www.pcwelt.de/1998643* verweisen. Über das Menü „Rettungswerkzeuge“ starten Sie Tools, über die Sie beispielsweise das Windows-Passwort zurücksetzen, die Festplatte testen und Dateien oder Partitionen wiederherstellen. Unter „Weitere Wartungswerkzeuge“ finden Sie das Partitionierungstool Gparted, mit dem sich Partitionen erstellen, vergrößern oder verkleinern lassen. Außerdem gibt es den Registryeditor „Fred“, über den Sie Werte in der Windows-Registry einsehen und ändern können.

Im Terminalfenster starten Sie den Dateimanager Midnight Commander (mc), der über SSH auch die Datensicherung auf einen Linux-PC ermöglicht. Experten nutzen das Tool wimlib-imagex (*https://wimlib.net*), das unter Linux als Open-Source-Ersatz für Imagex und Dism dient. Damit lässt sich Windows in WIM-Dateien sichern oder aus WIM-Archiven extrahieren.

PC-WELT-Rettungs-DVD

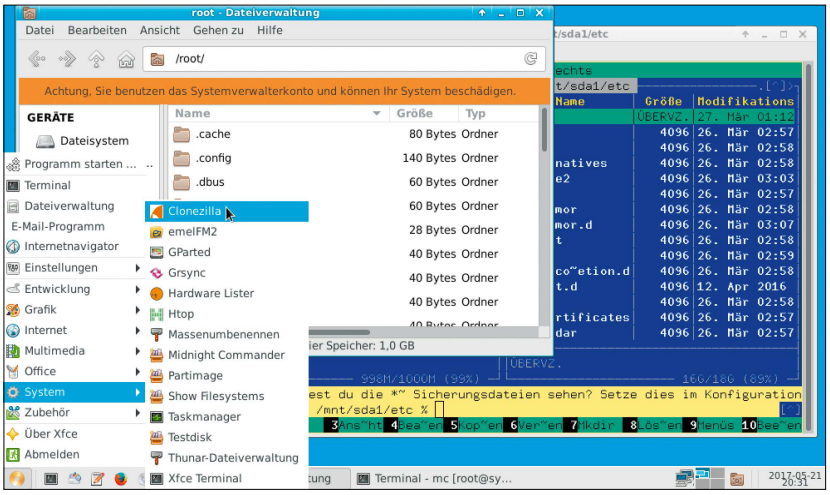
Systembasis:	Lesslinux
Einsatzzweck:	Rettungssystem für Windows
Zielgruppe:	Einsteiger bis Fortgeschrittene
Hardwareansprüche:	gering
Projektseite:	*www.pcwelt.de/1168242*
Merkmale:	Livesystem mit zahlreichen spezialisierten Tools zur Analyse und Reparatur von Windows-Problemen

Linux mit Zweitsystem reparieren

Einige Linux-Probleme lassen sich nur über ein zweites System beheben, das Sie bei Bedarf von einer DVD oder einem USB-Stick booten. Ein dafür spezialisiertes System ist die neue LinuxWelt-Rettungs-DVD (auf Heft-DVD).

Von **Thorsten Eggeling**

Eine Live-DVD ist bei der Linux-Reparatur vor allem in Fällen hilfreich, wo Sie das Passwort vergessen haben oder das installierte System aufgrund eines Fehlers in der Bootmanager-Konfiguration nicht mehr bootet. Zur Behebung der Probleme reicht meist schon das Installationsmedium des jeweiligen Linux-Systems aus. Mehr Komfort bieten jedoch Rettungssysteme, die spezielle Tools für Reparatur und Analyse bieten. Auf der Heft-DVD finden Sie dafür die „LinuxWelt-Rettungs-DVD“.



Spezialisiertes Reparatursystem: Die LinuxWelt-Rettungs-DVD startet mit einer grafischen Oberfläche und vielen wichtigen Werkzeugen, die Linux-Probleme beseitigen.

LinuxWelt-Rettungs-DVD starten

Die LinuxWelt-Rettungs-DVD basiert auf System Rescue CD (*www.system-rescue-cd.org*) und Gentoo Linux (*www.gentoo.org*). Anders als beim Original gibt es jedoch eine deutschsprachige Oberfläche und einige zusätzliche Tools. Das System startet standardmäßig mit der grafischen Oberfläche XFCE und deutscher Tastaturbelegung. Die Anleitungen *www.system-rescue-cd.org* gelten größtenteils auch für die LinuxWelt-Rettungs-DVD. PCs im Bios-Modus können direkt von der Heft-DVD booten. Wenn Sie das System im Uefi-Modus booten wollen, müssen Sie es auf einen USB-Stick übertragen. Einen bootfähigen USB-Stick erstellen Sie am einfachsten über das Tool dd wie auf *www.pcwelt.de/2261312* beschrieben. Verbinden Sie den USB-Stick mit dem PC und öffnen Sie ein Terminal. Mit dem Befehl

```
lsblk -p
```

ermitteln Sie die Kennung des USB-Laufwerks. 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“. Kopieren Sie dann die Datei „/Image-Dateien/lwRescue601.iso“ von der Heft-DVD in Ihr Home-Verzeichnis. Geben Sie dann im Terminal folgenden dd-Befehl mit angepassten Pfaden ein. Nach „if=“ folgt Pfad und Name der ISO-Datei, nach „of=“ der Gerätename des USB-Sticks:

```
sudo dd bs=1M if=/pfad/lw-
  Rescue601.iso of=/dev/sd[X]
```

„[X]“ steht hier für die Laufwerksbezeichnung, die Sie schon zuvor bei umount verwendet haben. Warten Sie ab, bis die Eingabeaufforderung wieder erscheint, dann können Sie den USB-Stick abziehen und verwenden.

Startvarianten: Wenn Sie die LinuxWelt-Rettungs-DVD direkt von der Heft-DVD booten, erhalten Sie ein anderes Menü als beim USB-Stick oder einer selbst erstellten DVD. In der Regel starten Sie das System mit dem ersten Menüeintrag. Sollte das System mit Fehlern starten oder nur einen schwarzen Bildschirm zeigen, verwenden Sie einen USB-Stick. Sie können dann zwischen einem Kernel mit 32 Bit oder 64 Bit wählen und beispielsweise „C) 64-Bit-Kernel (rescue 64) mit weiteren Optionen -> Rettungs-DVD mit VESA-Grafik“ wäh-

len. Über die Tasten F2 bis F7 blenden Sie Hilfetexte ein, die Informationen zu den Bootoptionen für die Problembehebung enthalten.

Netzwerk konfigurieren: Das Rettungssystem erkennt Netzwerkadapter und stellt eine Ethernet-Verbindung her. Nach einem Mausklick auf das Icon des Netzwerkmanagers im Panel am unteren Bildschirmrand sehen Sie dann den Menüeintrag „Kabelgebundene Verbindung 1“. Ist ein von Linux unterstützter WLAN-Adapter vorhanden, sehen Sie die verfügbaren WLAN-Netze und können sich mit dem Zugangspasswort anmelden.

Zugriff auf Festplattenpartitionen

Die LinuxWelt-Rettungs-DVD bindet Partitionen nicht automatisch ein. Wenn Sie auf die Dateien eines installierten Systems zugreifen möchten, verschaffen Sie sich zuerst über das Menü und „System -> Show Filesystems“ einen Überblick. Sie sehen, welche Festplatten im PC stecken, sowie die zugehörigen Partitionen, Partitionsgrößen und Dateisysteme.

In der Liste taucht beispielsweise „sda1“ auf, in der Spalte „FILESYS“ sehen Sie „ext4“. Binden Sie diese Partition über folgenden Befehl im Terminalfenster ein:

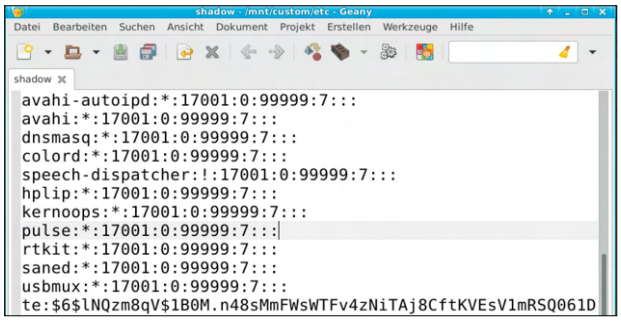
```
mount /dev/sda1 /mnt/custom
```

Sollte es sich um eine Windows-NTFS-Partition handeln, verwenden Sie beispielsweise diese Befehlszeile, damit auch der Schreibzugriff erlaubt ist:

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

Anschließend starten Sie den Dateimanager über „Zubehör -> Thunar Dateiverwaltung“. Im Terminal steht Ihnen außerdem der Dateimanager Midnight Commander zur Verfügung (mc).

Über den Dateimanager greifen Sie auf die eingehängten Partitionen unter „/mnt“ zu. Über das Kontextmenü bearbeiten Sie in Thunar Konfigurationsdateien („Mit Geany öffnen“) oder sichern Ordner in einer tar.gz-Datei („Archiv erstellen“). Per Klick auf „Netzwerke durchsuchen“ greifen Sie auf Netzwerkfreigaben zu, die Sie etwa für die Datensicherung verwenden.



Ohne Passwort anmelden: Wenn Sie Ihr Passwort vergessen haben, öffnen Sie die Datei „shadow“ des installierten Systems und löschen das verschlüsselte Passwort.

Passwort löschen oder Grub reparieren

Wenn Sie das Passwort für die Linux-Anmeldung nicht mehr wissen, binden Sie die Partition des installierten Systems ein wie im vorherigen Punkt beschrieben. Gehen Sie in das Verzeichnis „/etc“ der eingehängten Linux-Partition und öffnen Sie die Datei „shadow“ über Thunar per Rechtsklick und „Mit Geany öffnen“. Sie sehen Einträge wie

```
[UserName]:$1$aB7mx
  0L[...]:16668:0:99999:7:::
```

Die lange Zeichenfolge hinter dem Benutzernamen zwischen den Doppelpunkten ist das verschlüsselte Passwort. Sie löschen die Zeichenfolge einfach und speichern die Datei. Danach starten Sie das installierte System und melden sich ohne Passwort an.

Bootmanager reparieren: Bei einem standardmäßig installierten Linux-System im Bios-Modus hängen Sie zuerst die Systempartition in „/mnt/custom“ ein wie oben beschrieben. Dann verwenden Sie im Terminalfenster folgende sechs Befehlszeilen:

```
mount -o bind /dev /mnt/custom/dev
mount -o bind /sys /mnt/custom/sys
mount -t proc /proc /mnt/custom/
  proc
chroot /mnt/custom /bin/bash
grub-install /dev/sdX
update-grub
```

„/dev/sdX“ ersetzen Sie durch den Laufwerkspfad der Festplatte, auf der das System installiert ist.

Bei einem Uefi-System müssen Sie zusätzlich die EFI-Partition in „/mnt/custom/boot/efi“ einhängen. Starten Sie in der chroot-Umgebung *grub-install* ohne Angabe der Zielpartition und danach *update-grub*.

Weitere Tools der LinuxWelt-Rettungs-DVD

Über das Menü oder Terminalfenster starten Sie Programme, die Ihnen bei der Analyse oder Reparatur eines Linux-Systems helfen können. Mit an Bord sind der Webbrowser Firefox, der FTP-Client Filezilla, ein Bildbetrachter und ein PDF-Viewer. Über „System -> Hardware Listener“ oder im Terminal mit *lshw* ermitteln Sie, welche Hardware im PC steckt. Mit Testdisk stellen Sie im Terminal versehentlich gelöschte Partitionen wieder her, mit Photorec gelöschte Dateien. Clonezilla erstellt Imagebackups von Partitionen und Festplatten und stellt diese bei Bedarf auch wieder her. Mit Gparted partitionieren Sie Festplatten oder ändern Partitionsgrößen ohne Datenverlust.

LinuxWelt-Rettungs-DVD

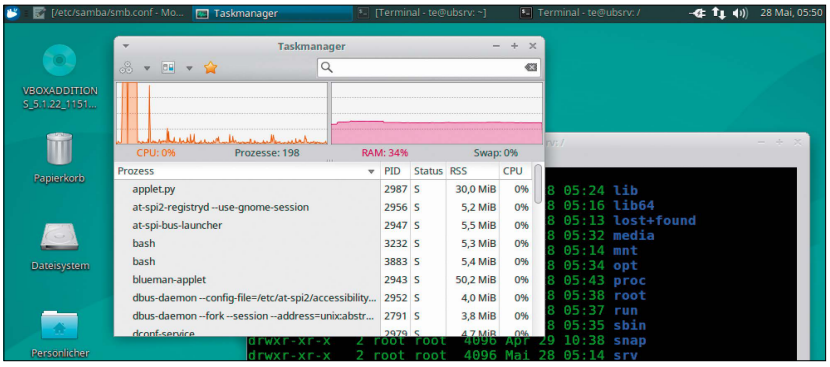
IT MEDIA PUBLISHING GMBH & CO KG

Systembasis:	Gentoo Linux
Einsatzzweck:	Notfallsystem für Linux-Systeme
Zielgruppe:	Einsteiger bis Fortgeschrittene
Hardwareansprüche:	gering
Merkmale:	ähnlich dem bewährten Rettungssystem System Rescue CD, aber deutschsprachig und um Software und WLAN-Treiber erweitert

Ubuntu Server einrichten

Die Serverversion von Ubuntu ist schnell installiert und läuft auch auf älterer Hardware. Nutzen Sie das System, wenn Sie beispielsweise einen zentralen Speicherplatz im eigenen Netzwerk benötigen.

Von **Thorsten Eggeling**



Für Einsteiger meist praktischer: Der Ubuntu-Server lässt sich mit einer grafischen Oberfläche wie XFCE ausstatten (Paket: „Xubuntu desktop“).

Ein Server ist ein PC im Netzwerk, der eine bestimmte Rolle einnimmt. Er bietet Dienste wie Dateifreigaben, Webapplikationen oder Multimedia-Streaming an. Für den privaten Gebrauch mit wenigen Benutzern muss ein Server nicht besonders leistungsfähig sein. Ein älterer PC oder ein Notebook ist ausreichend. Bei Dauerbetrieb sollten Sie aber besser in neuere Hardware investieren, weil hier die Energiekosten geringer sind. Als Betriebssystem kommt ein beliebiges Linux infrage.

Die Serverversion von Ubuntu 16.04.4 LTS ist jedoch besonders gut geeignet, weil sich hier schon bei Installation nur die für einen Server nötigen Pakete auswählen lassen.

Ubuntu Server installieren

Das Installationstool von Ubuntu 16.04.4 lädt alle Pakete über das Internet herunter. Eine kabelgebundene Netzwerkverbindung ist erforderlich. WLAN wird nicht unterstützt. Booten Sie den PC von der Heft-DVD und gehen Sie im Menü auf „Ubuntu Server 16.04.4 (64/32) Bit“. In der Regel wählen Sie die 64-Bit-Version. Ein 32-Bit-Linux sollte nur auf älteren PCs bis vier GB, maximal acht GB Hauptspeicher zum Einsatz kommen. Sie können auch aus einer der ISO-Dateien – auf der DVD im Ordner „Image-Dateien“ – einen USB-Stick für die Installation erzeugen. Dazu verwenden Sie das Kommandozeilentool dd wie unter *www.pcwelt.de/2261312* beschrieben.

Die Installation erfolgt über einen Assistenten, den Sie über die Tastatur steuern. Folgen Sie einfach den Anweisungen auf dem Bildschirm. Die Schritte entsprechen in etwa denen bei einer Standardinstallation von Ubuntu Desktop und sind weitestgehend selbsterklärend.

Eine Besonderheit ist die Auswahl für die automatische Installation von Sicherheitsupdates. Hier sollten Sie die Option „Sicherheitsaktualisierungen automatisch installieren“ wählen, vor allem, wenn der Server auch aus dem Internet erreichbar sein soll. Andernfalls müssen Sie das System selbst regelmäßig updaten. Im Fenster „Softwareauswahl“ können Sie vorbereitete Paketgruppen wählen. Es ist in jedem Fall sinnvoll, „Basic Ubuntu Server“ und „OpenSSH server“ auszuwählen. Alles Weitere hängt vom Einsatzgebiet ab. Soll der PC als Dateiserver für Linux und Windows dienen, wählen Sie „Samba file server“. Sind Webanwendungen geplant, aktivieren Sie „LAMP server“ (Linux, Apache, My SQL, PHP). Weitere für einen Server wichtige Paketgruppen können „Virtual Machine Host“ und „Mail server“ sein. Standardmäßig wird keine Desktopoberfläche installiert und Konfiguration und Wartung erfolgen ausschließlich über die Kommandozeile beziehungsweise über SSH. Wenn Sie einen Desktop bevorzugen, wählen Sie den gewünschten aus – beispielsweise „Xubuntu desktop“ (XFCE).

Fernzugriff per SSH

Wenn der Ubuntu-Server ohne Bildschirm läuft und Sie vor einem anderen Linux-PC sitzen, öffnen Sie ein Terminalfenster und führen dann folgenden Befehl aus:

```
ssh [User]@[Servername].local
```

Den Platzhalter „[User]“ ersetzen Sie durch den Namen des Benutzers, den Sie bei der Installation erstellt haben. Für „[Servername]“ tragen Sie den Rechnernamen des Servers mit einem angehängten „.local“ ein. Bei der ersten Anmeldung müssen Sie den SSH-Schlüssel mit „yes“ bestätigen. Windows-Nutzer verwenden ein Tool wie Putty (auf Heft-DVD) für die SSH-Verbindung zum Server.

Sollte das nicht funktionieren, installieren Sie – wenn noch nicht vorhanden – auf allen PCs und dem Ubuntu-Server folgendes Paket

```
sudo apt update
sudo apt install avahi-daemon
```

Alternativ können Sie statt des Servernamens immer auch die IP-Adresse des Servers verwenden. Sie sehen diese in den Infomeldungen, wenn Sie sich auf dem Server bei einer Konsole anmelden.

Netzwerkfreigaben einrichten

Samba verwendet als globale Konfigurationsdatei „/etc/samba/smb.conf". Darin sind die allgemeinen Einstellungen für den Samba-Server und die Freigaben festgelegt. Öffnen Sie die Datei im Terminalfenster etwa mit

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

Wenn Sie eine die grafische Oberfläche XFCE nutzen, setzen Sie statt „nano" den Editor „mousepad" ein.

Standardmäßig sind bereits die wichtigsten Optionen in der Datei enthalten und Kommentare beschreiben deren Bedeutung. Mit der Zeile „workgroup=WORKGROUP" im Abschnitt „[global]" legen Sie die Arbeitsgruppe fest.

Windows verwendet diese Gruppe ebenfalls standardmäßig, so dass Sie die Einstellung belassen können. Wenn Sie eine andere Bezeichnung wünschen oder in Ihrem Netzwerk bereits verwenden, ändern Sie den Wert entsprechend.

Samba lässt sich ausschließlich mit einem Gastkonto verwenden, also ohne Anmeldung. Aus Sicherheitsgründen sollten Sie jedoch zumindest den Schreibzugriff auf authentifizierte Benutzer beschränken. Samba verwendet eine eigene Passwortdatenbank. Damit Benutzer auf die Freigaben zugreifen können, muss für jeden Benutzer auch ein Samba-Passwort festgelegt sein. Dazu verwenden Sie folgende Befehlszeile:

```
sudo smbpasswd -a [User]
```

Für „[User]" setzen Sie einen Benutzernamen ein, der ein Konto auf dem PC besitzen muss. Um die Verwaltung zu vereinfachen, sollten alle Benutzer auf allen PCs dieselbe Kombination von Benutzernamen und Passwort verwenden.

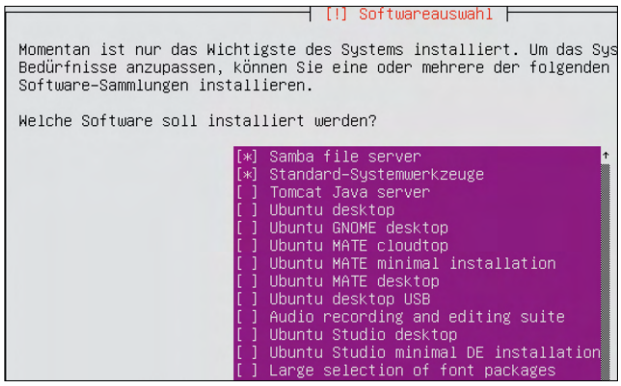
Verzeichnisse freigeben: Wenn die angelegten Benutzer über das Netz Zugriff auf ihr Home-Verzeichnis auf dem Server erhalten sollen, entfernen Sie alle Kommentarzeichen („;") im Abschnitt „[homes]". Ändern Sie „read only = yes" auf „read only = no", um den Schreibzugriff zu erlauben. Eine neue Freigabe für ein beliebiges Verzeichnis lässt sich beispielsweise über diese vier Zeilen erstellen:

```
[Filme]
path = /shares/videos
writeable = no
guest ok = yes
```

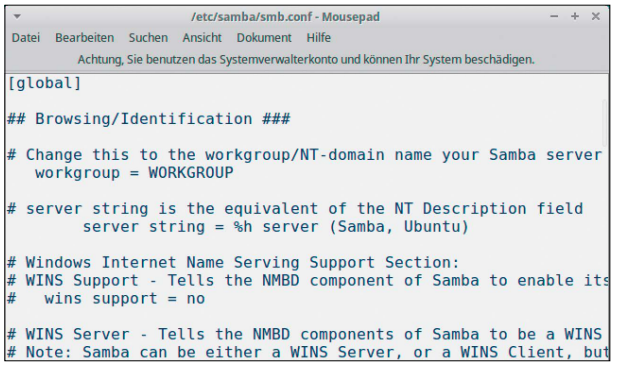
Fügen Sie den Block ganz am Ende der Konfigurationsdatei ein. In diesem Beispiel wird das Verzeichnis „/shares/videos" unter der Bezeichnung „Filme" freigegeben. Mit den genannten Samba-Optionen gewähren Sie nur Lesezugriff („writeable = no"), eine Anmeldung ist nicht zwingend erforderlich („guest ok = yes").

Speichern und anwenden: Nachdem Sie die gewünschten Änderungen in der Datei „/etc/samba/smb.conf" durchgeführt haben, drücken Sie in nano Strg-O und bestätigen mit der Enter-Taste. Beenden Sie nano mit Strg-X. Damit die neuen Optionen wirksam werden, muss Samba die Konfigurationsdatei neu einlesen. Dafür verwenden Sie den Befehl

```
sudo service smbd reload
```



Softwarevorauswahl: Bereits bei der Installation lässt sich das Einsatzgebiet des Servers festlegen. Wählen Sie „Samba file server" für einen Dateiserver.



Netzwerkfreigaben konfigurieren: Alle Samba-Einstellungen sind in der Datei „/etc/samba/smb.conf" enthalten. Hier legen Sie auch die Arbeitsgruppe fest.

Ubuntu Server

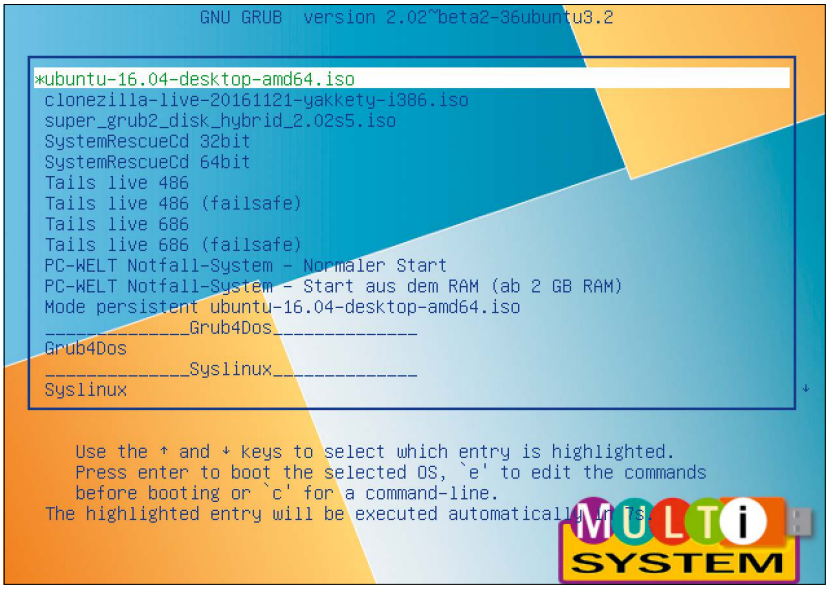
Systembasis:	Ubuntu
Einsatzzweck:	Serversystem
Zielgruppe:	Fortgeschrittene
Hardwareansprüche:	gering
Projektseite:	*www.ubuntu.com*
Merkmale:	Ubuntu Server unterscheidet sich von den Desktopsystemen nur in Details. Über den Netzwerkinstaller wählen Sie für ein schlankes System nur die Pakete, die Sie für die Serverfunktionen wirklich brauchen.

Multiboot-Umgebungen schaffen

Mehrere Betriebssysteme auf dem gleichen Rechner oder einem USB-Datenträger? Das geht. Dabei können Sie es sich je nach Anspruch sehr einfach oder technisch komplizierter machen. Wir zeigen Ihnen, worauf Sie achten müssen.

Von **Stephan Lamprecht**

Häufigstes Szenario für Dual- oder Multiboot-Umgebungen sind Parallelinstallationen von Linux und Windows. Wer auf sein Windows-System nicht verzichten will oder kann, aber hauptsächlich mit Linux arbeiten will, wird mit einer parallelen Installation beider Systeme keine Schwierigkeiten haben. Entscheidend ist, dass Windows zuerst installiert ist: Nachfolgend installierte Linux-Varianten erkennen das bestehende Windows und bieten automatisch eine parallele Einrichtung an. Dualboot von Linux und Windows ist aber nicht das einzige Multiboot-Motiv: Auch der Start mehrerer Linux-Systeme von einem Datenträger ist häufig erwünscht.



Alles auf einem Stick: Multisystem bringt mehrere Livesysteme auf einem USB-Stick unter. Sie haben somit Reparatursysteme, Zweitsysteme und Installer immer mobil dabei.

Multiboot-Stick mit mehreren Livesystemen

Unetbootin, Etcher, Win 32 Disk Imager sind Tools, die genau ein Systemabbild bootfähig auf USB kopieren. Wer auf größeren USB-Sticks oder auf USB-Festplatten mehrere Reparatur- und Zweitsysteme für jeden Einsatzzweck unterbringen will, kann ebenfalls auf einschlägige Werkzeuge zurückgreifen:

1. Unter Linux geht das am einfachsten über das Tool Multisystem, für das Sie einen FAT32-formatierten USB-Stick benötigen. Installieren Sie das Tool in einem Terminalfenster über die folgenden vier Zeilen:

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

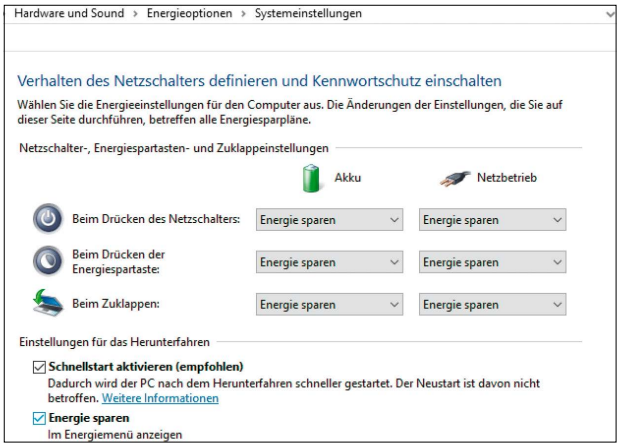
Starten Sie dann Multisystem, wählen Sie den USB-Stick in der Liste aus und klicken Sie auf „Überprüfen“. Bestätigen Sie die Installation des Grub2-Bootloaders mit „OK“. Dann ziehen Sie die ISO-Datei des gewünschten Systems vom Dateimanager auf den Bereich unter „Drag and Drop ISO/img“ im Fenster von Multisystem und bestätigen die Kopieraktion mit Ihrem root-Passwort. Diese Aktion wiederholen Sie für jedes System, das Sie von USB-Stick starten möchten.

Per Klick auf das Augen-Symbol blenden Sie ein erweitertes Menü ein. Bei Ubuntu-Systemen können Sie über die Schaltfläche mit dem Disk-Symbol einen persistenten Speicher einrichten: Das bedeutet, dass das an sich unveränderliche Livesystem nachträgliche Installationen und Konfigurationsänderungen erlaubt. Klicken Sie auf die Schaltfläche mit den Reglern und dann auf „grub.cfg“, um beispielsweise die Beschriftung der Grub-Menüeinträge zu bearbeiten. Multisystem unterstützt mehr als 200 populäre Systeme. Einige Systeme entpackt das Tool auf den USB-Stick, andere startet es direkt aus

der ISO-Datei. Für jedes System ist die Konfiguration des Bootloaders in der Datei „/usr/local/share/multisystem/os_support.sh“ hinterlegt. Bei Bedarf können Sie diese Datei bearbeiten und nicht unterstützte Systeme einbauen.

2. Unter Windows ist Yumi 2.0.5.1 („Your Universal Multiboot Installer“) das derzeit beste Tool, um mehrere Linux-Systeme auf USB-Datenträger zu kopieren. Wer die Wahl hat, sollte dem unkomplizierteren Yumi unter Windows gegenüber Multisystem unter Linux den Vorzug geben. Die Linux-Variante von Yumi ist inzwischen leider eingestellt.

Yumi gibt es unter *www.pendrivelinux.com/yumi-multiboot-usb-creator/* zum Download. Es ist unter Windows ohne Installation sofort ausführbar, befördert mehrere Linux-Distributionen bootfähig auf USB und bietet beim Boot sein Auswahlmenü sowie den Boot über Festplatte. Die wenigen Arbeitsschritte sind einfach: Sie wählen in „Step 1“ das gewünschte Zielaufwerk, in „Step 2“ die Distribution und im letzten Schritt das ISO-Image. Nach absolvierter Kopie fragt Yumi jedes Mal automatisch nach: „Would you like to add more ISOs…“. Mit „Yes“ können Sie dann nach demselben Strickmuster weitere Systeme aufnehmen, solange der Platz des Datenträgers reicht. Beim Booten des Datenträgers erscheint der Yumi-Bootloader und bietet unter „Linux Distributions“ die eingerichteten Systeme an. Standardmäßig lädt Yumi nach 30 Sekunden Wartezeit das festinstallierte System der ersten Festplatte.



Damit die Installation von Linux nicht schiefgeht, schalten Sie vorher den „Schnellstart“ in den Energieoptionen von Windows aus.

Multiboot von installierten Linux-Systemen

Technisch völlig verschieden vom Start mehrerer Livesysteme ist ein Multiboot von ordentlich installierten Linux-Systemen.

Linux-Multiboot auf Festplatte: Soll auf einem PC mit Linux-Betriebssystem ein weiteres Linux installiert werden, hängt die richtige Vorgehensweise vom Installer des neuen Systems ab. Während sich alle Installer inzwischen sorgsam hüten, ein vorhandenes Windows zu shreddern, ist Linux-Rücksicht untereinander ungewiss. Der Ubuntu-Installer erkennt nach unserer Erfahrung die meisten bereits vorhandenen Linux-Systeme und bietet dann unter „Installationsart“ die Parallelinstallation an. Nach einem Klick auf „Weiter“ kommt sogar eine per Schieberegler skalierbare Verkleinerung der vorhandenen Partition, um für Ubuntu eine neue Partition zu schaffen. Wenn Sie der Installationsroutine eines weiteren zu installierenden Linux-Systems nicht trauen, können Sie an dieser Stelle bereits weitere Partitionen für die späteren Installationen anlegen. Möglich sind logische Partitionen mit dem Mountpoint „/“, die als Rootpartition für die dritte Distribution dient, eine Partition, die als zweiter Auslagerungsspeicher genutzt wird, sowie eine dritte, die Sie unter „/home“ einhängen wollen. Bei jedem Installer, der das bestehende Linux nicht erkennt, hilft nur die manuelle Partitionierung wie bei der USB-Installation.

Was macht Grub eigentlich?

Damit Sie beim Einschalten des Systems zwischen den verschiedenen Betriebssystemen wählen können, benötigen Sie einen Bootloader.

Im Falle der bekannten und aktuellen Linux-Distributionen ist das Grub 2. Sind nur Linux-Systeme installiert, lädt Grub 2 den gewünschten Kernel, der dann das Betriebssystem initialisiert. Bei einer Multiboot-Konfiguration leitet Grub bei Bedarf die Anforderung an den Windows-Bootloader weiter.

Grub 2 muss allerdings mit einer Vielzahl unterschiedlicher Konfigurationen zurechtkommen. Aktuelle PCs booten standardmäßig von einer Partition im GPT-Format und verwenden Uefi-Firmware. Ältere PCs nutzen dagegen Bios und MBR-Partitionen (Master Boot Record). Bei herkömmlichem Bios werden bei der Linux-Installation 512 Bytes des Grub-2-Bootloaders („boot.img“) in den MBR der ersten Festplatte geschrieben.

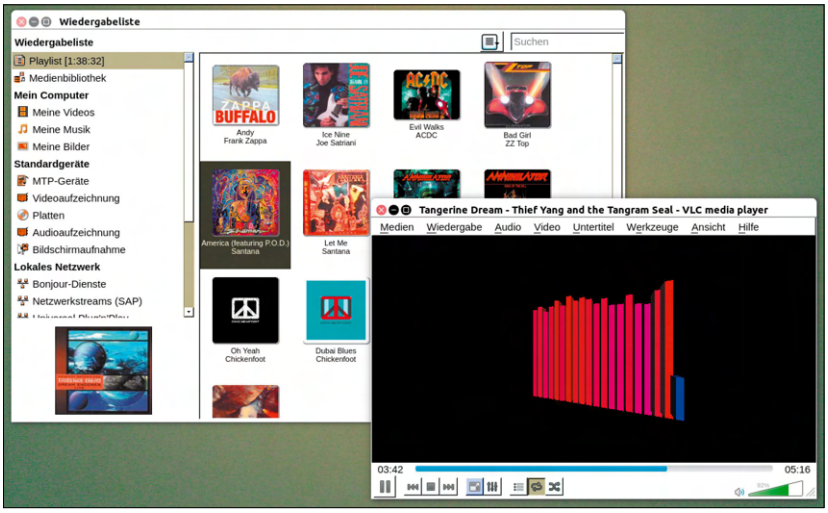
Damit findet der Bootloader den ersten Sektor der Datei „/boot/grub/core.img“ und führt den enthaltenen Code aus. Er lädt die Module, die für den Zugriff auf das Dateisystem nötig sind, und zeigt sein Bootmenü an. Ist Linux dagegen im Uefi-Modus installiert, liegt der Bootloader in der EFI-Partition, die in das Dateisystem unter „/boot/efi“ eingebunden ist. Für jedes System gibt es ein eigenes Verzeichnis – zum Beispiel „/boot/efi/EFI/ubuntu“. Die Konfiguration von Grub 2 erfolgt automatisch über die Scripts unter „/etc/grub.d“. Das wichtigste Script sucht unter „/boot“ nach Linux-Kerneln („vmlinuz-“) und Ramdisk-Dateien („initrd.img“) und erstellt die Einträge für das Bootmenü.

Alleskönner VLC

Der Mediaplayer VLC darf auf keinem Linux- oder Windows-Rechner fehlen, weil er praktisch alle Video- und Musikformate abspielt. Viele Möglichkeiten vergräbt das Multitalent hinter Schaltern und einer anspruchsvollen Konfigurationsoberfläche.

Von **Hermann Apfelböck**

Der VLC – kurz für „Videolan Client" – kann eigentlich alles rund um Film und Sound und macht diverse Playeralternativen und Multimedia-Tools weitgehend überflüssig. Optischer Schick und benutzerfreundliche Konfiguration sind freilich nicht seine Stärken. So bleibt meist viel Potenzial ungenutzt oder es kommen neben dem VLC weitere ergänzende Player und Helfer zum Einsatz. Das ist nicht falsch und manchmal komfortabler, aber technisch notwendig wäre es nicht, wie dieser Ratgeber zeigen soll.



VLC-Installation unter Linux

Alle Linux-Distributionen halten den VLC Media Player in ihren Standard-Paketquellen bereit. Die Installation ist entsprechend einfach und problemlos. Installieren Sie das Paket „vlc", optional zusätzlich „browser-plugin-vlc" (Browserintegration):

```
sudo aptget install vlc browser-
 plugin-vlc
```

Nicht immer, insbesondere bei älteren LTS-Versionen, ist schon die neueste Version verfügbar. Zu Redaktionsschluss war die Version 3.0.1 vom VLC aktuell. Diese war aber bei einigen Systemen nocht nicht verfgbar.

Die funktionalen Unterschiede sind aber meist nicht gravierend. Notwendige Sicherheitsupdates erhalten auch die älteren Versionen. Wer trotzdem stets den aktuellsten VLC nutzen will, kann auf das PPA des Herstellers Videolan ausweichen:

```
sudo add-apt-repository
 ppa:videolan/stable-daily
sudo apt update
sudo apt install vlc
```

Unentbehrlich zur Wiedergabe von DVDs ist ferner die Bibliothek „lib-dvd", die Sie mit den Befehlen

```
sudo apt-get install libdvd-pkg
sudo dpkg-reconfigure libdvd-pkg
```

nachrüsten und integrieren.

Basisfunktionen des Players

Der VLC spielt nicht nur Audio- oder Videodateien fast jeden Dateiformats (Audio u. a. APE, FLAC, MID, MP3, OGG, WMA; Video u. a. AVI, DivX, FLV, MKV, MP4, MPEG, VOB, WMV). Er beherrscht außerdem Musik-CDs, Film-DVDs, Blu-rays und Internetstreams, gibt das Medienangebot von UPnP/DLNA-Servern im Heimnetz wieder, dient – in allerdings engen Grenzen – selbst als solcher UPnP-Streaming-Server und greift auf DVB-T-Hardware zu. Auch Aufnehmen und Konvertieren in andere Formate ist möglich.

Bedienungsgrundlagen: Der VLC besteht aus zwei Hauptfenstern – das Wiedergabefenster und die Wiedergabeliste. Im Allgemeinen ist es einfacher und übersichtlicher, beide Fenster zu kombinieren, was über „Ansicht -> Angedockte Wiedergabeliste" auch die Standardvorgabe ist. In der „Wiedergabeliste" (Strg-L) zeigt der Player in der Navigationsspalte links zahlreiche Medienquellen. Unter der aktuellen Wiedergabeliste und der optional angelegten Medienbibliothek gibt es zunächst die lokalen Standardordner wie „Meine Videos", die lediglich auf die entsprechenden Standardverzeichnisse unter „/home/[user]" verweisen. Unter „Standardgeräte" gibt es den Zugriff auf „Platten", also auf CD- und DVD-Laufwerke, ferner auf „MTP-Geräte", also mobile MP3-Player, sofern angeschlossen. Eventuelle Medienserver im lokalen Netz (UPnP/DLNA und iTunes) zeigt der VLC unter „Lokales Netzwerk". Darunter folgt noch eine Reihe von namhaften Audiostreaming-

Diensten unter „Internet“, besonders ergiebig Icast und Jamendo.

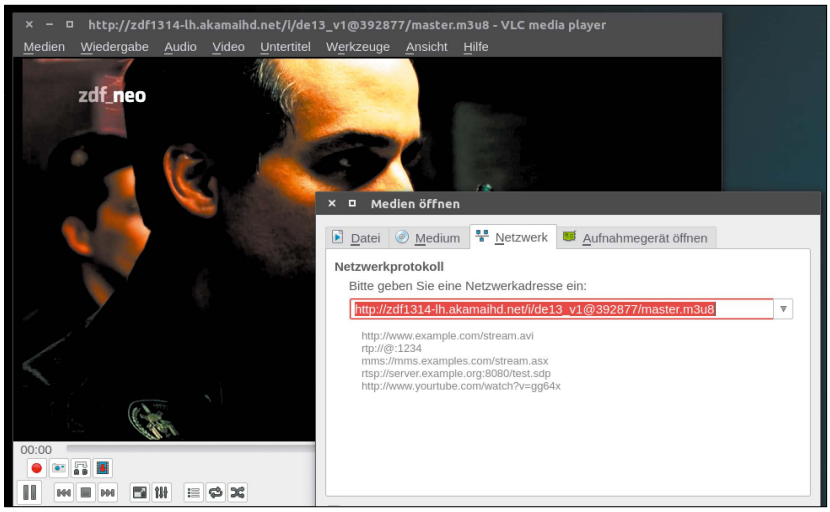
Dateien und Medien öffnen: Sowohl das Wiedergabefenster als auch die Wiedergabe beherrschen Drag & Drop mit der Maus. Das ist der einfachste Weg, um schnell aus dem Dateimanager eine Mediendatei abzuspielen. Dabei kann der VLC auch unvollständige Videos und Audiopakete etwa schon während eines Downloads anspielen. Noch besser: Der VLC beherrscht auch ZIP- und RAR-Archive sowie das Mounten von ISO-Images. Diese Formate sind also ohne Bearbeitung sofort zu benutzen.

Das Menü „Medien“ fürs Öffnen von Dateien enthält insgesamt sechs Befehle zum Starten von Medien. Der erste Eintrag „Datei öffnen“ ist klassisch und erlaubt nach Navigation zur Quelldatei den Start derselben. Es ist hier aber auch mit den typischen Tasten Strg und Umschalt eine Mehrfachauswahl von Dateien möglich. Der Extraeintrag „Mehrere Dateien öffnen“ ist daher nur dann notwendig, wenn sich die Auswahl über unterschiedliche Verzeichnisse erstrecken soll; außerdem gibt es hier die zusätzliche Option, die ausgewählten Medien durch eine synchrone Mediendatei zu begleiten – etwa private Videos durch eine passende Audiodatei.

„Ordner öffnen“ kann praktisch sein, um alle Audiodateien eines Verzeichnisses einschließlich aller Unterordner (Achtung!) in die aktuelle Wiedergabeliste zu übernehmen. Auch bei typischen DVD-Rips mit mehreren VOB-Dateien ist diese Methode eleganter, als die Dateien mit Filmunterbrechung einzeln zu starten.

„Medium öffnen“ benötigen Sie, um eine eingelegte DVD, Blu-ray-Disc oder Audio-CD abzuspielen. Der Dialog zeigt einige elaborierte Optionen zum Einsprungpunkt und zur Startzeit, die Sie im Normalfall ignorieren können.

„Netzwerkstream öffnen“ ist der Startdialog für jegliches lokales oder Internetstreaming (Mediatheken, Youtube). Zum lokalen Streamen lesen Sie an späterer Stelle mehr. Für das



VLC „öffnet“ alles: Das Menü „Medien“ zeigt sechs Optionen zum Starten von Film und Musik. Hier wurde „Netzwerkstream“ gewählt und die URL einer Mediathek eingegeben.

Streamen eines Webvideos oder Webradiosenders genügt es, die URL zu wissen und in diesem Dialog einzutragen – etwa *http://br-brklassik-live.cast.addradio.de/br/brklassik/live/mp3/128/stream.mp3*. Der Streamingdienst wird dann wie jedes andere Medium in die Wiedergabeliste eingetragen (in diesem Beispiel als „BR-Klassik“) und beginnt sofort mit der Wiedergabe. Zuverlässige, aktuelle und umfassende Tabellen mit direkten Stream-URLs sind rar, recht brauchbar sind *www.stream-urls.de/webradio* (Radio), *https://wiki.ubuntuusers.de/Internet-TV/Stationen* (TV) und *https://wiki.ubuntuusers.de/Internetradio/Stationen (Radio)*.

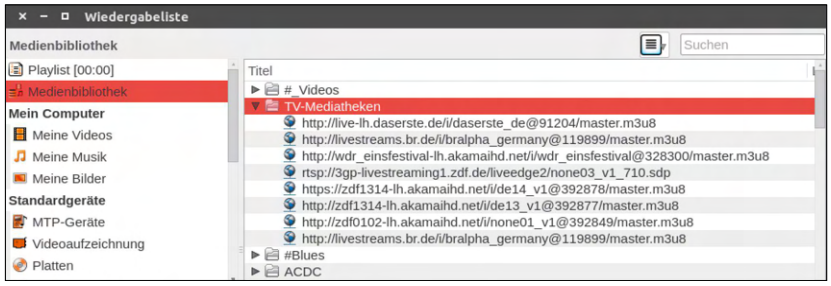
Mediensammlung anlegen

Zur bequemen Benutzung der Medien vom lokalen Rechner oder von Netzwerkfreigaben ist das manuelle Öffnen über das „Medien“-Menü nicht ausreichend. Dafür gibt es die Medienbibliothek. Um eine solche Mediensammlung anzulegen, klicken Sie in der Wiedergabeliste („Ansicht -> Wiedergabeliste“) auf den Eintrag „Medienbibliothek“ und dann im Listenfenster nach Rechtsklick auf „Verzeichnis hinzufügen“. Sie erhalten dabei keine Rückmeldung, wann der Player die Dateien einschließlich Medientags eingelesen hat. Je nach Menge der Medien ist daher Geduld erforderlich. Die integrierten Stücke erscheinen dann in einer einfachen Tabelle, die sich über das Suchfeld rechts oben filtern lässt.

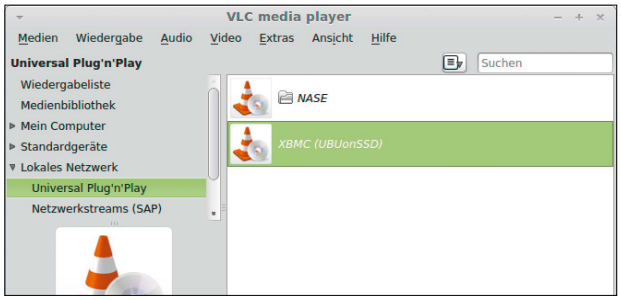
Die Darstellung kann über das kleine Symbol neben dem Suchfeld oder nach Rechtsklick und „Ansicht der Wiedergabeliste“ umstellen und zeigt mit der Option „Symbole“ die Alben- oder Filmcover. Auch die Größe können Sie mit Strg-Mausrad verändern. Dennoch kann die Medienverwaltung mit den schickeren und strukturierten Bibliotheken anderer Player nicht mithalten. Für Puristen ist sie aber völlig

Mehr Infos zum VLC

Projektseite und Download:	*www.videolan.org*
Dokumentation:	*http://wiki.videolan.org* mit Infos zu Installation, Menüangebot, Konfiguration, Startparameter, Netzwerkstreaming, Streamausgabe und vieles mehr. Nutzen Sie in der linken Spalte den Eintrag „Documentation“.
Weitere Tipps & Infos:	*http://wiki.ubuntuusers.de/vlc*



Webstreams in der Medienbibliothek: Wenn Sie die Streams in der Wiedergabeliste sammeln und als Datei speichern, kann die Datei wiederum in die Bibliothek integriert werden.



UPnP im VLC: Der Videolan Player zeigt Medienserver unter „Lokales Netzwerk“. Wenn es keinen UPnP-Server gibt, fehlt der Eintrag „Universal Plug'n'Play“.

ausreichend oder gar willkommen. Überflüssige Medien lassen sich mit „Ausgewählte entfernen“ wieder aus der Bibliothek löschen. Die Dateien selbst bleiben dabei erhalten.

Streamingdienste in der Medienbibliothek

Die Medienbibliothek kann auch Streamingangebote aus dem Internet aufnehmen. Dazu ist ein kleiner Umweg erforderlich: Zunächst nehmen Sie, wie oben beschrieben, eine Reihe von Radio- oder TV-Angeboten über „Medien -> Netzwerkstream öffnen“ in die temporäre Wiedergabeliste auf. Diese Wiedergabeliste, die inhaltlich möglichst homogen sein sollte, speichern Sie dann über „Medien -> Wiedergabeliste in Datei speichern“ als XSPF-Datei. Wer auf Ordnung Wert legt, kann diese XML-Datei zunächst in einen Editor laden und Standardtitel „Wiedergabeliste“, der in der dritten Zeile als

```
<title>Wiedergabeliste</title>
```

erscheint, nach Wunsch ändern – etwa auf „Rock-Radio“ oder was immer passend. Danach lässt sich diese URL-Sammlung nach Rechtsklick im Fenster der Medienbibliothek und „Datei hinzufügen“ wie ein Medium in die Bibliothek integrieren. Die XSPF-Datei muss dauerhaft erhalten bleiben, wenn die VLC-Bibliothek den geänderten Titel anzeigen soll. Mit gepflegten URL-Sammlungen in der Bibliothek ist der VLC komfortabler als Lesezeichen im Browser oder spezialisierte Tools wie etwa Radiosure.

Der VLC als Bildviewer

Als Viewer für Fotos und Bilder ist der VLC nur zweite Wahl. Natürlich kann er Bildformate anzeigen und wenn Sie mit der Maus eine Menge markierter Bilder vom Dateimanager in das Wiedergabefenster oder in die Wiedergabeliste ziehen, wird er sie sogar sofort als Slideshow im Zehn-Sekunden-Takt wiedergeben. Dabei sind aber weder das Intervall noch eine feste Fenstergröße konfigurierbar.

Eine für diesen Einsatzzweck unentbehrliche, aber auch für Videos im Fenstermodus nützliche Option ist das Kästchen „Interface an Videogröße anpassen“ unter „Werkzeuge -> Einstellungen -> Interface“. Diese Option sollte deaktiviert werden, damit das Wiedergabefenster ungeachtet der Bild- (oder Video-)größe konstant bleibt. Mehr als ein Hilfsviewer, wenn nichts Besseres an Bord ist, ist der VLC für Bilder dennoch nicht.

Der VLC und UPnP/DLNA-Server

Der VLC Player beherrscht in der Wiedergabeliste via „Universal Plug'n'Play“ den Zugriff auf lokale UPnP/DLNA-Server (NAS, Kodi, Plex, Minidlna). Einen korrekt im Netzwerk eingebundenen UPnP-Server zeigt der Player dort an und mit einem Doppelklick auf einen Eintrag navigieren Sie in der Struktur des Servers. Bei großen Mediensammlungen des UPnP-Servers kann es irritierend sein, dass der VLC die Wiedergabe erst anbietet, wenn er sämtliche Medien via Netzwerk eingelesen hat. Dies kann eventuell so lange dauern, dass der Nutzer an der Funktionalität zweifelt.

Bei anderen UPnP-tauglichen Playern sind die ersten Audio- oder Videodateien sofort sichtbar und benutzbar, während der Player im Hintergrund weiter nachlädt. Der VLC zeigt und spielt nach komplett abgeschlossenem Vorgang.

Der VLC als Streamingserver

Einen schicken UPnP/DLNA-Server erhalten Sie mit dem VLC nicht, jedoch ist er durchaus in der Lage, ad hoc einige Filme über eine Netzwerkadresse für Abspielclients bereitzustellen.
Die Vorgehensweise am Rechner („Server“), der den Film bereithält:

1. Gehen Sie zunächst auf „Medien -> Stream“ (relativ am Ende des Menüs). Unter „Dateiauswahl“ navigieren Sie mit „Hinzufügen“ zur gewünschten Mediendatei. Danach klicken Sie im selben Dialog unten auf „Stream“. Im folgenden Dialog des Assistenten geht es mit „Nächstes“ einfach weiter.

2. Im Fenster „Ziel einstellen“ verwenden Sie am besten „RTP / MPEG Transport Stream“ und klicken nach dieser Auswahl rechts auf die Schaltfläche „Hinzufügen“. Geben Sie als Adresse

```
239.0.0.1
```

ein, den Standardport 5004 können Sie unverändert übernehmen. Beachten Sie, dass diese Multicastadresse unabhängig von Ihrem lokalen Adressbereich zu benutzen ist. Ihr Adressraum und die IP-Adresse des Server-PCs spielen hier keine Rolle.

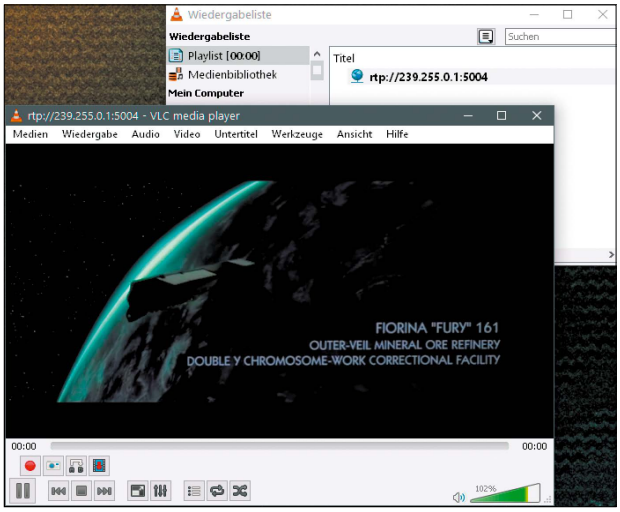
3. Nach Klick auf „Nächstes“ kommt die Transcodierungsauswahl, die Sie auf Standard belassen können und erneut „Nächstes“ klicken. Im letzten Fenster aktivieren Sie „Alle Elementarstreams streamen“ und schließen die Aktion mit der Schaltfläche „Stream“ ab.

Beim Client – idealerweise erneut ein VLC Player – ist der Weg einfach: Gehen Sie auf „Medien -> Netzwerkstream“. Als Netzwerkadresse geben Sie hier die vorher eingerichtete Multicastadresse samt Port

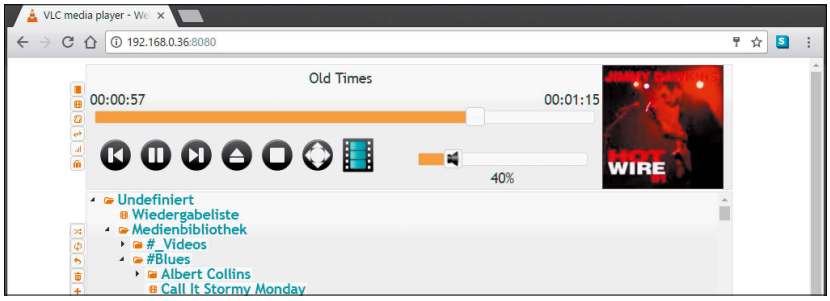
```
rtp://239.255.0.1:5004
```

ein und klicken im selben Dialog unten auf die Schaltfläche „Wiedergabe“.

Hinweis: Die Methode funktioniert analog auch ohne Multicastadresse, sofern Sie einen Stream gezielt nur an einen Rechner schicken wollen. Dann geben Sie am Server die LAN-IP des Zielclients ein – etwa 192.178.1.10 – und greifen dann am Client den Netzwerkstream mit der Adresse „rtp://192.178.1.10“ ab. Die Multicastmethode ist jedoch einfacher, weil Sie sich dabei um die lokalen IP-Adressen nicht kümmern müssen.



VLC als Streamingserver: Das funktioniert technisch einwandfrei über eine Multicast-IP oder auch direkt an die Zielrechner-IP. UPnP-Komfort ist hier nicht das Ziel.



HTTP-Server: Diese VLC-Fernbedienung via Browser leistet fundamentalen Remotezugriff, ist aber insgesamt etwas fummelig.

VLC-Fernbedienung mit HTTP-Server

Der VLC hat einen einfachen eingebauten HTTP-Server, 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 lediglich die Medienauswahl und Lautstärke erledigt. Der HTTP-Server bietet weder eine sonderlich schicke Oberfläche noch nennenswerten Bedienkomfort, genügt aber zur fundamentalen Fernsteuerung. Dies insbesondere dann, wenn im VLC eine Medienbibliothek eingerichtet ist und die Medien nicht im Dateisystem gesucht werden müssen.

Theoretisch sollte der Webserver über „Einstellungen -> Alle -> Interface -> Hauptinterfaces“ oder auch über „Ansicht -> Interface hinzufügen -> Web“ neben der normalen Oberfläche ladbar sein. Das ist uns nicht gelungen, da der Server ein Passwort verlangt, das an dieser Stelle in den Einstellungen nicht zu vergeben ist. Hingegen funktioniert der Start des HTTP-Servers unter allen Betriebssystemen im Terminal mit dieser Kommandozeile:

```
vlc --intf http --http-password
  nix
```

Danach ist der VLC remote über jeden Browser mit der Adresse

```
[IP-Adresse]:8080
```

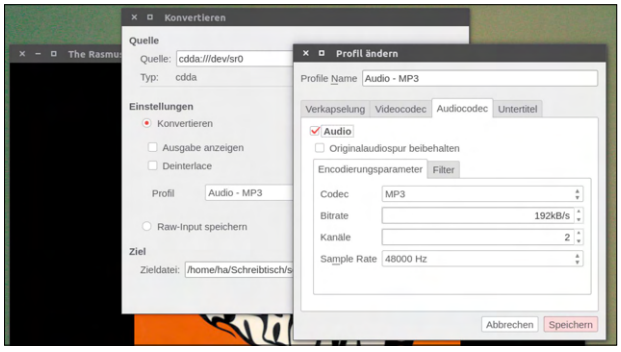
erreichbar. Bei der Authentifizierungsabfrage lassen das Feld „Benutzernamen“ leer und geben nur das Passwort ein. Statt des Stellvertreters „[IP-Adresse] verwenden Sie die tatsächliche lokale IP des Rechners, auf dem der VLC läuft – also beispielsweise „192.168.1.25:8080“. Soll der VLC neben dem HTTP-Server auch noch seine normale Oberfläche anzeigen, ist folgender Befehl einschlägig:

```
vlc --intf qt --extraintf http
  --http-password nix
```

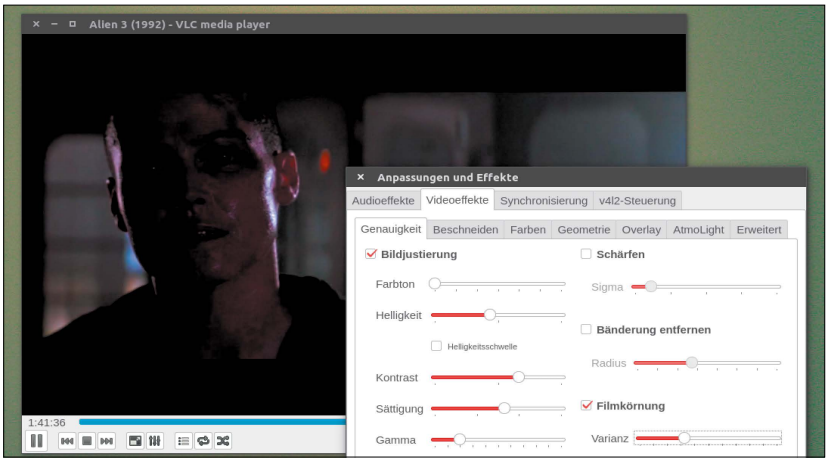
Das Interface „qt“ ist die Standardoberfläche (auch unter Windows), und über den Parameter „--extraintf …“ wird zudem der Webserver gestartet.

Der VLC als Konvertierer

Für den VLC sind exotische Formate kein Problem, für Smart-TV oder Tablets hingegen schon. Ungeachtet spezialisierter Tools wie Handbrake können Sie den VLC auch zum Konvertieren nutzen. Über „Medien -> Konvertieren/Speichern“ startet der zugehörige Assistent. Im Folgedialog bestimmen Sie über „Hinzufügen“ die Mediendatei und klicken dann unten auf „Konvertieren/Speichern“. Unter „Profil“ gibt es eine Drop-down-Liste mit populären Audio- und Videoformaten, wobei auch Android-Geräte, iPod und Youtube speziell berücksichtigt sind. Nachdem Sie eine Zieldatei angegeben haben, kann der Vorgang mit „Start“ beginnen. Die Konvertierung verläuft je nach Rechner in mehrfacher Geschwin-



Konvertieren mit dem VLC: Technisch arbeitet der VLC einwandfrei, fordert aber bei Musik (mehr als bei Videomaterial) einige Klicks und eventuelle Nachbearbeitung.



Helligkeit, Farben und Sättigung: Was sich am Monitor oder TV nicht korrigieren lässt, kann der VLC über diverse Filter signifikant verbessern.

digkeit, wenn Sie auf die Option „Ausgabe anzeigen“ verzichten.

Das Konvertieren funktioniert selbstverständlich auch bei Audiodateien oder Audio-CDs (wobei Sie hier statt einer Quelldatei das Medium angeben – meist „/dev/sr0“).

Bei einer typischen Audiokonvertierung nach „Audio - MP3“ sollten Sie dieses Ausgabe-„Profil“ unbedingt bearbeiten, da standardmäßig nur 128 KBit/s vorgesehen sind. Profiländerung erledigen Sie neben der Dropdown-Liste entweder punktuell über das Schraubenschlüsselsymbol oder Sie legen mit der Schaltfläche „Neues Profil erstellen“ (ganz rechts) dauerhaft ein passendes Profil etwa mit 192 KBit/s Bitrate und 48 000 Hz Samplingrate an.

Generell zeigt sich der VLC beim Konvertieren technisch makellos, aber ohne den Komfort von Spezialisten: So bleibt die Namensvergabe beim Audiorippen eine manuelle Mühe.

Optimieren der Videoausgabe

Das Untermenü „Werkzeuge -> Effekte und Filter“ ist überaus umfangreich und erlaubt fundamentale und detaillierte Darstellungsoptimierung. Wir nennen hier nur drei fundamentale Eingriffe:

Bild und Ton synchronisieren: Über „Werkzeuge -> Effekte und Filter -> Synchronisierung“ gleichen Sie aus, wenn Bild und Ton asynchron laufen – also der Ton vorauseilt oder hinterherhinkt. Den Wert müssen Sie dort in Millisekunden eingeben. Beispiel: Um den Ton um eine Sekunde nach vorne zu versetzen, wäre der Wert „-1000“ einschlägig, während „1000“ den Ton um eine Sekunde verzögert.

Drehen von Videos: Bei Videos mit dem Smartphone sind um 90 Grad gedrehte Filme recht häufig. Das kann der VLC mühelos korrigieren: Das einschlägige Werkzeug finden Sie unter „Werkzeuge -> Effekte und Filter“ auf der Registerkarte „Videoeffekte“, hier wiederum auf der Unterregisterkarte „Geometrie“. Zunächst müssen Sie die Option „Transformieren“ aktivieren. Danach lässt sich das Video per Vorgabeoptionen in der Drop-down-Liste um 90, 180 oder 270 Grad drehen, im Prinzip aber auch filigran in Gradstufen (Option „Drehen“).

Helligkeit und Farben: Ebenfalls unter „Werkzeuge -> Effekte und Filter -> Videoeffekte“ ist eine zu dunkle oder zu farblose Filmwiedergabe deutlich zu korrigieren. Das Register „Genauigkeit“ bietet unter anderem Schieberegler zu Helligkeit, Kontrast, Sättigung und Gammawert. Da ein laufender Film das Resultat der Einstellung sofort anzeigt, ist die Wiedergabe in wenigen Sekunden optimiert.

Optimale Größe bei Vollbildwiedergabe

Je nach Filmmaterial können bei der Wiedergabe auf Smart-TVs oder PC-Monitoren platzverschwendende schwarze Ränder horizontal wie vertikal erscheinen. Über den Menüpunkt „Video“ oder auch im Vollbild nach Rechtsklick und dem Kontextmenü „Video“ können Sie den Monitor eventuell besser ausnutzen. Die Optionen „Seitenverhältnis“ und „Beschneiden“ erlauben Dehnungen des Bildes und das Abschneiden von Randbereichen. Hier hilft nur empirisches Ausprobieren, da sowohl zu starke Verzerrung als auch das Abschneiden von zu viel Filmmaterial kontraproduktiv sind. Ein ganz genaues Beschneidewerkzeug gibt es außerdem unter „Werkzeuge -> Effekte und Filter -> Videoeffekte -> Beschneiden“.

Normalisierung der Lautstärke

Mediendateien haben oft sehr unterschiedliche Lautstärkepegel. Dies erfordert dann mitunter hektische Korrektur an den Lautsprecherboxen oder im Soundapplet. Der VLC Player hat zwar keinen Einfluss auf die Lautsprecherstellung und den Lautstärkemixer, jedoch kann er den Startpegel reduzieren und die Lautstärke der Mediendateien angleichen (normalisieren).

Die Optionen finden Sie unter Werkzeuge -> Einstellungen -> Audio“. Stellen Sie den Schieberegler neben „Audio-Start-Pegel immer zurücksetzen“ auf ein moderates Maß. Ferner aktivieren Sie im selben Dialog die Option „Normalisiere die Lautstärke“.

TV-Aufnahmen und Screenshots

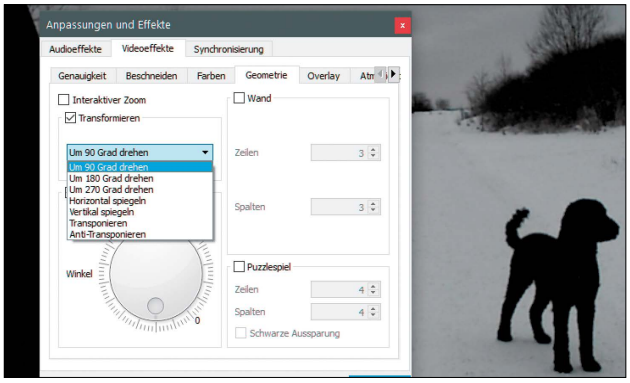
Der VLC kann über „Wiedergabe -> Aufnehmen“ einen aktuell laufenden Film aufnehmen, also auf die Festplatte schreiben. Wer dies häufiger benötigt, kann unter „Ansicht“ die „Erweiterte Steuerung“ aktivieren. Dann erscheinen im Wiedergabefenster weitere Bedienelemente, unter anderem der Aufnahmeknopf.

Alle Aufnahmen werden unter Angabe der Zeit, des Senders und Namen der Sendung unter „~/Downloads/“ als „.ts“-Datei abgelegt. Über „Werkzeuge -> Einstellungen -> Eingang / Codecs“ können Sie neben „Ausnahme-Verzeichnis oder Dateiname“ auch einen eigenen Pfad festlegen.

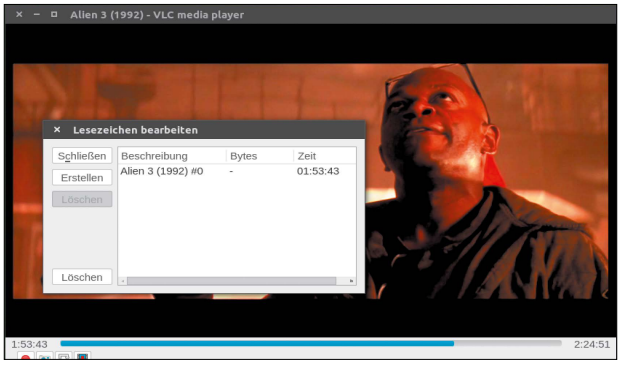
Über „Video -> Schnappschuss machen“ legen Sie einen Screenshot der aktuellen Filmszene ab. Zielverzeichnis und Namen für diese Bilder können Sie unter Werkzeuge -> Einstellungen -> Video“ im Bereich „Videoschnappschüsse“ selbst festlegen.

Desktopvideos mit VLC

Der VLC unterstützt Sie auch, wenn Sie Ihre Desktopaktivitäten filmen möchten, um ein Videotutorial herzustellen. Für diese Aufgabe gehen Sie auf „Medien -> Aufnahmegerät öffnen“. Wählen Sie als „Aufnahmemodus“ den Eintrag „Desktop“. Unter „Optionen“ geben Sie die gewünschte Anzahl an Bildern pro Sekunde an. Für einen flüssig wirkenden Screencast ist die Voreinstellung „1,00 f/s“ zu wenig, wenigstens zwei sollten Sie eintragen. Wenn Sie vor dem Start noch etwas vorbereiten müssen, klicken Sie auf „Mehr Optionen anzeigen“ und geben eine Startzeit an. Um mit der Aufnahme zu beginnen, klicken Sie unten auf die Schaltfläche mit dem kleinen Pfeil rechts neben „Wiedergabe“ und auf „Konvertieren“. Im folgenden Dialogfenster legen Sie die „Zieldatei“ und das Format des Videos fest und beginnen die Aufnahme mit „Start“.



Jetzt steht der Hund auf den Beinen: Das Drehen von falsch aufgenommenen Videos ist für den VLC kein Problem (siehe „Werkzeuge -> Effekte -> Videoeffekte -> Geometrie“).



Lesezeichen setzen: Zum Anhalten und Fortsetzen an einer bestimmten Filmstelle hat der VLC eine Verwaltung von Sprungmarken, die in einer Playlist gespeichert werden muss.

Lesezeichen im Film setzen

Im VLC gibt es eine Möglichkeit, Lesezeichen zu setzen, um einen Film später genau an dieser Stelle fortzusetzen. Lesezeichen für die aktuelle Stelle verwaltet der VLC über den Menüpunkt „Wiedergabe -> Benutzerdefinierte Lesezeichen“. Ein Klick auf „Erstellen“ legt einen neuen Zeitpunkt auf der Merkliste an, der als Sprungmarke funktioniert.

Damit ist die Marke aber noch nicht permanent gespeichert. Dazu muss erst noch eine Playliste als Datei gespeichert werden, was Sie unter „Medien -> Wiedergabeliste in Datei speichern“ erledigen. Ein Klick auf die resultierende Datei im Dateimanager öffnet dann den Film wieder im VLC und unter „Benutzerdefinierte Lesezeichen“ liegt die Sprungmarke zur gewünschten Stelle.

Mit Resetkommando zum Standard

Dieser Artikel hat alle Skins und LUA-Erweiterungen für den VLC ausgeklammert, da sie unterm Strich die Bedienung des VLC nicht signifikant verbessern und die Stabilität verringern. Es bleibt gegen unsere Empfehlung aber jedem Nutzer vorbehalten, sich hier umzusehen. Unter „Werkzeuge -> Plugins und Erweiterungen“ lässt sich der Plug-in-Manager des VLC öffnen. Die im Web verfügbaren Erweiterungen zeigt das Tool nach Klick auf „Zusätzl. Erweiterungen im Netz finden“. Weil das Spielen mit experimentellen Skins aber schon mal dazu führt, dass der Player nicht mehr bedienbar ist und auch seine Einstellungen nicht mehr anbietet, um dort das Problem rückgängig zu machen, ist folgender Startparameter wichtig:

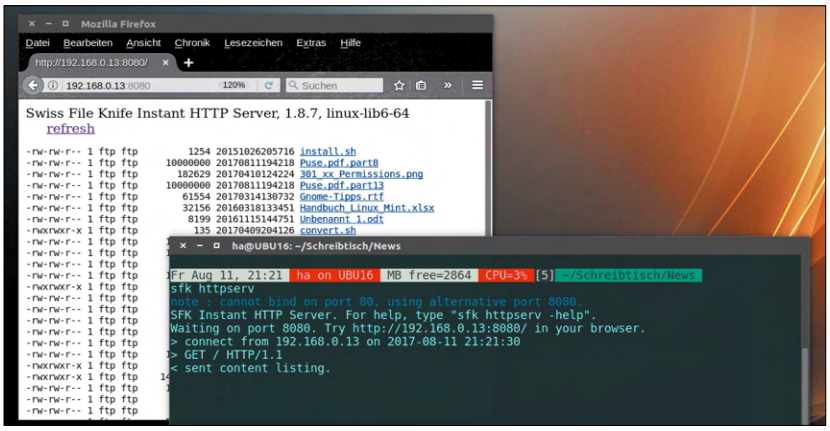
```
vlc --reset-config
```

Das setzt den Player auf seine Standardoberfläche zurück, andere Einstellungen wie etwa eine eingerichtete Medienbibliothek bleiben jedoch erhalten.

Swiss File Knife

Seit Jahren kann das Tool Swiss File Knife beachtliche Downloadzahlen und gute Bewertungen vermelden. Was es kann und wie es im Zoo der Kommandointerpreter einzuordnen ist, zeigt dieser Beitrag.

Von **Hermann Apfelböck**



Swiss File Knife (SFK) sieht sich als „Schweizer Messer" für Dateiobjekte und Dateioperationen aller Art. Das englischsprachige Werkzeug ist unter *https://sourceforge.net/projects/swissfileknife/* kostenlos verfügbar, weitere Infos liefert die Hersteller-Website *http://stahlworks.com/dev/swiss-file-knife.html*. Dort gibt es auch eine kostenpflichtige „Extended Edition" für 40 Dollar, die sich vor allem durch die Unterstützung einiger Packformate auszeichnet. Wir haben uns ausschließlich die kostenlose Variante angesehen. Die maßgeblichen Motive, sich auf SFK einzulassen, sind

1. installationsfreie Portabilität – eine relativ kleine Datei (unter zwei MB) im Pfad genügt – fertig!
2. plattformunabhängiges, konformes Arbeiten unter Linux, Windows und Mac-OS.

Einrichtung und Funktionsumfang

Nach dem Download der zum System passenden Variante von sourceforge.net erhält man für Linux eine „sfk187-linux-64.exe" und für Windows eine „sfk187.exe". Unter Linux genügt es dann, die Datei nach „sfk" umzubenennen und sie mit

```
chmod +x sfk
```

ausführbar zu schalten. Danach ist das Tool im Terminal aus dem aktuellen Verzeichnis mit dem Aufruf

```
./sfk
```

sofort startklar. Im Dauerbetrieb bequemer ist eine Kopie in ein Path-Verzeichnis – etwa:

```
sudo cp sfk /usr/bin
```

Danach läuft es jederzeit im Terminal nach Eingabe *sfk*. Da man mit Userrecht in den meisten Path-Verzeichnissen kein Schreibrecht hat, SFK aber für einige Komfortfunktionen temporäre Scripts anlegt, ist es noch besser, SFK etwa unter „/home/ha/sfk" abzulegen und dies in den Path aufzunehmen (in der Datei „~/.bashrc"):

```
PATH=$PATH:/home/ha/sfk
```

Unter Windows sollte man die erhaltene „sfk187.exe" der Bequemlichkeit halber auf den Dateinamen „sfk.exe" verkürzen und ebenfalls in ein Path-Verzeichnis kopieren – hier etwa nach „\Windows\System32". Danach läuft es jederzeit im Terminal (cmd) nach der Eingabe *sfk*. Diese Eingabe ohne Parameter liefert eine Kurzhilfe zu den knapp 120 Einzelbefehlen. Eine Hilfe zu jedem Einzelbefehl erscheint, wenn Sie diesen ohne weitere Angaben eingeben – etwa *sfk sort*.

Die Syntax dieses Kommandointerpreters ist gewöhnungsbedürftig, aber logisch und der Funktionsumfang beachtlich. Die Basissyntax lautet immer:

```
sfk [Optionen] Befehl
  [Dateiobjekt(e)]
```

Konkrete Beispiele sehen dann so aus:

```
sfk list /media/ha
sfk -hidden -minsize=40m list /me
  dia/ha
```

Der eigentliche Befehl lautet hier „list", was einem „ls" oder „find" der Linux-Bash, beziehungsweise „dir" unter Windows nahekommt. Neben den wichtigsten Befehlen sollte man auch die globalen Optionen kennen, die der Befehl „sfk help options" auflistet. Die Optionen, die immer mit Bindestrich nach „sfk" angegeben werden, eröffnen interessante Filtermöglichkeiten, wie das obige Beispiel belegt. Anders als bei typischen Bash-Kommandos mit ihren je eigenen Schaltern gelten diese Optionen für viele SFK-Befehle (jedoch offenbar nicht für alle, wie die Kurzhilfe andeutet).

Ein weiteres Beispiel:

```
sfk -yes -withsub deblank /home/
  ha/Schreibtisch .png
```

Der eigentliche Befehl lautet „deblank" und ersetzt Leerzeichen durch Unterstriche in Dateinamen. Die globalen Optionen „-yes" und „-withsub" geben an, dass die Aktion wirklich durchgeführt werden und alle

Unterverzeichnisse umfassen soll. Beachten Sie, dass SFK Ordnernamen und Dateinamen getrennt sehen will. Zwischen dem Zielordner und der zu bearbeitenden Extension „.png“ ist daher tatsächlich ein Leerzeichen.

Mit dem Befehl „run“ hat SFK auch einen Schlüssel zu binären Außenwelt:

```
sfk run ~/myscript.sh
```

Dieses Komando würde das genannte Shell-Script starten.

Die Durchsicht der etwa 120 Befehle macht schnell deutlich, dass Swiss File Knife den Fokus tatsächlich auf Dateiobjekte legt: Netzwerkbefehle sind unterrepräsentiert und hier wird auch nicht deutlich, warum etwa „sfk wget“ eine eigene Wget-Variante benutzt, die aber bei weitem nicht den Umfang des bekannten Wget erreicht. Hübsch ist hingegen der „Instant HHTP-Server“, der nach

```
sfk httpserv /home/ha
```

das angegebene Verzeichnis übers Netzwerk für jeden Browser freigibt (siehe Aufmacherbild). Unter Linux geht das zwar auch mit anderen Mitteln, aber unter Windows ist das ein Highlight.

Bei Dateien und Ordnern ist an alles gedacht. Neben erwartbaren Befehlen wie „list“, „copy“, „delete“, „deltree“, „rename“, „filefind“, „treesize“, „mkdir“, „xfind“, „sort“ hat SFK viele Spezialitäten an Bord, die man andernorts nur über Zusatztools oder eigene Scripts erreicht. Interessante Möglichkeiten bieten etwa die Indexfunktionen:

```
sfk gindex /media/ha/
```

Dieser Befehl ist nicht spektakulär, da er lediglich alle Daten des angegebenen Pfads in eine Sammeldatei schreibt. Jedoch muss man sich um das Wo und Wie nicht kümmern, sondern kann danach mit

```
sfk name Steuer 2016 Steinmann
```

umstandslos komplex suchen. Alles, was hier nach dem Befehl „name“ folgt, sind Suchwörter.

„sfk split“ und „sfk join“ sind Kommandos, die große Dateien zerlegen oder kleine Teile zu einer großen zusammenlegen: Der Befehl

```
sfk split 10m Datei.pdf
```

```
ha@UBU16: ~/Schreibtisch/News
sfk
SFK - The Swiss File Knife File Tree Processor.
Release 1.8.7 Base/XD Revision 2 of Jul 15 2017.
StahlWorks Technologies, http://stahlworks.com/
Distributed for free under the BSD License, without any warranty.

type "sfk commandname" for help on any of the following.
some commands require to add "-help" for the help text.

   file system
      sfk list       - list directory tree contents.
                       list latest, oldest or biggest files.
                       list directory differences.
                       list zip jar tar gz bz2 contents.
      sfk filefind   - find files by filename
      sfk treesize   - show directory size statistics
      sfk copy       - copy directory trees additively
      sfk sync       - mirror tree content with deletion
      sfk rename     - flexible multi file rename
      sfk partcopy   - copy part from a file into another one
      sfk mkdir      - create directory tree
      sfk delete     - delete files and folders
      sfk deltree    - delete whole directory tree
      sfk deblank    - remove blanks in filenames
      sfk space [-h] - tell total and free size of volume
      sfk filetime   - tell times of a file
      sfk touch      - change times of a file
      sfk index      - create index file(s) for fast lookup
      sfk name       - lookup file names using index files
      sfk setbytes   - set bytes at offset within a file

   conversion
      sfk lf-to-crlf - convert from LF to CRLF line endings
      sfk crlf-to-lf - convert from CRLF to LF line endings
      sfk detab      - convert TAB characters to spaces
      sfk entab      - convert groups of spaces to TAB chars
```

Eine erste Befehlsübersicht liefert die Eingabe sfk ohne Parameter. Zu den einzelnen Befehlen gibt es ausführliche Hilfe nach „sfk [Befehl]“ – also etwa nach sfk sync.

```
ha@UBU16: ~/Schreibtisch/News
sfk list -hidden -minsize=50m /media/ha/ToshibaRed
/media/ha/ToshibaRed/Büro/Privat/Pusteblume/Pusteblume_2009.pdf
/media/ha/ToshibaRed/Büro/_Artikel/LinuxWelt/_OLD/2012-04/ZV/Linux Format September 2011 (UK).pdf
/media/ha/ToshibaRed/Büro/_Artikel/LinuxWelt/_OLD/2013-04/_Layouts/_Booklet/2013-04_PCWL-E-Booklet.pdf
/media/ha/ToshibaRed/Büro/_Artikel/LinuxWelt/_OLD/2013-05/_Booklet/2013-05-06_PCWL-E-Booklet.pdf
/media/ha/ToshibaRed/Büro/_Artikel/LinuxWelt/_OLD/2013-05/_Layouts/_Booklet/2013-04_PCWL-E-Booklet.pdf
/media/ha/ToshibaRed/Büro/_Artikel/LinuxWelt/_OLD/2013-05/_Layouts/_Booklet/2013-05-06_PCWL-E-Booklet.pdf
/media/ha/ToshibaRed/Büro/_Artikel/LinuxWelt/_OLD/2014-01/_Layouts/Booklet_2014-01/2013-05-06_PCWL-E-Booklet.pdf
/media/ha/ToshibaRed/Büro/_Artikel/LinuxWelt/_OLD/2014-02/_Layouts/Booklet/2014-02_PCWL-E-Booklet.pdf
/media/ha/ToshibaRed/Büro/_Artikel/LinuxWelt/_OLD/2014-03/_Layouts/Booklet/2014-03_PCWL-E-Booklet.pdf
/media/ha/ToshibaRed/Büro/_Artikel/LinuxWelt/_OLD/2015-06/203 Mediencenter/OpenELEC-imx6.arm-5.0.2.img
/media/ha/ToshibaRed/Büro/_Artikel/LinuxWelt/_OLD/2016-02/203 Medienserver Emby/emby/Linux_Format__November_2015.pdf
/media/ha/ToshibaRed/Büro/_Artikel/PDFs und Manus/IDG-Sonderhefte/SoHe AndroidWelt 06 2014.pdf
/media/ha/ToshibaRed/Büro/_Artikel/PDFs und Manus/IDG-Sonderhefte/SoHe Freeware XXL 2011.pdf
/media/ha/ToshibaRed/Büro/_Artikel/PDFs und Manus/IDG-Sonderhefte/SoHe Hacks 2016.pdf
/media/ha/ToshibaRed/Büro/_Artikel/PDFs und Manus/IDG-Sonderhefte/SoHe Sicherheit XXL 2012.pdf
/media/ha/ToshibaRed/Büro/_Artikel/PDFs und Manus/IDG-Sonderhefte/SoHe WLAN 2016.pdf
/media/ha/ToshibaRed/Büro/_Artikel/PDFs und Manus/IDG-Sonderhefte/SoHe WLAN_2013.pdf
/media/ha/ToshibaRed/Büro/_Artikel/PDFs und Manus/PC-Welt/2011_02.pdf
/media/ha/ToshibaRed/Büro/_Artikel/PDFs und Manus/PC-Welt/2011_03.pdf
```

Eingängige Filteroptionen: Hier sorgt der list-Schalter „-minsize=50m“ (50 MB) für die Ausgabe entsprechend großer Dateien.

macht aus einer großen PDF-Datei Zehn-MB-Häppchen, die nummerierte Namen „Datei.pdf.part1“ und so fort erhalten. Weitere Spezialtools zum inhaltlichen Bearbeiten, Patchen und Zerlegen von Medien- und Binärdateien sind „setbytes“, „partcopy“ und „media“.

Fazit und Einordnung

Die wenigen Beispiele konnten nicht ansatzweise die Möglichkeiten des Swiss File Knife andeuten. Es handelt sich um eine konzeptionell durchdachte Werkzeugsammlung. Einige einfache Basisbefehle sind schnell habituiert, die überaus komplexen Detailoptionen fordern allerdings erhebliche Einarbeitungszeit. Hier liegt das Problem: Ein Einsteigertool ist SFK gewiss nicht – oder jedenfalls nur in engen Grenzen. Echte Kommandozeilenfreaks aber haben es sich ihrer Shell längst gemütlich gemacht und eventuelle Defizite durch externe Erweiterungen oder Scripts kompensiert.

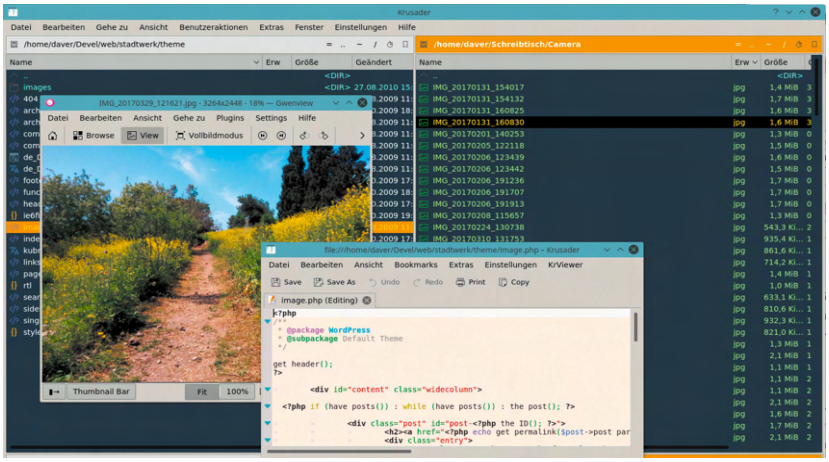
Bleibt noch das relativ starke Argument plattformübergreifender Konsistenz. Aber auch das verliert an Gewicht: Der heutige Shell-Guru kann sich eine Bash-Shell unter Windows 10 einrichten oder andersrum eine Windows-Powershell unter Linux (jedenfalls unter Ubuntu-basiertem Linux). Danach verbleibt als Kernzielgruppe des SFK eigentlich nur noch der Windows-User, der mit der Windows-Powershell nicht klarkommt (das ist die Regel) und die traditionelle Cmd unter Windows als defizitär erachtet (das ist ebenfalls die Regel). Folgerichtig arbeitet SFK unter Windows ausgereifter, während es unter Linux einige Detailmängel zeigt. ●

Zwei Fenster zum Dateisystem

Nach 30 Jahren noch ein Hit: Zwei-Fenster-Dateimanager überzeugen auch heute, denn meist sollen Dateien von A nach B gehen. Linux hat in der Shell und auf dem Desktop einige Dateimanager dieser Art auf Lager.

Von **David Wolski**

Es gibt Software, deren Bedienkonzept zeitlos ist. In den 80er-Jahren brachte der Norton Commander mit zwei Fenstern eine komfortable Dateiverwaltung auf ein spärliches DOS-Textinterface. Mit einer Reihe von Tastenkürzeln, die viele Anwender der alten Schule immer noch im Muskelgedächtnis haben, ließ sich der NC ohne Maus und grafische Oberfläche blitzschnell bedienen. Seitdem hat diese Bedienführung mit ihrer Fensteraufteilung und Tastenbelegung viele andere Betriebssysteme wie Linux und natürlich grafische Oberflächen erobert. Der Beitrag stellt die wichtigsten Vertreter dieser Art Dateimanager für Linux vor.



Krusader setzt sich im Funktionsumfang ab: Der Dateimanager ist dank der verwendeten KDE-Tools und Bibliotheken der mächtigste Vertreter dieser Klasse.

Das Multitalent: Krusader

Das KDE-Programm Krusader ist ein Alleskönner unter den Dateimanagern. Das liegt zum großen Teil an den Funktionen der KDE-Bibliotheken und KDE-Standardtools. Wie es sich für ein KDE-Programm geziemt, sind das Aussehen und die vorgegebene Tastenbelegung frei konfigurierbar und es gibt ein Menüsystem für eigene Aktionen. Krusader liegt seit kurzem in Version 2.6 vor, die für die neue KDE-Inkarnation Plasma 5 neu geschrieben wurde. Neben allen einfachen und komplexen Dateioperationen beherrscht der Krusader auch das Splitten und Zusammenfügen von Binärdateien, kann Archive als Ordner öffnen, ausgewählte Dateien packen und Textdateien mit dem eigenen Texteditor bearbeiten. Krusader ist generell unter allen Linux-Desktops eine gute Wahl für Poweruser.

Besonderheiten: In den Adresszeilen der Dateifenster unterstützt Krusader die Netzwerkprotokolle der KIO-Slaves von KDE, um über SSH, SFTP, FTP, Webdav und Samba auf Dateien im Netzwerk zuzugreifen. Der Clou ist, dass Krusader und andere KDE-Programme diese Dateien direkt öffnen und bearbeiten können.

Installation: Krusader ist in den verbreiteten Distributionen mit KDE 4 oder Plasma 5 nicht vorinstalliert. Das Paket „krusader“ ist aber überall verfügbar, denn es gehört zur offiziellen KDE-Programmsammlung „Extragear“. Bei der Installation ist darauf zu achten, dass auch die KIO-Slaves mitinstalliert werden. In Ubuntu und Co. sind diese im Paket „kio-extras“ untergebracht.

Der Flexible: Sunflower

Das Python-Programm hat sich von einem Mauerblümchen zu einem ausgewachsenen Dateimanager entwickelt. Als Toolkit für seine weitgehend deutschsprachige Oberfläche nutzt Sunflower GTK von Gnome und passt sich gut in Gnome und Gnome-ähnliche Desktopumgebungen wie Unity, Mate, Cinnamon und XFCE ein. Die Entwicklungsgeschwindigkeit von Sunflower kann sich sehen lassen: Es gibt keine längeren Pausen und regelmäßig neue Funktionen. So kam zuletzt beispielsweise eine Unterstützung für Android-Geräte hinzu.

Bei seiner Bedienung folgt Sunflower der typischen Tastenbelegung des alten Norton Commander und legt

die wichtigsten Dateioperationen auf die F-Tasten.

Besonderheiten: Für den Zugriff auf Netzwerkressourcen (Samba, SSH, Webdav, FTP) und Android-Geräte gibt es den eigenen Mountmanager unter „Tools“. Dateien auf so eingebundenen Laufwerken kann Sunflower umbenennen, kopieren, verschieben, aber nicht einfach zur Bearbeitung oder Betrachtung öffnen. Dies ist eine Beschränkung seitens Gnome, das diesen transparenten Netzwerkzugriff nicht unterstützt.

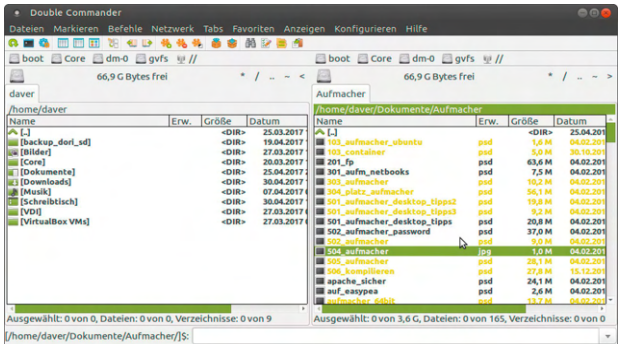
Installation: In den Paketquellen der verbreiteten Linux-Distributionen ist Sunflower nicht zu finden, aber die Entwickler liefern Pakete (GNU Public License) für alle populären Linux-Systeme.

Webseite: *http://sunflower-fm.org/de*

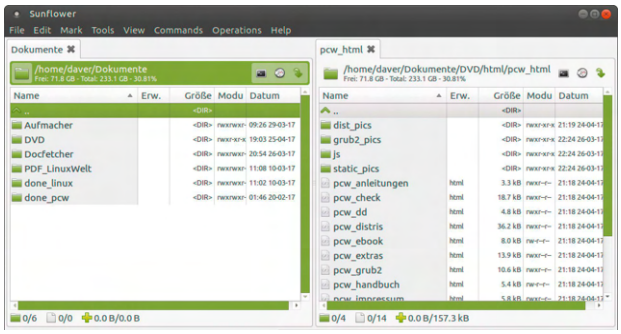
Bekanntes Äußeres: Double Commander

Wer unter Windows den Dateimanager Total Commander nutzt, findet hier das Linux-Pendant. Den Double Commander gibt es mit GTK2-Toolkit und auch mit QT, um sich gut in alle Linux-Desktops einzufügen. Auf dem Gnome-Desktop ist der Dateimanager ein guter Ersatz für den zurzeit instabilen Gnome Commander, der mit aktuellen Desktops nicht zusammenarbeitet.

Optisch orientiert sich das Gnome-Programm inklusive der Farbgebung stark am Total Commander. Archive werden wie Ordner behandelt. An Netzwerkprotokollen spricht das Programm zunächst nur Samba und FTP. SSH und andere sind aber über Plug-ins verfügbar.



Open-Source-Variante des Total Commander: Die Entwickler des Double Commander verheimlichen nicht, dass der beliebte Dateimanager für Windows als Vorbild dient.



Mehr als Basisfunktionen: Sunflower hilft bei Zugriffen auf Netzressourcen, kann Verzeichnisse abgleichen und hat ein Umbenennungstool sowie einen Archivmanager als Plug-in.

Besonderheiten: Laut Entwickler steht der Double Commander dem Total Commander so nahe, dass sich sogar die Plug-ins des Windows-Programms einbinden lassen.

Installation: Das beliebte Tool ist in den Standard-Paketquellen von Debian und Ubuntu vorhanden. Das Paket heißt dort „doublecmd-gtk“ beziehungsweise „doublecmd-qt“. Die Webseite liefert zudem ausführbare Programmdateien für alle Distributionen – sogar für Windows.

Webseite:
https://doublecmd.sourceforge.io

Der Schlanke: Emelfm2

Auf betagten Rechnern oder Platinen kann der schlichte Emelfm2 als besonders schlanker Dateimanager mit zwei Fenstern punkten. Der Funktionsumfang fällt etwas schmaler aus als bei den Verwandten, aber es gibt alle grundlegenden Dateioperationen mit den üblichen Tastenkürzeln, Lesezeichen zu Verzeichnissen und eine Übersicht eingehängter Laufwerke. Netzwerkfunktionen fehlen.

Besonderheiten: Trotz schlichter Aufmachung hat Emelfm2 interessante Funktionen für Fortgeschrittene, so etwa eine eingebaute Befehlszeile mit Ausgabefenster.

Installation: In Ubuntu und seinen Varianten liegt der Dateimanager als „emelfm2“ in den Standard-Paketquellen.

Webseite: *http://emelfm2.net*

Der Midnight Commander

Der Midnight Commander ist kein grafisches Programm für den Linux-Desktop, sondern ein Terminalprogramm. Er eignet sich ideal zur Dateiverwaltung auf Linux-Servern via SSH. Unter den Linux-Programmen ist der Midnight Commander damit dem klassischen Norton Commander am ähnlichsten. Es gibt Netzwerkfunktionen im Menü, um per SSH, SFTP, FTP und Samba auf andere Rechner zuzugreifen. Der Dateimanager wird in allen verbreiteten Linux-Distributionen über das Paket „mc“ bereitgestellt.

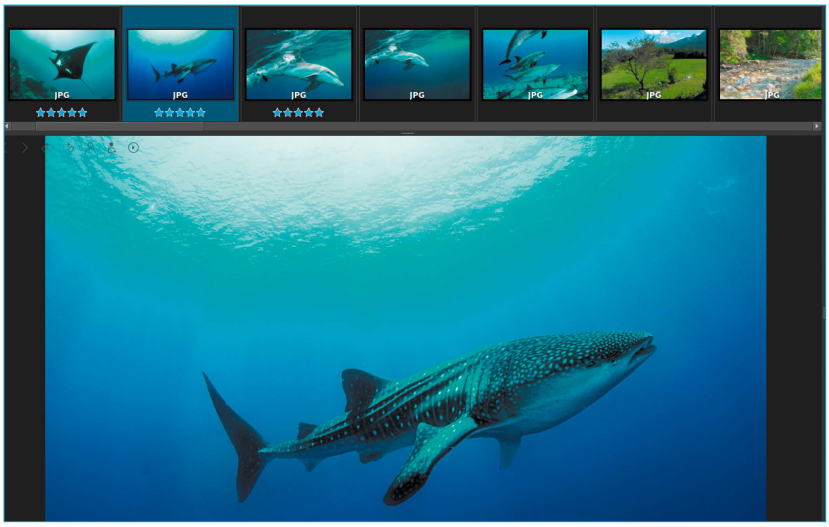


Kann auch ins Netz: Der Midnight Commander spricht einige Netzwerkprotokolle wie SSH, SFTP, FTP und Samba.

Fotos mit Digikam optimal verwalten

Möchten Sie Ihre Urlaubsfotos verwalten, verschlagworten, sortieren und nachbearbeiten? Dafür gibt es unter Linux eine Reihe von tauglichen Programmen, das Werkzeug erster Wahl ist jedoch Digikam.

Von **Jürgen Donauer**



Die Software Digikam ist sehr umfangreich und lässt praktisch keine Wünsche offen. Der Einstieg ist relativ einfach, die vielen Funktionen optimal zu meistern, bedarf aber Zeit und Übung. Das Programm erschöpfend zu erklären, würde annähernd eine komplette LinuxWelt erfordern: Dieser Artikel stellt Digikam vor und behandelt in erster Linie das Verwalten von Bildern. Lassen Sie sich von Digikams Umfang nicht abschrecken. Starten Sie mit den hier gezeigten Schritten. Dann haben Sie Ihre Fotosammlung im Griff und können Bilder suchen und filtern. Mit dem Handbuch und etwas Neugier bekommen Sie den Rest auch schnell in den Griff. Einige elaborierte Funktionen werden Sie vermutlich niemals benötigen.

Digikam installieren

In den Repositories der großen Distributionen finden Sie Digikam mit Sicherheit. Ob das immer die neueste Version ist, steht auf einem anderen Blatt. Aktuell ist derzeit Digikam 5.6. Verwenden Sie Ubuntu, Linux Mint oder ein anderes Ubuntu-Derivat, können Sie ein externes PPA verwenden. Dort erscheint die neueste Version von Digikam immer relativ schnell.

```
sudo add-apt-repository
  ppa:philip5/extra
sudo apt-get update
sudo apt-get install digikam5
```

Je nach Version lautet die letzte Zeile

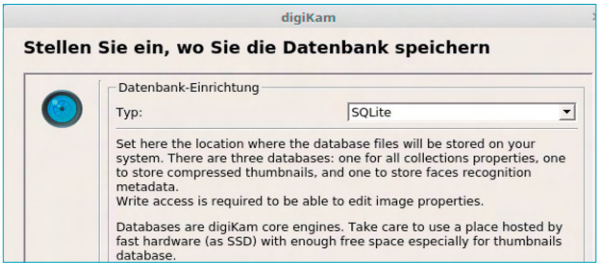
```
sudo apt-get install digikam
```

für Ubuntu 17.04 oder

```
sudo apt-get install digikam5
```

für Ubuntu 16.04 oder Linux Mint 18. Die Entwickler von Digikam stellen außerdem ein distributionsunabhängiges Appimage zur Verfügung. Was es damit auf sich hat und wie Sie das Appimage verwenden, lesen Sie im Kasten „Digikam als Appimage“. Sofern Sie nicht KDE als Desktop verwenden, werden Sie feststellen, dass die Installation von Digikam jede Menge zusätzlicher Bibliotheken benötigt. Grund dafür ist, dass Digikam früher sehr eng mit KDE verzahnt war. Die Entwickler sind derzeit dabei, die Software Schritt für Schritt von KDE zu entkoppeln. Wenn Sie die Masse der abhängigen Pakete abschreckt, können Sie das bereits angesprochene Appimage verwenden.

Hinweis: Es gibt drei Vorteile bei einer Installation über die Standardrepositories gegenüber dem Appimage. Zum einen sind Updates kleiner, da nur bestimmte Teile aktualisiert werden. Bei

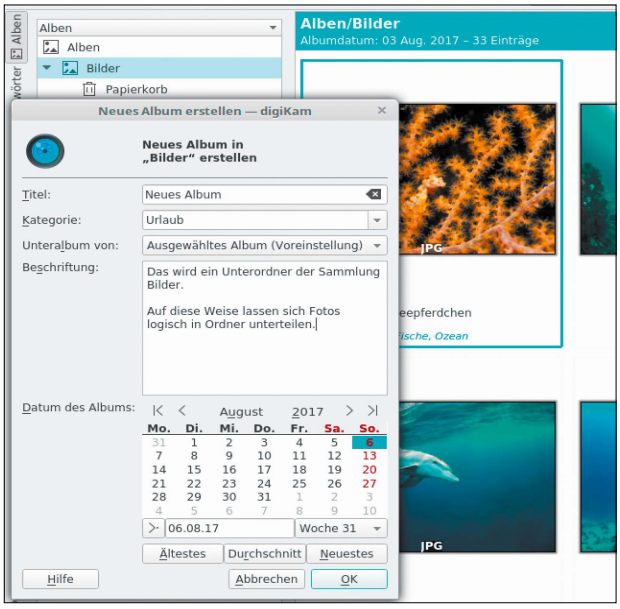


Datenbanktyp: Digikam kann auch My SQL als Datenbank verwenden, sicherer ist allerdings die Verwendung von Sqlite. Damit wird auch das Backup einfacher.

einem Appimage müssen Sie immer das komplette Paket herunterladen. Zweitens hält sich eine Installation an das Thema des restlichen Desktops. Das Programm sieht besser integriert aus, während ein Appimage manchmal optisch wie ein Fremdkörper wirkt. Der dritte Vorteil ist, dass in der Regel der Dateimanager des Systems mit Digikam zusammenarbeitet. Das bedeutet unter anderem den komfortableren Zugriff auf Wechseldatenträger.

Digikam starten und einrichten

Beim ersten Start von Digikam nimmt Sie ein Einrichtungsassistent an die Hand und Sie konfigurieren die Software. Die Einstellungen lassen sich später jederzeit ändern. Geben Sie einen Ordner an, in dem sich Ihre Bilder befinden und wo Sie die Datenbank speichern möchten. Per Standard handelt es sich um eine Sqlite-Datenbank und das ist zugleich die sicherste Option für den Privatgebrauch. Die Software könnte auch My SQL verwenden, aber diese Option ist noch als experimentell gekennzeichnet. Außerdem ist ein Backup wesentlich einfacher, wenn Sie Sqlite verwenden, da lediglich die entsprechende Datei zu kopieren ist. Legen Sie die Sqlite-Datenbank im selben Verzeichnis wie die Bilder an, dann



Ein rechter Mausklick auf die Sammlung (in unserem Fall „Bilder“) bietet die Erstellung eines neuen Albums an. Es wird dann zu einem Unterordner auf dem Datenträger.

genügen später Backups des kompletten Ordners – damit ist neben den Bildern auch die Datenbank gesichert.

Hinweis: Für das Backup ist wichtig zu wissen, dass die Software drei Datenbanken pflegt. „digikam4.db“ ist die Hauptdatei, „thumbnails-digikam.db“ ist für die Vorschaubilder zuständig und „recognition.db“ für die Gesichtserkennung.

Im nächsten Schritt fragt Digikam, wie mit Rohdateien (RAW-Format) umgegangen werden soll. Schießen Sie sowieso nur im JPG-Format, dann belassen Sie die Standardeinstellung. Profis wissen an dieser Stelle, welche Option sie bevorzugen.

Wie die Metadaten gespeichert werden sollen, ist allerdings sehr wichtig. Es geht an dieser Stelle darum, wo die Metadaten gespeichert werden. Lassen Sie für den Moment den Standard eingestellt. Die für eine effiziente Verwaltung wichtigen Metadaten beschäftigen uns später ausführlicher. Ob Sie im nächsten Schritt eine verkleinerte Versi-

Digikam als Appimage

Ein Appimage ist ein Paket, das alle Abhängigkeiten mit sich bringt. Die Software lässt sich damit unabhängig von der Distribution ausliefern. Appimages laufen auf allen modernen Distributionen wie Ubuntu, Linux Mint, Open Suse, Fedora, Red Hat, Debian, Arch.

Für die Entwickler hat das den Vorteil, dass sie nicht für jede Distribution speziell ein Paket erstellen müssen. Appimages lassen sich nach dem Herunterladen einfach ausführen.

Für Anwender ist es ein kleiner Nachteil von Appimages, dass die Pakete relativ groß ausfallen. Dafür bekommen Sie aber neue Software sofort geliefert und müssen nicht abwarten, bis der Distributor seine Paketquellen aktualisiert.

Im Downloadbereich von Digikam *https://www.digikam.org/download/* finden Sie Images für 32 und 64 Bit (circa 400 MB). Haben Sie das Appimage heruntergeladen, müssen Sie es zunächst ausführbar machen. Das funktioniert in vielen Distributionen über den Rechtsklick im Dateimanager und „Eigenschaften“. Hier finden Sie Option, die Datei „ausführbar“ zu machen. Die universelle Methode ist die Kommandozeile:

```
chmod a+x digikam*.appimage
```

Danach können Sie die Datei über den Dateimanager öffnen oder Sie erledigen das gleich auf der Kommandozeile:

```
./[Dateiname].appimage &
```

Für die aktuelle Version ist

```
./digikam-5.6.0-01-x86-64.appimage &
```

der passende Aufruf.

Möglicherweise fragt das System, ob das Appimage im System integriert werden soll. Das bedeutet nur, dass Digikam in das Hauptmenü aufgenommen wird. Ob Sie das wünschen oder nicht, bleibt Ihnen überlassen.

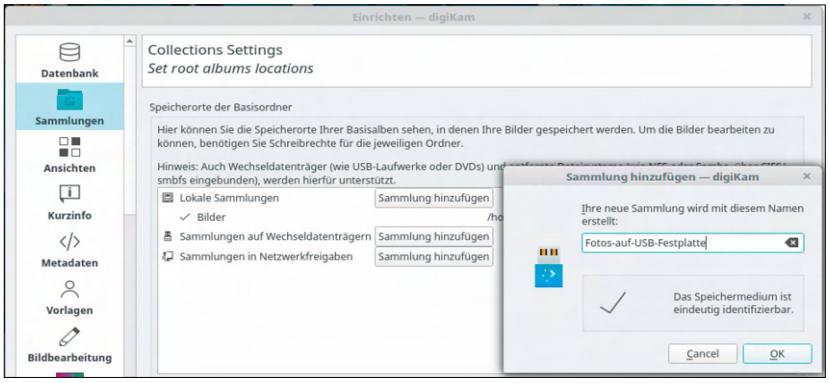
Hinweis: Auf unserem Linux Mint 18.2 mussten wir das Paket „libopenal1“ manuell nachinstallieren, nachdem Digikam 5.6 den Start verweigert hatte. Genau das sollte bei einem Appimage eigentlich nicht der Fall sein.

on der Vorschau laden lassen wollen oder nicht, bleibt Ihnen überlassen. Das gilt auch für das Verhalten, wenn die Software Dateien öffnet oder wie sich die Anzeige von Kurzinfos verhalten soll. Lesen Sie sich die ausführlichen Hinweise bei den Konfigurationsschritten durch und fällen dann die Entscheidung, die Ihnen sympathischer ist.

Erste Schritte mit Digikam

Befinden sich bereits einige Bilder im Ordner, den Sie für Digikam bestimmt haben, dann tauchen diese in Form von Vorschaubildern auf. Auf der linken Seite sehen Sie ein Menü, das per Standard auf „Alben“ steht. Die rechte Seitenleiste zeigt die „Beschreibung“ an. An dieser Stelle ist es unerlässlich, die Begriffe „Alben“ und „Sammlungen“ richtig einzuordnen: Während der Erstkonfiguration haben Sie in Digikam einen Order mit Bildern hinterlegt – das ist eine „Sammlung“. In dieser Sammlung können Sie weitere „Alben“ erstellen. Klicken Sie mit der rechten Maustaste auf „Bilder“ und danach auf „Neu“. Nun erstellen Sie ein Album, was in den Standardeinstellungen einem Unterordner im Verzeichnis „Bilder“ entspricht. Eine neue Sammlung fügen Sie hingegen über „Einstellungen -> Digikam einrichten -> Sammlungen“ hinzu. Eine Sammlung ist ein Basispfad, der auch auf einen Wechseldatenträger oder auf eine Netzwerkfreigabe zeigen kann.

Richten wir als Beispiel eine neue Sammlung ein, die sich auf einem USB-Datenträger befindet. Klicken Sie auf „Einstellungen -> Digikam einrichten -> Sammlungen“. Danach finden Sie unter „Sammlungen auf Wechseldatenträgern“ die Schaltfläche „Sammlung hinzufügen“. Navigieren Sie nun zum Pfad des USB-Datenträgers. Moderne Distributionen binden USB-Geräte gewöhnlich im Pfad „/media“ ein. Digikam beginnt danach sofort, die Fotos zu indexieren und Vorschaubilder zu erstellen. Ist der USB-Datenträger später einmal nicht angeschlossen, sehen Sie die Vorschaubilder trotzdem. Sie können dann auch nach Fotos suchen



Um Ihre Fotos zentral verwalten zu können, müssen sich nicht alle Sammlungen auf der lokalen Festplatte befinden. Digikam unterstützt Wechseldatenträger und Netzlaufwerke.

und so weiter. Nur eine Bearbeitung des Originals ist logischerweise so lange nicht möglich, bis der Wechseldatenträger wieder am Computer hängt.

Hat eine Sammlung mehrere Unterordner, dann kann Digikam entweder alle Bilder anzeigen oder nur jene des aktuell markierten Ordners. Dafür zuständig ist die Einstellung „Ansicht -> Albenunterbaum einschließen“.

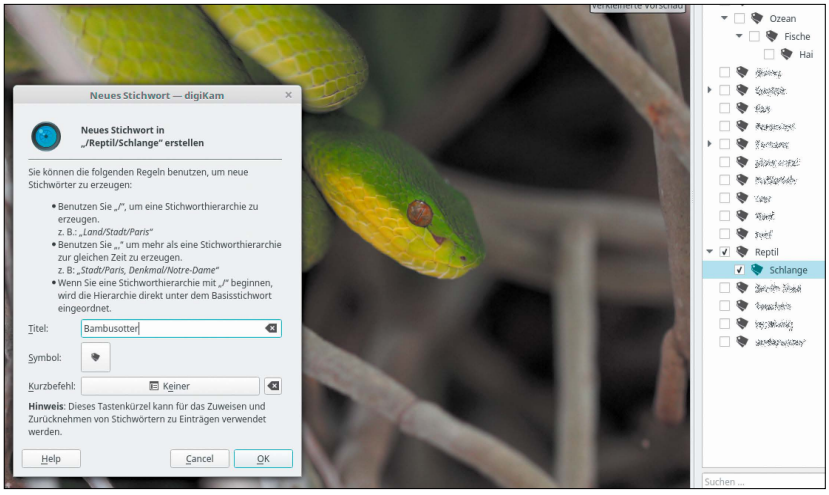
Stichwörter und Metadaten

Für die Verwaltung größerer Fotosammlungen sind Stichwörter unverzichtbar. Anhand dieser Schlagwörter lassen sich Fotos sehr schnell auffinden. Markieren Sie einfach das gewünschte Foto, klicken Sie in der rechten Seitenleiste auf „Stichwörter“ und legen Sie danach über die rechte Maustaste ein neues Stichwort an. Klicken Sie unten rechts auf „Anwenden“, dann werden die Metadaten für dieses Bild in die Datenbank geschrieben.

Tipp: Sie können jederzeit auch mehrere passende Fotos markieren und allen gleichzeitig ein Stichwort spendieren.

Klicken Sie nun auf „Einstellungen -> Digikam einrichten -> Metadaten“. Hier finden Sie die Sektion „Lesen und Schreiben der Metadaten“. Eine wichtige Einstellung ist die Behandlung von Nebendateien. Sie haben an dieser Stelle die Möglichkeit, Stichwörter und andere Metadaten in eine „xmp“-Datei schreiben zu lassen. Aus solchen Dateien können Digikam und andere Programme Metadaten lesen und damit erhöhen Sie die Kompatibilität zu anderen Programmen.

Zu den Metadaten gehört außerdem eine Bewertung des jeweiligen



Stichwörter als Metadaten: Hier erstellen wir das Stichwort „Bambusotter“ in der Stichworthierarchie „Reptil -> Schlange“. Damit ist das Kriechtier aufgeräumt und eingeordnet.

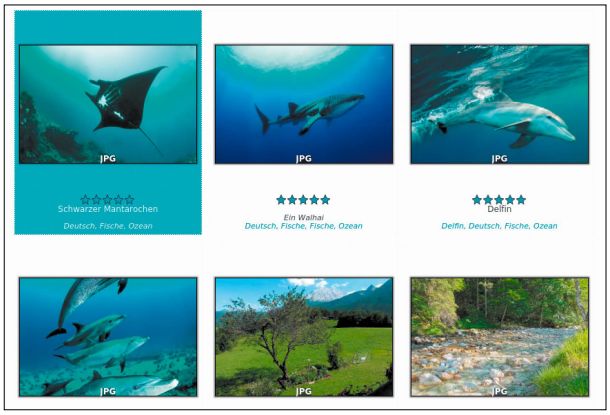
Fotos. Fahren Sie mit der Maus über ein Foto, erscheinen am unteren Rand fünf Sterne. Auf diese Weise bewerten Sie die Fotos auf einer Skala von eins bis fünf. Klicken Sie mit der rechten Maustaste auf das Foto, sehen Sie ganz unten im Menü die Option „Assign Labels“. Damit vergeben Sie einen Farbcode.

Hardwaretipp: Bei wirklich großen Fotosammlungen macht Digikam auf einer SSD wesentlich mehr Spaß. Hinterlegen Sie viele Stichwörter für sehr viele Fotos und lassen diese sowohl in die Bilder als auch in die Nebendateien schreiben, kommt es zu sehr vielen Schreiboperationen. Das kann bei einer herkömmlichen Festplatte unangenehm lange dauern und das Programm reagiert zeitweise nicht mehr. Besserung bringt an dieser Stelle die Option „Use lazy synchronization“. Damit werden Operationen in eine Warteschlange geschickt und erst dann in die Datenbank geschrieben, wenn der Anwender den Vorgang anstößt oder Digikam beendet. Die Funktion ist aber mit Vorsicht zu genießen. Es gibt Fehlerberichte, dass die Metadaten dabei nicht in die Nebendatei geschrieben werden.

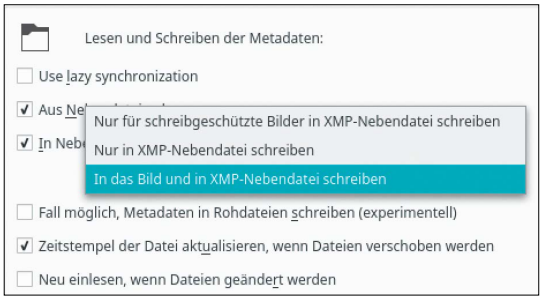
Fotos suchen und finden

Bei einer umfangreichen, aber mit Stichwörtern versehenen Fotosammlung finden Sie gewünschte Fotos im Handumdrehen: Klicken Sie in der Leiste links auf „Stichwörter“. Sie sehen eine Baumstruktur mit den Stichwörtern, die Sie angelegt haben. Klicken Sie sich einfach auf das gewünschte Schlagwort oder geben unten im Suchfeld das entsprechende Stichwort ein. Befinden sich sehr viele Stichwörter in der Datenbank, ist das die schnellere Lösung. Das Programm wird sofort das Ergebnis präsentieren.

„Beschriftungen“ nennt sich das Register unter den Stichwörtern. Damit können Sie nach Bewertungen und Farbcodes suchen. Bekommen zum Beispiel alle Unterwasserfotos immer den Farbcode „blau“, haben Sie mit einem einzigen Klick Zugriff auf die gesamte Kategorie.



Die Bewertung der eigenen Fotos ist sinnvoll, wenn Sie später mit wenig Aufwand Ihre besten Aufnahmen wiederfinden wollen. Fünf Sterne sind die Topauszeichnung.



Die Metadatenoption mit Nebendateien kann sehr wichtig sein. Sie brauchen nicht viel Platz und können sich als wertvolle Informationsquelle für andere Programme erweisen.

Pflege der Datenbanken

Damit Digikam immer schnell und sauber läuft, sollten Sie ab und zu die Datenbanken optimieren. Das ist auf zwei Arten möglich (bevor Sie mit den Datenbankdateien arbeiten, raten wir unbedingt zu einer Sicherung).

Klicken Sie auf „Extras -> Wartung“, finden Sie einen Punkt „Perform Database Cleaning“. Aktivieren Sie diese Option, wird die Hauptdatenbank „digikam4.db“ stets automatisch aufgeräumt. Sie können auch die beiden anderen Datenbanken aktivieren und weiterhin einstellen, dass die Datenbanken in der Größe optimiert werden. Sind die Datenbanken sehr groß, könnte das Programm temporär nicht mehr reagieren. Das ist bei der Verwaltung großer Sammlungen auf mechanischen Festplatten erfahrungsgemäß sehr lästig.

Daher empfehlen wir eine alternative Option über die Kommandozeile. Stellen Sie vor der Verwendung des Terminalbefehls vorsichtshalber sicher, dass Digikam geschlossen ist. Dann brauchen Sie noch das Paket „sqlite3“, das Sie unter Debian/Ubuntu und Derivaten wie folgt installieren:

```
sudo apt-get install sqlite3
```

Sie prüfen eine Datenbank auf deren Integrität mit diesem Befehl:

```
sqlite3 -line /[Pfad]/digikam4.db
 'pragma integrity_check;'
```

Als Ergebnis bekommen Sie im Idealfall die Antwort „integrity_check = ok“. Im Anschluss können Sie dann die Datenbank optimieren, was sich positiv auf die Größe auswirkt:

```
sqlite3 -line /[Pfad]/digikam4.db
 'vacuum;'
```

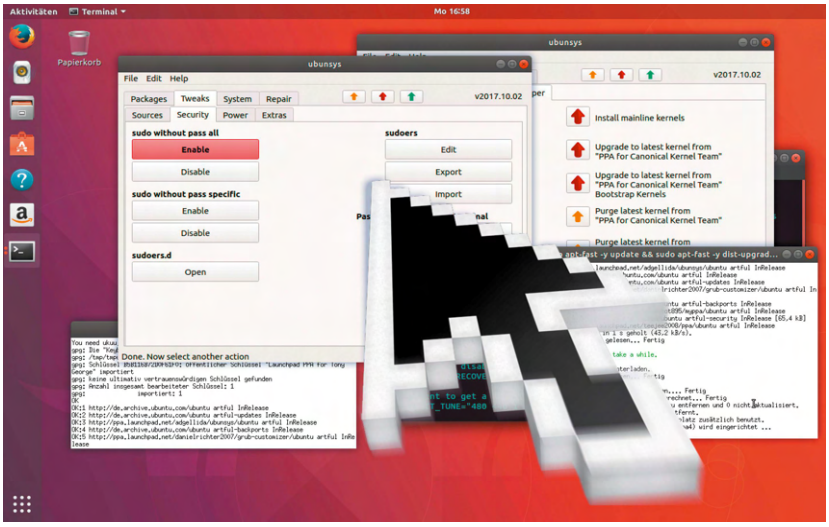
Danach prüfen Sie die Integrität am besten noch einmal. Vergessen Sie an dieser Stelle nicht, dass Digikam drei Datenbankdateien verwendet!

Sollten Sie die Datenbanken aus irgendwelchen Gründen verlieren, können Sie die Metadaten wieder aufbauen, wenn sie sich in den Bildern selbst oder in gespeicherten Nebendateien befinden. Je nach Umfang der Sammlung dauert das eine Weile.

Mehr Infos:
Digikam-Homepage:
https://www.digikam.org/
Digikam-Dokumentation (Englisch):
https://www.digikam.org/documentation/

Ubunsys: Admin-Tool für Ubuntu

Zur Administration eines Linux-Systems reicht üblicherweise die Shell. Ubuntu ist da keine Ausnahme. Einsteiger fragen oft, ob das nicht einfacher geht. Das Tool Ubunsys kann trotz langem Beipackzettel hilfreich sein.



Von **David Wolski**

Erfahrene Linux-Admins brauchen zum Aufbau und zur Pflege eines Systems selten mehr als vertraute Kommandozeilentools und einen Texteditor. Grafischen Admin-Hilfen hängt nicht zu Unrecht der Ruf nach, zu unflexibel, schnell veraltet und fehleranfällig zu sein. Es ist leicht, aus der Warte eines erfahrenen Sysadmins Tools dieser Art generell zu verdammen: Die Vereinfachung neuralgischer Systemeingriffe macht es einfacher, ein robustes Linux-System völlig lahmzulegen. Gerade im Umkreis Ubuntus, wo sich im Vergleich zu anderen Linux-Distributionen viele Einsteiger und Desktopanwender versammeln, gibt es aber einen stetigen Bedarf an grafischen Administrationshilfen.

Hilfe für Gelegenheits-Admins

Das neueste Programm aus dieser Kategorie ist Ubunsys, das speziell auf Ubuntu-Systeme zugeschnitten ist. Ein Schwerpunkt liegt auf der Verwaltung von Paketquellen (Repositories), ein anderer bei der Konfiguration von sudo zur Delegation von root-Rechten an Benutzer. Für experimentierfreudige Anwender gibt es die Möglichkeit, neuere Kernel-Versionen aus den Ubuntu-Entwicklungszweigen zu installieren. Spätestens hier wird klar, dass Ubunsys fortgeschrittene Desktopanwender und Linux-Bastler bedienen will, die ein System gerne bis ins Details anpassen möchten, aber lange Ausflüge in die Kommandozeile scheuen. So zeigt sich auch gleich ein Dilemma aller Programme dieser Art: Ubunsys hat trotz seines überschaubaren Funktionsumfangs ein großes Potenzial, bei unbedachten Gebrauch das Linux-System zu verkonfigurieren.

Installation und erster Start

Nach diesem obligatorischen Warnhinweis zur Installation: Der Entwickler pflegt den Quellcode von Ubunsys auf Github (*https://github.com/adgellida/ubunsys*), stellt aber zur einfachen Einrichtung auch ein PPA bereit. Aus diesem Repository wird Ubunsys mit den Befehlen

```
sudo add-apt-repository
  ppa:adgellida/ubunsys
sudo apt-get update
sudo apt-get install ubunsys
```

unkompliziert in Ubuntu 16.04/17.10 und dessen offiziellen Varianten installiert.Ubunsys ist ein grafisches Front-End in C++, das seine eigentlichen Funktionen in Bash-Scripts ausgelagert hat, die beim Start aktualisiert werden. Ein Aufruf per *ubunsys* in einem Terminalfenster sollte die bevorzugte Startmethode sein, da sich so die internen Meldungen im Terminal zeigen. Beim ersten Start installiert Ubunsys das Tool apt-fast nach und verlangt dazu die Eingabe des sudo-Passworts.

Die Menüstruktur im englischsprachigen Ubunsys ist in zwei Ebenen unterteilt, mit den Kategorien „Packages“, „Tweaks“, „System“ und „Repair“ jeweils mit Unterkategorien. Während die erste Kategorie zur Installation von Paketen dient, sind die inte-

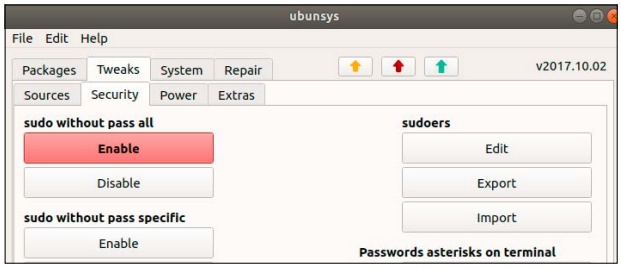
ressantesten Funktionen unter „Tweaks“ sowie „System“ untergebracht. Die folgende Liste zeigt einige Highlights jener Menüpunkte, die eine passable Hilfe oder eine Abkürzung bei der Administration sind.

Passwortloses sudo: Der Menüpunkt „Tweaks -> Security -> sudo without pass all -> Enable“ ist gleich eine der potenziell gefährlichsten Einstellungen in Ubunsys. Mit dieser Einstellung darf der aktuell angemeldete User nach der Eingabe von *sudo* im Terminal als root schalten und walten, ohne dazu noch sein Passwort angeben zu müssen. Diese Konfiguration kommt nur auf lokalen Systemen zu Hause infrage, wenn keinerlei Einbruchsgefahr über eine Netzwerkverbindung besteht. Untergebracht ist die Einstellung recht geschickt in der separaten Konfigurationsdatei „/etc/sudoers.d/all_sudoers_addition“. Ein Klick auf „Disable“ aktiviert die Passwortabfrage wieder und entfernt die genannte Datei aus dem System.

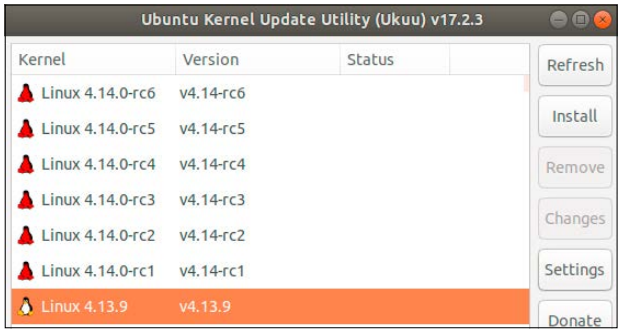
Einzelne Programme ohne Passwort: Weniger riskant als ein generell passwortloses sudo ist die Definition eines einzelnen Kommandozeilenprogramms, das der aktuell angemeldete User ohne Passwort aufrufen darf. Der Menüpunkt „Tweaks -> Security -> sudo without pass all -> Enable“ öffnet ein Terminal, das erst den Namen des gewünschten Programms und dann dessen Pfad abfragt.

Sterne für sudo-Passwörter: Aus Sicherheitsgründen verzichtet sudo auf eine Rückmeldung bei der Passworteingabe. Die Punkte unter „Tweaks -> Security -> Passwords asterisks on terminal“ aktivieren beziehungsweise deaktivieren die Anzeige von Sternchen nach dem Aufruf von sudo.

Alte Kernel-Versionen entfernen: Beim Wechsel in Ubuntu 16.04 auf einen neuen Hardware Enablement Stack (HWE) mit neuer Kernel-Version behält das System zunächst auch die ältere Kernel-Version. Unter dem Punkt „System -> Advanced user -> Clean ancient kernels“ kann Ubunsys obsolete Kernel deinstallieren. Diese Funktion nutzt im Hintergrund das Ubuntu-Tool byob und entfernt tatsächlich nur veraltete Linux-Kernel.



Gewagt: Ubunsys ist derzeit noch eine Gemischtwarenhandlung an Funktionen, die Desktopanwendern die Administration erleichtern will.



Externes Tool zur Auswahl einer Kernel-Version: Bei Bedarf rüstet Ubunsys als weitere Hilfe das Programm Ukuu nach, das inoffizielle Kernel installieren kann.

Zusätzliche Kernel installieren: Für jede Ubuntu-Ausgabe gibt es einen ausgiebig getesteten, offiziell unterstützten Kernel. Darüber hinaus baut das Entwicklerteam Ubuntus aber auch laufend weitere Kernel-Versionen zu Testzwecken und stellt diese als DEB-Paket unter *http://kernel.ubuntu.com/~kernel-ppa/mainline/v4.13.9* bereit. Wenn aktuelle Hardware, etwa AMDs Ryzen-Prozessoren, mit einem älteren Kernel instabil laufen, dann kann der Wechsel auf eine neue Kernel-Version weiterhelfen. Allerdings ist die manuelle Installation neuerer Kernel als DEB-Paket nicht ganz einfach. Unter „System -> Developer -> Install mainline kernels“ hilft das eigenständige Tool Ukuu bei der Auswahl und Installation einer neueren Kernel-Version weiter. Der Menüpunkt installiert sie bei Bedarf aus einem weiteren PPA und startet sie anschließend.

Fazit: Nützlich bis riskant

Nach einigen Experimenten mit Ubunsys, die man tunlichst nicht auf einem produktiv eingesetzten Ubuntu-System unternehmen sollte, wird klar, dass es sich noch um Betaware handelt. Die Funktionen unter „Tweaks -> Power“ sind in einigen Ubuntu-Versionen wirkungslos und sollten lieber über die verwendete Desktopumgebung konfiguriert werden. Auch der Schalter unter „Tweaks -> Security -> Firewall“ ist ohne eine vorherige manuelle Konfiguration der „Uncomplicated Firewall“ (ufw) Ubuntus nicht sinnvoll. Der Entwickler, der übrigens nach unserem Test seines Tools erfreulich schnell auf Bugreports reagiert hat, muss noch einige Unstimmigkeiten beheben, damit Ubunsys eine universale Administrationshilfe für Ubuntu-Systeme wird. Davon abgesehen hat Ubunsys einige nette Abkürzungen auf Lager, die erfahrenen Desktopanwendern einige Handgriffe abnehmen.

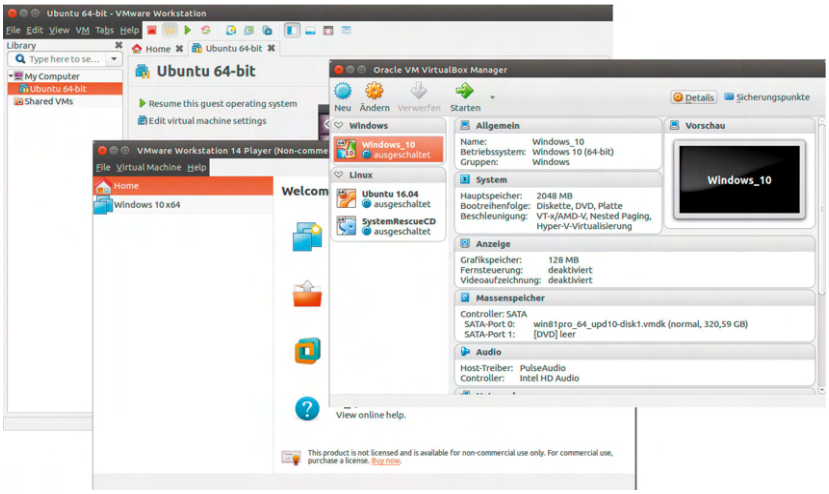
Ubunsys: Pro und Contra

- ⊕ erledigt als Front-End wichtige Handgriffe der Administration
- ⊕ liegt für alle Ubuntu-Varianten vor (16.04/17.10)
- ⊕ Entwickler reagiert schnell auf Bugreports
- ⊖ arbeitet als Front-End und öffnet Terminals (xterm) für Aktionen
- ⊖ bietet allzu einfachen Zugriff auf riskante Einstellungen
- ⊖ befindet sich noch in der Entwicklung (Betastadium)

Grundlagen der Virtualisierung

Dank Virtualisierungstechnologie lassen sich unter Linux auch Windows-Anwendungen nutzen. Virtualisierung ist aber auch für System- oder Softwaretests interessant.

Von **Thorsten Eggeling**



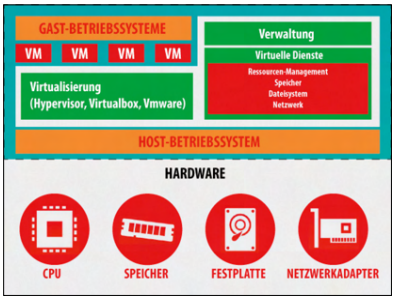
Virtualisierungssoftware: Virtualbox und Vmware Workstation Player sind ohne große Einarbeitung leicht zu bedienen. Vmware Workstation bietet zusätzliche Funktionen für Profis.

Wer mehrere Betriebssysteme auf seinem PC nutzen möchte, muss diese nicht nebeneinander auf der Festplatte installieren. Einfacher geht's mit Virtualisierungssoftware, über die sich weitere Systeme in einem Fenster oder bildschirmfüllend starten lassen. Das ist praktisch, wenn Sie neue Betriebssysteme ausprobieren oder unter Linux auch Windows-Programme nutzen müssen. Im Vergleich zur herkömmlichen Installation auf der Festplatte bieten virtuelle Maschinen einige Vorteile: Sie können mehrere virtualisierte Systeme gleichzeitig nutzen, der aktuelle Zustand lässt sich jederzeit sichern sowie wiederherstellen und Sie können Software gefahrlos ausprobieren, ohne das installierte Hauptsystem zu gefährden. Es gibt jedoch auch Nachteile: Virtualisierte Systeme laufen etwas langsamer, die Grafikleistung ist geringer und Sie benötigen ausreichend CPU-Leistung und Hauptspeicher für zwei oder mehr Betriebssysteme.

So funktioniert Virtualisierung

Virtualisierungssoftware bildet einen kompletten Rechner („virtuelle Maschine") mit allen Komponenten wie Festplatten-, Grafik und Netzwerkadapter nach. Wenn im virtuellen System („Gastsystem") ein Zugriff beispielsweise auf das Netzwerk erfolgt, läuft dieser über einen virtuellen Netzwerkadapter und dann über einen Treiber des installierten Systems („Hostsystem") zum physikalisch vorhanden Netzwerkadapter. Das Gastsystem sieht also nicht die tatsächlich vorhandene Hardware, sondern nur die virtuellen Komponenten.

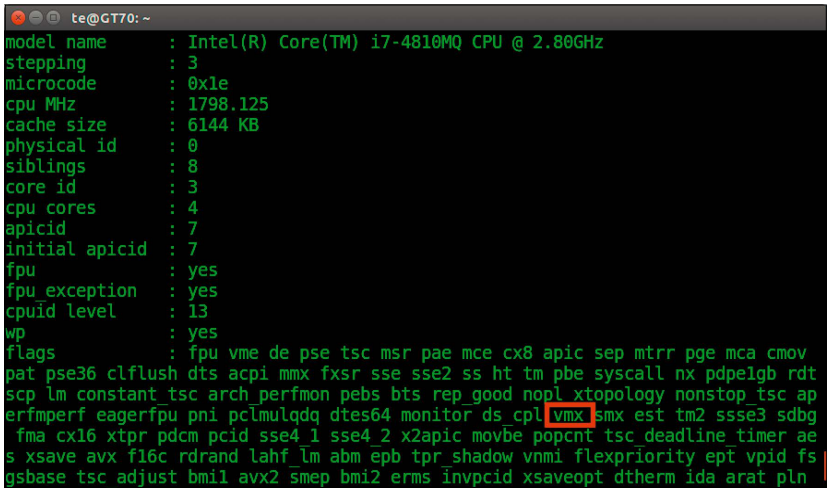
Bei der Virtualisierung fängt eine Virtualisierungsschicht Befehle ab, die das Gastsystem an Prozessor und Hardware sendet. Nur das zuerst gestartete Betriebssystem darf privilegierte CPU-Instruktionen verwenden, die später gestarteten Anwendungen dagegen nicht. Dieser privilegierte Zugriff findet im „Ring 0" der CPU statt („Kernel-Mode") und umfasst direkten Zugriff auf Interrupts und RAM. Die abgesicherten Ringe darüber, Ring 1, 2 und 3, gehören zum „User-Mode". Treiber dürfen beispielsweise im Ring 1 und 2 arbeiten, normale Programme für das Betriebssystem arbeiten dagegen nur ab Ring 3. Das gilt auch für die Virtualisierungssoftware. Damit trotzdem CPU-Befehle aus dem Gastsystem beim Prozessor ankommen, baut ein Hypervisor die Anweisungen bei Bedarf um. Dafür ist eine ständige Analyse der Befehle aus dem Gastsystem nötig. Was umgebaut werden muss, hängt von der Art des virtuellen Systems und



Ein Gastsystem („VM") kann die Hardware im PC nicht direkt verwenden. Virtuelle Dienste sorgen für die Zuteilung.

der Plattform ab (32 oder 64 Bit). In der Virtualisierungssoftware gibt es daher Vorlagen mit unterschiedlichen Optionen für ein 32-Bit- sowie 64-Bit-Windows oder Linux.

Paravirtualisierung: Bei diesem Verfahren greift der Kernel des Gastsystems über eine abstrakte Verwaltungsschicht auf die Hardwareressourcen zu, was zu einer Verbesserung der Geschwindigkeit führen kann. Der Kernel muss dafür speziell angepasst sein, was aber bei aktuellen Linux- und Windows-Systemen standardmäßig der Fall ist.



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

Virtuelle Maschinen beschleunigen

Ursprünglich war für die üblichen x86-Prozessoren, die in den meisten PCs und Notebooks stecken, die Virtualisierung von Betriebssystemen nicht vorgesehen. Es kann nur ein einziges System laufen, das die volle Kontrolle über den Prozessor und die sonstige Hardware hat. Seit längerer Zeit schon lassen sich jedoch Virtualisierungsfunktionen über Treiber und Software nachrüsten, ohne dass die Hardware das explizit unterstützen muss. Die damit erreichbare Leistung ist zufriedenstellend, wenn auch nicht optimal.

Seit 2006 unterstützen die Prozessorhersteller AMD und Intel die Virtualisierung auch direkt und hardwareseitig in der CPU. Das hat seither die Leistung der virtualisierten Systeme deutlich verbessert. Außerdem ist es möglich, in einer virtuellen Maschine ein 64-Bit-Betriebssystem (Gastsystem) zu betreiben, selbst wenn diese unter einem 32-Bit-System (Hostsystem) ausgeführt wird. AMD nennt die Technik AMD Virtualization (AMD-V). Sie ist in AMD-Prozessoren seit dem Athlon 64 von 2006 enthalten. Bei Intel heißt die vergleichbare Erweiterung „Virtualization Technology", „Intel VT" oder „Intel VT-x" und ist seit dem Pentium 4 Modell 662 verfügbar.

In der Praxis spielt das jedoch keine große Rolle. Kaum jemand wird einen mehr als zehn Jahre alten PC mit wenig CPU-Leistung und Hauptspeicher nutzen, um darauf mehrere Betriebssysteme zu virtualisieren. PCs und Notebooks mit 64-Bit-Prozessor und einem 64-Bit-Betriebssystem sind inzwischen Standard. Zu Testzwecken kann man jedoch auch ein 32-Bit-Gastsystem installieren.

Die hardwaretechnischen Virtualisierungsfunktionen sind in der PC-Firmware allerdings häufig deaktiviert. Genauen Aufschluss über die Fähigkeiten der CPU zeigt unter Linux folgende Befehlszeile in einem Terminalfenster

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

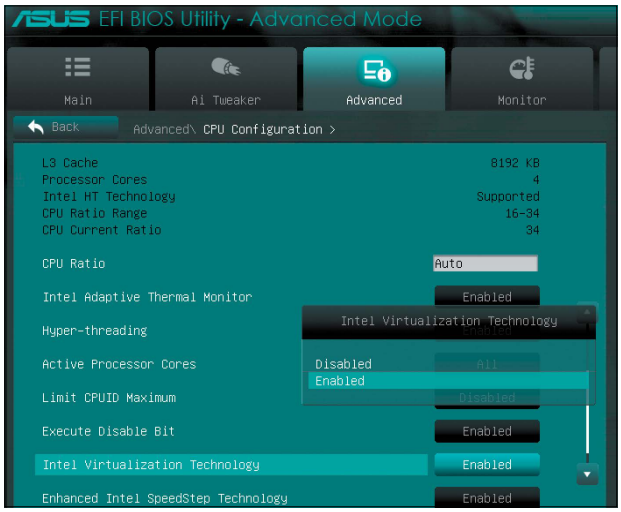
Wenn Sie in der Ausgabe einen Wert größer „0" sehen, dann unterstützt der Prozessor Virtualisierungsfunktionen und diese sind auch aktiv. Bei einem Intel Core i7 beispielsweise lautet das Ergebnis „8", weil alle acht Prozessorkerne Intel-VT unterstützen. Mit

```
cat /proc/cpuinfo
```

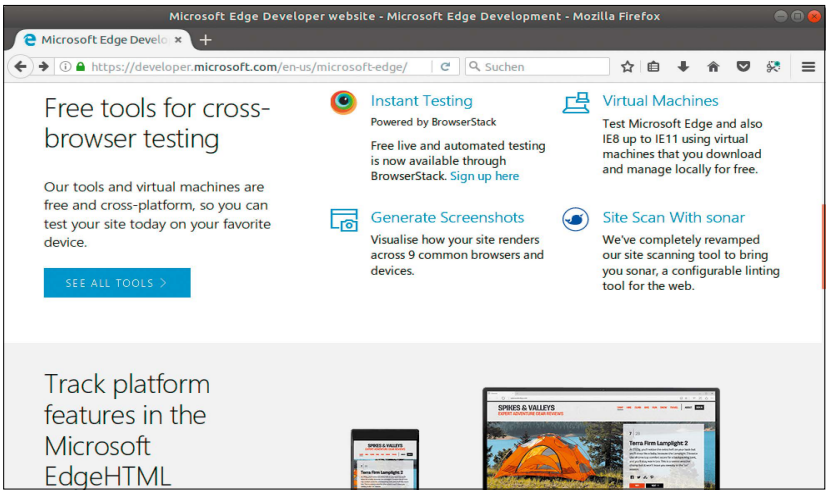
können Sie sich auch die komplette Liste der CPU-Eigenschaften anzeigen

Virtualisierungsoftware für Linux

	KVM/Qemu	Oracle Virtualbox 5	Vmware Workstation Player 14	Vmware Workstation 14
Internet	*http://linux-kvm.org*	*www.virtualbox.com*	*www.vmware.com*	*www.vmware.com*
Preis	kostenlos (Open Source)	kostenlos (teilweise Open Source)	private Nutzung kostenlos, sonst ab 170 Euro	ab etwa 275 Euro
Funktionen				
Gemeinsame Zwischenablage	ja	ja	ja	ja
Gemeinsame Ordner	nur für Linux-Gastsysteme	ja	ja	ja
VM-Schnappschüsse	ja	ja	nein	ja
VM-Klonfunktion	ja	ja	nein	ja
Mehrere VMs parallel	ja	ja	nein	ja
3D-Beschleunigung im Gastsystem	nein	ja	ja	ja
USB 2.0/3.0 im Gastsystem	ja/eingeschränkt	ja/ja	ja/ja	ja/ja



Bios-Einstellungen: Intel-VTx ist oft nicht standardmäßig aktiviert. Setzen Sie die Option etwa bei „Intel Virtualization Technologie“ auf „Enabled“.



Windows zum Download: Fertige virtuelle Maschinen gibt es kostenlos von Microsoft. Sie laufen 90 Tage lang, was zum Ausprobieren oder für Softwaretests ausreicht.

lassen. Die einschlägigen Werte „vmx“ beziehungsweise „svm“ tauchen hinter „flags:“ auf. Erscheint in der Ausgabe von cpuinfo dagegen eine „0“, dann Sie im Bios/Firmwaresetup nach, ob sich AMD-V oder Intel-VT („vt-x“, „Intel Virtualization Technologie“) aktivieren lässt. Manchmal gibt es auch Optionen für „AMD-Vi“ beziehungsweise bei Intel „Vt-d“. Sofern vorhanden, aktivieren Sie diese ebenfalls.

Dahinter verbirgt sich die I/O-Virtualisierung („Input/Output“), über die sich der Datenaustausch mit Netzwerkadaptern, Grafikchips und Festplattencontrollern beschleunigen lässt. Virtualisierungssoftware wie Virtualbox oder Vmware (siehe die beiden nachfolgenden Artikel) funktioniert notfalls auch ohne direkte Hardwareunterstützung – wenn auch oft etwas langsamer. Allerdings ist es dann nicht möglich, beispielsweise ein 64-Bit-System zu virtualisieren, wenn der PC unter einem 32-Bit-Linux läuft.

Hypervisor für Desktop und Server

Es gibt verschiedene Techniken, Gastbetriebssysteme auf einem Rechner in virtuellen Umgebungen zu starten. Bei diesen Techniken unterscheidet man zumeist danach, auf welcher Ebene die Abstraktionsschicht angesiedelt ist, auf der die Virtualisierung vonstatten geht. Die verschiedenen Methoden liefern je nach angestrebten Einsatzzweck, etwa auf Desktops, Servern und für den Zugriff über das Netzwerk, die beste Leistung bei niedrigem Verwaltungsaufwand.

Typ-2-Hypervisor: Setzt eine Virtualisierungsumgebung als Basis ein ausgewachsenes Betriebssystem voraus, dann spricht man von einem „Typ-2-Hypervisor“. Generell ist ein Hypervisor, auch „Virtual Machine Monitor“ genannt, jene Verwaltungssoftware, welche die Kontrolle über die virtuellen Maschinen hat, diese starten und anhalten kann sowie Ressourcen zuweist. Beispiele für diesen Typ 2 sind die verbreiteten Virtualisierungsprogramme für den Desktop: Vmware Workstation Player, Vmware Workstation und Oracle Virtualbox.

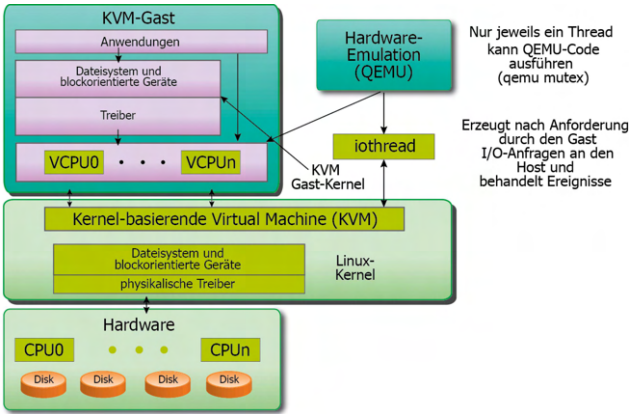
Typ-1-Hypervisor: Läuft der Hypervisor direkt auf der Hardware und ersetzt dabei das Betriebssystem, dann handelt es sich um einen Typ-1-Hypervisor. Diese Virtualisierungsumgebungen werden beim Einsatz auf Servern und in Rechenzentren auf Computern bevorzugt, die sowieso nur virtuelle Maschinen beherbergen sollen – dann allerdings gleich dutzendweise. Beispiele dafür sind Vmware Vsphere , Oracle VM Server und Citrix Xen Server.

Mischformen: Hyper-V von Microsofts Serverbetriebssystemen und Windows 8.1/10 Pro sowie die Technik „KVM“ des Linux-Kernels sind Mischformen. Die Virtualisierungsfunktionen sind hier Teil des Betriebssystems selbst oder werden wie bei von Linux direkt als Kernel-Modul geladen. Das Betriebssystem kann sich so selbst virtualisieren und mehrere unabhängige Instanzen starten.

Virtuelle Maschinen installieren oder herunterladen

In der Regel installieren Sie das gewünschte Gastbetriebssystem selbst in einer virtuellen Maschine. Dafür benötigen Sie die zugehörige ISO-Datei, die Sie auch sonst für die Installation auf der Festplatte verwenden würden. Tipps zur Installation von Virtualbox und Vmware und der Einrichtung virtueller Maschinen finden Sie auf den

folgenden Seiten. Es gibt aber bereits komplett vorbereitete virtuelle Maschinen zum Download. Microsoft beispielsweise bietet auf *www.modern.ie* wahlweise Windows 7, 8.1 und 10 als Testumgebungen für den Internet Explorer an (90 Tage). Folgen Sie auf der Seite dem Link „Virtual Machines“. Für Virtualbox ist *www.virtualboximages.com* eine gute Anlaufstelle. *www.osboxes.org* bietet Dateien für Virtualbox und Vmware an und *https://solutionexchange.vmware.com* nur für Vmware.



Eingebauter Virtualisierer: Im Linux-Kernel ist die Virtualisierungssoftware bereits enthalten. Die Paravirtualisierung sorgt für eine gute Leistung bei Linux-Gastsystemen.

Für Profis: Virtualisierung mit Kernel Virtual Machine (KVM)

KVM (Kernel Virtual Machine, *www.linux-kvm.org*) ist bereits seit längerer Zeit als Modul ein Bestandteil des Linux-Kernels. Zwingende Voraussetzung für KVM ist, dass die CPU des Systems die Virtualisierungserweiterungen von Intel (Intel VT-x) oder AMD (AMD-V) mitbringt. KVM selbst leistet keine Emulation, kann aber Geräte wie Netzwerk- und Festplattenadapter paravirtualisieren und an das Gastsystem weiterreichen. Für die Emulation von virtuellen Geräten wie Grafik- und Soundkarte zieht KVM bei Bedarf QEMU heran.

KVM besteht im Wesentlichen nur aus einem Kernel-Modul. Tools zur Konfiguration und Verwaltung der virtuellen Maschinen gehören nicht zum KVM-Projekt. Als grafisches Front-End dient der Virtual Machine Manager (*https://virt-manager.org*), der in den Repositories der meisten populären Distributionen enthalten ist. Die Verbindung zur Grafikausgabe des Gastsystems erfolgt über VNC oder über das Protokoll Spice. Unter Ubuntu installieren Sie die nötigen Pakete in einem Terminalfenster mit folgender Befehlszeile:

```
sudo apt install qemu-kvm libvirt
  -bin bridge-utils virt-manager
  qemu-system python-spice-client-
  gtk
```

Der aktuell angemeldete sudo-Benutzer wird bei der Installation der Programmpakete automatisch zur Gruppe „libvirtd“ hinzugefügt. Starten Sie Linux neu oder melden Sie sich ab und wieder an, damit diese Änderung wirksam wird.

Mit dem Virtual Machine Manager (Ubuntu-Dash: „Virtuelle Maschinenverwaltung“) sind Einrichtung der virtuellen Maschinen und Anpassungen bei den Gastsystemen komplizierter als bei Virtualbox oder Vmware. KVM wird überwiegend zur Virtualisierung von Linux-Servern genutzt. Hauptmotiv für KVM ist gegenüber Virtualbox und Vmware eine noch deutlich verbesserte Leistung. Bei der Windows-Virtualisierung ist KVM jedoch unterlegen. Hier müssen Sie sogar mit Abstrichen bei der Geschwindigkeit rechnen. Für Windows ab Vista (32 Bit und 64 Bit) gibt es von Red Hat entwickelte und von Microsoft signierte Gerätetreiber (Virtio-Driver, *www.pcwelt.de/vlc_ql*), um paravirtualisierte Geräte des Hosts im Gast zu verwenden. Infos zu KVM finden Sie auf *www.pcwelt.de/2199855*.

Simulation – Emulation – Virtualisierung

Im Zusammenhang mit dem Thema Virtualisierung tauchen häufig Begriffe wie Simulator, Emulator und virtuelle Maschine auf, die zwar Ähnliches, aber nicht dasselbe bedeuten. In einer Simulation wird ein fremdes System mit seinen Hardware- und Softwareeigenschaften vollständig abgebildet. Ein Beispiel dafür ist die Softwaresimulation (*www.wpavel.de*) des ab 1955 entwickelten historischen Computers Zuse Z22.

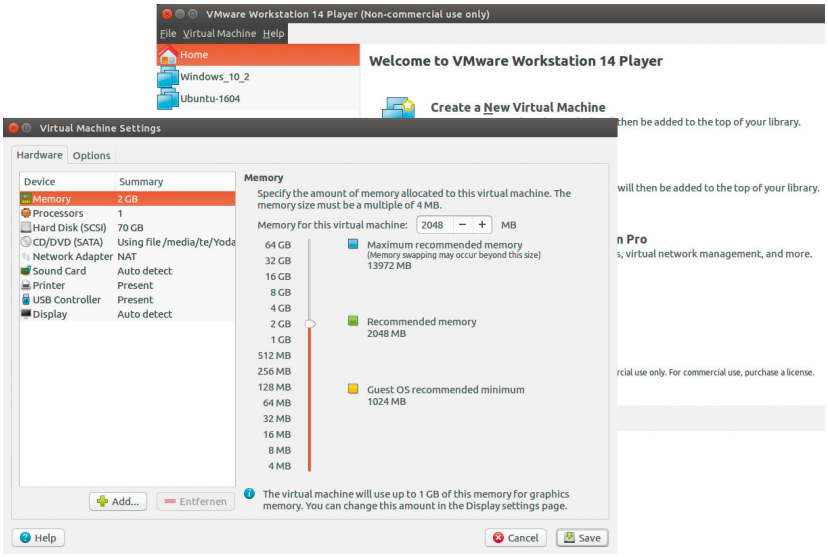
Für die Emulation genügt es, die Äußerlichkeiten nachzubilden – etwa, damit Programme kompatible Soft- und Hardwareschnittstellen vorfinden. Gemäß dieser Definition handelt es sich beispielsweise bei Wine (*www.winehq.org*) eher um eine Art Emulator. Wine bildet die Windows-API nach, die Funktionsaufrufe für Linux umsetzt. Das kann eine Alternative zur Virtualisierung sein, wenn Sie nur einzelne Windows-Programme unter Linux starten möchten. Allerdings funktioniert das nicht mit jedem Programm reibungslos und ohne Einschränkungen. Zu Wine und seinem Konfigurationswerkzeug Playonlinux finden Sie weitere Informationen im Artikel *www.pcwelt.de/2111210*.

Virtualisierung bedeutet, dass einem Gastbetriebssystem eigene Instanzen von Hard- und Software zugewiesen werden mit dem Ziel, mehrere konkurrierende Systeme gleichzeitig auszuführen, ohne das Wirtsbetriebssystem zu ändern. Bei dieser Technik geht es darum, möglichst wenig zu simulieren oder zu emulieren. Stattdessen werden Hardwarezugriffe möglichst immer an die tatsächlichen Systemkomponenten wie Prozessor, Grafikkarte, Festplatte durchgereicht und von der Virtualisierungsumgebung nur verwaltet.

Vmware in der Praxis

Vmware ist einer der bekanntesten Hersteller für Virtualisierungssoftware. Vmware Workstation ist eher für Profis gedacht, der kostenlose Player leistet vor allem bei privaten Anwendern gute Dienste, wenn auch mit kleinen Einschränkungen.

Von **Thorsten Eggeling**



Kleine Einschränkungen: Der kostenlose Vmware Player bietet bewährte Stabilität, aber nicht alle Funktionen der Bezahlsoftware Vmware Workstation Pro.

Seit 1998 liefert Vmware Programme für virtuelle Maschinen (VMs) auf Standard-PCs und in Rechenzentren. Vmware Workstation Pro (275 Euro) richtet sich an Endanwender aus dem professionellen Umfeld, die mehrere VMs gleichzeitig nutzen oder mit mehreren Anwendern im Team zusammenarbeiten wollen. Vmware Workstation Player ist für Privatanwender kostenlos (kommerzielle Nutzung: 166 Euro) und konnte ursprünglich nur die mit der Pro-Version erstellen VMs starten, aber nicht selbst erzeugen. Diese Einschränkung ist jedoch seit Version 3.0 aufgehoben. Im Vergleich zu Vmware Workstation Pro fehlen dem Player einige nützliche Funktionen, was sich aber mit ein paar Tricks beheben lässt.

Der technische Unterbau ist bei beiden Produkten in etwa gleich und damit auch die Leistung. Vmware unterstützt die Virtualisierung von mehr als 200 Gastsystemen, die zuverlässig und flüssig im virtuellen PC laufen. Im direkten Vergleich schneidet das kostenlose Virtualbox (siehe Seite 100) jedoch nicht schlechter ab. Die Software bietet aber einen Funktionsumfang, der ungefähr dem der teuren Vmware Workstation Pro entspricht. Eine Motivation, trotzdem zum funktionsreduzierten Vmware Workstation Player zu greifen, kann die einfache Oberfläche sein oder die Kompatibilität zu anderen Vmware-Produkten, wenn Sie diese bereits einsetzen.

Die folgenden Tipps und Anleitungen beziehen sich zumeist auf den kostenlosen Vmware Workstation Player. Allerdings funktionieren alle gezeigten Techniken so oder ähnlich auch mit der Vmware Workstation 14.

Bitte beachten Sie: Vmware Workstation Pro und Vmware Workstation Player gibt es nur als 64-Bit-Versionen. Unter einem 32-Bit-Linux lässt sich die Software nicht verwenden.

1. Vmware Workstation oder Player installieren

Workstation Player können Sie über *www.vmware.com/de.html* herunterladen. Klicken Sie in der Navigation auf der linken Seite auf „Downloads“ und unter „Kostenlose Produkt-Downloads“ auf „Workstation Player“. Klicken Sie hinter „VMware Workstation 14.0.0 Player for Linux 64-bit“ auf „Download“.

Für Vmware Workstation Pro verwenden Sie den direkten Link *www.vmware.com/go/tryworkstation-linux-64*. Für die Installation etwa unter Ubuntu oder Linux Mint öffnen Sie dann das Terminal und führen den folgenden Befehl

```
sudo sh Downloads/Vmware-Pla
  yer-7.1.4-3848939.x86_64.bundle
```

oder für die Variante Vmware Workstation Pro diesen Befehl

```
sudo sh Downloads/VMware-Worksta
  tion-Full-14.0.0-6661328.x86_64.
  bundle
```

aus. Passen Sie den Pfad „Downloads“ und die Dateinamen bei Bedarf an. Das Workstation-Setup richtet übrigens auch den Player mit ein. Ist Vmware Player schon auf dem System vorhanden, müssen Sie das Programm vorher entfernen.

Folgen Sie den Anweisungen des Installationsassistenten. Sie müssen die Lizenzbedingungen abnicken und werden dann zur Eingabe des Lizenzschlüssels aufgefordert. Lassen Sie das Feld leer und klicken auf „Next“. Wenn Sie den Player das erste Mal

starten, wählen Sie die Option „Use VMware Workstation 14 Player für free for non-commercial use“, bei der Workstation „I want to try VMware Workstation 14 for 30 days“ (30-Tage-Test). Wenn Sie einen Lizenzschlüssel gekauft haben, können Sie diesen später nach über „Help -> Enter License Key“ (Player) beziehungsweise „Help -> Enter Serial Number“ (Workstation) eingeben.

Vmware-Software deinstallieren: Um Vmware Workstation wieder zu entfernen, verwenden Sie diese Befehlszeile im Terminal:

```
sudo sh Downloads/Vmware-Worksta
 tion-Full-14.0.0-6661328.x86_64.
 bundle -u vmware-workstation
```

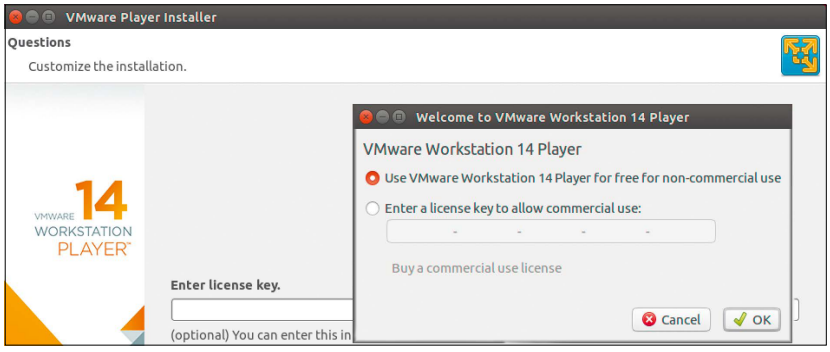
Den Player werden Sie mit dieser Zeile

```
sudo sh Downloads/Vmware-Pla
 yer-7.1.4-3848939.x86_64.bundle
 -u vmware-player
```

wieder los.

2. Linux oder Windows in einer VM installieren

Nach dem Start des Vmware Workstation Players klicken Sie auf „Create a New Virtual Machine“.



Mit oder ohne Lizenz: Private Nutzer dürfen Vmware Player ohne Lizenzschlüssel installieren, müssen aber eine nicht-kommerzielle Verwendung noch einmal bestätigen.

Schritt 1: Wählen Sie die Option „I will install the operating system later“, damit Sie vor der Installation noch einige Anpassungen vornehmen können. Hinweise zu einer alternativen Installationsmethode für Windows finden Sie am Ende dieses Abschnitts.

Schritt 2: Nach Klick auf „Next“ wählen Sie das Betriebssystem. Wenn Sie Ubuntu oder verwandte Distributionen wie Linux Mint, Kubuntu, Xubuntu oder Lubuntu installieren wollen, wählen Sie hinter „Version“ den Eintrag „Ubuntu“ (32 Bit) oder „Ubuntu 64-Bit“. Sollte das gewünschte System nicht in der Liste enthalten sein, entscheiden Sie sich für einen der Einträge, die mit „Other Linux“ beginnen.

Schritt 3: Klicken Sie auf „Next“. Vergeben Sie eine aussagekräftige Bezeichnung für das virtuelle System. Darunter können Sie bei Bedarf den Speicherort ändern, etwa wenn unter „/home/[User]/vmware“ nicht genügend Platz vorhanden ist.

Schritt 4: Nach „Next“ legen Sie die Größe der virtuellen Festplatte fest. Es empfiehlt sich, einen größeren Wert einzugeben als vorgeschlagen, damit auch nach einigen Updates und Soft-

Im Uefi- statt im Bios-Modus booten

Neuere PCs verwenden eine Uefi-Firmware statt des bisherigen Bios. Damit lässt sich auch von Festplatten mit mehr als zwei TB booten und die Firmware kann beispielsweise Updates direkt aus dem Internet herunterladen, obwohl diese Funktion kaum ein Hersteller nutzt. Außerdem lässt sich über Secure Boot die Bootumgebung vor Schadsoftware schützen. In einer virtuellen Maschine bietet Uefi allerdings kaum Vorteile.

Trotzdem unterstützt Vmware die Technik, damit Sie beispielsweise zu Testzwecken ein Betriebssystem auch im Uefi-Modus installieren können. In Vmware Workstation lässt sich Uefi über die grafische Oberfläche aktivieren. Erstellen Sie eine neu virtuelle Maschine (siehe Punkt 2). Gehen Sie auf „Edit virtual machine settings“ auf die Registerkarte „Options“ und auf „Advanced“. Wählen Sie die Option „UEFI“ und setzen Sie bei Bedarf ein Häkchen vor „Enable secure boot“. Speichern Sie die Einstellungen per Klick auf „Save“.

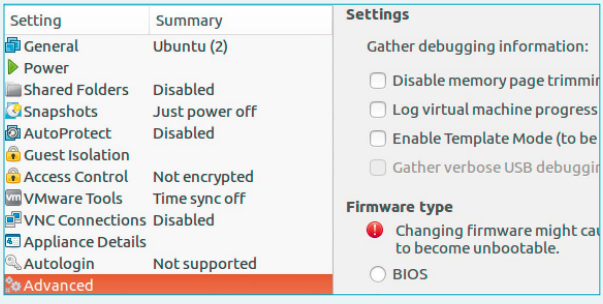
Da der Player die mit der Workstation erstellten VMs öffnen kann, beherrscht auch er diese Einstellungen, bietet diese Optionen jedoch nicht an. Stattdessen öffnen Sie hier die Konfigurationsdatei der virtuellen Maschine in einem Texteditor wie in Punkt 6 beschrieben. Fügen Sie ganz am Ende die Zeile

```
firmware = "efi"
```

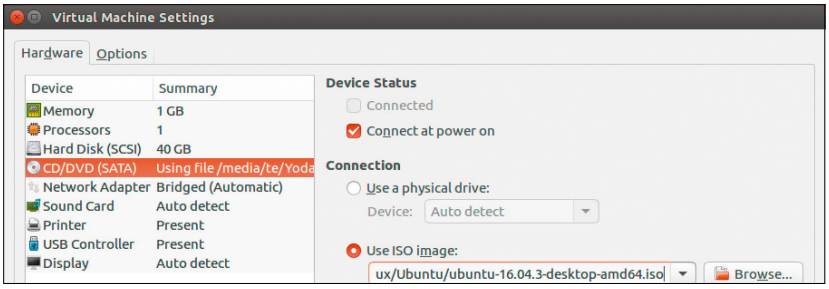
ein, für Secure Boot zusätzlich diese Zeile:

```
uefi.secureBoot.enabled = "TRUE"
```

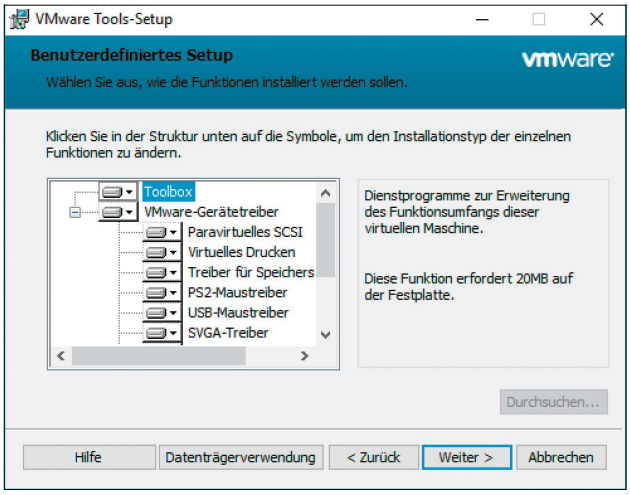
Richten Sie dann ein Betriebssystem in der virtuellen Maschine ein, das Uefi unterstützt, beispielsweise Ubuntu 16.04 oder Windows 10. Im Uefi-Modus lassen sich nur 64-Bit-Versionen installieren.



Uefi-Modus: In Vmware Workstation aktivieren Sie Uefi in den Einstellungen. Beim Vmware Workstation Player müssen Sie manuell Werte in die VMX-Datei eintragen.



Gastsystem einrichten: Für die Installation geben Sie den Pfad zu einer ISO-Datei an. Ein Setupmedium im CD/DVD-Laufwerk lässt sich ebenfalls verwenden.



Vmware-Tools-Setup: Unter Windows müssen Sie nur auf „Virtual Machine -> Install VMware Tools“ gehen, das Setup starten und den Anweisungen des Assistenten folgen.

wareinstallationen genügend Platz bleibt. Wählen Sie für maximale Leistung die Option „Store virtual disk as a single file“. Ist „Split virtual disk into multiple files“ aktiv, teilt Vmware die Datei auf, was das Backup erleichtert, aber die Lese- und Schreibgeschwindigkeit reduziert. Klicken Sie auf „Next“, „Finish“ und „Close“.

Schritt 5: Klicken Sie auf „Edit virtual machine settings“. Gehen Sie unter „Device“ auf „CD/DVD (SATA)“. Wählen Sie unter „Connection“ die Option „Use a physical drive:“, wenn Sie eine Installations-DVD besitzen. Andernfalls klicken Sie auf „Use ISO image:“ und wählen die Datei über „Browse“ aus (ISO-Dateien für Linux-Installation erhalten Sie über die Webseiten der jeweiligen Distribution wie etwa www.ubuntu.com, *https://linuxmint.com* oder *http://lubuntu.net*).

Oder Sie verwenden eine ISO-Datei aus dem Ordner „Image-Dateien“ der beiliegenden Heft-DVD. Wie Sie an ein Windows-Installations-ISO herankommen, beschreiben wir im Artikel „Virtualbox in der Praxis“ ab Seite 100. Speichern Sie die Änderungen per Klick auf „Save“.

Schritt 6: Starten Sie die virtuelle Maschine mit Klick auf „Power on“. Im virtuellen PC installieren Sie Linux oder Windows wie gewohnt. Wenn Sie in das Fenster des laufenden Gastsystems klicken, bleibt der Mauszeiger darin gefangen. Mit der Tastenkombination Strg-Alt lässt er sich wieder freigeben.

Beim Player erscheint nach einiger Zeit das Fenster „Software Update“ für die Vmware-Tools. Klicken Sie auf „Remind Me Later“. Wie Sie die Vmware-Tools herunterladen, installieren und nutzen, erfahren Sie in Punkt 3.

Easy Install nutzen: Wenn Sie im ersten Schritt nach „Create a New Virtual Machine“ die Option „Use a physical drive:“ oder „Use ISO image:“ wählen, versucht Vmware das Betriebssystem auf dem Installationsmedium zu erkennen. Bei Windows kommt dann „Easy Install“ zum Einsatz. Ein entsprechender Hinweis erscheint im Fenster. Nach einem Klick auf „Next“ können Sie den Windows-Produktschlüssel eingeben, eine der Windows-Editionen auf der DVD wählen (Home oder Pro), sowie Benutzernamen und Passwort für die Windows-Anmeldung vorab festlegen. Wenn Sie die virtuelle Maschine starten, läuft dann das Windows-Setup automatisch und ohne Benutzereingaben durch.

3. Vmware-Tools installieren

Die Vmware-Tools sind Hilfsprogramme und Treiber, welche die Leistung einer virtuellen Maschine verbessern und zusätzliche Funktionen mitbringen:

- deutlich bessere Grafikleistung vor allen bei Systemen, die Transparenz- oder 3D-Effekte nutzen
- Bildschirmgröße passt sich automatisch an, wenn Sie das Fenster der virtuellen Maschine vergrößern oder verkleinern
- gemeinsame Ordner für Gast- und Hostsystem
- gemeinsame Zwischenablage für Gast- und Hostsystem
- verbesserte Leistung der Maus und automatische Freigabe des Mauszeigers
- Uhrzeit von Gast- und Hostsystem lässt sich synchronisieren

Vmware-Tools für Windows-Gäste: Starten Sie das Windows-Gastsystem und klicken Sie im Menü auf „Virtual Machine -> Install VMware Tools“. Sollte das passende Toolpaket sich noch nicht auf dem Host-PC befinden, bietet Ihnen Vmware den Download an. Klicken Sie auf „Download and Install“ und bestätigen Sie mit dem root-Passwort. Die ISO-Datei mit den Vmware-Tools wird dann automatisch im Gastsystem eingehängt. In Windows starten Sie das Programm „setup64.exe“ beziehungsweise „setup.exe“ (32 Bit) von der virtuellen DVD und folgen den Anweisungen des Assistenten.

Vmware-Tools für Linux-Gäste: Einige Linux-Systeme bieten die Vm-

ware-Tools über die Paketverwaltung an. In Ubuntu 16.04 installieren Sie diese folgendermaßen in einem Terminalfenster:

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

Bei anderen Linux-Systemen oder alternativ auch unter Ubuntu verwenden Sie die Standard-Installationsmethode:

Schritt 1: Klicken im Menü auf „Virtual Machine -> Install VMware Tools“. Wenn es Ihnen Vmware anbietet, laden Sie die Vmware-Tools für Linux herunter und installieren das Paket im Hostsystem.

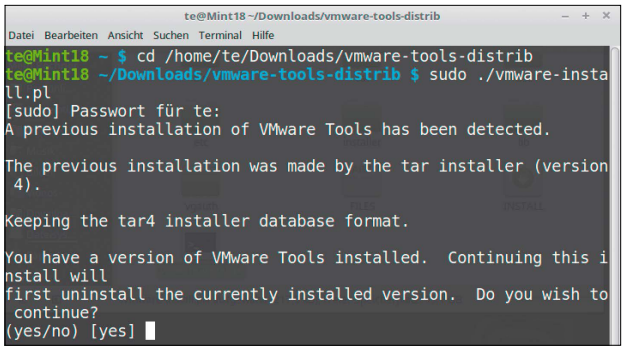
Schritt 2: Im Gastsystem öffnen Sie die virtuelle DVD im Dateimanager, klicken Sie die Datei „Vmware-Tool-10.1.15-6627299.tar.gz“ mit der rechten Maustaste an und wählen Sie „Entpacken nach...“. Wählen Sie einen Zielordner, beispielsweise „Downloads“ in Ihrem Home-Verzeichnis.

Schritt 3: Geben Sie in Ihrem Home-Verzeichnis den folgenden Terminalbefehl ein:

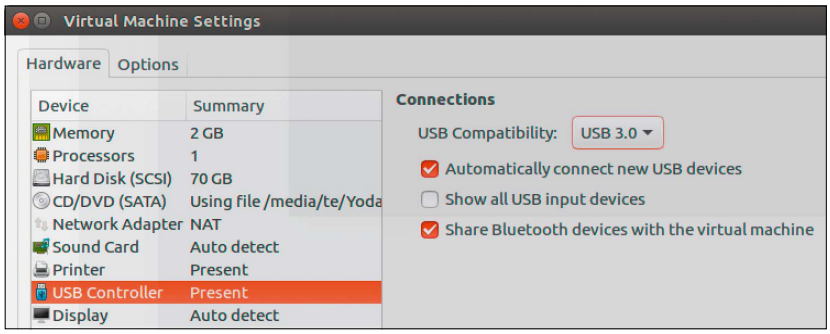
```
sudo Downloads/vmware-tools-dis
  trib/vmware-install.pl
```

Passen Sie den Pfad an, wenn Sie das Paket in ein anderes Verzeichnis geladen haben. Bei einigen Systemen, beispielsweise Ubuntu 16.04, erhalten Sie eine Meldung, wie „open-vm-tool packages are available from the OS vendor“. Übergehen Sie diese durch Eingabe von „yes“ gefolgt von der Eingabetaste. Wenn bereits eine Vorgängerversion installiert ist, bestätigen Sie deren Deinstallation mit „yes“. Alle weiteren Abfragen des Assistenten bestätigen Sie mit der Eingabetaste, außer Sie bevorzugen andere Pfade für die Installation. Nach Abschluss der Installation starten Sie Linux neu.

Tipp: Sie können die Vmware-Tools für alle unterstützten Betriebssysteme auf einmal herunterladen oder aktualisieren. Gehen Sie dazu auf „File -> Player Preferences“ und klicken Sie auf „Download All Components Now“. Wenn Sie Vmware Workstation installiert haben, sind die ISO-Dateien mit den Vmware-Tools Teil der Standardinstallation.



Vmware-Tools installieren: Linux-Nutzer müssen für die Einrichtung das Terminalfenster bemühen, aber auch hier führt ein Assistent schnell durch die Installation.



USB-Konfiguration: Vmware bietet Unterstützung für USB-2.0- oder USB-3.0-Geräte, die sich über „Virtual Machine – Removable Devices“ in das Gastsystem einbinden lassen.

4. USB-Geräte in eine VM einbinden

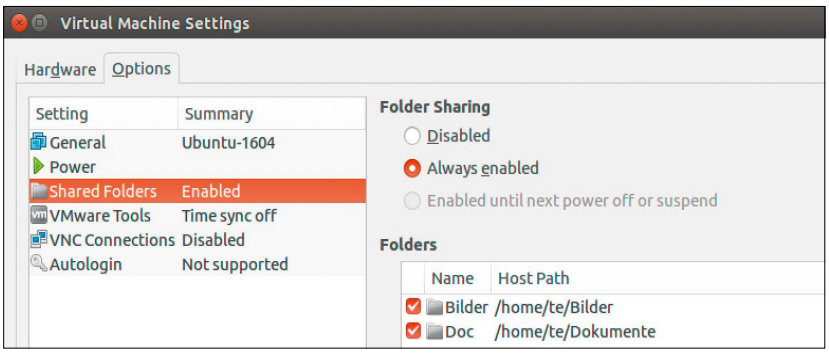
Eine virtuelle Maschine bildet einen eigenständigen PC und hat in der Regel keinen direkten Zugriff auf die tatsächliche Hardware. Eine Ausnahme sind USB-Geräte, die sich direkt einbinden lassen. Sie können beispielsweise einen Drucker am USB-Port im Gastsystem verwenden oder Daten auf einem USB-Stick speichern.

Die USB-Unterstützung ist standardmäßig aktiviert. Um das zu kontrollieren, gehen Sie bei einer virtuellen Maschine auf „Edit virtual machine settings“ und dann auf „USB Controller“. Hinter „USB Compatibility:“ stellen Sie „USB 3.0“ ein. Sollten sich USB-Geräte nicht in das Gastsystem einbinden lassen, wählen Sie das stabilere „USB 2.0“.

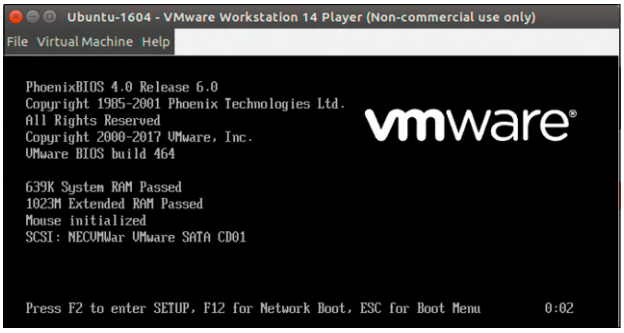
Beim Start einer virtuellen Maschine öffnet sich ein Fenster, in dem Ihnen Vmware die verfügbaren USB-Geräte anzeigt. Setzen Sie ein Häkchen vor „Never show this hint when starting a VM“, wenn Sie das Fenster nicht jedes Mal per Klick auf „OK“ schließen wollen. Die Geräte zeigt Ihnen der Player ohnehin in Menüs unter „Virtual Machine – Removable Devices“ an. Klicken Sie beim gewünschten USB-

Appliances: Fertige VMs nutzen

Vmware Player kann Abbilder mit vorbereiteten virtuellen Maschinen importieren. Gehen Sie auf „Open a Virtual Machine“ und wählen Sie die gewünschte „ovf“- oder „ova“-Datei aus. Da es sich um ein universelles Austauschformat handelt, kann die Software auch Dateien einlesen, die Sie in Virtualbox über „Datei -> Appliance exportieren“ gespeichert haben. In Vmware Workstation verwenden Sie „File -> Export to OVF...“. Der Player besitzt keine Exportfunktion. Fertige virtuelle Maschinen erhalten Sie beispielsweise auf *https://solutionexchange.vmware.com* oder *www.osboxes.org*. In den Beschreibungen finden Sie Hinweise zur enthaltenen Software und zu den vorkonfigurierten Benutzernamen und Passwörtern.



Datenaustausch: Über gemeinsam genutzte Ordner („Shared Folders“) übertragen Sie bequem Dateien zwischen Host- und Gastsystem.



Startauswahl: Aktivieren Sie „bios.bootdelay“ in einer VMX-Datei. Dann haben Sie beim Start einer VM genügend Zeit, die F2- oder Esc-Taste zu drücken.

Gerät auf „Connect (Disconnect from host)“. Es steht dann im Gastsystem zur Verfügung und wird im Gegenzug beim Hostsystem abgemeldet. Wenn Sie es nicht mehr benötigen, hängen Sie es im Dateimanager des Gastsystems aus, damit keine Daten verloren gehen, und wählen dann den Menüpunkt „Disconnect (Connect to host)“.

5. Datenaustausch zwischen Gast- und Hostsystem

Bei einer Standardkonfiguration besitzt das Betriebssystem in einer VM Internetzugriff, sieht aber nichts vom lokalen Netzwerk. Um das zu ändern, fahren Sie das Gastsystem herunter, gehen auf „Edit virtual machine settings“ und dann auf „Network Adapter“.

Wählen Sie die Option „Bridged: Connect directly to the physical Network“. Klicken Sie auf „Save“ und starten Sie die VM. Jetzt können Sie auf Ressourcen im lokalen Netzwerk zugreifen. Beachten Sie, dass es ein theoretisches Sicherheitsrisiko darstellt, wenn Betriebssysteme wie Windows Schreibzugriff auf Netzwerklaufwerke erhalten. Erpressungs-Trojaner können auch Netzwerklaufwerke verschlüsseln. Eine weitere Möglichkeit für den Datenaustausch finden Sie in den Einstellungen unter „Shared Folders“ (Vmware-Tools erforderlich). Aktivieren Sie die Option „Always enabled“ und klicken Sie auf „Add“. Tippen Sie unter „Name“ eine Bezeichnung ein und wählen Sie über „Browse“ den gewünschten Ordner auf dem Hostsystem. Aus Gründen der Sicherheit sollten Sie ein Häkchen vor „Read-only“ setzen, vor allem wenn Windows in der virtuellen Maschine installiert ist. Erlauben Sie den Schreibzugriff nur, wenn es nötig ist. Speichern Sie die Änderungen und starten Sie das virtualisierte System. Unter Linux tauchen gemeinsame Ordner unterhalb von „/mnt/hgfs“ auf, im Windows-Explorer unter „Netzwerk -> vmware-host -> Shared Folders“ beziehungsweise dem UNC-Namen „\\vmware-host\Shared Folders“.

Die gemeinsame Zwischenablage ist beim Player standardmäßig aktiviert, sofern die Vmware-Tools installiert sind. Sie können beispielsweise im Hostsystem einen Textabschnitt mit der Maus markieren, mit Strg-C kopieren und im Gastsystem mit Strg-V einfügen. Drag & Drop funktioniert zwischen allen Betriebssystemen meist ebenfalls zuverlässig, etwa zwischen dem Dateimanager oder Desktop des Host- und Gastsystems.

6. Bios einer virtuellen Maschine konfigurieren

Zu einer virtuellen Maschine gehört auch ein emuliertes Bios, über das Sie beispielsweise die Bootreihenfolge einstellen können. Vmware Player und Workstation starten von der CD/DVD beziehungsweise einem ISO-Image, solange die Festplatte leer ist. Ist das Betriebssystem installiert, steht die Festplatte an der ersten Stelle in der Bootreihenfolge. Wenn Sie ein anderes System installieren möchten, ändern Sie die Bootreihenfolge. In das Bios-Setup gelangen Sie über die F2-Taste. Esc führt zu einem Menü, über das Sie das Bootgerät auswählen. Es ist aber nicht einfach, ins Bios von Vmware zu kommen oder mal schnell ein anderes Laufwerk zum Boot auszuwählen, da die Anzeigedauer des Bootbildschirms extrem kurz ist.

Eine Einstellung, die das ändert, gibt es in der Menüoberfläche nicht. Sie können aber einen Parameter in der Konfigurationsdatei einer virtuellen Maschine setzen. Wo diese zu finden ist, ermitteln Sie über „Edit Virtual Machine Settings -> Options -> General“ unter „Working directory“ Vmware Workstation zeigt den Pfad gut sichtbar auf der Übersichtsseite rechts unten im Feld „Configuration file“ an.

Gehen Sie mit einem Dateimanager in dieses Verzeichnis und öffnen Sie mit einem Texteditor die dort liegende VMX-Datei. Am Ende der Datei fügen Sie folgende Zeile

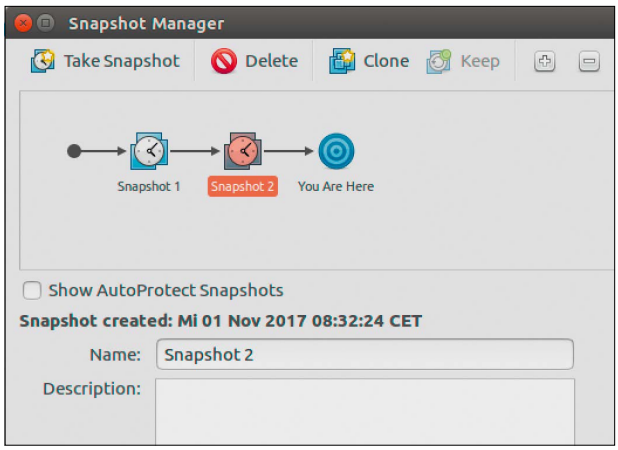
```
bios.bootdelay = "7000"
```

ein. Die Anzeigedauer des Bootbildschirms verlängert sich damit auf immerhin sieben Sekunden – genug Zeit für die Taste F2, um die Bios-Einstellungen zu ändern oder über die Esc-Taste ein anderes Bootlaufwerk auszuwählen.

7. Sicherungspunkte erstellen

Einer der Vorteile von virtuellen Maschinen ist, dass sich der aktuelle Zustand jederzeit sichern lässt. In Vmware Workstation gehen Sie im Menü auf „VM -> Snapshot -> Take Snapshot“. Geben Sie der Sicherung einen Namen und optional auch eine Beschreibung. Klicken Sie auf „OK“. Über „VM -> Snapshot -> Snapshot Manager“ lassen sich Sicherungspunkte klonen oder wiederherstellen.

In Vmware Player fehlt die Snapshotfunktion. Ein manuelles Backup ist jedoch schnell erstellt und fällt bei genügend Festplattenplatz auch kaum ins Gewicht. Fahren Sie das System in der virtuellen Maschine herunter. Gehen Sie dann im Dateimanager ins Verzeichnis einer virtuellen Maschine, das standardmäßig unter „/home/[User]/vmware“ zu finden ist. Im Unterverzeichnis mit dem Namen der VM liegen deren Festplattendateien mit der Endung „.vmdk“. Kopieren Sie die „vmdk“-Dateien in ein Backupverzeichnis. Für die Wiederherstellung kopieren Sie die gesicherten „vmdk“-Dateien beziehungsweise den kompletten Ordner zurück in das Verzeichnis der virtuellen Maschine.



Sicherungspunkte: Vmware Workstation bietet eine komfortable Snapshotverwaltung. Nutzer des Players müssen Backups manuell über den Dateimanager erstellen.

Virtuelle Festplatten verwalten

Gehen Sie bei einer virtuellen Maschine auf „Edit Virtual Machine Settings -> Hardware -> Hard Disk (SCSI)“. Unter „Disk Utilities“ gibt es einige interessante Funktionen für die virtuelle Festplatte. Per Klick auf „Mount“ lässt sich eine „vmdk“-Datei in das Dateisystem einhängen. Bestätigen Sie mit Ihrem root-Passwort und wählen Sie dann hinter „Volume:“ eine Partition aus. Bestimmen Sie hinter „Target directory:“ über „Browse“ einen Ordner, in den die Datei eingehängt werden soll. Für eine bessere Übersicht legen Sie jeweils eigene Order unterhalb von „/mnt“ an. Das lässt sich über die Schaltfläche rechts oben im Dialog „Select a directory“ erledigen. Klicken Sie auf „Öffnen“ und dann auf „Mount“. Sie können jetzt Dateien auf der virtuellen Festplatte ändern oder kopieren. Mit Klick auf „Unmount Disk“ hängen Sie die „vmdk“-Datei wieder aus. Auch diese Aktion müssen Sie als root legitimieren. Zur Optimierung einer virtuellen Festplatte klicken Sie auf „Compact disk...“. Damit geben Sie belegten, aber nicht mehr genutzten Platz frei. Danach wählen Sie „Defragment Disk...“, um die Datenstruktur neu zu organisieren.

Über „Expand Disk...“ vergrößern Sie das Volumen des virtuellen Datenträgers, wenn der Platz knapp geworden sein sollte. Vmware vergrößert dabei die Festplatte, aber nicht die Partition. Das müssen Sie selbst erledigen. Unter Windows als Gastsystem verwenden Sie die Datenträgerverwaltung, die Sie über den Befehl *diskmgmt.msc* aufrufen. Klicken Sie die Partition mit der rechten Maustaste an, wählen Sie „Volume erweitern“ und folgen Sie den Anweisungen des Assistenten. Bei einem Linux-System wie Ubuntu booten Sie die VM vom Installationsmedium und starten Gparted, weil sich die Größe der eingehängten Systempartition beim laufenden System nicht verändern lässt.

In der Regel müssen Sie zuerst die Swappartition und dann die erweiterte Partition löschen, wenn diese hinter Systempartition liegt. Dann vergrößern Sie die Linux-Partition über den Kontextmenüpunkt „Größe ändern/Verschieben“, lassen aber dahinter zwei oder vier GB frei. Legen Sie über den Kontextmenüpunkt „Neu“ wieder eine erweiterte Partition und darin eine Swappartition an.

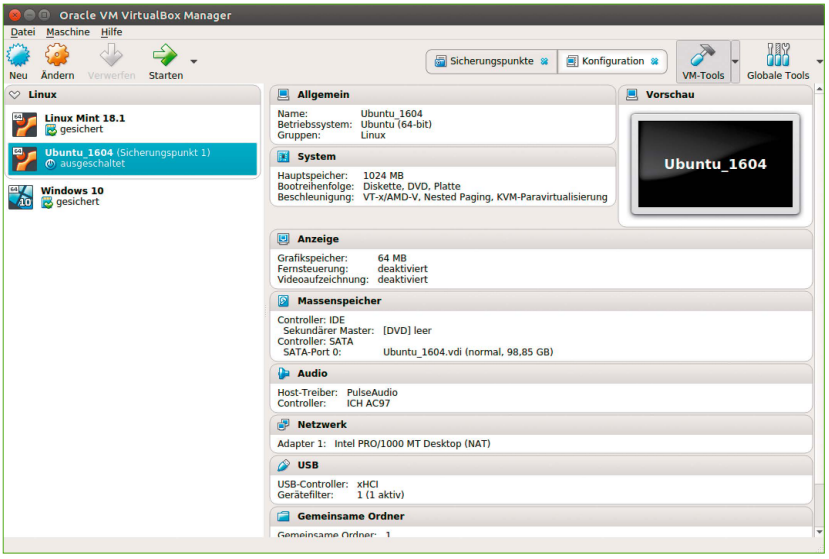
Im Vergleich: Vmware Player und Workstation Pro

Funktion	Player	Workstation Pro
Neue VMs erstellen	ja	ja
Große VMs (16 CPUs, 64 GB RAM)	ja	ja
Mehr als 200 unterstützte Gastsysteme	ja	ja
Host-Gast-Dateiaustausch	ja	ja
3D-Unterstützung (DX10 und Open GL 3.3)	ja	ja
4K-Monitore	ja	ja
USB-3.0-Unterstützung	ja	ja
Verschlüsselte VMs starten/erstellen	ja/nein	ja/ja
Mehrere VMs gleichzeitig	nein	ja
Sicherungspunkte anlegen	nein	ja
Klonfunktion	nein	ja
Uefi-Boot/Secure-Boot	ja/ja	ja/ja
VMs im Team verwenden (Workstation Server)	nein	ja

Virtualbox in der Praxis

Virtualbox ist bei Linux-Nutzern eine der beliebtesten Virtualisierungslösungen. Wie Sie die Software optimal einrichten und nutzen, erfahren Sie in diesem Artikel.

Von **Thorsten Eggeling**



Virtualbox: Die Einstellungen der virtuellen Maschinen lassen sich schnell per Klick auf eine Kategorie wie „Massenspeicher“ oder „Netzwerk“ erreichen.

Virtualbox stellt einen Zweit-PC per Software bereit. Aus Sicht des darin installierten Betriebssystems (Gastsystem) handelt es sich um einen PC mit eigener Hardware, der völlig unabhängig von der tatsächlichen im Gerät verbauten Hardware arbeitet (Hostsystem). Virtualbox ist in den Standardrepositorien der meisten Linux-Distributionen enthalten. Die Software läuft zuverlässig und bietet eine übersichtliche Oberfläche. Der Funktionsumfang deckt alle Bereiche ab, die von einer Virtualisierungssoftware für den Desktop zu erwarten sind. Der Hersteller Oracle gibt regelmäßig Aktualisierungen heraus, damit sich auch die neuesten Betriebssysteme problemlos in einer virtuellen Maschine installieren lassen.

1. Virtualbox installieren

Virtualbox lässt sich in fast allen Linux-Distributionen über das Paketmanagement installieren. Nutzer von Ubuntu, Linux Mint oder verwandten Systemen verwenden in einem Terminalfenster diese Befehlszeile:

```
sudo apt install virtualbox virtu
  albox-qt virtualbox-dkms
```

Damit installieren Sie beispielsweise unter Ubuntu 16.04 die Version 5.0.40 von Virtualbox. Aktuell war bei Redaktionsschluss die Version 5.2.8, die einige Verbesserungen enthält. Wir empfehlen daher, die neueste Version zu verwenden. Für die Installation können Sie das aktuellste Softwarepaket bei *www.virtualbox.org* herunterladen. Nach einem Klick auf „Download Virtualbox 5.2“ auf der Startseite klicken Sie unter „VirtualBox 5.2.8 platform packages“ auf „Linux distributions“.

Sie sehen dann eine Liste mit Linux-Distributionen wie Ubuntu, Debian, Open Suse und Fedora und dahinter jeweils Downloadlinks. Nutzer von Ubuntu 16.04 oder Linux Mint 18 klicken hinter „Ubuntu 16.04“ auf „i386“ (32 Bit) oder „AMD64“ (64 Bit). Die heruntergeladene deb-Datei öffnen Sie per Doppelklick im Dateimanager mit der Paketverwaltung und folgen den Anweisungen zur Installation. Wie beziehen uns in diesem Artikel vorwiegend auf die aktuelle Version 5.2. Die Unterschiede bei der Bedienung gegenüber den Vorgängern sind jedoch marginal.

Paketquelle für Ubuntu/Mint hinzufügen: Für die meisten Anwender ist es praktischer, die Downloadquelle von Virtualbox in die Paketverwaltung einzubinden. Sie erhalten dann automatisch Updates, sobald diese verfügbar sind. Bei Debian-basierenden Systemen wie Ubuntu und Linux Mint verwenden Sie dazu die folgenden zwei Befehlszeilen im Terminal:

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

Damit importieren Sie den Oracle-Schlüssel in die Liste der vertrauenswürdigen Softwareanbieter. Danach installieren Sie Virtualbox mit diesen drei Befehlszeilen:

```
sudo echo deb http://download.vir
  tualbox.org/virtualbox/debian
  xenial contrib > /etc/apt/sour
  ces.list.d/virtualbox.list
sudo apt update
sudo apt-get install dkms virtua
  lbox-5.2
```

Ersetzen Sie „xenial“ (Ubuntu 16.04/Linux Mint 18) durch den Codenamen der gewünschten Distribution.

Wenn Sie diesen nicht kennen, sehen Sie in der Datei „lsb-release“ (Ubuntu) oder „os-release“ (Debian) nach. Wenn Sie eine ältere Version von Virtualbox aus der Oracle-Paketquelle installieren wollen, ändern Sie die Versionsnummer auf „virtualbox-5.1“ oder „virtualbox-5.0“. Anschließend fügen Sie die Benutzer, der Virtualbox verwenden sollen, zur Gruppe „vboxusers“ hinzu:

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

Ersetzen Sie den Platzhalter „[User]“ durch den Kontonamen des Benutzers. Wiederholen Sie die Befehlszeile für alle gewünschten Benutzer. Melden Sie sich dann bei Linux ab und wieder an oder starten Sie das System neu.

Nach einem Kernel-Upgrade sollte DKMS (Dynamic Kernel Module Support) dafür sorgen, dass die Kernel-Module für Virtualbox automatisch neu erstellt werden. Das klappt jedoch nicht immer zuverlässig. Sollte beim Start einer VM eine Fehlermeldung auftauchen, die ein fehlendes Kernel-Modul bemängelt, führen Sie folgende Befehlszeile aus:

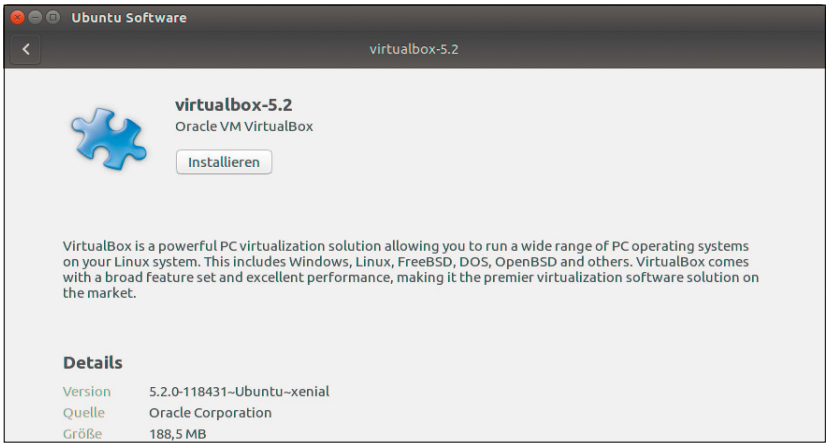
```
sudo /etc/init.d/vboxdrv setup
```

Die bei der Virtualbox-Installation erzeugten Kernel-Module sind nicht digital signiert. Sollte Ihr PC im Uefi-Modus bei aktiviertem Secure Boot starten, kann Linux die Kernel-Module nicht laden. Deaktivieren Sie deshalb – wenn vorhanden – Secure Boot im Bios/Firmwaresetup Ihres PCs oder Notebooks. Kontrollieren Sie bei der Gelegenheit ebenfalls im Bios/Uuefi auch, ob Intel-Vt-x beziehungsweise AMD-V aktiviert sind.

Bitte beachten Sie außerdem, dass eine Parallelinstallation von Virtualbox 5 neben einer älteren Version nicht möglich ist. Bei einem Upgrade bleiben jedoch Einstellungen und virtuelle Maschinen erhalten. Sie dürfen auch die Installation aus den Ubuntu-Paketquellen nicht mit der von Oracle mischen. Entfernen Sie daher mit

```
sudo apt remove virtualbox virtu
  albox-qt virtualbox-dkms
```

eine eventuell bestehende Installation, bevor Sie beispielsweise Virtualbox 5.2.8 installieren.



Aktuellere Version: Oracle bietet ein fertiges deb-Paket für Virtualbox 5.2 an, das sich über das Paketmanagement („Ubuntu Software“) installieren lässt.

2. Erweiterungspaket installieren

Das Virtualbox-Basispaket steht unter der Lizenz GNU General Public License V2, der Quellcode ist frei verfügbar.

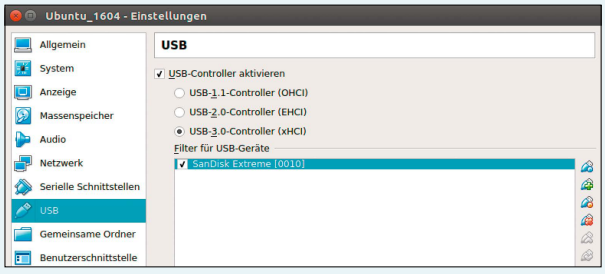
Direkter Zugriff: USB-Konfiguration anpassen

Eine virtuelle Maschine hat keinen direkten Zugriff auf die Hardware des Host-PCs. Ausnahmen sind USB-Geräte wie Drucker, Scanner oder Sticks. Diese lassen sich direkt einbinden, stehen dann aber auf dem Hostsystem nicht mehr zur Verfügung, solange das Gastsystem läuft. Die USB-Unterstützung aktivieren Sie in der Konfiguration einer virtuellen Maschine nach einem Klick auf „USB“. Setzen Sie ein Häkchen vor „USB-Controller aktivieren“. Darunter wählen Sie die gewünschte Option für USB-1.1, 2.0 oder 3.0, je nachdem, an welchen Port das USB-Gerät angeschlossen ist. Die Einstellungen wirken nur, wenn Sie das Erweiterungspaket installiert haben (siehe Punkt 2). Starten Sie den virtuellen PC, gehen Sie auf „Geräte -> USB“ und setzen Sie ein Häkchen vor ein USB-Gerät, das Sie einbinden möchten.

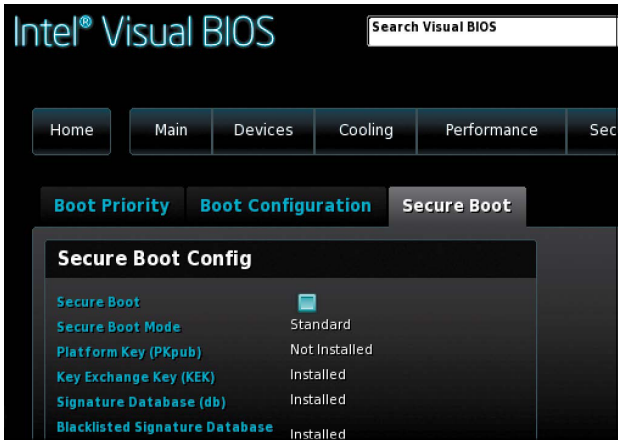
Sie wollen ein USB-Gerät automatisch einbinden? Bei den USB-Einstellungen sehen Sie den Bereich „Filter für USB-Geräte“. Über die Schaltfläche mit dem „+“-Symbol wählen Sie das gewünschte Gerät aus. Es lässt sich dann nach einem Neustart – oder sobald Sie es mit dem USB-Port verbinden – sofort in der virtuellen Maschine verwenden.

Problembehebung: Sollte sich ein USB-Gerät nicht einbinden lassen, kontrollieren Sie zuerst die Porteinstellung. Hängt es an einem USB-3.0-Port, aber USB 2.0 ist eingestellt, dann funktioniert es nicht.

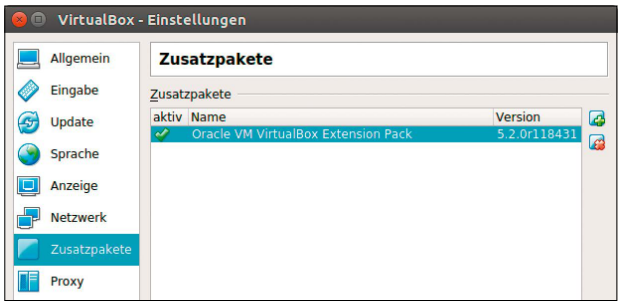
Kontrollieren Sie außerdem im Terminal mit dem Befehl *groups*, ob Sie zur Gruppe „vboxusers“ gehören. Wenn nicht, werden Sie Mitglied der Gruppe wie in Punkt 1 beschrieben.



Direktzugriff: Legen Sie Filter für USB-Geräte fest, damit Virtualbox beispielsweise ein USB-Laufwerk oder einen USB-Drucker automatisch in das Gastsystem einbindet.



Firmwareeinstellungen: Deaktivieren Sie Secure Boot im Bios des Computers. Sonst lädt Linux die neuen Kernel-Module nicht und Sie können Virtualbox nicht nutzen.



Funktionserweiterung: Über ein Zusatzpaket rüsten Sie beispielsweise die Unterstützung für USB-3.0-Geräte im Gastsystem nach.

Weitere Komponenten stellt Oracle als Erweiterungspaket unter der Personal Use and Evaluation License (PUEL) zur Verfügung. Für private Nutzer, Bildungszwecke oder Testumgebungen ist die Nutzung kostenlos. Das Erweiterungspaket enthält folgende Bestandteile:

- Unterstützung für virtuelle USB-2.0-Geräte
- Unterstützung für virtuelle USB-3.0-Geräte
- Virtualbox Remote Desktop Protocol (VRDP, Fernsteuerung)
- Unterstützung für Webcams
- Netzwerk Boot-ROM (Intel PXE)
- experimenteller Zugriff auf PCI-Geräte (PCI-Passthrough)
- AES-Festplattenverschlüsselung

In der Regel werden Sie zumindest die Unterstützung für USB-2.0- und USB-3.0-Geräte nutzen wollen, um beispielsweise einen Drucker oder Scanner direkt aus einem System in der virtuellen Maschine anzusteuern.

Den Link zum Erweiterungspaket finden Sie auf der Downloadseite *www.virtualbox.org/wiki/Downloads*. Es muss die gleiche Versionsnummer tragen wie Virtualbox. Bei Redaktionsschluss war die Datei „Oracle_VM_VirtualBox_Extension_Pack-5.2.0-118431.vbox-extpack“ aktuell. Erweiterungspakete für ältere Virtualbox-Versionen finden Sie über *www.virtualbox.org/wiki/Download_Old_Builds*, beispielsweise auch für ein Virtualbox 5.0, das Sie aus den Ubuntu-Paketquellen installiert haben.

Nach dem Download installieren Sie das Erweiterungspaket per Doppelklick im Dateimanager. Sie können auch in Virtualbox auf „Datei -> Einstellungen“ und dann auf „Zusatzpakete“ gehen. Per Klick auf das Icon mit dem „+“-Symbol wählen Sie das Erweiterungspaket zur Installation aus. Über die Schaltfläche mit dem Kreuzsymbol entfernen Sie veraltete Erweiterungspakete.

3. Linux-System in Virtualbox installieren

Wenn Sie Virtualbox starten, erhalten Sie ein Fenster, über das Sie Ihre virtuellen Maschinen verwalten und deren Konfiguration anpassen. Mit der Schaltfläche „Neu“ erstellen Sie eine virtuelle Maschine. Tippen Sie hinter „Name:“ eine aussagekräftige Bezeichnung ein. Wählen Sie hinter „Typ:“ den Eintrag „Linux“ und darunter die Version des Betriebssystems. Bei Linux sind nicht alle bekannten Distributionen aufgeführt. Nehmen Sie den Eintrag, der der gewünschten Version am nächsten kommt, etwa „Ubuntu (32-bit)“ für Xubuntu oder Lubuntu. Ist nichts Passendes dabei, entscheiden Sie sich für „Other Linux (32-bit)“ oder „Other Linux (64-bit)“. 32-Bit-Systemen sollten Sie den Vorzug geben, wenn 64 Bit nicht zwingend erforderlich sind. Der Speicherbedarf ist geringer und die Leistung dadurch besser.

Klicken Sie auf „Weiter“. Geben Sie die Hauptspeichergröße (RAM) an, die der virtuellen Maschine zur Verfügung stehen soll. Meist sind 1024 oder 2048 MB ausreichend. Es sind auch deutlich größere Werte möglich, wenn es erforderlich sein sollte. Dann muss der PC aber über ausreichend RAM verfügen, damit für das Hostsystem genügend verbleibt. Nach einem Klick auf „Weiter“ wählen Sie die Option „Festplatte erzeugen“ und klicken auf „Erzeugen“. In der Regel werden Sie die Option „VDI (VirtualBox Disk Image)“ wählen.

Das VHD-Format ist für Nutzer gedacht, die eine virtuelle Festplatte auch mit der Virtualisierungssoftware Microsoft Hyper-V verwenden möchten. VMDK ist das Standardformat bei Vmware.

Klicken Sie auf „Weiter“ und wählen Sie die gewünschte Option. Bei „dynamisch alloziert“ erstellt Virtualbox eine virtuelle Festplattendatei mit minimaler Größe. Wenn das Gastsystem Daten auf die Festplatte schreibt, wächst die Größe entsprechend an. Mit „feste Größe“ legen Sie eine Datei an, die von Anfang an eine bestimmte Kapazität besitzt. Das ist unflexibler, verbessert aber die Leistung. Nach einem Klick auf „Weiter“ legen Sie die Kapazität der virtuellen Festplatte fest.

Es empfiehlt sich, deutlich mehr Speicherplatz als vorgeschlagen zu verwenden, damit genügend Platz für Up-

dates und Softwareinstallationen bleibt. Eine virtuelle Festplatte lässt sich später nur umständlich vergrößern. Sie können aber jederzeit eine zweite Festplatte in den virtuellen PC „einbauen“.

4. Konfiguration der virtuellen Maschine anpassen

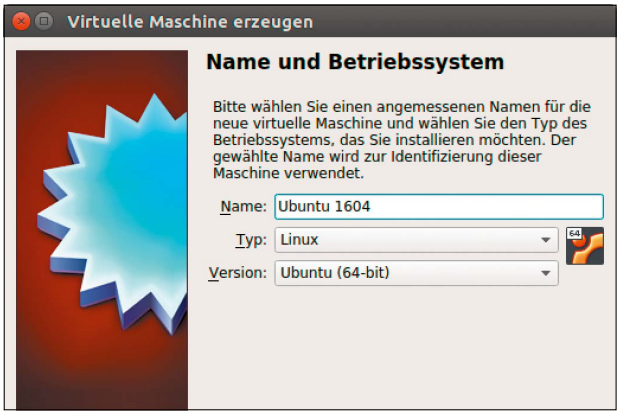
Nach Abschluss des Assistenten sehen Sie im Virtualbox-Hauptfenster eine Übersicht mit der Konfiguration. Klicken Sie auf „Anzeige“. Stellen Sie hinter „Grafikspeicher:“ mindestens „64 MB“ ein und setzen Sie das Häkchen vor „3D-Beschleunigung aktivieren“. Die Option „2D-Video-Beschleunigung aktivieren“ hat nur Auswirkung bei Windows-Gastsystemen.

Gehen Sie auf „Massenspeicher“, klicken Sie auf das CD-Icon und dann rechts im Fenster auf das CD-Icon mit dem kleinen Pfeil. Geben Sie über „Datei für optisches Medium auswählen...“ den Speicherort der ISO-Datei einer Linux-Installations-DVD an. Oder Sie wählen „Hostlaufwerk“, wenn Sie eine Installations-DVD verwenden möchten, die im DVD-Laufwerk des PCs liegt.

Unter „Netzwerk“ ist standardmäßig „NAT“ eingestellt. Der virtuelle PC erhält dann Internetzugang über das Hostsystem, aber keinen Zugang zum lokalen Netzwerk. Das kann aus Sicherheitsgründen erwünscht sein. Wenn Sie auf Freigaben im lokalen Netz zugreifen wollen, stellen Sie hinter „Angeschlossen an: “ den Wert „Netzwerkbrücke“ ein. In einer virtuellen Maschine können Sie dann über den Linux-Dateimanager oder den Windows-Explorer wie gewohnt auf Netzwerkfreigaben zugreifen.

Beenden Sie die Konfiguration per Klick auf „OK“. Klicken Sie auf „Starten“. Der virtuelle PC bootet vom Installationsmedium. Danach führen Sie die Linux Installation wie gewohnt durch.

Tipp: Einen in der virtuellen Maschine „gefangenen“ Mauszeiger befreien Sie über die „Host-Taste“. Das ist standardmäßig die rechte Strg-Taste.



Neues Gastsystem: Geben Sie Typ und Version des Gastbetriebssystems an. Virtualbox setzt dann automatisch die passenden Einstellungen.



Virtuelle Festplatte: Dynamische Festplatten belegen anfänglich nur wenig Platz, sind aber langsamer als virtuelle Laufwerke mit fester Größe.

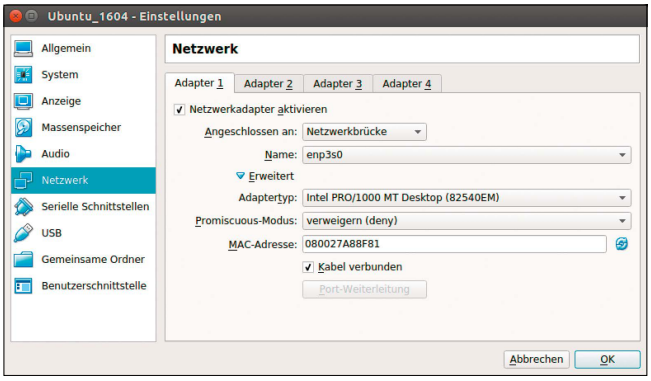
5. Windows in Virtualbox installieren

Die Installation eines Windows-Gastsystems läuft ab wie bei Linux. Nach

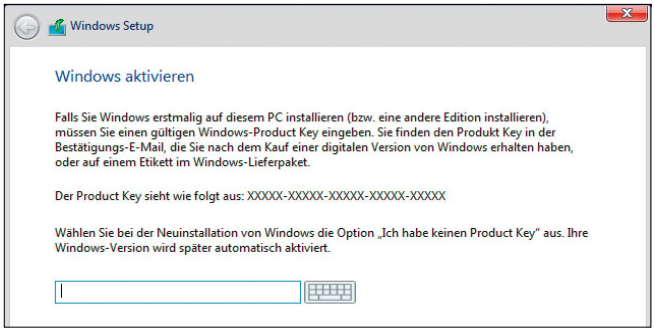
Sicherungspunkte, Klons und Appliances

Virtuelle Maschinen verhalten sich ähnlich wie richtige PCs. Sie müssen das Gastsystem beispielsweise nicht herunterfahren, Sie können es auch das Fenster schließen und dann die Option „den Zustand der virtuellen Maschine speichern“ wählen. Das entspricht in etwa dem Standby-Modus. Virtualbox stellt aber auch Funktionen zur Verfügung, die Sie bei einem herkömmlich installierten System vergebens suchen. Per Klick auf „Maschine -> Sicherungspunkt erstellen“ legen Sie einen Schnappschuss des aktuellen Zustands an.

Sie können beliebig viele Sicherungspunkte erstellen, die allerdings reichlich Platz auf der Festplatte belegen. Im Virtualbox-Hauptfenster lassen Sie sich die Backups über die Schaltfläche „VM-Tools -> Sicherungspunkte“ anzeigen. Wählen Sie den gewünschten Sicherungspunkt aus und klicken Sie auf „Wiederherstellen“. Belassen Sie das Häkchen vor „Sicherungspunkt des aktuellen VM-Zustands erstellen“, damit Virtualbox den aktuellen Systemzustand sichert. Sie benötigen für Tests eine exakte Kopie einer virtuellen Maschine? Dann gehen Sie auf „Maschine -> Klonen“. Für ein komplettes Backup von virtuellen Maschinen müssen Sie nur die zugehörigen Ordner sichern, die standardmäßig unter „/home/[User]/VirtualBox Vms“ liegen. Eine andere Methode lässt sich über „Datei -> Appliance exportieren“ aufrufen. Folgen Sie einfach den Anweisungen des Assistenten. Damit erstellen Sie eine „ova“-Datei, die Sie bei Bedarf über „Datei -> Appliance importieren“ einlesen. Das funktioniert auch auf einem anderen PC, der unter Linux oder Windows laufen kann.



Netzwerkeinstellungen: Wählen Sie die Option „Netzwerkbrücke“, um im Gastsystem nicht nur Internetzugang, sondern auch den Zugriff auf das lokale Netzwerk zu erreichen.



Windows aktivieren: Wenn Sie das System nur kurze Zeit ausprobieren wollen, benötigen Sie keinen Produktschlüssel bei der Windows-Installation.

Klick auf die Schaltfläche „Neu“ vergeben Sie eine Bezeichnung, stellen hinter „Typ“ als System „Windows“ ein und hinter „Version“ das gewünschte System, etwa „Windows 10“. Auch bei Windows gilt: Ein 32-Bit-System läuft etwas flotter in einer virtuellen Maschine, was auch auf ältere Systeme wie Windows 7 zutrifft. Für Windows 10 mit 64 Bit schlägt Virtualbox 2048 MB Hauptspeicher vor und eine virtuelle Festplatte mit 32 GB. Es darf bei beidem gerne etwas mehr sein, wenn der Host-PC mit mehr als vier GB RAM und einer Festplatte mit ausreichend Kapazität ausgestattet ist. Nach Abschluss des Konfigurationsassistenten passen Sie die Einstellungen an wie im vorherigen Punkt beschrieben.

Für Windows benötigen Sie die Installations-DVD der gewünschten Version oder eine ISO-Datei davon. Für Testzwecke genügt Windows 10 Enterprise, das Sie nach einer kostenlosen Registrierung über *www.microsoft.com/de-de/evalcenter/evaluate-windows-10-enterprise* herunterladen können. Eine ISO-Datei der aktuellen Windows-10-Version (Home und Pro) erhalten Sie über *www.pcwelt.de/win10iso*. Wenn Sie die Webseite unter Linux aufrufen, erkennt Microsoft, dass Sie kein unterstütztes Betriebssystem besitzen, und bietet Ihnen den direkten Download der ISO-Datei an. Klicken Sie auf „Editionsauswahl“, dann auf „Windows 10“ und auf „Bestätigen“. Danach wählen Sie die Produktsprache und nach einem Klick auf „Bestätigen“ sehen Sie Downloadlinks für die 32- und 64-Bit-Version.

Die heruntergeladene ISO-Datei binden Sie ein wie in Punkt 3 für Linux beschrieben. Klicken Sie auf „Starten“ und führen Sie die Windows-Installation wie gewohnt durch. Wenn Sie Windows 10 Home oder Pro dauerhaft nutzen wollen, benötigen Sie einen Produktschlüssel. Das gilt auch für den Betrieb in einer virtuellen Maschine. Für die Installation ist kein Produktschlüssel erforderlich. Klicken Sie einfach auf „Ich habe keinen Product Key“, wenn das Setupprogramm Sie danach fragt. Es gibt dann jedoch einige Einschränkungen. Sie können beispielsweise in den „Einstellungen“ (Win-I) unter „Personalisierung“ keine Änderungen vornehmen.

6. Gasterweiterungen installieren

Die Leistung eines virtuellen PCs lässt sich über die Gasterweiterungen verbessern, die Treiber etwa für die Maus und den virtuellen Grafikadapter enthalten. Bei einigen Linux-Systemen sind die Virtualbox-Gasterweiterungen bereits standardmäßig installiert. Wenn Sie beispielsweise unter Ubuntu 16.04 Virtualbox 5.0.40 aus den Standard-Paketquellen eingerichtet haben, müssen Sie weiter nichts unternehmen. Haben Sie hingegen das aktuelle Virtualbox 5.2 installiert, richten Sie für die optimale Leistung auch die dazu passenden Gasterweiterungen ein.

Bringen Sie zuerst das Gastsystem auf den aktuellen Stand:

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get install dkms
```

Mit der letzten Zeile installieren Sie – wenn noch nicht vorhanden – das Paket für die dynamische Erstellung von Kernel-Modulen. Starten Sie das Gastsystem neu. Gehen Sie im Fenster der laufenden virtuellen Maschine auf „Geräte -> Gasterweiterungen einlegen“. Bei Ubuntu 16.04 oder Linux Mint erscheint dann ein Fenster, in dem Sie auf „Ausführen“ klicken und mit dem root-Passwort bestätigen. Ein Script erstellt die nötigen Kernel-Module automatisch. Sollte das Script nicht automatisch starten, führen Sie im Terminalfenster die folgenden zwei Befehle aus:

```
cd /media/[User]/Vbox_Gas_5.2.0
sudo ./VBoxLinuxAdditions.run
```

Passen Sie die Pfadangaben für Ihr System beziehungsweise die Version der Gasterweiterungen an. Wo die ISO-Datei mit den Gasterweiterungen eingehängt ist, sehen Sie im Dateimanager. Kommt Windows als Gastbetriebssystem zum Einsatz, starten Sie „VBoxWindowsAdditions.exe“ vom Medium mit den Gasterweiterungen und folgen den Anweisungen des Assistenten. Nach einem Neustart des Gastsystems stehen jetzt noch zusätzliche Funktionen zur Verfügung. Sie können beispielsweise eine höhere

Bildschirmauflösung wählen und der Mauszeiger löst sich automatisch, wenn Sie ihn aus dem Fenster ziehen. Außerdem lässt sich das Gastsystem über Host-L (rechte Strg-Taste zusammen mit der L-Taste) in den „nahtlosen Modus“ und wieder zurück in den Fenstermodus schalten. Dann sind nur die im Gastsystem geöffneten Fenster auf dem Linux-Desktop zu sehen. Die Windows-Taskleiste blendet Virtualbox dann am unteren Bildschirmrand ein.

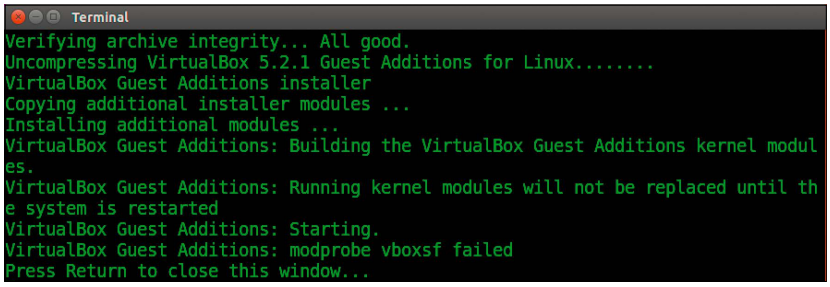
Probleme bei der Installation: Die Gasterweiterungen der Version 5.2.0 ließen sich bei Redaktionsschluss im November 2017 unter Ubuntu 16.04 (Kernel 4.10.0-28) nicht kompilieren. Wahrscheinlich sind auch andere Distributionen mit neueren Kerneln betroffen. Auf der Seite *www.virtualbox.org/wiki/Downloads* bietet Oracle ein aktuelleres ISO mit der Versionsnummer 5.2.1-118447 an, das bei unseren Tests mit Ubuntu 16.04 keine Probleme zeigte. Für die Kernel-Version 4.14 gibt es einen eigenen Download mit der Versionsnummer 5.2.1-118452. Die Situation kann sich aber geändert haben, wenn Sie dieses Heft in den Händen halten.

Probieren Sie daher zuerst die Installation aus wie oben beschrieben. Sollte dabei ein Fehler wie „Look at /var/log/vboxadd-setup.log to find out what went wrong“ erscheinen, binden Sie die neueren Gasterweiterungen „VboxGuestAdditions_5.2.1-118447.iso“ über den Punkt „Geräte -> Optische Laufwerke -> Abbild auswählen“ in die virtuelle Maschine ein und installieren diese dann.

Die Fehlermeldung „modprobe vboxsf failed“ ist immer zu sehen, weil sich das Modul nicht laden lässt, solange sich die ältere Version des Moduls „vboxguest“ noch im Speicher befindet. Starten Sie das Gastsystem neu und ermitteln Sie die geladenen Module mittles des Befehls

```
lsmod | grep vbox
```

In der Ausgabe tauchen „vboxsf“, „vboxvideo“ und „vboxguest“ auf, wenn alles korrekt installiert ist.



Optimale Leistung: Bei der Installation der Gasterweiterungen werden neue Kernel-Module erzeugt. Ein Fehler darf nur bei „vboxsf“ auftreten.



Datenaustausch: Binden Sie über „Gemeinsame Ordner“ einen Ordner des Hostsystems ein. Dateien lassen sich dann in beide Richtungen kopieren.

7. Datenaustausch zwischen Host und Gast

Eine virtuelle Maschine ist in der Standardkonfiguration vom Hostsystem weitestgehend abgekoppelt. Über das Netzwerk haben Sie Zugriff auf Freigaben, wenn Sie den virtuellen Netzwerkadapter als „Netzwerkbrücke“ konfiguriert gaben (siehe Punkt 4). Zur Datenübertragung zwischen Host- und Gastsystem können Sie auch einen gemeinsamen Ordner verwenden. Voraussetzung dafür sind die im Gastsystem installierten Gasterweiterungen (-> Punkt 6). Gehen Sie im Fenster der virtuellen Maschine auf „Geräte -> Gemeinsame Ordner -> Gemeinsame Ordner“. Über die „+“-Schaltfläche bestimmen Sie einen Ordner für den Datenaustausch auf dem Hostsystem. Setzen Sie Häkchen vor „Automatisch einbinden“ und „Permanent erzeugen“. Damit ein Nutzer im Gastsystem den gemeinsamen Ordner nutzen kann, fügen Sie ihn beispielsweise unter Ubuntu mit folgender Befehlszeile zur Gruppe „vboxsf“ hinzu:

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

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

Drag & Drop funktioniert bei Dateien beispielsweise zwischen dem Dateimanager des Hostsystems und dem Desktop des Gastsystems. Die Funktion ist jedoch noch nicht ausgereift. Bei manchen Systemen ist Drag & Drop wenigstens in eine Richtung möglich, bei anderen gar nicht. Aber vielleicht ist auch das mit dem nächsten Virtualbox-Update behoben. ●

Shredder: Alle Benutzerdaten löschen

In diesem ersten Artikel unseres zeigen wir Ihnen, wie Sie Benutzerordner während der Anmeldung am System sicher löschen. Dazu genügen ein paar wenige Grundlagen der Script-Programmierung, die wir hier vermitteln.

Von **Stephan Lamprecht**



Quelle: Eisenhans - Fotolia.com

Wer sich in Deutschland mit dem Thema Datenverschlüsselung oder sicheres Löschen von Dokumenten beschäftigt, setzt sich schnell einem Generalverdacht aus. Nun muss man aber nicht Terrorist sein oder Illegales im Schilde führen, um verhindern zu wollen, dass die persönlichen Daten in fremde Hände geraten. Dieser Beitrag zeigt, wie Sie das Benutzerverzeichnis eines Linux-Systems per Script sicher löschen. Die Grundelemente können Sie problemlos mit anderen Scripts kombinieren. Auf dem Raspberry könnten Sie das Script beispielsweise mit einem anderen Programmaufruf kombinieren, der ausgeführt wird, wenn ein am Raspberry angeschlossener Knopf gedrückt wird. Alle Bestandteile des Scripts funktionieren auch mit anderen Linux-Systemen.

Die Grundbestandteile

Das System würde aus dem Tritt geraten, wenn Sie versuchten, während oder nach der Anmeldung das eigene Benutzerverzeichnis zu löschen. Deswegen legen Sie einen anderen Nutzer an, der dann auf Ihr Home-Verzeichnis zugreifen darf, weil Sie ihm root-Rechte einräumen. Das können Sie direkt in einem Terminal erledigen, ohne das aktuelle Benutzerkonto zu verlassen:

```
sudo adduser testbenutzer
sudo adduser testbenutzer sudo
```

Nach der Ausführung des ersten Kommandos werden Sie zusätzliche Informationen zu diesem Benutzer anlegen müssen. Dazu gehören dessen vollständiger Name sowie das Passwort, mit dem er sich später am System anmelden kann. Der zweite Funktionsaufruf sorgt dann dafür, dass dieser Nutzer auch Systemkommandos ausführen darf. Installieren Sie jetzt zusätzlich ein Softwarepaket, das für das sichere Löschen von Dateien genutzt wird. Das erledigen Sie am einfachsten mit diesem Befehl im Terminal:

```
sudo apt-get install secure-delete
```

Bleiben Sie ruhig weiterhin mit Ihrem aktuellen Benutzer eingeloggt. Es geht jetzt darum, den Kern des Notfallsystems zu entwickeln.

Script für das Löschen von Dateien: Um ein Shell-Script zu schreiben, benötigen Sie einen Texteditor. Auf dem Raspberry bietet sich Nano an. Dem Programmaufruf übergeben Sie dann den gewünschten Dateinamen. Es ist üblich, ein Shell-Script mit der Endung „sh“ zu kennzeichnen. Um das Script in einem Systemordner ablegen zu können, müssen Sie root-Rechte besitzen:

```
sudo nano /etc/security/notfall.sh
```

Damit wird die Datei „notfall.sh“ angelegt und Sie befinden sich bereits im Editiermodus. Jetzt fügen Sie eine wichtige Zeile ein, die stets Bestandteil von Script-Dateien ist und dazu führt, dass Linux den Inhalt ausführt:

```
#!/bin/bash
```

Zukünftig soll der Nutzer am System über zwei Passwörter verfügen. Zum einen das Passwort, mit dem er sich am System anmeldet. Zum anderen besitzt er ein Notfallkennwort. Gibt er das ein, so wird das Benutzerverzeichnis unwiderruflich und zuverlässig geleert.

```
read password
if [ "$PAM_USER" = "name"] &&
  ["$password" = "notfallpass
  wort"]
then
   srm -rvvv /home/name
   sfill /home/
```

```
fi
exit 0
```

Wenn Sie eine Bedingung überprüfen wollen, benötigen Sie in einem Script das Kommando „if“. Trifft die Bedingung zu, dann werden ein oder mehrere Kommandos ausgeführt. Unsere Konstruktion besteht aus drei Schlüsselwörtern. Nach der Prüfung erfolgt die Ausführung mehrerer Befehle, die hinter der Einleitung „then“ stehen. Das Wort „fi“ schließt den Block, damit das System weiß, dass an dieser Stelle nichts mehr folgt. Ausgeführt werden sollen zwei Befehle aus den Tools für das sichere Löschen. Mit „srm“ wird das angegebene Verzeichnis sicher entfernt. Der zweite Befehl „sfill“ überschreibt den leeren Platz.

Das Script an das System anpassen

Nun wird es Zeit, den Rohbau mit Leben zu füllen. Dazu passen Sie die Variablen an die aktuellen Gegebenheiten des Systems an. Notieren Sie also in der zweiten Zeile statt „name“ den Benutzernamen, um den es geht. Also den Testbenutzer, den Sie vorhin angelegt haben. Statt „notfallpasswort“ tragen Sie das später verwendete Kennwort für das Löschen ein (nicht das Anmeldepasswort des Nutzers!). Schließlich passen Sie noch die Pfadangabe in der Zeile „srm“ an. Ändern Sie den Namen auf den Benutzernamen, dessen Verzeichnis gelöscht werden soll.

Achtung: Bevor Sie das Script testen, sollten alle wichtigen Daten gesichert sein! Damit Linux in der Script-Datei mehr sieht als reinen Text, muss sie noch ausführbar gemacht werden:

```
sudo chmod a+x notfall.sh
```

Damit sind die Grundlagen geschaffen. Nun müssen Sie es noch schaffen, dass das Script während des Anmeldeprozesses ausgeführt werden kann. Dazu ist eine Ergänzung an einer Systemdatei notwendig. Editieren Sie diese entsprechend vorsichtig! Dazu öffnen Sie jetzt mit root-Recht und dem Editor Nano diese Datei:

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

Suchen Sie darin die Zeile, die mit „auth [success=1]““ beginnt. Ändern Sie den Wert auf „2“. Fügen Sie unmittelbar darunter diese Zeile ein:

```
auth optional pam_exec.so expose_
  authtok /etc/security/notfall.sh
```

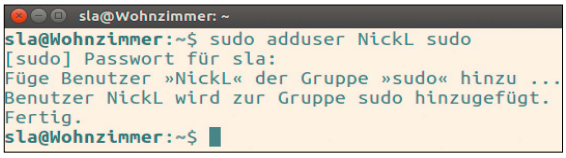
Nach dem Speichern (Strg-O) können Sie das Script erstmals testen. Nutzen Sie also den neuen Nutzer und geben Sie das Kennwort für den Notfall ein. Das System scheint während der Anmeldeprozedur zu hängen. Das hat aber damit zu tun, dass jetzt im Hintergrund die Sicherheitstools bereits die Arbeit leisten und den im Script definierten Ordner vollständig und sicher löschen.

Vielseitig einsetzbar – auch als Falle

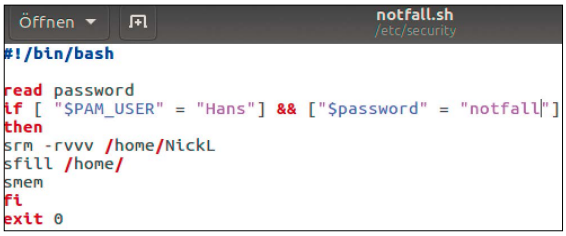
Mit dem kleinen Script haben Sie die Grundlagen für einen universellen Löschknopf geschaffen. Natürlich können Sie den Ablauf so erweitern, dass Sie mehrere Benutzerverzeichnisse löschen.

Anmerkung zum Raspberry: Auf dem Raspberry ließe sich das Script auch mittels eines Hardwareschalters ausführen. Dieser Panikknopf startet dann das Kommando. In diesem Fall brauchen Sie als Kernfunktionalität lediglich die Zeilen zwischen „then“ und „fi“. Die Herausforderung liegt hier eher daran, einen Schalter zu finden, um diesen mit den GPIO-Pins korrekt zu verbinden. Hinweise dazu, beispielsweise auch für die Wahl des optimalen Widerstands, finden Sie in den diversen Foren der Raspberry-Community.

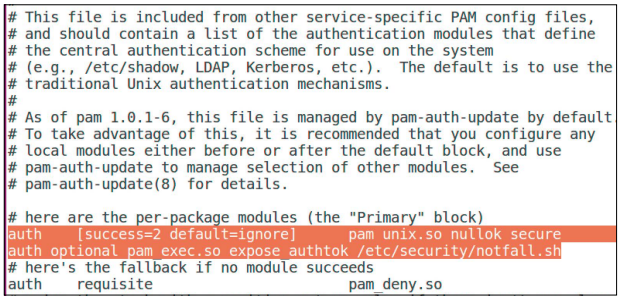
Anmerkung für Fallensteller: Legen Sie ein Benutzerkonto an, dem Sie das Script zuweisen, und arbeiten Sie auf dem System lediglich mit anderen Usern, die das Script nicht ausführen können. Im „Panikfall“ loggen Sie sich rasch mit dem besonderen Notfallnutzer ein. Falls Sie das Script auf einem Notebook einsetzen, könnten Sie einen Dieb sogar in die Irre führen, in dem Sie auf dem Gerät die Log-in-Daten notieren. Die Wahrscheinlichkeit ist ja hoch, dass der unbefugte Dritte auf diese verlockende Falle anspringt und sich als dieser Benutzer anmelden wird. Damit hat er aber keinen Zugriff mehr auf persönliche Dokumente. Einer der großen Vorteile der Shell-Scripts liegt darin, dass sie universell nutzbar sind. Sie arbeiten überall, wo eine Bash-Shell installiert ist – egal ob Sie Ubuntu, Linux Mint oder Open Suse einsetzen. ●



Legen Sie zunächst einen neuen Benutzer an mit der Befugnis, auch als Systemverwalter Aufgaben erledigen zu können.



Das eigentliche Script zum Löschen eines Benutzerordners ist einfach aufgebaut und kann später nach Belieben erweitert werden.



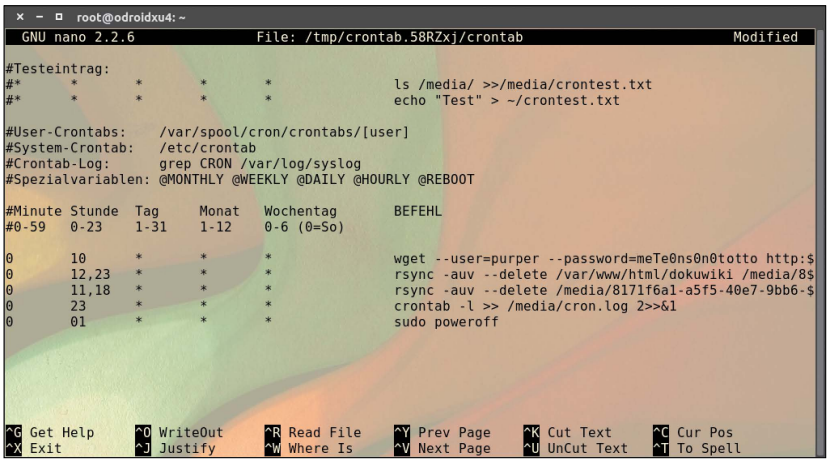
Damit während des Startvorgangs das Notfall-Script ausgeführt werden kann, muss diese Datei mit root-Recht bearbeitet werden.

Cronjobs ausgereizt

Zeitgesteuerte Aktionen via Cron-Daemon sind eine Domäne für Server im Dauerbetrieb, aber auch am Desktop ein nützlicher Service. Dabei bietet die sperrige Crontab Spielraum und Optionen, die längst nicht jedem Linux-User geläufig sind.

Von **Hermann Apfelböck**

Die Crontab ist bei Linux-Einsteigern ähnlich unbeliebt wie die fstab. Dabei muss man das simple und flexible Format der Datei nur einmal verstanden haben, um es danach den grafischen Crontab-Übersetzern wie gnome-schedule (für aktuelle Ubuntu-Systeme derzeit nicht verfügbar) oder kde-config-cron klar vorzuziehen. Dabei hilft es schon, die Crontab-Textdatei sauber zu formatieren und ein wenig übersichtlicher zu kommentieren, als es der Standard vorsieht.



Persönlich kommentierte und sauber mit Tabstopps formatierte Crontab: Die an sich unfreundliche Konfigurationsdatei wird damit sofort zugänglicher.

Cron-Standards und das Zeitformat

Standardmäßig kann jedes Benutzerkonto auf einem Linux-System eine Crontab mit eigenen Cronjobs einrichten. Wo dies nicht erlaubt sein soll, müssen unter „/etc/cron.d/cron.deny and /etc/cron.d/cron.allow“ explizite Blacklists oder Whitelists angelegt werden. Alle Cronjobs werden auch dann ausgeführt, wenn der dem Cronjob zugehörige User aktuell **nicht angemeldet ist**. Anderslautende Aussagen sind falsch und haben stets die einfache Ursache, dass der Userjob fehlerhaft ist und nicht die nötigen Rechte besitzt, um seine Aufgabe zu erledigen. In der Folge fällt der Cronjob einfach stumm unter den Tisch. Die Benutzer-Crontab kann mit *crontab -l* eingesehen („l“ für „list“) und mit

```
crontab -e
```

erstellt oder geändert werden („e“ für „edit“). Der Editor arbeitet dabei mit einer temporären Datei, die eigentliche Datei wird unter „/var/spool/cron/crontabs“ mit dem Namen des Benutzerkontos gespeichert. Änderungen an einer Crontab sind sofort nach dem Speichern gültig.

Wer den oben angesprochenen Rechteproblemen aus dem Weg gehen will, kann mit dem Befehl

```
sudo crontab -e
```

Cronjobs für das uneingeschränkte root-Konto anlegen.

Neben den Benutzer-Crontabs gibt es auch noch die systemweite „/etc/crontab“. Diese kann mit jedem Editor, jedoch nur mit root-Recht bearbeitet werden. Inhaltlich unterscheidet sich „/etc/crontab“ nur dadurch von den Benutzer-Crontabs, dass in einer zusätzlichen sechsten Spalte ein Benutzerkonto anzugeben ist. Im Resultat ist es unerheblich, ob ein angemeldeter Benutzer mit *crontab -e* seine persönliche Tabelle editiert oder sich mit root-Recht (sofern sudo-berechtigt) und seinem Kontonamen in die systemweite Tabelle einträgt. Der weitere Beitrag lässt daher die systemweite „/etc/crontab“ außen vor.

Um zu kontrollieren, welche Cronjobs gestartet werden, hilft ein Blick in das syslog-Protokoll:

```
grep CRON /var/log/syslog
```

Grep filtert hier gleich die gesuchten Cron-Einträge. Wer genau wissen muss, was die stummen Cronjobs im Detail abarbeiten, kann den Standardoutput protokollieren – dazu unten gleich mehr.

Das Format: Jeder Cronjob hat genau eine Zeile in der Crontab. Die ersten fünf Spalten dienen der Zeitangabe, alles Nachfolgende interpretiert der Cron-Dienst als den auszuführenden Befehl. In der schon angesprochenen System-Crontab gibt es als sechste Spalte eine zusätzliche Kontoangabe und erst ab Spalte 7 folgt der Befehl. Es empfiehlt sich für optimale Lesbarkeit, die Spalten statt mit Leerzeichen (auch erlaubt) mit Tabulatoren abzugrenzen. Die abschließenden Befehle dürfen durchaus komplex ausfallen, jedoch ist für aufwendigere Jobs ein knapper Script-Aufruf übersichtlicher und au-

ßerdem das Script Cron-unabhängig zu debuggen.

Die Tabelle rechts unten zeigt das generelle Format sowie einige Beispiele. Sämtliche Zeitangaben sind entweder positive Integerzahlen oder der Stellvertreter „*“, der für das jeweilige Zeitelement keine Regel vorsieht: Ein Stern für „Tag“ bedeutet daher „an jedem Tag“. Das kleinste mögliche Cron-Intervall ist minütlich und hat dann folglich diese Zeitangabe:

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

Sinnvoll sind Minutenjobs eher selten, aber sie eignen sich gut zum Testen von Cronjobs hinsichtlich Rechten und Ergebnis. Ein stündlicher Job benötigt eine Vergabe der exakten Minute – etwa Minute „0“:

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

Dieser Job würde jeweils zur Minute „0“, also immer zur vollen Stunde laufen, während

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

nur noch genau einmal am Tag, nämlich um 10:00 startet.

Zeitangaben und Befehle genauer erklärt

Die Beispiele in der Tabelle rechts unten zeigen, dass die Crontab noch weitere Differenzierungen erlaubt. Jede der fünf Zeitangaben kann auch mehrere durch Komma getrennte Werte enthalten (Leerzeichen sind unbedingt zu vermeiden!).

Eine Angabe für die Stunde wie „08,14,20“ startet die Aufgabe folglich dreimal am Tag um 8:00, 14:00 und 20:00 Uhr. Eine weitere Variante ist die Bereichsangabe „09-18“, was folglich für die Stundenspalte eine stündliche Ausführung zwischen 9:00 und 18:00 bedeutet.

Das gleiche Beispiel der Tabelle schränkt mit der weiteren Bereichsangabe „1-5“ beim Wochentag den Job auf die Tage Montag bis Freitag ein. Nicht ganz logisch und erklärungsbedürftig sind Angaben wie „*/4“. Für das Stundenfeld bedeutet das keineswegs „jede Viertelstunde“, sondern vielmehr jede vierte Stunde. Die unteren Beispiele der Tabelle zeigen noch weitere Möglichkeiten: So wird ein rsync-Job einschließlich eventuellem Erroroutput in eine Logdatei protokolliert, um die stumme Aktion bei Bedarf kontrollieren zu können. Das nachfolgende Kommando zeigt, dass die Crontab auch mehrere durch „&&“ verkettete Befehle akzeptiert. Die Tasks werden asynchron abgearbeitet: Der zweite startet erst, wenn der erste erledigt ist. Das dort verwendete „sudo poweroff“ ist nur im root-Kontext sinnvoll, jedoch ist vorangestelltes „sudo“ notwendig, obwohl das Kennwort im root-Kontext nicht abgefragt wird.

Schließlich gibt es auch die Option, grafische Programme per Cron zu starten, wobei aber eine „Display:0“-Angabe vorangehen muss. Sinnvolle Szenarien für zeitgesteuerte Starts grafischer Programme sind allerdings rar. Unsere Beispiele verzichten aus Gründen der Übersichtlichkeit auf eine weitere Option, die nur bei Darstellung einer kompletten Crontab nachvollziehbar wird und sich auch in umfangreiche Tabellen lohnt: Die Datei kann Variablen verwenden: Wird etwa eine Variable vor den eigentlichen Cron-Zeilen mit

```
SCRIPTS=/home/ha/scripts/
```

definiert, dann lässt sich die Variable „$SCRIPTS“ beliebig in die Cron-Befehle einbauen. Eine weitere Abkürzung bietet die Variable „PATH“:

```
PATH=/bin:/sbin:/usr/bin:/usr/
  sbin:/home/ha/scripts
```

Dies erspart die Angabe der vollen Pfadnamen für Scripts und Programme, die in den angegebenen Verzeichnissen liegen.

Abkürzende Variablen

Das Leiden der User an der Crontab hat die Entwickler zu einigen Abkürzungen bewogen, welche die üblichen fünf Felder durch eine einzige Angabe ersetzen. Wirklich notwendig sind diese Vereinfachungen nicht:

@yearly (und identisch @annually) entspricht der Angabe 0 0 1 1 * und startet jährlich an Neujahr um 0:00 Uhr.

@monthly entspricht der Angabe 0 0 1 * * und startet am ersten Tag jeden Monats, unabhängig vom Wochentag.

@weekly entspricht 0 0 * * 0 und startet in jedem Monat und an jedem Tag, sofern es ein Sonntag ist (Tag „0“) – im Resultat jeden Sonntag.

@daily (und identisch @midnight) entspricht 0 0 * * * und startet täglich um Mitternacht.

@hourly entspricht 0 * * * * und läuft stündlich.

@reboot startet nach jedem Neustart des Systems und ist somit Cron-untypisch zeitunabhängig.

Crontab: Generelles Format und Beispiele

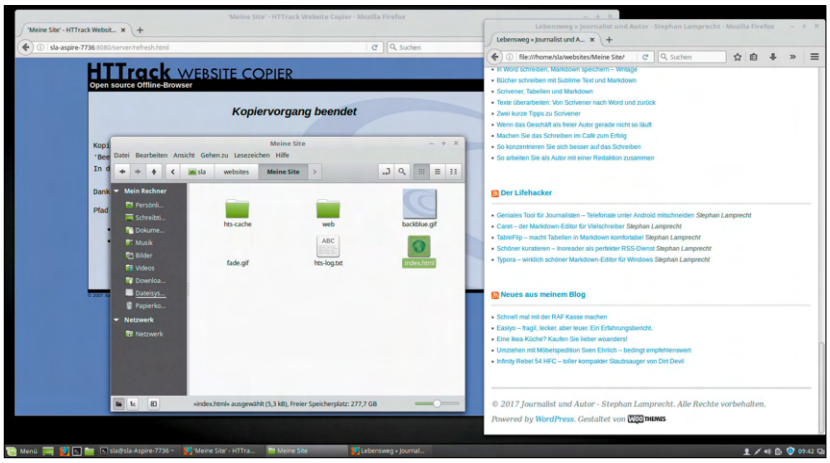
Minute	Stunde	Tag	Monat	Tag*	Kommando
0–59	0–23	1–31	1–12	0–6	Script | Programm
Crontab: Konkrete Beispiele					
*	*	*	*	*	echo "Minutentest" > ~/test.txt
0	10	*	*	*	rsync -auv --delete /var/www/html/dokuwiki /media/backups/dokuwiki
0	08,14,20	*	*	*	wget --user=ha --password=G3H3IM http://server.de/dl/my.php
0	09-18	*	*	*	wget --user=ha --password=G3H3IM http://server.de/dl/my.php
0	*/4	*	*	*	df -h | grep /dev/sd >> ~/disk.txt
0	10	*/3	*	*	ntpdate ntp.ubuntu.com
0	09-18	*	*	1-5	rsync -auv /media/data /media/backup >/media/cron.log 2>&1
0	01	*	*	*	sh ~/mirror.sh && sudo poweroff
0	9	*	*	*	DISPLAY=:0 LANG=de_DE.UTF-8 firefox

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

Websites einfach klonen

Sie benötigen eine funktionsfähige Kopie einer Webseite, um damit etwa auch ohne Internetverbindung zu arbeiten? Oder eine Vorlage für die eigene Site? Mit den richtigen Linux-Tools ist das kein großes Problem.

Von **Stephan Lamprecht**



Um den Jahrtausendwechsel erreichten Apps, mit denen sich Webseiten für die lokale Nutzung speichern lassen, den Gipfel ihrer Popularität. Das Internet, namentlich das World Wide Web, faszinierte immer mehr Menschen, aber von schnellen Anschlüssen, wie sie heute viele Nutzer gewohnt sind, war man weit entfernt. So boten einige Entwickler sogar kommerzielle Lösungen für dieses Einsatzgebiet an. Inzwischen haben sich die meisten Anwender daran gewöhnt, im Zweifel schnell noch einmal online zu gehen, um eine Information zu beschaffen. Doch noch gibt es nicht überall schnelles Internet und wer beispielsweise unterwegs in der Bahn mit einer Kopie einer Site arbeiten will, kann zu verschiedenen Lösungen greifen.

Httrack: Klonen auf die komfortable Art

Bei diesem Downloadprogramm handelt es sich eigentlich um einen Dienst für die Konsole. Aber da die Operation mit Parametern und Schaltern im Terminal nicht von jedem Anwender geschätzt wird, gibt es eine passende HTML-basierte Oberfläche, die den Namen Webhttrack trägt. Die Anwendung steht für alle populären Distributionen in Form von binären Paketen zur Verfügung. Unter Ubuntu oder Linux Mint öffnen Sie ein Terminal und installieren die Software mit diesem Befehl:

```
sudo apt-get install httrack
  webhttrack
```

Die Anwendung starten Sie danach entweder über einen Eintrag im Startmenü oder ebenfalls im Terminal mittels *webhttrack*. Damit wird ein lokaler Webserver aufgerufen sowie im Browser ein Assistent gestartet, der durch die nächsten Schritte führt.

Sie vergeben im ersten Dialog einen Namen für Ihr Projekt und legen das Verzeichnis fest, in das die Kopie der Webseite abgelegt werden soll. Im nachfolgenden Fenster geben Sie die Adressen der Webseiten ein, die Sie speichern wollen.

Die Software unterstützt die Protokolle HTTP, HTTPS und sogar FTP. Das Programm kennt verschiedene Modi, um die Dateien herunterzuladen. So ist es auch möglich, einfach alle gefundenen Dokumente auf den lokalen Rechner zu übertragen. Dabei gehen dann aber die Links verloren. Nutzen Sie am einfachsten den Modus „Automatische Web-Site-Kopie“.

Richtig interessant wird es, wenn Sie die „Einstellungen“ aufrufen. Denn dahinter verbergen sich unzählige Schalter und Optionen, um das Klonen exakter zu steuern. Nehmen Sie hier keine Änderungen vor, überträgt Httrack die Struktur der Site genau so, wie sie dort angelegt ist. Im Abschnitt „Struktur“ haben Sie aber zahlreiche Variationen zur Auswahl. So ist es beispielsweise möglich, die verschiedenen Dateitypen voneinander separiert in einer Ordnerstruktur abzurufen. Das ist ganz praktisch, wenn Sie etwa alle PDF-Dateien, die auf einer Seite angeboten werden, an zentraler Stelle sammeln wollen.

Mit Filtern die Datenmenge beschränken

Für das Programm spielt die Art der Website, die Sie einlesen wollen, keine Rolle. Wird dort auf zahlreiche externe Quellen und Dateien verlinkt, verfolgt Httrack diese Links und lädt die Ressourcen herunter. Damit würden dann aber auch viele Dateien auf Ihrem Rechner landen, die Sie vielleicht gar nicht benötigen. Mit den Einstellungen im Abschnitt „Filterregeln“ nehmen Sie das Feintuning vor.

Um beim Beispiel der PDF-Dateien zu bleiben: Wenn Sie diese von der Übertragung ausschließen wollen,

geht das mit einem vorangestellten Minuszeichen und der Angabe des Dateityps. Ein Filter

```
- www.abc.de/*.pdf
```

lädt alle Dokumente der Domain herunter, nur eben nicht die PDF-Dateien. Filter können auch kombiniert werden und sind ein mächtiges Werkzeug, allerdings dauert es eine Weile, bis man sich mit allen Möglichkeiten vertraut gemacht hat. Für alle Nutzer, die Speicherplatz auf dem lokalen System sparen wollen, gibt es Größenbeschränkungen. Die Angabe

```
-*.zip[>2048]
```

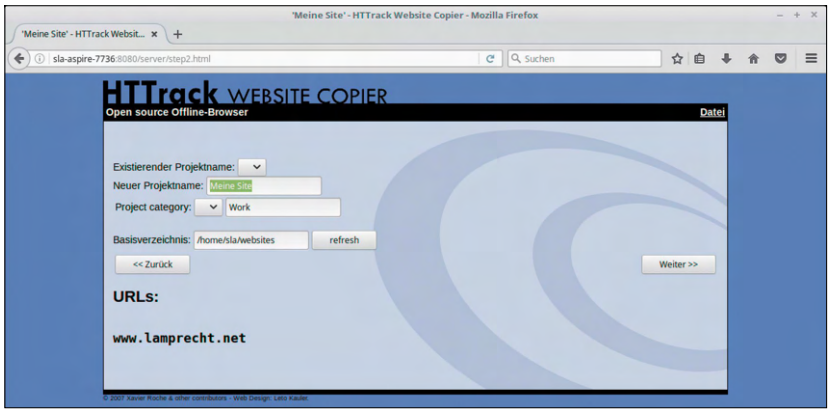
ignoriert alle ZIP-Archive mit einer Größe von mehr als zwei Megabyte. Haben Sie alle Filter und Bedingungen hinterlegt, beginnen Sie die Übertragung. Das kann je nach Internetverbindung und Komplexität der eingestellten Regeln eine Weile dauern. Sie gelangen zu den geklonten Sites am einfachsten, indem Sie die Datei „index.html“ in jenem Verzeichnis aufrufen, das Sie als Zielordner beim Programmstart definiert haben.

Wget für den Puristen

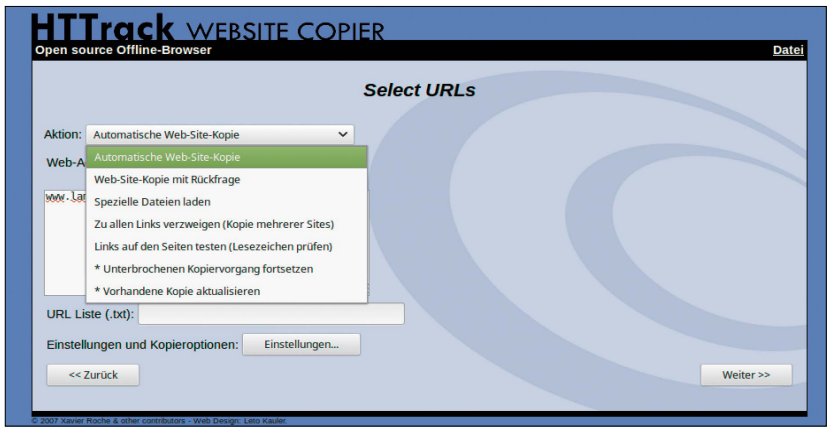
Rein funktional steht der Klassiker wget der App Httrack in nichts nach. Allerdings arbeitet das Programm ausschließlich auf der Konsole und sollte bei den meisten Distributionen bereits vorab installiert sein. Wget wurde nicht in erster Linie dazu konzipiert, um Sites zu klonen oder zu spiegeln, sondern kann sehr vielseitig dazu genutzt werden, um Dateien automatisiert aus dem Internet herunterzuladen. Ein einfacher Funktionsaufruf sieht etwa so aus:

```
wget http://www.abc.xy/beispiel/
  datei.ext
```

Damit laden Sie die entsprechende Datei direkt in das aktuelle Verzeichnis. Dem Funktionsaufruf dürfen Sie eine Textdatei übergeben, die eine ganze Reihe von diesen URLs enthält. Dazu nutzen Sie den Parameter „-i“ oder „--input-file=“ und setzen dahinter den Namen der Datei. Damit ist es etwa möglich, verschiedene Downloads vorzubereiten, um diese dann



Webhttrack ist dank eines Assistenten einfach zu bedienen: Zunächst muss das Verzeichnis definiert werden, in dem die Dateien landen sollen.



Webhttrack kennt eine Reihe von Modi, wie der Klon angelegt wird. Automatisch und ohne Rückfragen geht es am schnellsten.

auf einen Rutsch zu übertragen. Wer sich mit *man wget* die Manpages der Anwendung ansieht, dürfte überrascht sein, wie viele Parameter wget beherrscht. Sie können etwa die Bandbreite limitieren, die für den Download genutzt wird, die Tiefe der Verzeichnisebene definieren, die verfolgt wird, den Useragent anpassen, aber auch Benutzernamen und Passwort für geschützte Verzeichnisse auf dem eigenen Server übergeben.

Um eine Website zu klonen, um sie offline nutzen zu können, müssen verschiedene Schalter miteinander kombiniert werden. Ein Beispiel könnte folgendermaßen aussehen:

```
wget -r -k -E -l 4 http://bei
  spiel.xyz
```

In diesem Fall würde die Seite rekursiv („-r“) bis zur vierten Verzeichnisebene besucht und eingelesen („-l“ für Level). Der unscheinbare Schalter „-k“ sorgt dafür, dass Links so konvertiert werden, dass diese auch lokal funktionieren, während „-E“ die Dokumente mit der Endung „html“ versieht. Da die meisten Internetseiten heute ja dynamisch erzeugt werden und somit oftmals eine Endung wie „PHP“ oder „ASP“ tragen, würde das lokale Blättern nicht funktionieren.

Durch die Konvertierung entstehen aber statische Dokumente, die dann auch in Ruhe betrachtet werden können. Das ist auch zugleich die Grenze des Klons. Änderungen, die im Back-End des Content-Management-Systems durchgeführt werden, stehen ja in einer Datenbank. Der Inhalt der Seite entsteht üblicherweise in dem Moment des Aufrufs. Deswegen sind Klons bei dynamisch erzeugten Seiten nur eine aktuelle Momentaufnahme. ●

Verspielte Terminaltools

Basteleien dürfen auch mal sinnfrei und verspielt ausfallen. Das verleiht dem eigenen Linux-System oder manchen Shell-Scripts einen individuellen Charme. Der Beitrag erläutert einige einschlägige Hilfsmittel.

Von **Hermann Apfelböck**

Die Spaßwerkzeuge für das Terminal sind zum Großteil gar nicht so trivial zu benutzen, wie es ihrem Stellenwert eigentlich angemessen wäre. Freundliche Ausnahmen sind sl und cmatrix. Alle weiteren hier genannten Tools verlangen Experimente und Bastelei, bis das Ergebnis stimmt – das sich dann aber durchaus sehen lassen kann.

Textkunstwerke mit Figlet & Co.

Für die Linux-Konsole gibt es eine Reihe von Tools, die einen Text mehr oder weniger kunstvoll mit Sonderzeichen und in mehrfacher Fontgröße darstellen. Das vergleichsweise primitive Banner schreibt nach

```
banner Willkommen!
```

den angegeben Text mit dem Zeichen „#“ in siebenfacher Zeilenhöhe auf den Bildschirm. Weit komplexer sind die Werkzeuge Toilet und Figlet (mit gleichnamigen Paketnamen). Sie werden nicht nur gerne im Terminal genutzt, sondern auch als Vorlage für effektvolle Mailsignaturen oder Texte. Beachten Sie allerdings, dass dies nur bei Formatierung als Reintext zu den gewünschten Ergebnissen führt. Folgender Befehl dreht den angegebenen Text um 180 Grad und stellt ihn somit auf den Kopf:

```
toilet -f term -filter 180 echo
  "Sehr geehrte Damen und Herren" >
  dh.txt
```

Der im Beispiel in die Ausgabedatei geleitete Text kann dann an anderer Stelle genutzt werden. Farbcodierungen mit Toilet (Schalter „--filter gay“ und „--filter metal“) funktionieren aber nur im Terminal selbst. Besonders hübsche Kunstwerke fabriziert das Tool Figlet. Simple Beispiele sind

```
figlet "Max Mustermann"
```

oder auch:

```
figlet -c "Max" "" "Mustermann"
```

Schalter „-c“ zentriert die Ausgabe, das doppelte Anführungszeichen in der Mitte erzeugt einen Zeilenumbruch. Das folgende Beispiel zeigt die aktuelle Uhrzeit an

```
figlet $(date +%H:%M)
```

und dieser Befehl

```
figlet -R "Willkommen!"
```

schreibt den Text von hinten. Die verfügbaren Fonts finden sich unter „/usr/share/figlet/“ und können mit Schalter „-f“ und nachfolgendem Fontnamen gewechselt werden:

```
uname -n | figlet -f big
```

Im Allgemeinen ist der Standardfont mit das Attraktivste, was Figlet zu bieten hat. Maximale Aufmerksamkeit erzielen Sie eventuell mit Fonts wie pagga oder future. Mit der folgenden For-Schleife

```
for n in /usr/share/figlet/*.tlf;
  do figlet -t -f $n $n;done
```

können Sie einfach mal alle Fonts durchprobieren.



Hübsche Bastelarbeit: Zutaten sind hier ein transparentes Drop-down-Terminal (Gnome-Extension) im Vollbild sowie Figlet-Malereien mit Echtzeitdaten auf Basis eines Shell-Scripts.

Sprachausgabe mit Espeak

Dias Tool Espeak (mit identischem Paketnamen) hat eigentlich einen ernsten Hintergrund, insofern es eine synthetische Audioausgabe von Text- und HTML-Dateien vorsieht und sich als Vorlesewerkzeug für Sehbehinderte eignet. Die mechanisierte Phonetik ist allerdings sehr gewöhnungsbedürftig und erst nach etwas Akklimatisierung zu verstehen. Die unangenehmsten Effekte lassen sich durch zahlreiche Schalter teilweise kompensieren.

Eine Kapitellesung aus einer vorliegenden Textdatei könnte so aussehen:

```
espeak -vde -f buddenbrooks15.txt
  -s 200 -g 15 -p 60
```

Hier ist mit Schalter „-v“ eine deutsche Sprachausgabe gewählt und mit „-f“ die Datei angegeben. Die restlichen Schalter bestimmen die Vorlesege-

schwindigkeit („-s“), die Pausen zwischen Einzelwörtern („-g“) und die Tonhöhe („-p“). Den Wert von Espeak als Vorleseroboter können letztlich nur Sehbehinderte angemessen beurteilen. Für Systembasteleien mit kurzen Ansagen eignet sich Espeak aber bestens. So kann etwa folgende Zeitansage

```
espeak -vde "Hallo Apfelböck! Es
 ist jetzt $(date +%H) Uhr" -s 220
 -p 10 -g 15
```

als stündlicher Cronjob angelegt werden (siehe dazu Seite 106). Da die Crontab die verwendete Variable nicht auflösen kann, ist der Umweg über ein Shell-Script erforderlich. In der Crontab steht dann etwa

```
0    *    *    *    *    sh
 ~/zeitansage.sh
```

und das hier angegebene Script enthält wiederum den espeak-Befehl.

Matrix-Screensaver für die Konsole

Cmatrix ist über die Standardpaketquellen zu beziehen und unter Debian/Ubuntu/Mint mit

```
sudo apt-get install cmatrix
```

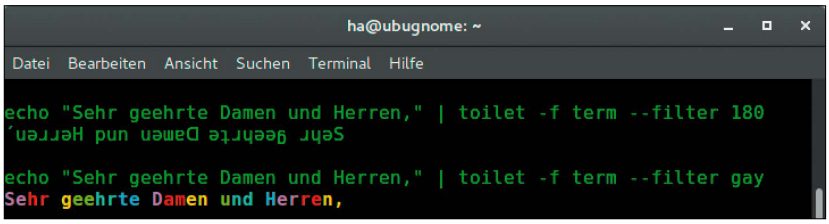
schnell installiert. Nach Eingabe von *cmatrix* regnet es grüne Buchstaben im Terminal mit der Anmutung des Filmeklassikers „Matrix“. Wer die Animation farblich (Schalter „-C“) oder in der Geschwindigkeit (Schalter „-u“) beeinflussen will, hat dafür mehrere Parameter zur Verfügung – etwa:

```
cmatrix -sab -u 6 -C red
```

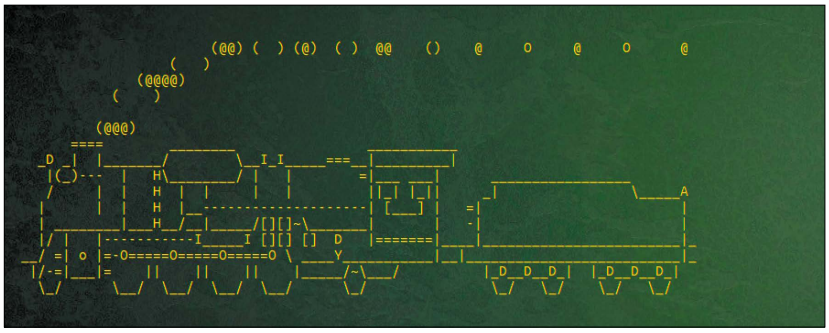
Schalter „-s“, hier im Beispiel kombiniert mit weiteren Optionen, ist zu empfehlen, wenn sich Cmatrix wie ein Terminal-Screensaver verhalten und nach jeder eingegebenen Taste stoppen soll. Andernfalls hilft Taste „Q“ oder die allgemeine Tastenkombination Strg-C, um den Buchstabenregen zu beenden.

sl – „Steam Locomotive“

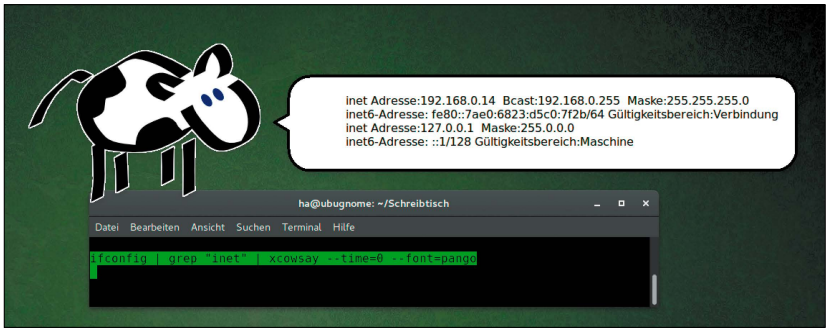
Manchmal muss man einfach mal die Dampflokomotive durchs Terminal fahren lassen – etwa in Shell-Scripts. Das sinnfreie, aber hübsch gemachte Kommandozeilentool sl (mit identischem Paketnamen) zeigt eine aufwendige Ascii-Animation, um eine Dampflok mit Waggon von rechts nach links durchs Terminal zu schicken. Die wenigen Schalter sind keiner Erwähnung wert – sl genügt in der Regel vollauf. Ursprüngliches Motiv für sl war eine Aufheiterung nach Buchstabendreher beim Allerweltsbefehl „ls“.



Schmutziger Name – hübsches Tool: Toilet beherrscht Farb- und Dreheffekte, um einen vorgegebenen Text zu verschönern oder zu verfremden.



Ohne Kommentar: sl („Stream Locomotive“) ist wohl schon durch jedes Admin-Terminal gefahren.

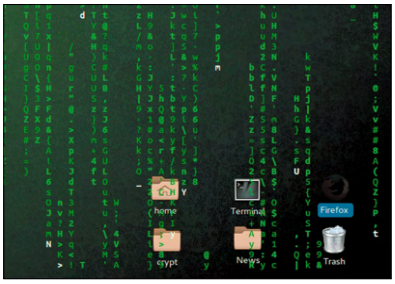


Kühe, Gnus oder Elefanten informieren: Wer sachliche Infos auflockern will, greift zu Cowsay oder Xcowsay.

Die Kuh weiß alles

Mit Cowsay und Xcowsay (mit gleichen Paketnamen) lassen sich Texte oder Terminalbefehle einer Kuh ins Maul legen – wobei die Terminalvariante Cowsay unter „/usr/share/cowsay/cows“ eine Menge weiterer Kreaturen bevorratet:

```
ls -AlF | cowsay -f gnu -n
```



Sinnfrei, aber attraktiv: Die herabfallenden Buchstaben von Cmatrix machen den Konsolenalltag unterhaltsamer.

Die grafische Variante Xcowsay kennt lediglich Kühe unterschiedlicher Größe, die mit dem Schalter „--at=100,100“ (Beispiel) beliebig positioniert werden können. ●

Dateien und Ordner im Griff

Dieser Ratgeber hat den komfortablen, souveränen bis raffinierten Umgang mit Dateien und Ordnern zum Thema. Im Zentrum stehen die grafischen Dateimanager und diverse Tools und Finessen für das Terminal.

Von **Hermann Apfelböck** und **Thorsten Eggeling**



Einen guten Teil des PC-Alltags und der Serververwaltung verbringt der Nutzer mit Klicks zum gesuchten Verzeichnis, mit der Suche nach der richtigen Benutzer-, Konfigurations- oder Systemdatei, mit dem Kopieren auf Wechseldatenträger oder mit dem Inventar der Mediensammlung. Es gibt keinen Ort im PC-Alltag, wo sich tieferes Know-how und entsprechendes Tuning mehr lohnen als beim Dateimanager und bei der Dateibehandlung in der Shell: Wo andere vier Mal klicken, reicht dann einmal. Und statt mühsam Dutzende von Dateien zu löschen oder umzubenennen, genügt vielleicht ein einziger messerscharfer Befehl. Dieser Artikel nennt die wesentlichen Methoden und Tools für den souveränen Umgang mit Dateien und Ordnern.

Hinweis: Alle komplizierteren Kommandos und Scripts dieses Artikels finden Sie in der Datei „Dateikommandos.txt“ auf Heft-DVD (unter „/Software“).

Dateilisten und Suche

Dateilisten und Suche (1): Eigenheiten in Nautilus & Co.

Um Dateien zu suchen, blenden Sie in Nautilus (Ubuntu) oder Nemo (Mint) das Lupensymbol ein. Die rekursive Suche beginnt standardmäßig im aktuell geöffneten Ordner. Sie können in allen Dateimanagern auf „Alle Dateien“ erweitern oder einen anderen Startordner angeben. In der Regel gibt es noch wie in Nautilus einen Filter („+“-Zeichen), um die Suche auf Dateitypen wie „Dokumente“ oder „Musik“ zu beschränken.

Für Terminalnutzer ungewöhnlich ist die Tatsache, dass diese Dateisuche die Stellvertreter „*“ und „?“ nicht kennt. Verwenden Sie einfach mehrere Strings getrennt durch Leerzeichen, die dann als „Und“-Verknüpfung gelten: „steuer 2017“ findet Dateien, „steuer*2017“ nicht (ohne Anführungszeichen eingeben).

Dateilisten und Suche (2): Versteckte Dateien im Terminal

Platzhalter wie der Asterisk (*) werden von der Shell interpretiert, nicht vom ausgeführten Befehl. Dies bedeutet, dass es von der Shell-Konfiguration abhängt, ob ein Kommando mit dem Platzhalter „*“ versteckte Dateien und Verzeichnisse berücksichtigt.

Voreinstellung ist in der Regel, dass versteckte Dateien und Verzeichnisse ignoriert werden. Unter Linux zeichnen sich versteckte Dateiobjekte lediglich dadurch aus, dass der Dateiname mit einem Punkt beginnt. Wenn Sie den Befehl

```
tar -cvzf archiv.tar.gz *
```

eingeben, um das aktuelle Verzeichnis in ein „tar.gz“-Archiv zu komprimieren, dann bleibt alles außen vor, was versteckt ist. Dieses Bash-Verhalten können Sie mit dem Befehl shopt (Shell-Options) ändern. Nach dem Set-Befehl

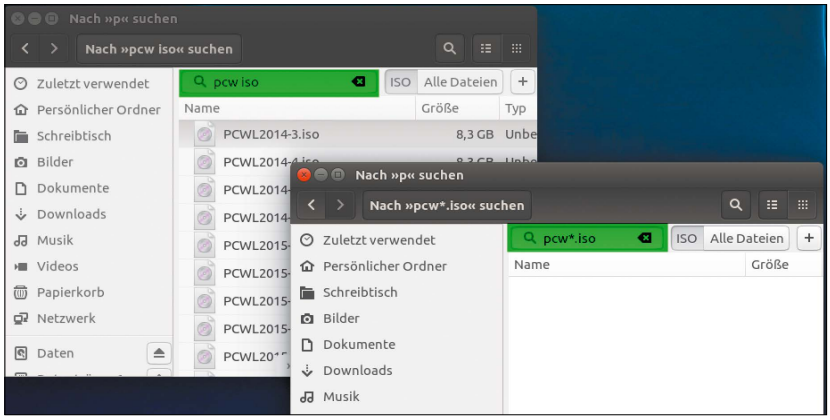
```
shopt -s dotglob
```

werden auch versteckte Dateiobjekte berücksichtigt. Die Einstellung gilt aber nur für die aktuell geöffnete Shell. Um das Verhalten permanent zu ändern, tragen Sie den shopt-Befehl als zusätzliche Zeile in die Konfigurationsdatei „~/.bashrc“ ein.

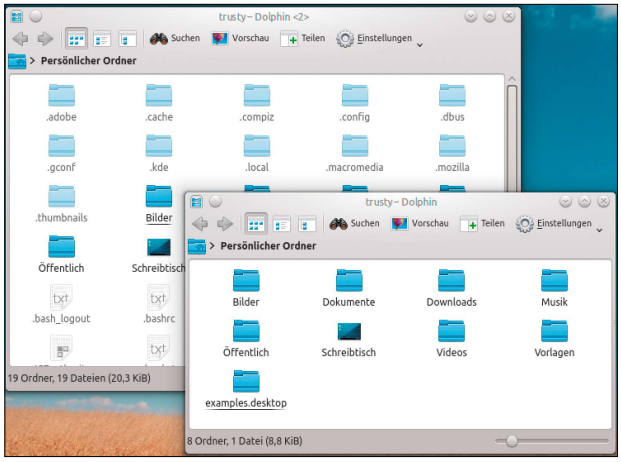
Dateilisten und Suche (3): Verstecktes im Dateimanager

Versteckte Dateien und Verzeichnisse sind hauptsächlich die Domäne von Konfigurationsdateien, mit welchen typische Desktopanwender selten direkt in Kontakt kommen. Daher blenden die Dateimanager und Dateidialoge der Desktopumgebungen alles Versteckte zunächst aus.

Ist es aber doch einmal nötig, eine versteckte Datei zu bearbeiten oder einen versteckten Ordner zu öffnen, dann gibt es sowohl unter Gnome, Unity, XFCE als auch unter KDE Tastenkombinationen, um im jeweiligen Dateimanager alles Versteckte zu zeigen: In Gnome, Unity und XFCE drücken Sie die Tastenkombination Strg-H. KDE nutzt wie der Midnight Commander die Tastenkombination Alt und Punkt.



Dateien auf der Festplatte finden: Die Suchfunktion von Dateimanagern kann mit den Stellvertreterzeichen nichts anfangen. Die „Und“-Verknüpfung im oberen Fenster funktioniert.



Versteckt oder sichtbar: In den Dateimanagern der verschiedenen Desktopumgebungen können Sie per Tastenkombination versteckte Dateien und Ordner ein- und ausblenden.

Dateilisten und Suche (4): find im Terminal

Der typische Befehl ls beherrscht mit Schalter „-R“ auch eine verzeichnisübergreifende Suche und liefert etwa in Zusammenarbeit mit grep

```
ls -R /media | grep -i "schönberg"
```

schnelle Ergebnisse. Wenn für die Weiterbearbeitung in der Bash-Shell oder für zielsicheres Auffinden des Verzeichnisses der komplette Pfad benötigt wird, ist der ls-Befehl aber nicht ideal, weil er nur bei Verzeichnissen den Pfad zurückgibt, bei Dateien hingegen nicht. Das Kommando find ist hier die bessere Wahl:

```
find /media -iname "schönberg"
```

Um nur Dateien anzuzeigen und Verzeichnisse wegzufiltern, hilft der Schalter „-type f“ (file):

```
find /media -type f -iname "schön
  berg"
```

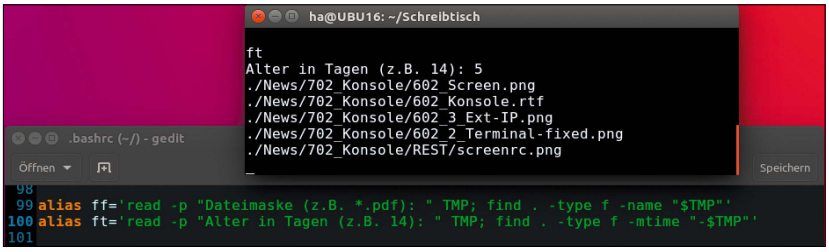
Die wichtigsten der zahlreichen Filter-Möglichkeiten von find legt man sich zur komfortableren Nutzung am besten als Alias oder Function zurecht:

```
alias fn='read -p "Muster (z.B.
  .pdf): " tmp; find /media -iname
  "*$tmp*"'
```

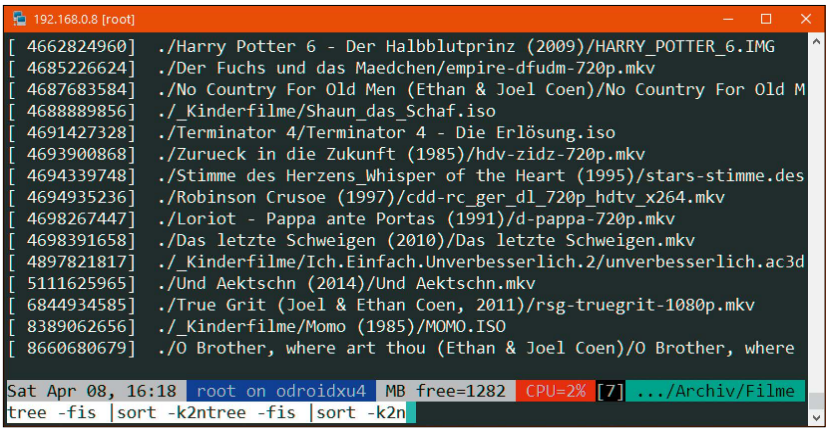
Als Function – etwa in der Datei „~/.bashrc“ – wird das Ganze noch etwas flexibler:

```
function fn ()
{
tmp=$*
if [ -z "$tmp" ];then
  read -p "Dateimuster (z.B. *.pdf
  oder *steuer*): " tmp
fi else
find /media -iname "*$tmp*"
}
```

Danach ist sowohl die direkte Stringübergabe *fn schönberg* möglich als auch die Eingabe des Suchstrings nach Aufruf *fn*. Weitere sinnvolle Varianten dieses Strickmusters wären



Find ist unentbehrlich: Die wichtigsten Suchaktionen können Sie sich mit komfortablen Aliases oder Bash-Functions vereinfachen.



Die größten Dateien ermitteln: Der Befehl tree kann Dateigrößen in Byte ausgeben. Diese tree-Liste wird dann von sort numerisch sortiert.

```
alias ft='read -p "Alter in Tagen
  (z.B. 14): " tmp; find /media
  -mtime "-$tmp"'
```

zum Filtern nach Dateien bestimmten Alters. Beachten Sie, dass die übergebene Anzahl in Tagen mit dem Minus-Vorzeichen („-$tmp“) übergeben wird. Dies bewirkt, dass find alle Dateien meldet, die so alt oder jünger sind als die angegebene Tageszahl. Um Dateien bestimmter Größe zu suchen, eignet sich ein find-Filter dieser Art:

```
alias fs='read -p "Größe in MB
  oder GB (z.B. 4000M oder 4G): "
  tmp; find /media -size "+$tmp"'
```

Eine Eingabe wie „1G“ liefert dann alle Dateien mit mindestens einem GB und größer, da der Parameter mit „+“-Vorzeichen übergeben wird.

Achtung: Die genannten Beispiele verwenden den Ordner „/media“ als Ausgangspunkt. Je nach Situation ist dies etwa durch das Home-Verzeichnis zu ersetzen. Theoretisch ist auch das root-Verzeichnis möglich, was aber die Suche verlangsamt, ohne root-Recht zu diversen Zugriffsfehlern führt und außerdem nicht auf die typische Suche nach Benutzerdateien fokussiert.

Dateilisten und Suche (5): Ordner als Baumstruktur

Das Konsolenprogramm tree erstellt rekursive Inhaltsangaben von Verzeichnissen in einer Baumstruktur, ausgehend vom momentanen Ort oder von einem gezielt angegebenen Verzeichnis. Dabei berechnet das Tool auch die Anzahl der enthaltenen Unterordner sowie der Dateien und gibt auf Wunsch auch den Platzbedarf an.

Die verbreiteten Linux-Distributionen haben tree nicht im Repertoire, allerdings ist das Programm schnell nachinstalliert – in Ubuntu, Debian, Raspbian mit diesem Kommando:

```
sudo apt-get install tree
```

Der Aufruf von *tree* ohne Parameter präsentiert die Verzeichnis- und Dateistruktur unterhalb des aktuellen Ordners. Die Option „-a“ sorgt dafür, dass auch versteckte Dateien und Verzeichnisse angezeigt werden. Wer sich nur für Verzeichnisse interessiert, kann alle Dateien mit *tree -d* ausblenden. Weil die Ausgabe von tree sehr umfangreich ausfallen kann, gibt es auch eine Möglichkeit, die Baumstruktur mittels des Befehls

```
tree -no ordner.txt
```

in eine Textdatei zu schreiben.

Dateilisten und Suche (6): Die dicksten Dateien finden

Welche Dateien belegen den meisten Platz? Auf der Kommandozeile gibt es unter Linux diverse Wege, Platzfressern auf die Spur zu kommen: Die Tools tree und find sind bestens geeignet, sich eine Übersicht zum Inhalt und zur Größe von Verzeichnissen zu verschaffen. Der Befehl tree zeigt hübsche Baumansichten zur Visualisierung von Dateien und Ordnerstruktur – zusammen mit den Parametern

```
tree -fash
```

auch mit Größenangabe pro Datei, ausgehend vom aktuellen Verzeichnis. Die Befehlskombination

```
tree -fis |sort -k2 -n
```

sortiert die Dateigrößen aufsteigend.

Dateilisten und Suche (7): Dateitypen zählen

Wie viele Dateien eines Typs befinden sich in einem Verzeichnisbaum? Mit Befehlsverkettungen können Sie sowohl die Anzahl wie den Festplattenbedarf von Dateitypen ermitteln. Das folgende Kommando

```
ls -R | tr [:upper:] [:lower:] |
  grep -oP '\.[^\.]+$' | sort |
  uniq -c | sort -n
```

setzt erst alles auf Kleinbuchstaben, filtert mit grep die Extensionen heraus, sortiert das Ergebnis alphabetisch, zählt dann das Vorkommen der Extensionen und zeigt schließlich das Ergebnis in aufsteigender Reihenfolge – also die häufigsten Dateitypen zuletzt.

Eine andere Inventurmethode berechnet den Platzbedarf eines bestimmten Dateityps:

```
find . -iname "*.mkv" -type f
  -exec du -ch {} + | tail -n1
```

Hier hilft das Tool du, um die Dateigrößen zu ermitteln, und tail schneidet alles bis auf das Gesamtergebnis ab.

Dateilisten und Suche (8): ISO-Abbilder durchsuchen

Wer auf dem Linux-Desktop nach einer bestimmten Datei in einem einzigen ISO-Image sucht, kann die ISO-Datei mit dem Programm File-Roller („Archivmanager“) verwenden. Wenn eine Datei aber in mehreren ISO-Dateien liegen kann, ist dieser Weg zu umständlich.

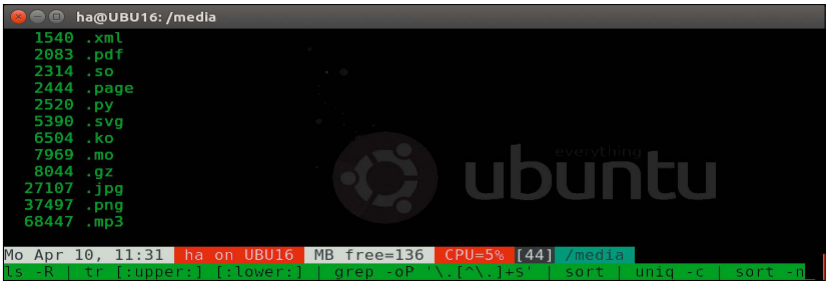
Im Terminal finden Sie Dateien in ISO-Daten mit Hilfe des Befehls isoinfo. Isoinfo ist Teil des Pakets „mkisofs“ und gehört bei nahezu allen Linux-Distributionen zum Standardrepertoire. Das einfachste Anwendungsbeispiel für isoinfo ist die Ausgabe aller Dateien in einem Image, als ob dieses ein Verzeichnis wäre:

```
isoinfo -l -i name.iso | less
```

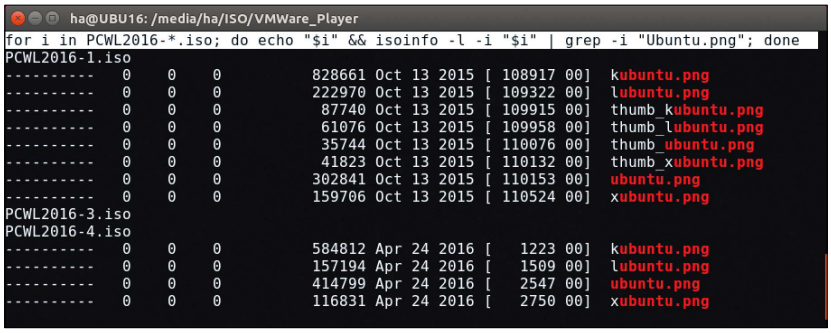
Dieser Befehl zeigt alle Dateien des ISO-Abbilds, nach Verzeichnissen geordnet. Der nach dem Pipe-Symbol („|“) abgehängte Befehl „less“ bewirkt eine seitenweise Ausgabe der Liste, die sich mit den Cursor-Tasten durchblättern und mit der Taste Q jederzeit beenden lässt. Zum Suchen einer Datei hilft grep:

```
isoinfo -l -i name.iso | grep -i
  "wichtig.txt"
```

Der Befehl dauert auch bei großen DVD-Images nur Sekunden und zeigt sofort, wenn die Datei gefunden wurde. Die Abbildung rechts zeigt ein Beispiel, wie Sie ein ganzes Archiv mit ISO-Dateien durchsuchen können.



Typenkunde: Dieser Befehl gibt eine Liste aus, wie viele Dateien eines Typs im aktuellen Verzeichnisbaum vorhanden sind.



Nadel im Heuhaufen: isoinfo spielt seine Stärke bei der Suche nach Dateien in ISO-Images aus. In Sekunden sind Dateien in ISO-Dateien gefunden.

Dateibearbeitung

Dateibearbeitung (1): Basisbedienung von Dateimanagern

In der Basisbedienung unterscheiden sich Nautilus (Ubuntu), Nemo (Linux Mint) oder Caja (Ubuntu Mate) kaum und folgen weitgehend Standards, die man auch von Windows und Mac-OS X kennt. Dennoch bleiben oft schon bei der fundamentalen Bedienung wichtige Optionen ungenutzt:

Dateiobjekte markieren: Um mit der Maus mehrere Dateiobjekte auszuwählen, verwenden Sie für eine selektive Auswahl zusätzlich die Taste Strg, für eine zusammenhängende Auswahl die Umschalt-Taste. Beim Drag & Drop zwischen zwei geöffneten Dateimanagerfenstern können Sie mit gedrückter Umschalt-Taste das Verschieben erzwingen, mit der Strg-Taste das Kopieren. Diese Tasten sind wichtiger als unter Windows, weil die meisten der Linux-Dateimanager kein Drag & Drop mit rechter Maustaste (und folgendem Kontextmenü) beherrschen.

Endgültiges Löschen: Beim Löschen mit der Taste Entf verwenden die Dateimanager standardmäßig den Papierkorb. Es lohnt sich, unter „Dateien -> Einstellungen -> Verhalten“ (Nautilus) die Konfiguration aufzusuchen und „Einen Löschbefehl bereitzustellen, der den Papierkorb umgeht“ und endgültig löscht. Dieser zusätzliche Befehl erscheint als „Löschen“ im Kontextmenü.

Skalieren mit Hotkey: Die Größe der Dateiobjekte ist mit den Hotkeys Strg-+ und Strg-- bequem zu regeln.

Favoriten: „Lesezeichen“ in der Navigationsspalte bieten einen schnellen Weg zu wichtigen Ordnern, Medien und Webservern. Um ein neues Lesezeichen anzulegen, gehen Sie in das gewünschte Verzeichnis, klicken rechts oben auf das Zahnradsymbol und wählen „Lesezeichen für diesen Ordner anlegen“. Schneller geht’s mit dem Hotkey Strg-D. Außerdem gibt es den Menüpunkt „Datei -> Lesezeichen“, um die Ordnerfavoriten zu verwalten.

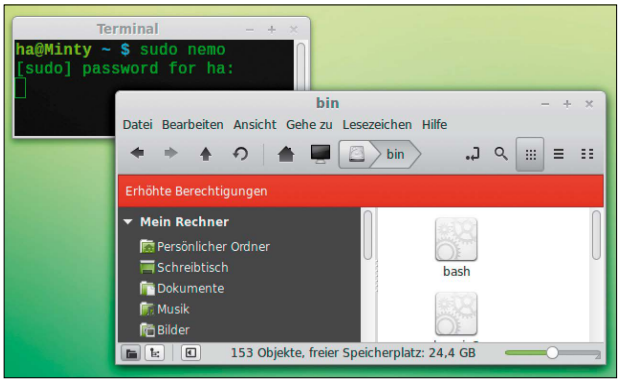
Arbeiten mit Tabs: Mit den Tasten Strg-T oder nach Klick auf das Zahnrad-Symbol rechts oben und „Neuer Reiter“ öffnen Sie einen neuen Tab. Tabs scheinen auf den ersten Blick für Mausaktionen weniger komfortabel als mehrere Fensterinstanzen, jedoch funktioniert das Drag & Drop von Dateien auch hier – nämlich über die Titelleisten der Tab-Registerkarten.

Zwei-Fenster-Modus: Besonders praktisch zum Kopieren und Verschieben ist der klassische Zwei-Fenster-Modus wie in orthodoxen Dateimanagern, den Sie jederzeit mit Taste F3 aktivieren und wieder deaktivieren (Nemo, Caja). Ubuntus Standardmanager Nautilus bietet diese Ansichtsoption nicht.

Dateimanager als root: Außerhalb von „/home“ darf der normale User nicht viel: Wenn Sie mit dem Dateima-



Zuordnung von Dateitypen: Über „Öffnen mit" weisen Sie einem Dateiformat das gewünschte Anzeige- oder Bearbeitungsprogramm zu.



Der Dateimanager erhält hier beim Start erhöhte Rechte. Diese gelten, bis Sie das Programm wieder schließen.

nager im Dateisystem spazieren gehen, erkennen Sie das daran, dass die Optionen „Ordner/Datei anlegen" meist inaktiv sind. Nach *sudo nautilus* besitzt der Dateimanager erhöhte Rechte.

Dateitypen zuordnen: Welches Programm startet, wenn Sie einen bestimmten Dateityp im Dateimanager anklicken, ist in den Systemeinstellungen hinterlegt. Individuelle Dateizuordnungen erreichen Sie nach Rechtsklick auf einen Dateityp mit der Option „Eigenschaften -> Öffnen mit", indem Sie dann in der Liste das gewünschte Programm wählen und schließlich „Als Vorgabe festlegen".

Dateibearbeitung (2): Suchen und Ersetzen mit rename

In Debian und Ubuntu gibt es neben dem mv-Befehl das spezialisierte Programm rename. Dank Platzhaltern und regulären Ausdrücken beherrscht der Befehl auch komplizierte Änderungen an Namen ganzer Dateilisten. Ein Bei-

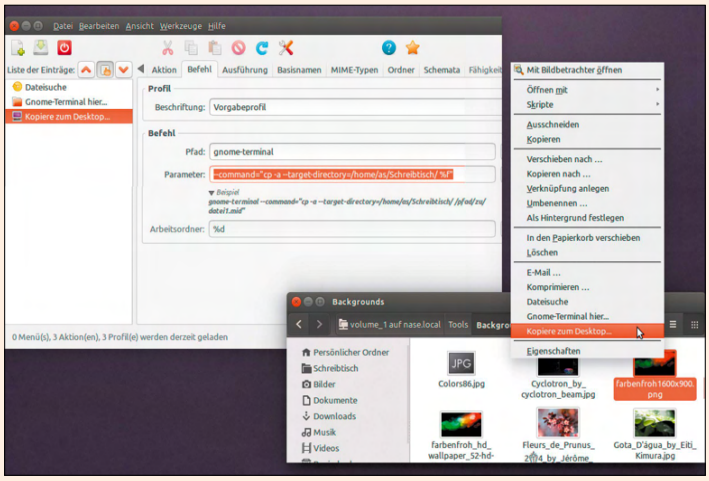
Nautilus/Caja/Nemo: Anpassen der Kontextmenüs

Praktisch alle Linux-Dateimanager erlauben den individuellen Ausbau mit benutzerdefinierten Kontextmenüs. Das heißt, dass ein Rechtsklick auf bestimmte Dateitypen ein individuelles Angebot von passenden Programmen oder Scripts anbietet. Das Anpassen von Nautilus, Nemo & Co. erfordert allerdings etwas Geduld und Zeit.

Nautilus/Caja (Ubuntu/Ubuntu Mate): Für Nautilus und Caja ist eine spezielle Erweiterung erforderlich. Je nach benutztem Dateimanager installieren Sie sie mit einem dieser Befehle

```
sudo apt-get install nautilus-actions
sudo apt-get install caja-actions
```

nach. Die beiden Erweiterungen sind funktionsidentisch und als „Einstellungen für Nautilus[Caja]-Aktionen" im Dash oder Hauptmenü zu finden.



Zusatztool Nautilus-Actions: Das Werkzeug gibt es identisch für Caja („Caja-Actions") und bietet Bastlern eine Spielwiese für zusätzliche Kontextmenüs.

Trotz grafischer Bedienung ist es nicht ganz trivial, den Dateimanager damit erfolgreich zu erweitern. Verwenden Sie zunächst nur die wichtigsten Registerkarten „Aktion" und „Befehl": Unter „Aktion" muss „Eintrag im Auswahl-Kontextmenü anzeigen" aktiviert und ferner ein Name („Kontextbezeichner") definiert sein. Unter „Befehl" geben Sie den Programmnamen oder den kompletten Pfad zum gewünschten Programm ein.

„Parameter" sind je nach Programm sinnvoll bis notwendig. Die Schaltfläche „Legende" zeigt, welche Variablen das Tool weitergeben kann: Eindeutig am wichtigsten sind mit „%d" der Pfadname für einen rechtsgeklickten Ordner, mit „%f" der Pfadname einer Datei. Um etwa ein Terminal nach Rechtsklick am Dateiobjekt zu öffnen, genügt als Befehl „gnome-terminal" und als Parameter „--working-directory=%d". Im Feld „Arbeitsordner" sollte die Variable „%d" nie fehlen, da viele Programme die Arbeit sonst einfach kommentarlos verweigern.

Unter „Basisnamen", „MIME-Typen", „Ordner" lassen sich die Kontextmenüs gezielt filtern: Wird für ein Kontextmenü etwa als Basisname „*.zip" eingestellt, so erscheint die Menüoption nur bei „zip"-Dateien.

spiel für den simplen Einsatz ist die Umwandlung von Dateinamen in Kleinbuchstaben, falls die Schreibweise uneinheitlich gemischt oder in Großbuchstaben vorliegt:

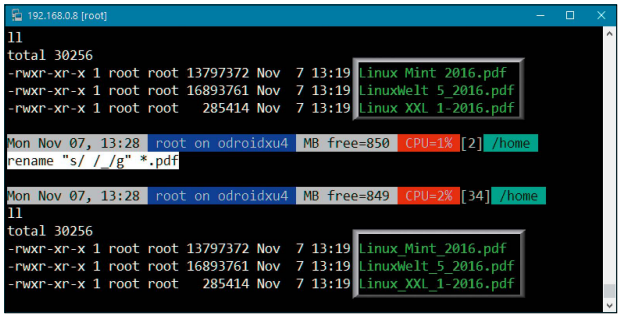
```
rename 'y/A-ZÄÖÜ/a-zäöü/' *
```

Der Befehl kommt auch mit Leerzeichen im Namen klar und kümmert sich auch um die Umlaute „ÄÖÜ“, während alle anderen Sonderzeichen unberührt bleiben.

Ein weiteres typisches Problem sind Dateien mit Leerzeichen im Namen. Mit folgendem Befehl

```
rename "s/ /_/g" *
```

wandeln Sie alle Leerzeichen in Unterstriche um. Die Angabe der String-Ersetzung in Anführungszeichen erfolgt jeweils in Perl-Syntax. Die Ersetzung wird durch das „s“ veranlasst und das nachfolgende „g“ steht für „global“, um den Befehl auf alle zutreffenden Dateinamen anzuwenden.



Systematisches Umbenennen: Rename unter Ubuntu & Co. hat eine gewöhnungsbedürftige Python-Syntax. Einfachere Ersetzungen gelingen aber mühelos.

Das ähnlich einfache Beispiel

```
rename "s/:/_/g" *
```

ersetzt alle Doppelpunkte durch Unterstriche, was etwa für den Austausch von Dateien zwischen Linux und Windows hilfreich ist.

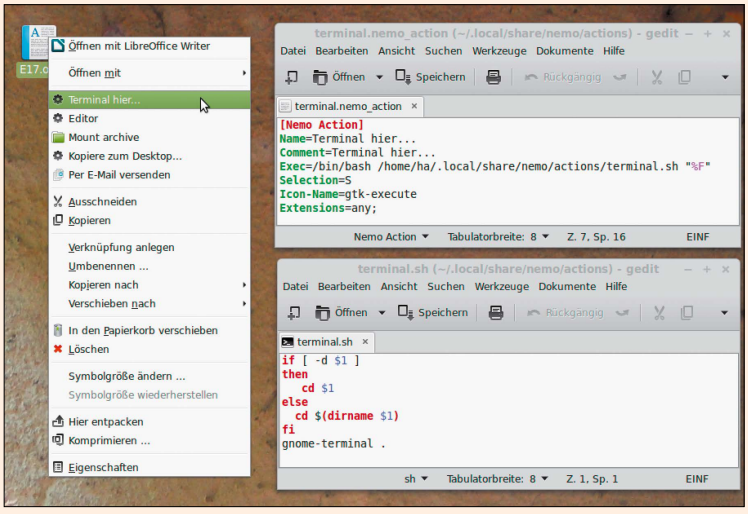
Kontrolle vorab: Bei Zweifeln über das gewünschte Resultat bietet rename den wichtigen Schalter „ -n“. Hier zeigt das Tool zwar die Ergebnisnamen an, führt aber die eigentliche Aktion noch nicht aus.

Dateibearbeitung (3): Rekursives Arbeiten mit find

Diverse Terminaltools bieten Schalter für verzeichnisübergreifende Aktionen, andere wiederum nicht. Sie können sich in den meisten Fällen die Syntaxrecherche sparen, indem Sie gleich auf find zurückgreifen und die gewünschte Aktion einfach mit dem Schalter „-exec“ anschließen. Find erspart auch viel Bash-Akrobatik, um sich mit Verzeichnislisten oder Schleifen durch Verzeich-

Eine globale Option finden Sie unter „Bearbeiten -> Einstellungen“: Dort lässt sich ein „Basismenü“ für die Optionen anlegen oder eben nicht. Das Basismenü fasst alle selbst erstellen Menüs unter „Nautilus-Actions“ zusammen, andernfalls landen die zusätzlichen Optionen einzeln im Kontextmenü.

Nemo (Mint): Der Dateimanager von Linux Mint (Cinnamon) hat für den Ausbau alles an Bord, verzichtet aber auf ein grafisches Tool. Hier müssen Sie mit Konfigurationsdateien hantieren, deren Aufbau jedoch nicht kompliziert ist. Nemo zeigt eine Option „Bearbeiten -> Module“, die allerdings nur vorhandene Erweiterungen für Kontextmenüs aktiviert oder deaktiviert. Ansonsten muss man unter „/usr/share/nemo/actions/“ aktiv werden (global) oder unter „~/.local/share/nemo/actions/“. Die Dateien an dieser Stelle müssen die Endung „.nemo_action“ besitzen. Unter „/usr/share/nemo/actions/“ finden Sie vordefinierte Dateien wie „mintstick.nemo_action“, die Sie als Vorlage für eigene Aktionen verwenden können.



Neue Menüs für Nemo: Das Anlegen neuer „Nemo-Actions“ ist recht transparent. Trotzdem wird es schnell komplex, wenn als „exec“-Befehl ein Shell-Script zwischengeschaltet wird.

Entscheidend ist die Anweisung „exec=…“ mit dem Programmaufruf. „selection=“ bestimmt, ob die Aktion bei einem Rechtsklick auf allen Dateiobjekten („any“), einem einzelnen („s“ für single) oder mehreren („m“ für multiple“) aktiv wird. Wenn das Kontextmenü nur für einen bestimmten Dateityp angezeigt werden soll, verwenden Sie „extensions=…“. Weitere Möglichkeiten wie etwa den Rechtsklick im Ordnerhintergrund nennt die Kurzdokumentation „sample.nemo_action“. Um etwa für alle Dateien, aber nicht für Ordner, den Editor xed anzubieten, verwenden Sie folgende Einträge:

```
Exec=/usr/bin/xed "%F"
Selection=S
Extensions=nodirs;
```

Außer dem Header „[Nemo Action]“, der am Beginn stehen muss, ist die Reihenfolge der Einträge egal.

nisse zu hangeln: Die übliche Syntax für einen Befehl, der über einen ganzen Verzeichnisbaum ausgeführt werden soll, sieht so aus:

```
find ~ -iname "*.pdf" -exec echo
 {} \;
```

Find startet hier im Home-Verzeichnis („~“). Die Dateimaske „*.pdf“ ist mit „-iname“ angegeben, um im Unterschied zu „-name“ Groß- und Kleinschreibung zu ignorieren. Eine Verbindung mit dem oben genannten rename könnte etwa die Namen einer Mediensammlung vereinheitlichen:

```
find /media -type f -iname "*Sin
 fonie*" -exec rename -n 's/Sinfo
 nie/Symphony/g' {} \;
```

rename ist hier noch mit Schalter „-n“ auf die reine Anzeige gezähmt, um den Vorgang vorab zu kontrollieren.

Der Befehl

```
find ~ -iname "*2016.pdf" -exec cp
 {} . \;
```

kopiert alle Dateien, die der angegebenen Namensmaske entsprechen, in das aktuelle Verzeichnis. Ein Befehl zum globalen Löschen von bestimmten Dateien sieht so aus:

```
find / -type f -iname "thumbs.db"
 -exec rm {} \;
```

Die Angaben „-type -f“ (Files) und „-type -d“ (Directories) können als zusätzlicher Filter dienen, um Befehle nur auf Dateien oder nur auf Ordner anzuwenden.

Eine sichere, aber bei großen Datenmengen anstrengende Alternative zu „-exec“ ist der Schalter „-ok“, der bei jeder gefundenen Datei nachfragt, ob die Aktion ausgeführt werden soll. Zum Löschen ist das Delegieren an einen externen Löschbefehl („-exec rm“) nicht unbedingt nötig, denn mit („-delete“)

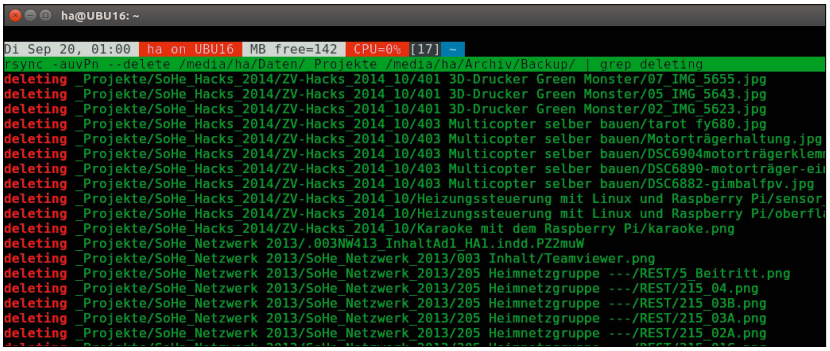
```
find / -iname "Thumbs.db" -delete
```

bringt find einen eigenen Löschschalter mit, der immer am Ende stehen muss.

find ermöglicht auch exklusives Löschen: Oft geht es bei Löschaktionen in einem Verzeichnis darum, alle Dateien bis auf einen bestimmten Dateityp zu löschen. Der übliche Löschbefehl „rm“ hat dafür keine brauchbare Lösung. Folgendes Kommando hilft, um alle Dateien bis auf jene mit der Endung „.txt“ zu löschen:

```
find /media/texte -type f ! -iname
 "*.txt" -delete
```

Das Ausrufezeichen vor „-iname“ bedeutet so viel wie „NOT“ und kehrt die nachfolgende Suchmaske um: Der Befehl findet alle Dateien, die nicht auf „.txt“ enden, und löscht sie anschließend.



Schalter „-n“ (oder „--dry-run“): Was rsync mit der Option „--delete“ ausrichten würde, können Sie vorab kontrollieren. Hier filtert grep gleich die zu erwartenden Löschaktionen.

Dateibearbeitung (4): Kopieren und Synchronisieren

Geht es um Kopieren und Backups, steht unter Linux meist das mächtige rsync (und sein grafisches Front-End Grsync) im Fokus. Nun ist es aber nicht so, dass dieses alternativlos wäre. Für einfache Sicherungen reicht cp völlig aus, das einen „--recursive“-Schalter (kurz „-r“) und einen „--update“-Schalter mitbringt – etwa:

```
cp -rvu [Quellordner]/* [Zielord
 ner]/
```

Freefilesync: Eine weitere grafische Alternative ist die Freeware Freefilesync (*www.freefilesync.org*), die es aktuell für Ubuntu, Debian und Open Suse gibt. Es genügt, das „tar-gz“-Archiv herunterzuladen und an geeigneter Stelle auszupacken. Die Linux-Version ist identisch mit der Windows-Variante und analysiert die angegebenen Quell- und Zielordner (Schaltfläche „Vergleichen“). Für den Vergleich gibt es mehreren Optionen, jedoch reicht in den meisten Fällen das einfache Kriterium „Dateigröße und -datum“ aus. Danach zeigt das Tool die Unterschiede in zwei Fenstern nebeneinander an. Bevor Sie die eigentliche Aktion mit „Synchronisieren“ und „Start“ auslösen, können Sie noch manuell eingreifen und einzelne Dateien durch Entfernen des Häkchens ausschließen.

rsync kontrollieren: Bei Medienarchiven ist es oft erwünscht, Original und Sicherungskopie exakt identisch zu halten. Für solche 1:1-Spiegelsicherung eignet sich das genannte Freefilesync ebenso wie rsync. Beide können nicht nur kopieren und updaten, sondern auch alle Dateien und Ordner, die in der Quelle nicht mehr existieren, auf dem Backupziel löschen. Das ist immer mit Risiken verbunden, wenn auf dem Zielpfad neue und wichtige Dateien hinzugekommen sind. Freefilesync bietet grafische Kontrolle. Bei rsync sollte im Zweifel immer ein Testlauf vorausgehen. Statt daher sofort

```
rsync -avP --delete /home/ha/ /me
 dia/ha/Data/backup
```

zu spiegeln, kann man sich mit „--dry-run“ das voraussichtliche Ergebnis anzeigen lassen:

```
rsync -avP --delete --dry-run /
 home/sepp/ /media/user/USB-Data/
 backup
```

„--dry-run“ oder kurz „-n“ zeigt alle zu erwartenden Aktionen, ohne sie tatsächlich auszuführen. Um sich gleich auf die Löschaktionen zu konzentrieren, filtern Sie diese am besten gleich mit „ | grep deleting“ (einfach am Ende anhängen). Diese Kontrolle ist relativ fix, da keine Datenübertragung erfolgt. Ist dabei alles in Ordnung, können Sie den Befehl danach ohne „--dry-run“ abschicken.

Dateibearbeitung (5): Spezialist für Dubletten

In umfangreichen Dateisammlungen kommt es immer zu Dubletten – in verschiedenen Verzeichnissen oder auch im selben Ordner mit unterschiedlichen Namen. Unterscheiden sich die Dateinamen erheblich, dann ist es beinahe unmöglich, Dubletten manuell aufzuspüren. Für diese Aufgabe gibt es Fdupes. Unter Debian und Ubuntu ist die Einrichtung mit

```
sudo apt-get install fdupes
```

im Handumdrehen erledigt.

Fdupes vergleicht zunächst die Größen von Dateien in einem Verzeichnis sowie deren MD5-Checksumme. Um zufällige MD5-Kollisionen auszuschließen, unterzieht Fdupes die so ermittelten Kandidaten zusätzlich noch einem Bytevergleich, der sicherstellt, dass es sich tatsächlich um identische Dateien handelt.

Einen Verzeichnisbaum inklusive aller Unterordner durchsucht Fdupes mit diesem Kommando:

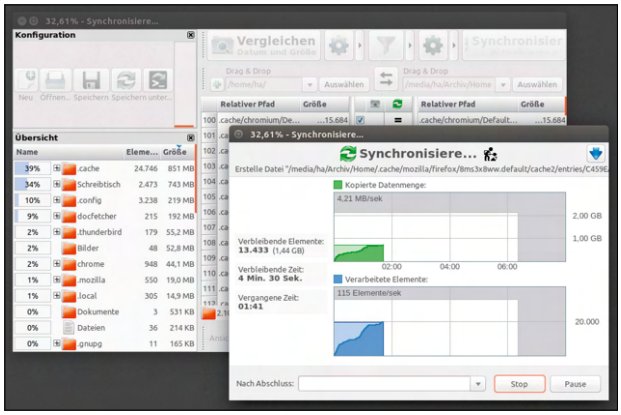
```
fdupes -r [Verzeichnis]
```

Das Tool zeigt den Fortschritt in Prozent an und präsentiert anschließend eine Liste doppelter Dateien mit kompletten Pfaden, wobei identische Dateien übersichtlich in Blöcken zusammengefasst sind.

Dateibearbeitung (6): Samba versus SSH

Aufräumarbeiten auf Linux-Servern via Netzwerk lassen sich natürlich auch auf Netzfreigaben – typischerweise über Samba – erledigen. Der effizienteste Weg ist das aber definitiv nicht, vor allem wenn diese Arbeiten viele Löschaktionen beinhalten. Umfangreiches Aufräumen ist über ein SSH-Terminal und damit direkt am Server erheblich schneller als mit der Vermittlung über Samba.

Hinzu kommen die nativen und in diesem Beitrag zum Teil beschriebenen Terminalmethoden, die direkter und schneller mit dem Linux-Dateisystem umgehen als etwa ein Windows auf einer Netzfreigabe. Aufräumen besser immer mit SSH!



Hübsches Backup- und Sync-Tool für Terminalfeinde: Freefilesync ist für private Nutzer und für Home-Office völlig ausreichend und bietet grafische Kontrolle über alle Aktionen.

Ordnernavigation

Ordnernavigation (1): Kommandozeile mit Ortskenntnis

Eine spezielle Variable „CDPATH“ ermöglich im Terminal den schnellen Wechsel in häufig benötigte Verzeichnisse. Die Variable kann mehrere Ordnerpfade speichern. Danach können Sie überall mit „cd [Verzeichnis]“ in ein Unterverzeichnis eines der gespeicherten Verzeichnisse springen.

Ein praktisches Beispiel: Unter „/var/www/html“ liegen einige Unterverzeichnisse des Webservers (etwa „logs“), die Sie häufig aufsuchen müssen. Um den Pfad in die Variable „„ aufzunehmen, geben Sie im Terminal

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

ein. Nun können Sie an beliebiger Stelle mit „cd htdocs“ und „cd logs“ direkt in die Verzeichnisse unterhalb „/var/www/html/“ wechseln, so als ob diese Unterverzeichnisse am aktuellen Ort wären. Dabei funktioniert sogar die automatische Pfadergänzung mit Tabulatortaste. Die Variable lässt sich durch eine beliebige Anzahl weiterer Verzeichnisse erweitern – jeweils durch Doppelpunkt getrennt:

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

Hier besteht der „CDPATH“ aus dem aktuellen Verzeichnis („.“), dem Home-Verzeichnis („~“), dem Webserververzeichnis und einem Mountordner. Es empfiehlt sich, mit „.:“, also dem aktuellen Verzeichnis zu beginnen, damit dieses bei gleichnamigen Ordnern immer die höchste Priorität behält. Für einen dauerhaften „CDPATH“ müssen Sie die Exportanweisung in die Datei „.bashrc“ eintragen.

Ordnernavigation (2): Im Terminal mit Popd

Die meisten Terminalnutzer verwenden cd für den Verzeichniswechsel. Die Alternativen pushd und popd bieten eigentlich mehr Komfort, vor allem dann, wenn es häufig von einem Ordner zum anderen und wieder zurückgehen soll. Daher sorgen folgende simplen Alias-Definitionen

```
alias cd='pushd'
alias +='pushd'
alias _='popd'
```

dafür, dass sich die Bash-Shell nach „cd“ oder „+“ grundsätzlich das letzte Verzeichnis merkt. Mit „_“ kehren Sie danach umstandslos wieder zurück zum letzten Verzeichnis. Das normale Minuszeichen („-“) ist als Alias-Kürzel nicht möglich.

Ordnernavigation (3): Farbige Dateien und Ordner

Das Terminal stellt Dateitypen und Ordner in unterschiedlichen Farben dar. Die Voreinstellungen müssen Sie nicht akzeptieren: Wenn Sie bestimmte Farben ändern möchten, erstellen Sie mit folgendem Befehl eine persönliche Konfigurationsdatei im Home-Verzeichnis:

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

Die versteckte Datei „.dircolors“ können Sie dann mit einem Editor öffnen und einzelne Farbdefinitionen umstel-

len, etwa Ordner gelb einfärben:

```
DIR 01;33
```

Die Einstellungen Ihrer persönlichen Farbtabelle dominieren dann dauerhaft über die Standardeinstellungen. Die Farbcodes sind unkomfortabel, aber im Web gut dokumentiert (siehe etwa *https://wiki.archlinux.de/title/Bash-Prompt_anpassen*).

Linux-Rechte

Linux-Rechte (1): Dateirechte anzeigen und ändern

Die Linux-Rechte für lokale Dateien und Ordner sind mit Schreiben, Lesen, Ausführen nicht wirklich kompliziert, aber es ist weder trivial, die bestehenden Rechte schnell zu erfassen, noch sie rational zu bearbeiten. Die symbolische Darstellung nach

```
ls -l
```

ist sehr unkomfortabel lesbar: Das erste Zeichen „d“ oder „-“ gibt wieder, ob es sich um ein Verzeichnis handelt. Danach folgen „rwx“ (die Rechte read, write, execute) des Besitzers, falls er diese besitzt. Bei einem fehlenden Recht steht ein „-“. Die nächsten drei Stellen „rwx“ zeigen die Rechte der Gruppe, falls diese solche besitzen. Die letzten drei Stellen zeigen schließlich die Rechte aller sonstigen Systemkonten.

Nach gewisser Gewöhnung besser lesbar ist die oktale Darstellung, welche die Rechte für Besitzer, Gruppe und Sonstige jeweils in einer Zahl zusammenfasst. Dabei gelten die folgenden Werte:

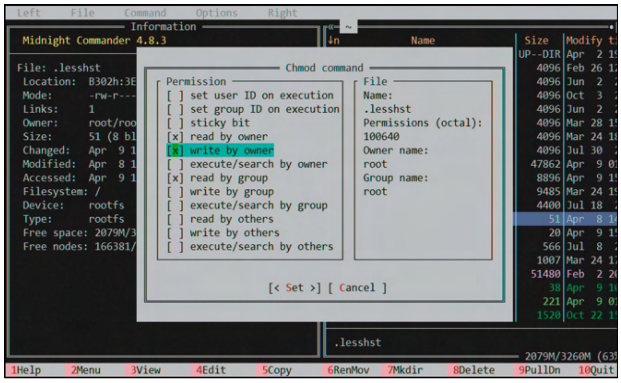
- Leserecht (Read) = 4
- Schreibrecht (Write) = 2
- Ausführen (Execute) = 1

Eine „7“ bedeutet also alle Rechte, eine „6“ Lese- plus Schreibrecht. Hat nun eine Datei insgesamt die oktale Rechtemaske „640“, so bedeutet das, dass der Besitzer sie lesen und ändern darf, die Gruppe aber nur lesen. Andere haben keinerlei Rechte.

Wer die oktale Schreibweise bevorzugt, kann sich diese in der Kommandozeile mit dem Tool stat anzeigen lassen. Folgender Befehl liefert in dieser Reihenfolge die oktalen Rechte (%a), den Besitzer (%U), die Gruppe (%G) und den Dateinamen (%n):

```
stat -c '%a %U %G %n' *
```

Dieser oder ein ähnlicher stat-Befehl wäre auch ein Kandidat für ein einfaches Alias.



Rechte und Rechteänderungen im Midnight Commander: Der Terminal-Dateimanager zeigt das Oktalformat der Dateirechte und bietet einen handlichen Chmod-Dialog.

Tipp: Mit das übersichtlichste und komfortabelste Tool, um Dateirechte zu sichten und zu ändern, ist der Midnight Commander. Wenn Sie im einen Fenster die normale Dateiliste verwenden und im anderen das Infofenster einblenden („Rechts | Links -> Info“ oder auch Tastenkombination Strg-X und Taste I), dann haben Sie für das markierte Dateiobjekt alle Infos einschließlich der oktalen Rechte vor sich. Über „Datei -> Chmod“ ändern Sie einzelne Rechte.

Die obersten drei „Zugriffsrechte“ sollten Sie außen vor lassen. Die darunter folgenden neun Rechte entsprechen den oben besprochenen für „owner“, „group“ und „others“.

Linux-Rechte (2): Execute-Bit für Scripts

Ausführbare Dateien unter Linux müssen in ihren Zugriffsrechten als ausführbar gekennzeichnet sein (Execute-Bit), andernfalls wird sie das System nicht starten. Diese Vorsichtsmaßnahme verhindert, dass Sie versehentlich heruntergeladene Scripts und Programme starten. Um eigene und vertrauenswürdige Scripts auszuführen, gibt es zwei Möglichkeiten. Der übliche Weg ist, den Dateirechten dauerhaft das Ausführen-Bit hinzuzufügen. Das kann sowohl der grafische Dateimanager („Eigenschaften -> Zugriffsrechte -> Ausführen“) als auch die Kommandozeile erledigen:



Um ein Script oder ein Programm auszuführen, müssen Sie dieses erst ausführbar schalten. Das erledigt wahlweise der Dateimanager oder chmod im Terminal.

```
sudo chmod +x [Dateiname]
```

Alternativ können Sie eine Script-Datei auch direkt mit dem Script-Interpreter starten, was bei kleinen und temporären Scripts praktisch ist, die Sie später nicht mehr benötigen. Um ein Shell-Script direkt zu starten, geben Sie einfach den Befehl

```
sh [Scriptname]
```

ein. Dies funktioniert auch mit Python- und Perl-Scripts („python [Scriptname]“ oder „perl [Scriptname]“). Das so ausgeführte Script muss nicht als „ausführbar“ markiert werden.

Linux-Rechte (3): Zugriffsrechte rekursiv ändern

Um in einem Ordner samt Unterverzeichnissen allen Dateien und Ordnern neue Zugriffsrechte zu geben, ist chmod das typische Werkzeug. Mit Parameter „-R“ berücksichtigt chown rekursiv alle Unterordner. Da chmod aber nicht zwischen Dateien und Verzeichnissen unterscheidet, ergibt sich

ein spezielles Problem: Das Execute-Recht (Ausführen) ist bei den meisten Dateien weder nötig noch erwünscht, bei Ordnern ist es hingegen fundamental: Entzieht man einem Benutzer das Recht zum „Ausführen“ eines Ordners, so lässt sich dieser nicht mehr öffnen.

Folglich brauchen Sie für rekursive Änderungen jeweils gesondert ein chmod für Ordner und Dateien mit unterschiedlichen Rechten. Hier hilft wieder das Universaltool find: Um alle Dateien für den Besitzer lesbar und beschreibbar zu machen, verwenden Sie diesen Befehl:

```
find . -type f -exec chmod 664 {}
 \;
```

Analog lässt sich find mit „-type d“ auf Verzeichnisse anwenden („directory“). Um alle Ordner und Unterordner „ausführbar“ zu machen und somit das Öffnen zu erlauben, geben Sie den folgenden Befehl ein:

```
find . -type d -exec chmod 775 {}
 \;
```

In diesen Beispiel beginnt die Aktion im aktuellen Verzeichnis („.“)

Linux-Rechte (4): Zugriffsrechte finden

Vor allem auf gemeinsam genutzten Servern sind allzu großzügige Rechte weder im Sinne des Datenschutzes noch der Datensicherheit. Sie können Dateien und Verzeichnisse mit unbeschränkten Zugriffsrechten einfach ausfindig machen. Erneut ist hier der Allesfinder find einschlägig, der mit Schalter „-perm“ nach oktalen Dateirechten fahndet. Das Kommando

```
find / -path /proc -type f -perm
 666
```

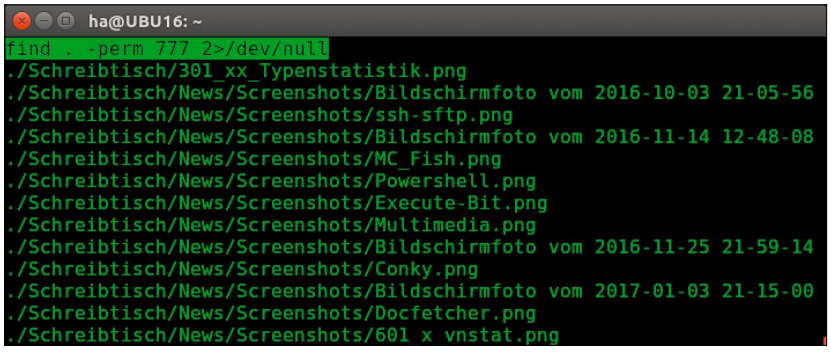
findet alle Dateien im gesamten Dateisystem (ausgenommen „/proc“), die von allen gelesen und beschrieben werden dürfen. Ferner listet

```
find / -path /proc -prune -o -type
 f -perm 777
```

alle Dateien auf, die dazu noch ausführbar sind. Genauso findet

```
find / -path /proc -prune -o -type
 d -perm 777
```

Verzeichnisse, die zum Lesen und Schreiben offenstehen.



Rechte kontrollieren: Der find-Schalter „-perm“ (Permissions) ermittelt alle Dateiobjekte der angegebenen Rechtemaske – hier „777“ für uneingeschränkten Zugriff für alle.

Linux-Rechte (5): Spezialattribut für Dateien und Ordner

Wer als root im Dateisystem unterwegs ist, sollte mit Löschaktionen besonders vorsichtig sein. Es gibt auf Linux-Dateisystemen ein zusätzliches Attribut, das Dateien und Verzeichnisse unveränderbar macht – zunächst auch für root. Der Befehl chattr kann erweiterte Attribute setzen und entfernen. Seine Verwendung ist root vorbehalten. Um beispielsweise eine Datei namens „config.php“ für alle Benutzer und Gruppen unlöschbar und unbeschreibbar zu machen, genügt dieser Befehl:

```
sudo chattr +i config.php
```

Der setzt das Bit „immutable“. Sogar root darf dann diese Datei nicht mehr ändern, solange das Bit mit chattr nicht wieder zurückgesetzt ist. Das Kommando

```
sudo chattr -i config.php
```

entfernt das Attribut wieder. Nützlich sind diese erweiterten Attribute bei wichtigen Konfigurationsdateien, aber auch dort, wo ein Systemprozess, der als root läuft, seine eigene Konfiguration nicht ändern soll.

Konvertierung

Konvertierung (1): Audio-CDs rippen

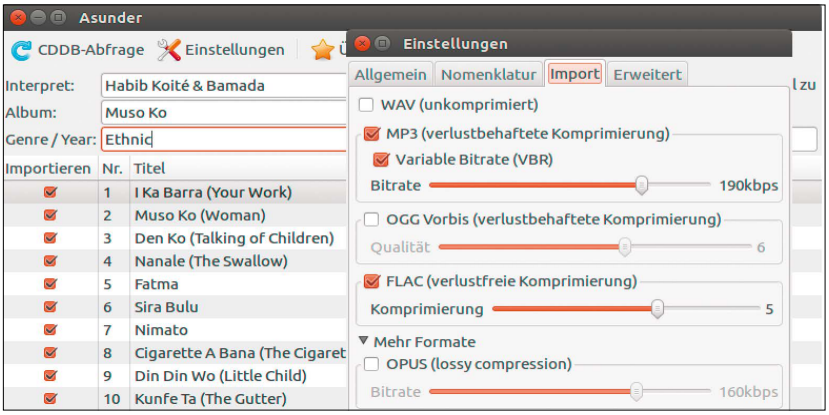
Die Musik auf Audio-CDs ist bereits digitalisiert. Unter Linux sehen Sie in den Ordnern der CD WAV-Dateien wie „Track 1.wav“ und „Track 2.wav“, die Sie einfach über den Dateimanager kopieren können. Für eine Musiksammlung ist es jedoch sinnvoll, den Dateien sprechende Namen zu geben und auch Metainformationen wie „Titel“ „Album“ und „Interpret“ darin unterzubringen. Ein Programm für diesen Zweck ist Asunder. Installieren Sie außerdem das Paket „lame“, wenn Sie MP3-Dateien erstellen möchten.

Legen Sie eine Audio-CD ein und starten Sie Asunder. Das Programm sucht automatisch nach Informationen zu der CD und zeigt die Titel der Musikstücke an. Klicken Sie auf „Einstellungen“ und legen Sie auf der Registerkarte „Allgemein“ den Zielordner fest. Auf der Registerkarte „Import“ setzen Sie Häkchen vor das gewünschte Dateiformat, etwa „MP3“ und/oder „FLAC“. Wenn Sie mehrere Formate aktivieren, erzeugt Asunder für jedes eine Datei. Übernehmen Sie die Änderungen per Klick auf „OK“. Mit einem Klick auf „Importieren“ starten Sie die Umwandlung.

Konvertierung (2): Audiodateien umwandeln

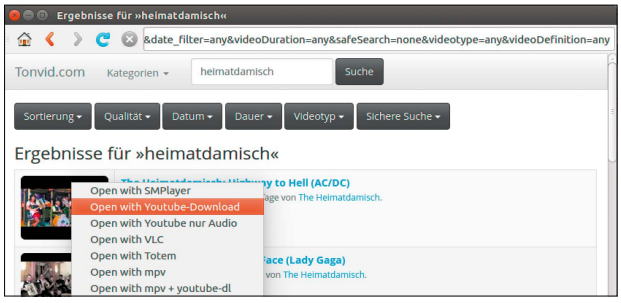
Zum Umwandeln von Audiodateien verwenden Sie das Programm Soundconverter und zusätzlich das Softwarepaket „gstreamer1.0-plugins-ugly“. Im Programm wählen Sie über „Dateien hinzufügen“ oder „Ordner hinzufügen“ diejenigen Dateien aus, die Sie umwandeln wollen.

Klicken Sie auf „Einstellungen“. Hier geben Sie den Ausgabeordner an, die Benennung der Zieldateien, das Zielfomat und Bitrate sowie Qualität. Klicken Sie auf „Schließen“, um die Einstellungen zu speichern. Mit einem



Audio-CDs umwandeln: Asunder liest die Dateien von der CD, holt Infos zum Inhalt aus dem Internet und speichert die Musik als Flac-, MP3- oder OGG-Dateien.

Youtube-Videos herunterladen: Mit der Kombination von smtube mit youtube-dl speichern Sie Youtube-Filme oder nur die Audioinhalte auf Ihrer Festplatte.



Klick auf „Umwandeln“ starten Sie den Prozess.

Konvertierung (3): Youtube-Videos herunterladen

youtube-dl ist ein Tool für die Kommandozeile, mit dem Sie Videos von Streaminganbietern wie Youtube herunterladen können. Es kann auch nur den Audioinhalt etwa von Musikvideos extrahieren. Installieren Sie zusätzlich das Paket „libav-tools“.

Um youtube-dl über eine grafische Oberfläche zu bedienen, können Sie zusätzlich das Paket „smtube“ installieren. Nach dem Start von smtube gehen Sie auf „View -> Settings“. Legen Sie per Klick auf die „+“-Schaltfläche einen neuen Eintrag an. Hinter „Name:“ tippen Sie „Youtube-Download“ ein und hinter „Executable:“ gehört „xterm“. Als „Parameters:“ verwenden Sie folgende Zeile

```
-e youtube-dl %u -o "~/
  Videos/%(title)s-%(id)s.%(ext)s"
```

Setzen Sie außerdem ein Häkchen vor „This player supports video sites“. Klicken Sie auf „OK“, um die Änderungen zu speichern. Sie benötigen nur den Audiostream eines Videos? Dann erstellen Sie über „+“ einen weiteren Eintrag nach dem gleichen Muster. Verwenden Sie hinter „Parameters:“ diese Zeile:

```
-e youtube-dl %u -x --audio-format
  mp3 -o "~/Musik/%(title)s-%(id)
  s.%(ext)s"
```

Suchen Sie in smtube nach dem gewünschten Video. Klicken Sie das Vorschaubild mit der rechten Maustaste an und wählen Sie im Menü „Youtube-Download“. Die Datei wird standardmäßig im Home-Verzeichnis unter „Videos“ gespeichert.

Konvertierung (4): Videoformate umwandeln

Mit Handbrake lassen sich Videos in den Formaten x264, MP4, AVI, OGM oder MKV in MPEG-4- oder MKV-Containern unterbringen. Dabei können Sie beispielsweise die Videocodecs h.264 oder h.265 verwenden. Handbrake bietet eine Liste mit Voreinstellungen, etwa „Android 480p30“ „iPad“ oder „Playstation 1080p30 Surround“. Die Neucodierung mit einer geringeren Auflösung ist immer mit einem Verlust bei der Bildqualität verbunden. Experimentieren Sie mit verschiedenen Einstellungen, um das optimale Format für Ihr Gerät zu finden.

Sie können Handbrake (Pakete: „handbrake“ und „handbrake-cli“) aus dem Ubuntu-Standard-Repository installieren. Informationen zu aktuelleren Versionen erhalten Sie über *https://handbrake.fr*. Diese bieten neben Optimierungen meist auch eine umfangreichere Liste mit Voreinstellungen. Ubuntu-Nutzer installieren die aktuellste Version über ein PPA. Dazu führen Sie folgende drei Befehlszeilen in einem Terminalfenster aus:

```
sudo add-apt-repository
  ppa:stebbins/handbrake-releases
sudo apt-get update
sudo apt install handbrake-gtk
  handbrake-cli
```

Für diesen Artikel nutzen wir die Version 1.0.3, die teilweise englischsprachige Menüs zeigt.

Die Verwendung von Handbrake ist einfach. Gehen Sie im Menü auf „Datei -> Open Single Title“ und wählen Sie die gewünschte Videodatei aus. Klicken Sie unter „Voreinstellungsliste“ auf das gewünschte Zielformat. Auf den Registerkarten unter „Ziel“ können Sie die Parameter für die Konvertierung individuell anpassen. Danach klicken Sie auf „Start Encoding“.

Konvertierung (5): Von Libre Office zu Text oder PDF

Der Writer von Libre Office bietet einen Schalter, um alle Dateien eines Ordners konvertieren. Die interessantesten Exportformate sind purer Text „txt:Text“ und PDF „pdf:writer_pdf_Export“ – im Prinzip:

```
libreoffice --writer --convert-to
  txt:Text *.odt
libreoffice --writer --convert-to
  pdf:writer_pdf_Export *.odt
```

Diese Optionen reichen aus, um alle Writer-Dokumente im gerade aktuellen Verzeichnis zu verarbeiten. Eine verzeichnisübergreifende Aktion erreichen Sie unter Zuhilfenahme von find:

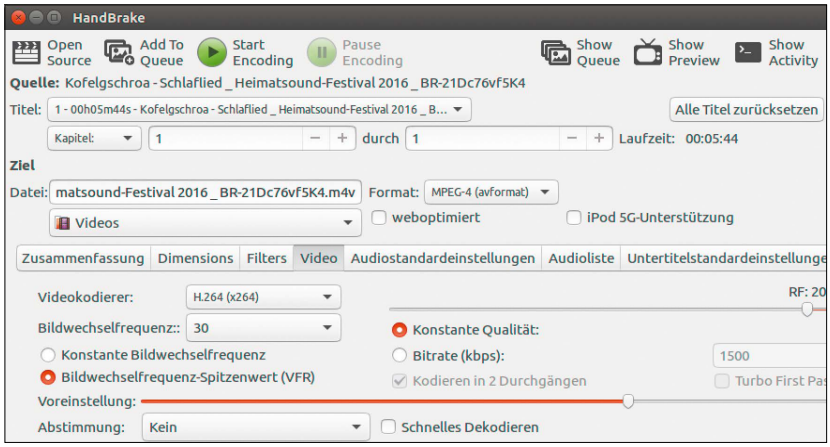
```
find . -type f -iname *.odt -exec
  libreoffice --writer --convert-
  to txt:Text {} \;
```

Der Nachteil: Diese Aktion versammelt alle konvertierten Dokumente im Ausgangspfad. Dies kann erwünscht sein, aber wenn die Exportdateien jeweils im Ordner der Quelldateien landen sollen, hilft nur ein kleines Bash-Script. Das abgebildete Script (siehe Abbildung rechts) ist so einfach wie möglich gehalten und vom Konzept her auch auf andere Aktionen übertragbar, wo find allein nicht ausreicht, weil sowohl Ordner- wie Dateinamen verarbeitet werden müssen.

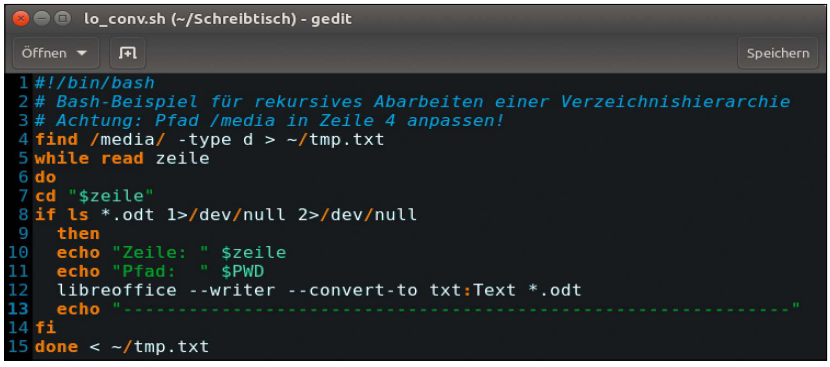
Kurzerklärung: find legt alle Verzeichnispfade in einer temporären Datei ab, die danach Zeile für Zeile mit der Variable „$zeile“ durchlaufen werden. Wo der ls-Befehl auf ODT-Dateien trifft, schlägt der Writer mit der Konvertierung zu.

Konvertierung (6): Bildformate umwandeln

Wer Hunderte von Fotos von einem Format in ein anderes übertragen will, kann Stunden mit stereotypen Klicks in einer Bildbearbeitung verbringen. Diese Aufgabe ist ein klarer Fall für ein Shell-Script. Notwendiger und nicht standardmäßig installierter Helfer ist dafür Imagemagick mit seinen Terminaltools, das mit dem gleichnamigen Paketnamen schnell nachinstalliert ist. In diesem Fall ist es dessen Tool convert, das den Job erledigt:



Video konvertieren: Handbrake überführt Videos in MP4- oder MKV-Container. Das Zielformat bestimmen Sie selbst oder Sie wählen es aus einer Voreinstellungsliste.



Alle Writer-Dateien in Text konvertieren: Das Script-Schema lässt sich auch auf andere rekursive Aufgaben übertragen, die in jedem Ordner eine bestimmte Aktion abarbeiten sollen.

```
#!/bin/bash
find . -iname "*.jpg" > ~/tmp.txt
while read zeile
do
echo $zeile
convert "$zeile" "${zeile%.*}.png"
 done < ~/tmp.txt
```

Das Script setzt voraus, dass Sie vor dem Script-Aufruf mit cd in das richtige Verzeichnis navigieren. Als Ausgangsformat ist hier JPG angenommen, als Zielformat PNG. Die konvertierten Dateien werden in denselben Ordner geschrieben.

Das geeignete Multimedia-Format

Musik und Filme können in unterschiedlichen Formaten vorliegen. Verbreitet sind MP3 bei Audio- und AVI, MKV oder MP4 bei Videodateien. Für die Wiedergabequalität ist die Bitrate entscheidend, bei Videos auch die Auflösung. Umso besser die Qualität, desto größer wird allerdings die Datei. Wer Videos auf dem Smartphone oder Tablet betrachten will, belegt dann viel vom meist knappen Speicherplatz. Außerdem kann die Wiedergabe ruckeln. In diesem Fall ist es sinnvoll, Videos speziell für mobile Geräte neu zu codieren.

AVI, MKV und MP4 sind Containerformate. Darin können mehrere Audio- und Videospuren untergebracht sein. Weit verbreitet ist die Kombination MP4/h.264 mit MP3-Tonspur. Andere Codecs, etwa h.265-Video und AC3-Audio, bieten teilweise eine bessere Qualität, aber nicht jedes mobile Gerät kann die Dateien ohne zusätzliche Software abspielen. Auf Linux-PCs können Sie hingegen fast jedes beliebige Format verwenden.

Bei MP3s ist die Dateigröße dank effektiver Komprimierung kaum ein Problem. Sind diese jedoch mit zu geringer Bitrate erstellt worden, hört sich das selbst für ungeübte Ohren nicht immer gut an. Daran lässt sich nachträglich nichts mehr ändern. Wer seine Audio-CDs archiviert, sollte besser ein Format mit verlustfreier Komprimierung wählen, beispielsweise Flac. Um auf dem Smartphone Platz zu sparen, können Sie die Flac-Dateien in MP3 oder OGG mit der gewünschten Bitrate umwandeln.

Defekte Hardware

Der Ausfall einer Hardwarekomponente ist kein Grund, ein Gerät abzuschreiben. PCs machen den Zugang zum Innenleben besonders leicht, aber auch viele Notebooks unterstützen den Tausch von Standardkomponenten.

Von **Hermann Apfelböck**

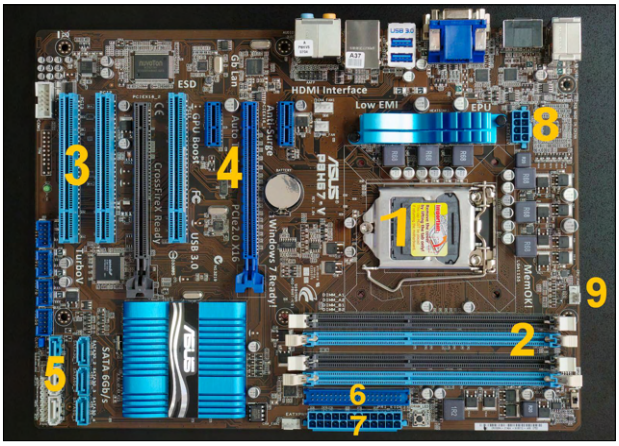
Hardwarefehler sind am einfachsten zu diagnostizieren, wenn insgesamt oder an bestimmter Stelle gar nichts mehr geht. Aber defekte Hardware kann sich auch diffuser äußern – mit Softwareabstürzen oder instabilem Netzwerk. Da hilft es dann gar nichts, an System und Software zu tunen: Einzige Abhilfe ist der Ersatz der Hardwarekomponente. Das Risiko, den Rechner zu beschädigen, ist minimal, die Gefahr freilich, falsche oder ungünstige Hardware einzukaufen, deutlich höher.

1. Wichtige Austauschkomponenten

Die Abbildung auf dieser Seite zeigt ein Mainboard mit wesentlichen Bauteilen. Abgesehen vom Austausch des Netzteils und des Mainboards bestehen typische Reparaturen darin, die alte Komponente vom Mainboard zu nehmen und die neue einzusetzen. Bei RAM, CPU, PCI-Karten, CMOS-Batterie ist es damit schon getan, Laufwerke, Lüfter und auch einige PCI-Karten benötigen zudem eine direkte Verbindung zum Netzteil.

Prozessor mit Lüfter (1): Der Prozessor ist auf dem Sockel mit Hilfe eines einrastbaren Metallbügels fixiert. Sockel und CPU werden in der Regel von einem CPU-Lüfter verdeckt.

Speicherbänke (2): Die zwei bis vier Bänke für RAM-Module können lediglich die von der Bauweise des Slots vorgegebenen RAM-Riegel aufnehmen. Der Einbau falscher Module ist physisch ausgeschlossen. Die Speicherriegel, heute meist DDR3 und DDR4 (DDR=Double Data Rate), haben je nach Typ Kerben an unterschiedlichen Stellen.



Die wichtigsten Mainboardstellen und Anschlüsse für den Komponententausch: Kurze Erläuterungen zu den Bauteilen finden Sie im Haupttext mit Angabe der Ziffer.

PCI-Erweiterungssteckplätze (3/4): Auf heutigen Mainboards finden Sie mindestens einen PCI-Slot (3) und mindestens einen längeren PCI-Express-Slot (4). PCI-Slots eignen sich für Peripherie wie Netzwerk-, TV- oder Soundkarten, während PCI-Express üblicherweise für die Grafikkarte genutzt wird.

SATA-Anschlüsse (5): SATA ist der aktuelle Übertragungsstandard zwischen Laufwerken und dem Prozessor. Hier schließen Sie Festplatten, SSDs und optische Laufwerke an. Die 40-Pin-Slots für alte IDE/PATA-Festplatten (6) sind auf jüngeren Boards nicht mehr vorhanden.

Mainboard-Stromstecker (7): Der 20- oder 24-polige ATX-Stromanschluss versorgt die Hauptplatine mit Strom. Der passende Stecker kommt vom ATX-Netzteil.

CPU-Stromstecker (8): Der Prozessor hat seine eigene Stromversorgung. Der achtpolige, eventuell quadratisch-vierpolige Stromanschluss für die CPU befindet sich in der Nähe der CPU. Der passende Stecker kommt vom ATX-Netzteil.

Lüfteranschlüsse (9): Für CPU- und Gehäuselüfter gibt es drei- oder vierpolige Anschlüsse, die mit „xxx_FAN“ beschriftet sind. Der CPU-Lüfter sollte aufgrund seiner Steuerungsoptionen im Bios immer an den Anschluss „CPU_FAN“.

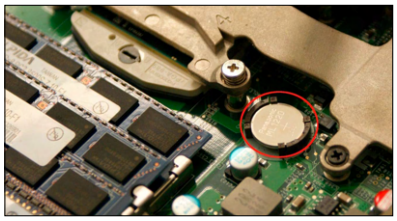
Hauptplatinen informieren mit Piepcodes oder Debug-LEDs über Probleme mit CPU, RAM oder Grafikchip. Die Erklärung der Codes finden Sie im Handbuch des Mainboards oder als PDF auf den Supportseiten des jeweiligen Herstellers.

2. Notebook- und Netbookakkus erneuern

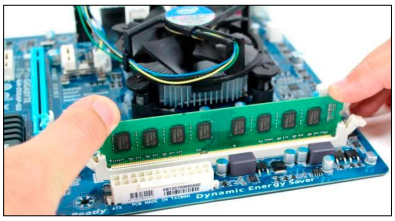
Beim Akkutausch genügen wenige Handgriffe. Typischerweise gibt es auf der Unterseite einen oder zwei Entriegelungshebel. Nach der Entriegelung lässt sich der alte Akku aus dem Gerät ziehen. Einzige Herausforderung ist es, den passenden Akku zu einem akzep-



Akku für Notebook und Netbook: Nach der Bestellung eines passenden Ersatzes genügen zwei Handgriffe.



CMOS-Batterie: In PCs ist der Austausch unkompliziert, bei Mobilgeräten wie Notebooks aber oft unzumutbarer aufwendig.



Einsatz von Speicher: Wenn die seitlichen Halterungen gut zugänglich sind, ist der Austausch von Speicherbausteinen einfach.

tablen Preis zu finden. Hier hilft eine Internetsuche mit der exakten Gerätebezeichnung oder noch präziser mit der Produktkennung, die der alte Akku zeigt. Dort finden Sie einen Aufkleber oder Aufdruck mit dem Hinweis „Replace with…“ und der Akkubezeichnung. Originalakkus kosten 50 Euro und (deutlich) aufwärts. Passende Nonameakkus, die Sie nicht über die Akkubezeichnung, sondern über die Gerätebezeichnung recherchieren, sind hingegen schon ab 30 Euro erhältlich. Umweltbewusste sollten etwas teurere Akkus wählen, die der EU-Richtlinie RoHS entsprechen (Restriction of Hazardous Substances).

3. Einsetzen einer Bios-Batterie

Die Hauptplatine besitzt eine Knopfzellenbatterie, damit die Bios/Uefi-Einstellungen auch bei abgeschaltetem Rechner erhalten bleiben. Die CMOS-Batterie wird im Gerätebetrieb stets aufgeladen und hält viele Jahre durch. Ist die Batterie am Ende, vergisst der PC permanent Uhrzeit sowie Boot- und Peripherieoptionen. Hinzu kommen Fehlermeldungen beim Systemstart wie „CMOS Read Error“. In solchen Fällen sollten Sie den PC ausschalten, vom Stromnetz trennen, das Gehäuse öffnen und die Knopfzelle ausfindig machen. Meistens handelt es sich um Lithium-Knopfzellen vom Typ CR2032 (3 Volt, 225-230 mAh). Ein flacher Schraubendreher genügt, um die alte Batterie herauszulösen. Da solche Batterien auch in Uhren und Kfz-Schlüsseln zum Einsatz kommen, sind sie ab 1,50 Euro in jedem Supermarkt und an Tankstellen zu finden. Auf Notebooks ist ein Batteriewechsel nicht so mühelos. Netbooks fordern oft sogar das Wegklappen der Tastatur und weiteren Komponentenausbau, wobei die Gefahr besteht, Kabelverbindungen zum Display oder Touchpad zu trennen. Wenn Sie dort die Batterie wechseln müssen, sollten Sie eine Anleitung im Internet suchen, die möglichst genau zu Ihrem Gerät passt.

4. Neuen Arbeitsspeicher einsetzen

RAM-Defekte manifestieren sich, wenn sie vornehmlich bei hoher Speicherauslastung auftreten. Gewissheit über den Zustand des Arbeitsspeichers verschaffen Sie sich mit Memtest86+ (auf Heft-DVD unter „Extras und Tools“). Defekte Module zu ersetzen ist sehr einfach. Es genügt, die seitlichen Halterungen nach außen zu klappen, die alten Module zu entnehmen und die neuen mit sanftem Druck einzulegen, bis die Halterungen einrasten. Die benötigte DDR-Generation (DDR, DDR2, DDR3, DDR4) und die Taktrate des Motherboards lassen sich im Bios oder auch unter Linux mit

```
sudo dmidecode --type 17
```

ermitteln. Idealerweise besitzen alle Speicherbausteine die Taktrate, wie sie der Chipsatz des Mainboards vorgibt. Schnellere Module sind kein Problem, arbeiten dann aber langsamer, als sie eigentlich könnten.

In engen Gehäusen liegen die Speicherbänke eventuell schlecht zugänglich unterhalb des Netzteils. In extremen Fällen scheiden technisch geeignete Module aufgrund ihrer Bauhöhe aus. Dies sollten Sie vorab prüfen.

Notebooks beherbergen statt Dimms kleinere SO-Dimms. Diese Speicherbausteine befinden sich auf der Unterseite der Notebooks und sind nach Entfernen einer Schraube leicht zugänglich. Schwierige Kandidaten sind Netbooks und Chromebooks: Hier ist von Modell zu Modell zu entscheiden, ob der Austausch die handwerklichen Fähigkeiten überfordert.

5. Die Grafikkarte ersetzen

Bleibt der Bildschirm schwarz, ist die häufigste Ursache ein loses Monitorkabel, denn HDMI- und unverschraubte DVI-Stecker sitzen nicht besonders fest. Hochwertige Grafikkarten haben zwei Problemfelder. Eines ist Überhitzung, die sich durch Bildfehler oder Abstürze äußert. Die Temperatur lässt sich unter Linux mit dem Terminaltool sensors überwachen. Dazu müssen Sie das Paket „lm-sensors“ nachinstallieren und mittels des Befehls

```
sudo sensors-detect
```

konfigurieren, wobei Sie alle Nachfragen mit „yes“ beantworten. Künftig geben Sie einfach *sensors* ein. Die Temperatur der Grafikkarte wird unter „PCI-Adapter“ angezeigt, eventuell auch mit Modellbezeichnung. Die Schwellenwerte „high“ und „crit“ bieten gute Orientierung.

Ein zweites Problem ist mangelhafte Stromversorgung der Grafikkarte. Zwar liefert manches Netzteil eine hohe Gesamtleistung, aber nicht genug Strom auf der 12-V-Leitung. In diesem Fall sind Abstürze oder ein schwarzer Bildschirm die Folge. Trifft das zu, so benötigen Sie ein leistungsstärkeres Netzteil (siehe Punkt 8).

Der Einbau einer neuen Grafikkarte ist einfach, sofern Mainboard und Gehäuse genügend Platz bieten. Aktuelle

Grafikkarten nutzen den (längeren) PCI-Express-Anschluss. Um die defekte Karte zu entfernen, müssen Sie bei den meisten Gehäusen zuerst die betreffende Schraube mit einen Schraubendreher entfernen. Danach lässt sich die Karte bei gleichzeitigem Drücken des kleinen Plastikhebels aus dem Slot ziehen. Die neue Karte drücken Sie senkrecht in den PCI-Express-Slot und setzen die Schraube wieder ein. Einfache Grafikkarten beziehen Strom via PCI-Slot, hochwertige benötigen Stromversorgung über einen sechspoligen Stecker, den jedes Netzteil vorsieht.

Einfache Grafikkarten kommen oft ohne aktiven Lüfter aus, fordern aber mit großen Passivkühlkörpern viel Platz. Eventuell wird dadurch der nächstgelegene PCI-Slot unbenutzbar.

6. Prozessor und Lüfter austauschen

Moderne PC-Hardware schützt die CPU vor kritischer Überhitzung, trotzdem kann ein System, das ständig heiß läuft, unberechenbar sein. Überprüfen Sie bei Systemen, die nach längerer Laufzeit instabil werden, die Temperatur von CPU, GPU und Hauptplatine. Unter Linux eignet sich das bereits genannte Tool sensors (im Paket „lm-sensors"). Wenn die Temperaturen schon im Normalbetrieb nahe 70 Grad liegen, schalten Sie den PC ab, öffnen das Gehäuse und überprüfen die Lüfter: Staub und Schmutz könnten die Luftzirkulation stören. Schalten Sie den Rechner bei geöffnetem Gehäuse ein, um zu sehen, ob die Lüfter überhaupt anlaufen.

Sind harmlosere Ursachen auszuschließen und der Prozessor veraltet oder dauerüberhitzt, benötigen Sie eine neue CPU, die zum Mainboardsockel passt. Läuft der Rechner im Prinzip noch, ist das Tool i-nex eine bewährte Hilfe, das Sie unter *https://launchpad.net/i-nex* als DEB-Paket für Debian/Ubuntu-Systeme erhalten. i-nex liefert detaillierte Infos zu CPU, GPU und Hauptplatine. Im Prinzip sollte aber auch der Befehl

```
sudo dmidecode -t 4
```

ausreichen, der die genaue CPU-Bezeichnung ermittelt, anhand derer Sie den Sockel im Web recherchieren können. Der CPU-Tausch ist an sich nicht schwierig und ohne Werkzeuge zu erledigen. Hindernisse können sich aber durch beengte Verhältnisse ergeben: So ist oft bei kleinen Gehäusen der direkte Zugriff auf die CPU ohne Ausbau anderer Komponenten nicht möglich. Bei ausreichendem Platz können Sie die alte CPU samt Kühler entnehmen. Ziehen Sie zunächst den Stromstecker des Kühlers ab (Anschluss „CPU-Fan"). Lösen Sie dann den Justierungshebel des CPU-Sockels und klappen Sie den Halterrahmen hoch.

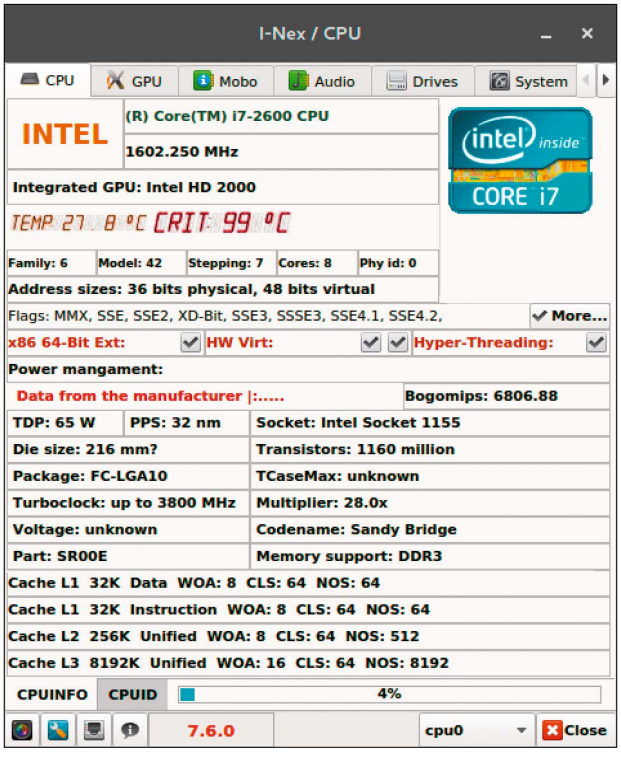
Die alte CPU lässt sich nun entnehmen. Den neuen Prozessor legen Sie so ein, dass sich die beiden Dreiecksmarkierungen auf dem Sockel und auf der CPU in derselben Ecke befinden. Dann lässt sich der Prozessor butterweich einsetzen.

Notebooks: Hier ist ein CPU-Wechsel mit Aufwand und Risiken verbunden. Zum Teil lässt sich der Prozessor nicht ausbauen, weil er mit der Hauptplatine verlötet ist. Recherchieren Sie im Internet nach einer seriösen Anleitung zu Ihrem Notebookmodell, um den Aufwand einschätzen zu können. In jedem Fall müssen Sie das Gerät aufschrauben und das Kühlsystem entfernen. Ob dies ohne Entnahme der Tastatur funktioniert, ist von Modell zu Modell verschieden. Den Notebookprozessor lösen Sie durch Drehen einer Schraube (Intel) oder Ziehen eines Hebels (AMD). Sobald Sie ein Knacken hören, können Sie die CPU herausnehmen und die neue einsetzen.

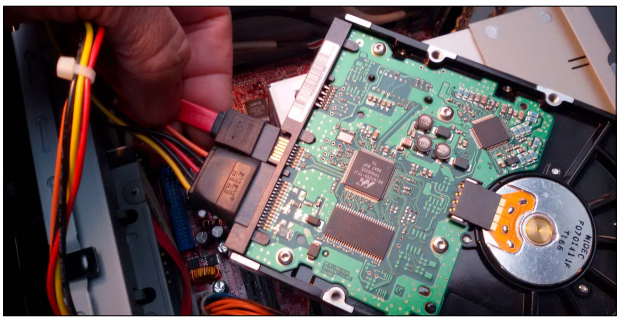
7. Defekte Festplatten und SSDs

Der Ausfall von Festplatten und SSDs gehört zu den schlimmeren Defekten, da er meist mit Datenverlust einhergeht. Beim Austausch eines Datenträgers mit der Systempartition ist darüber hinaus die Neuinstallation des Systems erforderlich. Anzeichen, dass ein Datenträger nicht mehr funktioniert oder sein Ableben naht, sind schleifende oder knackende Geräusche.

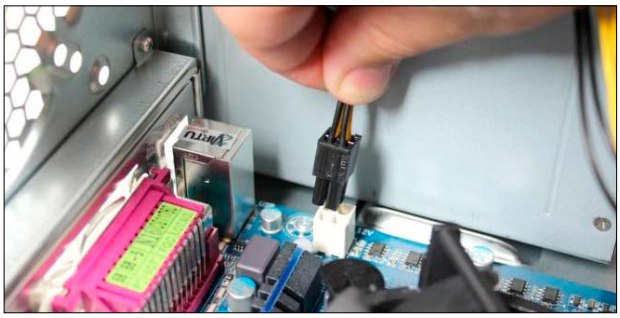
Vor allen anderen Maßnahmen sollten Sie das SATA-Kabel prüfen und eventuell auswechseln, selbst wenn es unbeschädigt scheint. Defekte SATA-Kabel sind Auslöser für Fehler aller Art. Lassen sich marode Kabel aus-



Prozessorinfos: Das Tool i-nex zeigt vor einem geplanten CPU-Tausch alle relevanten Daten inklusive Sockelbezeichnung.



SATA-Festplatte: Festplatten brauchen Strom vom Netzteil und die SATA-Datenverbindung zum Mainboard.



Einbau eines neuen Netzteils: Es gibt unscheinbare Stromstecker wie hier für die CPU, ohne die im Falle des Falles gar nichts geht.

schließen, dann überprüfen Sie die Festplatte mit dem Diagnosesystem SMART (Self Monitoring, Analysis and Reporting Technology). Unter Ubuntu & Co kann das etwa das Standardtool gnome-disks („Laufwerke"), das für ein markiertes Laufwerk die Option „SMART-Werte und Selbsttests" anbietet. Die Werte sind nicht einfach zu interpretieren: Anfänger können sich an der Spalte „Einschätzung" orientieren, die bei allen Kriterien „OK" lauten sollte. Der eigentliche Messwert steht in der Spalte „Wert". Eine hohe „Lesefehlerrate" ist ein ernstes Signal.

Hardwaretechnisch ist der Austausch von Festplatten und SSDs beim PC problemlos. Im typischen Fall sind Festplatten durch vier Schrauben im Gehäuse befestigt, die Sie lösen müssen. Nach Abziehen des SATA-Datenkabels und des Stromsteckers können Sie die alte Platte entnehmen, die neue einsetzen und mit Strom- und Datenkabel verbinden.

Bei vielen Notebooks geht der Austausch ebenfalls einfach von der Hand, da Sie nur eine Abdeckung auf der Unterseite entfernen müssen. Hier werden kleinere mechanische Laufwerke oder SSDs mit 2,5 Zoll eingebaut.

Heikler ist der Ersatz von SSD-Speicher im stark variierenden M.2-Format. Diese Speichermedien ähneln eher einem RAM-Modul und benötigen keinen zusätzlichen Stromanschluss. Welche M.2-SSD passt, müssen Sie im Gerätehandbuch, beim Hersteller oder anhand des alten Moduls recherchieren.

8. Defektes ATX-Netzteil austauschen

Netzteile verabschieden sich selten aufgrund von Defekten. Arbeitende, aber überlastete Netzteile sind aber nicht selten – vor allem nach Aufrüsten des PCs mit Grafikkarte oder leistungsstärkerer CPU. Wenn der Rechner gar keinen Mucks mehr macht, überprüfen Sie den Hauptschalter auf der Rückseite des Netzteiles und den Sitz des Stromnetzanschlusskabels.

ATX-Netzteile für PCs haben Normmaße und passen in jeden PC. Schwieriger ist die Entscheidung, welche Leistung das Netzteil erbringen muss. 500 Watt sind für Büroaufgaben ausreichend, für Spielerechner etwa 750 Watt. Es handelt sich um Maximalwerte, nicht um den Durchschnittsverbrauch.

In großen Towergehäusen müssen manche Kabel bis zu 50 Zentimeter zum Peripheriegerät überbrücken. Billignetzteile sind für solche Distanzen nicht ausgelegt. Die Länge des Kabelstrangs zu recherchieren, ist allerdings selbst bei vorbildlichen Onlineshops kaum möglich. Im Zweifel sollten Sie direkt im Laden einkaufen.

Der Austausch des Netzteils ist zeitaufwendig, aber nicht schwierig. Als Werkzeug genügt ein Kreuzschlitzschraubendreher. Ziehen Sie vor dem Ausbau alle Kabel ab, wobei sich Unerfahrene am besten jede Komponente notieren. Andernfalls werden später unscheinbare, aber unentbehrliche Stecker leicht übersehen, so etwa der zweipolige Anschluss für den Powerknopf oder der CPU-Stecker.

9. Mainboards auf Fehler prüfen und ersetzen

Der erste Schritt ist die Suche nach physikalischen Beschädigungen. Eindeutig sind aufgeblähte Kondensatoren der Spannungsregler neben der CPU. Ist nichts zu finden, bauen Sie die Hauptplatine aus. Verbogene Bleche und lose Schrauben hinter der Platine können einen Kurzschluss ausgelöst haben. Danach erfolgt ein Rückbau mit den absolut notwendigen Komponenten – CPU, ein RAM-Modul im ersten Slot und eine Grafikkarte, sofern kein Onboardchip vorhanden ist. Tut sich auch in dieser Minimalkonfiguration nichts, obwohl das Netzteil in Ordnung ist, ist die Hauptplatine wahrscheinlich defekt.

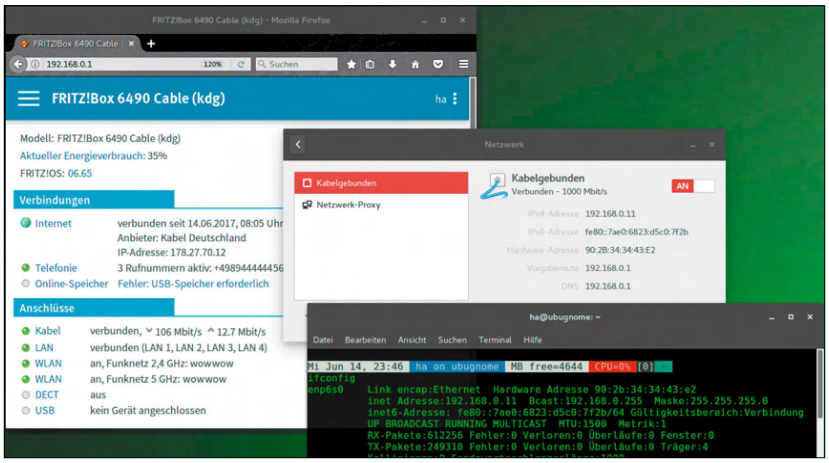
Der Austausch von Mainboards ist aufwendig, da sich sämtliche Aktionen hinzuaddieren, die dieser Beitrag angesprochen hat. Sind alle Komponenten entnommen, ist das Board nach dem Lösen einiger Gewindeschrauben aus dem Gehäuse zu entnehmen.

Beim Kauf des neuen Mainboards müssen Sie den richtigen Formfaktor ermitteln. Das verbreitete ATX-Format kennt mittlerweile ein halbes Dutzend Varianten für unterschiedliche Gehäusegrößen. Wenn Sie die bisherigen Komponenten wie CPU und RAM auf der neuen Platine weiternutzen wollen, brauchen Sie ein Board mit dem richtigen CPU-Sockel, mit den passenden Speicherbänken sowie dem passenden Bustakt. Die übrige Boardausstattung ist unkritisch, sofern sie keine Antikhardware wie IDE-Festplatten oder AGP-Grafik unterstützen muss. ●

Netzwerkprobleme lösen

Netzwerke bestehen aus diversen Hard- und Softwarekomponenten. Entsprechend komplex sind die Ursachen bei Netzwerkproblemen. Mit systematischer Fehlersuche grenzen Sie Fehler ein und reparieren an der richtigen Stelle.

Von **Hermann Apfelböck**



Wenn der Browser keine Webseiten mehr anzeigt oder der Zugriff auf den Datenserver nicht mehr klappt, dann ist die Fehlersuche nicht immer einfach. Der Fehler kann vorübergehend beim Internetprovider liegen. Der DSL-Router kann ebenso schuld sein wie Verkabelung, Switch oder der Netzwerkadapter des PCs. Nicht zuletzt gibt es Softwareeinstellungen im Betriebssystem und im Browser, die Netz und Web blockieren. Hier hilft nur systematisches Vorgehen.

1. Netzwerkadapter des Rechners prüfen

Aktuelle PCs und Notebooks besitzen Onboard-Netzadapter auf der Hauptplatine. Neben der Netzwerkbuchse sehen Sie meist zwei LEDs. Die grüne LED leuchtet, wenn Verbindung zu einem Netzwerk besteht, die orangefarbene blinkt, wenn Daten übertragen werden. Bei Notebooks gibt es in der Regel keine LEDs an der Ethernet-Buchse und USB-WLAN-Adapter sind meist mit nur einer LED ausgestattet: Sie leuchtet, wenn der Treiber geladen und der Adapter aktiv ist, und blinkt bei Übertragungsaktivität.

Wenn die grüne LED nicht leuchtet, probieren Sie mit einem anderen PC oder Notebook aus, ob die Netzwerkverbindung funktioniert. Wenn auch hier nichts geht, sollten Sie das Verbindungskabel vom PC zum DSL-Router austauschen. Andernfalls ist der Fehler beim PC zu suchen. Prüfen Sie im Bios, ob der Netzwerkadapter überhaupt aktiviert ist. Die Einstellungen finden Sie meist unter „Integrated Peripherals“ oder „Advanced“. Bei Notebooks lässt sich der WLAN-Adapter häufig über eine Spezialtaste oder einen Schalter am Gerät aktivieren.

Treiber und Konfiguration: Wenn die grüne LED leuchtet, die gelbe aber nicht, ist der Fehler eher bei der Software zu suchen. Ob Linux den Netzwerkadapter erkannt hat, ermitteln Sie auf der Kommandozeile:

```
ifconfig
```

Die Ausgabe zeigt bei Kabelverbindungen Informationen zu „eth0“ (oder „enp6s0“). bei WLAN-Verbindungen zu „wlan0“ (oder „ra0“). Dahinter steht jeweils die IP-Adresse für IPv4 („inet“) und IPv6 („inet6“). Taucht „eth0“ zwar auf, aber ohne IP-Adresse, dann klappt die Verbindung zum Router nicht. Prüfen Sie in diesem Fall die Verkabelung.

Passt die IP-Adresse nicht zum Router-Adressraum, ist vermutlich ein zweiter DHCP-Server aktiv. Prüfen Sie bei anderen Geräten wie etwa Access Points, ob dort DHCP aktiviert ist: In einem Netzwerk darf es immer nur einen DHCP-Server geben. Meldet ifconfig nur den Loopback-Adapter „lo“, dann ist kein Treiber für den Netzwerkadapter geladen. In diesem Fall erscheint in der Systemleiste auch kein Symbol des grafischen Netzwerkmanagers. Während Ethernet-Adapter vom Linux-Kernel durchgehend gut unterstützt werden, funktionieren unter Linux nicht alle USB-WLAN-Adapter, weil Treiber fehlen.

Am einfachsten gehen Sie Treiberproblemen aus dem Weg, indem Sie schon vor dem Kauf eines WLAN-Ad-



WLAN-USB-Dongle CSL 300: Dieser Funknetzadapter bietet für wenig Geld sorglosen Zugang zum Drahtlosnetzwerk unter Linux.

apters ermitteln, ob Linux das Produkt unterstützt. Empfehlenswerte USB-Adapter sind etwa Edimax EW-7811UN Wireless, Asus N10 Nano WLAN-Stick, CSL 300 Mbit/s USB 2.0 oder Fritz Wlan USB Stick-N v2.4 (Preise ab circa sieben bis 23 Euro).

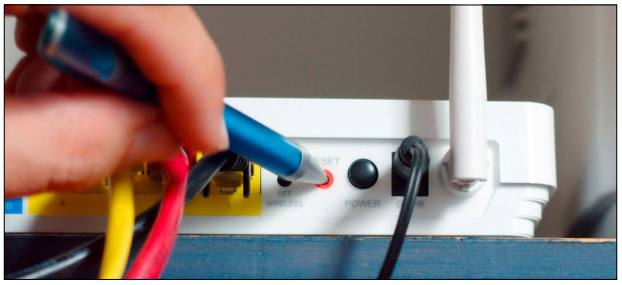
2. Verbindung zum Router testen

Das wichtigste Gerät im Netzwerk ist der DSL-Router oder das Kabelmodem. Diese Geräte verbinden das öffentliche Internet mit dem lokalen Netz in Ihrer Wohnung. Der Router dient meist auch als WLAN-Access-Point und als DHCP-Server für die Verteilung der IP-Adressen (Dynamic Host Configuration Protocol). Ein Router mit der IP-Adresse „192.168.0.1“ vergibt IP-Adressen aus dem Bereich 192.168.0.2 bis 192.168.0.254 an die Geräte.

Dabei übermittelt er auch die Standard-Netzwerkmaske 255.255.255.0 und die Adressen des Standardgateways und des DNS-Servers (beide in der Regel identisch mit der IP-Nummer des Routers).

Prüfen Sie bei allen Netzwerkproblemen zu allererst, ob der Router mit Strom versorgt ist, ob die LEDs leuchten (Internet, LAN, WLAN) und ob der Router erreichbar ist. Geben Sie im Browser die IP-Adresse des Routers ein, typischerweise „192.168.1.1“ oder „192.168.178.1“ (Fritzbox). Die Router-IP ermitteln Sie im Zweifel auch über *ifconfig* im Terminal, wobei Sie die letzte Zahl der Rechner-IP („inet -Adresse“) durch die „1“ ersetzen.

Wenn die Verbindung zum Router nicht funktioniert, also die Konfigurationsseite des Routers nicht im Browser erscheint, gibt es dafür mehrere Ursachen: Der Router ist falsch konfiguriert oder defekt, das Netzwerkkabel ist locker oder defekt oder der Netzwerkadapter des zugreifenden Geräts ist inaktiv. Um Sicherheit zu erhalten, nehmen Sie den Router vom Stromnetz und schließen ihn erneut an. Wiederholen Sie den Routerzugriff am besten mit einem anderen Gerät. Wenn auch dies nicht funktioniert, sollten Sie jegliche zusätzliche Fehlerquellen wie



Routerreset nur im äußersten Notfall: Das setzt den Router auf den Werkszustand zurück und verwirft alle Einstellungen.

WLAN, Switches, Ethernet-Kabel, Powerline ausschließen: Verbinden Sie einen Rechner direkt mit dem Router und wiederholen Sie den Versuch.

Funktioniert auch das nicht, bleibt noch die Chance, dass eine Fehlkonfiguration durch einen Routerreset zurück auf die Werkseinstellungen korrigiert werden kann. Bei einigen Modellen gibt es einen Resetknopf, bei den meisten muss auf der Rückseite ein spitzer Gegenstand für einige Sekunden in ein kleines „Reset“-Loch gedrückt werden. Der Reset löscht alle Konfigurationseinstellungen, macht aber das Gerät mit den Standardeinstellungen wieder funktionsfähig, sofern kein technischer Defekt vorliegt.

3. Die Konfiguration des Routers prüfen

Wenn der Router arbeitet, erhalten alle Netzwerkgeräte per DHCP eine lokale IP-Adresse. Das lokale Netz sollte daher in jedem Fall funktionieren, folglich auch der Aufruf der Routerkonfiguration im Browser. Falls dies scheitert, können Sie notfalls manuell eine IP-Adresse anfordern (siehe -> Punkt 4). In der Konfigurationsoberfläche können Sie prüfen, ob der DHCP-Dienst eingeschaltet ist, und ihn gegebenenfalls aktivieren. In der Fritzbox ist dazu die „erweiterte“ Ansicht erforderlich. Gehen Sie anschließend im Menü auf „Heimnetz -> Netzwerkeinstellungen -> IPv4-Adressen“. Hier muss das Häkchen vor „DHCP-Server aktivieren“ gesetzt sein.

Unter „Heimnetz -> Netzwerk -> Geräte und Benutzer“ erscheinen oben mit einer grünen Markierung alle Geräte, die aktuell mit der Fritzbox verbunden sind („Aktive Verbindungen“). Darunter stehen frühere Verbindungen („Ungenutzte Verbindungen“). Sollte unter „Aktive Verbindungen“ ein derzeit angeschlossenes Gerät fehlen, dann ist der Fehler bei diesem Gerät zu suchen.

WLAN-Einstellungen: Alle WLAN-Geräte, die sich mit dem Funknetz des Routers verbinden wollen, müssen die gleiche Verschlüsselungsmethode und das im Router eingestellte Kennwort verwenden. In der Regel sollte WPA2-Verschlüsselung aktiv sein. Bei einer Fritzbox finden Sie die Einstellung und



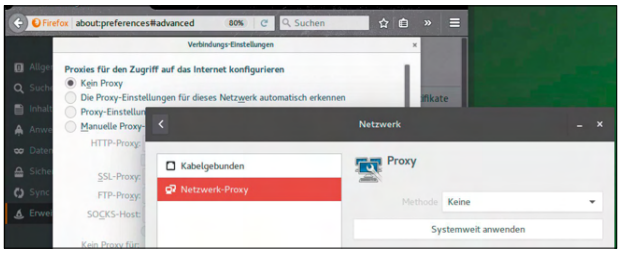
WLAN-Zugang: Alle Clientgeräte müssen Verschlüsselungsmethode und Kennwort des Routers nutzen – es sei denn, es gibt weitere WLAN-Access-Points mit anderen Vorgaben.

das Zugangskennwort unter „WLAN -> Sicherheit“. Stellen Sie bei den Netzwerkgeräten ebenfalls WPA2 ein.

Internetverbindung: Jeder Router zeigt an, ob eine Verbindung zum Provider besteht. Dies ist Voraussetzung für die Internetbenutzung. Bei einer Fritzbox sehen Sie auf der Übersichtsseite unter „Verbindungen“ den Eintrag „Internet“ und daneben „verbunden seit“, andernfalls „nicht verbunden.“ Konnte keine Verbindung zum Internetanbieter aufgebaut werden, prüfen Sie, ob die Anmeldeinformationen unter „Internet -> Zugangsdaten“ stimmen. Der Fehler muss aber nicht bei Ihnen liegen, vielleicht ist aktuell der Anschluss in Ihrer Region gestört. Alle großen Internetprovider bieten eine Website mit aktuellen Störungsmeldungen, die Sie in diesem Fall aber nur über das Mobilnetz Ihres Smartphones erreichen.

4. IP-Adresse manuell anfordern

Auch wenn die Netzwerkhardware funktioniert, wird ein Gerät erst durch seine IP-Adresse zum Netzwerkbeitritt befähigt. Die erhält es automatisch via DHCP, sofern DHCP im Router aktiv ist. Wenn nicht, entsteht eine Sackgasse: Der Rechner erhält keine IP, kann folglich die Konfigurationsoberfläche des Routers nicht laden und somit auch DHCP nicht einschalten. In diesem Fall müssen Sie im Netzwerkmanager die „IPv4“-Einstellungen aufsuchen, statt „Automatisch (DHCP)“ die Option „Manuell“ wählen und dann Adresse, Netzmaske, Gateway und DNS-Server eintragen. Die „Netzmaske“ lautet standardmäßig 255.255.255.0. „Gateway“ und „DNS-Server“ sind identisch, nämlich die lokale IP-Adresse des Routers. Diese und damit den resultierenden lokalen Adressraum zu kennen, ist hier unerlässlich, weil es keine Möglichkeit gibt, dies abzufragen. Typisch für die Fritzbox ist „192.168.178.1“, viele andere Router verwenden „192.168.1.1“ oder „192.168.0.1“. Im Zweifel helfen ein Reset des Routers auf Werkseinstellungen und dann der Blick ins Routerhandbuch, das die Standard-IP mitteilt.



Bei Direktverbindung zum Provider „Kein Proxy“: Ein vergessener Proxyserver in der Konfiguration kann den Webzugang lahmlegen.

Die manuell angeforderte IP des Rechners selbst ergibt sich aus der IP-Adresse des Routers: Ist diese etwa „192.168.178.1“, dann können Sie für den Rechner jede Endziffer von 2 bis etwa 250 verwenden, also etwa die IP „192.168.178.100“.

5. Lokales und öffentliches Netzwerk testen

Nach den bisherigen Tests wissen Sie, ob der Adapter funktioniert, ob der DSL-Router erreichbar ist und ob der Netzwerkadapter eine IP-Nummer aus dem IP-Bereich des Routers erhalten hat. Geben Sie auf der Kommandozeile folgenden Befehl ein:

```
ping 192.168.178.1
```

Die IP-Nummer im Beispiel ersetzen Sie durch die tatsächliche des Routers. Der Router wird die Anfrage mit „64 bytes from 192.168.178.1…“ beantworten. Wo immer dies der Fall ist, sollten Sie mit derselben IP auch die Konfigurationsoberfläche des Routers im Browser erreichen (einfach im Adressfeld eingeben).

Den Internetzugang testen Sie etwa mit *ping google.de*. Wie im lokalen Netzwerk erhalten Sie eine Antwort in der Form „64 byte from“. Wenn solches ping erfolgreich war, dann steht die Internetverbindung und die Namensauflösung über DNS (Domain Name System), denn Sie haben nicht die IP-Adresse, sondern den Domainnamen „google.de“ abgefragt.

Nicht alle Webdomains beantworten Pinganfragen. Wer ganz sicher gehen will, verwendet mit

```
traceroute google.de
```

eine Routenverfolgung zum Zielserver, die bei intakter Internetverbindung in jedem Fall funktioniert. Traceroute kann unter Debian-basierten Systemen mit *sudo apt install traceroute* nachinstalliert werden.

Internetbrowser und Proxy: Zeigt der Browser trotz dieser erfolgreichen Tests keine Webseiten, dann haben Sie kein Internet-, sondern ein Browserproblem. Das tritt gelegentlich bei Notebooks auf, die Sie in anderer Umgebung umkonfigurieren mussten, um dort ins Internet zu kommen. Während öffentliche Einrichtungen und Firmen über einen Zwischenserver (Proxy) ins Internet gehen, nutzen Sie zu Hause in aller Regel eine Direktverbindung zum Provider.

Hier muss die Proxykonfiguration folglich wieder gelöscht werden. Der Netzwerkmanager zeigt unter den LAN-Einstellungen einen Eintrag „Netzwerk-Proxy“, der deaktiviert sein sollte. Der Firefox hat zusätzlich eine unabhängige Proxykonfiguration unter „Einstellungen -> Erweitert -> Netzwerk -> Verbindung -> Einstellungen“. Auch hier sollte die Option „Kein Proxy“ gelten.

6. Peripheriegeräte wie Scanner und Drucker

Wenn Netzwerkdrucker den Dienst verweigern, gibt es dafür zahlreiche Ursachen wie Papierstau oder ein angefordertes Seitenformat, das dieser nicht unterstützt.

Bei Netzwerkgeräten, die über Ethernet oder WLAN arbeiten, wird dabei gerne eine noch trivialere Fehlerursache übersehen: Weiß das Gerät überhaupt, dass es arbeiten soll? Daher sollten Sie prüfen, ob der Router LAN und WLAN per LED anzeigt, ferner ob das Gerät selbst eine Netzverbindung meldet. Wer gut organisiert ist, kann den kleinen Webserver

solcher Geräte per Browserlesezeichen aufrufen und sieht dann sofort, ob der Drucker oder Scanner online ist. Ist das Gerät offline, hilft in der Regel abschalten und neu starten. Wenn ein Gerät über WLAN arbeitet und die Zugangsdaten zum Funknetz „vergessen“ hat, hilft nur der vorübergehende Anschluss ans Kabelnetz und erneutes Eintragen des SSID-Funknetznamens inklusive Zugangsdaten.

7. Funknetze optimieren

Die Antennen von WLAN-Routern arbeiten als Rundstrahler, die horizontal in alle Richtungen die gleiche Sendeleistung abgeben. Andere Stockwerke werden vertikal schlecht versorgt. Außerdem wird das Signal durch Wände und Möbel gedämpft. Eine leichte Neigung der Antennen oder Positionsänderung des Routers kann große Auswirkungen auf die Signalqualität haben. Vor allem lohnt der Versuch mit unterschiedlichen Antennenwinkeln, wenn auch andere Stockwerke abgedeckt werden sollen.

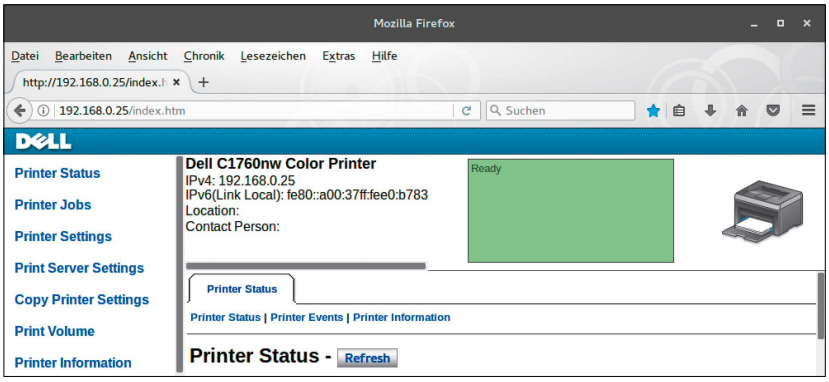
Zum Ermitteln der besten Ausrichtung eignet sich auf einem Linux-Notebook das Tool LinSSID. Es zeigt alle Funknetze in Reichweite mit Kanal und Sendeleistung. DEB-Pakete für Debian- und Ubuntu-Distributionen gibt es auf der Projektwebseite (*http://sourceforge.net/projects/linssid/files/*).

Aber es geht auch noch einfacher in der Kommandozeile: Das WLAN-Signal wird in der Datei „/proc/net/wireless“ protokolliert, die Sie so in kurzen Abständen anzeigen können:

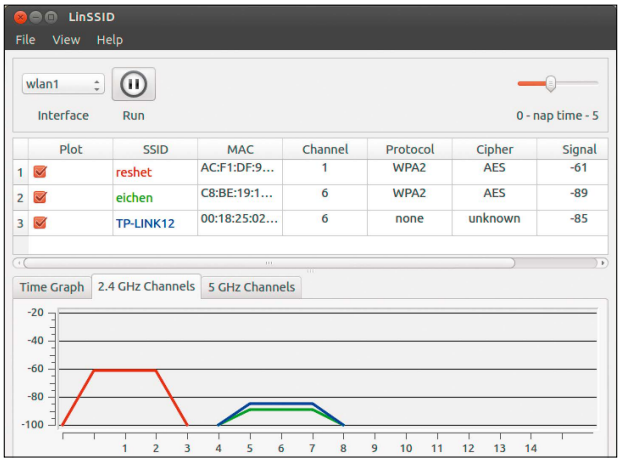
```
watch -n cat /proc/net/wireless
```

Der Wert von „link“ in der Spalte „Quality“ zeigt die Signalqualität an.

Wenn die Sendeleistung des Router trotz allem nicht genügt, sollten notorisch unterversorgte Funknetzbereiche dennoch kein Thema sein: Repeater sind eine Hilfe, weit besser sind Powerline-Adapter, die es auch mit Wi-Fi-Sender gibt (Devolo Starterset ab circa 70 Euro). Wo Ethernet verlegt ist, kann ein zusätzlicher Access Point funken (ab 30 Euro).



Weboberfläche eines Netzdruckers: Wenn Sie die IP-Adressen Ihrer Netzgeräte als Lesezeichen im Browser ablegen, wissen Sie mit einem Klick, ob das Gerät online ist.



WLAN-Übersicht: Um zu sehen, welche Netzwerke mit welcher Signalstärke auf welchem Kanal in Reichweite liegen, eignet sich das Tool LinSSID.

8. Ursachen für instabiles Netzwerk

Ein konstant langsames Netzwerk ist unbefriedigend, aber technisch oft fehlerlos. Eine echte Herausforderung ist ein instabiles Netz mit typischen Symptomen: Der Router wirft Rechner immer wieder aus dem Netz, das Netz ist eine Minute pfeilschnell und hängt dann wieder komplett. Neustarts des Routers oder des Geräteadapters schaffen nur kurzzeitig Abhilfe. Solche Szenarien sprechen für ein Hardwareproblem, das Sie eingrenzen müssen.

- Am einfachsten ist es, wenn die Aussetzer lediglich bei einem Gerät auftreten: Halten Sie sich dann nicht mit Softwareeinstellungen im Netzwerkmanager auf, denn Konfigurationsfehler produzieren klarere Problembilder. Hier hilft in der Regel nur der Austausch des Netzadapters.
- Funktioniert der Router immer erst nach einem Reset wieder eine Zeitlang korrekt, dann prüfen Sie, wie heiß das Gerät ist. Handwarm ist normal für Router im Dauerbetrieb. Sorgen Sie für ausreichend Belüftung, etwa indem Sie den Router auf Holzklötze stellen oder unter Papierbergen ausgraben. Ein Problem von älteren Routern sind defekte Kondensatoren auf der Platine. Nach unserer Erfahrung sind Internetanbieter bei Defekten oft großzügig und schicken kostenlos oder günstig Ersatz.
- Treten die Netzwerkhänger ab einer bestimmten Weiche (aber nicht vorher) bei allen Geräten dahinter auf, dann können Sie Adapterprobleme am Einzelgerät ausschließen. Entweder ist das Netzwerkkabel zur bewussten Weiche beschädigt oder der Verteilerswitch am Ende der Strecke. Beides ist nur durch Austausch dieser Komponenten zu verifizieren. Dasselbe gilt auch für eventuelle Brücken mit Powerline-Adapter. ●

Starthilfen für den Bootloader

Linux-Systeme nutzen den Bootloader Grub 2, der sich bei Parallelinstallation auch um den Start anderer Systeme wie Windows kümmert. Insbesondere nach Windows-Installationen ist stets eine Reparatur dieses Bootloaders nötig.



Von **David Wolski**

Der Verlust des Linux-Bootloaders Grub 2 auf einem System ist ärgerlich, aber keine Katastrophe. Auf reinen Linux-Systemen mit einem installierten System sind Bootloader-Probleme selten. Denn die verbreiteten Linux-Distributionen suchen schon bei der Installation die Datenträger nach bereits vorhandenen Betriebssystemen ab und berücksichtigen diese dann bei der Einrichtung des Bootloaders. Umgekehrt ist das nicht Fall: Windows ignoriert bei einer Parallelinstallation sämtliche, eventuell schon vorhandene Linux-Systeme auf einem PC. Deren Grub-2-Bootloader wird komplett mit dem Windows-Bootloader ersetzt, der nur Windows-Systeme booten will.

Der Verlust des Linux-Bootmanagers bedeutet aber nicht das Ende der bestehenden Linux-Installationen. Sofern die Linux-Partitionen noch vollständig sind und nur der Master Boot Record (MBR) beziehungsweise der Bootloader überschrieben wurden, ist eine Reparatur möglich. Vier Wege bieten sich dazu an, die zum Teil einfach und komfortabel sind. Bei diffizilen Problemen mit dem zu rettenden Linux-System sind bisweilen auch Klimmzüge in gestarteten Livesystemen nötig. Die folgenden Anleitungen spielen die Reparaturmöglichkeiten durch und beginnen mit dem einfachsten Weg.

Möglichkeit 1: Die Super Grub Disk

Der Bootloader Grub 2 wurde überschrieben – was tun? Der erste Schritt sollte immer der Versuch sein, das liegengebliebene Linux-System mit der Super Grub Disk (auf Heft-DVD, Download unter *www.supergrubdisk.org/super-grub2-disk*, 20 MB) zu booten. Es handelt sich dabei um kein ausgewachsenes Livesystem, sondern um eine Bootumgebung mit Grub 2, die alle Datenträger nach bekannten Betriebssystemen durchsucht. Gefundene Linux- und Windows-Systeme versucht die Super Grub Disk dann mit einem generischen, per Script generierten Booteintrag zu starten. Diese Mini-Bootumgebung kann mit Bios und Uefi umgehen. Es ist aber wichtig, ein Linux- oder Windows-System im richtigen Modus zu starten, denn nur dann wird die anschließende Reparatur dessen Bootumgebung gelingen.

Bios-Modus: Auf der Heft-DVD ist die Super Grub Disk 2 startfähig im Multibootmenü unter „Extras und Tools“ vertreten. In diesem Untermenü dient der Eintrag „Super Grub Disk 2.02s9 -> Detect and show boot methods“ zum Auffinden vorhandener Systeme. Je nach Festplatten- und Systemkonstellation kann der Vorgang etwas dauern, bis das nächste, dynamisch erzeugte Menü alle gefunden Linux-Kernel und Windows-Systeme in einer Liste anzeigt. Darunter, unterhalb von „Entries from...“ findet sich aber auch ein Eintrag mit dem Namen der Distribution. Keine Sorge übrigens, wenn das liegengebliebene Linux-System mit Cryptsetup-LUKS verschlüs-

selt ist: Beim Systemstart wird eine Eingabeaufforderung das Cryptsetup-Passwort mit „Enter Passphrase“ abfragen. Wenn das ursprüngliche System läuft, öffnen Sie ein Terminal-Fenster und geben dort die beiden Befehle

```
sudo grub-install --recheck /dev/
  sd[X]
sudo update-grub
```

ein. Anstatt dem Platzhalter [X] ist die Angabe der Datenträgerkennung nötig, die üblicherweise zum Booten dient. In den meisten Fällen ist dies Partition /dev/sda. Dies ist nicht zwingend die Systempartition, sondern einfach die Festplatte, welche den MBR des Bootloaders für den Systemstart über Bios enthält. Grub 2 erstellt dann ein neues Bootmenü mit allen erkannten Betriebssystemen und schreibt den MBR neu.

Uefi-Modus: Für diesen Fall ist es nötig, die ISO-Datei super_grub2_disk_hybrid_2.02s9.iso (auf der Heft-DVD im Verzeichnis „Extras“) auf ein neues Bootmedium zu übertragen, etwa auf eine CD/DVD oder einen USB-Stick. Unter Linux, und dafür genügt ein beliebiges Livesystem, kann das Befehlszeilentool dd die Übertragung auf USB-Stick erledigen. Wichtig ist, das USB-Laufwerk vor dem Beschreiben durch dd auszuhängen, was das Kommando

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

für alle Partitionen des USB-Laufwerks erledigt – wobei /dev/sd[X] die Laufwerkskennung des angesteckten USB-Sticks sein muss. Ist diese nicht bekannt, so listet das Kommando

```
lsblk -p
```

die erkannten Laufwerke auf. Zum Beschreiben des Sticks mit der Super Grub Disk 2 dient dann dieser Befehl:

```
sudo dd if= super_grub2_disk_
  hybrid_2.02s9.iso of=/dev/sd[X]
```

Das Booten und der Rest der Reparatur im wieder laufenden Linux-System unterscheidet sich nicht von der Vorgehensweise im Bios-Modus.



System ohne Bootloader wiederbeleben: Die Super Grub Disk 2 sucht die Festplatten nach startfähigen Betriebssystemen ab und erkennt sogar bestehende Grub-2-Menüdateien.

Möglichkeit 2: Livesysteme

Die Reparatur von Grub 2 können Sie auch mit einer Live-CD der installierten Distribution erledigen. Achten Sie darauf, dass es sich um die gleiche Version wie beim installierten System handelt, da unterschiedliche Versionen von Grub 2 nicht immer kompatibel sind.

Wenn Sie also ein Ubuntu 16.04 LTS reparieren möchten, brauchen Sie eine Live-CD von Ubuntu/Kubuntu/Xubuntu/Lubuntu 16.04 LTS oder von Linux Mint 18.2. Auch die Architektur muss passen (32 Bit oder 64 Bit). Die Reparatur per Livesystem ist ein Stück anspruchsvoller und nur dann notwendig, wenn das Booten über Super Grub Disk nicht klappt.

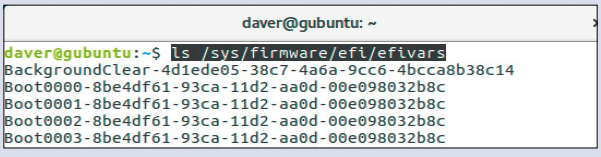
Bios-Modus: Läuft das Livesystem, so gilt es zunächst herauszufinden, auf welcher Partition das primäre Linux-

Unterschiede: Uefi und Bios

Generell muss immer unterschieden werden, ob ein System im Uefi-Modus installiert wurde oder im alten Bios-Modus. Die Bootmethoden von Bios und Uefi unterscheiden sich erheblich voneinander, und zur Reparatur muss ein System immer in dem Modus gebootet werden, in dem es ursprünglich installiert wurde. Damit ein PC oder Notebook wirklich im Uefi-Modus startet, sollte in den Firmware-Einstellungen die Bios-Bootmethode über „CSM“ beziehungsweise „Legacy“ deaktiviert sein. Im Uefi-Bootmenü des Rechners, das Sie je nach Modell mit den Tasten Esc, F8 oder auch F12 aufrufen, wählt man dann den USB-Stick als Bootmedium aus. Um sicherzustellen, dass der Start dann tatsächlich im Uefi-Modus erfolgte, belegt folgender Terminal-Befehl:

```
ls /sys/firmware/efi/efivars
```

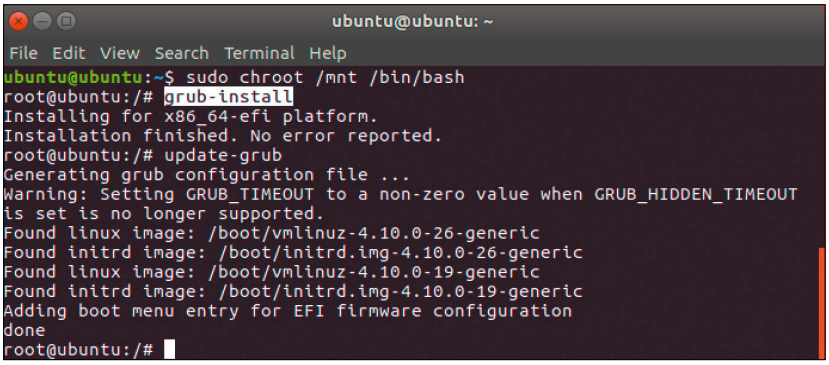
Zeigt die Ausgabe eine Dateiliste, ist alles in Ordnung. Ist das abgefragte Verzeichnis nicht vorhanden, so befindet sich das System im Bios-Modus.



Welcher Modus? Dieser Befehl findet im Verzeichnis /sys/firmware/efi/efivars nur dann Dateien, wenn das Linux-System tatsächlich im Uefi-Modus läuft.



Der einfachste Weg: Läuft die ursprüngliche Linux-Installation wieder, dann können diese Befehle den Bootloader im Bios- und auch im Uefi-Modus restaurieren.



Grub-Reparatur über eine Chroot-Umgebung: Dieser Weg ist sehr zuverlässig, verlangt aber auf Uefi-Installationen einige Vorbereitung und das vorherige Einhängen der EFI-Partition.

System installiert ist. Bei der Identifikation hilft das Kommando

```
sudo fdisk -l
```

in der Befehlszeile oder auch auf dem Desktop das Partitionierungstool Gparted, das in vielen Livesystemen enthalten ist. In diesem Beispiel gehen wir davon aus, dass Linux auf der Partition /dev/sdb1 installiert ist und die Festplatte /dev/sda vom Bios gebootet wird. Davon ausgehend muss erst folgender Befehl in der Konsole die Systempartition nach /mnt einhängen:

```
sudo mount /dev/sdb1 /mnt
```

Als Nächstes können die in Grub 2 enthaltenen Tools, die es auch im Live-System gibt, den Bootloader und dessen Menü neu schreiben:

```
sudo grub-install --root-directo
 ry=/mnt /dev/sda
```

Wenn alles geklappt hat, zeigt sich nach dem nächsten Neustart ein neues Grub-2-Menü, das Einträge für alle installierten und erkannten Betriebssysteme enthält. Sollte es nicht klappen, so liegt dies meist an einer separaten /boot-Partition des Linux-Systems.

Bei einer separaten Partition für /boot, was bei einer Partitionierung mittels LVM der Standard ist, braucht es noch einen Zwischenschritt: In diesem Fall liegt die Grub-2-Konfiguration nie auf der Systempartition, sondern unter /boot auf seiner eigenen Partition. Zur Reparatur braucht das Livesystem Zugriff auf beide Partitionen. Angenommen, die Systempartition hat die Kennung /dev/sdb1 und die zusätzliche Partition /boot hat die Kennung /dev/sdb6, so hängt man im Livesystem trotzdem erst die Systempartition ein:

```
sudo mount /dev/sdb1 /mnt
```

Anschließend kommt mit einem weiteren mount-Befehl die /boot-Partition hinzu:

```
sudo mount /dev/sda6 /mnt/boot
```

In der eingehängten Systempartition gibt es jetzt ein Unterverzeichnis /boot, das den tatsächlichen Inhalt dieser Partition enthält. Beachten Sie, dass Sie die Partitionen immer in dieser Reihenfolge einhängen müssen. Jetzt können Sie Grub 2 neu installieren, in diesem Fall in den Master Boot Record der Festplatte /dev/sda, die vom Bios des PCs nach dem Bootsektor durchsucht wird:

```
sudo grub-install --root-directo
 ry=/mnt /dev/sda
```

Uefi-Modus: In diesem Modus ist im Livesystem ein anderer Weg zur Restaurierung von Grub 2 gefragt. Ein paar Befehle im Terminal erstellen anhand des installierten, wenn auch nicht bootfähigen Systems eine Chroot-Umgebung. Zuerst hängt man wieder die Systempartition ein, in diesem Beispiel /dev/sdb1:

```
sudo mount /dev/sdb1 /mnt
```

Dann ziehen die folgenden drei Mount-Befehle die weiteren, benötigten Verzeichnisse hinzu:

```
mount -o bind /dev /mnt/dev
mount -o bind /sys /mnt/sys
mount -t proc /proc /mnt/proc
```

Damit Grub 2 die EFI-Partition findet, muss auch diese eingehängt werden. Der Befehl

```
sudo fdisk -l
```

zeigt deren Gerätekennung an, beispielsweise /dev/sda1. Mit dem Kommando

```
sudo mount /dev/sda1 /mnt/boot/efi
```

hängen Sie diese ebenfalls ein. Anschließend geht es zur eigentlichen Reparatur:

```
chroot /mnt/ /bin/bash
```

Dies startet die Chroot-Umgebung, und die beiden Kommandos

```
grub-install
update-grub
```

schreiben Grub 2 im Uefi-Modus neu. Die Tastenkombination Strg-D beendet die Chroot-Umgebung, und das System ist jetzt mit Grub-2-Bootloader wieder startbereit. Sollte es nicht geklappt haben, dann empfiehlt sich eine genauere Prüfung der Partitionskennungen, denn hier lauert eine häufige Fehlerquelle. ●

PC-WELT

Virtuelle PCs



Sonderheft
für nur
9,90 €

7 virtuelle PCs auf DVD!

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

1. Formular ausfüllen **2. Foto machen** **3. Foto an shop@pcwelt.de**

Ja, ich bestelle das PC-WELT Sonderheft Virtuelle PCs für nur 9,90 €.

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

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PC-WELT erscheint im Verlag 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

ISO-Dateien booten

Der Bootloader Grub 2 kann eine ganze Menge mehr als einfach nur ein Menü darstellen und verschiedene Betriebssysteme starten. Grub 2 kann Livesysteme auch direkt aus ihren ISO-Dateien heraus booten.

Von **David Wolski**



Ein Livesystem, das unabhängig vom fest installierten Linux-Betriebssystem läuft, ist immer wieder nützlich zur Arbeit an Festplatten oder für Komplettbackups und deren Wiederherstellung. Aber wo war gleich wieder der USB-Stick mit dem benötigten System? Für Betriebssystembastler gibt es einen anderen Weg, häufig benötigte Livesysteme zu starten als über externe Bootmedien. Mit geringem Aufwand kann das Bootmenü des Bootloaders Grub 2 ein Livesystem starten, das als ISO-Datei auf Festplatte liegt. Das gelingt ohne komplizierte Installationsprozedur oder Auspacken der Systemdateien aus dem Image.

Allerdings wollen nicht alle Linux-Distributionen und Livesysteme aus dem ISO heraus starten. Als Voraussetzung, dass das klappt, müssen die Init-Scripts des Linux-Systems dies unterstützten. Die wichtigsten Live- und Notfallsysteme unterstützen den Start per ISO-Datei, so etwa auch die LinuxWelt-Rettungs-DVD (auf Heft-DVD), die hier als Beispiel dienen soll.

Grub 2: Aufbau der Konfiguration

Der Schlüssel zum Booten des ISO ist ein Menüeintrag in Grub 2 mit den passenden Bootparametern. Es ist nicht immer ganz einfach, die richtigen Parameter von Linux-Distribution und Livesystemen zu ermitteln, denn diese sind oft komplett undokumentiert. Viele Systeme nutzen aber sehr ähnliche Init-Scripts und deshalb funktionieren dieselben Parameter.

Der Bootloader „Grand Unified Bootloader 2“ – kurz „Grub 2“ ist kein Buch mit sieben Siegeln, wartet aber mit umfangreichen Konfigurationsscripts auf. Grub 2 muss mit unterschiedlichen Linux-Systemen sowie Windows zurechtkommen.

Damit deren Einbindung automatisch erfolgt, kümmern sich einige Scripts im Verzeichnis „/etc/grub.d“ um die Erstellung der eigentlichen Konfiguration. Diese Script-Dateien sind durchnummeriert und werden in der vorgegebenen Reihenfolge bei einem Update der Grub-2-Konfiguration ausgeführt, beispielsweise bei jedem Upgrade auf einen neuen Kernel.

Das wichtigste Script „10_linux“ sucht unter „/boot“ nach Linux-Kernels, den zugehörigen initialen Ramdisk-Images und erstellt daraus die Einträge für das Bootmenü.

Das Script „30_os-prober“ ist für die Suche nach Windows-Systemen zuständig, „30_uefi_firm-ware“ bindet Dateien von der EFI-Partition ins Menü ein. Dazu steuern Variablen in der Datei „/etc/default/grub“ das Verhalten von Grub 2. Üblicherweise müssen Anwender nur in Ausnahmefällen etwas an der Datei „/etc/default/grub“ ändern und an den Scripts noch seltener. In diesem Fall ist aber eine Ergänzung der Scripts gefragt, um eine ISO-Datei dauerhaft ins Bootmenü zu bringen.

Loopback: Ein ISO-Image booten

Die Fähigkeit, Livesysteme und Distributionen aus der ISO-Datei heraus zu starten, hat Grub 2 schon seit seiner Beta-Phase. Der Bootloader bindet Images über Parameter über ein Loopback-Device ein und startet den enthaltenen Kernel mit der initialen Ramdisk. Ab dann übernimmt das Linux-System den weiteren Start aus dem ISO. Es dauerte eine Weile, bis Linux-Distributionen sich diese Möglichkeit zunutze machten. Seit Ausgabe 3/2011 nutzt die LinuxWelt-Heft-DVD Grub 2 als Bootloader und liefert, immer wenn möglich, die bootfähigen Systeme als unveränderte ISO-Datei aus.

Dieser Ansatz lässt sich auch mit dem Grub-2-Bootlaoder des fest installierten Linux-Systems nachbauen. Im folgenden praktischen Beispiel dient dazu die LinuxWelt-Rettungs-DVD, deren ISO-Datei „lwRescue621.iso“ sich auf Heft-DVD im Verzeichnis „Image-Dateien“ befindet. Als installiertes Linux-System dient ein Ubuntu 16.04, jedoch sollte der gezeigte Weg mit allen Distributionen gleichermaßen funktionieren.

1. Die ISO-Datei „lwRescue621.iso“ kommt mit diesem Befehl im Terminal kurzerhand ins Verzeichnis „/boot“ auf der Systempartition:

```
sudo cp lwRescue621.iso /boot
```

2. Das Verzeichnis der ISO-Datei ist nun bekannt. Aber es wird noch die Kennung von Laufwerk und Partition gebraucht, auf der „/boot“ liegt. Diese zeigt der Befehl

```
df /boot
```

unter „Dateisystem an“, beispielsweise „/dev/sda1“. Dies wäre die erste Partition auf dem ersten Laufwerk.

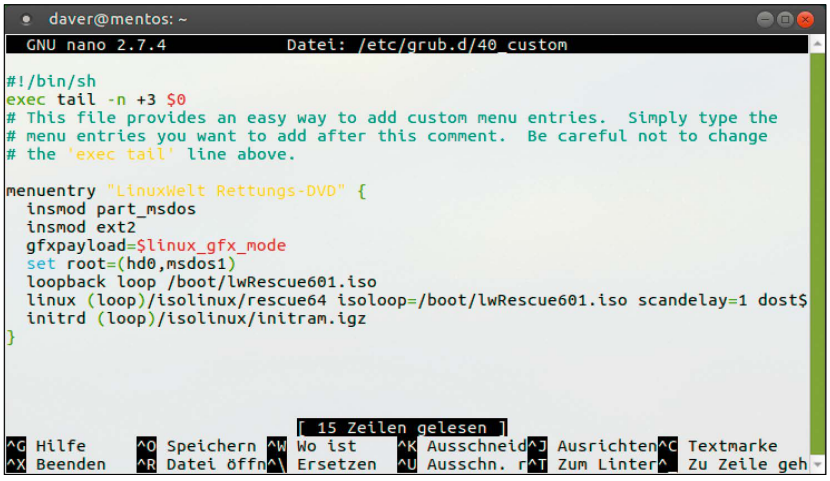
3. Netterweise gibt es unter den Grub-2-Scripts bereits eine Vorlagendatei namens „40_custom“, die benutzerdefinierte Booteinträge aufnimmt. Diese Datei lädt man mit sudo oder root-Rechten in einen Texteditor:

```
sudo nano /etc/grub.d/40_custom
```

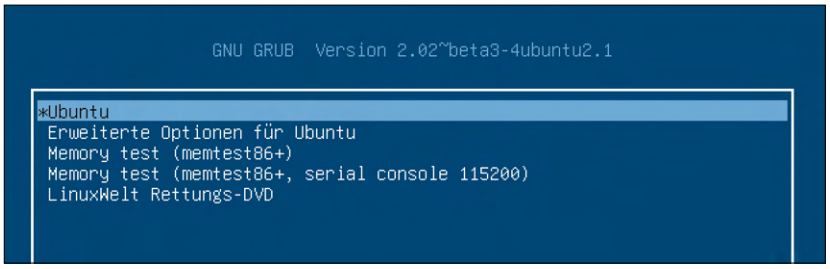
4. In die Datei „40_custom“ kommt nun unter die wenigen bereits bestehenden Zeilen ein neuer Menüeintrag, den der Inhalt des Kastens „Menüeintrag: LinuxWelt-Rettungs-DVD booten“ zeigt. Anzupassen wäre hier lediglich die Zeile „set root=(hd0,msdos1)“, die der im Schritt 2 ermittelten Laufwerks- und Partitionskennung entspricht. Der Parameter „hd0“ steht für die erste Festplatte und „msdos1“ für die erste Partition.

5. Nach einer Kontrolle des neuen Menüeintrags und dem Speichern der Datei „40_custom“ geht es noch in die Datei „/etc/default/grub“. Hier gilt es, beim Systemstart das Bootmenü anzuzeigen, das in Ubuntu standardmäßig ausgeblendet ist. Dazu setzt man vor die Zeilen

```
GRUB_HIDDEN_TIMEOUT=3
```



Menüeintrag für die LinuxWelt Rettungs-DVD: Grub 2 liefert mit der Datei „40_custom“ schon eine Vorlage mit, die eigene Ergänzungen für das Bootmenü aufnimmt.



Der fertige Eintrag im Grub-Bootmenü: Der neue Punkt „LinuxWelt Rettungs-DVD“ startet jetzt das Livesystem von der Festplatte direkt aus der ISO-Datei heraus.

```
GRUB_HIDDEN_TIMEOUT_QUIET=true
```

jeweils das Zeichen #, um diese auszukommentieren. Außerdem ändert man die Zeile „GRUB_TIMEOUT“ ab, falls nötig:

```
GRUB_TIMEOUT=10
```

Dies zeigt ab jetzt beim Systemstart für zehn Sekunden das Bootmenü an.

6. Der letzte Schritt ist die Aktualisierung des Bootmenüs:

```
sudo update-grub
```

Fehler finden und beheben: Beschwert sich Grub 2 bei der Wahl des neuen Booteintrages darüber, dass die Datei „/boot/lwRescue621.iso“ nicht gefunden wurde, so ist eine Kontrolle des Speicherpfades und der Laufwerks- sowie Partitionskennung (siehe -> Schritt 4) nötig.

Denn bei diesen Angaben schleichen sich gerne Fehler ein. Schlägt der Befehl sudo update-grub wegen eines Syntaxfehlers fehl, so fehlt meist am Ende des gesamten Menüeintrags in der Datei „40_custom“ eine abschließende geschweiften Klammer. Nach jeder Änderung in der Konfigurationsdatei muss stets der Update-Befehl

```
sudo update-grub
```

von Grub 2 ausgeführt werden.

Grub-Menüeintrag für die LinuxWelt-Rettungs-DVD

```
menuentry "LinuxWelt Rettungs-DVD
  (64 Bit)" {
insmod part_msdos
insmod ext2
gfxpayload=$linux_gfx_mode
set root=(hd0,msdos1)
loopback loop /boot/iso/lwRescue621.
  iso
linux (loop)/isolinux/rescue64 iso
  loop=/boot/lwRescue621.iso scande
  lay=1 dostartx setkmap=de
initrd (loop)/isolinux/initram.igz }
```

Starthilfe mit Kernel-Parametern

Ein Linux-System bootet von USB-Stick oder DVD, aber dann tut sich nichts mehr. Meist liegen solche Startprobleme an Hardware in PC oder Notebook, die der Linux-Kernel des Systems noch nicht unterstützt. Kernel-Parameter helfen weiter.

Von **David Wolski**



Sie sind seltener geworden, die gefürchteten Inkompatibilitäten des Linux-Kernels zu Hardwarekomponenten. Hersteller von Rang und Namen sorgen sich früh darum, dass die nötige Unterstützung für neue Prozessoren und Grafikchips zeitig in den Kernel kommt. Trotzdem gibt es leider weiterhin sporadische Probleme eines Linux-Systems beziehungsweise dessen Kernel mit der Hardware eines Rechners. Gerade Notebooks, die auf Microsoft Windows zugeschnitten sind, bereiten mit ihren zahlreichen Bios-Versionen, abweichenden ACPI-Stromsparfunktionen und Chipsatzvarianten häufiger Ärger. Mal bleibt der Bildschirm dunkel, mal geht nach den ersten Bootmeldungen nichts mehr weiter.

Tatsächlich drehen sich Leseranfragen zu beilegenden Heft-DVDs der LinuxWelt häufig um das Problem, dass auf einem Notebook ein Livesystem nicht startet. Was tun? Meist helfen spezielle Kernel-Parameter weiter.

Bootloader: Grub 2 und Isolinux

Jedes Linux-System bietet eine ganze Reihe von Kernel-Parametern – in der Dokumentation von Linux-Systemen auch oft Bootparameter oder Cheatcodes genannt.

Diese Parameter steuern Kernel-Eigenschaften, Treiberoptionen und die Ansteuerung von Hardwarekomponenten. Neben den grundlegenden Standardparametern, die jedes Linux-System erwartet und dem Kernel Anweisungen über root-Partition und Name des Kernel-Images mitgeben, gibt es weitere optionale Angaben, die Kernel-Eigenschaften und Hardwareunterstützung beeinflussen.

Alle diese Parameter werden als Optionen im verwendeten Bootloader angegeben, also in Grub 2 oder in Isolinux. Die Vorgehensweise unterscheidet sich je nach Bootloader ein Stück.

Grub 2 im Livesystem: In den meisten Fällen übernimmt Grub 2 den Boot von Livesystemen und Installationsmedien. Beim Boot eines Livesystems im Uefi-Modus sowieso, denn Grub 2 ist dabei fast immer der verwendete Bootloader.

Ganz einfach deshalb, weil nur dieser der bisher alle Uefi-Eigenschaften wie Secure Boot unterstützt. In Grub 2 drückt man nach der Markierung eines Booteintrags die Taste E und bekommt dann einen Texteditor für den jeweiligen Eintrag gezeigt. Der Editor ist mehrzeilig und bricht überlange Zeilen am Ende zur besseren Übersicht um. Die Navigation im Textfeld erfolgt mit den Cursortasten. Grundsätzlich müssen Kernel-Parameter nur am Ende jener Zeile angegeben werden, die mit „linux“ beginnt. Nach der Änderungen startet ein Druck auf die Taste F10 den Booteintrag mit den neuen Einstellungen.

Grub 2 auf fest installiertem System: Auch bei einem bereits instal-

lierten Linux-System kommt Grub 2 zum Einsatz. Zum Testen lassen sich im Bootloader die gewünschten Kernel-Parameter beim Start genauso angeben wie in einem Livesystem. Die Änderungen sind dabei natürlich nicht permanent. Um einen Kernel-Parameter nach den ersten erfolgreichen Tests dauerhaft zu setzen, ist eine Bearbeitung der Konfigurationsdatei „/etc/gefault/grub“ nötig. In Ubuntu und Linux Mint kann man diese Datei beispielsweise mit dem Befehl

```
sudo -H gedit /etc/gefault/grub
```

mit root-Berechtigungen in den Editor Gedit laden.

Dort definiert die Zeile

```
GRUB_CMDLINE_
 LINUX="[parameter1]=[wert1]
 [parameter2]=[wert2]"
```

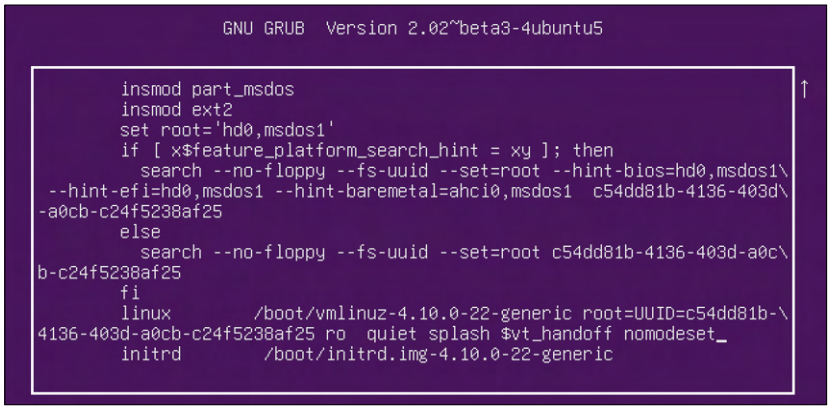
die manuell hinzugefügten Kernel-Parameter. Stehen hier schon Parameter, so ergänzen Sie die eigenen nach einem Leerzeichen in dieser Zeile. Nach Änderung und Sicherung der Konfigurationsdatei ist die Änderung aber noch nicht wirksam, denn erst muss noch der Bootloader mit diesem Befehl im Terminal aktualisiert werden:

```
sudo update-grub
```

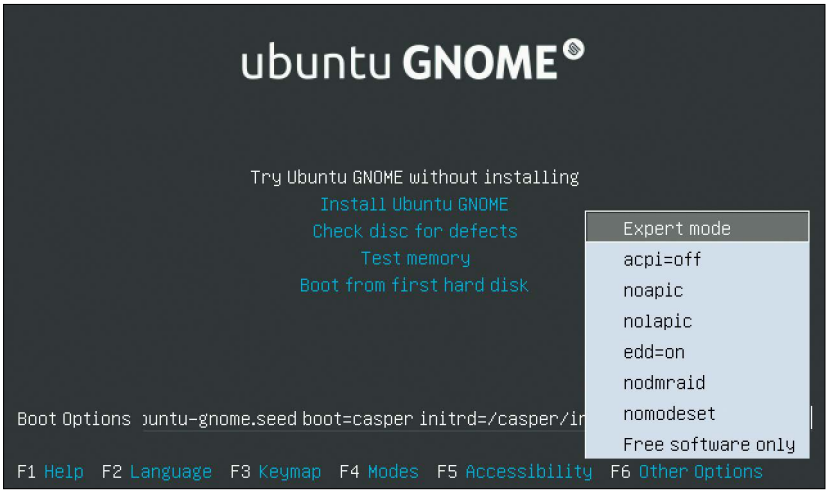
Erst danach starten die vorhandenen Einträge im Grub-2-Bootmenü mit den hinzugefügten Kernel-Parametern.

Isolinux: Bei einigen Livesystemen wie Ubuntu und Co. meldet sich Isolinux als Bootloader, falls das System im Bios-Modus und nicht über Uefi gestartet wird. Wird ein Countdown angezeigt, so unterbricht diesen der Druck auf eine beliebige Taste. Isolinux zeigt meist eine Oberfläche mit einigen Menüpunkten an, etwa zur Auswahl der Sprache. Die Tabulatortaste verwandelt die untere Zeile in eine Eingabezeile und zeigt zum gerade ausgewählten Menüeintrag die Kernel-Parameter an. Am Ende der Zeile lassen sich weitere Kernel-Parameter ergänzen und der Druck der Eingabetaste bootet das System mit den neuen Optionen.

In Ubuntu und seinen Varianten ist der Weg ein anderer: Hier ruft die Taste F6 ein Untermenü auf, in welchem



Menü von Grub 2: In Ubuntu muss beim Start erst noch die Umschalttaste gedrückt werden, damit sich das Bootmenü mit seinen Bearbeitungsmöglichkeiten zeigt.



Kernel-Parameter manuell ergänzen: Der Bootloader Isolinux von Ubuntu bringt ein Menü für wichtige Bootoptionen mit. F6 startet den „Expert mode“ für manuelle Parameter.

der Punkt „Expertenmodus“ beziehungsweise „Expert mode“ die Eingabezeile für Kernel-Parameter öffnet.

Bootoptionen: Ärger mit ACPI

Ein Dauerthema, das auf vielen Notebooks den Start von Linux-Systemen

Übersicht: Alle Kernel-Parameter



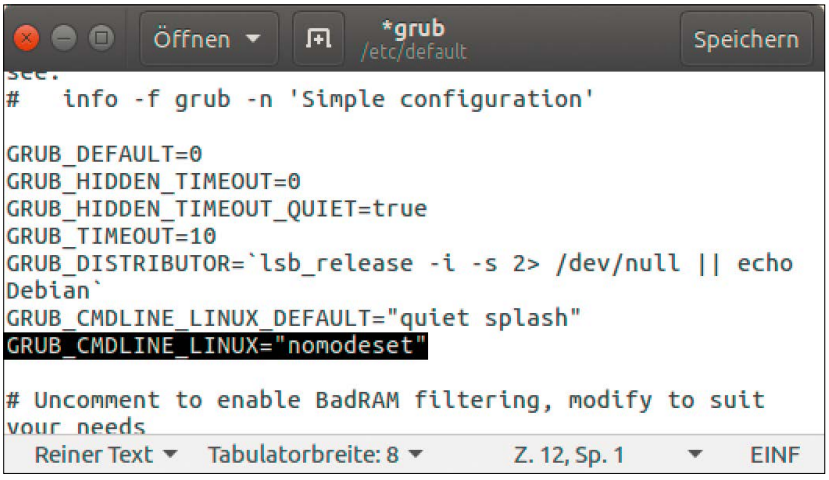
Generell sind Kernel-Parameter mit einem Leerzeichen voneinander abgetrennt und folgen diesem Schema

```
[Parameter]=[Wert]
```

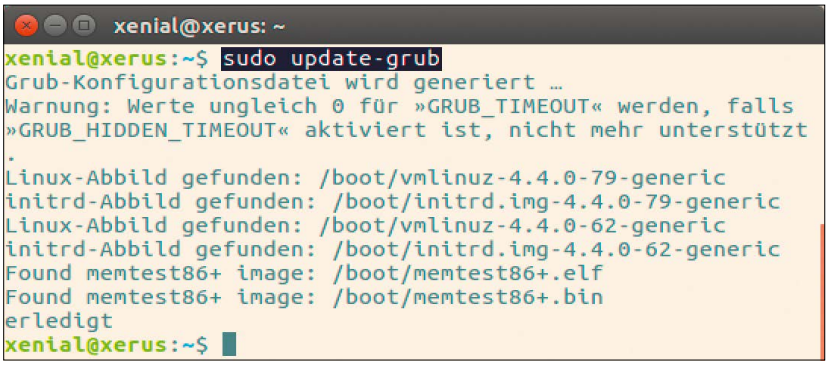
oder bestehen auch einfach aus einem einzigen Schlüsselwort.

Mehrere Parameter sind frei miteinander kombinierbar und die Reihenfolge spielt keine Rolle. Ungültige und unbekannte Parameter ignoriert der Linux-Kernel ohne Unterbrechung des Bootvorgangs, aber auch ohne Anzeige einer Fehlermeldung. Die hier vorgestellten Kernel-Parameter sind nur die wichtigsten Helfer bei häufigen Problemen, es gibt aber noch etliche Parameter mehr. Für Ubuntu und Co. liefert die englischsprachige Hilfeseite *https://help.ubuntu.com/community/BootOptions* eine Übersicht geläufiger Bootparameter.

Die komplette Liste der Parameter mit Beschreibung für Entwickler kann die offizielle Kernel-Dokumentation unter *www.kernel.org/doc/html/v4.10/admin-guide/kernel-parameters.html* bieten.



Bootmenü von Grub 2 ergänzen: Kernel-Parameter, die permanent alle vorhandenen Booteinträge ergänzen sollen, müssen in der Datei „/etc/gefault/grub“ festgelegt werden.



Booteinträge neu erstellen: Erst auf dieses Kommando hin erstellt Grub 2 aus der vorhandenen Konfiguration das Bootmenü neu. Dieser Befehl ist nach jeder Änderung nötig.

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 wirklich 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 Hyperthreading und die Lüfterregelung sind abgeschaltet.

acpi=ht: Mit dieser Option beachtet der Linux-Kernel gerade mal so viele ACPI-Fähigkeiten der Hardware, dass Hyperthreading der CPU funktioniert. Andere Stromsparfunktionen bleiben dagegen deaktiviert.

acpi=strict weist die ACPI-Unterstützung des Kernels an, nur ACPI-Merkmale der vorhandenen Hardware zu beachten, die exakt dem Standard folgen. Auf problematischen Notebooks ist diese Option immer einen Versuch wert.

acpi_osi=linux umgeht die Abfrage des Linux-Kernels, ob das ACPI eines Rechners kompatibel ist. Sinnvoll ist dieser Parameter, wenn einige Stromsparfunktionen nicht verfügbar sind oder die Drehzahlsteuerung der Lüfter nicht funktioniert.

Parameter für Grafikprobleme

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 das Wechseln in den Grafikmodus und bleibt bei purem Text.

Sonstige Hardwarehürden

Eine weitere APIC-Komponente nennt sich „Local APIC“ und nimmt die Interruptanforderungen auf jedem Prozessorkern entgegen. Der Parameter „nolapic“ löst vielfältige Probleme mit heiklen Bios-Versionen, reduziert aber in jedem Fall die Zahl der vorhandenen CPU-Kerne auf einen. Geeignet ist dies nur als erste Hilfe, bis ein Bios-Update oder eine neue Kernel-Version echte Abhilfe schafft.

noapic: Verhindert, dass APIC für die Auflösung von Hardwarekonflikten auf Interruptebene verwendet wird. Der Parameter hilft auf Systemen mit einem unverträglichen Bios und inkompatiblen ACPI-Funktionen im 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 zusammen mit Linux nicht immer, was zum Ausfall von USB-Ports oder Netzwerkchip führt. Dieser Parameter aktiviert zusammen mit abgeschaltetem IOMMU im Bios/Uefi ein softwaremäßiges IOMMU. ●

PC-WELT

Sicherheits-Handbuch 2018



Sonderheft
für nur
12,90 €

Auf DVD:
Komplett-Schutz
für Ihr System

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

1. Formular ausfüllen **2. Foto machen** **3. Foto an shop@pcwelt.de**

Ja, ich bestelle das PC-WELT Sonderheft Sicherheit für nur 12,90 €.

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

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PC-WELT erscheint im Verlag 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

Instabile Systeme

Nicht ohne Grund hat Linux den ausgezeichneten Ruf, ein robustes System zu sein. Auch gibt es im Falle von Problemen eine Reihe von Analysetools und Logs, die Auskunft über die Ursache von Abstürzen geben.

Von **David Wolski**



Auch unter Linux gibt es Probleme mit alternder oder defekter Hardware, die sich nicht gleich im Totalausfall des Rechners zeigen, sondern ganz subtil in spontanen Abstürzen. Nachinstallierte Kernel-Module, etwa proprietäre Grafik- oder Netzwerktreiber, können ebenfalls für Fehler verantwortlich sein. Wenn sich PC-Probleme häufen, ein reproduzierbarer Fehler auch durch geänderte Konfiguration am Betriebssystem einfach nicht zu beseitigen ist, so ist eine systematische Fehlersuche gefragt. Dabei helfen Standardtools – die meisten davon sind bereits vorinstalliert. Es handelt sich um systemnahe Arbeiten, die eine Exkursion in die Kommandozeile erfordern.

Kernel-Meldungen: Was bisher geschah

Eine der wichtigsten Logdateien ist das Kernel-Protokoll, das ein Linux-System ab dem Bootvorgang anlegt. Hier informiert der Kernel auch über erkannte Hardware, Laufwerke und Aktionen von Treibern.

Stürzen Prozesse wegen fehlerhafter Treiber oder defekter Hardware ab, dann wird der Kernel dies in diesem Protokoll melden. In der Shell dient der handliche Befehl

```
dmesg -T
```

dazu, alle Kernel-Meldungen mit Zeitstempel anzuzeigen. Neben allgemeinen Infos finden sich in der langen Liste auch Fehlermeldungen und Warnhinweise. Besser ist deshalb dieses Kommando:

```
dmesg -T -l err
```

Es reduziert die Ausgabe auf Fehler und blendet dabei alle anderen Meldungen aus.

Hardwarefehler: CPU und RAM

Speicherfehler in CPU und RAM können auch auf einem gesunden System auftreten und müssen nicht immer gleich zu Abstürzen führen. Moderne Prozessoren haben einen internen Mechanismus, über Checksummen korrumpierte Speicherbereiche zu erkennen, und lösen dann eine „Machine Check Exception“ aus, die sich protokollieren lässt. Dazu ist die Installation des Pakets mcelog nötig, das in allen verbreiteten Linux-Distributionen bereitsteht und in Debian/Ubuntu/Mint mit

```
sudo apt-get install mcelog
```

installiert wird. Ab jetzt werden die MCE-Fehlermeldungen in der Datei „/var/log/mcelog“ protokolliert. Auf Linux-Systemen mit Journald als Loggingdienst (Debian, Ubuntu, Fedora, Open Suse und Arch Linux) überprüfen Sie mit dem Kommando

```
journalctl _SYSTEMD_UNIT=mcelog.service
```

das mcelog. Treten dort Fehler nicht nur sporadisch, sondern regelmäßig auf, dann weist das auf defekte Hardware oder ein überhitztes System hin.

Temperaturen: Überhitztes Silizium

Gerade in Notebooks mit beengten Platzverhältnissen läuft die CPU aufgrund beengter Verhältnisse recht heiß. Wer rechenintensive Programme ausführt, sollte die Temperatur des Prozessors im Auge behalten, um bei Bedarf für bessere Kühlung zu sorgen. Denn ein überhitztes System wird fehleranfällig.

Unter Linux dient das Programm sensors dazu, die Temperaturfühler von Prozessor und Hauptplatine aus-

zulesen. Zur Installation in Debian/Ubuntu dient der Befehl

```
sudo apt-get install lm-sensors
```

und in Fedora lautet der entsprechende Befehl

```
sudo dnf install lm_sensors
```

(mit Unterstrich im Paketnamen) und bei Open Suse so:

```
sudo zypper install sensors
```

Anschließend müssen die Temperatursensoren von CPU und Mainboard eingebunden werden. Dazu liefert lm_sensors ein Installationsscript mit, das der Aufruf

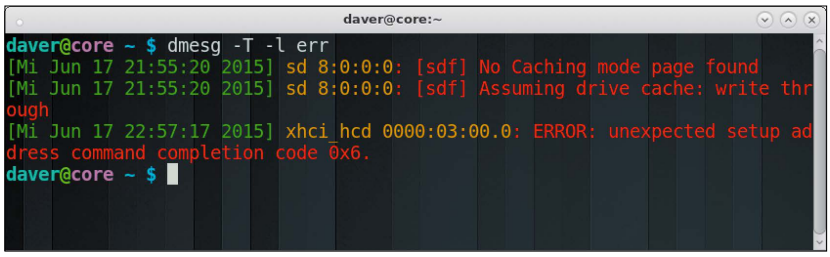
```
sudo /usr/sbin/sensors-detect
```

startet. Die Suche nach unterstützten Chips verlangt einige Bestätigungen mit „yes“. Das Installationsscript zeigt zum Abschluss die Liste gefundener Sensoren an und erstellt die Konfigurationsdatei automatisch. Zudem wird das benötigte Kernel-Modul i2c-dev auch gleich geladen. Die Eingabe von

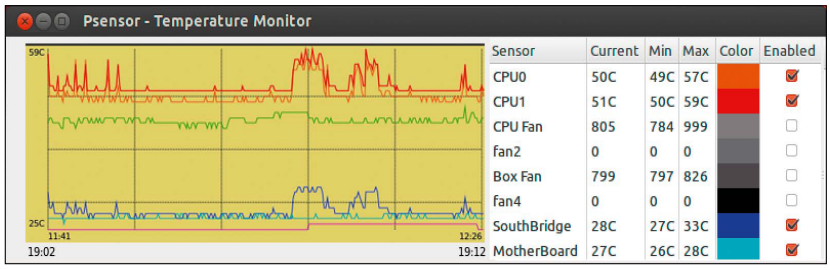
```
sensors
```

fragt anschließend die Temperaturfühler ab.

Für Desktopumgebungen gibt es zur Auswertung das Programm Psensor, das in den Standard-Paketquellen der meisten Distributionen bereitliegt.



Fehler rund um Geräte, Treiber und Laufwerke zeigt der Befehl dmesg: In diesem Beispiel sorgt eine fehlerhafte USB-Schnittstelle für Abstürze von Dateimanagern.



Systemtemperaturen im Blick: Auf dem Desktop zeigt Psensor die Temperaturen an. In der Kommandozeile gibt der Befehl sensors die Temperatur von CPU und Chipsatz aus.

Logwatch: Logdateien im Blick

Wer sich die Übersicht über die Protokolle des Linux-Systems vereinfachen will, kann auf das Tool logwatch zurückgreifen. Logwatch erstellt einen verkürzten Bericht und schickt diesen per Mail in das lokale Postfach eines Benutzers auf dem System. Empfehlenswert ist die Einrichtung von Logwatch auf Linux-Systemen wie Servern, die wichtige Aufgaben erfüllen. Debian, Raspbian, Ubuntu, Cent-OS und Open Suse bieten alle das Paket „logwatch“ in ihren Paketquellen. In Debian, Ubuntu und deren Derivaten wird es mit

```
sudo apt-get install logwatch
```

installiert. In seinen Standardeinstellungen trägt sich logwatch als täglicher Cronjob unter „/etc/cron.daily“ ein und legt seine Konfiguration unter „/usr/share/logwatch/default.conf/logwatch.conf“ ab. In dieser Konfigurationsdatei geben Sie mit der Zeile

```
"MailTo = root"
```

an, welcher Benutzer auf dem System die Zusammenfassung bekommt. Hier ist root als Standard angegeben, aber man kann hier auch den eigenen Benutzernamen eintragen. Zur Kontrolle des lokalen Postfachs auf dem System dient das Mailprogramm Mutt in der Kommandozeile.

Symptome: Fehler richtig deuten



Der erste Schritt bei der Diagnose ist die Eingrenzung der Fehlerquelle auf Hardware oder Software. Folgende, typische Fehlerbilder auf einem Linux-System liefern wichtige Hinweise, wo das Problem sitzt.

Kernel Panic: Abstürze des Kernels selbst meldet dieser mit „Kernel Panic“ und einem Stack Trace – einer Übersicht von Speicheradressen im Textmodus. Danach wird das System angehalten, denn es handelt sich um einen kritischen Fehler. Ständige Kernel Panics sind typische Anzeichen für überhitzte Systeme, defektes RAM oder fehlerhafte CPUs. Das Tool Memtest86+ (bootfähig unter „Extras und Tools“ auf Heft-DVD) hilft mit einem Speichertest weiter, um Speicherproblemen auf die Spur zu kommen. Diese Tests sollte man ruhig ein paar Stunden durchführen, auf jeden Fall aber mehr als einen Durchlauf.

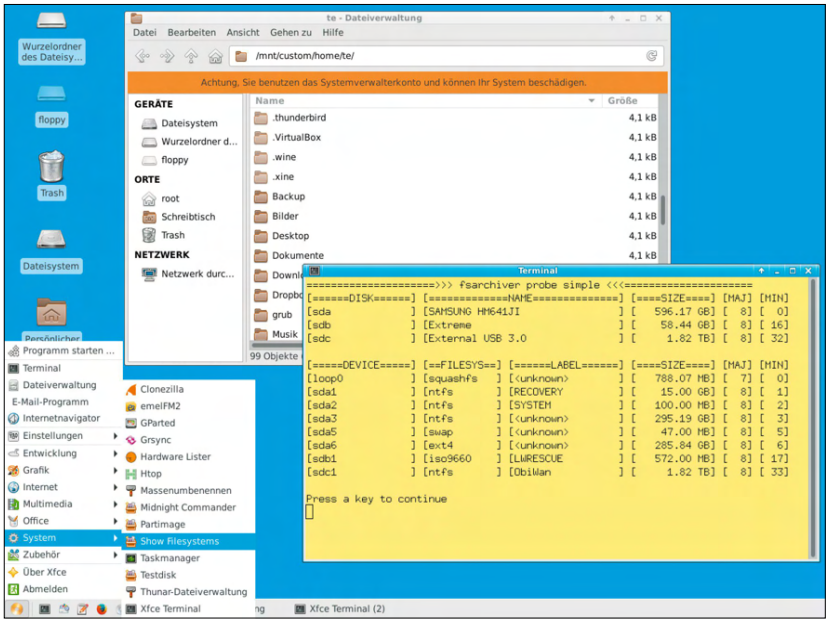
Segmentation Fault: Greift ein Programm auf Speicherbereiche zu, auf die es keinen Zugriff hat, so beendet der Kernel das Programm mit „Segmentation Fault“ (Schutzverletzung). Dahinter muss kein Hardwaredefekt stecken; ein Bug im Quellcode oder eine Panne beim Kompilieren sind häufiger. Es empfiehlt sich, zum Vergleich ein Livesystem auf dem Rechner zu starten. Treten auch hier Segmentation Faults auf, so ist ein Hardwarefehler wahrscheinlich.

Stille Programmabstürze: In der überwiegenden Zahl der Problemfälle auf dem Linux-Desktop beenden sich Programme still und leise, ohne Rückmeldung. Eine Fehlermeldung ist aber dann zu sehen, wenn das Programm über ein Terminal aufgerufen wird. Auch grafische Programme melden dann ihre Fehlermeldung zurück ans Terminal, was für die weitere Fehleranalyse unerlässlich ist.

Datenrettung mit Zweitsystem

Festplatten halten nicht ewig und das Dateisystem kann auch durch Softwarefehler Schaden nehmen. Für die behutsame Datenrettung stehen unter Linux mehrere Tools zur Verfügung.

Von **Thorsten Eggeling**



Dateizugriff: Über die LinuxWelt-Rettungs-DVD kommen Sie jederzeit an Ihre Dateien heran, sofern sich eine Partition noch in das Dateisystem einhängen lässt.

Festplatten und SSDs gehören zu den kritischen Komponenten in PC oder Notebook. Beide können aufgrund von Produktmängeln oder Überhitzung ausfallen, Festplatten auch durch mechanische Einflüsse wie Stoß oder Sturz. Das Dateisystem kann aber auch bei einem Absturz des Betriebssystems oder bei einem Stromausfall beschädigt werden.

1. Fehlerursache feststellen

Ist das Dateisystem defekt, startet Linux nicht mehr, das System stürzt ab oder einzelne Dateien lassen sich nicht mehr öffnen. Handelt es sich um eine externe Festplatte, einen USB-Stick oder eine Speicherkarte, lässt sie sich nicht in das Dateisystem einbinden, es fehlen Dateien oder Dateien sind nicht lesbar. Im günstigsten Fall ist nur das Dateisystem in Unordnung geraten. Mit geeigneten Rettungstools lässt es sich in der Regel reparieren oder Sie können einzelne Dateien wiederherstellen.

Physischer Defekt: Es kann auch sein, dass eine Festplatte physisch defekt ist – manchmal an leisen Klack-Geräuschen zu erkennen. Ein Indiz ist, dass das Bios des PCs die Festplatte nicht mehr erkennt. Prüfen Sie das im Bios. Untersuchen Sie auch den festen Sitz der Anschlusskabel der Festplatte. Diese können sich etwa beim Transport des PCs lockern. Probieren Sie mit einem Rettungssystem aus, ob die Festplatte hier erkannt wird. Ein weiterer Test sollte in einem zweiten PC oder über einen SATA-USB-Adapter erfolgen, um einen defekten SATA-Adapter auszuschließen. Wenn sich die Festplatte trotzdem nicht ansprechen lässt, können Sie selbst nichts mehr machen. Sie müssen dann überlegen, wie viel Geld Ihnen die Daten wert sind.

Professionelle Datenrettung ist aufwendig und damit teuer. Holen Sie zuerst einen Kostenvoranschlag ein, bevor Sie den Auftrag erteilen. Angebote finden Sie beispielsweise bei Kroll Ontrack (*www.krollontrack.de*) oder Convar (*www.convar.com*).

2. Schnelle Datenrettung

Wenn das installierte Linux-System nicht mehr startet, kommen Sie trotzdem an Ihre Dateien heran. Die Voraussetzung dafür ist, dass sich das Dateisystem noch einhängen lässt. Wenn nicht, lesen Sie in -> Punkt 3 weiter. Außerdem benötigen Sie eine zweite interne oder externe Festplatte, auf die Sie die Dateien sichern können.

Booten Sie den PC von der LinuxWelt-DVD und wählen Sie im Menü die LinuxWelt-Rettungs-DVD (siehe Seite 66). Im LinuxWelt-Rettungssystem gehen Sie im Menü auf „System -> Show File Systems“. Sie sehen eine Übersicht mit den gefundenen Laufwerken und Partitionen.

Anhand der Größe identifizieren Sie die Linux-Systempartition, beispielsweise „sda1“, oder eine andere Partition, auf die Sie zugreifen möchten.

Wechseln Sie zum root-Terminalfenster, das sich beim Start des Systems automatisch geöffnet hat. Hängen Sie die Partition in das Dateisystem ein:

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

Passen Sie den Gerätepfad „/dev/sda1“ für Ihr System an. Hängen Sie dann die Backupfestplatte ein (Beispiel):

```
mount /dev/sdb1 /mnt/backup
```

Die Mountordner „/mnt/custom“ und „/mnt/backup“ müssen allerdings bereits vorhanden sein.

Starten Sie den Dateimanager über „System -> Thunar-Dateiverwaltung“, klicken Sie auf „Dateisystem“ und navigieren Sie zu „/mnt/custom“. Die Dateien und Ordner aus Ihrem Home-Verzeichnis finden Sie unter „/mnt/custom/home/[Benutzername]“.

Es empfiehlt sich, über „Datei -> Neues Fenster“ ein zweites Thunar-Fenster mit dem Ordner „/mnt/backup“ zu öffnen. Sie können Dateien oder Ordner dann bequem per Drag & Drop, mit Strg-C und Strg-V oder auch über die Kontextmenüpunkte „Kopieren“ und „Einfügen“ sichern.

Kopierprobleme: Sollte das Kopieren einzelner Dateien über Thunar fehlschlagen, weil die Dateien beschädigt sind, verwenden Sie das Tool safecopy:

```
safecopy [Quelle]/dokument.odt
  [Ziel]/dokument_rettung.odt
```

Die Platzhalter „[Quelle]“ und „[Ziel]“ ersetzen Sie durch die kompletten Pfade zu den Dateien unterhalb von „/mnt/custom“ und „/mnt/backup“. Das Tool versucht, die Quelldateien Byte für Byte zu lesen. Was unlesbar bleibt, füllt es mit Nullen auf. Diese Methode eignet natürlich nicht für jeden Dateityp. Am besten arbeitet das Tool bei gewöhnlichen Textdateien, aber auch Bildformate und Sounddateien sind aufgrund ihrer Struktur robust.

3. Abbild von Datenträgern

Sollte das Dateisystem stark beschädigt sein, lässt es sich über mount nicht einhängen. Es empfiehlt sich, nicht direkt mit dem Laufwerk zu arbeiten, sondern ein Abbild zu erstellen. Dadurch vermeiden Sie weitere Schäden. Das geeignete Programm dazu ist ddrescue, das direkt von Geräten liest und dabei defekte Blöcke überspringt:

```
ddrescue -n /dev/sda1 /mnt/backup/
  image.img /mnt/backup/fehler.log
```

„/dev/sda1“ ist der Gerätepfad zur Systempartition, die Sie über „System -> Show File Systems“ ermittelt haben (siehe -> Punkt 2). Wenn die Dateien auf einem USB-Stick, einer SD-Karte oder einer anderen Festplatte liegen, funktioniert das entsprechend. Auf dem Ziellaufwerk, das unter „/mnt/backup“ eingehängt ist, muss genügend Platz vorhanden sein, um das Image des defekten Datenträgers aufzunehmen.

Wenn ddrescue sich über Lesefehler beschwert, dann setzen Sie das Tool in einem zweiten Durchlauf nochmal auf die Disk an, um möglichst alle Blöcke in der Logdatei gezielt zu retten:

```
ddrescue -d /dev/sda1 /mnt/backup/
  image.img /mnt/backup/fehler.log
```

Das Tool beginnt nun, die im ersten Durchlauf als fehlerhaft markierte Sektoren in kleinere Blöcke zu unterteilen, um zumindest einen Teil der Daten zu retten. Das kann je nach Kapazität und Fehlermenge viele Stunden dauern.

4. Daten aus Abbilddatei retten

Das gerettete Image lässt sich wie ein Laufwerk behandeln und Sie können das Tool fsck zum Beheben von Dateisystemfehlern anwenden. Sie müssen die zum Dateisystem passende Variante verwenden. Für das Dateisysteme Ext4 geben Sie folgenden Befehl ein:

```
fsck.ext4 /mnt/backup/image.img
```

Bei Fat32 kommt fsck.vfat zum Einsatz. Gelingt die Wiederherstellung, dann können Sie die Imagedatei einhängen und auf deren Inhalt zugreifen. Erstellen Sie den Ordner „/mnt/image“, und hängen Sie das Festplattenabbild mit diesem Befehl ein:

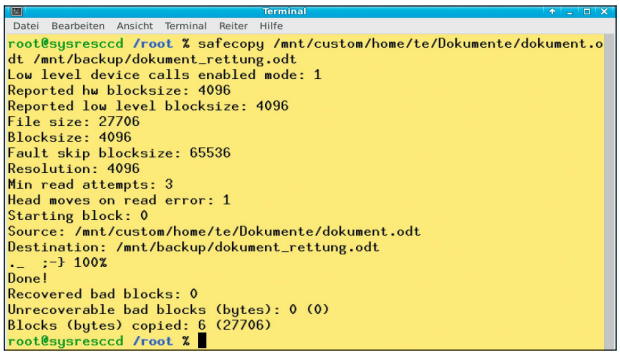
```
mount /mnt/backup/image.img /mnt/
  image
```

Über den Dateimanager Thunar kopieren Sie Dateien und Ordner wie unter -> Punkt 2 beschrieben.

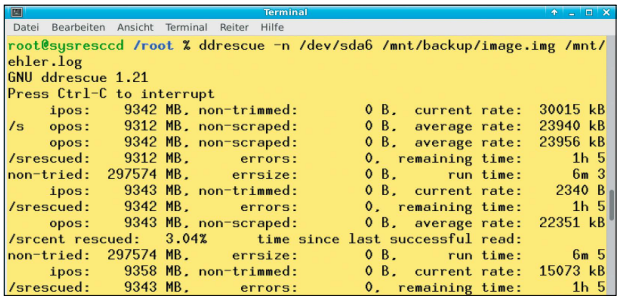
Im Prinzip können Sie die reparierte Imagedatei mit dd wieder auf die Festplatte schreiben:

```
dd if=/mnt/backup/image.img of=/
  dev/sda1
```

Wir empfehlen das jedoch nicht. Installieren Sie Linux besser neu und stellen Sie die persönlichen Dateien aus der Imagedatei wieder her. Beobachten Sie, ob das System ohne Probleme läuft und ob nicht doch ein Festplattendefekt Ursache für den Fehler war. Im Zweifelsfall tauschen Sie das Laufwerk besser aus. ●



Safecopy in Aktion: Das Kommandozeilentool versucht, auch von nicht mehr einwandfrei lesbaren Datenträgern die angegebene Datei Byte für Byte zu kopieren.

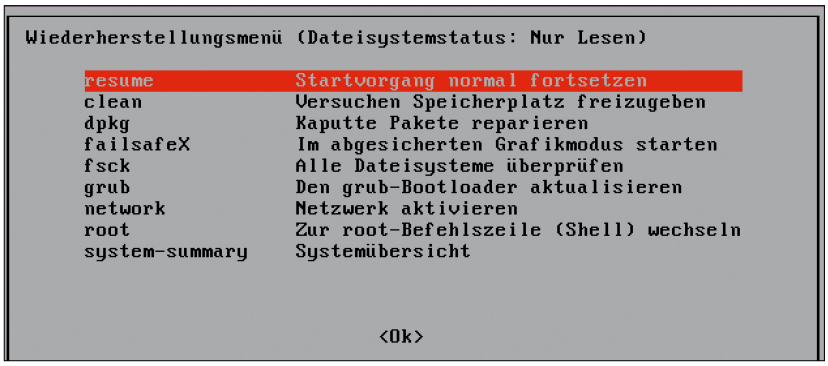


ddrescue: Das Tool ist spezialisiert, Daten von beschädigten Laufwerken in eine Imagedatei zu schreiben. Das Image lässt sich später als Laufwerk mounten.

Wenn Desktop und X-Server streiken

Probleme mit der grafischen Oberfläche sind bei Linux selten geworden. Sollte der Desktop dennoch fehlerhaft arbeiten, ist meist eine zerstörte Konfiguration dafür verantwortlich.

Von **Thorsten Eggeling**



Rettungssystem: Über das Wiederherstellungsmenü rufen Sie eine root-Befehlszeile auf, über die sich Fehler untersuchen und Treiber entfernen lassen.

Die Basiskonfiguration der grafischen Oberfläche (X-Server) erfolgt bei Linux automatisch. Wenn Grafikchip und Monitor richtig erkannt werden, ist die Darstellung auf dem Bildschirm optimal. Wenn sich der Desktop nicht mehr zeigt oder ständig abstürzt, obwohl direkt nach der Linux-Installation alles funktioniert hat, ist in der Regel eine fehlerhafte Konfiguration oder ein unbrauchbarer Treiber schuld. Wir beziehen uns in diesem Artikel auf Ubuntu 16.04 LTS. Bei anderen Distributionen läuft die Reparatur ähnlich ab, die einzelnen Schritte können sich jedoch deutlich unterscheiden.

1. Desktopprobleme untersuchen

Wir gehen in diesem Artikel davon aus, dass nach der Installation des Linux-Systems der Desktop bereits zu sehen und zu benutzen war. Beim Linux-Desktop sind zwei Problemfelder zu unterscheiden:

A. Fehlerhafte oder auch fehlende Treiber sorgen dafür, dass der Desktop überhaupt nicht erscheint beziehungsweise der für die Darstellung erforderliche X-Server nicht startet (siehe Punkt 2). Es kann zwar Startversuche geben, aber der Bildschirm bleibt schwarz. Oder die Bildschirmauflösung ist extrem niedrig und der Desktop fast unbenutzbar.

B. Sollte der Anmeldebildschirm erscheinen und Probleme etwa mit Anwendungen oder der Steuerung des Desktops treten erst nach der Anmeldung auf, ist wahrscheinlich nur die Konfiguration des Desktops oder von Anwendungen beschädigt.

Problem B lässt sich relativ leicht ausschließen und beheben. Wechseln Sie mit der Tastenkombination Strg-Alt-F1 auf eine Textkonsole und melden Sie sich an. Beenden Sie den Window-Manager mit dieser Befehlszeile:

```
sudo service lightdm stop
```

Benennen Sie Ihr Home-Verzeichnis um, erstellen Sie ein neues Home-Verzeichnis und setzen Sie folgendermaßen die Zugriffsrechte:

```
sudo mv /home/sepp /home/sepp.bak
sudo mkdir /home/sepp
sudo chown sepp:sepp /home/sepp
```

Den Namen unseres Beispielnutzers „sepp“ ersetzen Sie durch die Bezeichnung Ihres Benutzerkontos. Danach starten Sie mit diesem Befehl wieder den Window-Manager:

```
sudo service lightdm start
```

Melden Sie sich an und testen Sie das System. Wenn keine Probleme mehr auftauchen, muss der Fehler in den Konfigurationsdateien aus Ihrem Home-Verzeichnis liegen. Damit beginnt dann der mühsamere Teil der Problemanalyse. Sie können einzelne Ordner oder Unterordner nach und nach aus der Sicherungskopie („[Benutzername].bak“) in das Home-Verzeichnis kopieren. Die Konfigurationsverzeichnisse beginnen mit einem Punkt und werden erst sichtbar, wenn Sie im Dateimanager „Ansicht -> Verborgene Dateien anzeigen“ wählen. Sinnvoll ist das vor allem für Verzeichnisse wie „.mozilla“ und „.thunderbird“, in denen Firefox beziehungsweise Thunderbird nicht nur die Konfiguration, sondern auch gespeicherte Formulardaten und Passwörter ablegen. Bei den meisten anderen Programmen und den Desktopeinstellungen geht eine Neukonfiguration oft schneller als die Suche nach der vorherigen Konfigurationsdatei.

Hinweis: Sollte der Wechsel auf eine Textkonsole mit Strg-Alt-F1 nicht klap-

pen, benennen Sie das Home-Verzeichnis über das Ubuntu-Recovery-System (siehe -> Punkt 2) oder die LinuxWelt-Rettungs-DVD (siehe Seite 66) um.

2. Treiberprobleme beheben

Bei Problemen mit dem Grafiktreiber hilft es in der Regel, die Standardeinstellungen wiederherzustellen. Dazu starten Sie Ubuntu im Recovery-Modus. Sollte bei Ihrer Installation das Grub-Bootmenü nicht automatisch erscheinen, halten Sie beim Start des PCs die Shift-Taste gedrückt. Im Bootmenü gehen Sie auf „Erweiterte Optionen für Ubuntu“ und wählen dann den ersten Eintrag „(recovery mode)“. Sie sehen das „Wiederherstellungsmenü“ mit einigen Optionen.

Der Menüpunkt „failsafeX“ ist für den Start im abgesicherten Grafikmodus gedacht. Darüber lassen sich auch Probleme beim Start des X-Servers ermitteln. Sie können beispielsweise Fehlermeldungen einsehen. Es gibt auch die Menüpunkte „Try running with default graphical mode“ und „Reconfigure graphics“. Die haben jedoch auf keinem unserer Testgeräte zum Erfolg geführt. Die Neukonfiguration des X-Servers ist ohnehin nicht vorgesehen, weil es standardmäßig keine Konfigurationsdatei mehr gibt. Die Konfiguration erfolgt vollautomatisch anhand der erkannten Hardware.

Treiber entfernen oder installieren: Gehen Sie im Menü auf „network“ und dann auf „root“. Bestätigen Sie mit der Eingabetaste. Über die Kommandozeile haben Sie jetzt schreibgeschützten Zugriff auf das Dateisystem. Um das zu ändern,verwenden Sie folgende Befehlszeile:

```
mount -o remount,rw /
```

Prüfen Sie, ob eine möglicherweise fehlerhafte und unnötige Konfigurationsdatei vorhanden ist:

```
cat /etc/X11/xorg.conf
```

Wird ein Inhalt ausgegeben, benennen Sie die Datei um:

```
mv /etc/X11/xorg.conf /etc/X11/
  xorg.conf.bak
```

Da wahrscheinlich ein falscher oder fehlerhafter Treiber den Start des X-Servers verhindert, entfernen Sie nachträglich installierte Treiber. Bei einem Nvidia-Chipsatz verwenden Sie

```
sudo apt-get purge nvidia*
```

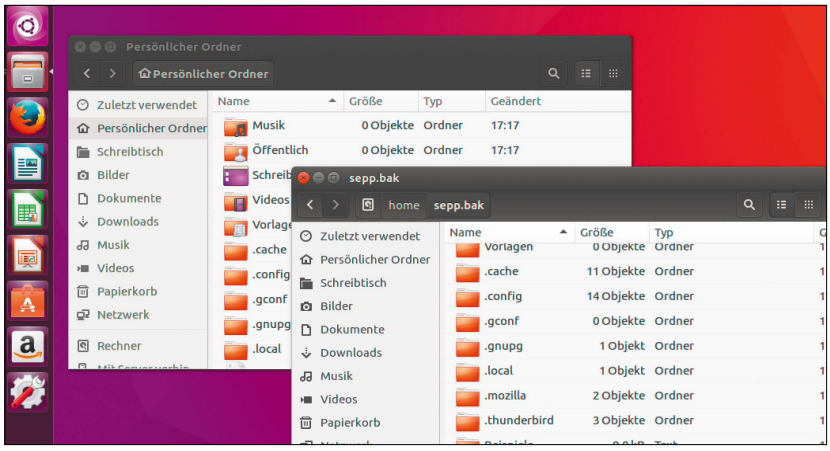
und bei einem AMD/ATI-Chipsatz

```
sudo apt-get purge fglrx*
```

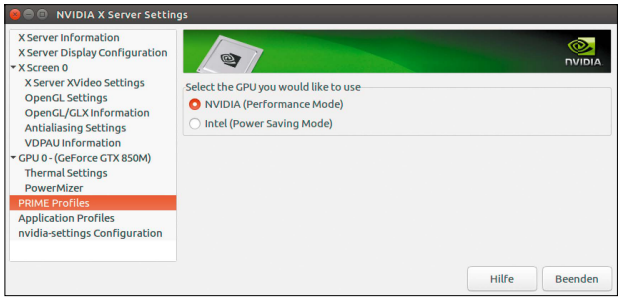
Ohne proprietäre Treiber verwendet Linux wieder den Standardtreiber. Mit *reboot* verlassen Sie das Rettungssystem und starten Linux neu. Die grafische Oberfläche sollte jetzt wieder starten.

Gehen Sie in den Systemeinstellungen auf „Anwendungen & Aktualisierungen“ und die Registerkarte „Zusätzliche Treiber“. Hier sehen Sie, ob für den Grafikchip proprietäre Herstellertreiber verfügbar sind.

Die Herstellertreiber leisten fast immer mehr als die Linux-Standardtreiber. Wählen Sie den Eintrag mit dem Zusatz „Proprietär, getestet“. Sollte dieser erneut Probleme bereiten, wiederholen Sie die oben beschriebenen Schritte im Rescuesystem. In diesem Fall bleiben Sie beim Standardtreiber, bis das Problem durch ein Treiberupdate behoben ist.



Desktopkonfiguration zurücksetzen: In einem leeren Home-Verzeichnis erzeugt Ubuntu automatisch eine neue und saubere Standardkonfiguration.



Energie sparen: Bei Notebooks mit Hybridgrafik aktivieren Sie den Nvidia-Treiber nur, wenn Sie die Leistung brauchen. Mit dem Intel-Treiber hält der Akku länger durch.

3. Notebooks mit zwei Grafikchips

Wenn sich beim Linux-Notebook der Akku zu schnell leert, kann der verwendete Grafiktreiber daran schuld sein. Notebooks sind häufig mit Hybridgrafik ausgestattet. Standardmäßig sollte hier der Grafikadapter des Intel-Prozessors aktiv sein. Dadurch sinkt die Leistungsaufnahme und der Akku hält länger durch. Ist mehr Leistung für HD-Videos und Spiele erforderlich, kommt der Nvidia-Chip zum Einsatz. Die Umschaltung funktioniert nur, wen Sie den Nvidia-Treiber über „Zusätzliche Treiber“ installiert haben (siehe -> Punkt 2). Suchen Sie bei Ubuntu über das Dash nach „Nvidia“ und starten Sie „Nvidia X Server Settings“. Gehen Sie auf „PRIME Profiles“. Aktivieren Sie die Option „Intel (Power Saving Mode)“ und bestätigen Sie mit dem root-Passwort. Danach melden Sie sich bei Ubuntu ab und wieder an. Für höhere Geschwindigkeit schalten Sie wieder auf den Nvidia-Adapter um, indem Sie die Option „NVIDIA (Performance Mode)“ aktivieren. ●

Zugriff erlaubt, Zugriff verboten

Kein Zugriff auf Dateien und Ordner? Die Rechteverwaltung im Linux-Dateisystem stammt von Unix: root, Benutzer und Gruppen sind einfache Grundlagen. Einige Szenarien verlangen trotzdem trickreiche Lösungen.



Von **David Wolski**

Die Systematik der Unix/Linux-Zugriffsrechte im Dateisystem ist einfach gehalten, aber äußerst wirksam. Für Server und Mehrbenutzersysteme ist Linux damit ideal, schließlich wollen systemnahe Dateien wirksam durch Zugriffe durch unprivilegierte Benutzer und deren Prozesse geschützt sein. Bei der Administration des eigenen Linux-Systems kann es nach größeren Konfigurationsänderungen aber immer wieder mal wieder Ärger mit Zugriffsrechten geben. Wenn Dateimanager oder die Kommandozeile „Zugriff verweigert“ beziehungsweise „Permission denied“ bei Dateizugriffen melden oder Editoren geöffnete Dateien nicht speichern wollen, dann fehlen die Rechte auf die Datei oder das Verzeichnis. Auslöser sind meist Nachlässigkeiten bei der Arbeit mit sudo oder mit dem root-Konto. Die typischen Zugriffsprobleme sind aber auch schnell wieder behoben.

Übrigens sind Zugriffsrechte unter Linux nur auf Unix-Dateisystemen relevant und dauerhaft. Externe Datenträger mit den Windows-Dateisystemen FAT, exFAT und NTFS bekommen für alle Dateien die Rechte des aktiven Benutzers zugewiesen.

Kein Zugriff: Dateien und Ordner

Ein häufiges Szenario unzureichender Zugriffsrechte im Dateisystem spielt sich im eigenen Home-Verzeichnis ab: Dort abgelegte Dateien oder Ordner verweigern dem Benutzer wegen fehlender Rechte den Zugriff. Ein Auslöser, der solche Dateien und Verzeichnisse überhaupt erst entstehen lässt, sind meist mit dem root-Account oder über sudo ausgeführte Aktionen oder Scripts, die Ordner und Dateien anlegen. Die Lösung besteht in einer Änderung der Besitzrechte in der Kommandozeile mit dem Befehl chown. Generell dürfen Rechte an Dateien und Ordnern, die anderen Benutzern oder root gehören, auch nur wieder mit root-Privilegien geändert werden, deshalb verlangt dieser Befehl ein vorangestelltes sudo oder einen Wechsel zum root-Konto mit su:

```
sudo chown [Benutzer] [Datei/Ordner]
```

Dies ändert den Besitzer einer angegebenen einzelnen Datei auf den angegebenen Benutzer. Handelt es sich beim Ziel um eine ganze Ordnerstruktur mit Dateien und Unterverzeichnissen, so arbeitet chown mit dem Parameter „-R“ auch rekursiv:

```
sudo chown -R [Benutzer] [Ordner]
```

Nicht ausführbar: Scripts und Programme

Ausführbare Dateien unter Linux müssen in ihren Zugriffsrechten als ausführbar gekennzeichnet sein, ansonsten wird sie das System nicht einfach starten. Auch Programmdateien, die von externen Medien stammen, welche mit Windows-Dateisystem formatiert sind, lassen sich zunächst nicht ausführen. In der Kommandozeile fügt der Befehl

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

das Ausführen-Bit hinzu und anschließend ist die Script- oder Programmdatei im aktuellen Verzeichnis mit dem Aufruf *./[Datei]* ausführbar. Linux geht dabei nicht nach der Dateiendung, um den Typ des Scripts oder Programms zu erkennen.

Binaries haben eine typische Bytefolge am Anfang der Datei. Bei Scripts gibt die erste Zeile, beispielsweise

„#!/bin/bash“ vor, welcher Script-Interpreter gefragt ist.

Sicherheitslücke: Unbegrenzter Vollzugriff

Wer keine Gruppen für gemeinsame Zugriffsrechte für Verzeichnisse und Dateien einrichtet, behilft sich oft mit einer simplen, aber potenziell unsicheren Vereinfachung: Dateien bekommen die kurzerhand mit chmod die oktalen Zugriffsrechte 666 oder im Fall von Verzeichnissen gar die Rechte 777 zugewiesen. So hat alle Welt Vollzugriff auf diese Dateisystem-Objekte. Auf externen Datenträgern mit Unix-Dateisystem wie Ext2/3/4, die aber trotzdem überall lesbar und beschreibbar sein sollen, ist das in Ordnung. Aber auf Servern und auf den meisten Desktop-PCs ist dies schlicht ein Konfigurationsfehler und eine Sicherheitslücke. Denn auch unprivilegierte Benutzer und Prozesse könnten diese Dateien und Verzeichnisse manipulieren.

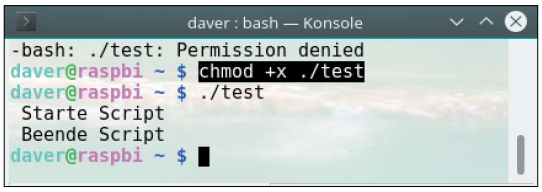
Es gilt deshalb, zunächst Dateien und Verzeichnisse mit unbeschränkten Zugriffsrechten ausfindig zu machen. Das Kommando

```
sudo find / -path /proc -prune -o
  -type f -perm 666
```

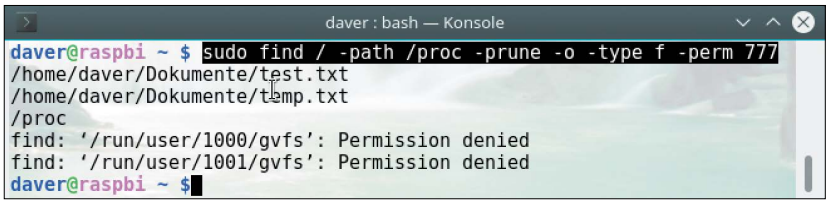
findet alle Dateien im gesamten Dateisystem, ausgenommen „/proc“, die von allen gelesen und beschrieben werden dürfen, und

```
sudo find / -path /proc -prune -o
  -type f -perm 777
```

listet Dateien auf, die dazu noch ausführbar sind. Genauso findet



Um eine Script-Datei oder ein Programm auszuführen, müssen Sie dieses unter Linux ausführbar schalten. Dazu setzen Sie mit chmod das Execute-Bit.



Zu laxe Zugriffsrechte: Der Befehl find durchsucht das gesamte Dateisystem ausgenommen „/proc“, nach Dateien mit den oktalen Rechten 777, das heißt – für alle beschreibbar.

```
sudo find / -path /proc -prune -o
  -type d -perm 777
```

Verzeichnisse, die allen zum Lesen und Schreiben offen stehen.

Ein besserer Weg: Anstatt für Dateien und Verzeichnisse uneingeschränkten Vollzugriff zu setzen, ist es sinnvoll, Gruppen für gemeinsam genutzte Dateien und Verzeichnisse zu verwenden. Der Befehl

```
chgrp [Gruppe] [Datei/Ordner]
```

ändert die Gruppe von Dateisystem-Objekten. Für den Vollzugriff für Besitzer und Gruppe genügen dann bei Verzeichnissen die Rechte 775 sowie bei Dateien 664.

Rechte: Dateien oder Ordner

Der Befehl chmod kann nicht zwischen Dateien und Verzeichnissen unterscheiden. Bei einer Anwendung des Befehls auf eine Ordnerstruktur hätte das unerwünschte Auswirkungen, da sich beispielsweise Verzeichnisse nicht mehr öffnen lassen, wenn man ihnen die Berechtigungen zum Ausführen entzieht (das „Ausführen“-Recht bedeutet bei Ordnern das Recht, sie zu öffnen). Stattdessen brauchen Sie ein trickreicheres Kommando, das Verzeichnisse in Ruhe lässt und sich nur um Dateien kümmert. Um alle Dateien in Ordnern und Unterordnern im aktuellen Verzeichnis für Besitzer und Gruppe les- und schreibbar zu machen, ohne dabei Zugriffsrechte für Verzeichnisse zu ändern, dient dieser Befehl:

```
find . -type f -exec chmod 664 {}
  \;
```

Analog dazu lässt sich find auch nur auf Verzeichnisse anwenden. Dazu ersetzen Sie den Parameter „f“ für „file“ gegen „d“ für „directory“:

```
find . -type d -exec chmod 775 {}
  \;
```

Dieser Befehl wendet chmod 775 nur auf Ordner und Unterordner an, nicht aber auf Dateien.

Berechtigungen: Auflistung mit ls

Das wichtigste Werkzeug zur Auflistung und Änderung von Zugriffsrechten im Dateisystem bleibt die Kommandozeile: Hier zeigt die Eingabe des Befehls

```
ls -lha
```

links in der Dateiliste die Zugriffsrechten. Lesen ist „r“, Schreiben entspricht „w“ und Öffnen beziehungsweise ausführen ist als „w“ angegeben.

Die erste Dreiergruppe betrifft den Besitzer der Datei, die zweite alle Benutzer seiner Gruppe und die dritte alle anderen Benutzer. Ein vorangestellter Buchstabe „d“ steht für Ordner (Directory).



Berechtigungen im Verzeichnis auflisten: Statt der oktalen Berechtigungsbits zeigt der ls-Befehl pro Dateisystemobjekt die Read-Write-Execute-Rechte in Dreiergruppen als „r“, „w“ und „x“.

Alles verschlüsselt!

Mobile Notebooks, handliche USB-Sticks, öffentliche Cloud: Alles, was das Haus und das heimische Netz verlässt, kann in fremde Hände gelangen oder ist bereits in fremden Händen. Verschlüsselung sorgt dafür, dass die Daten nichts Persönliches preisgeben.



Von **Hermann Apfelböck**

Hinsichtlich Datenschutz und Verschlüsselung spaltet sich die Gesellschaft so schizophren wie sonst auch: Die einen werfen ihre Privatsphäre bedenkenlos ins World Wide Web, die anderen sorgen sich bei jeder Dropbox-Datei, dass die NSA mitlesen könnte. Es ist aber nicht Ziel dieses Beitrags, die Naiven zu bekehren oder die Paranoiden zu beruhigen. Hier geht es allein um die technischen Möglichkeiten, die Linux in großer Vielfalt und Abstufung bereithält, um Daten zu verschlüsseln. Der Artikel stellt alle Methoden vor, bewertet sie und bringt eine vollständige Praxisanleitung für die Einrichtung und Nutzung.

1. Luks-verschlüsseltes Linux-System

Die kompromisslose Methode, die lokalen Daten vor Fremdzugriff zu schützen, ist die Verschlüsselung der kompletten Festplatte. Mit dem auf dem Kernelmodul dm-crypt basierenden Linux Unified Key Setup (Luks) lassen sich sowohl externe USB-Datenträger (-> Punkt 2) als auch die Systemfestplatte selbst sicher verschlüsseln. Wir beginnen mit dem technisch anspruchsvollsten Szenario der verschlüsselten Systemfestplatte, da es durch moderne Installer zur einfachen Übung gerät und bei der Alltagsbenutzung nicht mehr Aufwand bedeutet als die Schlüsseleingabe beim Systemstart.

Trotzdem sollte sich jeder Anwender, der seine Systemfestplatte verschlüsselt, im Klaren sein, dass die Partitionierung komplexer wird und bei Bootproblemen höheren Reparaturaufwand verursacht.

Empfehlung: Eine Luks-verschlüsselte Systemfestplatte ist die richtige Maßnahme für Notebooks, die viel unterwegs sind und auch jenseits des Home-Verzeichnisses vertrauliche und private Daten enthalten. Der verschlüsselte Datenträger lässt beim Booten durch ein Fremdsystem keinerlei Einblick in die Verzeichnisstruktur und in die Daten zu. Das Einzige, was ein Fremdzugriff anhand der Partitionierungsfakten in Erfahrung bringen kann, ist die Tatsache, dass die Festplatte Luks-verschlüsselt ist.

Installation mit Luks und LVM: Es gibt diverse grafische Linux-Installer, die beim Setup eine Luks-verschlüsselte Systempartition einrichten können. Neben Yast unter Open Suse, dem Debian-Installer und dem Fedora-Installer bieten alle Ubuntu-basierten Distributionen inklusive Linux Mint den Installer Ubiquity, der dies beherrscht. Die folgende Anleitung orientiert sich an Ubiquity. Beachten Sie aber, dass der Ubuntu-Installer den bequemen Weg zur Luks-verschlüsselten Systemfestplatte nur anbietet, wenn Sie ihm dafür die gesamte primäre Festplatte überlassen. Eine kompliziertere Situation mit Multiboot oder anderweitigen Partitionsaufteilungen ist nicht vorgesehen. Die Festplatte wird bei diesem Vorgang komplett gelöscht.

Starten Sie die Installation im Livesystem eines Ubuntu-Systems und folgen Sie dem Setupassistenten bis zum Punkt „Installationsart“. Hier wählen Sie die erste Option „Festplatte löschen und […] installieren“. Darunter aktivieren Sie das Kästchen „Die neue Ubuntu-Installation zur Sicherheit ver-

schlüsseln“. Sobald Sie dies tun, wird zugleich der weitere Punkt „LVM […] verwenden“ aktiv. Der Logical Volume Manager ist eine Abstraktionsschicht, um Festplatten und Partitionen flexibler zu verwalten, zusammenzufassen und dynamisch zu erweitern. In diesem Fall ist LVM notwendig, um neben der kleinen unverschlüsselten Bootpartition die Luks-formatierte Partition und die virtuelle LVM-Partition unterzubringen, die bei korrekter Kennworteingabe unverschlüsselt ins Dateisystem geladen wird.

Wenn Sie im Assistenten mit den genannten Optionen auf „Weiter“ klicken, folgt noch die Abfrage des Sicherheitsschlüssels. Dieses Kennwort sollte komplex genug sein, um vom Assistenten als „Starkes Passwort“ gelobt zu werden. Andererseits muss die Eingabe zumutbar bleiben, denn sie ist künftig bei jedem Systemstart erforderlich. Die weitere Installation unterscheidet sich nicht mehr von einem üblichen Ubuntu-Setup.

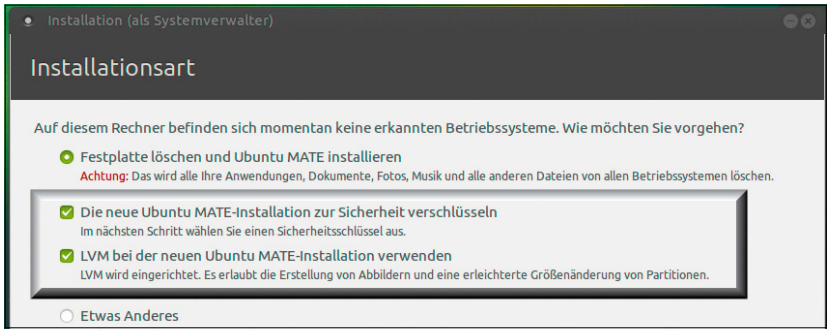
Wenn Sie ein Luks-verschlüsseltes System booten, erscheint künftig das Eingabefeld „Please unlock disk […]“. Dort geben Sie das Passwort ein und erst danach kann der Systemstart fortsetzen, wobei das Luks-Volume entsperrt und unverschlüsselt nach „/dev/mapper/[sd…]“ gemountet wird.

2. Luks-verschlüsselte (USB-)Datenträger

Interne Laufwerke, die als reine Datenpartition dienen, sowie externe USB-Datenträger lassen sich ebenfalls mit Luks verschlüsseln. Technisch ist dies weniger anspruchsvoll und kommt ohne LVM-Unterstützung aus.

Die Einrichtung und Benutzung erfolgt auf modernen Linux-Distributionen komplett mit grafischen Werkzeugen, die den komplizierteren Weg über Terminalbefehle in der Regel überflüssig machen.

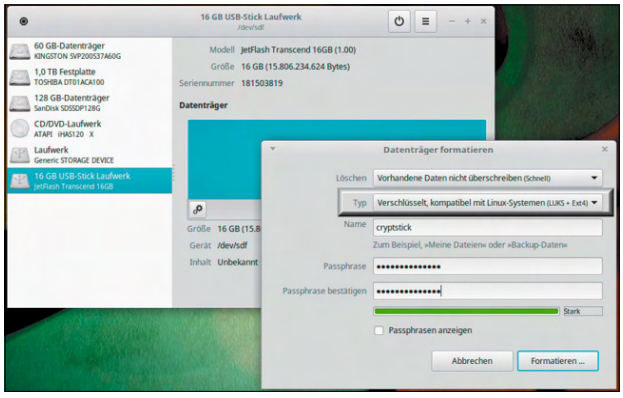
Empfehlung: Besonders USB-Sticks und handliche USB-Festplatten gehen oft verloren oder werden vergessen. Luks ist für mobile Speicher erste Wahl, sofern die Datenträger überwiegend mit Linux gelesen und beschrieben werden. Überall dort, wo auch ein Windows oder ein Mac-OS zugreifen soll, ist Veracrypt (-> Punkt 6) die bessere Option.



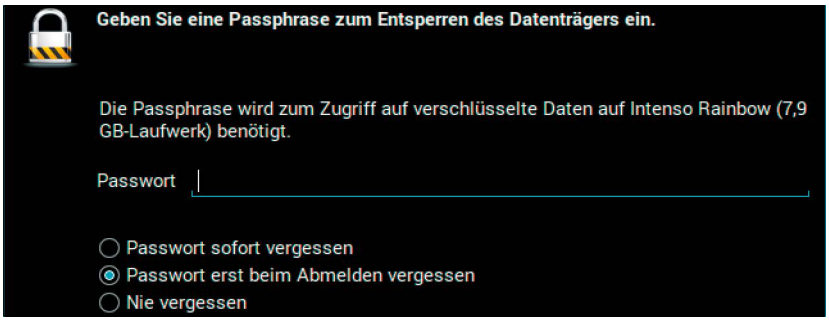
Dies ist die entscheidende Einstellung beim Ubuntu-Installer. Mit LVM und Luks-Verschlüsselung bootet das System erst nach korrekter Kennworteingabe.

Einrichten mit grafischen Werkzeugen: Erfreulicherweise hat Luks-Verschlüsselung in die Systemwerkzeuge längst Einzug gehalten. Die KDE-Umgebung bietet den „KDE Partition Manager“ (partitionmanager), und die Gnome-affinen Desktops (Gnome, Mate, Unity, Cinnamon, XFCE) haben das Tool „Laufwerke“ (gnome-disks) an Bord. Wir beschreiben die wenigen Klicks zur Luks-Verschlüsselung eines USB-Laufwerks am Beispiel von gnome-disks: Nach Anschließen des USB-Datenträgers hängen Sie das Laufwerk zunächst mit dem kleinen schwarzen Symbol links unterhalb der Partitionsanzeige aus. Danach klicken Sie auf das Zahnradsymbol und verwenden die Option „Partition formatieren“. Im Folgedialog wählen Sie als „Typ“ den Eintrag „Verschlüsselt, kompatibel mit Linux-Systemen (LUKS + Ext4)“. Der Eintrag „Name“ ist nicht unbedingt erforderlich, macht aber den späteren Mountpunkt lesbarer. Entscheidend ist darunter die „Passphrase“ – also das Kennwort. Hier gilt wie unter Punkt 1: Das Kennwort sollte komplex sein, die Eingabe aber zumutbar bleiben, denn sie ist künftig bei jeder Nutzung des Datenträgers erforderlich. Mit Klick auf „Formatieren“ schließen Sie den Vorgang ab. Sie können nach der Formatierung den Datenträger sofort mit gnome-disks einhängen und nutzen, indem Sie auf den unteren Balken der symbolischen Anzeige klicken und die Partition mit dem Pfeilsymbol links einhängen.

Für die künftige Alltagsbedienung genügen die typischen Dateimanager Nautilus, Nemo, Caja, Dolphin. Wenn Sie das USB-Gerät anschließen, erscheint nach kurzer Frist automatisch der Dialog „Geben Sie eine Passphrase zum Entsperren […] ein“. Nach Eingabe des korrekten Kennworts ist das Medium entsperrt und im Dateimanager unter „Geräte“ normal benutzbar. An gleicher Stelle im Datei-



Luks-Verschlüsselung für USB-Datenträger: Diese Aufgabe beherrschen die typischen Partitionsmanager von Desktopdistributionen – hier gnome-disks unter Linux Mint.



Automatischer Dialog: Luks-verschlüsselte USB-Sticks lösen beim Anschluss diese Abfrage aus. Bei korrekten Kennwort erscheint das Laufwerk im Dateimanager.

manager können Sie den Datenträger dann wieder trennen („Laufwerk sicher entfernen“).

3. Verschlüsseltes Home-Verzeichnis (Ecrypt FS)

Ubuntu-Systeme einschließlich Linux Mint machen bei der Installation das Angebot, das Home-Verzeichnis zu verschlüsseln. Diese Option ist bei einer Neuinstallation immer gut zu überlegen, zumal sie nachträglich für den ersteingerichteten Benutzer nicht mehr vorgesehen ist und dann doch einige Klimmzüge erfordert. Technisch zuständig ist in diesem Fall das Modul Ecrypt FS, das Ubuntu & Co. standardmäßig im Kernel mitbringen. Ecrypt FS ist nicht zu verwechseln mit Enc FS (-> Punkt 5), wenngleich sich beide Techniken ähneln.

Empfehlung: Ein Ecrypt-FS-verschlüsseltes Home-Verzeichnis ist für typische Desktopsysteme, auch für mobile Notebooks, oft der angemessene und der komfortabelste Schutz. Bei Fremdzugriff ist zwar der Großteil des Dateisystems lesbar, nicht aber der Inhalt von „/home/[user]“. Dieser liegt verschlüsselt unter „/home/.ecryptfs/[user]/.Private“ und wird automatisch unverschlüsselt nach „/home/[user]“ geladen, sobald sich der Benutzer am System anmeldet. Wenn sich der Gerätebesitzer daran hält, seine Daten stets unter „/home“ abzulegen, ist für Datendiebe nichts zu holen. Lediglich die Anzahl der Verzeichnisse und Dateien sowie deren ungefähre Größen sind unter „/home/.ecryptfs/[user]/.Private“ ersichtlich – die Inhalte nicht. Die Dateinamen sind ebenfalls verschlüsselt.

Einrichten der Home-Verschlüsselung: Bei der Installation von Ubuntu-Systemen erscheint zu einem späteren Zeitpunkt das Fenster „Wer sind Sie?“. Hier legen Sie den Erstbenutzer des Systems an. An unterster Stelle gibt es die Option „Meine persönlichen Daten verschlüsseln“. Ein Häkchen genügt, um Ecrypt FS für das Home-Verzeichnis des Erstbenutzers zu aktivieren. Nach der ersten Anmeldung am neu installierten System erscheint dann ein

Exkurs: Manuelle Luks-Verschlüsselung

Luks-Verschlüsselung für ein externes USB-Laufwerk kann auch ohne grafische Werkzeuge etwa auf einem Headless-Server eingerichtet werden. Die folgende Ergänzung zu den Punkten 1 und 2 dient nicht nur der Vollständigkeit, sondern soll auch die zugrunde liegenden Werkzeuge vorstellen, die unter der Haube auch von grafischen Tools wie gnome-disks genutzt werden. Zunächst ermitteln Sie mit

```
lsblk
```

die Gerätekennung des USB-Datenträgers. Alle folgenden Kommandos gehen von der Beispielkennung „/dev/sde“ aus, die in Ihrem Fall natürlich anders lauten kann und unbedingt entsprechend angepasst werden muss. Zunächst wird die Partitionstabelle des Sticks mit fdisk neu geschrieben:

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

Geben Sie am fdisk-Prompt „o“ ein. Dieser Befehl legt eine neue DOS-Partitionstabelle an. Sie müssen die Aktion anschließend mit dem Schreibbefehl „w“ realisieren, was zugleich fdisk beendet. Starten Sie dann fdisk erneut:

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

Jetzt legen Sie mit dem Befehl „n“ eine neue Partition an und verwenden dabei „p“ für „primary“, „1“ für Partition 1. Die zwei Abfragen der Start- und Endsektoren quittieren Sie einfach mit der Eingabetaste. Auch hier muss abschließend der Write-Befehl „w“ erfolgen, um die Aktion tatsächlich auf den Datenträger zu schreiben. Nun hängen Sie das Laufwerk mit

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

aus und formatieren es mit Luks. Das dazu notwendige Tool namens cryptsetup steht auf allen verbreiteten Distributionen zur Verfügung:

```
sudo cryptsetup luksFormat /dev/sde1
```

Der Parameter „luksFormat“ muss genau so eingegeben werden. Die nachfolgende Bestätigung mit „YES“ ist ebenfalls case-sensitiv und erfordert Großbuchstaben.

Dann werden Sie nach dem „Passsatz“ gefragt, also dem Zugangskennwort. Die Eingabe erfolgt ohne Textanzeige und ohne Stellvertreterzeichen.

Nun können Sie das Laufwerk mit „luksOpen“

```
sudo cryptsetup luksOpen /dev/sde1 Stick
```

in das System laden. Der Name, hier „Stick“, ist frei wählbar. Das Laufwerk wird nun unter „/dev/mapper/Stick“ gemountet. Zu guter Letzt braucht das Laufwerk neben Luks noch ein normales, unverschlüsseltes Dateiformat, was Sie mit

```
sudo mkfs.vfat /dev/mapper/Stick -n Stick
```

erledigen. Das war's. Entfernen Sie nun den Stick einfach vom Rechner. Die Prozedur ist für jeden USB-Datenträger nur einmal erforderlich.

Fenster mit dem Hinweis „Ihre Verschlüsselungspassphrase notieren“. Klicken Sie auf „Diese Aktion ausführen“.

Danach geben Sie das Systempasswort ein und bestätigen mit der Eingabetaste. Sie sehen dann das von Ubuntu & Co. zufällig generierte Passwort für die Home-Verschlüsselung. Notieren Sie sich dieses, denn Sie benötigen es für den (unwahrscheinlichen) Fall, dass einmal die Wiederherstellung eines defekten Dateisystems nötig werden sollte. Für den alltäglichen Zugriff auf das Home-Verzeichnis genügt die Anmeldung am System. Vor anderen Benutzern am selben PC ist das verschlüsselte Home-Verzeichnis ebenfalls sicher. Diese erhalten beim Zugriff eine Fehlermeldung, die auf fehlende Rechte hinweist. Besitzen andere Systembenutzer root-Recht, können Sie zwar den Ordner „/home/.ecryptfs/[user]/.Private“ betreten, sehen dort aber nicht mehr als verschlüsselte Ordner- und Dateinamen.

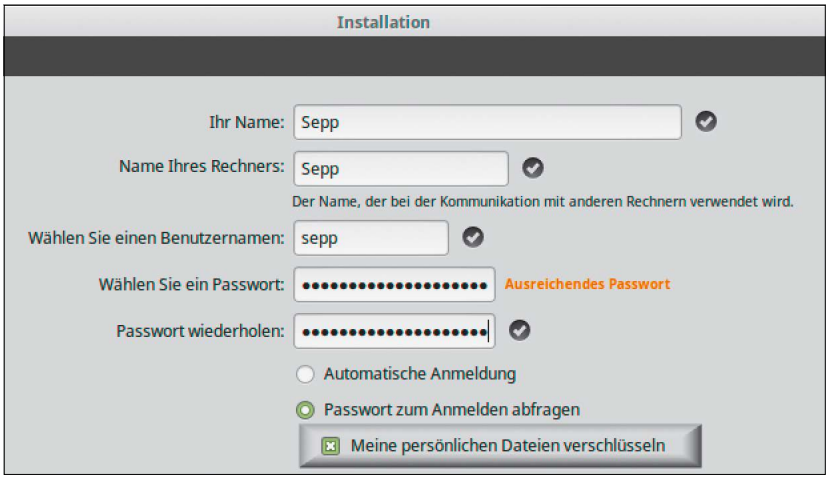
Weitere verschlüsselte Home-Verzeichnisse: Die Home-Verschlüsselung bei der Installation gilt nur für den dort eingerichteten Erstbenutzer. Wenn ein weiterer Benutzer ein verschlüsseltes Home-Verzeichnis erhalten soll, gibt es zwei Wege:

1. Die grafische Methode über „Einstellungen -> Benutzer/Users“ ist aktuell noch die Ausnahme. Linux Mint 18.2 bietet in der Benutzerverwaltung beim Anlegen eines neuen Kontos ganz unten die Option „Persönlichen Ordner verschlüsseln […]“.

2. Bei den meisten Distributionen ist die Home-Verschlüsselung nur über die Kommandozeile zu erreichen. Es genügt dieser Befehl:

```
sudo adduser --encrypt-home [user
 name]
```

Falls der Befehl scheitert, installieren Sie das Paket „ecryptfs-utils“ (*sudo apt install ecryptfs*) und wiederholen den Befehl. Legen Sie das Passwort für den neuen Benutzer hinter „Geben Sie ein neues UNIX-Passwort ein:“ fest. Danach geben Sie die Benutzerinformationen ein oder bestätigen einfach alles mit der Eingabetaste. Ab sofort kann sich der neue Benutzer anmelden und das verschlüsselte Home-Verzeichnis nutzen. Auch er erhält einen Hinweis, sich die Verschlüsselungspassphrase zu notieren.



Die Ubuntu-Installation kann das Home-Verzeichnis verschlüsseln. Das gilt jedoch nur für den Erstbenutzer. Für weitere Benutzer müssen Sie die Verschlüsselung selbst aktivieren.

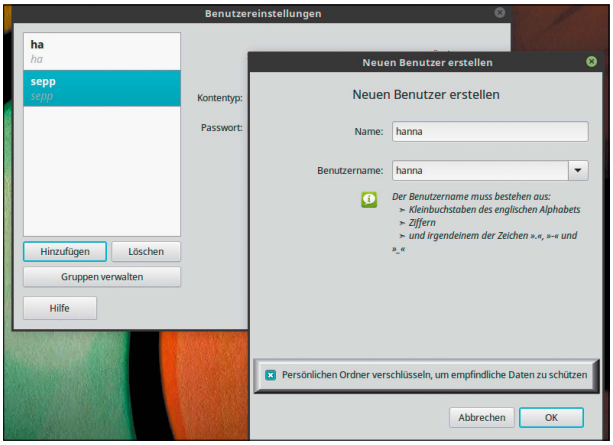
Home-Verzeichnis nachträglich verschlüsseln: Es ist nicht vorgesehen, die Verschlüsselung nachträglich zu aktivieren. Die einfachste Lösung ist es daher, alle Dateien im Home-Verzeichnis vorübergehend an einen anderen Ort zu verschieben, dann ein neues Benutzerkonto mit verschlüsseltem Home-Verzeichnis anzulegen und die gesicherten Dateien danach in das neue Home-Verzeichnis zu kopieren. Das ursprüngliche Konto kann danach im Prinzip gelöscht werden. Tun Sie dies aber erst, wenn der Systemalltag reibungslos funktioniert: So sollte zum Beispiel der sudo-berechtigte Erstbenutzer nicht gelöscht werden, solange kein neues Konto mit sudo-Recht eingerichtet ist (*visudo*).

4. Verschlüsselung mit Enc FS

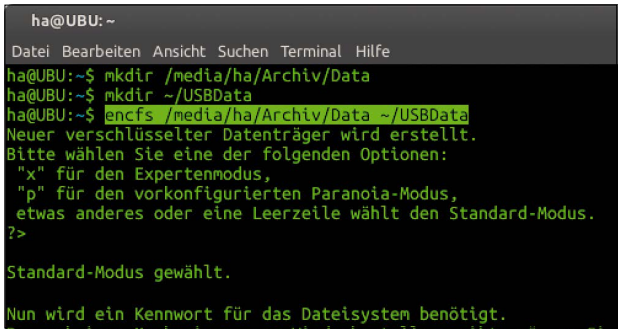
Enc FS ist ein flexibles ordner- und dateiorientiertes Verschlüsselungswerkzeug. Der Ruf des Tools hat etwas gelitten, nachdem vor Jahren eine theoretische Lücke bekannt wurde, welche die Robustheit von Enc FS infrage stellte. Diese Lücke besteht immer noch und wird bei der Installation des Pakets gemeldet. Unterm Strich handelt es sich aber um ein akademisches Problem, das normale Anwender nicht betrifft. Technisch ähnlich wie bei Ecrypt FS wird ein verschlüsselter Ordner durch Eingabe des richtigen Passworts entsperrt und der Inhalt unverschlüsselt in einen zweiten Ordner gemountet, wo die Dateien dann normal zu verwenden sind. Verschlüsselte Enc-FS-Ordner sind überall flexibel einzurichten – auf internen und externen Datenträgern mit FAT, FAT32, NTFS oder einem Linux-Dateisystem.

Empfehlung: Enc FS ist das richtige Werkzeug für alle Situationen, die im Alltag plötzlich Verschlüsselung ratsam erscheinen lassen: Dieses oder jenes Verzeichnis auf der USB-Festplatte hat Verschlüsselung verdient, ein Unterordner von „Home“ muss geschützt werden oder ein Clouddienst soll über den verschlüsselten Sync-Ordner nur noch geschützte Dateien bevorraten. Enc FS kann an jeder Stelle und auf jedem Datenträger einspringen und eignet sich auch für größere Datenmengen. Neben Linux können Android-Geräte mit der App Cryptonite Enc-FS-Daten lesen. Für Mac-Anwender gibt es nach einem gewissen Installationsaufwand ein praktisch identisches Enc FS. Für den Austausch mit Windows gibt es Encfs4win, das allerdings experimentell bleibt (*https://encfs.win*).

Enc FS mit grafischem Cryptkeeper: Enc FS ist meist nicht installiert,



Home-Verschlüsselung für neue Konten: In Linux Mint 18.2 erscheint diese Option im grafischen Benutzermanager, bei den meisten Distributionen ist der Gang ins Terminal erforderlich.



Ersteinrichtung eines Enc-FS-Ordners: Sie benötigen lediglich einen Ordner als Mountpunkt (hier „USBData“ im Home-Verzeichnis) und ein Kennwort.

doch finden Sie das relativ kleine Paket in den Repositories aller wichtigen Linux-Distributionen. Unter Ubuntu/Mint installieren Sie es mit

```
sudo apt install encfs
```

und können dann sofort loslegen. Enc FS ist an sich ein reines Kommandozeilentool, jedoch werden die meisten Anwender Enc FS über das grafische Front-End Cryptkeeper bedienen.

Auch dieses kleine Tool muss mit

```
sudo apt install cryptkeeper
```

erst nachinstalliert werden. Nach dem Aufruf *cryptkeeper* präsentiert sich dieser als Schlüsselsymbol in der Hauptleiste. Die Option „Erstelle verschlüsselten Ordner“ richtet ein neues verschlüsseltes Verzeichnis ein, wobei Sie in der oberen Zeile den Ordnernamen vergeben und unten zum gewünschten Ort navigieren, etwa zu einem USB-Stick unter „/media“ im Dateisystem. Mit der Schaltfläche „Vor“ geht es weiter zur Passwortvergabe. Der neue und noch leere Mountordner wird zum Abschluss automatisch im Dateimanager geöffnet und kann dann befüllt werden. Sie arbeiten in diesem Ordner wie mit unverschlüsselten Dateien. Die eigentlichen Dateien liegen auf gleicher Ebene in einem versteckten Ordner „.[name]_enfcs“. Um einen Enc-FS-Ordner auszuhängen und damit zu schützen, klicken Sie auf das Cryptkeeper-Symbol und dann auf den betreffenden Ordnereintrag.

Über die „Einstellungen“ können Sie vorgeben, dass Mountordner nach dem Entladen („Aushängen“) gelöscht und dass nicht genutzte Enc-FS-Ordner nach bestimmter Frist automatisch entladen werden. Diese zweite Sicherheitsmaßnahme ist ein Alleinstellungsmerkmal von Enc FS.

Enc FS auf der Kommandozeile: Im Terminal ist Enc-FS-Verschlüsselung etwas mühsamer, andererseits flexibler. Die Kernsyntax lautet:

```
encfs /Pfad1/verschlüsselte_Daten/
  /Pfad2/unverschlüsselte_Daten/
```

„Pfad1“ ist der zu verschlüsselnde Ordner, „Pfad2“ der Mountpunkt, wo die Daten unverschlüsselt genutzt werden. Das Beispiel

```
mkdir /media/sepp/data/privat
mkdir ~/privat
encfs /media/sepp/data/privat ~/
  privat
```

erstellt unter „/media/sepp/data“ das neue Verzeichnis „privat“, ferner den gleichnamigen Mountpunkt im Home-Verzeichnis. Die dritte Zeile lädt das noch leere Verzeichnis in den Mountpunkt. Danach ist noch die Vergabe eines neuen Kennworts notwendig. Unter „~/privat“ arbeiten Sie mit den Daten.

Während bei Cryptkeeper das verschlüsselte Verzeichnis und das Mountverzeichnis stets auf gleicher Ebene liegen, kann Enc FS auf Kommandozeile von beliebiger Stelle in einen beliebigen Mountpunkt laden. Wenn Sie einen verschlüsselten Ordner nicht mehr benötigen, entladen Sie seinen Mountpunkt:

```
fusermount -u ~/privat
```

Neuerliches Laden geschieht mit genau demselben Enc-FS-Befehl wie bei der Ersteinrichtung.

Tipp: Auf der Kommandozeile (nicht im Cryptkeeper) können Sie Enc FS auch auf ein bereits bestehendes Verzeichnis ansetzen. Alle Dateien, die sich dort bereits befinden, bleiben dort allerdings weiterhin unverschlüsselt. Sollen diese nachträglich verschlüsselt werden, verschieben Sie die Dateien einfach in das Mountverzeichnis des Enc-FS-Ordner-Paares.

5. Container mit Veracrypt

Veracrypt ist der Nachfolger des Verschlüsselungsklassikers Truecrypt, der 2014 eingestellt wurde. Veracrypt arbeitet mit verschlüsselten Containerdateien und einem eigenen Format. Der Inhalt solcher Container wird durch die „Mount“- (oder „Einbinden“-) Schaltfläche und nach korrekter Passworteingabe unverschlüsselt ins Dateisystem gemountet, wobei auch gleich der zuständige Dateimanager zur Anzeige und Dateibearbeitung gestartet wird. Die Größe der Containerdateien muss bei der Einrichtung definiert werden und ist später nicht mehr dynamisch erweiterbar.

Empfehlung: Veracrypt eignet sich für große und sehr große Datenmen-

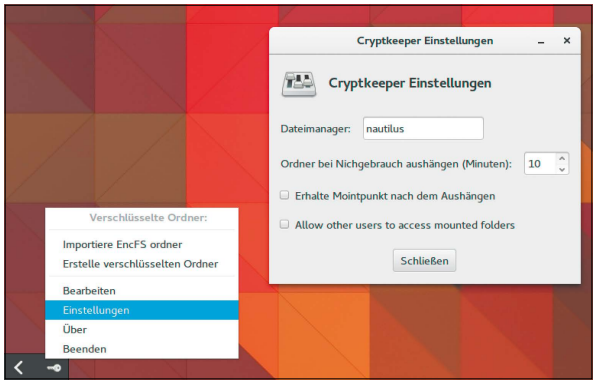
gen, allerdings nur auf lokalen Rechnern oder im lokalen Netzwerk. Für den Transfer in die Cloud ist es ungeeignet, da auch bei geringen Datenänderungen immer der Transport des gesamten Containers notwendig wäre. Ein entscheidendes Plus von Veracrypt sind Versionen für Linux, Windows, Mac-OS, Free BSD und Raspbian. Damit sind Veracrypt-Container zwischen allen PC-Systemen austauschbar.

Installation und Containerbetrieb: Anlaufstelle für die meisten Betriebssysteme ist die Projektseite *https://www.veracrypt.fr/en/Downloads.html*. Für Ubuntu, Mint & Co. ist die Installation über ein PPA allerdings deutlich komfortabler:

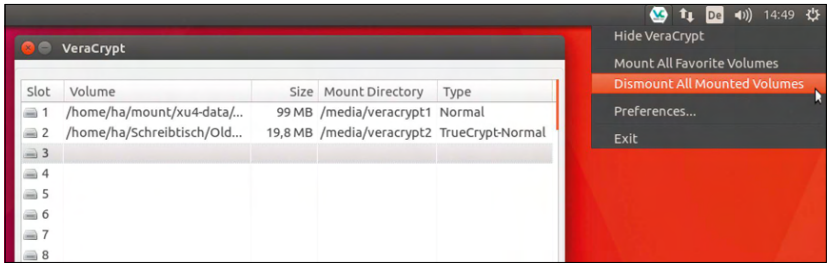
```
sudo add-apt-repository
  ppa:unit193/encryption
sudo apt-get update
sudo apt-get install veracrypt
```

Im Unterschied zur Windows-Version bietet Veracrypt unter Linux keine deutsche Übersetzung, weswegen die nachfolgenden Menübezeichnungen englischsprachig ausfallen. Um eine neue Containerdatei anzulegen, klicken Sie im Hauptdialog auf „Create Volume -> Create an encrypted file container“ und anschließend auf „Standard VeraCrypt volume“. Hier geben Sie Pfad und Namen einer bisher nicht existierenden Datei an. „Encryption Option“ belassen Sie einfach auf den Standardvorgaben. Danach geben Sie die Größe der Containerdatei an. Diese sollte großzügig ausfallen, weil die Kapazität nicht mehr zu ändern ist und viele kleine Container unübersichtlicher sind als wenige große.

Danach kommt die Passwortvergabe. Zur Schlüsselerstellung auf Basis des Passworts erwartet Veracrypt Mausbewegungen im eigenen Fenster. Nach beendeter Fortschrittsanzeige schließen Sie mit „Format“. Damit ist der Container einsatzbereit. Mit „Select File“ im Hauptdialog navigieren Sie zur Containerdatei. Mit Klick auf „Mount“ wird diese geladen und im Dateimanager geöffnet (falls nicht, lässt sich das unter „Preferences -> System Integration“ einstellen). Linux



Grafisches Front-End für Enc FS: Das kleine Tool Cryptkeeper erscheint als Schlüsselsymbol in der Hauptleiste und bietet die wesentlichen Enc-FS-Funktionen.



Systemintegration von Veracrypt: Veracrypt entspricht bei der Bedienung seinem Truecrypt-Vorgänger. Laden und Entladen von Containern gelingt auch über das Panelsymbol.

mountet Container nach „/media/veracrypt[nummer]“, Windows auf freie Laufwerkbuchstaben. Auf diesen Datenträgern lesen, arbeiten, kopieren Sie wie auf einem normalen Laufwerk. Mit „Dismount“ im Hauptdialog entladen Sie den Container, der somit wieder geschützt ist. Zur besseren Systemintegration nistet sich das Veracrypt-Symbol zusätzlich in der Systemleiste des Linux-Desktops ein. Hier sind im Kontextmenü einige fundamentale Aktionen wie das Mounten aller „Favorites“ oder das Abschalten aller aktuell geladenen Container. Eingerichtete „Favorites“ ersparen die Sucherei nach verstreuten Containerdateien, sodass es sich durchaus lohnt, das Menü „Favorites“ zu organisieren.

Beachten Sie, dass Sie beim Mounten von Veracrypt-Containern zusätzlich zum Containerpasswort auch noch nach dem sudo-Kennwort gefragt werden, das mit dem Veracrypt-Passwort nichts zu tun hat und vermutlich anders lautet.

Tipp 1: Veracrypt ist auch komplett über Terminalbefehle zu steuern (siehe *veracrypt -help*). So entlädt etwa

```
veracrypt --dismount
```

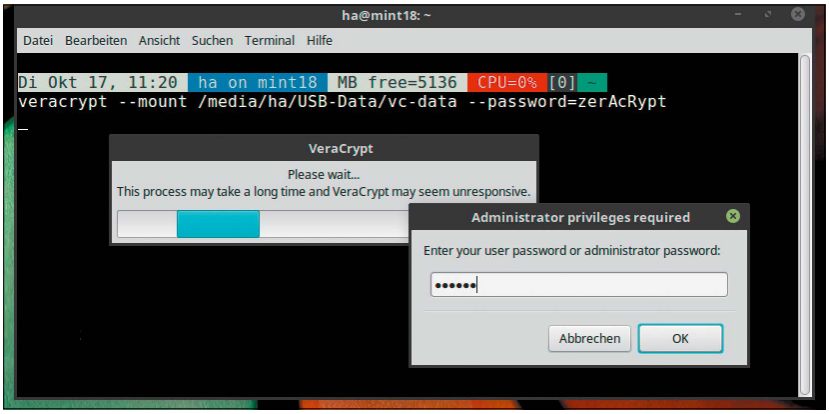
alle geladenen Containerdateien. Und auf stationären, privaten PCs kann es vertretbar sein, einen Container durch ein Terminal-Alias zu laden und dabei das Passwort im Klartext mitzugeben:

```
veracrypt --mount /home/ha/vc-data
  --password=Sehr-GeH3im
```

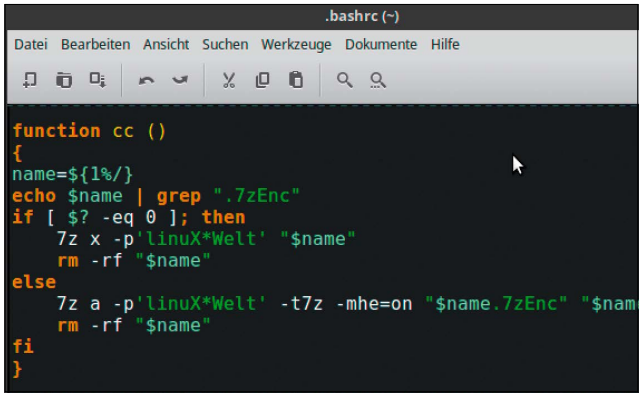
Tipp 2 für ältere Truecrypt-Container: Unter „Select File“ wählen Sie die Containerdatei aus oder mit „Select Device“ das verschlüsselte Laufwerk. Nach einem Klick auf „Mount“ aktivieren Sie im angezeigten Dialog vor der Angabe des Passworts die Option „TrueCrypt Mode“. In einigen Fällen funktioniert das nicht und Veracrypt öffnet den Container nicht. Hier hilft es, die Einstellung „Options -> Mount volume as read-only“ zu aktivieren. Damit sind die Daten erreichbar und können bei Bedarf an eine andere Stelle kopiert werden.

6. Einfaches Verschlüsseln mit Packern

Einfachster Schutz bei geringeren Datenmengen ist die Ad-hoc-Verschlüsselung von Einzeldateien oder eines Ordners. Ohne Einschränkung für alle Dateien und Ordner anwendbar ist ein



Veracrypt im Terminal: Alle Funktionen der Verschlüsselungssoftware sind auf Wunsch auch über die Kommandozeile zu steuern.



Vereinfachte Packerverschlüsselung: Ein Script kann die lästige Aufgabe übernehmen, das Kennwort an 7-Zip zu übergeben.

Packer mit eingebauter Verschlüsselung wie 7-Zip. Diese ist sicher, wenn Sie das Passwort komplex und lang wählen. Packerverschlüsselung erfordert diszipliniertes Verhalten und ist nicht so komfortabel wie andere Methoden.

Empfehlung: Geschützte Packerarchive eignen sich für Dateien in der Cloud, können aber auch für mobile Datenträger ausreichen, wenn die Dateimengen überschaubar sind. Da es 7-Zip für Linux, Windows und MacOS (7zX) gibt, ist der Austausch solcher Archive problemlos. Unter Android können nicht alle Apps mit einem „zip“ im Namen auch mit passwortgeschützten Archiven umgehen, aber der kostenlose, werbefinanzierte 7Zipper (von Polar Bear) beherrscht dies.

Manuelles Verpacken: Installieren Sie zunächst, sofern noch nicht geschehen, den 7-Zip-Packer:

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

7-Zip erscheint unter Desktop-Linux nicht als selbständiges grafisches Programm, sondern integriert sich in die „Archivverwaltung“. In Zusammenarbeit mit dieser Archivverwaltung oder dem 7z-Filemanager unter Windows ist Verschlüsseln und Entschlüsseln recht komfortabel: Sie ziehen Datei oder Ordner einfach mit der Maus in das Fenster („Archivverwaltung“ oder „7-Zip“), bestätigen unter Linux, dass damit ein neues Archiv angelegt werden soll, und geben dann das Format „7z“ an.

Unter „Erweiterte Einstellungen“ vergeben Sie das Passwort. Die Option „Dateiliste ebenfalls verschlüsseln“ sorgt dafür, dass die Archivverwaltung später auch keine Dateinamen verrät. Beim späteren Doppelklick des Archivs wird automatisch das Kennwort abgefragt und nur bei richtiger Eingabe entpackt.

Komfortfunktionen: Der Hauptaufwand für sichere passwortgeschützte Archive entsteht durch die Eingabe des komplexen Kennworts. Dieser Komfortverlust lässt sich etwa durch Terminal-Aliases oder -Funktionen minimieren. Für hier soll ein Beispiel für das Terminal genügen, das am besten als „Function“ in der Datei „~/.bashrc“ zu realisieren ist:

```
function cc ()
{
name=${1%/}
echo $name | grep ".7zEnc"
if [ $? -eq 0 ]; then
  7z x -p'linuX*Welt' "$name"
else
  7z a -p'linuX*Welt' -t7z -mhe=on
  "$name.7zEnc" "$name"
fi
}
```

Danach erledigt im Terminal die Eingabe des Befehls

```
cc [datei]
```

das Ein- oder Auspacken des Archivs im aktuellen Verzeichnis. Ob Einpacken oder Auspacken als Aufgabe ansteht, erkennt die Funktion anhand der Dateiextension. Das Kennwort „linuX*Welt“ ist natürlich anzupassen.

Ähnliche und zum Teil noch komfortablere grafische Lösungen hat die LinuxWelt in früheren Ausgaben vorgestellt, so den Ausbau des jeweiligen Dateimanagers mit speziellen Kontextmenüs. Die LinuxWelt Ausgabe 6/2017 (*www.pcwelt.de/linuxwelt*) zeigte eine Lösung mit einem Incron-überwachten Ordner, der die Verschlüsselung per Drag & Drop erledigt. Im Prinzip basieren aber alle diese Komfortlösungen auf einem Shell-Script ähnlicher Machart wie oben.

7. Kennwortschutz in Office-Software

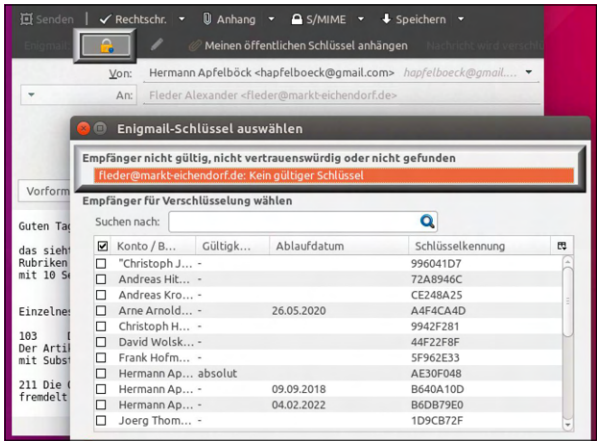
Libre Office und Microsoft Office bieten eine eigene integrierte Verschlüsselung. Das ist bequem, bleibt aber eine Insellösung, die auf die wenigen Office-Formate beschränkt ist. Außerdem hat diese softwareinterne Kryptographie den großen Nachteil, dass Sie auf Office-Suiten angewiesen sind, um ein Dokument lesen zu können. Immerhin kann Libre Office auch passwortgeschützte Microsoft-Dateien öffnen, umgekehrt ist das nicht der Fall.

Empfehlung: Diese Methode, Dateien einzeln zu verschlüsseln, eignet sich nur für wenige sensible Texte oder Tabellen. Für größere Datenmengen ist sie zu unbequem beziehungsweise zeitaufwendig. Der häufigste Einsatz ist der Austausch vertraulicher Tabellen innerhalb eines Arbeitsteams.

Praktische Nutzung: Libre Office bietet die Option „Datei -> Speichern unter -> Mit Kennwort speichern“. Das Kennwort muss jeweils beim Öffnen eingegeben werden. Dass das Dokument geschützt ist, ist Libre Office bei der Weiterbearbeitung klar: Es genügt daher künftig, normal zu speichern. In Microsoft Office findet sich die Verschlüsselung unter „Datei -> Speichern unter -> Tools -> Allgemeine Optionen“.

8. Mailverschlüsselung unter Thunderbird

Ob der persönliche Mailaustausch Verschlüsselung benötigt, muss jeder selbst entscheiden. Tatsache ist, dass US-Anbieter wie Google oder Yahoo der Neugier von Geheimdiensten wenig Datenschutzanstrengungen entgegensetzen. Auch wenn Sie deutsche Provider oder sogar einen eigenen Mailserver benutzen, ist die Mail doch an den Knotenpunkten theoretisch abzufangen – am einfachsten in öffentlichen WLANs.



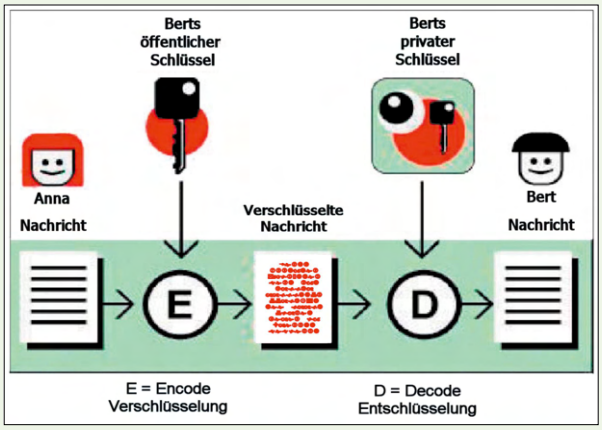
Verschlüsselte Mail mit Gnu PG und Enigmail: Wenn Sie versuchen, verschlüsselt zu senden, aber für den Adressaten kein Schlüssel vorliegt, öffnet sich automatisch die Schlüsselverwaltung.

Empfehlung: Mailverschlüsselung ist wie jede Datenschutzmaßnahme mit Mehraufwand verbunden. Die Kombination von Gnu PG (GNU Privacy Guard) plus Thunderbird mit Erweiterung Enigmail ist die wohl komfortabelste Lösung, aber auch sie erfordert Gewöhnung und zumindest einen Anteil von Mailpartnern, die ebenfalls Gnu PG nutzen. Unter Linux sind

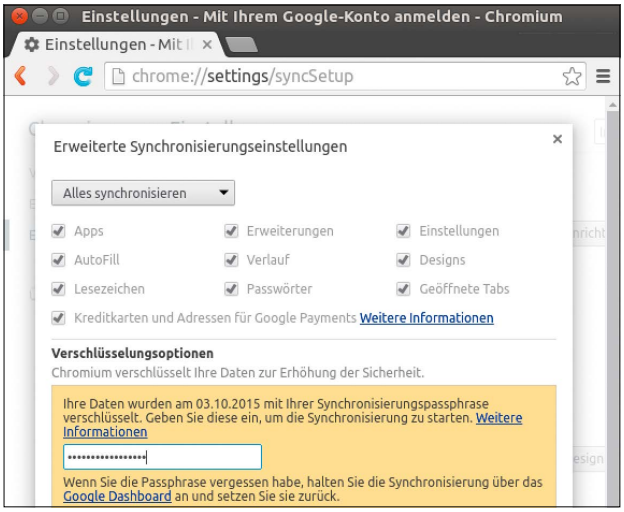
Asymmetrische Verschlüsselung

Alle bisher genannten Verschlüsselungsvarianten (Punkt 1 bis 7) gehören zur Kategorie symmetrischer Verschlüsselung: Ein Kennwortschlüssel verändert die Ausgangsdaten unlesbar, genau derselbe Schlüssel stellt den lesbaren Zustand wieder her. Dieses Verfahren ist optimal, wenn Sender und Empfänger dieselbe Person sind: Sie verschlüsseln Dateien oder Datenträger, die Sie später wieder entschlüsseln. Die Verschlüsselung hat nur den Zweck, dass keine andere Person die Datei lesen kann. Sobald Sender und Empfänger verschiedene Personen sind, wird symmetrische Verschlüsselung problematisch: Erstens muss der Schlüssel auf einem sicheren Weg von Person A zu Person B kommen. Zweitens brauchen Sie strenggenommen für Person C einen anderen Schlüssel, für Person D einen weiteren und so fort. Bei einem Austausch vieler Personen wie bei der Mailkorrespondenz ist dies nicht praktikabel.

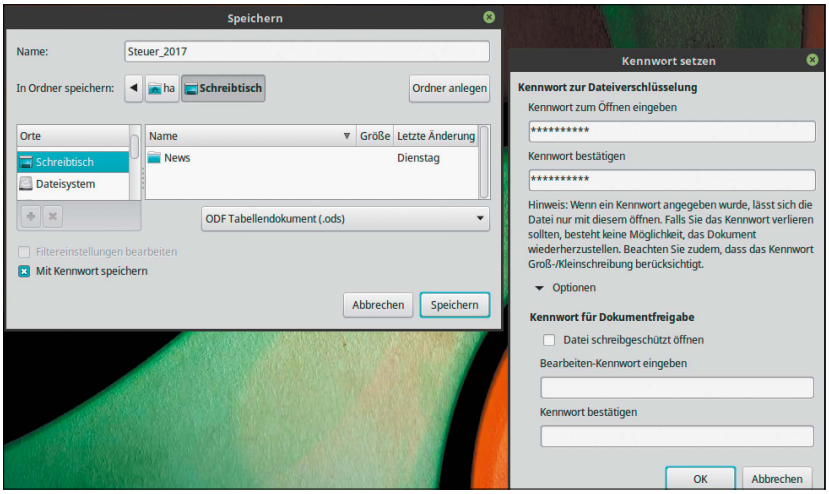
Wesentliches Merkmal der asymmetrischen Verschlüsselung (siehe Punkt 9) sind zwei unabhängige Schlüssel: ein öffentlicher zum Verschlüsseln, ein privater zum Entschlüsseln. Die komplementären Schlüssel generiert die Software – etwa Gnu PG – auf Ihrem Rechner. Beide Schlüssel stehen zwar in eindeutigem Verhältnis, jedoch ist die Berechnung des privaten Schlüssels aus dem öffentlichen durch den Einsatz mathematischer Einwegfunktionen extrem aufwendig bis unmöglich. Der öffentliche Schlüssel zum Verschlüsseln kann daher ohne Geheimniskrämerei an alle Kommunikationspartner direkt oder zu einem öffentlichen Keyserver im Web geschickt werden. Nun chiffrieren alle Partner Nachrichten an Sie mit Ihrem öffentlichen Schlüssel – und Sie sind die einzige Person, die diese Nachrichten mit dem passenden privatem Schlüssel lesbar machen kann. Umgekehrt codieren Sie Ihre Nachrichten mit den öffentlichen Schlüsseln Ihrer Partner und haben die Sicherheit, dass nur der Empfänger mit dem komplementären privaten Schlüssel die Nachricht lesen kann.



Asymmetrische Verschlüsselung: Der Absender einer verschlüsselten Nachricht benötigt zum Chiffrieren („E“ – Encrypt) nur den öffentlichen Schlüssel des Empfängers. Empfangen und entschlüsselt („D“ – Decrypt) wird mit dem privaten Schlüssel.



Sync-Daten verschlüsseln: Diese Maßnahme hält Googles Big-Data-Sammler von Lesezeichen und Verlaufsdaten fern.



Einzeldateien unter Libre Office verschlüsseln: Diese Ad-hoc-Maßnahme ist ein Notbehelf für geringe Datenmengen.

Thunderbird und Gnu PG oft vorinstalliert und falls nicht über die Paketnamen „thunderbird“ und „gnupg“ schnell nachgerüstet. Für Windows gibt es Downloads unter *www.mozilla.org* und *www.gnupg.org*). Enigmail finden und installieren Sie dann direkt in Thunderbird über „Add-ons“.

Einrichtung und Mailalltag: Nach der Installation der Enigmail-Erweiterung und einem Thunderbird-Neustart verwenden Sie im automatisch startenden Einrichtungsassistenten die „ausführliche Konfiguration“. Im ersten Schritt geben Sie die „Passphrase“ ein. Das Passwort benötigen Sie später stets, um auf Ihre Schlüssel zuzugreifen. Es bildet auch die Grundlage für die beiden Schlüssel. Nach der doppelten Eingabe legt Enigmail das neue Schlüsselpaar an (öffentlich/privat). Falls Sie auf einem anderen Rechner bereits ein eingerichtetes Enigmail und ein Schlüsselpaar besitzen, wählen Sie im Assistenten die Option, bestehende Schlüssel zu importieren. Schlüssel lassen sich über „Enigmail -> Schlüssel verwalten“ als Ascii-Dateien exportieren und auf anderen PCs importieren.

Öffnen Sie wie gewohnt den Editor zum Verfassen von Nachrichten. Dort hat Enigmail jetzt eine weitere Symbolleiste platziert. Möchten Sie eine ausgehende Nachricht verschlüsseln, benötigen Sie den öffentlichen Schlüssel des Empfängers. Wenn dieser als Textdatei vorliegt, können Sie den Schlüssel über „Enigmail -> Schlüssel verwalten -> Datei importieren“ einlesen. Alternativ gibt es Schlüsselserver, die öffentliche Schlüssel aufbewahren.

Über „Schlüsselserver -> Schlüssel suchen“ sehen Sie nach, ob die Empfängeradresse dort eingetragen ist; falls ja, importieren Sie den Schlüssel mit einem Klick. Umgekehrt ist es sinnvoll, den eigenen öffentlichen Schlüssel über „Schlüsselserver -> Schlüssel hochladen“ im Web zugänglich zu machen.

Nach einem Schlüsselimport ist der neue Mailempfänger Enigmail/Gnu PG bekannt. Künftig klicken Sie beim Verfassen einer Nachricht an diesen Empfänger auf das Symbol mit dem Schloss. Um Mails verschlüsselt zu versenden, müssen Sie Ihr Passwort eingeben. Wenn Sie mit dem Schloss-Symbol verschlüsselt senden wollen, jedoch für den Empfänger kein Schlüssel vorliegt, erscheint automatisch der Hinweis, dass dieser Empfänger „nicht gültig“ ist. Dann besorgen Sie sich entweder den öffentlichen Schlüssel oder Sie senden unverschlüsselt. Erhalten Sie umgekehrt eine Mail, die verschlüsselt wurde, erkennt Enigmail das automatisch. Wenn Sie im Vorschaubereich von Thunderbird auf das Element klicken, werden Sie dazu aufgefordert, das Passwort einzugeben. Wenige Augenblicke später erscheint die Nachricht.

Beachten Sie, dass Sie bei der Nutzung mehrerer Rechner die Schlüsselverwaltung immer manuell synchron halten müssen. Eine wichtige Hilfe ist wieder „Enigmail -> Schlüssel verwalten -> Datei exportieren“, wobei Sie einfach sämtliche Schlüssel markieren. Die resultierende Ascii-Datei lässt sich auf dem nächsten PC importieren.

9. Verschlüsselte Browsersynchronisierung

Die Browsersynchronisierung von Lesezeichen, Einstellungen, Erweiterungen und Skins bedeutet für Nutzer mehrerer Geräte unschätzbaren Komfort. Bedenklich scheint allerdings der Nebenaspekt, dass dabei Mengen von persönlichen Daten auf diversen Google- oder Mozilla-Servern hinterlegt werden müssen.

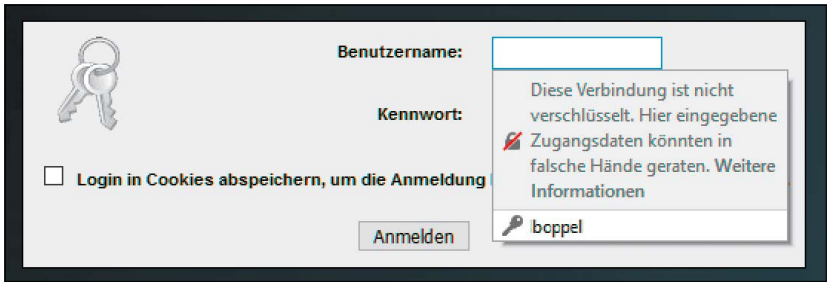
Empfehlung: Firefox verschlüsselt standardmäßig alle Daten, wobei der Schlüssel auf dem Gerät des Benutzers verbleibt. Damit ist Firefox in puncto Datenschutz erste Wahl. Jedoch lässt sich auch der Google-Browser so einstellen, dass alle Synchronisierungsdaten sicher verschlüsselt sind.

Abhörsichere Synchronisierung für Chrome/Chromium: Standardmäßig werden hier nur die Kennwörter verschlüsselt. Aber unter „Einstellungen -> Erweiterte Synchronisierungseinstellungen“ (vorherige Google-Anmeldung vorausgesetzt) gibt es die Option „Alle synchronisierten Daten […] verschlüsseln“, bei der Sie ein individuelles Kennwort zur Sync-Verschlüsselung vergeben, das unabhängig vom Google-Kennwort ist. Der Komfortverlust ist nicht gravierend, da Sie dieses Kennwort auf jedem weiteren Gerät nur ein einziges Mal eingeben müssen. Damit landen sämtliche Daten verschlüsselt auf dem Google-Server, der Schlüssel dazu (Kennwort) verbleibt auf dem lokalen Gerät.

10. Verschlüsselung im Internet

Der Datenaustausch über unverschlüsselte Verbindungen ins Internet kann im Klartext mitgelesen werden. Das gilt verschärft in öffentlichen Funknetzen, innerhalb von lokalen Firmennetzen und theoretisch auch außerhalb des lokalen Netzwerks an Verteilerknoten, die von Providern, Geheimdiensten oder Hackern abgehört werden. Im Fokus stehen die meistgenutzten Protokolle HTTP (Webseiten) und FTP (Datentransfer). Die folgenden Infos beziehen sich ausschließlich auf die Clientseite des Webnutzers, nicht auf die Serverseite des Betreibers.

HTTP und HTTPS: Im Sinne des Datenschutzes ist, wo immer möglich, auf verschlüsselte Verbindung zu achten. Zwingend erforderlich ist dies überall, wo zur Anmeldung persönliche Zugangsdaten verschickt werden (Bank, Onlineshop). Alle Browser zeigen sichere (HTTPS-)Webadressen in der Adresszeile mit einem grünen Schloss-Symbol an. HTTPS garantiert, dass es



Firefox ultravorsichtig: Der Mozilla-Browser zeigt bei Anmeldungen auf unverschlüsselten Webseiten diese Warnung. Google Chrome wird künftig vermehrt vor solchen Sites warnen.

für Kriminelle und Geheimdienste selbst dann nichts Lesbares zu lesen gibt, wenn der Angreifer im Netz sitzt und den Netzverkehr abhört.

Firefox und Chrome signalisieren unverschlüsselte HTTP-Sites explizit als „nicht sicher“. Dies ist kein Urteil über die Seriosität der Website, sondern ausschließlich die Aussage, dass eine Site keine TLS-(Transport Layer Security) oder SSL-Verschlüsselung bietet (Secure Socket Layer). Datenschutztechnisch noch einen Schritt weiter geht Firefox, der Anmeldungen auf unverschlüsselten Seiten automatisch bremst: „Diese Verbindung ist nicht verschlüsselt…“. Das ist im Prinzip verdienstvoll, kann aber – insbesondere bei lokalen Servern (Router, NAS) – auch nerven und über „about:config“ deaktiviert werden („security.insecure_field_warning…“).

FTP, FTPS und SFTP: Das File Transfer Protocol (FTP) bietet keine Verschlüsselung. Daher sollten Sie sich die Anmeldung auf unverschlüsselten FTP-Servern zumindest in öffentlichen WLANs verkneifen. Man mag sich als Clientnutzer auf den Standpunkt stellen, das Sicherheitsproblem sei Sache des Serverbetreibers. Jedoch fällt der Erstverdacht zunächst auf den Clientnutzer, wenn dessen unverschlüsselte Anmeldedaten abgegriffen und destruktiv missbraucht werden. Sicherheitsbewusste FTP-Betreiber werden FTPS (FTP mit SSL- oder TLS-Verschlüsselung) anbieten. FTP-Clients wie Filezilla zeigen im Servermanager unter „Verschlüsselung“ an, ob die Verbindung abhörsicher ist.

Eine sichere Alternative zu FTP ist der Datenaustausch über SSH, das über sein Protokoll SFTP auch die direkte verschlüsselte Dateiübertragung vorsieht. Mit den ähnlich klingenden Protokollen FTP und FTPS hat das nichts zu tun, sondern mit SSH-Servern, die auf Linux-Systemen SSH-Verbindungen entgegennehmen. Mit Rücksicht auf Windows-Systeme, die standardmäßig keinen SSH-Client enthalten, bleibt FTP und FTPS das verbreitete Austauschprotokoll. Wirklich triftig ist diese Rücksicht nicht, da der unter Windows vielgenutzte FTP-Client Filezilla auch das Protokoll „SFTP“ beherrscht.

Unentbehrlicher Browsertipp

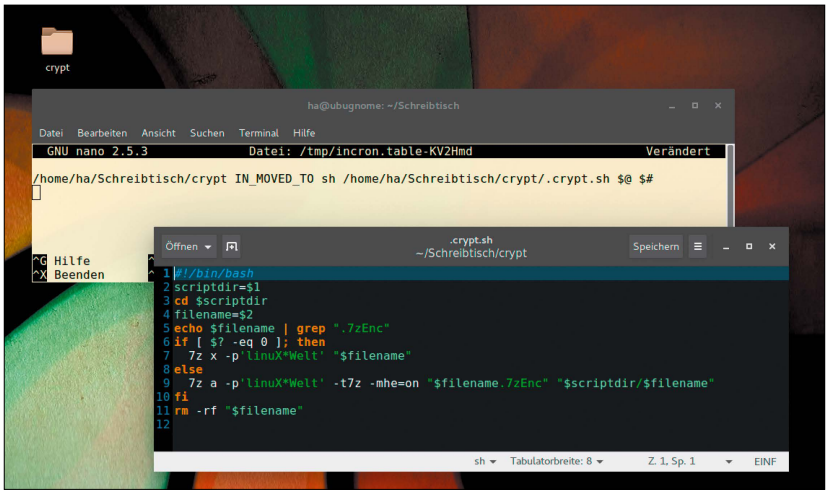
Mit dem Thema „Verschlüsselung“ hat dieser kleine Exkurs nichts zu tun, aber viel mit dem übergeordneten Thema „Datenschutz“: Wer gerade vorhat, sich eine Jacke, Gitarre oder Kettensäge zu kaufen, sollte die Angebote tunlichst nicht über normales Google & Co. recherchieren. Dann sieht man nämlich die nächsten Wochen im Web überall nur noch Jacken, Gitarren und Kettensägen. Einfache Abhilfe schafft der „Private Modus“ im Firefox oder „Inkognito“ bei Chrome. Damit können Sie in Google & Co. suchen, ohne die Werbeindustrie über Ihre Interessen zu informieren. Wer solche Belästigung generell hasst, kann auch die Suchmaschine *duckduckgo.com* verwenden – dort ist der Datenschutz inklusive.

Verschlüsseln per Mausaktion

Lästige Pflichtaktionen wie das Verschlüsseln von Dateien vor dem Ablegen auf eine Internetcloud oder einen mobilen Datenträger lassen sich deutlich komfortabler einrichten. Das folgende Szenario nutzt dafür das Tool Incron.

Von **Hermann Apfelböck**

Aufgabe und Ziel dieser Systembastelei ist ein Ordner, der dorthin verschobene Dateiobjekte (Ordner und Dateien) automatisch verschlüsselt oder umgekehrt entschlüsselt, falls das verschobene Objekt bereits verschlüsselt ist. Im einfachsten Fall liegt dieser Ordner am Desktop, weil dieser stets komfortabel für Mausaktionen erreichbar ist. Wenn eine Linux-Distribution den Desktop nicht als Dateiablage vorsieht, kann auch ein beliebiger anderer Ordner definiert werden, was dann aber die Benutzung im Dateimanager erfordert.



Die Bestandteile eines Incron-Automatismus: Alles, was die Maus in den Desktopordner „crypt“ wirft, wird dort automatisch ver- oder entschlüsselt.

Wichtige Incron-Grundlagen vorab

Da wir nicht davon ausgehen können, dass alle Leser mit dem Inotify-Subsystem des Linux-Kernels und dem darauf basierenden Tool Incron vertraut sind, müssen wir hier die wichtigsten Basics vorausschicken: Incron kann definierte Ordner überwachen (nur die Ordnerebene ohne Unterverzeichnisse) und auf diverse Ereignisse im überwachten Ordner umgehend reagieren. Wir nennen hier nur die in der Praxis wichtigsten Ereignisse:

- IN_CREATE (neue Datei)
- IN_MODIFY (Dateiänderung)
- IN_MOVED_TO (neue, in den Ordner verschobene Datei)

Auf welche(s) Ereignis(se) das Tool in Aktion treten soll, kann der Systembenutzer selbst bestimmen, indem er mit

```
incrontab -e
```

die maßgebliche Konfigurationsdatei bearbeitet. Eine Incrontab-Zeile besteht aus drei Elementen:

```
[Ordnerpfad] [Ereignis(se)]
  [Aktion mit optionalen
  Übergabeparametern]
```

Als Aktion genügt in den allereinfachsten Fällen

```
/home/ha/ IN_CREATE cp $@/$# /me
  dia/data/backup/$#
```

ein einziger Shell-Befehl (hier „cp“), meistens ist aber ein Shell-Script unerlässlich. Als wichtigste Übergabeparameter an den eigentlichen Befehl gibt es „$@“ für den überwachten Pfad und „$#“ für den Namen des auslösenden Dateiobjekts.

Incron ist kein Systemstandard, sondern muss über den gleichnamigen Paketnamen nachinstalliert werden. Wer das Tool benutzen darf, ist über die Datei „/etc/incron.allow“ zu steuern. Es genügt hier der Eintrag der Benutzernamen

```
ha
root
```

als je eigene Zeile. Standardmäßig ist nach der Incron-Installation niemand berechtigt, auch nicht root.

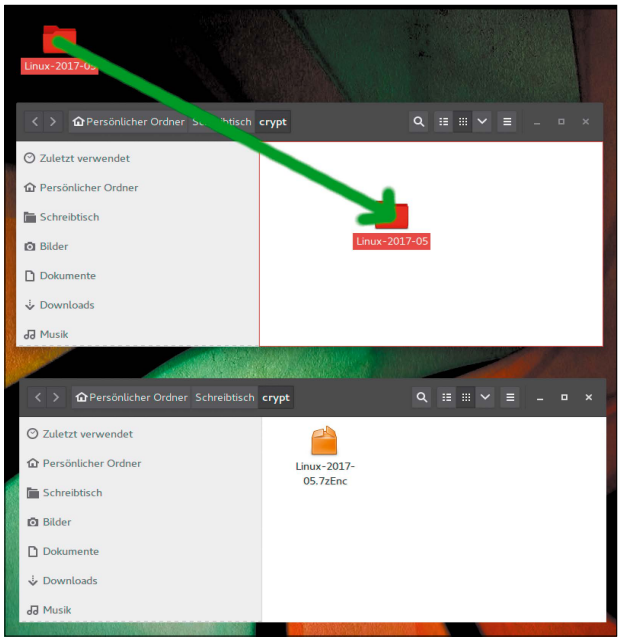
Verschlüsselungsordner mit Incron

Basis des Verschlüsselungsautomatismus ist zunächst eine Zeile in der Incron-Tabelle, die Sie mit Befehl *incrontab -e* laden. Die Zeile sieht in unserem Beispiel wie folgt aus:

```
/home/ha/Schreibtisch/crypt IN_MO
  VED_TO sh /home/ha/Schreibtisch/
  crypt/.crypt.sh $@ $#
```

Da Incron keine Bash-Variablen ver-

steht, müssen alle Pfade immer komplett ausgeschrieben werden. Im konkreten Beispiel soll der Ordner „crypt“ am Userdesktop überwacht werden. Alles, was per Maus (oder mit *mv* im Terminal) in den überwachten Ordner „crypt“ verschoben wird, löst das Script „crypt.sh“ aus, wie es die erste Abbildung dieses Artikels zeigt. Das Script erhält als ersten Übergabeparameter den Ordnerpfad des überwachten Verzeichnisses (die Incron-Variable „$@“ wird als „$1“ im Script weiterverarbeitet). Der zweite Parameter ist der pure Dateiname ohne Pfad (die Incron-Variable „$#“ wird als „$2“ im Script weiterverarbeitet). Beachten Sie, dass das hier gewählte Dateisystem-Ereignis „IN_MOVED_TO“ nicht auf Kopieraktionen reagiert, sondern wirklich nur auf ein Verschieben.



Datenschutz per Drag & Drop und ohne Kennworteingabe: Das 7z-Passwort holt sich der Incron-Mechanismus aus der zugehörigen Script-Datei.

Das Script verarbeitet Dateien wie Ordner. Ob verschlüsselt oder entschlüsselt wird, entscheidet die künstliche Extension „.7zEnc“, die alle verschlüsselten Objekte automatisch erhalten. Als Werkzeug dient der Packer 7z, der natürlich installiert sein muss (Paketname „p7zip-full“). Das hier genutzte Beispielpasswort „linux*Welt“ sollten Sie individuell abändern, dann aber dauerhaft beibehalten. Beachten Sie, dass späteres Ändern des Passworts vorheriges Entschlüsseln aller vorhandenen Archive mit der Endung „.7zEnc“ erfordert. Mit einem neuen Passwort kommen Sie nicht mehr an die Inhalte älterer passwortgeschützter 7z-Archive.

Die Benutzung des „crypt“-Ordners ist intuitiv: Sie ziehen einfach das zu verschlüsselnde Dateiobjekt auf das Ordnericon oder in den geöffneten Ordner „crypt“. Es wird dann umgehend passwortgeschützt eingepackt und mit der künstlichen Endung versehen. Umgekehrt werden Dateiobjekte mit der Endung „.7zEnc“ wieder ausgepackt. Die Originaldateien werden standardmäßig gelöscht gemäß letzter Zeile im Script „crypt.sh“. Wenn Sie dies nicht möchten, tilgen Sie einfach diese Zeile.

Dateiobjekte von externen Datenträgern oder von Netzfreigaben werden nicht als „IN_MOVED_TO“-Ereignis interpretiert, selbst wenn sie mit *mv* oder mit gedrückter Umschalttaste explizit verschoben werden. Hier bietet es sich an, den Desktop als Zwischenstation zu nutzen – also erst dorthin zu kopieren und von dort in den „crypt“-Ordner zu verschieben.

Fehlersuche bei Incron

Incron arbeitet schnell, zuverlässig und ressourcensparend. Bis es allerdings soweit ist, kostet jedes Szenario genaue Planung und eine oft mühsame Fehlersuche. Zu den offensichtlichsten Fehlern gehören fatale Endlosschleifen etwa bei einer Kombination eines „IN_CREATE“-Events und eines Kopierbefehls in das überwachte Verzeichnis selbst. Ebenfalls offensichtliche Fehler sind ein nicht laufender Incron-Daemon (das lässt sich im Zweifel mit *systemctl status incron.service* abfragen) oder fehlende Incron-Rechte (*sudo gedit /etc/incron.allow*). Beim Einsatz von Shell-Scripts müssen diese wie üblich als „ausführbar“ markiert sein.

Das gewählte Dateisystemereignis sollte genau ausreichen, die gewünschte Aktion auszulösen, aber nicht mehr. Von allzu großzügigen Optionen ist abzuraten (so gibt es etwa auch einen globalen Trigger „IN_ALL_EVENTS“, außerdem sind mehrere Events kombinierbar – durch Kommata getrennt).

Besonders knifflig ist die Kontrolle der Übergabeparameter an Shell-Scripts, das Quoting von Variablen mit passenden Anführungszeichen sowie Korrekturen an den Shell-Scripts selbst, die ja völlig stumm im Hintergrund laufen. Während der Einrichtung ist es meistens notwendig, im Script zumindest die wichtigsten Variablen und Script-Befehle mit „echo“

```
echo $1 >> ~/debug.txt
```

an eine Protokolldatei zu schicken und danach dort das Ergebnis zu prüfen. Verbleibende Script-Fehler entdecken Sie am einfachsten, wenn Sie das Script im Terminal manuell starten und dabei die Parameter etwa mit

```
sh /home/ha/Schreibtisch/crypt/.crypt.sh /home/ha/
  Schreibtisch/crypt test.txt
```

genauso übergeben, wie sie auch von Incron weitergereicht würden.

Routertuning

Der DSL-Router ist die zentrale Schaltstelle im Heimnetzwerk. Dieser Beitrag erklärt wesentliche Funktionen und liefert Tipps für den effektiven Einsatz und die optimale Konfiguration.

Von **Thorsten Eggeling**



DSL-Router stehen meist in einer dunklen Ecke und verrichten unbeachtet ihre Arbeit. Das spricht für ihre Zuverlässigkeit. Ab und zu sollten Sie dem Gerät jedoch etwas mehr Aufmerksamkeit schenken. Denn der Router ist direkt mit dem Internet verbunden und damit zahlreichen Angriffen ausgesetzt. Ein Firmware-Update kann für mehr Sicherheit sorgen.

Neue Firmware bringt oft auch neue Funktionen mit. Vor allem die weit verbreitete Fritzbox von AVM (*www.avm.de*) bietet viele interessante Möglichkeiten, weshalb sich der Artikel auch hauptsächlich auf diesen DSL-Router bezieht. Die Tipps lassen sich aber auch auf mehrere Speedport-Modelle der Telekom anwenden, wenn auf diesen die AVM-Firmware läuft. Einige Internetprovider, beispielsweise 1&1, liefern dagegen eine Original-Fritzbox-Firmware aus. Es gibt aber auch Provider, die die AVM-Software in einigen Bereichen einschränken. Manchmal ist es beispielsweise nicht möglich, ein Firmwareupdate selbst durchführen. In diesem Fall fehlt der zugehörige Menüpunkt. Sie müssen dann auf das Update vom Provider warten. Wenn Sie das nicht wollen, fragen Sie beim Internetanbieter nach den Zugangsdaten und einem uneingeschränkten Router.

Bevor Sie loslegen, lesen Sie den Kasten auf der nächsten Seite, „Zugriff auf die Weboberfläche von Routern“. Er enthält grundlegende Informationen über den Zugriff auf die Konfigurationsoberfläche von Routern.

1. Backups und neue Firmware

Vor einem Firmware-Update oder ebenso größeren Konfigurationsänderungen sollten Sie ein Backup der Einstellungen anlegen. Rufen Sie die Weboberfläche der Fritzbox auf, und gehen Sie auf „System -> Sicherung“ oder bei älteren Fritzboxen auf „System -> Einstellungen sichern“. Klicken Sie auf „Sichern“ um das Backup zu speichern. Über die Registerkarte „Wiederherstellen“ stellen Sie bei Bedarf die Einstellungen aus der Sicherungsdatei wieder her.

Neue Firmware: Gehen Sie in der Weboberfläche auf „System -> Update“ oder „System -> Firmware-Update“. Klicken Sie auf „Neues FRITZ!OS suchen“ beziehungsweise „Neue Firmware suchen“. Wird ein

Update gefunden, folgen Sie einfach den Anweisungen auf dem Bildschirm.

Seit Version Fritz-OS 6.20 gibt es unter „System -> Update“ eine Automatikfunktion, um Updates selbsttätig zu installieren. Klicken Sie auf „Auto-Update“, um die Einstellungen zu überprüfen und gegebenenfalls anzupassen. Mit der Option „Über neue Fritz!OS-Versionen informieren und […] automatisch installieren“ beziehen Sie jede neue Firmwareversion automatisch.

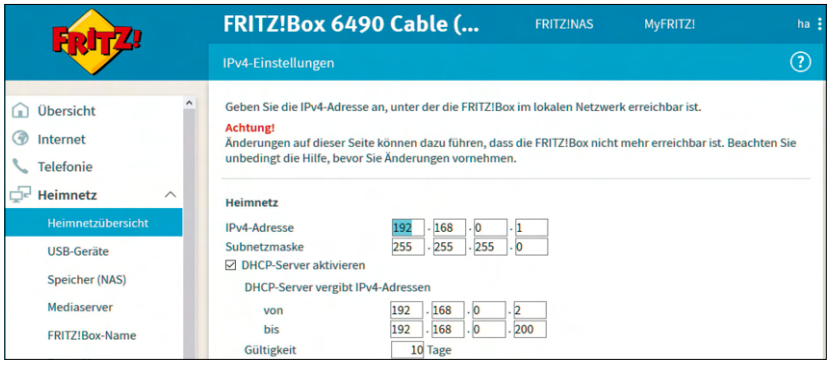
2. IP des Routers und den Adressraum ändern

Typischen 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 Datenserver mit fester IP, Serverdienste wie SSH eingerichtet sind, und Scripts oder Browserlesezeichen bestimmte IP-Adressen erwarten. Hier wäre die Umstellung aller Details auf einen neuen Adressraum eine zeitraubende Aufgabe.



Backup der Konfiguration: Vor umfangreichen Änderungen in den Einstellungen empfiehlt es sich, eine Sicherungskopie anzulegen.



IP-Adresse einer neuen Fritzbox ändern: Dies ist eine wichtige Einstellung, wenn ein neuer Router in ein sorgfältig eingerichtetes Netzwerk Einzug hält.

Alle Router sehen daher die manuelle Einstellung der eigenen IP vor. In der Fritzbox gehen Sie auf „Heimnetz -> Heimnetzübersicht -> Netzwerkein-

Zugriff auf die Weboberfläche von Routern

Auf Routern und anderen Netzwerkgeräten wie etwa WLAN-Access-Points oder WLAN-Repeatern läuft standardmäßig ein Webserver. Dieser liefert die Webseiten für die Konfiguration des Gerätes aus. Bei der Erstkonfiguration sollte die Verbindung zum PC oder Notebook immer direkt per Ethernet-Kabel erfolgen.

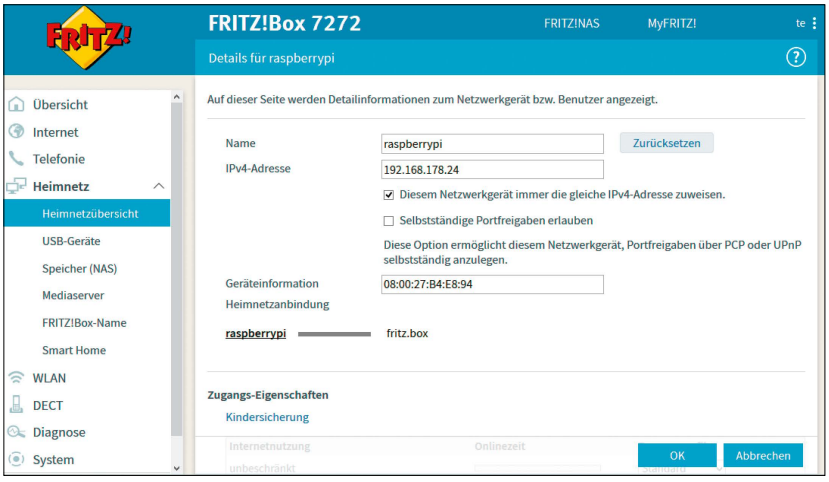
WLAN funktioniert nur, wenn der Hersteller die SSID des Funknetzes und das Passwort vorkonfiguriert hat. Informationen dazu finden Sie dann auf dem Typenschild am Gerät, im beigelegten Installationsleitfaden oder auf der Webseite des Herstellers.

DSL-Router verwenden im Auslieferungszustand immer eine feste IP-Adresse, meist 192.168.0.1, 192.168.1.1, 192.168.2.1 (Telekom Speedport) oder 192.168.178.1 (Fritzbox). Die Standard-IP-Adresse ist oft auf dem Typenschild oder im Installationsleitfaden zu finden. Die IP-Nummer tippen Sie in die Adressleiste des Browsers ein, um sich mit dem Router zu verbinden.

Statt der IP-Nummer funktioniert meist auch eine spezielle URL, beispielsweise *http://fritz.box* (Fritzbox), *https://speedport.ip* (Telekom) oder *http://tplinkmodem.net* (TP-Link-Geräte). Aber Vorsicht: Konfigurations-URLs wurden in der Vergangenheit manchmal gekapert und könnten für kriminelle Zwecke missbraucht werden. Vertipper sind ebenfalls gefährlich, denn auch diese können zu gefälschten Webseiten führen. Verwenden Sie daher aus Sicherheitsgründen besser die IP-Nummer.

Beim ersten Aufruf der Gerätewebseite erfolgt meist eine Passwortabfrage, oder Sie müssen ein Passwort festlegen. Das Standard-Passwort für die Erstinstallation ist auf dem Gerät oder in der Dokumentation zu finden.

Bei der Fritzbox gibt es noch eine Besonderheit: Die Weboberfläche zeigt standardmäßig nicht alle Einstellungen, sondern nur die Basiskonfiguration. Je nach Fritz-OS-Version lässt sich im Menü rechts oben die „Erweiterte Ansicht“ einschalten, oder Sie finden links unten oder in der Mitte der Seite „Ansicht: Standard“. Mit einem Klick darauf wechseln Sie zu „Ansicht: Erweitert“. Die Oberfläche zeigt dann mehr Einstellungen, die wir teilweise in diesem Artikel erwähnen.



Feste IP-Nummer: Server sollten im Netzwerk immer über dieselbe Adresse erreichbar sein. Bei einer Fritzbox lässt sich das für jedes einzelne Gerät festlegen.

stellungen“. In der erweiterten Ansicht finden Sie die Schaltfläche „IPv4-Adressen“. Hier können Sie ganz oben die gewünschte IP-Adresse festlegen.

3. Fast Ethernet oder Gigabit-LAN

Wer überwiegend Gigabit-Netzgeräte besitzt, sollte unbedingt unter „Heimnetz -> Heimnetzübersicht“ die „Netzwerkeinstellungen“ aufsuchen. 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.

Wo immer Sie vollen Gigabit-Durchsatz brauchen und der angeschlossene Client das unterstützt, setzen Sie auf „Power Mode“.

4. 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“. Fritz-OS setzt davor automatisch ein Häkchen, wenn Sie die gewünschte IP-Adresse eintragen. Soll die aktuelle IP-Nummer beibehalten werden, setzen Sie das Häkchen selbst. Klicken Sie auf „OK“, um die Änderungen zu übernehmen. Das Gerät erhält jedoch seine neue IP-Nummer erst nach einem Neustart des Betriebssystems.

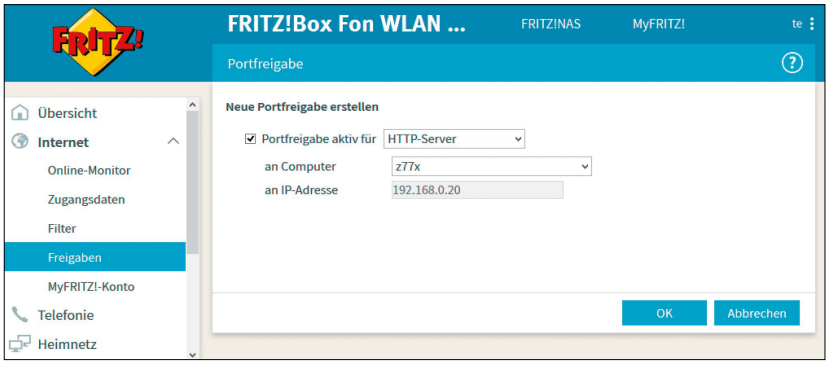
5. IPv4-Portfreigaben für Server einrichten

Wer einen heimischen Datenserver, Webserver oder sonstigen Dienst (SSH, FTP, Wiki, Kalender) über das Internet erreichen will, muss einen oder mehrere Ports nach außen hin öffnen. Prüfen Sie zuerst, ob Ihr Router von außen nur über eine IPv4-Adresse, nur über eine IPv6-Adresse oder beides zu erreichen ist. Sie erkennen das in der Weboberfläche auf der Startseite „Übersicht“. Steht unter „Verbindungen“ die Zeile „FRITZ!Box verwendet einen DS-Lite-Tunnel“ oder ähnlich, lesen Sie in Punkt 6 weiter. Wenn ein Eintrag wie „IPv4, verbunden“ und darunter eine IPv4-Adresse auftaucht, können Sie IPv4-Freigaben einrichten.

Wie genau die Konfiguration des Routers durchzuführen ist, hängt vom jeweiligen Modell ab. Auf *https://portforward.com* finden Sie Anleitungen in englischer Sprache für zahlreiche Geräte. Bei einer Fritzbox mit Fritz-OS 06.50 (bei Version 06.83 siehe Punkt 6) gehen Sie auf „Internet -> Freigaben -> Portfreigaben“. Nach einem Klick auf „Neue Portfreigabe“ wählen Sie hinter „Portfreigabe aktiv für“ beispielsweise „HTTP-Server“ aus und darunter den Computer, auf dem der Webserver läuft. Damit der



IPv4 auf Sparflamme: Einige Provider bieten nur DS-Lite. Dann gibt es keine öffentliche IPv4-Adresse, und es sind nur IPv6-Portfreigaben möglich.



Loch in der Firewall: Ist eine Portfreigabe konfiguriert, erreichen Pakete aus dem Internet einen sonst durch die Firewall blockierten PC im lokalen Netzwerk.

Server über einen Domainnamen ständig aus dem Internet erreichbar ist, obwohl sich die IP-Adresse regelmäßig ändert, benötigen Sie einen Anbieter für dynamisches DNS.

Fritzbox-Besitzer können über „Internet -> MyFRITZ!“ ein kostenloses Konto erstellen und dann über „Freigaben -> MyFRITZ!-Freigaben“ neue „MyFRITZ!-Adressen“ konfigurieren. Wer ein anderes Gerät verwendet, nutzt einen der kostenlosen Dyn-DNS-Dienste (siehe Kasten „Domains für dynamische IP-Adressen“).

6. IPv6-Freigaben bei Dual Stack (Lite)

Bei IPv6 erhält jedes Gerät im Netzwerk ein Subnetz-Präfix. Das sind die ersten vier Gruppen der Adresse, beispielsweise „2001:a63:1267:4601:921c:34fa:fe47:7807“. Das Präfix ist bei allen Geräten im Netz gleich. Die letzten vier Gruppen der Adresse (Interface Identifier, IID) erzeugt das Betriebssystem („2001:a63:1267:4601:921c:34fa:fe47:7807“). Standardmäßig gibt es mehrere IPv6-Adressen pro PC. Welche das sind, können Sie im Terminalfenster über den Befehl

```
ip -6 addr
```

herausfinden. Bei Ubuntu 16.04 taucht hier eine Adresse mit dem Zusatz „scope global temporary dynamic“ auf. Das ist die öffentliche IPv6-Adresse des PCs. Sie können das auf einer Website wie *http://ipv6-test.com* prüfen. Die Adresse ändert sich basierend auf einem Zufallswert, nach der hinter „preferred_lft“ angegebenen Zeit. Dafür sind die „Privacy Extensions“ verantwortlich. Diese sollen bewirken, dass Ihr PC im Internet nicht eindeutig identifizierbar ist.

Zusätzlich erhält der DSL-Router vom Provider regelmäßig ein neues Präfix, wodurch sich auch der erste Teil der Adresse ändert. Wenn Sie den Router oder PC neu starten oder einige Zeit warten, sehen Sie unter *http://ipv6-test.com* eine andere Adresse.

Die Privacy Extensions sind nicht bei jedem Linux-System aktiviert. Mit folgendem Befehl



Feste IPv6: Sind die „Privatsphärenerweiterungen“ deaktiviert, ändert sich die IID (Interface Identifier) nicht mehr. Die Konfiguration über den grafischen Linux-Netzwerk-Manager arbeitet jedoch nicht immer stabil.

```
cat /proc/sys/net/ipv6/conf/
  enp5s0/use_tempaddr
```

finden Sie heraus, was auf Ihrem PC gilt. „enp5s0“ ersetzen Sie durch den Gerätenamen des Netzwerkadapters, den der Befehl *ip -6 addr* anzeigt. Lautet die Ausgabe „0“, sind die Privacy Extensions nicht aktiv. Dann ändert sich bei der IPv6-Adresse nur das Präfix, und die IID bleibt.

Ständig wechselnde IPv6-Adressen sind für Freigaben nicht zu gebrauchen. Die Umstellung auf statische Adressen kann Ubuntu 16.04 über den Netzwerkmanager erledigen. Klicken Sie dessen Symbol in der Systemleiste an und wählen Sie „Verbindungseinstellungen“. Klicken Sie auf die aktive Netzwerkverbindung, etwa „Kabelnetzwerkverbindung 1“, und dort auf „Bearbeiten“. Auf der Registerkarte „IPv6-Einstellungen“ setzen Sie die „IPv6-Privatsphärenerweiterungen“ auf „Deaktiviert“. Klicken Sie auf „Speichern“, und starten Sie Linux neu.

Zuverlässigere Methode: Leider arbeitet die beschriebene Konfiguration über den Netzwerkmanager unter Ubuntu 16.04 nicht immer korrekt. Nach den beschriebenen Änderungen war teilweise keine öffentliche IPv6-Adresse mehr vorhanden. Es ist daher derzeit besser, den Netzwerkmanager zu umgehen. Ändern Sie dazu mit einem Editor und root-Recht in der unten angegebenen Datei

```
sudo gedit /etc/
  sysctl.d/10-ipv6-privacy.conf &
```

folgende Werte:

```
net.ipv6.conf.all.use_tempaddr = 0
net.ipv6.conf.default.use_tem
  paddr = 0
```

Domains für dynamische IP-Adressen

***http://freedns.afraid.org* bietet kostenlos dynamisches DNS für IPv4 und IPv6.** Sie erreichen den heimischen PC dann über Adressen wie „MyDomain.mooo.com“. Nach der Registrierung gehen Sie auf „Dynamic DNS“ und konfigurieren die Adresse per Klick auf „[add]“. Wählen Sie hinter „Type:“ den Eintrag „AAAA“, wenn Sie eine IPv6-Adresse verwenden wollen. Anschließend klicken Sie auf „Check out: dynamic update interface (version 2)!“ und dann auf „cron script“. Im Browserfenster sehen Sie ein Cron-Script, das die aktuelle IP-Adresse eines Linux-PCs alle fünf Minuten an afraid.org überträgt und dabei bei Bedarf aktualisiert. Die Installation des Cronjobs erfolgt, indem Sie *crontab -e* in einem Terminalfenster aufrufen und die vorbereiteten Zeilen in den Crontab-Editor einfügen.



IPv6-Freigaben: Wenn Sie bereits das derzeit aktuelle Fritz-OS 06.83 verwenden, tragen Sie die Interface-ID ein, die der Befehl *ip -6 addr* für das Gerät ausgibt.

Speichern Sie die Datei, und laden Sie dann die nächste:

```
sudo gedit /etc/network/interfaces
 &
```

Hier tragen Sie diese vier Zeilen ein:

```
auto enp5s0
iface enp5s0 inet dhcp
iface enp5s0 inet6 auto
pre-up modprobe ipv6
```

„enp5s0“ ersetzen Sie durch den Gerätenamen Ihres Netzwerkadapters (gemäß der Auskunft von *ifconfig*). Speichern Sie die Datei, und starten Sie Linux neu.

Jetzt müssen Sie die Weiterleitung an die IPv6-Adresse konfigurieren. Bei einer Fritzbox gehen Sie auf „Internet -> Freigaben -> IPv6“. Sollte die Registerkarte fehlen, klicken Sie auf „Ansicht: Standard“.

Nach einem Klick auf „Neues Gerät“ wählen Sie den gewünschten PC aus und legen den Port fest, für den die Freigabe gelten soll. Die Angabe hinter „Interface-ID“ muss der IID entsprechen, die *ip -6 addr* ausgibt. Wenn nicht, korrigieren Sie die Werte. Klicken Sie auf „OK“. Über „Freigaben -> MyFRITZ!-Freigaben“ erstellen Sie anschließend wie bei IPv4 eine MyFritz-Adresse.

Beim neueren Fritz-OS 06.83 hat AVM die Portfreigaben für Ipv4 und IPv6 zusammengelegt. Auf der Registerkarte „Portfreigaben“ klicken Sie auf „Gerät für Freigaben hinzufügen“ und tragen dann die „IPv6 Interface-ID“ ein. Klicken Sie auf „Neue Freigabe“, um die Anwendung beziehungsweise den Port festzulegen.

7. Fritz-NAS als zentraler Speicher

Einfacher und kostengünstiger als mit dem eingebauten Fritz-NAS kommen Sie nicht an einen zentralen Netzwerkspeicher. Dabei hat die Fritzbox nebenbei die angenehme Eigenschaft, permanent zu laufen, was bei Netzfreigaben von PCs und selbst bei Datenservern nicht so sicher gewährleistet ist. Einziger Nachteil gegenüber echten Servern ist der geringere Datendurchsatz, wenn nur USB-2.0.Ports für externe Laufwerke vorhanden sind. Dies ist etwa auch bei neuen Fritzboxen 6490 von Vodafone der Fall, die somit keinesfalls ganz baugleich mit der DSL-Fritzbox 7490 ausfallen.

Wird unter „Heimnetz -> Speicher (NAS)“ die NAS-Funktion über „Spei-

Kleine Tipps für die Fritzbox

Netzrechner per Fritzbox „wecken“: Sie möchten per SSH oder Remotedesktop auf einen PC zugreifen oder dessen Freigabe nutzen – aber der schläft in einem Energiesparmodus. Je nachdem, wie die räumlichen Verhältnisse liegen, ist es eventuell einfacher, ihn über die Fritzbox zu wecken als per Mausklick. Dazu gehen Sie unter „Heimnetz -> Heimnetzübersicht -> Netzwerkverbindungen“ auf das Stiftsymbol des Rechners und klicken unter „Wake on LAN“ auf die Schaltfläche „Computer starten“.

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).

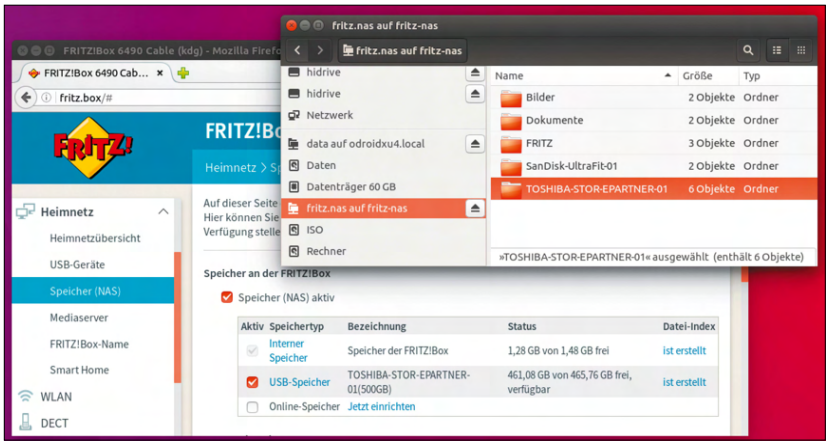
An diese Mailadresse werden die Faxe dann weitergeleitet und auf Wunsch auch noch im Fritzbox-Speicher abgelegt. Bei mehreren Telefonanschlüssen können Sie die gewünschte Rufnummer für den Faxempfang auswählen.

Fritzbox als Druckerserver: Der Router bringt auch ältere Drucker mit USB-Anschluss (aber ohne LAN und WLAN) ins Heimnetz. Theoretisch geht das auch durch Anschluss des Druckers an einen PC und dessen Druckerfreigabe. Der Nachteil dabei ist, dass der PC dann ständig laufen müsste. Die Fritzbox tut's. Schließen Sie daher den Drucker an einen USB-Port des Routers an und schalten Sie ihn ein. Die Fritzbox sollte den Drucker unter „Heimnetz -> USB-Geräte -> Geräteübersicht“ melden. Nun gehen Sie auf einem Linux-PC etwa mit Ubuntu in den Systemeinstellungen auf „Drucker“ und „Hinzufügen“. In der Geräteliste wählen Sie „AppSocket/HP JetDirect“ und geben rechts oben als „Rechner“ entweder den Hostnamen „fritz.box“ an oder die IP-Adresse der Fritzbox. Unter Windows nutzen Sie unter „Geräte und Drucker -> Drucker hinzufügen“ die Option „Drucker unter Verwendung einer TCP/IP-Adresse oder eines Hostnamens hinzufügen“.

„Stealth-Modus“: Die Fritzbox unterbindet unerwünschten ein- und ausgehenden Datenverkehr, indem sie das lokale Netzwerk vom

cher (NAS) aktiv“ eingeschaltet, ist sofort der interne Speicher im Netz verfügbar. 512 MB bis 1,5 GB bieten neuere Fritzboxen an internem Speicher an. Das reicht, um einige zentrale Scripts oder Dokumente bereitzustellen, ist aber natürlich für einen Datenserver zu wenig. Sobald Sie an einen der beiden USB-Ports einen USB-Datenträger anschließen, wird dieser unter „Heimnetz -> Speicher (NAS)“ angezeigt und kann durch die Klickbox für das Fritz-NAS aktiviert werden. Dies ist übrigens auch der richtige Ort, um einen Datenträger wieder abzumelden – das Abziehen des USB-Kabels ohne Abmeldung birgt die Gefahr des Datenverlusts. Vorbereitungen auf Seiten des USB-Datenträgers sind nicht nötig: Fritz-OS versteht sich auf Linux- (Ext2) wie Windows-Dateisysteme (NTFS, FAT).

Die Daten lassen sich im Prinzip über die Fritzbox-Weboberfläche unter „Fritz!NAS“ oder durch direkte Eingabe von *fritz.nas* in der Browser-Adresszeile einsehen und bearbeiten. Standard-IP für das Fritz-NAS ist xxx.xxx.xxx.254. Beachten Sie, dass der Hostname „fritz.nas“ eine Standardvorgabe ist, die sich unter „Heimnetz -> Speicher (NAS)“ auch personalisieren lässt.



Fritz-NAS auf der Konfigurationsoberfläche und im Dateimanager: Das Einrichten und Nutzen eines USB-Datenträgers via Fritzbox ist einfacher als jede Serverlösung.

Die Datennutzung über die Weboberfläche ist begrenzt. Als „Upload“ zur Fritzbox sind nur Dateien, keine Ordner möglich. Beim Download von der Fritzbox entsteht ein ZIP-Archiv, das Sie erst entpacken müssen. Das sind Standards, die sich für die Freigabe im Web eignen, aber nicht fürs lokale Netz. Hier verhält sich das Fritz-NAS wie jede andere Samba-Freigabe: Der Standard-Hostname „fritz.nas“ erscheint unter „Netzwerk“ im Dateimanager von Linux- und Windows-PCs, und die Daten lassen sich nutzen, sofern sich der Netzteilnehmer ausweisen kann. Die Einrichtung mindestens eines Benutzerkontos erledigen Sie unter „System -> Fritz!Box-Benutzer“.

8. Alte Fritzbox als WLAN-Repeater nutzen

Viele ausgemusterte Router können noch gute Dienste als WLAN-Repeater leisten, also das Funksignal an geeigneter Stelle der Wohnung verstärken und so die Reichweite erhöhen. Ein WLAN-Repeater dient als Signalverstärker und vergrößert die Reichweite des Funksignals im Netzwerk. Mit den meisten Repeatern ist gleichzeitiges Empfangen und Senden im WLAN nicht möglich. Der Repeater muss also

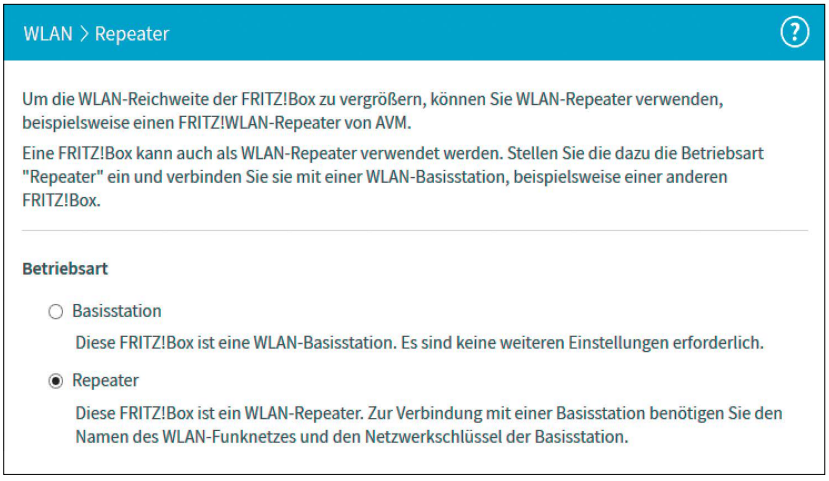
Internet strikt trennt. Das jüngste Fritz-OS 6.50 bietet nun auch eine Option, Ping-Anfragen aus dem Web zu unterbinden. Diesen Stealth-Modus können Sie unter „Internet -> Filter -> Listen“ aktivieren. Erhöhte Sicherheit bietet dies vor allem dann, wenn Sie mit Portfreigaben heimische Serverdienste über das Internet erreichbar machen. Denn Angreifer nutzen zunächst Ping-Kommandos, um nach erreichbaren Internetadressen zu suchen.

Achtung: Manche Internetprovider liefern die Fritzbox ohne diese Funktion aus.

Geräteliste aufräumen: Im Laufe der Zeit wächst die Liste der Geräte, die schon einmal mit der Fritzbox verbunden waren. Darunter sind auch PCs oder Smartphones, die Sie längst nicht mehr benutzen. Das behindert die Übersicht und ist lästig, wenn Sie etwa bei Portfreigaben zahlreiche irrelevante Geräte aus der Dropdown-Liste ausfiltern müssen.

Um auszumisten, klicken Sie auf „Heimnetz -> Heimnetzübersicht -> Netzwerkverbindungen“. Am Ende sind die inaktiven Geräte aufgeführt „(Ungenutzte Verbindungen“), und mit „Entfernen“ räumen Sie die Liste auf. Die Aktion betrifft nur die Geräte, für die Sie keine individuellen Einstellungen aktiviert haben – etwa eine feste IP-Adresse oder eine Filterregel. Über das rote Kreuz ganz rechts bei jedem Gerät lässt sich jedes Gerät aus der Liste löschen – jedoch nur je einzeln.

Priorisierung von Geräten: Ihr Heimnetz ist ohne manuellen Eingriff demokratisch: Jedes Gerät kann die volle Bandbreite beanspruchen. Das ist überall dort, wo es konfliktfrei funktioniert, der einfachste Zustand. Wenn aber der Produktiv-PC etwa bei der Recherche gebremst wird, weil an anderer Stelle weniger produktive Downloads laufen, kann die Fritzbox helfen: Der Punkt lautet „Internet -> Filter -> Priorisierung“. Über „Neue Regel“ unter „Priorisierte Anwendungen“ geben Sie das Gerät an, das möglichst ungebremst arbeiten soll. Der Filter kann auf eine bestimmte Anwendung wie etwa SSH beschränkt werden oder für einen privilegierten Rechner global gelten („alle“ unter „Netzwerkanwendungen“).



Fritzbox zweitverwerten: Wird eine Fritzbox nicht mehr als DSL-Router benötigt, lässt sie sich als WLAN-Repeater weiter verwenden.

Netzwerkpakete zunächst empfangen und kann sie erst danach wieder senden – das halbiert zwar die effektive Bandbreite, kann aber das Funknetz in schlecht erreichbaren Wohnungsbereichen trotzdem deutlich verbessern.

Am einfachsten ist die Zusammenarbeit von Basisrouter und dem zweitem Router bei Geräten desselben Herstellers. Der Kauf eines Repeaters ist oft unnötig, wenn noch eine ältere, ausgediente Fritzbox vorhanden ist: Über eine WLAN-Verbindung lassen sich zwei Fritzboxen zusammenschalten.

Vorbereitungen treffen: Schließen Sie nur die Fritzbox, die als Repeater dienen soll, per Ethernet-Kabel an den PC an. In unserem Beispiel verwenden wir eine ältere Fritzbox 7270 als Repeater und eine Fritzbox 7490 als Basisstation. Rufen Sie die Benutzeroberfläche der Repeater-Fritzbox auf, indem Sie im Browser die Standard-IP „192.168.178.1“ in die Adresszeile eintippen und die Eingabetaste drücken. Geben Sie der Fritzbox eine neue IP-Adresse, sodass sie nicht mit der anderen Fritz kollidieren kann. Wählen Sie in der linken Spalte der Fritzbox-Oberfläche „Heimnetz -> Heimnetzübersicht“ und auf der rechten Seite den Reiter „Netzwerkeinstellungen“. Hier finden Sie etwa in der Mitte der Seite die Schaltflächen für IPv4- und IPv6-Adressen. Hier interessieren nur die IPv4-Adressen. Die v6-Adressen lassen Sie unberührt. Tragen Sie die neue v4-Adresse ein, etwa „192.168.178.100“. Bestätigen Sie diese mit einem Klick auf „OK“.

Nach der Änderung der IP-Adresse müssen Sie sich an der Repeater-Fritzbox unter der jetzt aktuellen IP-Adresse neu anmelden. Klicken Sie in der Fritzbox-Benutzeroberfläche auf „WLAN -> Funknetz“, und aktivieren Sie das WLAN-Funknetz, falls noch nicht geschehen. Ebenfalls auf dieser Seite setzen Sie ein Häkchen vor die Optionen „Name des WLAN-Funknetzes sichtbar“ und „Alle neuen WLAN-Geräte zulassen“. Klicken Sie zum Speichern der Einstellungen auf „Übernehmen“.

Basisstation einrichten: Schalten Sie nun die Basis-Fritzbox ein, und verbinden Sie sie per LAN-Kabel direkt mit dem Rechner. Melden Sie sich über die Standard-IP-Adresse „192.168.178.1“ an. Klicken Sie in der Benutzeroberfläche der Fritzbox auf „WLAN -> Repeater“, und aktivieren Sie die Option „Basisstation“, falls das nicht der Fall sein sollte.

Zum Speichern der Einstellungen klicken Sie auf „Übernehmen“. Es sind keine weiteren Einstellungen erforderlich. Für den Verbindungsaufbau mit einem Fritzbox-Repeater wird lediglich der WLAN-Netzwerkschlüssel benötigt, der auf der Seite „WLAN -> Sicherheit“ zu finden ist.

Repeater einrichten: Sorgen Sie dafür, dass die Repeater-Fritzbox im Netzwerk über eine LAN-Verbindung erreichbar ist, und melden Sie sich über die zuvor vergebene IP-Adresse „192.168.178.100“ an. Gehen Sie zu „WLAN -> Repeater“. Unter „Betriebsart“ aktivieren Sie die Option „Repeater“. Automatisch werden nun die Funknetzwerke in Reichweite des Repeaters angezeigt. Beachten Sie, dass Sie die Repeater-Fritzbox nur mit WLAN-Funknetzen verbinden können, die das Verfahren zur Reichweitenvergrößerung unterstützen. Wählen Sie ein WLAN aus, indem Sie ein Häkchen am Anfang der Zeile setzen. Tragen Sie dann noch den WLAN-Netzwerkschlüssel in das entsprechende Feld ein, und speichern Sie die Einstellungen mit „Übernehmen“. Jetzt wird die WLAN-Verbindung zwischen den beiden Fritzboxen hergestellt.

Ist alles in Ordnung, erscheint auf der nächsten Seite die Meldung „Die Einrichtung wurde erfolgreich abgeschlossen“, und Sie können den Repeater etwa in einem anderen Stockwerk aufstellen – idealerweise auf der Hälfte der Strecke zwischen Basisstation und WLAN-Empfänger.

Clients verbinden: Da Fritzbox-Basisstation und -Repeater den gleichen Netzwerknamen, den gleichen Funkkanal und die gleichen Sicherheitseinstellungen verwenden, brauchen Sie an den bisher schon verwendeten WLAN-Clients wie Notebook, Smartphone und Tablet keine Änderungen vorzunehmen. Sie verbinden sich automatisch mit der Fritzbox in Reichweite, die ein stärkeres WLAN-Signal liefert. Vom Wechsel zwischen Basisstation und Repeater bekommen Sie auf Clientseite nichts mit.

9. Fritzbox als Access Point verwenden

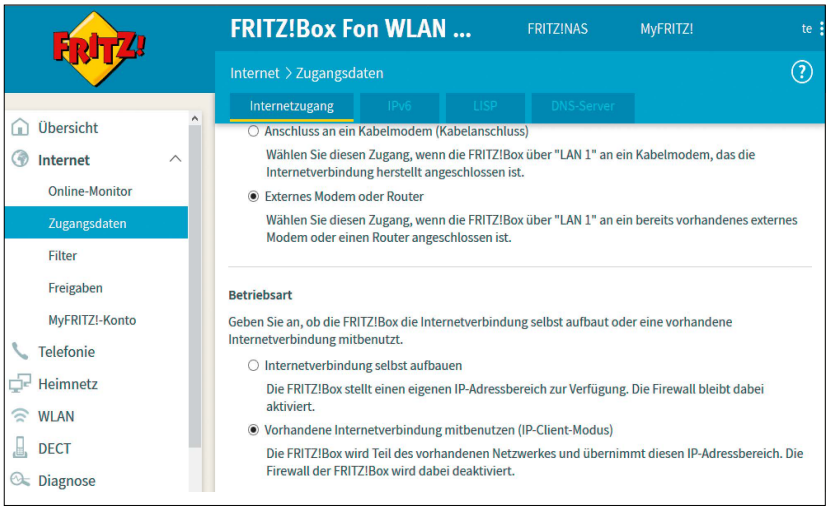
Mit einem zusätzlichen Access Point, der per Ethernet oder Powerline angeschlossen ist, erweitern Sie die Reichweite des WLANs. Alte Router eignen sich nach einigen Vorbereitungen ideal: Der Router, der als Access Point

dient, muss eine statische IP-Adresse bekommen, und nur der Hauptrouter darf als DHCP-Server aktiv sein. Im Vergleich zur Repeaterkonfiguration (siehe Punkt 8) ist die Geschwindigkeit höher, weil Senden und Empfangen gleichzeitig erfolgen. Es muss jedoch ein Ethernet-Kabel zum Access Point führen.

Gehen Sie in die DHCP-Einstellungen des Hauptrouters, und legen Sie dort einen eingeschränkten Adressbereich fest, beispielsweise von 192.168.1.0 bis 192.168.1.100. Den alten Router verbinden Sie nun per LAN-Kabel zur weiteren Konfiguration mit einem PC und klemmen diesen temporär vom WLAN ab.

Das Altgerät gibt dem PC eine IP-Adresse, und Sie können die Konfigurationsoberfläche im Browser aufrufen. Dort geben Sie dem Router eine IP-Adresse, die außerhalb des zuvor definierten DHCP-Bereichs liegt, beispielsweise 192.168.1.101. Schalten Sie zudem den DHCP-Server ab. Sie finden die Einstellungen nach Klicks auf „Heimnetz -> Heimnetzübersicht -> Netzwerkeinstellungen“ und die Schaltfläche „IPv4-Adressen“.

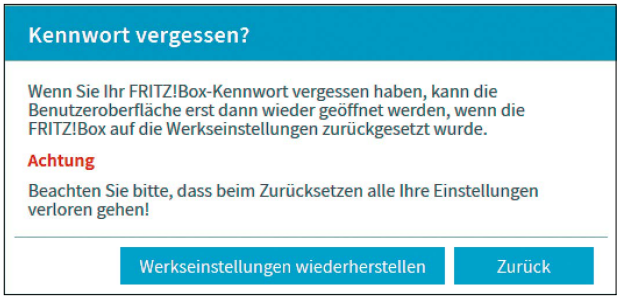
Ihr zweites WLAN richten Sie dann nach Belieben mit SSID und Kennwort ein. Bei einer AVM-Fritzbox müssen Sie auf „Internet > Zugangsdaten“ gehen. Wählen Sie „Weitere Internetanbieter“ und dann „Andere Internetanbieter“. Unter „Anschluss“ wählen Sie „Externes Modem oder Router“ und „Vorhandene Internetverbindung im Netzwerk mitbenutzen (IP-Client)“. Danach führen Sie einen Router-Neustart durch, klemmen den umfunktionierten Router vom PC ab und verbinden ihn als neuen Access Point über den LAN-Port (nicht über WLAN/DSL) mit dem zentralen DSL- oder WLAN-Router.



WLAN erweitern: Die Fritzbox kann eine vorhandene LAN/Internetverbindung eines anderen Routers verwenden und den Zugriff darauf per WLAN ermöglichen.



Zurück auf null: Einige Router besitzen einen Reset-Knopf, über den sich das Gerät auf die Werkseinstellungen zurücksetzen lässt.



Rettung für die Fritzbox: Ist das Kennwort nicht mehr auffindbar, hilft nur die Wiederherstellung der Werkseinstellungen.

10. Routerpasswort vergessen

Wie lautet das Passwort für die Konfigurationsoberfläche des WLAN-Routers? Damit wieder das Standardpasswort des Herstellers funktioniert, ist ein vollständiges Zurücksetzen der Routerkonfiguration erforderlich. Hierzu müssen Sie bei den meisten Routern, ausgenommen der Fritzbox, den im Szene-Jargon „30/30/30-Reset“ genannten Kaltstart durchführen:

1. Sie schalten den Router ein und drücken 30 Sekunden lang die Reset-Taste. Bei vielen Geräten ist dafür ein spitzer Gegenstand notwendig, da der Schalter im Gehäuse versenkt ist.

2. Bei gedrückter Reset-Taste trennt man das Gerät vom Strom und hält die Reset-Taste für weitere 30 Sekunden.

3. Bei weiterhin gedrückter Reset-Taste stecken Sie das Gerät wieder an das Stromnetz an. Nach zusätzlichen 30 Sekunden lassen Sie die Reset-Taste schließlich los.

Besonderheit bei Routern von Asus: Diese Geräte schalten nach einem solchen Reset zunächst einmal in einen Recovery-Modus. Nach Schritt 3 trennen Sie Asus-Router aus diesem Grund nochmals von der Stromversorgung und schließen sie erst nach einigen Sekunden wieder an.

Die Fritzbox von AVM kann Ihnen einen Zugangslink zusenden, falls Ihre Mailadresse in der Routerkonfiguration hinterlegt ist. Klicken Sie dazu einfach auf der Weboberfläche auf „Kennwort vergessen?“ unterhalb der Kennwortabfrage und im folgenden Schritt auf „Push Service Mail senden“. Wenn keine Mailadresse hinterlegt ist, dann müssen Sie auch hier alles zurücksetzen. Dies gelingt innerhalb der ersten zehn Minuten nach dem Start der Fritzbox auf der Weboberfläche über „Kennwort vergessen? -> Werkseinstellungen wiederherstellen“.

Nach einem Router-Reset müssen Sie einen Rechner per Ethernet-Kabel mit dem Router verbinden, damit der PC über DHCP eine IP-Adresse erhält. Im Anschluss daran erreichen Sie im Browser mit der IP-Adresse die Routerkonfiguration.

Die IP-Adresse des Routers wiederum erhalten Sie über die Eingabe von *ifconfig* im Terminal, wobei Sie die vierte Zahl der IPv4-Adresse durch „1“ ersetzen. Die bekannten Log-ins der werkseitig vergebenen Standardzugänge von Routern sind auf der Webseite *www.routerpasswords.com* zusammengetragen.

11. Notfall-Reset bei der Fritzbox

Bei der in Deutschland weit verbreiteten Fritzbox gibt es keinen Reset-Knopf. Wenn Sie sich bei der Fritzbox anmelden können, gehen Sie auf „System -> Sicherung“ und dann auf die Registerkarte „Werkseinstellungen“. Klicken Sie auf „Werkseinstellungen laden“. Sie können stattdessen auch ein Telefon verwenden, das mit dem Anschluss für ISDN-Geräte („FON S0“) verbunden ist. Eine Beschreibung finden Sie über *www.pcwelt.de/FWUBzP*.

Sollte kein Zugriff mehr möglich sein, probieren Sie das AVM-Wiederherstellungsprogramm aus. Darüber installieren Sie die Firmware neu und löschen alle Einstellungen. Sie finden das Programm unter *ftp://ftp.avm.de/fritz.box/*. Gehen Sie in den Ordner mit der Bezeichnung Ihrer Fritzbox und dann in den Ordner „x_misc/deutsch“. Laden Sie die EXE-Datei mit der höchsten Versionsnummer herunter, für eine Fritzbox 7390 zurzeit beispielsweise die Datei „fritz.box_fon_wlan_7390.annexb.06.83.recover-image.exe“.

Eine Linux-Version gibt es bislang nicht, so dass Sie die Wiederherstellung an einem Windows-PC durchführen müssen. Eine virtuelle Windows-Maschine etwa innerhalb von Virtualbox funktioniert ebenfalls. Eine ausführliche Anleitung zum Wiederherstellungsprogramm finden Sie über *www.pcwelt.de/FIMQIh*. Sollte auch das Wiederherstellungsprogramm nicht funktionieren, ist das Gerät wahrscheinlich defekt.



Fritzbox-Zubehör: Über die Fritzbox lassen sich Steckdosenschalter oder Heizungsthermostate steuern. Das geht im Heimnetz, aber auch über das Internet.

12. Smart Home mit der Fritzbox

Die Fritzbox kann auch Schalter oder Heizungsthermostaten steuern, die Sie als Zubehör erwerben können. Das funktioniert über die Weboberfläche der Fritzbox, mit Apps fürs Smartphone oder mit Scripts. Zurzeit gibt es beispielsweise den Schalter Fritz Dect 200 (etwa 45 Euro, *http://avm.de*) und den Heizkörperregler Fritz Dect 300 (etwa 50 Euro, *http://avm.de*). Fritz Dect 200 erfordert eine Fritzbox mit Fritz-OS ab Version 5.50. Fritz Dect 300 benötigt Fritz-OS ab Version 6.60.

Geräte bei der Fritzbox anmelden: Um beispielsweise eine Fritz Dect 200 mit der Fritzbox zu koppeln, stecken Sie die Fritz Dect 200 in eine Steckdose möglichst in der Nähe der Fritzbox, damit Sie während des Drückens der Dect-Taste die Fritz Dect 200 im Blick haben. Drücken Sie dann die Dect-Taste auf der Fritzbox. Dafür haben Sie zwei Minuten Zeit. Nach etwa zehn Sekunden sollte die Fritz Dect 200 an der Fritzbox registriert sein. Aktualisieren Sie dazu die Ansicht in der Weboberfäche der Fritzbox – jetzt sollten Sie die Fritz Dect 200 auf der Übersichtsseite unter „Heimnetz“ sehen. Nun können Sie die Fritz Dect 200 dort in die Steckdose stecken, wo sie künftig ihre Dienste verrichten soll.

Gehen Sie auf „Heimnetz -> Smart Home“. Den Schalter der Fritz Dect 200 können Sie hier unter „Aus / An“ bedienen. Beim Thermostat Fritz Dect 300 klicken Sie auf die Schaltfläche mit dem Stift-Symbol und können dann die Temperatur regeln oder einen Zeitplan erstellen.

13. Smart-Home-Schalter per Script steuern

Damit sich die Fritzbox über ein Script oder Programm steuern lässt, muss die Anmeldung mit Benutzernamen und Passwort aktiviert sein. Sollte das noch nicht der Fall sein, rufen Sie die Fritz-

box-Oberfläche im Browser auf und gehen auf „System -> FRITZ!Box-Benutzer“. Über die Schaltfläche „Benutzer hinzufügen“ legen Sie einen neuen Benutzer an. Gehen Sie danach auf die Registerkarte „Anmeldung im Heimnetz“, und aktivieren Sie die Option „Anmeldung mit FRITZ!Box-Benutzernamen und Kennwort“.

Über *www.pcwelt.de/82Ecau* laden Sie das ZIP-Archiv „SmartFritz.zip“ herunter. Es enthält das Bashscript „smart_fritz_terminal.sh“ für die Kommandozeile. Öffnen Sie es in einem Editor, unter Ubuntu etwa mit gedit:

```
gedit smart_fritz_terminal.sh &
```

Passen Sie am Anfang des Scripts die Werte für die Fritzbox-URL, das Passwort und den Benutzernamen an.

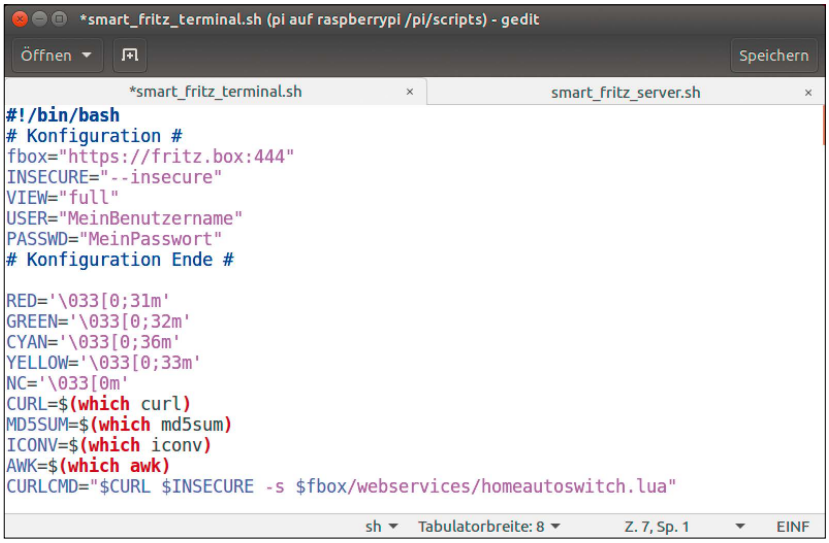
Das Script verwendet das Tool curl für den Zugriff auf die Fritzbox. Bei Ubuntu 16.04 ist es standardmäßig nicht installiert. Holen Sie das mit dieser Befehlszeile nach:

```
sudo apt install curl
```

Starten Sie dann das Script im aktuellen Verzeichnis:

```
./smart_fritz_terminal.sh
```

Es gibt die gefundenen Aktoren-IDs aus, ferner deren Status, die aktuelle Leistungsaufnahme, die bisherige Gesamtleistungsaufnahme und die Temperatur.



Script für Smart Home anpassen: In die Datei „smart_fritz_terminal.sh“ tragen Sie die Adresse Ihrer Fritzbox im lokalen Netzwerk und die Daten für die Benutzeranmeldung ein.

Über folgende Befehlszeile schalten Sie das erste gefundene Gerät aus:

```
./smart_fritz_terminal.sh 1 off
```

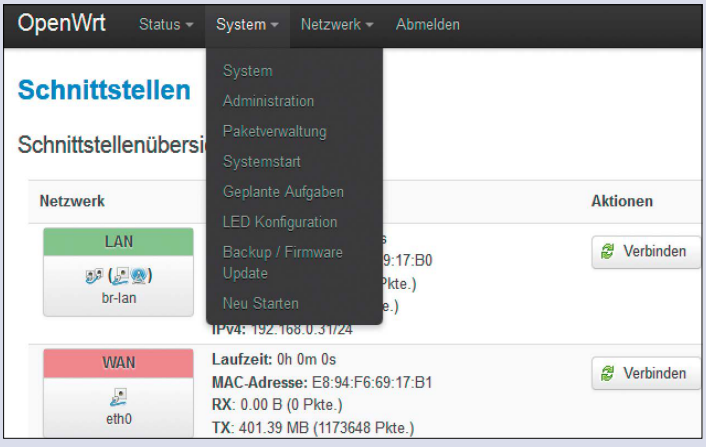
Ersetzen Sie „off“ durch „on“, um es wieder einzuschalten. „toggle“ schaltet den Zustand um.

Die Bedienung eines Schalters geht komfortabler, wenn Sie Verknüpfungen zum Script auf dem Desktop ablegen. Im Download von „SmartFritz.zip“ finden Sie die Dateien „Switch 1 on“ und „Switch 1 off“, die Sie in Ubuntu im Dateimanager in den Ordner „Schreibtisch“ unter „Persönlicher Ordner“ kopieren. „smart_fritz_terminal.sh“ kopieren Sie (als root) nach „/usr/local/bin“. Per Doppelklick auf das jeweilige Desktop-Icon lässt sich der Schalter anschließend ein- und ausschalten.

Alternative Firmware: Alte Router aufgefrischt

Auf handelsüblichen Routern läuft ein vom Hersteller angepasstes Linux-System als Betriebssystem, das nicht immer alle Möglichkeiten ausschöpft. Alternative Routerfirmware zielt darauf ab, alle Funktionen und Einstellungen offenzulegen. Mittlerweile gibt es alternative Firmwarevarianten für Hunderte von Routermodellen.

Das Aufspielen ist bei einigen Geräten so einfach wie ein Softwareupdate, bei anderen sind Geduld und Experimentierfreude gefragt. Einige Router, wie der Belkin (Linksys) WRT1900AC, bewirbt der Hersteller sogar ausdrücklich mit der Kompatibilität zu Open-Source-Firmware. Drei Open-Source-Firmwares haben sich als gut gepflegte Projekte etabliert: DD-WRT (*https://www.dd-wrt.com/site*), Open WRT (*https://openwrt.org*) und Tomato USB (*http://tomatousb.org*).



Router aufwerten: Alternative Firmware wie Open WRT bietet mehr als die vom Hersteller standardmäßig auf dem Router installierte Software.

In einer anderen Liga spielen die Router von AVM, die als Fritzbox, Speedport oder 1&1 Home Server vermarktet werden. Inoffizielle Firmware-Images können aus rechtlichen Gründen nicht zum Download angeboten werden, sondern erfordern das Kompilieren auf eigene Faust (*http://pcwelt.de/1955419*).

Privates Netz mit Pi VPN

Ein Virtual Private Network (VPN) stellt eine sichere Verbindung zu einem internen Netzwerk über das Internet her. Open VPN ist eine bewährte Lösung. Dessen Einrichtung macht die Script-Sammlung Pi VPN auf dem Raspberry Pi einfacher.

Von **David Wolski**



In den wenig vertrauenswürdigen Gewässern öffentlicher Internetverbindungen ist das Virtual Private Network ein sicherer Hafen. Ein VPN verschlüsselt den gesamten Datenverkehr auf Netzwerkebene. Es ist auch ein sicheres Eingangstor zum Netzwerk dahinter und kann mit dem richtigen Routing eine Verbindung zum gesamten Netzwerk herstellen. Für diese Rolle ist der Raspberry Pi geradezu prädestiniert, da hier alle Werkzeuge zur Verfügung stehen. Die Leistung der CPU und die Geschwindigkeit des 100-MBit-Ethernet-Ports reichen für ein kleineres Netzwerk, das per DSL an die Außenwelt angebunden wird.

Einfachere Einrichtung durch Pi VPN

Open VPN ist die verbreitete VPN-Lösung für Linux-Systeme. Es ist Open Source, gilt als sehr sicher, was ein unabhängiger Sicherheitsaudit im Mai 2017 wieder bestätigt hat. Open VPN ist aber für den professionellen Einsatz geschaffen und die Konfiguration des Servers stellt eine Hürde dar. Diese erfolgt ganz nach Linux-Tradition in der Kommandozeile und mittels textbasierenden Konfigurationsdateien. Bevor das VPN steht, gilt es, eine Menge an Dokumentation zu wälzen. Ungeduldige Anwender werden lieber gleich etliche Konfigurationsbeispiele durchprobieren. So oder so macht einem Open VPN den Anfang nicht leicht.

Es geht aber inzwischen deutlich einfacher: Pi VPN (*http://www.pivpn.io*) ist ein Bash-Script, das alle wesentlichen Konfigurationsschritte in textbasierten Menüs im Terminal abhakt. Zwar ist das Pi im Namen ein Hinweis auf den Raspberry Pi, da die Platine oft als kleiner VPN-Server eingesetzt wird. Pi VPN arbeitet aber an sich auf beliebiger Hardware und auf vielen Linux-Distributionen. Unterstützt wird nicht nur Raspbian, sondern auch Debian, Ubuntu und alle Abkömmlinge.

Pi VPN ist schon ein paar Jahre verfügbar, von seinen Entwicklern aber erst vor kurzem fit für die aktuellen Debian- und Ubuntu-Ausgaben gemacht worden. Weil es sich um Open VPN handelt, gibt es an Clientsoftware sowieso keinen Mangel: Für Linux, Windows, Mac-OS X, Android und iOS gibt es Clients.

Die Vorbereitungen für Pi VPN

Bei den Vorarbeiten unterscheidet sich der VPN-Aufbau mittels Pi VPN nicht von anderen Lösungen:

1. Der VPN-Server, also der Raspberry Pi oder der Linux-Rechner, braucht im LAN eine feste IP-Adresse vom Router. Diese Vorarbeit erledigt man in der Administrationsoberfläche des Routers anhand der MAC-Adresse des VPN-Servers. Je nach Routermodell unterscheidet sich die Einrichtung der festen IP für einen Rechner im LAN. Bei der AVM Fritzbox lautet die Funktion „Diesem Netzwerkgerät immer die gleiche IPv4-Adresse zuweisen“ und ist unter Heimnetz -> Heimnetzübersicht -> Netzwerkverbindungen -> Bearbeiten“ zu finden.

2. Diese feste lokale IP-Adresse muss nun durch eine Portweiterleitung des Routers von außen aus dem Internet erreichbar sein. Ein Beispiel dazu: Der übliche Port für Open VPN ist der Port 1194. Wenn der Open-VPN-Server im LAN die IP 192.168.1.77 hat, dann muss der Router den Verkehr vom Typ UDP des Ports 1194 auf die lokale IP-Adresse des Raspberry und den dortigen Port 1194 umleiten.

3. Die öffentliche Internet-IP ist bei DSL-Anbindung nicht feststehend, da der Provider bei jedem Verbindungs-

aufbau und mindestens einmal täglich eine zufällige neue IP-Adresse vergibt.

Hier kommt ein dynamischer DNS-Dienst wie beispielsweise das kostenlose No-IP (*www.noip.com*) zur Hilfe, das einer sich ändernden IP-Adresse nach Rückmeldung durch den Router einen festen Hostnamen zuteilt. Die meisten DSL-Router unterstützen No-IP und teilen dem Dienst automatisch bei jeder Neuverbindung die zugeteilte IP mit.

Pi VPN: Erster Start

Weil es sich um ein Bash-Script handelt, verlangt Pi VPN keine Installation im eigentlichen Sinne. In der Kommandozeile laden Sie mit wget

```
wget -O pivpn https://install.
 pivpn.io
```

einfach das Script in das aktuelle Verzeichnis herunter und starten es von dort mittels

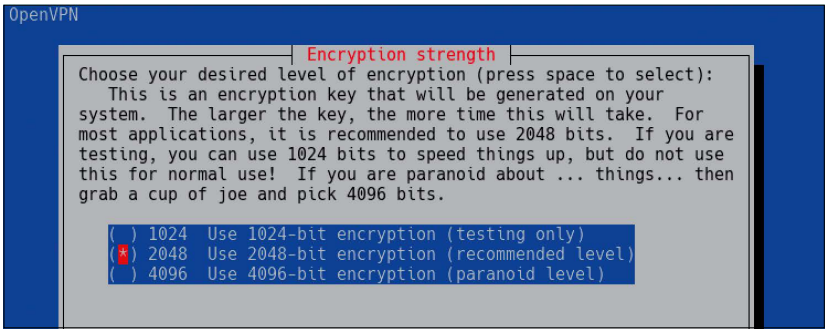
```
bash pivpn
```

Für einige Aktionen wird das Script nach dem sudo-Passwort fragen und zunächst automatisch per apt-get die noch benötigten Pakete installieren. Danach beginnt die eigentliche Einrichtung von Open VPN über die englischsprachigen Menüs von Pi VPN: Die Pfeiltasten bewegen den Cursor zwischen Optionen und Tab wechselt zu „OK“ beziehungsweise „Cancel“.

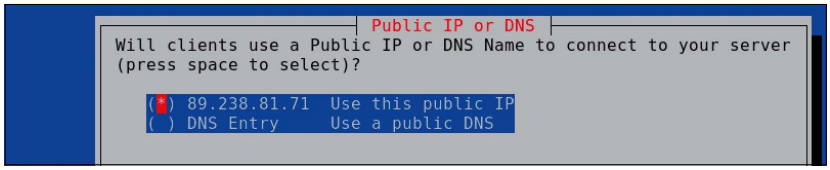
Pi VPN beginnt mit dem Hinweis, dass eine statische IP-Adresse konfiguriert werden sollte. Wenn dieser Schritt schon in den Vorarbeiten auf dem Router erledigt wurde, überspringen Sie diesen Punkt.

Der nächste Dialog „Choose a local user that will hold your ovpn configurations“ fragt nach einem lokalen Benutzerkonto, in dem die Open-VPN-Konfiguration liegen soll. Hier wählen Sie das eigene Benutzerkonto aus. Im folgenden Schritt schlägt Pi VPN vor, automatische Updates („unattended upgrades“) einzuschalten, falls dies noch nicht der Fall ist.

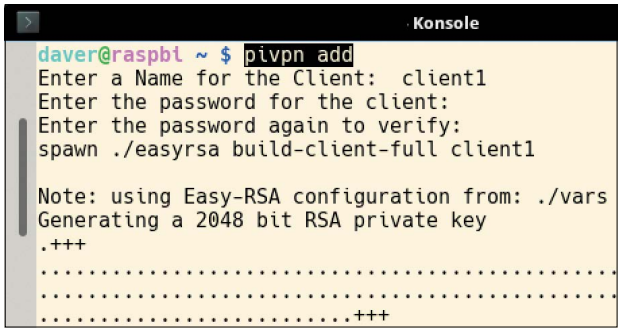
Die anschließende Frage, ob UDP oder TCP als VPN-Protokoll zum Einsatz kommen soll, belässt man auf UDP. Auch die vorgeschlagene Portnummer sollte bei 1194 bleiben, da dies der Standardport für Open VPN ist. Die empfohlene Schlüssellänge von 2048 Bit ist ebenfalls in Ordnung.



Schlüssellänge auswählen: 2048 Bit gelten als sicher. Auf dem Raspberry Pi wird es eine Weile dauern, bis der ARM-Prozessor den Schlüssel erzeugt hat.



Ein Server mit fester IP im Internet ist über diese IP-Adresse erreichbar. Für heimische Server muss in der Regel ein dynamischer Hostname aushelfen („DNS Entry“).



Clients erstellen: Pi VPN erzeugt auch die Clientkonfiguration in wenigen Schritten. Die fertige Datei liegt im Verzeichnis „~/ovpns“ und enthält auch sämtliche Schlüssel.

Danach erstellt Pi VPN die serverseitigen kryptografischen Schlüssel, was auf kleinen Platinenrechnern wie dem Raspberry Pi eine Weile dauert. Der Dialog „Public IP or DNS“ fragt dann, ob der VPN-Server per IP-Adresse oder per Hostname („DNS Entry“) erreichbar ist. Im Fall eines heimischen Servers ist das der dynamische Hostname, den sich der Router bei einem der eingerichteten DNS-Dienste holt (No-IP oder vergleichbar). Der nächste Schritt gibt eine Reihe an DNS-Servern zur Auswahl, die Clients verwenden sollen, wenn diese über das VPN das Internet nutzen. Danach schlägt Pi VPN einen Neustart vor, um den Open-VPN-Dienst in Gang zu setzen.

Die Netzwerkclients hinzufügen

Auch für das Erzeugen von VPN-Zertifikaten, mit der sich Clientrechner bei Open VPN anmelden, hat Pi VPN ein Hilfs-Script parat: Mit dem Kommando

```
pivpn add
```

erstellt man im Nu die Clientkonfigurationsdateien. Dieses Script fragt nur nach dem gewünschten Clientnamen und einem Passwort, anschließend liegt die fertige Konfigurationsdatei mit dem Namen „[Client].ovpn“ im Ordner „~/ovpns“. Nur diese eine Datei benötigt man auf den zugreifenden Clients und kann sie dort in den verwendeten Open-VPN-Client importieren. Auch alle Schlüssel und das Serverzertifikat sind in dieser einen Datei untergebracht. Das Script kann mittels

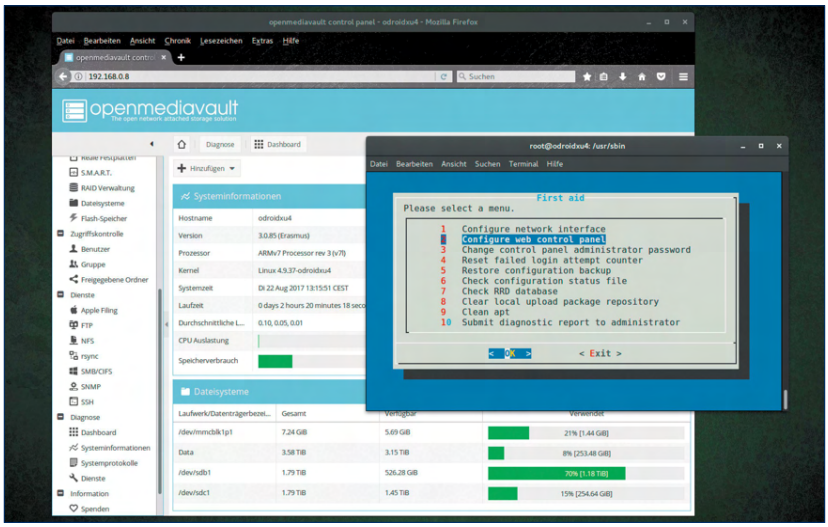
```
pivpn revoke
```

auf Wunsch einen Client jederzeit auch wieder entfernen. ●

Tipps zu Open Media Vault 3

Das NAS-System Open Media Vault Version 3 „Erasmus“ ist seit längerem verfügbar und läuft nun sehr stabil. Trotzdem gibt es bei der Bedienerführung einiges zu beachten. Hier erfahren Sie, wie Sie das System installieren, einrichten und bedienen.

Von **Hermann Apfelböck**



Das Debian-basierte Open Media Vault (OMV) hat sich die letzten Jahre zum Standard unter den freien NAS-Systemen entwickelt. Das mit allen wesentlichen NAS-Funktionen ausgestattete OMV (attraktive Web-GUI via Nginx-Server, SSH, Samba, FTP, neues AFP – Apple Filing, NFS, Energieverwaltung, SMART, Software-Raid, Benutzerverwaltung, Plug-ins) läuft seit jeher auf x86-Plattformen, hat aber umgehend auf Raspberry & Co reagiert. Das System NAS-4Free ist im Prinzip gleichwertig, hatte aber den Platinenboom zunächst verschlafen. Erst seit 2015 gibt es NAS-4Free auch für ARM-Architektur und Raspberry, wo sich Open Media Vault aber schon seit den Raspberry-Anfängen 2012 etabliert hatte. Die nachfolgenden Tipps zu OMV 3 beziehen sich auf den Einsatz auf Platinenrechnern. Natürlich gibt es nach wie vor auch eine x86-Variante für PCs. Falls Sie diese einsetzen, benötigen Sie das Image „openmedia-vault_3.0.99-amd64.iso“ und zwei USB-Sticks – einen für das ISO mit der Installationsroutine, den zweiten als Zieldatenträger.

Hinweise zur Installation auf Raspberry & Co.

Der Weg vom Image zum OMV-Start ist unproblematisch: Unter *https://sourceforge.net/projects/openmediavault/files/* gibt es neben der x86-Variante ARM-Images für Raspberry Pi, Odroid, Cubietruck oder Banana Pi. Der Download ist 7-Zip-gepackt und beträgt nur circa 250 MB. Beim Entpacken (unter Windows ist die Freeware 7-Zip erforderlich) entsteht eine IMG-Datei mit annähernd zwei GB. Diese kopieren Sie dann mit den einschlägigen Tools (dd, Etcher oder Win 32 Disk Imager) auf eine SD-Karte.

Damit wäre die „Installation“ eigentlich schon erledigt, aber je nach Kartenkapazität sollten Sie eventuell schon vor der Inbetriebnahme eine Korrektur vornehmen: OMV genügen im Prinzip zwei GB auf SD-Karte (Platine). Bei größeren Kapazitäten partitioniert das System den Datenträger so, dass die Systempartition acht GB erhält und der Rest an eine ungenutzte zweite Partition fällt. Ein Expandieren der Systempartition wie bei Raspbian (raspi-config) gibt es bei OMV nicht. Am einfachsten ist es, von vornherein einen Acht-GB-Flashspeicher zu verwenden. Wenn Sie den Platz eines größeren Datenträgers nicht verschenken möchten, dann nutzen Sie gleich nach dem Schreiben auf SD-Karte den Partitionierer Gparted auf dem PC. Damit können Sie die Systempartition auf die gesamte Kapazität erweitern oder den ungenutzten Plattenplatz als kleine Datenpartition einrichten.

Upgrade von älterer Version: Wer OMV 2.x laufen hat, kann theoretisch direkt auf 3.0 upgraden. Die Entwickler warnen allerdings vor dem Upgrade insbesondere bei installierten Plug-ins. Die Aktion erfordert im Prinzip nur den Befehl *omv-release-upgrade* im SSH-Terminal. Besser ist es, das System vorher auf Stand zu bringen:

```
apt-get update
apt-get dist-upgrade
omv-update
omv-release-upgrade
```

Die Prozedur ist langwierig (mehrere Stunden), der Ausgang ungewiss. In unserem Fall lief das Upgrade mit marginalen Fehlermeldungen erfolgreich durch, doch hatte das Resultat eine Reihe gravierender Probleme, so dass nach Sicherung der Konfigurationsdateien eine Neuinstallation fällig war. Bei der kommenden Version OMV 4 wird das vermutlich ähnlich sein.

Fundamentale Konfigurationsschritte

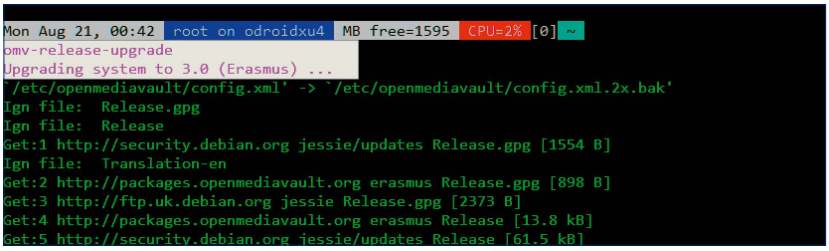
Egal ob Sie per Browser-Oberfläche oder über SSH zugreifen - in jedem Fall benötigen Sie die lokale IP-Adresse des Systems, die Sie vor dem ersten Zugang am einfachsten im Router Ihres Netzwerks ermitteln. Für den komfortablen Dauerbetrieb ist es zu empfehlen, dem Platinenserver über den Router gleich eine feste IP zuzuteilen.

Voreingestellter Anmeldestandard für die Oberfläche ist „admin“ und Kennwort „openmediavault“. Für den SSH-Zugriff, der seit Version 3.0 standardmäßig aktiv ist, lautet der Standard „root“ mit Kennwort „openmediavault“.

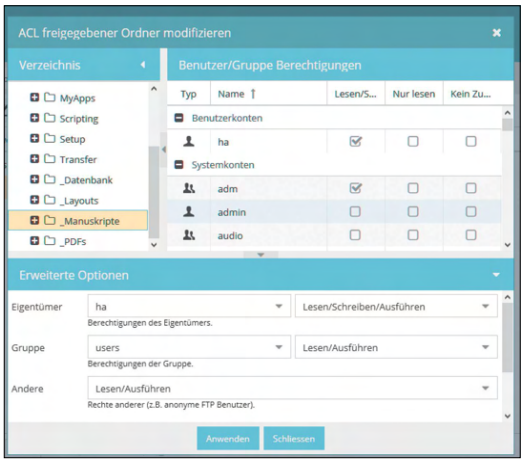
Die Oberfläche ist komplett deutsch, sofern Sie dies beim Log-in oder danach in der GUI angeben. Farben und Schriften wurden in Version 3.0 schick modernisiert, funktional unterscheidet sich 3.0 aber nur marginal vom Vorgänger (siehe „Dienste -> Apple Filing“). Auch der typische Zweischritt ist unverändert, der nach Einstellungsänderungen und „Speichern“ dann auch noch den Klick auf „Anwenden“ einfordert.

Angeschlossene Datenträger (FAT, NTFS, Ext und ab 3.0 auch exFAT) lädt OMV beim Systemstart automatisch ins Dateisystem und zeigt sie als physische Festplatten unter „Datenspeicher -> Reale Festplatten“ (Energieoptionen, Spindown, Cache) sowie als logische Partitionen unter „Datenspeicher -> Dateisysteme“ (ein/aushängen, neu erstellen, löschen). Wenn Sie Datenträger im laufenden Betrieb anschließen, melden Sie diese über „Datenspeicher -> Reale Festplatten“ und „Suchen“ am System an. Unter „Dateisysteme“ können Sie die zusätzliche Platte „Einbinden“.

Wesentliche erste Konfigurationswege führen in der Regel zu den Netzdiensten („Dienste“). So muss etwa für plattformunabhängige Netzfreigaben an Windows, Linux, Mac-OS „SMB/CIFS“ aktiviert werden. Danach kann sofort im Register „Freigaben“ ein Datenträger oder Ordner freigegeben



OMV-Upgrade von 2.x auf 3: Trotz technischer Upgradeoption raten die Entwickler zur Neuinstallation. Das wird beim kommenden OMV-Upgrade auf 4 nicht anders sein.



OMV kann auch Dateirechte ändern: Unter „Zugriffskontrolle -> Freigegebene Ordner“ gibt es „Privilegien“ und „ACL“. Ersteres regelt den Netzzugriff, zweiteres die Dateirechte.

werden. Die zugriffsberechtigten Konten richten Sie unter „Zugriffskontrolle -> Benutzer“ ein. Unter „Zugriffskontrolle -> Freigegebene Ordner“ finden Sie die vorher unter „SMB/CIFS“ eingerichteten Freigaben, die hier über „Privilegien“ (Netzwerkrechte) detaillierter konfiguriert werden können. Über das Register „ACL“ sind im Bedarfsfall auch Änderungen der lokalen Dateirechte möglich (Besitzer, Zugriffsrechte).

Konfigurationsoberfläche und SSH

Dass OMV 3 trotz schicker Weboberfläche auch die SSH-Administration als wichtige Alternative sieht, belegt die Tatsache, dass SSH als einziger Dienst ab Werk aktiv ist.

Beachten Sie in Problemsituationen auch die stattliche Anzahl von Terminalhilfsprogrammen unter „/usr/sbin“, allesamt mit „omv“ im Programmnamen – etwa omv-firstaid oder omv-sysinfo. Damit lassen sich theoretisch OMV-Basiseinstellungen via SSH auch dann einrichten, wenn die GUI streikt. Praktisch gibt OMV aber so gut wie nie Anlass, diese Nothelfer zu bemühen.

Wen es dennoch gewohnheitsmäßig mehr zur SSH-Konsole zieht, wird in Version 3 auf zwei kleine Probleme stoßen: Die Datenträger werden jetzt nicht mehr unter „/media“ eingehängt, sondern unter „/srv“. Dies entspricht den Regeln des Filesystem Hierarchy Standard (FHS) und folgt den Standardisierungstendenzen für Unix-basierte Systeme. Auf der GUI spielt das keine Rolle, aber im SSH-Terminal kann das einige Umbauten erfordern. In unserem Fall mussten wir altgewohnte rsync-Jobs und ein paar Navigations-Aliases nach dem Umstieg erst einmal auf die neuen Pfade umschreiben.

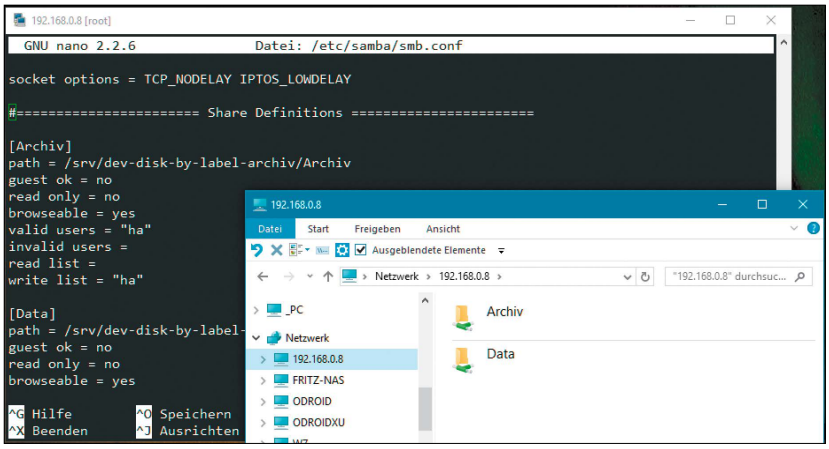
Noch eine Kleinigkeit: Gewohnte Tasten scheinen unter OMV im SSH-Terminal nicht mehr zu funktionieren. Ursache ist eine benutzerspezifische „~/.inputrc“ für das root-Konto. Globale Einstellungen in der Datei „/etc/inputrc“ gelten erst wieder, wenn man die benutzerspezifische löscht oder umbenennt. ●

Der Samba-Server

Ein Datenserver auf Samba-Basis ist die verbreitetste und universellste Serverrolle im Heimnetz. In diesem Beitrag erläutern wir die grundsätzliche Einrichtung eines Samba-Servers sowie die Vor- und Nachteile dieser Methode.

Von **Hermann Apfelböck**

Dieser und die nachfolgenden Artikel präsentieren eine stattliche Anzahl von multifunktionalen, aber auch von sehr speziellen Serverrollen. Spezialisierte Server etwa für das Medienstreaming oder für die Bereitstellung von E-Books oder Kalenderdaten werden immer mediengerechter, präsentabler und komfortabler ausfallen als universelle Lösungen. Dennoch stellen wir hier den universellen Samba-Datenserver an die Spitze unserer Serverlösungen: Ein gut organisierter Samba-Server kann als Dauerläufer im Heimnetz die meisten Aufgaben erfüllen. Er kann Musik, Film und Foto ebenso anbieten wie Termine oder E-Books – dies freilich nur auf trockener Ordner- und Dateiebene und mit entsprechender Rechteverwaltung.



Samba-Konfiguration und Resultat beim zugreifenden Client: Ein einfacher Samba-Datenserver für wenige Benutzer ist allein mit Editor und Terminal schnell eingerichtet.

1. Voraussetzungen für Samba-Freigaben

Wer es sich möglichst bequem machen will, wird auf seinem Heimserver (typischerweise, aber nicht zwangsläufig ein Platinenrechner) ein System mit einer klickfreundlichen Weboberfläche einsetzen. Beliebteste Wahl ist dafür aktuell die Debian-basierte Distribution Open Media Vault (*www.openmediavault.org*), die unter *https:/sourceforge.net/projects/openmediavault/* für x86-Architektur und für alle namhaften Platinen erreichbar ist.

Auf die Konfiguration dieses NAS-ähnlichen Systems gehen wir an dieser Stelle nicht näher ein, weil für einen einfachen Datenserver im Heimnetz ein solcher Überbau nicht nötig ist. Wenige Kommandos im Terminal des Servers oder per SSH-Fernwartung genügen, um Netzwerkfreigaben via Samba zu realisieren. Man muss dabei nur die beiden unterschiedlichen Methoden und Kontoregeln beachten und ferner für Netzwerkrechte und lokale Dateirechte sorgen, die sich ergänzen.

Voraussetzung ist in jedem Fall ein installiertes Samba-Serverpaket (bei Serverdistributionen ist es meist schon vorinstalliert):

```
sudo apt update
sudo apt upgrade
sudo apt install samba-common sam
 ba
```

Da Netzwerkrechte allein für den Zugriff nicht genügen, muss jeder Benutzer, der auf Freigaben zugreifen soll, auf dem Server ein reguläres Systemkonto mit Passwort besitzen:

```
sudo adduser sepp
```

Das Systempasswort wird nach Eingabe dieses Befehls automatisch abgefragt. Zweitens muss dieser Benutzer zusätzlich ein Samba-Kennwort erhalten, denn Samba hat seine unabhängige Kennwortverwaltung:

```
sudo smbpasswd -a sepp
```

Wer die Verhältnisse so einfach wie möglich halten will, wird das Samba-Kennwort identisch mit dem Systemkennwort wählen. Das ist nicht maximal sicher, aber in einem Heimnetz jederzeit legitim und üblich.

2. Freigaben über die zentrale Datei „smb.conf“

Samba verwendet als einzige Konfigurationsdatei „/etc/samba/smb.conf“. Darin sind alle Basiseinstellungen und die Freigaben festgelegt. Das Editieren der „smb.conf“ erfordert root-Recht, ist aber umfassender und oft auch bequemer als die alternativen net-Befehle (siehe -> Punkt 3):

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

Beachten Sie, dass alle Änderungen in der „smb.conf“ erst wirksam werden, wenn Sie den Samba-Dienst mit

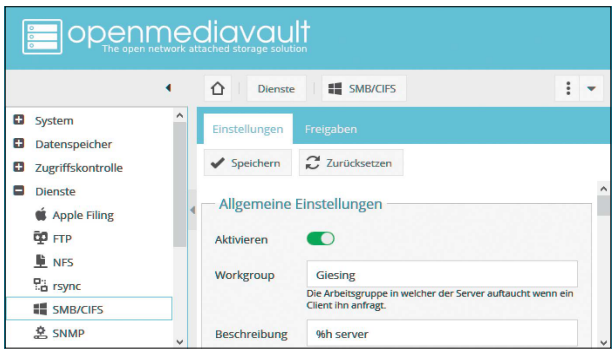
```
sudo service smbd restart
```

neu starten.

Arbeitsgruppe: Der Eintrag „workgroup=WORKGROUP“ unter „[global]“ legt die Arbeitsgruppe fest. Wenn Sie in Ihrem Netzwerk eine an-



Samba-Freigaben erscheinen als „Windows-Speicher" im grafischen Dateimanager. Die Zugangsdaten speichert Linux wie Windows auf Wunsch dauerhaft.



Samba auf Linux-Serversystemen: Wie hier im NAS-System Open Media Vault erscheint Samba typischerweise als Dienst „SMB/CIFS".

ders benannte Gruppe verwenden, ändern Sie hier den Wert entsprechend. Für den Zugriff auf die Freigaben ist die Arbeitsgruppe an sich nicht wesentlich, jedoch zeigen Linux-Dateimanager nicht einfach alle Rechner mit Freigaben in einer Liste an, sondern organisieren sie in Arbeitsgruppen unterhalb von „Windows-Netzwerk". Sie sparen sich also unnötige Mausklicks, wenn Sie alle Rechner in derselben Gruppe unterbringen. Außerdem kann beim späteren Zugriff auf eine Freigabe bei der Abfrage „Domäne" die Arbeitsgruppe eingetragen werden (oder der Rechnername des Servers).

Home-Verzeichnisse freigeben: In der „smb.conf" gibt es einen auskommentierten Abschnitt, der mit „;[homes]" beginnt. Entfernen Sie das Kommentarzeichen (Semikolon), um die Home-Verzeichnisse aller Benutzer standardmäßig freizugeben. Soll Schreibzugriff erlaubt sein, ändern Sie „read only = yes" auf „no". Damit ist mit geringstem Aufwand für alle Benutzerkonten eine Freigabe eingerichtet. Jeder Benutzer sieht dabei nur sein eigenes Home-Verzeichnis als Freigabe. Die Maßnahme ist etwa sinnvoll, wenn mehrere Familienmitglieder ihr je eigenes Home-Verzeichnis für Arbeiten und Backups erhalten sollen.

Allgemeine Freigaben: Für ein zentrales Serverangebot von Dokumenten und Medien sind benutzerbezogene Home-Freigaben natürlich ungeeignet. Eine allgemeine Freigabe für ein beliebiges Verzeichnis lässt sich im allereinfachsten Fall mit drei Zeilen realisieren, die Sie am Ende der Datei „smb.conf" im Abschnitt „Share Definitions" folgendermaßen einfügen:

```
[Archiv]
path = /media/archiv
writeable = yes
```

In diesem Beispiel wird das Verzeichnis „/media/archiv" unter der Bezeichnung „Archiv" freigegeben. Der Ordner muss existieren und die Benutzer müssen auf der Ebene des Dateisystems zumindest Leserechte besitzen. Sie gehen Rechtekonflikten zwischen Netzberechtigungen und lokalen Berechtigungen am einfachsten aus dem Weg, wenn Sie auf dem Server ein künstliches Pseudokonto wie etwa „archiv" einrichten (siehe -> Punkt 1), das dann alle Personen für den Zugriff auf die allgemeine Freigabe benutzen. Die zusätzlich nötigen Zeilen in der „smb.conf" würden in diesem Fall so lauten:

```
valid users = "archiv"
write list = "archiv"
```

Bei dieser vereinfachten Freigabe, die rechtetechnisch nicht weiter differenziert, muss nur vorab sichergestellt sein oder entsprechend korrigiert werden, dass das Systemkonto „archiv" Besitz und Schreibrecht auf „/media/archiv" hat.

3. Freigaben auf Benutzerebene

Es gibt eine alternative Samba-Freigabemethode, die auch Home-Admins kennen sollten, um den Durchblick zu behalten. Netzfreigaben konnten lange Zeit nur über die zentrale Samba-Konfiguration und nur mit root-Recht eingerichtet werden – wie in Punkt 2 beschrieben. Seit etlichen Jahren erlaubt Samba aber auch Freigaben auf Benutzerebene ohne root-Recht. Der Klarheit halber sollten Sie sich bei Ihrem Datenserver auf eine der beiden Methode beschränken. Der alternative Weg führt über den Befehl „net usershare […]", den unter der Haube auch grafische Dateimanager für Freigaben verwenden. Die Erlaubnis, „net usershare" ohne root-Recht und ohne sudo zu verwenden, hat jeder Systembenutzer, der in der Gruppe sambashare aufgenommen ist. Das ist bei Bedarf mit

```
sudo usermod -aG sambashare sepp
```

schnell nachgeholt. Diese neue Gruppenzugehörigkeit gilt ab der nächsten Anmeldung dieses Benutzers. Danach kann dieser beliebige Verzeichnisse, sofern er Besitzer auf lokaler Dateiebene ist, dauerhaft im Netzwerk freigeben:

```
net usershare add Filme /media/
  Filme "" sepp:F
```

Auch eine Freigabe für andere Konten ist möglich:

```
net usershare add Filme /media/
  Filme "" sepp:F,Everyone:R
```

Hier wird das Verzeichnis „/media/Filme" als Freigabe mit dem Namen „Filme" für den User „sepp" mit Vollzugriff, für andere Konten mit Lesezugriff freigegeben. Der Befehl „net usershare", der seine Freigaben natürlich auch wieder entfernen („net usershare delete Filme") oder auflisten kann („net usershare list") ist unabhängig von den Freigaben in der „/etc/samba/smb.conf". Vielmehr werden solche Userfreigaben unter „/var/lib/samba/usershares" eingetragen. Ansonsten gelten für solche Freigaben aber dieselben Einstellungen, wie sie in der zentralen „smb.conf" hinterlegt sind. ●

Daten in der Home-Cloud

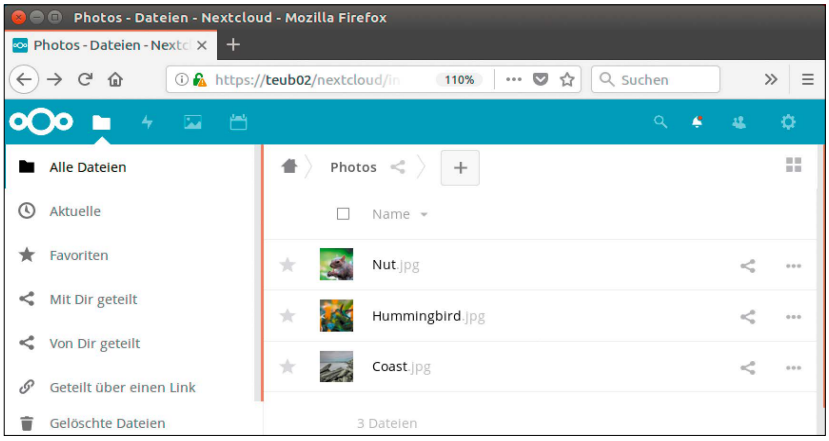
Dateien lassen sich mit vielen Methoden im eigenen Netzwerk ablegen und organisieren. Ein Nextcloud-Server bietet sich jedoch als Universallösung für Dateien, Bilder, Kalender und einiges mehr an.

Von **Thorsten Eggeling**

Der Begriff „Cloud“ bezeichnet einen Datenspeicher im Netzwerk. In der Regel sind damit Server im Internet gemeint. Beim Zugriff auf eine private Home-Cloud über das Internet (*www.pcwelt.de/1904327*) ergeben sich Einschränkungen, denn bei DSL liegt die Upload-Bandbreite oft nur bei einem bis zwei MBit/s. Für eine kleine Fotosammlung, Dokumente oder MP3-Streams ist das aber ausreichend. Wer mehr benötigt, richtet die Software für den Cloudserver auf einem gemieteten Server im Rechenzentrum ein. Die Vorteile gegenüber kommerziellen Angeboten wie Onedrive oder Google Drive liegen auf der Hand: Sie behalten die vollständige Kontrolle über Ihre Daten und können den Server individuell einrichten.

Owncloud oder Nextcloud?

Die erste Version von Owncloud erschien im Jahr 2010 (*https://owncloud.org*). Inzwischen bietet die Software fast alles, was für den Datenaustausch erforderlich ist – Kalender, Adressbuch, Fotogalerie, Wiedergabe von Musik und Videos und gemeinsames Arbeiten an Dokumenten. Plug-ins erweitern die Funktionen. Der Zugriff erfolgt über eine Weboberfläche oder eine Clientsoftware für Windows, Mac-OS, Linux, Android oder iOS. Nextcloud (*https://nextcloud.com*) ist eine Abspaltung von Owncloud, die erstmals 2016 erschien und inzwischen einige Funktionen mehr bietet als Owncloud. Wir besprechen in diesem Artikel daher die Installation von Nextcloud.



Cloudserver: Nextcloud bietet eine übersichtliche Weboberfläche, über die sich Dateien hochladen und teilen lassen. Für Fotos gibt es eine Galerieansicht.

Nextcloud als Snap-Paket installieren

Am komfortabelsten ist die Installation über ein Snap-Paket. Dabei wird automatisch alles eingerichtet, was die Nextcloud benötigt. Wenn der Apache-Webserver bereits auf dem PC installiert ist, müssen Sie diesen vorher deinstallieren oder den Standardport in der Datei „/etc/apache2/ports.conf“ sowie in allen Konfigurationsdateien unter „/etc/apache2/conf-available“ und „/etc/apache2/sites-available“ ändern. Sie können Apache auch vorübergehend mittels

```
sudo service apache2 stop
```

anhalten, bevor Sie Nextcloud über Snap installieren, und dann bei der Apache-Snap-Instanz den Port ändern.Soll ein herkömmlich installierter Apache-Webserver mehrere Webanwendungen auf Port 80 bereitstellen, installieren Sie Nextcloud besser manuell (siehe nächsten Punkt und den Kasten „Alternative Installationsmethoden“). Ab Ubuntu 16.04 ist Snapd bereits enthalten, Nutzer von Ubuntu 14.04 müssen die Software zuerst installieren (*sudo apt install snapd*). Das Nextcloud-Paket installiert dann dieser Befehl:

```
sudo snap install nextcloud
```

Wenn Apache/Nextcloud einen anderen Port verwenden soll, verwenden Sie dieses Kommando:

```
sudo snap set nextcloud ports.ht
  tp=81
```

„81“ ersetzen Sie durch den gewünschten Port. Der HTTPS-Port lässt sich bei Bedarf beispielsweise vom Standardport 443 auf 444 ändern:

```
sudo snap set nextcloud ports.htt
  ps=444
```

SSL müssen Sie für Nextcloud aber erst aktivieren. Für ein selbst signiertes Zertifikat verwenden Sie diesen Befehl:

```
sudo nextcloud.enable-https self-
  signed
```

Sollte Linux diesen Befehl nicht finden, verwenden Sie den vollständigen Pfad „/snap/bin/nextcloud.enable-https“. Im Browser müssen Sie für dieses Zertifikat eine Ausnahmeregel festlegen (Firefox: „Ich kenne das Risiko -> Aus-

nahme hinzufügen... -> Sicherheits-Ausnahmeregel bestätigen“).

Rufen Sie im Webbrowser die URL „http://[Server]“ auf oder „http://[Server]:[Port]“, wenn Sie den Port geändert haben. Ersetzen Sie den Platzhalter durch den tatsächlichen Namen Ihres Linux-Servers. Tippen Sie Benutzernamen und Passwort für ein neues Administratorkonto ein und klicken Sie auf „Installation abschließen“.

Nextcloud manuell installieren

Ubuntu-Nutzer installieren alle Nextcloud-Abhängigkeiten mit den folgenden Kommandos:

```
sudo apt update
sudo apt upgrade
sudo apt install lamp-server^ php-
 zip php-mbstring php-dom php-gd
 php-curl
```

Beachten Sie das Zeichen „^“ hinter „lamp-server“. Wenn Sie auf einem Raspberry Pi Raspbian („Jessie“) oder OSMC installiert haben, verwenden Sie diese Befehle:

```
sudo apt update
sudo apt full-upgrade
sudo apt install apache2 php5 li
 bapache2-mod-php5 php5-gd php5-
 json php5-mysql php5-curl php5-
 intl php5-mcrypt php5-imagick
 mariadb-server
```

Bei der Paketinstallation von My SQL oder Maria DB werden Sie nach einem Passwort für den root-Benutzer der Datenbank gefragt. Tippen Sie ein Passwort ein. Sie benötigen es später für bei der Nextcloud-Installation.

Alternativ ist auf dem Raspberry Pi Sqlite statt Maria DB empfehlenswert. Diese Datenbank eignet sich nicht für viele gleichzeitige Nutzer, spart aber knappe Systemressourcen. Dafür ersetzen Sie in der obigen Zeile „php5-mysql mariadb-server“ durch

```
php5-sqlite sqlite
```

Wer das aktuelle Raspbian („Stretch“) installiert hat, verwendet diese apt-Zeile:

```
sudo apt install apache2 php7.0
 php7.0-gd php7.0-curl php7.0-
 common php7.0-intl php-pear
 php7.0-apcu php7.0-xml libapa
 che2-mod-php7.0 php7.0-mbstring
 php7.0-zip curl libcurl3 lib
 curl3-dev php7.0-mysql mariadb-
 server
```

Soll Sqlite zum Einsatz kommen, ersetzen Sie die letzten beiden Pakete:

```
php7.0-sqlite sqlite
```

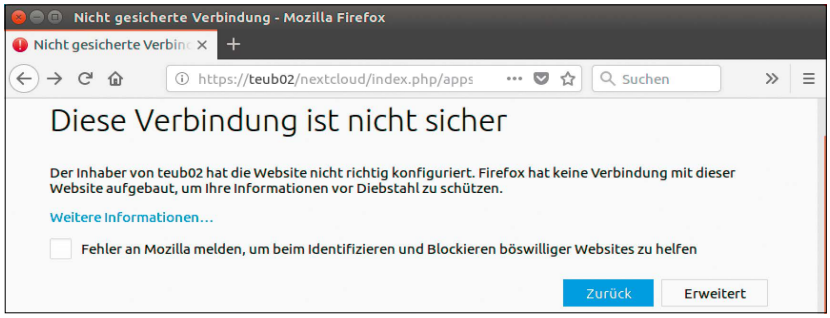
Starten Sie zum Abschluss Apache neu:

```
sudo service apache2 restart
```

Nextcloud einrichten: Rufen Sie im Browser *https://nextcloud.com/install* auf und klicken Sie unter „Get Nextcloud Server“ auf „Download“. Gehen Sie im unteren Bereich des Fensters auf „Web Installer“ und laden Sie die Datei „setup-nextcloud.php“ herunter (rechter Mausklick auf „here“ und „Ziel speichern unter...“). Im Terminal legen Sie dann ein Verzeichnis für Nextcloud an, kopieren die PHP-Datei hinein und ändern die Zugriffsrechte:

```
sudo mkdir /var/www/html/nextcloud
sudo cp ~/Downloads/setup-next
 cloud.php /var/www/html/next
 cloud
sudo chown -R www-data:www-data /
 var/www/html/nextcloud
```

Passen Sie die Pfade entsprechend der Konfiguration Ihres PCs an. Rufen Sie im Browser die URL „http://[MeinServer]/nextcloud/setup-nextcloud.php“ auf. Der Setupassistent prüft die Voraussetzungen und zeigt an, wenn ein PHP-Modul fehlen sollte. Andernfalls erscheint „All Nextcloud dependencies found“ und Sie geben darunter einen Punkt ein, damit die Installation im aktuellen Verzeichnis „/var/www/html/nextcloud“ erfolgt. Klicken Sie auf „Next“. Das Setuptool lädt die Nextcloud-Datei herunter. Klicken Sie nach der Meldung „Success“ auf „Next“ und geben Sie Benutzername und Passwort für das neue Administratorkonto



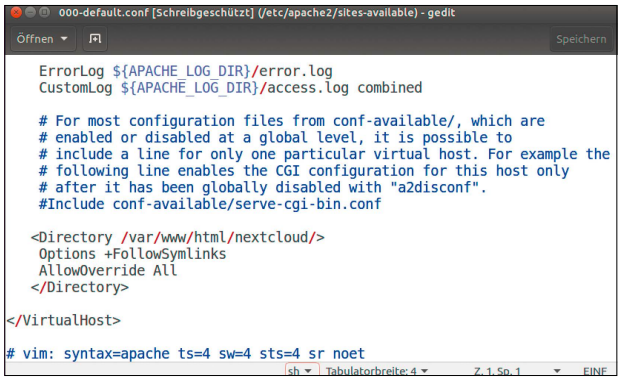
HTTPS-Verbindung: Bei selbst signierten SSL-Zertifikaten blockiert Firefox den Zugriff. Sie können für eigene Websites jedoch bedenkenlos eine Ausnahmeregel festlegen.

Nextcloud: Alternative Installation

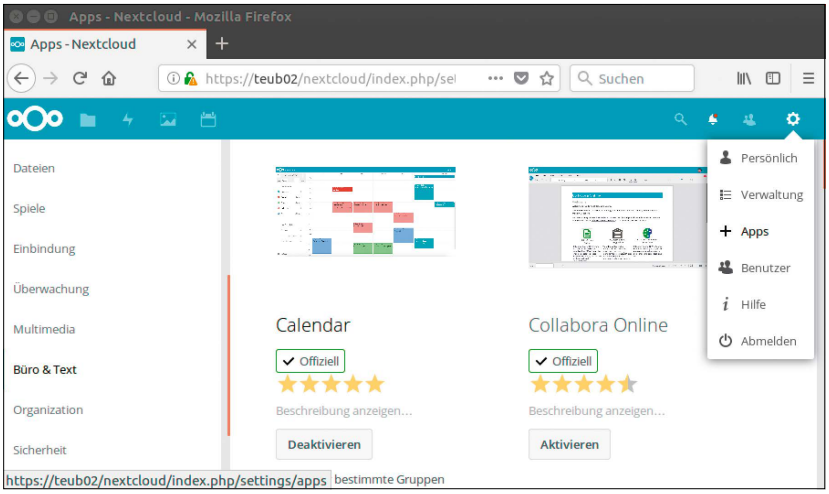
Wer Nextcloud ohne Aufwand installieren möchte, lädt sich eine virtuelle Appliance herunter. Die gibt es kostenlos als OVA-Datei auf Ubuntu-Basis unter *https://github.com/nextcloud/vm/releases/* zum Import in Virtualbox (*www.virtualbox.org*) oder Vmware Player (*www.pcwelt.de/a6uMDP*).

Der Benutzername lautet „ncadmin“, das Passwort „nextcloud“. Der Anbieter hat unter *www.techandme.se/nextcloud-vm* weitere kostenpflichtige Nextcloud-Appliances mit unterschiedlichen Konfigurationen im Angebot (ab 16 US-Dollar). Für den Raspberry Pi gibt es unter *https://www.techandme.se/nextberry-rpi* Systemabbilder auf der Basis von Raspbian mit vorinstalliertem Nextcloud. Empfehlenswert ist außerdem das Nextcloud-Community-Projekt Nextcloud Pi (*https://goo.gl/MYGUX7*).

Die Imagedateien schreiben Sie mit den üblichen Mitteln auf eine SD-Karte – mit Etcher (*https://etcher.io*) unter allen Betriebssystemen, mit dd unter Linux und Mac-OS oder auch mit dem Win 32 Disk Imager unter Windows (auf Heft-DVD). Ausführliche Informationen zu Nextcloud Pi finden Sie in englischer Sprache über *www.pcwelt.de/najN72*.



Apache-Konfiguration: Damit der Webserver die Konfiguration aus der Datei „.htaccess“ berücksichtigt, bauen Sie den abgebildeten „<Directory>“-Block ein.



Nextcloud erweitern: Nach einem Klick auf den Menüpunkt „+ Apps“ aktivieren Sie zusätzliche Plug-ins, beispielsweise einen Online-Terminkalender.

ein. Darunter fragt Nextcloud die Verbindungsinformation für die Datenbank ab. Für My SQL oder Maria DB geben Sie den Benutzernamen („root“) und das Passwort ein, das Sie bei der Paketinstallation festgelegt haben. Der Datenbankname ist frei wählbar, beispielsweise „nextcloud“. Im letzten Feld bleibt „localhost“ stehen, da die Datenbank auf demselben Server wie Nextcloud installiert ist. Wenn Sie Sqlite statt Maria DB installiert haben, müssen Sie keine Informationen eingeben. Sind beide Datenbanksysteme verfügbar, wählen Sie das gewünschte unter „Speicher & Datenbank“ aus. Klicken Sie auf „Installation abschließen“. Danach erscheint automatisch die Nextcloud-Oberfläche.

Klicken Sie rechts oben auf das Zahnradsymbol und im Menü auf „Verwaltung“. Unter „Grundeinstellungen -> Sicherheits- & Einrichtungswarnungen“ erhalten Sie wahrscheinlich die Meldung „Die .htaccess-Datei funktioniert nicht.“ In diesem Fall bearbeiten Sie die Serverkonfiguration:

```
sudo gedit /etc/apache2/sites-
  available/000-default.conf
```

Bauen Sie vor „</VirtualHost>“ die folgenden vier Zeilen ein:

```
<Directory /var/www/html/next
  cloud/>
Options +FollowSymlinks
AllowOverride All
</Directory>
```

Speichern und schließen Sie die Datei und starten Sie den Webserver neu:

```
sudo service apache2 restart
```

HTTPS aktivieren: Wenn Sie Nextcloud über das Internet zugänglich machen, sollten Sie die SSL-Verschlüsselung aktivieren. Führen Sie dazu folgende Befehle aus:

```
sudo a2enmod ssl
sudo openssl genrsa -out /etc/ssl/
  private/apache.key 4096
sudo openssl req -new -x509 -key /
  etc/ssl/private/apache.key -days
  365 -sha256 -out /etc/ssl/certs/
  apache.crt
```

Nach der zweiten Zeile werden einige Informationen zum Zertifikat abgefragt, die jedoch keine Rolle spielen. Sie können hier eintragen, was Sie wollen. Bei der Angabe „Common Name“ tragen Sie den Namen Ihres Servers ein.

Öffnen Sie die SSL-Beispielkonfiguration in einem Editor:

```
sudo gedit /etc/apache2/sites-
  available/default-ssl.conf
```

Passen Sie die Pfade für die zuvor erzeugten Dateien an:

```
SSLCertificateFile /etc/ssl/certs/
  apache.crt
SSLCertificateKeyFile /etc/ssl/
  private/apache.key
```

Speichern Sie die Datei und schließen Sie den Editor. Aktivieren Sie die SSL-Konfiguration und lassen Sie den Webserver die geänderte Konfiguration neu einlesen (zwei Zeilen):

```
sudo a2ensite default-ssl
sudo service apache2 restart
```

Der Webserver ist danach weiterhin über „http://[Server]/nextcloud“ erreichbar, für die SSL-verschlüsselte Website ersetzen Sie „http“ durch „https“. Browser stufen die Verbindung wegen des selbst signierten Zertifikats als „nicht sicher“ ein.

In Firefox klicken Sie auf „Erweitert“, dann auf „Ausnahme hinzufügen...“ und auf „Sicherheits-Ausnahmeregel bestätigen“, damit die Website angezeigt wird.

Erste Schritte in Nextcloud

Als erste Aktion sollten Sie weitere Nextcloud-Benutzer anlegen. Klicken Sie in der rechten oberen Ecke auf das Zahnradsymbol und gehen Sie im Menü auf „Benutzer“. Tippen Sie den Benutzernamen sowie ein Passwort ein und klicken Sie auf „Erstellen“. Fügen Sie dann über „+Apps“ Plug-ins hinzu, beispielsweise Calendar, Contacts und Notes. Die Erweiterungen für Bilder (Gallery) und Dateien (File sharing) sind standardmäßig installiert. ●

Zentrale Infos, Texte und Notizen

Eine Heimnetzzentrale für Notizen, Adressen, technische Infos und oft benötigte Dateien ist eine hervorragende Einrichtung. Im Optimalfall sollte dieser Serverdienst einfach zugänglich und hardwaretechnisch anspruchslos sein.

Von **Hermann Apfelböck**

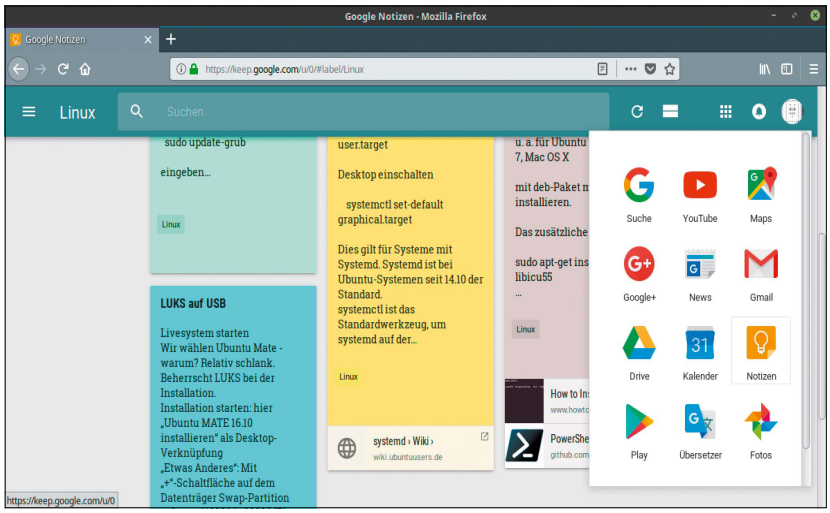
Es sind Kriterien der Textmengen, der Datenschutz-Sensibilität und der Anzahl der Clientgeräte, die darüber entscheiden, ob man für seine Infos einen Netzwerkdienst braucht. Wer immer ausschließlich an einem PC arbeitet, kann seine Notizen dort auch lokal ablegen. Für unsensible Einkaufsnotizen genügen sicher auch die „Google Notizen". Wenn aber Adressen, Kennwörter, technische Infos, Scripts, Webrecherchen von mehreren Personen auf mehreren Geräten zentral, bequem und sicher zugänglich sein sollen, ist das ein Fall für eine Infozentrale.

Dies steht im Zentrum dieses Artikels, der aber zunächst auch andere populäre Lösungen streift.

Lokale Notizen und Cloudnotizen

Komfortable Notizenprogramme gibt es in Menge für jedes System. Wenn es unter Linux eine rein lokale Rechnerlösung sein darf, ist Tomboy (Paketname „tomboy") erste Wahl: Das Tool organisiert Einzelnotizen in Notizbüchern, bietet reichhaltige Textformatierungen und eine schnelle Suchfunktion. So wirklich zeitgemäß sind aber lokale Lösungen wie Tomboy oder „Klebezettel" nicht mehr.

Die populärsten Notizsammler sind plattformübergreifend und nutzen einen externen Cloudspeicher – so etwa Evernote (*https://evernote.com*), Google Keep (*https://keep.google.com/*) oder Microsofts One Note (*https://onedrive.live.com*). Diese Text- und Infosammler sind ausgereift und elegant (die „Google-Notizen" eher simpel), haben aber zwei Nachteile: Alle Infos lagern auf amerikanischen Servern. Außerdem sind sie in erster Linie auf die persönliche Infoablage einer Person mit einem Zugangskonto ausgerichtet, nicht primär für Personengruppen.

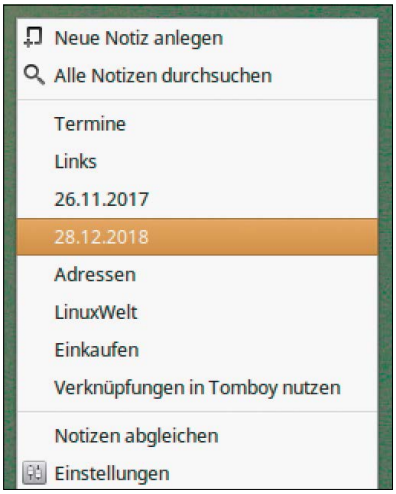


Google Notizen („Google Keep"): Solche Cloudlösungen sind für viele Nutzer technisch ausreichend. Für persönliche oder sensible Daten sind solche Angebote aber ungeeignet.

Wer es komplexer haben will, landet schnell bei Kollaborationssoftware wie Google Docs, Nextcloud oder Feng Office. Diese Lösungen ermöglichen natürlich auch einfache Infosammlungen, schießen aber mit zahlreichen weiteren Funktionen und einem zum Teil beträchtlichen Einrichtungsaufwand (Nextcloud, Feng Office) weit übers Ziel hinaus.

Empfehlenswerte Wiki-Lösungen

Wikis sind eine ideale Plattform, um umfangreiche Textsammlungen zu sammeln und zu organisieren. Selbst bei der Einschränkung auf kostenlose Angebote ist die Anzahl solcher Wiki-Lösungen mittlerweile unübersichtlich, wie die Wikipedia-Seite *https://de.wikipedia.org/wiki/Liste_von_Wiki-Software* zeigt. Die populärsten Lösungen basieren auf PHP und das gilt auch für die beiden hier empfohlenen Kandidaten Mediawiki (*www.mediawiki.org*) und Dokuwiki (*www.dokuwiki.org*). Beide bieten weit mehr als nur Textsammlungen, wobei die meisten Audio-, Video- und Bildfunktionen durch zahlreiche externe Plug-ins gelöst werden. Das Mediawiki ist die angestammte Basis der Wikipedia und



Lokale Notizen mit Tomboy: Technisch ist das nicht mehr zeitgemäß, aber wo dies genügt, ist Tomboy eine ausgereifte Lösung.



Seiten anlegen: Wenn Sie als Dokuwiki-Adresse eine nicht existierende ID eingeben, erscheint diese Meldung und mit „Seite anlegen“ entsteht eine neue Seite (und Datei).

kann daher exzellente Pflege und Zukunftssicherheit garantieren. Das Dokuwiki steht dem aber kaum nach und hat wesentliche Vorteile für Heimanwender, da es auf mehreren Ebenen einfacher ist als das Mediawiki:

- Das Dokuwiki benötigt keine Datenbank und speichert alles in einfachen Textdateien.
- Die Trennung der Daten von der Software und ist rigoros, sodass die Sicherung oder Synchronisierung des kompletten Datenbestands des Unterverzeichnisses „data“ (typischerweise „/var/www/dokuwiki/data/“) sehr einfach wird.
- Die Struktur in gliedernde Namensräume (auf Dateiebene Verzeichnisse) und Seiten (auf Dateiebene TXT-Dateien) ist simpel.
- Auszeichnungssprache und Editor sind relativ einfach. Wysiwyg bietet der Standardeditor nicht, kann aber über einen Plug-in-Editor nachgerüstet werden.
- Für Nutzer, die auch Windows verwenden, gibt es ein absolut einfaches Gesamtpaket mit integriertem Apache.

Vorbereitungen für das Dokuwiki

Ideales Gerät für ein Wiki ist ein ständig laufender Server von der Sorte Raspberry & Co. Im Falle des Dokuwiki können Raspberry & Co. diese zusätzliche Aufgabe mühelos neben sonstigen Serverdiensten übernehmen, denn das Dokuwiki stellt geringe Ansprüche an die Hardware. Voraussetzung ist jedoch ein laufender Apache-Server mit PHP. Sofern dieser noch nicht vorliegt, installieren Sie diesen unter Raspbian, Debian oder Ubuntu mit diesem Kommando:

```
sudo apt install apache2 php5 li
 bapache2-mod-php5 php5-curl
```

Das lediglich gut drei MB große Installationspaket von Dokuwiki holen Sie mit wget ab.

```
wget http://download.dokuwiki.org/
 src/dokuwiki/dokuwiki-stable.tgz
```

Unter den Debian/Raspbian-Distributionen liegt das Standardverzeichnis für Apache-Webdienste unter „/var/www/“, bei Ubuntu unter „/var/www/html“. Entpacken Sie mit

```
sudo tar xzvf dokuwiki-stable.tgz
 -C /var/www/[html/]
```

das Archiv an die richtige Stelle. Das dort entstandene Verzeichnis mit Versionsangabe im Namen benennen Sie mittels des Befehls

```
sudo mv /var/www/[html/]dokuwiki*
 /var/www/[html/]dokuwiki
```

nach „dokuwiki“ um und setzen die Zugriffsrechte für Apache:

```
sudo chown -R www-data:www-data /
 var/www/[html/]dokuwiki
```

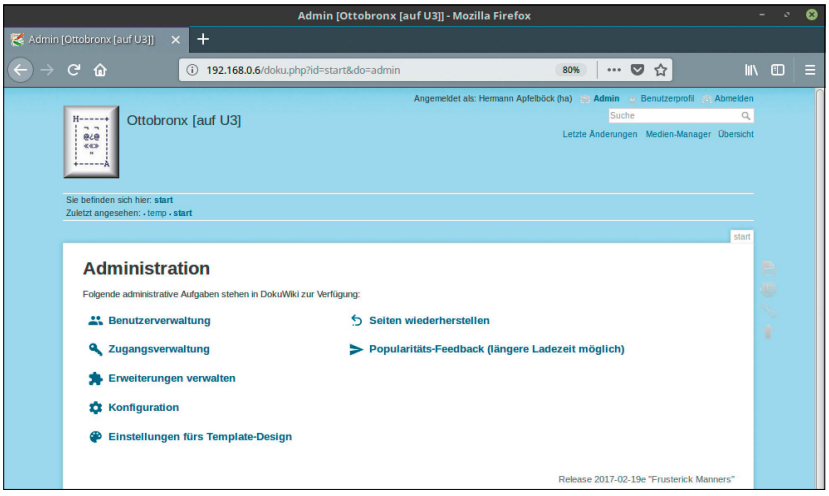
Ab sofort ist das Wiki betriebsbereit und die weitere Einrichtung erfolgt im Browser mit der Adresse „http://[IP-Adresse]/dokuwiki/install.php?l=de“, wobei als „[IP-Adresse]“ diejenige des Serverrechners einzugeben ist. Beim Start des Install-Scripts mit Firefox kommt es vor, dass der Browser den Script-Inhalt anzeigt, anstatt das Script zu starten: Verwenden Sie in diesem Fall einfach einen beliebigen anderen Browser.

Die Grundkonfiguration erfordert nur wenige Schritte: Notwendig sind das Einrichten eines Administratorkontos und die Vergabe eines Wiki-Namens. Weitere Einstellungen wie das Festlegen der Startseite oder der Sprache finden Sie jederzeit auch später unter „Admin -> Konfiguration“.

Dokuwiki: Seiten anlegen und organisieren

Eine neue Wiki-Seite entsteht dadurch, dass Sie in der Browseradresse hinter „[IP]/dokuwiki/doku.php?id=“ einen bisher nicht benutzten Seitennamen eintragen und dann auf „Seite anlegen“ klicken. Der Editor erlaubt Auszeichnungen wie fett oder kursiv, Überschriftenebenen und das Einfügen von Bildern und Dateien. Für das Einfügen von internen Links innerhalb des Wikis und externen URLs gibt es Schaltflächen, welche die Eingabe deutlich vereinfachen. Der Editor entspricht weitgehend demjenigen anderer Wikis oder Blogeditoren wie Wordpress. Einige Eigenheiten sollte man aber kennen:

Beachten Sie, dass ein Return im Editor keinen Zeilenumbruch auf der Ergebnisseite bewirkt. Sie müssen im Editor mit zwei Returns eine sichtbare



Der Dokuwiki-Link „Admin" führt zur Konfiguration: Beschränken Sie sich am besten auf die Basiseinstellungen unter „Konfiguration" und Farbeinstellungen für das Design.



Versionsverwaltung: Dokuwiki speichert Bearbeitungszustände und kann auf ältere Seitenversionen zurückkehren.

Leerzeile erzeugen oder das Zeilenende durch Doppelbackslash (\\) erzwingen. Bei Listen aller Art (Telefonliste, Adressen, Scripts) wäre es nicht zumutbar, die notwendigen Zeilenumbrüche manuell einzutragen. Formatieren Sie in solchen Fällen den gesamten Text mit dem Button „Listenpunkt".

Ohne weitere Gliederung landen alle Seiten auf oberster Ebene, was selbst bei kleinen Sammlungen schnell unübersichtlich wird. Um hierarchische Ebenen zu organisieren, gibt es „Namensräume" (Namespaces). Um einen Namensraum anzulegen, verwenden Sie den Befehl

```
[IP-Adresse]/dokuwiki/doku.
 php?id=[Namensraum:][Seitenname]
```

oder als konkretes Beispiel „[IP-Adresse]/dokuwiki/dokuphp?id=Anna:Adressen". Die neue Wiki-Seite „Adressen" wird dann unter der neuen Ebene „Anna" eingerichtet.

Da Namensräume auf Dateiebene durch Verzeichnisse, Wiki-Seiten durch TXT-Dateien repräsentiert werden, ist es für den Basisaufbau oder bei Umbauten des Wikis oft einfacher, die Grundstruktur unter „/var/www/[html/]dokuwiki/data/pages" auf Dateiebene zu unternehmen. Die Wiki-Ansicht im Browser folgt solchen Änderungen sofort oder spätestens nach dem Seitenrefresh mit Taste F5.

Für das Löschen oder Umbenennen von Seiten gibt es keine Option. Zum Löschen öffnen Sie die Wikiseite und gehen auf „Diese Seite bearbeiten". Nach Löschen des kompletten Inhalts und „Speichern" ist die Seite entfernt. Namensräume verschwinden automatisch, wenn alle Seiten unterhalb des Namensraums gelöscht werden. Zum Umbenennen von Seiten kopieren Sie den kompletten Inhalt in eine neue Seite mit dem gewünschten Namen und löschen dann die ursprüngliche Seite auf die beschriebene Weise.

Dokuwiki: Anpassung und Erweiterungen

Über „Admin -> Konfiguration" erreichen Sie die zahlreichen Basiseinstellungen. Ganz oben unter „Basis" definieren Sie die Designvorlage. Das ist beim Dokuwiki nicht nur eine optische Entscheidung, sondern bestimmt auch, ob und wo die Wiki-Übersicht, die Editieraktionen und die Konfiguration erreichbar sind. Beachten Sie, dass jedes Design im allerletzten Punkt „Template" der Konfiguration noch diverse Detailanpassungen vorsieht: Das betrifft nicht nur die Farben, sondern auch die gewünschte Position der Elemente.

Über „Admin -> Erweiterungen verwalten -> Suchen und Installieren" ist das Dokuwiki erweiterbar. Es gibt zahlreiche funktionale Erweiterungen und Templates. Wer in den Plug-ins stöbern will, sollte zunächst die Seite *www.dokuwiki.org/extensions* aufsuchen und danach die gewünschte Erweiterung über „Suchen und Installieren" in der Konfigurationsoberfläche einrichten. Ein auf diese Weise heruntergeladenes Template können Sie dann unter „Admin -> Konfiguration -> Designvorlage" auswählen und dann ganz unten auf „Speichern" gehen. In der Regel benötigt der Browser mit Taste F5 einen Seitenrefresh, um das neue Theme anzuzeigen.

Dokuwiki: Portabel für Windows

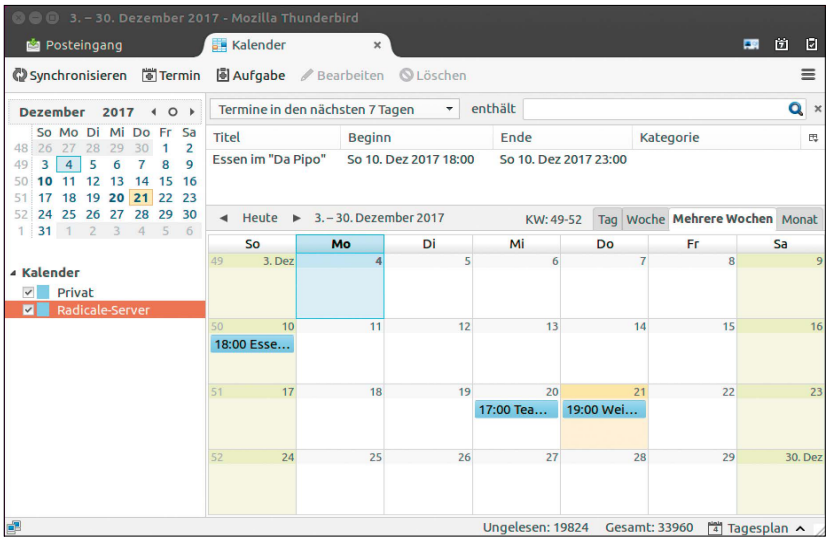
Sowohl das Dokuwiki als auch das Mediawiki gibt es auch als portables Windows-Paket, jedoch ist hier das Dokuwiki erneut ungleich einfacher einzurichten. Diese Option ist nützlich für ein gemischtes Heimnetz, um auf einfachste Weise ein vollständiges Windows-Backup vorzuhalten. Den Download finden Sie unter *https://download.dokuwiki.org/* und hier ganz nach unten als „MicroApache". Dieses Paket enthält das Dokuwiki komplett mit einem minimalen Apache-Webserver – einfach entpacken und im entstandenen Ordner die Batchdatei „run.cmd" aufrufen.

Das Wiki lädt automatisch im Standardbrowser am lokalen Rechner, andere Rechner erreichen es über die Adresse „http://[IP-Adresse]:8800/doku.php". ●

Server für Termine und Adressen

Ein Kalenderserver im eigenen Netzwerk hilft bei der Verwaltung Ihrer Termine. Er ist schnell eingerichtet und lässt sich auch von mehreren Personen verwenden.

Von **Thorsten Eggeling**



Termine im Netz. Das Thunderbird-Add-on Lightning bietet einen lokalen Terminkalender, kann die Daten aber auch mit einem Kalenderserver abgleichen.

Kostenlose Online-Terminkalender gibt es mehrere, etwa von Google oder Microsoft. Wer sich nicht an diese Anbieter binden und persönliche Daten lieber auf dem heimischen Rechner speichern möchte, installiert sich einen eigenen Kalenderserver. In diesem Artikel beschreiben wir unkomplizierte Lösungen, die sich relativ schnell einrichten lassen. Wer mehr Funktionen benötigt, etwa zusätzlich den Austausch von Dateien, den gemeinsamen Zugriff auf Dokumente und mehrere Benutzerkonten, sollte sich beispielsweise Nextcloud ansehen (*www.nextcloud.com*).

Die Anleitungen in diesem Artikel gelten für Ubuntu 16.04 und verwandte Systeme wie Linux Mint 18. Die Installation der genannten Software funktioniert auch auf einem Raspberry Pi unter Raspbian beziehungsweise OSMC. Wie Sie auf den Heimserver über das Internet zugreifen, lesen Sie unter *www.pcwelt.de/1904327*.

Serversoftware für Caldav und Carddav

Welche Serversoftware für Sie infrage kommt, hängt davon ab, ob Sie Termine oder Adressbücher nur für einen Nutzer oder für ein Team bereitstellen wollen. Sind mehrere Personen beteiligt, besteht wahrscheinlich der Wunsch, die Zugriffsrechte festzulegen. Mit steigenden Ansprüchen an Funktion und Bedienbarkeit erhöht sich auch der Installations- und Wartungsaufwand.

Bei **Radicale** (*http://radicale.org*), das wir im nächsten Punkt ausführlicher vorstellen, ist der Aufwand relativ gering, der Funktionsumfang ist für private Anwender und kleine Teams ausreichend. Webserver und Datenbank sind nicht erforderlich, die Konfiguration ist daher schnell erfolgt. Wer möchte, kann aber auch Radicale zum Mehrbenutzersystem ausbauen. Anleitungen dazu gibt es auf der Website des Anbieters.

Baikal (*http://baikal-server.com*) geht einen Schritt weiter. Die Software ist in PHP programmiert und bietet eine Weboberfläche, über die sich Benutzerkonten anlegen und verwalten lassen. Das setzt jedoch die Installation eines Apache-Webservers und einer Datenbank wie My SQL oder Sqlite voraus (siehe etwa *www.pcwelt.de/1472577*).

Wenn es auf eine detaillierte Rechtevergabe für größeren Teams ankommt, ist Davical die richtige Wahl (*www.davical.org*). Auch hier kommt PHP zum Einsatz. Sie benötigen den Apache-Webserver und die Datenbank Postgre SQL. Die Verwaltung von Davical erfolgt über eine Weboberfläche. Hier lassen sich Benutzer und Gruppen in „Benutzerfunktionen -> Prinzipalen anlegen“ erstellen und Rechte zuweisen. Eine Installations- und Bedienungsanleitung finden Sie auf der Website des Anbieters.

Radicale: Einfacher und schlanker Server

Radicale (*http://radicale.org*) ist ein Server für Caldav (Kalender) und Carddav (Kontakte). Die Software ist in Python programmiert und benötigt weder Webserver noch Datenbank. In

der Grundkonfiguration gibt es keine Benutzerkonten und keine Anmeldung. Radicale eignet sich daher für Einzelanwender oder Teams mit wenigen Personen, wo Zugriffsbeschränkungen keine Rolle spielen. Die Software ist im Terminalfenster mit

```
sudo apt install radicale
```

schnell installiert. Öffnen Sie die Konfigurationsdatei mit

```
sudo nano /etc/default/radicale
```

Entfernen Sie das Kommentarzeichen „#“ vor der Zeile „ENABLE_RADICALE=yes“. Speichern Sie die Datei mit Strg-O, bestätigen Sie mit der Enter-Taste und schließen Sie den Editor mit Strg-X. Starten Sie den Serverdienst über die Befehlszeile

```
sudo service radicale start
```

Bei einem Linux-Neustart wird der Radicale-Server automatisch aktiviert.

Testen Sie die Installation, indem Sie im Webbrowser die Adresse „http://localhost:5232“ aufrufen. Auf einem anderen PC ersetzen Sie „localhost“ durch den Namen Ihres Linux-Servers oder dessen IP-Adresse. Es erscheint dann die Meldung „Radicale works!“.

Clientsoftware für Radicale konfigurieren

Wenn Sie beispielsweise das Add-on Lightning in Thunderbird installiert haben, gehen Sie im Menü auf „Datei -> Neu -> Kalender“. Wählen Sie die Option „Im Netzwerk“ und klicken Sie auf „Weiter“. Klicken Sie darauf die Option „CalDAV“ an und tippen Sie unter „Adresse“ die URL für den Radicale-Server ein:

```
http://[IP]:5232/[User]/kalender.ics/
```

Den Platzhalter „[IP]“ ersetzen Sie durch den Namen oder die IP-Adresse Ihres Linux-PCs und „[User]“ durch den gewünschten Benutzernamen. Dieser ist frei wählbar. Auch der Dateiname „kalender.ics“ kann beliebig lauten. Wichtig: Am Ende der Adresse muss das Zeichen „/“ stehen – sonst funktioniert der Zugriff nicht. Klicken Sie dann auf „Weiter“ und tippen Sie hinter „Name:“ eine aussagekräftige Bezeichnung für den neuen Kalender ein. Klicken Sie auf „Weiter“ und auf „Fertig stellen“.



Netzwerkadressbuch: Onlineadressbücher binden Sie in Thunderbird über das Add-on Cardbook ein. Sie müssen hier nur die URL zum Radicale-Adressbuch konfigurieren.

Gehen Sie auf „Termine und Aufgaben -> Kalender“, um einen Tab mit der Kalenderansicht zu öffnen. Per Doppelklick auf einen Tag oder eine Uhrzeit sowie über das Menü „Termine und Aufgaben -> Neuer Termin“ erstellen Sie einen neuen Kalendereintrag. Achten Sie dabei darauf, dass hinter „Kalender:“ der Onlinekalender eingestellt ist. Ein Onlineadressbuch lässt sich in Thunderbird über das Add-on Cardbook nutzen. Erstellen Sie das Adressbuch, indem Sie im Browser die Adresse

```
http://[IP]:5232/[User]/adressen.vcf/
```

aufrufen. „[User]“ ist ein beliebiger Benutzername, den Dateinamen können Sie ebenfalls frei wählen. Beachten Sie wieder den Slash „/“ am Ende der Zeile. Gehen Sie in Thunderbird auf „Extras -> Cardbook“. Klicken Sie die Menüschaltfläche links oben in der Symbolleiste an und gehen Sie auf „Adressbuch -> Neues Adressbuch“. Wählen Sie „Im Netzwerk“ und klicken Sie auf „Weiter“. Aktivieren Sie die Option „CardDAV“ und tippen Sie hinter „URL“ Folgendes

```
http://[IP]:5232/[User]/adressen.vcf/
```

ein. Die Platzhalter ersetzen Sie wie oben beschrieben. Hinter „Benutzername“ und „Passwort“ tragen Sie dann beliebige Zeichen ein, klicken auf „Überprüfen“ und dann auf „Weiter“. Vergeben Sie einen Namen für das neue Adressbuch, klicken Sie auf „Weiter“ und auf „Fertigstellen“. Wichtig: Cardbook verwendet eigene Adressbücher, die nicht mit dem Standardadressbuch synchronisiert werden.

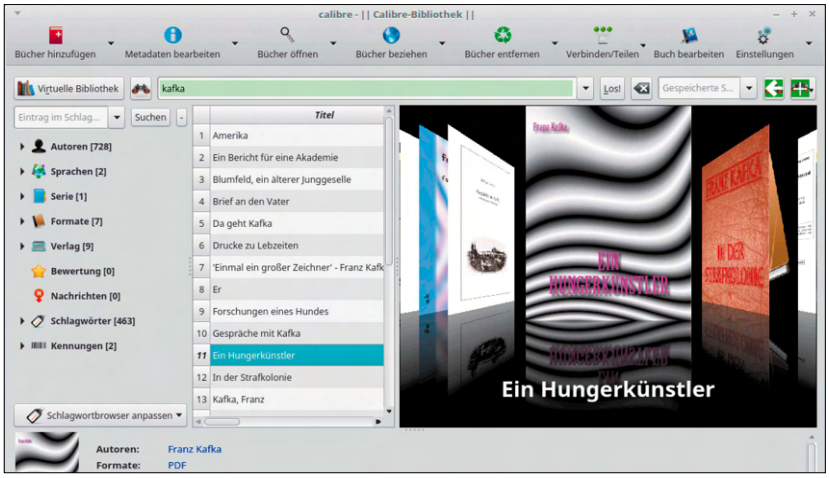
Clientsoftware für Kalender & Adressen

Die meisten Kalender- und Adressbuchanwendungen unterstützen die Standardprotokolle Caldav (Calender Distributed Authoring and Versioning) und Carddav (vCard Extensions für Webdav). Verbreitete Programme sind die Thunderbird-Add-ons Lightning und Cardbook, die sich schnell über „Extras -> Addons“ und eine Suche nach dem Programmnamen installieren lassen. Alternative Desktopanwendungen sind Evolution und Korganizer, die Sie über die Paketverwaltung Ihrer Linux-Distribution installieren. Für Android gibt es beispielsweise Caldav-Sync (*www.pcwelt.de/Ela8LZ, 2,59 Euro*) und Carddav-Sync (*www.pcwelt.de/AzBOV*, 1,90 Euro). iPhone-Nutzer können die Standardkalender- und Kontakte-App für die Verwendung von Netzwerkressourcen konfigurieren.

PDF-Server Calibre

Das Open-Source-Programm Calibre hat sich ganz auf die Verwaltung von E-Books spezialisiert. Für wirklich große Sammlungen lohnt sich Calibre als Server, der die Bibliothek über jeden Browser für alle Netzgeräte bereitstellt.

Von **Hermann Apfelböck**



Mit der Verbreitung von Tablets gewinnen E-Books – oft im PDF-, Mobi-, CHM- oder Epub-Format – immer mehr Freunde. Selbst bibliophile und konservative Leser sind leicht durch die unbestreitbaren Vorteile zu überzeugen, die E-Books auf einem handlichen Tablet bieten: Textgröße, Kontrast, Helligkeit lassen sich an jede Situation anpassen. Und auf einem Tablet passt eine ganze Bibliothek ins Handgepäck. Für eine opulente oder systematische Sammlung belletristischer und technischer Bücher ist aber die Aufbewahrung auf verstreuten Lesegeräten suboptimal: Neben der Frage „Was habe ich eigentlich wo (doppelt)?“ wird dort auch schnell der Speicher knapp. Eine ideale zentrale Lösung für das Heimnetz bietet die Software Calibre mit seiner Serverkomponente.

Calibre installieren und Bibliothek erstellen

Calibre gibt es für alle Betriebssysteme unter *https://calibre-ebook.com/download*. Diese Anlaufstelle ist auch für Linux zu empfehlen, weil eine Installation über die Paketquellen etwa unter Debian/Ubuntu/Mint mit dem Kommando

```
sudo apt install calibre
```

nur ältere Versionen anbietet. Für die lokale Nutzung auf einem Rechner spielt das keine große Rolle, aber gerade die Serverkomponente hat in den aktuellen Versionen funktional dazugelernt und kommt auch optisch wesentlich frischer daher. Verwenden Sie daher zur Installation diese Befehlskombination:

```
wget -nv -O- https://download.ca
 libre-ebook.com/linux-installer.
 py | sudo python -c "import sys;
 main=lambda:sys.stderr.
 write('Download failed\n');
 exec(sys.stdin.read()); main()"
```

Das recht komplexe Kommando kann von der oben genannten Downloadseite ohne Tippaufwand direkt ins Terminal kopiert werden. Diese Installationsmethode funktioniert auch als Update einer älteren Version, wobei eine bereits bestehende Bibliothek erhalten bleibt.

Calibre ist nach der Installation über das Desktopmenü oder mit dem Aufruf *calibre* im Terminal zu erreichen. Für den Aufbau und die Erweiterung einer Bibliothek dient die Schaltfläche „Bücher hinzufügen“. Den Massenimport von heterogenen Formaten und ganzer Verzeichnisebenen ermöglicht die Unteroption „Bücher aus verschiedenen Verzeichnissen […], jede e-Book-Datei ist ein anderes Buch“.

Damit integrieren Sie unstrukturierte Sammlungen von PDF-, HTML-, Epub- und Office-Formaten in die Calibre-Datenbank. Beachten Sie, dass Calibre alle Dateien physisch kopiert und standardmäßig im Ordner „~/Calibre-Bibliothek/“ einsammelt. Beim Import aus unstrukturierten Quellen wird die Software versuchen, aus Dateinamen und Metadaten Informationen zu beziehen, um jedes Buch sinnvoll zu katalogisieren. Fehler aufgrund unzulänglicher Metadaten sind beim Massenimport unvermeidlich, können aber später über „Metadaten bearbeiten“ manuell und mit der Hilfe von Onlinediensten („Metadaten herunterladen“) korrigiert werden.

Die Suche bestimmter Titel erfolgt im Suchfeld über dem Hauptfenster. Weitere Filtermöglichkeiten bieten Kategorien in der linken Navigationsleiste wie „Autoren“, „Formate“, „Bewertung“ oder „Schlagwörter“. Zum Lesen eines markierten Titels verwenden Sie die Schaltfläche „Bücher öffnen“.

Da es nicht primärer Gegenstand dieses Beitrags ist, die zahlreichen Filter-, Konvertierungs- und Einstellungsoptionen der komplexen Software zu

erläutern, verweisen wir an dieser Stelle auf das größtenteils deutschsprachige Onlinehandbuch unter *https://manual.calibre-ebook.com/de/*.

Calibre als Lektüreserver im Netz

Ist eine Bibliothek erst einmal eingerichtet, kann Calibre diese für das Netzwerk freigeben. Für den Start der Serverkomponente genügt der Klick auf „Verbinden/Teilen -> Inhalteserver starten“. Danach informiert Sie ein weiterer Klick auf „Verbinden/Teilen“, unter welcher Adresse der Bibliotheksserver zu erreichen ist. Eine Angabe wie „192.168.178.10, port 8080“ zeigt, dass jeder Browser im lokalen Netz mit der Adresse „192.168.178.10:8080“ zum Calibre-Server gelangt.

Wie bei jedem Server ist es auch hier von Vorteil, diese IP-Adresse statisch zu setzen (über den Router), damit Sie sich künftig jederzeit mit einem Lesezeichen verbinden können. Der Calibre-Server kann unter „Einstellungen -> Netzwerkserver“ detailliert konfiguriert werden. Falls nötig, gibt es unter „Benutzerkonten“ auch eine Benutzerverwaltung mit Zugriffskennwörtern.

Auf Client-Seite ist das wichtigste Werkzeug das Lupensymbol im Seitentitel. Im einfachsten Fall geben Sie im Suchfeld einen Autoren- oder Titelnamen ein. Die Treffer werden mit ihrem Titelbild angezeigt und ein Klick darauf bietet Detailinformationen sowie die Optionen „Lesen“ und „Herunterladen“. Für die Option „Lesen“ wechselt der Browser automatisch in den Vollbildmodus. Bei einer umfangreichen und gut gepflegten Calibre-Bibliothek können Sie unterhalb des Suchfeldes die Suchkategorie eingrenzen und etwa nur in der Kategorie „Schlagwörter“ nach einem bestimmten Begriff suchen oder unter „Bewertung“ nach einem speziellen Rating.

Calibre-Server „headless“: Die bislang beschriebenen Einrichtungs- und Servermöglichkeiten orientierten sich an der grafischen Oberfläche von Calibre. Für den grundsätzlichen Aufbau der Bibliothek und insbesondere für Nachbesserungen an den Metainformationen ist die grafische Oberfläche in der Tat dringend zu empfehlen. Calibre bietet jedoch darüber hinaus Kommandozeilenwerkzeuge, die eine vollständige Steuerung über eine SSH-Konsole ermöglichen. Somit kann der Lektüreserver auch auf einem Platinenrechner ohne Monitor und Tastatur laufen (headless). Der wichtigste Befehl (Beispiel)

```
calibre-server /home/ha/Calibre-
  Bibliothek/
```

startet die Serverkomponente und ist im Prinzip gleichbedeutend mit dem Menüpunkt „Verbinden/Teilen -> Inhalteserver starten“ an der grafischen Oberfläche. Der Befehl gibt nur den einfachsten Einsatz wieder, ist aber für das Heimnetz in der Regel völlig ausreichend. Die Hilfeseite

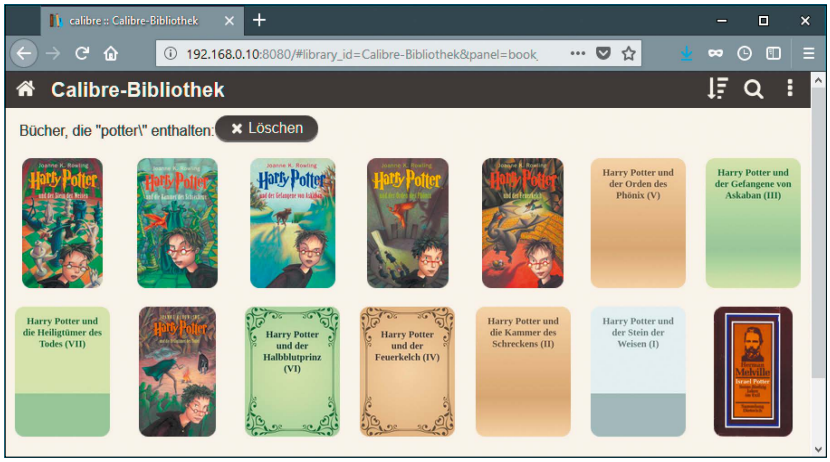
```
calibre-server --help
```

informiert darüber, dass Sie auf der Kommandozeile alles steuern können, was auch auf der grafischen Oberfläche unter „Einstellungen -> Netzwerkserver“ zu finden ist.

Für den Ausbau und die Verwaltung der Bibliothek ist das mächtige Kommandozeilenprogramm calibredb zuständig. Der wichtigste Schalter „add“ kann alles, was die Optionen unter „Bücher hinzufügen“ auf der grafischen Oberfläche anbieten. So importiert der Befehl

```
calibredb add --recurse /media/ha/
  Data/PDFs
```

alle E-Book- und Textformate, die im angegebenen Pfad liegen, in die Calibre-Bibliothek. Weitere add-Optionen zeigt die Hilfeseite *calibredb add --help* und den Gesamtumfang des Tools calibredb der Befehl *calibredb --help*. Theoretisch lässt sich damit ein Calibre-Server von Anfang an und vollständig ohne Oberfläche betreiben – wirklich komfortabel ist das allerdings nicht. Wir empfehlen daher, mindestens die Basis im grafischen Programm zu legen. Der Serverstart und gelegentliche Nachbesserungen bereiten hingegen über das SSH-Terminal im Headlessbetrieb keine Mühe. ●



Calibre-Bibliothek übers Netzwerk durchsuchen: Die Suchergebnisse werden mit Buchtitel angezeigt, nach einem Klick darauf erscheinen weitere Optionen.



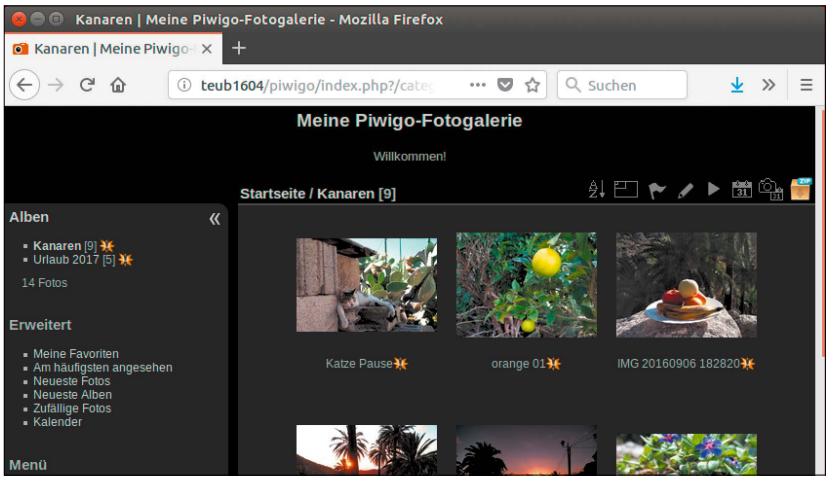
„Lesen“ oder „Herunterladen“: Nach Auswahl eines Buchtitels kann die Lektüre beginnen. Beim direkten „Lesen“ ist Voraussetzung, dass der Browser das Format versteht.

Der eigene Fotoserver

Einfache PHP-Scripts für eine Fotogalerie sind schnell installiert und genügen für heimische Präsentation oder für Webfreigaben für den Freundeskreis. Es gibt aber auch Bilderserver für größere Personengruppen.

Von **Thorsten Eggeling**

In einer Fotogalerie lassen sich Bilder perfekt organisieren und für die Präsentation vorbereiten. Dieser Artikel nennt sehr einfache bis anspruchsvollere Lösungen für die Bildverwaltung. Wer seine Bildersammlung nicht nur zu Hause zeigen, sondern online dem Freundeskreis zugänglich machen will, macht den Webserver zu Hause auch über das Internet erreichbar (*www.pcwelt.de/1904327*).



Fotos auf dem eigenen Server: Piwigo bietet fast alles, was man von einer Online-Bildergalerie erwartet. Zusatzfunktionen lassen sich über Plug-ins ergänzen.

Galerien mit und ohne Datenbank

Single File PHP Gallery ist besonders einfach gehalten (*https://sye.dk/sfpg*) und benötigt nur einen Apache-Server und PHP. Die private Nutzung ist kostenlos, von kommerziellen Anwendern erwartet der Hersteller eine Spende ab zehn Dollar. Diese Galerie besteht nur aus einer einzigen PHP-Datei (siehe nächster Punkt) und bietet eine schlichte Ordner- und Bilderübersicht. Bei Bedarf lassen sich auch Admin-Funktionen aktivieren, über die sich Dateien hochladen oder löschen lassen.

Auch **Tiny Web Gallery** (*www.tinywebgallery.com*) kommt ohne Datenbank aus. Die Software ist für Privatpersonen kostenlos. Über eine Gratisregistrierung lassen sich weitere Funktionen freischalten. Für 19 Euro erhalten Sie eine Standardlizenz für eine Domain und ab 39 Euro auch kommerziell verwendbare Lizenzen für mehrere Domains.

Tiny Web Gallery bietet eine gefällige Oberfläche und kann auch MP3s und Videos streamen (Flashplayer erforderlich). Außerdem besteht die Möglichkeit, mehrere Benutzer einzurichten und Kommentare sowie Bewertungen auf der Webseite zu hinterlassen. Auf der Webseite des Herstellers gibt es mehrere Demos, über die Sie die Funktionen ausprobieren können.

Die **Fotogalerie Piwigo** (*http://piwigo.org*) steht unter einer Open-Source-Lizenz und bietet umfangreiche Funktionen. Sie lässt sich durch Plugins erweitern, etwa für den Download von Fotoalben als ZIP-Datei. Zu den Standardfunktionen gehören eine Benutzerverwaltung, Rechtevergabe für Fotoalben, Kommentare, Schlagwörter und eine Diashow. Neben einem Webserver und PHP benötigt Piwigo auch die Datenbank My SQL oder Maria DB. Eine Anleitung zur Installation finden Sie am Ende des Artikels.

Single File PHP Gallery installieren und nutzen

Wenn noch nicht geschehen, installieren Sie den Webserver Apache und PHP in einem Terminalfenster unter Ubuntu mit folgender Zeile:

```
sudo apt install apache2 php liba
  pache2-mod-php php-gd
```

Dann starten Sie Apache

```
sudo service apache2 restart
```

und erstellen das Verzeichnis, das die Bildergalerie aufnehmen soll:

```
sudo mkdir /var/www/html/fotos
```

Laden Sie die beiden Dateien „Single_File_PHP_Gallery_4.7.0.zip“ und „sfpg_test_1.5.1.zip“ von *https://sye.dk/sfpg/* herunter und entpacken Sie die Dateien. Starten Sie den Dateimanager über das Terminalfenster mit root-Recht:

```
sudo nautilus &
```

Kopieren Sie die Dateien „index.php“ und „sfpg_test.php“ nach „/var/www/html/fotos“. Erstellen Sie ein Unterverzeichnis, das bereits einige Bilder enthält. Geben Sie dann dem Webserver die Schreibrechte in diesem Ordner:

```
chown -R www-data:www-data /var/
  www/html/fotos
```

Starten Sie dann in einem Browser im lokalen Netz folgenden Test:

```
http://[IP]/fotos/sfpg_test.php
```

Das Test-Script prüft, ob alle Voraussetzungen erfüllt sind. Wenn nicht, erhalten Sie eine Fehlermeldung mit Hinweisen zur Beseitigung des Problems. Den Platzhalter „[IP]“ ersetzen Sie durch die IP-Adresse oder den Namen Ihres Linux-Servers.

Öffnen Sie dann die Adresse *http://[IP]/fotos* im Browser. Sollte die Meldung „You have to set the SECURITY_PHRASE in the top of the script! “ erscheinen, laden Sie die Seite neu, indem Sie die Taste F5 drücken. Sie sehen dann den Bilderordner, den Sie zuvor nach „/var/www/html/fotos“ kopiert haben. Nach einem Klick darauf öffnen Sie die Bilder oder Sie starten per Klick auf „Slideshow“ eine Diashow.

Single File PHP Gallery konfigurieren: Öffnen Sie die Datei „index.php“ in einem Editor, im Terminalfenster beispielsweise mit

```
gedit /var/www/html/fotos/index.
 php &
```

Gleich zu Beginn finden Sie Variablen, die das Verhalten des Scripts steuern. Tragen Sie beispielsweise in die Zeile

```
define('PASSWORD', '');
```

ein Passwort zwischen den einfachen Anführungszeichen ein. Der Zugang zur Bildergalerie ist dann nur noch nach Passworteingabe möglich.

Wenn Sie bei „define(‚ADMIN‘, FALSE);“ den Wert „FALSE“ durch „TRUE“ ersetzen, blendet das PHP-Script die Schaltfläche „Admin“ ein. Nach einem Klick darauf sehen Sie weitere Schaltflächen, um Bilder hochzuladen, umzubenennen oder zu löschen. Auf einem öffentlich zugänglichen Server sollten Sie diese Option aus Sicherheitsgründen besser nicht aktivieren.

Piwigo unter Ubuntu installieren

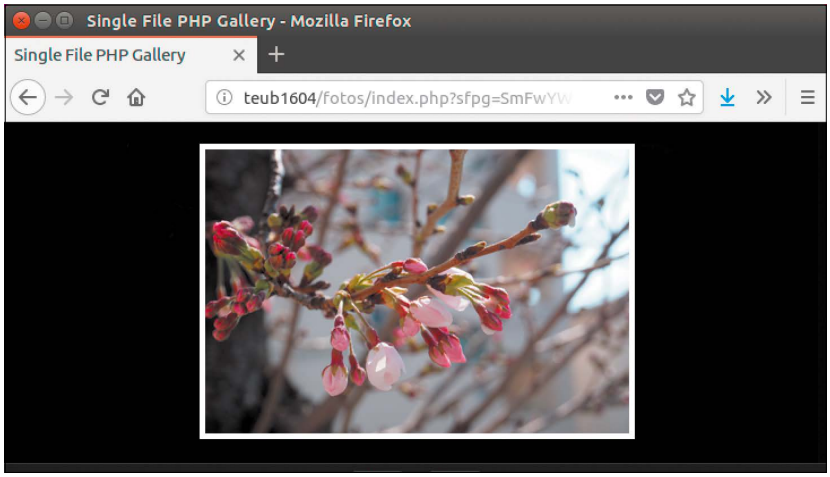
Da Piwigo eine Datenbank benötigt, ist die Installation etwas komplizierter. Installieren Sie zuerst in einem Terminalfenster die nötigen Pakete:

```
sudo apt install apache2 libapa
 che2-mod-php mysql-common mysql-
 server php php-cli php-mysql php-
 imagick php-gd
```

Dabei legen Sie ein My-SQL-Passwort für den Benutzer „root“ fest. Erstellen Sie eine My-SQL-Datenbank und einen Datenbanknutzer (fünf Zeilen):

```
mysql --default-character-set=utf8
 -uroot -p
CREATE DATABASE piwigo DEFAULT
 CHARACTER SET utf8 DEFAULT COL
 LATE utf8_general_ci;
GRANT USAGE ON piwigo.* TO dbuser@
 localhost IDENTIFIED BY '[Pass
 wort]';
GRANT ALL PRIVILEGES ON piwigo.*
 TO dbuser@localhost;
FLUSH PRIVILEGES;
```

Nach der ersten Zeile tippen Sie das Passwort des My-SQL-Benutzers „root“ ein. Den Platzhalter „[Passwort]“ ersetzen Sie durch das Passwort des neuen My-SQL-Benutzers „dbuser“. Das My-SQL-Tool beenden Sie über die Tastenkombination Strg-D.



Minigalerie mit Single File PHP Gallery: Das Tool besteht aus einem einzigen PHP-Script und bietet nur einfache, aber oftmals ausreichende Funktionen.

Laden Sie Piwigo von *http://piwigo.org/basics/downloads* per Klick auf „Download Package“ herunter. Entpacken Sie die ZIP-Datei und kopieren Sie den Inhalt als „root“ beispielsweise nach „/var/www/html/piwigo“. Ändern Sie dort die Zugriffsrechte mittels des Kommandos

```
chown -R www-data:www-data /var/
 www/html/piwigo
```

Rufen Sie dann im Browser die URL

```
http://[IP]/piwigo
```

auf. In das Formular tragen Sie hinter „Benutzer“ den Namen „dbuser“ ein, darunter das beim Anlegen der Datenbank vergebene Passwort sowie den Datenbanknamen „piwigo“. Unter „Administrationseinstellungen“ legen Sie Benutzernamen und Passwort für Piwigo fest. Klicken Sie auf „Start der Installation“ und danach auf „Galerie ansehen“. Per Klick auf „Tour starten“ verschaffen Sie sich einen Überblick über die Grundfunktionen.

PHP-Konfiguration anpassen

Bei Ubuntu 16.04 beträgt die maximale Größe beim Dateiupload nur zwei MB.

Das ist für Bildergalerien in der Regel zu wenig. Um das zu ändern, öffnen Sie die PHP-Konfiguration im Editor:

```
sudo nano /etc/php/7.0/php.ini
```

Passen Sie den Pfad für Ihre PHP-Installation an. Ändern Sie die Variablen in der Datei wie folgt:

```
upload_max_filesize = 64M
post_max_size = 64M
max_execution_time = 300
```

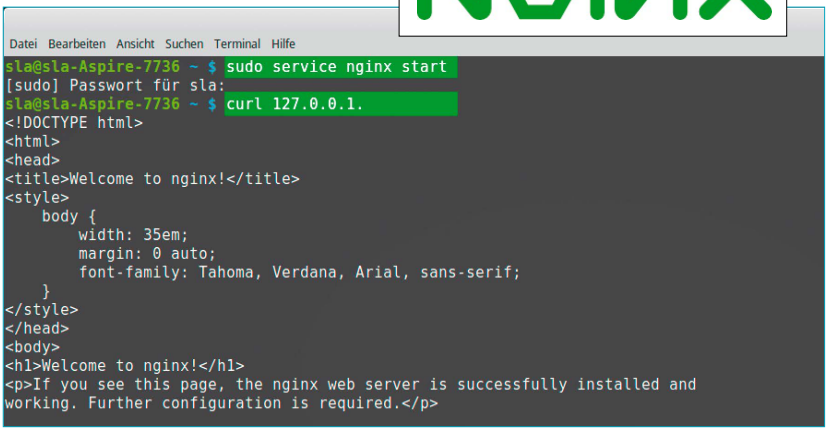
Sie erhöhen damit das Dateilimit auf 64 MB und geben außerdem Scripts etwas mehr Zeit für die Ausführung.

Nginx – der schnelle Webserver

Nginx ist eine leistungsstarke Alternative zum bekannteren Apache-Webserver. Gerade auf limitierten Systemen bietet die Software durchaus Vorteile. Wir stellen den Webserver vor.

Von **Stephan Lamprecht**

Ginge es ausschließlich um Leistung, hätte Nginx („Engine X“) dem Klassiker Apache wahrscheinlich längst den Rang abgelaufen. Unzählige Vergleichstests im Internet belegen die Geschwindigkeitvorteile gegenüber dem Webserver Apache. Nginx kann im gleichen Zeitraum deutlich mehr Anfragen bearbeiten und benötigt weniger Speicher. Mit anderen Worten dauert es bei identischer Hardwareausstattung eines physikalischen Servers deutlich länger, bis dieser an seine Grenzen stößt. Die Gründe, dass noch nicht jeder Webserver mit Nginx läuft, liegen woanders. Einer davon dürfte ohne Zweifel darin bestehen, dass Nginx bei der Konfiguration viele Dinge anders handhabt. Das auf Apache gesammelte Wissen ist daher nicht ohne Weiteres zu übertragen.



Sobald die Installation von Nginx abgeschlossen wurde und der Service gestartet ist, zeigt beispielsweise das Kommando curl, dass der Webserver läuft.

Perfekt für kleinere Systeme

Hat man für ein Projekt die freie Wahl hinsichtlich der eingesetzten Software, spricht einiges dafür, Nginx zu nutzen. Das gilt insbesondere auf Systemen, die in ihrer Hardware limitiert sind, wie beispielsweise kleine Platinenrechner. Hier kommt es ja gerade darauf an, möglichst wenig Ressourcen zu verbrauchen. Das gilt auch für Cloudserver, die sich im Zweifel zwar schnell skalieren lassen, dann aber auch mehr Geld kosten. Doch jetzt kommt bereits ein zweiter Grund, der Admins dazu verleiten kann, bei Apache zu bleiben. Denn an manchen Stellen ist der schlanke Server nicht so flexibel wie der Apache, zum Beispiel kennt Nginx keine Anpassungen der Konfiguration auf Verzeichnisebene, wie sie mit den „.htaccess-Dateien“ möglich sind. Und wenn eine Anwendung partout auf ein Apache-Modul Wert legt und es ausdrücklich in den Systemvoraussetzungen erwähnt, kommen Sie mit Nginx wohl nicht weiter.

Nginx ist modular aufgebaut und kann nicht nur die Aufgabe eines Webservers übernehmen, sondern in viele Rollen schlüpfen. Darunter ist die eines Reverse Proxys für Heimanwender wahrscheinlich die interessanteste. Sie kennen das: Um unterwegs auf das Mediencenter oder die Zentrale für die Heimsteuerung zugreifen zu können, muss ihr Internetzugang nicht nur über eine URL erreichbar sein (meist mittels Dyn DNS realisiert), sondern Sie müssen am Router auch noch Ports freischalten, um das Gerät zu erreichen. Ein Reverse Proxy verhindert, dass der Router so löchrig wie ein Schweizer Käse wird. Er nimmt die Anfragen der externen Clients entgegen und leitet diese dann intern an die richtigen Geräte weiter.

Nginx ist schnell installiert

Die Installation von Nginx ist verhältnismäßig unkompliziert, da die Software inzwischen bei allen bekannten Distributionen in den Paketquellen vorhanden ist. Die Einrichtung der Pakete kann somit schnell in einem Terminal mit

```
sudo apt-get install nginx
```

erfolgen. Da stets nur jeweils ein Webserver die Anfragen bearbeiten kann, sollten Sie einen eventuell laufenden Apache beenden. Das erledigen Sie auf der Konsole mit diesem Kommando:

```
sudo service apache2 stop
```

Jetzt können Sie Nginx mit dem Befehl

```
sudo service nginx start
```

aufrufen. Um zu prüfen, ob der Start funktioniert hat, geben Sie im gleichen Terminal das Kommando

```
curl 127.0.0.1
```

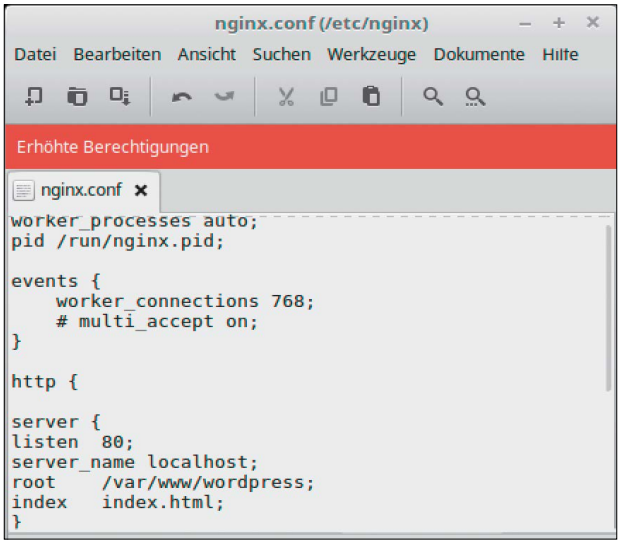
ein oder Sie nutzen einen Browser und rufen hier die Seite „http://localhost“ auf. In beiden Fällen sollte sich der Nginx-Server melden.

Die Konfiguration läuft anders

Was Nginx und Apache verbindet, ist die Aufteilung der Einrichtungsdateien. Die Optionen des Servers befinden sich in der Textdatei „etc/nginx/nginx.conf“, die mit einem beliebigen Texteditor bearbeitet werden kann. Die Optionen zur Einrichtung als Webserver befinden sich im Block, der mit „http“ beginnt. Eine ganz einfache Konfiguration definiert den Port, den Nginx überwacht, den Namen, unter dem der Server erreichbar sein soll, sowie das Verzeichnis, in dem sich die Dokumente oder die Webapplikationen befinden, die ausgeliefert oder ausgeführt werden sollen. So könnte man das CMS Wordpress beispielsweise im Ordner „/var/www/wordpress“ installieren. Einen Überblick über alle Parameter stellen die Entwickler in einem eigenen Wiki zur Verfügung.

Nginx unterscheidet sich aber von Apache grundlegend in seiner Architektur. Bei Apache genügt die Aktivierung eines Moduls, um dynamische Inhalte per PHP auszuliefern. PHP muss bei Nginx dagegen über einen Hilfsprozess ausgeführt werden. In der Praxis nimmt der Server dann eine PHP-Anfrage entgegen und übergibt diese an den Hilfsprozess, der sie dann an den PHP-Interpreter auf dem Server weiterreicht. Die Antwort wird dann wieder an den Webserver geleitet.

Was sich eher umständlich und langsam anhört, bringt aber im Endeffekt genau die hohe Arbeitsgeschwindigkeit des Servers. Denn die Anfrage belastet den Server nur kurz, die Generierung des dynamischen Inhalts übernimmt die Hilfsanwendung. Dieser Fast Process Manager (FPM) ist ebenfalls in den Paketquellen der Distributionen dabei und kann somit auch durch die Angabe des Paketnamens („php-fpm“) installiert werden. Sofern PHP noch nicht auf dem System installiert wurde, erledigt das der Paketmanager dann auch gleich mit, da die Script-Sprache als Abhängigkeit definiert ist.



In der Datei mit den Optionen von Nginx richten Sie die Auslieferung mit diesem Codeblock ein. In diesem Beispiel soll das Stammverzeichnis der Ordner „Wordpress“ sein.

Nach der Installation des Pakets muss der Prozessmanager als Service zunächst gestartet werden:

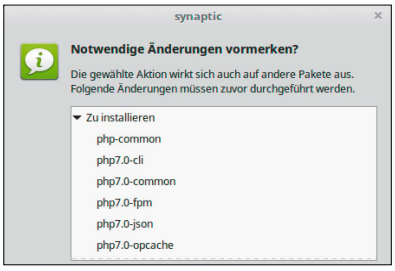
```
sudo service php7.0-fpm start
```

Aber Achtung: Je nach installierter PHP-Version und Distribution kann der Service unter Umständen anders heißen. Wenn der gerade genannte Aufruf nicht zum Ziel führt, lassen Sie sich mit

```
sudo service --status-all | grep -i fpm
```

das richtige Paket nennen. Nutzen Sie das Ergebnis dann als Parameter für den Aufruf. Zum Abschluss muss jetzt noch die Verbindung zwischen Nginx und dem Prozessmanager hergestellt werden. Dazu wird in die Serversektion der Nginx-Konfigurationsdatei dieser Block aufgenommen:

```
location ~ [^/]\.php(/|$) {
fastcgi_split_path_info ^(.+?\.
 php)(/.*)$;
fastcgi_pass unix:/var/run/php7.0-
 fpm.sock;
fastcgi_index index.php;
include fastcgi_params;
}
```



Damit dynamische Inhalte Einzug halten, braucht Nginx den Fast Process Manager. Der installiert, falls nötig, die Script-Sprache PHP gleich mit.

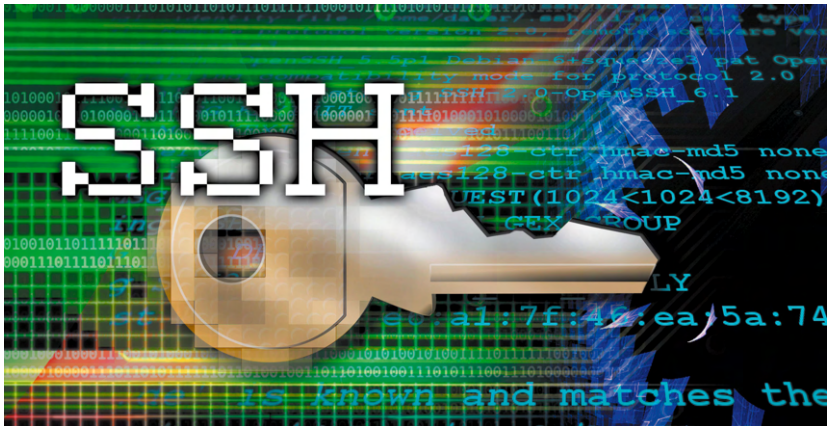
Danach starten Sie Nginx erneut. In das Stammverzeichnis für Dokumente („/var/www“ oder was Sie in der Konfiguration definiert haben) legen Sie dann eine Datei „index.php“ ab, die lediglich diesen Eintrag enthält: „<?php echo phpinfo(); ?>“. Speichern Sie diese und rufen Sie die Datei im Browser auf. Wenn Sie eine Fehlermeldung erhalten, ändern Sie im gerade gezeigten Block die Zeile „fastcgi_pass unix:127.0.0.1:9000;“ ab. Installation und Einrichtung funktionieren so auch auf dem Raspberry Pi.

Mit Standardanwendungen wie Wordpress, Joomla oder Magento werden Sie keine Probleme und kaum Anpassungsarbeit haben. Die Apps arbeiten reibungslos mit Nginx zusammen. Im Falle des Falles hält das Wiki *https://www.nginx.com/resources/wiki/start/* detaillierte Beschreibungen für die Konfigurationsanpassung parat. ●

Sichere Verbindungen mit Sshuttle

In den wenig vertrauenswürdigen Gewässern des Internets ist das Virtual Private Network (VPN) ein sicherer Hafen. Dessen Einrichtung ist aber aufwendig. Sshuttle ist ein recht unkomplizierter Ersatz mit minimaler Konfiguration.

Von **David Wolski**



Ein VPN verschlüsselt den gesamten Datenverkehr auf Netzwerkebene. Gegenüber anderen Lösungen wie beispielsweise verschlüsselten Protokolle HTTPS oder SFTP schützt ein VPN alle Arten von Verbindungen. Der VPN-Server ist damit ein sicheres Eingangstor zum Netzwerk dahinter und kann mit dem richtigen Routing eine Verbindung zum gesamten Netzwerk herstellen – so als ob man sich direkt im lokalen Netzwerk befände. VPN-Lösungen wie das verbreitete Open VPN sind zwar Open Source und in den Paketquellen der meisten Linux-Distributionen verfügbar, doch ist die Einrichtung und Konfiguration ein komplexes Unterfangen und verschreckt viele Anwender.

Sshuttle: Alles per SSH

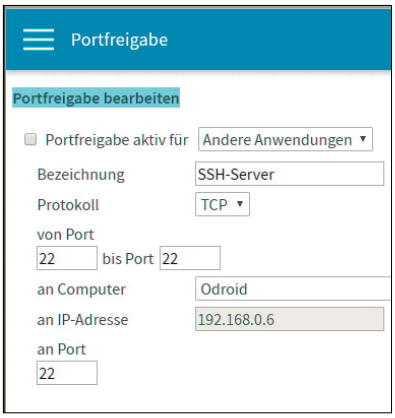
Es geht auch viel einfacher: Sshuttle (*http://sshuttle.readthedocs.io*) ist eine findige Lösung, die auf dem SSH-Protokoll aufsetzt und auf dem VPN-Server lediglich einen laufenden OpenSSH-Server verlangt. Genau genommen handelt sich bei Sshuttle nur um eine Clientkomponente. Diese wurde kürzlich in Python 3 neu geschrieben und läuft deshalb auf nahezu jedem Linux-System. Auf dem Client, der am entfernten Netzwerk teilnehmen soll, baut Sshuttle lediglich eine verschlüsselte SSH-Verbindung zum Server auf. Über diese Verbindung überträgt das Tool während dem Verbindungsaufbau ein weiteres kleines Python-Programm – die Serverkomponente. Clientseitig erstellt dann Sshuttle mit temporären iptables-Regeln einen transparenten Proxy, der allen Datenverkehr annimmt, der für das entfernte Netzwerk bestimmt ist. Die Serverkomponente nimmt diesen Verkehr an, leitet ihn entsprechend an die dortigen Dienste oder ins lokale Netzwerk weiter und sendet den Traffic zurück zum Client.

Soweit arbeitet Sshuttle wie ein SSH-Tunnel. Allerdings arbeitet Sshuttle mit beliebig vielen TCP-Ports und ist nicht wie gewöhnliches SSH auf einen einzigen pro Verbindung beschränkt. Zudem vermeidet das Tool durch eine Reassemblierung der Netzwerkpakete eine ungünstige TCP-über-TCP-Kapselung, welche zu Leistungseinbußen führt.

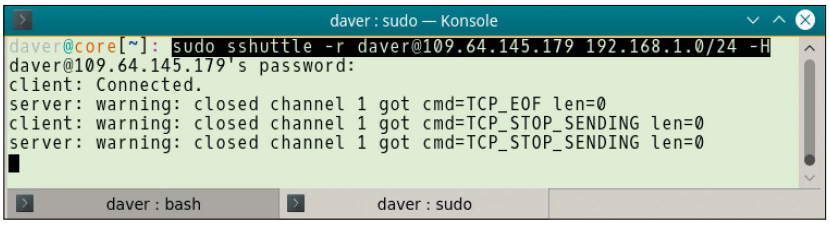
Drei Einschränkungen dürfen aber nicht unerwähnt bleiben: Sshuttle leitet nur TCP-Verbindungen sowie optional auch DNS-Abfragen weiter. UDP und Pings über ICMP funktionieren also über Sshuttle nicht. Diese Protokollarten sind aber für das Web und Zugriffe auf Windows- oder NFS-Freigaben auch nicht notwendig. Auf dem Client verlangt Sshuttle root-Rechte, da es dort iptables-Regeln ändert. Da Sshuttle auf diesen Standard-Systemkomponenten aufbaut, funktioniert es nur auf Linux und Mac-OS X. Windows bleibt außen vor.

Vorarbeit: Port 22 freigeben

Damit man mit Sshuttle über das Internet in das eigene Netzwerk zu Hause oder im Büro kommt, muss dort nur ein System mit laufendem OpenSSH-Server als Gateway von außen erreichbar sein. Diese Rolle kann gut ein kleiner Platinenrechner übernehmen. Die Leistung eines Raspberry und die Geschwindigkeit des 100-MBit-Ethernetports reichen für



Einen Port für SSH weiterleiten: Der Router muss den Port 22 (TCP) von außen erreichbar machen und im lokalen Netzwerk an die IP-Adresse des Linux-Servers weiterleiten.



Sshuttle in Aktion: Das Python-Programm öffnet am Client eine Verbindung per SSH zum Server und baut ein VPN zum Netzwerk 192.168.1.0 auf. Strg-C beendet die Verbindung.



Die „Magie" hinter Sshuttle: Das Tool manipuliert auf dem Client die iptables-Regeln und baut so einen transparenten Proxy für die Adressen im entfernten Netzwerk auf.

ein Netzwerk aus, das per DSL an die Außenwelt angebunden wird.

Der DSL-Router muss nur wissen, dass Anfragen an den SSH-Port aus dem Internet durchgelassen werden und welcher Teilnehmer im Netzwerk der Open-SSH-Server ist. Zu diesem Zweck richten Sie auf dem Router eine Portfreigabe für Port 22 ein. Wenn der Open-SSH-Server im LAN beispielsweise die IP 192.168.0.6 hat, dann leiten Sie im Router den TCP-Verkehr an Port 22 auf diese interne IP-Adresse und den dortigen Port 22 weiter. Nützlich ist außerdem ein dynamisch aktualisierter Hostname für den Router, damit dieser trotz wechselnder öffentlicher IP unter dem stets gleichen Hostnamen erreichbar ist. Für diesem Fall kommt ein dynamischer DNS-Dienst wie beispielsweise Noip(*www.noip.com*) zur Hilfe, der auch einer sich ändernden IP-Adresse feste Hostnamen im DNS zuteilt. Die meisten DSL-Router unterstützen Noip und teilen dem Dienst nach der Einrichtung automatisch die neue IP des Providers mit.

Installation auf Client und Server

Der Server muss lediglich den Open-SSH-Server ausführen, der auf Servern meist standardmäßig läuft und in Debian, Ubuntu und Co mit

```
sudo apt-get install openssh-ser
  ver
```

auch schnell nachinstalliert und in Gang gesetzt ist. Mehr ist dort nicht zu tun. Auf dem Client installieren Sie das Python-Programm Sshuttle, das sich bei Debian, Ubuntu sowie Varianten, Fedora und Arch Linux in den Standard-Paketquellen befindet. In Debian/Ubuntu ist der Client mit

```
sudo apt-get install sshuttle
```

schnell installiert.

Wer Open Suse einsetzt, bekommt eine recht frische Version des Programms im Build-Service unter *http://software.opensuse.org/download.html?project=security&package=sshuttle*.

Sshuttle starten: Verbindungen öffnen

Sshuttle ist ein Kommandozeilenprogramm, das ohne Konfiguration einfach über Aufrufparameter gesteuert wird. Für den Einsatz als VPN erwartet Sshuttle mindestens die Angabe des Zielservers (Hostname oder IP) und eine Netzwerkmaske mit den Adressen des entfernten Netzwerks. Soll das entfernte Netzwerk 192.168.0.1 bis 192.168.0.254 auf dem Client erreichbar sein, so öffnet der Befehl

```
sudo sshuttle -r [User]@[Server]
  192.168.1.0/24
```

diese Verbindung. Falls der nach außen freigegebene Port vom Standard 22 abweicht, muss dies in dieser Form angegeben werden:

```
sudo sshuttle -r [User]@
  [Server]:[Portnummer]
  192.168.1.0/24
```

Möchte man die Rechner im entfernten Netzwerk über ihren dortigen Hostnamen erreichen, dann startet

```
sudo sshuttle -r [User]@[Server]
  192.168.1.0/24 -H
```

eine automatische Suche nach den Hostnamen, die Sshuttle dann temporär in die Datei „/etc/hosts" schreibt. Das letzte Beispiel

```
sudo sshuttle -r [User]@[Server]
  192.168.1.0/24 --dns
```

nutzt den DNS-Server des entfernten Netzwerks zur Namensauflösung.

Sshuttle: Stärken und Schwächen

- ⊕ verlangt keine umfangreiche Konfiguration
- ⊕ kommt ohne komplexe Firewall-Regeln aus
- ⊕ braucht nur einen SSH-Server und SSH-Client
- ⊖ kümmert sich nur um TCP-Verbindungen
- ⊖ erfordert root-Recht auf dem Client
- ⊖ läuft nur auf Linux, BSD und Mac-OS X

IMPRESSUM

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*

Chefredakteur: Sebastian Hirsch (v.i.S.d.P – Anschrift siehe Verlag)

Gesamtanzeigenleitung:
IDG Tech Media GmbH, Lyonel-Feininger Str. 26, 80807 München,
Tel. 089/36086-0, Fax 089/36086-118,
Sebastian Wörle, E-Mail: swoerle@idg.de

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,
Jürgen Donauer, Thorsten Eggeling, Stephan Lamprecht,
David Wolski

Titelgestaltung: Schulz-Hamparian, Editorial Design / Thomas Lutz

Freier Mitarbeiter Layout/Grafik: Alex Dankesreiter
Freie Mitarbeiterin Schlussredaktion: Andrea Röder
Herstellung: Melanie Arzberger
Freier Mitarbeiter digitale Medien: Ralf Buchner
Redaktionsassistenz: Manuela Kubon

Einsendungen: Für unverlangt eingesandte Beiträge sowie Hard- und Software übernehmen wir keine Haftung. Eine Rücksendegarantie geben wir nicht. Wir behalten uns das Recht vor, Beiträge auch auf anderen Medien, etwa auf DVD oder online, zu veröffentlichen.
Copyright: Das Urheberrecht für angenommene und veröffentlichte Manuskripte liegt bei der IT Media Publishing GmbH & Co. KG. Eine Verwertung der urheberrechtlich geschützten Beiträge und Abbildungen, insbesondere durch Vervielfältigung und/oder Verbreitung, ist ohne vorherige schriftliche Zustimmung des Verlags unzulässig und strafbar, soweit sich aus dem Urheberrechtsgesetz nichts anderes ergibt. Eine Einspeicherung und/oder Verarbeitung der auch in elektronischer Form vertriebenen Beiträge in Datensysteme ist ohne Zustimmung des Verlags unzulässig.

Haftung: Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Die Veröffentlichungen in der LinuxWelt erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Auch werden Warennamen ohne Gewährleistung einer freien Verwendung benutzt.

Bildnachweis: 123RF - gl0ck33; sofern nicht anders angegeben: Anbieter

ANZEIGENREPRÄSENTANZ
IDG Tech Media GmbH, Lyonel-Feininger Str. 26, 80807 München,
Tel. 089/36086-210, Fax 089/36086-263,
E-Mail: *media@pcwelt.de*

Gesamtanzeigenleitung:
Sebastian Wörle (-113)
(verantwortlich für den Anzeigenteil)

Digitale Anzeigenannahme – Datentransfer:
Zentrale E-Mail-Adresse: *AnzeigendispoPrint@pcwelt.de*
Digitale Anzeigenannahme – Ansprechpartner:
Walter Kainz (-258), E-Mail: *wkainz@idg.de*
Anzeigenpreise: Es gilt die Anzeigenpreisliste 34 (1.1.2017).
Bankverbindungen: Deutsche Bank AG,
Konto 666 22 66, BLZ 700 700 10;
Postbank München, Konto 220 977-800,
BLZ 700 100 80
Anschrift für Anzeigen: siehe Anzeigenabteilung
Erfüllungsort, Gerichtsstand: München

Verlagsrepräsentanten für Anzeigen in ausländischen Publikationen:
Europa: Shane Hannam, 29/31 Kingston Road, GB-Staines,
Middlesex TW 18 4LH, Tel.: 0044-1-784210210

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

Anzeigen-Hotline Print:
Sven Schrader, E-Mail: *schrader@it-media.de*, 089/3398052-41

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: 49,50 € (D), 64,50 CHF (CH) und 53,50 € (A, Benelux) inkl. Versandkosten
Bankverbindung für Abonnenten:
Postbank Stuttgart, BLZ 600 100 70, Konto 311704
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.

PC-WELT

Sonderheft-Abo

Für alle Sonderausgaben der PC-WELT



Sie entscheiden, welche Ausgabe Sie lesen möchten!

Die Vorteile des PC-WELT Sonderheft-Abos:

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

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

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

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

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

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

BEZAHLEN

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

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PWSJO14130

PC-WELT erscheint im Verlag 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



Unterwegs-Power

Die ultramobilen Linux-Workstations von TUXEDO Computers

Erleben Sie jetzt die leistungsfähigsten TUXEDO Notebooks aller Zeiten

Dank neuester Intel® Core™ i-Prozessoren, bis zu 32 GB Arbeitsspeicher und flexibel wählbarem Festplatten- und SSD-Speicher sind Ihnen keine Grenzen gesetzt. Mit integriertem 4G LTE Modem und bis zu 24h Akkulaufzeit sind Sie "always on".

Immer die Leistungsfähigkeit im Blick haben wir ultramobile Begleiter geschaffen, die dank flacher Bauweise und leichter Materialien ideal für den Einsatz unterwegs sind.

Das alles funktioniert durch sorgfältig ausgewählte und aufeinander abgestimmte Komponenten zu 100% mit Linux und Windows - *garantiert!*

Direkt zum Vorzugspreis sichern!

Konfigurieren Sie jetzt Ihr TUXEDO Notebook individuell und sparen dabei exklusive 3% mit dem Rabattcode "LXWELTIB13" - *aber nur für kurze Zeit!*

TUXEDO COMPUTERS

tuxedocomputers.com