MULTIBOOT-DVD: 8 SYSTEME SOFORT STARTKLAR

4 196691 608505 01

LINUX WELT

ANDROID WELT Sonderheft
1/2018 · Dezember / Januar
Deutschland 8,50 € · Schweiz 16,90 sfr · Österreich + Benelux 9,45 €

Ein Rechner – viele Systeme

- So nutzen Sie Multiboot mit Linux
- Alles gefahrlos testen mit Vmware und Virtualbox

PLUS: Ubuntu 17.10 auf DVD

Das neue Linux-Mega-Paket

1000 Seiten Linux-Wissen!

- Der komplette Jahrgang 2017
- 303 Seiten Linux-Know-how als E-Book

Tipps für Linux-Profis

- Portable Apps für jedes System
- Raspberry Pi als Firewall
- So bleibt Ihr Linux immer aktuell
- NEU: Mit I2P unsichtbar im Netz

NEU!

Ubuntu 17.10 Radikal anders!

Das bringt das neueste Linux:

- Komplett neuer Desktop · Schneller Display-Server
- Komfortabler Anmelde-Manager · Übersichtliches Dock
- Funktionstarkes Kontrollzentrum · Stabiler Audioplayer
- Bessere Druckfunktion · Funktionsreicher Kalender u.v.m.

Großes Special

Sichern Sie Ihr Linux!

- So verschlüsseln Sie Dateien für USB-Stick, Mail, Cloud u.v.m.
- Sicherer Datenaustausch mit Windows & Android
- Zuverlässig geschützt beim Surfen und Mailen

PLUS: Alle Infos zur WLAN-Lücke Krack

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

PC-WELT

Sonderheft-Abo

Für alle Sonderausgaben der PC-WELT

Sie entscheiden, welche Ausgabe Sie lesen möchten!

Die Vorteile des PC-WELT Sonderheft-Abos:

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

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

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

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

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

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

BEZAHLEN

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

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PWSJO14130

PC-WELT erscheint im 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

Verschlüsselung in Gefahr

Kryptologen warnen: Künftige Quantencomputer können die heutige Kommunikationsverschlüsselung spielend knacken. Bislang gelten verschlüsselte Daten unter anderem dann als sicher, wenn sich der geheime Code auch mit größter Rechenpower nicht in angemessener Zeit errechnen lässt. Benötigen aktuelle Superrechner für einen Schlüssel mehrere Jahrzehnte, scheint die Verschlüsselung ausreichend sicher.

Quantenrechner: Wenn aus Jahren Tage werden

Doch diese Zeitspanne könnte zu Tagen schrumpfen, wenn es in fünf bis zehn Jahren funktionsfähige Quantencomputer geben wird. Ein Quantenrechner arbeitet nicht mit den Gesetzen der klassischen Physik, sondern auf der Basis quantenmechanischer Zustände. Diese scheinbar spukhaften Mechanismen ermöglichen Rechenmethoden, die Codes extrem schnell entschlüsseln.

Die gute Nachricht: Es bleibt noch Zeit

Doch noch gibt es keine Quantencomputer, wenn man vom umstrittenen Rechner D Wave absieht. Uns Anwendern bleibt also noch etwas Zeit, auf neu entwickelte Verschlüsselungsalgorithmen zu warten. Wie Sie die beste Verschlüsselung einsetzen, die es heute gibt, verrät unser Special zum Thema ab Seite 56.

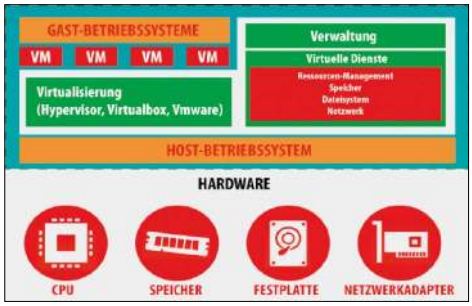
Herzlichst, Ihr

Arne Arnold
Redakteur
aarnold@it-media.de

Webserver für Heimnetz und Internet

Webserver gehören nicht nur ins Internet, sondern leisten auch im lokalen Netzwerk nützliche Dienste. Der Schwerpunkt zeigt, wie Sie Webserver mit Apache oder Nginx einrichten und optimieren.

S. 24



Virtualisierung

Grundlagen und Praxistipps zur Technik von Vmware und Virtualbox.

S. 36

Linux-Multiboot

Linux-Multiboot auf einem PC scheint einfach, hat aber seine Finessen.

S. 52

Die Highlights auf der DVD

Die Multiboot-DVD steht dieses Mal im Zeichen des brandneuen Ubuntu 17.10. Insgesamt vier „Flavours“ von Ubuntu – mit Gnome, Mate, Budgie und LXDE – starten von der DVD, lassen sich ausgiebig ausprobieren und auf Wunsch installieren.

S. 10

Ubuntu 17.10 mit Gnome-Desktop
Ubuntus Standardausgabe kehrt mit Version 17.10 bekanntlich wieder zur Gnome-Oberfläche zurück. Mit kleinen optischen und funktionalen Maßnahmen an Gnome hält der Desktop Kontinuität zum bisherigen und nunmehr eingestellten Unity.

Ubuntu 17.10 mit Mate-Desktop
Das sparsame, aber funktionsreiche und anpassungsfähige Ubuntu Mate ist ein beliebtes System für nicht mehr taufrische Hardware. Außerdem ist der Desktop enorm anpassungsfähig und bringt nun auch noch einige Unity-Mimikrys mit.

Ubuntu 17.10 mit Budgie
Dieser Neuling unter den offiziellen Ubuntu-Distributionen leiht sich vom Distributionsprojekt „Solus“ den Desktop Budgie. Die aufgeräumte Oberfläche unterscheidet sich vor allem durch eine innovative, multifunktionale Seitenleiste.

Distributionen und Software

Raspberry & Server

Praxis

Standards

Achtmal Linux

Ubuntu im Umbruch
Die LinuxWelt Heft-DVD 1/18!

Ubuntu 17.10 (64 Bit)
Version 17.10 läutet große Veränderungen auf dem Ubuntu-Desktop an: Ab jetzt arbeitet die primäre Ausgabe Ubuntus mit Gnome (3.26), der hier allerdings einige Erweiterungen bekommen hat, um Ähnlichkeit zu Unity herzustellen. Auch als ISO-Datei auf DVD.

Ubuntu Mate 17.10 (64 Bit)
Mit seiner Softwareauswahl und einem Assistenten für die ersten Schritte ist diese Distribution ein perfekter Einstieg in Linux auf dem Desktop. Die gründlich aktualisierte Ubuntu-Variante wird mit viel Liebe zum Detail entwickelt und ist zum Vorzeigesystem für den Mate-Desktop geworden. Auch als ISO-Datei auf DVD.

Ubuntu Budgie 17.10 (64 Bit)
Auch dies ist eine offizielle Ubuntu-Ausgabe: Der Budgie-Desktop ist eine Abspaltung von Gnome 3 mit einem traditionelleren Aufbau der Arbeitsfläche und etwas geringeren Hardwareanforderungen. Auch als ISO-Datei auf DVD.

Lubuntu 17.10 (32 Bit)
Noch einmal mit LXDE, bevor Lubuntu zum Nachfolgerdesktop LXQT wechselt: Lubuntu ist die Ubuntu-Ausgabe mit den geringsten Hardwareansprüchen und deshalb in 32-Bit-Ausführung auf der DVD. Auch als ISO-Datei auf DVD.

Open Suse Tumbleweed (64 Bit)
Tumbleweed ist jener Open-Suse-Zweig, der zuerst die neuesten Versionen von Programmpaketen bekommt. Es handelt sich um einen eigenen Distributionszweig für Fortgeschrittene, vergleichbar mit Debian Sid, und ist als „Rolling Release" konzipiert. Der Desktop ist ein laufend aktualisiertes KDE Plasma 5. Auch als ISO-Datei auf DVD.

Antergos 17.10 (64 Bit)
Das stets sehr aktuelle Antergos ist ein Livesystem zur vergleichsweise komfortablen Installation von Arch Linux – mit grafischem Installer. Das Linux-System eignet sich dennoch primär für Fortgeschrittene. Der Installer bietet verschiedene Desktopumgebungen wie Gnome, KDE, Mate und XFCE an. Auch als ISO-Datei auf DVD.

Porteus 3.2.2 (32 Bit)
Porteus ist ganz auf den Einsatz als komfortables Livesystem und Surfsystem spezialisiert. Die hier angebotene Version nutzt Mate als Desktop und bietet wahlweise die Browser Firefox, Chrome und Opera.

Gparted Live 0.30 (32 Bit)
Perfekt partitionieren: Vor der Installation eines Linux-Systems ist es bei Parallelinstallation oft nötig, auf den Datenträgern durch die Verkleinerung bestehender Partitionen Platz zu schaffen. Für solche Aufgaben ist das Livesystem Gparted Live prädestiniert – das offizielle System der Gparted-Entwickler. Auch als ISO-Datei auf DVD.

Extras & Tools

Super Grub Disk 2.02s9
Das startfähige Tool Super Grub Disk 2 liefert eine Boothilfe für Linux-Systeme, bei welchen der Bootloader vom Typ Grub 2 nicht mehr intakt ist oder von Windows überschrieben wurde. Im Multibootmenü der DVD ist das Tool unter „Extras und Tools" startklar und liegt auch als ISO-Datei im Ordner „Extras".

Plop Bootmanager 5
Dieser Bootmanager kann von USB-Geräten booten, auch wenn dies das Bios des Rechners nicht unterstützt. Plop bietet dafür ein eigenes Bootmenü und lässt sich von DVD starten, um ein angeschlossenes USB-Laufwerk zu booten.

Hardware Detection Tool 0.5.2
Einen Überblick zur kompletten Hardware eines Systems bietet das startfähige Hardware Detection Tool, auch wenn kein Betriebssystem installiert ist. In einem englischsprachigen Fenster zeigt HDT Kategorien wie RAM, Prozessor, PCI und Bios an.

Memtest 86+ 5.01
Der aktuelle Memtest 86+ testet den Arbeitsspeicher und unterstützt auch moderne Intel-Chipsätze. Das Diagnoseprogramm läuft auf jedem PC mit 32-Bit- wie 64-Bit-CPUs und mit allen verbreiteten RAM-Typen. Es beginnt sofort nach dem Start mit den Tests, die jederzeit unterbrochen werden können.

DBAN 2.3
Darik's Boot and Nuke (DBAN) löscht Daten auf magnetischen Datenträgern endgültig durch Überschreiben. Auch Wiederherstellungstools können dann keine Daten mehr rekonstruieren. DBAN eignet sich nur für Festplatten. Auf Flashspeichern, SSDs und USB-Sticks ist das Tool wirkungslos.

Software auf DVD

Imgburn 2.5.8.0
Kompaktes, deutschsprachiges Brennprogramm für alle Windows-Versionen, um Imagedateien auf CDs/DVDs zu schreiben. Werbefinanzierte Freeware. Hinweis: Die Installation bietet optional die Einrichtung der Ask-Toolbar und von Werbelinks auf dem Desktop an.

Unetbootin 6.55
Das nützliche Tool mit grafischer Oberfläche transferiert mit wenigen Klicks die ISO-Images von Ubuntu und seinen Abkömmlingen sowie einige weiteren Distributionen bequem auf USB-Stick oder Speicherkarten und macht diese mit einem eigenen Bootmenü startfähig. Auf DVD finden sich die 32-Bit- und 64-Bit-Ausgaben für Linux (alle Linux-Distributionen) sowie Versionen für Windows und Mac-OS.

Putty 0.70
Der Terminalclient für SSH und Telnet eignet sich für alle Windows-Systeme. Putty liegt in Form einer EXE-Datei vor und braucht nicht installiert zu werden. Das Open-Source-Programm ist englischsprachig.

Kitty 0.70.0.2
Kitty ist ein Terminalclient für SSH und eine fast identische Abspaltung von Putty, ergänzt es allerdings um einige bequeme Features (automatische Passwortübergabe). Wie Putty wird es einfach über seine EXE-Datei gestartet.

Win 32 Disk Imager 1.0
Das Windows-Programm überträgt ISO-Images und IMG-Dateien bootfähig auf USB und Speicherkarten. Es entspricht technisch dem Rohkopierer dd unter Linux. Das Tool liegt als Installer auf DVD, ferner als ZIP-Archiv, das nach dem Entpacken keine weitere Installation benötigt.

Wahl-O-Mat Distributionen
Überarbeiteter Fragebogen und Informationssystem zur Wahl der optimalen Linux-Distribution auf der HTML-Oberfläche der DVD.
Der interaktive Fragebogen benötigt keine Onlineverbindung und ist komplett in Javascript (Jquery) realisiert.

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

WEITERE INFOS

Auf der DVD ist nicht nur das brandaktuelle Ubuntu 17.10 vertreten. Detaillierte Vorstellungen der Systeme auf DVD finden Sie im Heftbeitrag ab Seite 10.
Zusätzliche Anleitungen und Hinweise zu den Distributionen auf Heft-DVD liefert die dortige Übersicht, die Sie über die Datei „index.html" in einem Browser öffnen.
Das erste Special dieser Ausgabe dreht sich ab Seite 24 um die Grundlagen bei der Einrichtung von Webservern.
Ein zweites Special ab Seite 36 nimmt sich Multibootumgebungen sowie Virtualisierung vor.
Das dritte Special ab Seite 56 erklärt alle namhaften Verschlüsselungstechniken unter Linux.

- Startfähiges Livesystem auf DVD
- Livesystem plus ISO-Datei auf DVD
- Programm auf DVD

PDF-E-BOOK 1/18

Extragroßes E-Book
Auf über 300 Seiten präsentiert das E-Book neu zusammengestelltes Linux-Wissen und Know-how rund um Open-Source-Programme aus den letzten Ausgaben. Neben Grundlagenartikeln gibt es eine Rubrik zu den wichtigsten Distributionen und Livesystemen. Viele zeitlose Praxisartikel liefern die Rubriken zu Linux-Server, Hardware, Distributionen und Sicherheit. Das Special für fortgeschrittene Systembastler aus der letzten LinuxWelt 6/2017 ist komplett enthalten.

LinuxWelt: Jahrgang 2017 als PDF Nachlese
Als Service liegt diesmal der komplette Jahrgang 2017 der LinuxWelt auf Heft-DVD. Die sechs Ausgaben liegen jeweils als PDF-Datei vor, um ganz unkompliziert Lesestoff und Material für das eigene digitale Archiv vergangener Hefte zu liefern.

PC-WELT

Windows 10.4 – das komplette Handbuch

Sonderheft
für nur
12,90 €

Alle neuen Funktionen zum Herbst-Update

Jetzt bestellen unter
www.pcwelt.de/windows 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 Windows 10.4 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

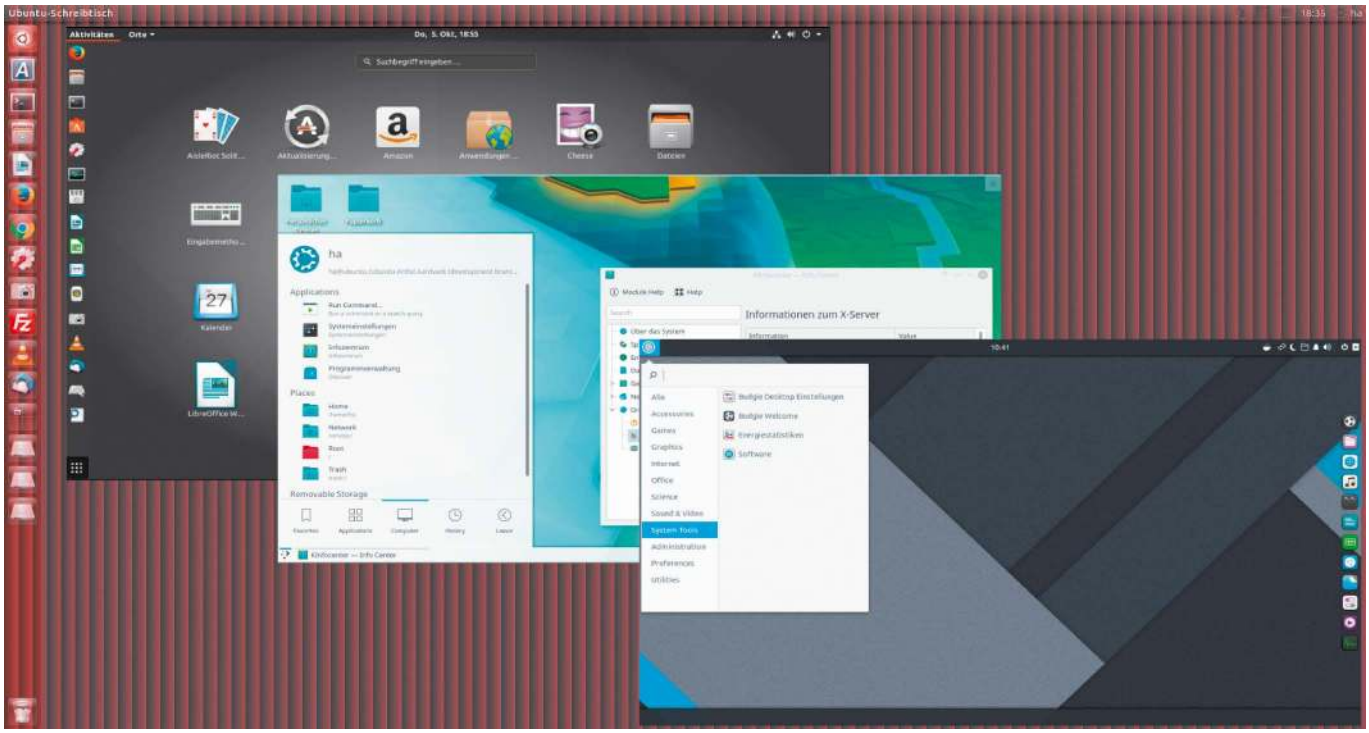
IBAN

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

Warum wir Ubuntu brauchen



Ubuntu 17.10 folgt der Releasepolitik Canonicals: Zweimal im Jahr gibt es eine neue Version – mithin Gelegenheit, die Softwarepakete aufzufrischen. Wirklich Neues gibt es auch, aber in homöopathischer Dosierung. Trotzdem bleibt Ubuntu relevant.

VON HERMANN APFELBÖCK

Der Ubuntu-eigene Desktop Unity ist ebenso Geschichte wie der Displayservers (MIR): Nach dem Scheitern der Pläne, mit Unity und MIR alle Geräteklassen vom Handydisplay bis zum Desktopmonitor zu bedienen, stellen Kritiker die Relevanz von Ubuntu und der Firma Canonical in Frage. Und wer schon mal anfängt zu zweifeln, wird leicht noch weitere gescheiterte Pläne Canonicals an Land ziehen: Der eigene Init-Daemon Upstart konnte ebenso wenig bestehen wie der ambitionierte Clouddienst Ubuntu One. Die Zusammenarbeit mit dem Amazon Store musste Canonical nach harscher Kritik teilweise zurücknehmen. Partnerschaften mit den „Amazon Web Services“ und Microsofts Cloud „Azure“ sind zwar erfolgreich, aber für die reine Linux-Lehre ein Ausverkauf an Monopolkapitalisten. Dass neuerdings Ubuntu als Subsystem unter Windows arbeitet und sogar im Windows Store erhältlich ist, passt für Linux-Ideologen ins böse Bild.

Geht’s auch ohne Ubuntu? Etwa mit der Debian-Mutter oder dem Ubuntu-Abkömmling Linux Mint, der ja schon als alternative Linux Mint Debian Edition (LMDE) vorliegt? Wer so denkt, unterschlägt großartige Leistungen von Ubuntu: Der Installer Ubiquity hat Standards gesetzt, vor denen so mancher gruselige Linux-Installer deutlich abfällt. Der Ubuntu-Erscheinungszyklus mit LTS-Versionen alle zwei Jahre (und fünf Jahren Support) bringt Nachhaltigkeit für Server und Desktop. Die Softwareverteilung gewinnt durch Canonicals Launchpad.net und das Snappy-Format bietet erhebliche Freiheiten. Nicht zuletzt steht hinter Ubuntu eine große Community, die mit *ubuntu users.de* eine der besten Linux-Informationsquellen überhaupt pflegt.

Wer gar – mit Hinweis auf das generell zweifelhafte Ranking von Distrowatch – das

schon angesprochene Linux Mint gegen Ubuntu ausspielen will, ist ein Milchmädchen: Dort liegt Mint zwar scheinbar vor Ubuntu, aber nur deshalb, weil diese Liste die Ubuntu-„Flavours" einzeln abbildet. Wer die Ubuntus zusammenzählt, was gerecht wäre, hat einen anderen Sieger.

Ubuntu 17.10 und die Heft-Schwerpunkte

Ubuntu bleibt relevant und wie es mit Version 17.10 seine Rückkehr zum Gnome-Desktop absolviert, lesen Sie ab Seite 16, Infos zu weiteren Ubuntu-Varianten gibt es ab Seite 10.

Die großen Themen in diesem Heft gehen aber in andere und technisch anspruchsvolle Richtungen:

Das erste Special bringt Grundlagen und Optimierungstipps für die **Webserver Apache und Nginx.**

Ein zweiter Schwerpunkt legt die Grundlagen der Systemvirtualisierung und bringt praxisnahe Komplettratgeber zu den Virtualisierern **Vmware und Virtualbox.** Außerdem finden Sie hier einen Ratgeber zum **Multiboot von Linux-Systemen.**

Ein drittes Special benennt und bewertet alle prominenten Verschlüsselungsmethoden unter Linux und erklärt den praktischen Alltag mit **Luks, Ecrypt FS, Enc FS, Veracrypt, Gnu PG, 7z.**

Die Multiboot-DVD

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 rechts oben) 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 installierte Betriebssystem. Dies gilt natürlich dann nicht mehr, wenn Sie aus dem Livesystem die Installation starten.

Alle Systeme liegen auch als ISO-Images auf der DVD vor (unter „Image-Dateien") und lassen sich auf eigene CD/DVDs oder USB-Sticks schreiben. Technisch notwendig ist dies, wenn ein System im Uefi-Modus installiert werden muss. ■

So startet die Heft-DVD: Die angezeigten Livesysteme sind startklar auf DVD. Die Ubuntu-Varianten, Antergos und Open Suse bieten die Installation aus dem Livesystem. Porteus und Gparted Live sind reine Livesysteme.

Mehr Linux-Know-how auf Heft-DVD: Neben dem E-Book mit Linux-Grundlagen finden Sie alle sechs LinuxWelt-Ausgaben des Jahres 2017 auf dem Begleitmedium.

AUF DVD

10 Ubuntu Mate 17.10 *(64 Bit)*
Ubuntu mit Mate-Desktop

11 Ubuntu Budgie 17.10 *(64 Bit)*
Ubuntu mit Budgie-Desktop

12 Lubuntu 17.10 *(32 Bit))*
Ubuntu mit LXDE-Desktop

13 Open Suse Tumbleweed *(64 Bit)*
Aktuellster Open-Suse-Zweig

14 Antergos 17.10 *(64 Bit)*
Arch Linux mit grafischem Installer

15 Porteus 3.2.2 *(32 Bit)*
Zweitsystem mit Browserauswahl

15 Gparted Live 0.30 *(32 Bit)*
Livesystem mit Partitionierer

16 Ubuntu 17.10 *(64 Bit)*
Ubuntu-Standardausgabe mit angepasstem Gnome-Desktop

1000 Seiten Linux-Wissen
LinuxWelt-Jahrgang 2017 als PDF
Linux-Grundlagen im PDF-Booklet

Software für ISO-Abbilder
Imgburn, Win 32 Disk Imager, Unetbootin zum Kopieren von Linux-Abbildern

„Extras und Tools"
Boothelfer und Hardwareanalyse: Supergrub, Memtest, HDT

Ubuntu Mate 17.10

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 17.10 (64-Bit-Version auf Heft-DVD) mit interessanten Neuerungen.

VON DAVID WOLSKI

Ubuntu Mate 17.10 ist nicht weniger als die bisher wichtigste Ausgabe dieser offiziellen Ubuntu-Variante. So die Ankündigung der Entwickler des besonders einsteigerfreundlichen Linux-Systems.

Die Ubuntu-Variante bleibt zwar ihrem Konzept und dem Mate-Desktop treu, geizt aber nicht mit interessanten Neuerungen, die dem Desktop eine erfreuliche Anpassungsfähigkeit verleihen. Ubuntu Mate wird damit zu einem attraktiven System für jene Anwender, die bereits jetzt schon den Unity-Desktop vermissen. Denn einige der Vorzüge der eingestellten Desktopumgebungen hat das neue Ubuntu Mate übernommen oder geschickt mit anderen Mitteln nachgebaut.

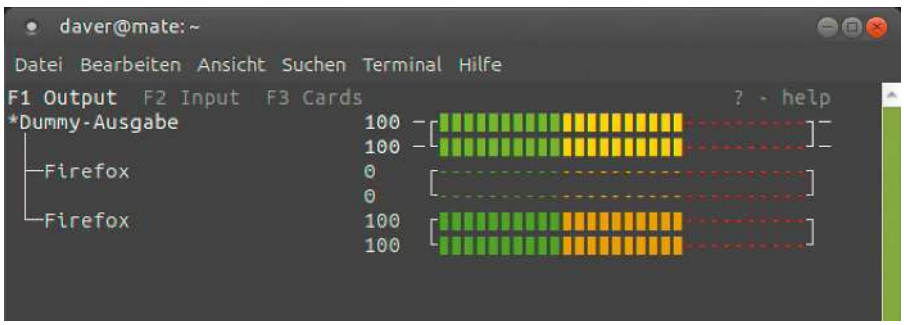
Zuvorkommend: Der Willkommensbildschirm von Ubuntu Mate zeigt nicht nur Infos, sondern führt auch gleich zur Programmauswahl über die bequeme „Software-Boutique“.

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 zeigt gleich die „Software Boutique“, um bei Bedarf populäre Programmpakete mit wenigen Klicks nachzurüsten.

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 ist 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.



Mixer in der Kommandozeile: Dieses Programm ist als Snappaket vorinstalliert. Ubuntu Mate ist damit die erste Ubuntu-Variante, die dafür das neue Paketformat nutzt.

Anwendungen als Snappaket

Ubuntu Mate bringt eine Softwareausstattung, die für den Gnome-Desktop typisch ist. Standardmäßig an Bord sind Firefox 56, Libre Office 5.4, Thunderbird 45.8 inklusive der Kalenderanwendung Lightning. Der Musikplayer ist Rhythmbox 3.4.1 und für Videos und Filme ist VLC 2.2.6 zuständig. 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. Als erste Ubuntu-Version liefert diese Distribution bereits ein vorinstalliertes Snappaket mit: Es handelt sich um die Terminalanwendung „pulsemixer“, die einen Lautstärkeregler für Pulse Audio anzeigt. ■

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

Ubuntu Budgie 17.10

Viel Feinschliff ging in den Desktop von Ubuntu Budgie 17.10 (64-Bit-Version auf Heft-DVD). Im Kreis der offiziellen Ubuntu-Varianten ist Budgie der jüngste Zugang, der sich als weitere Alternative zum Gnome-Desktop positioniert.

VON DAVID WOLSKI

Ubuntu Budgie ist erst seit der letzten Version 17.04 vom April in den Zoo der regulären Ubuntu-Distributionen aufgenommen worden. So wie bei Gnome und Unity handelt es sich auch bei Budgie um einen Desktop mit dem GTK3-Framework. Allerdings folgt Budgie einem traditionellen Aufbau mit aufklappendem Anwendungsmenü und einem Dock (Plank), das auch als Taskleiste dient.

Der Budgie-Desktop entstand zunächst als Teil der unabhängigen Linux-Distribution Solus und ist eine Neuinterpretation von Gnome 3, die schnell viele Freunde gefunden hat. Eine Portierung zu Ubuntu ließ deshalb auch nicht lange auf sich warten und Ubuntu-Gründer Mark Shuttleworth äußerte den Wunsch, aus dem zunächst inoffiziellen „Budgie Remix" möglichst schnell ein reguläres Ubuntu zu machen.

Alternative zu Gnome: Wem Ubuntu mit Gnome nicht zusagt, bekommt mit dem Budgie-Desktop eine verwandte Arbeitsumgebung, die auf traditionelle Desktopelemente setzt.

Von Ubuntu Mate inspiriert

Auch Ubuntu Budgie zeigt nach erfolgter Installation ein Willkommensfenster an, das jetzt größtenteils nach Deutsch übersetzt ist. Es zeigt Abkürzungen zu den ersten Schritten, die üblicherweise nach der Ubuntu-Installation fällig sind: Unter „Updates und Extras" installiert eine Option gleich weitere Codecs und Schriftarten, „Treiber" öffnet die Suche nach benötigten proprietären Hardwaretreibern und die „Browser-Auswahl" erlaubt den Wechsel des Webbrowsers. Vorinstalliert ist Chromium, aber das ist hier mit wenigen Klicks geändert.

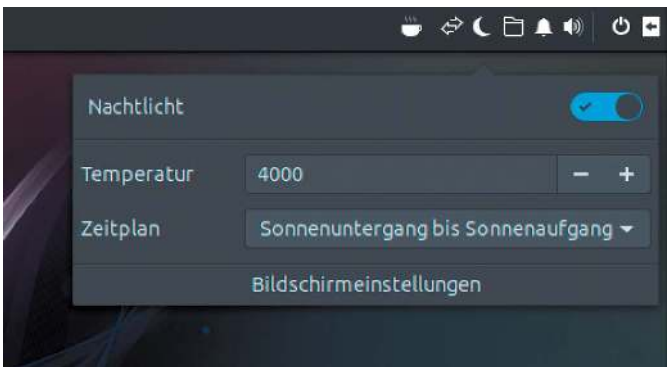
Der Desktop ist darauf ausgelegt, den Platz auf dem Bildschirm möglichst effizient zu nutzen. Rechts gibt es eine großzügige Seitenleiste für Applets, die ein Klick auf das Pfeilsymbol rechts oben einblendet. Neu ist in Ubuntu Budgie das Applet Nachtlicht, das die Farbtemperatur des Desktops abhängig von der Tageszeit regelt, um bei langen Arbeiten die Augen zu schonen. Außerdem gibt es mit Caffeine ein Applet, das den Bildschirmschoner per Klick deaktiviert – nützlich ist das insbesondere, wenn der PC als Mediaplayer dient.

Vorinstallierte Programme

Die mitgelieferten Standardprogramme von Ubuntu Budgie entsprechen bis auf einige Ausnahmen jenen von Gnome 3.26 mit Nautilus als Dateimanager, dem Texteditor Gedit und Rhythmbox als Videoplayer. Das Konfigurationsangebot der zentralen „Systemeinstellungen" ist mit jenem von Gnome identisch. Als Terminalanwendung bevorzugt Budgie das fortgeschrittene Programm Tilix, dessen Fenster sich in mehrere Sitzungen aufteilen lässt. Tilix steht auch über die Taste F12 bereit.

Als Office-Anwendung dient Libre Office 5.4 und um die Installation weiterer Software kümmert sich „Ubuntu Software" als grafischer Paketmanager. ■

Website: *https://ubuntubudgie.org*
Dokumentation: *https://ubuntubudgie.org/about*



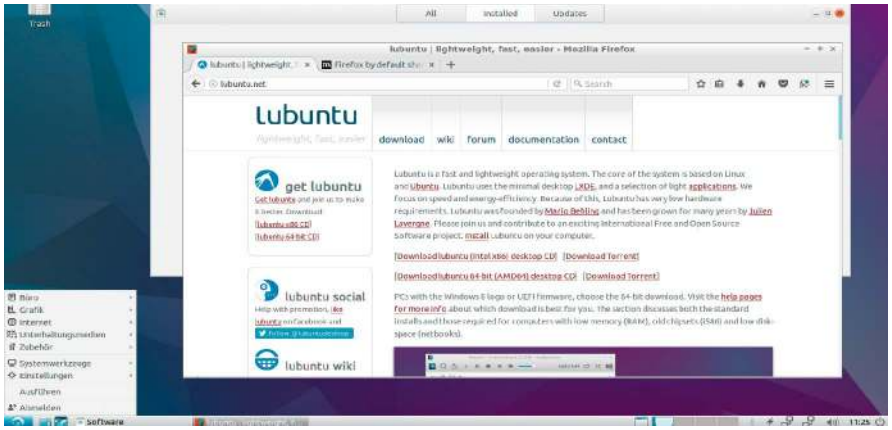
Nachtlicht wie in Gnome 3.26: Dieses Applet passt die Farbtemperatur der Bildschirms an die Tageszeit an und sorgt nachts für einen höheren Rotanteil.

Lubuntu 17.10

Ein echtes Leichtgewicht: Lubuntu ist ein aktuelles Ubuntu 17.10 mit LXDE als Arbeitsumgebung. Diese offizielle Ubuntu-Variante ist stets eine gute Wahl für ältere PCs. Deshalb liegt die Distribution in der 32-Bit-Version auf Heft-DVD.

VON DAVID WOLSKI

Die Ubuntu-Variante mit LXDE ist seit langem ein sicherer Hafen für Umsteiger und Einsteiger, die einen älteren Rechner noch eine Weile betreiben wollen und dazu eine möglichst ressourcenschonende Arbeitsumgebung benötigen. Der hier verwendete Desktop LXDE ist schon mit einem GB Speicher zufrieden und folgt einem traditionellen Aufbau mit Arbeitsfläche, Anwendungsmenü und gewohnter Taskleiste mit Infobereich. Damit kommt jeder Anwender klar. LXDE stellt dabei nur die Basisbestandteile für eine Desktopumgebung bereit. Als Window-Manager dient das besonders schlanke Openbox. Alle weiteren Anwendungen sind von Gnome und XFCE übernommen, wobei man auch beliebige Programme aus dem Ubuntu-Fundus nachrüsten kann. Dies klingt nach Stückwerk, aber dem Entwicklerteam ist es seit der ersten Version vor über vier Jahren gelungen, einen konsistenten und ansehnlichen Desktop aus den Komponenten um LXDE zu gestalten. Bei den vorinstallierten Programmen haben sparsame Alternativen stets den Vortritt: Lubuntu verzichtet auf eine ausgewachsene Office-Suite, um stattdessen Abiword und Gnumeric anzubieten. Libre Office 5.4 lässt sich natürlich auch installieren.



Wie aus einem Guss: LXDE besteht aus einer Mischung verschiedener Desktopkomponenten. Dies sieht man Lubuntu und seiner Arbeitsumgebung aber nicht an.

Die nachträgliche Ergänzung von Programmen für den PC-Alltag ist bei Lubuntu generell ein Muss, denn die vorhandene Programmauswahl ist bis auf Firefox zu sparsam, um damit im Alltag arbeiten zu können. Zumindest Libre Office, VLC als Videoplayer und einen bequemen Dateimanager wie Thunar oder Nemo sollte man installieren. Nach der Einrichtung auf Festplatte mit dem komfortablen Ubuntu-Installer benötigt die auf DVD vorliegende 32-Bit-Version lediglich fünf GB. ■

Website: *http://lubuntu.net*
Dokumentation: *https://wiki.ubuntu.com/Lubuntu*

AUSBLICK AUF LUBUNTU NEXT

Lubuntu steht vor einem Wechsel der Desktopumgebung, denn LXDE soll in naher Zukunft vom ebenfalls schlanken Nachfolger LXQT abgelöst werden. LXQT wird aber bei seinen Desktopelementen wie KDE Plasma 5 das Toolkit Qt einsetzen und damit ein Stück ansehnlicher ausfallen als LXDE. Die Macher Lubuntus bereiten den Umstieg bereits seit 2014 vor, warten aber geduldig, bis LXQT bis ins Detail ausgereift ist. In Lubuntu 17.10 hat es die neue Desktopumgebung deshalb noch nicht geschafft. Es gibt aber bereits eine separate Ausgabe der Distribution mit dem Namen Lubuntu Next. Dieses Linux-System eignet sich laut Entwickler noch nicht für den produktiven Einsatz. Neugierige können es aber bereits in einem installierbaren Livesystem ausprobieren. Lubuntu Next steht unter *http://cdimage.ubuntu.com/lubuntu-next/daily-live/pending* als ISO-Datei zum Download bereit (32 und 64 Bit; ca. 1,2 GB).

Die Arbeitsfläche von LXQT: Der LXDE-Nachfolger hat wegen des verwendeten Toolkits Qt mehr mit KDE Plasma 5 gemein und gibt vielen KDE-Programmen den Vorzug.

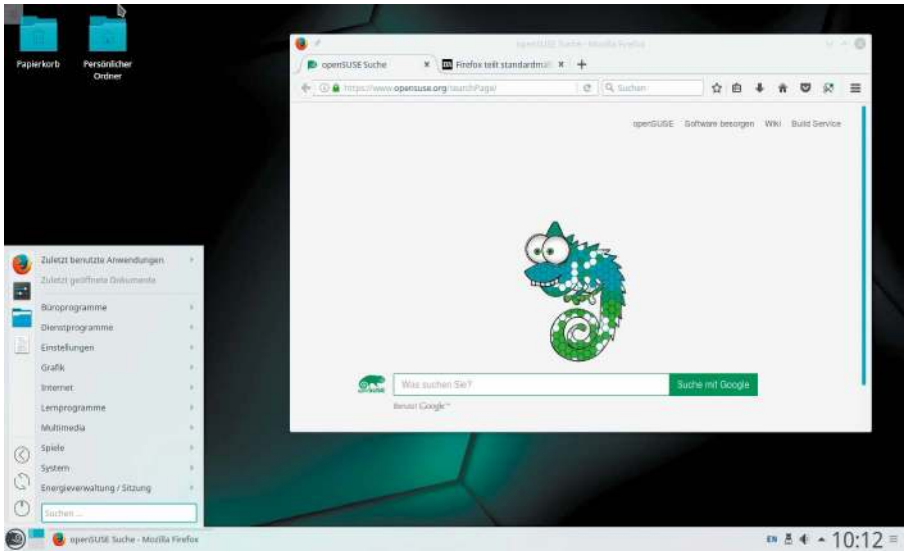
Open Suse Tumbleweed

Es gibt Open Suse auch weiterhin als installierbares Livesystem. Der Distributionszweig Tumbleweed (in 64 Bit auf Heft-DVD) richtet Fortgeschrittenen ein laufend aktualisiertes Open-Suse-System mit besonders frischen Paketen ein.

VON DAVID WOLSKI

Tumbleweeds sind Gräser und Steppenläufer, die der Wind mal hierhin, mal dorthin weht. Auch Open Suse Tumbleweed ist stets in Bewegung, da hier die neuesten, nicht immer ausgiebig getesteten Programmpakete ankommen. Es handelt sich um einen eigenen Distributionszweig für Fortgeschrittene, vergleichbar mit Debian Sid und ebenfalls als Rolling Release konzipiert. Diesen Zweig gibt es schon seit Open Suse 11.4, setzte damals aber voraus, dass die eingetragenen Repositories in einer aufwendigen Bastelaktion manuell auf die Tumbleweed-Paketquellen geändert werden. Gerade bei der Verwendung zusätzlicher Paketquellen gelang diese Umstellung nicht immer reibungslos.

Solcher Aufwand ist bei dieser Open-Suse-Ausgabe nicht nötig: Open Suse Tumbleweed richtet automatisch diese alternativen Repositories ein, die größere Versionssprünge und Aktualisierungen auf Lager haben.



Frisches Plasma für Open Suse: Anders als die reguläre Ausgabe ist Tumbleweed als Rolling Release konzipiert und lässt sich, einmal installiert, über den Paketmanager aktuell halten.

Immer in Bewegung

Der Zweig ist Teil der neuen Formel von Open Suse: Unter der Oberfläche setzt die reguläre Ausgabe der Distribution (Open Suse Leap) auf ältere, besonders stabile Pakete vom Serversystem Suse Linux Enterprise. Tumbleweed ist dagegen das Reagenzglas, in dem aktuelle Softwarepakete liegen. Das macht diese Version von Open Suse interessant für jene Anwender, die nicht auf ausführlich getestete Software pochen, sondern stattdessen aktuelle Pakete bevorzugen. Der Kernel ist hier beispielsweise schon in Version 4.13 vorhanden, während er in Open Suse Leap zurzeit noch bei Version 4.4 steht.

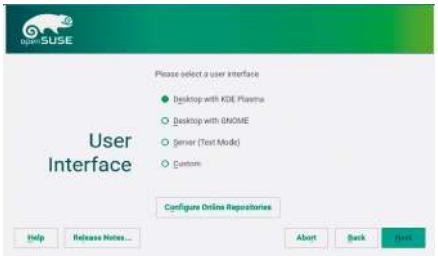
Die Arbeitsumgebung von KDE Plasma 5.11 ist derzeit einer der Desktops von Tumbleweed. In Open Suse Leap muss man noch mit KDE Plasma 5.8 Vorlieb nehmen. Die neuen Pakete machen die Distribution aber auch anspruchsvoller: Es gibt einzelne vorübergehende Ungereimtheiten auf dem Desktop, wenn dieser nach Updates einen größeren Versionssprung getan hat.

Proprietäre Nvidia-Treiber

Die Installation proprietärer Nvidia-Treiber war in Open Suse Tumbleweed immer vergleichsweise hakelig: Es gab keine fertigen Treiberpakete und die Grafiktreiber mussten aus den Quellen des Herstellers kompiliert werden. Weil es vergleichsweise häufig Kernel-Updates für diese Distribution gibt, stand dieser aufwendige Schritt häufig an. Die Open-Suse-Entwickler haben dieses Problem Ende September entschärft und für Tumbleweed ein eigenes Nvidia-Repository erstellt, in welchem die fertig kompilierten Treiber als RPM-Paket liegen (*https://download.nvidia.com/opensuse/tumbleweed*). Das Repository findet sich in Tumbleweed nicht in den Standard-Paketquellen, ist aber schnell über seine URL in Yast aufgenommen.

Das grafische Konfigurationstool Yast übernimmt, wie seit Jahren in Open Suse gewohnt, die Installation und die Administration des Linux-Systems. Open Suse startet von Heft-DVD mit KDE-Desktop, kann aber auch Gnome 3.26 installieren. Yast bietet dazu ein Auswahlmenü für die gewünschte Desktopumgebung an. ■

Website: *https://en.opensuse.org/openSUSE:Tumbleweed_installation*
Dokumentation: *https://en.opensuse.org/Portal:Tumbleweed*



Desktops zur Auswahl: Neben KDE Plasma 5.11 gibt es auch Gnome 3.26 zur Installation. Weitere Optionen wie LXDE und XFCE finden sich unter „Custom“.

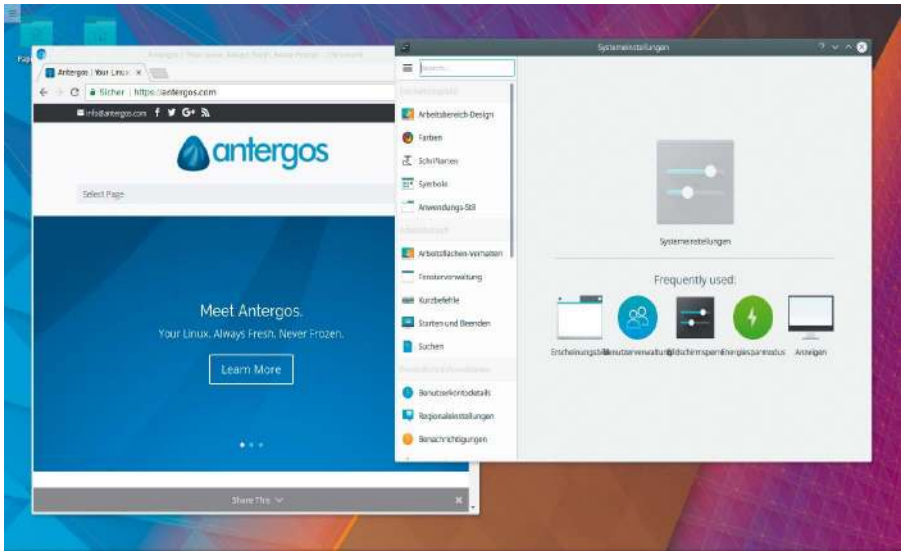
Antergos 17.10

Ist Arch Linux tauglich für den Desktopalltag? Fortgeschrittenen Freunden des Linux-Desktops will Antergos 17.10 (für 64-Bit-PCs auf Heft-DVD) das beweisen. Es präsentiert Arch als Livesystem mit grafischem Installationsprogramm.

VON DAVID WOLSKI

An Arch-Abkömmlingen gibt es derzeit keinen Mangel: Manjaro, Chakra und Archlabs buhlen um die Gunst der Arch-Anwender. Und diese immer noch kleine Zielgruppe wächst seit Jahren beständig. Antergos bleibt nah an Arch Linux und nutzt dessen Paketquellen. Die Distribution öffnet mit ihrem grafischen Installer Cnchi aber auch weniger erfahrenen Anwendern einen Zugang zu Arch, die mit der größtenteils manuellen Einrichtung eines puren Arch Linux überfordert wären.

Das Resultat ist immer noch ein echtes Arch Linux mit vielen seiner Vorzüge: Die Pakete sind stets sehr aktuell, denn das Paketformat von Arch erlaubt es den Entwicklern, fertige Pakete ohne großen Aufwand aus dem Quellcode von Programmen zu erzeugen. Als Rolling Release lässt sich die Distribution allein über den Paketmanager aktuell halten und bleibt, einmal installiert, über Jahre ohne aufwendige Neuinstallation frisch. Der Unterschied zu Arch-Varianten wie Manjaro ist, dass Antergos die originalen Repositories von Arch nutzt.



Arch Linux mit komfortablen Ergänzungen: Der Installer ist einer der schnellsten Wege zu einem fertig eingerichteten Arch-System. Aktuelle Desktops wie KDE Plasma 5.11 stehen bereit.

Desktops zur Auswahl

Es stehen bei der Installation gleich mehrere Desktops in ihren neuesten Versionen zur Auswahl: Gnome 3.26, KDE Plasma 5.11, Cinnamon 3.2, Mate 1.20, XFCE 4.12, aber auch Openbox und Deepin aus dem chinesischen Ubuntu-Derivat Kylin bietet der Installer an. Es empfiehlt sich, das System gleich auf der Einstellungsseite des Installationsprogramms anzupassen. Hier kann man den Webbrowser auswählen, Libre Office mitinstallieren, externe Repositories (AURs) aktivieren, Steam installieren und den SSH-Dienst sowie die Firewall bei Bedarf einschalten.

Eine sinnvolle Option für Desktopanwender ist der Punkt „Kernel (LTS Version)“. Ist sie aktiviert, dann arbeitet Antergos mit einem bewährten Kernel mit Langzeitunterstützung, was den Administrationsaufwand des Systems senkt.

Angebotene Arbeitsflächen: Der Installer Cnchi erweitert die Auswahl der Desktops. Die Pakete werden erst beim Installationsprozess heruntergeladen.

Einfacher als pures Arch

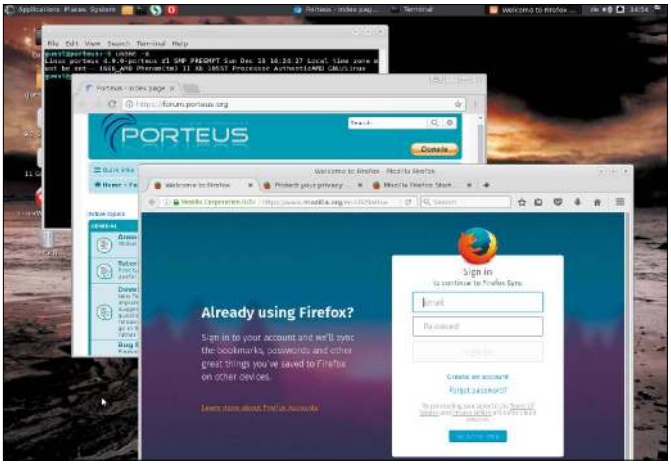
Für das Paketmanagement steht auf dem Desktop das grafische Tool Pamac zur Verfügung und auf der Kommandozeile das traditionelle Arch-Tool pacman. Wie Arch Linux verzichtet auch Antergos ansonsten auf grafische Werkzeuge zur Systemadministration. Ein gewisses Interesse an den tieferen Funktionsweisen eines Linux-Systems und entsprechende Grundkenntnisse sind unerlässlich, um diese Distribution auf lange Sicht zu betreiben.

Wer sich allerdings die Mühe macht, bekommt ein stets sehr aktuelles Linux-System, unter dem vieles einfacher geht als in einem puren Arch Linux. Generell bleibt es aber wichtig, Arch-basierte Systeme regelmäßig mit Updates zu versorgen: Ein Arch-System, das einige Monate keine Aktualisierungen bekommen hat, verlangt beim nächsten großen Update umso mehr Nacharbeiten. ■

Website: *http://antergos.com*
Dokumentation: *http://wiki.antergos.com*

Porteus 3.2.2

VON DAVID WOLSKI

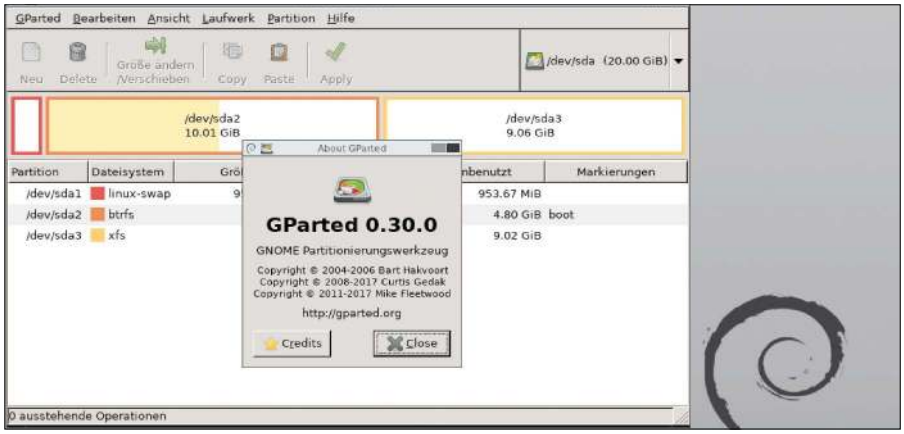


Kein umfangreiches Livesystem mit großer Softwareauswahl, sondern ein schlankes Surfsystem: Porteus hat nicht den Anspruch, eine möglichst komplett eingerichtete Arbeitsumgebung zu starten, sondern ist ein flott startendes Zweitsystem. In seiner Basisvariante ohne Extras ist Porteus ein besonders kleines, erweiterbares Slackwaresystem. In der angepassten LinuxWelt-Version hat Porteus 3.2.2 (in 32 Bit auf Heft-DVD) bereits die Browser Firefox 45.2 ESR, Chromium 55 und Opera 45 an Bord. Für ein Surfsystem ist diese Auswahl an Webbrowsern einmalig. Alle drei sind mit einem Flash-Plug-in ausgestattet und finden sich im Menü „Applications -> Internet“. Chromium erwartet beim ersten Aufruf noch die Vergabe eines optionalen Passworts für seinen verschlüsselten Passwortspeicher, der im Livesystem nicht permanent ist. In dieser Porteus-Edition ist die deutsche Tastaturbelegung bereits voreingestellt, das System selbst liegt in Englisch vor. Die Übertragung auf USB-Stick gelingt im Livesystem mit dem Installer unter „System Tools -> Create live USB“. Um weitere Programme zur Laufzeit zu installieren, hat Porteus einen Paketmanager im Anwendungsmenü unter „Applications -> System Tools -> USM (Unified Slackware Package Manager)“. Der Kernel des Systems ist auf Version 4.9 aktualisiert und auch für Intel-CPUs der Generation Skylake und Kaby Lake neu genug. Im Livebetrieb ist der angemeldete Standardbenutzer „guest“ und hat das Passwort „guest“. Dieses wird zur Rückkehr vom Bildschirmschoner zum Desktop abgefragt. Das root-Passwort lautet „toor“ und wird vom Paketmanager benötigt. ■

Website: *www.porteus.org*
Dokumentation: *www.porteus.org/info.html*

Gparted Live 0.30

VON DAVID WOLSKI



Egal ob Linux oder Windows: Gparted Live ist ein universell nützliches Livesystem mit dem mächtigen Partitionierer Gparted 0.30 im Mittelpunkt. Gparted eignet sich bestens zur Neupartitionierung, Partitionsänderung und Formatierung von Festplatten. Gparted ist zwar bei vielen Livesystemen an Bord, hier aber startet es sofort und liegt in einer frischen Version vor, da es das offizielle Livesystem der Gparted-Entwickler ist. Es unterstützt eine grandiose Anzahl von Dateisystemen und Partitionstabellen aus dem Umfeld von Linux, Unix und Windows. Neben allen Linux-Dateisystemen wie BTRFS, Ext3, Ext4, XFS, JFS, F2FS und ReiserFS kann es auch NTFS (Windows) und HFS/HFS+ (Mac) bearbeiten. In der Version 0.30 aktualisiert Gparted Live seine Pakete und Softwareversionen aus dem Debian-Zweig Sid. Gparted 0.30 kann nun mit Laufwerksnamen im Unicode-Zeichensatz umgehen und verbessert die Kompatibilität mit Windows bei Größenanpassungen von FAT32-Laufwerken. Das auf Heft-DVD vorliegende 32-Bit-System läuft ohne Einschränkungen auch auf 64-Bit-PCs. Dank dem frischen Kernel 4.13 startet Gparted Live jetzt auch auf Intels neuester Chipgeneration Kaby Lake und auf Rechnern mit AMDs Ryzen-Prozessor. Nach dem Start des Livesystems muss noch eben die deutsche Tastaturbelegung über „Select keymap from arch list“ ausgewählt werden. Der Partitionierer Gparted startet automatisch. ■

Website: *http://gparted.org/livecd.php*
Dokumentation: *http://gparted.org/faq.php“*

Das neue Ubuntu 17.10

Ubuntus turnusgemäße, halbjährliche Zwischenversionen richten sich insbesondere an Ubuntu-Fans, die keinen Zwischenschritt auslassen möchten. Die aktuelle Version 17.10 verdient aber schon deshalb genaueres Hinsehen, weil sie eine Wende einläutet.

VON HERMANN APFELBÖCK

Canonical hat Ubuntu 17.10 („Artful Aardvark“) am 19. Oktober 2017 veröffentlicht. Es ist der letzte Zwischenschritt vor der wieder eminent wichtigen LTS-Version 18.04 mit fünf Jahren Support, die im April 2018 erscheinen wird. Ubuntu 17.10 erhält nur die für Zwischenversionen typischen neun Monate Support, kann aber im Juli 2018 oder schon ab April 2018 auf den Nachfolger 18.04 aktualisiert werden. Auf dem gleichen Weg (über „Anwendungen & Aktualisierungen“) ist es zum jetzigen Zeitpunkt möglich, ein bestehendes Ubuntu 17.04 auf das jüngste 17.10 zu hieven.

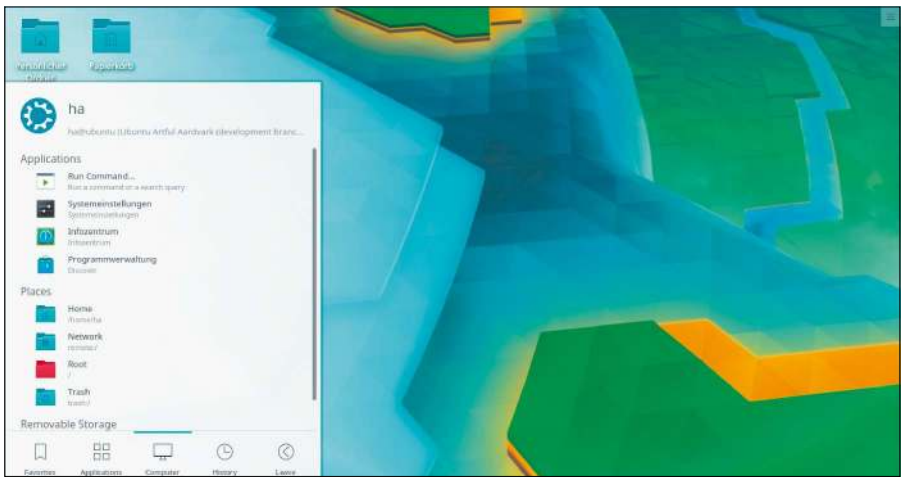
Das alles sind Ubuntu-Standards, die seit Jahren gelten und die Zwischenversionen attraktiver machen, insofern sie nicht als kurzfristige Einbahnstraßen enden. Dennoch ist eine Version 17.10 in erster Linie ein Fanartikel, der weder für Serverinstallationen noch für Desktopeinsteiger empfehlenswert oder notwendig wäre. Wer Ubuntu 17.10 testen oder installieren möchte, findet auf der Heft-DVD die Livesysteme mit Installationsoption folgender Desktop-„Flavours“:

- **Ubuntu 17.10 Standardedition** mit Gnome (64 Bit)
- **Ubuntu 17.10 Mate** (64 Bit)
- **Ubuntu 17.10 Budgie** (64 Bit)
- **Lubuntu 17.10 mit LXDE** (32 Bit)

Die weiteren prominenten Ubuntu-Editionen mit KDE (Kubuntu) und XFCE (Xubuntu) gibt es auf den jeweiligen Projektseiten zum Download (*https://kubuntu.org/*, *https://xubuntu.org/*). Für das noch experimentelle Ubuntu Next mit modernem LXQT, das im nächsten Jahr das bisherige Lubuntu ablösen soll, war bei Redaktionsschluss noch keine offizielle Downloadseite zu ermitteln.

Basisänderungen in den Ubuntu-Varianten

Jedes Ubuntu 17.10 basiert auf dem aktuellen Linux-Kernel 4.13 vom September



Wenig Neues in Kubuntu 17.10: Die Editionen Kubuntu, Xubuntu und Lubuntu bringen nicht viel mehr als den aktuelleren Kernel und frische Paketversionen.

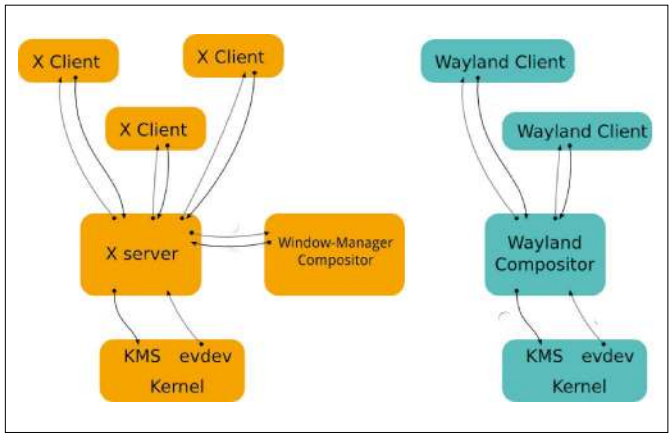
2017. Dies verspricht Hardwareunterstützung durch neue Kernel-Treiber für neueste CPUs, AMD-GPUs und weitere Hardware. Nebenbei bringt Kernel 4.13 Verbesserungen für Samba und Ext4-Dateisysteme mit. Selbstverständlich werden ferner zahlreiche Programmversionen auf den aktuellen Stand gehievt. So liegt Libre Office, sofern in der jeweiligen Edition enthalten, in der aktuellsten Version 5.4 vor. VLC (2.2.6), Rhythmbox (3.4.1), aber auch Zubehör wie der Editor Gedit (3.22.1) oder Dateimanager Nautilus (3.26) sind auf dem neuesten Stand. Browser Firefox (55.0) und Mailclient Thunderbird (45.8) sind aufgrund der häufigen Sicherheitsupdates typischerweise nicht auf dem allerneuesten Stand, was zur üblichen Pflicht aufruft, das System mit

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

umgehend zu aktualisieren.

Alle weiteren Neuerungen gelten bereits nicht mehr allgemein, sondern für die jeweiligen Ubuntu-Editionen. So will Canonical die 32-Bit-Varianten seiner Ubuntus gerne loswerden, geht diesen Schritt aber vorerst allein bei der Hauptversion (mit Gnome). Die übrigen „Flavours" einschließlich Kubuntu und Budgie bleiben weiterhin auch in 32 Bit verfügbar. Und selbst die Hauptversion, die kein 32-Bit-Installationsmedium mehr bietet, lässt sich über ein Distributionsupgrade der Vorversion 17.04 noch als 32-Bit-Ausführung installieren (sofern die Vorversion in 32 Bit vorliegt).

Der Displayserver Wayland: Den Umstieg vom alten X11-Display-Server (Xorg) zum neuen Wayland hat Ubuntu 17.10 längst nicht in umfassender Weise vollzogen. Von allen Varianten, die uns (bei Redaktionsschluss allerdings noch als Beta) vorlagen, nutzt lediglich die Hauptversion mit Gnome den neuen Wayland-Grafikserver, alle anderen weiterhin das alte X11. Und selbst bei dieser Hauptversion kann der User über das Zahnrad neben der „Anmelden"-Schaltfläche zwischen „Ubuntu" (mit Wayland) und „Ubuntu on Xorg" wählen, um eventuellen Kompatibilitätsproblemen aus dem Weg zu gehen. Im laufenden Betrieb konnten wir keinen signifikanten Unterschied zu einer X11-basierten Anzeige feststellen – was zunächst zu begrüßen ist und für den reibungslosen Einbau von Wayland in Gnome spricht. Punktuelle Nachteile bringt aber Wayland nach wie vor mit sich (dazu unten mehr).



Ebenen des Linux-Desktops: Der einfachere Aufbau von Wayland verkürzt und beschleunigt die Wege der Grafikausgabe gegenüber einem herkömmlichen X11 (links).

Warum überhaupt Wayland? Das aus den 80er-Jahren stammende X-Window-System X11 ist ein relativ komplexes Client-Server-Konstrukt. Die grafischen Linux-Programme kommunizieren nämlich nicht direkt mit X11, sondern über einen Window-Manager und einen Compositor, die ihrerseits Kontrollelemente, Fonts und Effekte auf den Bildschirm bringen. Dass diese Komplexität nicht zu sichtbaren Leistungseinbußen führt, ist allein der Leistungsfähigkeit moderner PCs zu verdanken.

Wayland verspricht schnellere Grafikdarstellung, flüssige Videos und Touchbedienung vor allem auch für schwächere Hardware mit ARM-Prozessoren.

Denn Wayland verkürzt und vereinfacht grafischen Programmen den Weg auf den Bildschirm. Der Compositor, den die Desktopumgebung stellt, kommuniziert hier direkt mit Wayland.

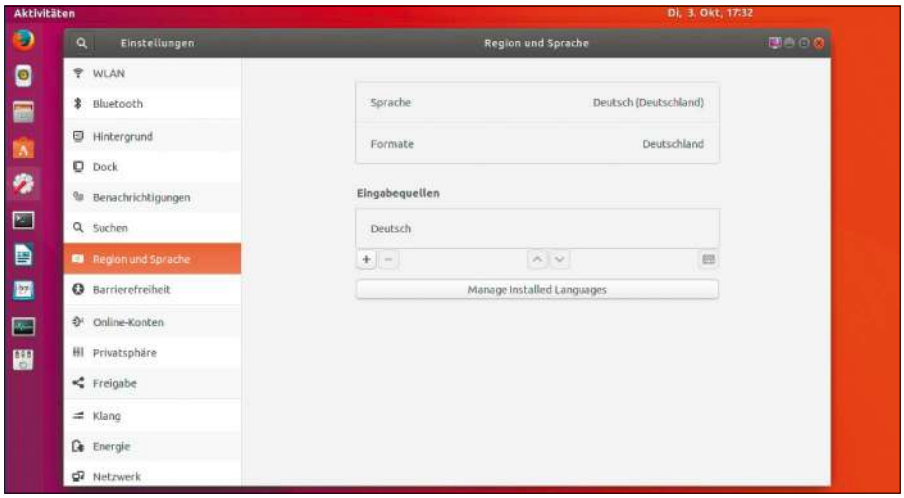
Die Umstellung auf Wayland ist keine Aufgabe der Anwendungsentwickler: Stattdessen ist es die Aufgabe der jeweiligen Desktopumgebung, Window Manager und Compositor auf Wayland zu trimmen. Ein Gnome-Programm, das mit dem GTK-Toolkit geschrieben ist, muss sich um Wayland nicht kümmern, denn das erledigt Gnome selbst. Und für Programme, die ihr eigenes Toolkit mitbringen, gibt es eine Kompatibilitätsschicht namens Xwayland.

Ubuntu 17.10 spiegelt den aktuellen Stand hinsichtlich Wayland: Sowohl Wayland selbst als auch die Integration in die Desktopumgebung befinden sich noch in der Entwicklung. Aktuell ist nur der Gnome-Desktop so weit, Wayland für Produktivsysteme anzubieten, und nur dort ist Wayland in Ubuntu 17.10 standardmäßig aktiv. Auch unter KDE ist dieser Einbau relativ weit gediehen und kann für das kommende Ku-

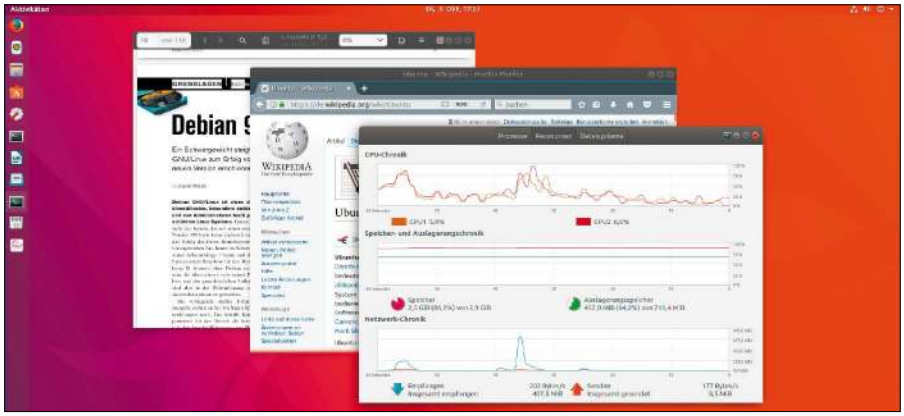
Ubuntu-Hauptausgabe mit Gnome: Bei der Anmeldung kann optional auf das alte X11-Grafiksystem umgeschaltet werden.

buntu 18.04 mindestens als Option erwartet werden. Unter Wayland gibt es nach wie vor gewisse Einschränkungen: So ist die Anzeige grafischer Programme über das Netzwerk via SSH derzeit nicht möglich (das bekannte X11-Forwarding). Auch beliebte Tools wie xprop oder xkill arbeiten unter Wayland nicht oder nicht erwartungsgemäß. Screenshots und Screencasts scheinen inzwischen aber zumindest mit den Gnome-eigenen Programmen wie etwa gnome-screenshot problemlos möglich. Ein schmerzhaftes Defizit ist die Tatsache, dass die zahlreichen beliebten Gnome-Erweiterungen unter *https://extensions.gnome.org* unter Wayland offenbar nicht arbeiten. So zumindest bis zur Betaversion, die wir für diesen Artikel an der Hand hatten.

Generell gilt: Wer Ubuntu mit Gnome und Wayland nutzt, sollte diese Tatsache nicht aus den Augen verlieren. Notfalls hilft das Umschalten auf Xorg (X11) am Anmeldebildschirm.



Gnome-Control-Center mit neuem Layout: Die „Einstellungen“ werden durch die Navigationsspalte übersichtlicher und komfortabler, aber am Umfang hat sich nichts geändert.



Mindestens 4 GB RAM für Standard-Ubuntu mit Gnome: Die hier für eine Betatestinstallation bereitgestellten 3 GB waren stets schnell verbraucht, wenn zwei, drei größere Programme liefen.

Ubuntu 17.10: Hauptausgabe mit Gnome

Ubuntu 17.10 mit Gnome 3.26 liegt in der 64-Bit-Ausgabe auf Heft-DVD. Das System ist relativ speicherhungrig und sollte halbwegs moderne Hardware mit mindestens vier GB Speicher vorfinden.

Gnome 3.x ist für erstaunlich viele Linux-Nutzer ein Hassobjekt. Diesen Desktop wieder als Standard der Ubuntu-Hauptausgabe einzusetzen, ist daher ein gewisses Risiko, kommt aber dem bisherigen und 2017 aufgegebenen Standarddesktop Unity optisch und funktional sicher am nächsten. Canonical hat sich sogar etliche Mühe gegeben, das brandaktuelle Gnome 3.26 so zu modifizieren, dass es beinahe wie ein Unity aussieht:

- Anders als unter originalem Gnome ist die Favoritenleiste hier standardmäßig sichtbar. Das entspricht optisch ganz der bisherigen Unity-Starterleiste.
- Die Gnome-Favoritenleiste ist über „Einstellungen -> Dock“ flexibel auch rechts oder am unteren Bildschirmrand positionierbar, außerdem größenskalierbar. Auch das ist kein Gnome-Standard.
- Die Desktopoberfläche kann standardmäßig als Dateiablage genutzt werden, was man einem normalen Gnome erst über ein Tweak-Tool beibringen muss.

Das gnome-control-center – auf deutschem System schlicht „Einstellungen“ – erhält ein komplett neues Layout. Statt der bisherigen gruppierten Iconsammlung für die Applets gibt es jetzt links eine Navigationsspalte mit den Hauptkategorien. Das ist zwar nicht hübscher, aber deutlich übersichtlicher als vorher, da die Hauptkategorien in der Navigationsspalte immer erreichbar bleiben. Vor allem erspart dieses Layout das umständliche Zurückblättern von einem Unterapplet zur Gesamtübersicht, wenn man weitere Einstellungen vornehmen will.

Für tiefere Gnome-Anpassungen ist traditionell das Zubehör gnome-tweak-tool („Optimierungen“) zuständig, das Ubuntu 17.10 standardmäßig mitliefert. Der Einstellungsumfang hat sich nicht geändert, zur schnellen Orientierung im Praxisalltag bringen wir nachfolgend dennoch die wichtigsten Optionen in Erinnerung:

„Arbeitsoberfläche -> Symbole anzeigen -> AN“ bedeutet, dass der Desktop als Dateiablage genutzt werden kann. Dies ist gleichzeitig Voraussetzung für weitere Einzeloptionen – so die Anzeige des Papierkorbs oder eingehängter Datenträger. Der Desktophintergrund ist hier ebenfalls komfortabel einstellbar: Anders als in den allgemeinen „Einstellungen“ navigiert das Gnome-Tweak-Tool zu einem Bilderordner Ihrer Wahl.

„Fenster -> Knöpfe der Titelleiste -> Platzierung -> Rechts“ befördert die Knöpfe der Programmfenster auf die klassische Seite rechts. Unter „Fensterfokus“ können Sie einstellen, dass ein Fenster bereits bei Mouse-over-Bewegung den Eingabefokus erhält (Modus „Gleitend“). Fenster unter Gnome lassen sich nicht nur an der Titelleiste, sondern an jeder Position verschieben, wenn Sie gleichzeitig die Taste Super (Windows) drücken.

„Obere Leiste -> Anwendungsmenü“: Hier lässt sich das globale Anwendungsmenü (der jeweils im Fokus stehenden Anwendung) im Systempanel abschalten.

Unter **„Startprogramme“** gelingt das Einrichten von Autostarts komfortabler als über das Systemtool „Startprogramme“ (gnome-session-properties). Sie erhalten hier nämlich die komplette Softwareliste unter „/usr/share/applications“ angezeigt und wählen per Mausklick Programme, die nach der Anmeldung automatisch starten sollen.

Unter **„Erweiterungen“** verwaltet das Gnome-Tweak-Tool die Gnome-Extensions. Über „AN“ und „AUS“ schalten Sie installierte Module mit sofortiger Wirkung. Beachten Sie aber eventuelle Einschränkungen unter Wayland (siehe oben).

Ubuntu 17.10 Mate

Die Mate-Edition ist neben der Hauptausgabe die Variante mit den größten Änderungen. Dem sparsamen Desktop angemessen gibt es Ubuntu Mate weiterhin auch in der 32-Bit-Variante. Das auf Heft-DVD angebotene System hat allerdings

64 Bit, kommt aber selbst in dieser Ausführung mit zwei GB RAM aus.

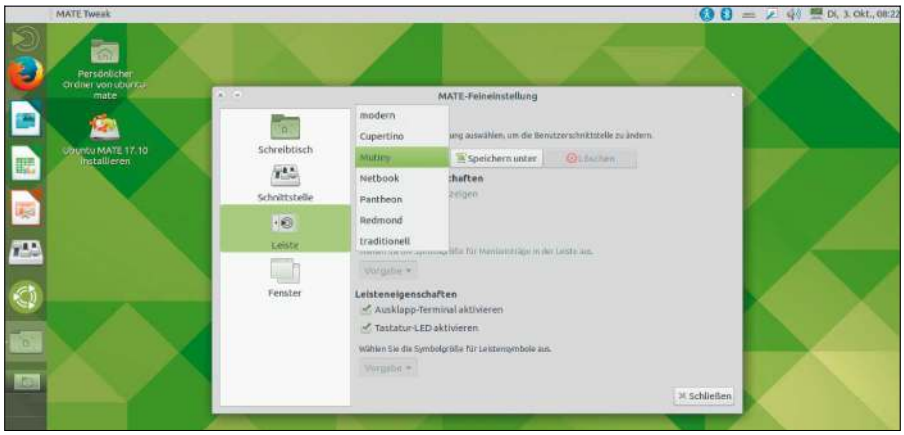
Der vom älteren Gnome 2 abgeleitete Mate-Desktop entwickelt sich immer mehr zum Liebling der Ubuntu-User. Die Oberfläche ist klassisch, aber hervorragend anzupassen und bemüht sich an allen Ecken, Mängel und hinterlassene Lücken anderer Linux-Desktops zu schließen. Das prominenteste Beispiel unter Ubuntu 17.10 sind die Panel-Layouts, die das Bordmittel mate-tweak („Mate-Feineinstellung“) unter dem Punkt „Leiste“ vorsieht. Hier gibt es mehrere Voreinstellungen wie „Cupertino“, „Pantheon“ oder „Redmond“, die jeweils automatisch ein bestimmtes Leistenlayout einrichten.

Für bisherige Ubuntu-Nutzer, die das verstorbene Unity vermissen, bringt das Layout „Mutiny“ größtmögliche Nähe zum bisherigen Ubuntu-Standarddesktop.

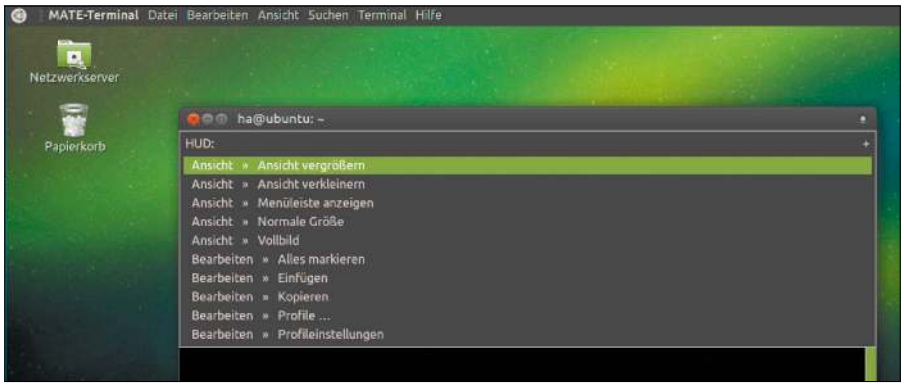
Hübscher fallen allerdings „Cupertino“ und „Pantheon“ aus, die jeweils ein zusätzliches Plank-Dock platzieren. Das Ganze ist keine Zauberei und von einem erfahrenen Anwender in wenigen Schritten ebenso arrangiert, aber doch ein hübscher Service für Einsteiger.

Die Unity-Mimikry unter Mate geht aber noch weiter: An die unter Unity zunächst viel geschmähten globalen Menüs (in der Systemleiste) haben sich inzwischen offenbar viele Nutzer gewöhnt. Die Panel-Vorlagen „Mutiny“ und „Cupertino“ aktivieren daher zusätzlich die globale Menüanzeige. Das Head-up-Display (HUD) wurde bereits seit Ubuntu Mate 16.10 eingeführt, bisher aber wenig überzeugend.

Wie die globalen Menüs ist auch das HUD von bestimmten Leistenlayouts abhängig und funktioniert derzeit unter „Contemporary“, „Cupertino“ und „Mutiny“. Ausgelöst wird die HUD-Befehlsübersicht durch die Taste Alt oder Super-Alt in einer beliebigen Software. Das HUD liefert dann in alphabetischer Sortierung sämtliche Menübefehle, die sich durch Eingabe einiger Zeichen – etwa „med“ im VLC – auf die „Medien“-Befehle filtern lassen. Die Eingabetaste startet den gerade markierten Befehl. Das HUD wirkt im Terminal, in Libre Office oder VLC auf den ersten Blick ziemlich cool; letztlich muss man aber doch eine Vorstellung haben, wo sich eine gesuchte Funktion verstecken könnte. Eine brauchbare Filterfunktion bietet das HUD aber allemal.



Mate macht auf Unity: Das Tweak-Tool bietet voreingestellte Leistenlayouts, wovon „Mutiny“ dem verstorbenen Unity am ähnlichsten kommt.

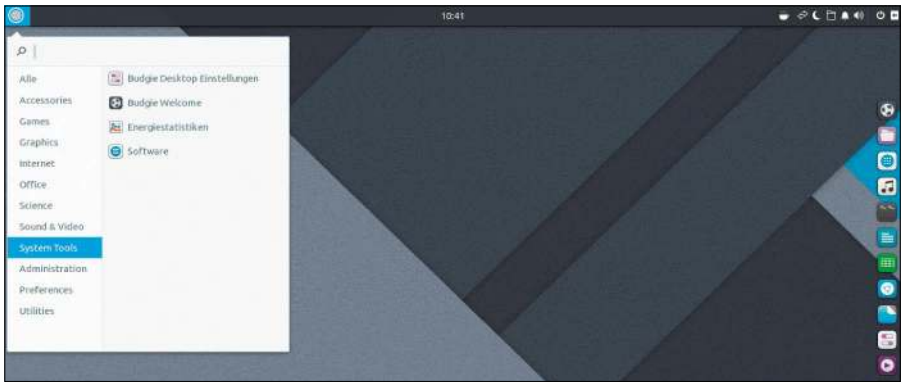


Head-up-Display: Nach Drücken der Alt-Taste in einer Software klappt eine Befehlsübersicht aus, die ein Filtern der gewünschten Funktion erlaubt.

Weitere Ubuntu-Editionen

Die weiteren Ubuntus 17.10 bringen die genannten Aktualisierungen von Kernel und Softwarepaketen unter der Haube, unterscheiden sich sonst aber nicht wesentlich von ihren Vorgängern.

Insbesondere bei Kubuntu, Xubuntu und Lubuntu bleiben die Neuerungen marginal. Noch am ehrgeizigsten zeigt sich die mittlerweile offizielle Edition mit dem Budgie-Desktop (in 64 Bit auf Heft-DVD). Budgie-Menü, Budgie-Desktop, Seitenleiste, Arbeitsflächen-Applet und Welcome-Programm erhalten zahlreiche kleine, insbesondere optische Verbesserungen. Nebenbei hat die Distribution diverses Standardzubehör ausgemistet und zum Teil durch Alternativen ersetzt, so etwa gnome-photos durch gthumb oder Terminix durch das Tilix-Terminal.



Ubuntu Budgie 17.10: Diese Variante arbeitet noch intensiv und mit vielen Detailkorrekturen am relativ neuen Budgie-Desktop, den sich Ubuntu vom Solus-Projekt ausgeliehen hat.

Samsung: Linux auf Smartphones

Ein weiteres Industrie-Schwergewicht nimmt sich das Thema Konvergenz vor, das Smartphones und Tablets beschreibt, die sich in voll funktionsfähige Desktop-PCs verwandeln können. Samsung hat mit „Linux on Galaxy" (*https://seap.samsung.com/linux-on-galaxy*) ein Projekt vorgestellt, das einen Linux-Desktop auf das Galaxy S8, S8+ und Note 8 bringt. Dazu startet eine App eine grafische Linux-Umgebung in einem Container, der weiterhin den vorhandenen Linux-Kernel des Android-Systems nutzt. Dieses Funktionsprinzip hatte bereits das Android-ROM Maru-OS erfolgreich demonstriert, welches einen ausgewachsenen Debian-Desktop auf ein Nexus 5 zaubert (*https://maruos.com*). Samsung hat für seine konvergenten Geräte auch schon die passenden Hardwareergänzungen: Um die Anbindung von Tastatur, Maus und Monitor kümmert sich die Dockingstation Dex, die seit April 2017 auf dem Markt ist. ■

Windows: Neues Subsystem für Linux

Mit dem Fall Creators Update für Windows 10 hat auch dessen Windows-Subsystem für Linux (WSL) eine Aktualisierung bekommen, die offiziell die Betaphase dieser Systemkomponente beendet. Das Subsystem für Linux holt eine Linux-Shell auf Windows 10 und steht jetzt mit den Tools zahlreicher Linux-Distributionen im Microsoft Store zur Installation bereit. Bisher sind die Shells von Ubuntu, Open Suse und Suse Linux Enterprise Server im Store verfügbar, Fedora soll demnächst folgen. Zudem kann Windows 10 nun mehrere dieser Linux-Umgebungen parallel installieren. ■

Kernel: Version 4.14 veröffentlicht

Anfang November hat Linus Torvalds den Kernel 4.14 mit Langzeitunterstützung freigegeben. Was ist neu in 4.14?

Im Zuge der neuen Version haben sich die Kernel-Entwickler darauf geeinigt, den Unterstützungszeitraum für diese speziellen Kernel-Ausgaben von zwei auf sechs Jahre zu erhöhen. Diese Änderung betrifft auch rückwirkend die noch gepflegten Linux-Kernel 4.4 und 4.9 mit Langzeitsupport. Der längere Zeitraum hilft vor allem den zahlreichen Herstellern von Android-Geräten, die sich mit Updates generell schwertun: Eine gleichbleibende Kernel-Version mit zurückportierten Patches ist in Android- und Embedded-Systeme erfahrungsgemäß einfacher einzubinden.
In Sachen Hardwareunterstützung hat Kernel 4.14 einen Speichermanager für die RAM-Verschlüsselungstechnik SME (Secure Memory Encryption) von AMD erhalten, die sich in den neuen Epyc-Prozessoren findet. Für aktuelle Intel-Chips gibt es mit dem Address Space Identifier (ASID beziehungsweise PCID) eine Speicherzugriffsmethode, die einen optimierten Übersetzungspuffer nutzt und den Prozessoren theoretisch eine höhere Leistung entlocken kann. Jenseits von regulärer Alltagshardware unterstützt Kernel 4.14 nun fünfstufiges Speicherpaging, das ab jetzt einen adressierbaren Speicherbereich von kolossalen vier Petabyte zulässt. Bisher lag das Limit bei 64 Terabyte – und das wurde von einigen Supercomputern bereits erreicht. ■

Linux Mint: Künftig ohne KDE-Edition

In Zukunft wird das Team um Linux Mint keine Systeme mehr mit KDE zusammenstellen, wie Clement Lefebvre als maßgeblicher Entwickler auf seinem Blogeintrag bekanntgegeben hat. Die letzte Edition von Linux Mint KDE wird die kommende Version 18.3 sein. Zu den populären Geschmacksrichtungen von Linux Mint hatte die KDE-Ausgabe dieser Linux-Distribution nie gehört: Eine Nutzungsstatistik auf *https://community.linuxmint.com* zeigt, dass nur noch 11,7 Prozent der Mint-Anwender KDE einsetzen, während Mate bei 19 Prozent liegt und der primäre Desktop Cinnamon bei 50 Prozent. Was auch zur baldigen Einstellung der KDE-Ausgabe beigetragen haben dürfte, sind sinkende Spendeneinkünfte für Linux Mint, die im vergangenen Jahr um 60 Prozent zurückgingen. Außerdem ist KDE Plasma 5 mit seiner großen Zahl an Einzelpaketen deutlich aufwendiger in der Pflege als andere Desktopumgebungen. Aber auch in Zukunft wird KDE Plasma 5 in Linux Mint aus den zugrundeliegenden Ubuntu-Paketquellen nachträglich installierbar bleiben. ■

Ubuntu 18.04 LTS wird ein Biber

Auch nach dem Richtungswechsel der Firma Canonical hinter Ubuntu bleibt die Linux-Distribution ihrer Tradition treu, neuen Ausgaben tierische Codenamen zu geben. Die kommende Ubuntu-Version 18.04, trägt den Namen „Bionic Beaver" (Bionischer Biber) soll im April 2018 erscheinen und wieder ein Ubuntu mit Langzeitsupport von fünf Jahren werden. ■

Alle News von David Wolski

Mozilla: Firefox will schlauer werden

Bislang hatte es Firefox vermieden, die Surfgewohnheiten seiner Nutzer auszuwerten, um Inhalts- und Suchempfehlungen zu geben. Zusammen mit der Münchner Cliqz GmbH entstand das gleichnamige Add-on Cliqz, das Webseiten- und Suchbegriff-Vorschläge den Interessengebieten von Firefox-Nutzen generiert. Das Add-on geht jetzt in einen öffentlichen Test und wird gerade vereinzelten Anwendern vorgeschlagen, die Firefox von *https://www.mozilla.org* herunterladen.
Rund ein Prozent aller Firefox-Anwender sollten das deinstallierbare Add-on erhalten. Mozilla und Cliqz versprechen, dass die erhobenen, anonymisierten Daten nicht für Werbezwecke weiterverwendet werden und sich keiner IP-Adresse zuordnen lassen. ■

Sicherheit: Audit für Dnsmasq

Bei Dnsmasq handelt es sich um einen kompakten DNS-Cache und DHCP-Server für Linux, der besonders in lokalen Netzen zur Namensauflösung nützlich ist. Weil Dnsmasq auch in vielen Linux-Systemen von Embedded-Geräten wie Routern und Access Points arbeitet, ist der Serverdienst weit verbreitet. Aus diesem Grund hat Google im Oktober einen Sicherheitsaudit für Dnsmasq durchführen lassen, um systematisch möglichst viele Bugs auszumerzen, die ein Sicherheitsproblem darstellen könnten. Tatsächlich hat der Audit sieben Bugs identifiziert, die jetzt mit Dnsmasq 2.78 behoben sind (*www.thekelleys.org.uk/dnsmasq/doc.html*). ■

Schleswig-Holstein: Ahoi, Open Source

Während die Stadt München, Sitz der Microsoft-Deutschlandzentrale, eine Rückmigration von Linux auf Windows plant, will der hohe Norden den umgekehrten Weg gehen: Die neue schwarz-grün-gelbe Landesregierung in Schleswig-Holstein hat sich in ihrem Koalitionsvertrag auf einen Abschied von Microsoft-Produkten geeinigt, die an vielen Stellen in der Verwaltung durch Open-Source-Software ersetzt werden soll. „Um dieses Ziel zu erreichen, werden wir unter anderem die entsprechenden Ausschreibungsbedingungen überarbeiten“, so der verabschiedete Koalitionsvertrag. ■

KRACK: WPA2 UNTER BESCHUSS

Lange galt das Verschlüsselungsverfahren WPA2 für Funknetzwerke als ausreichend sicher.
Mitte Oktober 2017 haben zwei Kryptografieexperten an der Universität Leuven (Belgien) die Ergebnisse einer Forschungsarbeit veröffentlicht, die einen praktischen Angriff auf WPA2 zeigt. Die gefundene Lücke betrifft den mehrstufigen Schlüsselaustausch während eines Verbindungsaufbaus im WLAN zwischen Basisstation und Clients. Zum Schlüsselaustausch kommt, wie in anderen Verfahren, ein Einmalschlüssel zum Einsatz, der danach in dieser Verbindung eigentlich nicht mehr zum Einsatz kommen darf. Ein Angreifer in Reichweite des Funknetzes kann verschlüsselte Pakete mitlesen, was alleine aber noch nichts nutzt. Deshalb stört der Angreifer den Austausch des Einmalschlüssels, sodass der gleiche Schlüssel, genannt „NONCE“ („Number Send Once“), wieder und wieder gesendet wird. Nach einer Weile hat der Angreifer genügend verschlüsselte WPA2-Pakete mit verschiedenem Inhalt gesammelt, die aber mit immer dem gleichen Einmalschlüssel chiffriert wurden.
Mit einer kryptografischen Analyse ist es jetzt möglich, den gesamten Schlüssel der WPA2-Verbindung zu rekonstruieren. Die Sicherheitsforscher haben bereits seit 2016 an der praktischen Umsetzung dieser Attacke gearbeitet, die zur Veröffentlichung den griffigen Namen „KRACK“ bekommen hat, eine Abkürzung für „Key Reinstallation Attack“. Es sind sowohl ungepatchte Clients als auch Access Points betroffen – zudem alle Betriebssysteme, da die Schwachstelle im WPA2-Verschlüsselungsprotokoll selbst steckt.
Auch Linux ist betroffen: Das Kernel-Modul „wpa_supplicant“ von Linux, das auch in Android und den meisten Embedded-Systemen auf Routern, Modems und Access Points arbeitet, ist sogar noch ein Stück anfälliger für Krack. Die Kernel-Entwickler hielten es für eine gute Idee, den Einmalschlüssel im Speicher nach der ersten Verwendung mit Nullen zu überschreiben. Sie hatten aber nicht damit gerechnet, dass diese Zeichenkette unverändert öfter gesendet wird – folglich bestehen die wiederholten Schlüssel auch nur aus Nullen. Die kryptografische Analyse ist damit besonders einfach. In Linux-Distributionen kamen die ersten Patches für WPA2 einen Tag nach der Veröffentlichung der Angriffsmethode. Microsoft und Apple folgten, Google hatte mit Android etwas länger zu tun. Viele ältere Smartphones, Router und Access Points mit abgelaufener Herstellerunterstützung werden aber kein Update mehr erhalten. Es empfiehlt sich deshalb, auch in privaten WLANs mit verschlüsselten Protokollen wie HTTPS und SSH zu arbeiten. ■

Debian: Wechsel zu Wayland

Nachdem Ubuntu 17.10 nicht nur Gnome zur primären Desktopumgebung gemacht, sondern auch den neuen Displayserver Wayland zum Standard erhoben hat, folgt auch Debian diesem Beispiel: Ab Debian 10 „Buster" soll Wayland zumindest für Gnome der Standard werden und Xorg ersetzten, das aus Kompatibilitätsgründen als Option erhalten bleibt. Debian 10 ist wird voraussichtlich Mitte 2019 als nächste stabile Ausgabe erscheinen. ■

Ubuntu Touch: Ubports macht weiter

Canonical hat das Smartphone- und Tabletsystem Ubuntu Touch zwar offiziell begraben, aber die freie Entwicklergemeinde um Ubports hat das Projekt übernommen. Mit der Version OTA-2 hat Ubports das zweite große Update für Ubuntu Touch freigegeben und dabei sogar die Hardwareunterstützung auf zwei weitere Geräte ausgedehnt: Ubuntu Touch läuft jetzt auch auf den Nexus 4 und dem Nexus 7. Die Liste unter *https://ubports.com/page/get-ubuntu-touch* zeigt alle unterstützten Modelle. ■

Let's Encrypt: HTTPS auf dem Vormarsch

Rund 60 Prozent aller Webseiten sind inzwischen verschlüsselt per HTTPS erreichbar, wie eine Studie der gemeinnützigen Organisation Let's Encrypt zeigt (*https://letsencrypt.org*). Keinen kleinen Anteil daran dürften die kostenlosen SSL-Zertifikate von Let's Encrypt haben, das im Dezember 2015 mit der Unterstützung gewichtiger Sponsoren wie Cisco, Akamai und HP Enterprise Mozilla an den Start ging. Zum Gründungszeitpunkt der Organisation lag der Anteil an Seitenaufrufen per HTTPS erst bei 39,5 Prozent. ■

Blueborne: Angriff per Bluetooth

Einige Mitte September gefundene Sicherheitslücken im Bluetooth-Protokoll können Linux, Android und Windows gefährlich werden. Die IT-Sicherheitsfirma Armis hat die Lücke „Blueborne" genannt und ausführlich dokumentiert. Der Fehler steckt in der automatischen Suchfunktion des Bluetooth-Protokolls, mit der die Umgebung nach möglichen Verbindungen abgesucht wird. Auf ungepatchten Linux-Systemen kann Blueborne zum Ausführen von Schadcode genutzt werden. Die nötigen Patches für Linux-Distributionen trudelten vergleichsweise langsam ein. Armis hat unter *https://goo.gl/8RD1yM* eine kostenlose Android-App zum Aufspüren von betroffenen Systemen bereitgestellt. ■

Linux: Development Report 2017

Die Kernel-Entwicklung in Zahlen veranschaulicht der Linux Kernel Development Report 2017, die die Linux Foundation dieses Jahr mit einiger Verspätung veröffentlicht hat. Der Bericht steht als PDF unter *www.linuxfoundation.org/2017-linux-kernel-report-landing-page* zum Download bereit. Die Zahlen sind beeindruckend: Seit letztem Jahr haben sich über 4300 Entwickler am Kernel beteiligt; davon waren rund ein Drittel neue Entwickler.

Im Schnitt gibt es 204 Änderungen am Quellcode pro Tag, das sind 8,5 Änderungen pro Stunde. 8,2 Prozent der Entwickler sind Hobbyprogrammierer. Die aktivste Firma mit dem meisten aufgenommenen Kernel-Patches ist Intel, gefolgt von Red Hat, Linaro und IBM. ■

Linux: Entwickler gegen Copyrightklagen

Auch die Open-Source-Szene ist nicht vor Copyrighttrollen und professionellen Abmahnern sicher. Das zeigten die wiederholten Fälle von Copyrightklagen eines ehemaligen Linux-Entwicklers gegen Softwarefirmen, die gegen die GNU Public License verstoßen. Patrick McHardy, der an der Kernel-Firewall Netfilter beteiligt war, zerrte vorzugsweise in Deutschland diverse Firmen wegen Lizenzstreitigkeiten vor Gericht. In den letzten Jahren fand sich unter anderem AVM unter den verklagten Firmen. Die Linux-Community kritisierte das rechtliche Vorgehen gegen Firmen immer wieder und warf Patrick McHardy persönliche Bereicherung durch diese Klagen vor. Um Copyrighttrollen die Grundlage zu entziehen, haben Linus Torvalds und Greg Kroah-Hartmann mit der Linux Foundation die Lizenz (GNU Public License 2) des Kernel-Quellcodes um das „Enforcement Statement" ergänzt. Diese Ergänzung in Form einer Entwicklervereinbarung gibt Firmen ausreichend Zeit, Lizenzverstöße auszuräumen, ohne mit Klagen rechnen zu müssen. ■

Oracle: Ciao Solaris!

Das Betriebssystem Solaris ist eines der wenigen traditionellen Unix-Systeme, das vom Linux-Boom noch nicht überrollt wurde. Solaris ist nach dem Ende von Sun Microsystems im Zuge der Übernahme bei Oracle gelandet. Im Januar 2017 ist Solaris 12 aus den offiziellen Oracle-Entwicklungsplänen verschwunden und im September hat der Rest des Solaris-Teams die Kündigung erhalten. Das Ende von Solaris und das Ende einer Ära scheinen damit besiegelt zu sein. Oracle favorisiert bereits eine Weile Linux als Plattform und pflegt den eigenen Red-Hat-Klon „Oracle Linux". ■

UPDATETELEGRAMM

Fedora 27

Leicht verspätet ist Fedora Anfang November in Version 27 erschienen. Der Standarddesktop ist Gnome 26 und es gibt auch offizielle Fedora-Spins mit KDE Plasma 5, Xfce, LXDE, LXQT, Mate und Cinnamon. Download unter *https://getfedora.org*. ■

LXQT 0.12

Der schlanke Desktop von den Machern der ebenso genügsamen LXDE-Oberfläche verbessert die Unterstützung von Hi-DPI-Bildschirmen. LXQT 0.12 wird in Ubuntu 18.04 nächstes Jahr enthalten sein und LXDE ablösen. Wer den Desktop jetzt schon nutzen möchte, ist mit Arch Linux oder einem seiner Ableger wie Antergos (auf Heft-DVD) am besten beraten (*http://lxqt.org*). ■

Q4OS 2.4

Dieser Debian-Ableger versorgt alte Notebooks und PCs, auf welchen aktuelle Linux-Distributionen nicht mehr zufriedenstellend laufen. Q4OS arbeitet mit dem Trinity-Desktop, einer Fortführung von KDE 3.5, und aktualisiert das Basissystem auf Debian 9 (Download unter *http://q4os.org*). ■

Nextcloud Android Client 2.0

Für die Owncloud-Abspaltung Nextcloud, hinter der zwei der ehemaligen Owncloud-Gründer stehen, gibt es eine neue Version des Android-Clients. Diese App kann Kontakte in der Nextcloud speichern und auf ein anderes Android-Gerät herunterladen. Zur Anmeldung am eigenen Nextcloud-Server gibt es jetzt mehrere Zwei-Faktor-Authentifizierungsverfahren. Der neue Client ist auf Google Play erhältlich (*https://goo.gl/aiiXAE*). ■

Android Studio 3.0

Google hat die Entwicklerumgebung Android Studio in Version 3.0 freigegeben. Sie übernimmt einige neue Möglichkeiten von Java 8, eignet sich für die Internet-of-Things-Plattform Android Things und kann mit der neuen Programmiersprache Kotlin umgehen (Download unter *https://developer.android.com/studio*). ■

Kali Linux 2017.2 mit neuen Tools

Die auf Sicherheitstools spezialisierte Distribution Kali kombiniert ein Debian Testing mit Programmen zum Aufspüren von Sicherheitslücken. Zu den neu aufgenommenen Tools gehören ein SSH-Server-Auditor und das Automated Penetration Testing Toolkit. Das installierbare Livesystem liegt auf *www.kali.org/downloads* bereit. ■

Cent-OS 7.4

Der beliebte Red-Hat-Klon liegt in Version 7.4 vor und zieht damit Red Hat Enterprise Linux 7.4 vom August gleich. Cent-OS wird aus den gleichen Quellcode-Paketen wie das Vorbild gemacht, steht aber frei zum Download bereit (*www.centos.org/download*), während Red Hat Enterprise Linux nur im Rahmen von Supportverträgen verfügbar ist. ■

Manjaro 17.0.6 nur noch in 64 Bit

Mit hübscher Regelmäßigkeit gibt es neue Installationsmedien des Arch-Abkömmlings Manjaro. Jetzt verabschiedet sich Manjaro von der 32-Bit-Unterstützung und liegt nur noch in 64 Bit vor. Manjaro 17.0.6 steht als installierbares Livesystem mit KDE Plasma 5.11, Gnome 3.246 sowie Xfce 4.12 zum Download bereit (*http://manjaro.org*) und ist als Rolling Release konzipiert. ■

KDE Plasma 5.11

Zuletzt machte KDE Plasma 5 große Fortschritte und Ausgabe 5.11 vom Oktober 2017 ist da keine Ausnahme. Zu den neuen Funktionen gehören eine neue Übersichtsseite für Systemeinstellungen, verbesserter Wayland-Support und das Verschlüsselungstool Plasma Vault. Der schnellste Weg zum neusten KDE ist die Distribution KDE Neon User Edition (*https://neon.kde.org*). ■

Webserver-Grundlagen

Webserver sind ein wichtiger Bestandteil des Internets, leisten aber auch im eigenen Netzwerk nützliche Dienste. Wie Sie einen Webserver mit Apache oder Nginx konfigurieren, erfahren Sie in diesem Artikel.

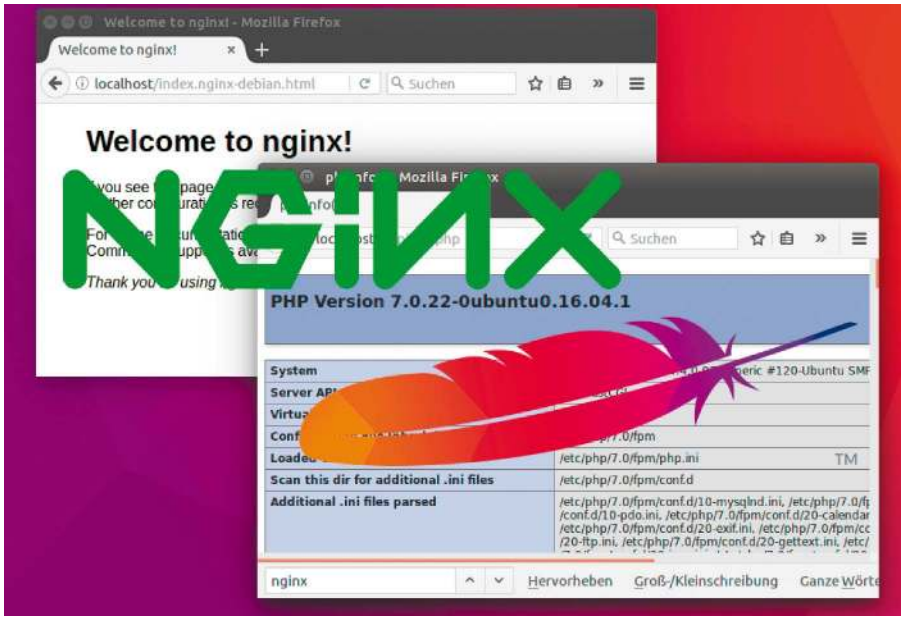
VON THORSTEN EGGELING

Die Grundfunktion eines Webservers besteht in der Auslieferung von HTML- und Bildinhalten über die Protokolle HTTP oder HTTPS. Wenn Sie in Ihrem Browser eine Webadresse aufrufen, fordert der Browser beim Webserver auf Port 80 („http://“) oder Port 443 („https://“) die Auslieferung der Startseite an. Webserver und Browser sind Schlüsseltechnologien des Internets. Beide stellen eine Infrastruktur bereit, um Informationen abzurufen, Daten zu speichern, online einzukaufen und in sozialen Netzwerken zu kommunizieren. Grund genug, sich mit den zugrundeliegenden Technologien intensiver zu beschäftigen. Ein Webserver im eigenen lokalen Netzwerk kann nützliche Webanwendungen für den Eigenbedarf oder für kleine Teams anbieten.

Wir beziehen uns in diesem Artikel auf Ubuntu 16.04. Die Konfigurations- und Installationsanleitungen gelten für verwandte Systeme wie Linux Mint 18 und ähnlich auch für andere Systeme. Alle Kommandozeilen und Beispielkonfigurationen können Sie als Textdatei über *www.pcwelt.de/JFuN4E* herunterladen.

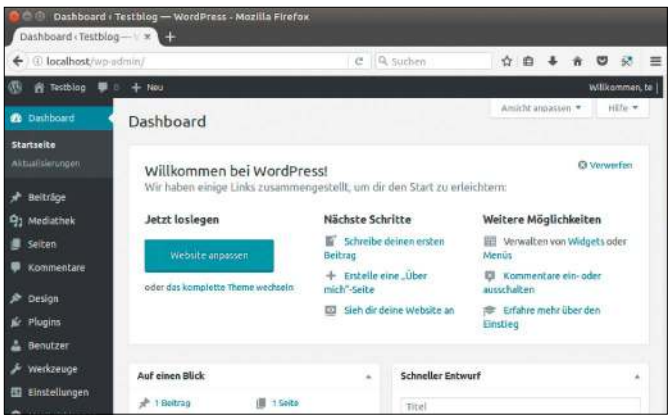
1. Das leisten Webserver

Der Apache HTTP-Server (*https://httpd.apache.org*) gehört zu den am meisten genutzten Webservern. Es gibt ihn schon seit gut 20 Jahren und viele Beispielkonfigurationen beziehen sich auf Apache. Eine Alternative ist der Nginx-Webserver (*https://nginx.org*), der sparsamer mit den PC-Ressourcen umgeht und sich oft besser für weniger leistungsfähigere Hardware und für Server mit sehr vielen Zugriffen eignet. In einigen Fällen kann auch die Kombination von Apache mit Nginx als Reverse-Proxy sinnvoll sein. Der Vorteil dabei: Die Last lässt sich zwischen beiden Servern verteilen und die Gesamtleistung steigern.



Es gibt noch einige weitere Webserver, die sich durch geringen Ressourcenverbrauch oder eine besonders einfache Konfiguration auszeichnen. Ein Beispiel dafür ist Lighttpd (*www.lighttpd.net*). Der leichtgewichtige Webserver erfüllt fast die gleichen Aufgaben wie Apache, jedoch fehlen einige Funktionen, sodass sich nicht jedes CMS (Content-Management-System) ohne Anpassungen mit Lighttpd nutzen lässt. Wir gehen deshalb in diesem Artikel nicht weiter auf Lighttpd ein.

Webseiten dynamisch erzeugen: Meist werden Sie auf einem Webserver nicht einfache, statische HTML-Dateien verwenden, sondern ein CMS oder eine andere Webanwendung nutzen. Wordpress, Joomla und Webanwendungen wie Nextcloud (Cloudserver) oder Piwigo (Bildergalerie) erstellen die Webseiten dynamisch. Der Webserver



Dynamische Webinhalte: Content-Management-Systeme wie Wordpress erzeugen die HTML-Inhalte dynamisch mit PHP-Scripts und Datenbankabfragen.

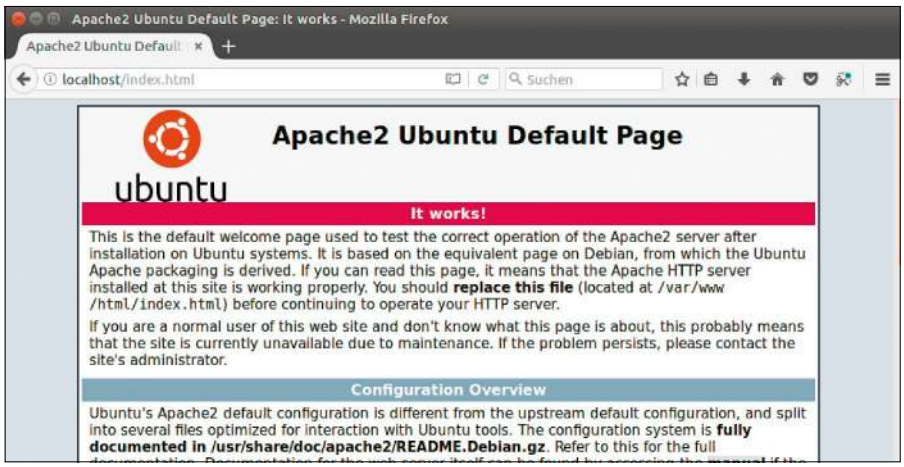
kann dafür mit zusätzlichen Modulen ausgestattet werden, die Scripts verarbeiten. Die Scripts produzieren HTML-Code auf der Basis von Vorlagen meist aus Datenbankinhalten. Als Script-Sprachen dienen meist PHP, Perl oder Python. Grundsätzlich kann der Webserver beliebige externe Programme unabhängig von der verwendeten Programmiersprache starten, deren HTML- oder Textausgabe er an den Client (Browser) weiterleitet.

2. Die Apache-Basiskonfiguration

Apache lässt sich bei fast allen Linux-Distributionen schnell über das Paket „apache2 „installieren. Nutzer von Ubuntu, Linux Mint und Debian verwenden dafür die jeweilige Paketverwaltung oder am einfachsten die Kommandozeile:

```
sudo apt update
sudo apt install apache2
```

Danach rufen Sie am selben Rechner im Webbrowser die Adresse *http://localhost* auf. Sie sehen dann die Standard-Webseite mit einigen grundlegenden Informationen zur Konfiguration. Sie erfahren hier beispielsweise, dass alle Apache-Konfigurationsdateien unter „/etc/apache2“ liegen und die Webdokumente unter „/var/www/html“ („DocumentRoot“). In diesem Ordner liegt bisher nur die Datei „index.html“ mit der Standard-Webseite. Der Webserver liefert immer automatische die Datei „index.html“ an den Webbrowser aus, wenn diese in einem Ordner vorhanden ist. Andernfalls zeigt er standardmäßig den Verzeichnisinhalt an.



Funktionsprüfung: Nach der Installation des Apache-Webservers rufen Sie auf dem Server-PC die Adresse „http://localhost“ auf. Wenn der Server funktioniert, sehen Sie den Inhalt der Startseite.

3. Webserver im lokalen Netzwerk

Auf anderen Geräten im Netzwerk erreichen Sie den Server über „http://[Hostname]“ oder „http://[IP-Nummer]“. Je nach Router funktionieren auch „http://[Hostname].local“, „http://[Hostname].lan“ oder „http://[Hostname].fritz.box“. Mit

```
nslookup [Hostname]
```

ermitteln Sie im Terminalfenster, über welchen Namen und welche IP-Adresse der Server im Netzwerk erreichbar ist.

In einem lokalen Netzwerk ohne eigene Domain und Domain Name Service (DNS) sind die Möglichkeiten der Namensvergabe beschränkt.

Ein Server kann nur einen und nicht mehrere Hostnamen besitzen und deshalb ist ohne weitere Maßnahmen nur ein Webserver pro PC konfigurierbar. Es gibt jedoch mehrere Möglichkeiten, diese Einschränkung zu umgehen. Soll der PC mehrere Webdienste anbieten, etwa Wordpress und Nextcloud, kann die Installation in ein Unterverzeichnis erfolgen, beispielsweise „/var/www/html/wordpress“. Das CMS ist dann über „http://[Hostname]/wordpress“ erreichbar. Fast alle CMS oder Webanwendungen bieten diese Installationsart an. Mit Apache lassen sich aber auch virtuelle Server einrichten. Es ist dann möglich, unterschiedliche Webanwendungen auf einem Server über andere Ports oder Subdomains zu erreichen.

Subdomains oder alternative Hostnamen legen Sie im lokalen Netzwerk in der Datei

NGINX ALS REVERSE-PROXY

Nginx liefert statische Inhalte schneller aus als Apache. Deshalb ist es oft von Vorteil, die Aufgaben zu verteilen, wobei Apache hauptsächlich für die dynamisch erzeugten Seiten zuständig ist. Dieses Reverse-Proxy genannte Verfahren ist auch nützlich, wenn das gewünschte CMS nicht mit Nginx zusammenarbeitet.

Im ersten Schritt ändern Sie die Apache-Konfiguration, damit der Server nur auf einem höheren lokalen Port erreichbar ist. In der Datei „/etc/apach2/ports.conf“ darf beispielsweise nur

```
listen 8000
```

stehen. In der Datei „/etc/apache2/sites-enabled/000-default.conf“ ändern Sie die erste Zeile in

```
<VirtualHost 127.0.0.1:8000>
```

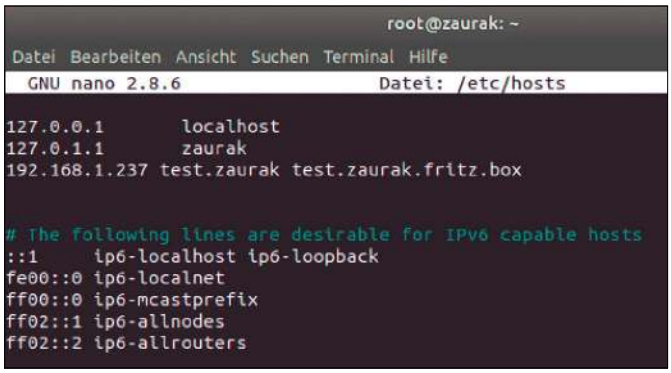
In die Nginx-Site-Konfiguration „/etc/nginx/sites-enabled/default“ bauen Sie folgenden Block ein:

```
location / {
proxy_pass http://127.0.0.1:8000;
include /etc/nginx/proxy_params;
}
location ~* .(js|css|jpg|jpeg|gif|png|svg|ico|pdf|h
  tml|htm)$ {
expires 30d;
}
```

Weitere „location“-Blöcke entfernen Sie aus der Datei. Die PHP-Konfiguration für Nginx ist nicht mehr erforderlich, weil Apache diese Aufgabe übernimmt. Starten Sie dann beide neu:

```
service apache2 restart
service nginx restart
```

Über „http://localhost“ erreichen Sie jetzt den Nginx-Server, der die Anfragen an Apache weiterleitet.



Servernamen vergeben: Webangebote sind auch über Subdomains erreichbar, wenn Sie IP-Nummer und Namen auf jedem PC im Netz in die Datei „/etc/hosts“ eintragen.

„/etc/hosts“ fest. Öffnen Sie diese über das Terminalfenster in einem Editor, etwa mit:

```
sudo nano /etc/hosts
```

In der Datei finden Sie beispielsweise diese Einträge:

```
127.0.0.1 localhost
127.0.1.1 zaurak
```

„zaurak“ ist in unserem Beispiel der Hostname, den Sie bei der Installation festgelegt haben. Ergänzen Sie folgende Zeile

```
192.168.178.131 test.zaurak test.
  zaurak.fritz.box
```

Verwenden Sie die IP-Adresse, die Sie zuvor über *nslookup* ermittelt haben. Die beiden Hostnamen passen Sie entsprechend Ihrer Konfiguration an. Tragen Sie die Zeile bei allen PCs im Netzwerk in die Datei „/etc/hosts“ ein, die auf den Webserver zugreifen sollen. Speichern die Änderungen mit Strg-O und Eingabetaste.

Der Webserver ist jetzt auch über die beiden alternativen Namen erreichbar. Beide zeigen jedoch die identische Webseite an, weil bisher noch nichts anderes konfiguriert ist (siehe Punkt 4).

Hinweis: Befindet sich der Webserver in einer Internetgdomäne bei einem Webhoster, sind keine Änderungen in der „/etc/hosts“ nötig. In der Regel leiten DNS-Server alle Anfragen an eine Domäne beziehungsweise Subdomäne an den Webserver oder andere Dienste weiter.

4. Virtuellen Apache-Server erstellen

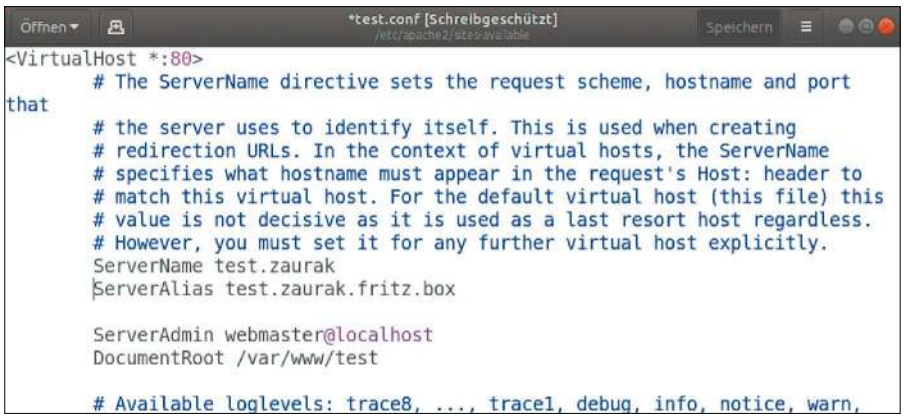
Unter „/etc/apache2/sites-available“ liegen die Konfigurationsdateien für virtuelle Webserver. „virtuell“ bedeutet, dass zwar nur ein Webserver läuft, dieser aber Dateien aus unterschiedlichen Ordnern und damit unterschiedliche Webseiten ausliefert. Sie können das selbst ausprobieren, indem Sie eine Kopie der Datei „000-default.conf“ erstellen und die Kopie bearbeiten:

```
cd /etc/apache2/sites-available
sudo cp 000-default.conf test.conf
sudo nano test.conf
```

Entfernen Sie das Kommentarzeichen „#“ vor „ServerName“ und tragen Sie dahinter eine Subdomain wie

```
ServerName test.zaurak
```

ein, die Sie in Punkt 3 in die Datei „/etc/hosts“ verwendet haben. Bei einem gehosteten Webserver setzen Sie den für Sie registrierten Domainnamen beziehungsweise eine Subdomain ein.



Virtuelle Hosts: Für mehrere Webanwendungen konfigurieren Sie virtuelle Server, auf die Sie über Subdomains oder über unterschiedliche Ports zugreifen.

Zusätzlich können Sie mit der Zeile

```
ServerAlias test.zaurak.fritz.box
```

noch eine zweite Domain festlegen.

Ändern Sie den Pfad hinter „Document Root“ auf „/var/www/test“ und hinter „ErrorLog“ und „CustomLog“ die Dateinamen für die Logdateien. Bauen Sie beispielsweise ein „test“ in die Dateinamen ein. Aktivieren Sie die Konfiguration mit den folgenden zwei Befehlszeilen:

```
a2ensite test
systemctl reload apache2
```

Damit erstellen Sie die Verknüpfung „/etc/apache2/sites-enabled/test.conf“ mit „/etc/apache2/sites-available/test.conf“ und veranlassen den Webserver, die Konfiguration neu einzulesen.

Jetzt müssen Sie noch das gewählte „DocumentRoot“ mit Inhalt füllen (zwei Zeilen):

```
sudo mkdir /var/www/test
sudo echo Testserver > /var/www/
  test/index.html
```

Rufen Sie im Browser die Domänen auf, die Sie hinter „ServerName“ und „ServerAlias“ festgelegt haben. Beide zeigen den Inhalt der Datei „index.html“ aus dem Ordner „/var/www/test“.

Webserver über Ports ansteuern: In der ersten Zeile der Datei „/etc/apache2/sites-available/test.conf“ steht „<VirtualHost *:80>“. Der Apache-Webserver antwortet daher auf alle Anfragen, die an den Standardport 80 gestellt werden und die zu den Angaben hinter „Servername“ und „Server Alias“ passen. Für eine alternative Konfiguration ändern Sie die erste Zeile:

```
<VirtualHost *:8080>
```

Vor „Servername“ und „ServerAlias“ setzen Sie jeweils das Kommentarzeichen „#“. Öffnen Sie eine weitere Apache-Konfigurationsdatei im Editor:

```
sudo nano /etc/apache2/ports.conf
```

Hier stehen hinter „Listen“ die Ports, auf die der Webserver hört. Das sind die Ports 80 und 443, letzterer aber nur, wenn das Apache-SSL-Modul geladen ist (siehe Punkt 5). Setzen Sie hinter „Listen 80“ die Zeile

```
Listen 8080
```

ein. Die Portnummer ist frei wählbar, soweit sie nicht anderweitig belegt ist. Üblich ist der Bereich von 8000 bis 8139. Aktivieren Sie diese Änderungen:

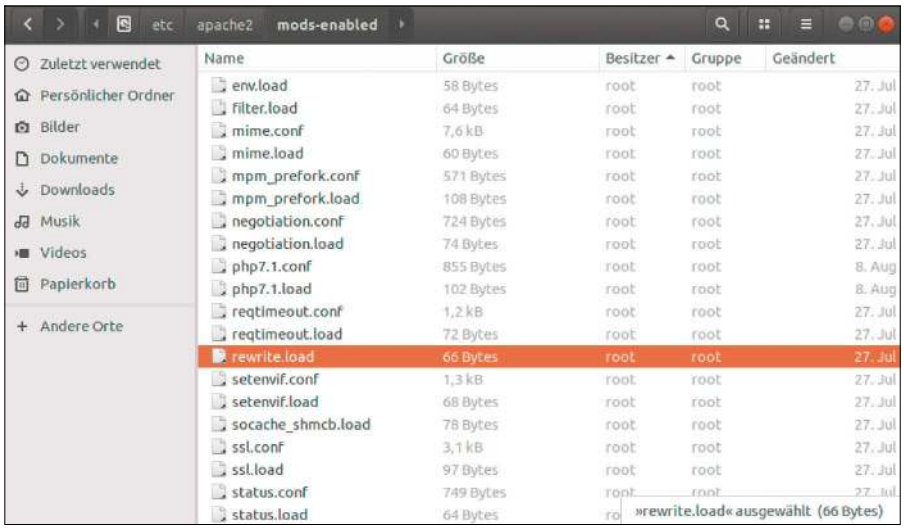
```
systemctl reload apache2
```

Den Inhalt von „/var/www/test“ rufen Sie jetzt auf dem Server im Browser über „http://localhost:8080“ ab. Auf anderen PCs hängen Sie „:8080“ an den Hostnamen an.

Der Vorteil der Portmethode: Hier müssen Sie die Datei „/etc/hosts“ nicht auf allen Rechnern ändern. Andererseits sind Portnummern schwerer merkbar als aussagekräftige Subdomainnamen. Aber auch das lässt sich mit einem einfachen Trick verbessern. Bauen Sie einfach in die Datei „/var/www/html/index.html“ des Hauptservers eine Liste mit Links auf die virtuellen Server mit den passenden Ports ein.

5. Zusätzliche Apache-Module aktivieren

Das Paketmanagement kopiert bei der Apache-Installation Start-Scripts zahlreicher Module in das Verzeichnis „/etc/apache2/mods-available“. Welche davon bereits aktiviert sind, sehen Sie an den symbolischen Links im Verzeichnis „/etc/apache2/mods-enabled“.



Apache erweitern: Welche zusätzlichen Apache-Module aktiviert sind, sehen Sie an den Verknüpfungen im Verzeichnis „/etc/apache2/mods-enabled“.

Wenn Sie Webseiten beispielsweise verschlüsselt per HTTPS übertragen wollen, müssen Sie das zugehörige Modul folgendermaßen aktivieren:

```
a2enmod ssl
```

Ähnlich wie bei „a2ensite“ (siehe Punkt 4) erstellen Sie damit einen symbolischen Link für das SSL-Modul in „/etc/apache2/mods-enabled“. Jetzt benötigen Sie noch einen privaten Schlüssel und ein SSL-Zertifikat. Beides erzeugen Sie in einem Terminalfenster mit diesen zwei Befehlszeilen:

```
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 für die Funktion jedoch keine Rolle spielen. Sie können daher eintragen, was Sie wollen. Bei „Common Name“ tragen Sie den Servernamen mit Domain ein, wie ihn nslookup anzeigt (siehe Punkt 3).

Öffnen Sie die SSL-Beispielkonfiguration in einem Editor:

```
sudo nano /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
systemctl reload apache2
```

Der Webserver ist danach weiterhin über „http://[Hostname]“ erreichbar, die SSL-verschlüsselte Website rufen Sie über „https://[Hostname]“ auf. Webbrowser 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.

Umleitung auf HTTPS: Soll eine Website nur noch SSL-verschlüsselt aufrufbar sein, definieren Sie eine Umleitungsregel. Erstellen Sie die Datei „.htaccess“ im Document-Root des Webservers:

```
sudo nano /var/www/html/.htaccess
```

Tippen Sie die folgenden fünf Zeilen ein:

```
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_
  HOST}%{REQUEST_URI} [R=301,L]
</IfModule>
```

Speichern Sie die Datei und beenden Sie den Editor. Damit Apache die Kommandos in der Datei „.htaccess“ berücksichtigt, müssen Sie noch eine Änderung in der Datei „/etc/apache2/sites-available/000-default.conf“ vornehmen. Ergänzen Sie folgende vier Zeilen unterhalb der Zeile, die mit „DocumentRoot“ beginnt:

```
<Directory /var/www/html>
Options Indexes FollowSymLinks
  MultiViews
AllowOverride FileInfo
</Directory>
```

Danach aktivieren Sie das Rewrite-Modul und starten Apache neu:

```
sudo a2enmod rewrite
sudo systemctl restart apache2
```

Weitere Einsatzmöglichkeiten: Das Rewrite-Modul kommt auch bei vielen CMS zum Einsatz. Hier dient es dazu, komplexe URLs suchmaschinenfreundlich umzuschreiben. Aus Adressen wie „www.meinblog.de/?p=123“ wird dann beispielsweise „www.meinblog.de/meine-reise-nach-panama“. Solche Inhaltsbeschreibung in der URL erhöht das Ranking bei Suchmaschinen.

6. Unterstützung für PHP aktivieren

Die am weitesten verbreitete Script-Sprache im Internet ist PHP. Zurzeit findet hier ein Versionssprung von PHP 5 auf PHP 7 statt. Bei Ubuntu 16.04 und 17.10 beispielsweise wird standardmäßig der PHP-Interpreter in der Version 7 ausgeliefert. PHP 7 bietet zwar mehr Leistung, ist aber nicht vollständig kompatibel zu älteren PHP-Versionen. Die meisten größeren Webprojekte wie Wordpress, Drupal, Piwik sind bereits fit für PHP 7, einige kleinere Projekte und Eigenentwicklungen können aber Probleme machen, wenn diese noch nicht für PHP 7 angepasst wurden. Sehen Sie daher bei den Systemvoraussetzungen des gewünschten CMS nach, ob PHP 5 oder 7 unterstützt werden.

PHP 7 installieren: Zur Installation verwenden Sie unter Ubuntu 16.04 im Terminalfenster die Befehlszeile

```
sudo apt install php php-cli php-
 mysql libapache2-mod-php
```

Damit richten Sie PHP, das Kommandozeilentool php, die häufig genutzten Bibliotheken für die Verbindung zu My-SQL-Datenbanken und das PHP-Modul für Apache ein. Letzteres wird automatisch aktiviert. Für einige Webanwendungen sind zusätzliche PHP-Erweiterungen erforderlich, beispielsweise php-imagick und php-gd (Bilder generieren und manipulieren), php-sqlite3 (Zugriff auf Sqlite-Datenbanken) oder php-pgsql (Zugriff auf Postgre-SQL-Datenbanken). Eine Liste der benötigten Module finden Sie in der jeweiligen Installationsanleitung.

PHP 5 installieren: Wenn Sie PHP 5 benötigen, kann die Installation über ein externes Repository (PPA) erfolgen. PHP 5 lässt sich parallel zu PHP 7 installieren, allerdings können Sie nicht beide Versionen gleichzeitig benutzen. Die PHP-Konfiguration ist für beide Versionen getrennt: Für PHP 5.6 liegt die Konfigurationsdatei unter „/etc/php/5.6/apache2/php.ini“ und für Version 7.0 unter „/etc/php/7.0/apache2/php.ini“. Die Konfigurationsdatei für das Kommandozeilentool php liegt jeweils im Unterverzeichnis „cli“.

```
sudo add-apt-repository
 ppa:ondrej/php
sudo apt-get update
sudo apt-get install php5.6 php5.6-
 mysql php-gettext php5.6-mbstring
 libapache2-mod-php5.6
```

Mit diesen drei Befehlen wechseln Sie von PHP 7 zu PHP 5:

```
sudo a2dismod php7.0
sudo a2enmod php5.6
sudo service apache2 restart
```

Und wieder zurück zu Version 7 geht es mit diesen drei Zeilen:

```
sudo a2dismod php5.6
sudo a2enmod php7.0
sudo service apache2 restart
```

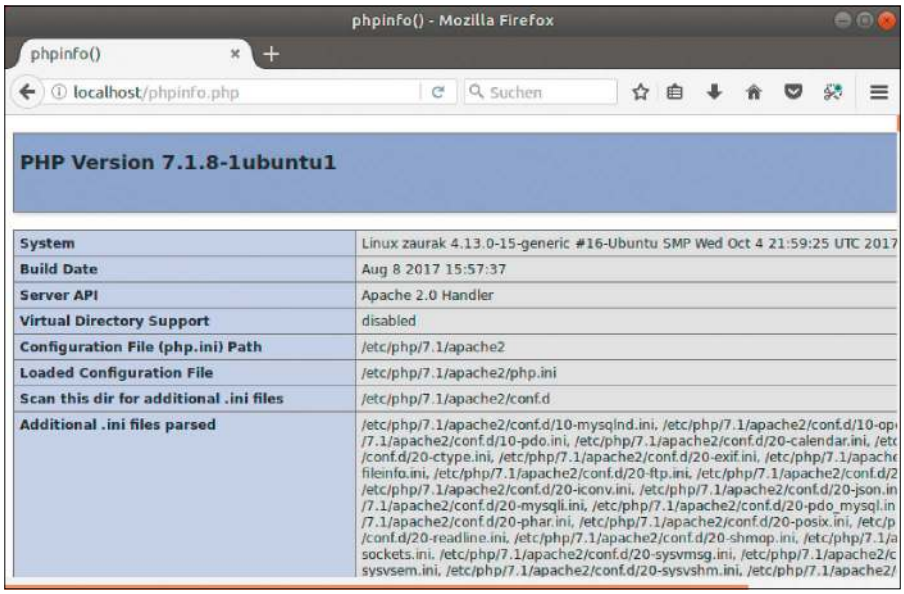
PHP-Installation ausprobieren: Erstellen Sie eine Testdatei mit

```
sudo nano /var/www/html/phpinfo.
 php
```

und tippen Sie diese drei Zeilen ein:

```
<?php
phpinfo();
?>
```

Speichern Sie den Inhalt und beenden Sie den Editor. Rufen Sie im Webbrowser „http://localhost/phpinfo.php“ auf. Die angezeigte Webseite informiert Sie über die PHP-Version, die aktuelle Konfiguration, die Konfigurationspfade und die installierten Zusatzmodule.



PHP testen: Ob die PHP-Installation erfolgreich war, lässt sich über eine kleines Script ermitteln. Die Funktion „phpinfo()“ zeigt alle wichtigen Informationen.

7. Die Nginx-Basis-Konfiguration

Wenn Sie den Webserver Nginx verwenden wollen und Apache bereits installiert ist, müssen Sie Apache zuerst beenden:

```
sudo service apache2 stop
```

Soll nur noch Nginx zum Einsatz kommen, deinstallieren Sie Apache oder deaktivieren den Dienst mit dieser Befehlszeile:

```
sudo systemctl disable apache2
```

Lesen Sie aber vorher die Ausführungen im Kasten „Nginx als Reverse-Proxy nutzen“, ob für Sie nicht die Kombination von Nginx mit Apache infrage kommt.

Installieren Sie dann Nginx:

```
sudo apt install nginx
```

Rufen Sie im Browser „http://localhost“ auf. Nginx liefert in der Standardkonfiguration die Datei „index.html“ aus dem Ordner „/var/www/html“ aus, wenn sie bereits vorhanden ist.

Andernfalls sehen Sie den Inhalt der Nginx-Beispieldatei „index.nginx-debian.html“. Die Nginx-Konfigurationsdateien befinden

IP-KONFIGURATION UND DYNAMISCHE IP

Ein Server sollte im lokalen Netzwerk möglichst immer unter derselben IP-Adresse erreichbar sein. Fast alle Router bieten eine Einstellung dafür. Bei einer Fritzbox beispielsweise gehen Sie in der Weboberfläche auf „Heimnetz -> Heimnetzübersicht“. Klicken Sie bei Ihrem Server in der Spalte „Eigenschaften“ auf „Details“. Setzen Sie ein Häkchen vor „Diesem Netzwerkgerät immer die gleiche IPv4-Adresse zuweisen“ und klicken Sie auf „OK“.

Wenn der Webserver auch aus dem Internet erreichbar sein soll, nutzen Sie einen Dienst für dynamische IP-Adressen. Sie erhalten einen Domainnamen, der den weltweiten Zugriff auf den Server ermöglicht. Besitzer einer Fritzbox können den Router über die Benutzeroberfläche kostenlos bei Myfritz anmelden (*www.myfritz.net*). Weitere kostenlose Dienste sind *https://twodns.de*, *www.selfhost.de* sowie *http://freedns.afraid.org*. Damit der Zugriff auf einen Webserver hinter der Firewall des DSL-Routers klappt, müssen Sie zusätzlich eine Portweiterleitung einrichten. Wie das funktioniert, lesen Sie auf in einem Betrag unter *www.pcwelt.de/8532494*.

sich unter „/etc/nginx“. „/etc/nginx/nginx.conf“ enthält die Basiskonfiguration, die weitere Dateien einbindet. „/etc/nginx/sites-enabled/default“ ist eine Verknüpfung mit „/etc/nginx/sites-available/default“. Öffnen Sie die Konfigurationsdatei mit

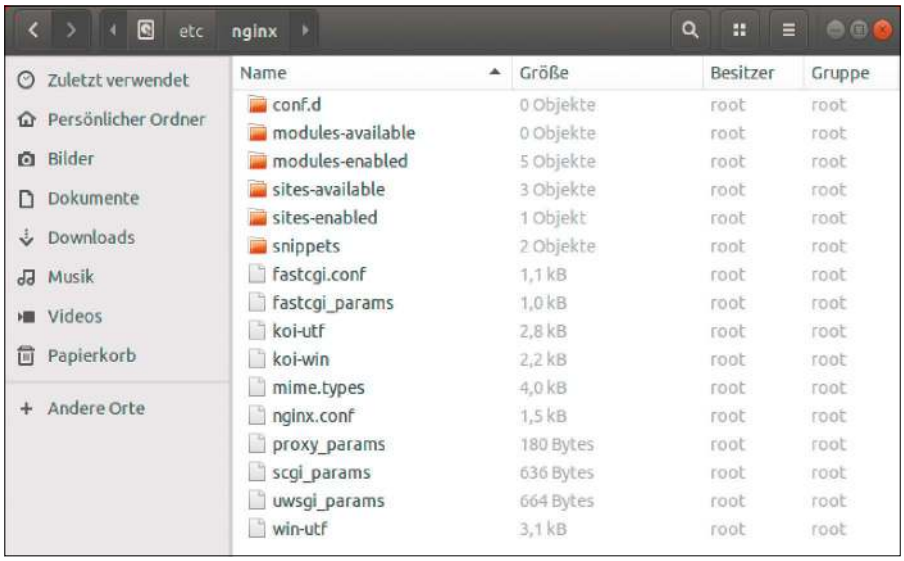
```
sudo nano /etc/nginx/sites-enabled/default
```

im Editor. Die Parameter für den Webserver stehen im Block hinter „server“ innerhalb der geschweiften Klammer („server {...}“). „listen 80“ legt den Port fest, auf dem der Webserver auf Anfragen horcht. „listen [::]:80“ aktiviert Nginx auch für die IPv6-Adresse des PCs. „root /var/www/html“ bestimmt das Verzeichnis, aus dem der Server Dateien ausliefert.

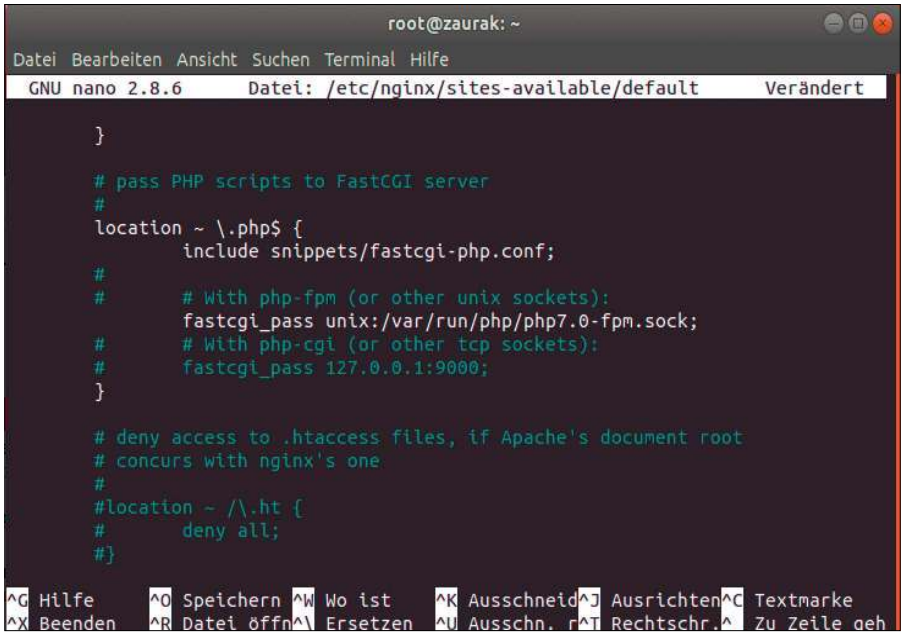
Für den HTTPS-Zugriff gibt es eine auskommentierte Beispielkonfiguration. Die Pfade zu den Schlüsseln sind in der Datei „/etc/nginx/snippets/snakeoil.conf“ zu finden. Bei Bedarf erzeugen Sie eigene Schlüssel, wie in Punkt 5 beschrieben. Wie bei Apache können Sie mehrere virtuelle Hosts verwenden, indem Sie weitere Konfigurationsdateien unter „/etc/nginx/sites-available“ anlegen und Symlinks dazu in „/etc/nginx/sites-enabled“ erstellen.

Verwenden Sie eine Kopie von „/etc/nginx/sites-available/default“ als Vorlage. Entfernen Sie „default_server“ hinter den „listen“-Zeilen, tragen Sie den gewünschten Ordner hinter „root“ ein und vergeben Sie einen Namen hinter „server_name“.

Für mehrere Server verwenden Sie unterschiedliche Ports oder tragen Namen in die Datei „/etc/hosts“ ein (siehe Punkt 3).



Nginx-Einstellungen: Im Ordner „/etc/nginx/“ liegen alle Konfigurationsdateien des Webservers. „/etc/nginx/sites-enabled“ nimmt Verknüpfungen zu virtuellen Hosts auf.



PHP mit Nginx: In der Nginx-Beispielkonfiguration ist ein auskommentierter Block für PHP enthalten. Entfernen Sie Kommentarzeichen wie abgebildet, um PHP zu aktivieren.

8. Nginx für PHP konfigurieren

Nginx verwendet kein Modul für den Aufruf von PHP-Scripts. Stattdessen kommt ein Dienst zum Einsatz, an den Nginx die Scripts weiterleitet und dessen Ausgaben der Server als Webseiten zum Client sendet. Der Befehl

```
sudo apt install php-fpm
```

installiert die nötige Software für PHP 7 unter Ubuntu 16.04. Wenn Sie PHP 5 verwenden (Installation siehe Punkt 6), geben Sie als Paketnamen „php5.6-fpm“ an. Sollte PHP noch nicht installiert sein, richtet Ubuntu die benötigten Pakete automatisch ein.

Öffnen Sie dann die Konfigurationsdatei:

```
sudo nano /etc/nginx/sites-enabled/default
```

Ein Abschnitt für PHP ist in der Beispieldatei bereits auskommentiert vorhanden. Entfernen Sie die Kommentarzeichen, sodass folgende Zeilen aktiv sind:

```
location ~ \.php$ {
include snippets/fastcgi-php.conf;
fastcgi_pass unix:/run/php/php7.0-fpm.sock;
}
```

Danach starten Sie die Dienste neu:

```
sudo service nginx restart
sudo service php7.0-fpm restart
```

Nutzer von PHP 5 ersetzen „7.0“ jeweils durch „5.6“. Sollte für das Linux-System, beispielsweise Ubuntu 17.10, eine neuere PHP-Version verfügbar sein, passen Sie die Bezeichnungen entsprechend an („7.1“, „7.2“). Welche php-fpm-Dienste laufen, ermitteln Sie mit

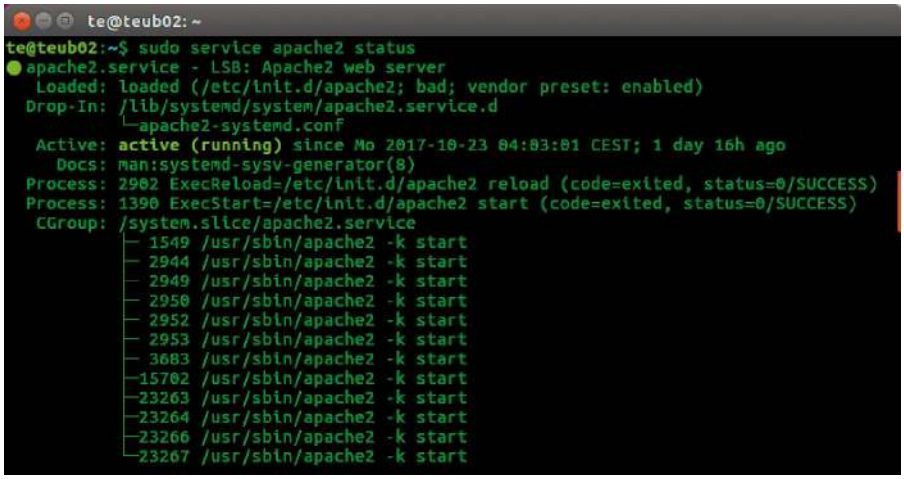
```
sudo service --status-all | grep -i fpm
```

Es können gleichzeitig mehrere aktiv sein, etwa php7.0-fpm und php5.6-fpm. Dadurch ist es möglich, für Nginx virtuelle Hosts zu erstellen, die unterschiedliche PHP-Versionen verwenden, wenn Webanwendungen dies erfordern. ■

Problemlösungen für Apache und Nginx

Nicht immer laufen Apache und Nginx oder das installierte Content-Management-System wie gewünscht. Tools und Logdateien helfen jedoch bei der Fehlersuche.

VON THORSTEN EGGELING



Läuft der Serverdienst überhaupt? Der Befehl „sudo service apache2 status“ zeigt Informationen über den Dienststatus an. Bei der Ausgabe „Active: active (running)“ ist alles in Ordnung.

Auch wenn die Installation von Webservern wie Apache und Nginx erst einmal unkompliziert erscheint, birgt die Konfiguration doch einige Tücken. Da ist nicht immer auf den ersten Blick zu erkennen, ob das Problem bei der Serverkonfiguration, beim jeweiligen Webdienst, bei einem Zusatzmodul oder schlicht bei falsch gesetzten Rechten im Linux-Dateisystem zu suchen ist.

Status des Servers prüfen

Wenn Apache oder Nginx installiert sind, sollte der Aufruf von „http://localhost“ im Webbrowser zur Startseite des Servers führen. Erscheint stattdessen „Fehler: Verbindung fehlgeschlagen“, läuft der Server wahrscheinlich nicht. Nutzen Sie dann in einem Terminalfenster folgende Befehlszeile:

```
sudo service apache2 status
```

Beim Einsatz von Nginx verwenden Sie „nginx“ statt „apache2“. Mit der Taste Q beenden Sie den Editor, der die Statusmeldungen anzeigt. In der Ausgabe sollte „Active: active (running)“ auftauchen. Erscheint stattdessen „Active: inactive (dead)“, läuft der Serverdienst nicht.

Häufig ist ein blockierter Port die Ursache dafür, dass der Server nicht startet. Für die Standardports 80 beziehungsweise 443 (HTTPS) darf kein anderer Dienst konfiguriert sein. Ob Port 80 bereits belegt ist, finden Sie mit dieser Befehlszeile heraus:

```
sudo netstat -anp | grep :80
```

Wenn Apache diesen Port benutzt, erhalten Sie etwa eine Ergebniszeile wie folgende:

```
tcp6 0 0 :::80 :::* LISTEN 28308/
 apache2
```

Für „tcp“ (Ipv4) gibt es kein Ergebnis, weil Apache die Umsetzung von IPv4-Adressen intern behandelt. Bei Nutzern von Nginx sieht die Ausgabe etwa so aus:

```
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN
 28397/nginx: master
tcp6 0 0 :::80 :::* LISTEN 28397/
 nginx: master
```

Sollte etwas anderes als „apache2“ oder „nginx“ in der netstat-Ausgabe auftauchen, verwendet ein anderer Dienst den Port 80. Deinstallieren Sie die Software oder beenden Sie den Dienst (*service [Dienstname] stop*). Danach sollten Apache oder Nginx starten. Wenn Sie mehrere Webserver betreiben wollen, müssen Sie diese auf jeweils anderen Ports konfigurieren (siehe Seite 24 ff.).

Server ist für andere PCs nicht erreichbar

Auf anderen PCs im lokalen Netzwerk rufen Sie die Website über „http://[IP-Adresse]“ oder „http://[Hostname]“ auf. Sollte das nicht funktionieren, ist der Server-PC entweder nicht erreichbar oder Port 80 des Servers ist durch eine Firewall geschützt. Einen einfachen Test führen Sie im Terminalfenster eines PCs im Netzwerk mit

```
ping [IP-Adresse]
```

durch. Lautet die Meldung „Destination Host Unreachable“, prüfen und reparieren Sie die Netzverbindung der PCs. Wenn ping ein positives Ergebnis liefert, der Server aber trotzdem nicht erreichbar ist, installieren und nutzen Sie das Tool nmap:

```
sudo apt install nmap
nmap -p1-9000 [IP-Adresse]
```

In diesem Beispiel prüft nmap die Ports 1 bis 9000. In der Ausgabe sollte dann „80/tcp open http“ zu sehen sein. Wenn nicht, dann ist der Port 80 wahrscheinlich durch eine Firewallregel blockiert. Ob die Firewall ufw auf Ihrem Server-PC aktiv ist, prüfen Sie mit diesem Befehl:

```
sudo ufw status
```

Sollte in der Ausgabe „Status: Aktiv“ auftauchen, fügen Sie eine Regel für den Webserver hinzu:

```
sudo ufw allow 80/tcp
```

Wiederholen Sie den Befehl für die anderen genutzten Ports, beispielsweise 443 (HTTPS). Wenn Sie die Firewall nicht zwingend benötigen, können Sie ufw mit

```
sudo ufw disable
```

auch ganz deaktivieren.

Log- und Konfigurationsdateien untersuchen

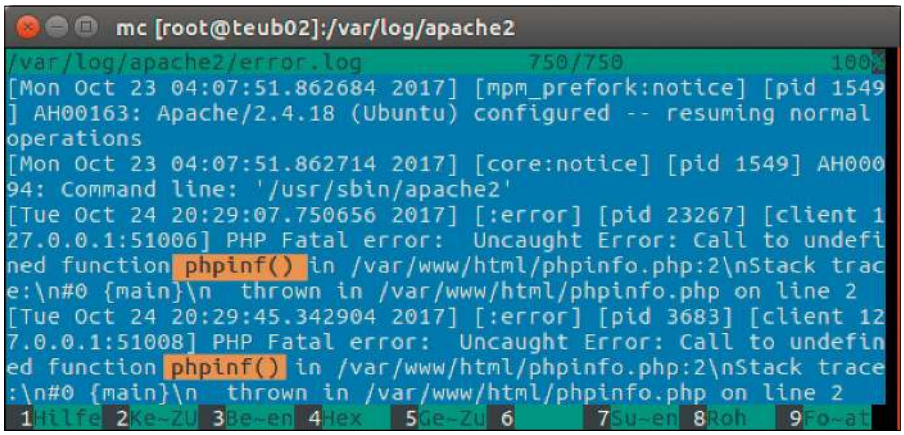
Die Logdatei von Apache heißt „/var/log/apache2/error.log“, jene von Nginx „/var/log/nginx/error.log“. Sie finden darin Meldungen, die bei der Fehlersuche hilfreich sind. In den Logdateien vermerken die Server auch Fehler in der Konfiguration. Diese lässt sich bei Apache schnell mit

```
sudo apache2ctl -t
```

prüfen. Nginx-Benutzer verwenden diesen Befehl:

```
sudo nginx -t
```

Das Testtommando zeigt Ihnen die Datei an, in der sich der Fehler befindet, sowie die Zeilennummer – und meist auch einen Hinweis zur Problembehebung. Fehler in PHP-Scripts finden Sie ebenfalls in den Logdateien. Auch hier ist die Datei vermerkt, in der der Fehler auftritt, und es gibt Informationen zum Fehlertyp.



Logdateien: Die Apache-Logdatei „error.log“ protokolliert auch Fehler im PHP-Code. In diesem Fall zeigt sich der simple Syntaxfehler „phpinf()“ statt korrekt „phpinfo()“.

Die Rechte im „Documentroot“

Apache und Nginx laufen unter Ubuntu mit den Rechten des Benutzers „www-data“, der zur gleichnamigen Gruppe gehört. Ein Webserver benötigt wenigstens Lesezugriff für alle Dateien und Ordner unter „/var/www/html“. Eine Schreibberechtigung ist bei einzelnen Dateien und Ordnern jedoch ebenfalls erforderlich, wenn Sie beispielsweise ein CMS installieren, über das CMS Dateien hochladen oder das CMS über das Back-End aktualisieren wollen. Wenn Sie beispielsweise für eine Wordpress-Neuinstallation die heruntergeladene ZIP-Datei (*https://de.wordpress.org*) nach „/var/www/html“ entpackt haben, führen Sie diese Befehlszeile aus:

```
sudo chown -R www-data:www-data /
  var/www/html
```

Besitzer und Gruppe „www-data“ erhalten damit Schreibzugriff auf alle Elemente in „/var/www/html“. Für Wordpress muss das Apache-PHP-Modul aktiviert sein (siehe Seite 24 ff.). Außerdem ist das Paket „mysql-server“ erforderlich. Für den bequemen Zugriff auf die Datenbank über „http://localhost/phpmyadmin“ installieren Sie das Paket „phpmyadmin“ und erstellen eine Datenbank für Wordpress. Gehen Sie auf „http://[Hostname]“ und folgen Sie den Anweisungen des Assistenten.

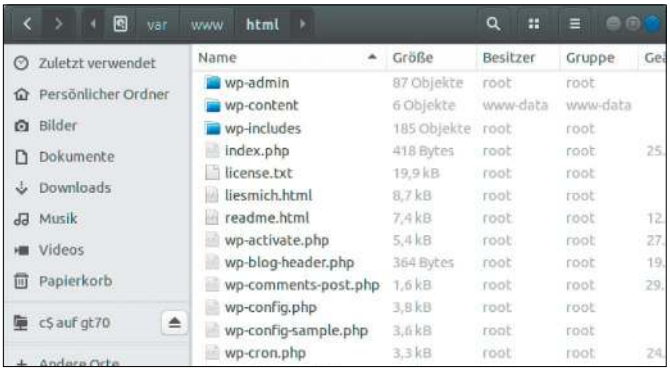
Nach Abschluss der Installation entziehen Sie zur Verbesserung der Sicherheit den Schreibzugriff für den Webserver:

```
sudo chown -R root:root /var/www/
  html
```

Damit Wordpress Dateien im Ordner „wp-content“ ablegen kann, ändern Sie Benutzer und Gruppe:

```
chown -R www-data:www-data /var/
  www/html/wp-content
```

Weitere Informationen zur Absicherung einer Wordpress-Installation finden Sie unter *www.pcwelt.de/8OBeGw*. ■



Rechtevergabe: Aus Sicherheitsgründen sollte der Webserver nur Schreibzugriff auf Ordner unter „/var/www/html“ erhalten, wenn es zwingend erforderlich ist.

PHP-KONFIGURATION ANPASSEN

Einige Probleme, die bei der Arbeit mit einem Content-Management-System auftreten können, sind auf die Script-Sprache PHP und nicht auf den Webserver zurückzuführen. Ein Beispiel dafür ist die Begrenzung der Uploadgröße, die bei Ubuntu auf knappe zwei MB eingestellt ist. Wenn Sie größere Dateien für Ihre Website in Wordpress hochladen, erhalten Sie nur eine Fehlermeldung. Um das zu ändern, öffnen Sie die PHP-Konfiguration im Editor:

```
sudo nano /etc/php/7.0/php.ini
```

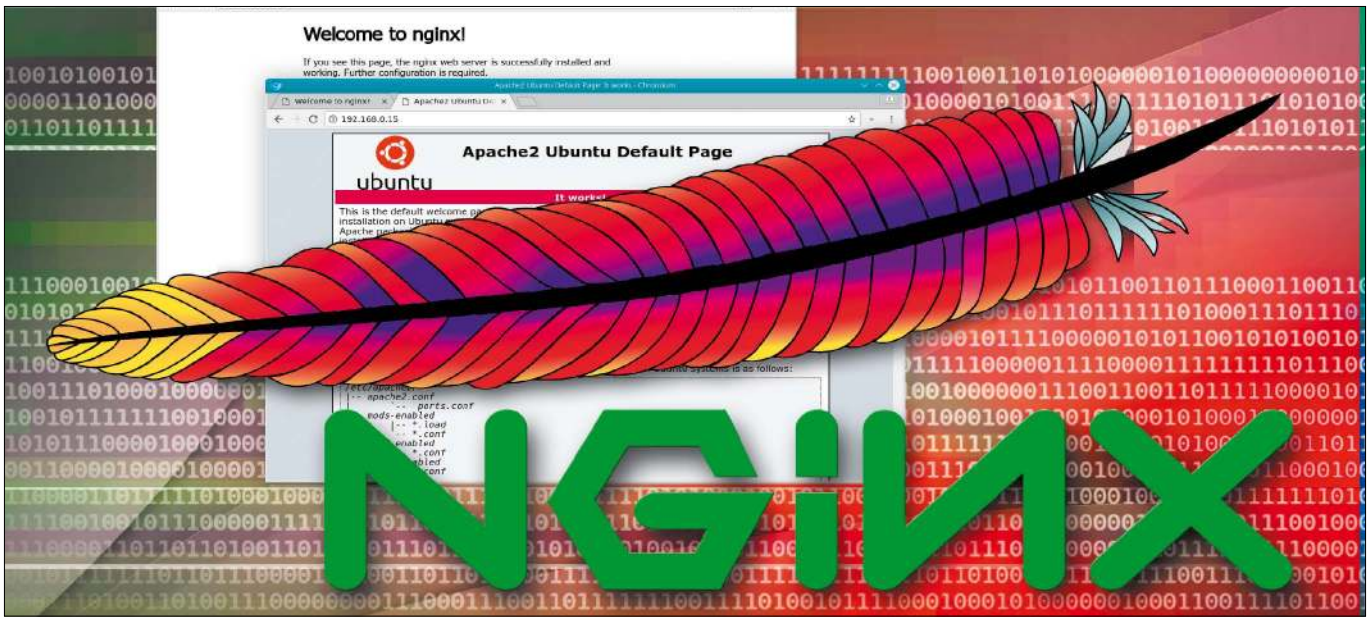
Passen Sie den Pfad für Ihre PHP-Installation an. Ändern Sie die Variablen in der Datei wie folgt:

```
upload_max_filesize = 64M
post_max_size = 64M
max_execution_time = 300
```

Sie erhöhen damit das Dateilimit auf 64 MB und geben Scripts außerdem etwas mehr Zeit für die Ausführung.

Webserver optimieren

Alle Linux-Distributionen haben Apache und Nginx in ihren Paketquellen. Die dabei mitgelieferte Konfiguration geht von leistungsfähiger Hardware aus. Auf schwacher Hardware und unter hoher Last gibt es Anpassungsbedarf.



VON DAVID WOLSKI

Zog der Webserver Apache einst einsam seine Kreise, so drängt inzwischen ein anderer Webserver in die Weiten des Web, wie der Branchendienst Netcraft (*www.netcraft.com*) nach Auswertung von 1,8 Milliarden Domains im Oktober 2017 abermals gezeigt hat: Auf aktiven Sites holt der besonders performante Webserver Nginx mit 21 Prozent Anteil beständig auf (Apache: 44 Prozent).

Gerade die Administratoren großer Webseiten mit viel Traffic schätzen den schlanken Server Nginx, der dank seines Aufbaus sehr effizient arbeitet.

Auch ein schwächlicher Webserver auf einem Raspberry Pi oder auf einem günstigen Rootserver bei einem Webhoster kann mit Nginx zur Hochform auflaufen und mehr Besucher bedienen. Damit ist Apache aber keineswegs obsolet, denn er glänzt mit einer erfreulichen Anzahl an Modulen, die dem Webserver beispielsweise PHP, Perl und Python vergleichsweise unkompliziert beibringen.

Apache oder Nginx: In jedem Fall gibt es nach der Installation mit Standardwerten noch Optimierungspotenzial.

Apache2buddy: Hilfe für Apachen

Eine gute Orientierung, wo es bei einer Apache-Konfiguration noch Bedarf an Feintuning gibt, liefert das Perl-Script „Apache2buddy" (*https://github.com/richardforth/apache2buddy*). Es überprüft nach dem Aufruf in der Shell des Webservers die diversen Konfigurationsdateien einer Apache-Installation und des PHP-Moduls. Das Script gibt Hinweise auf mögliche Probleme und Optimierungsmöglichkeiten.

Der Download des Scripts auf den Webserver erfolgt dort in der Shell direkt mit dem Tool wget:

```
wget https://raw.
  githubusercontent.com/
  richardforth/apache2buddy/
  master/apache2buddy.pl
```

Das Script verlangt root- beziehungsweise sudo-Privilegien zum Aufruf:

```
sudo perl apache2buddy.pl
```

Im Terminal zeigt Apache2buddy nun der Reihe nach die überprüften Parameter an. Am Ende folgt eine Zusammenfassung mit Empfehlungen, wobei die wichtigsten Hinweise rot ausgezeichnet sind. Diese Empfehlungen verlangen meist noch Recherche in der Dokumentation zu Apache (*https://httpd.apache.org/docs/2.4/de*), wo die betreffende Einstellung genau zu finden ist.

Ein praktisches Beispiel: Auf vielen Ein-Platinen-Systemen wie dem Raspberry Pi wird Apache2buddy den Hinweis „Your MaxRequestWorkers setting is too high" und darunter eine Empfehlung geben. Der Parameter „MaxRequestWorkers" befindet sich in der Konfigurationsdatei „/etc/apache2/mods-enabled/mpm_prefork.conf" und hat standardmäßig den Wert „150". Mit einem Texteditor setzen Sie diesen Parameter nun auf den empfohlenen Wert von Apache2buddy und starten den Webserver neu.

Feineinstellungen für Nginx

Auch wenn die Standardkonfiguration für Nginx zunächst weniger Optimierungsbedarf hat, so kann sich auf Servern mit beschränkten Ressourcen die Anpassung folgender Parameter lohnen.

Anzahl der Prozesse: Nginx liefert laut Dokumentation (*www.nginx.com/blog/tuning-nginx*) die beste Leistung, wenn der Server für jeden Prozessorkern einen Prozess startet. Damit dies automatisch geschieht, sollte in der Konfigurationsdatei „/etc/nginx/nginx.conf" der Parameter „worker_processes" diesen Wert haben:

```
worker_processes auto
```

Eine Ausnahme sind schwächliche Platinen wie der Raspberry Pi. Hier sollte die Zahl der „worker_processes" niedriger sein, denn das System ist sonst schnell überlastet und gerät an die Grenzen seines Arbeitsspeichers. Für ältere Raspberry-Pi-Platinen der ersten Generation ist nur der Wert „1" akzeptabel, für den Raspberry Pi 2/3 ist der Wert „2" empfehlenswert.

Anzahl der Verbindungen: Jeder laufende Nginx-Prozess kann maximal eine vorgegebene Zahl an Verbindungen bedienen. Festgelegt ist diese Zahl im Parameter „worker_connections".

```
worker_connections 786
```

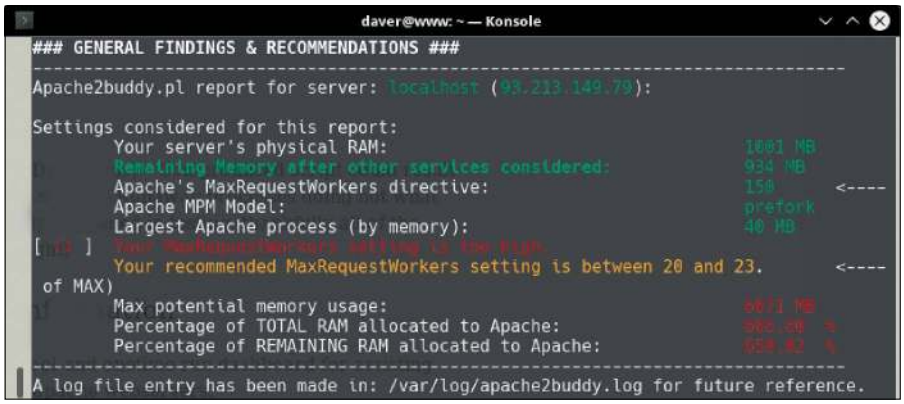
Jeder Webseitenbesuch baut mindestens zwei Verbindungen auf, sodass diese Zahl nicht den maximal möglichen Clients entspricht. Auf einem Serverboliden mit mehreren GB Speicher kann man den Wert auf 1024 erhöhen, auf einer Platine mit begrenztem Speicher eher reduzieren: „512" ist ein passender Wert für einen Raspberry Pi 2/3, „256" ist auf dem Raspberry Pi 1 und Zero realistisch.

Reverse Proxy: Nginx vorschalten

Einen bestehenden Apache-Server gegen Nginx auszutauschen, ist mit Aufwand verbunden. Die größten Hindernisse sind umfangreiche „.htaccess"-Dateien von Apache, die umgeschrieben werden müssen, und die PHP-Konfiguration mittels PHP-FPM ist anspruchsvoller. Oft ist ein Umzug aber gar nicht nötig, denn Nginx erfüllt seinen Zweck auch als umgekehrter Proxyserver, der vor den Apache geschaltet wird und Anfragen annimmt, während sich Apache im Hintergrund ganz auf die dynamischen Inhalte konzentrieren kann. Der Aufbau nennt sich „Reverse Proxy" und setzt einen Apache-Server voraus, denn man auf internen Localhost (127.0.0.1) auf einem hohen Port wie 8000 lauschen lässt. Auf Port 80 nimmt Nginx auf der öffentlich erreichbaren IP-Adresse alle Anfragen entgegen und verbindet sich intern mit Apache, um von dort die angeforderten Inhalte durchzureichen. Im einfachsten Fall gelingt dies in der Site-Konfiguration von Nginx schon mit diesen zwei Zeilen:

```
proxy_pass http://localhost:8000;
include /etc/nginx/proxy_params;
```

Ausführlichere Infos zu „ Nginx als Reverse-Proxy" bietet der Artikel ab Seite 24 in diesem Heft. ■



Apache2buddy in Aktion: Das häufig aktualisierte Perl-Script nimmt auf dem Webserver die Apache-Konfiguration unter die Lupe und gibt Hinweise zur Optimierung.

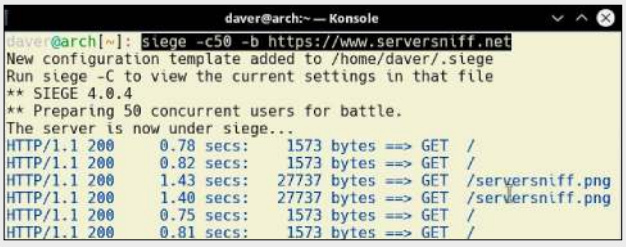
Die Einstellungen von Nginx: Die Parameter „worker_processes" und „worker_connections" sollten auf Ein-Platinen-Computern wie dem Raspberry Pi reduziert werden.

BELASTUNGSTEST: WEBSERVER IM STRESS

Wie sich ein Webserver unter Last verhält, zeigt das Werkzeug „Siege". Es flutet den Zielserver mit eine konfigurierbaren Anzahl von Anfragen und kann schon über eine DSL-Verbindung eine ordentliche Last erzeugen. Es ist deshalb wichtig, nur zeitlich begrenzte Stresstests zu starten – und natürlich sollte man nur eigene Server belagern. Debian, Ubuntu, Mint und Fedora stellen das Tool über das Paket mit dem Namen „siege" bereit. Das Kommando

```
siege -c50 -b [URL]
```

öffnet 50 Verbindungen zur angegebenen Adresse und lässt den Test endlos weiterlaufen, bis ihn die Tastenkombination Strg-C abbricht. Anschließend zeigt Siege eine Statistik der Messwerte an.



Belagerungszustand: Siege öffnet eine vorgegebene Zahl gleichzeitiger Verbindungen zum Server. Es empfiehlt sich, währenddessen auf dem Server die Systemlast im Auge zu behalten.

Webserver absichern

Webserver wie Apache und Nginx schlagen sich in Sachen Sicherheit recht wacker. Oft sind es aber Konfigurationsfehler oder ungünstige Standardeinstellungen, die Angreifern zu viele Systemdetails preisgeben.

VON DAVID WOLSKI

Kritische Lücken in Apache und Nginx sind rar. Verwundbar sind selten die Webserver selbst, eher die darauf laufenden Frameworks, PHP-Projekte und Scripts. Trotzdem gehört zum vernünftigen Setup eines Webservers auch die sicherere, restriktive Konfiguration des Serverdienstes.

Die folgenden Punkte helfen, eine typische Installation von Apache und Nginx besser zu abzusichern. Der wichtigste Punkt gleich vorneweg: Sicherheit verlangt regelmäßige Aktualisierungen – nicht nur der Webserver-Pakete der Linux-Distribution, sondern vor allem Updates des verwendeten CMS, Blogsystems, Shopframeworks oder sonstiger Scripts, die auf dem Server zum Einsatz kommen.

Header: Nicht zu viel verraten

Webserver stellen sich auf HTTP-Anfragen im Antwortheader höflich mit Namen und Versionsnummer vor, aktivierte Module wie PHP ebenfalls. Diese Header lassen Rückschlüsse auf das verwendete System, den Webserver, dessen Module und Softwareversionen zu. Direkt nach der Einrichtung sind diese Infos im Testbetrieb nützlich. Im produktiven Betrieb und im Internet gehen diese Interna aber niemanden etwas an und verraten zu viel über das System. Die standardmäßig aktivierten Versionsinfos in Apache und Nginx sind aber schnell deaktiviert.

Apache: In Debian/Ubuntu/Raspbian ist die Konfigurationsdatei „/etc/apache2/conf-available/security.conf“ verantwortlich. In der Datei muss nur die Zeile „ServerTokens OS“ zu

```
ServerTokens Prod
```

geändert werden, gefolgt von einem Apache-Neustart. Danach sind die Angaben zu Apache-Version und Modulen aus dem Header getilgt.

Nginx: Die Einstellung von Nginx, die eine Versionsangabe im Header unterdrückt, ist in der Datei „/etc/nginx/nginx.conf“ untergebracht. Innerhalb der HTTP-Sektion, die mit

```
http {
```

beginnt, fügen Sie vor der abschließenden geschweiften Klammer als letzte Zeile diese Angabe ein:

```
server_tokens off;
```

PHP: Auch der PHP-Interpreter für Webserver ist geschwätzig und verrät in der Standardkonfiguration seine Versionsnummer. Diese Einstellung ist unabhängig vom verwendeten Webserver in der Datei „php.ini“ zu finden.

Deren Speicherort ist je nach Version und Installationsart verschieden. Ist PHP (Version 7.0) als Apache-Modul eingerichtet, so liegt die relevante „php.ini“ im Verzeichnis „/etc/php/7.0/apache2/php.ini“. Falls PHP für Nginx als externer Script-Interpreter über das Paket „PHP-FPM“ installiert ist, dann findet sich diese Datei unter „/etc/php/7.0/fpm/php.ini“.

In der Datei muss die Zeile

```
expose_php = On
```

nach

```
expose_php = Off
```

geändert werden

Nicht vergessen: Nach jeder dieser Änderungen ist ein Neustart des Webservers mit

```
sudo service apache reload
```

beziehungsweise

```
sudo service nginx reload
```

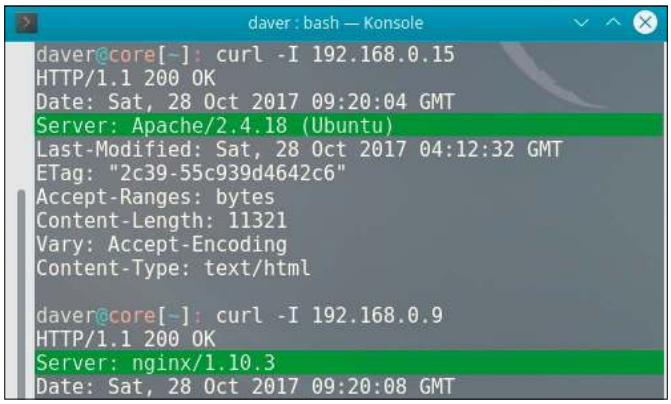
im Fall von Nginx nötig. Außerdem muss das Modul „PHP-FPM“, das unabhängig vom Webserver-Dienst läuft, mit folgendem Befehl

```
sudo service php7.0-fpm restart
```

neu geladen werden.

Extra-Sicherheit per Modul

Wer immer einen Dienst anbietet, sei es nur ein Webserver mit statischen HTML-Seiten, erst recht mit dynamischen Inhalten per PHP, wird irgendwann die Bekanntschaft mit automatisierten Scanprogrammen wie Nikto (siehe Kasten) machen.



Versionsnummern im HTTP-Header: Dieser curl-Befehl zeigt die Header einer HTTP/-HTTPS-Antwort an – in diesem Fall die Versionen von Apache und Nginx.

Antwort verweigert: Auch Nginx lässt sich über ein eingebautes Modul so konfigurieren, dass der Server eine Anfrageflut mit einer 503-Meldung quittiert.

Apache: Mit dem Extra-Modul „libapache2-mod-evasive“ weicht Apache typischen Scanattacken, massenhaften Seitenaufrufen und einfachen Angriffen selbständig aus. Wird eine Seite in schneller Folge von einer IP-Adresse aus mehrmals pro Sekunde angefordert oder werden 50 gleichzeitige Requests pro Apache-Prozess ausgelöst, dann landet diese IP-Adresse einige Sekunden auf einer schwarzen Liste und erhält nur eine 403-Meldung (Forbidden). Die Erweiterung ist in Ubuntu/Debian/Raspbian mittels des Kommandos

```
sudo apt-get install libapache2-
 mod-evasive
```

leicht installiert. Auch Cent-OS kennt das Modul unter diesem Namen und unter Open Suse nennt es sich „apache2-mod-evasive“. Nach einem Neustart des Webservers ist das Modul mit Standardregeln aktiv. Das Modul lässt sich leicht bei einem Besuch des Webservers im Browser durch einen häufigen Druck auf die F5-Taste testen.

Nginx: Für diesen Webserver gab es bis vor einigen Jahren das Tool Naxsi, dessen Entwicklung aber momentan ruht. Es empfiehlt sich, Nginx gegen die Flutung mit Anfragen über das eingebaute Modul „ngx_http_limit_req_module“ zu schützen. Dazu öffnen Sie die Konfigurationsdatei „/etc/nginx/nginx.conf“ mit root-Recht in einem Texteditor und fügen im Abschnitt „http {“ die Zeile

```
limit_req_zone $binary_remote_addr
  zone=one:10m rate=1r/s;
```

ein. In der Sitekonfiguration, die in Debian/Ubuntu/Raspbian üblicherweise unter „/etc/nginx/sites-available/default“ liegt, kommt nun noch in die Sektion „server {“ folgende Zeile:

```
limit_req zone=one burst=5;
```

Nach einem Neustart wird Nginx auf zu häufigen Anfragen mit einer 503-Meldung antworten („Temporary unavailable“). Weitere Beispiele zu diesem Modul nennt die Nginx-Dokumentation unter *http://nginx.org/en/docs/http/ngx_http_limit_req_module.html*.

SCANNER: WEBSERVER IM CHECK

Kaum jemand macht sich die Mühe, alle potenziellen Schwachstellen und Konfigurationsfehler eines Webservers manuell abzuklopfen.

Das ist auch nur in Ausnahmen nötig, denn für die üblichen Schwachpunkte gibt es Scanprogramme, die einen Check weitgehend automatisieren.

Nikto: Nikto ist ein Tool, das systematisch bei der Analyse von möglichen Konfigurationsfehlern hilft (*https://cirt.net/Nikto2*). Es ist ein Kommandozeilenprogramm und überprüft einen Webserver auf 6700 typische Probleme, die ein potenzielles Risiko darstellen. Installiert ist Nikto in den verbreiteten Linux-Distributionen schnell über den jeweiligen Paketmanager, in Debian/Ubuntu beispielsweise mit diesem Kommando:

```
sudo apt-get install nikto
```

Um einen Webserver zu untersuchen, dient dieser Aufruf:

```
nikto -h [Hostname/IP]
```

Nikto wird im Terminal nach seinen Checks ein ausführliches Protokoll mit weiterführenden Infos ausgeben.

Wapiti: Dieser Scanner ist in Python programmiert und sucht genauer nach Problemen auf Webauftritten. Wapiti (*http://wapiti.sourceforge.net*) sucht nach unsicheren PHP-Includes, nach potenziellem Cross-Site-Scripting, SQL-Injections, verräterischen Dateien und fehlerhaften Webserver-Regeln in „.htaccess“-Dateien. Aus den Paketquellen von Debian/Ubuntu installiert das Kommando

```
sudo apt-get install wapiti
```

den Scanner. Der Befehl

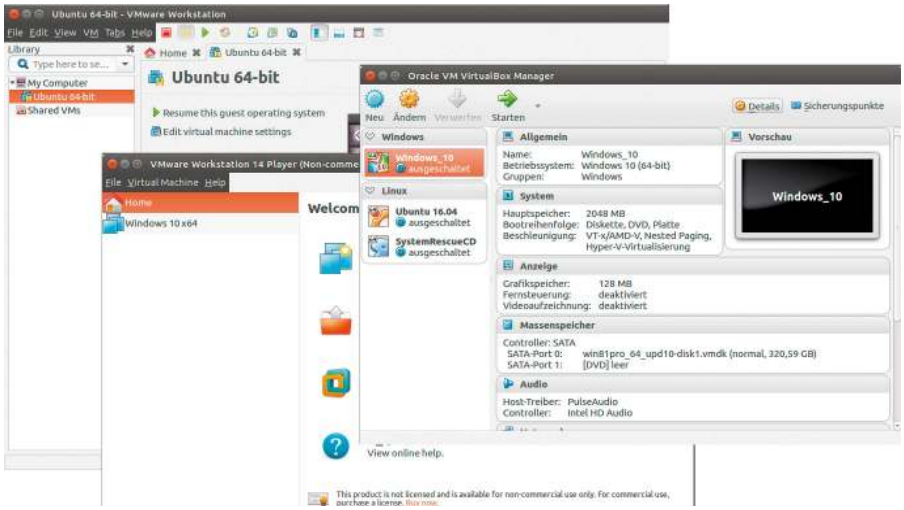
```
wapiti [URL] -v 1 -n 99 -b folder
```

startet einen Check der angegebenen URL. Die Ergebnisse präsentiert Wapiti in einer HTML-Datei, die nach dem Scan im Verzeichnis „~/.wapiti/generated-reports“ liegt.

Wapiti wurde fündig: Auf unserer Test-Site hat der automatische Scanner eine Cross-Site-Scripting-Schwachstelle gefunden und präsentiert diese in seinem Report.

Grundlagen der Virtualisierung

Dank Virtualisierungstechnologie lassen sich unter Linux auch Windows-Anwendungen nutzen. Virtualisierung ist aber auch für System- oder Softwaretests interessant.



Virtualisierungssoftware: Virtualbox und Vmware Workstation Player sind ohne große Einarbeitung leicht zu bedienen. Vmware Workstation bietet zusätzliche Funktionen für Profis.

VON THORSTEN EGGELING

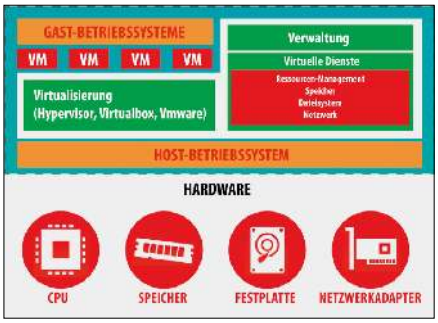
Wer mehrere Betriebssysteme auf seinem PC nutzen möchte, muss diese nicht nebeneinander auf der Festplatte installieren. Einfacher geht's mit Virtualisierungssoftware, über die sich weitere Systeme in einem Fenster oder bildschirmfüllend starten lassen. Das ist praktisch, wenn Sie neue Betriebssysteme 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 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 Verbesse-



Begrenzter Zugriff: Ein Gastsystem („VM") kann die Hardware im PC nicht direkt verwenden. Virtuelle Dienste sorgen für die Zuteilung etwa von Speicher.

rung der Geschwindigkeit führen kann. Der Kernel muss dafür speziell angepasst sein, was aber bei aktuellen Linux- und Windows-Systemen standardmäßig der Fall ist.

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 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.

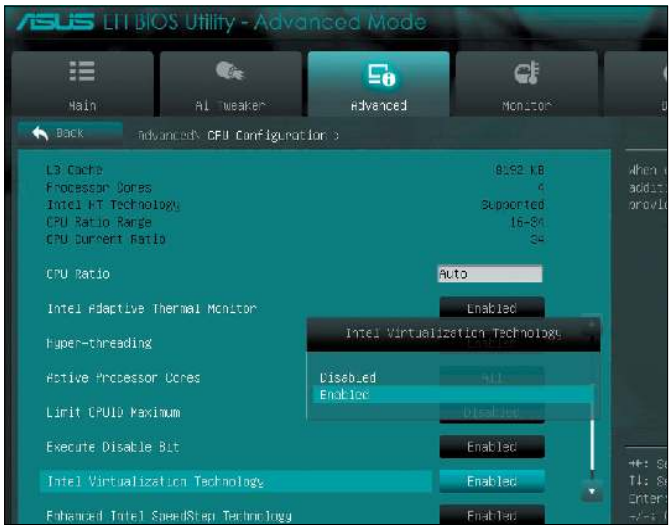
Dahinter verbirgt sich die I/O-Virtualisierung („Input/Output"), über die sich der Datenaustausch mit Netzwerkadaptern, Grafikchips und Festplatten-Controllern beschleunigen lässt.

Virtualisierungssoftware wie Virtualbox oder Vmware (siehe die beiden nachfolgenden Artikel) funktioniert notfalls auch ohne direkte Hardwareunterstützung – wenn

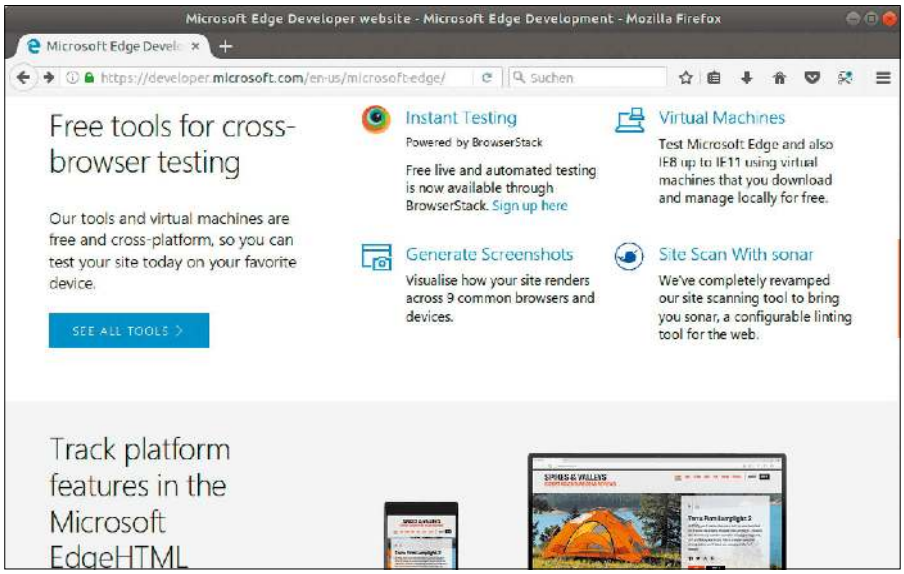
Virtualisierungserweiterungen: „cat /proc/cpuinfo" gibt Infos zum Prozessor aus. Erscheint bei einer Intel-CPU „vmx", dann lässt sich Intel-VTx zur Beschleunigung nutzen.

VIRTUALISIERUNGSSOFTWARE 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.

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 verwendet 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.

Für Profis: Virtualisierung mit 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

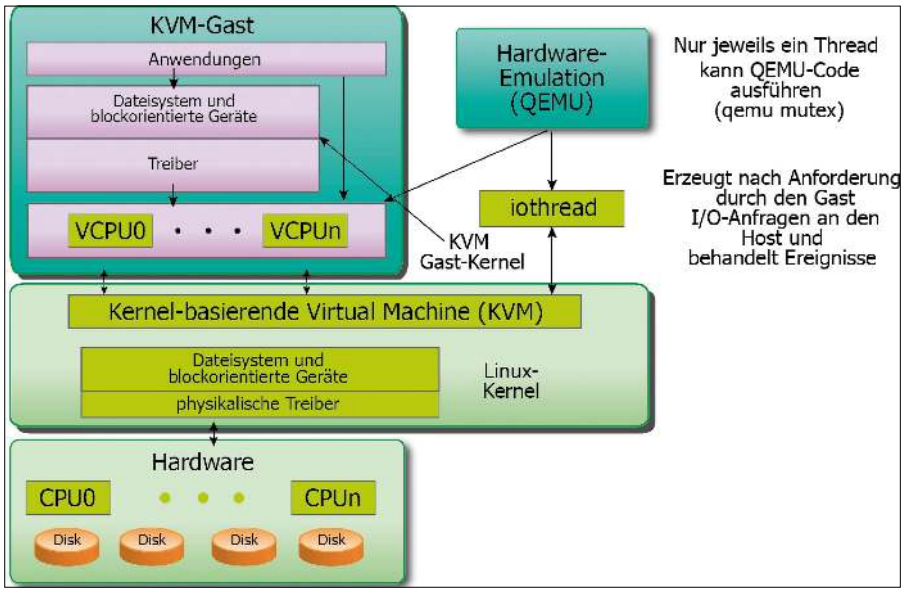
gehören nicht zum KVM-Projekt. Als grafisches Front-End dient der Virtual Machine Manager (*https://virt-manager.org*), der in den Repositories der meisten populären Distributionen enthalten ist. Die Verbindung zur Grafikausgabe des Gastsystems erfolgt über VNC oder über das Protokoll Spice.

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. Ausführliche Infos und Tipps zu KVM finden Sie auf *www.pcwelt.de/2199855*. ■



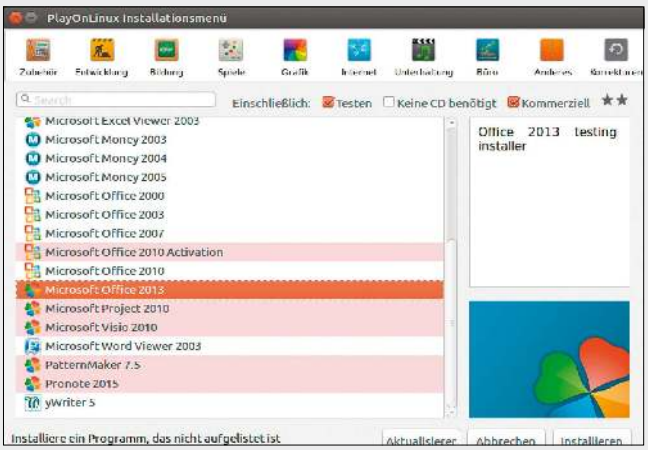
Eingebauter Virtualisierer: Im Linux-Kernel ist die Virtualisierungssoftware bereits enthalten. Die Paravirtualisierung sorgt für eine gute Leistung bei Linux-Gastsystemen.

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.



Es muss nicht immer Virtualisierung sein: Mit Playonlinux lassen sich einige Windows-Anwendungen auch unter Linux installieren und nutzen.

Vmware in der Praxis

Vmware ist einer der bekanntesten Hersteller für Virtualisierungssoftware. Vmware Workstation ist eher für Profis gedacht, der kostenlose Player leistet aber auch privaten Anwendern gute Dienste.

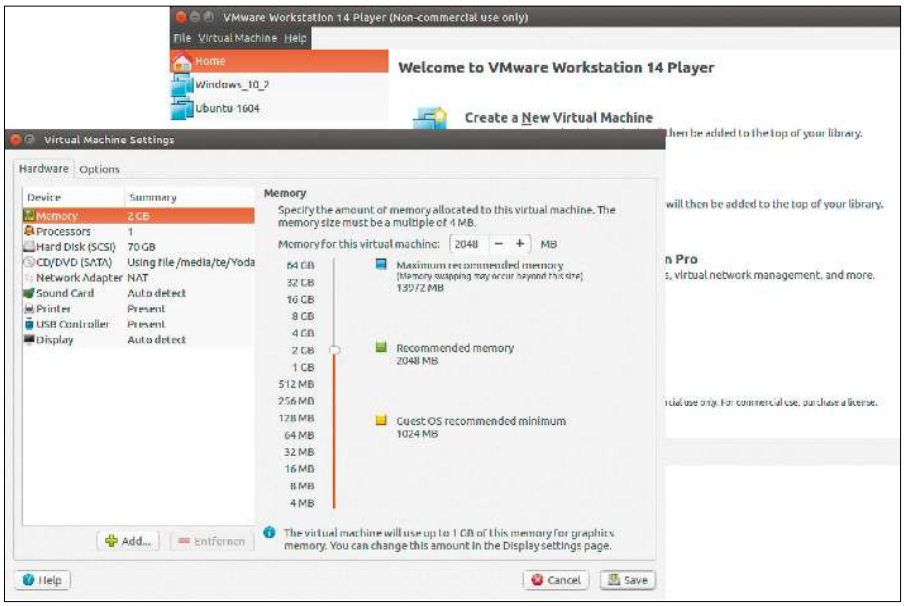
VON THORSTEN EGGELING

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 46) 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.



Kleine Einschränkungen: Der kostenlose Vmware Player bietet bewährte Stabilität, aber nicht alle Funktionen der Bezahlsoftware Vmware Workstation Pro.

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 diesen Befehl

```
sudo sh Downloads/Vmware-
  Player-7.1.4-3848939.x86_64.
  bundle
```

oder für Vmware Workstation Pro den folgenden Befehl

```
sudo sh Downloads/VMware-
  Workstation-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) bezie-

hungsweise „Help -> Enter Serial Number“ (Workstation) eingeben.

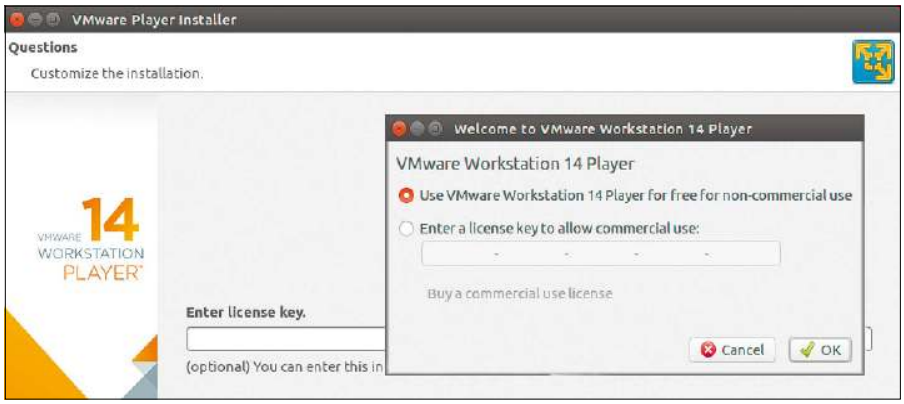
Vmware-Software deinstallieren: Um Vmware Workstation wieder zu entfernen, verwenden Sie diese Befehlszeile im Terminal:

```
sudo sh Downloads/Vmware-
 Workstation-Full-14.0.0-6661328.
 x86_64.bundle -u vmware-
 workstation
```

Den Player werden Sie mit dieser Zeile

```
sudo sh Downloads/Vmware-
 Player-7.1.4-3848939.x86_64.
 bundle -u vmware-player
```

wieder los.



Mit oder ohne Lizenz: Private Nutzer dürfen Vmware Player ohne Lizenzschlüssel installieren, müssen aber eine nicht-kommerzielle Verwendung noch einmal bestätigen.

2. Linux oder Windows in einer VM installieren

Nach dem Start des Vmware Workstation Players klicken Sie auf „Create a New Virtual Machine“.

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 Softwareinstallationen 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

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“.

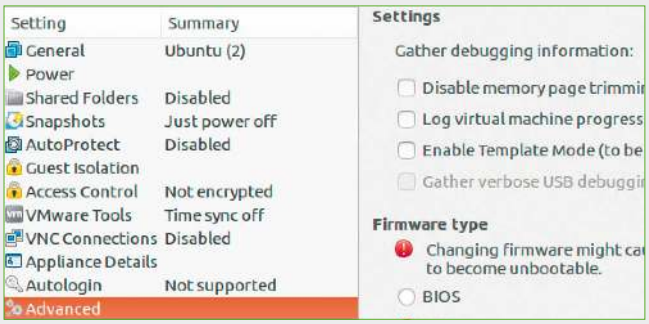
Da der Player die mit der Workstation erstellten VMs öffnen kann, beherrscht auch er diese Einstellungen, bietet diese Optionen jedoch nicht an. Stattdessen öffnen Sie hier die Konfigurationsdatei der virtuellen Maschine in einem Texteditor wie in Punkt 6 beschrieben. Fügen Sie ganz am Ende die Zeile

```
firmware = "efi"
```

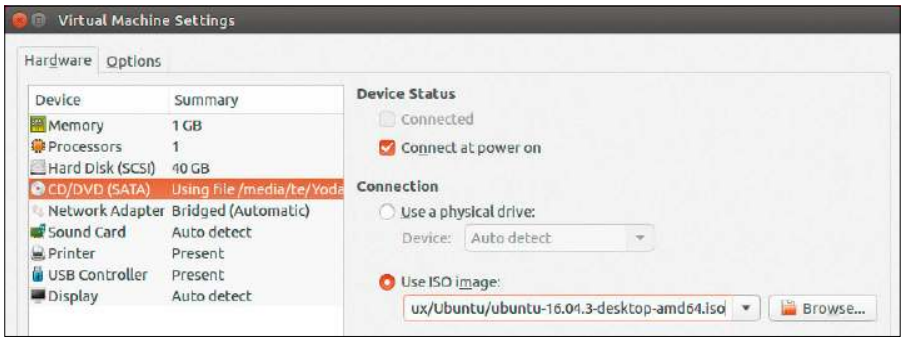
ein, für Secure Boot zusätzlich diese Zeile:

```
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.

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 46. 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 Vmware-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
```

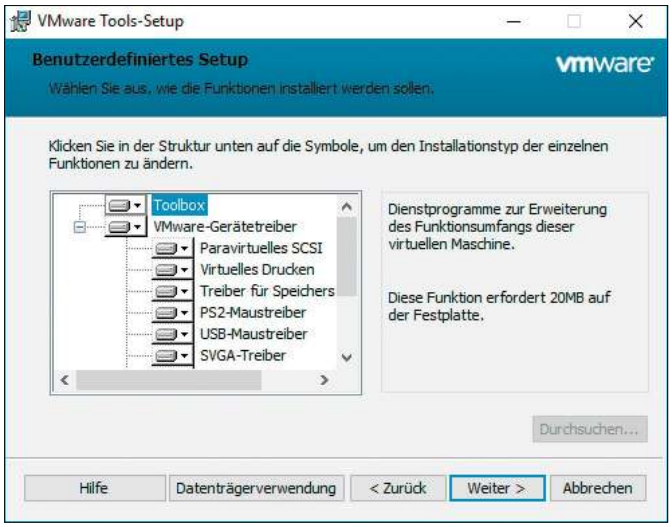
Bei anderen Linux-Systemen oder alternativ auch unter Ubuntu verwenden Sie die Standard-Installationsmethode:

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 „VmwareTool-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 folgenden Terminalbefehl ein:

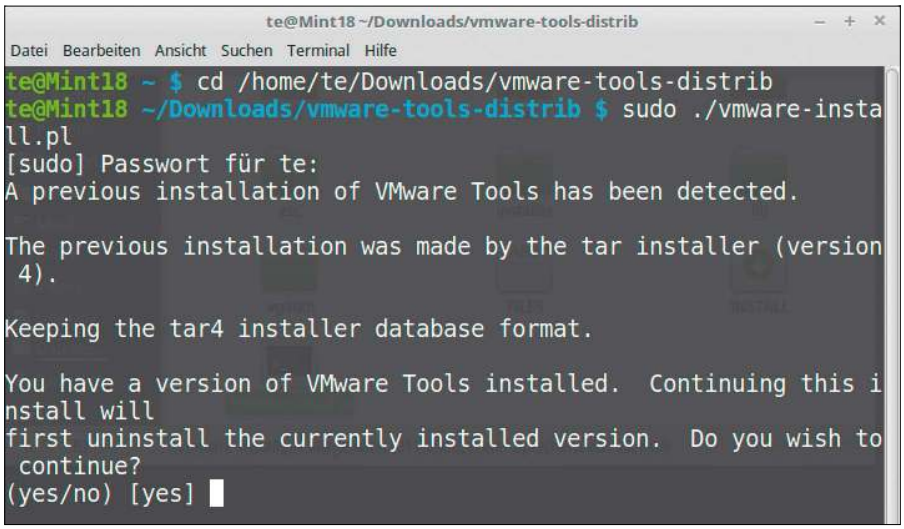
```
sudo Downloads/vmware-tools-
  distrib/vmware-install.pl
```



Vmware-Tools-Setup: Unter Windows müssen Sie nur auf „Virtual Machine -> Install VMware Tools" gehen, das Setup starten und den Anweisungen des Assistenten folgen.

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 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.



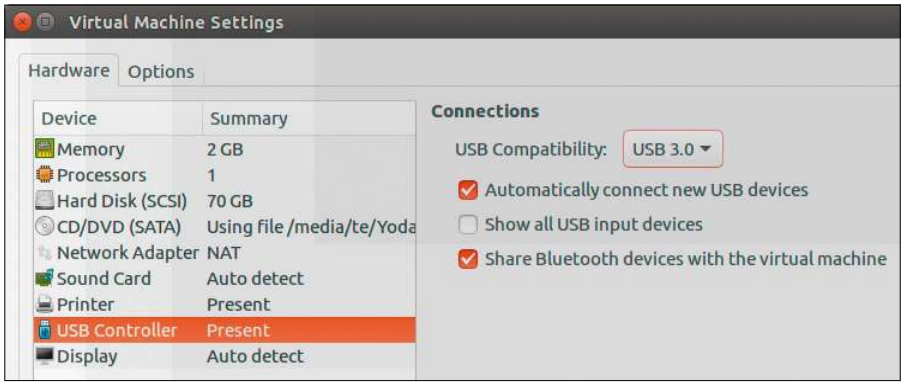
Vmware-Tools installieren: Linux-Nutzer müssen für die Einrichtung das Terminalfenster bemühen, aber auch hier führt ein Assistent schnell durch die Installation.

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-Geräte 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



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.

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

APPLIANCES: FERTIGE VMS NUTZEN

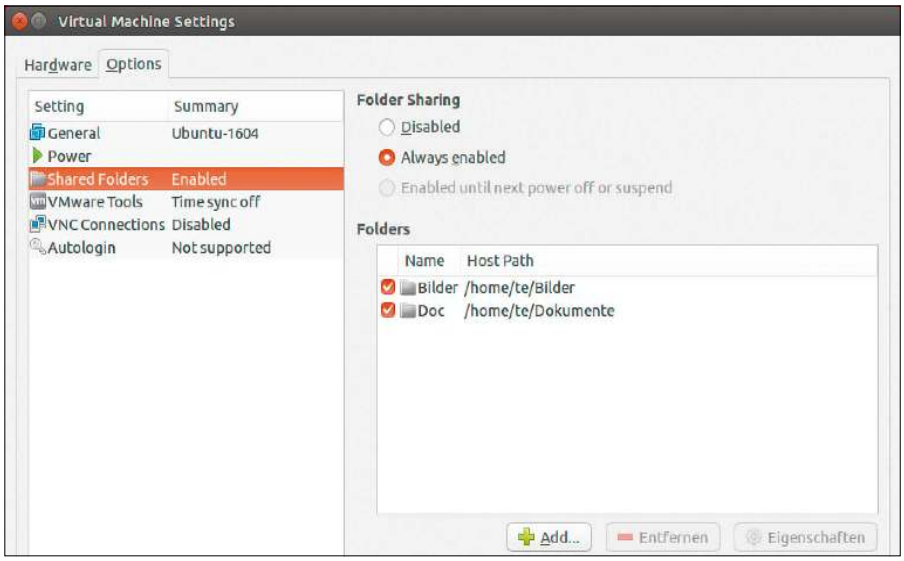
Vmware Player kann Abbilder mit vorbereiteten virtuellen Maschinen importieren. Gehen Sie auf „Open a Virtual Machine“ und wählen Sie die gewünschte „ovf“- oder „ova“-Datei aus. Da es sich um ein universelles Austauschformat handelt, kann die Software auch Dateien einlesen, die Sie in Virtualbox über „Datei -> Appliance exportieren“ gespeichert haben. In Vmware Workstation verwenden Sie „File -> Export to OVF...“. Der Player besitzt keine Exportfunktion.

Fertige virtuelle Maschine 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.

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. Erpressungstrojaner 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 und Drop funktioniert zwischen allen Betriebssystemen meist ebenfalls zuverlässig, etwa zwischen dem Dateimanager oder Desktop des Host- und Gastsystems.



Datenaustausch: Über gemeinsam genutzte Ordner („Shared Folders“) übertragen Sie bequem Dateien zwischen Host- und Gastsystem.

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.

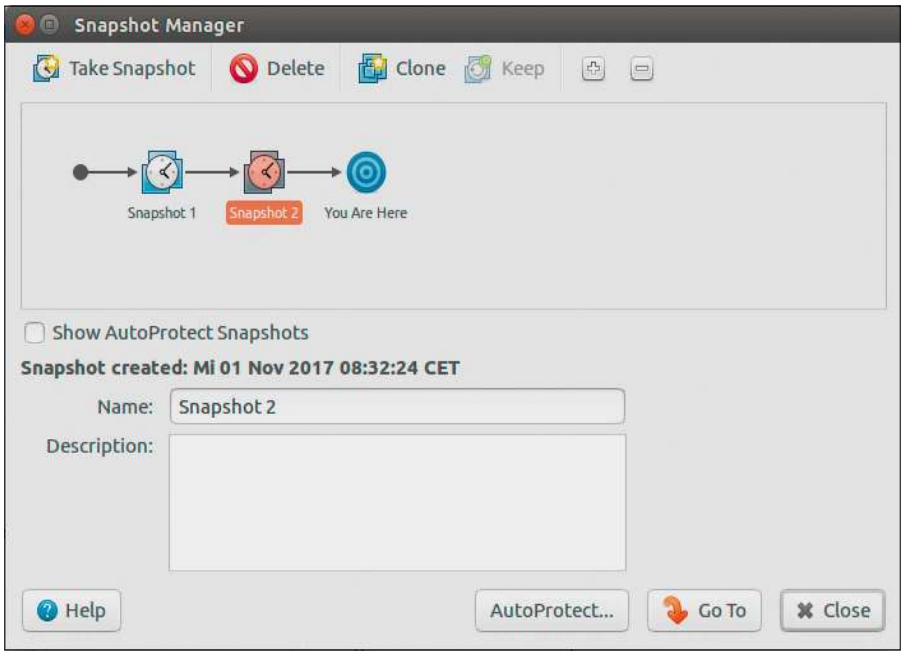
7. Sicherungspunkte erstellen

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 ->

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.

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. ■

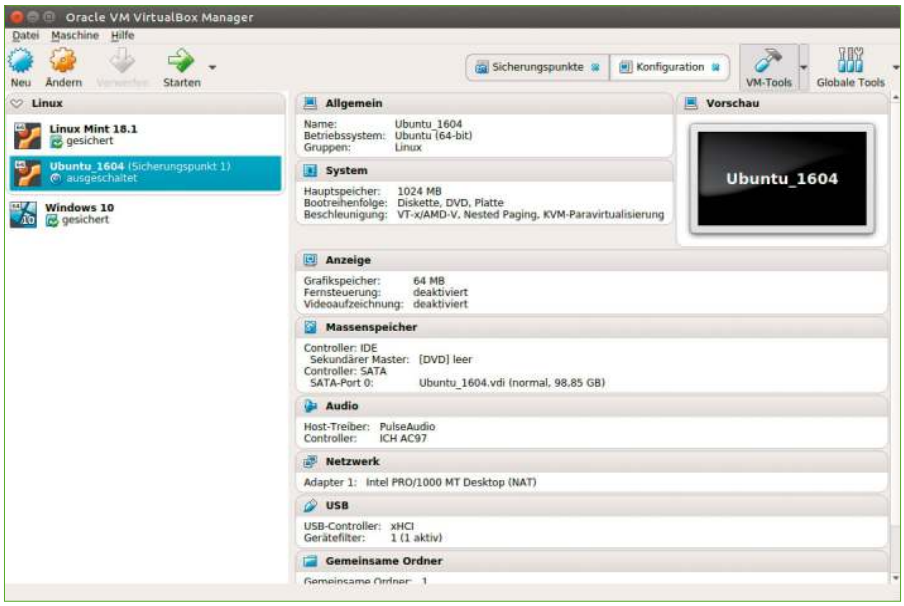
IM VERGLEICH: VMWARE PLAYER UND WORKSTATION PRO

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
  virtualbox-qt virtualbox-dkms
```

Damit installieren Sie zur Zeit beispielsweise unter Ubuntu 16.04 die Version 5.0.40 von Virtualbox. Aktuell war bei Redaktionsschluss die Version 5.2.0, 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 5.2.0 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.
  virtualbox.org/virtualbox/debian
  xenial contrib > /etc/apt/sources.
  list.d/virtualbox.list
sudo apt update
sudo apt-get install dkms
  virtualbox-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 auch, ob Intel-Vt-x beziehungsweise AMD-V aktiviert sind (siehe Artikel ab Seite 36).
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
  virtualbox-qt virtualbox-dkms
```

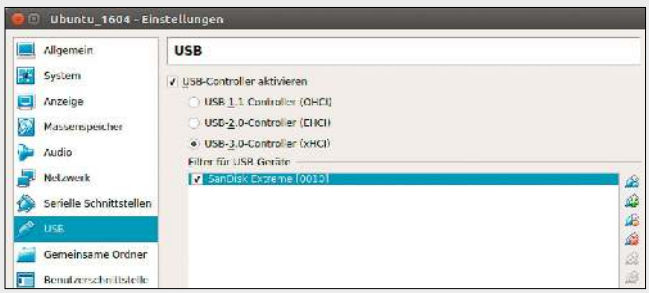
eine bestehende Installation, bevor Sie beispielsweise Virtualbox 5.2 installieren.

Aktuellere Version: Oracle bietet ein fertiges deb-Paket für Virtualbox 5.2 an, das sich über das Paketmanagement („Ubuntu Software“) installieren lässt.

DIREKTER ZUGRIFF: USB-KONFIGURATION ANPASSEN

Eine virtuelle Maschine hat keinen direkten Zugriff auf die Hardware des Host-PCs. Eine 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.

2. Erweiterungspaket installieren

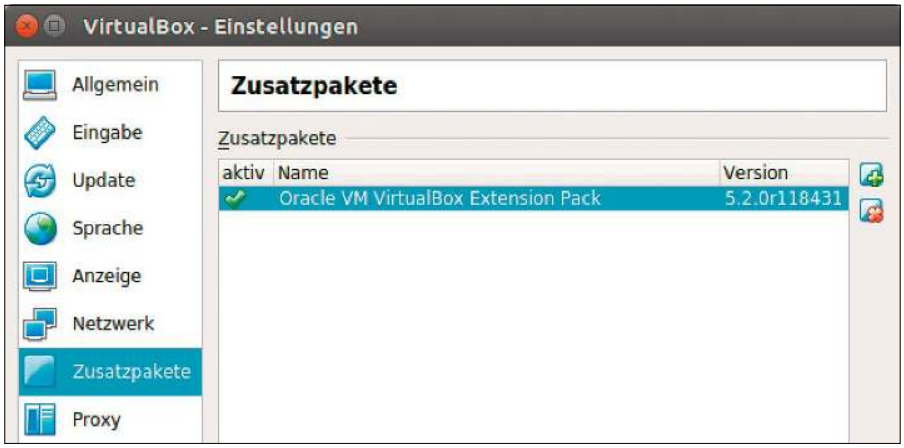
Das Virtualbox-Basispaket steht unter der Lizenz GNU General Public License V2, der Quellcode ist frei verfügbar. Weitere Komponenten stellt Oracle als Erweiterungspaket unter der Personal Use and Evaluation License (PUEL) zur Verfügung. Für private Nutzer, Bildungszwecke oder Testumgebungen ist die 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.



Funktionserweiterung: Über ein Zusatzpaket rüsten Sie beispielsweise die Unterstützung für USB-3.0-Geräte im Gastsystem nach.

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 (siehe Seite 40). 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 Updates und Softwareinstallationen bleibt. Eine virtuelle Festplatte lässt sich später nur umständlich vergrößern. Sie können aber jederzeit eine zweite Festplatte in den virtuellen PC „einbauen“.

Neues Gastsystem: Geben Sie Typ und Version des Gastbetriebssystems an. Virtualbox setzt dann automatisch die passenden Einstellungen.

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.

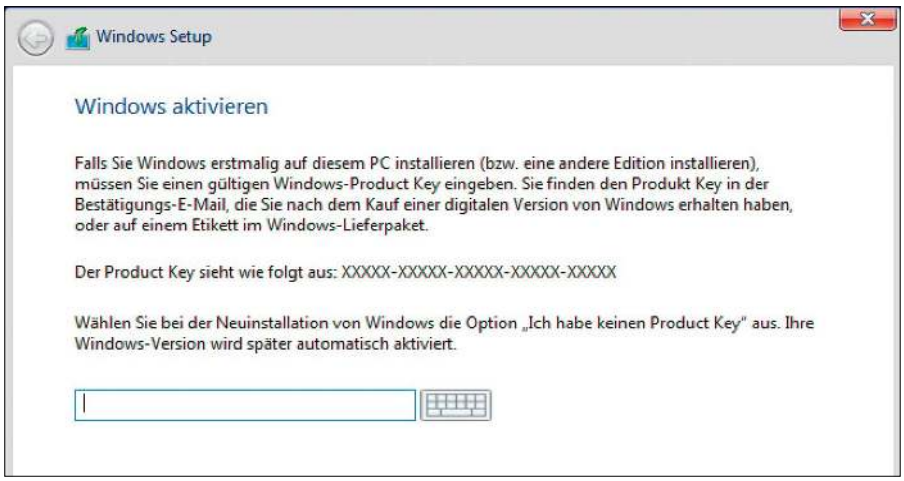
Virtuelle Festplatte: Dynamische Festplatten belegen anfänglich nur wenig Platz, sind aber langsamer als virtuelle Laufwerke mit fester Größe.

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.

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.

Tipp: Einen in der virtuellen Maschine „gefangenen“ Mauszeiger befreien Sie über die „Host-Taste“. Das ist standardmäßig die rechte Strg-Taste.

5. Windows in Virtualbox installieren

Die Installation eines Windows-Gastsystems läuft ab wie bei Linux. Nach 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 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.

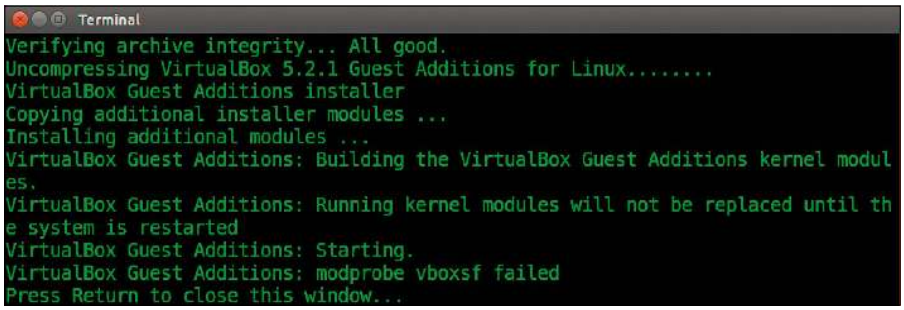
Probleme bei der Installation: Die Gasterweiterungen der Version 5.2.0 ließen sich bei Redaktionsschluss im November 2017 unter Ubuntu 16.04 (Kernel 4.10.0-28) nicht kompilieren. Wahrscheinlich sind auch andere Distributionen mit neueren Kerneln betroffen. Auf der Seite *www.virtualbox.org/wiki/Downloads* 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 „Geräte -> Optische Laufwerke -> Abbild auswählen“ in die virtuelle Maschine ein und installieren diese dann.

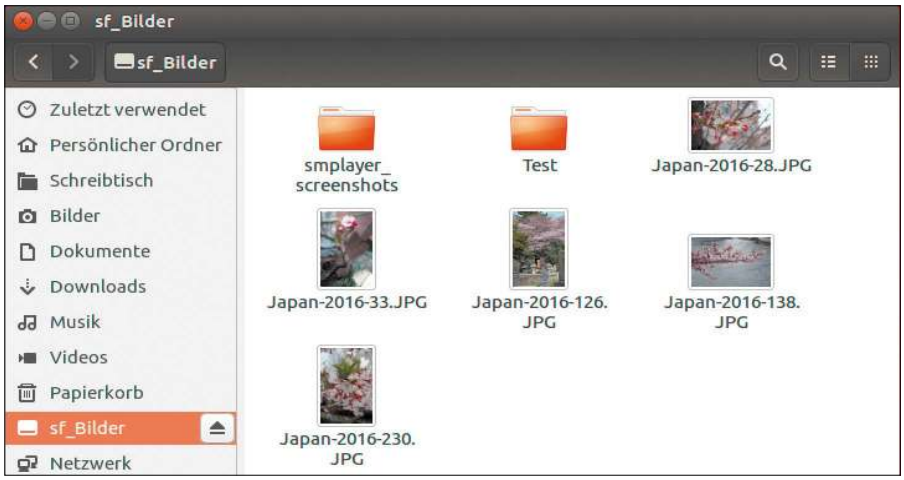
Die Fehlermeldung „modprobe vboxsf failed“ ist immer zu sehen, weil sich das Modul nicht laden lässt, solange sich die ältere Version des Moduls „vboxguest“ noch im Speicher befindet. Starten Sie das Gastsystem neu und ermitteln Sie die geladenen Module mit

```
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. ■

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 – insbesondere auf mobilen USB-Datenträgern, die einen ganzen Linux-Werkzeugkasten mitbringen sollen.

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:

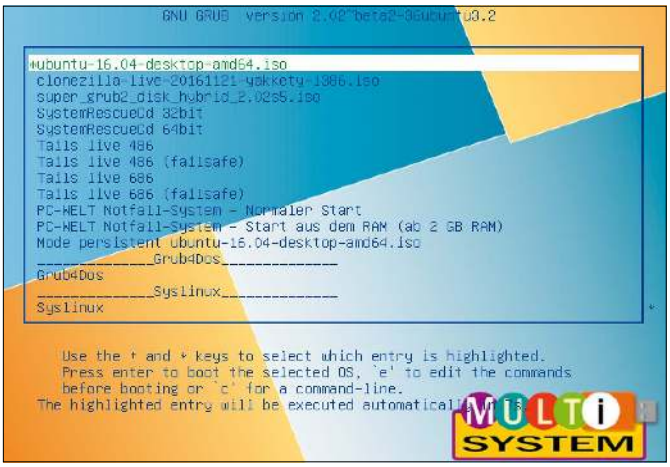
1. Unter Linux geht das am einfachsten über das Tool Multisystem, für das Sie einen FAT32-formatierten USB-Stick benötigen. Installieren Sie das Tool in einem Terminalfenster über die folgenden vier Zeilen:

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

Starten Sie dann Multisystem, 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.

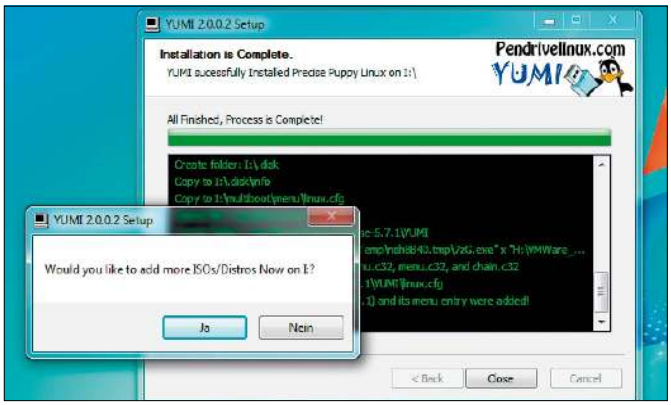
Per Klick auf das Augen-Symbol blenden Sie ein erweitertes Menü ein. Bei Ubuntu-Systemen können Sie über die Schaltfläche mit dem Disksymbol einen persistenten Speicher einrichten: Das bedeutet, dass das an

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 auch nicht unterstützte Systeme einbauen.



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

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 Ziellaufwerk, 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.



Multiboot mit Yumi: Das Windows-Tool kopiert Schritt für Schritt mehrere Linux-Livesysteme (ISO-Abbilder) auf den USB-Datenträger und erstellt dort ein Auswahl-Bootmenü.

Ubuntu-Installer: Bei erkanntem existierendem System bietet das Setup die Teilung der bestehenden Partition an, wobei die Partitionsgrößen per Maus skalierbar sind.

Multiboot von installierten Linux-Systemen

Technisch völlig verschieden vom Start mehrerer Livesysteme ist ein Multiboot von ordentlich installierten Linux-Systemen. Und auch hier sind noch einmal zwei verschiedene Situationen zu unterscheiden:

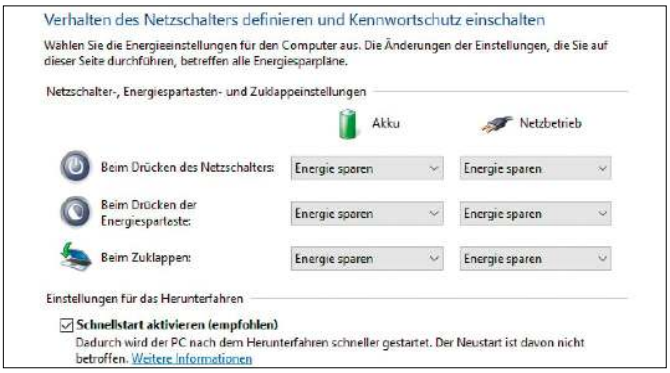
Linux-Multiboot auf Festplatte: Soll auf einem PC mit Linux-Betriebssystem ein weiteres Linux installiert werden, hängt die richtige Vorgehensweise vom Installer des neuen Systems ab. Während sich alle Installer inzwischen sorgsam hüten, ein vorhandenes Windows zu shreddern, ist Linux-Rücksicht untereinander ungewiss. Der Ubuntu-Installer erkennt nach unserer Erfahrung die meisten bereits vorhandenen Linux-Systeme und bietet dann unter „Installationsart“ die Parallelinstallation genauso an wie nachfolgend unter „Linux und Windows“ (Schritt 3) beschrieben. Die Partitionierung, im Bedarfsfall die Verkleinerung der bestehenden Partition, erfolgt dann weitgehend automatisch. Bei jedem Installer, der das bestehende Linux nicht erkennt, hilft nur die manuelle Partitionierung wie bei der USB-Installation.

Linux-Multiboot auf USB: Linux läuft uneingeschränkt auf USB-Medien, jedoch ist das Setup auf eine Einrichtung auf die interne Festplatte ausgelegt. Wenn Sie mehrere Linux-Distributionen ordentlich (nicht bloß als Livesystem) auf USB einrichten möchten, ist manuelle Partitionierung zwingend. Im Falle des Ubuntu-Installers heißt das, dass Sie im entscheidenden Dialog „Installationsart“ den Punkt „Etwas An-

deres“ wählen müssen. Für das erste System muss das Laufwerk neu partitioniert und formatiert werden. Klicken Sie auf die „-“-Schaltfläche, um vorhandene Partitionen zu entfernen. Erstellen Sie dann über die „+“-Schaltfläche so viele Partitionen, wie Sie vorhaben, Systeme einzurichten. Eine zusätzliche Swappartition ist nicht notwendig. Für das aktuelle installierte System wählen Sie hinter „Einbindungspunkt“ den Eintrag „/“ aus der Liste.
Unter „Gerät für die Bootloader-Installation“ wählen Sie unbedingt das USB-Medium aus, auf dem Sie installieren – beispielsweise „/dev/sdb“. Klicken Sie zum Abschluss auf „Jetzt installieren“.
Die Einrichtung der nachfolgenden Linux-Systeme verläuft analog. Sie müssen nur darauf achten, in die noch ungenutzten Partitionen zu installieren.

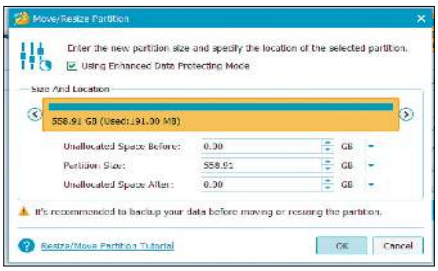
Linux und Windows parallel

Wer Windows nur benötigt, um einmal im Monat seine Überweisungen per Homebankingsoftware zu senden, spart sich Zeit und potenzielle Fehlerquellen, wenn er Windows unter einem Virtualisierungsprogramm installiert (siehe die Artikel zu Vmware und Virtualbox in diesem Heft, Seite 40 und 46 ff.). Geht es um häufigen Einsatz und optimale Leistung, kommt man aber um ein Multiboot-System nicht herum:
Schritt 1: Windows sollte zuerst installiert werden, da Windows bei der Installation standardmäßig die Grub-Bootumgebung von Linux überschreibt. Dies ist keine Katastrophe, zieht aber lästige Hilfsmaßnahmen mit der Super Grub Disk und der Grub-Reparatur nach sich (siehe unten).
Schritt 2: Wer nach installiertem Windows mit dem Aufspielen des ersten Linux-Systems beginnt, muss unter Windows zwei Optionen kontrollieren, die regelmäßig zu Problemen führen. Zum einen sollte der Schnellstart in den Systemeinstellungen unter den „Energieoptionen“ ausgeschaltet werden. Dort gibt es einen Eintrag, der bestimmt, was beim Drücken des Netzschalters passieren soll. Wenn Sie hier mit dem Link die Einstellungen freischalten, die „momentan nicht verfügbar“ sind, findet sich unter „Einstellungen für das Herunterfahren“ die Option „Schnellstart“. Diese Option müssen Sie deaktivieren.
Kontrollieren Sie in den „Eigenschaften“ der Festplatte zusätzlich, ob sich um einen „dynamischen Datenträger“ handelt. Mit



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

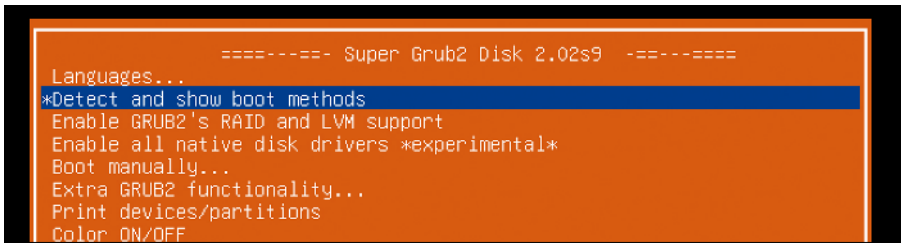
dieser Art der Partitionierung kann keine Installationsroutine von Linux umgehen.
Schließlich booten Sie den Rechner, unterbrechen den normalen Start (F2, F8, Esc und andere Varianten) und gehen in das Bios. Suchen Sie dort die Option „fastboot“, um sie auf „disabled“ zu setzen.
Schritt 3: Jetzt kann es mit der eigentlichen Installation des ersten Linux losgehen. Das Setup sollte das vorhandene Windows erkennen und eine friedliche Koexistenz vorschlagen. So markiert der Ubuntu-Installer im Dialog „Installationsart“ dann standardmäßig die Option „Ubuntu neben Windows installieren“ und bietet nach „Weiter“ sogar eine per Schieberegler skalierbare Verkleinerung der Windows-Partition an, um für Linux 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 anlegen.
Um sich Arbeit zu ersparen, wären dies eine logische Partition 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.
Exkurs: Alle wesentlichen Partitionierungsaufgaben kann ein Installer wie Ubuntus Ubiquity im Zuge des Setups erledigen. Wenn Sie Partitionen und Größen genau planen, geht das aber auch vorab mit Gparted unter Linux oder mit der Datenträgerverwaltung unter Windows (diskmgmt.msc). Unter Windows gibt es zudem das kostenlose Minitool Partition Wizard (*www.minitool.com/partition-manager/partition-wizard-home.html*), das besonders einfach zu handhaben ist.
Schritt 4: Notieren Sie sich die Bezeichnungen der Partitionen, damit Sie bei der Installation auch später noch wissen, welche



Die Partitionierung können Sie auch vorab erledigen. Das kann mit Gparted unter Linux, mit der Datenträgerverwaltung oder dem Minitool Partition Wizard unter Windows geschehen.

Rolle beispielsweise „/dev/sda7“ übernehmen sollte. Nach der Installation der ersten Linux-Distribution und dem Neustart des Systems sollten Sie die Wahl haben, zwischen Linux und Windows zu wechseln. Booten Sie nacheinander beide Betriebssysteme, um zu überprüfen, dass die Installation problemlos verlaufen ist. Konnten Sie Linux und Windows erfolgreich starten, starten Sie Ihren Rechner mit dem bootfähigen Startmedium eines eventuell dritten Betriebssystems. Es sollte das vorhandene Linux erkennen, aber feststellen, dass dafür kein Platz ist. Nutzen Sie jetzt entweder die bereits schon angelegten Partitionen oder verkleinern Sie die erste Partition des bereits installierten Linux.
Schritt 5: Der Wunsch, unter jedem gestarteten System auf den gleichen Bestand an Dokumenten zugreifen zu können, ist am einfachsten durch eine separate Festplatte oder Partition zu erreichen, die ausschließlich für Dokumente genutzt wird. Diese Datenpartition wird dann unter einem zweiten oder dritten System eingebunden und so konfiguriert, dass sie beim Systemstart zur Verfügung steht.
Diese Extrapartition oder Festplatte empfehlen wir auch beim Multiboot Linux–Linux, weil diese Konstruktion nach allen

Erfahrungen weniger fehleranfällig ist, als systemübergreifende Home-Verzeichnisse zu benutzen. Für den unkomplizierten Austausch zwischen Windows und Linux empfiehlt sich das Dateisystem NTFS, eventuell auch rechteloses exFAT, was unter Linux nur die Nachinstallation der Pakete „exfat-fuse“ und „exfat-utils“ erfordert.



Boothelfer Super Grub Disk (auf Heft-DVD): Ist die Bootumgebung defekt (regelmäßig nach Windows-Installationen), sucht und startet dieses bootfähige Tool vorhandene Linux-Systeme.

Die (gelegentliche) Grub-Malaise

Hat alles funktioniert, sollten Sie die Wahl zwischen mehreren Systemen haben. Soweit die Theorie. In der Praxis funktioniert das wahrscheinlich in über 90 Prozent aller Fälle. Zeigt Ihnen der Bootmanager das dritte System nicht an, dürfte in den allermeisten Fällen nur der Menüeintrag nicht angelegt worden sein. Öffnen Sie im erfolgreich installierten Linux-System ein Terminal und geben Sie dort

```
sudo update-grub
```

ein. Damit werden alle Scripts von Grub ausgeführt und auch die Systemsuche läuft durch. Starten Sie danach das System komplett neu. Hat das zu keinem Ergebnis geführt, liegt das Problem wahrscheinlich tiefer. Mit Rescatux (*www.supergrubdisk.org/rescatux/*) gibt es ein bootfähiges Minisystem mit einigen Scripts, mit deren Hilfe sich ein lahmender Bootmanager reparieren lässt. Es unterstützt den Anwender, das Bootmenü von Grub zu bearbeiten und manuell Systeme hinzuzufügen. Vom gleichen Entwicklerteam stammt die bootfähige Super Grub Disk (auf Heft-DVD, „Extras und Tools“). Damit den PC gebootet, wählen Sie die Option „Detect and show boot methods“ und wählen danach das gewünschte System aus, das Sie starten wollen. Dort öffnen Sie ein Terminal und stellen mittles des Befehls

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

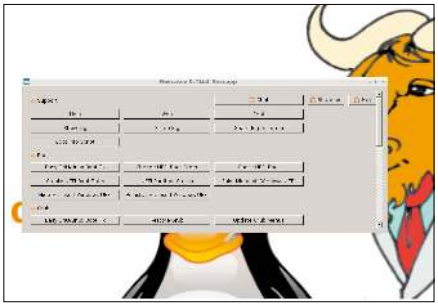
die Bootumgebung wieder her.

Die Alternative refind

Streng genommen ist Grub aus Sicht der Rechnerarchitektur bei einem Uefi-System überflüssig. Es ist aber aus historischen Gründen und mit Rücksicht auf ältere Bios-Hardware immer noch dabei. Eine Alternative zu Grub ist das von einem unabhängigen Entwickler programmierte refind („rEFInd“). Es steht in verschiedenen Versionen zur Verfügung und kann unter Linux, Windows und sogar auf dem Mac installiert werden.

Wenn also Windows aktuell das einzige System auf dem Rechner ist, nutzen Sie die passende Variante des Bootloaders. Nach erfolgreicher Einrichtung meldet sich stets zunächst refind, auch für den Fall, dass Sie lediglich Windows auf dem Rechner haben. Sie können danach dann mit dem Setup eines weiteren Systems beginnen, wie exemplarisch gezeigt, also Platz für das zweite System per Partitionierer schaffen. Dann legen Sie das Bootmedium des zweiten Betriebssystems ein und starten den Rechner neu.

Das Werkzeug wird Ihnen dann den Start vom eingelegten Datenträger anbieten, so dass Sie mit der Installation des zweiten Betriebssystems beginnen können. ■



Reparatursystem Rescatux: Das Minisystem ist keine Desktopschönheit, beherrscht aber umfangreiche Rettungsarbeiten am Grub-Bootloader (*www.supergrubdisk.org/rescatux*).

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.

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 (siehe 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.

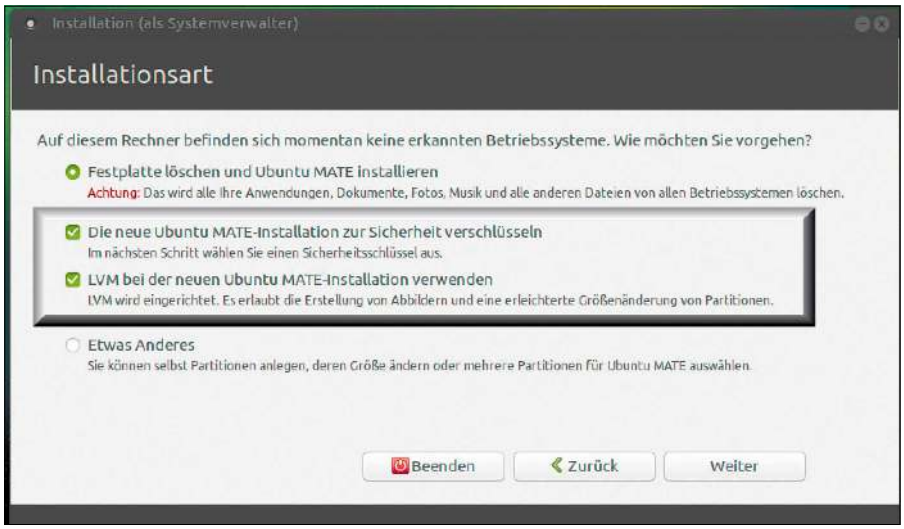
Installation mit Luks und LVM: Es gibt diverse grafische Linux-Installer, die beim Setup eine Luks-verschlüsselte Systempartition einrichten können. Neben Yast unter Open Suse, dem Debian-Installer und dem Fedora-Installer bieten alle Ubuntu-basierten Distributionen inklusive Linux Mint den Installer 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 verschlüsseln". 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.



Systemverschlüsselung per Setup: Dies ist die entscheidende Einstellung beim Ubuntu-Installer. Mit LVM und Luks-Verschlüsselung bootet das System erst nach korrekter Kennworteingabe.

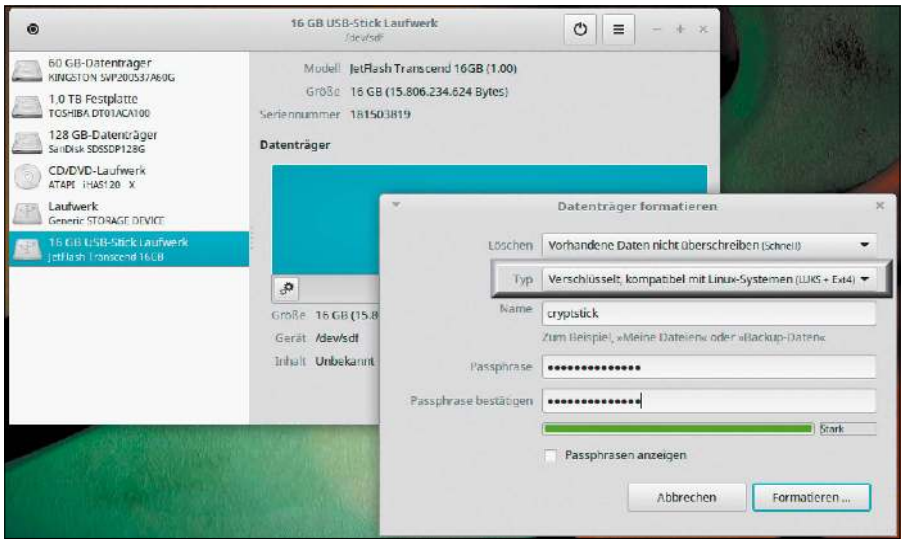
2. Luks-verschlüsselte (USB-)Datenträger

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.

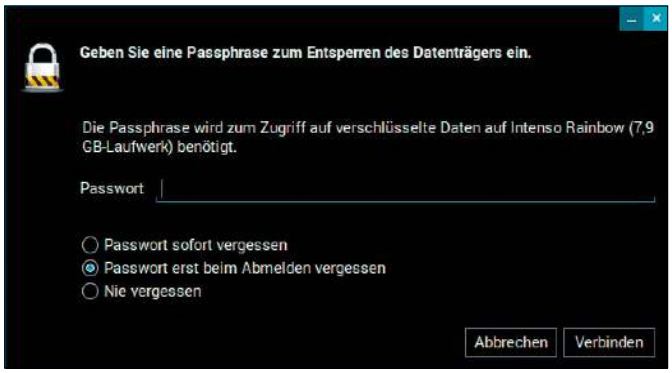
Die Einrichtung und Benutzung erfolgt auf modernen Linux-Distributionen komplett mit grafischen Werkzeugen, die den komplizierteren Weg über Terminalbefehle in der Regel überflüssig machen.

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. Dort, wo auch ein Windows oder ein Mac-OS zugreifen soll, ist Veracrypt (siehe Punkt 6) die bessere Option.

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



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.

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 Dateimanager können Sie den Datenträger 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 Ecryptfs, das Ubuntu & Co. standardmäßig im Kernel mitbringen. Ecrypt FS ist nicht zu verwechseln mit Enc FS (siehe 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]/.

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 zugrundeliegenden 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 casesensitiv 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.

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.

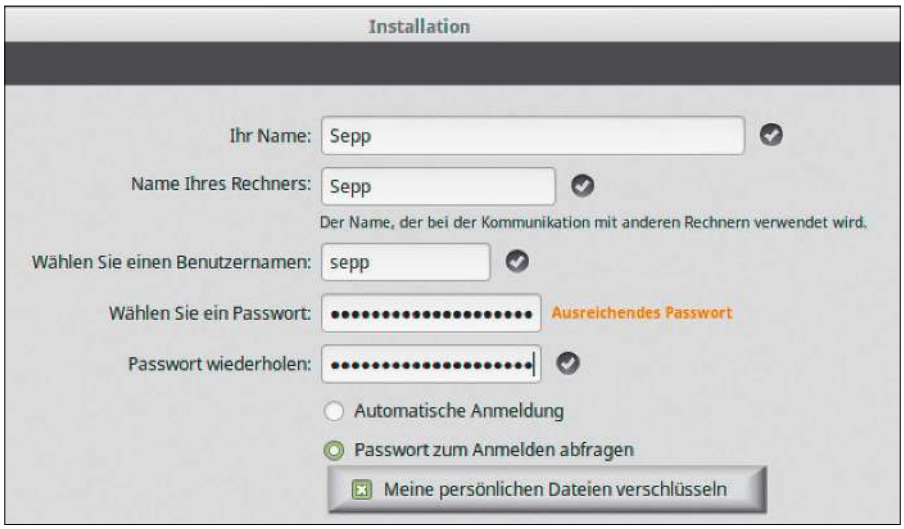
Einrichten der Home-Verschlüsselung: Bei der Installation von Ubuntu-Systemen erscheint zu einem späteren Zeitpunkt das Fenster „Wer sind Sie?“. Hier legen Sie den Erstbenutzer des Systems an. An unterster Stelle gibt es die Option „Meine persönlichen Daten verschlüsseln“. Ein Häkchen genügt, um Ecryptfs für das Home-Verzeichnis des Erstbenutzers zu aktivieren. Nach der ersten Anmeldung am neu installierten System erscheint dann ein 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.

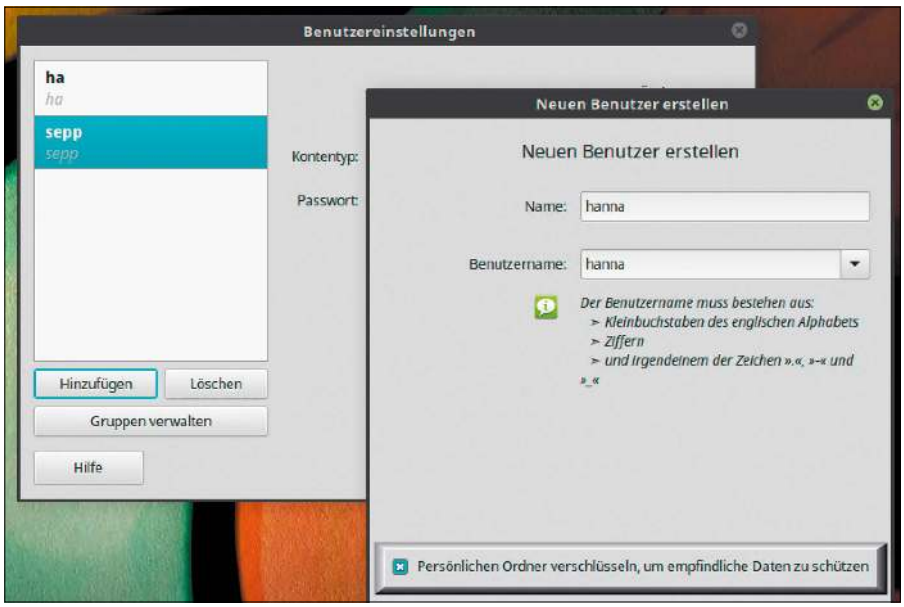
Für den alltäglichen Zugriff auf das Home-Verzeichnis genügt die Anmeldung am System. Vor anderen Benutzern am selben PC ist das verschlüsselte Home-Verzeichnis ebenfalls sicher. Diese erhalten beim Zugriff eine Fehlermeldung, die auf fehlende Rechte hinweist. Besitzen andere Systembenutzer root-Recht, 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 […]“.



Ubuntu bietet bei der Installation an, das Home-Verzeichnis zu verschlüsseln. Das gilt jedoch nur für den Erstbenutzer. Für weitere Benutzer müssen Sie die Verschlüsselung selbst aktivieren.



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.

2. Bei den meisten Distributionen ist die Home-Verschlüsselung nur über die Kommandozeile zu erreichen. Es genügt dieser Befehl:

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

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 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.

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

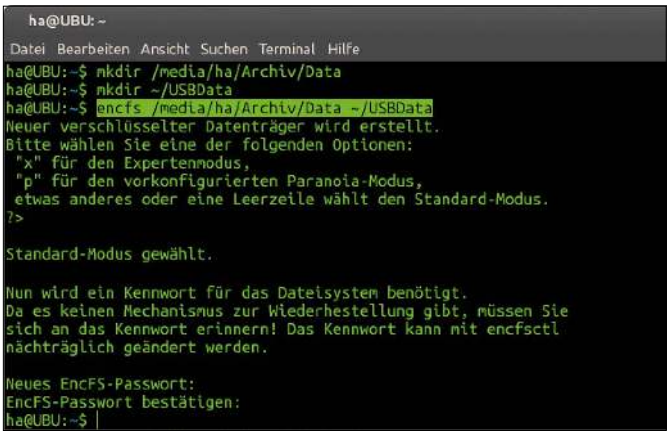
Enc FS ist ein flexibles Ordner- und Dateiorientiertes Verschlüsselungswerkzeug. Der Ruf des Tools hat etwas gelitten, nachdem vor Jahren eine theoretische Lücke bekannt wurde, welche die Robustheit von Enc FS infrage stellte. Diese Lücke besteht immer noch und wird bei der Installation des Pakets gemeldet. 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 EncFS. 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, 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.



Ersteinrichtung eines Enc-FS-Ordners: Sie benötigen lediglich einen Ordner als Mountpunkt (hier „USBData" im Home-Verzeichnis) und ein Kennwort.

Grafisches Front-End für Enc FS: Das kleine Tool Cryptkeeper erscheint als Schlüsselsymbol in der Hauptleiste und bietet die wesentlichen Enc-FS-Funktionen.

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.

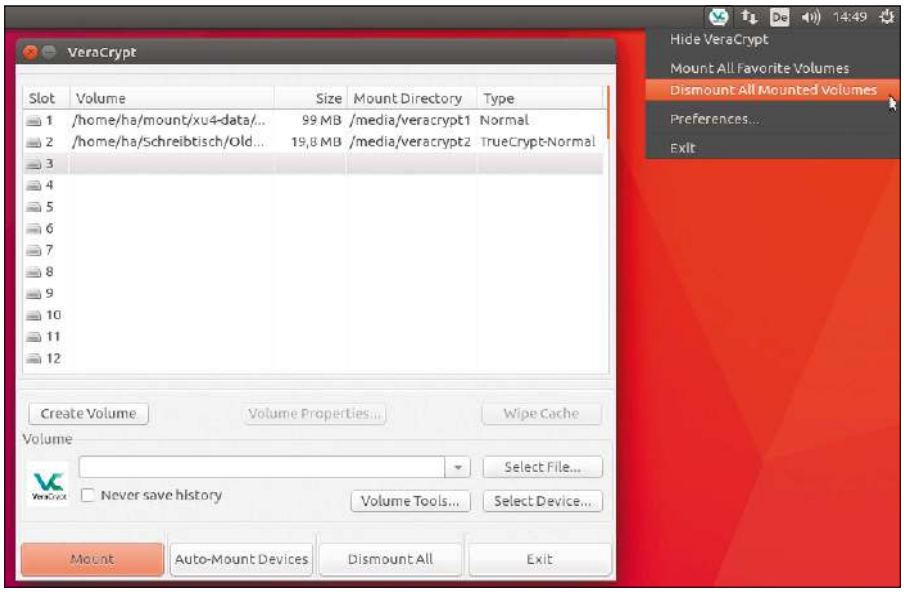
5. Container mit Veracrypt

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.

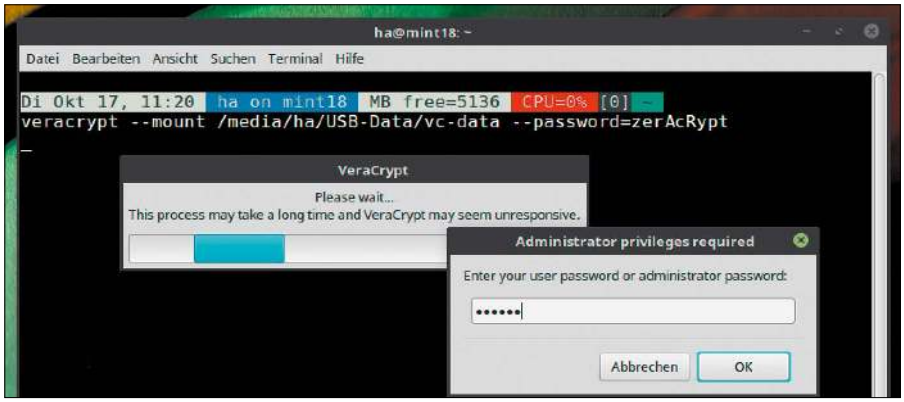
Empfehlung: Veracrypt eignet sich für große und sehr große Datenmengen, allerdings nur auf lokalen Rechnern oder im lokalen Netzwerk. Für den Transfer in die Cloud ist es ungeeignet, da auch bei geringen Datenänderungen immer der Transport des gesamten Containers notwendig wäre. Ein entscheidendes Plus 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
```



Hauptdialog und Systemintegration von Veracrypt: Veracrypt entspricht bei der Bedienung seinem Truecrypt-Vorgänger. Laden und Entladen von Containern gelingt auch über das Panelsymbol.



Veracrypt im Terminal: Alle Funktionen der Verschlüsselungssoftware sind auf Wunsch auch über die Kommandozeile zu steuern.

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 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:

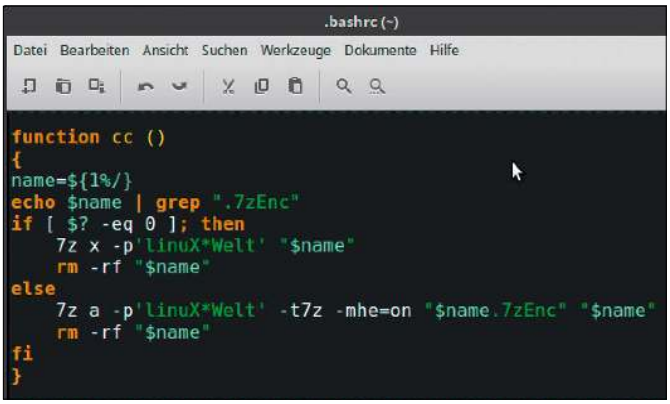
```
veracrypt --mount /home/ha/vc-data
 --password=Sehr-GeH3im
```

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 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 Mac-OS (7zX) gibt, ist der Austausch solcher Archive problemlos. Unter Android



Vereinfachte Packerverschlüsselung: Ein Script kann die lästige Aufgabe übernehmen, das Kennwort an 7-Zip zu übergeben.

können nicht alle Apps mit einem „zip“ im Namen auch mit passwortgeschützten Archiven umgehen, aber der kostenlose, allerdings 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

```
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 letzte Ausgabe der LinuxWelt zeigte eine Lösung mit einem Incron-überwachten Ordner, der die Verschlüsselung per Drag & Drop erledigt. Alle nötigen Infos dazu finden Sie im PDF-Booklet auf Heft-DVD. 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.

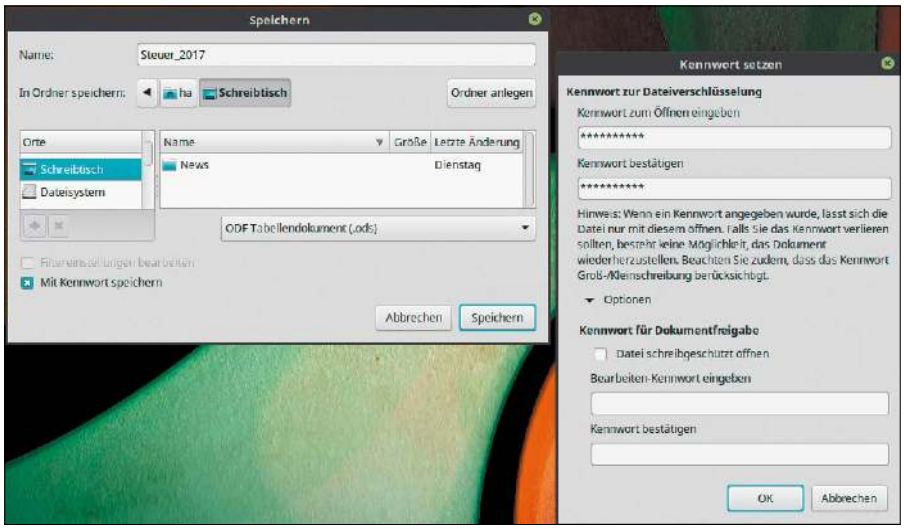
Empfehlung: Diese Methode, Dateien einzeln zu verschlüsseln, eignet sich nur für wenige sensible Texte oder Tabellen. Für

größere Datenmengen ist sie zu unbequem. 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.



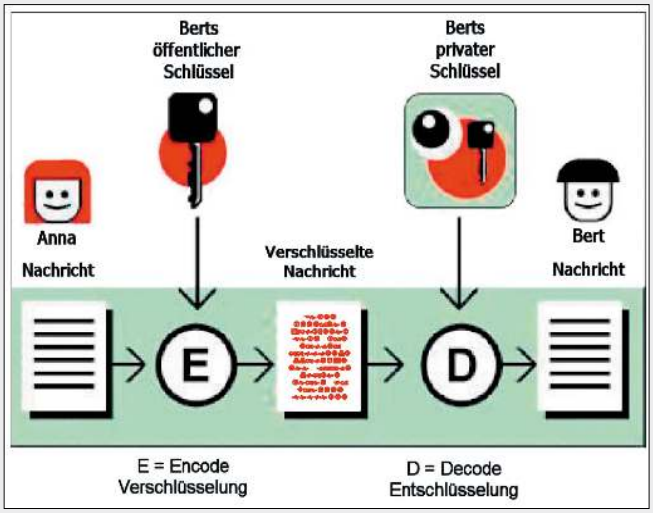
Einzeldateien unter Libre Office verschlüsseln: Diese Ad-hoc-Maßnahme ist ein Notbehelf für geringe Datenmengen.

Empfehlung: Mailverschlüsselung ist wie jede Datenschutzmaßnahme mit Mehraufwand verbunden. Die Kombination von Gnu PG (GNU Privacy Guard) plus Thunder-

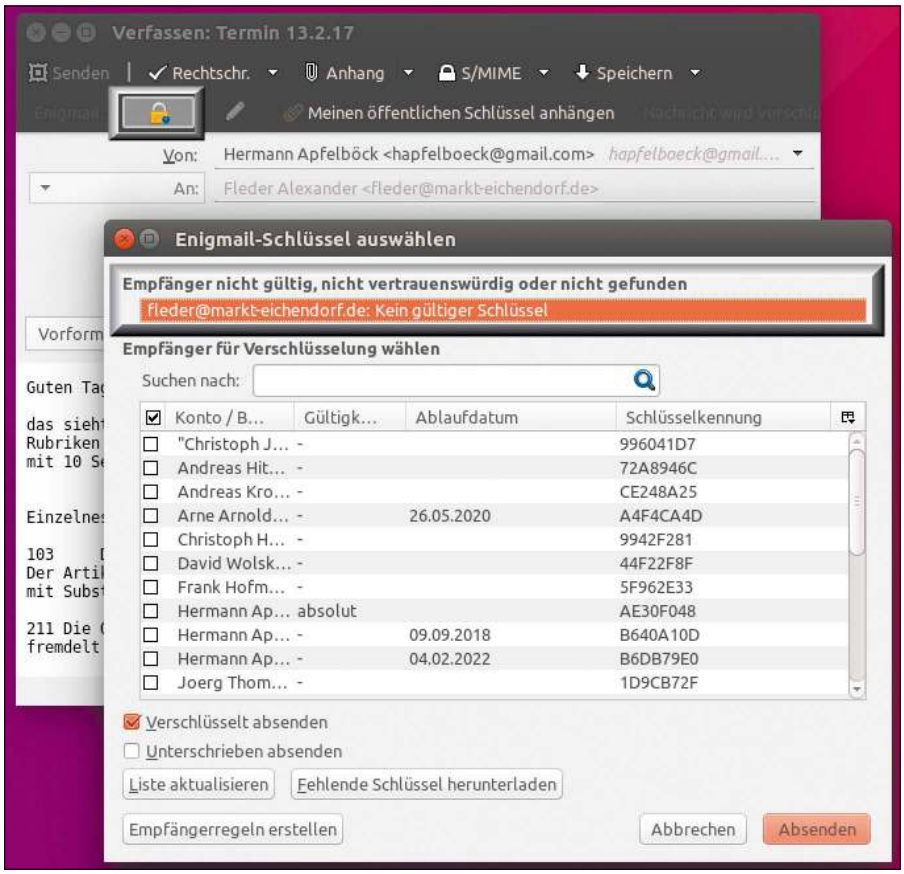
ASYMMETRISCHE VERSCHLÜSSELUNG

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.



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.

bird 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 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 Rechnern 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 Rechner importieren.

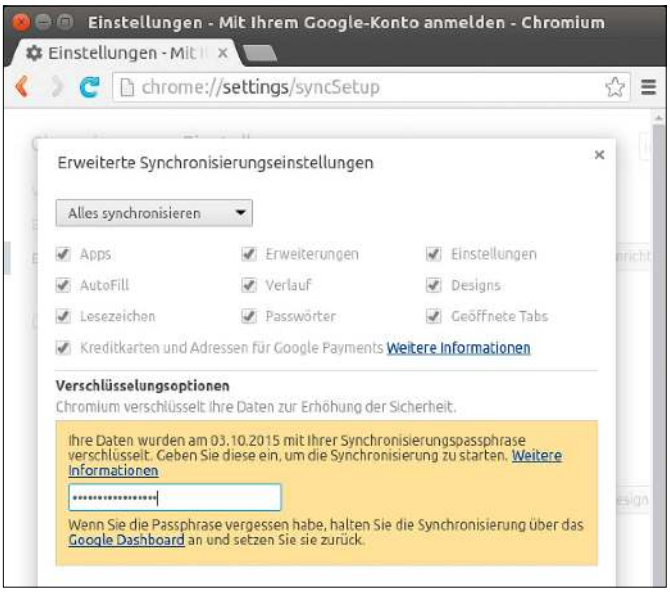
9. Verschlüsselte Browsersynchronisierung

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 Google- oder Mozilla-Servern hinterlegt werden müssen.

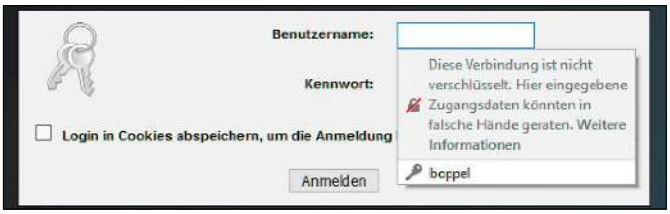
Empfehlung: Firefox verschlüsselt standardmäßig alle Daten, wobei der Schlüssel auf dem Gerät des Benutzers verbleibt. Damit ist der Mozilla-Browser in puncto Datenschutz erste Wahl. Jedoch lässt sich auch der Google-Browser so einstellen, dass alle Synchronisierungsdaten sicher verschlüsselt sind.

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-Kenn-

wort 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.



Sync-Daten verschlüsseln: Diese Maßnahme hält Googles Big-Data-Sammler von Lesezeichen und Verlaufsdaten fern.



Firefox ultravorsichtig: Der Mozilla-Browser zeigt bei Anmeldungen auf unverschlüsselten Webseiten diese Warnung.

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 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 auf Windows allerdings nicht, da der auch unter Windows vielgenutzte FTP-Client Filezilla auch das Protokoll „SFTP - SSH File Transfer Protocol" 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.

True OS – was ist dran?

True OS basiert auf Free BSD. Dieser Unix-Abkömmling hat viele Ähnlichkeiten mit Linux, aber auch signifikante Unterschiede. Zu den Besonderheiten von True OS zählen das Dateisystem ZFS und die portable Home-Verschlüsselung mit „Personacrypt“.

VON HERMANN APFELBÖCK

Auf *http://distrowatch.com* klopft in der letzten Zeit häufiger die Distribution True OS an die Top Ten. Ihre bisherige Top-Platzierung ist Platz 11, während sie bis vor ein, zwei Jahren noch unter „ferner liefen“ zu suchen war. Was ist dran an diesem System? – das fragen uns die LinuxWelt-Leser. Eine Frage, die wir an dieser Stelle gerne beantworten, zumal True OS ein schnelles Ausprobieren in einem Livesystem nicht vorsieht. Echtes Installieren ist unvermeidlich, um das System zu testen.

Download und Installation

Erste Informationen über True OS finden Sie auf der Projektseite: *https://www.trueos.org/*. Wer sich vorab detaillierter über die Hardwarevoraussetzungen und den Praxisalltag unter True OS informieren will, sollte einen Blick werfen auf das Onlinehandbuch *https://www.trueos.org/handbook/trueos.html*, das auch direkt über die Projektseite erreichbar ist. Aufgrund des Dateisystems ZFS sind für das an sich schlanke System etwa vier GB RAM empfohlen, absolutes Minimum ist ein GB.

Auf der Downloadseite *https://www.trueos.org/downloads/* finden Sie Angebote aus dem Stable- und Unstable-Zweig (Stable empfohlen). Der Download des „Latest TrueOS Stable“ beträgt etwa 2,5 GB. Das ISO-Image schreiben Sie dann mit einem Tool Ihrer Wahl am besten auf eine DVD (Brasero unter Linux, Imgburn unter Windows). Eigentlich sollte auch ein USB-Stick als Installationsgerät funktionieren, jedoch war dies in unserem Fall weniger zuverlässig als das optische Medium.

Wenn Sie den Zielrechner damit starten, erhalten Sie kein Livesystem, sondern einen reinen Installer. Neben der typischen Abfrage der Systemsprache geht es um die Entscheidung, ob eine grafische Oberfläche installiert und ein proprietärer Treiber für die Grafikkarte genutzt werden soll. Dann geht es zur Partitionierung: Wenn True OS die erste Festplatte „ada0“ nicht oder nicht in vollem Umfang übernehmen darf, ist der Klick auf „Customize Disk Settings“ erforderlich. Die Schaltfläche „Customize Disk Settings“ ist unbedingt auch dann notwendig, wenn True OS das alte MBR-Partitionierungsschema verwenden soll. Standardmäßig geht es von einer Uefi/GPT-Installation aus. Der hiermit gestartete „TrueOS Disk Wizard“ ist für Erfahrene akzeptabel, für Anfänger eher riskant. Wer Multiboot oder die umfassenden Pool- und Raid-Optionen von ZFS einrichten will, sollte unbedingt Erfahrung mitbringen und parallel das angesprochene Onlinehandbuch benutzen.

Ersteinrichtung von True OS

Nach erfolgreicher Installation und dem ersten Start fordert das System ein Passwort für den Rootzugang und danach ein erstes Benutzerkonto.

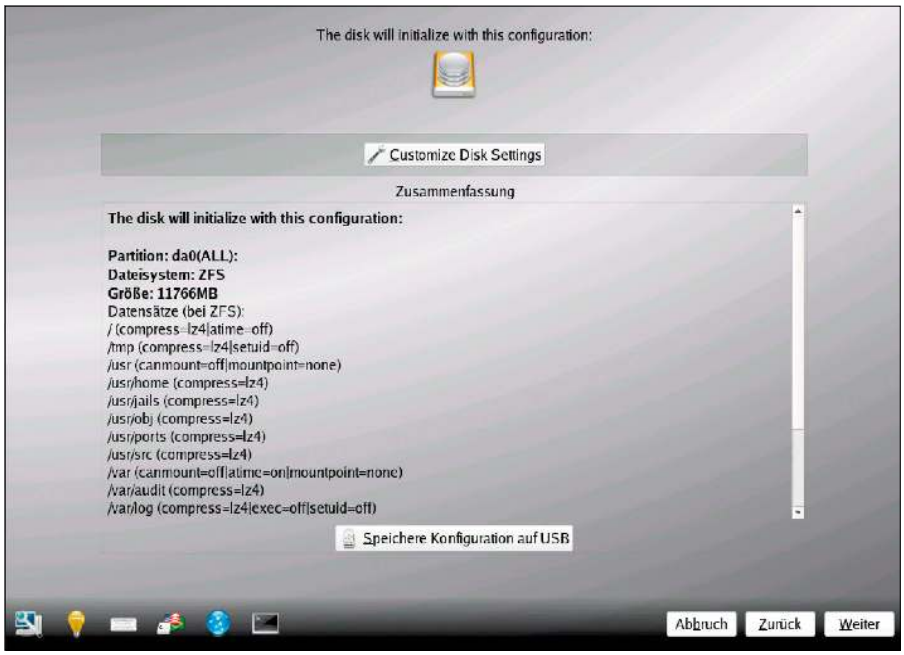
Die Personacrypt-Verschlüsselung: Schon bei Einrichtung des Erstkontos fällt die zweite Registerkarte „PersonaCrypt“ ins Auge, die auch später im „Usermanager“ für alle Benutzerkonten auftaucht. Es handelt sich um die optionale Verschlüsselung des jeweiligen Home-Verzeichnisses. Wie bei Linux-Systemen kann das Home-Verzeichnis geschützt werden, indem bei „Device“ die Option „On Disk Encryption (PEFS)“ gewählt wird. True OS kann aber an dieser Stelle mehr: Bei angeschlossenem USB-Datenträger wird dieser als „Device“ angezeigt und kann dann als Ziel für die verschlüsselten Dateien definiert werden. Das

unter „PersonaCrypt“ eingegebene Passwort ist unabhängig vom Systempasswort, kann aber der Einfachheit halber auch identisch gewählt werden.

Im späteren Betrieb reagiert True OS auf PersonaCrypt-Konten wie folgt: Konten mit lokaler „On-Disk-Verschlüsselung“ werden am Anmeldebildschirm immer angezeigt, selbstverständlich auch alle Konten ohne jede Verschlüsselung. Personacrypt-Konten mit externen USB-Medien erscheinen jedoch nicht, sofern der Datenträger nicht angeschlossen ist. Mit anderen Worten: Die Anmeldung eines solchen Kontos ist nur möglich, wenn der Nutzer seinen Datenträger dabei hat und anschließt. Für die Anmeldung von Personacrypt-Konten sind immer zwei Kennwörter nötig – das Systempasswort und zusätzlich das Verschlüsselungspasswort.

Der Lumina-Desktop: Standardmäßig startet True OS seinen Stammdesktop Lumina. Diese Oberfläche ist keine Schönheit, orientiert sich aber mit Startmenü, Systemleiste und Rechtsklickmenü am Desktop weitgehend an geläufigen Standards. Über den Desktop-Rechtsklick und „Einstellungen -> Desktop Actions“ kann der Desktop als Ordner und Dateiablage genutzt werden. Wer es ganz minimalistisch haben will, kann am Anmeldebildschirm auch auf Fluxbox umstellen.

Das Softwarecenter: Die Softwareausstattung ist standardmäßig ausreichend, aber eher spartanisch. Ihre Ausstattung ergänzen Sie recht komfortabel mit dem grafischen Paketmanager „AppCafe“. Ähnlich wie bei Ubuntu gibt es verschiedene Paketquellen, zwischen denen Sie über das Listenfeld in der Mitte wechseln. Stöbern Sie in den Kategorien oder suchen Sie gezielt nach Programmen. Viele der bekannten Linux-Klassiker wie Libre Office, VLC, Filezilla, MC oder Gimp sind auch in Versionen für True OS (Free BSD) zu bekommen. Auch alternative Desktops wie Mate oder XFCE sind verfügbar. Das „AppCafe“ bietet nicht den Umfang von Debian/Ubuntu-Distributionen, aber alles Wesentliche ist hier erhältlich.



Installer mit mäßiger Partitionierungshilfe: Die Einrichtung ist nichts für Anfänger. So fehlt etwa jeder Hinweis, dass eine MBR-Installation unter „Customize“ explizit eingestellt werden muss.

Hier gibt es ein unverschlüsseltes Konto „hanna“ und ein verschlüsseltes Konto „klaus“, dessen Verschlüsselungsgerät vorliegt („Ready“). Die Anmeldung fordert zwei Kennwörter.

Fazit: Viele Kompromisse

Den Hauptschub für das aktuelle Interesse an True OS dürfte die Veröffentlichung des Stable-Zweiges im Juli 2017 ausgelöst haben: Ähnlich wie Debian arbeitet True OS nun mit einem Unstable-Zweig, der stets die neuesten Entwicklungen einbaut, während der Stable-Zweig nur bewährte Pakete ausliefert.

Das Hauptmotiv für True OS ist wohl nicht das mächtige Dateisystem ZFS mit vielen serverrelevanten Optionen für Festplattenpools und Systemsnapshots. Vielmehr dürfte bestimmte Nutzer das ungewöhnliche Personacrypt faszinieren: Die eigenen Daten sind unzugänglich, das maßgebliche Konto am Log-in-Bildschirm nicht einmal ersichtlich, solange der Nutzer nicht das passende USB-Gerät aus seiner Schublade holt und anschließt. Ob man solche Zwei-Geräte-Sicherheit als konsequente Datenschutzmaßnahme interpretieren oder doch überwiegend in der Ecke schmuddeliger Versteckspiele verorten will, überlassen wir dem Urteil des Lesers.

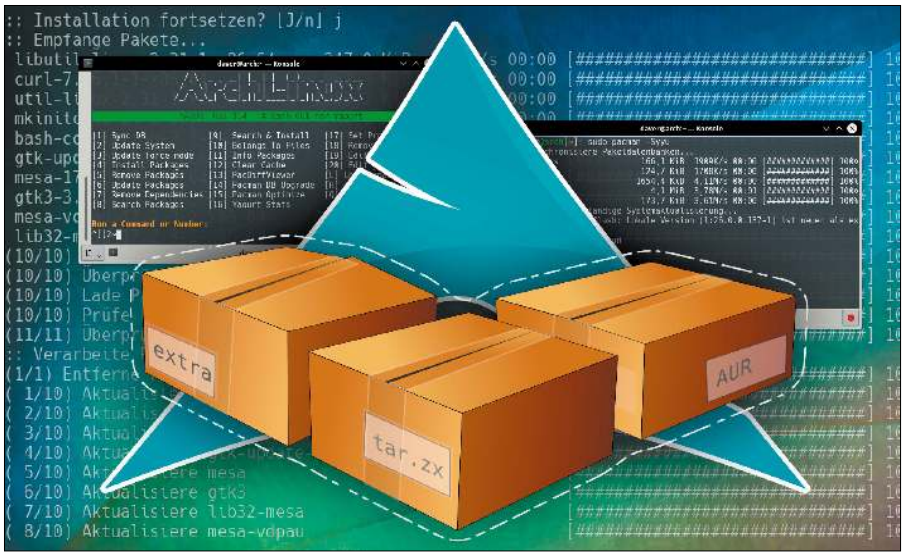
Deutlich ist, dass der Anwender für das eine oder andere interessante True-OS-Feature einige Kompromisse in Kauf nehmen muss: True OS kann weder beim Installerkomfort noch bei der Hardwareerkennung einem Debian/Ubuntu das Wasser reichen.

Mit dem voreingestellten Lumina-Desktop gibt es dann eine allenfalls brauchbare Bedienoberfläche – selbst ein einfaches LXDE (auf Lubuntu oder Debian) kann da mindestens mithalten. Nebenbei ist das System kein Schnellbooter und fordert, gemessen am grafischen Komfort, relativ viel Arbeitsspeicher (wegen ZFS). ■

Die Paketverwaltung von Arch Linux

Einer der Vorzüge von Arch Linux und dessen Abkömmlingen wie Antergos und Manjaro sind die sehr aktuellen Pakete und zahlreichen externen Repositories. Das Paketformat und das Paketmanagement von Arch hat daran großen Anteil.

VON DAVID WOLSKI



Ein möglichst neuer Kernel mit neuen Hardwaretreibern, eine besonders frische Ausgabe von Libre Office mit besserer Microsoft-Office-Kompatibilität: Arch Linux verwöhnt seine Anwender mit sehr aktuellen Paketen. Die Verfügbarkeit sehr frischer und breit gefächerter Pakete hat Arch Linux populär gemacht. Zudem ist ein Arch ein Rolling Release und lässt sich im Idealfall jahrelang ohne Neuinstallation über den Paketmanager fit halten. Die Distribution ist seit 2002 verfügbar und läutete zusammen mit Gentoo nicht nur den Aufstieg von Rolling Releases ein, sondern brachte ein Comeback der Selbstbaudistributionen. Denn Arch Linux liegt in seiner ursprünglichen Form als Bausatz vor, aus dem sich erfahrene Linux-Experten selbst ein System einrichten.

Paketquellen: sauber aufgeteilt

Arch unterhält mit „Core“ und „Extras“ zwei Hauptrepositories: Alles, was zum minimalen Betrieb des System und zum Kompilieren nötig ist, liegt im kleinen und ausgiebig getesteten Repository Core, das nur etwa 200 Pakete umfasst. In den Extras liegen dann die wichtigen Programme, Desktopumgebungen und generell alles, was mindestens fünf Prozent der Arch-Nutzer haben wollen. Weitere offizielle Pakete liegen im Communityrepository, um das sich die „Trusted User“ kümmern, die sich meist auf bestimmte Programme spezialisieren.

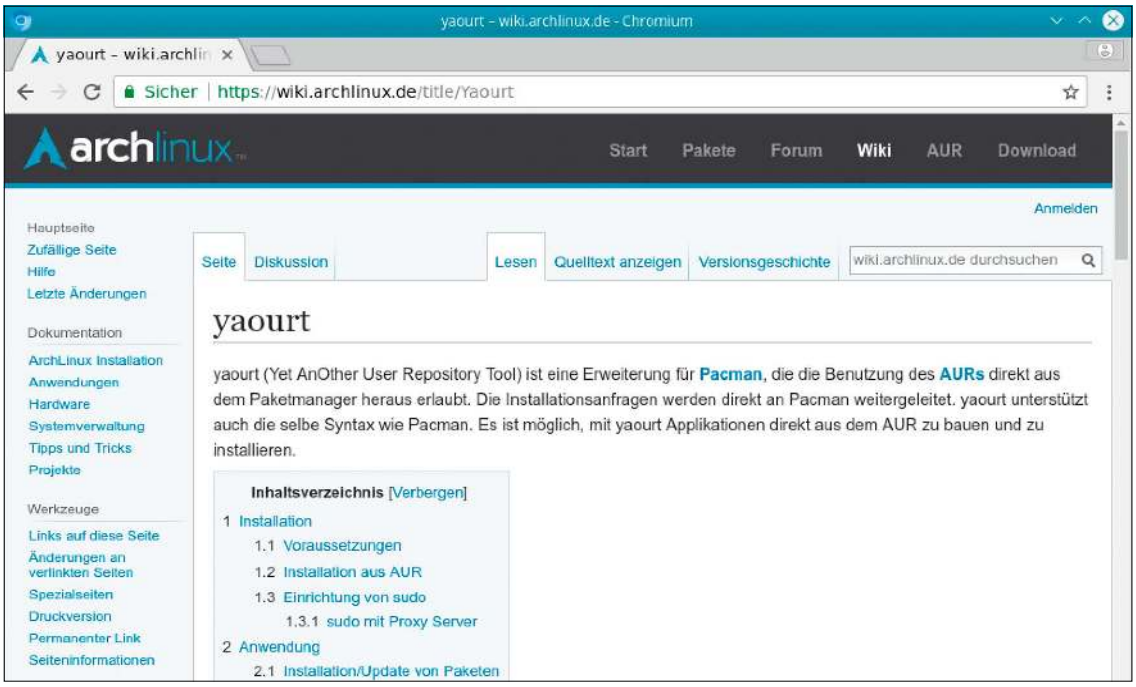
Da Arch an den originalen Softwareversionen nichts ändert und die Erstellung von Paketen kaum aufwendiger als das Kompilieren ist, bietet Arch neue Programmversionen schneller als andere Distributionen. Entwickler erhalten von Arch-Anwendern meist die ersten Rückmeldungen zu neuen Programmversionen. Während ein Paket bei anderen Distributionen erst im Betazweig ist, gibt es das Programm für Arch meist schon im regulären Repository. Die rund 6000 Pakete in den offiziellen Repositories gelten als exzellent gepflegt und sehr stabil, obwohl nur drei Dutzend Entwickler und nochmal so viele Trusted User an Arch arbeiten – übrigens alle davon auf freiwilliger Basis, ohne große Sponsoren im Rücken.

Unterschiede zu anderen Distributionen

Der Schlüssel dazu ist ein robustes Paketsystem, das nicht nur Programmierern die Erstellung von paketierten Programmen für Arch ermöglicht. Dieses Paketsystem hält die Wege vom originalen Quellcode zum fertigen Arch-Paket sehr kurz. Auch weniger populäre Software, für welche vielleicht nur eine Handvoll Benutzer Verwendung haben, ist für Arch häufig in inoffiziellen Repositories zu finden, die ungleich größer sind als jene von Ubuntu oder Debian. Ein weiterer Vorzug ist das Arch Build System (ABS), das aus nacktem Quellcode Arch-Pakete baut, diese über den Paketmanager sauber einspielt und damit das gesamte System konsistent hält. Arch Linux setzt dazu nicht auf das Paketformat DEB oder RPM: Arch-Pakete liegen als LZMA-gepackte „tar“-Dateien im Format „tar.xz“ vor.

Paketmanagement mit Pacman

Der zentrale Paketmanager nennt sich Pacman. Er kümmert sich um die Pflege der Paketdatenbank installierter Software, um



Das Arch-Wiki in Deutsch: Mit zur Popularität von Arch Linux hat die umfangreiche Dokumentation beigetragen, die akribisch alle Details eines Linux-Systems beschreibt.

den Download neuer Pakete und deren Installation sowie Aktualisierung. Dieser Paketmanager führt in der Kommandozeile mittels des Befehls

```
pacman [Optionen]
```

die gewünschten Aktionen aus und übernimmt dabei wie die moderne Version von APT in Debian/Ubuntu den Download sowie die Installation von Paketen. Voraussetzung ist, den Paketmanager als root oder mit vorangestelltem sudo auszuführen. Die folgenden Pacman-Befehle braucht jeder Arch-Anwender häufiger:

Zum Suchen der Pakete anhand von Name und Beschreibung dient der Befehl

```
pacman -Ss [Begriff]
```

und zum Installieren dient einfach der Parameter „-S“, gefolgt vom Programmnamen:

```
pacman -S [Paketname]
```

Für das Entfernen von Pakete gibt es zwei Optionen:

```
pacman -R [Paketname]
```

löscht nur das einzelne angegebene Paket, lässt aber die Abhängigkeiten intakt, während

```
pacman -Rs [Paketname]
```

auch die Abhängigkeiten und nicht mehr weiter benötigten Bibliotheken vom System wirft. Allerdings wirklich nur dann, wenn sie von keinem anderen Paket mehr gebraucht werden.

Ein Komplett-Update des installierten Systems erledigt der Befehl

```
pacman -Syu
```

und zeigt bei wichtigen Änderungen an Paketen und deren Konfiguration vor der Aktualisierung ein Änderungsprotokoll der Entwickler mit Hinweisen an, was sich mit dem Update genau ändert.

Überspringen kann man die Anzeige dieser Changelogs aber auch mit einem weiteren „y“ als Parameter:

```
pacman -Syyu
```

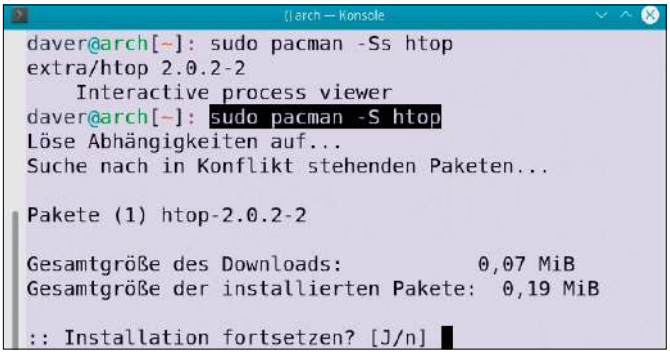
AUR: Externe Repositories

Weitere Programme lassen sich über das inoffizielle Arch User Repository (kurz AUR) finden und kompilieren. Diese Quelle ist im Prinzip vergleichbar mit den PPAs für Ubuntu – mit dem Unterschied, dass im AUR keine fertigen Pakete liegen, sondern lediglich die Bauanleitungen mit der Beschreibung für den Paketmanager, auf welche Weise ein Programm aus dem Quellcode zu einem Arch-Paket kompiliert werden soll. Diese Repositories bieten also Arch-Anwendern die Möglichkeit, eigene Ergänzungen über Paketbeschreibungsdateien (PKGBUILDs) in einer standardisierten Form weiterzugeben.

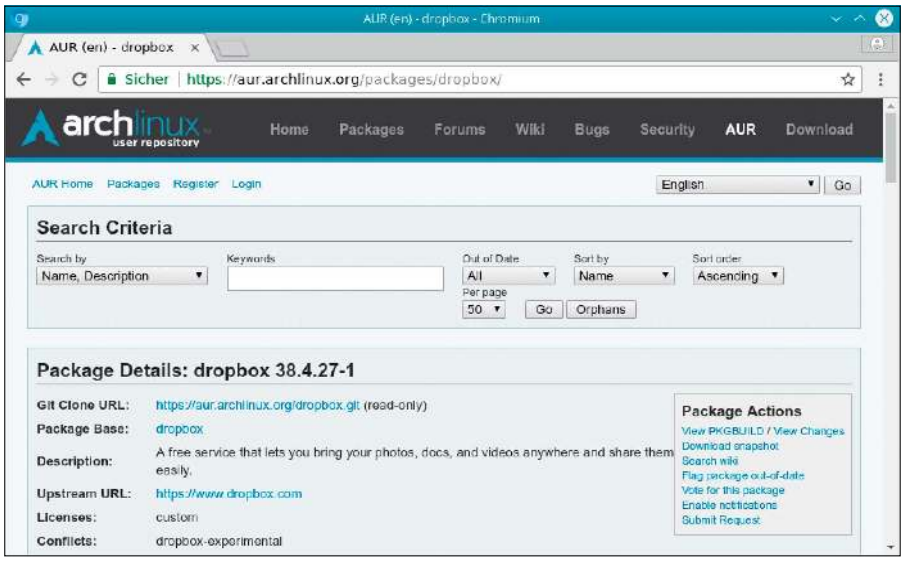
Aus den PKGBUILD-Dateien und dem Quellcode macht das Tool makepkg das fertige Binärpaket, das sich dann wieder mit Pacman installieren lässt.

So kommen auch Anwender auf ihre Kosten, die gerne Programmen beim Kompilieren zusehen, allerdings muss man nicht alle Schritte manuell ausführen. Denn auch für das AUR gibt es den inoffiziellen Paketmanager Yaourt, um Programme zu finden und zu installieren. Der Name ist eine Abkürzung für „Yet Another User Repository Tool“ und ist, einmal eingerichtet, auch gleich ein Front-End für Pacman und mit der Suche von Paketen in AURs ein universeller Paketmanager.

Hinweis: Anders als die offiziellen Repositories unterliegen die Inhalte im Arch User



Gesucht und gefunden: Der schnelle Paketmanager pacman dient in Arch Linux zur Suche und Installation von fertigen Paketen aus den offiziellen Repositories.



Inoffizielle Quellen: Mit dem Arch User Repository (AUR) kann Software aus dem Quellcode gebaut werden. Die Onlinesuche auf *https://aur.archlinux.org* bietet eine Paketübersicht.

Repository keiner strengen Kontrolle. Während reguläre Arch-Pakete kryptografisch signiert sind, um deren Quelle eindeutig zu verifizieren, ist das bei Inhalten aus dem AUR nicht der Fall. Es gibt keine Garantie, dass die aus einem AUR gebauten Programme technisch einwandfrei sind. Immerhin gibt es aber als Kontrollinstanz ein Bewertungssystem anderer engagierter Arch-Anwender für Softwarepakete im Arch User Repository. Schon allein deshalb möchte die Arch-Gemeinde den Zugriff auf diese potenziell riskanten Softwarequellen eigentlich nicht zu einfach machen und verzichtet darauf, das Tool Yaourt in fertiger Form auszuliefern.

Mit Yaourt fremde Pakete laden

Im Arch-Abkömmling Manjaro ist Yaourt bereits vorinstalliert und in der Kommandozeile einsatzbereit. Ein unverändertes Original-Arch-System kennt das Tool und auch das Paket aber zunächst nicht. In diesem Fall ist die erste Einrichtung mit etwas mehr Aufwand verbunden, denn Yaourt ist selbst in einem AUR verfügbar und muss erst von Github im Quellcode bezogen und kompiliert werden. Für Ungeduldige gibt es aber ein fertiges Paket im Repository *http://repo.archlinux.fr*.

Um diese Quelle zu nutzen, öffnet man die Datei „/etc/pacman.conf“ mit root-Privilegien in einem Texteditor und fügt ganz am Ende diese drei Zeilen ein:

```
[archlinuxfr]
SigLevel = Never
Server = http://repo.archlinux.fr/$arch
```

Jetzt kann der Terminalbefehl

```
pacman -Syu yaourt
```

Yaourt installieren. Die Syntax des Tools ist mit jener von pacman identisch. Die Eingabe von

```
yaourt -Ss [Begriff]
```

sucht ein Paket anhand des Suchbegriffs. Dabei listet Yaourt immer erst die Treffer aus den offiziellen Arch-Repositories auf (falls vorhanden) und sucht erst dann im Arch User Repository. Besonders interessant bei den Treffern aus dem AUR ist die angezeigte Zahl dahinter, denn diese gibt die positiven Bewertungen an, die ein Paket von anderen Anwendern bekommen hat. Je höher diese Zahl ausfällt, desto vertrauenswürdiger ist ein Paket. Meist gibt es zu einer Suche mehrere Treffer und man sollte stets jenen mit der besten Wertung auswählen.

Die Installation mittels

```
yaourt -S [Paketname]
```

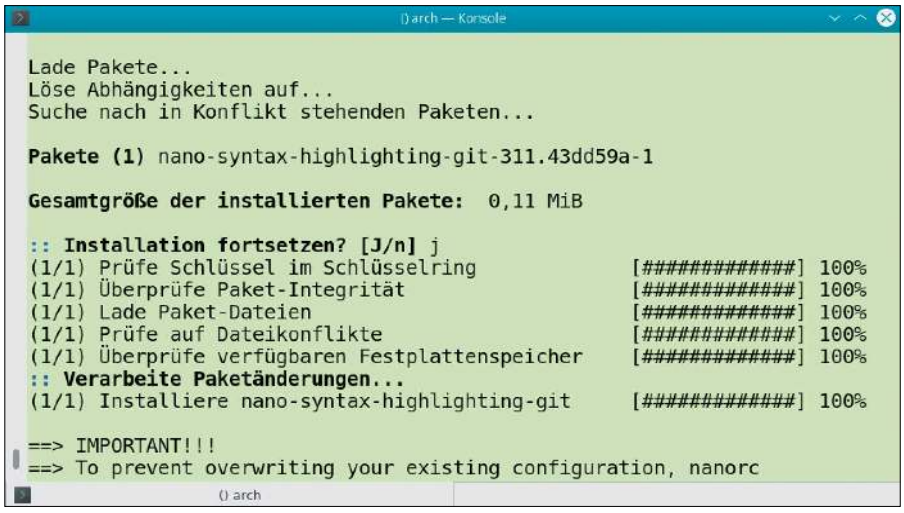
läuft nicht geradlinig durch wie mit Pacman, denn das gewünschte Paket muss ja erst noch kompiliert werden:

1. Yaourt lädt für das gewünschte Paket die Bauanleitung PKGBUILD herunter und fragt nach, ob der Anwender diese nachbearbeiten will. Diese Nachfrage kann man in der Regel verneinen.

2. Nun überprüft Yaourt, ob alle benötigten Abhängigkeiten vorhanden sind, und zeigt in einer Liste, welche anderen Pakete als Voraussetzung mitinstalliert werden. Dieser Schritt wartet auf eine Bestätigung.

3. Bevor es mit dem Download und dem Kompilieren losgeht, zeigt eine Übersicht an, welche Pakete nun insgesamt auf das System geholt werden und wie viel Platz sie benötigen. Es empfiehlt sich, hier immer genau nachzusehen, damit man sich keinen Rattenschwanz an Abhängigkeiten auf das System zieht.

4. Yaourt fragt ein letztes Mal nach, ob es mit der Installation des Pakets fortfahren soll, beginnt dann mit dem Download des Quellcodes und dem Kompilieren. Falls weitere Pakete als Abhängigkeit ebenfalls aus einem AUR bezogen werden, erledigt das Tool alle diese Schritte nacheinander, fordert aber vor jedem Kompilierdurchgang wieder eine Bestätigung des Systembenutzers.



Pakete holen oder selber bauen: Der optionale Paketmanager Yaourt findet Pakete in den Arch User Repositories, arbeitet aber auch als Front-End für Pacman.

Front-Ends: Hilfen zum Paketmanagement

Der Paketmanager Pacman in der Kommandozeile hat den Vorteil, sehr schnell zu arbeiten. Trotzdem ist ein grafischer Paketmanager auf einem Desktopsystem natürlich komfortabler. Zwar liegt der Schwerpunkt von Arch nicht bei grafischen Hilfen zur Administration, aber zwei bequeme Programme zur Suche, Auswahl und Installation von Programmen in den Paketquellen gibt es dennoch.

Pamac: Dieser grafische Paketmanager ist durch die Arch-Variante Antergos bekannt geworden und dort bereits vorinstalliert. Pamac ist mit Synaptic unter Debian/Ubuntu vergleichbar und erlaubt die Suche und Auswahl von Programmen aus den regulären Paketquellen.

In Arch und seinen Varianten ist das Tool mittels des Kommandos

```
yaourt -S pamac
```

schnell nachinstalliert.

Yaourt-GUI: Es handelt sich um kein grafisches Tool, sondern um ein Kommandozeilenwerkzeug mit textbasierten Menüs zur Verwaltung inoffizieller Pakete.

Yaourt-GUI: Der Namenzusatz „GUI" dieses Paketmanagers speziell für AURs ist irreführend, denn es handelt sich um keine grafische Anwendung. Dieses Programm arbeitet in der Kommandozeile und stellt ein textbasiertes Menü bereit, um Pakete zu finden und zu installieren oder um alle Pakete aus externen Repositories auf dem System zu aktualisieren. Es ist mittels

```
yaourt -S yaourt-gui
```

aus einem AUR installiert und wird dann mit *yaourt-gui* aufgerufen. Die Steuerung erfolgt über die Eingabe der Nummer des gewünschten Menüpunkts. ■

PRO UND CONTRA: ARCH LINUX

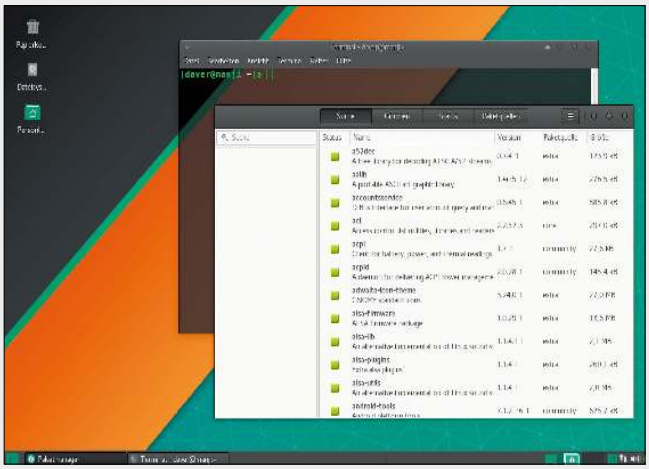
+ schnelles, schlankes, flexibles Linux-System mit neuesten Paketen
+ sehr detaillierte und kompetente Dokumentationen unter *https://wiki.archlinux.org und https://wiki.archlinux.de*
+ kann als Rolling Release jahrelang allein über den Paketmanager aktuell bleiben
– anspruchsvolle, manuelle Installation bei einem puren Arch-System
– Arch-Systeme verlangen relativ häufig Paketupdates
– eignet sich aufgrund der häufigen Updates weniger gut als Serversystem

Arch – Antergos – Manjaro: Die meisten Linux-Distributoren möchten es dem Anwender so leicht wie möglich machen: Livesystem booten, Installer ausführen, fertig. Welche Software dabei auf den PC gelangt und wie die Konfiguration genau aussieht, kann der angehende Anwender dabei zwar selbst bestimmen, aber die Distribution liefert eine vorbereitete Standardkonfiguration und erledigt eine Menge Arbeiten zur Einrichtung des Systems weitgehend selbständig im Hintergrund. Der Installationsprozess eines Ubuntu-Systems oder von Debian, Fedora oder Open Suse besteht aus einer Unmenge von Scripts, die dem Anwender so viele Schritte wie möglich abnehmen.

Arch Linux ist dagegen ein echtes Do-it-yourself-System. Der Arch-Anwender ist in der Regel ein Linux-Experte und installiert das System mittels Standardtools auf der Kommandozeile genau so, wie er es möchte. Arch-Adepten nennen diesen puristischen Ansatz „The Arch Way". Wer das lieber nicht möchte, weil für die Einarbeitung in die Details von Arch weder genügend Zeit noch ausreichend Interesse vorhanden ist, kommt auch nicht zu kurz.

Es gibt mittlerweile Arch-Varianten wie **Antergos** (*https://antergos.com*, Version 17.10 für 64-Bit-PCs ist auf Heft-DVD), die für die Installation kein Linux-Expertenwissen verlangen. Antergos liegt als startfähiges Livesystem mit einem grafischen Installationsprogramm vor, das jenem von Ubuntu ähnlich ist.

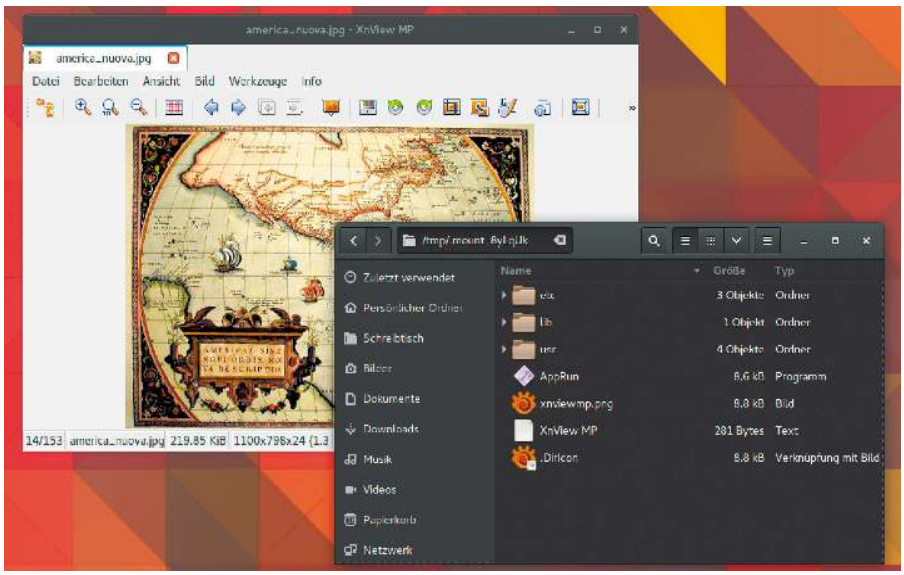
Noch weiter vom puren Arch entfernt ist die Distribution **Manjaro** (*http://manjaro.github.io*), das zwar auch mit Arch-Paketen gebaut ist, diese aber aus eigenen Repositories schöpft. Die Macher von Manjaro hoffen, damit einige raue Kanten zu beseitigen und noch ein Stück einsteigerfreundlicher zu sein.



Manjaro Linux: Die Distribution stammt von Arch Linux ab, hat aber das Ziel, Desktop-Anwendern einen sanfteren Einstieg ins Thema Arch Linux zu bereiten.

Portable Software für Linux

Die traditionelle Paketverwaltung unter Linux hat fundamentale Vorzüge gegenüber dem Softwarewildwuchs à la Windows. Sie ist aber andererseits auch unflexibel und wartungsaufwendig. Appimages sind eine willkommene Ergänzung.



Bildviewer Xnview als portables Appimage: Der Container wird beim Start mit allen Komponenten nach „/tmp/.mounf […] entpackt". Dort lädt das Apprun-Script die eigentliche Software.

VON HERMANN APFELBÖCK

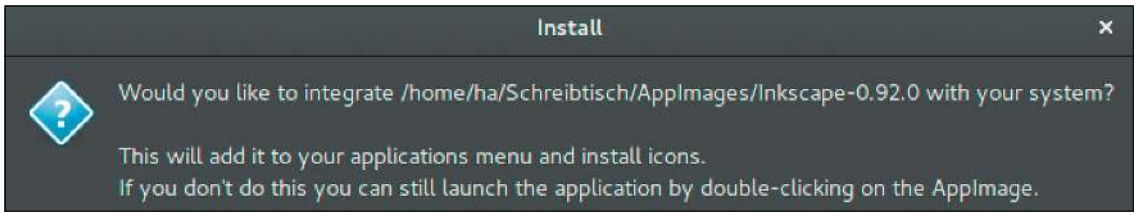
Containerformate haben Konjunktur. Sie bieten distributionsunabhängige Software, umgehen das Problem der Paketabhängigkeiten und erlauben den portablen Einsatz der Software. Gegenüber den technisch aufwendigeren Techniken Snap, Flatpak und Docker haben hier die Appimages einen entscheidenden Vorteil: Auf dem Zielrechner ist keinerlei Werkzeug erforderlich – keine Laufzeitumgebung, kein Paketwerkzeug. Die Images werden einfach heruntergeladen, ausführbar geschaltet und – laufen. Da Appimages keine Sandbox-Isolation (wie Docker & Co.) gegenüber dem übrigen System gewährleisten, wird der Einsatz allerdings zur Vertrauensfrage – ganz ähnlich zu Windows. Wer sich an die vertrauenswürdigen Quellen hält, hat jedoch eine überaus komfortable Technik an der Hand, seine Softwareausstattung zu ergänzen oder gezielt auf den portablen Einsatz auszurichten.

Das Appimage-Format

Appimages gehen auf das schon 2004 geschaffene Format „klik" zurück. Über dessen Folgeprojekt „Portable Linux Apps" erhielt die Weiterentwicklung 2013 die Bezeichnung „Appimage". Es gilt das Prinzip „1 app = 1 file". Typischerweise hat diese eine Containerdatei die Endung „.appimage" oder nur „.app". Dies dient nur der Erkennung für den Nutzer, technisch ist die Endung bedeutungslos und kann nach dem Download auch gelöscht werden. Die Containerdatei enthält neben dem eigentlichen Programm alle notwendigen Komponenten und Bibliotheken. Beim Start durch Doppelklick entpackt ein Wrapper-Script zur Laufzeit zunächst alle Komponenten in ein Verzeichnis „/tmp/.mount […]" und lädt dort dann das eigentliche Programm. Typischerweise erscheint die Software in Taskmanagern dann zweimal – eine Instanz für das eigentliche Programm, die zweite für den Start-Wrapper. Der gesamte Ladevorgang ist komplexer als bei einer nativ installierten Software, was sich aber auf modernen Rechnern allenfalls messbar, aber nicht spürbar auswirkt. Der autarke Container benötigt kein besonderes Ausgangverzeichnis, sondern ist an beliebiger Stelle, auch auf externen USB-Medien lauffähig.

Appimages in der Praxis

Die wichtigsten und vertrauenswürdigen Quellen für Appimages sind folgende:
https://github.com/AppImage/AppImageKit/wiki/AppImages: Diese Liste wurde zwar inzwischen durch *https://appimage.github.io/apps/* ersetzt, ist aber einfacher und übersichtlicher als ihr Nachfolger. Hier finden Sie namhafte Software wie Avidemux, Etcher, Gimp, Kdenlive, Krita, Openshot, Qupzilla, Scribus oder Xnview. Zum Download führt jeweils der Link „Releases" neben dem Produktnamen und nachfolgend der Downloadlink mit der Extension „.AppImage" im Dateinamen.
https://bintray.com/probono/AppImages/ ist eine weitere große Fundgrube für Appima-



Typische Appimage-Frage beim ersten Start: Wird dies bejaht, ist die portable Software auch über das Startmenü oder die Dash-Suche zu finden.

ges unter anderem mit relativ aktuellen Browsern (Firefox, Chromium, Vivaldi) und viel Softwareprominenz wie Calibre, Clementine, Fritzing, Geany, Inkscape, Nightingale, Thunderbird, VLC, Wireshark. Nutzen Sie hier bei der jeweiligen Software den Link „Files“ und dort das Downloadangebot mit der Endung „.AppImage“. Hier lohnt es sich ferner, auf den Zeithinweis „Updated“ zu achten, um das möglichst aktuelle Image auszuwählen.

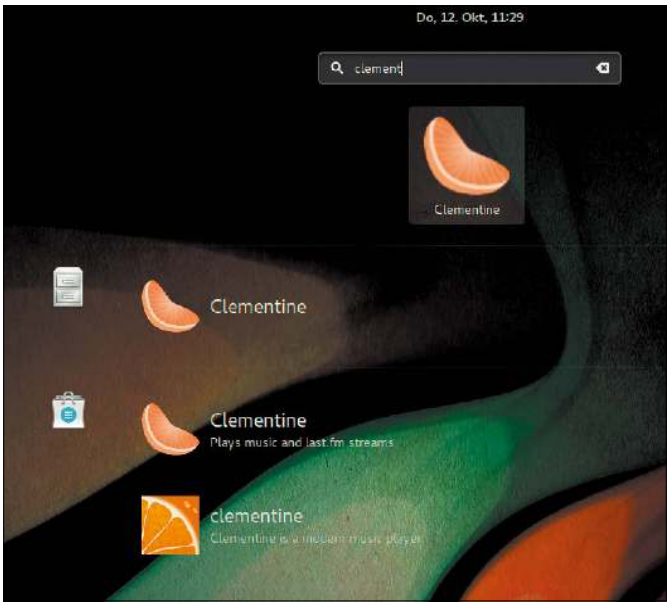
Ergänzend kann das kleinere Angebot auf *https://www.linux-appimages.org/* besucht werden. Es führt aber aktuell nur in Einzelfällen über den Umfang der beiden bereits genannten Quellen hinaus.

Nach dem Download sollten Sie bei aller Portabilität des Pakets dieses in ein Verzeichnis verschieben, wo es dann voraussichtlich verbleiben wird. Das dient erstens der Ordnung und ist zweitens sogar notwendig, wenn Sie die spätere Option zur Systemintegration wahrnehmen wollen (siehe unten). Danach schalten Sie die Imagedatei ausführbar, entweder mit

```
chmod +x [name]
```

im Terminal oder über „Eigenschaften -> Zugriffsrechte“ im Dateimanager. Ab sofort ist die Software einsatzbereit. Beim ersten Start erscheint häufig die Abfrage „Would you like to integrate...“. Wenn Sie mit „Yes“ zustimmen, schreibt das Programm unter „/usr/share/app-install/desktop“ seine „.desktop“-Datei. Dies führt dazu, dass es künftig im Startmenü oder Such-Dash des Systems auftaucht, außerdem im „Öffnen mit“-Dialog des Dateimanagers, was die Verknüpfung mit Dateitypen erlaubt. Kurz: Das portable Programm ist damit praktisch wie eine echt installierte Software in das System integriert.

Beachten Sie ferner, dass die Imagesoftware selbst zwar „readonly“ ist, aber durchaus anpassungsfähig, da sie die Einstellungen im Home-Verzeichnis des Benutzers unter „~/.config/[Software]“, zum Teil auch direkt unter „~/.[Software]“ speichert. Das gewährleistet eine weitestgehend normale Nutzung. Ein Chromium-Appimage kann also durchaus Designs integrieren, eine Software wie Openshot kann wie gewohnt individuell eingerichtet werden.



Der Clementine-Player ist nur als Appimage präsent, aber dennoch über die Gnome-Suche erreichbar. Dafür sorgt die beim Erststart erstellte „.desktop“-Datei.

Die „Deinstallation“ ist natürlich ebenso einfach: Es genügt, die Appimage-Datei auf Dateiebene manuell zu löschen, gegebenenfalls auch noch den Konfigurationsordner unter „~/.config“.

Da Appimages nicht updatefähig sind, sind sicherheitskritische Programme wie Browser und Mail nicht unbedingt erste Kandidaten. Einschlägig sind hingegen Tools wie Avidemux, Etcher, Krita, Openshot, Xnview, die man immer wieder mal und eventuell auf verschiedenen Linux-Systemen benötigt. ■

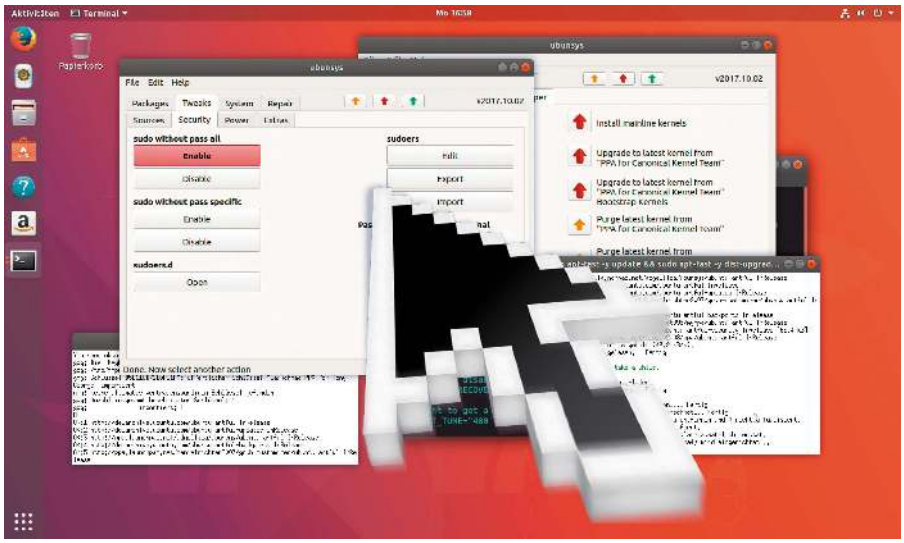
APPIMAGES: VORTEILE UND NACHTEILE

+ universelles, distributionsunabhängiges Format: Appimages laufen auf den allermeisten Linux-Distributionen
+ keine Installation, keine Paketabhängigkeiten
+ keine root-Rechte erforderlich, da keine Systemdateien berührt werden
+ eine Software = eine einzige Datei: läuft portabel aus jedem Ordner – auch von USB oder DVD
+ Appimages erlauben die Verwendung verschiedener Versionen nebeneinander
+ simple „Deinstallation“ durch Löschen der Appimage-Datei
+ individuelle Einstellungen durch Konfigurationsdateien unter „~/.config/[Software]“ oder „~/.[Software]“
+ optionale Systemintegration (Menü, „Öffnen mit“-Dialog) durch „.desktop“-Datei

– Appimages sind „readonly“ und folglich nicht updatefähig
– Appimage bieten keine Sandbox-Isolation
– Appimages stammen ohne Drittkontrolle direkt vom Softwareentwickler

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 interessantesten 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.

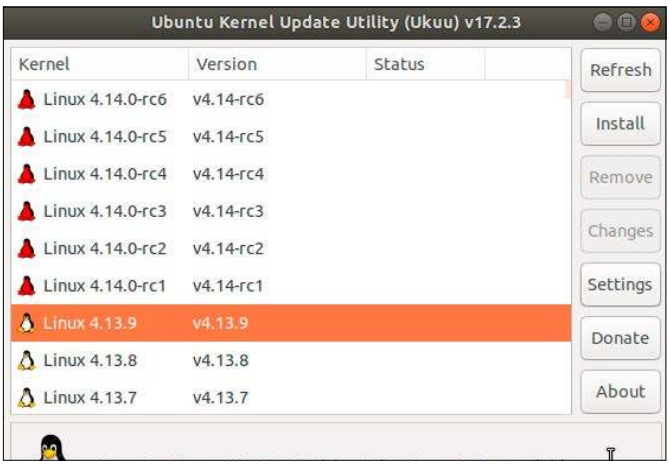
Einzelne Programme ohne Passwort: Weniger riskant als ein generell passwortloses sudo ist die Definition eines einzelnen Kommandozeilenprogramms, das der aktuell angemeldete User ohne Passwort aufrufen darf. Der Menüpunkt „Tweaks -> Security -> sudo without pass all -> Enable“ öffnet ein Terminal, das 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.

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.

Gewagte Einstellungen und Experimente: Ubunsys ist derzeit noch eine bunte 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.

Fazit: Nützlich bis riskant

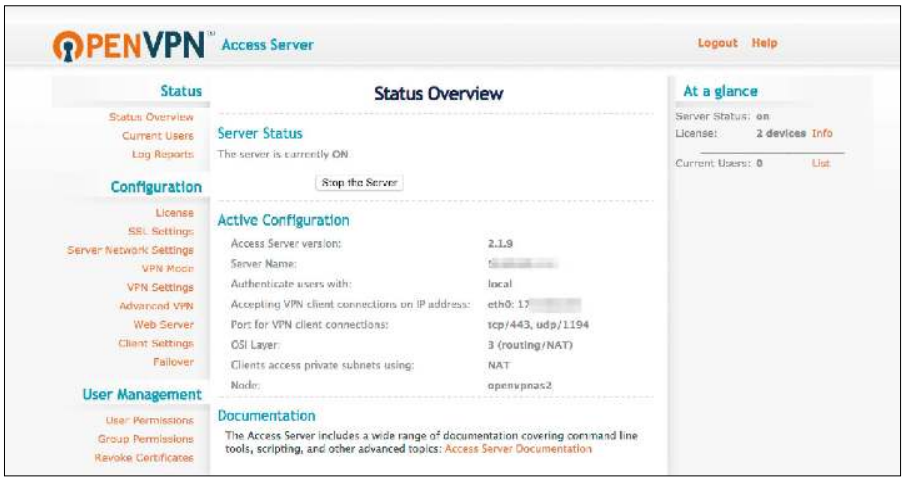
Nach einigen Experimenten mit Ubunsys, die man tunlichst nicht auf einem produktiv eingesetzten Ubuntu-System unternehmen sollte, wird klar, dass es sich noch um Betaware handelt. Die Funktionen unter „Tweaks -> Power“ sind in einigen Ubuntu-Versionen wirkungslos und sollten lieber über die verwendete 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)

Amazon Web Services unter Linux

Bei Amazon eingekauft hat wahrscheinlich schon jeder. Die Computingplattform des Handelsriesen kennen aber nur die wenigsten. Dabei arbeiten die Amazon Web Services ganz hervorragend mit Linux zusammen.



Beispiel für Amazon Web Services: Ein Open-VPN-Server ist schnell eingerichtet. Auf Wunsch ändern Sie die Einstellungen wie zum Beispiel einen abweichenden DNS-Server.

VON STEPHAN LAMPRECHT

Bei Amazon denkt man an Waren aller Art und vielleicht auch an Streaminginhalte. Dabei verdient der Konzern einen Großteil seines Geldes mit den Einnahmen aus seiner Cloudplattform. Die Amazon Web Services (AWS) wurden vor mehr als zehn Jahren vorgestellt und sind vor allen Dingen eines: preiswert. Riesige Datenmengen können in den Rechenzentren von Amazon gespeichert werden zu deutlich geringeren Kosten, als die Anschaffung eigener Hardware erfordern würde.

Amazon-Konto genügt

Für die Nutzung der meisten Dienste auf der Computingplattform von Amazon fallen Gebühren an. Es gibt hier aber auch Konfigurationen, die völlig kostenfrei laufen können, weil die Projekte sehr klein sind. Da ein laufendes System stets mit wenigen Mausklicks erweitert werden kann, ist für die Nutzung von AWS die Hinterlegung einer gültigen Kreditkarte notwendig. Wer bereits bei Amazon etwas gekauft hat und damit über ein Benutzerkonto verfügt, kann dieses einfach weiterverwenden. Besuchen Sie die Seite *https://aws.amazon.com/de/console/* und melden Sie sich dann dort an.

Universum von Möglichkeiten: Wer die Managementkonsole von AWS erstmals besucht, dürfte von den vielen Einträgen auf der Startseite wohl erschlagen sein. Im Kern bietet Amazon hier drei Grundfunktionen: Virtuelle Server mit unterschiedlichen Betriebssystemen, Massenspeicher in der Cloud sowie Datenbanken und Datenbankserver. Rund um diese drei Bereiche werden dann noch eine ganze Reihe weiterer Services offeriert.

Beispiel: Open VPN einrichten

AWS bieten in ihrem breiten Portfolio auch alles, was Sie für die Einrichtung eines eigenen VPN-Servers benötigen. Das Aufsetzen von Open VPN ist zudem ein überschaubares Beispiel, um sich mit dem Amazon-Dienst vertraut zu machen. Nachdem Sie ein Benutzerkonto eingerichtet haben, wählen Sie über das Listenfeld am oberen Rand den Standort für den virtuellen Server aus. Da Sie wohl kaum unter das Bundesdatenschutzgesetz fallen, haben Sie hier die freie Auswahl. Nutzen Sie beispielsweise das Datencenter in Irland. Über den Menüpunkt „Services“ wählen Sie „EC2“. Es gibt verschiedene Möglichkeiten, den Server Open VPN auf einem virtuellen Computer zu installieren. So können Sie manuell einen Server aufsetzen, sich per SSH damit verbinden, um dann als Root die passenden Softwarepakete zu installieren.

Schneller und richtig elegant ist der so genannte Marketplace von Amazon. Dort abonnieren Sie die Softwarepakete, die Sie brauchen, die dann auch gleich eingerichtet werden. Ein solches Abonnement wird wie alle Dienste bei AWS auf die Minute exakt abgerechnet und auch eine kostenlose Nutzung ist möglich.

Klicken Sie in der Mitte der Seite auf „Launch instance“. Im ersten Schritt müssen Sie sich für eine virtuelle Maschine entscheiden. Wechseln Sie hier in das Register „AWS Marketplace“. Suchen Sie dort nach „OpenVPN“ und nutzen Sie den Eintrag „OpenVPN Access Server“. Klicken Sie auf „Select“, erhalten Sie eine Zusammenfassung der Preisliste. Diese zeigt Ihnen an, was bei einer Nutzung der verschiedenen Ausbaustufen pro Stunde berechnet würde. Die Preise richten Sie dort nach der eingesetzten Instanz. Bestätigen Sie die Zusammenfassung und fahren Sie fort. Auf der nachfolgenden Seite klicken Sie in das Optionsfeld vor „t2.micro“. Klicken Sie auf „Review and Launch“.

Die nächste Option betrifft die SSD der virtuellen Maschine. Belassen Sie hier am besten alles bei den Voreinstellungen. Auf der nächsten Seite klicken Sie auf „Launch“. Jetzt folgt ein wichtiger Schritt. Sie müssen ein Schlüsselpaar für die Absicherung definieren. Aus dem ersten Listenfeld entscheiden Sie sich für „Create a new key pair“. Vergeben Sie einen eindeutigen Namen und drücken Sie auf „Download Key Pair“. In einem Terminal auf Ihrem lokalen System wechseln Sie in den Ordner mit dem heruntergeladenen Schlüssel und geben dort

```
sudo chmod 400 [Ihr-Schluessel].pem
```

ein. Jetzt können Sie, ebenfalls in einem Terminal, die eigentliche Installation durchführen. Dazu führen Sie den Befehl

```
ssh -i "schluesseldatei.pem"
  openvpnas@[IP-Adresse]
```

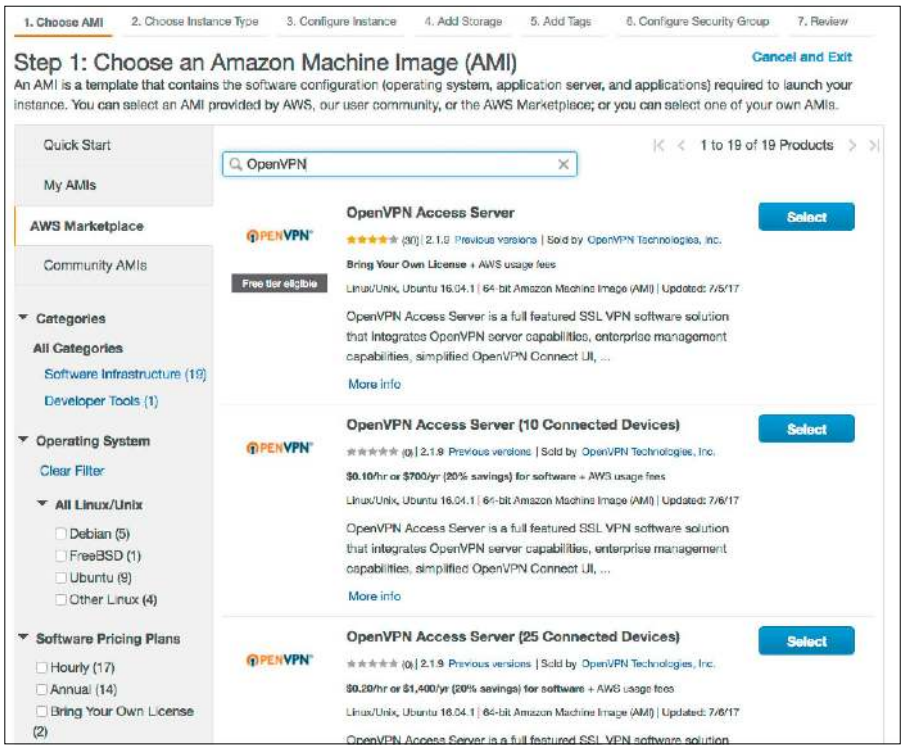
aus. Sie werden darauf hingewiesen, dass der Schlüssel nicht verifiziert werden kann. Bestätigen Sie die Ausnahme mit „Yes“. Danach durchlaufen Sie den Assistenten. Belassen Sie es bei allen Schritten bei den Voreinstellungen. Achtung! Verlassen Sie am Ende der Installation das System nicht, bevor Sie nicht das Passwort für den Admin geändert haben. Sie können sich sonst nicht mehr anmelden. Hat das System also „Initial Configuration Complete“ gemeldet, vergeben Sie nach dem Befehl

```
passwd -s openvpn
```

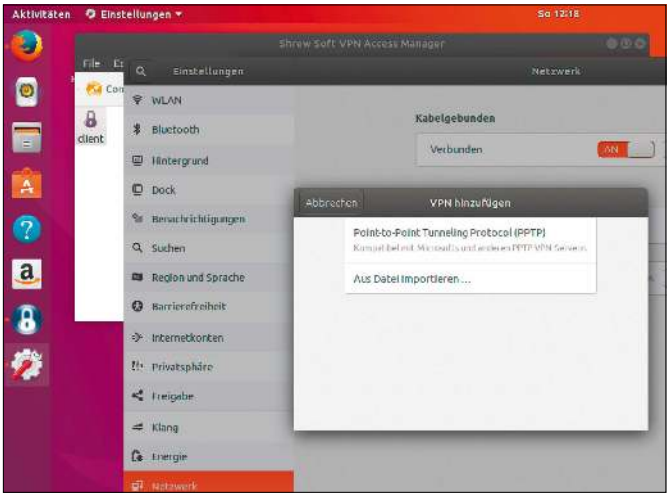
das neue Passwort.

Nutzer anlegen und Zugangsdaten abholen: Nachdem Sie das Passwort geändert haben, besuchen Sie mit einem Browser den Server „https://[IP-Adresse]:943/admin“. Sie melden sich als „openvpn“ und mit dem gerade vergebenen Passwort an. Unter „User Management“ rufen Sie die „User Permissions“ auf. Vergeben Sie einen Nutzernamen und klicken Sie auf „Save Settings“. Damit wird der neue Benutzer angelegt. Mit „Show“ neben einem Nutzernamen öffnen Sie weitere Optionen. Dort können Sie jetzt das Passwort hinterlegen. Verlassen Sie den Server und rufen Sie ihn jetzt erneut auf, diesmal ohne „/admin“ am Ende der URL. Loggen Sie sich jetzt als Nutzer ein, den Sie gerade eingerichtet haben. Am Ende der Seite können Sie sich eine Konfigurationsdatei herunterladen (Endung „.ovpn“).

Diese lesen Sie dann später unter Windows oder Mac-OS in VPN-Clients ein. Unter Ubuntu klicken Sie zum Einlesen auf das Netzwerksymbol in der oberen Navigation. Hier wählen Sie den Bereich „VPN Verbindungen“, führen die Konfiguration aus und nutzen die Importfunktion, um die Datei einzulesen. Fertig! Wenn Sie den Server gerade nicht benötigen, setzen Sie ihn einfach in den Stopmodus, um Gebühren zu sparen.



Der passende VPN-Server ist schnell gefunden: Über den Marketplace gehen Auswahl und Einrichtung neuer virtueller Instanzen einfach von der Hand.



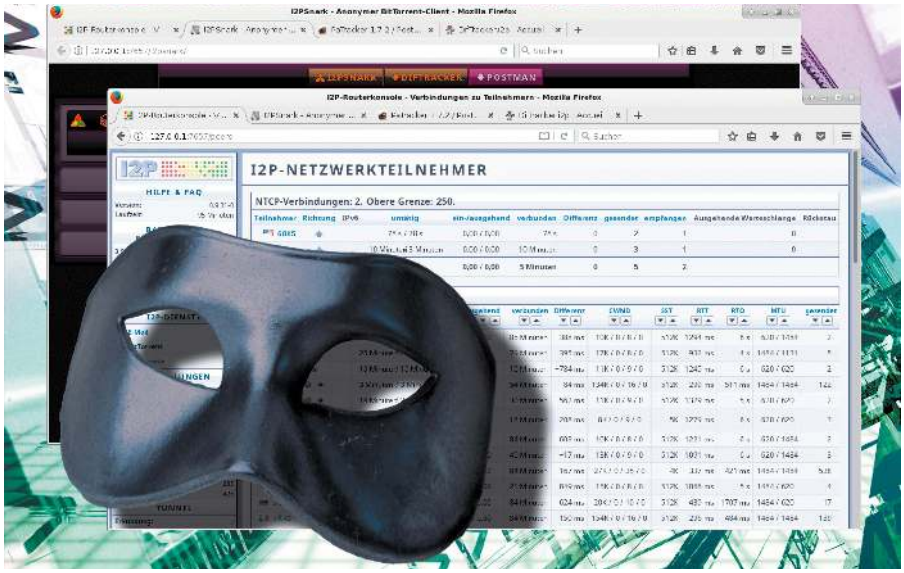
Optionen in den VPN-Client importieren (hier Ubuntu): Die individuellen Einstellungen für die Verbindung kann sich jeder Nutzer nach Anmeldung auf dem Server herunterladen.

Amazon als Datenspeicher verwenden

Eine andere Anwendung der Amazon Web Services ist die Nutzung von Amazon S3. Das ist unbegrenzter Speicherplatz in der Cloud, für den Gebühren bei der Übertragung anfallen. Die Einrichtung eines so genannten S3-Buckets ist selbsterklärend. Auf Github gibt es Projekte, die es erlauben, ein Amazon-Bucket als Dateisystem direkt unter Linux einzubinden (*https://github.com/s3fs-fuse/s3fs-fuse/wiki/Fuse-Over-Amazon*). Installation und Nutzung sind gut dokumentiert, sodass Sie binnen kürzester Zeit mit dem Cloudspeicher wie mit lokalem Speicher arbeiten können. Oder Sie probieren einmal das Programm Cross FTP aus, das ebenfalls mit S3 umgehen kann. ■

Invisible Internet Project I2P

Anonymität im Internet ist aufwendig und verlangt nach separaten, spezialisierten Netzwerken. Das „Invisible Internet Project“ arbeitet, anders als TOR, nach dem Peer-to-Peer-Prinzip, um ein alternatives Internet aufzubauen.



VON DAVID WOLSKI

Waren Anonymisierungsdienste wie TOR und das technisch verwandte „Invisible Internet Project“ (I2P) bislang hauptsächlich für Dissidenten in gefährlichen Regionen von Bedeutung, nebenher auch für Kriminelle und lichtscheue Zeitgenossen, so bekommen diese Netzwerke jetzt von allen Anwenderkreisen mehr Aufmerksamkeit. Die umfassende Überwachung von Onlineaktivitäten, Gesetze gegen freie Meinungsäußerung und die Datensammelwut privater Onlineunternehmen verleihen anonymen Netzen eine neue Legitimität. Die Motivation vieler Nutzer ist nicht mehr (nur) die Verschleierung von Straftaten, sondern der stille Protest gegen Datensammelwut und Vorratsdatenspeicherung mit praktischen Mitteln.

I2P: Die Unterschiede zu TOR

Während es TOR vornehmlich darum geht, verkettete Proxyserver als anonymisierende Vermittlungsstationen zwischen Besuchern und Servern bereitzustellen, liegt der Schwerpunkt von I2P auf einem abgeschotteten Netzwerk. Zwar kommt man auch aus dem I2P-Netz heraus auf reguläre Server, der vorrangige Zweck von I2P ist aber die Bereitstellung eines „Darknet“, also eines alternativen, abgeschotteten Internets. Die Server in diesem Darknet nennen sich „Eepsites“ und haben sogar die eigene Top-Level-Domain „.i2p“ – welche natürlich nur innerhalb des I2P-Netzwerks funktioniert.

Das I2P-Protokoll arbeitet mit durchgehender Punkt-zu-Punkt-Verschlüsselung zwischen Besucher und Server, die sich anhand eines stets neu generierten, kryptografischen Fingerabdrucks für die Dauer einer Verbindung identifizieren. Im Unterschied zu TOR funktioniert I2P dezentral ohne zentrales Knotenverzeichnis. Die Funktionsweise gleicht dem einer Tauschbörse im Peer-to-Peer-Prinzip: Jeder Teilnehmer wird zum Proxyknoten im internen I2P-Netzwerk und leitet den verschlüsselten Traffic anderer Teilnehmer weiter. Kein Teilnehmer wird dabei zu einem Ausgangsknoten (Exit-Node), der für andere Verbindungen ins Internet anonymisiert.

Außerdem werden allein durch die Teilnahme als Proxyknoten keine Daten anderer I2P-Teilnehmer verschlüsselt oder im Klartext auf dem eigenen Computer gespeichert. Anders als bei TOR ist im I2P-Netz die Verwendung von Bittorrent nicht verpönt, sondern ausdrücklich erwünscht. Dies ist auch eines der hauptsächlichen Anwendungsbereiche für I2P – als anonyme Bittorrent-Alternative.

Am „Invisible Internet Project“ teilnehmen

Der Zugang zum I2P-Netzwerk ist für jeden Internetnutzer möglich und erfolgt über einen Client, der in Java vorliegt und damit auf den meisten Betriebssystemen funktioniert. Der Java-Client arbeitet als lokaler Proxyserver auf dem Localhost. Um dann mit dem Browser auf das I2P-Netz zugreifen zu können, trägt man die Localhost-Adresse dieses Proxyservers in die Proxyeinstellungen des Browsers ein.

1. Die offiziellen, regelmäßig aktualisierten I2P-Clients für verschiedene Betriebssysteme liegen auf der Seite *https://geti2p.net/de/download*. Es empfiehlt sich für alle Linux-Systeme, zunächst mit dem Java-ba-

sierten Client zu arbeiten. Die dazu meist noch benötigte Java-Runtime ist in allen Distributionen schnell installiert, in Debian/Ubuntu beispielsweise mit diesem Befehl:

```
sudo apt-get install default-jre
```

2. Der weitere Befehl

```
java -jar i2pinstall_0.9.31.jar
```

startet im Terminal die Installation. Dabei entpackt sich lediglich der Client in den Ordner „~/i2p“ im Home-Verzeichnis.

3. Wieder im Terminal setzt nun das Kommando

```
~/i2p/i2prouter start
```

den Client in Gang und öffnet automatisch die Konfigurationsseite im Browser des I2P-Clients, der auf „http://127.0.0.1:7657“ eine Übersicht präsentiert.

4. Es empfiehlt sich, nicht den regulären Browser zur Teilnahme an I2P zu konfigurieren, sondern dafür einen separaten Browser zu installieren, um die Surfaktivitäten strikt zu trennen. Firefox gibt es für sämtliche Linux-Systeme als gepackte ausführbare Binary (auf *www.mozilla.org/de/firefox/all5*, 52 MB). In den Einstellungen des Browsers, hier Firefox 56, öffnet der Punkt „Einstellungen -> Allgemein -> Netzwerk-Proxy -> Einstellungen“ die Konfigurationsseite für den Proxy. Nach einem Klick auf „Manuelle Proxy-Konfiguration“ kommt in das Feld „HTTP-Proxy“ die Adresse „localhost“ und in das Feld „Port“ die Nummer 4444. Darunter, im Feld „SSL-Proxy“, geben Sie ebenfalls „localhost“ an und hier den Port 4445. Ganz unten müssen in das „Kein Proxy“ noch die lokalen Adressen „localhost, 127.0.0.1“ hinein.

Browser für I2P konfigurieren: Der I2P-Client arbeitet als lokaler Proxy-Server, der Verbindungen auf den Ports 4444 (HTTP) und 4445 (HTTPS) annimmt.

Damit ist der Browser bereit zur Teilnahme. Eine geeignete Testseite ist die interne Wiki *http://i2pwiki.i2p*, das auch gleich einige Links zu Eepsites kennt.

Fazit: Gebremstes Darknet

Wer im I2P-Netz unterwegs ist, braucht allerdings Geduld. Zunächst muss der I2P-Client eine Weile laufen, um genügend Peers zu finden. Es wird schnell klar, dass es wie in allen Peer-to-Peer-Netzen mit begrenzter Bandbreite zugeht. Auf der Konfigurationsseite „http://127.0.0.1:7657“ sollten Sie deshalb im Untermenü „Bandbreite“ die Werte für eingehende und ausgehende Verbindungen an die tatsächliche Leistung der Internetverbindung anpassen. Dann gilt es, über die Seite *http://identiguy.i2p* funktionierende Eepsites zu finden, die ebenso schnell entstehen, wie sie verschwinden. Insgesamt wirkt I2P wie eine Zeitreise in die ersten Jahre des World Wide Webs: Dies war auch noch weitgehend unreguliert, aber über Modemverbindungen ebenso langsam. ■

LIVE-CD: I2P MIT TAILS

Ein Test von I2P ist auch mit der älteren Version 2.11 des bekannten Livesystems Tails möglich.

Dies ist die letzte Version von Tails mit einem Client für I2P. Mangels Entwickler haben es die Macher von Tails nicht geschafft, den Client in die neue Versionsserie 3.x einzubauen. Tails 2.11 steht aber immer noch unter *https://archive.org/details/tails-i386-2.11* als ISO-Datei zum Download bereit (1,1 GB). Es handelt sich um keine offizielle Tails-Webseite und das Image ist deshalb nur eingeschränkt vertrauenswürdig, für einen Test aber ausreichend.

Zur Verwendung von I2P unterbricht man den Start des Livesystems auf dem Bootbildschirm mit der Tab-Taste und ergänzt die unten angezeigten Bootparameter nach einem Leerzeichen mit der Eingabe *i2p*.

Nach Druck der Eingabetaste startet Tails wie gewohnt, lädt aber einen I2P-Client im Hintergrund. Es sind jetzt einige Minuten Wartezeit gefragt, bis sich das Livesystem im I2P-Netz mit genügend Teilnehmern bekannt gemacht hat. Danach startet der Menüpunkt „Anwendungen -> Internet I2P-Browser“ den Firefox-Browser mit der I2P-Konfigurationsseite. Von dort geht es weiter ins I2P-Netz.

Teilnahme über Tails: Die ältere Version Tails 2.11 hat noch einen optionalen I2P-Client an Bord, den man beim Booten explizit aktivieren muss.

Neue Software

Neben Schwergewichten wie Kicad und Virtualbox gibt es wieder eine Zahl kleinerer, cleverer Tools für Linux. Auch Shareware ist dabei: Der Editor Sublime Text und die Buchhaltungssoftware Lin-Habu setzen auf dieses Modell.

VON DAVID WOLSKI

Entwickler von Open-Source-Programmen mit grafischer Oberfläche müssen sich früh in der Entstehungsphase entscheiden, mit welchem Toolkit Menüs und Fenster arbeiten sollen. Es ist nicht nur eine Frage der Äußerlichkeiten: GTK+ oder Qt oder etwas ganz anderes?

Die beiden verbreiteten Toolkits, GTK+ und Qt, sind dabei eng mit den Fortschritten der jeweiligen Desktopumgebungen verknüpft, in deren Windschatten sie gedeihen.

GTK+ ist eine Gnome-Bibliothek, kümmert sich seit den frühen Phasen dieser Arbeitsumgebung um deren Programm-GUIs und ist wie Gnome inzwischen bei Version 3.26 angelangt.

Qt ist ein Baustein von KDE, war aber schon 1991 erschienen und ist damit älter als der KDE-Desktop. Dieses Toolkit ist erst seit 2008 komplett und bedingungslos unter der GNU Public License freigegeben.

Bibliotheken sind entscheidend

Sowohl GTK+ als auch Qt können über Bindings in hohe Programmiersprachen wie C++, C#, D, Rust und viele weitere eingebunden werden. Dazu kommen noch führende Script-Sprachen wie Python, PHP und sogar Javascript. Auch sind GTK+ und Qt nicht nur auf eine Plattform wie den Linux-Desktop beschränkt, sondern haben Portierungen auf Windows, zu Mac-OS und Android erhalten. Die meisten hier vorgestellten Programme für Linux verwenden entweder GTK+ oder Qt, nur selten ein ganz anderes Toolkit. So verwendet beispielsweise das vorgestellte Virtualbox schon immer Qt, das Gnome-Programm Geary von Haus aus GTK+ und die Java-Software Filebox setzt auf Java FX für seine grafische Oberfläche.

GTK+ legt Steine in den Weg

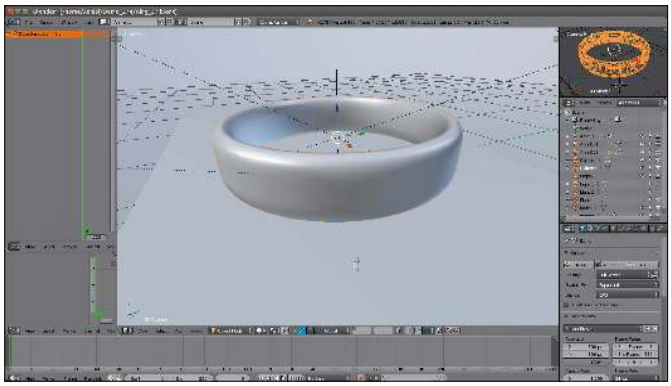
Das Gnome-Toolkit GTK+ genießt eigentlich einen Heimvorteil, ist in der Gunst der Entwickler in den letzten Jahren aber stark gefallen. GTK+ 1.0 wurde schon 1998 veröffentlicht und diente zunächst nur den Programmierern der Grafikbearbeitung Gimp als Bibliothek für deren Steuerelemente. Aufgrund seiner Lizenz und puren C-Bibliotheken wurde GTK+ unter Linux groß, galt aber schnell als veraltet und fehleranfällig. Seitdem hat GTK+ mit Version 2 und zuletzt mit Version 3 grundlegend neue Inkarnationen erlebt, die nicht abwärtskompatibel zu den Vorgängerversionen sind. Genau das bereitet Entwicklern Kopfzerbrechen: Die API in GTK+ ändert sich vergleichsweise oft und erfordert auch innerhalb einer Hauptversion Nacharbeiten am Programmcode.

Es gibt deshalb seit einiger Zeit die Tendenz, zum stabileren Qt abzuwandern, sogar bei den Desktopumgebungen: So wechselt LXDE mit LXQT das Toolkit und auch der Budgie-Desktop will sich demnächst in Qt neu erfinden.

Blender 2.79

3D-Modeller und Renderer
www.blender.org

Nach einem Jahr meldet sich der Renderer und Modeller Blender in neuer Version zurück. Er macht zur Berechnung von Szenen über Open CL ausgiebig von der GPU Gebrauch, was bei starken Grafikkarten einen Geschwindigkeitsschub bringt. Die Oberfläche sieht auf Hi-DPI-Bildschirmen besser aus, bei den Tools gibt es ein verbessertes Deformierungswerkzeug. Das PPA *https://launchpad.net/~thomas-schiex/+archive/ubuntu/blender* bietet Pakete für Ubuntu. ■

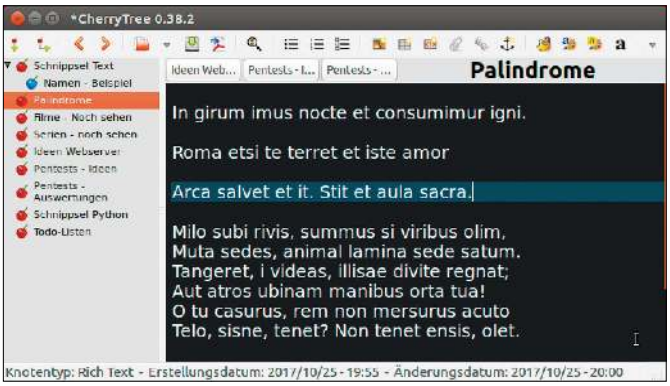


Es ist nie zu spät, sich in Blender einzuarbeiten: Blender ist das führende Open-Source-Programm zur 3D-Modellierung und Animation.

Cherrytree 0.38.2

Ordnung für Notizen
www.giuspen.com/cherrytree

Das Open-Source-Programm speichert Aufzeichnungen in einer frei definierbaren Baumstruktur und in Kategorien. Der Texteditor unterstützt Formatierung, To-Do-Listen, Bilder sowie Syntaxhervorhebung für mehrere Programmiersprachen. Die aktuelle Version bringt Zeitstempel für neue Einträge, bessere Formatierungswerkzeuge und eine Aufräumfunktion für die Sqlite-Datenbank. Die Projektseite liefert ein DEB-Paket für Ubuntu und einen Link zu einem PPA. ■

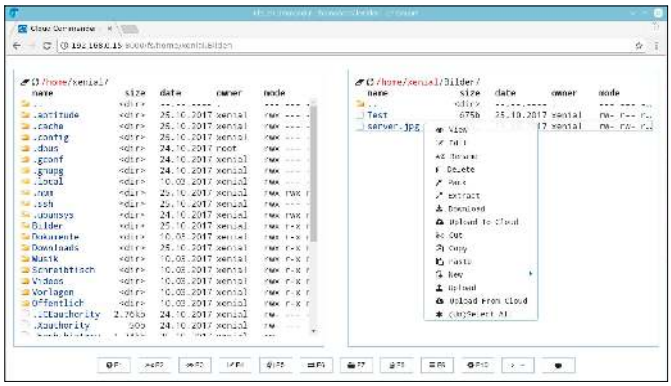


Informationen strukturiert ablegen: Cherrytree bringt Ordnung in eine Notizsammlung und speichert in einer Sqlite-Datenbank.

Cloud Commander 8.1.2

Zwei-Fenster-Dateimanager für Webserver
http://cloudcmd.io

Nicht nur in der Shell und auf dem Desktop haben sich Zwei-Fenster-Dateimanager bewährt. Der Cloud Commander ist ein Projekt für Node.JS, das einen Dateimanager dieser Art in den Browser bringt. Das Programm läuft serverseitig und stellt über eine Browseroberfläche Dateioperationen und einen Texteditor für die Serverdateien bereit. Nützlich ist dies auch für einen Raspberry Pi im LAN. Die Installation mittels NPM-Paket ist auf der Projektseite beschrieben. ■

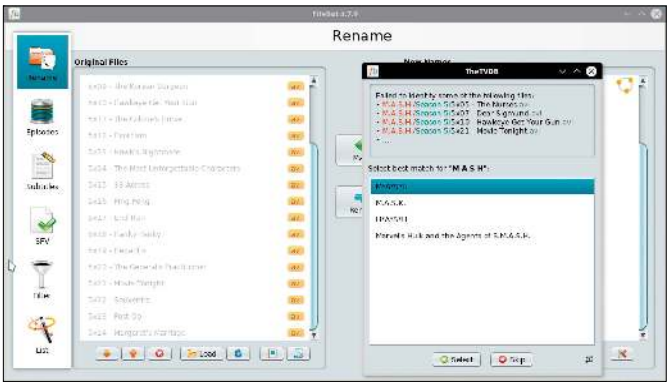


Zwei Fenster zum Server: Cloud Commander ist in Node.JS erstellt und bringt einen Dateimanager auf dem Server in den Browser.

Filebot 4.7.9

Bringt Ordnung in das Filmarchiv
www.filebot.net

Wenn sich heruntergeladene Serien aus verschiedenen Quellen mit abweichenden Namensschema auf der Festplatte tummeln, sorgt Filebot für Systematik. Das Tool verlangt eine Java-Runtime und ist damit systemunabhängig. Über die grafische (englischsprachige) Oberfläche wählt man Verzeichnisse, benennt Dateien anhand von Onlinedatenbanken um und ergänzt Untertitel. Es gibt auch eine Kommandozeilenversion und eine Script-Sammlung. ■

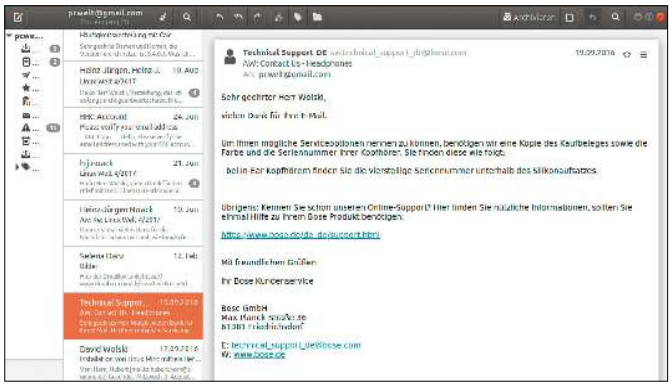


Aufräumen und ergänzen: Der Filebot gleicht Dateinamen von Serien und Filmen mit Onlinedatenbanken ab und lädt Untertitel herunter.

Geary 0.12

Mailclient für Gnome
https://wiki.gnome.org/Apps/Geary

Als Alternative zu Thunderbird mit einfach strukturierter Programmoberfläche hat Geary viele Freunde gefunden. Das Programm stammt von den Machern der Bildverwaltung Shotwell, ist jetzt aber bei der Gnome-Foundation untergekommen. Geary unterstützt das Protokoll IMAP und die Webdienste Gmail, Yahoo Mail und Outlook.com. Geary kann beliebig viele Mailkonten verwalten und liegt bereits in den Standard-Paketquellen von Ubuntu 17.10 bereit. ■

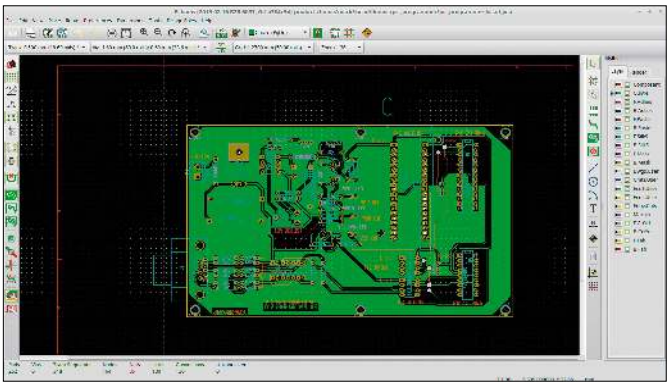


Unkomplizierter Mailclient: Geary ist mit Gmail, Yahoo Mail und Outlook.com schnell eingerichtet, unterstützt aber kein POP3 mehr.

Kicad 4.0.7

EDA-Programm zur Erstellung von Leiterplatten
www.kicad-pcb.org

Das Designprogramm für Leiterplatten macht mit Version 4.0 einen großen Sprung. Zur Grafikausgabe und Berechnung nutzt das Open-Source-Programm jetzt Open GL. Kicad wird vom Cern, der Raspberry Pi Foundation und der Universität Grenoble unterstützt und bildet alle Schritte von der Erstellung der Schaltpläne bis zur Ausgabe der Plotterdateien ab. Installationshinweise gibt es auf *www.kicad-pcb.org/display/KICAD/Installing+KiCad.* ■

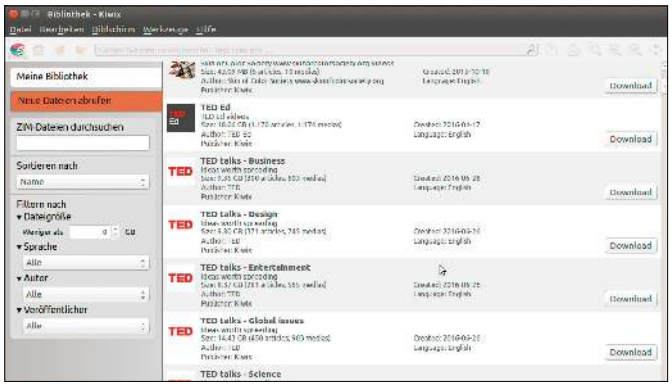


Bastelprojekte und komplexe Leiterplatten: Kicad hat Werkzeuge für Schaltpläne und Fertigung von PCBs parat.

Kiwix 0.9

Offlinereader für Wikipedia & Co.
www.kiwix.org

Kiwix kann ein Archiv an freien Bildungsinhalten aufbauen, die dann auch in Offlinezeiten auf dem Datenträger liegen. Downloadlinks zum Aufbau des Offlinearchivs umfassen beispielsweise Wikipedia, Wikitravel, Wiktionary oder die Videobibliothek der TED-Talks. Textinhalte speichert Kiwix komprimiert. Die gesamte Wikipedia belegt so nur 60 GB. Kiwix gibt es auf der Projektwebseite für Linux, aber auch für Windows, Mac-OS und Android. ■

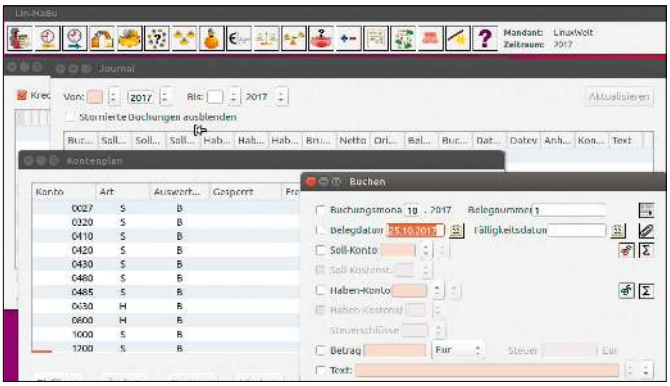


Nachlesen ohne Internet: Kiwix lädt freie Inhalte von Mediawiki-Webseiten wie Wikipedia zum späteren Offlinelesen.

Lin-Habu 17.2

Buchhaltung für Selbständige
https://goo.gl/RCEN8k

Beim Thema Buchhaltung ist die Auswahl an Linux-Software nicht groß. Lin-Habu ist eines der wenigen Programme für Selbständige, das dank stetiger Updates mit dem Steuerrecht mithält und regelmäßig neue Zertifikate der Steuerbehörde für Elster erhält. Das hat seinen Preis: Lin-Habu ist Shareware und läuft 60 Tage ohne Registrierung. Lizenzen gibt es je nach Funktionsumfang von 60 Euro bis 250 Euro. Lin-Habu liegt als ausführbare Binary vor. ■

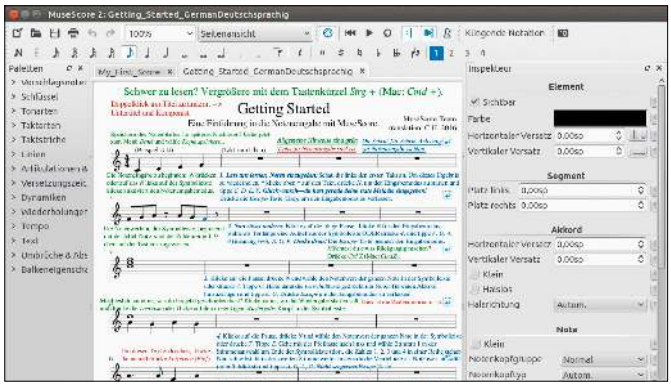


Buchhaltungssoftware mit Elster-Anbindung: Lin-Habu liegt in vier Versionen mit kleinem bis großem Funktionsumfang vor.

Musescore 2.1

Editor für Notensatz mit Midi-Schnittstelle
http://musescore.org

Das bemerkenswerte Update des Notensatzprogramms Musescore erlaubt die Eingabe von Musikstücken per Midi-Keyboard und bietet dafür jetzt auch ein Metronom. Das Programm kann Notenblätter auf *https://musescore.com/* in eine Tauschbibliothek hochladen, das Dateiformat von Guitar Pro importieren, Midi-Dateien erzeugen sowie PDFs ausgeben. Pakete für Ubuntu liefert das PPA *https://launchpad.net/~mscore-ubuntu/+archive/ubuntu/mscore-stable*.



Perfekte Musiknotation: Musescore ist Open Source und liefert einen mächtigen Noteneditor, der die Eingabe per Midi unterstützt.

Oracle Virtualbox 5.2

Hypervisor für virtuelle Maschinen
www.virtualbox.org/wiki/Downloads

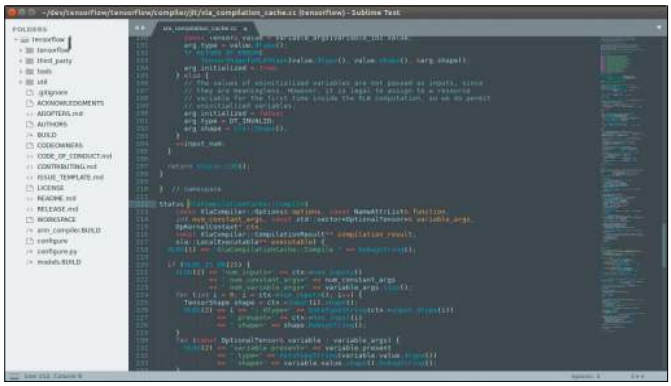
Neben zahlreichen Bugfixes und besserer Kompatibilität mit neuen Linux-Gastsystemen wie Ubuntu 17.10 realisiert Virtualbox 5.2 eine lange versprochene Funktion: Einige Systeme können automatisiert in VMs installiert werden. Dazu dient das Kommandozeilentool Vboxmanage mit dem neuen Parameter „unattended", der Daten wie Passwort und Benutzername an eine VM übergibt. Der Downloadlink liefert Pakete für alle wichtigen Distributionen.

Mit Autopilot: Virtualbox unterstützt nun wie Vmware die unbeaufsichtigte Installation von Gastsystemen.

Sublime Text 3

Schneller, moderner Codeeditor
www.sublimetext.com

Kein Open-Source-Programm, sondern Shareware: Sublime Text hat sich unter Mac-OS einen Namen als schneller Quellcodeeditor gemacht und liegt nun auch für Linux vor. Das Programm unterstützt Hi-DPI-Monitore, hat eine umfangreiche Syntaxhervorhebung und einen Symbolindexer für automatische Sprungmarken. Sublime Text 3 liegt für alle wichtigen Distributionen vor, kostet 80 Euro pro Anwender, lässt sich aber unbegrenzt lange testen.



Coden mit Stil: Sublime Text 3 ist ein Editor für anspruchsvolle Entwickler und hat den Weg von Mac-OS zu Linux geschafft.

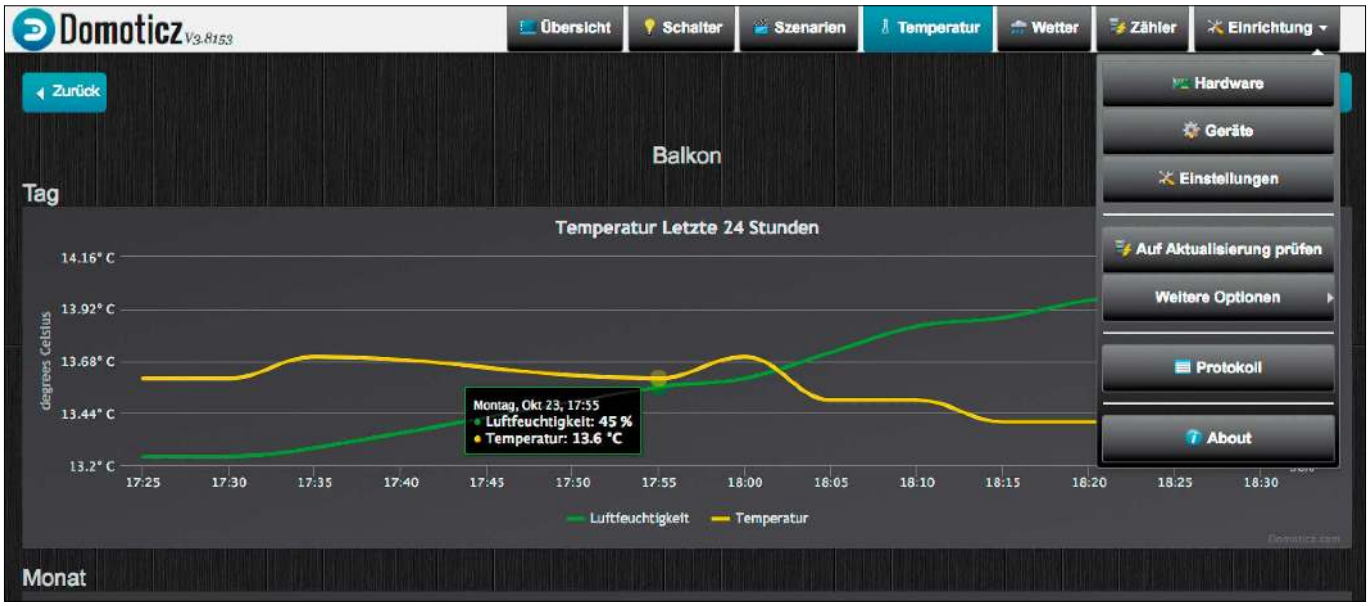
TV Tower

Remake des DOS-Spieleklassikers Mad TV
www.tvtower.org

Um das Management eines Trash-TV-Senders und der geschickten Sabotage von Konkurrenten geht es in der satirischen Wirtschaftssimulation TV Tower. Der Spieler muss Programmpläne, Werbeeinnahmen und Produktionskosten im Auge behalten. Die freie Neuauflage des DOS-Spiels Mad TV von 1991 liegt als ausführbare Binary vor. Unter 64-Bit-Linux sind noch einige Zusatzbibliotheken nötig, wie *https://github.com/TVTower/TVTower* auflistet.

Hektischer Alltag im TV-Tower: Damit die Werbeeinnahmen fließen und das Programm weiterläuft, gilt es, von Büro zu Büro zu eilen.

Hausautomatisierung mit Domoticz



Smart Home macht das Leben ein wenig komfortabler und sicherer – wenn das Problem mit den verschiedenen Gerätestandards nicht wäre. Eine Open-Source-Lösung zeigt sich als Steuerungszentrale überraschend vielseitig.

VON STEPHAN LAMPRECHT

Der Markt für Produkte wächst, die aus den eigenen vier Wänden ein Smart Home machen. Die Hersteller wittern Milliardenumsätze und so werden immer mehr Lösungen angeboten, etwa LED-Leuchten, die sich beim Verlassen der Wohnung ausschalten und das Licht wieder anschalten, wenn die Bewohner sich nähern. Und Thermostate an den Heizkörpern, die nach Zeitplänen arbeiten und die Außentemperatur berücksichtigen, sparen ordentlich Energie und Geld. Die Geräte lassen sich in aller Regel rasch in Betrieb nehmen und werden dann per App auf dem Smartphone oder Steuerungszentrale bedient. Leider kochen die Hersteller das sprichwörtlich eigene Süppchen. Was fehlt, sind Zentralen, mit denen sich herstellerübergreifend das Smart Home steuern lässt. Das hat etwa auch die Handelskette Conrad erkannt. Sie bietet seit einiger Zeit eine solche Zentrale direkt über das Internet an. Wer seine Geräte lieber nicht via Internet regeln will, kann sich mit der Software Domoticz eine individuelle Zentrale einrichten.

Dashboard für Raspberry, Linux, Windows und Mac

Domoticz ist ein quelloffener Lösungsbaustein für die Steuerung eines Smart Homes. Die Entwicklergemeinschaft bietet die Software für alle aktuellen Rechnerplattformen an. So hat der Nutzer die Wahl und größtmögliche Flexibilität, was den Unterbau seines Systems betrifft. Domoticz als Steuerungszentrale ist aus zwei Gründen sehr interessant: Zum einen ist die Zahl der unmittelbar unterstützten Geräte bereits beeindruckend. Zum anderen wurden auch Versionen entwickelt, die auf Ein-Platinencomputern mit ARM-Prozessoren laufen. Damit kann ein Raspberry Pi oder eine Odroid-Platine die Steuerungsaufgaben übernehmen. Deren Rechenkapazität reicht vollkommen aus.

Die Steuerung eines Smart Home besteht überwiegend aus – Warten. Einmal eingerichtet, wartet Domoticz den größten Teil des Tages passiv auf das Eintreten von Ereignissen, um erst dann ein Gerät anzusteuern. Und natürlich sind die Kleinstcomputer nicht hörbar und arbeiten energieeffizient. Deswegen soll in diesem Beispiel ein Raspberry genutzt werden. Unterschiede zu den anderen Hardwareplattformen ergeben sich aber nur für die Installation der Software. Die Hinweise zur Einrichtung sind auf alle Geräte übertragbar.

Das brauchen Sie für die Steuerungszentrale

Neben dem Raspberry brauchen Sie wahrscheinlich noch einiges aus dem Elektronikmarkt, um Ihre Geräte steuern zu können. Denn die Steuerungszentrale muss mit den externen Sensoren kommunizieren. Hier liegt ein mehr oder weniger weites Feld vor Ihnen. Kompatible Bausteine, die auf die WLAN-Struktur aufsetzen und deren Bridge entweder direkt oder per Switch mit Ihrem Router verbunden ist, sprechen Sie mit Domoticz unmittelbar an. Die Bridge wird dabei weiterhin gebraucht. Domoticz greift auf diesen Baustein zu, da in der Firmware der Bridge die Kommandos zur Steuerung hinterlegt sind.

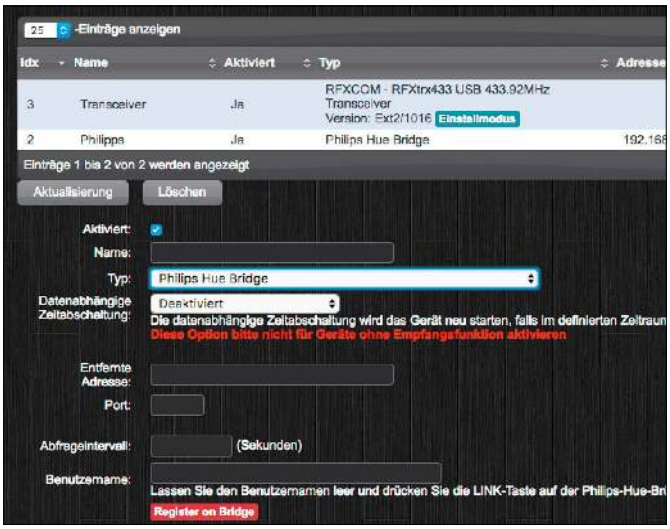
Wetterstationen oder per Fernbedienung steuerbare Steckdosen arbeiten dagegen in aller Regel per Funk auf der Frequenz 433 MHz. Auf dieses Funknetz kann der Raspberry mit Bordmitteln nicht zugreifen. Sie brauchen dazu ein Modul, das auf der Frequenz sowohl senden als auch empfangen kann, was dann gern zum Kunstwort Transceiver zusammengefasst wird. Sie sparen sich Arbeit und Mühe, wenn Sie vor der Anschaffung im Wiki der Entwickler nachschauen und ein dort ausdrücklich erwähntes Gerät anschaffen (*https://www.domoticz.com/wiki/*). Zwischen 70 und 100 Euro müssen Sie je nach Modell für die Anschaffung rechnen. Eventuelle bereits vorhandene Steuerungen für solche Funklösungen können aber teilweise auch per USB-Kabel an den Raspberry angeschlossen werden.

Domoticz auf Raspberry installieren

Um das System auf einem Raspberry zu installieren, öffnen Sie das Terminal und geben dort den Befehl

```
sudo curl -L install.domoticz.com | sudo bash
```

ein. Dazu muss der Rechner mit dem Internet verbunden sein. Alle notwendigen Komponenten werden heruntergeladen und an die korrekte Stelle kopiert. Ähnlich unkompliziert verläuft die Einrichtung auch auf anderen Platinen. Sind alle Elemente erfolgreich übertragen worden, können Sie bereits mit dem System arbeiten. Sie brauchen dazu lediglich einen Browser. Domoticz erreichen Sie im lokalen Netzwerk über *http://[IP des-Raspberry]:8080*. Wenn Sie direkt auf dem Raspberry selbst zugreifen wollen, nutzen Sie die Adresse „http://127.0.0.1:8080“. Um eine deutschsprachige Menüführung zu erhalten, klicken Sie in der oberen Navigation auf „Setup“ und danach „Settings“. Auf der nächsten Bildschirmseite schalten Sie dann die Sprache unter „Language“ um und aktivieren die Option mit „Apply Settings“.



Die Einrichtung der Geräte in Domoticz unterscheidet sich je nach Typ. Bei einer Hue Bridge muss binnen eines kurzen Zeitintervalls der Schalter der Bridge gedrückt werden.

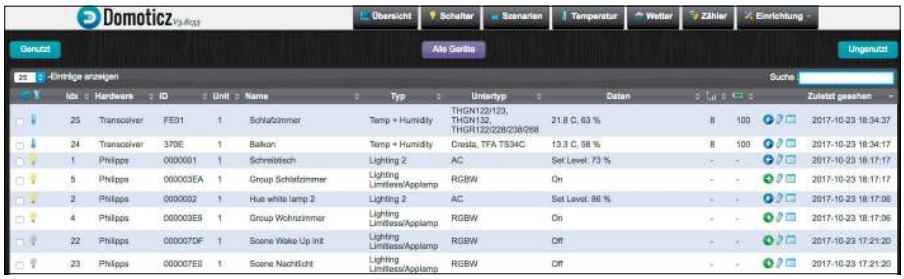
Damit der Transceiver die Signale der Sender empfängt, muss in den Einstelloptionen definiert werden, auf welche Hersteller das Gerät achten soll.

Ein (W-)LAN-Gerät einbinden

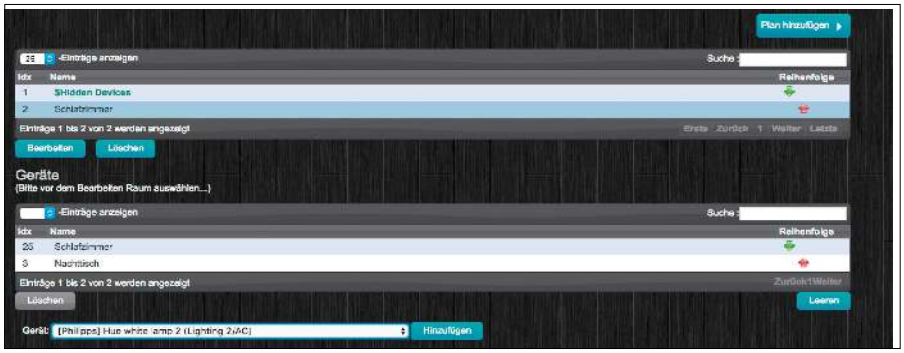
Domoticz kann eine Vielzahl unterschiedlicher Geräte und Sensoren verwalten. Darunter sind auch Bausteine, die nicht jeder Anwender mit einem Smart Home assoziieren würde, so etwa ein Kodi-Medienserver. Um ein Gerät einzubinden, das sich im gleichen lokalen Netz befindet, benötigen Sie dessen IP-Adresse – eine Information, die Sie am schnellsten im Router gewinnen. Beim Lichtsystem von Osram oder Philips müssen Sie noch nicht einmal die IP-Adresse der Bridge kennen: Hier gehen Sie auf „Einrichtung“ und danach „Hardware“ und unter „Typ“ wählen Sie dann „Philips Hue Bridge“ aus. Jetzt müssen Sie den Schalter der Bridge drücken und dann binnen 30 Sekunden auf der Oberfläche von Domoticz unter „Register on Bridge“ mit einem Klick auf „Hinzufügen“ den Sensor übernehmen. Jeder Hardwarebaustein kann eine unterschiedlich große Zahl an Geräten steuern. So kontrolliert die Bridge von Philips die daran angemeldeten Leuchten. Diese Geräte müssen Sie nach der Anmeldung einer Hardware ebenfalls dem System hinzufügen. Nutzen Sie dazu „Einrichtung -> Geräte“. In der Liste der von den Controllern erkannten Geräte klicken Sie auf den kleinen grünen Pfeil bei einem Eintrag.

Einen Funksensor einrichten

Um Steckdosen, Lichtschalter oder Wettersensoren bedienen zu können, die über das 433-MHz-Band kommunizieren, brauchen Sie einen passenden Transceiver. Problemlos lassen sich die Modelle des Herstellers Rfxcom mit dem Raspberry Pi und Domoticz betreiben. Basiert das Hostsystem auf Windows, müssen zuerst die passenden Treiber für den Baustein installiert werden. Auf dem Raspberry ist das nicht notwendig. Hier genügt es, den Transceiver mit der USB-Schnittstelle des Raspberry zu verbinden. Über „Einrichtung -> Hardware“ wählen Sie unter „Typ“ das gewünschte Modell aus. Unter „Serieller Port“ sollte die Auswahl von „/dev/tty/USB0“ ausreichen. Mit „Hinzufügen“ übernehmen Sie dann das Gerät in die Konfiguration.



Einmal im Netzwerk gefundene Geräte müssen im System hinterlegt werden. Ein Klick auf die Pfeile genügt, um ein Gerät aufzunehmen oder aus der Konfiguration zu entfernen.



Raumpläne bündeln die verbauten Schalter und Geräte und machen das System übersichtlich. Auf der Startseite wechseln Sie mit einem Listenfeld zwischen Räumen.

Szenarien bündeln den Schaltzustand von verschiedenen Geräten und Sensoren. Diese werden aus der Liste der dem System bekannten Geräte zusammengestellt.

Das genügt in diesem Fall aber noch nicht, um auch die entsprechenden Geräte ansteuern zu können. Das Frequenzband 433 MHz verwendet eine ganze Reihe von unterschiedlichen Geräten. Klicken Sie in der Liste der Hardware neben dem Transceiver auf den Schalter „Einstellmodus“. Auf der nachfolgenden Seite aktivieren Sie die Namen der Hersteller, von denen Sie Sensoren oder Schalter im Einsatz haben. Wenn Sie sich unsicher sind oder der Hersteller Ihres Sensors nicht aufgeführt ist, aktivieren Sie einfach alle und klicken auf „SetMode“. Wechseln Sie danach über „Einrichtung, Geräte“ in die Liste der verfügbaren Sensoren.

Falls die Liste zu lang sein sollte, klicken Sie auf „Alle Geräte“ und geben anschließend in das Feld „Suche“ den Filter „rfx“ ein, um nur die Elemente anzusehen, die vom Transceiver von Rfxcom angesteuert werden. Mit einem Kick auf den kleinen Pfeil nehmen Sie es in die Liste bekannter Sensoren auf.

Gruppen und Räume definieren

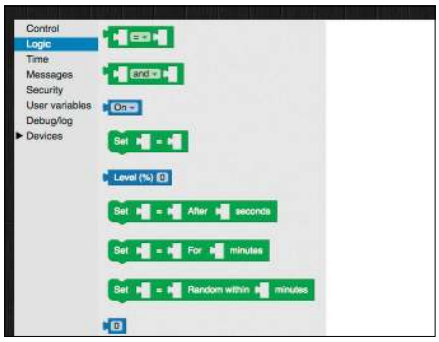
Die Software Domoticz hat natürlich keine Informationen darüber, wo sich die Sensoren und Schalter tatsächlich befinden. Damit Sie sich später schneller zurechtfinden, arbeiten Sie am besten mit Gruppen oder Räumen. Ihnen besonders wichtige Schalter ordnen Sie auf Wunsch gleich auf der Übersichtsseite an. Dazu müssen Sie bei einem Element nur auf den kleinen Pfeil in seinem Container klicken. Damit landet der Eintrag direkt auf der Startseite. Um Geräte zu einem Raum zusammenzufassen, wechseln Sie nach „Einrichtung“ zu „Weitere Optionen“ und anschließend zu „Pläne“. Dort entscheiden Sie sich für „Raumplan“. Auf der nachfolgenden Seite klicken Sie auf „Plan hinzufügen“ und vergeben anschließend einen Namen für den Raum. Jetzt fügen Sie über das Listenfeld am unteren Rand der Seite die Geräte hinzu, die zu diesem Raum gehören. Durch das Anlegen von Räumen haben Sie die Option, direkt auf der Übersichtsseite alle so eingerichteten Schalter eines Raumes aufzurufen. Dazu wechseln Sie über das Listenfeld am oberen Rand einfach zum gewünschten Raum.

Szenarien für Schalten und Walten

Haben Sie alle Geräte, Schalter, Sensoren und Regler eingerichtet, haben Sie mit Domoticz eine komplette Schaltzentrale. Sie brauchen nicht erst weitere Apps zu starten. Spendieren Sie dem Raspberry beispielsweise ein eigenes Display mit der Homepage von Domoticz als Startseite, macht das Kontrollzentrum auch optisch eine gute Figur. Und mit jedem beliebigen Browser aus dem Heimnetz greifen Sie ebenfalls darauf zu.

Die Macher bieten mit dem Service „MyDomoticz“ (*https://my.domoticz.com/mydomoticz/login*) sogar einen externen Zugriff per Internet auf das System an.

Mehr Komfort erreichen Sie auf jeden Fall durch das Anlegen von Szenarien. Ein „Szenario“ meint hier eine Kombination aus verschiedenen Schaltzuständen, die gleichzeitig erfolgen – so etwa das Einschalten aller Lampen in einem bestimmten Raum oder das Absenken der Raumtemperatur in allen Räumen. Ein Szenario fasst also verschiedene Geräte zusammen. Den höchsten Grad an Automatisierung erreichen Sie, wenn ein Szenario auf ein bestimmtes Ereignis reagiert. Ein Ereignis kann singulär



Blockly „programmiert“ Ereignisse: Die Kunst besteht darin, die richtigen Module zu finden, um das gewünschte Ereignis zu formulieren.

Es ist Samstag und die Temperatur auf dem Balkon ist höher als 12 Grad: Dies sind hier die Bedingungen in Blockly, um das Szenario „Abends“ auszulösen.

Im Register „Schalter“ erreichen Sie alle Schalter oder die eines bestimmten Raumes. Wird der kleine „Favoriten“-Stern aktiviert, landet das betreffende Element auf der Startseite.

sein, zum Beispiel das Erreichen einer bestimmten Uhrzeit oder eines Messwerts in einem Sensor. Ein Szenario kann aber auch verschiedene Zustände kombinieren: So ist das Einschalten der Heizung bei einem bestimmten Schwellwert vielleicht nur dann sinnvoll, wenn es sich nicht um ein Wochenende handelt. Der eigenen Fantasie sind hier keine Grenzen gesetzt.

Ein Szenario ist mit wenigen Schritten angelegt. Dazu wechseln Sie in das gleichnamige Register in der Hauptnavigation und wählen dort „Neues Szenario“. Vergeben Sie einen möglichst sprechenden Namen, und drücken Sie im nachfolgenden Dialog abschließend erneut auf „Neues Szenario“. Damit wird ein Eintrag in der Übersicht der Szenarien angelegt. Mit einem Klick auf das Schaltersymbol in dem Eintrag aktivieren Sie ein Szenario bei Bedarf jederzeit manuell. Szenarien können Sie auf drei Weisen aktivieren:

1. Sie klicken manuell auf einen Eintrag.
2. Sie steuern ein Szenario über ein Ereignis an.
3. Das Szenario läuft automatisch nach einem Zeitplan ab. Dazu dient der Schalter „Zeitschaltuhr“, der sich in dem Container eines Szenarios befindet.

Bevor es aber soweit ist, müssen Sie das Szenario erst mit Leben füllen. Dazu klicken Sie in dem Container auf „Bearbeiten“. Der Dialog ist sehr übersichtlich. Im unteren Bereich finden Sie über das Listenfeld alle Geräte, die im System eingerichtet worden sind. Darüber legen Sie deren Schaltzustand und eventuelle weitere Parameter fest. Mit „Hinzufügen“ übernehmen Sie dann den Eintrag in das Szenario. Domoticz bietet weitreichende Scripting-Möglichkeiten. Mit deren Hilfe lassen sich unter Umständen auch Geräte ansteuern, die sich über die Oberfläche nicht direkt schalten lassen. Das ist häufig dann der Fall, wenn ein Schalter einen ähnlichen Mechanismus verwendet wie ein direkt unterstütztes Element. Hier hilft dann ein Blick in das Wiki der Entwickler. In einem Szenario können Sie auf Wunsch auch ein Script aktivieren. Mit einem abschließenden Klick auf „Speichern“ legen Sie das Szenario endgültig an.

Automatisierung mit Ereignissen

Ereignisse werden bei Domoticz mit „Blockly“ zusammengestellt. In Form von Puzzlesteinen setzen Sie die verschiedenen Elemente zusammen. Diese optische Rückmeldung verhindert, dass Sie falsche oder unpassende Kombinationen zusammenstellen. Rufen Sie „Einrichtung -> Weitere Optionen“ auf und wählen Sie dann „Ereignisse“. Damit gelangen Sie zu einer noch leeren Arbeitsfläche. Die Bausteine sind in verschiedenen Kategorien zusammengefasst. Unter „Control“. können Sie auf das Zutreffen einer oder mehrere Bedingungen prüfen. Diese landen als Puzzle in den Bereich „If“. Treffen die Bedingungen zu, wollen Sie dann eines oder mehrere Kommandos ausführen. Die passenden Teile landen dann unter „Do“.

Wie bei einer umfangreichen Recherche im Internet besteht die Kunst darin, sich zu überlegen, welche Werte verglichen werden sollen, damit die entscheidende Bedingung eintritt. So werden oft auch Bausteine aus dem Bereich „Logic“ gebraucht, etwa dann, wenn mehrere Parameter miteinander verglichen werden sollen. Typisch ist etwa das Problem, auf Tageszeiten und zugleich auf gemessene Temperaturen logisch zu reagieren. Dazu gibt es hier Bausteine, die logische Operatoren (AND und OR) verbindet.

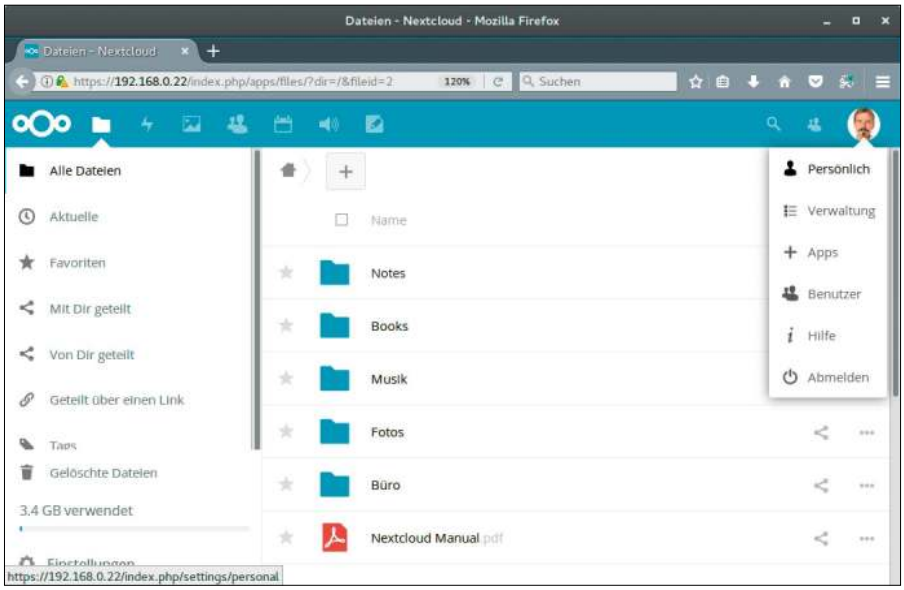
Ein einfaches Beispiel, um die Logik hinter den Bausteinen transparent zu machen: Sie wollen eine Schaltung ausführen, wenn die Temperatur eines Sensors einen kritischen Wert unterschreitet. Dann ziehen Sie zunächst unter „Control“ den Block „If“ auf die Fläche. Unter „Logic“ bewegen Sie den Baustein mit dem Gleichheitszeichen auf die Arbeitsfläche und setzen ihn an der richtigen Stelle in das Puzzle ein. Sofern Temperatursensoren zu Ihrem System gehören, finden Sie diese Sensoren in der Kategorie „Temperature“. Bewegen Sie ein Element auf die Zeichenfläche und setzen Sie ihn als Puzzlestein in die offene Verbindung des Bausteins mit dem Gleichheitszeichen. Im Bereich „Logic“ finden Sie auch ein Steinchen, das numerische Werte aufnehmen kann. Dieses setzen Sie dann noch an die freie Stelle ein. Danach können Sie den Schwellwert festlegen.

Jetzt müssen Sie noch festlegen, was passieren soll, wenn die Bedingung zutrifft („Do“). Hier haben Sie verschiedene Optionen. Szenarien aktivieren Sie über deren Einträge im Abschnitt „Scenes“. Unter „Messages“ stehen einige Funktionen zur Auswahl, die beim Eintreten einer Bedingung Mails oder SMS versenden. Das ist bei der Überwachung von Räumen ganz praktisch. Beginnen Sie am besten mit einfachen Aufgabenstellungen und arbeiten Sie sich dann langsam in die Tiefen der Möglichkeiten ein. Domoticz bietet umfassende Möglichkeiten, um auch komplexe Automatisierungsansprüche zu realisieren. ■

Raspbian mit Nextcloud inklusive

Die Nextcloud ist ein komplexer Server für Freigaben, Fotogalerien, Medienwiedergabe, Datensynchronisierung, Kollaboration, Kontakte, Kalender. Da ist es hochwillkommen, dass Images für den Raspberry die Nextcloud-Installation schon mitbringen.

VON HERMANN APFELBÖCK



Eine Nextcloud-Instanz lässt sich theoretisch auf wenige wesentliche Basisfunktionen reduzieren und damit relativ einfach verwalten. Die Regel ist das aber nicht, und je nach Menge der aktiven Appmodule und berechtigten Nutzer wird die Administration schnell komplex. Bevor man überhaupt in der Nextcloud-Oberfläche produktiv loslegen kann, steht erst noch die Installation und Einrichtung einer kompletten Lamp-Umgebung an (Linux, Apache, My SQL, PHP). Doch dank der Popularität der Nextcloud ist diese Basis für Neueinsteiger auf dem Raspberry Pi mittlerweile ganz schnell gelegt: Es gibt Images für den Raspberry Pi 3, die eine sofort lauffähige Nextcloud enthalten.

Download, Image schreiben und starten

Nach unserer Kenntnis gibt es zwei Raspberry-Images mit integrierter Nextcloud – das eine auf Basis von Ubuntu Core, das zweite auf Basis von Raspbian. Da wir mit dem Ubuntu-Image von nextcloud.com (*https://goo.gl/WssTtS*) erhebliche technische Probleme hatten, geht es nachfolgend ausschließlich um das Projekt Nextcloudpi von *https://ownyourbits.com* (*https://goo.gl/MYGUX7*), das Nextcloud 12 auf einem Raspbian 9 („Stretch“) mitbringt. Downloadlinks des 800-MB-Images finden Sie auf besagter Website unter „Get it“, darunter auch technische Hilfestellungen zur weiteren Vorgehensweise.

Achtung – der Server blockt bei häufigerem Zugriff offenbar die IP für einige Zeit, um sich vor Überlastung zu schützen. Nehmen Sie gegebenenfalls eine Wartefrist in Kauf, nach der Sie wieder zugreifen dürfen. Das Image ist „tar.bz2“-gepackt und mit der Archivverwaltung unter Linux schnell ausgepackt. Unter Windows eignet sich dafür das Open-Source-Programm 7-Zip (*www.7-zip.org*), das nicht zum Standardrepertoire gehört und im Bedarfsfall erst nachinstalliert werden muss. Resultat ist eine Imagedatei „NextCloudPi-[version].img“. Diese schreiben Sie dann mit den üblichen Mitteln auf eine SD-Karte – mit Etcher (*https://etcher.io*) unter allen Betriebssystemen, mit dd unter Linux oder Mac-OS

```
sudo dd if=NextCloudPi-[…].img of=/dev/sd[x] bs=1M
```

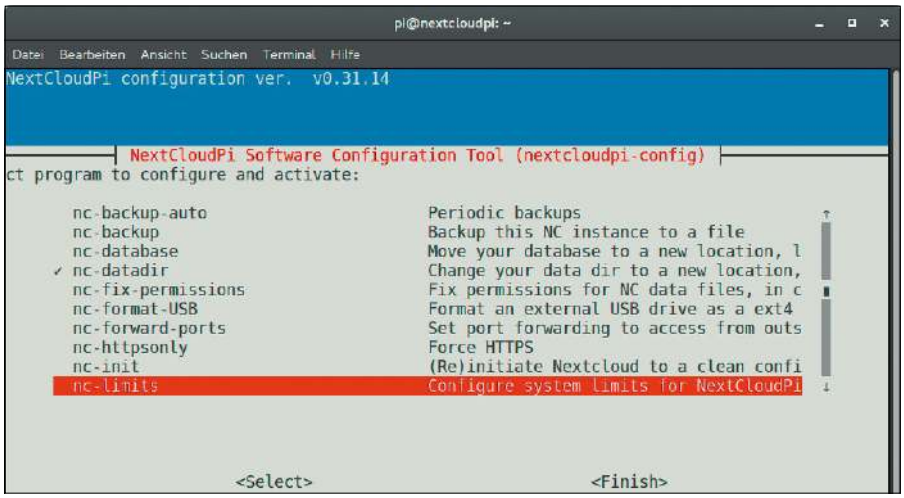
oder auch mit dem Win 32 Disk Imager unter Windows (auf Heft-DVD).

Im Prinzip ist die Nextcloud nach Einlegen der SD-Karte in den Raspberry und Booten desselben sofort konfigurationsbereit. Sie benötigen nur die IP-Adresse des Raspberry im Adressfeld eines beliebigen Browsers im lokalen Netz. Ein zuverlässiger Weg, die IP-Adresse herauszufinden, ist immer der Gang zum Router. Dort sollte ein neues Gerät mit dem Namen „nextcloudpi“ auftauchen. Am besten legen Sie an dieser Stelle gleich eine feststehende IP für den Nextcloud-Server fest. Hatte der Raspberry schon vorher eine Serverrolle mit fester IP, so bleibt diese weiterbestehen, weil sich an der maßgeblichen Hardwareadresse des Netzadapters durch das neue Raspbian-Nextcloud-System nichts ändert.

Die Log-in-Varianten zum Server

1. Die Nextcloud-Oberfläche ist, wie beschrieben, sofort nach dem ersten Start

Auf SD-Karte kopieren, Raspberry booten und sofort auf der Nextcloud anmelden: Ein Raspian-Image inklusive Nextcloud erspart das Installieren der Lamp-Umgebung.



Punkt „0 NextCloudPi Configuration“ in raspi-config: Die hier angebotenen Nextcloud-Einstellungen entsprechen exakt dem, was auch im Browser mit „[IP-Adresse]:4443“ erreichbar ist.

unter der lokalen IP-Adresse erreichbar. Der Browser wird eine „unsichere“ Verbindung monieren, was Sie je nach Browser über „Erweitert“ oder „Details“ im lokalen Netz ignorieren bzw. als Ausnahme erlauben können. Die Anmeldung erfolgt mit dem Konto „admin“ und dem vorgegebenen Standardpasswort „ownyourbits“.

2. Bei einem direkten Log-in am System mit Monitor und Tastatur benötigen Sie als Zugangsdaten das Standardsystemkonto „pi“ mit dem Standardpasswort „raspberry“. Eine kleine Hürde auf deutscher Tastatur ist hier die Tatsache, dass Sie als Passwort „raspberrz“ eingeben müssen, da das System von der englischen Tastaturbelegung ausgeht.

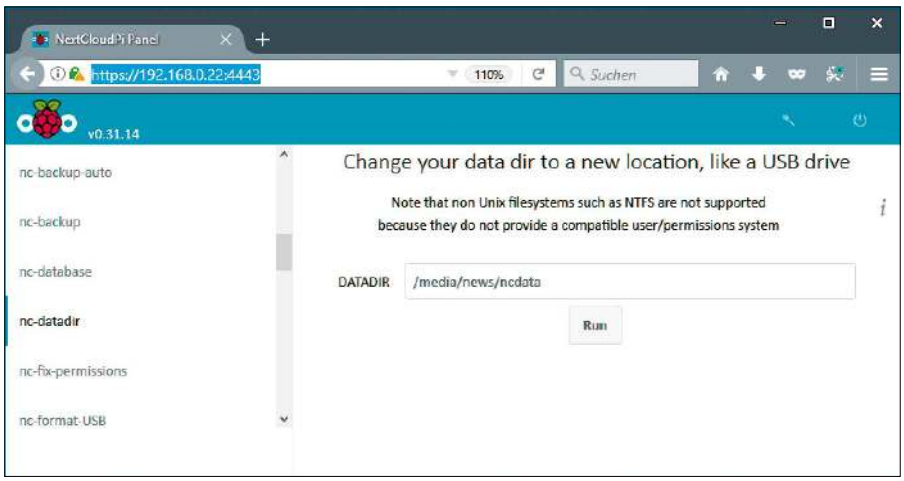
Zumindest für die allererste Basiskonfiguration empfiehlt sich der lokale Zugang mit Monitor und Tastatur – aus mehreren Gründen. Jüngeres Raspbian hat nämlich ab Start aus Sicherheitsgründen den SSH-Server zunächst deaktiviert, und in der Nextcloud-Oberfläche ist dies nicht zu korrigieren. Starten Sie daher nach lokaler Anmeldung mit

```
sudo raspi-config
```

das Konfigurationstool. Unter Punkt 5 „Interfacing Options“ finden Sie als zweiten Eintrag „SSH“, das sich einfach durch Markieren und Eingabetaste dauerhaft einschalten lässt.

Schon einmal das Tool raspi-config vor sich, lassen sich hier die üblichen Standards erledigen: So ist unter Punkt 7 „Advanced Options“ das Ausdehnen des Dateisystems auf die gesamte SD-Karten-Kapazität zu empfehlen, ferner die Lokalisierung auf Deutsch, ein individuelles Passwort für den Standarduser „pi“ oder ein spezieller Hostname. Mit nun aktiviertem SSH ist das alles aber jederzeit auch über Netz nachzuholen. Der für die Nextcloud-Konfiguration entscheidende Punkt in raspi-config ist der allererste „0 NextCloudPi Configuration“. Hier können Sie per SSH oder direkt am Server exakt jene Einstellungen treffen, die auch über den nachfolgenden Punkt 3 per Browser erreichbar sind.

3. Auf Port 4443 der Raspberry-IP – also insgesamt etwa mit einer Adresse wie „https://192.168.178.10:4443“ – ist zusätzlich das NextCloudPi Panel erreichbar. Es handelt sich um das grafische Konfigurations-Front-End für die zentrale Datei „config.php“, das mit den Authentifizierungsdaten eines Systemkontos betreten werden kann – also mit „pi“ und Kennwort „raspberry“, solange nichts anderes definiert ist. Inhaltlich entspricht das exakt dem Punkt „0 NextCloudPi Configuration“ im Tool raspi-config. Hier können Sie fundamentale Einstellungen festlegen, so etwa das „nc-datadir“ verlegen auf eine große USB-Festplatte (mit Ext4-Formatierung) unter „/media“, ferner die Dyn-DNS-Adresse festlegen („freeDNS“) oder die maximale Dateigröße der Uploads bestimmen („nc-limits“). Notfalls lässt sich hier auch eine komplette Installation auf die Standards zurücksetzen („ncinit“). Die knappen und englischsprachigen Erläuterungen in dieser Schaltzentrale sollten äußerst sorgfältig gelesen werden. Immerhin ist die Webvariante etwas gesprächiger als das spartanische raspi-config. Wer sich bei einer Einstellung nicht sicher ist, sollte sich genau informieren und im Zweifel besser Abstand nehmen. Wer weiß, was er tut, hat hier aber ein sehr komfortables Werkzeug an der Hand. ■



Konfigurationszentrale über Port 4443: Hier gibt es analog zu raspi-config hier fundamentale Direktiven für die Nextcloud-Instanz, die Vorsicht und Know-how erfordern.

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 Verbindungsaufbau 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

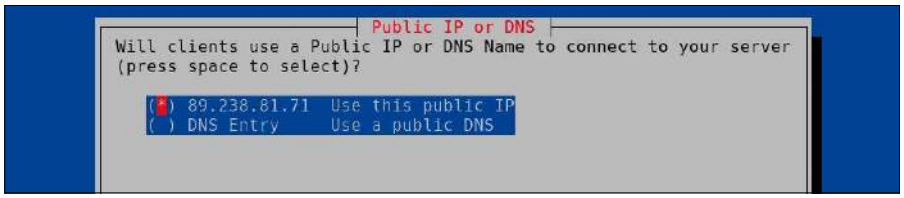
```
wget -O pivpn https://install.
 pivpn.io
```

einfach das Script in das aktuelle Verzeichnis herunter und starten es von dort:

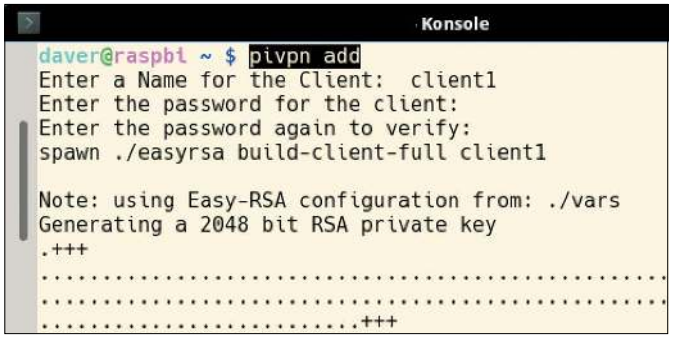
```
bash pivpn
```

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.
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.

Schlüssellänge auswählen: 2048 Bit gelten als sicher. Auf dem Raspberry Pi wird es eine Weile dauern, bis der ARM-Prozessor den Schlüssel erzeugt hat.



Öffentliche Adresse: Ein Server mit fester IP im Internet ist über die 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.

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. Der Clou: 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. ■

Den Raspberry Pi sicherer machen

Dank Energieeffizienz und flüsterleisem Betrieb kommt der Raspberry Pi in vielen IoT-Projekten zum Einsatz. Damit wird er zwangsläufig ein Angriffsziel für Hacker und Botnetze. Deswegen sollten Sie den kleinen Rechner besser absichern.

Wenn Sie den Port für den SSH-Zugang verändern, schlagen Sie Portscannern ein Schnippchen und verbessern die Sicherheit des Systems.

VON STEPHAN LAMPRECHT

Viele Kleinstcomputer sind permanent online, um ihre Aufgaben als VPN-Gateway oder in der Hausautomation zu erfüllen. Damit sind sie permanent Angriffsversuchen ausgesetzt. Daran ist grundsätzlich nichts zu ändern, jedoch kann man es möglichen Angreifern so schwer wie irgend möglich machen.

Risiko Nummer 1 – der Standardnutzer

Am einfachsten hat es jeder Angreifer mit einem System, das mit voreingestellten Standards aktiv ist. Beginnen Sie daher damit, dem Standardnutzer „pi“ ein neues Passwort zu geben. Es sollte möglichst lang sein und auch Sonderzeichen enthalten. Dazu genügt es, ein Terminal zu öffnen und dort

```
passwd
```

einzugeben. Legen Sie danach zusätzlich einen Benutzer mit individuellem Namen an, mit dem Sie dann standardmäßig arbeiten. Folgender Befehl

```
sudo useradd -m [benutzer] -G sudo
```

fügt einen neuen Benutzer hinzu, der auch zur Gruppe „sudo“ gehört. Damit kann er auch root-Kommandos ausführen. Auch diesem Benutzer weisen Sie nach *sudo passwd [benutzer]* ein sicheres Passwort zu. Und wenn Sie schon dabei sind, ist es auch eine gute Idee, ein neues Rootpasswort zu vergeben. Dazu lautet das Kommando

```
sudo passwd root
```

Da Sie jetzt ein neues Konto besitzen, das auch alle Aufgaben mit root-Rechten ausführen kann, können Sie den Standardbenutzer „pi“ deaktivieren. Dieses Konto, von dessen Existenz jeder Angreifer ausgeht, hat nach

```
sudo passwd --lock pi
```

erst einmal gar keine Rechte mehr.

Das System aktuell halten

Wie bei jedem modernen Computer gilt auch für den Raspberry, dass er möglichst aktuell gehalten werden muss. Sie sollten also in regelmäßigen Abständen die installierten Pakete aktualisieren und die Distribution frisch halten.

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

Wenn Sie es besonders bequem haben wollen, recherchieren Sie im Internet einmal nach dem Programm „unattended-upgrades“. Das kann dann sogar als Cronjob im System hinterlegt werden und wird in regelmäßigen Abständen automatisiert ausgeführt. Dann brauchen Sie sich um die Updates nicht mehr manuell kümmern.

SSH-Fernzugriff absichern

Der Zugriff per SSH ist sicherlich eines der mächtigsten Werkzeuge im täglichen Umgang mit einem Raspberry. Denn erst dieser Fernzugriff ermöglicht es, alle Systemfunktionen zu erreichen, ohne Tastatur oder Monitor an den Kleinstcomputer anschließen zu müssen. Deswegen dürften die meisten Anwender diesen Zugang im Rahmen ihrer Projekte einsetzen. Das wissen aber auch die Angreifer, und deswegen sollten Sie sich um die Absicherung von SSH kümmern.

Da Sie einen Benutzer angelegt haben, der sich auch root-Recht verschaffen kann, ist

es nicht mehr notwendig, dass es eine Anmeldung des Kontos root auf diesem Weg gibt. Versuche, sich als root anzumelden, können Sie leicht unterbinden. Öffnen Sie dazu mit einem Editor die entsprechende Konfigurationsdatei:

```
sudo nano /etc/ssh/sshd_config
```

Suchen Sie dort nach dem Eintrag „PermitRootLogin“ und setzen Sie dort den Wert auf „no“.

In aller Regel arbeiten automatisierte Angriffe mit Portscans: Dabei werden wahlweise Datenpakete an Systeme gesendet und geprüft, ob bestimmte Ports geöffnet sind. Wie Sie sicherlich wissen, sind für die verschiedenen Protokolle Standardports definiert. Bei SSH ist dies Port 22 – ein Port, den angreifende Portscans in jedem Fall abfragen. Ein System kann aber jederzeit so eingerichtet werden, dass ein Dienst wie SSH auf einem anderen Port angeboten wird. Dies ändern Sie beim Raspberry ebenfalls in der Konfigurationsdatei „sshd_config“. Sie müssen allerdings etwas aufpassen, denn die Portnummer darf nicht von einer anderen Anwendung oder einem Dienst belegt werden. Suchen Sie in der Datei nach der Zeile „Port“. Statt der 22 vergeben Sie dort einen anderen Wert (theoretisch 65 536 Möglichkeiten). Verändern Sie also zum Beispiel den Wert auf „22078“. Mit Strg-X und der anschließenden Bestätigung zum Speichern verlassen Sie den Editor wieder.

Änderungen der Konfigurationsdatei „sshd_config“ werden erst nach einem Neustart des Dienstes mit *sudo service ssh restart* wirksam.

Gescheiterte Log-in-Versuche limitieren

Die meisten Hackerangriffe versuchen ganz plump, eine Anmeldung mit Standardkontonamen und zufälligen Passwörtern auszuprobieren. Das System antwortet auf die Fehlversuche natürlich mit einer Fehlermeldung. Ein Softwarepaket kann solche gescheiterten Versuche nach einer bestimmten Anzahl einfach verbieten:

```
sudo apt-get install fail2ban
```

Nun kann es natürlich immer einmal zu Fehlversuchen beim Anmelden kommen. Einmal die Umstelltaste festgestellt und das an sich korrekte Passwort landet als Fehlangabe auf der anderen Seite. Über die Konfigurationsdatei des Programms sollten Sie daher festlegen, wie viele Fehlversuche Sie zulassen wollen und welche Sperre das zur Folge hat. Dazu laden Sie mit

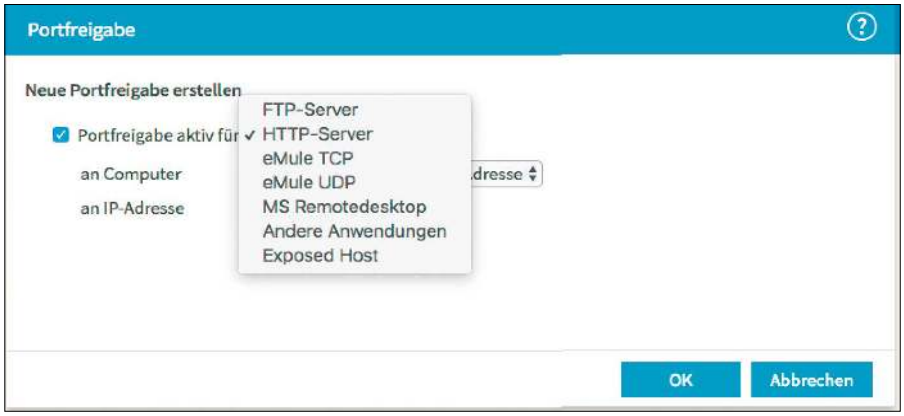
```
sudo nano /etc/fail2ban/jail.conf
```

die maßgebliche Datei in den Editor. Die Zahl der erlaubten Fehlversuche definieren Sie mit „Maxretry“. „Findtime“ bestimmt, innerhalb welcher Zeitspanne die Fehlversuche erfolgen müssen, damit diese gezählt werden. Die Dauer der Blockade für die zugreifende IP definiert die Variable „bantime“. Die Angaben erfolgen in beiden Fällen in Sekunden.

```
sla@raspi:~$ sudo useradd -m huenutzer -G sudo
[sudo] Passwort für sla:
sla@raspi:~$ sudo passwd huenutzer
Geben Sie ein neues UNIX-Passwort ein:
Geben Sie das neue UNIX-Passwort erneut ein:
passwd: Passwort erfolgreich geändert
sla@raspi:~$
```

Legen Sie ein neues Konto an, das auch root-Rechte besitzt: Vermeiden Sie auf dem Raspberry Pi den Standard-Nutzer „pi“, den jeder Angreifer kennt.

Konfigurationsdatei von fail2ban: Hier legen Sie fest, innerhalb welcher Zeitspanne wie viele Fehlversuche erfolgen dürfen, bevor die IP gesperrt wird.



Portfreigaben im Router: Die Regel lautet „genau und nur das, was unbedingt nötig ist“. Vergessen Sie nicht, Portfreigaben wieder aufzuheben, sobald sie nicht mehr benötigt werden.

Firewall installieren und aktivieren

Ist der Rechner mehr oder weniger die gesamte Zeit online, dann sollte darauf eine Firewall aktiviert sein. Am besten arbeitet diese nach dem Prinzip, nur den Datenverkehr durchzulassen, der explizit erlaubt worden ist. Sie finden im nachfolgenden Artikel (S. 94) Anleitungen für eine besonders einfach konfigurierbare Firewall. Versuchen Sie ferner, sofern es die eingesetzte Software zulässt, ähnlich wie beim SSH-Zugang den Port der Anwendung zu verändern. Ein System, das auf Anfragen an den Standardports nicht reagiert, ist für automatisierte Angriffe zu kompliziert.

Router nicht vergessen: Die Absicherung eines Raspberry-Systems ist die eine Sache, die andere ist die des Routers. Die meisten Modelle sind herstellerseitig mit einer zuverlässigen Firewall geschützt. Weichen Sie diesen Schutz nach Möglichkeit nicht durch unnötige Portfreigaben auf. Der Router sollte unter den Portfreigaben (Fritzbox: „Internet -> Freigaben -> Portfreigaben“) nur genau die Freigabe(n) anzeigen, die ein Dienst wie SSH oder ein Raspi-Projekt erfordert. ■

Der Raspberry Pi als Firewall

Über den Sinn einer Desktop-Firewall lässt sich trefflich streiten. Ist ein Rechner aber mehr oder weniger ständig online, kann eine Firewall vor unliebsamen Überraschungen schützen. Ein Raspberry Pi lässt sich mit wenig Aufwand als Firewall verwenden.

Foto: © valerybrozhinsky – Fotolia.com

VON STEPHAN LAMPRECHT

Wer ab und an im Internet surft und seine Büroarbeit erledigt, ist durch den Router und dessen integrierte Firewall gut geschützt. Das sieht etwas anders aus, wenn ein Heimnetz etwa im Zusammenhang mit IoT-Projekten ständig mit dem Internet verbunden ist und durch Portfreigaben auch eingehende Verbindungen akzeptieren muss. Damit ist das an sich abgeschottete Heimnetz nach außen geöffnet und hier erhöht eine Firewall die Sicherheit spürbar. Einmal installiert, kann der Raspberry dann gleich auch als sicherer Access Point für WLAN eingesetzt werden.

Die „Uncomplicated Firewall“ einrichten

Beim Thema Netzwerk sind Einsteiger unter Linux rasch überfordert. Das Betriebssystem ist zwar perfekt für alle Arbeiten im Netz, aber viele Werkzeuge für die Einrichtung sind nur über die Kommandozeile zu erreichen oder es müssen mit root-Recht kryptisch erscheinende Konfigurationsdateien bearbeitet werden. Diese sind zwar dokumentiert, aber die Kommentare bleiben für jeden undurchsichtig, der nicht über tiefergehende Kenntnisse zum Aufbau von Protokollen verfügt. Deutlich einfacher zu verstehen ist das Programm „Uncomplicated Firewall“ (ufw), das eigentlich keine Firewall ist, sondern dem Nutzer nur dabei hilft, die eingebauten Systemfunktionen leichter zu konfigurieren. Das Paket installieren Sie mit

```
sudo apt-get install ufw
```

und damit ist auch gleich eine Reihe von Firewallregeln eingerichtet.

Eine Firewall geht davon aus, dass nur Verbindungen zugelassen werden, die ausdrücklich in einer Regel erlaubt sind. Das kann schlimmstenfalls dazu führen, dass man sich selbst vom System aussperrt. Daher sollten Sie unbedingt die Verbindung per SSH zulassen, um sich von einem externen System auf dem Raspberry anmelden zu können. Das erledigen Sie mit dem folgenden Befehl:

```
sudo ufw allow ssh
```

Das System sollte anschließend mit einem „Rules updated“ antworten. Jetzt können Sie die Firewall starten. Mit

```
sudo ufw enable
```

wird das Regelwerk aktiviert. Sie werden darauf hingewiesen, dass das Kommando eine möglicherweise bestehende SSH-Verbindung beeinträchtigen könnte. Mit „y“ fahren Sie fort. Damit sind die Regeln ab sofort gültig. Mit dem Zusatz „disable“ wird die Firewall wieder deaktiviert.

Wie schon bei der Einrichtung des SSH-Zugangs können Sie bei der Freigabe anderer Übertragungswege auch einfach die entsprechenden Protokolle verwenden. Soll der Raspberry als Webserver arbeiten, erlauben Sie den Datenverkehr wie folgt:

```
sudo ufw allow http
```

Arbeitet der Computer als Dateiserver, schalten Sie SMB (CIFS) frei (*sudo ufw allow cifs*). Daneben gibt es eine ganze Reihe von Anwendungen, die spezielle Regeln erfordern, die der Befehl

```
sudo ufw app list
```

auflistet. Mit „allow“ werden die Regeln für die Anwendung dann aktiviert. Auf Dateiebene landen alle diese Regeln unter „/etc/ufw“. Diese Dateien sollten Sie aber nicht direkt mit einem Editor bearbeiten.

Raspberry als sichere Bridge

Mit der Firewall schützt der Raspberry sich selbst und die darauf laufenden Anwendungen. Das ist eine gute Basis, um das Netzwerk insgesamt sicherer zu machen. Dazu lässt sich der Raspberry etwa zu einer

WLAN-Bridge einrichten. Damit können sich kabellose Clients auf dem Raspberry anmelden. Das angeschlossene Ethernet-Kabel stellt die Verbindung zum Heimnetz und Router her. Bei einer Bridge werden das Standardgateway (also die Verbindung zum Internet etwa über den DSL-Anschluss) und ein bereits vorhandener DHCP-Server genutzt. Einen DHCP-Server wird der DSL-Router anbieten. Der Betrieb zweier DHCP-Server im gleichen Netz erfordert komplexe Einstellungen. Wer sich in die Tiefen der Netzwerktechnik einarbeiten möchte, findet im Internet zahlreiche Hinweise zur Einrichtung des Raspberry als Access Point. Bei einer Bridge kümmert sich der Router um die Zuteilung der IP-Adressen an die Clients. Die Einrichtung des Systems ist an sich nicht schwierig. Je nach Modell muss erst geprüft werden, ob der Chipsatz den AP-Modus beherrscht:

```
iw list | grep AP
```

Werden mehrere Zeilen mit „AP“ angezeigt, kann es weitergehen. Wird das Kommando nicht ausgeführt, müssen die Tools erst mit *sudo apt-get install iw* installiert werden. Damit die Brücke funktioniert, ist es wichtig, dass der DHCP Client Daemon aktiviert ist. Das prüfen Sie einfach mit *service dhcpd status*. Außerdem müssen der Ethernet-Adapter und der WLAN-Adapter vorhanden sein und funktionieren. „ip l“ zeigt die gewünschten Informationen an. Die dabei ausgegebenen Informationen zur IP-Konfiguration spielen dabei keine Rolle.

Für die Bridge werden zwei Komponenten benötigt. Einerseits ein Daemon, der die Aufgabe als Access Point übernimmt, zum anderen die Software für die Netzwerkbrücke. Der Host Access Point Daemon („hostapd“) ist ein Programm, das WLAN-Funktionen verschlüsselt anbietet und sich um die Authentifizierung der Clients kümmert. Die Brücke selbst stellt das Paket „bridge-utils“ bereit. Die beiden Pakete werden erst einmal installiert:

```
sudo apt-get install hostapd
 bridge-utils
```

Danach kann die Konfiguration des Access Points beginnen. Dazu editieren Sie eine Konfigurationsdatei mit

```
sudo nano /etc/hostapd/hostapd.
 conf
```

Diese sollte bisher leer sein. Hier müssen einige Zeilen eingetragen werden, die Sie der nebenstehenden Abbildung entnehmen können. Unter „SSID“ vergeben Sie einen Namen für das Netzwerk, das die Clients nutzen können. Außerdem müssen Sie den Kanal (Channel) einstellen. Hier kann Ihnen die Analyse mit der Fritzbox zeigen, auf welchen Kanälen am wenigsten andere Netze aus der Nähe funken. Diesen Kanal nutzen Sie dann. Schließlich sollten Sie ein sicheres Passwort für die Verschlüsselung setzen. Der Block für die Verschlüsselung sieht dann so aus:

```
wpa=2
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
wpa_passphrase=PaSSw0rt
```

Falls in Ihrem Netz bereits ein Access Point vorhanden ist, darf das Funknetz des Raspberry durchaus den gleichen Namen tragen. Die Clients suchen sich dann den Zugangspunkt aus, der den besseren Empfang bietet. Zum Testen der Bridge sollten Sie aber einen abweichenden Namen geben. In der Konfigurationsdatei finden Sie einen Eintrag für den Treiber des WLAN-Adapters. Der ist in der abgebildeten Beispieldatei auskommentiert, da hostapd eigentlich automatisch den korrekten Treiber laden sollte. Lediglich wenn es zu keiner Verbindung kommt, können Sie hier manuelle Änderungen vornehmen. Mit Strg-O speichern Sie die „hostapd.conf“. Da die Datei das WLAN-Passwort im Klartext enthält, werden die Rechte besser so beschränkt, dass nur root Leserecht hat.

```
sudo chmod 600 /etc/hostapd/
 hostapd.conf
```

Jetzt verbleibt noch, die IP-Konfiguration der Interfaces einzurichten und die Details der Brücke einzurichten. Dazu editieren Sie mittels des Kommandos

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

die dafür zuständige Datei. Jetzt noch das System neu starten. Mit

```
hostapd -dd /etc/hostapd/hostapd.
 conf
```

können Sie danach überprüfen, ob Ihr neues WLAN online geht. ■

```
 GNU nano 2.8.6          Datei: /etc/hostapd/hostapd.conf          Verändert

# Bridge-Betrieb
bridge=br0

# Schnittstelle und Treiber
interface=wlan0
#driver=nl80211

# WLAN-Konfiguration
ssid=WLANbridge
channel=1
hw_mode=g
wmm_enabled=1
country_code=DE
ieee80211d=1
ignore_broadcast_ssid=0
auth_algs=1

# WLAN-Verschlüsselung
wpa=2
```

In der „hostapd.conf“ sollten Sie mindestens diese Zeilen anlegen. Die SSID und den Kanal (Channel) passen Sie an Ihre Wünsche und Gegebenheiten an.

```
 GNU nano 2.8.6          Datei: /etc/network/interfaces          Verändert

# Localhost
auto lo
iface lo inet loopback
# Ethernet
auto eth0
allow-hotplug eth0
iface eth0 inet manual
# WLAN
auto wlan0
allow-hotplug wlan0
iface wlan0 inet manual
wireless-power off
# Netzwerkbrücke
auto br0
```

Konfigurationsdatei „interfaces“: Hier konfigurieren Sie die Brücke. Für andere Konfigurationen mit statischen IP-Adressen oder einem vollständigen Access Point finden Sie viele Beispiele im Web.

Machen Sie mehr aus Ihrer Diskstation!

Mit seinen NAS-Modellen und dem Linux-basierten Betriebssystem DSM ist dem Hersteller Synology ein großer Wurf gelungen. Die Geräte leisten viel und mit externer Software sind sie noch vielseitiger einsetzbar.

VON STEPHAN LAMPRECHT

Während Leistungshungrige, Puristen und Bastler ein NAS eher mit einer Platine und kostenfreien Open-Source-Lösungen zusammenbauen, stellt sich diese Frage für die meisten Anwender wahrscheinlich gar nicht. Kommerzielle NAS-Lösungen bieten stimmige Hardware und machen es auch Laien einfach, das System aufzusetzen. Der Einbau der Festplatten ist ohne technisches Geschick im Handumdrehen erledigt und danach genügt ein Knopfdruck, um die Vorzüge des NAS zu nutzen. Das durchdachte und komfortable Betriebssystem DSM hat gewichtigen Anteil daran, dass die Modelle des Hersteller Synology besonders beliebt sind.

„Adieu iCloud“! „Goodbye Google!“

Viele Anwender haben inzwischen Skrupel, ihre Adressen und Telefonnummern einfach bei einem Anbieter in der Cloud zu speichern. Die meisten tun es trotzdem, schließlich scheint für den Smartphone-Zugriff kein Weg an iCloud oder Google vorbeizuführen. Zwar bietet etwa Owncloud/Nextcloud auch eine Möglichkeit für die Synchronisation solcher Daten, aber die diese mächtige Lösung einzurichten, erscheint dann doch etwas zu aufwendig, um ein paar Adressen aktuell zu halten.

Eigentlich unverständlich, dass Synology so wenig Werbung für seine eingebaute Kontakt- und Kalenderverwaltung macht. Damit Sie außerhalb Ihres heimischen Netzwerks Adressen und Termine synchronisieren können, müssen Sie hinter einem DSL-Anschluss mit einem dynamischen DNS-Eintrag arbeiten. Das kann direkt unter der Oberfläche des Systems erledigt werden.

Die Einrichtung der Synchronisation ist nicht sonderlich schwierig. Infos dazu gibt’s unter *www.pcwelt.de/2080638*. Kontakte und Termine werden von getrennten Anwendungen verwaltet und synchronisiert.

Um Kontakte auszutauschen, installieren Sie aus dem Paketzentrum die Anwendung Card DAV Server. Nach der erfolgreichen Einrichtung finden Sie diese als eigene Anwendung, die direkt gestartet werden kann. Unter den Einstellungen sollten Sie den Zugang mittels HTTPS abschalten, sofern Sie auf der Synology kein Zertifikat abgelegt haben. Über die Einstellungen müssen Sie unter „Berechtigungen“ dann noch den angelegten Anwendern Zugriff auf den Server geben. Die Optionen des Servers sind selbsterklärend. Wenn Sie wollen, können Sie im zentralen Adressbuch nicht nur Kontakte manuell eingeben, sondern auch die Daten aus anderen Quellen importieren. In allen Anwendungen, die auf das Adressbuch zugreifen sollen, müssen Sie den Pfad dazu eingeben. Im lokalen Netzwerk ist das „http://IP-Adresse:8443/addressbooks/users/[BENUTZER]/addressbook/“. Beim Benutzernamen handelt es sich um den User auf der Synology. Nutzen Sie Dyn DNS oder einen ähnlichen Server, dann verwenden Sie den Domainnamen statt der IP-Adresse. Damit der Zugriff von außen klappt, muss der Port 8443 an Ihrem Router freigeschaltet sein.

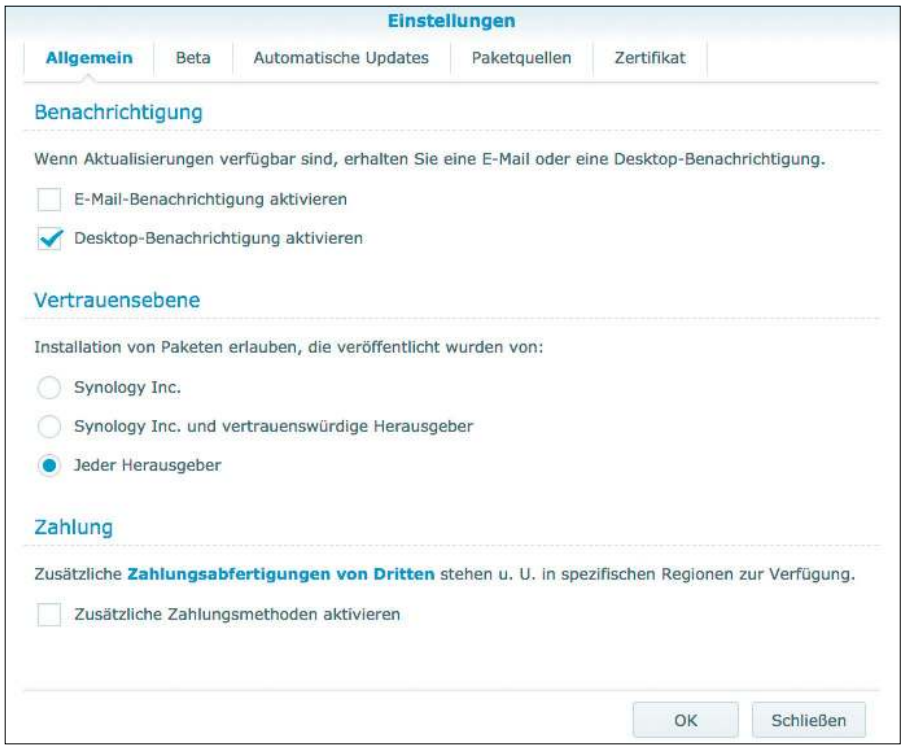
Die Verwaltung von Kalendern ist im Webdav-Server angelegt. Dieser wird ebenfalls über das Paketzentrum installiert und wird dann anschließend über die Systemsteuerung gestartet. Im Register „Kalender“ aktivieren Sie anschließend den Caldav-Dienst und unter „Kalenderliste“ legen Sie danach einen neuen Kalender an. Um auf den Kalender dann mit einer externen Anwendung zuzugreifen, benötigen Sie natürlich ebenfalls die URL. Diese setzt sich zusam-

men aus der IP-Adresse der Diskstation oder dem Namen der Domain und wird ergänzt um die Pfadangabe, die Sie aus der Liste der Kalender entnehmen können („Systemsteuerung -> WebDAV -> Kalenderliste anzeigen -> Ort“). Ein gültiger Eintrag könnte etwa „http://ip-adresse/web/Calendar/stephan/“ lauten. Aktuell gibt es im Internet auch noch Pakete des kleinen Baikal-Kalenders. Allerdings hat sich am Hauptprojekt bereits seit einiger Zeit nichts mehr getan und auf Github warten noch viele Nutzer auf Antworten auf ihre Bugreports, sodass wir von einer Installation derzeit eher abraten.

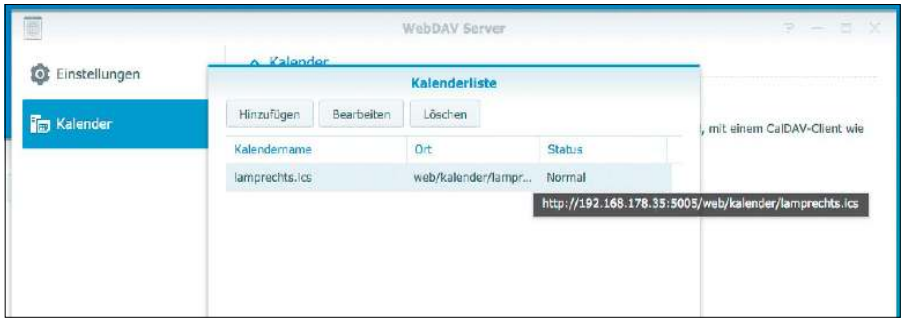
Plex auf der Synology installieren

Der Medienserver Plex hat sich in den vergangenen Jahren eine engagierte und treue Fangemeinde erobert. Auf der Synology ist dessen Installation nicht schwierig. Anders als die Software zur Synchronisation der Termine stammt Plex aber nicht aus den offiziellen Quellen. Um das Paket installieren zu können, müssen Sie erst die Einrichtung von Drittpaketen erlauben. Öffnen Sie dazu in der DSM-Oberfläche das Paketzentrum und klicken Sie dort auf „Einstellungen -> Allgemein -> Vertrauensebene -> Jeder Herausgeber“.

Je nach Modell hat Synology in seinen Geräten unterschiedliche Prozessoren verbaut. Wenn Sie sich nicht sicher sind, welcher Typ in ihrem NAS werkelt, besuchen Sie das Wiki unter *http://www.synology-wiki.de/index.php/Welchen_Prozessortyp_besitzt_mein_System%3F*. Dies ist wichtig für den nächsten Schritt: Auf der Downloadseite von Plex *https://www.plex.tv/de/downloads/* können Sie zwar sofort Synology als Plattform einstellen, müssen dann aber das zum Prozessor passende Paket wählen. Im DSM-Paketzentrum finden Sie dann den Schalter „Manuelle Installation“. Wählen Sie diese Option und navigieren Sie zum heruntergeladenen Paket von Plex. Mit „Weiter“ startet die Installation. Ist die Einrichtung auf dem Gerät erfolgreich verlaufen, erhält Plex einen eigenen Eintrag unter den Anwendungen und kann gestartet werden. Jetzt steht einer individuellen Einrichtung Ihres Servers nichts mehr im Wege.



Voraussetzung für das Mediencenter Plex: Um Pakete aus fremden Quellen installieren zu können, müssen Sie in der NAS-Konfiguration die Sicherheitsstufe herunterschalten.



Um einen Kalender in externen Anwendungen einzubinden, benötigen Sie die genaue URL. Diese finden Sie über den Webdav-Server heraus.

Synology als Ziel für Linux-Backups

Am Thema Backup unter Linux haben sich in den vergangenen Jahren einige Entwickler versucht. Meist handelt es sich lediglich um grafische Aufsätze für Werkzeuge wie tar und rsync. Rsync ist der Klassiker, um Daten extern zu kopieren und zu sichern. Die Synology kann dabei als Ziel für ein Backup über das Netz dienen. Dazu müssen Sie rsync unter DSM aber erst einmal einschalten. Rufen Sie die Systemsteuerung auf und gehen Sie unter „Dateidienste“ zum Register „rsync“. Klicken Sie dort auf „rsync-Dienst aktivieren“.

Anschließend wählen Sie den Schalter „rsync-Konto bearbeiten“, um Konten anzulegen, die den Service einsetzen dürfen. Dazu vergeben Sie einen Benutzernamen und ein Passwort. Damit wird es möglich, dass auch Nutzer, die kein eigenes Konto auf der Diskstation besitzen, den Dienst zur Datenübertragung einsetzen können. Die Datensicherung selbst ist dann nicht mehr schwer. Allerdings bietet rsync so viele Optionen, dass es sinnvoll ist, sich einmal die Manpages dazu anzusehen. Der Basissyntax sieht dabei so aus:

```
rsync -av [Quelle] [Ziel]
```

Damit die Daten vom Linux-System auf der Synology landen, könnten Sie das NAS-Backupverzeichnis unter Linux mounten. Es geht aber auch ohne Mounten:

```
rsync -av /home/ [benutzer]@[NAS-
  IP]::[Zielordner]
```

Diese spezielle Syntax sichert das Home-Verzeichnis des aktuellen Nutzers ohne Umwege auf dem Synology-NAS. ■

Sagen Sie uns Ihre Meinung – und gewinnen Sie!

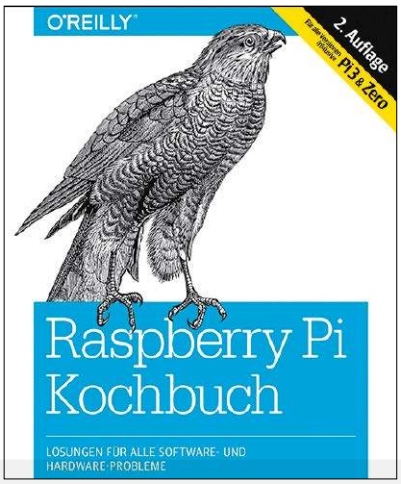
Wir möchten Linux-Hefte machen, die ganz Ihren Bedürfnissen und Interessen entsprechen. Dabei können Sie uns helfen! Füllen Sie einfach unseren Fragebogen im Internet aus. Das Beantworten der Fragen dauert nur rund zehn Minuten.

Unter allen Teilnehmern verlosen wir 3 Exemplare:

Raspberry-Pi-Kochbuch

- **Lösungen für alle Software- und Hardware-Probleme**
- **Für alle Versionen inklusive Pi 3 & Zero**

Die zweite Ausgabe dieses beliebten Kochbuchs bietet mehr als 240 Hands-on-Rezepte für den Betrieb dieses kleinen Low-Cost-Computers mit Linux, für die Programmierung des Pi mit Python und für die Anbindung von Sensoren, Motoren und anderer Hardware, einschließlich Arduino und das Internet der Dinge.
Power-Maker und Autor Simon Monk vermittelt grundlegendes Know-how, das Ihnen hilft, auch neue Technologien und Entwicklungen zu verstehen und so mit dem Raspberry-Pi-Ökosystem mitzuwachsen.



Raspberry-Pi-Kochbuch
Autoren: Simon Monk, Peter Klicman (Übersetzung)
Verlag: O'Reilly, 2., aktualisierte und erweiterte Auflage Dezember 2016, 484 Seiten, Broschur
ISBN: 978-3-96009-033-5, 29,90 Euro

Aus dem Inhalt
- Richten Sie Ihren Raspberry Pi ein und verbinden Sie ihn mit dem Netz
- Arbeiten Sie mit seinem Linux-basierten Betriebssystem Raspbian
- Lernen Sie, den Pi mit Python zu programmieren
- Geben Sie Ihrem Pi „Augen" mit Computer Vision
- Steuern Sie Hardware über den GPIO-Anschluss
- Arbeiten Sie mit Schaltern, Tastaturen und anderen digitalen Eingaben
- Verwenden Sie Sensoren zur Messung von Temperatur, Licht und Entfernung
- Realisieren Sie auf verschiedenen Wegen eine Verbindung zu IoT-Geräten

PLUS: Gratisheft für alle Teilnehmer

SO FUNKTIONIERT'S:

Auf *www.pcwelt.de/lin* gelangen Sie direkt zu unserer Leserbefragung und nehmen automatisch an der Verlosung teil. Von der Verlosung ausgenommen sind Mitarbeiter des Verlags und deren Angehörige. Der Rechtsweg ist ausgeschlossen.
Einsendeschluss für das Gewinnspiel in LinuxWelt 1/2018 ist der 23.1.2018.
Datenschutz: Wenn Sie gewinnen, schicken wir Ihnen den Preis per Post zu. Deshalb fragen wir Sie auch nach Ihrer Adresse.
Datenschutzerklärung: Alle auf unserer Webseite erhobenen Daten werden entsprechend den Vorschriften des Bundesdatenschutzgesetzes (BDSG) und des Informations- und Telekommunikationsdienstegesetzes (IuTDG) behandelt. Eine Weitergabe der Daten an Dritte ohne ausdrückliche Einwilligung des Betroffenen erfolgt nicht. Weitere Infos finden Sie unter *www.pcwelt.de/datenschutz*
Jeder Teilnehmer bekommt als Dankeschön LinuxWelt Extra 4/2017 „Der große Linux-Guide" als PDF (ohne Datenträger). Sie finden den Link zum Download des Hefts am Ende der Leserbefragung.

PC-WELT

Sicher surfen im Internet

Sonderheft
für nur
4,90 €

Auf Schutz-DVD:
Das komplette
Sicherheits-Paket

Jetzt bestellen unter
www.pcwelt.de/internet 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 Schritt für Schritt für nur 4,90 €.

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

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

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

Desktop de luxe

Gnome bekommt diesmal mehr Aufmerksamkeit, denn der Umstieg Ubuntus auf diese Desktopumgebung katapultiert den Anteil Gnomes am Linux-Desktop weit nach vorn. Aber auch KDE Plasma 5 kommt mit seinen Feinheiten nicht zu kurz.

Komorebi: Animierter Hintergrund für Ubuntu

Smartphone und Tablets haben animierte Hintergrundbilder etabliert. Es dauerte nicht lange, bis das Konzept auf den Linux-Desktop portiert wurde. Das Programm Komorebi 2 bringt bewegte Bilder auf den Desktop von Ubuntu und Co. Erfreulicherweise schafft Komorebi 2 nicht nur die Voraussetzungen für Animationen, sondern liefert gleich ein paar Dauerschleifen zum Ausprobieren mit. Allerdings wird nicht jede Ubuntu-Variante unterstützt.

In Linux Mint beispielsweise funktioniert das Programm nicht und Ubuntu 17.10 mit Gnome-Desktop verlangt Nacharbeiten. Komorebi 2 wurde in Ubuntu 16.04 entwickelt und läuft am besten in dieser Distribution. Zudem gibt es nur für 64-Bit-Systeme ein Paket. Zur Installation liefert der Entwickler auf seiner Github-Webseite (*https://github.com/iabem97/komorebi/releases*) ein DEB-Paket zur Installation aus. Dessen Einrichtung mit Abhängigkeiten gelingt einfach mit apt in der Kommandozeile:

```
sudo apt install ./
  komorebi-2-64-bit.deb
```

Der Befehl installiert das lokale Paket aus dem aktuellen Verzeichnis heraus und ersetzt das Tool Gdebi. Falls bereits Ubuntu 17.10 zum Einsatz kommt, ist ein weiterer Schritt nötig: Das Kommando

```
sudo ln -s /usr/lib/
  x86_64-linux-gnu/
  libgtop-2.0.so.11 /usr/
  lib/x86_64-linux-gnu/
  libgtop-2.0.so.10
```

erstellt einen Link zu einer Systembibliothek, die das Programm unter einem bestimmten Dateinamen erwartet, die aber in Ubuntu 17.10 einen geänderten Namen erhalten hat. Danach ist Komorebi 2 über die Dash-Übersichtsseite startklar. Der erste Aufruf ersetzt den herkömmlichen Hintergrund und ein Rechtsklick auf den Desktop erlaubt mit „Change Wallpaper" die Auswahl einer der mitgelieferten Animationen. **-dw**

Bewegter Desktop: Komorebi 2 zaubert Video-Endlosschleifen auf den Desktophintergrund und bringt geschmackvolle Beispiele mit, die allerdings Rechenpower verlangen.

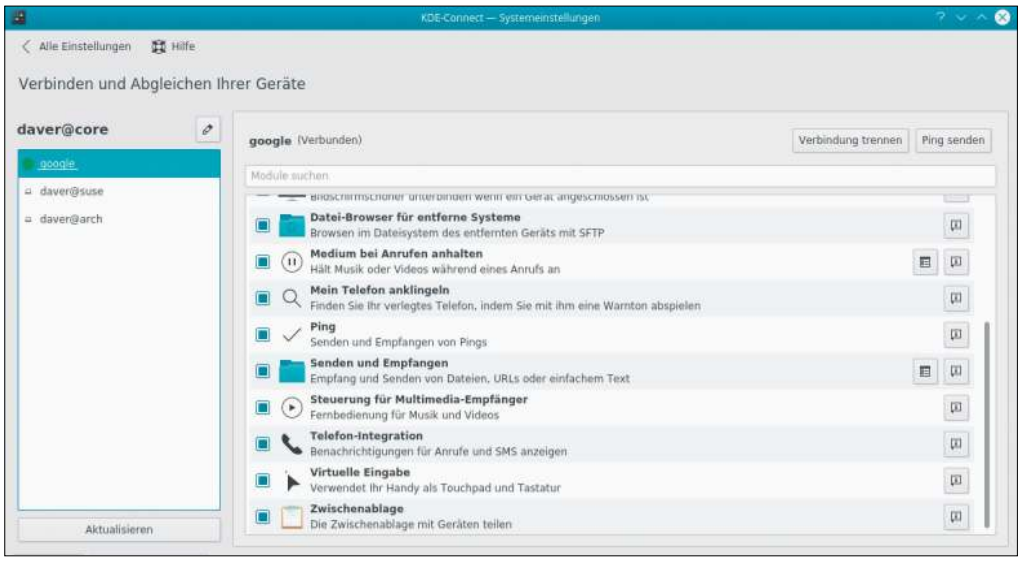
Spracheingabe: KDE Connect und Swiftkey Keyboard

Sprachsteuerung und Spracheingabe sind auf dem Linux-Desktop weit davon entfernt, brauchbar zu sein. Es gibt aber die Alternative, mit Hilfe der kostenlosen App Swiftkey Keyboard und dem Linux-Programm KDE-Connect das Smartphone zur Spracheingabe zu verwenden. Die beliebte Android-App Swiftkey hat hervorragende Spracherkennungsfähigkeiten für eine Reihe von Sprachen. Die App übersetzt die Stimmeingaben erstaunlich zuverlässig in Tastatureingaben, die wiederum KDE Connect an den Desktop und die aktive Anwendung weitergibt.

So funktioniert die Einrichtung: In Google Play steht unter *https://goo.gl/kivBp2* das Swiftkey Keyboard zur Installation auf dem Smartphone bereit. Zudem ist dort auch die App von KDE-Connect eine Voraussetzung, die unter *https://goo.gl/AgTnZY* in Google Play verfügbar ist. KDE Connect ist als Komponente der KDE-Arbeitsumgebung in den meisten Linux-Distributionen bereits vorinstalliert. Wenn nicht, findet es sich schnell über den Paketmanager zum Nachinstallieren.

Spracheingabe für Linux: Ist auf dem Smartphone zusätzlich noch das (kostenlose) Swiftkey Keyboard installiert, kann man Texte über KDE Connect diktieren.

Anschließend rufen Sie die KDE-Connect-App auf, gehen auf dem KDE-Desktop in die Sys-



KDE und Android kommen sich mit KDE-Connect näher: Über das Modul „Virtuelle Eingabe“ verwandelt sich das Smartphone in Tastatur und Maus.

temeinstellungen und dort auf das Symbol „KDE-Connect“. Damit sich Android und der PC gegenseitig sehen können, müssen beide im gleichen Netzwerk sein. Eine Verbindung können Sie sowohl von der Android-App als auch von der Einstellungsseite von KDE-Connect anfordern und bestätigen.

Sobald die Verbindung steht, legt man seitens KDE fest, welche Fernsteuerungsmodule aktiv sein sollen. Wichtig ist hier das Modul „Virtuelle Eingabe“ welches das Smartphone zur Tastatur macht. Jetzt funktioniert die Spracheingabe vom Smartphone aus: Dort starten Sie die App KDE Connect und wählen die Funktion „Ferneingabe“ aus.

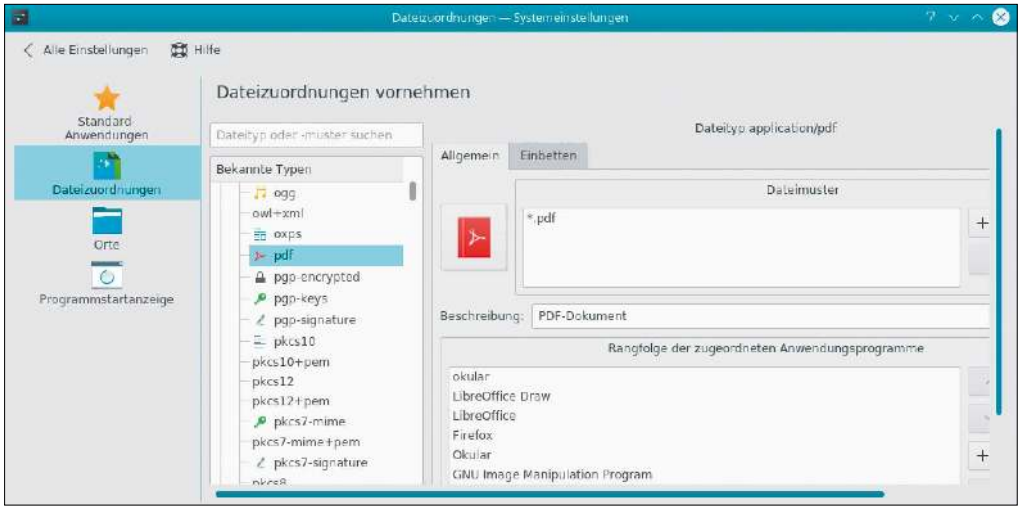
Statt der regulären Android-Bildschirmtastatur muss dort das Swiftkey Keyboard aktiviert werden. Nach einem Druck auf das kleine Mikrofonsymbol arbeitet Swiftkey mit Spracheingabe und sendet die Eingabe anschließend an KDE, wo sie in der aktuellen Anwendung als Text eingefügt wird. **-dw**

KDE Plasma 5: Standardprogramme für Dateitypen

Ein Doppelklick imn KDE-Dateimanager öffnet den jeweiligen Dateityp mit der registrierten Anwendung. Bei einem Rechtsklick auf eine Datei zeigen die Dateimanager in KDE die verfügbaren Anwendungen an, die für den jeweiligen Dateityp in Frage kommen. Es kommt vor, dass sich hier Programme mehrfach eingetragen haben, und nicht alle Einträge sind sinnvoll. Die Liste der Anwendungen, die für einen Dateityp in Frage kommen, ist in den Systemstellungen zum Bearbeiten hinterlegt. Dort gelangt man über den Punkt „Persönliche Informationen -> Anwendungen -> Dateizuordnungen“ zu einer Liste bekannter Dateitypen in einer Baumstruktur.

Nach dem Ausklappen eines Eintrags in der Liste, die nach Kategorien geordnet ist, zeigen sich nach einem Klick darauf auf der rechten Seite die eingetragenen Programme – im Feld „Rangfolge der zugeordneten Anwendungen“.

Mit den seitlichen Schaltflächen können Sie diese Einträge, die sich auch im Dateimanager zeigen, löschen, bearbeiten oder arrangieren. **-dw**



Dateitypen in KDE verwalten: Bei Dateitypen wie PDF versuchen gleich mehrere Programme, sich diesen Typ zu schnappen. Viele Zuordnungen sind doppelt oder auch wenig sinnvoll.

KDE Plasma 5: Aktive Feststelltasten anzeigen

Während gewöhnliche Tastaturen für den Desktop-PC mit LEDs anzeigen, ob gerade Numlock und Capslock eingeschaltet sind, sparen sich einige neuere Notebooks wie etwa der Lenovo Yoga diese sichtbare Anzeige. Und auch wenn es LEDs zur Statusanzeige gibt, so sind diese nicht immer im Blickfeld. Für KDE Plasma gibt es seit kurzem zur Anzeige von Capslock und Numlock ein Widget (Miniprogramm) für das Panel.

Dieses Widget ist jetzt im offiziellen KDE-Verzeichnis vorhanden und die Installation gelingt deshalb unabhängig von der verwendeten Linux-Distribution einfach über das Applet-Verzeichnis des neuen KDE: Nach einem Rechtsklick auf das KDE-Panel geht es dort auf „Kontrollleiste-Optionen“ und dann zu „Miniprogramme hinzufügen -> Neue Miniprogramme holen -> Neue Miniprogramme herunterladen“. Dieser Menüpunkt stellt eine Verbindung zum Onlineverzeichnis der KDE-Applets her und findet das Widget Key State schnell über das Feld „Suchen“. **-dw**

Status von Capslock und Numlock in KDE Plasma 5 anzeigen: Ein neues Widget zeigt im KDE-Panel an, wenn eine der Feststelltasten aktiviert ist.

Gnome und Blyr: Weichzeichner für den Desktop

Beim Einblenden des Unity-Dashs legt sich das Fenster der Übersichtsseite transparent über den Desktop und lässt den Hintergrund verschwimmen. Dieser Effekt lässt sich auch in Gnome mit dessen Anwendungsübersicht nachbilden. Die Gnome-Erweiterung „Blyr“ legt einen Weichzeichner beim Aufruf der „Aktivitäten“ in Gnome über den Hintergrund. Eigentlich wäre die Erweiterung einfach per Klick nach dem Besuch der Webseite *https://extensions.gnome.org/extension/1251/blyr* in Gnome installiert. Aber so simpel ist die Sache momentan nicht, weil Browser wie der Firefox keine Gnome-Shell-Integration mehr haben. Momentan zeigen die Browser beim Besuch der Seite die Meldung, dass es kein Browser-Add-on gibt. Auf bestehenden Gnome-Desktops verlangt deren Nachrüstung in Ubuntu und Fedora etwas Handarbeit:

1. Zuerst macht die Installation der angebotenen Firefox-Erweiterung von *https://extensions.gnome.org* oder auch von *https://addons.mozilla.org/en-US/firefox/addon/gnome-shell-integration* den Browser fit für Gnome.

2. Gnome selbst braucht auch noch die neue Komponente chrome-gnome-shell als Ergänzung. Die gibt es mittlerweile in Ubuntu 17.10 und Fedora 26 in den Standard-Paketquellen. Mit dem Kommando

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

ist es beispielsweise in Ubuntu installiert. Danach funktioniert nach einem Neustart des Firefox-Browsers die Aktivierung von Gnome-Erweiterungen wieder per Klick auf den angezeigten Kippschalter. **-dw**

Die rein kosmetische Gnome-Erweiterung Blyr“hinterlegt die Übersichtsseite „Aktivitäten“ mit einem schicken Weichzeichnereffekt im Stil von Unity.

Ubuntu-Anmeldung: Light DM mit Gnome verwenden

Die Anmeldung am Linux-System übernimmt auf der grafischen Oberfläche der Display-Manager, der den Willkommensbildschirm mit Eingabemaske sowie mit Menüs für die gewünschte Sprache und Desktopumgebung bietet. Ubuntu 17.10 arbeitet mit GDM, dem schlichten Display-Manager von Gnome 3.26. Noch gibt es aber einen Weg zurück zum gewohnten Anmeldebildschirm. Verschiedene Desktopumgebungen bringen ihren eigenen Display-Manager mit – nicht nur aus ästhetischen Gründen, sondern um die Programmbibliotheken der Desktopumgebung zu nutzen.

Der Display-Manager GDM kann wie Gnome bereits mit Wayland umgehen und ist nicht mehr auf Xorg angewiesen. Er folgt der Philosophie von Gnome, die in den letzten Jahren eine sehr schlichte Oberfläche bevorzugt hat.

Ubuntu 17.10 mit Gnome und dem Slick-Greeter von Ubuntu Mate: Der Display-Manager funktioniert als Ersatz für GDM prächtig, nutzt aber kein Wayland.

Obwohl Ubuntus eigener Display-Manager Light DM mit dem offiziellen Ende von Unity ebenfalls auf dem Abstellgleis gelandet ist, gibt es den ansprechenden Willkommensbildschirm noch. Denn Ubuntu Mate setzt ihn weiter in Form der Abspaltung Slick-Greeter ein und hat ihn in den Standard-Paketquellen platziert.

Dieser Willkommensbildschirm kann auch zusammen mit Gnome verwendet werden. Es gilt dabei nur zu beachten, dass die Bildschirmsperre in Gnome dann auch nicht mehr über GDM funktioniert, sondern über den Slick-Greeter.

Über das Optionsmenü oberhalb des Passwortfelds kann aber auch der Slick-Greeter eine Gnome-Session mit Xorg oder mit Wayland starten.

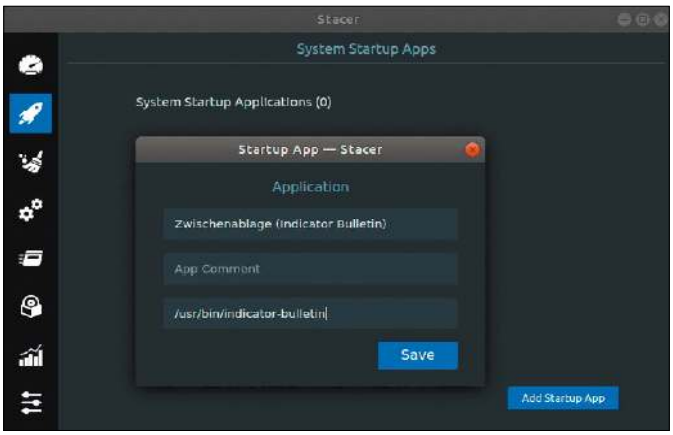
Zum Wechsel installiert man in einem Terminalfenster mit

```
sudo apt-get install
  slick-greeter
```

den alternativen Display-Manager. Nach der Installation wird das System noch abfragen, welcher Display-Manager ab jetzt zum Einsatz kommen soll. In diesem textbasierten Dialog wählen Sie „LightDM“ aus. Nach einem Neustart des Systems ist der Austausch komplett. Um später wieder zurück zu GDM zu wechseln, ist lediglich der Aufruf von

```
sudo dpkg-reconfigure gdm
```

nötig. **-dw**



Nützlicher Aspekt des Tools Stacer, da diese Funktion Gnome inzwischen fehlt: Die Verwaltung der Autostart-Einträge erlaubt die Ergänzung beliebiger Programme.

Gnome-Autostart: Einträge bearbeiten

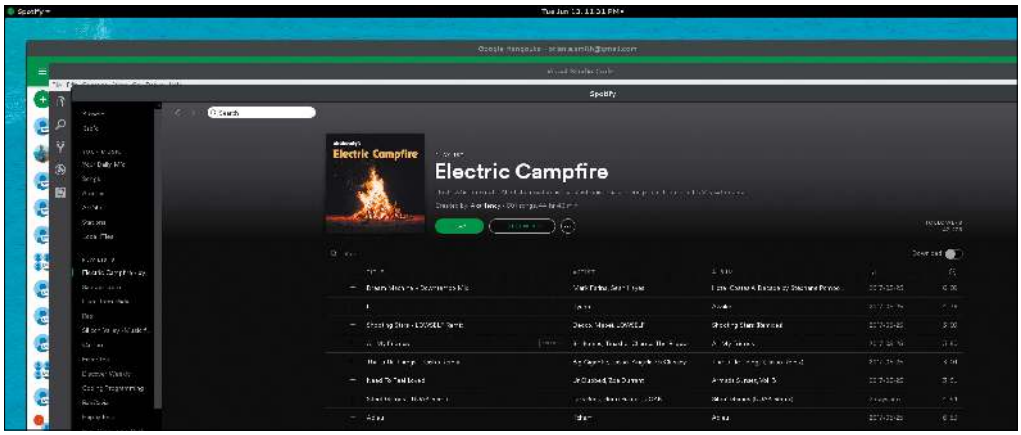
Systembastler haben es mit Gnome etwas schwerer, den Desktop an die eigenen Wünsche anzupassen, denn Gnome ist vergleichsweise unflexibel. So gibt es beispielsweise keine komfortable Möglichkeit, über die Gnome-Einstellungen oder über Gnome-Tweak selbst definierte Autostart-Einträge zu erzeugen. Ein anderes Tool kommt für diesen Zweck zu Hilfe: Das Programm „Stacer“ gehört zur Kategorie der Optimierungstools. Unbedarfte Anwender könnten mit diesem Tool viel kaputt-„optimieren“, aber zum Anlegen von Autostart-Einträgen ist Stacer uneingeschränkt zu empfehlen und eine tolle Ergänzung für Gnome 3.X. Stacer liegt für Ubuntu und Debian auf der Github-Webseite des Entwicklers als DEB-Paket vor und für Fedora als RPM-Paket (*https://github.com/oguzhaninan/Stacer/releases*) in jeweils 64 Bit. Nach der Installation über den jeweiligen Paketmanager, die auf der Projektwebseite kurz und bündig erklärt ist, ruft man das Tool auf, das unter dem Raketen-Icon einen Verwaltungsdialog für Autostart-Einträge zeigt. Mit wenigen Klicks ist hier ein neuer Eintrag erzeugt.

Die zugehörige Datei wird übrigens im Autostart-Ordner „~/.config/autostart“ angelegt und der eingetragene Befehl nach der Anmeldung am Desktop ausgeführt. **-dw**

Gnome-Programme: Kaskadierende Fenster

Gnome 3.x misst in seiner Benutzerführung Programmfenstern im Vollbildmodus große Bedeutung bei. Wenn mehrere Fenster geöffnet sind, wäre es trotzdem nützlich, alle Fenster auf dem Desktop übersichtlich übereinander anzuordnen. Auch für diese Funktion, an die sich vor allem Anwender von Windows 10 gewöhnt haben dürften, gibt es in Gnome eine Erweiterung.

Wenn Firefox bereits wieder darauf dressiert ist, Gnome-Shell-Erweiterungen ganz einfach im Browser zu aktivieren, so ist die Funktion schnell eingerichtet: Unter *https://extensions.gnome.org/extension/1240/cascade-windows* liegt Cascade Windows im offiziellen Erweiterungsverzeichnis bereit.



Stapelweise Fenster: Von Windows hat sich die Gnome-Erweiterung Cascade Windows die kaskadierende Anordnung der Programmfenster per Hotkey abgeschaut.

Übrigens gibt es für die kaskadierende Anordnung der Fenster auch einen Hotkey: Die Kombination aus Windows-Taste und C ordnet die Fenster stapelweise an. **-dw**

Geschickte Shell

Das Tool Maybe erlaubt das Ausprobieren von Befehlen nach dem Was-wäre-wenn-Prinzip. Eine nützliche Analyse mit Visualisierung der Startzeiten eines Linux-Systems ist in der Funktionsfülle des Init-Systems Systemd versteckt.

Netzwerk und IP-Nummer: Kurz und bündig

Das Tool ifconfig ist schon eine ganze Weile auf dem Abstellgleis und wird seit 2009 nicht mehr gepflegt. So ist es wenig überraschend, dass es in den neuen Ausgaben wichtiger Distributionen nicht mehr enthalten ist. So verzichten Debian 9 und Ubuntu 17.10 auf das Kommandozeilentool, an dessen Stelle der Befehl ip getreten ist.

Die Syntax des Befehls ip unterscheidet sich vom einfach gestrickten Tool ifconfig und kann mehr Informationen zur Netzwerkkonfiguration anzeigen, verlangt dazu aber die richtigen Parameter. Um die IP-Adressen aller Netzwerkschnittstellen in der Kommandozeile anzuzeigen, dient dieser Aufruf:

```
ip a
```

Dies listet alle Netzwerkschnittstellen auf und zeigt jeweils hinter „inet“ die lokale IPv4-Adresse und nach „inet6“ die IPv6-Adressen. Die erste Angabe zeigt die global gültige IPv6-Adresse des Systems und die zweite die IPv6-Adresse im lokalen Netzwerk. Das gibt es auch kürzer: Der Befehl

```
ip -4 a
```

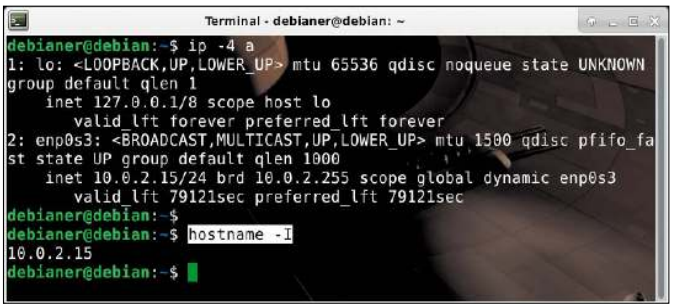
gibt nur IPv4-Adressen an und

```
ip -6 a
```

beschränkt sich allein auf die IPv6-Nummern. Trotzdem bleibt der Befehl vergleichsweise gesprächig. Eine kurze, bündige Alternative liefert das Kommando

```
hostname -I
```

ohne weitere Infos zur Netzwerkkonfiguration, wobei nur die IP-Nummern (IPv4 und IPv6) des Systems in einer Zeile aufgelistet werden.



Blick auf die Netzkonfiguration: Nicht nur auf Servern und Ein-Platinen-Computern ist die Kommandozeile die schnellste Methode zur Anzeige der IP-Adressen.

Hinweis: Wer ohne ifconfig nicht arbeiten will, kann in den verbreiteten Linux-Distributionen das Paket „net-tools“ über den jeweiligen Paketmanager nachinstallieren und dann noch eine Weile das altgewohnte Tool verwenden.

Da es mit modernen Linux-Kernels nicht mehr komplett kompatibel ist, muss man aber damit rechnen, dass dieses Paket bald gänzlich verschwinden wird. **-dw**

Systemanalyse mit Systemd: Bootzeit ermitteln

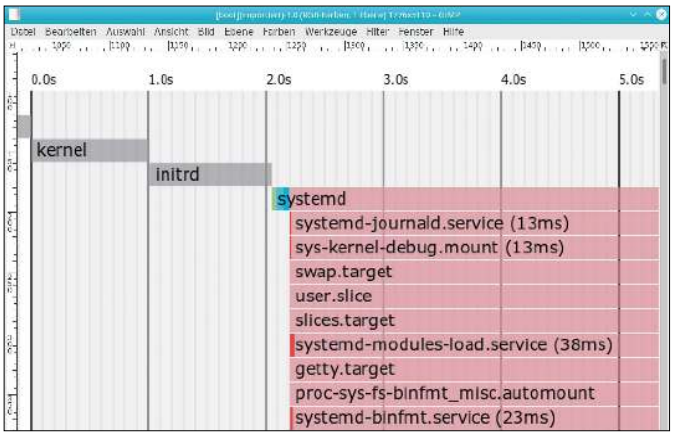
Der mittlerweile in allen gängigen Linux-Distributionen vorhandene Init-Dienst Systemd ist deutlich komplexer als das ältere System-V-Inits-System und wird dafür weiterhin kritisiert. Dafür bietet Systemd aber eine Reihe nützlicher Tools, um den Bootvorgang zu analysieren.

Systemd gibt recht komfortabel Auskunft darüber, wie lange der Bootvorgang vom Einschalten des Linux-Systems bis zur Anmeldung dauert. Nach dem Befehl

```
systemd-analyze
```

zeigt der Init-Dienst die Startzeit in Sekunden am Ende der ausgegebenen Zeile an und schlüsselt diese in ihre Bestandteile auf: Die Angabe vor „kernel“ (in Klammern) gibt die Ladezeit der systemnahen Komponenten an und „userspace“ die der Benutzerumgebung.

Ist das Linux-System unter Uefi installiert, zeigt das Analysetool auch an, wie viele Sekunden das Laden der Firmware, des Bootloaders und der initialen Ramdisk (initrd) dauerte. Noch ge-



Visualisierter Bootvorgang mit Systemd: Der Init-Prozess kann auf einem System dieses Diagramm erstellen, das den Startprozess grafisch darstellt.

nauer listet das Kommando

```
systemd-analyze blame
```

den Startvorgang auf. Es erstellt eine Liste der gestarteten Systemd-Dienste nach ihrer Startzeit absteigend sortiert. Nützlich ist diese Funktion, um Verzögerungen beim Start eines Desktopsystems auf den Grund zu gehen. Der häufige Check von Datenträgern durch den Dienst „systemd-fsck“ oder fehlgeschlagene mount-Aktionen für Laufwerke in der Konfigurationsdatei „/etc/fstab“ sind typische Bremsklötze.

Eine visuelle Darstellung des Bootvorgangs liefert dieses Kommando:

```
systemd-analyze plot > boot.svg
```

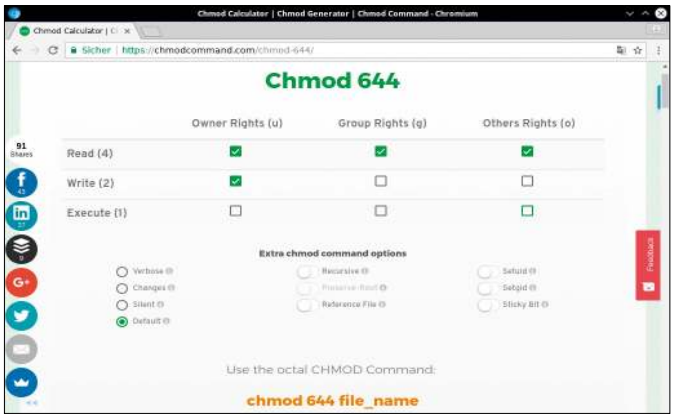
Hier entsteht ein Diagramm im SVG-Format, welches beispielsweise die Programme Libre Office Draw, Inkscape und Gimp öffnen können. Die X-Achse des Diagramms zeigt die Bootzeit in Sekunden an, die Y-Achse zeichnet chronologisch alle per Systemd gestarteten Dienste und Aktionen mit ihrer jeweiligen Dauer auf.

Die meisten davon werden parallel aktiviert und bremsen sich nicht gegenseitig aus. Die eigentliche Startzeit eines Dienstes ist hier mit kräftigen Rot hinterlegt. **-dw**

Dateiverwaltung: Hilfestellung für oktale Zugriffsrechte

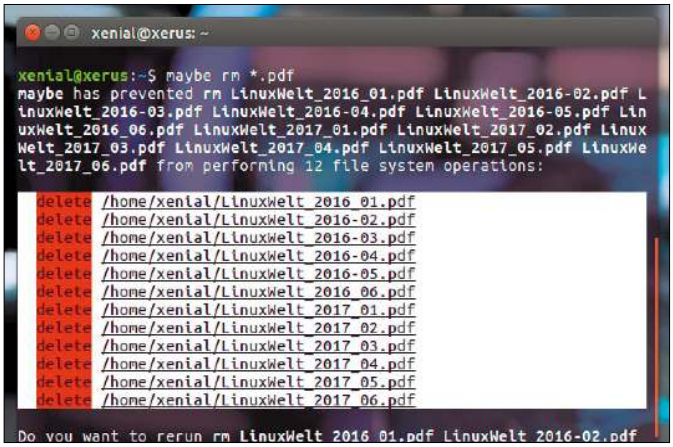
Die Grundlagen der Zugriffsrechte in einem Unix-Dateisystem sind alles andere als kompliziert. Schreibrecht, Leserecht und Rechte zum Ausführen lassen sich für einzelne Benutzer, ganze Gruppen und alle anderen festlegen. Für Einsteiger stellt die unter Linux übliche oktale Notation dieser Zugriffsrechte aber immer wieder eine Hürde dar.

Der Befehl chmod („change mode“) dient in der Shell schon seit grauen Unix-Vorzeiten zum Setzen und Entziehen von Zugriffsrechten im Dateisystem. Während Desktopanwender unter Linux damit nur äußerst selten Berechtigungen ändern müssen, kommt der Befehl bei der Administration eines Linux-Servers häufiger zum Einsatz. Wem als Gelegenheitsadministrator die oft benötigen oktalen Zugriffsrechte für chmod nicht geläufig sind, findet Hilfe im Web: Die englischsprachige Seite *https://chmodcommand.com* erlaubt die Zusammenstellung der gewünschten Berechtigungen mit einigen Klicks und präsentiert als Ergebnis den dafür benötigten chmod-Befehl. Wichtig ist dabei, nicht mit den voreingestellten Standards zu arbeiten, die zunächst auf die Rechte „777“ (Vollzugriff für alle) und Rekursion eingestellt sind. **-dw**



Rechte berechnen: Chmod-Calculator (*https://chmodcommand.com*) stellt im Browser ein komfortables Menü bereit, das den benötigten Befehl chmod einfach per Klick zusammenstellt.

Debugging mit Maybe: Sandkasten für Scripts und Befehle



Was wäre wenn? Das Tool Maybe zeigt, was die analysierten Scripts oder Befehle im Dateisystem anstellen würden, und blockiert diese Aktionen zunächst.

Aus dem Quellcode eines Scripts oder aus den Befehlen eines langen Kommandos ist nicht immer gleich ersichtlich, welche Auswirkungen auf das Dateisystem zu erwarten sind. Das in Python geschriebene Tool Maybe gibt Aufschluss darüber, welche Aktionen ein Befehl oder Script im Dateisystem ausführt.

Ohne tatsächlich Dateien zu ändern oder zu löschen, listet Maybe lediglich auf, was ein nachfolgendes Kommando oder Script tun würde. Das Kunststück gelingt mit dem Systemaufruf *Ptrace*, der die Dateioperationen entgegennimmt und auswertet, aber nicht ausführt.

Zur Installation von „Maybe“ dient nicht der Quellcode auf der Projektseite des Entwicklers unter *https://github.com/p-e-w/maybe*. Eine viel einfachere Installation erfolgt über ein Python-Paket, das mit dem Python-Installer Pip schnell eingerichtet ist. In Debian, Raspbian, Ubuntu, Mint sind zur Einrichtung im Terminal nur die Befehle

```
sudo apt install python-pip
```

und

```
sudo pip install maybe
```

nötig. Danach ist das Tool einsatzbereit und wird einem Aufruf einfach vorangestellt:

```
maybe [Script/Befehl]
```

Anschließend listet Maybe alle geplanten Änderungen am Dateisystem auf und fragt nach, ob man in einem zweiten Durchgang diese Aktionen erlauben möchte („permit these operations?“).

Hinweis: Der Entwickler weist darauf hin, dass Maybe kein Sicherheitstool ist und es durchaus Wege und Mittel gibt, aus dem Sandkasten von Ptrace auszubrechen. Zur Fehlersuche und für Tests weitgehend vertrauenswürdiger Scripts und Befehle ist das Tool aber gut geeignet. **-dw**

Komfortable Komponenten

Diesmal bekommen Notebooks mehr Aufmerksamkeit: USB-Adapter rüsten bei besonders kompakten Modellen den oft fehlenden Ethernet-Anschluss nach. Und ein Überwachungstool behält unter Ubuntu und Co. die Entladekurve des Akkus im Blick.

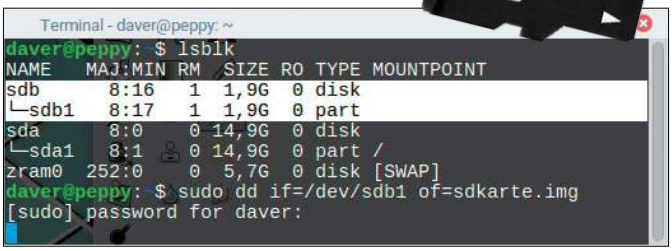
Micro-SD-Karten: Android-Smartphone als Kartenleser

Unterwegs ist nicht immer ein Kartenlesegerät oder eine Adapterkarte für SDHC-Karten zur Hand. Zur Not tut es aber auch ein Android-Smartphone oder -Tablet mit SDHC-Slot. Linux kann Android-Geräte nach dem Anschluss via USB wie einen Kartenleser einbinden und eine eingesteckte Karte sogar direkt mit dem Kommandozeilentool dd lesen und beschreiben.

Damit das Smartphone oder Tablet von Linux als externer Kartenleser eingebunden wird, stecken Sie die Karte in das Android-Gerät und verbinden dieses per USB-Kabel mit dem Linux-Rechner. Auf dem Display erscheint dann der Auswahldialog, um den Übertragungsmodus des Android-Geräts auszuwählen. Die richtige Option ist hier „Massenspeicher (MSC)“. Daraufhin zeigt Android noch einen Hinweis zur Bestätigung an, dass der Zugriff auf die Speicherkarte nur per USB erfolgen kann und währenddessen im Android-System nicht zur Verfügung steht.

Anschließend taucht das Gerät im Linux-System als Massenspeicher auf und die eingesteckte SD-Karte bekommt einen gewöhnlichen Device-Pfad im Stil von „/dev/[X][N]“ zugewiesen. Die Eingabe von

```
lsblk
```



Kartenleser: Hier dient ein Android-Smartphone am USB-Port als Lesegerät für SD-Karten. *lsblk* zeigt den Gerätepfad an, in diesem Beispiel „/dev/sdb1“.

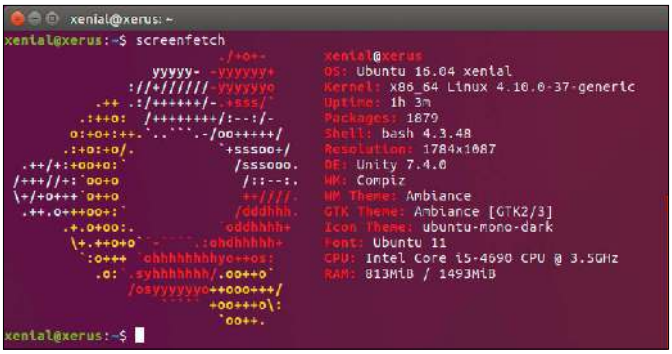
im Terminal zeigt diesen Device-Pfad an, anhand dessen sich die Karte auch mit dd lesen und beschreiben lässt.

Hinweis: Es sind von Herstellern angepasste Versionen von Android im Umlauf, in welchen der Massenspeichermodus für SD-Karten deaktiviert wurde. In diesem Fall hilft es oft weiter, in den Android-Einstellungen die Entwickleroptionen und dort das „USB-Debugging“ zu aktivieren. Diese Optionen zeigen sich nach einem siebenmaligen Antippen der „Build-Nummer“ im Untermenü „Über das Telefon/Geräteinformationen“. **-dw**

Server-Übersicht: Systeminfos beim Log-in

Arbeitet man mit mehreren Linux-Servern, so ist eine Übersichtsseite hilfreich, um das System gleich zu identifizieren. Das Script Screenfetch liefert dazu im Terminal Hardware- sowie Systeminformationen – auf Wunsch gleich nach der Anmeldung per SSH. Neben einem Distributionslogo im Textformat gibt Screenfetch die Kernel-Version, die bisherige Laufzeit (Uptime), die Anzahl der installierten Pakete, die verwendete Shell und Informationen zu CPU, Grafikchip und RAM aus.

In nahezu jeder Linux-Distribution steht Screenfetch zur Installation über den jeweiligen Paketmanager bereit. So ist es in Debian und Ubuntu mit



Systeminformationen auf einen Blick: Das Bash-Script Screenfetch sammelt die wichtigsten Daten zu System und Hardware auf einer Übersichtsseite im Terminal.

```
sudo apt-get install
  screenfetch
```

schnell eingerichtet. Die Eingabe von

```
screenfetch
```

im Terminal präsentiert eine farbige Übersichtsseite. Soll diese bei jeder Anmeldung am System angezeigt werden, dann öffnen Sie die Konfigurationsdatei „/etc/bash.bashrc“ („/etc/bashrc“ unter Fedora Linux) mit root-Recht in einem Texteditor und fügen die Zeile „/usr/bin/screenfetch“ ganz am Ende der Datei hinzu. **-dw**

Notebooks: Ethernet über USB-Adapter nachrüsten

Ein großer Teil der Notebooks im handlichen 13-Zoll-Fomat verzichtet auf einen Ethernet-Anschluss. Zum Übertragen großer Datenmengen ist die gelegentliche kabelgestützte Netzwerkverbindung aber unschlagbar. Bei regelmäßigen, umfangreichen Backups und beim weitgehend stationären Einsatz eines Notebooks auf dem Schreibtisch macht sich ein Ethernet-Adapter für den USB-Port schnell bezahlt.

Solche Adapter für USB 2.0, USB 3.0 und USB 3.1 mit USB-C-Port funktionieren unabhängig von Modell und Hersteller des Notebooks. Allerdings verlangen diese Adapter stets nach einem Treiber und deshalb funktionieren nicht alle mit Linux. Schon beim Kauf muss man daher darauf achten, dass der Netzwerkchip eines USB-Adapters im Linux-Kernel Unterstützung findet.

Ethernet nachrüsten: USB-Ethernet-Adapter mit einem Chip von Asix Electronics funktionieren auch unter Linux, da dieser taiwanische Hersteller Treiber zum Linux-Kernel beisteuert.

Die Erfahrung zeigt, dass die Chips von Asix Electronics unter Linux gut funktionieren, da der Halbleiterhersteller einen eigenen Linux-Treiber entwickelt hat und diesen regelmäßig aktualisiert.

In den verbreiteten Linux-Distributionen ist der Treiber als Kernel-Modul schon vorhanden. Erfreulicherweise ist der Netzwerkchip in zahlreichen erschwinglichen Ethernet-Adaptern verbaut.

USB 2.0: Für Notebooks mit dem älteren USB-Standard ist ein LAN-Adapter von Ugreen mit bis zu 100 MBit/s ausreichend, der im Versand rund 11 Euro kostet (*http://amzn.to/2kT7iZY*).

USB 3.0: Mit bis zu 1000 MBit/s können Ethernet-Adapter an einem USB-3.0-Port arbeiten, der an Notebooks an seiner blauen Farbe leicht zu erkennen ist. Für diese Anschlüsse ist unter Linux ein Adapter von CSL für 10 Euro empfehlenswert (*http://amzn.to/2zrLiZG*).

USB 3.1 (USB-C): Generell sind Geräte mit USB-C-Anschluss teure, als die nahe Verwandtschaft mit USB 3.0. Die günstigste Lösung ist der Adapter von Dodocool zu 14 Euro, der ebenfalls einen Asix-Chip nutzt und bis zu 1000 MBit/s leistet.

Nach dem Anstecken des Adapters zeigt der Befehl *lsusb* im Terminal das Gerät mit Hersteller und eindeutiger Geräte-ID an. Diese hexadezimale ID im Format „[XXXX]:[YYYY]“ eignet sich außerdem dazu, unbekannte Adapter eindeutig zu identifizieren.

Die Onlinedatenbank *https://usb-ids.gowdy.us/read/UD* hilft dabei, Hersteller-ID „[XXXX]“und Modell-ID „[YYYY]“ nachzuschlagen. Generell sollte das Drahtlosnetzwerk im Network-Manager komplett deaktiviert werden, wenn ein Ethernet-Adapter angeschlossen ist, damit das Linux-System den Netzwerkverkehr konsequent über das kabelgebundene Ethernet routet. **-dw**

Notebookakku: Der Aptik Battery Monitor

Wie steht es um die Batterie eines Notebooks und deren Entladung unter Berücksichtigung der CPU-Auslastung? Diese Frage beantwortet unter Ubuntu und Co. der Aptik Battery Monitor. Dieses Überwachungstool besteht aus zwei Komponenten: Ein Systemdienst protokolliert im Hintergrund die Entladekurve des Notebook-Akkus und die CPU-Auslastung.

Zur Auswertung und Anzeige dieser Daten gibt es das grafische Programm „/usr/bin/aptik-battery-monitor-gtk“, das man über das Anwendungsmenü der verwendeten Desktopumgebung aufruft. Ein angezeigtes Zeitdiagramm überlagert die Entladekurve des Akkus mit der Prozessoraktivität. Diese Auswertung gibt Aufschluss darüber, wieviel Laufzeit unter Last von einem alternden Akku noch zu erwarten ist.

Zur Installation des „Aptik Battery Monitor“ stellt der Entwickler ein PPA (externes Repository) für Ubuntu 16.04 und 17.10 bereit.

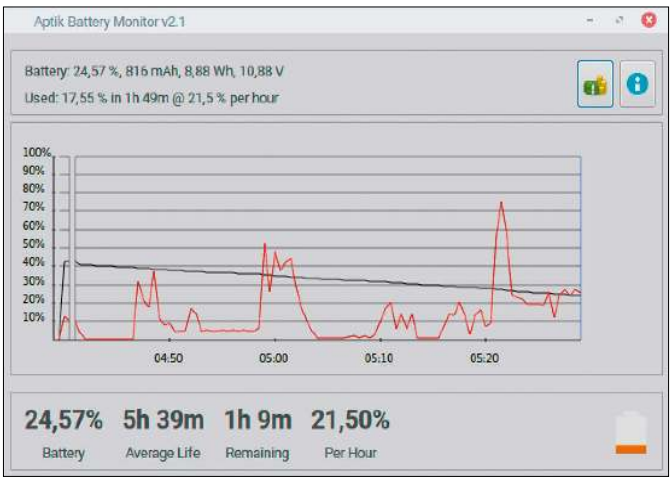
In einem Terminal nimmt das Kommando

```
sudo apt-add-repository
  ppa:teejee2008/ppa
```

das Repository auf und die beiden Befehle

```
sudo apt-get update
sudo apt-get install
  aptik-battery-monitor
```

installieren das Überwachungstool. Aktiv ist der Dienst zur Protokollierung der Daten aber erst nach einem Neustart des Systems. **-dw**



Akku und Auslastung: Der Aptik Battery Monitor protokolliert Entladung und CPU-Last. Diese Daten erlauben eine realistische Einschätzung der Akkulaufzeit.

Souveräne Software

Der beliebte Mediaplayer VLC ist immer für Überraschungen gut und kann mit einer Android-App gesteuert werden. Zudem geht es in den Softwaretipps um Libre Office und ausnahmsweise mal um Linux-Clients für Microsoft Exchange.

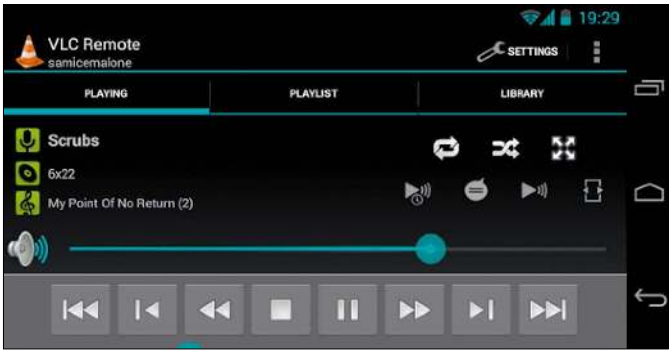
VLC-Player: Fernsteuerung per App

Remote for VLC (Fork) 0.7.5: *Android-App zur Fernsteuerung von VLC über das WLAN. Installation über Google Play (https://goo.gl/z1NdA5)*

Wenn ein PC mit dem Programm VLC als Videoplayer an einem TV-Gerät angeschlossen ist, dann ist meist eine Fernbedienung nützlich, um nicht für jede Aktion zum PC gehen zu müssen. VLC verfügt über eine schlichte, universelle Fernbedienungsfunktion über eine Webschnittstelle. Es geht aber noch bequemer – per Android-App auf dem Smartphone oder Tablet. Bevor VLC mit einer Android-App im gleichen WLAN Kontakt aufnehmen will, muss der Player jedoch erst entsprechend konfiguriert sein.

Diese Einstellungen sind tief in den Einstellungen vergraben. Im VLC-Player öffnen Sie über „Tools“ beziehungsweise „Werkzeuge“ den Punkt „Einstellungen“ und klicken unten links auf „Einstellungen zeigen -> Alle“. Die gesuchten Optionen finden sich in der Menüstruktur unterhalb von „Interface -> Hauptinterfaces -> Lua“. Dort gibt es Feld „Lua-HTTP -> Passwort“, wo Sie ein beliebiges Passwort eintragen. Ein Klick auf „Speichern“ übernimmt die Einstellungen.

Zurück auf der Programmoberfläche setzt der Menüpunkt „Ansicht -> Interface hinzufügen -> Web“ den Fernsteuerungsserver in Gang. Dieser Schritt ist übrigens immer nötig, bevor VLC eingehende Verbindungen akzeptiert. Auf dem gewünschten Android-Gerät benötigen Sie die App Remote for VLC (Fork) über Google Play (*https://goo.gl/z1NdA5*). Die Fernsteuerung ist zwar englischsprachig, dafür aber ohne lästige Werbung. Nach dem Start der App sucht diese automatisch nach einer laufenden VLC-Instanz im lokalen Netzwerk. Zur Verbindungsaufnahme ist in der Serververbindung dann nur noch das zuvor vergebene Passwort einzugeben, wenn die Meldung „Requires Authentication“ erscheint. **-dw**



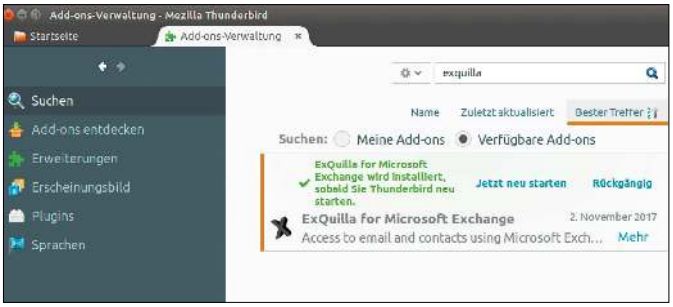
Fernsteuerung für den Player VLC: Eine komfortable Android-App für das Smartphone zur VLC-Fernsteuerung über das WLAN erspart den Gang zum PC.

Microsoft Exchange: Zugriff mit Linux

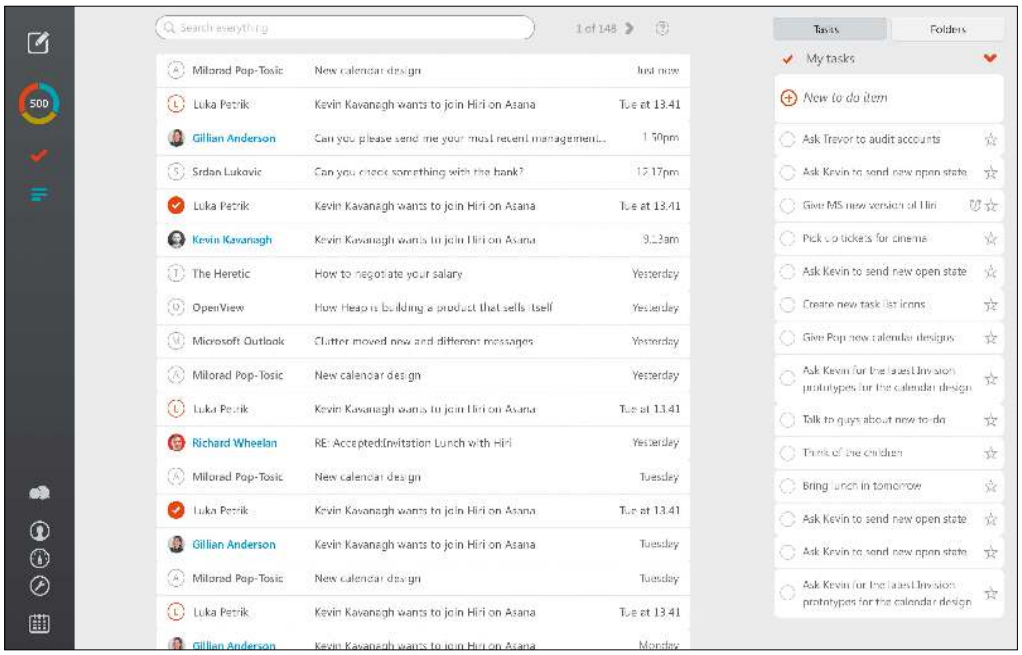
Exquilla 52.3: *Add-on für Thunderbird 52.x für den Zugriff auf Exchange-Server, deutschsprachige Shareware (10 US-Dollar pro Jahr), Download unter https://addons.mozilla.org/de-DE/thunderbird/addon/exquilla-exchange-web-services*

Hiri 1.3.2: *Grafischer Linux-Client für Exchange, Office 365 und Outlook.com, englischsprachige Shareware (39 US-Dollar pro Jahr), Download unter https://www.hiri.com*

Microsoft Exchange hat sich über die Jahre als Quasistandard für Groupwarelösungen etabliert. Ein häufiges Problem von Umsteigern auf Linux ist die Anbindung des Linux-Desktops mit geeigneten Programmen an einen Exchange-Server im Büro, um E-Mail, Kalendereinträge und Kontakte abzurufen. Für viele Anwender ist Exchange sogar ein Hauptmotiv, keinen Umstieg von Windows zu Linux zu wagen. Inzwischen stehen Linux-Anwender nicht mehr im Regen, denn es gibt mehrere Möglichkeiten, auch ohne parallel installiertes Windows-System oder virtuelle Maschine auf einen



Zugriff auf Microsoft Exchange mit Exquilla: Das Add-on erweitert Thunderbird, funktioniert aber mittlerweile nicht mehr mit allen Exchange-Versionen.



Exchange-Client Hiri: Dieses Programm ist Shareware und verbindet sich mit Exchange, Office 365 und Outlook.com. Zur Installation in Ubuntu gibt es ein Snappaket.

Exchange-Server zu kommen. Eine verbreitete Lösung für Thunderbird ist das Add-on Exquilla, das zum Abruf von E-Mails und Kontakten eine Verbindung zwischen Exchange und dem freien Mailprogramm herstellt. Exquilla ist aber nicht Open Source und kostenlos, sondern Shareware. Das Add-on ist im offiziellen Erweiterungsverzeichnis für Thunderbird 52.x verfügbar (*https://addons.mozilla.org/de-DE/thunderbird/addon/exquilla-exchange-web-services*).

Es bietet einen Testzeitraum von 60 Tagen, dann wird ein Obolus von zehn US-Dollar pro Jahr fällig. Nach der Installation findet sich das Add-on unter „Extras -> Exquilla für Microsoft Exchange“. Nach Berichten von Anwendern funktioniert es aber nicht mehr mit allen Versionen des Exchange-Servers und nicht mehr zuverlässig mit Office 365, aber der Testzeitraum lässt zumindest einen Langzeitversuch zu.

Falls das Add-on die Zusammenarbeit mit Exchange verweigert, gibt es noch eine weitere Möglichkeit: Hiri (*https://www.hiri.com*) ist ein neuerer Client für Exchange, Office 365 und Outlook.com. Das Programm kann Mails, den Kalender, Aufgaben und Kontakte von Exchange abrufen und verwalten. Auch Hiri ist nicht Open Source, sondern Shareware. Der Testzeitraum beträgt 14 Tage und eine Registrierung kostet 39 US-Dollar pro Jahr. Die Installation ist in Ubuntu vergleichsweise einfach als Snappaket möglich. **-dw**

Libre Office: Alle Dateisperren aufheben

Libre Office sperrt geöffnete Dateien, damit das Dokument nicht versehentlich mehrfach geöffnet wird. Wenn Libre Office abstürzt, der Rechner mit noch geöffneten Dokumenten abgeschaltet wird, dann kann es vorkommen, dass die Dateien gesperrt bleiben. Geöffnete Dokumente sperrt Libre Office auf eine ganz einfache Weise. Im gleichen Verzeichnis legt die Office-Suite zu jedem aktuell geöffneten Dokument eine versteckte Datei mit 0 Byte an, die einen Namen nach dem Schema

```
.~lock.[Dateiname].odt#
```

bekommt. Es handelt sich um eine Textdatei, in welcher der Name des Benutzers steht, der das Dokument gerade geöffnet hat, sowie der Hostname und der komplette Pfad. Beim Schließen des Dokuments entfernt Libre Office diese versteckte temporäre Datei wieder und gibt das Dokument damit frei.

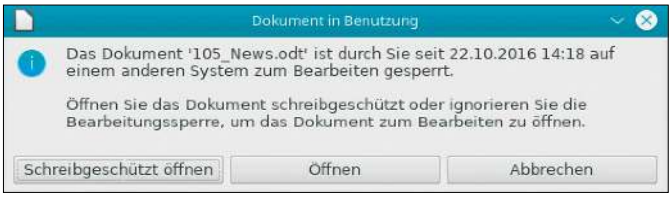
Findet Libre Office eine Datei dieser Art in einem Verzeichnis, geht es immer davon aus, dass dieses Dokument bereits geöffnet ist, und gibt einen Warnhinweis aus. Das Dokument kann dann als Kopie, im Nur-Lesen-Modus oder nach einer Bestätigung auch bearbeitend geöffnet werden. In größeren Dokumentarchiven kommt es im Laufe der Zeit immer dazu, dass mehrere Dateisperren zurückbleiben. Um diese systematisch zu finden, hilft folgender Befehl in der Kommandozeile:

```
find . -type f -name
  .~lock\*
```

Ausgehend vom aktuellen Verzeichnis listet dieser Befehl alle versteckten Sperrdateien von Libre Office in der Ordnerstruktur auf. Mit dem Kommando

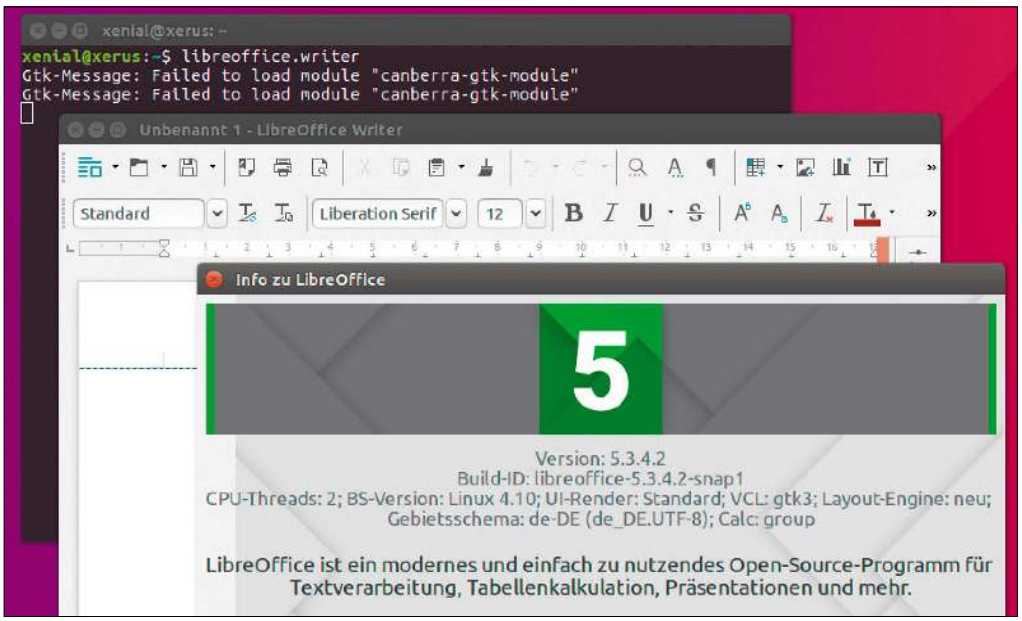
```
find . -type f -name
  .~lock\* -exec rm -i {} \;
```

ist es möglich, diese Dateien gleich zu löschen. Dieser Befehl fragt aber vor jeder Löschaktion noch einmal nach. **-dw**



Gesperrt: Findet Libre Office eine Sperre in Form einer versteckten Datei im gleichen Verzeichnis, will es das Dokument nicht zur Bearbeitung öffnen.

Ubuntu LTS: Neues Libre Office installieren



Libre Office als Snap installieren und ausführen: Programme aus Snappaketen sind inzwischen gut in den Ubuntu-Desktop integriert, verlangen aber nach einem manuellen Start.

Es kann dauern, bis aktuelle Programmversionen wie etwa das aktuelle Libre Office in die Paketquellen einer Linux-Distribution aufgenommen werden. Bei Ubuntu gibt es neue Versionsnummern von Programmen erst mit dem Schritt auf eine neue Ausgabe der Distribution. Ubuntu LTS mit Langzeitunterstützung bleibt deshalb fünf Jahre bei der gleichen Version von Libre Office. Während Ubuntu 17.10 (auf Heft-DVD) schon Libre Office 5.4 in den Paketquellen führt, verharrt das Office-Paket in Ubuntu 16.04 noch bei Version 5.1. Im Fall von Libre Office helfen inoffizielle Paketquellen weiter, denn die Bürosoftware ist so populär und essenziell, dass sich hier genügend Entwickler und Tester finden, um unabhängig von der offiziellen Ubuntu-Entwicklung frischere Pakete bereitzustellen.

Traditionelle Installation: Einen Weg für fortgeschrittene Anwender, das derzeit aktuelle Libre Office 5.4 in Ubuntu zu installieren, liefert ein inoffizielles Repository (PPA). Für dessen Einrichtung genügen in einem Terminalfenster diese beiden Befehle:

```
sudo add-apt-repository
  ppa:libreoffice/
  libreoffice-5-4
sudo apt-get update
```

Ein installiertes Libre Office 5.1 wird dann beim Aufruf von

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

automatisch auf den neuen Stand gebracht.

Die Installation über ein Repository hat den Nachteil, dass eine bisherige Version von Libre Office überschrieben wird. Möchte man wegen eines unerwarteten Bugs dann doch wieder zurück zur älteren Version aus den Standard-Paketquellen, sind damit einige Schritte verbunden:

Die zwei Kommandos

```
sudo apt-add-repository
  --remove
  ppa:libreoffice/
  libreoffice-5-4
sudo apt-get update
```

entfernen das PPA wieder und

```
sudo apt-get install
  libreoffice
```

installiert Libre Office aus den offiziellen Quellen.

Installation per Snap: Eine neue, einfachere Methode, Libre Office in Ubuntu LTS zu installieren, ist mit Snappaketen möglich. Dabei handelt es sich um abgeschottete Container, die alle Dateien eines Programms enthalten und deshalb mit installierten Systembibliotheken und vorhandenen Programmversionen nicht in Konflikt geraten. So installiert

```
sudo snap install
  libreoffice
```

die neuere Version 5.3 von Libre Office als Snap. Ein kosmetisches Problem ist dabei, dass Ubuntu installierte Snaps noch nicht im Anwendungsmenü des Desktops anzeigt.

Die als Snap installierten Office-Anwendungen müssen also manuell über das Terminal gestartet werden: *libreoffice.writer* startet den *Writer*, *libreoffice.calc* die Tabellenkalkulation und *libreoffice.draw* das Zeichenprogramm. **-dw**

Libre-Office-Formatvorlagen: Zurück zum Standard

Libre Office liefert ein umfangreiches Set an Formatvorlagen aus. Hat man diese Vorlagen geändert und möchte doch wieder die ursprünglichen Formatierungen, dann gibt es einen Weg zurück zum Standard. Zuerst öffnet die Taste F11 oder ein Klick auf „Vorlagen – Formatvorlagen“ die Liste der Vorlagen.

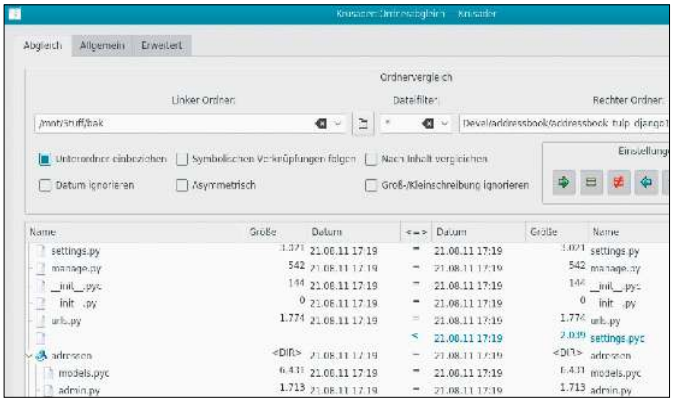
Dort klicken Sie mit der rechten Maustaste auf die gewünschte Vorlage, die zurückgesetzt werden soll, und wählen den Menüpunkt „Ändern“.

Im jetzt angezeigten Dialog verwenden Sie das Untermenü „Verwalten“. Im unteren Bereich des Dialogs zeigt der Dialog im Feld „Enthält“ die Formatabweichungen dieser Vorlage vom Standard. Steht hier beispielsweise „grün“, unterscheidet sich die Schriftfarbe dieser Vorlage vom ursprüngli-

chen Wert. Um diesen Wert zurückzusetzen, gehen Sie im gleichen Dialog auf das Untermenü „Schrifteffekt -> Schriftfarbe“ und klicken auf die Schaltfläche „Standard“. Abhängig davon, welche Formate der Vorlage vom Standard abweichen, kann man auf diese Weise alle angezeigten Abweichungen rückgängig machen. **-dw**

Vorlagen zurücksetzen: Ist bei der Bearbeitung von Formatvorlagen etwas schief gegangen, lassen sich die Änderungen auflisten und rückgängig machen.

Dateimanager Krusader: Ordner abgleichen



Ordnerinhalte abgleichen: Diese nützliche Funktion im Dateimanager Krusader bringt Verzeichnisse auf den gleichen Stand – auch über das Protokoll SSH.

Nicht ohne Grund hat das KDE-Programm Krusader den Ruf, der mächtigste Dateimanager für den Linux-Desktop zu sein. Einige der fortgeschrittenen Funktionen erschließen sich nicht gleich und sind in Untermenüs vergraben – etwa die nützliche Ordnersynchronisation, die Verzeichnisse auch über das Netzwerk abgleichen kann. Die Synchronisationsfunktion in Krusader ist besonders nützlich für manuell erstellte Backups und für den Abgleich von Verzeichnissen auf externen Medien. Sie befindet sich im Menü „Extras -> Ordner abgleichen“. Dabei übernimmt Krusader die aktuell geöffneten Verzeichnisse im linken und rechten Fenster in den Orderabgleich, der zunächst sein eigenes Fenster öffnet.

Hier lassen sich etliche Optionen zum Abgleich einstellen. Standardmäßig bezieht die Synchronisation Unterordner ein und vergleicht einzelne Dateien anhand des Namens und Änderungsdatums. Diese Optionen sind auf der zuerst angezeigten Menüseite „Abgleich“ bereits vorausgewählt. Unter „Allgemein“ und „Erweitert“ warten Feineinstellungen zum Abgleich, etwa Datei- und Datumsfilter. Ein Klick ganz unten auf „Vergleichen“ führt zuerst eine Analyse der Ordnerinhalte durch, synchronisiert aber noch keine Dateien. Stattdessen zeigt das Dateifenster in der Mitte eine Liste aller Dateioperationen zur Überprüfung an. Erst der Klick auf die Schaltfläche „Abgleichen“ führt den Abgleich tatsächlich aus.

Tipp: Der Ordnerabgleich von Krusader eignet sich auch vortrefflich, um Dateien über das Netzwerk zwischen Linux-Rechnern abzugleichen. Denn Krusader kann über das Netzwerkpräfix

```
fish://[Adresse]
```

direkt über SSH auf das Dateisystem eines SSH-Servers zugreifen. **-dw**

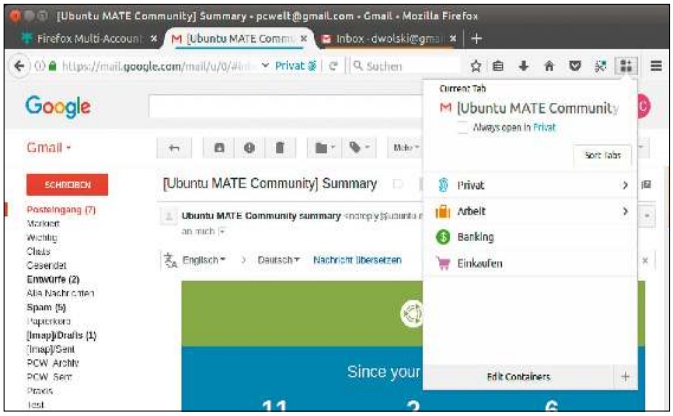
Firefox im Container: Mehrfachanmeldung bei Onlinediensten

Bisher war es nur über ein Inkognito-Fenster möglich, sich in Firefox zweimal an einem Onlinedienst wie Google Mail anzumelden. Eine neue Containerfunktion erlaubt die mehrfache Anmeldung über abgeschottete Browserinstanzen. Um Container zu nutzen, ist erst noch die Installation eines Add-ons nötig, das die Mozilla Foundation selbst erstellt hat. Die Firefox Multi-Account Containers liegen unter *https://addons.mozilla.org/de/firefox/addon/multi-account-containers* zur Installation bereit. Ein neues Icon in der Menüleiste steuert die momentan noch durchgehend englischsprachige Erweiterung.

Nach einer kurzen Erklärung in einer Diashow ist die Funktion einsatzbereit. Ein Klick auf das neue Icon öffnet ein Untermenü, das nun die Kategorien „Privat“, „Arbeit“, „Banking“ und „Einkaufen“ anbietet. Ein weiterer Klick auf eine Kategorie öffnet einen neuen, farbig hinterlegten Tab.

Diese Tabs sind als eigenständige Sitzungen voneinander getrennt und erlauben das mehrfache Anmelden an Diensten mit unterschiedlichen Identitäten.

Die Namen der Kategorien sind natürlich nur Vorschläge und lassen sich durch einen Klick auf „Edit Containers“ nach Belieben umbenennen. **-dw**



Einzelne Container sind jeweils eigene Identitäten: Die Firefox Multi-Account Containers erlauben dem Browser mehrere gleichzeitige Anmeldungen beim gleichen Onlinedienst.

Leserbriefe

Haben Sie Fragen zum Heft oder möchten Sie uns Ihre Meinung dazu mitteilen? Schreiben Sie bitte an *linux@it-media.de* oder per Post an Redaktion LinuxWelt, IT Media, Gotthardstr. 42, 80686 München. Von den vielen Zuschriften können wir nur eine Auswahl veröffentlichen. Sinnwahrende Kürzungen behalten wir uns vor.

Desktop auf Server abschalten

Auf die SD-Karte meines Platinenrechners habe ich vor Monaten ein Ubuntu-Systemimage mit grafischer Oberfläche kopiert. Inzwischen hat der Minirechner längst eine kleine Serverrolle übernommen, für welche der mitgestartete Desktop Mate völlig überflüssig ist und nur unnötig Speicher frisst. Wie schalte ich den Desktop ab?

Konrad R., per Mail

Die meisten jüngeren Linux-Distributionen verwenden als Systemmanager (Init-System) den zentralen Systemdienst systemd – so auch alle Ubuntu-Varianten. systemd steuert den Start aller weiteren Systemkomponenten wie auch die grafische Oberfläche. Das einschlägige Terminalwerkzeug für systemd ist das Kommando systemctl. Das mächtige Tool (siehe man systemctl) benötigt, abgesehen von einigen wenigen Infobefehlen, in aller Regel root-Recht. Das Kommando

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

schaltet den Desktop ab. Danach ist ein Neustart des Geräts erforderlich. Mit

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

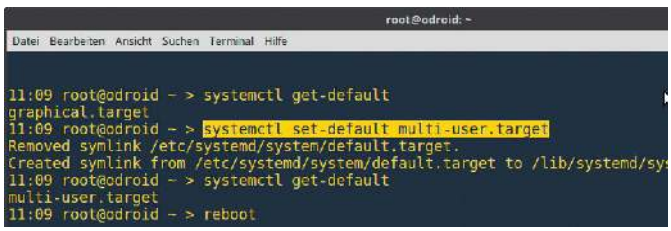
lässt sich der Desktop jederzeit wieder aktivieren. Im Übrigen können Sie bei standardmäßig abgeschalteter Oberfläche diese immer auch manuell mit *startx* nachladen.

Ubuntu meldet eine falsche Version

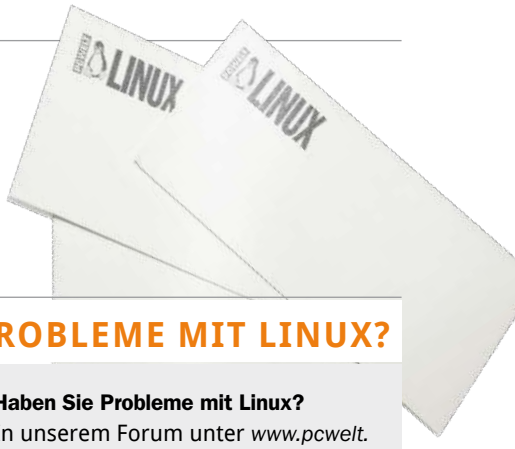
Beim Umstieg von einer älteren Ubuntu-Version 15.04 auf die LTS-Version 16.04 habe ich die saubere Neuinstallation einem Upgrade vorgezogen. Um den Neuanfang so komfortabel wie möglich zu halten, habe ich die gesicherten Verzeichnisse „/home“ mit den Benutzerdateien sowie „/etc“ mit den Konfigurationsdateien vom alten System in das neue übernommen. Ubuntu 16.04 läuft nun zwar, meldet aber die Version 15.04.

Johannes F., per Mail

Den Ordner „/etc“ einfach in ein anderes System zu kopieren, ist grob fehlerhaft! Damit haben Sie praktisch Motor und Getriebe des alten Systems in das neue übernommen – und es ist überraschend, dass Ubuntu 16.04 unter diesen Umständen überhaupt startet. Da im weiteren Betrieb durchaus größere Pannen als eine falsche Versionsangabe (in der Datei „/etc/issue“) zu befürchten sind, empfehlen wir Ihnen eine weitere Neuinstallation, bei der Sie anschließend nur das komplette Home-Verzeichnis des alten Systems übernehmen. Im Übrigen arbeitet Ubuntu in aller Regel sehr zuverlässig beim Systemupgrade auf eine neuere Version über den Aktualisierungsmanager. Damit vermeiden Sie derartige Probleme und ersparen sich zugleich den doppelten Kopieraufwand. Die Sicherung von „/home“ ist aber immer zu empfehlen.



Desktop abschalten: systemctl ermittelt den aktuellen Standard und stellt auf Wunsch von „graphical“ (Desktop) auf „multi-user“ um (kein Desktop).



PROBLEME MIT LINUX?

Haben Sie Probleme mit Linux?
In unserem Forum unter *www.pcwelt.de/forum* stehen Ihnen unter „Betriebssysteme -> Linux-Distributionen“ neben Linux-Experten auch andere Linux-Anwender mit Rat und Tat zur Seite und helfen bei Schwierigkeiten mit Linux. Aktuelle News rund um das Thema lesen Sie unter *www.pcwelt.de/computer-technik/betriebssystem-software/linux*.

Kontakt zur Redaktion
Wir freuen uns über jede Mail! Bei Fragen zum Heft LinuxWelt wenden Sie sich am besten an *linux@it-media.de*. Bitte beachten Sie, dass wir keinen Support für spezielle Hardware oder die Linux-Systeme auf der Heft-DVD leisten können.

LinuxWelt-Kundenservice für Einzelheft-Käufer
Haben Sie eine Ausgabe von LinuxWelt verpasst? Hier können Sie einzelne Hefte nachbestellen:
DataM-Services GmbH
Postfach 916, 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*

Digitalabo in der App
https://shop.pcwelt.de/portal/linux-welt-ipad-jahresabo-zukunft-ist-jetzt–2636

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, Thorsten Eggeling, Stephan Lamprecht, David Wolski
Titelgestaltung: Schulz-Hamparian, Editorial Design / Thomas Lutz
Freier Mitarbeiter Layout/Grafik: Alex Dankesreiter
Freie Mitarbeiterin Schlussredaktion: Andrea Röder
Freier Mitarbeiter digitale Medien: Ralf Buchner
Herstellung: Melanie Arzberger
Redaktionsassistenz: Manuela Kubon

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

KUNDENSERVICE

LinuxWelt-Kundenservice für Einzelheft-Käufer:
DataM-Services GmbH
Postfach 9161
97091 Würzburg
Tel.: 0931/4170-177
Fax: 0931/4170-497
(Mo bis Fr, 8 bis 17 Uhr)
E-Mail: *idg-techmedia@datam-services.de*

LinuxWelt-Kundenservice für Abonnenten: Fragen zum bestehenden Abonnement / Premium-Abonnement, zum Umtausch defekter Datenträger, zur Änderung persönlicher Daten (Anschrift, E-Mail-Adresse, Zahlungsweise, Bankverbindung) bitte an
Zenit Pressevertrieb GmbH
LinuxWelt-Kundenservice
Postfach 810580
70522 Stuttgart
Tel: 0711/7252-233
(Mo bis Fr, 8 bis 18 Uhr)
Fax: 0711/7252-333
E-Mail: *linuxwelt@zenit-presse.de*
Erscheinungsweise:
6x jährlich

Jahresbezugspreise LinuxWelt mit DVD: 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.

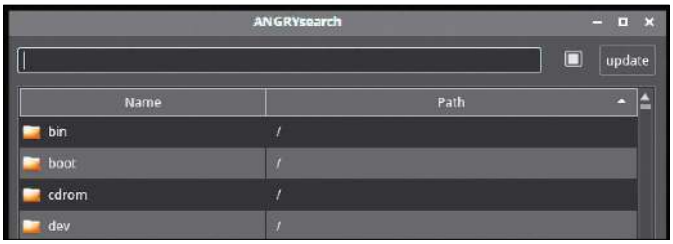
LinuxWelt 2/2018 erscheint am 26.1.2018

Aus Aktualitätsgründen können sich Themen ändern.

Die 20 Hürden des Windows-Umstiegs

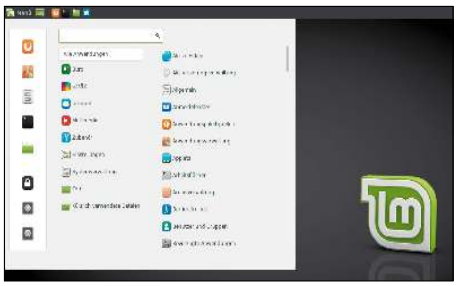
Stolpersteine und ernste Hindernisse: Die Wahl eines einsteigerfreundlichen Desktop-Linux ist eine wichtige Basis für den Windows-Umsteiger, aber keine Versicherung gegen Irritationen. Datenorganisation, Mountverhalten, Systeminformationen und Konfigurationsverhältnisse unterscheiden sich doch so gravierend, dass der bisherige Windows-Nutzer gelegentlich nicht mehr weiterweiß. Das Umsteiger-Special der nächsten LinuxWelt benennt die typischen Hindernisse und Missverständnisse. Dabei kommen die großen konzeptionellen Unterschiede ebenso zu Wort wie kleine Stolpersteine am Linux-Desktop.

Dateisuche mit Angry Search



Instantsearch für schnelle Dateisuche: Die Dateisuche mit dem Dateimanager oder mit find im Terminal ist vielen Linux-Nutzern nicht schnell oder nicht bequem genug. Es gibt manche Alternative für diese Aufgabe, unter anderem ein grafisches Python-Tool, das sich mit seinem Namen „AngrySearch“ schon mal ordentlich offensiv und angriffslustig bewirbt. Ob sich dies bei der Suchleistung tatsächlich bestätigt und wie komfortabel das Tool im Alltag ausfällt, lesen Sie in der kommenden LinuxWelt.

Linux Mint 18.3



Das nächste Point Release: Die Ubuntu-Basis hat im August 2017 das dritte Point Release der aktuellen Langzeitversion veröffentlicht (16.04.3). Wie immer ist danach das Linux-Mint-Team am Zuge, dieser Aktualisierung zu folgen – was gewöhnlich einige Monate dauert und dabei keinem exakten Releasezeitplan unterliegt. Die LinuxWelt 2/2018 berichtet daher entweder über die Betaversion von Mint 18.3 oder ausführlicher über die finale Version, die dann auch auf Heft-DVD vorliegt. Mint 18.3 wird in jedem Fall auch funktionale Neuheiten erhalten: Das Mint-Team kündigte an, Version 18.3 „Sylvia“ werde die Aktualisierung des Unterbaus zum Anlass nehmen, Verbesserungen am Cinnamon-Desktop, an Mintreport und an Timeshift einzubauen.

Fedora 27 Workstation

Fedora 27 mit erweitertem Flatpak-Angebot: Das Red-Hat-gesponserte Fedora ist ein Desktopsystem für Fans mit gewisser Linux-Erfahrung. Diese Fangemeinde wird auch die verspätete Version 27 wieder mit Ungeduld erwarten. Die stets innovative Distribution setzt dieses Mal ihren Fokus auf das hauseigene Containerformat Flatpak, das technisch verbessert wird und laut Ankündigung einen ansehnlichen Vorrat an Flatpak-Software mitbringen soll. Die kommende LinuxWelt berichtet über die Neuheiten und liefert das Livesystem startklar auf Heft-DVD.

PC-WELT PLUS

Stellen Sie uns auf die Probe!

3 x PC-WELT Plus zum Testpreis

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

16,99€

Satte **22%** gespart!

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

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

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

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

Ja, ich bestelle das PC-WELT Plus Testabo für 16,99€.

Möchten Sie die PC-WELT Plus anschließend weiter lesen, brauchen Sie nichts zu tun. Sie erhalten die PC-WELT Plus für weitere 12 Ausgaben zum aktuellen Jahresabopreis von z.Zt. 85,60 EUR. Danach ist eine Kündigung zur übernächsten Ausgabe jederzeit möglich.

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PWPMA14141

PC-WELT 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

Unendliche Möglichkeiten.

Die TUXEDO InfinityBook Serie

InfinityBook Pro 13		InfinityBook 14
13.3" Display QHD+ optional	HD	14" Display
Core i7 Quad-Core		Core i5 Dual-Core
bis zu 32 GB RAM		8 GB RAM
12h max. Akkulaufzeit		24h max. Akkulaufzeit
2x Speichermedien m.2 SSD + SATAIII HDD		1x Speichermedium m.2 SSD
aktiv gekühlt		lüfterlos, passiv gekühlt

Jetzt zum Vorzugspreis sichern

Konfigurieren Sie jetzt Ihr TUXEDO InfinityBook individuell und sparen dabei exklusiv als Leser 3% mit dem Rabattcode "LXWELTIB13" - *aber nur für kurze Zeit!*

TUXEDO COMPUTERS

tuxedocomputers.com