Multiboot-DVD mit 7 brandneuen Systemen
4/2018
Juni / Juli
Deutschland 8,50 €
Schweiz 16,90 sfr · Österreich + Benelux 9,45 €

LINUX WELT

Neue Version!
LinuxWelt
Rettungs-DVD

GROSSES SPECIAL!

Sichern Sie Ihr Linux!

Der perfekte Rundum-Schutz für Daten, PC und Netzwerk

- Optimal geschützt im Internet
- Linux-PC nach außen absichern
- System und Daten per Image sichern
- PLUS: Freigaben an der Fritzbox richtig einrichten

Profi-Tipps für Linux

- Firewalls für SSH-Verbindungen austricksen
- Logdateien einfacher kontrollieren
- Installationspakete umwandeln

Linux-Aufgaben automatisieren

- Cron-Jobs per Tool anlegen
- Fritzbox remote neu starten

Die besten Foto-Tools

- Fotos in der Konsole anzeigen
- Profi-Tools zur Bildbearbeitung
- Fotos einfacher verwalten

Neu: Ubuntu 18.04 LTS

Mehr Sicherheit, neue Funktionen und 5 Jahre Support!

Linux-Kernel 4.15 stopft Meltdown- und Spectre-Lücken
Schneller booten, Kernel-Patches ohne Neustart installieren u.v.m.

Medienserver perfekt einrichten

- Netflix und Amazon Video unter Kodi für Raspberry
- Plex als Multimedia-Software auf Mini-PCs

MULTIBOOT-DVD

Ubuntu 18.04 LTS
und weitere
6 Top-Systeme

Start-klar auf DVD!

Die neue LinuxWelt Rettungs-DVD 6.2.1

Auf DVD: Ubuntu 18.04 LTS

PLUS: Ubuntu Mate · Xubuntu · Lubuntu · Bunsenlabs Deuterium · Tiny Core

PLUS: 372 Seiten Linux-Profi-Wissen
Die besten Ratgeber, Tipps und Tricks der LinuxWelt in zwei handlichen PDFs

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

LINUX WELT

Stellen Sie uns auf die Probe!

2x LinuxWelt zum Testpreis

Jetzt testen:
2x LinuxWelt
gedruckt & digital

11,90 €

Satte **30%** gespart!

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

- ✓ **2x LinuxWelt als Heft frei Haus** mit Gratis-DVD
- ✓ **2x LinuxWelt direkt aufs Smartphone & Tablet** mit interaktivem Lesemodus

Jetzt bestellen unter
www.pcwelt.de/linuxtesten oder per Telefon: 0711/7252233 oder ganz einfach:

1. Formular ausfüllen **2. Foto machen** **3. Foto an linuxwelt@zenit-presse.de**

Ja, ich bestelle das LinuxWelt Testabo für 11,90 €.

Möchten Sie die LinuxWelt anschließend weiter lesen, brauchen Sie nichts zu tun. Sie erhalten die LinuxWelt für weitere 6 Ausgaben zum aktuellen Jahresabopreis von z.Zt. 49,50 EUR. Danach ist eine Kündigung zur übernächsten Ausgabe jederzeit möglich.

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

LWPMA14147

LinuxWelt erscheint im Verlag IT Media Publishing GmbH & Co. KG, Gotthardstraße 42, 80686 München, Registergericht München, HRA 104234, Geschäftsführer: Sebastian Hirsch.
Die Kundenbetreuung erfolgt durch ZENIT Pressevertrieb GmbH, Postfach 810580, 70522 Stuttgart, Geschäftsführer: Joachim John

Mehr Schutz von allen Seiten

Wir Verbraucher haben seit dem 25. Mai deutlich mehr Rechte, wenn es um den Datenschutz geht. Denn an diesem Tag ist die neue EU-weite Datenschutz-Grundverordnung (DSGVO) in Kraft getreten. Sie verbietet es Unternehmen, heimlich oder ohne Anlass Daten über uns zu sammeln. Und sie verleiht uns mehr Rechte gegenüber Firmen. So können wir etwa individuell einfordern, alle personenbezogenen Daten zu löschen.

Unternehmen müssen sehr vorsichtig sein, wenn sie Daten über ihre Nutzer speichern wollen. Bei einem Verstoß gegen die strengen Regeln der DSGVO drohen ihnen Geldbußen von bis zu 20 Millionen Euro oder 4 Prozent des Jahresumsatzes, je nachdem, was höher ist. Die DSGVO ist also anders als ihr Vorgänger kein zahnloser Papiertiger – gut für uns Verbraucher. Mehr Infos zur DSGVO gibt es hier: *www.pcwelt.de/2342614*.

Zum Thema Datenschutz und Sicherheit finden Sie in diesem Heft ein ausführliches Special. Auf über 30 Seiten zeigt die Linux-Welt, wie Sie noch sicherer im Internet unterwegs sein können, wie Sie Ihr Netzwerk besser schützen und wie Sie Ihr Linux-System selbst perfekt abschirmen.

Herzlichst, Ihr

Arne Arnold
Redakteur
arnold@it-media.de

Sicherheit durch Linux

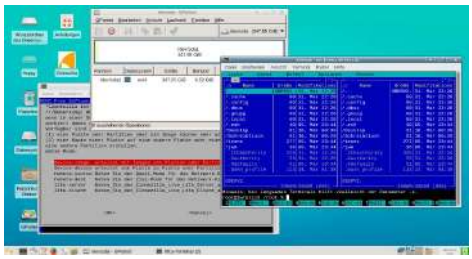
Linux ist sicher. Aber mehr noch: Unabhängige Livesysteme, Linux-Serverdienste, Routerprojekte und Klonprogramme erhöhen die Sicherheit für Netzwerk und Windows-Rechner.

S. 24

Odroid und Raspi

Odroid-Rechner und Raspberry Pi 3 B+: Was Odroid-Platinen leisten und was der jüngste Raspberry Pi 3 B+ zu bieten hat.

S. 96



Neuer Nothelfer

Gut gerüstet bei Linux-Pannen: Die neue LinuxWelt-Rettungs-DVD 6.2.1.

S. 68

Grundlagen

Special 1 – Sicherheit durch Linux

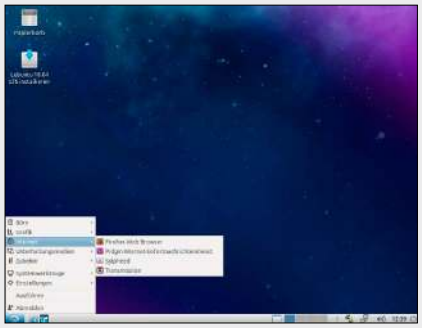
Die Highlights auf der DVD

Seit 26. April gibt es die neue Langzeitversion 18.04 von Ubuntu: Die Heft-DVD steht mit vier brandneuen Ubuntu-Editionen ganz im Zeichen des Linux-Desktopklassikers.

Ubuntu 18.04 LTS (S. 56–67)
Hauptedition mit Gnome-Oberfläche: Der elegante Desktop ist die richtige Wahl für moderne PCs und Notebooks. Nach der Vorstellung der allgemeinen Ubuntu-Neuerungen gibt der Artikel ab Seite 64 Praxistipps speziell zur Gnome-Hauptvariante.

Ubuntu Mate 18.04 LTS (S. 10)
Ein Ubuntu für alle Fälle: Der konservative, aber enorm anpassungsfähige Mate-Desktop kann sowohl Anfänger als auch Desktopbastler überzeugen. Die Mate-Edition hat moderate Ansprüche und gefällt auch bei hohen Bildschirmauflösungen.

Xubuntu/Lubuntu 18.04 LTS (S. 11 u. 14)
Ubuntu-Editionen für ältere Hardware: Mit den Desktops XFCE und LXDE ist Ubuntu seit Jahren eine solide Wahl für Rechner, auf denen kein aktuelles Windows mehr läuft. Xubuntu und Lubuntu bleiben auch in Version 18.04 Ressourcensparer.



Im Zeichen Ubuntus

Viermal Ubuntu plus drei Spezialsysteme

Ubuntu 18.04 (64 Bit)
Den Wechsel zu Gnome 3 als primären Desktop besiegelt diese Ubuntu-Version mit Langzeitsupport (LTS) bis ins Jahr 2023. Wer Gnome 3 bisher skeptisch gegenüberstand, bekommt aber vorinstallierte Gnome-Erweiterungen, die den Bruch mit Unity ein Stück weit abmildern. Liegt auch als ISO-Datei auf Heft-DVD.

Ubuntu Mate 18.04 (64 Bit)
Ist diese besonders einsteigerfreundliche Ubuntu-Variante der heimliche Star im Ubuntu-Zoo? Der Mate-Desktop bietet verschiedene Layouts an und kommt nun auch mit Hi-DPI-Bildschirmen klar. Die Softwareboutique macht die Einrichtung zusätzlicher Software besonders einfach. Liegt auch als ISO-Datei auf Heft-DVD.

Xubuntu 18.04 (64 Bit)
Der XFCE-Desktop ist in die Jahre gekommen, bleibt aber einer der komfortabelsten unter den schlanken Desktopumgebungen. Das stellenweise aufpolierte XFCE kann besser mit neuen Gnome-Programmen umgehen, beherrscht aber noch kein Hi-DPI. Bei der Softwareausstattung gibt es keine Unterschiede mehr zu den großen Ubuntu-Varianten. Liegt auch als ISO-Datei auf DVD.

Lubuntu 18.04 (32 Bit)
Lubuntu bietet alle Vorzüge eines Ubuntu-Systems für den Desktop, gibt sich aber mit der sparsamen LXDE-Oberfläche auch mit älterer Hardware zufrieden. Es ist die Ubuntu-Version mit dem kleinsten Fußabdruck und aus diesem Grund in der 32-Bit-Architektur auf DVD. Liegt auch als ISO-Datei auf DVD.

Bunsenlabs Deuterium (32 Bit)
Dieser ungewöhnliche Debian-Abkömmling hat einen extrem reduzierten, aber eleganten Desktop mit einem sorgfältig konfigurierten Openbox als Window-Manager. Bunsenlabs Deuterium basiert noch auf Debian 8, mit Updates bis 2020. Das Livesystem bietet ein separates Installationsprogramm, das über das Multibootmenü von Heft-DVD startet.

LinuxWelt-Rettungs-DVD 6.2.1 (32/64 Bit)
Das Livesystem des LinuxWelt-Redakteurs Thorsten Eggeling ist ein klassisches Notfallsystem für Linux-Anwender, das die neue Version des Partitionierers Gparted, das Backuptool Clonezilla sowie die Rettungstools Photorec und Testdisk mitbringt. Das weitgehend deutschsprachige System liegt auch als ISO-Datei auf Heft-DVD.

Tiny Core 9.0 (32 Bit)
Tiny Core ist mit großem Abstand das kleinste Livesystem auf der Heft-DVD: Tiny Core 9.0 bringt es samt dem Browser Firefox (Version 52 ESR), WLAN-Treibern, Tools und einem schlichten, aber ansprechenden Desktop auf weniger als 220 MB. Der Desktop ist minimalistisch und englischsprachig.

Extras & Tools

Super Grub Disk 2.02s9
Das bootfähige 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-Medien 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 PCI, RAM, Prozessor und Bios an.

Memtest 86+ 5.01
Der aktuelle Memtest 86+ testet den Arbeitsspeicher und unterstützt nun moderne Intel-Chipsätze. Das Diagnoseprogramm läuft auf jedem PC sowohl mit 32-Bit- als auch 64-Bit-CPUs und erkennt alle 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: Die Installation bietet optional die Einrichtung der Ask-Toolbar und von Werbelinks auf dem Desktop an.

Unetbootin 6.57
Das nützliche Tool mit grafischer Oberfläche transferiert mit wenigen Klicks die ISO-Images von Ubuntu und seinen Abkömmlingen (sowie weitere Distributionen) bequem auf USB-Stick oder Speicherkarten und macht diese mit einem eigenen Bootmenü startfähig. Auf DVD befinden sich die 32-Bit- und 64-Bit-Ausgabe für Linux (alle Linux-Distributionen), aber auch Versionen für Windows und Mac-OS.

Putty 0.70
Der Terminalclient für SSH und Telnet läuft unter allen Windows-Systemen. 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
Diese Abspaltung von Putty ist ebenfalls ein Terminalclient für SSH, allerdings mit einigen ergänzten Funktionen und bequemen Features. 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-Sticks und Speicherkarten. Das Programm liegt als ZIP-Archiv auf DVD, das keine Installation benötigt.

fritzbox-reboot.sh
Beispielscript zum Neustart einer AVM Fritzbox über das TR-064-Protokoll. Ideal für Cron-Jobs, um Router automatisiert neu zu starten.

conf.desktop und conf.sh
Begleitend zum Artikel im Heft (S. 14) liefern diese Scripts Abkürzungen zur Konfiguration von Ubuntu-Systemen.

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

LINUXWELT XXL DIGITAL

Das komplette Handbuch 4/18
Das stets aktualisierte E-Book auf Heft-DVD ist eine Nachlese zu Themen aus den letzten Ausgaben der LinuxWelt. Auf 305 Seiten vermittelt das neue E-Book Linux-Wissen und Know-how rund um Open-Source-Programme. Neben zeitlosen Themen zu Linux-Grundlagen ist das letzte Special zum Thema USB-Sticks und mobile Systeme enthalten. Außerdem geht es um den Raspberry Pi, und eine große Rubrik „Netzwerk und Internet“ fasst zahlreiche Beiträge aus diesem Themenbereich zusammen.

E-BOOK EXTRA

LinuxWelt digital „Server“
Auch in dieser Ausgabe gibt es wieder ein zusätzliches PDF: Das Thema ist Linux in der Serverrolle. Die Zusammenstellung wichtiger Artikel aus vergangenen Ausgaben zeigen Linux im Heimnetzwerk als Samba-Server für Windows-Freigaben, als Streamingserver für Musik und Filme sowie als Webserver.

WEITERE INFOS

Der Fokus der Heft-DVD liegt auf dem neuen Ubuntu 18.04, um das sich auch ein eigenes Heft-Special dreht. Die Vorstellung der DVD-Distributionen finden Sie im Heft ab Seite 10, den Ubuntu-Schwerpunkt ab Seite 56. Zusätzliche Hinweise zu den Distributionen auf Heft-DVD liefert die Übersicht auf der DVD, die Sie über die Datei „index.html“ in einem Browser öffnen. Das zweite Special dieser Ausgabe dreht sich ab Seite 24 um Sicherheit durch Linux: auf dem Desktop, im Heimnetz, auf dem Linux-Server und nicht zuletzt auch für Windows-Systeme.

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

Infotainment – Datenträger enthält nur Lehr- oder Infoprogramme

ANDROID WELT

Der große App-Guide 2018

Sonderheft
für nur
12,90 €

Über 500 Apps im Test!

Jetzt bestellen unter
www.pcwelt.de/appguide 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 AndroidWelt Sonderheft App-Guide 2018 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

Ubuntu 18.04 LTS auf Desktopsuche

Ubuntu 18.04 wird wieder über Jahre Linux am Desktop prägen. Es wird ja nicht nur durch offizielle Editionen repräsentiert, sondern auch durch Derivate wie Linux Mint. Die Systembasis ist gelungen, aber wie der ideale Ubuntu-Desktop aussehen soll, bleibt unbeantwortet.

VON HERMANN APFELBÖCK

Wir hatten alle offiziellen Editionen von Ubuntu 18.04 LTS in der Hand. Aufgrund des Produktionszeitraums dieser Ausgabe im April handelte es sich um die letzten Betaversionen, die sich aber nur noch durch Bugfixes von den endgültigen Versionen unterscheiden. Alle Editionen auf Heft-DVD sind finale Versionen.

Unser Fazit ist positiv: Sie dürfen sich auf ein solides Ubuntu freuen, das engagiert weiterentwickelt wurde. Ubuntu 18.04 bietet bietet mehr als eine aktualisierte Kernel-Basis und frische Softwareversionen. Der Ubiquity-Installer ist überarbeitet, was uns die zusätzliche Option einer „minimalen" Installation beschert. Außerdem wurde der Setupvorgang generell analysiert und gestrafft, was zu rekordverdächtig schnellen Installationen führt.

Andererseits hat Ubuntu das Angebot der Home-Verschlüsselung aus dem Installer genommen und empfiehlt die komplette Datenträgerverschlüsselung mit Luks, die weiterhin besteht. Über die genauen Gründe, Home-Verschlüsselung mit Ecrypt FS fallen zu lassen, hält sich Canonical bedeckt: Die Aussage, Ecrypt FS werde nicht mehr ausreichend gepflegt, bleibt unkonkret. Eventuell muss man die Aussage so interpretieren, dass sich Canonical nicht mehr in der Lage sieht, Ecrypt FS im eigenen Haus so zu pflegen, wie es einer LTS-Komponente gebührt: Ein Ecrypt-FS-Entwickler hat Canonical kürzlich verlassen.

Zurück zum Erfreulichen: Ubuntu 18.04 hat überragende Bootzeiten. Auf SSD bleiben die kleinen Ubuntus deutlich unter zehn Sekunden, selbst die große Hauptedition ist in gut elf Sekunden am Log-in.

Der überarbeitete Paketmanager Gnome-Software hat einen umfassenden Anspruch und integriert traditionelle Pakete, Snaps, Erweiterungen und Codecs.

Beim Gnome-Desktop der Hauptedition hat Canonical Investionen getätigt, die einen bruchlosen Übergang für bisherige Ubuntu-Nutzer erlauben sollen. Das rechts oder links positionierbare Startdock unterscheidet sich kaum vom früheren Unity-Starter. Trotzdem bleiben Zweifel, ob die Gnome-Edition zum legitimen Unity-Erben taugt: Ubuntu 18.04 mit Gnome 3 ist beim RAM-Verbrauch zum Dickschiff angewachsen – Tendenz: Richtung Windows. Und trotz modernem Schick haben die Gnome-„Aktivitäten" mehr Gegner als Freunde. Mate wird immer besser, kann aber seine altbackene Gnome-2-Herkunft nicht verbergen. Xubuntu und Lubuntu bleiben unbestrittene Kandidaten für schwächere Hardware, aber ohne Chance auf Schönheitstitel. Kubuntu und KDE? Auch das ist ein Sonderweg – ein populärer mit treuem Fanclub, aber nicht der Unity-Nachfolger.
Am besten gefallen hat uns die nunmehr offizielle Budgie-Edition (siehe Aufmacherbild), der es allerdings noch etwas an Reife und intuitiver Anpassung mangelt. Dennoch hat Budgie Potenzial, gegen Linux Mint und Cinnamon anzutreten.

Ubuntu-Hauptedition mit angepasstem Gnome-3-Desktop: Auf den ersten Blick unterscheidet sich die Oberfläche kaum vom bisherigen Unity.

Kontinuität bei Kubuntu mit KDE: Die Oberfläche hat sich wie XFCE (Xubuntu) und LXDE (Lubuntu) für die Ubuntu-Version 18.04 nicht extra hübsch gemacht.

Heftschwerpunkt „Sicherheit"

Das große Special in dieser Ausgabe dreht sich auf 32 Seiten und in zehn Beiträgen um das Thema „Sicherheit durch Linux" (ab Seite 24). Livesysteme zum Surfen, Systeme für Reparaturen und Virensuche, Routerprojekte und Klonprogramme auf Linux-Basis erhöhen die Sicherheit für das gesamte Netzwerk und für Windows- oder Mac-Rechner. Um das Thema für alle Internetbelange und für den kompletten Heimnetzschutz abzurunden, startet das Special mit allgemeinen Sicherheitsmaßnahmen für Router und Webbrowser.

Die Heft-DVD: Vier Ubuntus 18.04 und viel mehr

Die Liste rechts zeigt alle auf DVD enthaltenen Systeme und Inhalte. Um ein Livesystem zu starten, legen Sie die DVD ins Laufwerk und booten den Rechner von DVD. Beim Start eines Systems von der Heft-DVD bleiben Ihre Festplatte und das dort installierte Betriebssystem unberührt. Die meisten Systeme liegen auch als ISO-Image auf Heft-DVD (im Verzeichnis „/Image-Dateien"). Damit haben Sie die Möglichkeit, die Systeme selbst auf CD/DVD oder USB-Stick zu schreiben. ■

AUF DVD

10 Ubuntu Mate 18.04 LTS *(64 Bit)*
Ubuntu mit Mate-Desktop

11 Xubuntu 18.04 LTS *(64 Bit)*
Ubuntu mit XFCE-Desktop

13 Lubuntu 18.04 LTS *(32 Bit)*
Ubuntu mit LXDE-Desktop

12 Bunsenlabs „Deuterium" *(32 Bit)*
Schlanke Debian-Variante

68 LinuxWelt-Rettungs-DVD *(32/64 Bit)*
Neue Version 6.2.1 des Livesystems

13 Tiny Core 9.0 *(32 Bit)*
Minimales Surf- und Livesystem

56 Ubuntu 18.04 LTS *(64 Bit)*
Hauptausgabe mit Gnome

„Extras und Tools"
Boothelfer und Hardwareanalyse: Supergrub, Memtest, Hardware Detection Tool (HDT)

LinuxWelt Digital XXL (PDF)
305 Seiten technische Grundlagenartikel und Distributionsratgeber

LinuxWelt Digital „Server" (PDF)
67 Seiten über Serverrollen für Linux mit Optimierungs- und Sicherheitstipps

„Wahl-O-Mat"
Informationssystem zur Auswahl der passenden Linux-Distribution

Ubuntu Mate 18.04

Mit dieser LTS-Ausgabe macht sich Ubuntu Mate (64-Bit-Variante auf Heft-DVD) fit für die Zukunft: Der neue Mate-Desktop ist jetzt nicht mehr nur ein Nachgedanke zu Gnome 2, sondern kann jetzt auch mit Hi-DPI-Auflösungen aktueller Monitore umgehen.

VON DAVID WOLSKI

Modernisierter Mate-Desktop: Ubuntu Mate 18.04 ersetzt im Panel das übliche Anwendungsmenü mit dem neueren „Brisk Menu“. Der Willkommensbildschirm ist ein Markenzeichen der Distribution.

Ubuntu Mate erfüllt nun mehrere Rollen: Zum einen ist es die einsteigerfreundlichste Ubuntu-Variante, zum anderen ist das offizielle Ubuntu-System auch eine ausgereifte Alternative für erfahrene Anwender, die Gnome 3 mit seinen eingeschränkten Anpassungsmöglichkeiten und gewöhnungsbedürftiger Bedienung ablehnen. Dass der Distribution dieses Kunststück gelingt, liegt an den Fortschritten des Mate-Desktops, der hier in Version 1.20 enthalten ist, aber auch an Nettigkeiten, die nur Ubuntu Mate mit an Bord hat. So begrüßt den Anwender nach dem ersten Boot der inzwischen zum Markenzeichen gewordene Willkommensbildschirm mit Übersicht und Konfigurationshilfen wie der „Software Boutique“, die populäre Programme mit wenigen Klicks nachinstalliert. Diese freundliche Begrüßung ist ein echter Exportschlager geworden, den andere Ubuntu-Ausgaben übernehmen. So hat die Budgie-Version Ubuntus einen Fork des Willkommenbildschirms übernommen.

Zugleich alt und neu

Natürlich bleibt der Mate-Desktop eine konservative Antwort auf die Wege von Gnome 3 und wurde unter Linux Mint erwachsen und dann auch schon wieder alt, da moderne Funktionen fehlten. Diese traditionelle Desktopumgebung verdient im Kontext des Wechsels von Unity zu Gnome 3 in der Hauptausgabe Ubuntu aber wieder mehr Aufmerksamkeit und wird ihrem Anspruch gerecht: Gnome-3-Anwendungen fügen sich nun perfekt in den Desktop ein. Mate erkennt jetzt selbständig anhand der Monitorauflösung, ob es auf einem hochauflösenden Bildschirm läuft, und passt den Skalierungsfaktor automatisch an. Momentan kann der Vergrößerungsfaktor den Wert 1 (normaler Monitor) oder 2 (Hi-DPI) annehmen. Als einer der ersten alternativen Desktops, die nicht direkt von Gnome 3 abstammen, ist Ubuntu Mate damit fit für neue PCs und Notebooks.

Ein wenig Meuterei

Wer Unity vermisst und in den Gnome-Erweiterungen von Ubuntu 18.04 keine Entsprechung sieht, kommt mit Ubuntu Mate dem gewohnten Unity-Layout wieder ein Stück näher: Unter „Einstellungen → MATE Tweak → Leiste → Leisten“ gibt es überarbeite Optionen zur Anordnung der Desktopelemente. Die Einstellung „Mutiny“ klemmt das Mate-Panel im Stil von Unity mit großen Symbolen an den linken Bildschirmrand. Das Anwendungsmenü verwandelt sich dabei in eine bildschirmfüllende Übersichtsseite aller installierten Anwendungen. Generell arbeitet Mate auch ohne 3D-fähigen Grafikchip und durch weitere Aufräumarbeiten im Code, der von Gnome 2 geerbt wurde, haben sich auch die CPU-Anforderungen reduziert. Wer aber eine leistungsfähige GPU oder Grafikkarte im PC hat, braucht auf Effekte nicht zu verzichten: Aufwendigere 3D-Effekte lassen sich mit einem Wechsel zum mitgelieferten Fenstermanager Compiz per Klick in „MATE Tweak“ unter „Fenster → Fenster Verwaltung“ aktivieren. Neben KDE ist Mate damit speziell in dieser Distribution einer der anpassungsfähigsten Linux-Desktops geworden, erfordert aber bei weitem nicht so viel Einarbeitungszeit.

Ubuntu Mate im Stil von Unity: Diese Einstellung in „MATE Tweak“ bildet die Aufteilung von Unity ab, falls gewünscht auch mit Head-up-Display, das Menübefehle anzeigt.

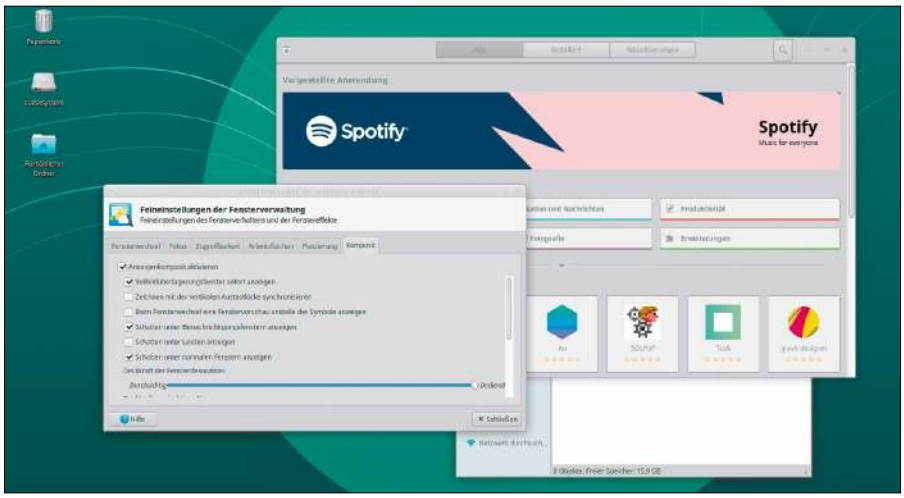
Website: *https://ubuntu-mate.org*
Dokumentation: *https://ubuntu-mate.org/about*

Xubuntu 18.04

Zwar ist es um den XFCE-Desktop, der in dieser offiziellen Ubuntu-Ausgabe im Mittelpunkt steht, in den letzten Monaten still geworden. Trotzdem kann Xubuntu 18.04 (64-Bit-Version auf Heft-DVD) mit etlichen Verbesserungen glänzen.

VON DAVID WOLSKI

Von wegen angestaubt: Xubuntu präsentiert einen aufgeräumten, gelungenen Desktop auf der Basis von XFCE. Diese oft reizlose umgesetzte Arbeitsumgebung zeigt sich hier dank der Anpassungen der Xubuntu-Entwickler von seiner besten Seite. Dafür sorgen in der vorliegenden LTS-Ausgabe 18.04 auch neue Apps im Panel. In vertikaler Position macht das Panel den Desktop auch zu einer guten Wahl für Notebooks, die kein Gnome mehr stemmen können. XFCE bleibt in Sachen Hardwarehunger gewohnt bescheiden.



Bescheiden, aber nicht anspruchslos: Der XFCE-Desktop hat länger kein größeres Update mehr bekommen. Trotzdem gibt es in Xubuntu 18.04 überlegte Ergänzungen und Erleichterungen.

Extraschlankes XFCE

Im Vergleich zu Gnome, KDE, aber auch dem alternativen Mate-Desktop ist XFCE zurückgefallen: Das letzte größere Update XFCE 4.12 erschien vor drei Jahren. Die Entwicklung ist zwar nicht stehengeblieben, geht aber nur langsam voran. Die neuen Herausforderungen sind für den XFCE-Desktop nicht weniger geworden: Die komplette Unterstützung des Gnome-Toolkits GTK3 und die Skalierung grafischer Elemente auf Hi-DPI-Monitoren sind Aufgaben, die XFCE noch vor sich hat. Aktuelle Gnome-Anwendungen können sich mittlerweile unter XFCE sehen lassen, bei sehr hohen Auflösungen muss der Desktop aber passen. Aber das ist auch so gar nicht die anvisierte Hardware, für die sich Xubuntu hübsch macht. Diese offizielle Ubuntu-Ausgabe mit Support bis 2021 braucht keinen aktuellen PC, um ordentlich zu laufen. System plus Desktop kosten deutlich unter 400 MB RAM. Das ist noch ein Stück weniger, als Ubuntu Mate verlangt.

Neues am Desktop

Im Panel gibt es zur Lautstärkekontrolle ein neues Pulse-Audio-Applet, das auch Steuerelemente für gerade laufende Mediaplayer anzeigt. Ein detaillierter Pulse-Audio-Mixer ist nur noch ein Klick entfernt und ein Klick mit der mittleren Maustaste auf das Symbol im Panel lässt den Ton sofort verstummen. Gleich links daneben haben nun die einzelnen Symbole in ihren Eigenschaften die Option bekommen, Icons im Panel zu verstecken. Notebookanwender dürfen sich über ein neues Applet zur Energieverwaltung freuen. Ein Klick darauf kann im „Präsentationsmodus“ den Bildschirmschoner bei Bedarf deaktivieren.

Das ausklappende Anwendungsmenü ist wie üblich das erweiterte, durchsuchbare „Whisker Menu“. Neu ist hier der überarbeitete Menüeditor, welcher sich bei einem Rechtsklick über „Menü bearbeiten“ öffnet. Dieser Editor macht nicht nur das Sortieren und Anlegen neuer Einträge einfacher, sondern kann auch das Menü nach fehlerhaften Verknüpfungen durchsuchen und neu angelegte Verknüpfungen auf ihre Funktion testen.

Xubuntu enthält einen Mix an vorinstallierten Programmen, die eigene Tools, Programme von Ubuntu Mate und typische Gnome-Anwendungen kombinieren. So ist der PDF-Viewer nun das von Mate bekannte Atril und auch der Taschenrechner und das Packprogramm stammen von den Kollegen. Diese Programme machen sich unter XFCE mit seiner nicht ganz fertigen GTK3-Unterstützung besser als die Pendants von Gnome. Allerdings dient zur grafischen Paketverwaltung auch hier das Programm „Gnome Software“. Xubuntu ist wie seine Verwandten auf die Verwendung von Snap-Paketen vorbereitet.

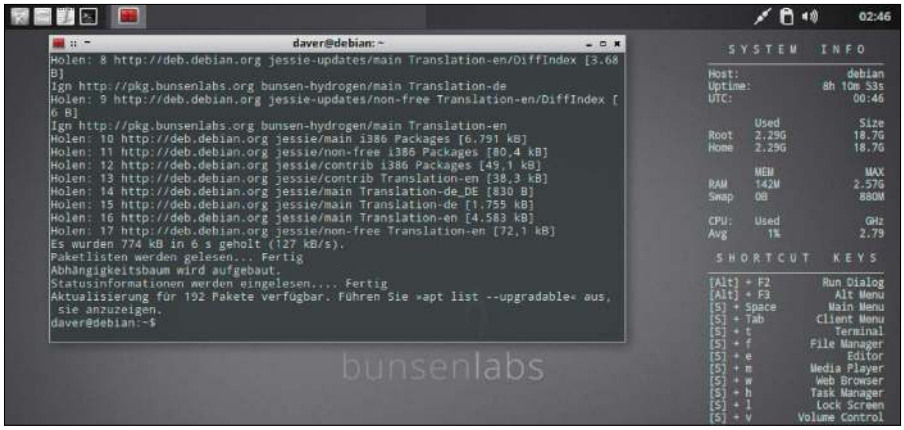
Der neue Menüeditor Menulibre macht es einfach, die Liste der Anwendungen zu bearbeiten. Neue Verknüpfungen lassen sich an Ort und Stelle testen.

Website: *www.xubuntu.org*
Dokumentation: *https://wiki.ubuntu.com/Xubuntu*

Bunsenlabs „Deuterium“

Darf es etwas weniger sein? Also weniger Desktop, dafür mehr Platz für das Wesentliche, nämlich für laufende Anwendungen. Diesen Ansatz verfolgt das Debian-System Bunsenlabs „Deuterium“ (32-Bit-Version auf Heft-DVD) überzeugend.

VON DAVID WOLSKI



Desktop als Nebensache: Bunsenlabs ist der Nachfolger des einst beliebten „Crunchbang“ mit stark reduziertem Openbox-Desktop. Als Basis dient ein Debian 8 mit Anpassungen.

Während einige Linux-Distributionen einen Desktop wie Gnome oder KDE mit Effekten, Erweiterungen und ausgefeilter Grafik präsentieren, pflegt Bunsenlabs eine äußerst zurückhaltende Arbeitsumgebung. Warum auch nicht – schließlich laufen auf Rechnern ohne hochauflösenden Monitor sowieso die meisten Anwendungen in bildschirmfüllenden Fenstern. Der Desktop von Bunsenlabs, dessen Name sich vom Bunsenbrenner in chemischen Labor ableitet, bleibt nicht nur farblich unaufdringlich im Hintergrund. Zielgruppe sind dabei eher fortgeschrittene Debianer. Um den Desktop kümmert sich der schlanke Window-Manager Openbox und das Anwendungsmenü wird mit schlichtem Rechtsklick auf den Desktophintergrund geöffnet. Für eine Leiste am oberen Bildschirmrand mit einigen Programmverknüpfungen und einer Fensterleiste sorgt das Tool Tint2 aus dem Fundus von Openbox. Diese Leiste ist zwar noch direkt über Konfigurationsdateien zu steuern, aber es gibt auch das grafische Konfigurationstool tint2conf. Auf der Arbeitsoberfläche zeigt der Systemmonitor Conky die Auslastung und einige nützliche Tastenkürzel an.

Gerade genug Debian

Bunsenlabs ist ein Debian 8 „Jessie“ und nutzt dessen Paketquellen, die mit eigenen Repositories ergänzt werden. Zwar ist Debian schon bei Version 9 angelangt, aber diese Debian-Ausgabe wird trotzdem noch mindestens bis ins Jahr 2020 mit Updates versorgt. Das bedeutet allerdings, dass es in Bunsenlabs keine besonders neuen Programmversionen gibt, sondern stabile und lange getestete Pakete. So ist der Kernel wie im regulären Debian noch bei 3.16, Libre Office ist noch auf dem Stand 4.3.3 und als Webbrowser dient Firefox 52 ESR. Thunar, der Dateimanager von XFCE, kommt standardmäßig auch in Bunsenlabs zum Einsatz. Anders als bei einem Debian von der Stange ist hier schon der Videoplayer VLC enthalten und die proprietären Firmwarepakete aus dem Non-Free-Repository. Das vereinfacht auch die Verbindung mit WLANs ungemein, da so mehr WLAN-Chips ab Werk unterstützt werden.

Um das fertige System möglichst schlank zu halten, ist neben der Grundausstattung nur wenig Software vorinstalliert: So ist beispielsweise der Libre Office Writer vorhanden, aber die anderen Programme des Büropakets müssen bei Bedarf nachinstalliert werden. Der Reiz des minimalen Systems ist, gezielt nur die benötigten Anwendungen einzurichten. Als grafische Paketverwaltung ist Synaptic enthalten.

Leiste anpassen: Für Tint2, das die Leiste am oberen Rand darstellt, gibt es mit tint2conf ein eigenes grafisches Konfigurationsprogramm.

Separate Installation

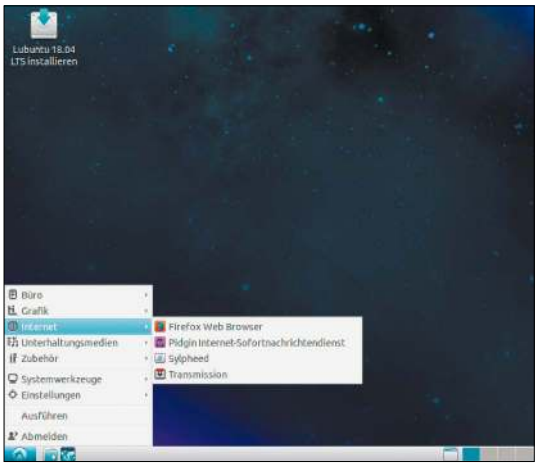
Bunsenlabs liegt seiner in der 32-Bit-Version auf DVD, denn es fühlt sich auch auf alten Rechnern noch wohl. Bei der Installation benötigt es mindestens drei GB Speicherplatz auf der Festplatte. Das Livesystem dient zur Demonstration des Desktops und bringt einen separaten Installer mit. Wie bei Openbox nicht anders zu erwarten, sind die Hardwarevoraussetzungen gering: Der Desktop verlangt nur nach rund 200 MB RAM. Der Installer ist von Debian übernommen und wird über einen separaten Eintrag im Multibootmenü der Heft-DVD gestartet, aber nicht aus dem Livesystem heraus.

Website: *www.bunsenlabs.org*
Dokumentation:
www.bunsenlabs.org/installation.html

Lubuntu 18.04

VON DAVID WOLSKI

Für den Desktop ist Lubuntu die leichteste Ubuntu-Ausgabe in Sachen Hardwareansprüchen. Dieses offizielle Ubuntu spricht speziell jene Anwender an, die kein schmückendes Beiwerk auf dem Desktop brauchen oder sehr betagte Rechner nicht mit anspruchsvolleren Desktops quälen wollen. Deshalb ist Lubuntu 18.04, das in dieser LTS-Ausgabe drei Jahre lang Updates bekommen wird, wieder in der 32-Bit-Ausgabe auf Heft-DVD. LXDE selbst bietet einen reduzierten Desktop samt Taskleiste mit Applets für Sound, Netzwerk und Uhrzeit sowie ein Startmenü. Die anderen mitgebrachten Anwendungen sind von Gnome und XFCE übernommen, wobei es auch ganz beliebige Programme aus dem Ubuntu-Fundus zum Installieren gibt. Dies klingt nach Flickwerk, aber dem Entwicklerteam ist es über die Jahre gelungen, einen konsistenten und ansehnlichen Desktop aus den Komponenten um LXDE zu gestalten.

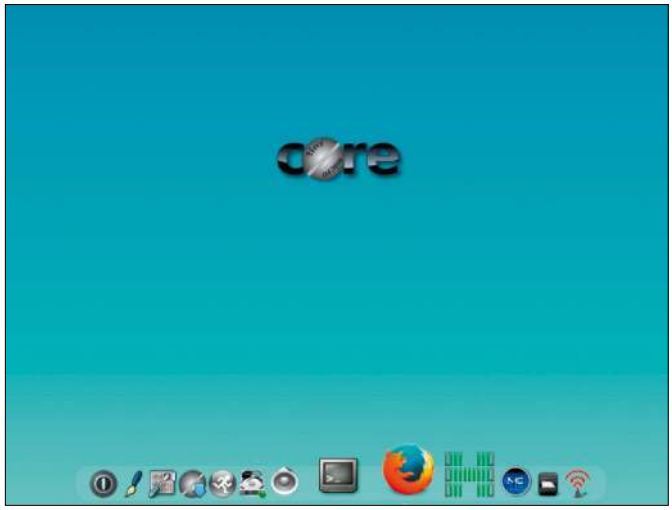


LXDE ist gewohnt genügsam: Bibliotheken für Gnome- oder KDE-Anwendungen werden nur bei Bedarf geladen. Alle sonstigen Programme und Desktopkomponenten leiht sich LXDE von anderen Arbeitsumgebungen, wobei es schlanken Alternativen stets den Vortritt gibt: Dateimanager ist Pcmanfm 1.2.5, als Browser ist Firefox 59 dabei. Lubuntu verzichtet, anders als Xubuntu, auf Libre Office, um stattdessen das leichtgewichtige Abiword und Gnumeric anzubieten. Libre Office 6.0 lässt sich natürlich nachinstallieren. Zur Paketverwaltung stehen Synaptic und das Gnome Software Center bereit. Als Videoplayer ist in Lubuntu erfreulicherweise MPV vorinstalliert, der auf schwachen Rechnern deutlich flotter arbeitet als VLC.

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

Tiny Core 9.0

VON DAVID WOLSKI



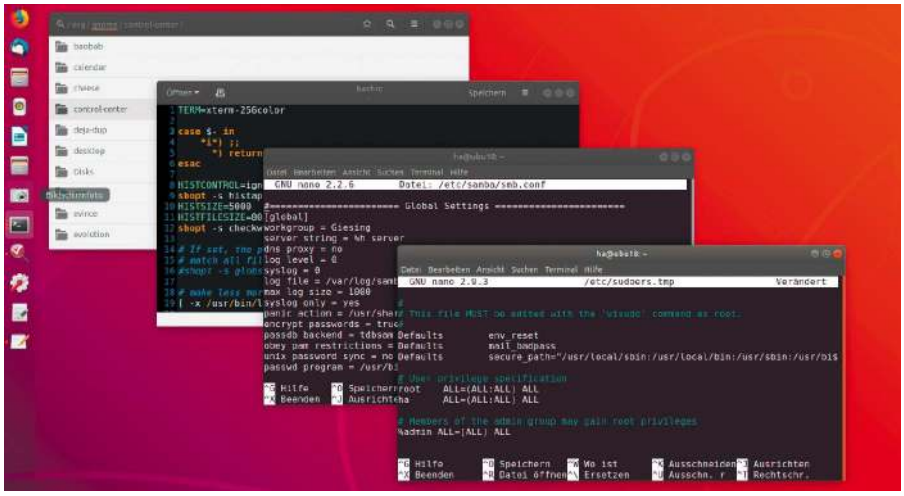
Das winzige Livesystem ist eine nützliche ausbaufähige Surfstation: Firefox ESR 52 ist vorinstalliert sowie Treiber für verbreitete WLAN-Chips, um möglichst flott online zu sein. Im Auslieferungszustand ist Tiny Core üblicherweise kein schlüsselfertiges System. Anwender müssen benötigte Programme nach dem Start des Livesystems erst noch selbst nach jedem Start über den mitgelieferten Paketmanager temporär installieren, inklusive Treiber und Tools für die Verbindung zu WLAN-Verbindung.
Diese Ausstattung ist für normale Anwendungsszenarios recht mager und die LinuxWelt-Edition von Tiny Core auf DVD (32 Bit) hat daher die wichtigsten Komponenten schon im Gepäck, um per Ethernet oder WLAN mit einem aktuellen Firefox 52 ESR online zu gehen. Die LinuxWelt-Edition enthält Firmwarepakete für die verbreiteten Wireless-Chipsätze von Intel, Atheros, Broadcom, Realtek, Marvell, Qlogic, Texas Instruments, Eagle und Neterion. Um eine WLAN-Verbindung aufzubauen, klickt man im unteren Dock auf das rote Wireless-Symbol und gibt im Terminalfenster manuell die Verbindungsdaten für das ausgewählte WLAN ein. Die deutsche Tastaturbelegung ist voreingestellt, das System selbst liegt aber in Englisch vor.
Als Dateimanager dienen Pcmanfm und der Midnight Commander. Der Open-SSH-Client für Netzwerkverbindungen erlaubt den Zugriff auf andere Linux-PCs über SSH für den Datenaustausch. Die Neuerungen zur letzten Version betreffen Programmversionen und den Kernel, der auf 4.14 aktualisiert ist. Tiny Core läuft auch noch auf sehr alten Rechnern.

Website: *www.tinycorelinux.net*
Dokumentation:
http://distro.ibiblio.org/tinycorelinux

Konfigurationsdateien unter Linux

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

VON HERMANN APFELBÖCK



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

Die typischen Pfade der Konfiguration

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

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

Trotzdem gibt es Situationen, in denen es hilfreich ist, die betreffenden Konfigurationsdateien und Ordner aufzusuchen: Wenn eine Software nicht mehr startet oder unbenutzbar verkonfiguriert wurde, können Sie unter „/home/[user]/“ alle benutzerbezogenen Einstellungen löschen. So wird etwa ein Chrome-Browser nach vollständigem Löschen des Ordners „/home/[user]/.config/google-chrome“ wieder so starten, als wäre er eben neu installiert. Nicht bei jeder Software ist die Benutzerkonfiguration so eindeutig in einem Ordner oder einer Datei zu lokalisieren: Einstellungen für den KDE-Desktop sind nicht nur unter „/home[user]/.kde“ zu finden, sondern auch unter „/home[user]/.config/menus“ und „/home[user]/.local/share/“. Auch die Einstellungen des Cinnamon-Desktops (Linux Mint) verteilen sich auf die Ordner „/home[user]/.cinnamon“, „/home[user]/.config/cinnamon-session“ sowie „/home/[user]/.config/dconf“, wobei der wichtigste dconf-Teil nicht lesbar ist (binär). Da die dconf-Datei auch Anweisungen für andere Software enthalten kann, ist deren komplettes Löschen nicht ratsam. Dazu unten gleich mehr …

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

Gconf- und dconf-Einstellungen

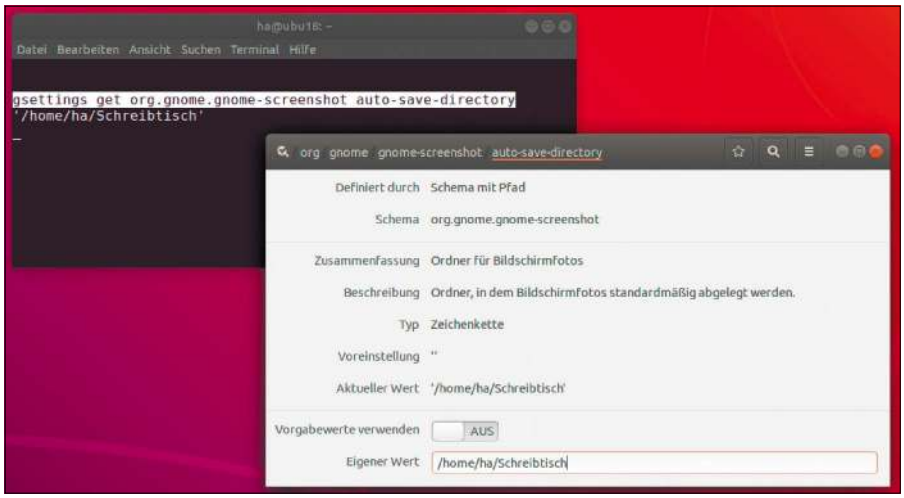
Wer die komplette Benutzerkonfiguration einsehen will oder muss, kommt an speziellen Hilfswerkzeugen nicht vorbei. Wie am obigen Beispiel Cinnamon schon angesprochen, liegt nicht alles in klar lesbaren Textdateien vor. Bei Gnome-affinen Oberflächen (und das ist die Mehrzahl mit Gnome, Cinnamon, Unity,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

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

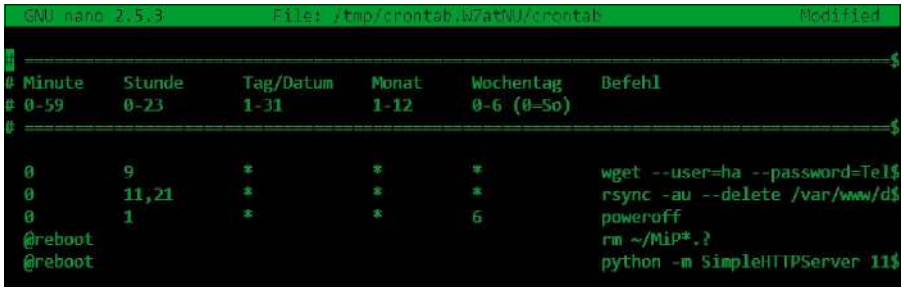
Das neuere, mit Gnome 3 eingeführte dconf-Konzept benutzt statt XML-Dateien die Binärdatei „/home/[user]/.config/dconf/[user]“. Zum manuellen Lesen und Bearbeiten dieser Konfigurationszentrale dient das grafische Tool dconf-editor, das in der Regel nicht vorinstalliert, aber mit dem gleichnamigen Paketnamen überall erreichbar ist. Wichtigere Schnittstelle für Softwareinstallationen und für automatische Anpassungen ist aber das Kommandozeilentool gsettings, das sich ebenfalls überall nachrüsten lässt. Die Syntax für die jeweilige Einstellung folgt dabei exakt der Hierarchie, wie sie der dconf-editor anzeigt – etwa:

```
gsettings set org.gnome.desktop.
  background picture-uri /home/ha/
  bild.png
```

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



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

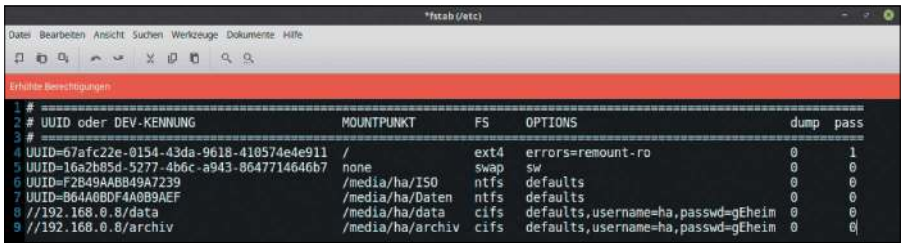


Persönlich kommentierte und sauber formatierte „crontab“: Die an sich leserunfreundliche Konfigurationsdatei wird damit sofort übersichtlicher.

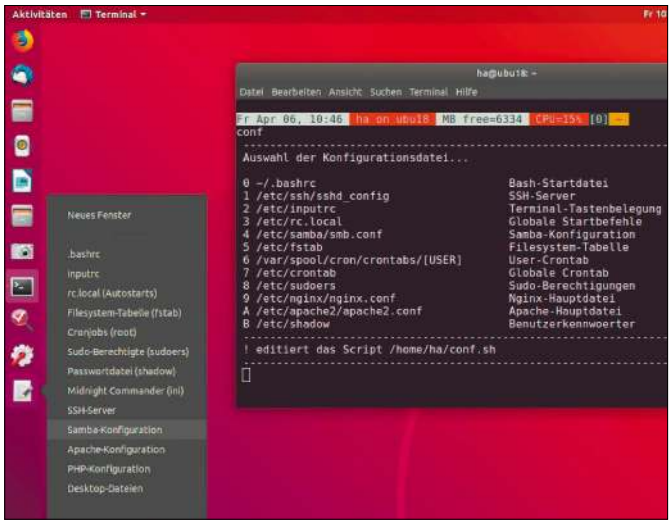
Kommentierung und Formatierung von Konfigurationsdateien

Welche Anweisungen eine Software in ihrer Konfigurationsdatei erwartet, ist so unterschiedlich wie die Software selbst. Einheitlich ist nur, dass je eine Zeile eine abgeschlossene Anweisung darstellt. Es gibt unstrukturierte Dateien, wo es keine Rolle spielt, an welcher Stelle eine Anweisung steht, so etwa in der SSH-Konfiguration über „/etc/ssh/sshd_config“. Andere Konfigurationsdateien wie etwa die Samba-Konfiguration „/etc/samba/smb.conf“ oder die „desktop“-Dateien unter „/usr/share/applications“ gliedern in Sektionen, die unterschiedliche Anweisungen erwarten. Wer sich dann mit den genauen Details beispielsweise einer „smb.conf“ beschäftigt, liest häufig den lapidaren Hinweis, dass diese Datei „gut kommentiert“ sei. Das stimmt einerseits, andererseits nicht.

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



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



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

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

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

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

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

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

Terminalzentrale für Konfigurationsdateien

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

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

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

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

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

und dann mit

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

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

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

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

Grafische Zentrale für Konfigurationsdateien

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

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

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

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

Kleine Tipps zu Konfigurationsdateien

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

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

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

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

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

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

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

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

WICHTIGE LINUX-KONFIGURATIONSDATEIEN

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

Umpacken! Linux-Pakete konvertieren

Am schnellsten lassen sich Linux-Programme mit dem Paketmanager der Distribution installieren. Fehlt ein benötigtes Programm, muss es aus dem Quelltext kompiliert werden. Die Alternative: Viele Binärpakete lassen sich konvertieren.

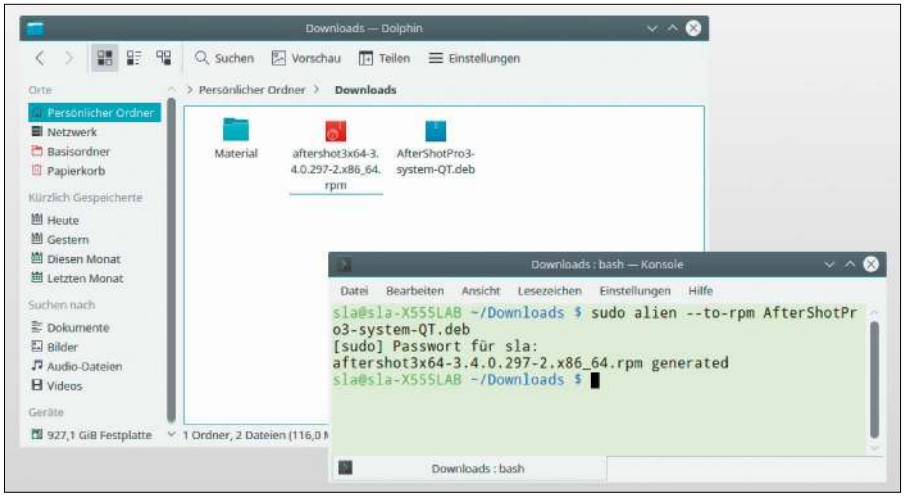
VON STEPHAN LAMPRECHT

Es gibt in jeder Distribution einen Bereich, der erstaunlicherweise von den Entwicklern seit Jahren kaum angetastet wird. Die Rede ist von der Paketverwaltung, die sich um die Verwaltung der installierten Anwendungen kümmert. Und so gibt es trotz allen Wandels nach wie vor zwei dominierende Paketformate, in denen Programme erscheinen: das ursprünglich von Red Hat entwickelte RPM, ferner das unter Ubuntu & Co. genutzte Debian-Format (DEB).

Alien – der Name ist fast Programm

Wie jeder fortgeschrittene Anwender aus eigener Erfahrung weiß, ist das Thema Paketmanagement nicht ganz trivial. Wer etwa eine Distribution mit Long Time Support einsetzt, kann leider nicht einfach eine aktuellere Programmversion aus dem aktuellen Release seiner Distribution ersetzen. Und bietet ein Entwickler seine Anwendung im RPM-Format an, müssen sich Ubuntu-Nutzer auf die Suche nach Alternativen machen oder den Quelltext kompilieren. Das ist auf dem Papier zwar nicht schwer, aber häufig verläuft das Kompilieren nicht reibungslos. Dann sind die entsprechenden Fehlermeldungen und Hinweise gewissenhaft abzuarbeiten, damit am Ende ein installierbares Paket herauskommt. Eine Alternative zum Kompilieren kann der Versuch sein, ein Paketformat in ein anderes zu konvertieren.

Für diese Aufgabe gibt es mit „Alien“ ein Programm, das für beide Paketplattformen angeboten wird und somit zwischen den



Die Syntax des Konverters Alien ist überschaubar. Nach erfolgreicher Konvertierung liegen die beiden Pakete in den unterschiedlichen Formaten einträchtig nebeneinander.

Formaten vermittelt. Sie können es auf Ihrem System einfach über die Paketverwaltung selbst installieren, unter Ubuntu beispielsweise so:

```
sudo apt install alien
```

Der Umgang mit dem Programm ist nicht schwierig, findet aber ausschließlich auf der Kommandozeile statt. Wenn Sie die Anwendung „myprog“ im RPM-Format in das Debian-Format konvertieren wollen, wechseln Sie im Terminal zunächst in den Ordner, in den Sie das Fremdpaket heruntergeladen haben. Dann führen Sie dieses Kommando aus:

```
sudo alien myprog.rpm
```

Nach der Konvertierung liegt im gleichen Verzeichnis ein DEB-Paket vor, das installiert werden kann. Allerdings kann Alien keine Wunder vollbringen. Die Quelle und das Ziel sollten der gleichen Architektur entsprechen. Wer versucht, ein RPM-Paket für 32 Bit in das 64-Bit-Format von Debian zu konvertieren, kann keinen Erfolg haben. Eine Garantie für die reibungslose Installation gibt es generell nicht, andererseits eine generelle Vorsichtsmaßregel: Sie sollten keinesfalls versuchen, wichtige Systemprogramme wie zum Beispiel init oder libc umzuwandeln. Damit riskieren Sie ein nicht mehr funktionierendes System, das sich schwerlich wieder retten lässt. Kandidaten für die Alien-Konvertierung sind eher die typischen Anwendungsprogramme.

Kann das von Alien konvertierte Paket nicht installiert werden, sind meistens fehlende Abhängigkeiten daran schuld. In diesem Fall sollten Sie die Rückmeldungen des Systems kontrollieren, weil sich darin oft Hinweise auf Pakete finden, die erst noch installiert werden müssen, bevor ein neuer Anlauf unternommen werden kann. Deswegen ist es auch empfehlenswert, das

Debian-Paket nicht mit der grafischen Oberfläche zu installieren, sondern stattdessen mit dem Terminal, das mehr Informationen liefert:

```
sudo dpkg -i myprog.deb
```

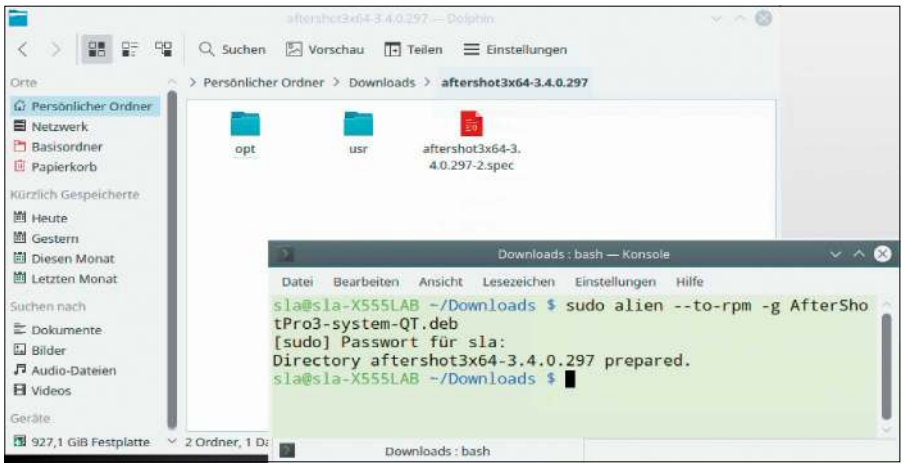
Wenn Sie sich den Zwischenschritt sparen wollen, ist es mit Alien möglich, das konvertierte Paket unmittelbar zu installieren. Dazu muss dem Aufruf lediglich der Schalter „-i“ hinzugefügt werden:

```
sudo alien -i myprog.rpm
```

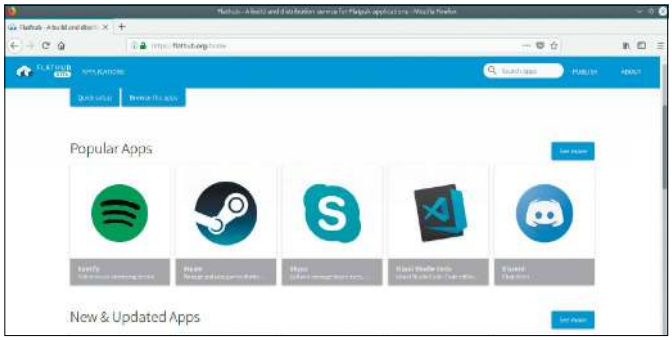
Alien ist so voreingestellt, dass es die Pakete automatisch in das Debian-Format umwandelt. Wer umgekehrt mit einer Distribution arbeitet, die auf RPM basiert, muss das Zielformat explizit mitteilen. Das kann mit dem Schalter „-r“ oder auch „--to-rpm“ erledigt werden:

```
sudo alien --to-rpm programm.deb
```

Fortgeschrittene Anwender und Profis schätzen die Option „-g“. Die Abkürzung steht für „Generate“ und weist Alien an, kein neues Paket zu erstellen, sondern ein Verzeichnis anzulegen, in das der spätere Paketinhalt abgelegt wird. Wer sich mit den Tiefen von Linux auskennt, kann so noch vor dem Packen des Pakets eingreifen, um Anpassungen vorzunehmen.



Um vor dem Packen zu analysieren, was da entsteht, hilft der zusätzliche Schalter „-g“. Dann legt Alien die Dateien in der späteren Struktur des Pakets ab.



Projekte wie Flatpak, das beispielsweise bei Linux Mint bereits an Bord ist, gehen neue Wege, damit Entwickler nicht mehrere Architekturen pflegen müssen.

Neue Formate am Horizont

Der Ansatz mit den Softwarepaketen stellt nicht nur den Endanwender gelegentlich vor Probleme, sondern mehr noch den Softwareentwickler. Wer seine Anwendungen für die populärsten Distributionen anbieten möchte, muss die verschiedenen Paketversionen erstellen und dann auch noch aktuell halten. Ein Paketformat für alle Plattformen – das ist der Grundgedanke einer ganzen Reihe von neuen Projekten. Die aktuell wohl populärsten sind Flatpack und Snap. Der Entwickler einer Anwendung muss sich bei diesem Ansatz nur darum kümmern, seine Software in einem der neueren Formate anzubieten. Flatpak und Snap stellen dann eine separate Systemumgebung zur Verfügung, die sich in das jeweilige Hostsystem (Ubuntu, Suse etc.) integriert. Bei Flatpak etwa laufen die Programme in einer Art von Container, den die Entwickler des Formats als Sandbox bezeichnen.

Jedes Flatpak-Programm nutzt seine eigene Sandbox. Davon bemerkt der Anwender nichts. Er installiert sich Flatpak auf seiner Distribution und kann dann bereits aus einer ganzen Reihe von Programmen wählen, die im neuen Format angeboten werden. Das funktioniert auch über einen Aufruf des Systems direkt aus dem Browser heraus. Unter *https://flathub.org/home* gibt es eine Art Schaufenster, das Informationen zu den Programmen bereithält. Einen ganz ähnlichen Weg geht Snap, dessen Entwickler unter *https://snapcraft.io/* über die Einrichtung des Systems und die verfügbaren Anwendungen informieren. ■

FÜR BASTLER: AB IN DEN KARTON

Einen neuen Ansatz nutzt die Anwendung „Karton“. Dahinter steckt der Gedanke, nicht einzelne Pakete in ein anderes Format zu konvertieren, sondern Anwendungen oder ganze Distributionen regelrecht einzupacken, um diese dann auf einem anderen System zu betreiben. Das funktioniert ähnlich wie eine virtuelle Maschine. Während diese aber wie eine Kapsel vom Rest des Systems getrennt ist, nutzt Karton als Basis Docker und wird „transparent“ ausgeführt. Damit ist gemeint, dass die per Karton gepackten Anwendungen Zugriff auf das lokale Dateisystem haben. So ist es möglich, nahtlos mit den externen Programmen auf dem Hostsystem zu arbeiten. Momentan beschränkt sich die erste Version von Karton auf Programme für die Kommandozeile. Anwendungen für grafische Oberflächen sind aber in Planung. Das Zusammenpacken mittels Karton ist derzeit aber noch etwas für experimentierfreudige Naturen. Die Systemvoraussetzungen sind gering. Lediglich Python und Docker müssen installiert sein. Die Zusammenstellung der eigenen Distribution erfolgt ausschließlich über eine Textdatei, in der die Eigenschaften und benötigten Komponenten definiert werden. Trotzdem wird es spannend, den Fortschritt des Projekts zu verfolgen. Denn damit können künftig die Systemgrenzen für Linux-Programme leichter überschritten werden.

Der neue Raspberry Pi 3 B+

Der Ein-Platinen-Computer, der 2016 als Model 3 B erschien, hat ein signifikantes Update bekommen: Der neue Raspberry Pi 3 B+ bietet WLAN mit fünf GHz nach dem Standard 802.11ac, zudem stromsparendes Bluetooth 4.2 und Gigabit-Ethernet. Etwas mehr Prozessorleistung hat das neue Topmodell ebenfalls, das übrigens nicht wesentlich mehr als Vorgänger kostet (unter 40 Euro). Der System-on-Chip von Broadcom taktet jetzt mit bis zu 1,4 GHz.
Der Artikel zur Odroid-Platinenfamilie ab Seite 96 wirft einen genaueren Blick auf die neue Raspberry-Platine. ■

Nvidia: Adieu 32 Bit!

Es sind noch einige Monate, doch hat Nvidia jetzt schon angekündigt, dass Ende 2018 keine offiziellen Grafiktreiber mehr für 32 Bit erscheinen werden. Etwa zeitgleich will der Hardwarehersteller auch die Unterstützung für seine Grafikprozessoren der „Fermi"-Serie einstellen, die ursprünglich 2010 erschienen war. Dies betrifft alte Karten der Serien Geforce 400 und 500, die heute wohl nur noch in anspruchslosen Büro-PCs anzutreffen sind. Für Linux-Anwender mit alten Nvidia-Karten bedeutet dies, dass die Treiberversion 390.x die letzte sein wird. Funktionieren werden die Karten weiterhin, da die Nvidia-Treiber vorerst nicht aus den Repositories verschwinden und es zudem die freien Nouveau-Treiber in jeder Linux-Distribution gibt. ■

Kernel 4.17 will Strom sparen

Aufräumarbeiten und viel Neues im nächsten Linux-Kernel: Voraussichtlich im Juni wird Linus Torvalds Version 4.17 freigeben.

Die bisher geplanten Entwicklungen lassen darauf schließen, dass es eine der spannenderen Kernel-Ausgaben wird. Neben Ergänzungen gibt es seit langem wieder eine große Aufräumaktion im Code, die den Quellcode um 500 000 Zeilen verkleinern will. Betroffen sind davon vor allem alte obskure Prozessorarchitekturen, um die sich schon geraume Zeit niemand mehr gekümmert hat. Unter anderem verschwindet die 32-Bit-Risc-Unterstützung neben sieben weiteren Architekturen, die kaum noch eine Rolle spielen. Eine Überarbeitung der Leerlauf-Loops für ungenutzte Prozessorkerne verspricht einen geringeren Energiebedarf um mehr als zehn Prozent. Zudem lernt der Kernel, selbst mit TLS umzugehen (Transport Layer Security) und Daten über die eigene Crypto-API zu ver- und entschlüsseln. Bislang erledigten das externe Bibliotheken wie Open SSL oder Libre SSL. Erste Ansätze, TLS in den Kernel zu verlegen, gibt es schon seit Version 4.13. Aber jetzt nimmt die interne Verschlüsselungsfunktion Gestalt an. ■

Tuxedo: Notebooks ohne Intel ME

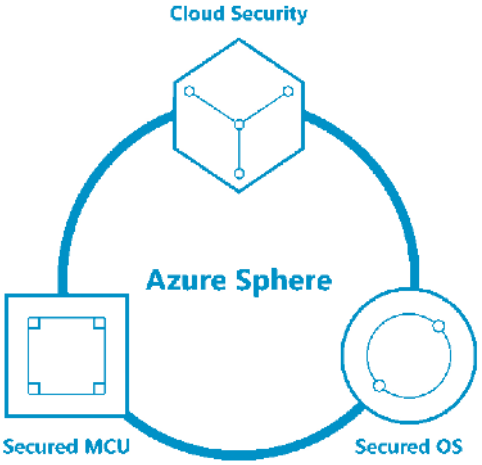
Nachdem einige Sicherheitslücken die Intel Management Engine (ME) heimgesucht haben, welche als Minibetriebssystem in zahlreichen Intel-Prozessoren enthalten ist, suchen OEMs und Systemhäuser nach Wegen, die Engine per Firmwarehack abzuschalten. Die ME ist von Intel nicht ausführlich dokumentiert, kann aber auf alle Daten des Computersystems zugreifen. Neben Dell fanden auch einige kleine Linux-affine Systemhäuser jetzt Möglichkeiten, Intels versteckte Schnittstelle auf ausgewählten Prozessoren zu deaktivieren. Tuxedo hat in seinem Notebook Infinity Book Pro 13 mit einem modifizierten Bios einen Schalter realisiert, der die Intel Management Engine per Bios-Einstellung stilllegt. Per Bios-Update gibt es den Schalter auch für bereits gelieferte Modelle des Infinity Book Pro 13. Bisher ist dieses Tuxedo-Notebook allerdings das einzige der OEMs mit dem neuen Bios-Schalter. ■

Red Hat Enterprise Linux 7.5

Mitte April hat Red Hat die neue Version des hauseigenen Red Hat Enterprise Linux (RHEL) veröffentlicht. Version 7.5 bringt die Administrationskonsole Cockpit in einer aufpolierten Fassung und zahlreiche Verbesserungen für den Betrieb des Systems in Rechenzentren und in der Cloud. Das System steht RHEL-Abonnenten zum Download bereit. Etwas später wird der freie Quellcode in Cent-OS einfließen. ■

Alle News von David Wolski

IoT: Microsoft setzt auf Linux



Ein Microcontroller für das „Internet der Dinge" (IoT) aus dem Hause Microsoft wird ganz offiziell mit einem modifizierten Linux-Kernel ausgestattet. Das Betriebssystem mit dem Namen „Azure Sphere OS" wird damit das erste Linux-System sein, das mit einem Microsoft-Produkt ausgeliefert wird. Laut Microsoft wird der Linux-Kernel mit Windows-Sicherheitsfunktionen kombiniert.

Der Microcontroller besteht aus mehreren ARM-Prozessoren und einem Wächter-Chip, der eine sichere Bootumgebung gewährleistet und den Netzwerkverkehr überwacht. Das Controllerdesign wird lizenzfrei sein; die Produktion der Hardware übernehmen Dritthersteller wie Mediatek. Die ersten Geräte sollten noch 2018 zusammen mit einem Developer Kit für Windows auf den Markt kommen. ■

Nextcloud in der Bundesverwaltung

An eine prominente Stelle hat es die private Cloudplattform Nextcloud im Zuge einer öffentlichen Ausschreibung geschafft: Der zentrale IT-Dienstleister der Bundesverwaltung hat sich bei der Bereitstellung und Synchronisation von Daten in einer Cloud für ein Konzept der Firma Computacenter und damit für Nextcloud entschieden. In Zukunft werden alle Behörden der Bundesverwaltung mit fast 300 000 Benutzerkonten auf Nextcloud Enterprise umgestellt. Vorangegangen war bereits ein Pilotprojekt mit Nextcloud im Jahr 2016, das die Machbarkeit einer sicheren, zuverlässigen Cloud mit der Open-Source-Software analysierte. Obwohl Nextcloud, so wie der Vorläufer Owncloud, in PHP geschrieben ist, konnte die Cloudlösung bei den Tests überzeugen. ■

SICHERHEITSNEWS

„Beep" ist böse

Eine kuriose, aber doch ernste Sicherheitslücke betrifft das Befehlszeilentool beep, das in Linux-Systemen einen Piepton über den Systemlautsprecher ausgibt. Für diesen direkten Zugriff auf die Hardware wird es mit dem Setuid-Bit installiert, damit beep bei jedem Aufruf automatisch root-Rechte erhält. Dies ist übliche Praxis, erfordert aber, dass ein Programm wirklich nur sehr eingeschränkte Aktionen ausführt. Bei beep war das nicht der Fall: User konnten sich mit dem Kommando root-Rechte besorgen. Die Lücke ist inzwischen behoben. Auf aktuellen Linux-Distributionen ist beep sowieso nicht mehr installiert. Die Entdecker des Problems machten sich dennoch einen Spaß daraus und erstellten im Stil prominenter Sicherheitslücken eine komplette Info-Webseite (*https://holeybeep.ninja*).

AMD: Verwundbare Chipsätze

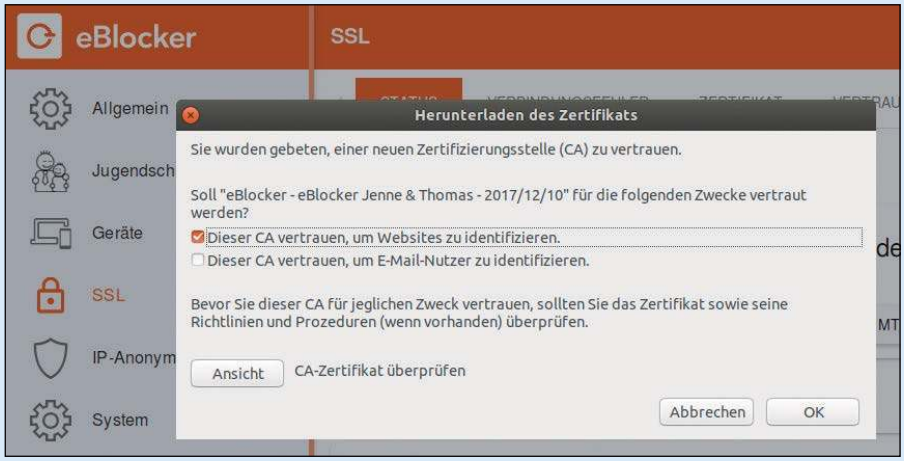
In einer ungewöhnlichen, scharf kritisierten Aktion hat eine bis dato unbekannte IT-Sicherheitsfirma einige ungepatchte Sicherheitslücken in AMD-Chipsätzen und CPUs beschrieben. Die Mitte April veröffentlichten Lücken sind in den Prozessoren Ryzen, Ryzen Pro, Epyc sowie dem Promontory-Chipsatz zu finden. AMD hatte vorab keine Notiz erhalten, wie dies in Sicherheitskreisen eigentlich üblich ist. Auch wurden die inzwischen von dritter Seite bestätigten Lücken anfangs nicht als CVE gemeldet, was erst einige Tage später passierte. Mittlerweile hat AMD alle zwölf der beschriebenen Bugs bestätigt und lässt Patches über Platinen- und PC-Hersteller verteilen.

TLS 1.3 kommt

Eine neue Version des Protokolls TLS (Transport Layer Security) verspricht eine bessere Verschlüsselung und höhere Geschwindigkeit für gesicherte Verbindungen wie HTTPS. Die Internet Engineering Task Force (IETF) hat die finalen Spezifikationen von TLS 1.3 Ende März veröffentlicht. Der neue Standard, der von Servern sowie Clientanwendungen unterstützt werden muss, reduziert die Schritte für einen initialen Verbindungsaufbau. Der neue strengere Standard behagt nicht allen: Der Bankensektor und die IT-Sicherheitsindustrie verlangen für die nachträgliche Untersuchungen übertragener Daten die Möglichkeit, einen Nachschlüssel (Master Key) zu hinterlegen. TLS 1.3 wird deshalb keinen leichten Stand haben. Firefox und Chrome/Chromium sowie der Webserver Nginx beherrschen TLS 1.3 bereits.

eBlocker Pro Privacy-Schutzbox selbst testen

Das Thema Datenschutz ist aktueller denn je: Der eBlocker Pro ist eine unkomplizierte Plug-and-Play-Lösung zum Schutz der Privatsphäre im Internet inklusive OpenVPN-Protokoll.
Mit LinuxWelt können Sie den „Privacy-Zauberwürfel“ auf einem Raspberry Pi oder Banana Pi selbst bauen und 90 Tage lang kostenfrei testen!



Ein Mausklick genügt: Mithilfe des eBlocker-Zertifikats überwacht die smarte Security-Box auf Wunsch auch verschlüsselte Verbindungen. Die SSL-Einstellungen können Sie für jedes im Netzwerk verfügbare Gerät individuell ein- und ausschalten.

von Thomas Raukamp

Facebook und kein Ende: Der aktuelle Skandal um das Analyse-Unternehmen Cambridge Analytica hat das Thema der Datensicherheit endgültig in der öffentlichen Diskussion ankommen lassen.
Spätestens jetzt ist klar: Wer seine Daten im Internet schützen will, muss selbst handeln, statt auf die Verschwiegenheit der Unternehmen und die Bemühungen der Internetanbieter zu setzen.

Trugschluss Linux-Sicherheit

Linux-Systeme gelten gemeinhin als besonders sicher – nicht ohne Grund, schließlich infizieren Computerviren vornehmlich Windows-PCs. Trotzdem sind auch Linux-Nutzer nicht vor dem Ausspähen etwa der IP-Adresse geschützt, die wie ein digitaler Fingerabdruck eine klar identifizierbare Spur Ihrer Aktivitäten im Netz legt.

Doch damit nicht genug: Unter der Oberfläche von weltweit 79 Prozent aller Webseiten greifen ausgeklügelte Tracking-Systeme ungeniert nach der Privatsphäre der Besucher – ganz gleich, welches Betriebssystem diese nutzen. Im Durchschnitt werkeln zwischen zehn und zwanzig Tracker im Hintergrund, um Informationen über das Konsumverhalten zu gewinnen und daraus ein möglichst feinmaschiges Persönlichkeitsprofil zu weben. Die in sozialen Online-Netzwerken wie Facebook und Twitter abgegriffenen persönlichen Informationen stellen somit nur die Spitze des Daten-Eisbergs dar.

Smarter Würfel für mehr Datensicherheit

Der eBlocker des gleichnamigen Hamburger Start-ups nimmt sich der beiden brennendsten Probleme im Datenschutz an: Die kleine weiße Box in der Größe eines Rubik-Zauberwürfels anonymisiert das Anwenderverhalten und schiebt Trackern und anderen Datenschnüfflern einen Riegel vor. Quasi nebenbei verbannt der eBlocker in seiner „Pro“-Variante auch noch lästige Onlinewerbung und macht so ressourcenfressende Browsererweiterungen überflüssig.

Und das geräteübergreifend: Einmal installiert, schützt das smarte Device nicht nur per Kabel am Router angeschlossene

JETZT MITMACHEN!

eBlocker Pro selbst bauen und 90 Tage testen!

Bewerben Sie sich noch heute unter:
www.eblocker.com/linuxwelt-test

LinuxWelt sucht fünf ambitionierte Leser, die den eBlocker Pro auf ihrem Raspberry Pi 2 oder 3 beziehungsweise Banana Pi M2(+) selbst installieren und ausprobieren möchten! Alle Gewinner erhalten eine eBlocker Pro-Testlizenz, die für 90 Tage kostenfrei gültig ist.
Auf die 5 Tester warten verschiedene Aufgaben. Wir freuen uns auf Ihr wertvolles Feedback.
PS: Bei Gutscheineinlösung erhalten Sie zusätzlich ein kostenloses Kurzabo von LinuxWelt, PC-WELT oder AndroidWelt.

Linux-PCs vor allzu neugierigen digitalen Blicken, sondern auch per WLAN am Netzwerk partizipierende Laptops, Smartphones, Tablets, Spielkonsolen, Set-Top-Boxen und alle erdenklichen Geräte anderer Hersteller und Betriebssystemanbieter.

Apropos Installation: Die ist denkbar einfach und belegt nicht mal eine der so wertvollen Schnittstellen am Rechner. Den eBlocker schließen Sie mit einem beiliegenden Netzwerkkabel direkt an einem freien LAN-Port Ihres Routers an; der autarke weiße Würfel richtet sich innerhalb von Minuten selbst ein und hält sich zudem mit der neuesten Firmware stets aktuell, um neue Tracker, Phishing-Fallen und Malware zu erkennen. Zusätzliche proprietäre Software auf den Endgeräten? Fehlanzeige und komplett überflüssig. Eine Anpassung an die eigene Daten-Freigebigkeit erfolgt – ähnlich wie bei einem Router – individuell für jedes genutzte Gerät im Webbrowser.

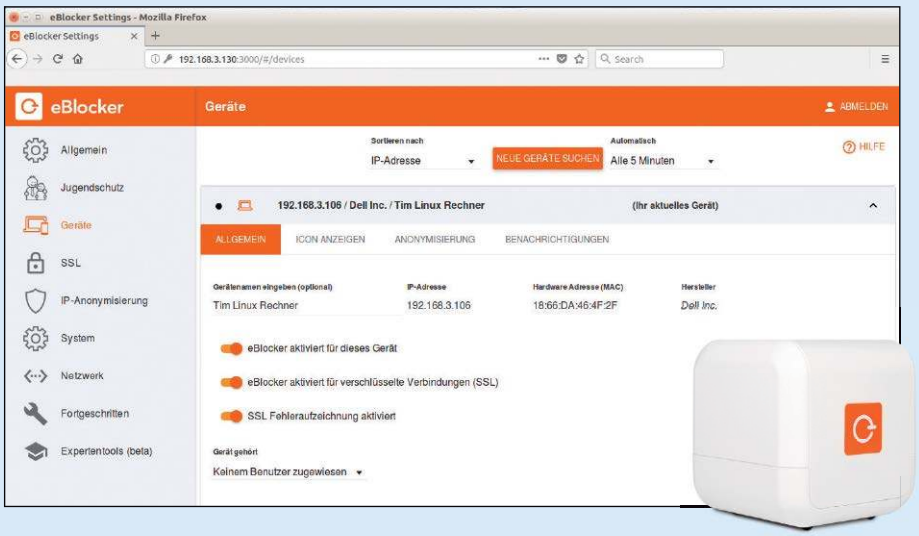
Trackern immer einen Schritt voraus

Einfache Installation und Handhabung, Der eBlocker Pro trickst neugierige Tracker noch vor dessen Datenabgriff aus. Browserbasierte Erweiterungen wie uBlock und Ghostery erweisen sich somit als obsolet. Zudem verwischt das smarte Device die IP-Adresse seines Besitzers. Standardmäßig greift der eBlocker dabei auf den quelloffenen Tor-Anonymisierungsdienst zurück, allerdings können Sie auch jeden anderen VPN-Dienst bestimmen, der das OpenVPN-Protokoll unterstützt – ein Wizard hilft bei der Einrichtung im Webbrowser.
Übrigens bleiben alle mit dem eBlocker verarbeiteten Daten lokal auf der Box und somit in den eigenen vier Wänden – eine Übertragung etwa in einen Cloud-Speicher des Herstellers entfällt.

Fazit

Einfache Installation und Handhabung, der nachhaltige Schutz der Privatsphäre auf allen Geräten im Netzwerk sowie ein extrem verbessertes Nutzererlebnis durch den Wegfall von Werbung – der eBlocker legt seinem Besitzer das gute Gefühl der gewährten Privatsphäre zurück in dessen eigene Hände. Testen Sie ihn am besten selbst!

Sie haben noch Fragen?
www.eBlocker.com



Wussten Sie schon,

… dass Online-Anbieter Ihr Surfverhalten auf jeder besuchten Webseite und über alle Endgeräte hinweg verfolgen? So entstehen genaue Persönlichkeitsprofile, die sogar intimste Details über Sie verraten.

… dass Kreditanbieter Ihr Onlineverhalten für Bonitätsbewertungen heranziehen? Frequentieren Sie etwa Seiten von Wettanbietern, kann sich dies negativ auf Ihre Kreditaussichten auswirken.

… dass softwarebasierte Werbeblocker wie Adblock Plus zwar Werbung ausblenden, nicht aber das Auslesen von persönlichen Daten wie Ihrer IP-Adresse verhindern?

… dass knapp 20 Prozent aller Internetnutzer Privacy-Erweiterungen und Werbefilter mit Virenschutzprogrammen verwechseln und sich so fälschlich sicher fühlen?

So finden Sie den passenden eBlocker

Der eBlocker Base …

… ist die preiswerte Plug-and-Play-Lösung zum Schutz der Privatsphäre. Nach dem simplen Anschluss per Kabel am Router erlaubt er die anonymisierte Internetnutzung auf allen verbundenen Geräten und Browsern.

Der eBlocker Pro …

… komplettiert die anonymisierte Internetnutzung um einen individuellen Werbefilter, trickst datensammelnde Tracker aus und schützt vor Malware.

Der eBlocker Family …

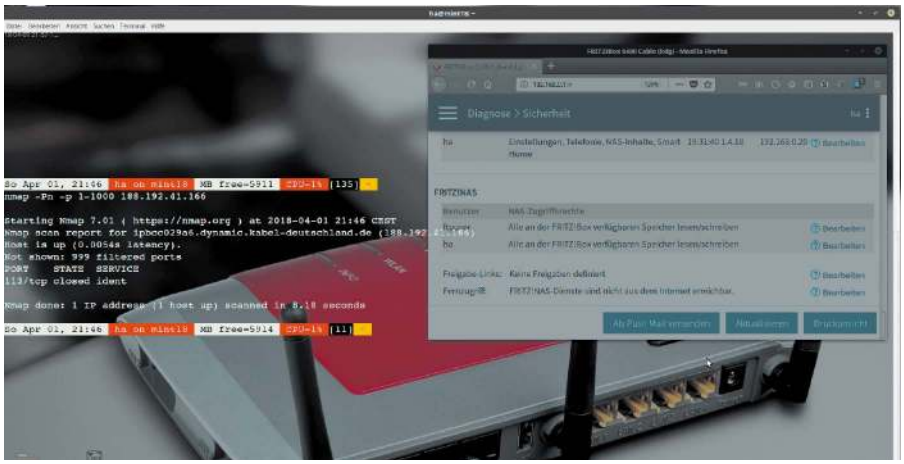
… erweitert die Funktionen des eBlocker Pro um eine Mehrbenutzer-Unterstützung mit Jugendschutz-Funktionen inklusive Surfzeiten-Beschränkung.

eBlocker.	BASE	PRO	FAMILY
Linux-kompatibel	✓	✓	✓
Schutz für alle Geräte im Netzwerk	✓	✓	✓
IP-Anonymisierung	✓	✓	✓
OpenVPN	✓	✓	✓
Multiuser-fähig	✓	✓	✓
Individualisierte Nutzereinstellungen	✓	✓	✓
Tracker Schutz	✓	✓	✓
Schutz vor Malware & Phishing	✗	✓	✓
Gerätetarnung	✗	✓	✓
Schutz mobiler Datenverbindungen	✗	✓	✓
Jugendschutzfunktionen	✗	✗	✓
Festlegung von Surfzeiten	✗	✗	✓
Preis (inkl. Updates für 12 Monate)	€ 119,-	€ 199,-	€ 249,-

Sichere Router

Der Themenschwerpunkt „Sicherheit durch Linux“ startet mit dem Heimrouter, also der zentralen Hardware für Netz und Internet. Routersicherheit ist kein dezidiertes Linux-Thema, erhält aber durch Webfreigaben von Linux-Servern zusätzliche Sensibilität.

VON HERMANN APFELBÖCK



Die folgenden zwei Seiten sprechen die wichtigsten Punkte an, um den aktuellen Routerstatus zu analysieren und das Sicherheitslevel zu erhöhen. Als Beispielrouter dient die AVM-Fritzbox (in der „erweiterten“ Ansicht). Bis auf wenige Ausnahmen wie etwa die „Push Services“ beherrschen auch andere Router die beschriebenen Funktionen, wenn auch an anderer Stelle. Der Wert der nachfolgend empfohlenen Einstellungen mag im Einzelfall bezweifelt werden, denn es gibt keine Maßnahme, die absolut schützt und durch erhöhten Aufwand nicht doch zu hintergehen wäre. Aber die Tatsache, dass Einbrecher auch gut verschlossene Türen knacken können, sollte uns nicht verleiten, die Türen einfach offenstehen zu lassen.

Verbesserte WLAN-Sicherheit

Dass ein WLAN WPA2-verschlüsselt sein muss („WLAN → Sicherheit → Verschlüsselung“), ist nicht wirklich erwähnenswert, denn im unverschlüsselten WLAN kann der Nachbar mindestens mitsurfen oder erhält zudem mit seiner lokalen IP-Adresse alle Möglichkeiten, die Daten des Heimnetzes abzugreifen.

MAC-Filterung ist eine verschärfende Maßnahme, die nur noch definierte Geräte ins WLAN lässt. Skeptiker werden einwenden, dass die dazu abgefragte Hardwareadresse (MAC-Adresse) des WLAN-Adapters so eindeutig nicht ist, weil jedes Linux eine beliebige MAC-Adresse vorgaukeln kann (mit *ifconfig*). Das ist richtig, jedoch müsste ein Einbrecher dazu zusätzlich wissen, welche MAC-Adressen der Router erlaubt. MAC-Filterung ist daher sehr wohl ein wirksamer WLAN-Schutz.

In der Fritzbox finden Sie die MAC-Filterung unter „WLAN → Sicherheit“ ganz unten: Standardmäßig sind alle neuen Geräte zugelassen. Die Option „WLAN-Zugang auf die bekannten WLAN-Geräte beschränken“ aktiviert den MAC-Filter. Beachten Sie, dass dieser Schutz nicht ganz bequem ist: Jedes hinzukommende Gerät im Haushalt oder jedes Besuchergerät muss hier später explizit mit seiner MAC-Adresse neu aufgenommen werden („WLAN-Gerät hinzufügen“). Es empfiehlt sich daher, vor dem Aktivieren alle benötigten Geräte anzumelden, so dass deren MAC-Adressen in der Liste der bekannten Geräte bereits aufgeführt sind.

Zum späteren Hinzufügen von Geräten finden Sie deren MAC-Adressen in Linux mit ifconfig („Hardware Adresse“), in Windows über „Netzwerk und Internet → Verbindungseigenschaften“, in Android unter „Einstellungen → Allgemein → Geräteinformationen → Status“.

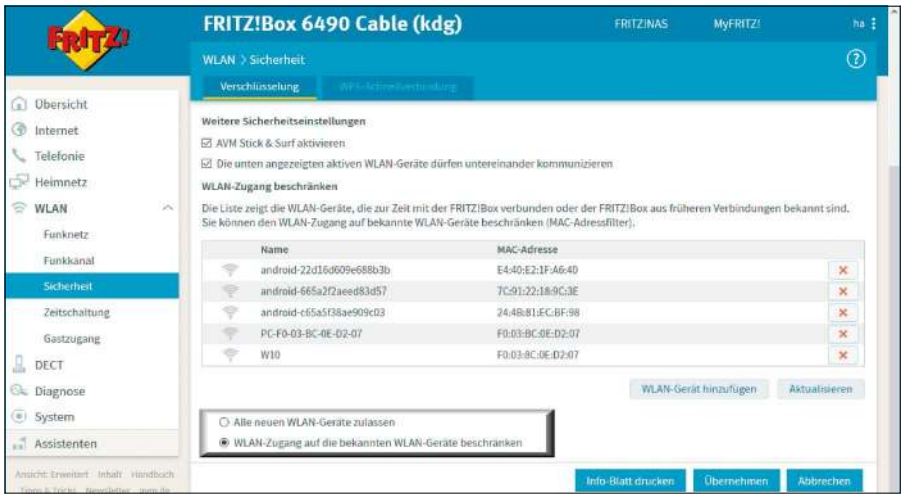
WLAN-Netzwerknamen unterdrücken: Die SSID muss nicht öffentlich für alle Nachbarn sichtbar sein. In der Fritzbox lässt sich diese Öffentlichkeit über „WLAN → Name des WLAN-Funknetzes sichtbar“ abschalten. Danach muss beim Zutritt zusätzlich zum WPA-WLAN-Kennwort auch der Name des WLANs explizit eingegeben werden. Jedoch zeigen spezialisierte Wi-Fi-Scanner den Netznamen auch dann an, wenn er unterdrückt wird. Die Maßnahme hilft also allenfalls gegen neugierige, aber technisch unbedarfte Nachbarn.

WPS (Wi-Fi Protected Setup): WPS vereinfacht die Erstanmeldung von WLAN-Geräten durch simplen Knopfdruck auf dem Router. In der Fritzbox war WPS nie ein Problem („WLAN → Sicherheit → WPS-Schnellverbindung“), während es bei einigen anderen Herstellern eine Sicherheitslücke enthielt. Bei älteren Modellen ist es sicherer, WPS abzuschalten und die Einrichtung von WLAN-Clients per Kennwort zu erledigen.

Router im „Stealth-Modus“

Die Fritzbox liefert zu der Sicherheitsoption unter „Internet → Filter → Listen → Firewall im Stealth Modus“ folgende Empfehlung: „Aktivieren Sie diese Option dann, wenn Sie die Identifikation Ihrer Fritz!Box gegenüber Portscans erschweren wollen.“ Dazu sollte man wissen, dass automatisierte Hackerscans massenhaft öffentliche IP-Adressen abfragen. Falls dem eigentlichen Portscan

ein allgemeiner Ping-Befehl vorausgeht, ob diese Adresse überhaupt erreichbar ist, dann wird das Hacker-Script in der Tat weiterreisen, weil Ihre Fritzbox nicht antwortet. Der Nutzwert bleibt aber relativ: Wenn der Angriffsversuch gleich mit einem zeitaufwendigen „nmap -Pn“ erfolgt, antwortet die Fritzbox – trotz Stealth-Modus. Es hängt also davon ab, welche Genauigkeit und welchen Zeitaufwand ein Portscan ansetzt. Wenn Hacker Tausende von zufälligen Adressbereichen möglichst schnell scannen wollen, nehmen sie unter Umständen nur einfachste Mittel. Diese einfachen Angriffsversuche wehrt der Stealth-Modus ab.



Diese Maßnahme ist nicht bequem, erhöht aber die WLAN-Sicherheit: Der MAC-Filter lässt nur noch per MAC-Adresse bekannte Geräte ins Funknetz.

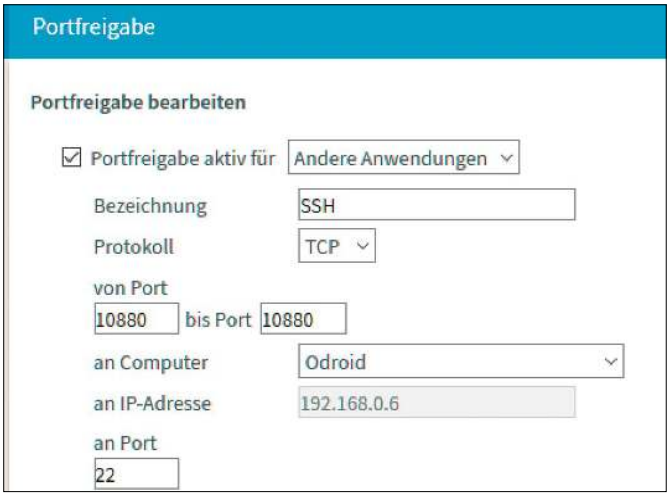
Kontrollierte Öffnung für Webanfragen

Standardmäßig lässt der Router nichts von außen (Web) nach innen (lokales Netz), was nicht vorher von innen explizit angefordert wurde (Browser, Mail-, FTP-, Bittorrent-Client). Wenn es keine triftigen Gründe gibt, sollte sich eine Fritzbox unter „Internet → Freigaben“ keinerlei Blößen geben („MyFritz!-Freigaben“, „Portfreigaben“, „Fritz!Box-Dienste“, „VPN“). Einen schnellen Gesamtüberblick dazu liefert auch „Diagnose → Sicherheit“, der im sichersten Fall überall „Keine Freigaben“ meldet.

Portfreigaben und Fritzbox-Dienste: Soll der Router selbst oder ein Heimserver über das Web erreichbar sein, sind Freigaben unerlässlich. Hier müssen dann allerdings hohe Sicherheitsansprüche gelten: Wer unter „Internet → Freigaben → Fritz!Box-Dienste“ den Internetzugriff auf den Router und/oder dessen NAS-Speicher erlaubt, muss unter „System → Fritz!Box-Benutzer → Benutzer“ ein individuelles Konto mit komplexem Passwort einrichten. Der „ftpuser“ sollte wegen des standardisierten Kontonamens keinen „Zugang aus dem Internet“ haben.

Wenn manuell Ports freigegeben werden müssen („Internet → Freigaben → Portfreigaben“), damit Sie vom Web auf einen heimischen HTTP- oder FTP-Server kommen, können non-konforme Ports Angriffe erschweren. Angreifer konzentrieren sich gerne auf Standardports, etwa 21 für FTP, 22 für SSH, 23 für Telnet, 80 und 8080 für Webserver. Darüber hinaus sind auch spezielle Routerports interessant, so etwa Port 41 441 für den Fernzugriff auf die Fritzbox. In allen Fällen macht man es den Angreifern schwerer, wenn man die Standardports vermeidet und Portnummern jenseits der 1000 verwendet. Natürlich kann jede öffentliche IP-Adresse mit einem Portscan auf alle 65 536 Ports hin gescannt werden – und dann werden auch Dienste an ungewöhnlichen Ports sichtbar. Das ist aber sehr zeitaufwendig. Die meisten automatisierten Portscanner werden sich aus Zeitgründen auf ganz wenige Standardports beschränken oder nur die ersten 1000 Ports abhaken (Standard beim Portscanner nmap).

Auf Ebene des lokalen Netzwerks müssen Sie an den Standardports nichts ändern. Nur in der Portfreigabe des Routers verwenden Sie die non-konforme Portnummer, die Sie dann an die konforme Portnummer des lokalen Rechners leiten. Beim Zugriff aus dem Web müssen Sie allerdings die Portnummer exakt wissen und nach Doppelpunkt an die Heimnetzadresse anhängen.



Non-konforme Portnummer: Die Abbildung zeigt ein Beispiel für den SSH-Fernzugriff auf ein heimisches Gerät, das zwar lokal den Standardport 22 nutzt, aber beim Webzugriff einen unkonventionellen Port.

UPnP-Freigaben: Portfreigaben sollten Sie immer kontrolliert in der Hand haben. Die Option unter „Internet → Freigaben → Portfreigaben“, die es Netzgeräten erlaubt, automatisch Ports freizugeben, ist ein Sicherheitsrisiko. Die Option ist daher standardmäßig abgeschaltet.

Nachrichten vom Router

Zur Sicherheit trägt auch bei, wenn Sie vom Router über Konfigurationsänderungen informiert werden. Das kann nicht jeder Router, aber die Fritzbox – unter „System → Push Service“. Sicherheitsrelevant ist der unterste Eintrag „Änderungsnotiz“, nützlich ist aber auch „Aktuelle IP-Adresse“, die bei jeder neuen Internetverbindung zum Provider die neue öffentliche IP-Adresse verschickt. Das gewünschte Mailkonto, an das die Fritzbox senden soll, tragen Sie unter „Absender“ ein. ■

Sichere Webbrowser

Den sicheren Webbrowser, der Sie sowohl vor Schädlingsangriffen als auch vor Datenverfolgung nachhaltig beschützt, gibt es nicht. Aber Sie können zwischen relativ sicheren und weniger sicheren Alternativen und Einstellungen wählen.

Linux plus Firefox plus Firefox-Erweiterungen: Ein bessere Kombination für Systemsicherheit und Datenschutz gibt es nicht.

VON HERMANN APFELBÖCK

Es ist paradox: Der Browser ist heute die wichtigste Software überhaupt. Er zeigt die HTML-Seiten aus dem Web, dem lokalen Netz (Router, Server) und dem lokalen System, ferner Bilder, Musik, Filme, PDF – inklusive Download. Trotzdem haben wir uns daran gewöhnt, dass Browser kostenlos sein müssen. Andererseits zahlen zumindest Windows-Nutzer bares Geld für die Müllabfuhr (AV-Software), die den Müll fernhält oder wegräumt, den der Browser durchgelassen hat.

Da mit Browsersoftware kein Geld zu verdienen ist, stellt sich die Frage nach dem Geschäftsmodell der Hersteller: Beim Marktführer **Chrome** ist es offensichtlich, dass wir selbst und unsere Daten das Produkt sind, womit der Hersteller Google sein Geld verdient. Bei **Opera** und der eingebauten „VPN"-Umleitung (eigentlich nur ein Proxy) schützen wir uns scheinbar vor der Datenverfolgung der Webserver, schicken dabei aber alle Daten an den mittlerweile chinesischen Opera-Besitzer (seit 2016). Hinter **Vivaldi,** das 2015 aus Opera entstand, steht ein kleines Team, das sich angeblich von den voreingestellten gesponserten Lesezeichen finanziert. Selbst **Firefox** lässt sich die voreingestellte Google-Suche bezahlen, wie denn Google generell längst als Hauptsponsor der Mozilla-Foundation auftritt. Aufgrund der Unverkäuflichkeit von Browsersoftware ist leider jeder Browser mehr oder weniger käuflich.

Chrome und Chromium

Der unaufhaltsame Aufstieg von Google Chrome und Chromium seit 2008 ist leicht erklärlich: Chrome ist nicht nur der schnellste Browser, sondern auch sicherheitstechnisch spitze – mit den wenigsten Sicherheitslücken und mit zeitgemäßen Sicherheitsoptionen. Der Browser nutzt eine Safe Browsing API, die auf eine ständig aktualisierte Datenbank schädlicher Websites zurückgreift. Diese Sicherheitsoption zeigt Chrome unter „Einstellungen → Erweitert → Sicherheit und Datenschutz" mit der Option „Mich und mein Gerät vor schädlichen Websites schützen". Sie ist standardmäßig aktiv und sorgt dafür, dass Chrome den Zugang auf gefährliche Sites blockiert und außerdem vor verseuchten oder „ungewöhnlichen" Downloads warnt.

Über die interne Chrome-URL „chrome://flags/" können Sie eine zusätzliche Sicherheitsoption aktivieren: Die Option „Strict site isolation" lädt jede Website als separaten Prozess, was zwar den Speicherbedarf erhöht, aber den Datenzugriff über Sitegrenzen hinweg unterbindet.

Die Sicherheit des Browsers bezahlt der Nutzer allerdings mit hartnäckiger Google-Verfolgung. Chrome erhält ab Einrichtung eine eindeutige Kennung, die an Google gesendet wird. Damit sind die Aktivitäten

des Browsers für Google stets protokollierbar. Lediglich der Inkognito-Modus unterdrückt Cookies, Browserverlauf und Downloadinfos.

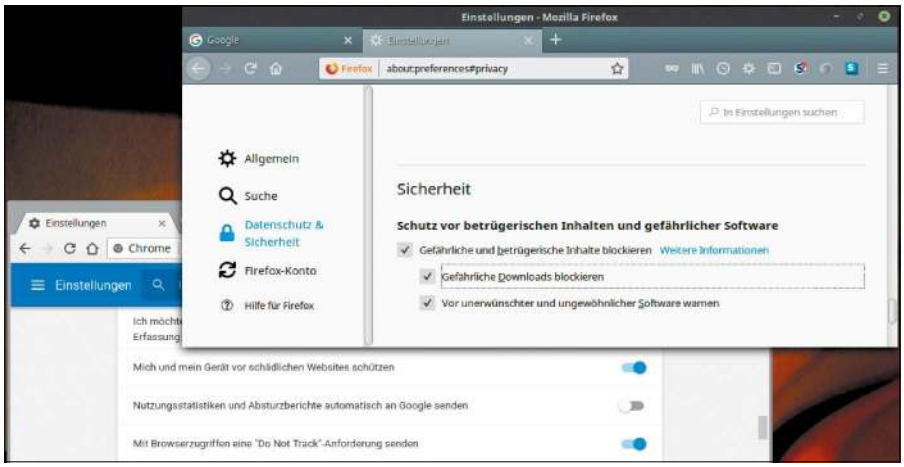
Zum offenen Buch wird der Chrome-Nutzer durch die Browsersynchronisierung. Wer diese über sein Google-Konto aktiviert, um mehrere Chrome-Instanzen abzugleichen, hinterlegt die kompletten Verlaufsdaten bei Google. Ein Sicherheitsproblem ist das nicht, aber ein ernstes Datenschutzproblem. Wer bei Chrome/Chromium die Synchronisierung benutzt, sollte unter „Einstellungen → Erweiterte Synchronisierungseinstellungen" die Option „Alle synchronisierten Daten [...] verschlüsseln" aktivieren. Dabei benötigen Sie ein individuelles Kennwort, das unabhängig vom Google-Kennwort ist. Der Komfortverlust ist nicht gravierend, da Sie dieses Kennwort auf jedem weiteren Gerät nur ein einziges Mal eingeben müssen. Alle Daten landen dann verschlüsselt auf dem Google-Server, der Schlüssel verbleibt auf dem lokalen Gerät.

Ein Plädoyer für Firefox

Der Mozilla-Browser verliert Jahr für Jahr Millionen Nutzer – die meisten an Chrome. Wer Sicherheit und Datenschutz priorisiert, sollte dem Firefox der gemeinnützigen Mozilla-Foundation besser treu bleiben, selbst wenn dieser ein wenig langsamer und fetter ist. Firefox bietet im Unterschied zu Chrome/Chromium

- optional den privaten Modus als Standardoption („Einstellungen → Datenschutz & Sicherheit → Chronik")
- optional ein Masterpasswort zum Verschlüsseln der Online-Zugangsdaten, was sowohl gegen Fremdzugriff wie gegen spezialisierte Malware hilft („Einstellungen → Datenschutz & Sicherheit → Formulare & Passwörter")
- standardmäßig verschlüsselte Browsersynchronisierung über das Firefox-Konto
- optional den kompletten Verzicht auf eine gespeicherte Verlaufschronik („Einstellungen → Datenschutz & Sicherheit → Chronik")

Als Schutz gegen betrügerische Sites nutzt Firefox die Safe Browsing API von Google Chrome. Die betreffenden Einstellungen finden Sie unter „Einstellungen → Datenschutz & Sicherheit → Sicherheit". Wer den Mozilla-Browser darüber hinaus dosiert mit bewährten Erweiterungen ausstattet („Add-ons → Erweiterungen" und Eingabe im Suchfeld), surft relativ sicher – sogar unter Windows:



Sicherheit und Datenschutz in Firefox und Chrome: Die Browsereinstellungen ähneln sich äußerlich und technisch bis in die Details. Beim Datenschutz hat Firefox etliche Vorteile.

Noscript: Diese Erweiterung ist nicht bequem, aber der Schädlingsstopp schlechthin. Sie müssen allerdings Scripting auf vielen Seiten erst explizit erlauben. Dies geschieht temporär über das Noscript-Symbol mit Klick auf das blaue „S" mit kleiner Uhr („Temp. Trusted") oder dauerhaft mit dem zweiten „S"-Symbol. Irritieren kann die Tatsache, dass manche als „Trusted" bewertete Seite rot markiert bleibt. Dies ist immer dann der Fall, wenn die Verbindung nicht HTTPS-verschlüsselt ist – typischerweise etwa zu Ihrem Router oder zu einem Datenserver im lokalen Netz. Wenn die Verbindung nur über HTTP funktioniert, müssen Sie die Rotfärbung akzeptieren. Das Umschalten auf „Grün" (durch Klick auf das Schloss-Symbol) würde die Adresse wieder auf „Untrusted" schalten, da „Grün" immer HTTPS voraussetzt.

WOT: Diese Communitydatenbank kam in Verruf, weil Benutzerdaten mit Verlaufsprotokollen verkauft wurden. In der Annahme, dass sich dieser skandalöse Datenhandel nicht wiederholt, hat Firefox die Erweiterung inzwischen wieder im Repertoire.

In puncto Datenschutz suspekt, ist diese Datenbank auf der anderen Seite in puncto Sicherheit ein erheblicher Gewinn: Die Sammlung mit betrügerischen Websites zeigt schon bei der Google-Suche einen grünen oder roten Ring. Beim Zugang auf gefährliche Seiten (direkt oder via Suchmaschine) erscheint eine Warnung und Sie können den Vorgang abbrechen.

HTTPS Everywhere: Die Erweiterung wählt, wo immer verfügbar, eine verschlüsselte HTTPS-Verbindung zu einer Website, auch wenn dies per Link oder Adresseingabe so nicht angefordert wurde. HTTPS ist vor allem bei Bankgeschäften und Einkäufen im Internet unverzichtbar, weil Sie Zugangsdaten oder Kreditkartendaten über das Netz versenden müssen. Der Browser zeigt verschlüsselte Verbindungen in der Adresszeile grün gefärbt. ■

ALTERNATIVE UND SPEZIALISIERTE BROWSER

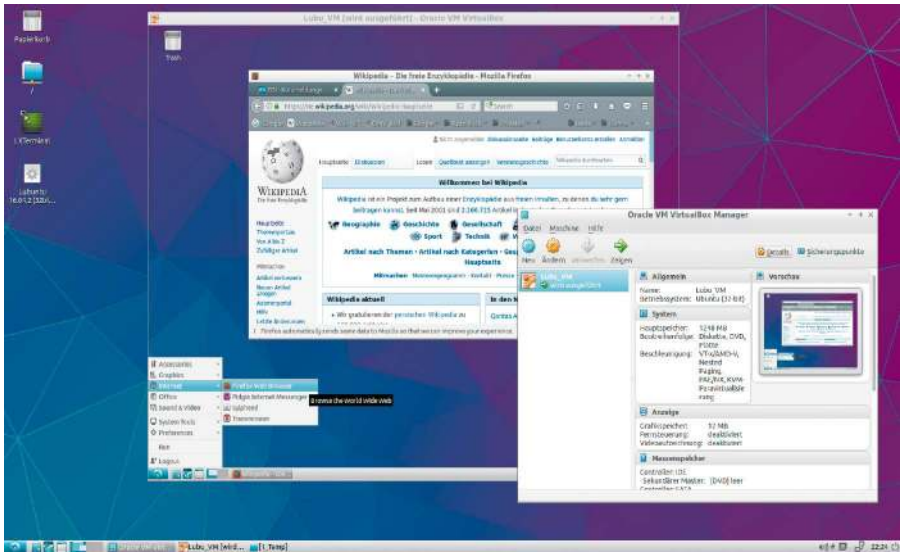
Browser wie Vivaldi, Opera oder Midori sind gute Software und schicke oder besonders schlanke Alternativen. Zudem gibt es vor allem für Windows eine ganze Reihe sogenannter „Sicherheitsbrowser" wie mit eingebautem Virenscanner für Downloads, mit voreingestellten Sicherheitserweiterungen oder mit Anonymisierung (Commodo Dragon, Avira Scout, TOR, Dooble). Gegen alle diese Browser spricht, dass sie unter der Haube einen Chrome/Chromium oder Firefox verwenden (einzige Ausnahme Midori). Erhöhte Sicherheit gibt es daher nicht von der Basis her, sondern nur durch zusätzliche Einbauten, die man auch durch etliche Browsererweiterungen erreicht (siehe Haupttext). Außerdem können kleine Nischenbrowser Google und Mozilla hinsichtlich Fehleranalyse und Updategeschwindigkeit kaum das Wasser reichen.

Sichere Surfsysteme

Geringe Verbreitung, technische Varianten, kompetente Nutzer: Linux ist kein beliebtes Angriffsziel für digitale Schädlinge. Dieser Artikel zeigt, wie sicheres Surfen mit Linux auch Windows-Nutzern hilft und wie Sie die Websicherheit noch optimieren.

VON HERMANN APFELBÖCK

Beim Thema „Sicher surfen“ vermischen sich oft Aspekte, die nichts miteinander zu tun haben, nämlich der Systemschutz vor digitalen Schädlingen und der Datenschutz vor den Nachstellungen von Datensammlern aller Couleur (Google, Oracle, Amazon, Polizei, Geheimdienste). In diesem Beitrag geht es ausschließlich um den Systemschutz, also um größtmögliche Sicherheit gegenüber Würmern, Viren und Trojanern aus dem Web. Der Schutz durch Livesysteme und virtuelle Systeme ist nachhaltig: Er garantiert sicheres Surfen, sicheres Onlinebanking, sichere Webeinkäufe und erlaubt sogar gezielte Ausflüge auf Trojaner- und Phishing-Sites.



Virtualisierung erhöht die Sicherheit signifikant: Im abgebildeten Beispiel Fall läuft der Browser Firefox in einem virtuellen Lubuntu unter Virtualbox und das Ganze wiederum in einem Lubuntu-Livesystem.

Sicherheit für Linux- und Windows

Internetschädlingen geht es immer darum, ausführbaren Code auf dem System zu starten und sich dann dauerhaft einzunisten. Die entscheidende Hürde für den Schädling ist die initiale Zündung auf dem System. Gelingt diese, mag das umfangreichere Folgeprogramm (Autostart-Mechanismus, Reproduktion, Schadfunktion) mehr oder weniger anspruchsvoll ausfallen, aber im Prinzip hat der Schädling bereits gewonnen. Wie kommt es zur Initialzündung des Schadcodes?

In der Regel lädt der Systembenutzer den Schadcode aktiv und freiwillig. Das geschieht durch die Installation verseuchter Downloads, durch den Doppelklick auf ausführbare Mailanhänge oder den Klick auf Web-URLs in Mails, die Javacripts auslösen, welche wiederum über Browser-Sicherheitslücken Code auf dem lokalen System ausführen. Im Vergleich zu den Zuständen vor zehn und 20 Jahren sind viele Gefahren inzwischen durch technische Filter entschärft: Viele Mailprovider verweigern ausführbare Anhänge, Makrocode in Office-Dokumenten wird nicht mehr ohne Warnung gestartet, Downloads müssen den Check von Smartscreen-Filtern oder AV-Scans bestehen. Trotzdem werden findige Hacker neue Wege auf das lokale System finden. Die beste Lösung ist daher ein System, das den Schädling ignoriert oder zumindest wieder entsorgt. Solche Lösungen gibt es in verschiedenen Abstufungen:

1. Linux-Nutzer sind per se zu 99 Prozent im sicheren Hafen: Die Masse der Schädlinge ist für Windows-Systeme programmiert und nur dort lauffähig.

2. Noch höhere Sicherheit bietet ein Linux in einer virtuellen Maschine (VM), das vom eigentlichen Betriebssystem isoliert ist. Ein Malwarebefall betrifft dann nicht das Hauptsystem. Außerdem kann man frühzeitig einen Klon des Originalzustands anlegen, der stets die Rückkehr zur garantiert unkompromittierten VM gestattet.

3. Es sind noch weitere Steigerungen möglich: Eine Option ist ein Linux-Livesystem als virtuelle Maschine. Dieses verwirft Änderungen am System automatisch. Eine weitere Option ist ein speziell gehärtetes Linux (Apparmor, Selinux) innerhalb einer virtuellen Maschine, wie es etwa das Projekt „Bitbox“ anbietet.

4. Hohe Sicherheit bietet jedes Linux-Livesystem, das unabhängig vom installierten Betriebssystem gestartet wird. Hier geschehen alle Programmaktionen im Arbeitsspeicher, so dass jeder Neustart alle Änderungen und eventuelle Schädlinge entsorgt.

Zu den Punkten 2, 3 und 4 lesen Sie nachfolgend praktische Anleitungen. Aus der Tatsache, dass Linux per se sicheres Surfen gewährleistet (Punkt 1), ist der wichtigste Adressat dieser Anleitungen der Windows-Anwender. Durch Linux-Unterstützung kann der Windows-Nutzer sicherheitstechnisch mit Linux gleichziehen, und dies je nach Lösung mit geringem Komfortverlust. Selbstverständlich eignen sich diese Lösungen aber auch, um die Sicherheit unter Linux zusätzlich zu erhöhen.

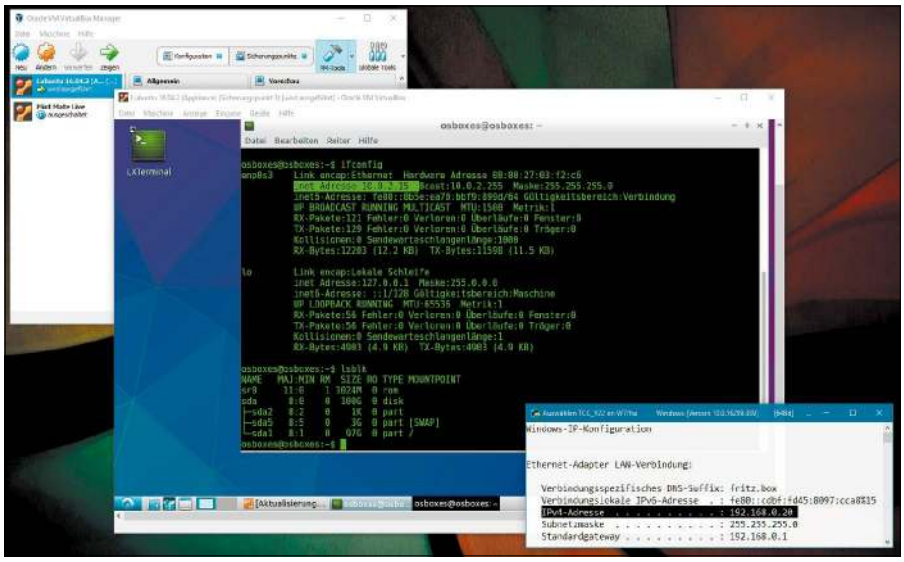
Surfen in virtuellen Maschinen

Als Virtualisierungssoftware benötigen Sie entweder Oracle Virtualbox oder Vmware Player. Das kostenlose Virtualbox erhalten Sie für Windows und für alle namhaften Linux-Distributionen unter *https://www.virtualbox.org/wiki/Downloads*. Den ebenfalls kostenlosen Vmware Player gibt es unter *https://my.vmware.com/de/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/12_0*. Unter Windows starten Sie zur Installation einfach den EXE-Installer per Doppelklick, unter Linux müssen Sie den Download erst mit *chmod +x […]* oder mit dem Dateimanager über „Eigenschaften → Zugriffsrechte“ ausführbar schalten.

Der Vmware Player ist mit Rücksicht auf die kostenpflichtige Vmware Workstation funktional eingeschränkt. Beim privaten Einsatz betrifft das zwar nur einige Komfortfunktionen wie etwa Snapshot-Sicherungen, dennoch ist Oracle Virtualbox die komplettere Virtualisierungssoftware für Heimanwender. Die nachfolgenden Anleitungen beziehen sich daher vorrangig auf Virtualbox.

Ein Linux-System in einer virtuellen Maschine verbindet hohen Bedienkomfort mit sehr hoher Sicherheit. Dass Schadprogramme aus dem virtuellen Linux-Gastsystem ausbrechen und das Hostsystem befallen, ist extrem unwahrscheinlich. Es ist nicht nur technisch so gut wie auszuschließen, sondern setzt auch voraus, dass der Schädling auf diese komplexe Situation vorbereitet ist. Das einzige nennenswerte theoretische Risiko ist eine VM für Virtualbox oder Vmware, die bereits vorab gezielt infiziert wurde. Netzwerktechnisch sind die Voreinstellungen so, dass die VM eine virtuelle IP-Adresse erhält, die nicht im Adressraum des lokalen Netzwerks liegt. Weder sieht die VM die anderen Netzrechner noch umgekehrt. Diese Voreinstellung (NAT) lässt sich zwar im Virtualisierer auch umschalten („Netzwerkbrücke“), ist aber die sicherste Option: Die VM kommt ins Internet, sieht aber nicht das lokale Netz.

Als weitere Absicherung gibt es in Virtualbox die Sicherungspunkte. Ein Sicherungspunkt lässt sich zu jedem Zeitpunkt über „Maschine → Sicherungspunkt erstellen“ anlegen. Die Rückkehr zu einem früheren Zustand erfolgt bei ausgeschalteter VM im Verwaltungsfenster über „Sicherungspunkte“ und die Option „Wiederherstellen“. Der Bedienkomfort einer VM ist deutlich höher



Netzwerk und Laufwerke aus der Sicht der VM: Die virtuelle erhält eine virtuelle IP-Adresse vom Host (ifconfig) und sieht nur seine eigene virtuelle Festplatte (lsblk).

als bei selbst bootenden Surfsystemen, weil der Benutzer kein Bootmedium suchen, sein Standardsystem nicht verlassen muss und somit neben seinem sicheren Browser in der VM gewohnt im Hauptsystem weiterarbeiten kann. Wenn der Rechner vier, besser acht GB RAM mitbringt und einen aktuellen Prozessor, läuft das Linux mit Browser in der VM praktisch genauso flüssig wie in einem nativen System.

Livesysteme – Appliances – Installationen: Je nachdem, wieviel individuelle Anpassung Sie von Ihrem Surfsystem in der virtuellen Maschine erwarten, gibt es mehrere Varianten mit unterschiedlichem Einrichtungsaufwand. Ein Linux-Livesystem ist unter Virtualbox nach wenigen Handgriffen startklar, bringt größtmögliche Sicherheit, aber nur einen Browser von der Stange ohne Anpassungsmöglichkeiten. Eine vorkonfigurierte VM (Appliance) ist ebenfalls im Handumdrehen eingerichtet und bietet alle Optionen individueller Anpassung. Aber erstens müssen Sie der heruntergeladenen VM vertrauen, zweitens gibt es nicht alles als fertige virtuelle Appliance. Händische Installationen verursachen den größten Einrichtungsaufwand, basieren aber auf den Installationsmedien der Distributionen und erzeugen eine absolut saubere, neue virtuelle Festplatte.

Einrichten virtueller Maschinen

Das Anlegen neuer VMs ist in Virtualbox wie Vmware eine Angelegenheit von wenigen Mausklicks.

Virtuelle Livesysteme: Eine virtuelle Festplatte ist hier nicht nötig. Sie müssen nur anschließend für das virtuelle optische Laufwerk den Pfad zum passenden ISO-Image angeben.

A. Livesystem: Dazu brauchen Sie zunächst das heruntergeladene ISO-Image der gewünschten Distribution. Da es hier in erster Linie um einen ordentlichen Browser und eventuell einen Mailclient geht, genügt im Hinblick auf den Speicherbedarf ein schlankes Exemplar wie etwa Lubuntu (32 Bit). In Virtualbox klicken Sie dann auf „Neu“, geben einen Namen an (etwa „Lubuntu 18.04“), als Typ „Linux“ und als Version in diesem Beispiel „Ubuntu (32 Bit)“. Nach „Weiter“ genügen unter „Speichergröße“ je nach System 1024, 1536 oder 2048 MB. Nach „Weiter“ benötigen Sie bei einem Livesystem unter „Platte“ keine virtuelle Festplatte. Sie wählen also „Keine Festplatte“ und klicken auf „Erzeugen“. Virtualbox warnt Sie, dass Sie keine Festplatte verwenden, was Sie mit „Fortfahren“ ignorieren. Der erstellten VM müssen Sie jetzt mit „Ändern“ unter „Massenspeicher“ das ISO-Abbild mitteilen. Dies geschieht unter

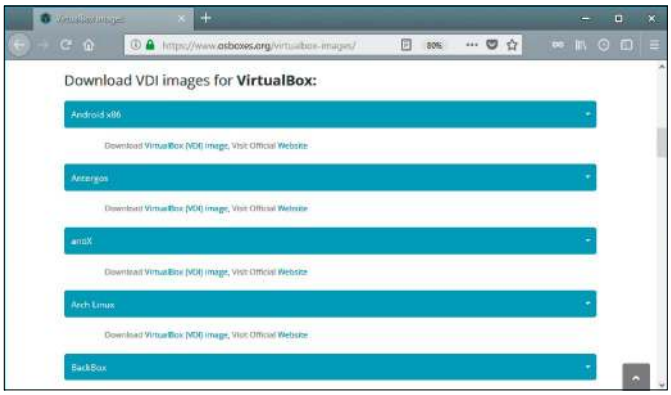
„Controller: IDE“ auf dem CD-Symbol, das aktuell noch als „leer“ angezeigt wird. Aktivieren Sie links das Kästchen „Live-CD/DVD“ und klicken Sie dann auf das CD-Symbol ganz links oben. Hier können Sie die „Datei für optisches Medium auswählen“ – sprich: Sie navigieren zum ISO-Image des gewünschten Livesystems. Damit ist das Livesystem startklar.

B. Appliance (fertige virtuelle Festplatte): Für Virtualbox wie Vmware gibt es zahlreiche, sofort lauffähige Linux-Systeme zum Download. Es handelt sich – im Unterschied zu Livesystemen – um vollwertige Installationen, die Sie anschließend etwa im Browser mit Lesezeichen oder mit persönlichen Konten im Mailclient beliebig anpassen können. Andererseits entfällt aber der Aufwand der Ersteinrichtung. Eine prominente und vertrauenswürdige Anlaufstelle für solche virtuellen Festplatten ist *https://www.osboxes.org*. Klicken Sie dort auf „VM Images“ und wählen Sie das benötigte Format – VDI für das hier bevorzugte Virtualbox, VMDK für Vmware. Die zahlreichen virtuellen Festplatten (von „Android x86“ bis „Zorin OS“) sind hier standardmäßig 7z-gepackt. Unter Windows muss daher der kostenlose Packer 7-Zip vorliegen (*http://www.7-zip.de*), unter Linux ist 7z-Unterstützung in der Regel Standard und im Bedarfsfall mit

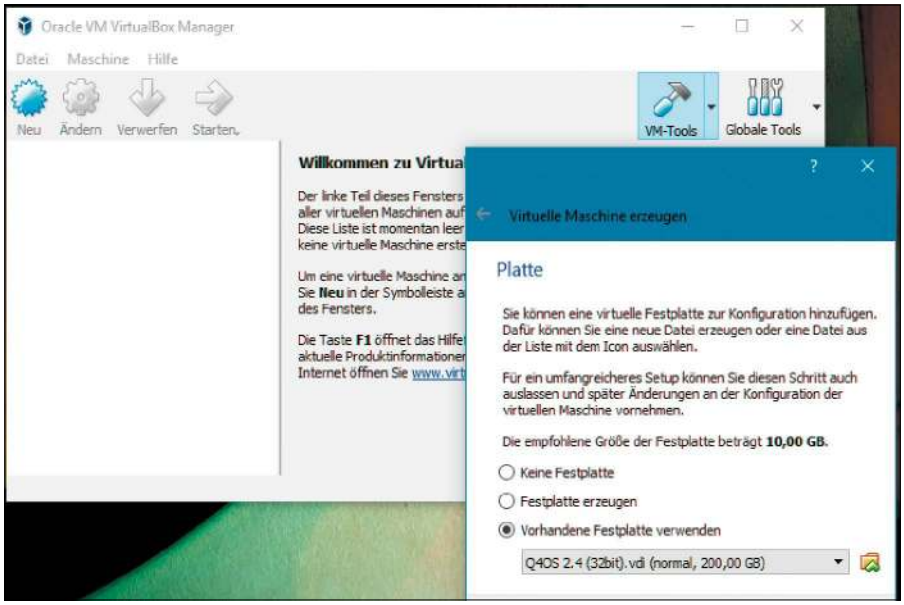
```
sudo apt-get install p7zip p7zip-full
```

auch schnell nachgerüstet. Nach dem Auspacken des Archivs erhalten Sie das Festplattenimage mit der Erweiterung VDI. Verschieben Sie dieses an einen Ort, wo es dauerhaft bleiben kann.

Danach starten Sie Virtualbox. Die ersten Schritte nach Klick auf „Neu“ entsprechen dem Vorgehen wie oben unter „ Livesystem in Virtualbox“. Beim Schritt „Platte“ wählen Sie hier hingegen „Vorhandene Festplatte verwenden“ und navigieren zur heruntergeladenen VDI-Datei. Nach Klick auf „Erzeugen“ ist das virtuelle System bereits eingerichtet, erscheint in der Systemübersicht in der linken Spalte und kann mit „Starten“ oder Doppelklick sofort loslegen. Am Anmeldebildschirm erscheint das Standardkonto „osboxes.org“ (oder „osboxes“), und mit dem Standardpasswort „osboxes.org“ können Sie sich anmelden. Diese Standardeinstellung können Sie später in der Benutzerverwaltung des Linux-Systems natürlich ändern.



Fertige VDI oder VMDK-Images: Angebote wie *www.osboxes.org* ersparen die Installation virtueller Systeme. Sie müssen nur die heruntergeladene virtuelle Festplatte in den Virtualisierer einbinden.



Fertige virtuelle Maschinen verwenden: Aus dem Web geladene virtuelle VDI-Images kann Virtualbox direkt einbinden. Beim Vmware Player (VMDK-Images) ist ein Umweg erforderlich.

Ein Tipp zum Vmware Player: Der Einrichtungsassistent des abgespeckten Players sieht den Einbau fertiger VDMK-Appliances nicht vor. Es geht aber trotzdem: Sie müssen erst eine leere virtuelle Festplatte erzeugen, wie es der Player vorgibt. Ist der Assistent durchlaufen und die VM eingerichtet, gehen Sie nach Rechtsklick darauf auf „Settings“ und löschen die „Hard Disk“ mit „Remove“. Wenn Sie danach mit „Add“ manuell eine „Hard Disk“ einrichten, erscheint die maßgebliche Option „Use an existing virtual disk“. Damit können Sie die VDMK einbinden.

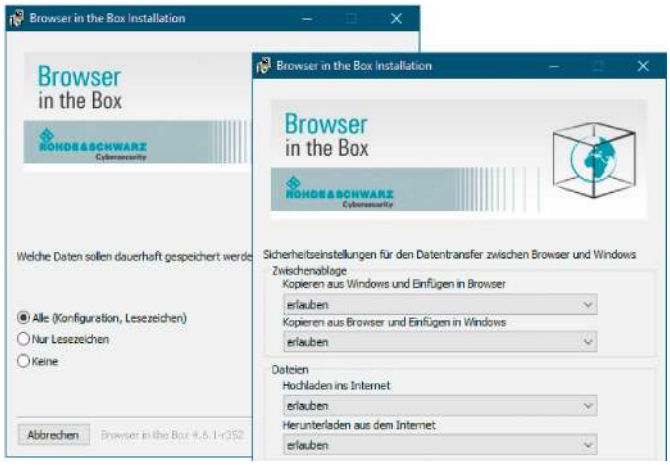
C. Manuelle Installation: Hier durchlaufen Sie den Virtualbox-Assistenten wie oben beschrieben und wählen dann im Dialog „Platte“ die Option „Festplatte erzeugen“, anschließend den Dateityp VDI. Als Größe genügen etwa acht GB, wenn es beim Surfsystem bleiben soll. Genau wie bei Variante A müssen Sie der eingerichteten VM anschließend mit „Ändern“ unter „Massenspeicher“ das ISO-Abbild des Installationsmediums mitteilen. Wenn Sie das virtuelle System danach „Starten“, lädt das ISO-Livesystem, mit dem Sie die Distribution danach in die virtuelle Festplatte installieren. Diese anschließende Einrichtung unterscheidet sich nicht von einer normalen Installation.

Spezialdistribution Bitbox: Browser in the Box

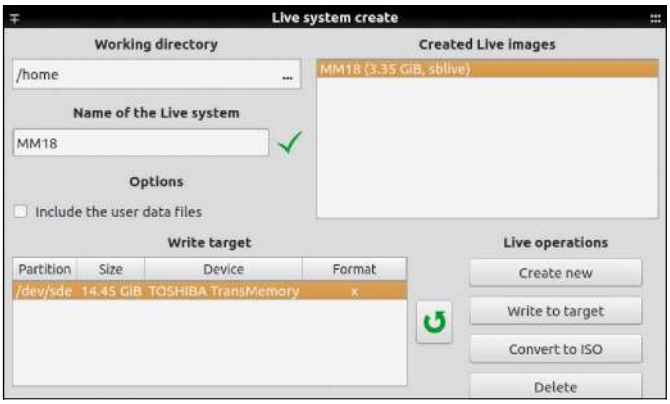
Die soeben beschriebenen Virtualisierungsvarianten genügen nach unserer Ansicht sehr hohen Sicherheitsansprüchen, sofern dann auch wirklich diszipliniert der virtuelle Browser genutzt wird. Dennoch gibt es immer wieder komplette Lösungen, die das technische Prinzip noch ein Stück weiterdrehen. Aktuell hochgelobt ist die Virtualbox-Appliance „Browser in the Box“ oder

kurz Bitbox von Rohde & Schwarz, das im Auftrag des BSI (Bundesamt für Sicherheit in der Informationstechnik) konzipiert wurde (siehe *https://cybersecurity.rohde-schwarz.com*). Als Basis dient ein virtualisiertes Debian Linux, das durch Apparmor-Härtung auch die root-Rechte beschränkt. Der Netzverkehr läuft verschlüsselt durch eine zweite Virtualbox-Instanz. Zudem kehrt das virtuelle System bei jedem Browserneustart auf den zertifizierten Ausgangszustand zurück. Aus Anwendersicht besteht das komplexe System nur aus einem Browserfenster – wahlweise Firefox oder Chromium. Der Nutzer hat weder mit Linux noch mit Virtualbox zu schaffen, da ein Installer die Einrichtung vollautomatisch übernimmt. Kostenlose Downloads von Bitbox (circa 700 MB) gibt es bei *https://cybersecurity.rohde-schwarz.com* nur unter Angabe ausführlicher Nutzerdaten, aber auch bei Onlineportalen wie *www.heise.de*.

Nachteile: Bitbox-Sicherheit bezahlen Sie mit mehreren Einschränkungen. Das Appliance gibt es nur für Windows-Systeme. Dort darf Virtualbox nicht installiert sein und kann daher nicht anderweitig genutzt werden. Obwohl das Bitbox-Projekt nur den Browser pur bietet, verbraucht es verglichen mit selbst eingerichteten virtuellen Systemen sehr viel Speicher und startet zäh. Auch das Schließen benötigt immer einige Zeit für Aufräumarbeiten. Der einmal geladene Browser selbst läuft hingegen jederzeit flüssig. Die Option, den Browser zumindest mit eigenen Lesezeichen und Einstellungen personalisieren zu dürfen, müssen Sie bereits bei der Einrichtung aktivieren.



Bitbox-Installation („Browser in the Box"): Für späteren Browserkomfort sollten Sie die bei der Einrichtung angebotenen Optionen sorgfältig auswählen.



Der einfachste Weg, Ubuntu-basiertes Linux in ein Livesystem umzuwandeln, ist das Tool Systemback. Damit gelingt auch ein Livesystem mit eingebautem virtuellem System.

Bootfähige Linux-Livesysteme

Einen Rechner mit einem Livesystem auf USB oder DVD neu zu booten, um ins Internet zu gehen, ist sicher nicht komfortabel. Wer sich aber bewusst auf riskante Seiten begeben will, wird diesen Weg in Rücksicht auf sein System nicht scheuen. Immerhin haben Livesysteme gegenüber virtualisierten Systemen einen wesentlichen Vorteil: Sie arbeiten voraussetzungslos und können mobil auf jedem Rechner gestartet werden. Ob Sie zum Surfen ein typisches Livesystem wie Porteus (*http://porteus.org/*) und Puppy Linux (*http://puppylinux.org*) oder das Live- und Installationsmedium einer Desktopdistribution wie Ubuntu – etwa von der Heft-DVD – verwenden, ist nur eine Komfortfrage. Sicherheitstechnisch spielt die Wahl keine wesentliche Rolle, denn spezielle „Kiosk"-Systeme wie Porteus haben einen anderes Motiv: Sie sollen das System vor dem Benutzer schützen, nicht vor Internetmalware.

Linux-ISO-Abbilder lassen sich mit einschlägigen Werkzeugen problemlos auf USB oder DVD schreiben. Der Umgang mit Livesystemen und den Werkzeugen Etcher, Imgburn, Unetbootin, dd, oder Win 32 Disk Imager war in der letzten LinuxWelt-Ausgabe ein Heftschwerpunkt, der im vollen Umfang im E-Book „LinuxWelt XXL digital" auf Heft-DVD enthalten ist. Wir verzichten hier daher auf genauere Anleitungen und verweisen auf dieses E-Book.

Wie immer lässt sich die Sicherheitsschraube aber auch hier eine ganze Stufe härter drehen: Livesysteme erhalten eine normale IP-Adresse im realen Adressraum und „sehen" somit die Rechner und auch den Router im lokalen Netzwerk. Außerdem sehen sie die Massenspeicher, die im lokalen Rechner stecken. Theoretisch könnte also auch ein Schädling diese Objekte „sehen". Wir stellen daher eine Versuchsanordnung zur Diskussion, die innerhalb eines Livesystems ein virtuelles Linux enthält, das ins Internet geht. Dies ist sicher keine Konstruktion, die der private Nutzer für sicheres Surfen benötigt, aber eine, mit der man dann auch mal gezielt schädliche Webseiten aufsuchen kann. Die Zutaten sind

- ein normal installiertes, schlankes Linux (Lubuntu)
- ein darin installiertes Virtualbox
- ein darin installiertes Tool Systemback
- ein unter Virtualbox angelegtes schlankes Linux (erneut Lubuntu als VDI-Appliance).

Das komplette und als tauglich getestete System konvertieren wir mit dem Tool Systemback zu einem Livesystem und schreiben es damit bootfähig auf USB-Stick. Die genauere Vorgehensweise in Systemback finden Sie ebenfalls im E-Book „LinuxWelt XXL digital" auf Heft-DVD. Das Ergebnis ist dann ein unveränderliches Livesystem, das bei Bedarf ein virtuelles Linux starten kann, Dieses erkennt keine physischen Medien des Rechners und arbeitet mit virtueller IP außerhalb des lokalen Adressraums. Das ist insgesamt gewiss kein warmes Biotop für handelsübliche (Windows-)Malware! ■

Der Raspberry Pi als Firewall

Mit einer Firewall wird der Netzwerkverkehr reglementiert. Zwar besitzt jeder Router eine solche Funktion, allerdings haben Sie darauf nur sehr eingeschränkten Zugriff. Wenn Sie mehr Sicherheit für Ihr Netzwerk wollen, dann bietet sich eine eigene Lösung an.

VON STEPHAN LAMPRECHT

Wer mit seinem Rechner nur im Internet surft und seine Büroarbeiten erledigt, wird sich mit dem Thema Firewall kaum beschäftigen. Kommen dagegen Geräte für die Heimautomatisierung oder andere IoT-Basteleien zum Einsatz, sieht das schon anders aus. Denn für den Fernzugriff auf Steuerelemente oder Sensoren muss das heimische Netzwerk nach außen für das Internet geöffnet werden. In solchen Szenarien erhöht eine selbst gebaute Firewall die Sicherheit spürbar.

Achtung, Sie verlassen die Komfortzone!

In diesem Artikel lernen Sie zwei verschiedene Ansätze kennen, wie ein Platinenrechner wie der Raspberry Pi als Firewall eingesetzt wird. Allerdings müssen Sie zur Umsetzung schon Spaß mitbringen, mit Terminalbefehlen und manuell in Konfigurationsdateien zu arbeiten. Und da sich alle Komponenten in einer stetigen Weiterentwicklung befinden, stoßen Sie möglicherweise auf Probleme, die sich eventuell nur nach einer intensiveren Recherche im Internet lösen lassen. Was etwa mit dem Raspberry 3 unter einer bestimmten Konfiguration funktioniert hat, muss es mit dem Modell 2 und ansonsten identischen Optionen leider nicht tun. Das hat unter anderem auch damit zu tun, dass die Hersteller von Chipsätzen sich nach wie vor sehr verhalten in ihre Karten schauen lassen, was es den Entwicklern erschwert, die Unterstützung der Geräte zu programmieren.

```
Datei  Bearbeiten  Ansicht  Suchen  Terminal  Hilfe
sla@raspi:~$ sudo ufw allow ssh
[sudo] Passwort für sla:
Regeln aktualisiert
Regeln aktualisiert (v6)
sla@raspi:~$
```

Die Steuerung von ufw erfolgt über einfache Kommandos in einem Terminal. Das Programm ist gut dokumentiert und das Set an Befehlen nicht schwer zu merken.

Lösungsansatz 1: WLAN-Bridge einsetzen

Anders als ein Router besitzt der Raspberry nur einen Ethernet-Anschluss. Und diese Tatsache erfordert Anpassungen und Bastelarbeiten, damit der Netzwerkverkehr durch den Ein-Platinen-Rechner geleitet wird. Der erste Lösungsansatz verwandelt den kleinen Computer in eine WLAN-Bridge. Die Daten werden per Ethernet-Kabel mit dem Router ausgetauscht und durchlaufen dabei die Firewall des Raspberry Pi. Die Clients melden sich drahtlos am Raspberry an und beziehen die so gefilterten Datenpakete. Das ist mit Bordmitteln umzusetzen. Zum Einsatz kommt das Programm Uncomplicated Firewall (ufw). Das ist streng genommen keine eigene Firewall im Wortsinn, sondern vereinfacht nur die Konfiguration der ohnehin eingebauten Funktionen. Das Paket installieren Sie wie gewohnt direkt aus einer Konsole heraus mit

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

Die Installation schließt auch gleich eine Reihe von fundamentalen Regeln für die Firewall ein.

Firewall aktivieren und Regeln hinterlegen: Im Grundzustand geht das System davon aus, dass nur Verbindungen zugelassen werden, die ausdrücklich erlaubt sind.

Deswegen sollten Sie zunächst die Verbindung per SSH zulassen, um sich von einem externen System auf dem Raspberry anmelden zu können. Das erledigen Sie mit

```
sudo ufw allow ssh
```

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

```
sudo ufw enable
```

aktivieren Sie das Regelwerk. Die Anwendung weist Sie darauf hin, dass das Kommando eine möglicherweise bestehende SSH-Verbindung beeinträchtigen könnte. Mit „y“ fahren Sie fort. Damit sind die Regeln ab sofort gültig. Mit dem Parameter „disable“ wird die Firewall bei Bedarf wieder deaktiviert – also:

```
sudo ufw disable
```

Bei der Einrichtung weiterer Regeln können Sie wie schon oben bei „ssh“ einfach die Protokollbezeichnungen verwenden. Soll der Raspberry als Webserver arbeiten, erlauben Sie den Datenverkehr über das Protokoll HTTP:

```
sudo ufw allow http
```

Arbeitet der Computer als Dateiserver, schalten Sie SMB (CIFS) frei. In diesem Fall erlauben Sie das Protokoll „cifs“. Daneben kennt das Regelwerk aber auch eine ganze Reihe von Anwendungen, die spezielle Regeln erfordern. Mit

```
sudo ufw app list
```

lassen Sie sich eine Liste der so erkannten Anwendungen ausgeben. Mit „allow appname“ werden die Regeln für die Anwendung dann aktiviert.

Raspberry Pi als sichere Bridge konfigurieren: Mit der Firewall schützt der Raspberry sich selbst und die darauf laufenden Anwendungen. Das ist eine gute Basis, um das Netzwerk insgesamt sicherer zu machen. Eine Bridge verwendet das Standardgateway (also die Verbindung zum Internet etwa über den DSL-Anschluss) und einen bereits vorhandenen DHCP-Server (in diesem Fall den des Routers).

Die Einrichtung des Systems ist an sich nicht schwierig. Je nach Modell (externer WLAN-Dongle) muss erst geprüft werden, ob der Chipsatz den AP-Modus beherrscht, also als WLAN-Access-Point arbeiten kann. Die Abfrage erledigen Sie mit dem folgenden Befehl:

```
iw list | grep AP
```

Werden mehrere Zeilen mit „AP“ angezeigt, kann es weitergehen. Wird das Kommando iw erst gar nicht ausgeführt, müssen Sie das Tool erst mit *sudo apt install iw* nachinstallieren.

So sieht exemplarisch die Konfiguration des WLANs aus, das in der Netzwerkbrücke des Raspberry verwendet werden soll.

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

# Bridge-Betrieb
bridge=br0

# Schnittstelle und Treiber
interface=wlan0
#driver=nl80211

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

# WLAN-Verschlüsselung
wpa=2
```

Damit die Brücke funktioniert, ist es wichtig, dass der DHCP Client Daemon aktiviert ist. Das prüfen Sie einfach mit diesem Befehl, der „active“ melden sollte:

```
service dhcpd status
```

Außerdem müssen sowohl die Ethernet-Schnittstelle als auch der WLAN-Adapter vorhanden sein und funktionieren. Der Befehl

```
ip l
```

zeigt die gewünschten Informationen an und meldet Ethernet als „eth0“ oder „enp5/6s0“, ferner den WLAN-Adapter als „wl[...]“.

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

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

Ist die Installation erfolgreich abgeschlossen, beginnt die Konfiguration des Access Points. Dazu editieren Sie zunächst eine Konfigurationsdatei:

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

Dort müssen einige Zeilen eingetragen werden. Unter „SSID“ vergeben Sie den Namen für das Netzwerk, das die Clients nutzen können. Außerdem müssen Sie den Kanal (Channel) einstellen. Weichen Sie hier am besten auf Kanäle aus, die nicht von den Routern aus der Nachbarschaft genutzt werden. Zur Kontrolle helfen Router wie die Fritzbox („WLAN → Funkkanal“), die eine Übersicht anbieten, wie viele andere Funknetzwerke aktuell auf den gleichen Kanälen senden. Schließlich sollten Sie ein sicheres Passwort für die Verschlüsselung setzen. Der ganze Block in der „hostapd.conf“ für die Verschlüsselung sieht dann so aus:

```
wpa=2
wpa_key_mgmt=WPA-PSK
rsn_pairwise=CCMP
wpa_passphrase=das.passwort.
```

In der Konfigurationsdatei finden Sie einen Beispieleintrag für den Treiber des WLAN-Adapters. Der ist auskommentiert, da hostapd eigentlich automatisch den korrekten Treiber laden sollte. Lediglich wenn es zu keiner Verbindung kommt, können Sie hier manuelle Änderungen vornehmen. Mit Strg-O und Strg-X speichern Sie die Datei und beenden den Editor. Da die Datei das Passwort für das WLAN im Klartext enthält, werden die Rechte so beschränkt, dass nur root Leserecht hat:

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

Jetzt verbleibt noch, die IP-Konfiguration der Schnittstellen einzurichten und die Details der Brücke einzurichten. Dazu editieren Sie mit

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

die dafür zuständige Datei. In der Abbildung auf der folgenden Seite sehen Sie unter „Netzwerbrücke“ die wesentlichen Einträge. Die beiden Adapter für Ethernet und WLAN haben hier die Kennung „eth0“ und „wlan0“.

Die Bridgefunktionalität und die Details für den Netzwerkzugriff werden ebenfalls in einer Textdatei geregelt.

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

# Localhost
auto lo
iface lo inet loopback
# Ethernet
auto eth0
allow-hotplug eth0
iface eth0 inet manual
# WLAN
auto wlan0
allow-hotplug wlan0
iface wlan0 inet manual
wireless-power off
# Netzwerkbrücke
auto br0
iface br0 inet manual
bridge_ports eth0 wlan0 # build bridge
bridge_fd 0             # no forwarding delay
bridge_stp off          # disable Spanning Tree Protocol
```

Danach starten Sie das System neu. Mit

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

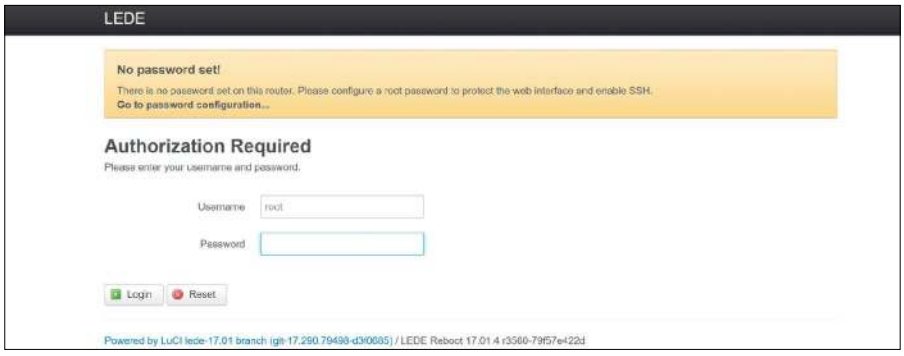
können Sie anschließend überprüfen, ob Ihr neues WLAN funktioniert.

Lösungsansatz 2: LEDE für Bastler

Der zweite Ansatz ist anspruchsvoller. Neben der Raspberry-Platine und einem zweiten Ethernet-Port benötigen Sie die Distribution LEDE – ein Fork des bekannteren Projekts Open WRT. Dabei handelt es sich im Kern um die Software für den Betrieb eines Routers. Den notwendigen zweiten Ethernet-Anschluss kann ein passender USB-Adapter nachrüsten. In unserem Fall kommt ein USB-Adapter mit einem MosChip 7830 vom Hersteller Hama zum Einsatz (circa 25 Euro). Für Platinen mit USB 3.0 eignet sich der Delock Adapter 62616 (circa 25 Euro).

Die nachfolgende Anleitung hat folgende grundsätzliche Abfolge: Zuerst wird erst die Distribution LEDE installiert, danach die zweite Ethernet-Schnittstelle mit dem Platinenrechner verbunden und schließlich die Schnittstelle zum Router des Providers eingerichtet. Zum Einsatz kommen in diesem Beispiel ein Raspberry Pi 3 und der genannte Hama-Adapter. An die zweite Ethernet-Schnittstelle können Sie am Ende etwa einen weiteren eigenen Router anschließen, mit dem Sie dann Ihr Heimnetzwerk verbinden.

LEDE installieren: Die Installation von LEDE auf dem Raspberry ist nicht schwierig. Das Projekt PINN (*https://github.com/procount/pinn*) hat die Software mit an Bord. Dabei handelt es sich um eine Variante von Noobs, dem bekannten grafischen Installer für den Raspberry. Laden Sie sich die aktuelle Version von der Projektseite und installieren Sie diese wie gewohnt. Dazu genügt es, eine SD-Karte zu formatieren und den Inhalt des ZIP-Archivs darauf zu übertragen. Verbinden Sie den Pi mit Tastatur, Maus, Monitor und dem Internet. Starten Sie den Raspberry und wählen Sie aus den angebotenen Distributionen „LEDE“ aus. Ist die Installation abgeschlossen, starten Sie den Rechner neu.



Sobald LEDE eine IP-Adresse vom Router erhalten hat, kann die weitere Einrichtung per Browser erledigt werden. Beim ersten Anmelden sollten Sie ein Passwort hinterlegen.

LEDE lauffähig machen: Die eigentliche Konfiguration des Systems können Sie mit dem Browser durchführen. Davor müssen Sie allerdings einmalig eine etwas umständliche Prozedur auf sich nehmen. Sobald LEDE keine Meldungen beim Systemstart ausgibt, drücken Sie die Eingabetaste, um auf die Konsole zu gelangen. Denn Sie müssen die Netzwerkkonfiguration anpassen, da LEDE eine statische IP-Adresse verwendet, die vom Router belegt sein dürfte. Zum Editieren steht Ihnen nur der Editor vi und das auch noch mit US-Tastaturbelegung zur Verfügung. Das Zeichen „/“ finden Sie auf der Taste „-“. Öffnen Sie im Terminal die maßgebliche Konfigurationsdatei mit vi:

```
vi /etc/config/network
```

Da Sie die Datei editieren wollen, müssen Sie zunächst „*i“ eingeben, um den Eingabemodus zu aktivieren. Dieser wird später dann wieder mit Esc-Taste beendet. Das Sternchen befindet sich beim englischen Layout auf der „Klammer-auf“-Taste. Ändern Sie in der Textdatei unter

```
config interface 'lan'
```

die Zeile mit dem Eintrag „static“ auf „dhcp“. Die gesamte Zeile sollte dann so aussehen:

```
option proto 'dhcp'
```

Löschen Sie die darunter angegebene IP-Adresse. Speichern und Schließen funktioniert bei vi mit „:x“ wobei der Doppelpunkt über „Ö“ einzugeben ist (Umschalt-ö).

Starten Sie anschließend den Pi neu. Der Raspberry hat vom Router eine neue IP-Adresse bezogen. Fragen Sie diese auf dem Raspberry mit ifconfig ab oder schauen Sie im Router nach.

Mit dieser IP-Adresse können Sie sich jetzt von einem anderen Rechner im lokalen Netz per Browser verbinden. Beim ersten Aufruf der Seite werden Sie um die Eingabe eines Kennworts gebeten. Dadurch wird auch der SSH-Zugang freigeschaltet. So können Sie sich später auch von anderen Rechnern direkt auf der Systemebene bewegen.

Klicken Sie nun auf „System → Software“. Sie müssen jetzt zunächst das für den Ethernet-Adapter passende Kernel-Modul laden. Das geht in der Regel unter Angabe des verwendeten Chipsatzes. In unserem Fall führt „mcs7830“ zum Erfolg. Den Suchbegriff geben Sie dabei in die Zeile neben „Find“ ein und klicken dann auf „Install“ neben dem Paketnamen. Dieser Adapter taucht dann später als weiterer Anschluss auf.

Neues Interface anlegen: Wechseln Sie nun nach „Network → Interfaces“. Dort ist ein Eintrag „WAN“ vorhanden. Diesen können Sie mit „Delete“ entfernen. Legen Sie dann über „Add new interface“ ein neues Interface an.

Erstellen Sie das Interface namens „WAN“ mit dem Protokoll „DHCP client“ für den Ethernet-Adapter „eth1“ (das ist der externe USB-Ethernet-Adapter). Dadurch wird dieser Anschluss als externe Schnittstelle zum Router definiert, der an Ihrer Anschlussdose hängt. Im Firewall-Tab des WAN-Interfaces legen Sie dann WAN als Firewall-Zone fest.

Internen Ethernet-Anschluss konfigurieren: Jetzt bearbeiten Sie mit einem Klick auf „Edit“ den LAN-Anschluss „eth0“. Der interne Anschluss des Raspberry wird jetzt mit statischer IP-Adresse und DHCP-Funktion ausgestattet, damit das interne Netzwerk automatisch IP-Adressen erhält. Ändern Sie dazu zunächst das Protokoll auf „static“ und bestätigen Sie. Anschließend können Sie eine statische Adresse aus dem bisherigen Adressraum vergeben, zum Beispiel „192.168.178.2“. „Ipv4 netmask“ setzen Sie auf 255.255.255.0, die restlichen Felder lassen Sie leer.

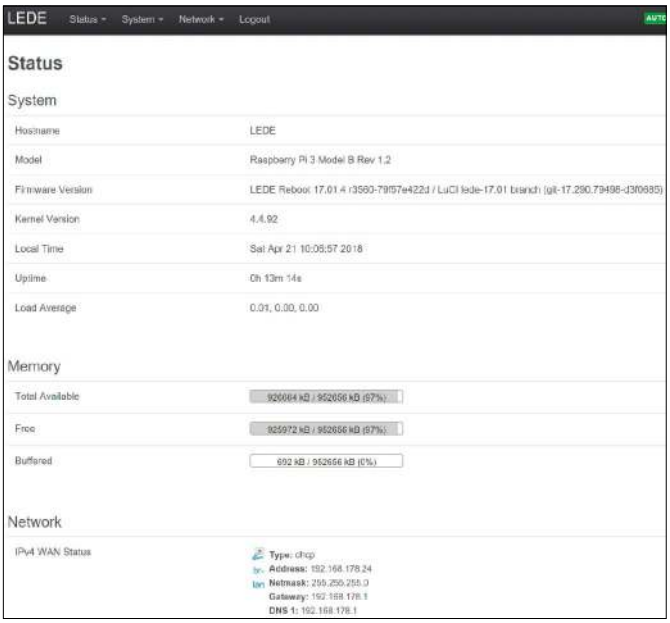
Die Adresse, die Sie vergeben haben, müssen Sie sich merken. Denn wenn Sie nun „Save & Apply“ geklickt haben, kann der Raspberry nur noch über diese Adresse erreicht werden. Unter „Advanced Settings“ können Sie noch die Force-Option setzen, damit andere DHCP-Server das System nicht stören. Rufen Sie nun das System über die neue Adresse auf und starten Sie das System über „System/Reboot“ neu.

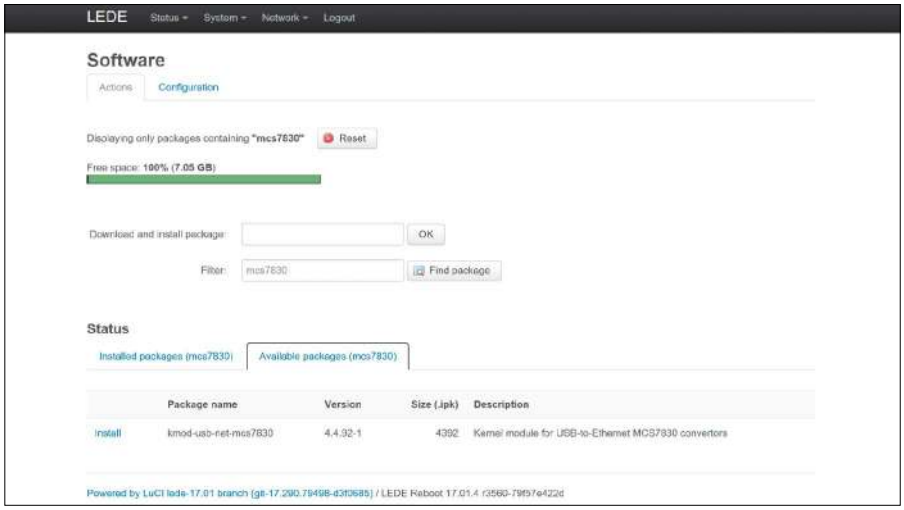
Der zweite Ethernet-Anschluss des Raspberry kann jetzt dazu genutzt werden, weitere Geräte anzuschließen.

Nutzen Sie zum Beispiel einen zweiten Router, um damit ein internes WLAN aufzuspannen. Bevor Sie sich an weitläufiges Umstecken machen, verbinden Sie aber zunächst einfach einen einzelnen Rechner direkt mit diesem zweiten LAN-Anschluss. Die Konfiguration funktioniert, wenn Sie dann die Oberfläche von LEDE wieder über die feste IP-Adresse des Geräts erreichen. Danach können Sie sich ans Experimentieren machen.

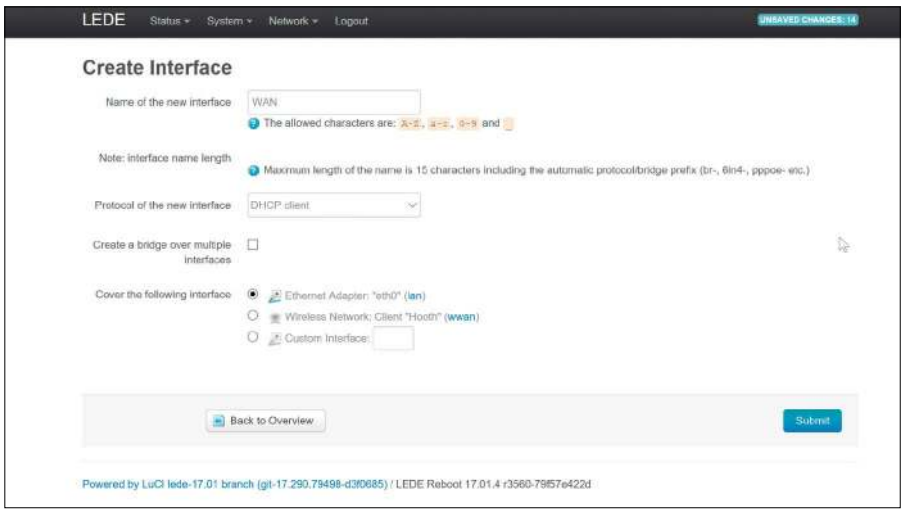
Sie betreiben jetzt eine eigene Firewall und haben eine Mauer zwischen Ihrem internen Netzwerk und dem Router für den Internetzugriff errichtet. ■

Mit der Statusseite behalten Sie das LEDE-System im Blick. Derzeit ist erst eine Schnittstelle angelegt, weil noch der Treiber für den externen Adapter fehlt.





Zum Betrieb des externen Ethernet-USB-Adapters wird ein Kernel-Modul benötigt. Über den verwendeten Chipsatz kann meist ein passendes Modul gefunden werden.



Hier legen Sie eine neue Schnittstelle in LEDE an. Deren Rolle ist hier als DHCP-Client definiert.

Proxyserver mit Linux

Als eine Internetverbindung noch über Modem oder ISDN ins Haus kam, waren eigene Proxyserver ein echter Geschwindigkeitsvorteil. Proxys sind aber auch zum Filtern oder Weiterleiten von Webtraffic über eine andere IP-Adresse sinnvoll.

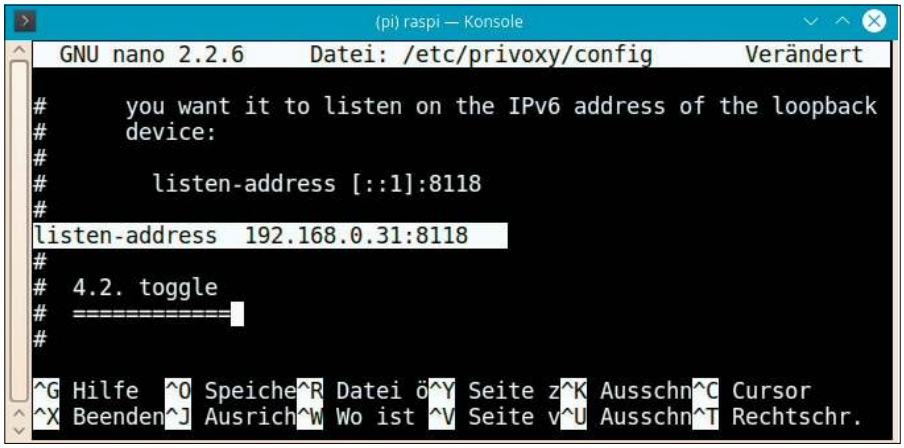
VON DAVID WOLSKI

Die Idee eines eigenen Proxyservers als zusätzlicher Zwischenspeicher für abgerufene Webinhalte kann Inhaber eines schnellen Internetzugangs ohne Volumenbegrenzung zunächst kalt lassen. Für jene Anwender, die eine langsame Internetverbindung haben, aus der mehrere Teilnehmer mit Webbrowsern beständig Daten zapfen, ist ein lokaler Proxy weiterhin interessant und verspricht bessere Geschwindigkeiten beim Surfen. Wo immer mehrere PCs und Geräte über den Browser Seiten aufrufen, gibt es Überschneidungen bei den abgerufenen Inhalten. Ein zwischenspeichernder Proxy liefert bereits per HTTP abgefragte Inhalte im Cache deutlich schneller aus als der entfernte Webserver. Reizvoll, gerade für Smartphones und Tablets, ist außerdem ein filternder Proxyserver, der bekannte Hosts von großen Werbefirmen blockiert und deren Werbebanner nicht weitergibt. Nicht zuletzt ist ein Proxyserver dann von Nutzen, wenn man im Browser seine eigene IP verschleiern möchte, um damit etwa Ländersperren zu umgehen.

Privoxy: Ein Proxy mit Filter

Ein zentraler Proxyserver im LAN kann als Client für Smartphones und Tablets als vorgeschalteter Werbefilter arbeiten. Der Proxy kann damit an einer zentralen Stelle dubiose Advertisingnetzwerke auf Webseiten blockieren, störende Banner filtern und Besuchertracker aussieben. Privoxy ist kein zwischenspeichernder Cache, sondern ein Filter. Der Proxy ist deshalb auch bei HTTPS-Verbindungen nützlich: Erkennt der Proxy einen Werbeanbieter in einer abgefragten URL, dann wird auch eine HTTPS-Anfrage blockiert. Andere HTTPS-Daten reicht der Proxy hingegen unverändert an den Browser weiter.

Privoxy läuft auf jedem Linux-System, kommt auch mit bescheidener Hardware zurecht oder läuft auf einem anderweitig genutzten Linux-PC brav im Hintergrund. Trotzdem haben sich die älteren beziehungsweise kleineren Modelle des Raspberry Pi als unzulänglich erwiesen: Die ARM-CPU mit einem Kern liefert für die Filterregeln von Privoxy nicht genügend Leistung, wenn mehrere Clients im Netzwerk auf den Proxy zugreifen. Erst ab einem Raspberry Pi 2 steht genügend Leistung bereit. Die Platine kann als Proxyserver nach empirischen Erfahrungswerten bis



Privoxy in Betrieb nehmen: Bevor der Proxyserver für andere im LAN erreichbar ist, muss diese Zeile in der Konfiguration mit der IP-Adresse des Server versehen werden.

zu fünf Netzwerkteilnehmer bedienen. In allen verbreiteten Linux-Distributionen steht Privoxy fertig als Paket zur unkomplizierten Installation über den jeweiligen Paketmanager bereit. Unter Debian, Ubuntu, aber auch in Raspbian, ist der Proxyserver über den Befehl

```
sudo apt-get install privoxy
```

in der Kommandozeile flott installiert. Privoxy erwartet aber noch die Konfiguration, damit der Proxyserver im Netzwerk bereitsteht. Die mitgelieferte Konfigurationsdatei „/etc/privoxy/config" verlangt dazu nur in einem Detail eine manuelle Anpassung: Um Privoxy erst mal mit Standardeinstellungen in Betrieb zu nehmen, ist im Abschnitt 4.1 die Zeile

```
listen-address localhost:8118
```

nach

```
listen-address [IP-Adresse]:8118
```

zu ändern, wobei der Platzhalter „[IP-Adresse]" für die die tatsächliche lokale IP-Adresse des Servers im LAN steht. Die Zeile lautet also beispielsweise „listen-address 192.168.1.31:8118". Wie bei jedem Serverdienst sollten Sie auch hier dafür sorgen, dass der zuständige Rechner vom Router eine feste IP erhält, damit die in die Proxykonfiguration eingetragene Adresse dauerhaft Gültigkeit hat.

Danach starten Sie den Privoxy-Dienst mit dem Befehl

```
sudo systemctl restart privoxy.service
```

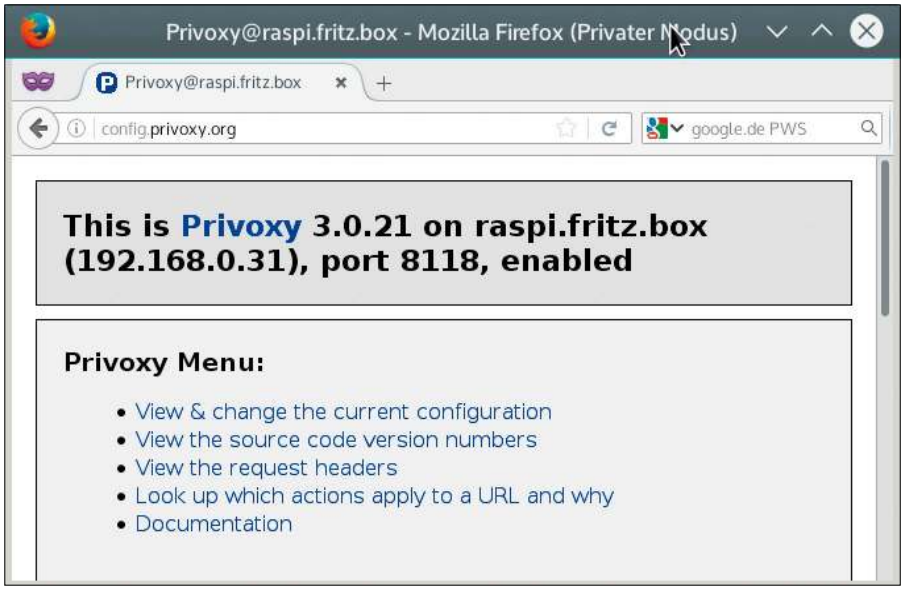
neu. Auf älteren Versionen von Debian und Ubuntu (ohne Systemd) lautet der Befehl folgendermaßen:

```
sudo service privoxy restart
```

Bei den Distributionen, die von Debian abstammen, hat sich Privoxy schon bei der Installation selbständig über das Init-System als Dienst eingerichtet, aber bei Fedora und Open Suse muss dieser Schritt noch mit dem Kommando

```
sudo systemctl enable privoxy.service
```

nachgeholt werden.



Verbindungstest: Die URL *http://config.privoxy.org* zeigt eine Diagnoseseite an, die auf einen Blick zeigt, ob die Einrichtung der Proxyadresse auf dem Client geklappt hat.

Ob der Proxyserver läuft und auf dem Port 8118 auf eingehende Verbindungen wartet, zeigt das Kommando

```
netstat -a | grep 8118
```

an. Gibt der Befehl etwa Folgendes aus, war die Einrichtung erfolgreich:

```
tcp 0 0 raspberrypi:8118 *:* LISTEN
```

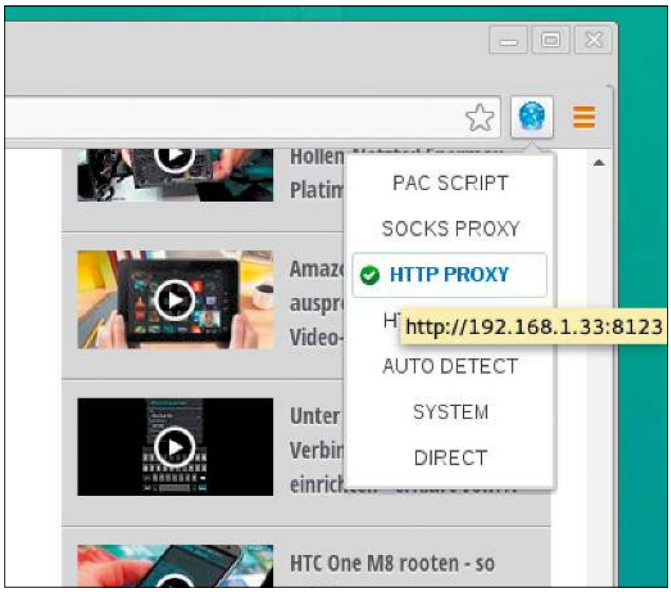
Jetzt können Sie in Browsern anderer PCs

PROXY IN OPERA: LÄNDERSPERREN UMGEHEN

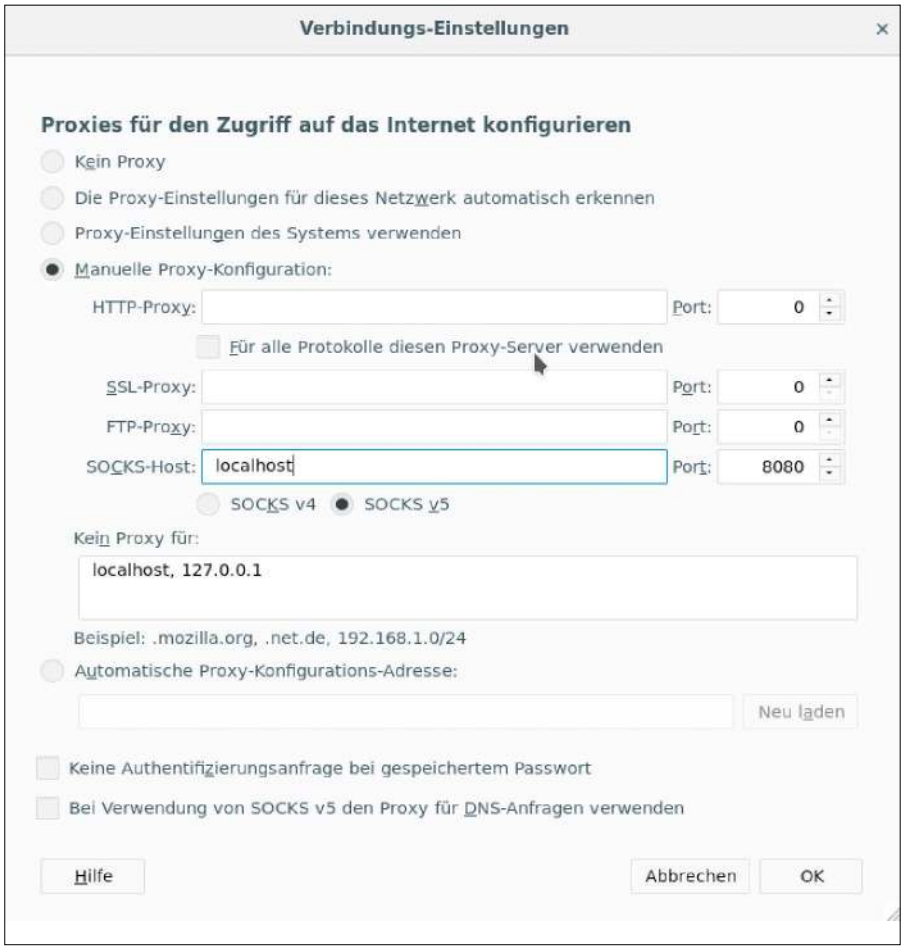
Der Browser Opera hat seit 2016 einen eigenen Proxydienst, der direkt im Browser verfügbar ist.

Opera steht als DEB-Paket für Debian, Ubuntu, Linux Mint und auch als RPM-Datei unter *http://www.opera.com* zum Download bereit. Der Proxyservice ist kostenlos und wird von der kanadischen Firma Surfeasy Inc. bereitgestellt. Meist nutzt Opera aber keine Server in Kanada, sondern in den Niederlanden, um die wahren IP-Adressen von Opera-Nutzern zu verschleiern. Irreführend ist, dass Opera diesen Proxy als „VPN" ausgibt, denn diese Bezeichnung trifft hier nicht. Anders als in einem echten VPN leitet der Browser nur den eigenen Traffic und DNS-Abfragen an einen Proxyserver weiter. Es gilt außerdem zu beachten, dass ist dieser Proxy kein Anonymisierungsdienst ist. Für eine schnelle Umgehung von Ländersperren ist der Dienst aber durchaus geeignet und schnell eingerichtet: In Opera findet sich die VPN-Option über das Menü „Bearbeiten → Einstellungen → Datenschutz & Sicherheit → VPN aktivieren". Ab sofort taucht neben der URL ein VPN-Symbol auf, das den Dienst ein- und ausschalten kann. Ein Klick darauf zeigt außerdem die eigenen Nutzungsstatistiken an.

Proxyservice inklusive: In Opera gibt es eine Funktion, den Traffic über den VPN-Anbieter Surfeasy umzuleiten. Ländersperren lassen sich damit aushebeln.



Chrome und Chromium: Da diese Browser den Standardproxy des Systems als Voreinstellung nehmen, ist die Browsererweiterung Proxy Helper eine sinnvolle und komfortable Ergänzung.



Socks-Proxy in Firefox: Ist die SSH-Verbindung mit Socks-Option aktiv, dann steht ein Proxyport auf dem „localhost“ zur Verfügung. Die Browseranfragen werden dann über SSH umgeleitet.

im lokalen Netzwerk sowie auf Mobilgeräten die IP-Adresse des Servers samt Port 8118 als Proxyserver angeben. Um die Konfiguration zu testen, rufen Sie im Browser zunächst die Diagnoseseite *http://config.privoxy.org* auf. Wenn sich Privoxy dort mit „This is Privoxy“ meldet, dann ist die Proxyverbindung aktiv.

Bereits ohne weitere Einstellungen filtert Privoxy mit sehr hoher Trefferquote ab sofort unerwünschte Werbung und Tracker beim Surfen aus und reduziert Banner in Apps.

Browser: Verbindung zum Proxy

Die Browser, welche Privoxy nutzen sollen, richten Sie nun so ein, dass diese die IP-Adresse des Raspberry Pi als Proxy verwenden. In Firefox finden Sie diese Option in den Einstellungen unter „Erweitert → Netzwerk → Verbindung → Einstellungen“. Aktivieren Sie hier die „manuelle Proxy-Konfiguration“ und tragen Sie im Feld „HTTP-Proxy“ die IP des Raspberry ein, in dieser Beispielanleitung als 192.168.1.33. Den „Port“ dahinter legen Sie auf „8118“ fest. Chrome/Chromium verwenden dagegen die Proxy-Standardeinstellung des Systems oder müssen mit der Proxyangabe als Startparameter nach dem Schema

```
/usr/bin/google-chrome --proxy-
  server="[IP-Adresse]:8123"
```

beziehungsweise bei Chromium mit

```
/usr/bin/chromium-browser --proxy-
  server="[IP-Adresse]:8118"
```

aufgerufen werden.

Die kostenlose Erweiterung Proxy Helper (*http://goo.gl/KWShDo*) vereinfacht die Proxykonfiguration in Chrome/Chromium, insofern sie ein Extrasymbol in der Symbolleiste der Browser unterbringt.

Socks-Proxy: Einfach per SSH

Um den Traffic im Browser im Stil eines Pseudo-VPNs verschlüsselt über einen Proxy umzuleiten, bedarf es nur wenig Vorbereitung und Konfigurationsarbeit. Denn der SSH-Server von Linux, der meist sowieso zur Grundausstattung gehört, kann auch als Proxyserver dienen und allen Browsern und Programmen über das Socks-Protokoll eine Schnittstelle bieten.

Nützlich ist ein eigener Socks-Proxy, um die IP des entfernten Systems für Besuche auf Webseiten zu nutzen oder um den eigenen Traffic im lokalen Netz durch Verschlüsselung wie in einem VPN zu schützen.

Der SSH-Serverdienst gehört auf einem Linux-System zur Grundausstattung, ist aber im Bedarfsfall auch schnell nachinstalliert. In Debian, Ubuntu und Raspbian erledigt der Befehl

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

nicht nur die Installation, sondern setzt den Dienst auch gleich in Gang.

Der einzig aufwendigere Schritt ist die allgemeine Vorbereitung des Servers, um über das Internet erreichbar zu werden. Hier ist wieder die typische Portweiterleitung im Router zum Rechner mit dem Socks-Proxy erforderlich. Der Standardport für SSH ist Port 22. Ebenfalls Standard in solchen Fällen ist die Einrichtung eines dynamischen Hostnamens etwa über No-IP (*https://www.noip.com*), Free DNS (*https://freedns.afraid.org*) oder ähnliche Dienste. Danach sind dann Anmeldungen über SSH aus dem Internet heraus möglich: Der Browser geht dann über den heimischen Anschluss ins Internet und der eigentliche Verkehr bleibt so in unsicheren Netzwerken und WLANs verborgen.

1. Zum Aufbau der Verbindung verbinden Sie sich in einem Terminalfenster mit dem folgenden Befehl

```
ssh -ND 8080 [User]@[Hostname]
```

zum eigenen Server zu Hause. Das Terminalfenster bleibt anschließend für die Dauer der Verbindung geöffnet.

2. Steht die SSH-Verbindung, geht man in die Browsereinstellungen und trägt dort als „SOCKS Host" beziehungsweise „SOCKS Proxy" einfach „localhost" ein und als Port 8080. Ab jetzt gehen die Browseranfragen per SSH zunächst zum Server, der die Webseiten als Proxy abruft und verschlüsselt zurück zum Browser schickt. Das Terminalfenster muss dazu geöffnet bleiben. Der Datendurchsatz zwischen SSH-Client und Server ist zwar nicht schnell, weil eine ungünstige Kapselung von TCP über TCP stattfindet, dabei aber verschlüsselt wie bei einem echten VPN.

Für Windows-Clients: Auch Windows profitiert vom Linux-Server zu Hause und kann die SSH-Verbindung nutzen. In dieser Konstellation braucht der Windows-Rechner den Terminalclient Putty (auf Heft-DVD, Download unter *http://www.pcwelt.de/729799*). In Putty geht man zum Aufbau eines Tunnels nach der Konfiguration der Serveradresse unter „Session" auf „Connection → SSH → Tunnels" und trägt unter „Source Port" eine Portnummer für den Tunnel ein, etwa die 8080. Außerdem aktiviert man die Option „Dynamic" und geht dann auf „Add", um einen Eintrag unter „Forwarded Ports" zu erzeugen. Im Webbrowser, am besten im Firefox, der seine eigene Proxykonfiguration mitbringt, ist jetzt ein Besuch der Proxyeinstellungen nötig: Unter „Einstellungen → Netzwerk-Proxy → Einstellungen" aktivieren Sie die „Manuelle Proxy-Konfiguration" und geben unter „SOCKS-Host" den „localhost" ein und als Port den zuvor in Putty eingerichteten Sourceport, in unserem Beispiel „8080". Soll die Verbindung zum Internet im Browser wieder ohne Socks-Proxy erfolgen, schalten Sie im Firefox diese Netzwerkeinstellungen wieder zurück auf „Kein Proxy". ■

PI-HOLE: WERBUNG BLOCKIEREN

Unerwünschte Inhalte filtern – das geht nicht nur mit einem Proxyserver, sondern auch mit einem filternden DNS-Server. Genau dies leistet die Open-Source-Software Pi-Hole (*https://git.io/vpChm*).

Weil dieser Filter auf DNS-Ebene arbeitet, funktioniert Pi-Hole für alle Protokolle und verlangt auf den Clientgeräten keine Anpassung der Proxyeinstellungen. Pi-Hole muss stattdessen als Domain Name Server eingetragen werden – am besten zentral auf dem verwendeten Router im Heimnetz. Die verbundenen Clients bekommen dann die Adresse des Pi-Hole-Servers als DNS automatisch per DHCP mitgeteilt.

Zwar weist schon der Name darauf hin, dass sich dieser Server auf einem Raspberry Pi zu Hause fühlt, die Software läuft aber auch auf jedem regulären Debian, Ubuntu, Fedora oder Cent-OS. Der PC oder die Platine, auf welcher Pi-Hole laufen soll, benötigt im LAN eine feste IP-Adresse, die man dem Rechner in der Administrationsoberfläche des Routers zuerst zuweisen muss.

Zur Installation liefern die Entwickler ein Bash-Script, das die Einrichtung in wenigen Schritten erledigt. Bevor Sie das Script herunterladen und ausführen können, sollten Sie sich noch das Kommandozeilentool curl installieren, das in den Paketquellen aller verbreiteten Linux-Distributionen vorliegt. Anschließend startet der Befehl

```
curl -sSL https://install.pi-hole.net | bash
```

die Installation. Das Script zeigt im Terminal zu jedem Schritt, der eine Eingabe zur Konfiguration erwartet, englischsprachige Menüs an und rüstet eventuell zusätzlich benötigte Pakete bei Bedarf über den jeweiligen Paketmanager nach. Nach der gelungenen Installation zeigt Pi-Hole nochmal die eigene IP-Adresse an sowie eine URL, die im lokalen Netzwerk eine hübsche Statistik im Browser anzeigt. Wichtig ist, sich das hier angezeigte Admin-Passwort für die erste Anmeldung auf dieser Übersichtsseite zu notieren.

Damit Pi-Hole etwas zu tun bekommt, trägt man die lokalen IP-Adressen (IPv4 und IPv6) des Pi-Hole-Servers in den DNS-Einstellungen des Routers ein. In den Administrationsmenüs der verbreiteten Fritzbox findet sich diese Einstellung beispielsweise unter „Internet → Zugangsdaten → DNS-Server", sofern rechts oben die „Erweiterte Ansicht" aktiviert ist. Falls der Router keine Änderung der DNS-Einstellungen gewährt, dann können Sie die IP-Adressen des Pi-Hole-Servers aber auch direkt auf den Clients in deren Netzwerkkonfiguration als DNS eintragen.

Blockiert DNS-Abfragen: Bei Pi-Hole handelt es sich um keinen Proxyserver, sondern um einen DNS-Server für das LAN. Das Programm filtert die bekannten Domains von Werbeanbietern.

Sicher im VPN

Zwei Nutzen hat ein Virtual Private Netzwerk (VPN): Erstens stellt es einen sicheren, verschlüsselten Tunnel ins heimische Netzwerk her. Zweitens verbirgt es den Inhalt des Datenverkehrs vor den Betreibern der Internetverbindung.

VON DAVID WOLSKI

Verschlüsselt und damit abhörsicher etabliert ein Virtual Private Network eine Verbindung zu einem VPN-Server oder zu einem VPN-Gateway zu einem lokalen Netzwerk. Eine bewährte Lösung dazu ist Open VPN: Es ist Open Source, hat zwei unabhängige Audits hinter sich, die keine schlimmen Lücken fanden, und es ist eine reine Softwarelösung. Das heißt, sie verlangt keine zusätzliche Hardware, keine speziellen VPN-Router und läuft auf jedem Linux-System.

Die Software ist allerdings für den professionellen Einsatz geschaffen und die erste Konfiguration eines Open-VPN-Servers und seiner Clients stellt immer eine gewisse Hürde dar. Allen die Beschreibung der Grundlagen wäre seitenfüllend. Stattdessen geht es hier um findige Alternativen zum unkomplizierten Aufbau eines VPNs mit den Mitteln einer typischen Linux-Distribution. Auch Open VPN ist dabei, allerdings in einer einfach gehaltenen Variante für den Raspberry Pi, die weitaus schneller eingerichtet ist.

Statt VPN das alternative Sshuttle

Das Python-Tool „Sshuttle“ (*http://sshuttle.readthedocs.io*) ist eine findige Lösung, die auf dem SSH-Protokoll aufsetzt und auf dem VPN-Server lediglich einen laufenden Open-SSH-Server verlangt. Diese Rolle kann jederzeit ein kleiner Raspberry Pi übernehmen. Die Leistung der Platine und die Geschwindigkeit des 100-MBit-Ethernet-Ports reichen für ein Netzwerk, das per DSL an die Außenwelt angebunden wird.

Genau genommen handelt sich bei Sshuttle nur um eine Clientkomponente. Diese wurde kürzlich in Python 3 neu geschrieben und läuft deshalb auf nahezu jedem Linux-System. Auf dem Client, der am entfernten Netzwerk teilnehmen soll, baut Sshuttle eine verschlüsselte SSH-Verbindung zum Server auf. Über diese Verbindung überträgt das Tool während des Verbindungsaufbaus ein weiteres kleines Python-Programm – die Serverkomponente. Clientseitig erstellt Sshuttle mit temporären iptables-Regeln dann einen transparenten Proxy, der allen Datenverkehr annimmt, der für das entfernte Netzwerk bestimmt ist. Soweit funktioniert Sshuttle wie ein SSH-Tunnel, allerdings arbeitet Sshuttle mit beliebig vielen TCP-Ports und ist nicht wie gewöhnliches SSH auf einen einzigen Port pro Verbindung beschränkt. Zudem vermeidet das Tool durch eine Reassemblierung der Netzwerkpakete eine ungünstige TCP-über-TCP-Kapselung, welche zu Performanceproblemen führt.

Das klingt nach einem perfekten kleinen Tool für den Aufbau eines VPNs mit erstaunlich primitiven Mitteln. Es gibt aber drei Einschränkungen von Sshuttle gegenüber einer ausgewachsenen VPN-Lösung wie Open VPN:

1. Sshuttle leitet nur TCP-Verbindungen sowie optional auch DNS-Abfragen weiter. UDP und Pings über ICMP funktionieren also über Sshuttle nicht. Diese Protokollarten sind für Webzugriffe oder für den Zugang auf Windows- oder NFS-Freigaben aber auch nicht notwendig.

2. Auch auf dem Client verlangt Sshuttle stets nach root-Rechten beziehungsweise nach dem Aufruf mit einem vorangestellten sudo, da es dort iptables-Regeln ändert. Das funktioniert nur als privilegierter Benutzer mit sudo-Berechtigung.

3. Da Sshuttle auf Standard-Systemkomponenten von Linux aufbaut, funktioniert es nur auf Linux- sowie BSD-Systemen wie Mac-OS. Windows bleibt selbst mit dem

Sichere Verbindungen mit Sshuttle: Vom Client aus öffnet das Python-Programm eine Verbindung per SSH zum Server und baut hier ein VPN zum Netzwerk 192.168.1.0 auf.

neuen WSL (Windows Subsystem for Linux) als Client außen vor, da Sshuttle mit iptables zu tief in die Netzwerkkonfiguration des Systems eingreifen will.

Exkurs: Bei DSL-Anbindungen gibt es keine feste IP-Adresse, da der Provider bei jedem Verbindungsaufbau neue IP-Adressen vergibt. Für diesem Fall kommt ein dynamischer DNS-Dienst wie beispielsweise das kostenlose No-IP (*http://www.noip.com*) zur Hilfe, das einer sich ändernden IP-Adresse nach Rückmeldung durch den Router einen festen Hostnamen im DNS zuteilt. Die meisten DSL-Router unterstützen No-IP und teilen dem Dienst automatisch die neue zugeteilte IP mit.

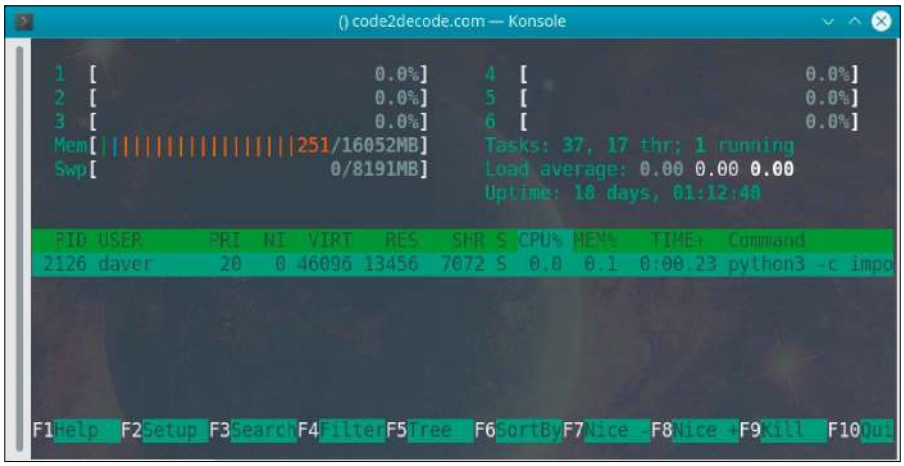
Sobald der SSH-Server im LAN per Portweiterleitung und dynamischen Hostnamen für den Router aus der Ferne aus erreichbar ist, kann Sshuttle starten. Auf dem Linux-Client installiert man das Python-Programm Sshuttle einfach aus den Repositories der Linux-Distribution. In Debian, Ubuntu sowie Varianten, Fedora und Arch Linux ist es in den Standard-Paketquellen vorhanden. In Debian/Ubuntu genügt beispielsweise der Befehl

```
sudo apt-get install sshuttle
```

bereits zur Installation. Wer Open Suse einsetzt, bekommt eine recht frische Version des Programms im Build-Service (*http://software.opensuse.org/download.html?project=security&package=sshuttle*) als inoffizielles Paket.

Sshuttle ist als Kommandozeilenprogramm konzipiert, das ohne vorherige Konfiguration einfach über Aufrufparameter gesteuert wird. Für den Einsatz als VPN erwartet Sshuttle mindestens die Angabe des Zielservers (Hostname oder IP) und eine Netzwerkmaske in CIDR-Notation mit den Adressen des entfernten Netzwerks. Soll das entfernte Netzwerk 192.168.0.1 bis 192.168.0.254 auf dem Client erreichbar sein, so öffnet der Befehl

```
sudo sshuttle -r [User]@[Server]
```



Blick hinter die Kulissen: Auf dem SSH-Server läuft ein Python-Script, das der Sshuttle-Client dort hinterlegt hat. Das Script zerlegt die Netzwerkpakete und nimmt DNS-Anfragen an.

```
192.168.1.0/24
```

diese Verbindung. Möchte man die Rechner im entfernten Netzwerk über ihren dortigen Hostnamen erreichen, so startet

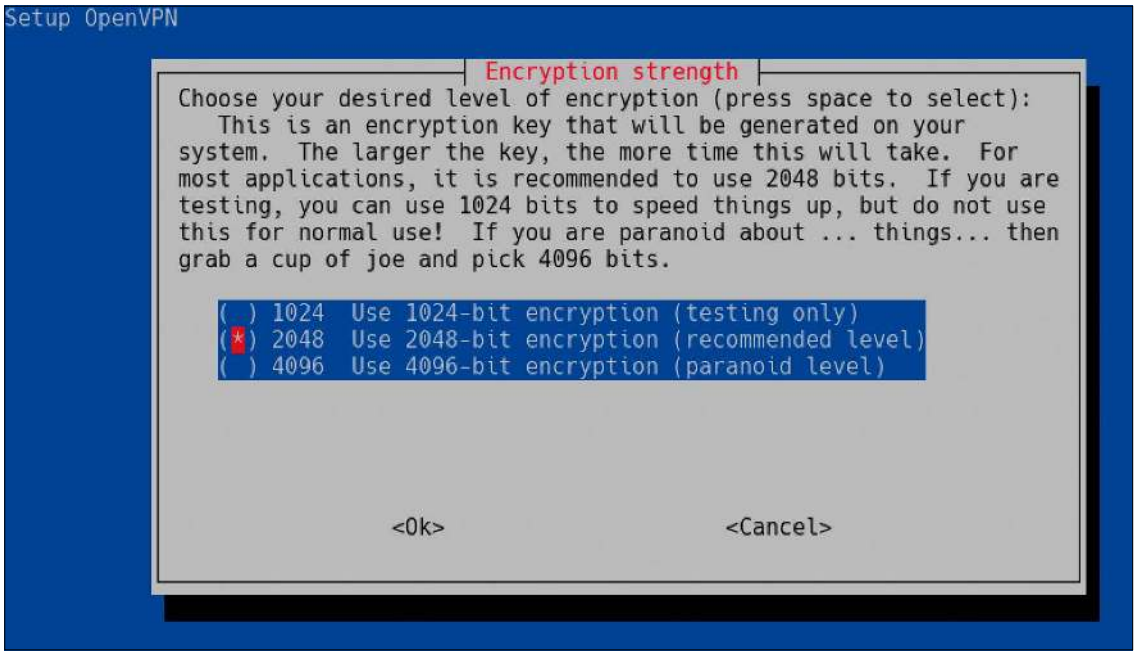
```
sudo sshuttle -r [User]@[Server]
 192.168.1.0/24 -H
```

eine automatische Suche nach den Hostnamen, die Sshuttle dann temporär in die Datei „/etc/hosts“ schreibt. Soll der DNS-Server des entfernten Netzwerks zur Namensauflösung verwendet werden, so erledigt das dieser Befehl:

```
sudo sshuttle -r [User]@[Server]
 192.168.1.0/24 --dns
```

TOR IST KEIN VPN: ANONYMITÄT VS. SICHERHEIT

Das Netzwerk TOR (The Onion Router) hat sich auf Anonymität im Internet spezialisiert und ist mittlerweile auch für seine versteckten Dienste für den Zugang ins Darknet bekannt (und berüchtigt). Um ein VPN handelt es sich jedoch nicht. Denn anders als in einem VPN leistet TOR keine vordefinierte, durchgehend verschlüsselte Verbindung zu einem Host, sondern arbeitet mit einer Proxykette von Zwischenknoten. Den Betreibern der Exit-Nodes innerhalb dieser Knoten wäre es durchaus möglich, unverschlüsselten Traffic, der nicht über HTTPS geht, mitzuschneiden und auszuwerten. Da Behörden ein großes Interesse an der Überwachung des TOR-Netzwerks haben, kann man damit rechnen, dass genau dies auch systematisch passiert. Genauso verhält es sich übrigens bei zahlreichen freien oder günstigen VPN-Diensten – eine Garantie, dass der Betreiber den Traffic nicht doch aufzeichnet, gibt es nicht, zumal sich bei TOR jedermann als Zwischenknoten anmelden kann. Auch bei der Nutzung von TOR oder VPN-Anbietern ist deshalb die Verwendung von HTTPS Pflicht, sobald irgendwo Benutzerdaten eingegeben werden.



VPN-Schlüssel erstellen: Eine Schlüssellänge ab 2048 Bit gilt als sicher. Auf dem Raspberry Pi wird es eine Weile dauern, bis der ARM-Prozessor diesen Schlüssel erzeugt hat.

DNS-Abfragen erfolgen zwar über UDP und nicht per TCP, aber Sshuttle übersetzt das Protokoll für diesen Fall nach TCP.

Pi VPN: Gelungener Einstieg

Um mit Linux als Server und beliebigen Clients ein eigenes VPN aufzubauen, bleibt Open VPN die beste Lösung – wenn es nur nicht so aufwendig (bis obskur) in seiner Konfiguration wäre. Es geht aber inzwischen deutlich einfacher: Pi VPN (*http://www.pivpn.io*) ist ein Bash-Script, das im Terminal alle wesentlichen Konfigurationsschritte in textbasierten Menüs abhakt. Zwar ist das Pi im Namen ein Hinweis auf den Raspberry Pi, da der Platinenrechner oft als kleiner VPN-Server eingesetzt wird, aber Pi VPN arbeitet auch auf beliebiger anderer Hardware und auf vielen Linux-Distributionen. Unterstützt werden nicht nur Raspbian, sondern auch Debian, Ubuntu und alle Abkömmlinge.

Pi VPN ist schon ein paar Jahre verfügbar, von seinen Entwicklern aber erst vor einem Jahr wieder fit für die aktuellen Debian- und Ubuntu-Ausgaben gemacht worden. 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, wobei die MAC-Adresse des VPN-Servers angegeben werden muss (siehe ifconfig und dessen Angabe zur „Hardware Adresse"). 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 interne 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 Port 1194. Wenn der Open-VPN-Server im LAN die IP 192.168.1.77 hat, dann muss der Router Internetanfragen am Port 1194 auf die interne IP-Adresse 192.168.1.77 und den dortigen Port 1194 weiterleiten.

Weil es sich bei Pi VPN um ein Bash-Script handelt, verlangt das Tool keine besondere Installation. Auf dem Server laden Sie das Script in der Kommandozeile mit

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

ins aktuelle Verzeichnis herunter und starten es dort folgendermaßen:

```
bash pivpn
```

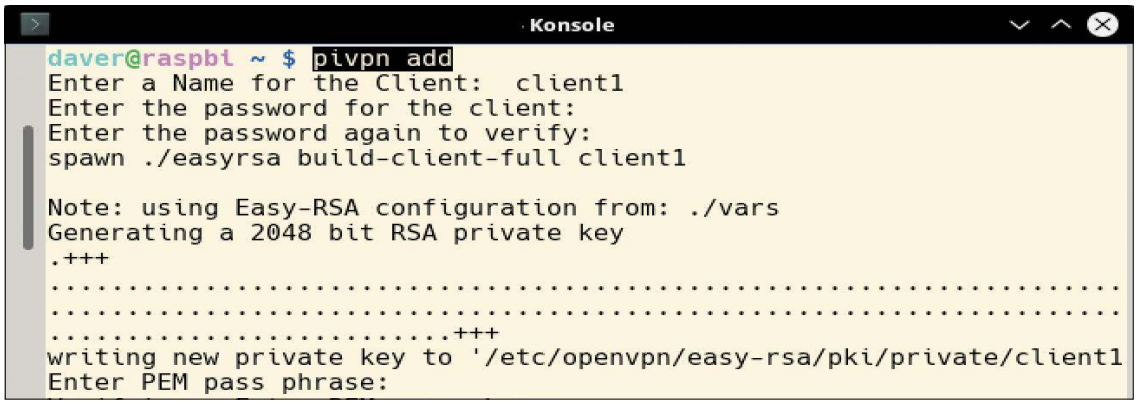
Für einige Aktionen wird das Script nach dem sudo-Passwort fragen und zunächst automatisch per apt-get die noch benötigten Pakete installieren.

Danach beginnt die eigentliche Einrichtung von Open VPN über die englischsprachigen Menüs von Pi VPN: Die Pfeiltasten bewegen den Cursor zwischen den Optionen und mit der Tab-Taste springen Sie zu „OK" beziehungsweise „Cancel".

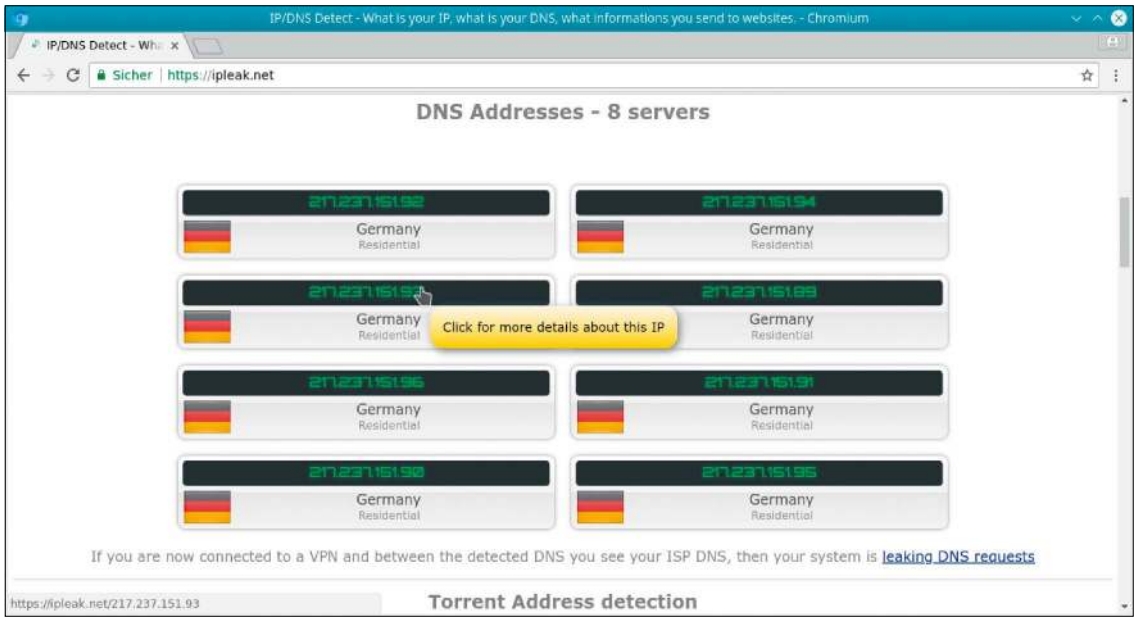
Pi VPN beginnt mit dem Hinweis, dass eine statische IP-Adresse konfiguriert werden sollte. Sofern dieser Schritt schon in den Vorarbeiten auf dem Router erledigt wurde, überspringen Sie diesen Punkt. Der nächste Dialog „Choose a local user that will hold your ovpn configurations" fragt nach einem lokalen 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 passiert ist.

Die anschließende Frage, ob UDP oder TCP als VPN-Protokoll zum Einsatz kommen soll, belassen Sie auf dem Standard 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 einem Raspberry Pi eine Weile dauert. Der Dialog „Public IP or DNS" fragt danach, 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 dem gewählten DNS-Dienst holt. Der nächste Schritt gibt eine Reihe an DNS-



Anbindung der Clients: Pi VPN erzeugt die Clientkonfiguration in wenigen Schritten. Die fertige Datei liegt im Home-Verzeichnis unter „~/ovpns“ und enthält sämtliche Schlüssel.



Diese VPN-Verbindung verrät besuchte Hosts über den DNS-Server: Auf *https://ipleak.net* kann man schnell herausfinden, ob auch die DNS-Abfragen über den VPN-Server gehen.

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.

VPN-Clients: Teilnehmer hinzufügen

Auch für das Erzeugen von VPN-Zertifikaten, mit der sich Clients an Open VPN anmelden, hat Pi VPN ein Hilfs-Script parat. Mit dem Kommando

```
pivpn add
```

erstellen Sie im Handumdrehen die Client-Konfigurationsdateien. Dieses Script fragt nur nach dem gewünschten Clientnamen und einem Passwort, anschließend liegt die fertige Konfigurationsdatei mit dem Namen „[Client].ovpn“ im Ordner „~/ovpns“. Auf den Clients benötigen Sie nur diese eine Datei und können 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 dann mittels

```
pivpn revoke
```

einen Client auf Serverseite jederzeit auch wieder entfernen.

DNS Leaks: Spuren trotz VPN

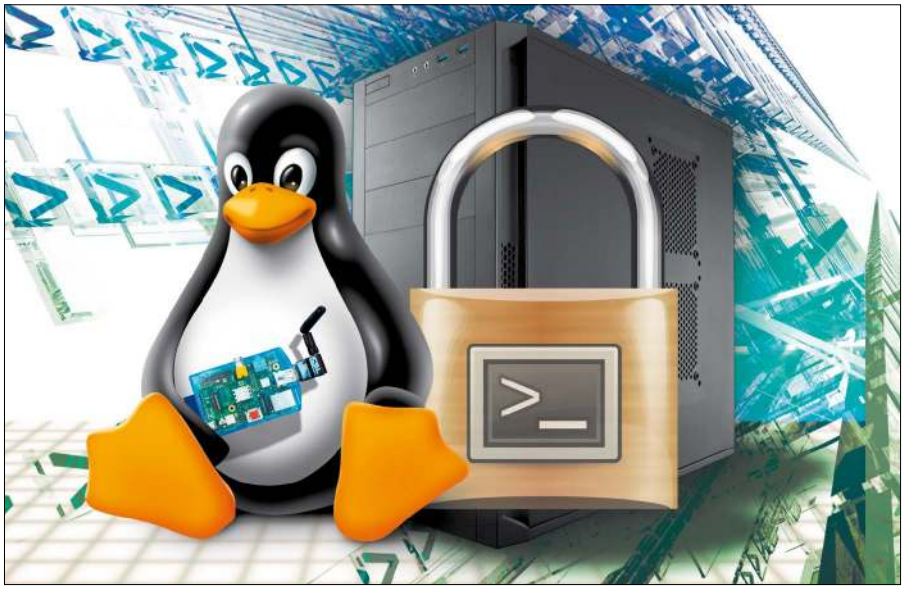
Der gesamte Surftraffic geht nun durch das VPN. Kann der Betreiber des WLANs oder lokalen Netzwerks trotzdem wissen, welche Seiten und Hosts ich besuche? Das geht tatsächlich noch, denn wenn die DNS-Abfrage an den lokalen DNS-Server des Netzwerks geht, weiß der natürlich Bescheid, welche Adressen abgerufen wurden. Das Phänomen nennt sich „DNS Leakage“ und lässt sich leicht nachvollziehen: Die Webseite *https://ipleak.net* zeigt, welche Informationen der Browser von sich und seiner Verbindung ins Internet preisgibt. Hier finden sich selbstverständlich bei einem VPN als Proxy ins Web die öffentlichen IP-Adressen des VPN-Servers (IPv4 und IPv6). Soweit wie gewünscht.

Aber es gibt bei nicht ganz vollständiger Konfiguration der VPN-Clients auch Unerwünschtes: Im unteren Abschnitt sind die verwendeten DNS-Adressen aufgelistet, die der Client zur Abfrage nutzt. Sollten sich hier die lokalen DNS-Serveradressen finden und nicht jene des VPN-Servers, so bedeutet dies, dass DNS-Abfragen nicht durch das VPN gehen. Abhilfe schafft bei Sshuttle die zusätzliche Option „--dns“. Falls Pi VPN oder ein manuell konfiguriertes Open VPN zum Einsatz kommt, dann verlangen Linux-Clients noch die manuelle Umstellung des DNS-Servers im Network-Manager. Alternativ zu einem DNS des VPN-Gateways bieten sich die öffentlichen DNS-Dienste 1.1.1.1 (2606:4700:4700::1111 für IPv6) von Cloudflare oder 8.8.8.8 (2001:4860:4860::8888 für Ipv6) von Google an. ■

Server, aber sicher!

Anschließen. Linux auf SD-Karte. Loslegen? Leider ist es bei Servern aller Art nicht ganz so einfach, das System sicher zu betreiben. Selbst wenn es sich nur um einen Raspberry Pi handelt, gehören zum sicheren Betrieb ein paar zusätzliche Handgriffe.

VON DAVID WOLSKI

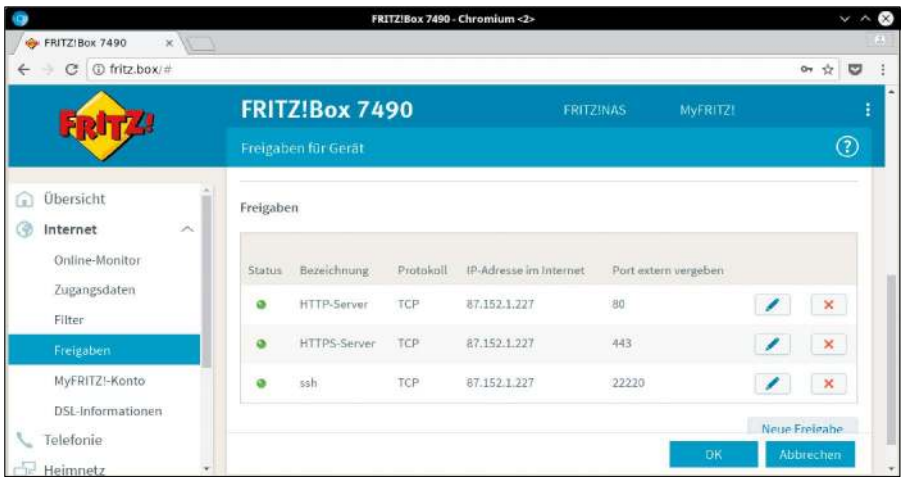


Erschwingliche Ein-Platinen-Computer wie der Raspberry Pi haben den Aufwand erheblich gesenkt, von zu Hause aus einen kleinen Linux-Server zu betreiben. Die niedrigen Einstiegshürden bedeuten aber nicht, dass es damit auch einfacher wird, einen Linux-Server auch wirklich ausreichend sicher zu betreiben. Klar, ein aktuelles Linux-System bringt die besten Voraussetzungen für eine sichere Konfiguration mit. Aber ganz automatisch geht es eben dann doch nicht. Bei jedem Server, der von außen – über das Internet – erreichbar ist, sind einige Sicherheitsvorkehrungen Pflicht, die das System möglichst sicher halten und einen Einbruch unwahrscheinlich machen. Das betrifft auch heimische Miniserver, die nur an einer DSL-Leitung hängen und lediglich über eine dynamische Hostadresse erreichbar sind. Auch dort werden ungebetene Besucher anklopfen und Einlass begehren. Dahinter stecken selten gezielte Angriffe, sondern automatisierte Scans, die nach dem Zufallsprinzip einen Adressbereich abklappern, um nach häufigen Sicherheitslücken und Einfallstoren zu suchen.

Zu einfach sollte man es diesen Wegelagerern nicht machen, denn diese sind inzwischen gut vernetzt: Die Suchmaschine Shodan (*https://www.shodan.io*) beispielsweise sucht mit Crawlern aktiv nach Routern, allen Sorten von Internet-of-Things-Geräten und von außen erreichbaren Raspberry-Pi-Platinen. Das Python-Script „Autosploit“ (*https://git.io/vpZwf*) kombiniert die Suchergebnisse von Shodan mit dem Metasploit-Framework und macht es so auch wenig versierten Hackern einfach, Exploit-Scripts gegen Hunderte von Adressen anzuwenden. Wer seinen Linux-Server korrekt konfiguriert und mit Updates versorgt, hat allerdings wenig zu befürchten.

Router: Nur benötigte Ports öffnen

Wer heimische Datenserver nur im lokalen Netz betreibt, bietet keine Angriffsfläche via Internet. Sicherheitskritisch sind hingegen Linux-Server oder Platinenrechner, die zu Hause stehen und per Router ins Internet gehen. Deshalb kommt auch erst einmal die richtige Routerkonfiguration an die Reihe. Der Router ist es nämlich, der per Portweiterleitung den Zugang von außen auf einen Dienst im lokalen Netzwerk öffnet. Der Router dient zugleich als Firewall, die nur den Netzwerkverkehr auf die er-



Portfreigabe einer AVM Fritzbox: Voraussetzung für weitergeleitete Ports ist eine feste IP-Adresse. Diese vergibt die Fritzbox unter „Heimnetz → Netzwerk“ an die Geräte im LAN.

laubten Ports durchlassen soll. Einige Router bieten in ihrer Konfiguration die Möglichkeit, einen „Exposed Host" beziehungsweise eine DMZ (Demilitarisierte Zone) einzurichten, um alle Anfragen ungefiltert an die angegebene Serveradresse im lokalen Netzwerk weiterzuleiten.

Diese Lösung scheint bequem, da man sich dann über die einzelnen Ports angebotener Dienste keine Gedanken machen muss. Sie kommt aber keinesfalls in Betracht: Der Server wäre damit völlig exponiert – ein unnötiges Risiko. Deshalb leitet man via Router besser ganz gezielt jene Ports an den Server im heimischen Netzwerk weiter, die dieser auch wirklich bedienen soll: Für den Wartungszugang per SSH brauchen Sie nur eine Weiterleitung von Port 22, HTTP verlangt Port 80 und HTTPS Port 443. Die Konfiguration einer Firewall mit iptables oder einem Hilfsprogramm wie ufw auf dem Linux-System kann dann entfallen.

Benutzer: Arbeiten ohne root-Konto

Server werden üblicherweise über SSH gepflegt, eine grafische Oberfläche auf Servern ist eher die Ausnahme. Bei SSH kommt es darauf an, dass alle Benutzeraccounts sichere, also komplexe Passwörter haben. Zudem sollten Standardaccounts wie „root" oder „pi" über SSH nicht direkt zugänglich sein, damit der Kontoname nicht einfach erraten werden kann.

1. In Ubuntu, Open Suse und neueren Ausgaben von Raspbian ist die Anmeldung als root sowieso nicht nötig, in Ubuntu und Co. ist die Anmeldung als root sogar deaktiviert. Alle administrativen Tätigkeiten werden per sudo erledigt. Diese Praxis empfiehlt sich auch für alle anderen Linux-Distributionen. Die Konfiguration von sudo liegt in der Datei „/etc/sudoers" vor, wobei eine manuelle Anpassung dieser Datei mit dem Editorbefehl visudo erfolgen sollte, da dieser die korrekte Syntax beim Speichern überprüft. Über den root-Account ruft man den Editor zur ersten Konfiguration mit dem Kommando

```
su -c "visudo"
```

auf. Die Definition von Benutzerprivilegien erfolgt ganz am Ende der Datei nach dem folgenden Schema

```
[benutzer] ALL=(ALL:ALL)
```

wobei der Platzhalter „[benutzer]" für den tatsächlichen Kontonamen steht. In Ubuntu/Debian/Raspbian ist in der Datei schon die Gruppe „sudo" eingetragen und es genügt, weitere Benutzer einfach mittels des Befehls

```
usermod -a -G sudo [Benutzername]
```

in diese Gruppe aufzunehmen, um sie damit für den Einsatz von sudo freizuschalten.

2. Der Systembenutzer „root" sollte sich über SSH gar nicht mehr anmelden dürfen. Damit man sich nicht selbst aussperrt, ist es wichtig, sich wirklich erst davon zu überzeugen, dass sudo mit eigenen Passwort funktioniert. Besteht darüber kein Zweifel, können Sie die Konfiguration des SSH-Dienstes in der Datei „/etc/ssh/sshd_config" anpassen und mit der Zeile.

```
PermitRootL ogin no
```

die SSH-Anmeldung für root verbieten. Die Änderung ist nach einem Neustart des SSH-Dienstes aktiv, was beispielsweise in Debian der Befehl

```
sudo service ssh restart
```

erledigt.

Gruppe statt Benutzer: In Debian und Ubuntu ist die Gruppe „sudo" vordefiniert. In diese müssen weitere Benutzer, denen Sie sudo erlauben wollen, nur noch aufgenommen werden.

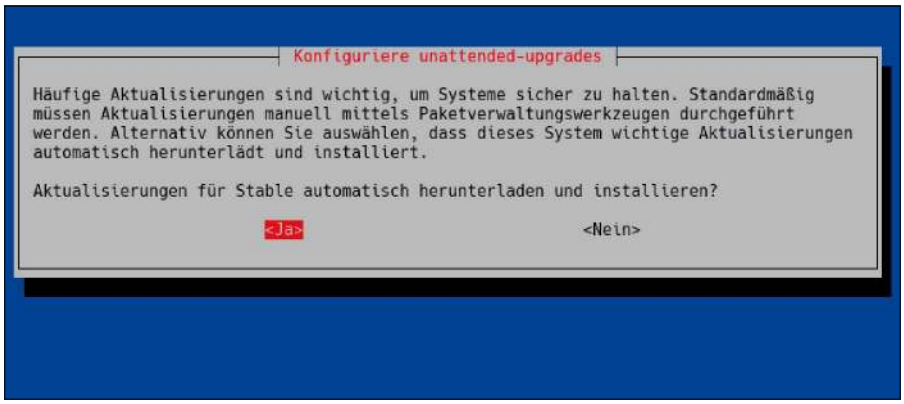
Türsteher: Der SSH Guard

Automatisierte Angriffe per Wörterbuchattacken auf den SSH-Port des Servers pral-

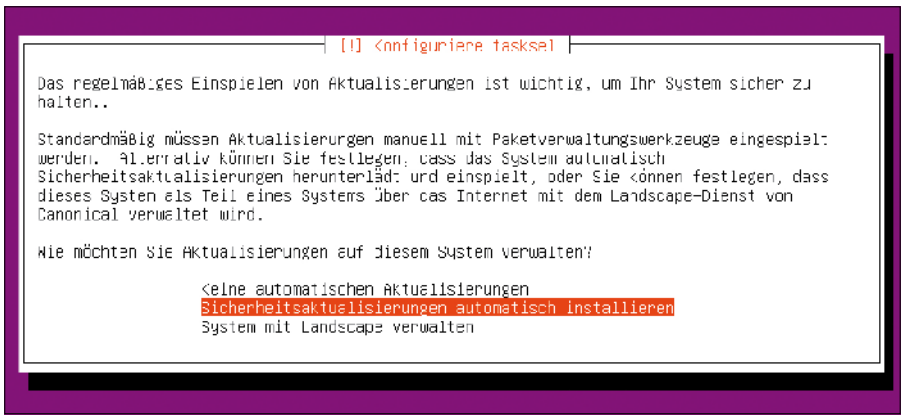
FIRMWARE: AUCH ROUTER BRAUCHEN UPDATES

Vorsicht vor Sicherheitslücken in alten Routern: Viele alte Modelle, hier der ehemals sehr verbreitete Cisco Linksys WRT-54GL, weisen Sicherheitslücken im UPnP-Protokoll auf.

Ein oft unterschätztes Risiko sind die Router selbst, die zur Anbindung des heimischen Servers ans Internet dienen und damit den eingehenden Datenverkehr regeln und per NAT (Network Address Translation) an die Teilnehmer im lokalen Netzwerk vermitteln. Nicht selten schlummern in der Firmware älterer Router Sicherheitslücken, die Einbrüche von außen, von der Internetverbindung aus ermöglichen. Eine gravierende Lücke betrifft aktiviertes UPnP (Universal Plug and Play), mit dem der Router Geräten und Programmen im LAN erlaubt, Ports nach außen automatisch zu öffnen. Diese Lücken wurden 2013 bekannt, aus Sicherheitsgründen von den Entdeckern aber damals nicht veröffentlicht, da Millionen von Routern verwundbar waren, etwa der damals immens populäre Cisco Linksys WRT54GL. Inzwischen hat sich der Schleier der Geheimhaltung gelüftet und die Studie von 2013 ist unter *http://defensecode.com/whitepapers/From_Zero_To_ZeroDay_Network_Devices_Exploitation.txt* veröffentlicht. Alte Router, für die es seit Jahren kein Firmwareupdate mehr gab, sind schlimmstenfalls genau für die UPnP-Lücke anfällig und sollten ausgemustert werden.



Unbeaufsichtigt immer auf dem neuesten Stand: Debian- und Ubuntu-Systeme liefern für regelmäßige Sicherheitsupdates per Cronjob ein unkompliziertes Konfigurations-Script mit.



Ubuntu-Server nach der Installation: Das System bietet die Einrichtung automatischer Updates selbst an.

len nach diesen ersten Maßnahmen schon zuverlässig ab. Bei mehreren Hundert gescheiterten Verbindungsversuchen täglich wird das Access-Logfile aber unübersichtlich. Dagegen ist ein Kraut gewachsen: SSH Guard ist ein Wächterdienst, der wiederholt gescheiterte Anmeldeversuche anhand deren ausgehender IP-Adresse abblockt und dabei auch IPv6 unterstützt. In Ubuntu, Debian und Raspbian ist der Dienst mit

```
sudo apt-get install sshguard
```

eingerichtet und sofort aktiv.

Ohne Aufsicht: Automatische Systemupdates

Linux-Distributionen machen dank ihres Paketmanagers die Aufgabe einfach, das System auf dem neuesten Stand und damit sicher zu halten. Auf Servern mit Ubuntu, Debian und Raspbian bietet es sich an, Sicherheitsupdates automatisch zu installieren. Die Serverausgabe Ubuntus bietet nach der Installation diese Option sogar explizit an.

Vorbereitete Scripts für unbeaufsichtigte Updates in Debian, Raspbian und Ubuntu installiert dieser Befehl:

```
sudo apt-get install unattended-
  upgrades
```

Danach verlangt das System nur noch kleinere Anpassungen. Ein Paketkonfigurations-Script startet dieses Kommando:

```
sudo dpkg-reconfigure
  --priority=low unattended-
  upgrades
```

Es zeigt eine Rückfrage nach dem automatischen Herunterladen und Installieren an, die man mit „Ja“ beantwortet. Die benötigten Einträge für einen täglichen Cronjob, der um 6:25 Uhr ausgeführt wird, erstellt das Konfigurationsscript nun selbständig. Der Befehl

```
sudo unattended-upgrades --dry-run
  -d
```

kann die automatische Updatefunktion testen, ohne dabei tatsächlich zu installieren. Die Logdatei „/var/log/unattended-upgrades/unattended-upgrades.log“ protokolliert die Updates. Eine komplette Distributionsaktualisierung, die auch geänderte Abhängigkeiten unter Paketen beachtet, muss hin und wieder manuell mit

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

aufgerufen werden.

Auch andere Linux-Distributionen kennen solche automatischen Updates. In Open Suse kümmert sich das Paket „yast2-online-update-configuration“ darum, das nach der Installation in Yast auf seine Konfiguration wartet. Cent-OS stellt mit „yum-cron“ einen Automatismus bereit, der mit

```
sudo systemctl enable yum-cron.
  service
```

in Gang gesetzt wird.

Zugangsdaten: Nur verschlüsselt anmelden

Es ist inzwischen zum großen Tabu geworden, im Internet mit unverschlüsselten Log-in-Daten zu arbeiten. Unverschlüsselte Protokolle wie FTP zur Datenübertragung oder HTTP zur Anmeldung auf Webseiten sind ein hohes Risiko.

Wer vom heimischen Server aus Webdienste anbietet, die ein Log-in erfordern, muss unbedingt auf die Verschlüsselung per HTTPS achten. Dazu benötigt der Webserver ein SSL-Zertifikat, das in die Webserver-Konfiguration eingebunden wird. Für den Eigenbedarf reicht ein selbst signiertes Zertifikat aus, das man sich selbst ausstellen kann. Bei dynamischen Domainnamen für den Router gibt es sowieso keine zuverlässige Alternative, da man dafür nicht einfach SSL-Zertifikate bekommt. Auf einem Ubuntu/Debian/Raspbian statten folgende Schritte einen Apache-2-Webserver mit einem selbst signierten Zertifikat und mit HTTPS aus:

1. Das selbst signierte Zertifikat und dessen Dateien erstellt dieser Befehl:

```
sudo openssl req -x509 -nodes -days
  720 -newkey rsa:2048 -keyout /etc/
  ssl/certs/apache.key -out /etc/
  ssl/certs/apache.crt
```

Das dabei angezeigte Frageformular können Sie mit beliebigen Angaben ausfüllen.

2. Der Webserver Apache liefert schon eine Standardkonfiguration für SSL mit, die in der Datei „/etc/apache2/sites-available/default-ssl“ vorliegt. Mit einem beliebigen Texteditor wie Nano tauschen Sie die Zeile

```
SSLCertificateFile  /etc/ssl/
  certs/ssl-cert-snakeoil.pem
```

gegen

```
SSLCertificateFile  /etc/ssl/
  certs/apache.key
```

aus sowie darunter die Zeile

```
SSLCertificateKeyFile /etc/ssl/
```

```
private/ssl-cert-snakeoil.key
```

Gegen diesen Eintrag:

```
SSLCertificateFile  /etc/ssl/
 certs/apache.key
```

3. Die gerade bearbeitete und gespeicherte Datei „default-ssl“ repräsentiert in Apache eine neue „Site“, die dann folgendes Kommando aktiviert:

```
sudo a2ensite default-ssl
```

4. Bevor Apache einen Port für HTTPS öffnen kann, müssen Sie noch das SSL-Modul von Apache mit dem Kommando

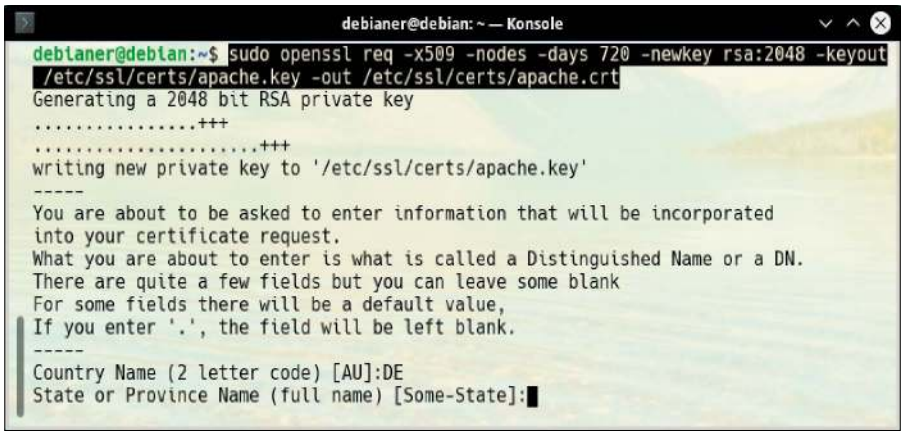
```
sudo a2enmod ssl
```

einschalten und anschließend den Webserver selbst mit

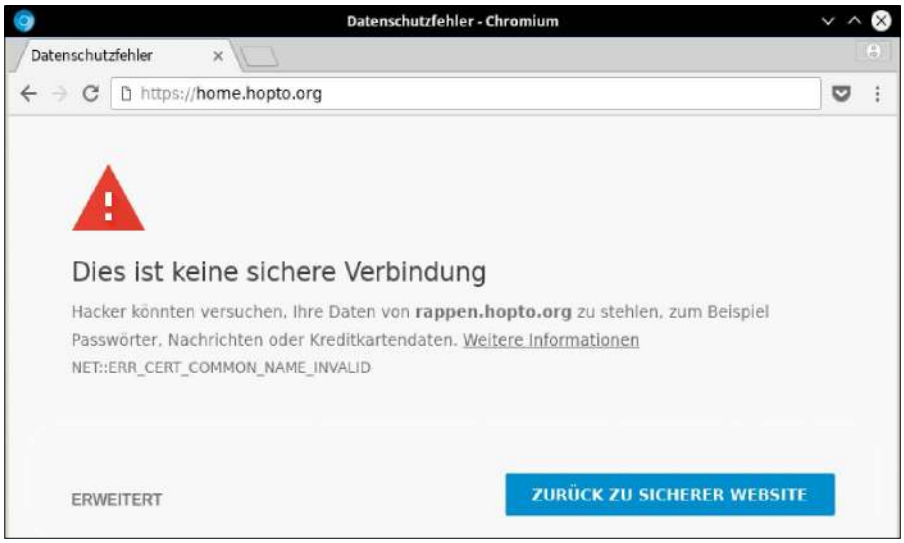
```
sudo service apache2 force-reload
```

neu starten. Falls ein Konfigurationsfehler auftritt, wird sich Apache jetzt mit einer Meldung beschweren. Die Warnung „Could not reliably determine the server's fully qualified domain name“ kann man indes ignorieren.

5. Bei einem ersten Aufruf des Webservers mit einem Browser über „https://[Server-Adresse]“ zeigt der Browser einen Warnhinweis über ein ungültiges Zertifikat an. Denn das eigene Zertifikat ist nicht durch eine zentrale Zertifizierungsstelle (CA) signiert und aktuelle Webbrowser stufen die Verbindung zunächst daher als nicht vertrauenswürdig ein. Die Verbindung ist aber trotzdem sicher verschlüsselt. In den üblichen Browsern wie Firefox und Chrome/Chromium müssen Sie nur einmalig eine Ausnahme für das eigene Zertifikat und für den genutzten Domainnamen gestatten. ■



Selbst signieren: Ein selbst ausgestelltes SSL-Zertifikat genügt für sicher verschlüsselte HTTPS-Verbindungen zum eigenen Server. Ein Linux-System liefert dazu alle Tools mit.



Als Ausnahme aufnehmen: Webbrowser weisen deutlich darauf hin, wenn ein Zertifikat keine CA-Signatur hat. Bei selbst signierten Zertifikaten ignorieren Sie diese Warnung.

SERVERADMINISTRATION: PANNEN UND SÜNDEN

Auch wenn es absolute Sicherheit auf Servern mit Internetanbindung nicht gibt, so sollte man es potenziellen Angreifern so schwer wie möglich machen. Die folgenden Konfigurationspannen treten häufiger auf, oft erst nach längerer Laufzeit im Dauerbetrieb.

- **Einfache Passwörter:** Alle Passwörter, nicht nur jene von root, müssen ausreichend komplex sein.
- **Keine Updates:** Auch wenn es selten vorkommt, so hat auch bewährte Open-Source-Software bisweilen Sicherheitslücken. Regelmäßige Updates des Systems sind Pflicht.
- **Unverschlüsselte Protokolle:** Sobald Benutzer-Log-ins übertragen werden, darf dies nur über verschlüsselnde Protokolle wie SSH, HTTPS oder bei Dateiübertragung per SFTP geschehen.
- **Obsolete Linux-Distributionen:** Reguläre Distributionen erreichen schon nach wenigen Monaten das Ende ihres Wartungszyklus. Für Server kommen deshalb nur Distributionen mit Langzeitsupport in Frage.
- **PHP-Software zu alt:** PHP hat sich als schnell zu erlernende Script-Sprache im Web durchgesetzt, aber Sicherheit bekommt von den PHP-Entwicklern, wenn überhaupt, oft nur wenig Aufmerksamkeit. Jedes PHP-Projekt muss akribisch auf dem neusten Stand gehalten werden.
- **Ungepflegte Webserver:** Vergessene Konfigurationsdateien, unsichere Zugriffsrechte auf Verzeichnisse oder fehlende SSL-Zertifikate lassen einen Webserver zu viel ausplaudern.
- **Offenstehende Datenbanken:** Eine Menge PHP-Projekte laufen mit einer Datenbank wie Maria DB oder My SQL im Rücken. Auch die Konten der Datenbank inklusive Datenbank-Rootzugang brauchen ein sicheres Passwort.

DNS und DHCP in Eigenregie

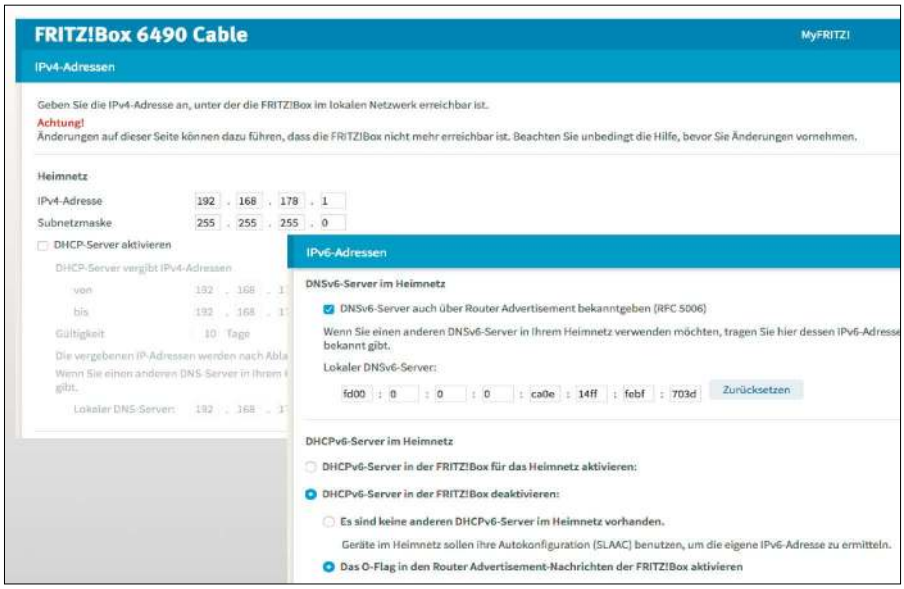
Einschalten. Anmelden. Surfen: Den meisten Anwendern sind die Grundlagen des Heimnetzes viel zu kompliziert. Wer seine eigenen Vorstellungen umsetzen will, muss sich um die Adresszuweisung seiner Rechner kümmern.

VON STEPHAN LAMPRECHT

Damit Rechner in einem Netzwerk kommunizieren können, brauchen sie eine individuelle IP-Adresse. Und damit im Browser aus dem Namen einer Webdomain die IP-Adresse des Zielsystems wird, darum kümmert sich der DNS-Server. Dieses Wissen hat inzwischen fast jeder ambitionierte Internetnutzer. Und im Normalfall genügt das auch. Denn der Router kümmert sich um die Zuweisung der IP-Adressen mittels des „Dynamic Host Configuration Protocol“ (DHCP) und um die Adressauflösung über das „Domain Name System“ (DNS). Wer aber vom Standard abweichen will oder muss, kann auch alles in Eigenregie betreiben.

Motive für die DHCP/DNS-Konfiguration

Mehr Geschwindigkeit bei der Namensauflösung ist bei anspruchsvollen Nutzern die Hauptmotivation, um sich mit einer eigenen Netzwerkkonfiguration zu beschäftigen. Die Komplexität eines selbst verwalteten DHCP erhöht aber auch die Sicherheit gegen Hacker und Cyberkriminelle, die stets von üblichen Standards ausgehen. Durch die nachfolgend vorgestellte dnsmasq-Konfiguration entsteht ein individueller Adressraum, der von den Standards abweicht. Ein weiterer Aspekt ist der erhöhte Datenschutz. Keiner weiß, was der DNS des Providers mit den Webabfragen macht und in welchem Umfang er diese speichert. Alternative DNS-Server wie etwa des zensurfreien Chaos Computer Clubs sind in diesem Punkt unverdächtig. Aber Achtung: Unerfahrene Nutzer gehen das Risiko ein, dass sie bei einer falschen Konfiguration ihren Router nicht mehr erreichen und schlimmstenfalls alle Systeme inklusive Router zurücksetzen müssen.



Abschlussarbeiten: Im Router muss der DHCP-Server deaktiviert werden. Wenn sich der Router weiter um die Vergabe von IPv6-Präfixen kümmern soll, dann hilft das Setzen von „O-Flag“.

Den eigenen Server aufsetzen

Wer kein Firmennetzwerk mit hundert Arbeitsplätzen zu versorgen hat, kann zu dnsmasq greifen. Dabei handelt es sich um einen schlanken DNS- und DHCP-Server, der für ein Heimnetz auf alle Fälle ausreicht. Installieren Sie zunächst das Tool dnsmasq auf dem Rechner, den Sie als DHCP- beziehungsweise DNS-Server nutzen wollen:

```
sudo apt install dnsmasq
```

Weitere Voraussetzungen sind nicht erforderlich. Sie können dann gleich an die Konfiguration gehen.

Wir gehen hier davon aus, dass Sie einen Raspberry Pi mit Raspbian verwenden. Leider gab es zwischen den verschiedenen Raspbian-Versionen eine Änderung des Namensschemas für die Schnittstellen. Damit Sie unser Beispiel nachvollziehen können, editieren Sie mit

```
sudo nano /boot/cmdline.txt
```

die Bootdatei des Rechners. Fügen Sie am Ende folgende Zeile mit einem vorangestellten Leerzeichen ein: „net.ifnames=0“. Nach dem Speichern und einem Neustart verwenden Sie das gleiche Schema wie in diesem Artikel.

Die eigentliche Installation eines abweichenden DNS-Servers ist nicht sonderlich schwierig, hängt aber vom verwendeten System ab. Um die Namen von Systemen

aufzulösen, schlägt dnsmasq an zwei Stellen nach. Lokale Systeme liegen in der Datei „etc/hosts/“. Systeme, die dort nicht gefunden werden, werden dann an die DNS-Server weitergereicht, die in der eigenen Konfiguration oder der Datei „/etc/resolv.conf“ genannt werden.

Distributionen, die für die Verwaltung der Netzwerkeinstellungen den grafischen Netzwerkmanager einsetzne, überschreiben allerdings die „/etc/resolv.conf“ dynamisch. Um im Zweifelsfall immer wieder auf den Standard zurückgreifen zu können, sichern Sie am besten zunächst die ursprüngliche Datei von dnsmasq. Nachdem Anlegen einer Sicherheitskopie laden Sie sich dann die Konfiguration in einen Editor:

```
sudo mv /etc/dnsmasq.conf /etc/
  dnsmasq.conf_alt
sudo nano /etc/dnsmasq.conf
```

In dieser Konfigurationsdatei müssen Sie jetzt wenigstens vier Aspekte regeln:

1. Sie legen fest, welche Schnittstellen berücksichtigt werden sollen.

2. Sie definieren den Adressbereich, der den Clients via DHCP zur Verfügung gestellt werden soll.

3. Sie legen das Gateway fest. Das ist der Rechner, der die Verbindung mit dem Internet herstellt – in der Regel der Router, in unserem Fall eine Fritzbox. Dazu definieren Sie eine feste IP-Adresse für den Router, die Sie dann auch im Router eintragen.

4. Schließlich definieren Sie den gewünschten externen DNS-Server.

Den DHCP-Server definieren

Dnsmasq bietet sehr viele Optionen, die den Rahmen des Artikels sprengen würden. Wir verwenden hier eine minimale, aber arbeitsfähige Konfiguration. Definieren Sie in der Datei „/etc/dnsmasq.conf“ zunächst die Schnittstellen:

```
interface=wlan0
interface=eth0
```

Um DHCP zu aktivieren, genügt es, den Adressbereich einzufügen, der an die Clients verteilt werden soll:

```
dhcp-range=192.168.178.100,192.16
  8.178.150,24h
```

Der letzte Wert „24h“ definiert, wie lange die Adressen gültig bleiben, bevor wieder neu verteilt wird. Jetzt können Sie noch wichtigen Datei- oder Druckerservern feste IP-Adressen zuweisen:

```
dhcp-host=00:07:95:26:2B:C9,death
  star,192.168.178.120,infinite
```

Die Steuerung des dnsmasq-Servers obliegt einfachen Textdateien. Durch das Setzen eines eigenen Pfads lassen sich auch schnell eigene Konfigurationsdateien einsetzen.

Wenn der grafische Netzwerkmanager zum Einsatz kommt, sind Optionen in der Datei „Resolv.conf“ wirkungslos. Externe DNS-Server müssen Sie dann im grafischen Manager eintragen.

Hier erhält der Rechner mit der eingetragenen MAC-Adresse („00:07:95…“), stets den Namen „deathstar“ und die dahinter notierte IP-Adresse. Mit der Option „infinite“ wird ausgeschlossen, dass diese sich im Laufe des Betriebs ändert.

Die DNS-Funktionalität bearbeiten

Damit die Fritzbox nach wie vor mit ihrem Namen erreicht werden kann (also die Eingabe von „fritz.box“ im Browser nicht dazu führt, dass diese an den externen DNS geht), tragen Sie in die Datei die folgenden Zeilen ein:

```
local=/local/
local=/fritz.box/
domain=fritz.box
```

Die gewünschten externen DNS-Server tragen Sie mit der Kennziffer „6“ ein: „dhcp-option=6, X.X.X.X, Y.Y.Y.Y“, also etwa konkret „dhcp-option=6,1.1.1.1,1.0.0.1“ wenn Sie die neuen Server von Cloudflare verwenden wollen.

Bleibt jetzt noch, das Standardgateway zu definieren (Router). Kennziffer „3“ ist für das Gateway reserviert. Der Eintrag, den Sie auf Ihre gewünschte IP-Adresse ändern müssen, sieht dann so aus:

```
dhcp-option=3,192.168.178.1
```

Damit haben Sie alle grundlegenden Einstellungen abgeschlossen. Nach

```
sudo service dnsmasq status
```

sollte das System zurückmelden, dass der Service läuft.

Optionen am Router bearbeiten

Zwei DNS/DHCP-Server im gleichen Netzwerk sind fehlerhaft. Daher müssen Sie DNS und DHCP im Router ausschalten. Bei der Fritzbox finden Sie die Einstellungen unter „Heimnetz → „Netzwerkeinstellungen“ und dort unter „IPv4-Adressen“ und „IPv6-Adressen“. Deaktivieren Sie die Option „DHCP-Server aktivieren“. Da anzunehmen ist, dass Sie vom Provider ein IPv6-Präfix zugewiesen bekommen, ist es ratsam, die IPv6-Adressen weiterhin vom Router zu beziehen. Dazu wählen Sie in den Optionen für IPv6 der Fritzbox das sogenannte „O-Flag“. Es sorgt dafür, dass die IPv6-Adressen vom Router kommen, alle anderen Optionen wie etwa der DNS-Server jedoch vom neu eingerichteten Server.

Der Router soll das Gateway ins Internet bleiben. Deswegen weisen Sie ihm abschließend die statische IP-Adresse zu, die Sie in der Konfiguration des DNS definiert haben. Nach dem Speichern in der Fritzbox starten Sie alle Systeme im Heimnetz neu und führen Tests durch, ob alle Rechner erreichbar sind. Das Vorgehen funktioniert auch an einem Anschluss über Kabel, wenn das Dual-Stack-Lite-Verfahren angewendet wird, was üblicherweise der Fall ist. ■

Mehr Sicherheit für Windows

Über eine Linux-Live-DVD prüfen Sie, ob sich Schadsoftware auf Ihrem Windows-PC befindet. Außerdem lassen sich wichtige Dateien sichern oder gelöschte Daten wiederherstellen.

Analyse mit Zweitsystem: Linux-Livesysteme mit Virenscanner helfen Windows-Nutzern bei der Suche nach Schadsoftware und bei der Datenrettung.

VON THORSTEN EGGELING

Bevor Sie ein von Schadsoftware befallenes Windows neu installieren, holen Sie eine zweite Meinung ein. Der installierte Virenscanner arbeitet nicht immer zuverlässig und es gibt auch noch andere Ursachen für Windows-Probleme als Viren und Trojaner. Ein Linux-Livesystem kann Ihnen bei der Analyse helfen und bei Bedarf auch zur Rettung oder Wiederherstellung von Dateien dienen.

Diverse Livesysteme für Windows-Reparaturen

Während Windows läuft, sind zahlreiche Dateien vom System gesperrt oder es fehlen die Zugriffsrechte. Schadsoftware kann sich außerdem so verstecken, dass Sie weder die zugehörigen Dateien noch alle laufenden Prozesse sehen. Ein unabhängiges Livesystem, das Sie von einer DVD oder einem USB-Stick starten, ist vor Schadsoftware geschützt und ermöglicht den uneingeschränkten Zugriff auf alle Dateien.

Die PC-WELT-Rettungs-DVD (*www.pcwelt.de/E08L0v*) enthält die Virenscanner von Avira, Eset NOD32 und Sophos. Auch bieten fast alle Hersteller von Antivirensoftware kostenlose Rettungssysteme zum Download an (siehe Kasten). Teilweise gibt es im Downloadbereich ein Tool oder eine spezielle Version für den USB-Stick. Wenn nicht, verwenden Sie unter Windows ein Tool wie Rufus (*https://rufus.akeo.ie*) oder unter Linux das in der Regel vorinstallierte dd (siehe *www.pcwelt.de/2089747*).

Nicht alle Systeme booten auf neueren PCs im Uefi-Modus. In diesem Fall müssen Sie im Bios/Firmware-Setup CSM aktivieren (Compatibility Support Module) und außerdem Secure Boot abschalten. Informationen dazu finden Sie unter *www.pcwelt.de/2077272*. Die größeren Livesysteme zeigen einen Linux-Desktop, etwa den von Ubuntu, und bieten auch einen Webbrowser, Dateimanager, Terminalfenster und weitere Tools. In den kleineren Systemen lässt sich nur der Virenscanner starten. Die Virenscanner müssen im Livesystem zuerst mit Updates versorgt werden, damit er auch die jüngste Schadsoftware erkennt. Dafür ist eine Internetverbindung nötig, die Sie über ein Ethernet-Kabel oder WLAN herstellen. Einige der Livesysteme basieren auf älteren Linux-Versionen, unter dem der WLAN-Adapter oft nicht erkannt wird. Bei den Minimalsystemen fehlt die WLAN-Unterstützung meist. In diesem Fall führen Sie das Update per Kabel durch.

Beim Sophos-Livesystem gibt es eine Besonderheit: Sie müssen die ISO-Datei mithilfe des Programms „sbavc.exe“ unter einem Windows erstellen, das garantiert frei von Schadsoftware ist. Linux und die aktu-

ellen Virensignaturen werden dabei frisch heruntergeladen.

Viren mit der PC-WELT-Rettungs-DVD suchen

Die PC-WELT-Rettungs-DVD ist mit vier Virenscannern ausgestattet, zwischen denen Sie nach einem Klick auf die Schaltfläche „Rettungswerkzeuge“ wählen können. Bevor Sie einen weiteren Virenscanner verwenden, starten Sie jeweils das System neu, damit mehr freier Hauptspeicher verfügbar ist. Gleich welche Antivirensoftware Sie nutzen – beim ersten Start erscheint das Fenster „Laufwerke einbinden“. Wählen Sie die Option „Alle NTFS- und FAT-Laufwerke automatisch nur lesbar einbinden“ und klicken Sie auf „Weiter“.

Bei Avira, Clamav und Sophos werden Sie aufgefordert, aktuelle Virensignaturen herunterzuladen. Bestätigen Sie mit „OK“. Danach sehen Sie eine einfache Oberfläche, über die Sie per Klick auf „Durchsuchen starten“ den Virenscan durchführen. Eset Nod32 Antivirus aktualisiert sich beim Start automatisch und bringt seine eigene Oberfläche mit.

Maßnahmen bei Virenalarm: Sollte ein Virenscanner fündig werden, informieren Sie sich zuerst im Internet über die Eigenheiten der Schadsoftware. Im Rettungssystem verwenden Sie dafür den Browser Firefox. Laden Sie die betroffene Datei für weitere Untersuchungen bei *https://virustotal.com* hoch. Wenn nur wenige Virenscanner eine Schadsoftware melden, handelt es sich wahrscheinlich um einen Fehlalarm.

In einigen Fällen kann es sinnvoll sein, die betroffene Partition mit Schreibzugriff einzubinden (siehe nächster Punkt) und dem Virenscanner die Bereinigung zu überlassen. Die Optionen dafür setzen Sie auf der Registerkarte „Expertenmodus“.

Avira im PC-WELT-Rettungssystem: Der Virenscanner ist mit einer einfachen Oberfläche ausgestattet, über die Sie die gewünschten Optionen einstellen.

Daten retten oder wiederherstellen

Um auf eine Windows-Partition oder eine externe Festplatte zuzugreifen, klicken Sie in der Symbolleiste auf das dritte Icon „Festplatten einbinden“. Sie sehen im Fenster „Laufwerke“ die gefundenen Festplatten und darunter Schaltflächen zum Einbinden, die jeweils für eine Partition stehen. Setzen Sie ein Häkchen vor „schreibbar?“, wenn Sie Dateien auf der Partition nicht nur kopieren, sondern ändern möchten.

Die Partitionen werden in das Dateisystem unterhalb von „/media/disk“ jeweils in eigene Ordner eingehängt („sda2“, „sdc1“). Der Dateimanager öffnet sich automatisch und Sie können auf den Inhalt zugreifen. Kopieren funktioniert im Linux-Dateimanager mit der Tastenkombination Strg-C. Wechseln Sie dann in das Zielverzeichnis und starten Sie den Kopiervorgang mit Strg-V.

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

Wurde versehentlich eine ganze Partition gelöscht, gehen Sie auf „Rettungswerkzeuge → Partition retten“. Gehen Sie auf „No Log“ und drücken Sie die Eingabetaste. Wählen Sie die Festplatte, auf der das vermisste Laufwerk sich befand, und dann „Proceed“. Danach bestimmen Sie den Typ der verlorenen Partitionen. Da Testdisk den Typ selbst ermittelt, können Sie die Vorgabe in den meisten Fällen übernehmen. Dann wählen Sie „Analyse“, „Quick Search“ und „Continue“. Mit „p“ lassen Sie sich die enthaltenen Dateien anzeigen, mit „q“ geht es wieder zurück. Drücken Sie die Taste „Cursor rechts“, um die Partition zur Wiederherstellung auszuwählen, und dann die Eingabetaste.

Abschließend legen Sie die Partitionstabelle über „Write“ neu an. ■

LIVESYSTEME MIT VIRENSCANNER

Hersteller	Beschreibung	Basiert auf	Letztes Update	Größe	Sprache	Internet
AVG	Minimalsystem, nur Virenscanner	Linux 4.3	2016	174 MB	Englisch	*www.pcwelt.de/712888*
Avira	Ubuntu-Desktop, keine Laufwerksauswahl	Ubuntu 12.04	2016	687 MB	Deutsch	*www.pcwelt.de/304999*
Bitdefender	XFCE-Desktop	Gentoo Linux 3.2	2017	683 MB	Deutsch	*www.pcwelt.de/1399815*
Dr. Web	Ubuntu-Desktop und Registry-Editor	Ubuntu 12.04	2017	618 MB	Englisch	*www.pcwelt.de/2QPc3h*
F-Secure	Minimalsystem, nur Virenscanner	Knoppix	2012	140 MB	Englisch	*www.pcwelt.de/308439*
Kaspersky	KDE-Desktop und Registry-Editor	Linux 3.4.24	2012	323 MB	Deutsch	*www.pcwelt.de/1485739*
PC-WELT	XFCE-Desktop, zahlreiche Tools	Lesslinux (2017), Linux 4.1.21	2017	1800 MB	Deutsch	*www.pcwelt.de/E08L0v*
Sophos	Minimalsystem, nur Virenscanner	Slax	2016	160 MB	Englisch	*www.pcwelt.de/SSdBH2*

Partitionen sichern und klonen

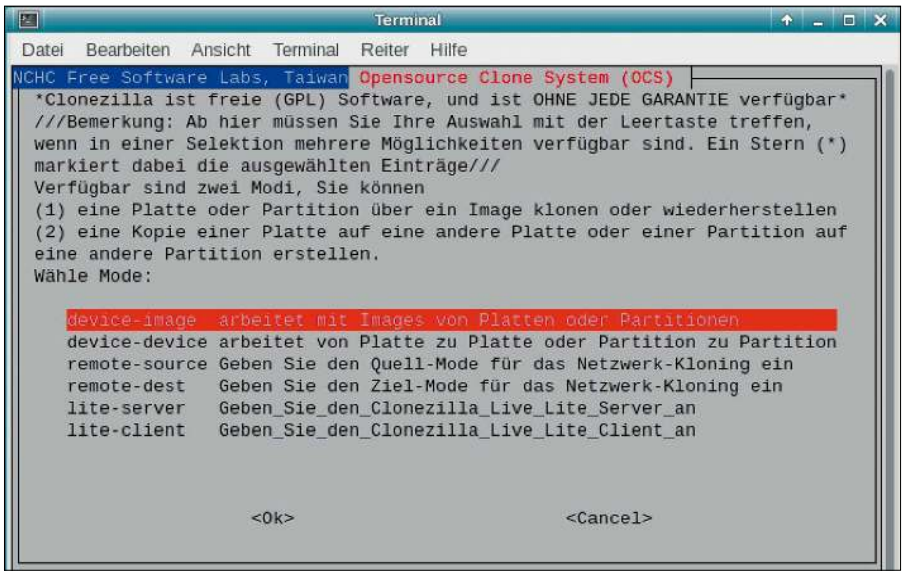
Clonezilla sichert Abbilder von Linux- und Windows-Partitionen. Außerdem hilft das Tool beim Umzug von Festplatte auf SSD, was jedoch einige Vorarbeiten erfordert.

VON THORSTEN EGGELING

Mit Clonezilla speichern Sie Abbilder von Festplatten als Backup (Imaging) oder übertragen den Inhalt einer Festplatte auf eine andere (Klonen). Imaging setzen Sie ein, wenn Sie den aktuellen Zustand eines Systems sichern und bei Bedarf wiederherstellen möchten. Das empfiehlt sich beispielsweise kurz nach der Neuinstallation, wenn das System perfekt eingerichtet ist und stabil läuft. Ordner, in denen sich häufig etwas ändert, etwa das Home-Verzeichnis, sichern sie regelmäßig über andere Tools (siehe Kasten „Regelmäßige Datensicherung“). Die Klonfunktion verwenden Sie beim Umzug des Systems auf eine neue Festplatte oder SSD.

1. So funktioniert Clonezilla

Clonezilla (*https://clonezilla.org*) besteht aus Bash-Scripts, die eine einheitliche Oberfläche für mehrere Kommandozeilentools bereitstellen. Das Tool kopiert nur Sektoren, die mit Daten belegt sind. Das sorgt für optimale Geschwindigkeit. Für das Imagebackup benötigen Sie eine zweite interne oder externe Festplatte mit ausreichend freiem Platz. Die Sicherung kann auch auf einen über SSH oder Samba/CIFS (Windows-Freigabe) erreichbaren Netzwerkspeicher erfolgen.

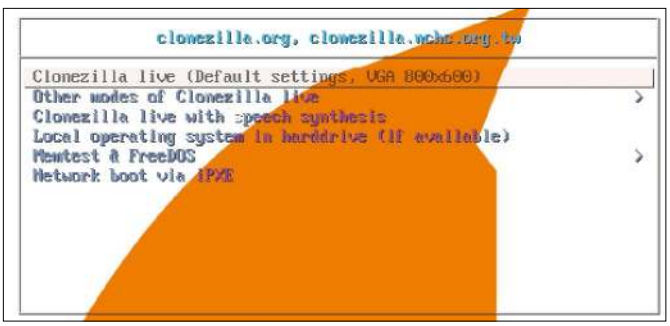


Festplatten klonen und sichern: Clonezilla läuft in einem Terminalfenster. Dank Menüsteuerung ist es jedoch übersichtlich und einfach zu bedienen.

Einschränkungen: Clonezilla unterstützt keinen Raid-Verbund. Ein erzeugtes Festplattenabbild kann außerdem nur komplett zurückgesichert werden, bei Bedarf aber auch auf eine andere Festplatte oder in einer virtuellen Maschine. Einzelne Dateien lassen sich nicht aus dem Abbild extrahieren.

Livesystem: Das Programm benötigt exklusiven Zugriff auf die Festplatte. Deshalb nutzen Sie Clonezilla immer in einem unabhängigen Livesystem, das Sie von einer DVD oder einem USB-Stick starten. Der Hersteller bietet im Downloadbereich von *https://clonezilla.org* mehrere Varianten an. In der Regel ist die 64-Bit-Version von „alternative stable“ zu empfehlen, die auf Ubuntu basiert. Clonezilla ist außerdem im LinuxWelt-Rettungssystem enthalten, das Sie auf der Heft-DVD finden (Download und Updates unter *www.pcwelt.de/2333818*). Die Beschreibungen in diesem Artikel beziehen sich auf das LinuxWelt-Rettungssystem (siehe Seite 68).

Clonezilla läuft im Terminal: Im Menü navigieren Sie mit den Pfeiltasten, Eingaben



Live-DVD: Das Originalsystem des Herstellers läuft auf einem Ubuntu-Unterbau. Es bietet aber nur Clonezilla und keine weiteren Tools, etwa um Partitionen zu verändern.

bestätigen Sie mit der Enter-Taste und über die Leertaste lassen sich Optionen auswählen. Die Oberfläche erscheint weitestgehend in deutscher Sprache, bei Bestätigungen steht jedoch „(y/n)“ in der Frage. Tippen Sie „y“ ein, um die weitere Ausführung fortzusetzen, und drücken Sie die Eingabetaste. „n“ bricht den Vorgang ab.

2. Vorbereitungen für Backup und Klonen

Damit die Sicherung oder der Systemumzug möglichst schnell abläuft, löschen Sie alle Dateien, die Sie nicht zwingend benötigen. Große Dateien, Videos, MP3s und Bilder verschieben Sie auf eine andere Festplatte.

Ubuntu/Mint-Nutzer entfernen unnötige Programmpakete und räumen den Paketcache auf. Das geht am schnellsten in einem Terminalfenster:

```
sudo apt-get autoremove
sudo apt-get autoclean
```

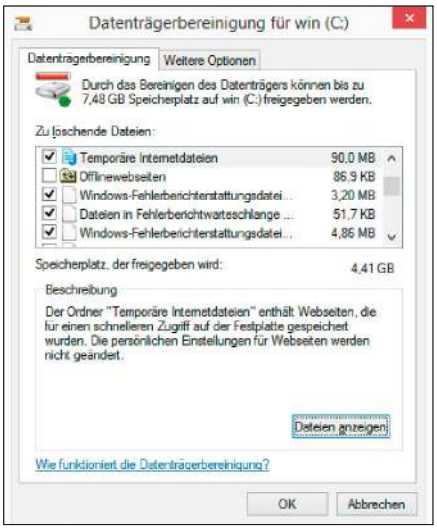
Unter Windows verwenden Sie die Datenträgerbereinigung (Win-R und Eingabe des Befehls „cleanmgr“). Wichtig ist hierbei, die Option „Systemdateien bereinigen“, um neben temporäre Dateien und Papierkorb auch Updatesicherungen und den eventuell noch vorhandenen Ordner „Windows.old“ zu löschen, in dem Windows 10 die Vorgängerversion sichert. Es empfiehlt sich außerdem, das Dateisystem zu prüfen. Dazu öffnen Sie eine Eingabeaufforderung oder Powershell als Administrator und tippen

```
chkdsk c: /f
```

ein. Starten Sie Windows neu, um die Prüfung durchführen zu lassen. Wenn Sie die Festplatte klonen wollen, sollten Sie das Dateisystem vorher defragmentieren. Beim Umzug von einer SSD auf eine neue SSD ist das nicht nötig. Suchen Sie über „Start“ oder im Startmenü nach „Defragmentierung“ und klicken Sie auf „Laufwerke defragmentieren und optimieren“. Markieren Sie das Laufwerk, das Sie defragmentieren wollen, und klicken Sie auf „Optimieren“.

Beenden Sie Windows 8.1 oder 10 anschließend über „Neu starten“ und booten Sie den PC von der LinuxWelt-Rettungs-DVD. Beenden Sie Windows nicht mit „Herunterfahren“, weil sonst unter Linux kein Zugriff auf das Dateisystem möglich ist.

Wenn Sie den Inhalt der bisherigen Festplatte auf eine neue Festplatte kopieren möchten, ist nichts weiter zu beachten, solange das Ziellaufwerk größer oder gleich



Datenvolumen reduzieren: Bevor Sie eine Windows-Partition sichern, löschen Sie überflüssigen Dateien und räumen das System über die Datenträgerbereinigung auf.

groß ist. Handelt es sich um eine SSD, bietet diese wahrscheinlich weniger Speicherplatz. In diesem Fall dürfen sich auf den Partitionen der alten Festplatte insgesamt nicht mehr Daten befinden, als auf die SSD passen (siehe Punkt 6).

Für das Imagebackup schließen Sie eine zweite Festplatte an den PC an, die mit dem Dateisystem NTFS oder Ext4 formatiert sein sollte. Oder Sie erstellen eine Netzwerkfreigabe auf einem NAS oder einem zweiten PC (siehe Punkt 3).

3. Imagebackup einer Festplatte erstellen

Booten Sie den PC von der LinuxWelt-Rettungs-DVD und starten Sie Clonezilla über das Symbol auf dem Desktop. Wählen Sie „device-image“ und dann „local_dev“. Sie haben jetzt Gelegenheit, ein USB-Laufwerk anzuschließen. Drücken Sie die Eingabetaste. Clonezilla zeigt Ihnen die verfügbaren Laufwerke an. Warten Sie, bis das USB-Laufwerk erscheint, und drücken Sie dann die Tastenkombination Strg-C. Wählen Sie das Ziellaufwerk aus und danach ein Verzeichnis, in dem Clonezilla das Backup speichern soll. Gehen Sie mit den Pfeiltasten auf „Done“ und drücken Sie zweimal die Eingabetaste.

REGELMÄSSIGE DATENSICHERUNG

Ein komplettes Backup der Festplatte ist für die meisten Nutzer nur bei umfangreichen Änderungen sinnvoll, etwa nach einem Systemupgrade. Persönliche Daten sollten Sie jedoch regelmäßig sichern, am besten auf einer externen Festplatte. Die folgenden drei Zeilen sichern das Home-Verzeichnis. Der Dateiname wird zusätzlich mit einer Datums- und Zeitangabe versehen.

```
#!/bin/bash
DATE=$(date +%Y-%m-%d-%H%M%S)
tar -cjpf /media/$USER/[USB-Laufwerk]/home_$USER-$DATE.tar.bz2
  $HOME
```

Erstellen Sie das Script in einem Texteditor und speichern Sie es in Ihrem Home-Verzeichnis, etwa als „~/backup.sh“. Machen Sie es dann ausführbar:

```
chmod 755 ~/backup.sh
```

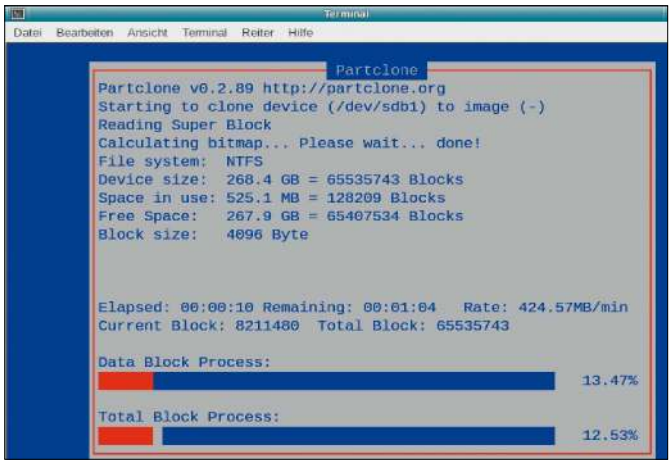
Damit das Script automatisch startet, rufen Sie im Terminalfenster *crontab -e* auf. Tippen Sie hier folgende Zeile ein:

```
0 18 * * * nice -n 19 ionice -c2 -n7 $HOME/backup.sh >/dev/null 2>&1
```

Speichern Sie die Änderung. Damit startet das Script jeden Tag um 18:00 Uhr. Wenn Sie statt „0 18“ den Wert „53 2“ eingeben, wird das Script um 2:53 Uhr ausgeführt.

Wer ein Programm mit grafischer Oberfläche bevorzugt, sollte sich beispielsweise das Backupzool von Ubuntu ansehen. Sie rufen es in den „Systemeinstellungen“ über „Datensicherung“ auf. Ein weiteres nützliches Programm ist Timeshift, mit dem Sie nach Zeitplan Momentaufnahmen des Dateisystems erstellen. Der erste Sicherungspunkt ist ein komplettes Backup der gewählten Verzeichnisse und kann recht groß ausfallen. Die weiteren Wiederherstellungspunkte sind dann deutlich kleiner, da Timeshift nur noch die Unterschiede zum vorherigen Sicherungspunkt speichert. Informationen zur Einrichtung von Timeshift findet Sie unter *www.pcwelt.de/2128851* oder auf der Seite des Herstellers (*www.teejeetech.in/p/timeshift.html*).

Sicherungsziel: Schließen Sie eine USB-Platte am besten vor dem Systemstart an. Clonezilla wartet aber auch, wenn die Platte noch nicht verbunden ist.



Kopierfortschritt: Während Clonezilla Festplatten kopiert, sehen Sie das Fenster von Partclone. Es informiert Sie, welche Partition gerade kopiert wird und wie lange das dauert.

Bestätigen Sie den Modus „Beginner“. Danach wählen Sie „savedisk“, wenn Sie ein Abbild der gesamten Festplatte erstellen möchten. Clonezilla sichert alle Partitionen inklusive Bootmanager. Es spielt keine Rolle, ob Windows, Linux oder beide Systeme installiert sind. Wenn Sie „saveparts“ wählen, sichert Clonezilla nur einzelne Partitionen.

Vergeben Sie einen aussagekräftigen Namen für das Backup. Anschließend wählen Sie die Festplatte oder Partition aus, die Sie sichern möchten. Bei den folgenden Dialogen übernehmen Sie die Voreinstellungen. Folgen Sie den weiteren Anweisungen des Assistenten, prüfen Sie die Einstellungen und bestätigen Sie mit „y“.

Sicherung auf ein Netzwerklaufwerk: Wenn Sie die Imagedateien über das Netzwerk sichern wollen, wählen Sie statt „local_dev“ den Menüpunkt „samba_server“. Danach geben Sie die IP-Adresse oder den Namen des Servers, die Bezeichnung der Freigabe sowie Benutzername und Passwort ein. Fahren Sie dann fort wie bei der lokalen Festplatte beschrieben.

4. Image einer Festplatte wiederherstellen

Starten Sie Clonezilla mit den Optionen „device_image“ und „local_dev“. Wählen Sie die Partition und das Verzeichnis aus, in dem ein zuvor gesichertes Image liegt. Gehen Sie auf „Beginner“ und dann auf „restoredisk“. Wenn Sie vorher einzelne Partitionen gesichert haben, verwenden Sie „restoreparts“. Clonezilla findet auf dem Backupmedium alle Abbilder automatisch und präsentiert sie in einer Liste. Danach wählen Sie die Zielpartition aus, in die das Image zurückgeschrieben werden soll. Nach zwei Sicherheitsabfragen spielt Clonezilla das Backup zurück.

Bei einer Netzwerksicherung läuft das Ganze entsprechend ab. Hier wählen Sie statt „local_dev“ den Menüpunkt „samba_server“ und geben die Verbindungsinformationen an.

5. Alte auf neue Festplatte klonen

Beim Klonen spielt es keine Rolle, ob es sich bei Quelle oder Ziel um Festplatten oder SSDs handelt. Wichtig ist nur die Größe des Ziellaufwerks. Ist es gleich groß oder größer, gehen Sie so vor:

Booten Sie den PC von der LinuxWelt-Rettungs-DVD und starten Sie Clonezilla. Wählen Sie „device-device“, dann „Beginner“ und anschließend „disk_to_local_disk“. Geben Sie die Festplatte an, die Sie klonen wollen. Im nächsten Schritt wählen Sie das Ziellaufwerk. Die folgenden beiden Dialoge bestätigen Sie mit der Eingabetaste, um die Voreinstellungen zu übernehmen. Folgen Sie den weiteren Anweisungen des Assistenten. Prüfen Sie die Einstellungen und bestätigen Sie mit „y“, wenn Sie dazu aufgefordert werden.

Nachdem Clonezilla seine Arbeit beendet hat, kontrollieren Sie die Partitionen auf dem neuen Laufwerk mit Gparted. Den freien Platz auf der Festplatte nutzen Sie, indem Sie die letzte Partition vergrößern.

6. Klonen auf ein kleineres Ziellaufwerk

Wenn auf dem neuen Datenträger weniger Platz verfügbar ist als bisher, müssen Sie die Partitionen zuerst verkleinern. Dafür verwenden Sie Gparted von der LinuxWelt-Rettungs-DVD. Wie bei jeder größeren Änderung der Partitionsstruktur sollten Sie sicherheitshalber vorher ein Backup erstellen wie in Punkt 3 beschrieben.

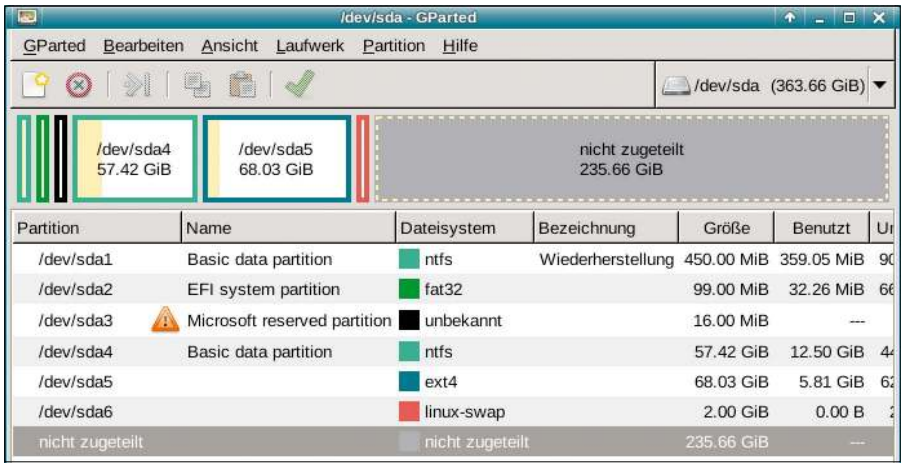
Partitionen verkleinern: Gparted lässt sich über das Desktopicon starten. Rechts oben wählen Sie die Festplatte aus, beispielsweise „sda“ für das erste Laufwerk im PC. Wählen Sie die Systempartition per Mausklick und gehen Sie im Kontextmenü auf „Größe ändern/Verschieben“. Wählen Sie mit dem Regler die gewünschte Partitionsgröße. Klicken Sie auf „Größe ändern“. Gparted führt die Änderung erst nach einem Klick auf „Anwenden“ in der Symbolleiste durch. Sind hinter der Systempartition weitere Partitionen vorhanden, verkleinern Sie auch diese. Schieben Sie die jeweilige Partition über den Regler an den Anfang, damit sich alle Bereiche hintereinander befinden. Beim Verschieben gibt Gparted eine Warnmeldung aus, die Sie ignorieren können.

Wichtig: Ändern Sie nur die Größe und/oder Position von System- und Datenpartitionen. Boot- und EFI-Partitionen lassen Sie unverändert.

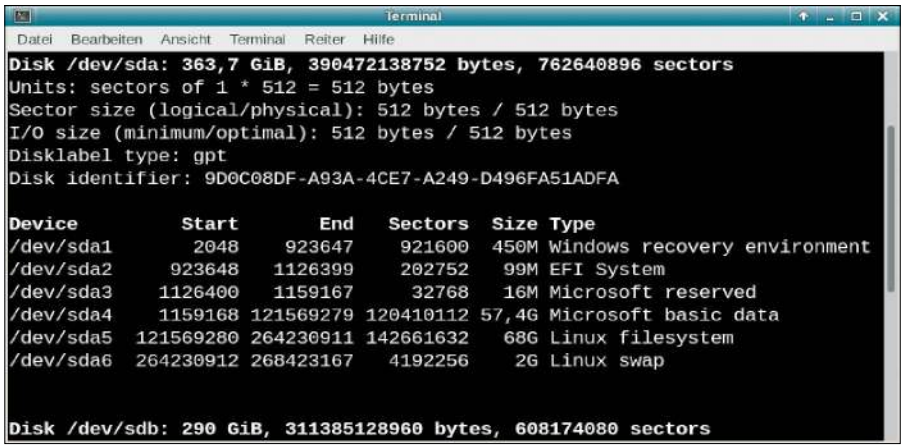
Beenden Sie das LinuxWelt-Rettungssystem und prüfen Sie, ob Linux beziehungsweise Windows noch starten. Wenn Sie Partitionen verschoben haben, müssen Sie in der Regel den Bootmanager reparieren. Wie das bei Linux geht, steht auf Seite 68. Informationen zur Reparatur der Windows-Bootumgebung finden unter *www.pcwelt.de/2058900* („Win RE“, „Starthilfe“).

Partitionstabelle kopieren: Die Zielfestplatte muss die gleichen Partitionen erhalten wie die Originalfestplatte. Führen Sie im Terminalfenster

`fdisk -l`
aus, um sich einen Überblick zu verschaffen. fdisk zeigt Ihnen hinter „Disklabel type:“ auch an, ob die Festplatte mit dem GPT- oder MBR-Partitionsstil eingerichtet ist („gpt“ oder „dos“).
In unserem Beispiel gehen wir davon aus, dass es sich bei „sda“ um die Originalfestplatte handelt und das Ziellaufwerk „sdb“ ist. Eine GPT-Partitionstabelle kopieren Sie mittels des Befehls
`sgdisk -R /dev/sdb /dev/sda`
Bei MBR verwenden Sie
`sfdisk -d /dev/sda | sfdisk -f /dev/sdb`
Alternativ können Sie die Partition auf der Zielfestplatte auch über Gparted erstellen. Gehen Sie dort auf „Laufwerk → Partitionstabelle“, um die neue Festplatte im GPT- oder MBR/MSDOS-Partitionsstil einzurichten. Wichtig ist, dass Anzahl und Typ der Partitionen denen der bisherigen Festplatte entsprechen und nur die Größe abweicht.
Festplatte klonen: Wählen Sie dazu nach „device-device“ statt des bisher benutzten „Beginner“-Modus den Eintrag „Expert“. Wählen Sie „disk_to_local_disk“ und danach Original- und Zielfestplatte aus. Als Nächstes erscheint ein Dialog mit Experteneinstellungen.
Aktivieren Sie mit der Leertaste zusätzlich die Option „-icds“. Bestätigen Sie die Einstellungen in diesem und dem folgenden Dialog mit der Eingabetaste. Danach wählen Sie die Option „-k KEINE Partition-Tabelle mit Bootsektor des Zielsystems erstellen“. Damit verzichtet Clonezilla darauf, die Partitionstabelle zu ändern. Folgen Sie den weiteren Anweisungen des Assistenten. Prüfen Sie die Einstellungen und bestätigen Sie mit „y“, wenn Sie dazu aufgefordert werden.
Kontrollieren Sie abschließend die Partitionen auf dem neuen Laufwerk mit Gparted. Sollte noch Platz am Ende frei sein, vergrößern Sie die letzte Partition.
Bauen Sie die alte Festplatte aus und starten Sie das System von der neuen geklonten Platte. Wenn Sie die alte Festplatte weiter im selben PC verwenden möchten, müssen Sie sie über Gparted neu partitionieren. Denn auf beiden Platten tragen die Partitionen die gleiche UUID, über die Linux die Laufwerke einbindet. Sind diese zweimal vorhanden, werden die Partitionen in den gleichen Pfad eingehängt, was zu Problemen führt. ■



Partitionen verändern: Wenn Sie ein größeres auf ein kleineres Laufwerk kopieren wollen, müssen Sie die Partitionen vorher mit Gparted verkleinern.



Festplatteninfos: fdisk zeigt die Partitionen auf der Festplatte an und informiert hinter „Disklabel type:“ über das verwendete Partitionsschema (gpt oder dos).

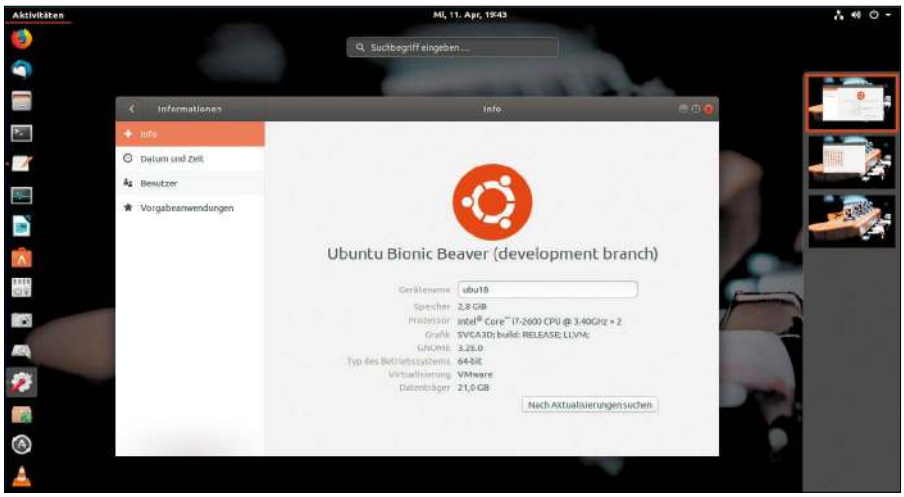
PROFIBACKUP FÜR WINDOWS

WIM-Dateien (Windows Imaging Format) eignen sich für platzsparende Backups von NTFS-Partitionen. Unter Windows verwenden Sie Tools wie Dism oder Imagex, um WIM-Dateien zu erstellen oder zu bearbeiten. Das Open-Source-Tool wimlib-imagex (*https://wimlib.net*) gibt es für Windows sowie Linux und es ist auch im LinuxWelt-Rettungssystem enthalten.
Wenn auch Windows auf Ihrer Festplatte installiert ist, bietet wimlib-imagex im Vergleich zu Clonezilla einige Vorteile: Das Tool arbeitet relativ schnell, außerdem können Sie bei Bedarf auch einzelne Dateien aus dem Backup extrahieren und inkrementelle Sicherungen erstellen. Unter Linux lassen sich nur komplette Partitionen sichern, bei der Windows-Version können Sie auch einzelne Ordner für die Sicherung auswählen.
Wenn Sie in einem Terminalfenster
`wimlib-imagex`
starten, erhalten Sie eine Übersicht mit allen Funktionen und Optionen. Es ist einfacher, die gewünschten Funktionen direkt aufzurufen. *wimcapture* beispielsweise verwenden Sie für Backups, *wimappend* für inkrementelle Backups und *wimapply*, um Windows wiederherzustellen. Ausführliche Informationen zu wimlib-imagex finden Sie unter *www.pcwelt.de/2056754*.

Das neue Ubuntu 18.04 LTS

Wie geht es weiter mit Canonical und seinem Ubuntu-System? Nach etlichen Niederlagen im Jahr 2017 ist das soeben erschienene Langzeit-Ubuntu 18.04 ein Seismograph, wie viel Desktopehrgeiz hinter Ubuntu steckt: Es sieht gut aus.

VON HERMANN APFELBÖCK



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

Nachdem Ubuntu im letzten Jahr ehrgeizige Projekte wie den Unity-Desktop oder den hauseigenen Displayserver Mir über Bord werfen musste, war nicht offensichtlich, wie das nächste LTS-System ausfallen würde. Jetzt liegt es vor – und es sieht gut aus, insbesondere die Hauptvariante mit dem Gnome-Desktop. Canonical hat Ubuntu nicht nur mit aktuellem Kernel und frischer Software aktualisiert, sondern an signifikanten Verbesserungen unter der Haube gearbeitet und nebenbei Feinschliff am Desktop betrieben.

Die nachfolgenden Seiten führen Sie newstechnisch und praktisch durch das neue Ubuntu 18.04 LTS („Bionic Beaver"), während Sie die Heft-DVD mit der Ubuntu-Hauptedition mit Gnome, ferner mit Ubuntu Mate, Xubuntu und Lubuntu versorgt. Trotz knapper Terminlage können wir auf Heft-DVD durchwegs die finalen Ubuntus 18.04 anbieten. Die weiteren Ubuntu-„Flavours" Kubuntu mit KDE und Ubuntu Budgie erhalten Sie unter *https://kubuntu.org/* und *https://ubuntubudgie.org*.

Die Artikel beziehen sich hingegen aus Termingründen auf die zweite und letzte Betaversion der erwähnten Distributionen. Diese hatte aber den „Feature Freeze" (Anfang März) längst hinter sich, so dass keine Abweichungen zur finalen Version zu erwarten sind.

Überarbeitete Installer Ubiquity und Subiquity

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

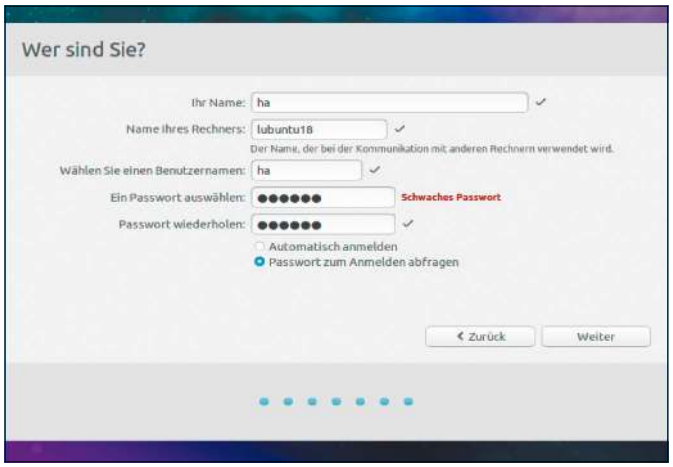
Installer mit neuer „Minimal"-Option (hier unter Ubuntu Budgie): Das kommt Nutzern entgegen, die sich die Anwendungssoftware individuell zusammenstellen möchten.

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

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

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

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



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

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

Rekordverdächtiger Systemstart

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

Aktueller Kernel 4.15 & Software

Ubuntu 18.04 wird mit dem Linux-Kernel 4.15 ausgeliefert. Den aktuellsten Kernel 4.16 von Anfang April konnte Ubuntu nicht mehr berücksichtigen. Version 4.15 enthält aber bereits die Schutzmechanismen vor den CPU-Bugs Meltdown und Spectre, ferner die neuesten Treiber für AMD-Grafikkarten. Auch Unterstützung für die jüngste Intel-CPU-Generation „Coffee Lake" (seit Ende 2017) ist gewährleistet.

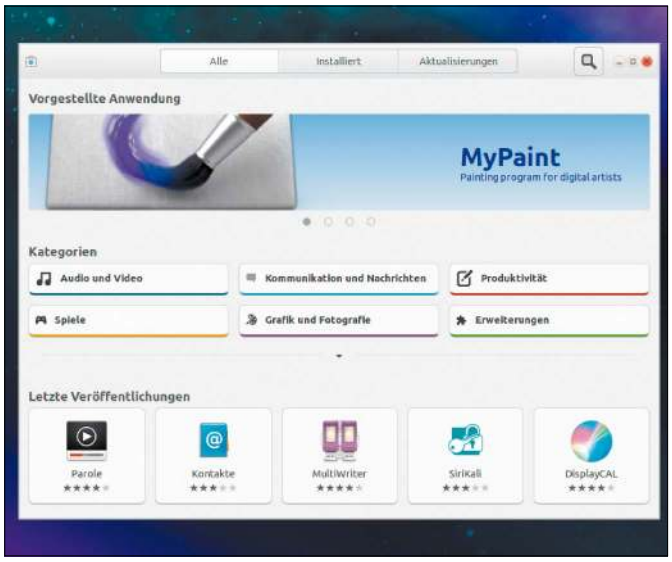
Unabhängig vom jeweiligen Desktop kommen frische Softwareversionen mit. Libre Office meldet Version 6.0.2.1, der VLC Media Player 3.0.1, der Firefox-Browser 59.0.2 und der unter Ubuntu Budgie genutzte Chromium-Browser die Version 65.0. Das ist alles Software neuesten Stands.

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

Xorg statt Wayland

Der Umstieg vom alten X11-Display-Server (Xorg) zu Wayland ist weiter verschoben. Alle Ubuntu-Editionen nutzen weiterhin Xorg als Standard. Die Hauptedition mit Gnome, ferner auch Kubuntu mit KDE bieten Wayland aber immerhin optional am Anmeldebildschirm. Wayland verspricht im Prinzip schnellere Grafikdarstellung und flüssigere Videos, denn er verkürzt und vereinfacht grafischen Programmen den Weg auf den Bildschirm. Der Effekt-Compositor, den die Desktopoberflächen verwenden, kommuniziert umweglos mit Wayland.

Unter Wayland gibt es aber immer noch diverse Probleme: So ist die Anzeige grafischer Programme über das Netzwerk via SSH derzeit nicht möglich (X11-Forwarding) und Tools wie xprop, xkill oder die Shell-Erweiterung „Force Quit" arbeiten unter Wayland nicht oder nicht erwartungsgemäß. Generell gilt: Wer Ubuntu oder Ku-



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

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

buntu mit Wayland nutzt, sollte diese Tatsache nicht aus den Augen verlieren und bei Problemen am Anmeldebildschirm wieder auf X11 zurückschalten – also auf „Ubuntu" statt „Ubuntu mit Wayland".

Die Softwarezentrale (Gnome-Software)

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

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

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

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

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

Ubuntu als Datenkrake?

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

Vollfarbige Emoji-Symbole

Farbige Emojis erforderten auf älterem Ubuntu die Installation von zusätzlichen Tools. Ab Version 18.04 LTS sind sie standardmäßig an Bord. Die Emojis sind die vertrauten Open-Source-Emojis von Android-Mobilgeräten. Das Tastaturkürzel auf deutschsprachigem System für die Emoji-Eingabeauswahl ist Strg-Umschalt-, (Komma). In den Beta-2-Versionen funktionierte das Einblenden der Emoji-Auswahl nur in der Standardedition mit Gnome einwandfrei. Andere Editionen antworten zwar auf den Hotkey, boten aber die Piktogramme nicht an. Wir nehmen an, dass das Problem in den finalen Versionen überall behoben ist.

Die Ubuntu-Varianten

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

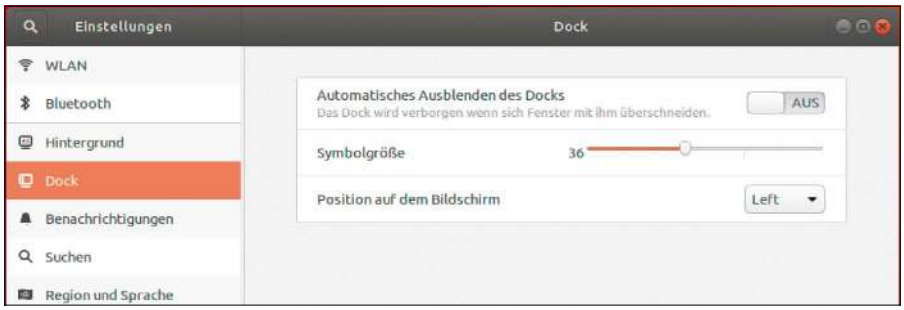
Ubuntu (Gnome): Die Umsteiger der bisherigen LTS-Version 16.04 auf 18.04 erwartet nun der Bruch, den Ubuntu schon mit der Zwischenversion 17.10 vollzogen hat. Man wird Canonical aber anerkennen, dass es den Übergang von Unity zu Gnome außerordentlich sanft ebnet.

Anders als unter originalem Gnome ist die Favoritenleiste standardmäßig sichtbar – ähnlich der bisherigen Unity-Starterleiste. Ihre Position ist über „Einstellungen → Dock“ flexibel auch rechts oder unten möglich. Anders als bei Gnome dient die Desktopoberfläche standardmäßig als Dateiablage. Für diese Funktion nutzt Ubuntu gezielt einen älteren angepassten Dateimanager Nautilus.

Nautilus, der identisch auch in Ubuntu Budgie enthalten ist, wurde generell überarbeitet und verschlankt: „Geräte“ und „Netzwerk“ ist zu „Andere Orte“ zusammengefasst und die Option „Mit Server verbinden“ erscheint automatisch in der Statusleiste, sobald man diesen Navigationspunkt auswählt.

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

Die GTK-Themen Radiance und Ambiance haben Ubuntu jahrelang begleitet. Ubuntu 18.04 bringt voraussichtlich ein neues moderneres Fenster- und Icon-Thema („Suru“) mit – „voraussichtlich“ deshalb, weil die uns vorliegende Beta zwar den manuellen Einbau des neuen „Communitheme“ samt „Suru“-Iconset erlaubte, das final eingebaute Thema aber noch fehlte. Die Optik geht in Richtung Ubuntu Budgie und der modernen Mint-Y-Themes von Linux Mint.



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

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

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

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

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

Ubuntu 18.04: Upgrade & Installation

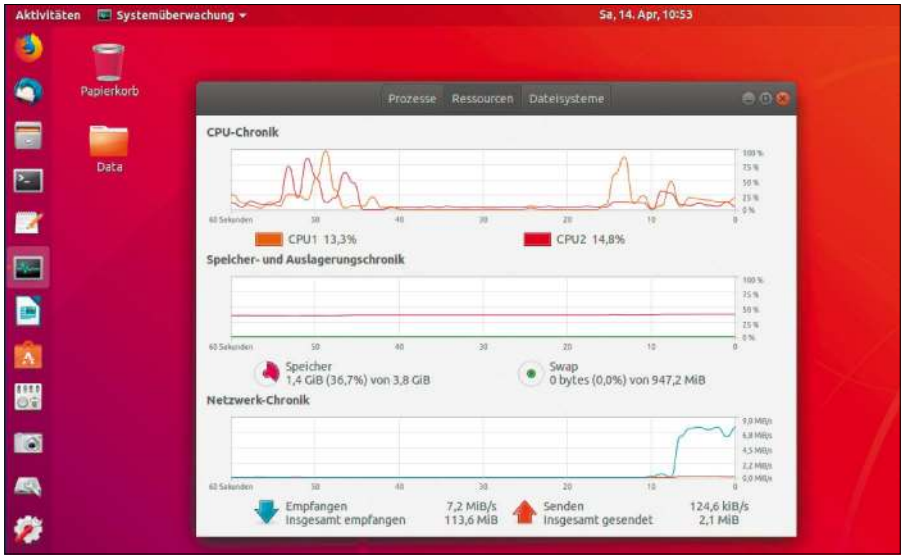
Ubuntu 18.04 hat am Installer Änderungen vorgenommen, die das Setup unterm Strich eher vereinfachen. Die Aufgaben der Partitionierung und Ersteinrichtung bleiben unverändert. Lediglich der Verschlüsselungsaspekt gewinnt zusätzliches Gewicht.

VON HERMANN APFELBÖCK

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

1. Das Upgrade älterer Versionen

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



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

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

2. Entscheidungen vor einer Neuinstallation

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

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

Dies der „belegte“ Speicher nach der Systemanmeldung. Überraschend ist zweierlei, erstens der vergleichsweise hohe RAM-Verbrauch des Gnome-Desktops (zum Vergleich: das ältere Ubuntu 16.04 mit

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

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

3. Uefi- und Bios-Installationen

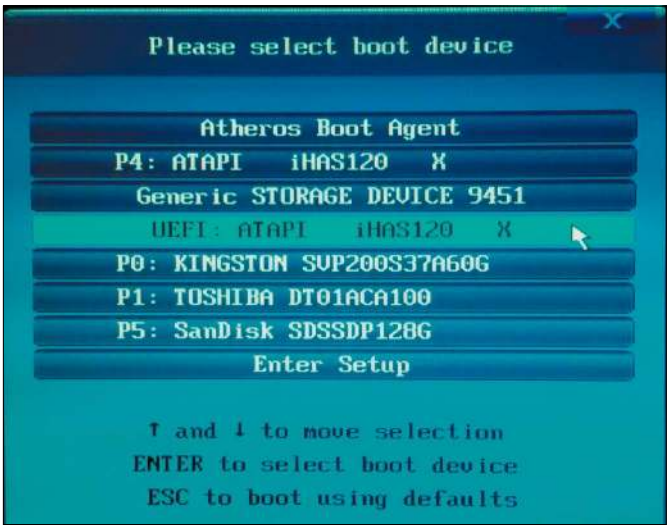
Um Ubuntu 18.04 neu zu installieren, nutzen Sie am besten die beiliegende Heft-DVD, sofern Sie eine der vier dort enthaltenen Editionen wünschen. Die Editionen mit Budgie- und KDE-Desktop (Kubuntu) sind nicht enthalten: Diese müssen Sie sich bei Bedarf aus dem Internet laden (*https://ubuntubudgie.org* und *https://kubuntu.org/*) und das ISO-Image auf einen eigenen Datenträger schreiben – am besten auf USB-Stick. Dafür verwenden Sie wahlweise den plattformübergreifenden Etcher (*https://etcher.io/*) oder dd unter Linux oder auch den Win 32 Disk Imager unter Windows (auf Heft-DVD).

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

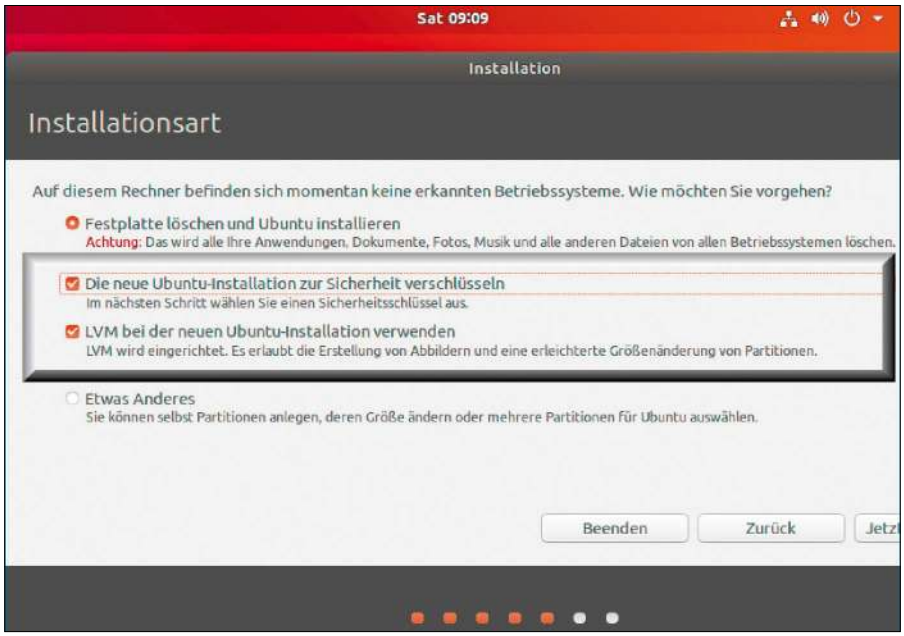
Vor der Notwendigkeit, im Uefi-Modus zu installieren, stehen Sie dann, wenn der Rechner bereits ein System im Uefi-Modus enthält (Windows 8/10) und Ubuntu parallel installiert werden soll.

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

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



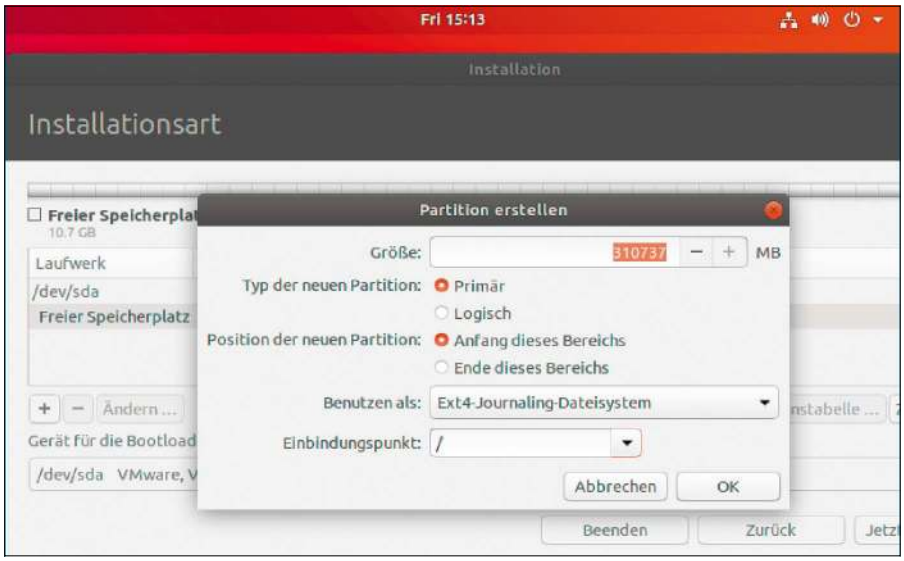
Uefi-Bootmenü: Eine eingelegte DVD erscheint hier als „P4: ATAPI" und als „UEFI: ATAPI". Für Uefi-Installationen muss die Uefi-Bootoption gewählt werden.



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

4. Im Installationsassistenten Ubiquity

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



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

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

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

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

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

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

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

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

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

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

5. Paketquellen und erste Aktualisierung

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

```
sudo apt update
```

zu den ersten Pflichten. Danach bringt der Befehl

```
sudo apt upgrade
```

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

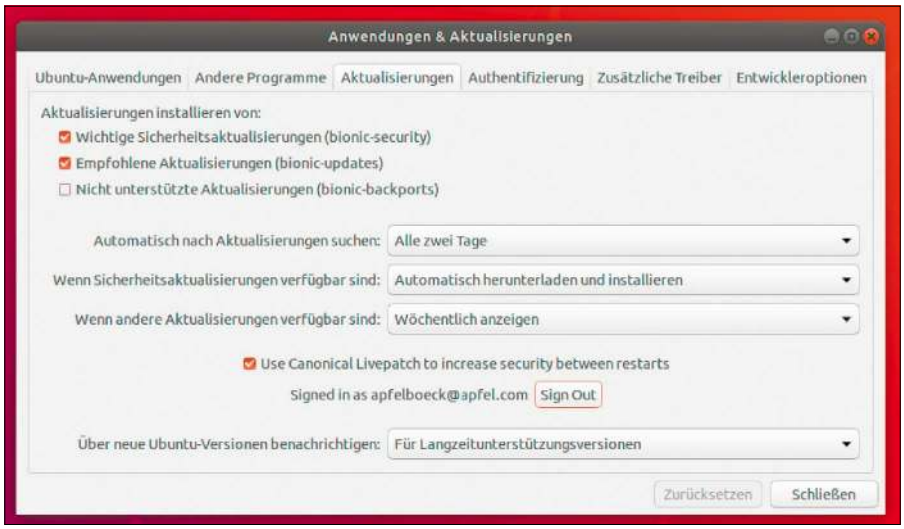
Im weiteren Alltag sorgt die „Aktualisierungsverwaltung“ (update-manager) automatisch dafür, dass die Updates regelmäßig eingepflegt werden. Unter „Anwendungen & Aktualisierungen → Aktualisierungen“

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

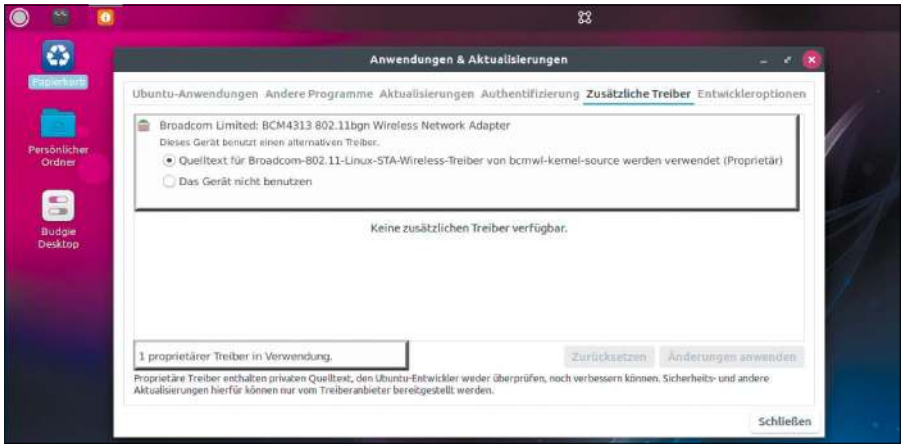
„Livepatches" für Server: Ein neuer Service in Version 18.04 blieb in der vorangehenden allgemeinen Ubuntu-Vorstellung unerwähnt (ab Seite 56), da er für Desktop-PCs keine Rolle spielt.

Ubuntu-Rechner als Serverdauerläufer können von Canonical „Livepatches" beziehen – dies zwar schon seit Version 16.04, nun aber ganz bequem an der grafischen Oberfläche unter „Anwendungen & Aktualisierungen" auf der Registerkarte „Aktualisierungen". Dazu ist ein Konto bei Canonicals Cloud „Ubuntu One" erforderlich. Bis zu drei Rechner pro Konto können kostenlos Livepatches beziehen.

Das Motiv für diese Technik sind sicherheitsrelevante Kernel-Patches, die eigentlich einen Neustart benötigten. Livepatches stopfen die Sicherheitslücken vorläufig im laufenden Betrieb, so dass störende Neustarts unbefristet verschoben werden können. Wie gesagt: Es handelt sich um einen Service für Serverdauerläufer. Auf PCs und Notebooks, die jeden Tag neu gestartet werden, sind die Livepatches definitiv irrelevant.



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



Herstellertreiber für Grafik- oder WLAN-Chips: Die Treibersuche unter „ Anwendungen & Aktualisierungen" betrifft meist nur diese beiden Geräteklassen.

6. Sprache, Hardware und Netzwerk einrichten

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

Sprachunterstützung: Bei der Installation legen Sie zwar die Sprache „Deutsch" und die Region „Deutschland" fest, was jedoch noch kein konsequent deutschsprachiges System ergibt. Nach der Installation ist es zu empfehlen, in den „Einstellungen" die Sprachpakete zu komplettieren. Der Punkt heißt „Region & Sprache" (Ubuntu) oder auch nur „Sprachen" (etwa in Xubuntu).

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

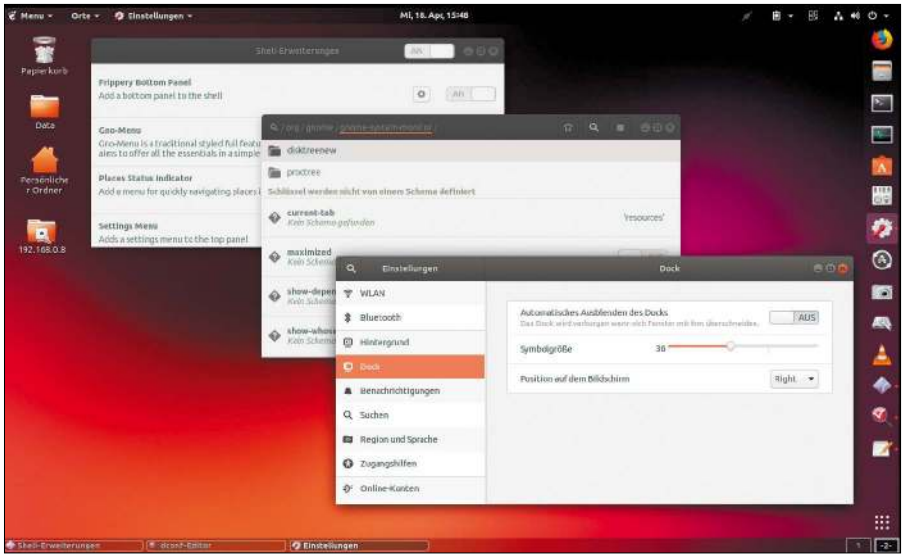
Monitoreinstellungen: Ubuntu erkennt die optimale Bildschirmauflösung automatisch. Trotzdem gibt es Anlässe, die Einstellungen nachzujustieren: Bei einem Betrieb mit zwei Monitoren ist es immer notwendig, den primären Bildschirm und die optimale Anordnung der Monitore festzulegen. Die wichtigsten Optionen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

Netzwerkadapter: Mit Kabelverbindung ist Ubuntu sofort im Netz und Internet. Mit WLAN-Adaptern besteht die übliche Pflicht, sich am eigenen WLAN anzumelden. Dies funktioniert über das Netzwerk-Symbol in der Systemleiste (Network-Manager). Wenn der WLAN-Adapter hardwaretechnisch nicht erkannt wird, fehlen dort die Option „Funknetzwerk aktivieren" sowie die Anzeige der nahen WLANs. Dann hilft eventuell eine vorübergehende Kabelverbindung und das Nachladen des proprietären Treibers (wie unter „Grafiktreiber installieren"). Es gibt allerdings USB-WLAN-Dongles, die unter Ubuntu nicht funktionieren. ■

Ubuntu 18.04 optimieren

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

VON HERMANN APFELBÖCK



Nicht weniger als sechs offizielle Editionen zählt die aktuelle Ubuntu-Desktop-Familie. Und jede Edition, selbst ein spartanisches Lubuntu, enthält eine Vielzahl von optischen und funktionalen Anpassungsmöglichkeiten. Dieser Artikel legt den Fokus auf die Gnome-Hauptedition und die Budgie-Variante. Das ist keine Wertung, sondern Reflex auf die Tatsache, dass hier der größte Informationsbedarf besteht: Gnome bedeutet für bisherige Ubuntu-LTS-Nutzer eine größere Umstellung und der Budgie-Desktop ist die aktuell agilste Oberfläche mit den meisten Neuerungen. Für KDE-, Mate-, XFCE- und LXDE-Nutzer bedeutet das Upgrade auf Ubuntu 18.04 weitestgehende Desktopkontinuität auf neuem Unterbau.

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

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

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

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

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

Das Optimierungstool gnome-tweaks

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

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

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

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

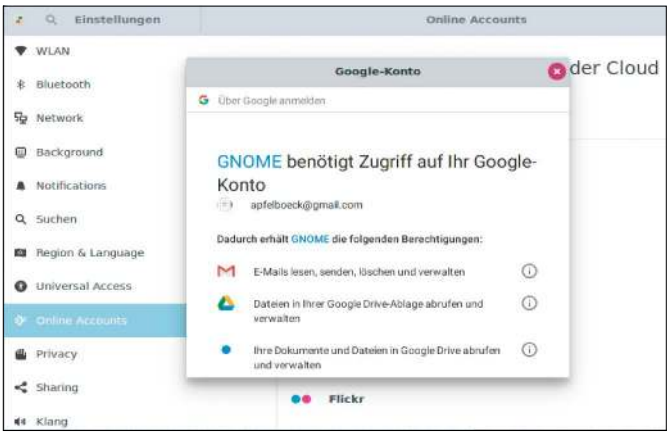
Unter „**Erweiterungen**“ verwalten Sie die aktuell installierten Gnome-Extensions. Über das Tweak-Tool schalten Sie Erweiterungen mit sofortiger Wirkung „An“ und „Aus“. Außerdem führt das Zahnradsymbol zu den Detaileinstellungen einer Erweiterung, sofern diese solche vorsieht. Mehr zu diesen Erweiterungen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

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

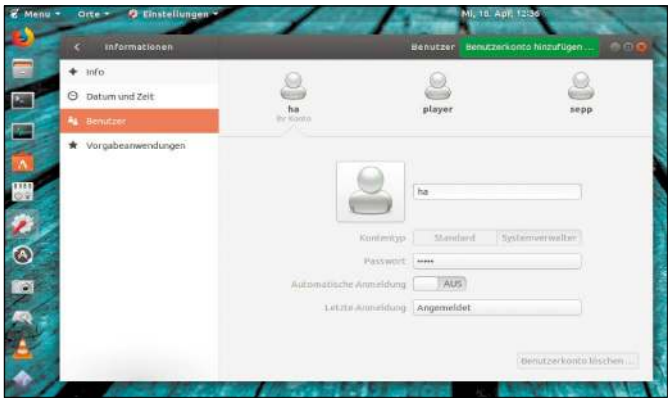
Der Punkt „**Schriften**“ erlaubt einen praktisch stufenlosen Skalierungsfaktor für die Schriften. Damit verändern Sie das Erscheinungsbild maßgeblich und passen es optimal an Bildschirm und Sehvermögen an.

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

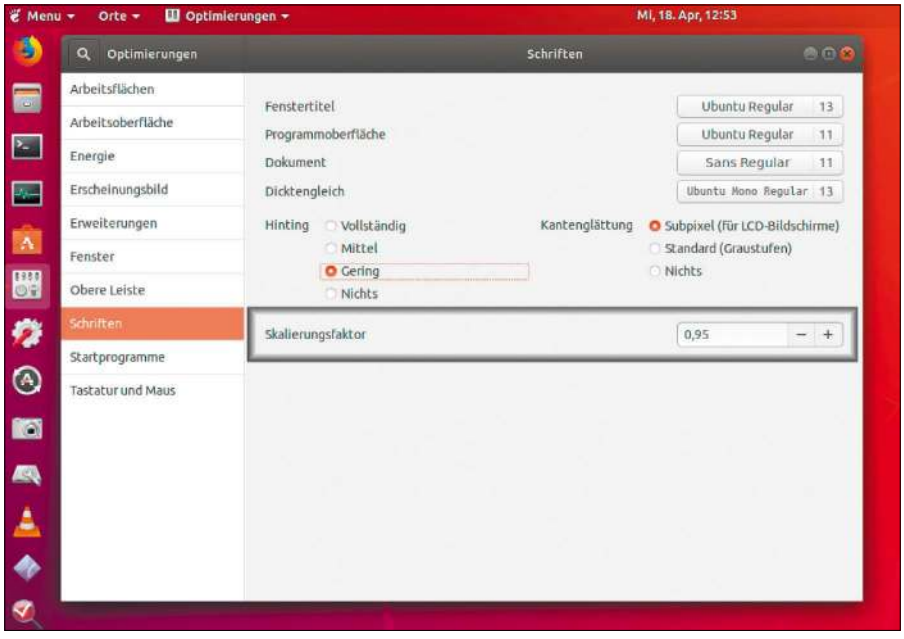
Unter „**Tastatur und Maus**“ finden Sie eine Reihe interessanter Angebote, Tasten stillzulegen, neu zu belegen oder zu vertauschen („Zusätzliche Belegungsoptionen“). So ist der Hotkey Strg-Alt-Del standardmä-



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

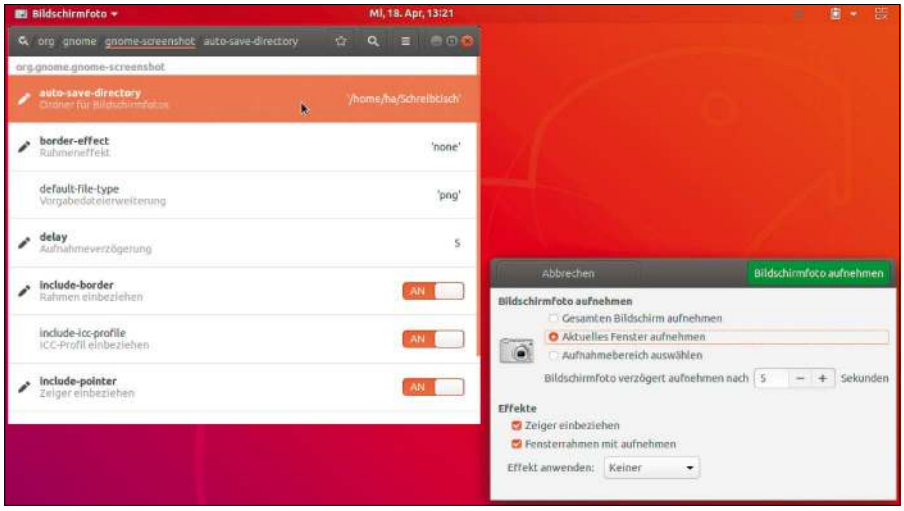


Benutzerkonten einrichten: Diese wichtige Anlaufstelle versteckt das gnome-control-center („Einstellungen“) unter der Kategorie „Information“.



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

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



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

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

Die Gnome-Erweiterungen

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

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

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

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

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

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

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

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

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

Feineinstellungen mit dem Dconf-Editor

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

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

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

leicht korrigieren.

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

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

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

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

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

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

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

auf die Standardwerte zurücksetzen. ■

DEN BUDGIE-DESKTOP EINRICHTEN

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

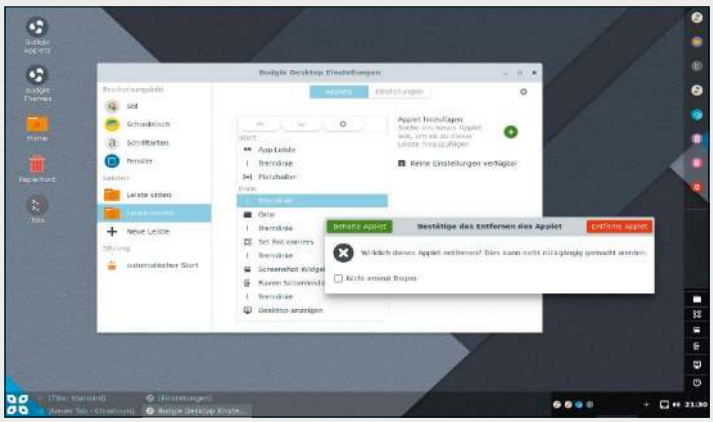
Budgie ist jung, in manchen Details etwas konfus, die deutsche Lokalisierung nicht vollständig und auch die überschätzte Benachrichtigungsleiste „Raven“ ist kein ernstes Motiv, sich in diesen Desktop zu vergucken.

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

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

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

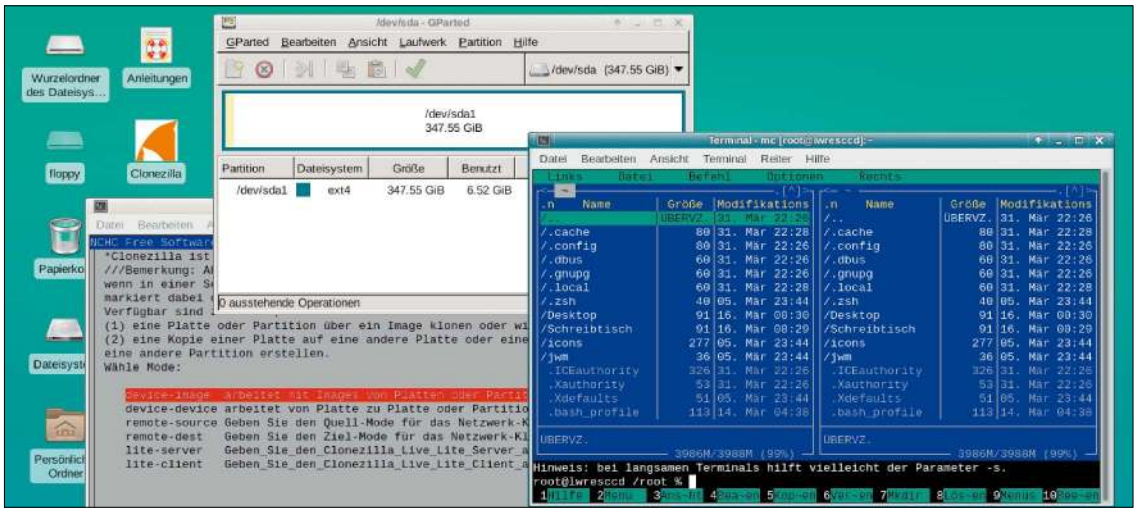
Wer sich in einer Leiste einen Favoriten-Starter einrichten will, wird zunächst nicht fündig: Einschlägig ist das Applet „App-Leiste“ („Icon Task List“). Gestartete Programme werden dann als Icon angezeigt und lassen sich nach Rechtsklick mit der Option „Zur Leiste hinzufügen“ dauerhaft anheften – die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



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

Neu: Die LinuxWelt-Rettungs-DVD 6.2.1

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



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

VON THORSTEN EGGELING

Jedes Livesystem kann bei der Windows- oder Linux-Reparatur helfen, wenn das installierte System nicht mehr startet. Ein spezialisiertes System wie die LinuxWelt-Rettungs-DVD hält jedoch bereits alle einschlägigen Werkzeuge für Reparaturen parat. Mit den enthaltenen Tools lassen sich beispielsweise Partitionen vergrößern oder verkleinern, Festplatten klonen oder in einer Abbilddatei speichern. Sie können damit eine defekte Bootumgebung reparieren und vergessene Anmeldepasswörter zurücksetzen.

LinuxWelt-Rettungs-DVD starten

Die LinuxWelt-Rettungs-DVD 6.2.1 basiert auf System Rescue CD 5.2.1 (*www.system-rescue-cd.org*) und Gentoo Linux (*www.gentoo.org*). Sie bietet aber eine deutschsprachige Oberfläche, zudem haben wir einige zusätzliche Tools eingebaut. Die Version 6.2.1 verwendet den relativ aktuellen Linux-Kernel 4.14.20 (64 oder 32 Bit).

Das System startet standardmäßig mit der grafischen Oberfläche XFCE und deutscher Tastaturbelegung. PCs im Bios-Modus können direkt von der Heft-DVD booten. Wenn Sie das System im Uefi-Modus booten wollen, müssen Sie es auf einen USB-Stick übertragen. Einen bootfähigen USB-Stick erstellen Sie am einfachsten über das Kommandozeilentool dd. Verbinden Sie den USB-Stick mit dem PC und öffnen Sie ein Terminalfenster. Mit dem Befehl

```
lsblk -p
```

ermitteln Sie die Kennung des USB-Laufwerks. In der Ausgabe sehen Sie beispielsweise „/dev/sdb1“ und dahinter „/media/[user]/[Kennung]“. Hängen Sie den USB-Stick mit dieser Befehlszeile aus dem Dateisystem aus:

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

Der Platzhalter „[X]“ steht für die Gerätebezeichnung, beispielsweise „/dev/sdb“. Kopieren Sie dann die Datei „/Image-Dateien/lwRescue621.iso“ von der Heft-DVD in Ihr Home-Verzeichnis. Geben Sie dann im Terminal folgenden dd-Befehl mit angepassten Pfaden ein. Nach „if=“ folgt Pfad und Name der ISO-Datei, nach „of=“ der Gerätename des USB-Sticks:

```
sudo dd bs=1M if=/pfad/lwRescue601.iso of=/dev/sd[X]
```

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

Startvarianten: Wenn Sie den PC mit dem LinuxWelt-Rettungssystem booten, wählen Sie im Menü in der Regel den ersten Eintrag. Sollte es damit Probleme geben oder nur

ein schwarzer Bildschirm erscheinen, verwenden Sie einen USB-Stick. Sie können dann zwischen einem Kernel mit 32 Bit oder 64 Bit wählen und beispielsweise „C) 64-Bit-Kernel (rescue64) mit weiteren Optionen → Rettungs-DVD mit VESA-Grafik" wählen. Über die Tasten F2 bis F7 blenden Sie Hilfetexte ein, die Informationen zu den Bootoptionen für die Problembehebung enthalten.

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

Zugriff auf Festplattenpartitionen

Die LinuxWelt-Rettungs-DVD bindet Partitionen nicht automatisch ein. Gehen Sie im Menü auf „System → Show Filesystems", um nachzusehen, welche Festplatten im PC stecken, sowie deren zugehörige Partitionen, Größen und Dateisysteme. In der Liste taucht beispielsweise „sda1" auf, in der Spalte „FILESYS" sehen Sie „ext4". Binden Sie diese Partition über folgenden Terminalbefehl ein:

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

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

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

Anschließend starten Sie den Dateimanager über „Zubehör → Thunar Dateiverwaltung". Im Terminal steht Ihnen außerdem der Dateimanager Midnight Commander zur Verfügung (mc). Über den Dateimanager greifen Sie auf die eingehängten Partitionen unter „/mnt" zu. Über das Kontextmenü bearbeiten Sie in Thunar Konfigurationsdateien („Mit Geany öffnen") oder sichern Ordner in einer tar.gz-Datei („Archiv erstellen"). Per Klick auf „Netzwerke durchsuchen" greifen Sie auf Netzwerkfreigaben zu, die Sie etwa für die Datensicherung verwenden.

Passwort löschen oder Grub reparieren

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

```
[UserName]:$6$I70lv
 Cp[...]:17565:0:99999:7:::
```

Die lange Zeichenfolge hinter dem Benutzernamen zwischen den Doppelpunkten ist das verschlüsselte Passwort. Sie löschen die Zeichenfolge einfach und speichern die Datei. Danach starten Sie das installierte System und melden sich ohne Passwort an. Windows-Passwörter lassen sich über „A) Extras und Tools starten → Ntpasswd" im Bootmenü der LinuxWelt-Rettungs-DVD löschen.

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

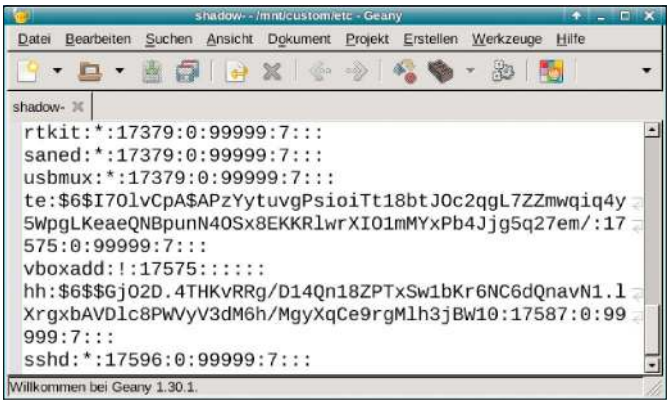
```
mount -o bind /dev /mnt/custom/dev
mount -o bind /sys /mnt/custom/sys
mount -t proc /proc /mnt/custom/
 proc
chroot /mnt/custom /bin/bash
grub-install /dev/sd[X]
update-grub
```

„/dev/sd[X]" ersetzen Sie durch den Laufwerkspfad der Festplatte, auf der das System installiert ist.

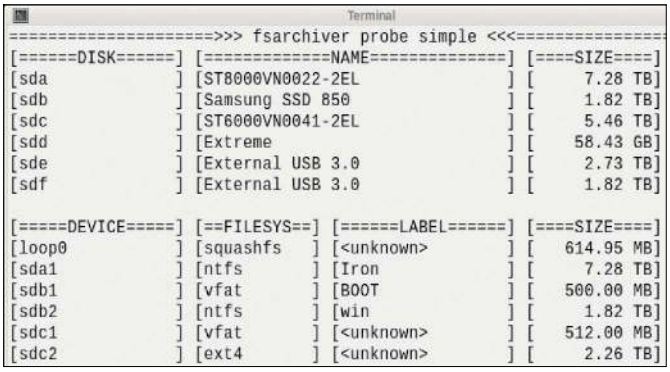
Bei einem Uefi-System müssen Sie zusätzlich die EFI-Partition in „/mnt/custom/boot/efi" einhängen. Verwenden Sie in der chroot-Umgebung grub-install ohne Angabe der Zielpartition und danach den Befehl *update-grub*.

Weitere Tools der LinuxWelt-Rettungs-DVD

Über das Menü oder Terminalfenster starten Sie Programme, die Ihnen bei der Analyse oder Reparatur eines Linux-Systems helfen können. Mit an Bord sind der Browser Firefox, der FTP-Client Filezilla, ein Bildbetrachter und ein PDF-Viewer. Über „System → Hardware Listener" oder im Terminal mit *lshw* ermitteln Sie, welche Hardware im PC steckt. Mit Testdisk stellen Sie im Terminal versehentlich gelöschte Partitionen wieder her, mit Photorec gelöschte Dateien. Clonezilla erstellt Imagebackups von Partitionen und Festplatten und schreibt diese bei Bedarf auch wieder zurück. Mit Gparted partitionieren Sie Festplatten oder ändern Partitionsgrößen ohne Datenverlust. Weitere Informationen zu Clonezilla und Gparted finden Sie in diesem Heft ab Seite 52. ■



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

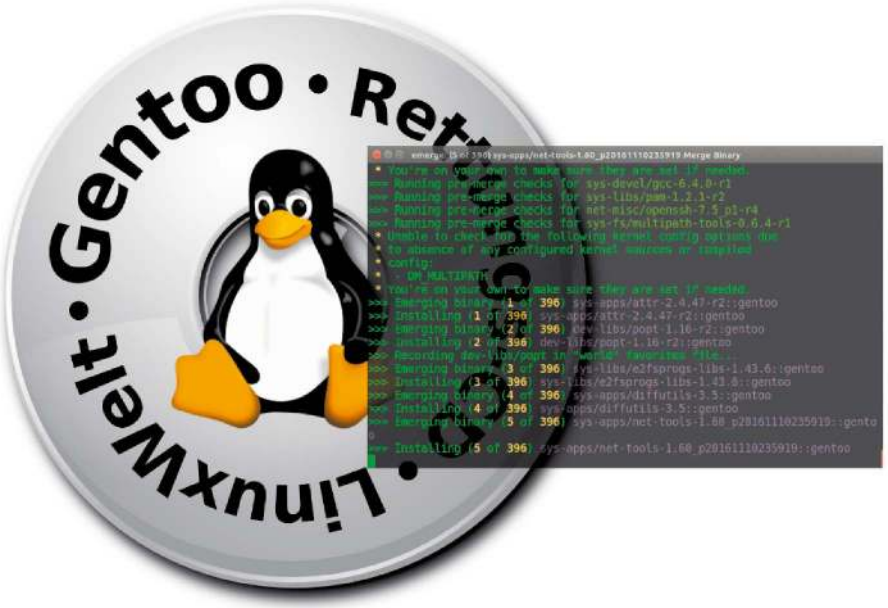


Laufwerke einbinden: Über „System → Show Filesystems" lassen Sie sich die Partitionen anzeigen, die Sie dann mit dem mount-Befehl in das Dateisystem einhängen.

Das eigene Livesystem

Erfahrene Linux-Bastler können sich ein Reparatursystem wie die LinuxWelt-Rettungs-DVD (siehe Artikel Seite 68) auch selbst zusammenstellen. Fügen Sie zusätzliche Tools hinzu, die Sie benötigen, oder entfernen Sie unnötige Programme.

VON THORSTEN EGGELING



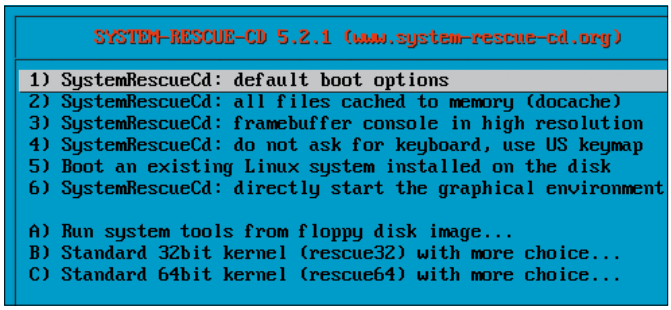
In den meisten Livesystemen lassen sich neue Softwarepakete während der Laufzeit installieren, obwohl die DVD schreibgeschützt ist. Ein spezielles Overlay-Dateisystem im RAM macht das möglich. Sie können daher Reparaturtools oder Analysesoftware nachinstallieren und auf das installierte System auf der Festplatte anwenden. Allerdings überdauern solche Installationen keinen Neustart. Wer bestimmte Tools ständig benötigt, kann sich für mehr Komfort ein individuelles Livesystem zusammenstellen. Neben dem reinen Nutzwert eines selbst angepassten Livesystems kommt das Verfahren für Sie infrage, wenn Sie sich mit Linux gut auskennen, sich noch intensiver mit der Technik dahinter beschäftigen möchten und den Zeitaufwand nicht scheuen.

1. Grundlagen für ein Livesystem

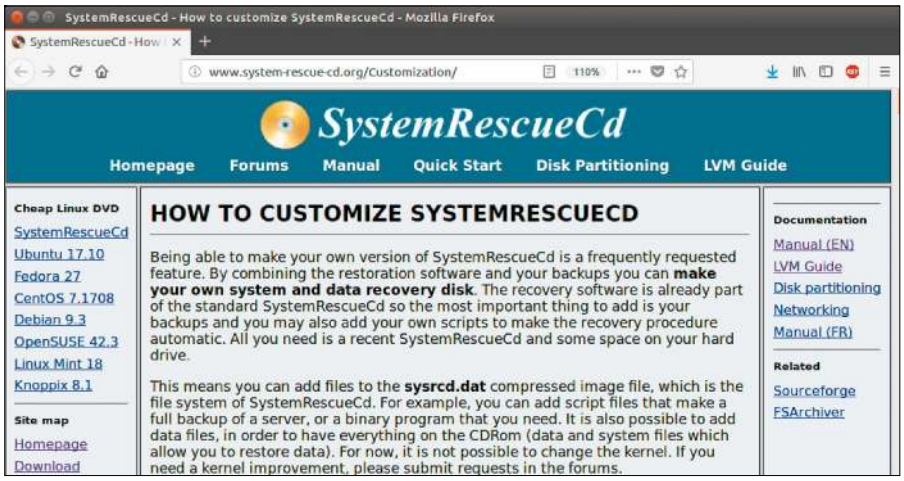
Für ein Livesystem verwenden Sie entweder die Binärpakete einer Linux-Distribution oder Sie setzen das System aus dem Quellcode zusammen, den Sie selbst kompilieren. Die fertigen Binärpakete ermöglichen es, das System schneller zu erstellen (siehe beispielsweise *www.pcwelt.de/2170193*). Allerdings gibt es bei jeder Distribution Besonderheiten, die Sie beachten müssen. Die Softwareauswahl ist beschränkt und Sie sind auf die vorgegebenen Programmversionen festgelegt. Der Umgang mit dem Quellcode ist letztlich flexibler und anpassungsfähiger. Der Nachteil: Die meisten Programme benötigen zusätzliche Headerdateien und Programmbibliotheken, damit sie sich kompilieren lassen. Das verlangsamt den Prozess erheblich, weil Sie auch die Buildabhängigkeiten erst erstellen müssen. Damit ein Livesystem möglichst schlank bleibt, müssen danach die Buildabhängigkeiten wieder entfernt werden. Es ist jedoch wichtig, nicht versehentlich auch Laufzeitabhängigkeiten zu löschen. Denn dann starten Programme nicht mehr, die diese benötigen.

2. Die Basis des LinuxWelt-Rettungssystems

Das LinuxWelt-Rettungssystem basiert auf Gentoo-Linux (*www.gentoo.org*) und verwendet die Anpassungen der System Rescue CD (*www.system-rescue-cd.org*). Gentoo ist eine Distribution, die standardmäßig nur ein schlankes Basissystem anbietet. Die meisten Programme werden als Quellpaket heruntergeladen und auf dem Rechner des Anwenders kompiliert. Ein Setuptool für die geführte Installation, wie Sie es von Ubuntu oder Fedora kennen, gibt es hier nicht.
Sie müssen alle nötigen Schritte, etwa die Partitionierung der Festplatte oder die Einrichtung des Netzwerks, manuell durchführen.Gentoo bietet Tools, die es für Livesysteme besonders attraktiv machen. Grundsätzlich können Sie eine fertige Live-CD wie System Rescue CD verwenden und anpassen. Wie das geht, ist unter *www.system-rescue-cd.org/Customization* beschrieben. Kleine Kommandozeilentools, die keine umfangreichen Buildabhängigkeiten besitzen, lassen sich schnell einbauen.
Programme für die grafische Oberfläche benötigen jedoch zahlreiche Bibliotheken und Headerdateien, etwa X11, GTK oder Qt. Auch diese Pakete haben Buildabhängigkeiten, die wiederum eigene Abhängigkeiten besitzen. Gentoo hat zwar Tools an Bord, die diese Abhängigkeiten automatisch auflösen sollen, das funktioniert jedoch nicht immer reibungslos. Oft ergeben sich zyklische Abhängigkeiten, die sich nicht ohne Weiteres auflösen lassen.
Es ist daher zuverlässiger, mit einem frischen Gentoo bei null zu beginnen. Die meisten Tools müssen ohnehin neu kompiliert werden, wenn das System sich in deutscher beziehungsweise einer anderen Sprache als Englisch melden soll. Dabei lassen sich auch aktualisierte Programmversionen problemlos installieren.



System Rescue CD: Das schlanke englischsprachige Livesystem auf Gentoo-Basis bietet viele Tools für die Wartung und Reparatur von Linux- und Windows-Systemen.



Livesystem anpassen: Auf der Webseite der System Rescue CD gibt es eine Anleitung, die aber nur zur Integration einfacher Tools ohne umfangreiche Abhängigkeiten hilft.

3. Das Gentoo-Buildsystem

Gentoo-Nutzer starten in der Regel mit einem Stage-3-Archiv (stage3-Tarball), das die erforderlichen Dateien für ein Basissystem enthält. Der Einrichtungsprozess ist ausführlich im Gentoo-Handbuch beschrieben (*https://wiki.gentoo.org*). Von einem Livesystem oder einem bereits installierten Betriebssystem aus lassen sich die gewünschten Programme in einer Chroot-Umgebung einrichten. Dann kommen noch der Bootmanager und ein Kernel hinzu und das neue System ist fertig.

Ursprünglich begann die Installation bei Gentoo mit einem minimalen Stage-1-Archiv, aus dem heraus die Stage 2 mit den gewünschten Werkzeugen (minimaler Toolchain: C-Compiler, C++-Compiler, Linker, Assembler) erzeugt wurden. In Stage 3 sind dann alle Tools aus Stage 2 enthalten plus die gewünschten Anwendungen.

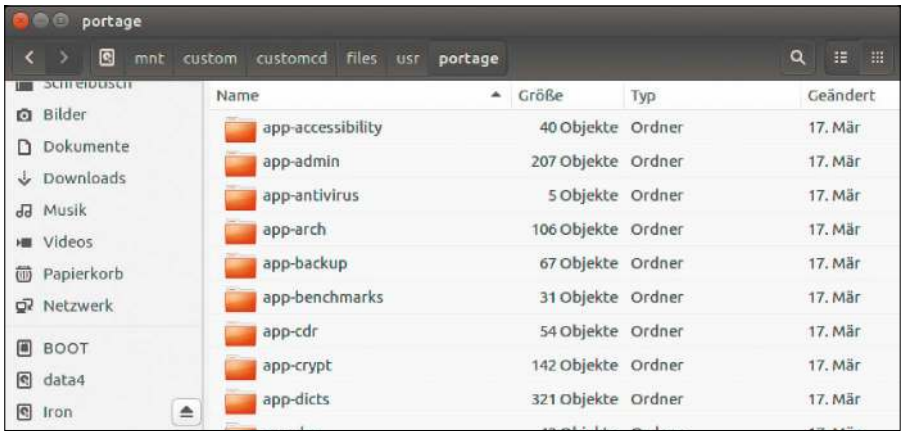
Software einrichten: Die Installation von Software erfolgt über das Tool emerge, das seine Informationen aus dem Portage-Tree bezieht. Der Portage-Tree ist ein Verzeichnisbaum, das Ordner wie „kde-apps“ oder „www-client“ enthält. Darin liegen Scripts, die Downloadadressen für den Quellcode, Versionsnummern, Patches und Compileranweisungen. Meist gibt es mehrere Scripts mit unterschiedlichen Versionsnummern für ein Programm. Standardmäßig installiert Gentoo nur als stabil bekannte Programme oder Langzeitversionen. Bei Bedarf können Sie aber auch neuere Versionen installieren. In vielen Fällen sind dafür aber auch neuere Versionen einiger gemeinsam genutzter Programmbibliotheken erforderlich. Im optimalen Fall sorgt emerge automatisch für die Installation der Abhängigkeiten, ohne dass Nebenwirkungen für andere Programme zu befürchten sind. Fehler sind jedoch nicht ausgeschlossen. Denn wahrscheinlich niemand hat jede Kombination von alten und neuen Programmen ausprobiert.

Der Portage-Tree wird täglich aktualisiert und steht unter *http://distfiles.gentoo.org/snapshots* zum Download bereit. Das gleiche gilt auch für die Stage-Dateien, den die Gentoo-Server auf Basis der jeweils aktuellen Portage-Datei jeden Tag neu erstellen (*http://distfiles.gentoo.org/releases/amd64/autobuilds* und *http://distfiles.gentoo.org/releases/x86/autobuilds*). Von Gentoo gibt es daher auch keine Distribution mit einer

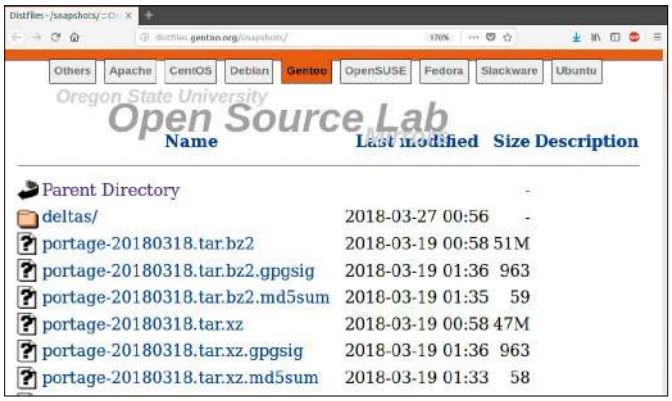
PORTAGE-OVERLAYS UND KERNEL

Gentoos Portage-Tree bietet alle offiziellen Programme für ein Gentoo-System. Wem das nicht genügt, der kann zusätzliche Portage-Overlays verwenden. Eine Übersicht bietet beispielsweise h*ttps://gpo.zugaina.org/Overlays*. Darüber ist es möglich, aktuellere Versionen zu installieren oder Programme einzurichten, die in den offiziellen Quellen nicht zu finden sind. Die Overlay-Dateien lassen sich einfach über den Ordner „etc/portage/repos.conf“ einbinden. Emerge berücksichtigt conf-Dateien, die darin liegen und Definitionen wie „location=/usr/local/portage-overlay“ enthalten.

Auch System Rescue CD verwendet ein Portage-Overlay („/mnt/custom/customcd/files/worksrc/sysresccd-src/portage-overlay“). Darin sind einige Scripts enthalten, die für die Live-CD erforderlich sind, sowie zusätzliche Programme. Wichtig ist hier vor allem der Kernel unter „/usr/local/portage-overlay/sys-kernel/std-sources/std-sources-4.14.ebuild“. Die ebuild-Konfiguration versorgt den Kernel (4.14.20) mit einigen Patches, die der korrekten Funktion des Livesystems dienen. Der Kernel ist relativ aktuell, die Langzeitversion von *www.kernel.org* trägt Ende März 2018 die Versionsnummer 4.14.30. Aufgrund der speziellen Patches ist es nicht leicht möglich, einen neueren Kernel zu verwenden. Wer nicht gerade ausgewiesener Kernel-Spezialist ist, sollte ab und zu bei *https://sourceforge.net/projects/system-rescuecd/* nachsehen. Klicken Sie auf „Code“, um zum Git-Repositorium zu gelangen. Sie finden hier alle Dateien, die wir für das LinuxWelt-Rettungssystem verwendet haben. Sollte ein neuer Kernel verfügbar sein, finden Sie das Update unter „portage-overlay/sys-kernel/std-sources“.



Software für Gentoo: Der Portage-Tree besteht aus Ordnern, die emerge-Scripts für den Download der Quelltextpakete, Patches und Compileranweisungen enthalten.



Aktuelle Software: Auf *http://distfiles.gentoo.org/snapshots* gibt es täglich einen neuen Portage-Snapshot, der neuere Programmversionen oder zusätzliche Software enthalten kann.

bestimmten Versionsnummer. Es handelt sich um ein „Rolling Release", das fortlaufend aktualisiert wird. Neben neuen Versionen berücksichtigt Gentoo in den Portage-Snapshots auch geänderte Downloadadressen, denn nicht jede Datei stammt von den Gentoo-Server. Damit direkte Downloads von den Servern der Entwickler kein Sicherheitsrisiko darstellen, sind für alle Dateien im Portage-Tree Prüfsummen hinterlegt. Bei Abweichungen wird die Installation verweigert. Alle Downloads landen im Ordner „/usr/portage/distfiles" und müssen daher bei einer erneuten Installation der gleichen Softwareversion nicht noch einmal heruntergeladen werden.

4. Gentoo-Entwicklungsumgebung einrichten

Catalyst (*https://wiki.gentoo.org/wiki/Catalyst*) ist ein Gentoo-Tool, mit dem sich Stage-Archive sowie Live-CDs erzeugen lassen. Das Tool funktioniert nur unter Gentoo-Linux. Sie müssen dafür aber Gentoo nicht auf der Festplatte installieren, eine Chroot-Umgebung genügt. Als Betriebssystem empfehlen wir Ubuntu 16.04 oder 18.04 mit 64 Bit. Debian oder Linux Mint eignen sich ebenfalls. Ein schneller PC (Intel Core i5, i7 oder AMD Ryzen) mit 16 GB RAM und etwa 50 GB freiem Platz auf der Festplatte ist empfehlenswert. Bei schlechter ausgestatteten Computern dauert der Build-Vorgang länger. Insgesamt müssen Sie für den ersten Durchlauf etwa 12 Stunden einplanen. Dank Compilercache benötigen weitere Durchläufe, etwa nach Änderungen bei der Softwareauswahl oder der Konfiguration, meist weniger als eine Stunde.

Schritt 1: Laden Sie über *www.pcwelt.de/LWRescue* die Datei „LiveCD.tar.bz2" herunter. Im Archiv sind auch alle Befehlszeilen aus diesem Artikel enthalten („Befehlszeilen.txt"). Öffnen Sie ein Terminalfenster, verschaffen Sie sich root-Rechte und entpacken Sie die Datei:

```
sudo -i
tar xvf ~/Downloads/LiveCD.tar.bz2
  -C /
```

Die entpackten Dateien liegen danach unter „/mnt/custom". Lassen Sie das Terminalfenster für die weiteren Schritte geöffnet.

Schritt 2: Wechseln Sie in den Ordner „/mnt/custom" und starten Sie das Download-Script:

```
cd /mnt/custom
./get_gentoo_files.sh
```

Das Script lädt die Stage-3-Dateien für ein 32-Bit- und ein 64-Bit-System sowie den Portage-Snapshot herunter, den wir für die LinuxWelt-Rettungs-DVD verwendet haben. Mit dabei sind außerdem einige Dateien, die inzwischen nicht mehr zum Download verfügbar sind.

Schritt 3: Verwenden Sie die Datei „stage3-amd64-baseos.tar.bz2" für das Build-System. Entpacken Sie die Datei mit

```
tar xvpf stage3-amd64-baseos.tar.
  bz2 --xattrs-include='*.*'
  --numeric-owner -C /mnt/custom/
  customcd/files
```

Im Zielordner liegt jetzt das Gentoo-Basissystem.

Schritt 4: Starten Sie das Script im Ordner „/mnt/custom" in einem root-Terminalfenster folgendermaßen:

```
./mnt_chroot.sh
```

Das Script bindet Ordner wie „/dev" und „/sys" des installierten Linux-Systems in „/mnt/custom/customcd/files" ein und wechselt per chroot in das Gentoo-System. Installieren Sie mit

```
emerge =dev-util/catalyst-2.0.17
  libisoburn cpio grub
```

das Tool catalyst (Version mit Patches für die System Rescue CD) und die Tools, die für ISO-Dateien (xorriso), die initiale Ramdisk (initram.igz) und den Bootmanager (grub) erforderlich sind.

Schritt 5: Wechseln Sie mit *cd* in das Verzeichnis „/worksrc/sysresccd-src/main-files". Hier liegen Konfigurationsdateien und Scripts zur Steuerung von Catalyst. Führen Sie diese in der Reihenfolge der Nummerierung aus. Beginnen Sie mit

```
catalyst -c catalyst.conf -f 01_
  sysresccd-base-stage4-i686.spec
catalyst -c catalyst.conf -f 02_
  sysresccd-base-stage4-amd64.spec
```

Damit erstellen Sie die Stage-4-Dateien, die als Ausgangspunkt für die weiteren Schritte dienen. Nach dem gleichen Muster wenden Sie auch die spec-Dateien 03 bis 05 an. Danach verfügen Sie über die Stage-4- und Stage-1-Dateien für ein 32- und 64-Bit-System. Catalyst erzeugt die Systeme automatisch innerhalb einer chroot-Umgebung und verwendet dabei die Angaben in den spec-Dateien.

Schritt 6: Starten Sie

```
./06_rebuild-kernel.sh rescue32
```

und danach das zweite Shell-Script:

```
./06_rebuild-kernel.sh rescue64
```

Das Script gibt am Ende den Fehler „catalyst: target_image_setup script failed“ aus. Der ist jedoch unbedenklich. Im Ordner „/worksrc/sysresccd-bin/kernels-x86“ liegen nun der 32- und der 64-Bit-Kernel für das Livesystem.

Schritt 7: Führen Sie diese Befehlszeile aus:

```
catalyst -c catalyst.conf -f 07_
  sysresccd-live-stage2-full.spec
```

Das Resultat ist das endgültige Dateisystem für die 32-Bit-Live-CD mit einem 32- und 64-Bit-Kernel. In diesem Schritt deinstalliert Catalyst auch überflüssige Entwicklungstools, löscht unnötige Dateien und erstellt die ISO-Datei im Ordner „/worksrc/isofiles“.

Schritt 8: In der ISO-Datei fehlen noch einige wichtige Dateien, die das Livesystem ausmachen. Diese befinden sich in den „overlay*“-Ordern in „sysresccd-bin“ und „sysresccd-src“. Darin enthalten sind beispielsweise das Bootmenü und einige Scripts für die initiale Ramdisk. Der Befehl

```
./08_recreate-iso.sh x86
```

kopiert den Inhalt der in Schritt 7 erstellten ISO-Datei, baut die erforderlichen Dateien ein und erstellt ein neues ISO mit der Bezeichnung „lwrescuecd-x86-6.2.1-full-[Datum]- [Uhrzeit].iso“ im Ordner „isofiles“. Mit *exit* verlassen Sie nun die chroot-Umgebung. Geben Sie abschließend den Befehl

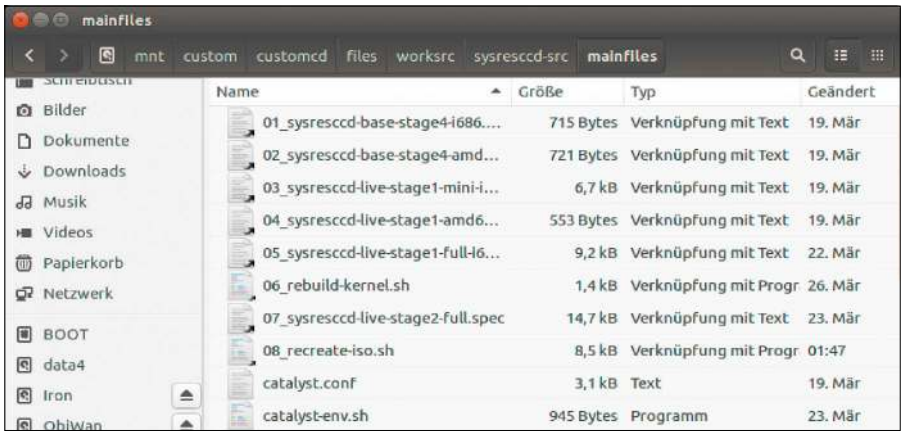
```
./umount_chroot.sh
```

ein, um die Einbindungen in das Dateisystem wieder zu lösen.

Testen Sie die ISO-Datei zuerst beispielsweise in Virtualbox. Danach brennen Sie aus der ISO-Datei eine DVD oder erstellen einen bootfähigen USB-Stick.

5. Anpassung des Livesystems

Wenn Sie Programme hinzufügen oder entfernen wollen, öffnen Sie die Datei „sysresccd-live-stage1-full-i696.spec“ in einem Editor. Löschen Sie dort Zeilen unter „livecd/packages:“ oder fügen Sie neue hinzu. Unter Umständen sind auch Anpassungen unter „livecd/use:“ erforderlich. In der Liste sind die Abhängigkeiten vermerkt und – mit einem vorangestellten „-“ Zeichen – solche, die nicht berücksichtigt werden sollen. Catalyst weist Sie darauf hin, wenn hier Änderungen nötig sind. Anschließend erstellen Sie Stage 1 und Stage 2 neu:



Gentoo-Build: Im Ordner „mainfiles“ liegen alle Steuerdateien und Scripts für das Livesystem. Führen Sie die Befehle in der Reihenfolge der Nummerierung aus.

Catalyst-Definitionen: Die Stage-2-spec-Datei erzeugt das Dateisystem für die Live-CD und entfernt unnötige Dateien. Was noch fehlt, baut „08_recreate-iso.sh“ in das ISO ein.

```
catalyst -c catalyst.conf -f 05_
  sysresccd-live-stage1-full-i686.
  spec
catalyst -c catalyst.conf -f 07_
  sysresccd-live-stage2-full.spec
```

Sehen Sie sich außerdem die Dateien in den Ordnern „sysresccd-bin/overlay-iso-x86“ und „sysresccd-src/overlay-iso-x86“ an, wenn Sie das Bootmenü ändern oder weitere Dateien zum ISO hinzufügen wollen. Führen Sie abschließend „./08_recreate-iso.sh“ aus, um eine neue ISO-Datei zu erstellen.

Updates für das Livesystem: Einige Zeit nach Erscheinen dieser LinuxWelt sollten Sie die von uns vorbereiteten Dateien (siehe Punkt 4, Schritt 2) nicht mehr verwenden. Aktuelle Versionen der Stage-3-Dateien und des Portage-Snapshots laden Sie über *http://distfiles.gentoo.org* herunter. Nur so ist sichergestellt, dass Sie fehlerbereinigte und neue Programmversionen erhalten. Die Stage-Archive gibt es bei Gentoo nur im xz-Format, Catalyst verlangt jedoch bz2-Dateien. Mit dieser Befehlszeile lässt sich eine Datei konvertieren:

```
xzcat stage3-i686-[Datum].tar.xz |
  bzip2 -c > stage3-i686-baseos.tar.
  bz2
```

Die Stage-Dateien kopieren Sie in den Ordner „worksrc/catalyst/builds/default“ und die Portage-Datei nach „worksrc/catalyst/snapshots“. Die Versionsnummer ist auch in den spec-Dateien hinterlegt.

Mit dem Script „setsnapshot.sh“ im Ordner „worksrc/sysresccd-src/mainfiles“ ändern Sie die Versionsnummer auf den vorherigen Tag. Ist der Snapshot älter, passen Sie im Script den Wert wie folgt an („2 days ago“, „3 days ago“):

```
date='1 days ago'
```

Danach erstellen Sie das System, indem Sie alle in Punkt 4 beschriebenen Schritte durchführen. ■

Tipps für Fotografen

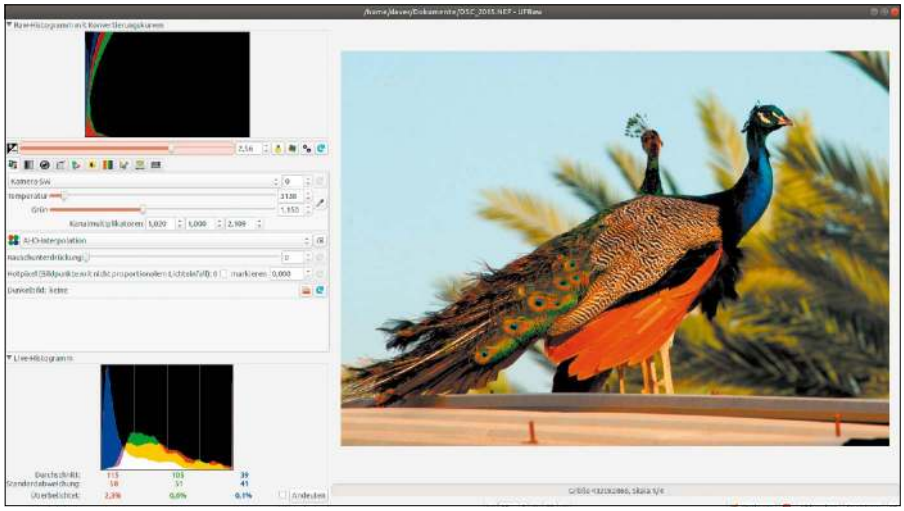
Nach jahrelanger Aufholjagd bietet Linux inzwischen eine stattliche Anzahl großer und kleiner Tools rund um Digitalfotografie und Retusche. Es sind gerade die speziellen Aufgaben, für die es vorzeigbare Open-Source-Werkzeuge gibt.

VON DAVID WOLSKI

Zum Thema Bildbearbeitung und Retusche präsentierte sich Linux bisher nicht als Vorzeigeplattform, zumal Photoshop als Maß aller Dinge weiterhin nur auf Mac-OS und Windows läuft und Adobe keine Anstalten macht, eine Linux-Version zu erstellen. Genauso lassen Kamerahersteller Linux links liegen und bieten keine Konvertierungsprogramme für modellspezifische Rohdatenbilder. Diese Formate sind meist undokumentiert und patentrechtlich geschützt. Das quelloffene DNG-Format wird von wenigen Kameramodellen unterstützt.

Aus der Not wurde Tugend: Wegen mangelnder Unterstützung von Linux durch Kamerahersteller begann der Programmierer Dave Coffin vor 20 Jahren mit der Entwicklung von Dcraw, einer freien Programmbibliothek für Rohdatenbilder, die heute Hunderte von Formaten kennt. Viele davon sind mühsam durch Reverse Engineering entschlüsselt. Mittlerweile ist Dcraw als universelle Bibliothek so ausgereift, dass sie von zahlreichen anderen Programmen genutzt wird, auch unter Windows und Mac-OS. Womit Linux ebenfalls glänzen kann, sind ergänzende Tools und clevere Programme zur Bildnachbearbeitung.

Darktable: Der RAW-Konverter ist ideal für den Workflow umfangreicher Fotoserien. Änderungen speichert Darktable in externen XMP-Dateien und lässt die Bilder zunächst unberührt.



Ufraw: Dies war eines der ersten Linux-Programme zum Decodieren und Konvertieren von RAW-Fotos. Für Einzelbilder und für einen sanften Einstieg ist das Tool immer noch gut geeignet.

RAW-Entwicklung: Format für Anspruchsvolle

Lichtquellen haben unterschiedliche Farbtemperaturen und ein sorgfältiger Weißabgleich anhand der Kameraeinstellungen ist für natürlich wirkende Farben unentbehrlich. Unter besonderen Lichtverhältnissen wie warmem Abendlicht und bei einem Mix inhomogener Lichtquellen bleibt der automatische Weißabgleich meist auf der Strecke. Es empfiehlt sich bei guten Motiven deshalb stets die (zusätzliche) Aufnahme im RAW-Format. Dieses unkomprimierte Format, das Systemkameras, DSLRs und bessere Kompaktkameras optional speichern, nimmt für jeden Pixel die Daten des Bildsensors unverändert auf.

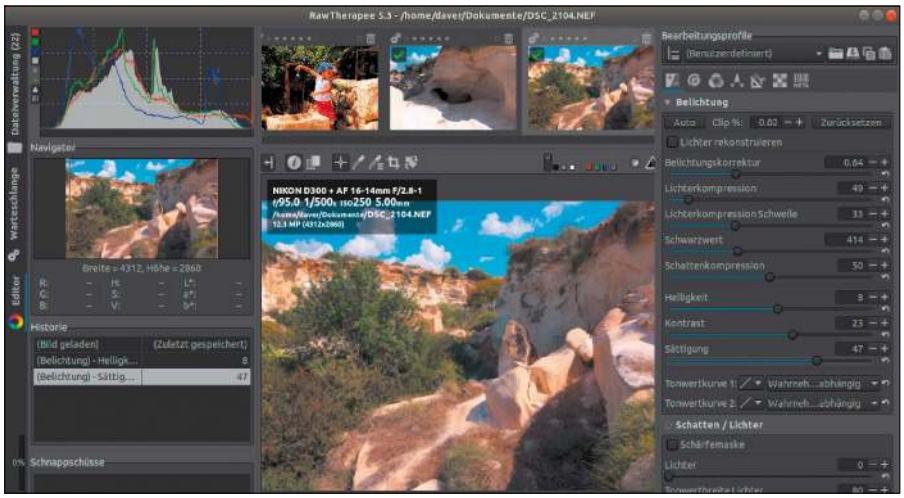
Zur Ausgabe eines fertigen Bilds zur Weitergabe oder Weiterverarbeitung ist ein Konvertierungsprogramm nötig, das die zahllosen Optimierungsmöglichkeiten ausschöpft, die auch nach dem Auslösen zur Bildoptimierung zur Verfügung stehen. Dazu gehören Belichtung und Nachbelichtung, Entrauschen, Weißabgleich, Farbsättigung, Kontrast und Histogramm. Die Aus-

wahl solcher RAW-Entwickler unter Linux kann sich inzwischen sehen lassen.

Darktable: Darktable hat sich als Open-Source-Alternative zu Adobe Lightroom einen Namen gemacht. Das Programm bildet den kompletten Workflow von der Auswahl der RAW-Bilder bis zum druckreifen Abzug ab. Frische Pakete für nahezu alle Linux-Systeme finden sich unter *www.darktable.org/install*. Unter den RAW-Entwicklern ist Darktable das anspruchsvollste Linux-Programm und erfordert Einarbeitungszeit. Für die nicht-destruktive Bildbearbeitung kann Darktable die Änderungen zu Bildern in XMP-Dateien schreiben.

Ufraw: Deutlich weniger Einarbeitung setzt das einfach gehaltene Tool Ufraw voraus, das Einzelbilder im RWA-Format in Form bringt. Die gesetzten Parameter kann Ufraw in den Standardeinstellungen speichern und erlaubt damit auch die Organisation eines sehr einfachen Workflows. Ufraw liegt mit gleichnamigem Paketnamen in den Standardquellen aller großen Linux-Distributionen vor.

Rawtherapee: Der RAW-Konverter ging als kommerzielles Programm an den Start, ist seit seiner Version 3 aber Open-Source-Software (GPL). Der Funktionsumfang ist mit jenem von Darktable vergleichbar, allerdings macht Rawtherapee Einsteigern die ersten Schritte bei der RAW-Bearbeitung ein Stück einfacher. Auch Rawtherapee ist mit gleichnamigem Paketnamen in den Standard-Paketquellen der verbreiteten Linux-Distributionen vertreten.



Rawtherapee: Nicht ganz so anspruchsvoll wie Darktable ist dieser RAW-Entwickler. Die Bearbeitungsschritte kann Rawtherapee in seiner Undo-Funktion speichern.

Gimp: Intelligentes Verkleinern

Es ist immer eine verlustreiche Angelegenheit, ein Bild zu verkleinern: Entweder man skaliert das ganze Bild auf eine geringere Größe, was insgesamt die Auflösung verringert oder das Motiv verzerrt. Die andere Prozedur ist das Zuschneiden des Motivs, wobei aber ganze Bildbereiche verlorengehen. Für viele Bilder eignet sich aber weder die eine noch die andere Methode.

Ein anderer Weg der Verkleinerung ohne deutlichen Informationsverlust ist der Algorithmus „Liquid Rescaling“. Es handelt sich um eine Mischung aus Skalieren und Zuschneiden, wobei der Algorithmus ein Motiv zuvor analysiert, um optisch wichtige Elemente unverändert zu behalten. Unbetonte Zwischenräume zwischen markanten Bildteilen lassen sich verkleinern und ein Motiv rückt zusammen.

So wird das Plug-in installiert: Liquid Rescaling liegt als Plug-in für die Bildbearbeitung Gimp ab Version 2.8 vor. In Debian und Ubuntu hat es der Algorithmus bereits in die Plug-in-Sammlung gimp-plugin-registry geschafft und ist zusammen mit anderen Gimp-Erweiterungen über

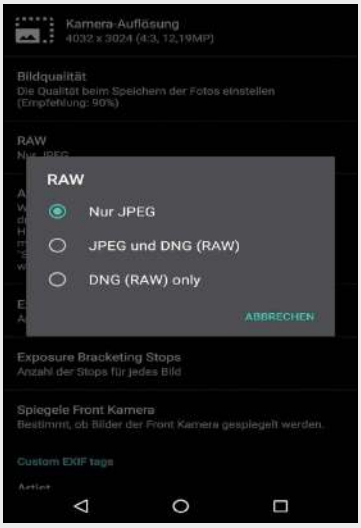
```
sudo apt-get install gimp-plugin-registry
```

installiert. Um das Plug-in einzusetzen, laden Sie das gewünschte Bild in Gimp und gehen in der Menüleiste des Bilderrahmens auf „Ebenen → Liquid Rescale“. Der Menüpunkt öffnet einen neuen Dialog zum Plug-in. Im automatischen Modus erledigt der Algorithmus viel selbst und es genügt, in den Feldern „Width“ und „Height“ die neuen Dimensionen einzugeben. Je nach Motiv erkennt das Plug-in Nahtstellen zwischen den wichtigen Bildteilen.

Optimal arbeitet die Skalierung aber erst, wenn Bereiche mittels Ebenen manuell

ANDROID: RAW-BILDER VON SMARTPHONES

Die populärsten Kameras sind inzwischen Smartphones, zumal heute fast jeder immer eines dabei hat. Aber die Bildqualität auch guter Smartphone-Kameras kann natürlich nicht mit der einer digitalen Spiegelreflexkamera mithalten. Zudem komprimieren Smartphones die Aufnahmen sehr stark, da der interne Speicher meistens nicht genug Platz für viele unkomprimierte Aufnahmen bietet. Wer die optimale Aufnahmequalität von einem Android-Smartphone erwartet und etliche Gigabyte Platz hat, etwa auf einer externen Micro-SD-Karte, bekommt mit der App Open Camera ein alternatives Aufnahmeprogramm, das in seinen Einstellungen die Option anbietet, Fotos im DNG-Format zu speichern. Dazu muss in der App die „Camera2-API“ aktiviert werden, was einen Neustart des Smartphones erforderlich macht. Open Camera ist Open Source und im Quellcode sowie im App Store von Google Play verfügbar (*https://opencamera.sourceforge.io*).



Android-App für Fotografen: Open Camera ist eine Open-Source-App für neuere Android-Geräte. In den Einstellungen gibt es die Option, unkomprimierte RAW-Bilder zu speichern.

Liquid Rescale: Der Algorithmus zum Verkleinern von Bildern skaliert auf Wunsch nur unwichtige Bildbereiche. Dazu bietet das Gimp-Plug-in Ebenenmasken zum Markieren der Bereiche.

Bildteile herausrechnen: Der Dialog des Plug-ins legt fest, in welchem Umfang der Resynthesizer umliegende Pixel analysieren soll, um eine Hintergrundtextur für die Auswahl zu berechnen.

markiert wurden. Dazu gehen Sie im Dialog des Plug-ins auf „Elementmasken → Elemente erhalten → New“ und markieren alle wichtigen Bildteile auf dieser neuen Ebene dem Pinselwerkzeug. Danach klicken Sie auf „OK“, um die Skalierung auf die angegebene Breite und Höhe zu starten. Analog dazu lässt sich auch eine Maske erstellen, deren markierte Bereiche bei der Skalierung verschwinden sollen. Dazu dient die Funktion „Feature discard selection“. Wer mit großen Bilddateien experimentiert, sollte Geduld mitbringen, da der Algorithmus ordentlich Rechenpower braucht.

Gimp: Bildelemente überzeichnen

Es ist kein Problem, Objekte zu bestehenden Bildern so hinzuzufügen, dass hinterher alles weiterhin realistisch aussieht. Aber der umgekehrte Weg erweist sich als mühsam: Wie lässt sich etwas ausschneiden und wegzaubern, ohne das Bild zu zerstören? Dazu muss das unerwünschte Objekt mit dem Bildhintergrund übermalt werden, was meist nur erfahrenen Grafikern gut gelingt.

Es ist aber nicht völlig unmöglich, störende Bildelemente automatisch zu entfernen. Die Lösung heißt Texturs ynthese. Bei dieser Technik wird der umliegende Bildhintergrund eines markierten Bildbereichs analysiert und eine passende, realistische Textur aus diesen Anhaltspunkten erzeugt, Das Gimp-Plug-in Resynthesizer bringt manuell markierte Objekte eines Bildes zum Verschwinden, indem es den Hintergrund auf diese Weise nachbildet. Das Plug-in spart langwieriges Klonen einzelner Bildausschnitte und liefert zunächst passable Ergebnisse, die nach etwas Nachbearbeitung dann erstaunlich gut aussehen. Das Plug-in ist so populär, dass es in die Paketquellen von Ubuntu und Debian aufgenommen wurde und sich bei diesen Distributionen einfach über den Paketmanager installieren lässt:

```
sudo apt-get install gimp-
  resynthesizer
```

Und so arbeitet dieses Plug-in: Auf dem Bild markieren Sie den gewünschten Bereich mit der Freihand-Funktion (F-Taste) als Auswahl. Die Auswahl muss dabei nicht pixelgenau den Bereich umfassen, der verschwinden soll, sondern darf etwas größer sein. Anschließend geht es im Menü nach „Filter → Verbessern → Heal selection“. Im darauffolgenden Dialog kann man nun noch eingeben, in welchem Umfang der Resynthesizer die umliegenden Pixel analysieren soll, um eine Textur als Füllung für die Markierung zu berechnen. Der Standardwert ist hier 100 Pixel.

Falls das markierte Element vor einem sehr unruhigen, abwechslungsreichen Hintergrund steht, sollten Sie diesen Wert um die Hälfte reduzieren, um ein gutes Ergebnis zu erhalten. Wenn es sich um einen redundanten, gleichmäßigen Hintergrund handelt, dann darf der Bereich auch größer ausfallen. Falls das Ergebnis zunächst nicht gefällt, können Sie sowohl mit diesem Parameter als auch mit der Auswahl des Objekts experimentieren.

Der Resynthesizer braucht eine Menge Speicher und CPU-Zeit, was natürlich abhängig von der Bildauflösung ausfällt. Bei einem 12-Megapixel-Foto sollte ein GB RAM frei sein, andernfalls wird Gimp möglicherweise instabil. In den meisten Fällen ist das Ergebnis des Resynthesizers passabel, braucht im Detail aber eine Nachbearbeitung. Dazu eignet sich im Anschluss das Klontool (C-Taste), mit dem man mit der Tastenkombination Strg-T einen Bildbereich als Stempel markiert, der sich dann auf andere Bereiche anwenden lässt.

Hugin: Panoramafotos selbst gemacht

Panoramen sind besonders in der Landschaftsfotografie reizvoll, um dramatische Stimmungen einzufangen. Für Android-Smartphones gibt es die Fotoapp Photosphere von Google für Panoramafotos schon einige Jahre. Auch Kamerahersteller wie Canon haben Panoramaprogramme in die Firmware vieler Modelle integriert, um

die Bilder dann am PC mit einer Zubehörsoftware wie Canon Photostitch zusammenzufügen.

Unter Linux funktioniert das mit der Open-Source-Software Hugin. Das Programm kann Panoramen aus überlappenden Serien von Einzelbildern erstellen. Die Installation ist nicht weiter kompliziert, denn das Programm wartet mit gleichnamigem Paketnamen in den Paketquellen der populären Linux-Distributionen auf die Installation. Hugin ist ein Werkzeug für Fortgeschrittene und man darf längere Experimente nicht scheuen, bis alle Funktionen des Programms ergründet sind. Empfehlenswert ist es, erst mal mit kleinen Panoramen aus zwei Einzelbildern zu beginnen.

Wichtig: Für gute Ergebnisse sollte immer die Brennweite aus den Metadaten der Einzelaufnahmen eingetragen werden. Manuell hinzugefügte Kontrollpunkte zwischen überlappenden Bildern verbessern das Ergebnis ganz erheblich. Eine detaillierte deutschsprachige Anleitung zu Hugin findet sich unter *http://rofrisch.wordpress.com/2012/05/19/hugin-tutorial01*.

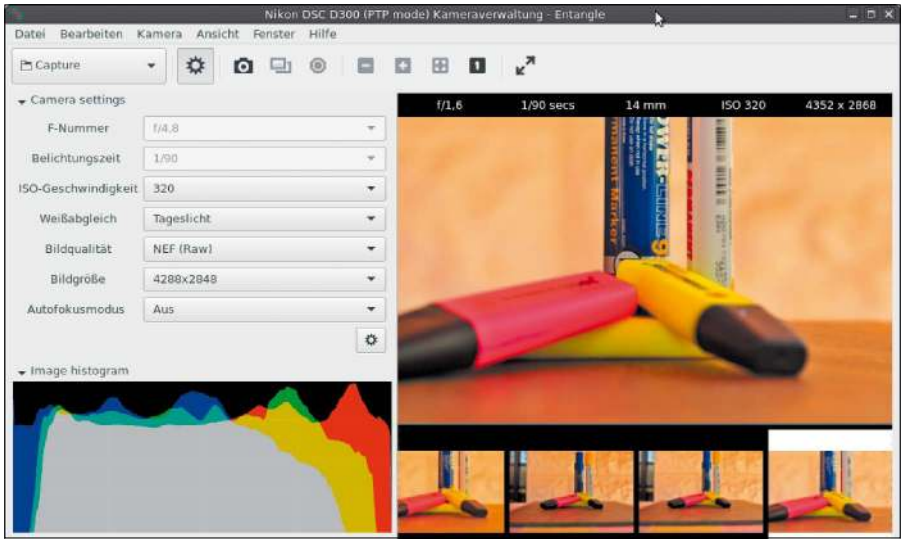
Panorama-Stiching mit Hugin: Das Open-Source-Programm ist anspruchsvoll in der Bedienung. Es liefert bei sorgfältiger Zusammenstellung der Einzelbilder hervorragende Ergebnisse.

Entangle: Kamera per USB steuern

Kabelgebundenes Fotografieren funktioniert mit den meisten digitalen Spiegelreflex- und Systemkameras und der per USB-Kabel verbundene PC dient dabei zur Steuerung der Aufnahmeeinstellungen. Nützlich ist dieser Aufbau für Studiofotografie und automatisierte Zeitrafferaufnahmen.

Das Open-Source-Programm Entangle bietet solches kabelgebundenes Fotografieren. Der verbundene PC zeigt eine Vorschau der Aufnahmen an und speichert die Bilder direkt, ohne Umweg über die Speicherkarte.

Entangle unterstützt Digitalkameras vieler Hersteller, die per USB angeschlossen werden. Es bietet eine Livevorschau, Fernauslöser und programmierbaren Timer, um Studioarbeiten auf den Linux-Desktop zu bringen. Entangle erfindet das Rad nicht neu, sondern baut auf der Bibliothek libgphoto2 auf, um mit Kameras zu kommunizieren. Damit das klappt, muss diese von der Bibliothek unterstützt werden. Eine Liste der Kameramodelle, vornehmlich von Nikon und Canon, findet sich auf der Projektwebseite unter *www.gphoto.org/doc/remote*. Ist das eigene Modell in der Auflistung vorhanden, dann richten



Kamera am Kabel: Entangle kann viele Kameras von Nikon und Canon über USB ansteuern. Das ist in der Studiofotografie und für Zeitrafferaufnahmen nützlich.

diese Schritte eine Verbindung von Kamera und Linux-System ein:

1. Die Installation von Entangle klappt bei den verbreiteten Distributionen Debian, Ubuntu, Fedora und Open Suse über den Paketmanager.

In Debian und Ubuntu beispielsweise mit diesem Terminalkommando:

```
sudo apt-get install entangle
```

Auch die anderen Linux-Distributionen kennen das Programmpaket unter dem Namen „entangle“.

2. Die meisten Kameras arbeiten zunächst bei einem Anschluss über USB an den PC im MSC-Modus (Mass Storage Class) und verhalten sich wie ein Massenspeicher. Im Kameramenü müssen die Geräte erst nach MTP (Media Transfer Protocol) beziehungsweise PTP (Picture Transfer Protocol) umgeschaltet werden, damit sie von Entangle erkannt werden.

3. Nach der Verbindung der Kamera mit dem PC und dem Start von Entangle gehen Sie im Menü auf „Kamera“ und „Connect“. Dort wählen Sie das erkannte Gerät aus und gehen auf „Verbinden“.

Im gleichen Menü gibt es noch eine optionale „Vorschau“, die allerdings nicht bei allen Kameras funktioniert. Für automatisierte Zeitrafferaufnahmen dient der Menüpunkt „Bearbeiten → Einstellungen → Plugins“ und dort die Erweiterung „Repeat Shooter“. Danach zeigt das Programmfenster links unter „Automation“ die Einstellungen für das Plug-in an, um Intervall und Bilderzahl vorzugeben. ■

Ordnung in der Fotosammlung

Es wird fotografiert wie nie zuvor: Dank immer besserer Smartphone-Kameras können wir jeden Moment festhalten. Aber man sollte hinterher auch wissen, wo die Bilder zu finden sind. Wir zeigen Ihnen, wie Sie Ordnung in Ihren Fotos schaffen.

VON STEPHAN LAMPRECHT

Vielleicht kennen Sie das auch: Die guten Vorsätze sind da – eigentlich will man nach der letzten Urlaubsreise die Fotos gleich von der Digitalkamera auf den Rechner kopieren und dabei auch in Ruhe durchsehen. Aber dann fehlt die Zeit, der interne Speicher droht knapp zu werden. Am Ende landen mit einem beherzten „Alles markieren“ und „Verschieben“ die Bilder doch wieder unbesehen auf der Festplatte. Und wenn sich einige Tausend Bilder angesammelt haben, wird es schwer, genau die Fotos zu finden, nach denen man gesucht hat. Ganz ohne Zeitinvestition bekommt man keine Ordnung in sein Chaos, aber mit dem richtigen Werkzeug bleibt der Aufwand moderat.

Organisieren mit sprechenden Dateinamen

Es sind gerade die Cloudanbieter wie Apple oder Google, die den Anwendern versprechen, dass es eigentlich gar nicht mehr nötig sei, Zeit mit dem Sortieren von Fotos zu verbringen. Oder gar mit so etwas Altmodischem wie Dateinamen zu hantieren. Damit die Fotos hübsch ansehnlich auf einer Landkarte positioniert werden oder auf einem Zeitstrahl erscheinen, werten die Dienste die in einem Bild versteckten Metainformationen aus. Das klappt natürlich nur dann, wenn die Informationen korrekt sind. Stimmen in der Kamera also weder Zeit und werden gar keine Informationen zum Standort ermittelt, funktioniert das automatische Sortieren natürlich nicht.

Fotoverwaltungsprogramme für das eigene System greifen auf die gleichen Metainformationen zu, haben also im Falle von falschen oder fehlenden Informationen das gleiche Problem. Ohne die dahinterstehende Datenbank bleiben die Erinnerungen einfach Bilddateien mit Namen wie „dsc1234.jpg“. Mal eben die externe Festplatte mit den Fotos mitnehmen und anderswo zeigen? Dann muss man auch die Verwaltungssoftware dabeihaben, um gezielt die gewünschten Aufnahmen zu präsentieren. Und im Falle eines Systemwechsels funktioniert möglicherweise der Fotoverwalter nicht mehr.

Werden die Fotos nach einem einheitlichen Schema benannt, lassen sich auch umfangreiche Bestände ordentlich organisieren – im Prinzip ganz ohne Bildverwaltung. Größere Mengen an Dateien rasch umzubenennen ist für Linuxsysteme kein Problem. Mit Batchprogrammierung lösen fortge-

schrittene Nutzer eine solche Aufgabe rasch und unkompliziert. Wer es lieber grafisch mag, nutzt am besten die Funktionen eines Dateimanagers. **Thunar**, der aus dem XFCE-Desktop stammt, besitzt eine übersichtliche Oberfläche für mächtigen Bearbeitungsfunktionen. Thunar funktioniert auch auf anderen Gnome-affinen Desktops sowie auch unter KDE. Um lediglich den Dateimanager ohne den vollständigen XFCE-Desktop zu installieren, verwenden Sie im Terminal diesen Befehl:

```
sudo apt install –no-install-
  recommends thunar
```

Möchten Sie das Programm nur zur Bearbeitung von Fotos nutzen, genügt dies schon. Falls Sie vorhaben, später auch Musikdateien auf die gleiche Weise zu bearbeiten, komplettieren Sie den Dateimanager mit den passenden Plug-ins:

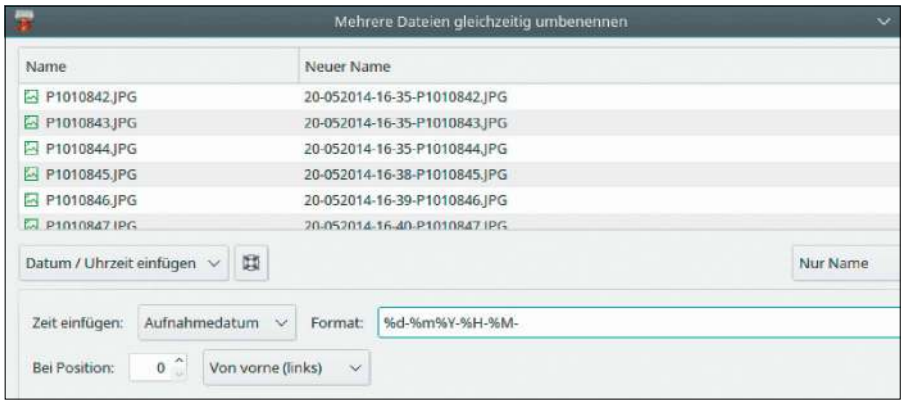
```
sudo apt install thunar-media-tags-
  plugin
```

Nach dem Start des Dateimanagers markieren Sie die Fotos mit der Maus und wählen das Menü „Bearbeiten → Umbenennen“. Im nachfolgenden Dialog markieren Sie aus dem Listenfeld den Eintrag „Datum / Uhrzeit einfügen“. Damit öffnen sich weitere Optionen am unteren Bildschirmrand. Markieren Sie „Aufnahmedatum“ aus der Liste unter „Zeit einfügen“. Um das Datum in der Reihenfolge Tag und Uhrzeit einzufügen, tragen Sie in das Feld „Format“ Folgendes ein:

```
%d-%m-%Y-%H-%M
```

Damit wird der bestehende Dateiname um die Zeitangabe „20-07-2017-15-34“ ergänzt. Die Parameter, die Sie hier nutzen können, leiten sich vom Terminalkommando „date“ ab. Wenn Sie also andere Angaben oder Formate wünschen, schauen Sie sich am besten die Manpage des date-Kommandos an.

Mit „Datei umbenennen“ starten Sie den Vorgang. Damit ist im Dateinamen schon einmal das Aufnahmedatum verewigt. Jetzt könnten Sie den alten Dateinamen entfernen. Da es aber nicht ausgeschlossen werden kann, dass Sie zum gleichen Zeitpunkt mehrere Fotos aufgenommen haben, fügen Sie am besten zunächst einen Zähler ein. Die Dateien sind in Thunar noch markiert. Rufen Sie also erneut das Werkzeug zum Umbenennen auf und nutzen Sie jetzt das Kommando „Nummerieren“. Wählen Sie ein Zahlenformat aus und ergänzen Sie über die kleine Maske am unteren Rand ein Trennzeichen. Das erleichtert den letzten Schritt. Diesmal entscheiden Sie sich für die Aktion „Zeichen entfernen“ und legen anschließend über die Position von links und rechts den Bereich fest, der gelöscht werden soll. Mittels der Option „Einfügen“ können Sie jetzt noch einen ergänzenden Ausdruck in den Namen aufnehmen, zum Beispiel „Urlaub“. Mit nur wenigen Arbeitsschritten erreichen Sie eine große Wirkung.



Thunar kann ganz einfach die Fotos nach dem Aufnahmedatum umbenennen. Das Namensformat legen Sie mittels vorgegebener Variablen fest.

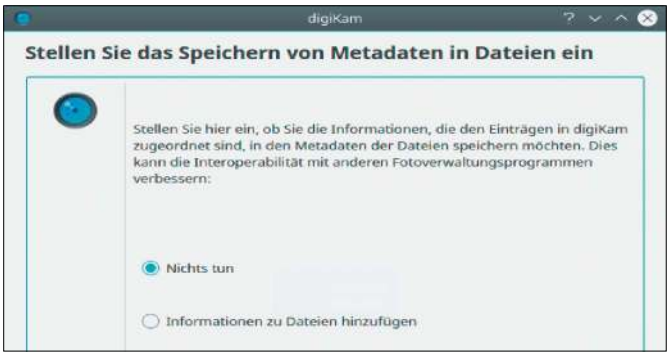
Thunar-Korrekturen: Mit weiteren Funktionen entfernen Sie später auch noch den alten Dateinamen und ergänzen Nummerierungen und Motivbeschreibungen.

Duplikate in der Bildersammlung

Jede größere Fotosammlung enthält Duplikate. Wenn Fotos vom Smartphone auf den Rechner kopiert werden, aber auf dem Handy verbleiben, hat man einige Wochen später das erste Kopieren vergessen und die Fotos gehen den Weg ein zweites Mal. Es gibt ein Programm für die Kommandozeile, das recht flott arbeitet und die Mehrzahl der Duplikate recht zuverlässig ermittelt. Die Chancen stehen gut, dass das Tool **findimagedupes** in den Paketquellen Ihrer Distribution zur Verfügung steht. Probieren Sie es einfach im Terminal mit

```
sudo apt install findimagedupes
```

aus. Kann das Paket nicht gefunden werden, besuchen Sie die Homepages des Projekts unter *https://github.com/opennota/findimagedupes*, um sich über die weiteren

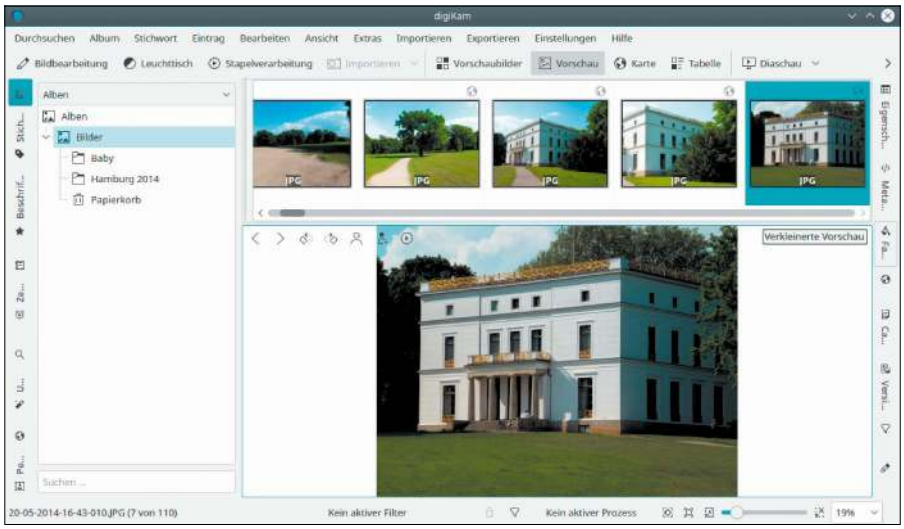


Der Digikam-Assistent führt durch die Einrichtung. Die Option, Metadaten direkt in die Dateien zu schreiben, macht die Metainformationen unabhängig von Speicherort und Programm.

Schritte für die Installation zu informieren. Die ist zwar nicht sonderlich schwer, nimmt dann aber etwas mehr Zeit in Anspruch.
Das installierte Tool starten Sie im Terminal mit *findimagedupes*. Die Steuerung erfolgt über einzelne Schalter. „R" („Recurse") definiert, dass auch Unterverzeichnisse durchsucht werden. Mit „t" und einem nachfolgenden Zahlenwert wird der Schwellenwert definiert, ab dem das Programm ein Bild als ähnlich interpretiert. Bei „0" sind dies exakt identische Bilder, und mit „63" stuft das Tool alle Bilder als ähnlich ein. Erfahrungsgemäß bringt ein mittlerer Wert von 30 die besten Ergebnisse. Schließlich müssen Sie noch festlegen, wie die Dubletten ausgegeben werden. Im nachfolgenden Beispiel

```
findimagedupes -R -t 30 -p feh ~/
 Bilder
```

landen diese beim Bildbetrachter feh, der für die Kommandozeile gut geeignet ist. Möglicherweise müssen Sie diesen auch erst auf Ihrem System nachinstallieren.



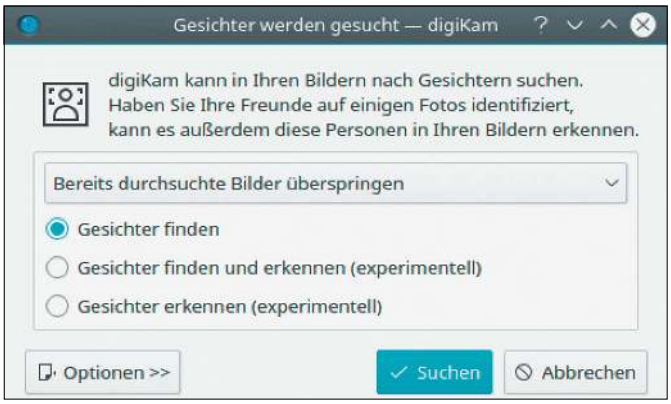
Dank verschiedener Ansichten bietet die Bildverwaltung Digikam alles, was Sie zur Organisation auch umfangreicher Fotosammlungen benötigen.

Elaborierte Fotoverwaltung mit Digikam

Sie wollen Fotos auch bewerten, zu einer „Diashow" zusammenstellen oder mit Stichwörtern arbeiten? Dann benötigen Sie eine ausgewachsene Fotoverwaltung. Inzwischen gibt es eine ganze Reihe von Programmen, mit denen Sie auch umfangreiche Sammlungen übersichtlich organisieren und die darin gespeicherten Bilder schnell betrachten können. Darktable ist derzeit die Software, die in Hinblick auf die Unterstützung des professionellen RAW-Formats und mit ihren Bearbeitungsfunktionen den besten Ruf genießt. Wer seine Fotos nicht nur organisieren, sondern direkt die Rohdaten aus der Kamera verwenden will, um Korrekturen vorzunehmen, findet in **Darktable** das passende Werkzeug. Allerdings sind die Einstiegshürden trotz aller Assistenten und Hilfsfunktionen doch recht hoch.
Wenn es lediglich um die Organisation und eventuelle kleinere Korrekturen geht, bietet sich **Digikam** an. Es ist eigentlich für den KDE-Desktop entwickelt, funktioniert aber auch unter Gnome-affinen Umgebungen. Digikam bietet alle wesentlichen Funktionen für die Bearbeitung und Verwaltung von Fotos. Außerdem macht es Digikam leicht, Bilddateien auch auf externe Datenträger auszulagern – ein gewichtiges Argument, wenn der Platz auf den internen Festplatten knapp zu werden droht.
Wer eine Distribution einsetzt, die den KDE-Desktop als Standard nutzt, dürfte bereits eine lauffähige Version von Digikam auf dem Rechner haben. Ansonsten ist es in den Paketquellen aller aktuellen Linux-Varianten zu finden. Nach dem ersten Aufruf der Software startet zunächst ein Assistent, der bei der Einrichtung des Programms hilft. Im ersten Schritt definieren Sie ein Verzeichnis, in das die Fotos abgelegt werden. Das kann der vorgeschlagene Ordner des Systems sein, aber auch eine Netzwerkfreigabe auf einem NAS oder einem anderen Rechner. Anschließend muss der Speicherort für die Datenbanken sowie deren Format festgelegt werden. Digikam speichert Informationen zu den Fotos, aber auch Miniaturen in verschiedenen Datenbanken. Entscheiden Sie sich am besten für das robuste und ausgereifte Sqlite-Format. Wer ohnehin nur vorhat, die Fotos von Kamera oder Smartphone rasch zu importieren, kann die Optionen zum Rohformat einfach bei den voreingestellten Werten belassen.
Wichtiger ist da die nächste Frage des Assistenten: Mit der Fotoverwaltung weisen Sie den Bildern auf Wunsch weitere Eigenschaften zu, zum Beispiel Informationen zum Ort der Aufnahme oder Personennamen. Digikam kann diese Informationen direkt in die Bilddatei als Metainformation schreiben. Das bietet den Vorteil, dass die Informationen auch beim Import in einer anderen Fotoverwaltung gelesen werden können und auch beim Kopieren auf andere Datenträger erhalten bleiben. Eingebettete Metadaten machen allerdings die Arbeit mit dem Programm etwas langsamer. Wägen Sie ab und entscheiden Sie sich im Zweifel dafür, den Voreinstellungen zu folgen.
Schließlich legen Sie noch fest, wie die Vorschaubilder in der Bildübersicht, dem Leuchttisch, dargestellt werden. Im Zusammenhang damit haben Sie die Wahl, Bilder vom Leuchttisch in der Vorschau zu öffnen oder direkt in einem Editor. Praktisch ist es, sich die Kurzinfos anzeigen zu lassen, wenn mit der Maus auf ein Bild in der Übersicht gezeigt wird.
Damit ist der Einrichtungsassistent absolviert. Mit „Abschließen" verlassen Sie die Einrichtung. Jetzt startet Digikam zum ersten Mal und liest die Bilder aus dem Verzeichnis ein, das Sie während der Einrichtung als Speicherort definiert haben.

Fotos in Digikam-Alben organisieren

Daran hat auch die Digitalfotografie nichts geändert: Fotos werden am besten in Alben sortiert. Digikam besitzt bereits einige eingebaute Funktionen, um schneller zum gesuchten Foto zu gelangen. Darauf haben Sie über die linke Seitenleiste Zugriff. Mit „Daten" werden die Fotos nach Aufnahmedatum gruppiert, „Karte" platziert sie anhand im Bild gespeicherter Geotags auf der Weltkugel. Der Klassiker sind aber schlicht Alben. Ein Album in Digikam entspricht auch einem Ordner auf der Festplatte. Besonders schnell legen Sie ein Al-



Die Digikam-Optionen zur Gesichtserkennung sind sehr übersichtlich und einfach. Das Tool liefert aber durchaus brauchbare Ergebnisse.

Nach der Erkennung von Gesichtern kommt die Bestimmung: Sie können der Software mitteilen, um welche Person es sich bei den Bildern handelt.

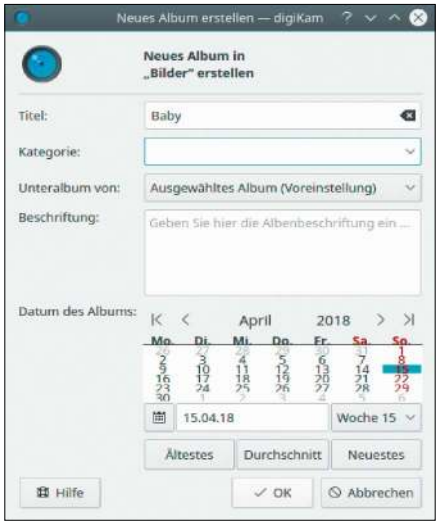
bum direkt aus der Übersicht heraus an. Markieren Sie die gewünschten Fotos und klicken Sie mit der rechten Maustaste. Wählen Sie im Kontextmenü „In Album verschieben“. Im nachfolgenden Dialog können Sie ein bereits bestehendes Album verwenden oder mit „Neues Album“ eine neue Sammlung anlegen. Praktischerweise können Sie das Album auch gleich zeitlich einordnen. Unter „Datum des Albums“ haben Sie die Wahl, den Zeitstempel der ältesten oder neuesten Aufnahme zu verwenden oder den Durchschnitt aus allen Bildern der Auswahl zu nutzen.

Mit Digikam Personen suchen und erkennen

Eine praktische Funktion, um die Fotos nach Personen zu ordnen, ist die automatische (experimentelle) Gesichtserkennung. Rufen Sie dazu den Bereich „Personen“ entweder über die Seitenleiste oder das Menü „Durchsuchen“ auf. Klicken Sie auf „Sammlung nach Gesichtern durchsuchen“. Entscheiden Sie sich danach für „Gesichter finden“. Der Vorgang dauert eine Weile, je nach Menge der Fotos. Digikam präsentiert Ihnen danach übersichtlich alle gefundenen Gesichter. Zeigen Sie mit der Maus auf ein Foto, können Sie jetzt den Namen der betreffenden Person eingeben. Über die Funktion „Gesichter erkennen“ können Sie später den Datenbestand dann nach bereits bekannten Personen durchsuchen. Der Name der Person wird automatisch zu einem Schlagwort in der Personenansicht. So finden Sie später jederzeit die passenden Aufnahmen wieder.

Mit Digikam Schlagwörter vergeben

Schlagwörter sind eine gute Ergänzung, um noch mehr Ordnung in die Fotosammlung



Neues Album mit mehreren Fotos: Bei der Anlage eines neuen Albums kann das Aufnahmedatum ausgewertet werden.

zu bekommen. Damit werden dann auch Aufnahmen wiedergefunden, die über mehrere Ereignisse oder Alben hinweg interessant sind – etwa Orte oder abstrakte Begriffe wie „Architektur“ oder „Fahrzeug“. Das geht in Digikam ebenfalls am schnellsten über das Kontextmenü gewählter Einträge. Nach dem Rechtsklick finden Sie im unteren Bereich des Menüs das Kommando „Stichwort zuweisen“. Anschließend können Sie aus den Stichwörtern wählen, die Sie vor kurzem erst genutzt haben. Oder Sie nutzen „Neues Stichwort hinzufügen“, um ein neues Stichwort anzulegen. Mit solchen Stichwörtern verleihen Sie der Sammlung den Feinschliff. Sie dürfen ruhig eng gewählt sein. Liegen die Aufnahmen etwa im Ordner „Hamburg Urlaub 2017“, dann könnten Sie mit den Stichwörtern auf Motivebene mehr Ordnung schaffen, wenn Sie etwa die Sehenswürdigkeiten auf dem Bild mit weiteren Stichwörtern versehen.

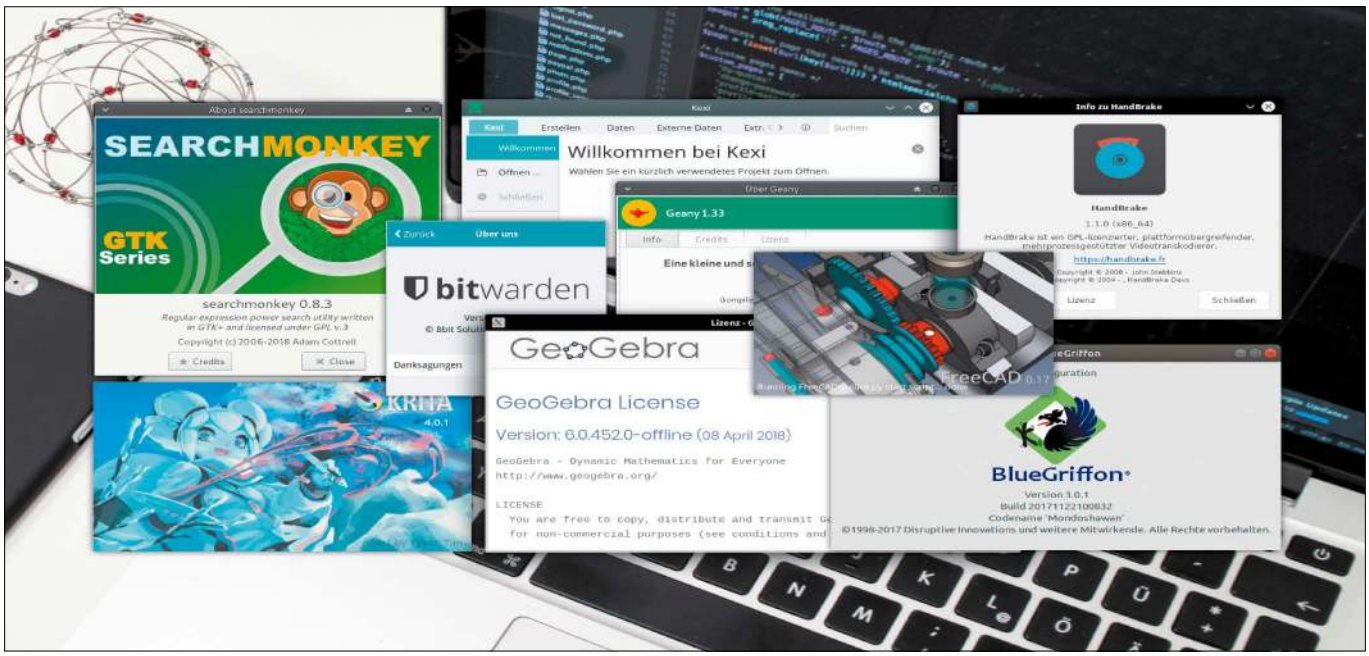
Digikam mit Export-Plug-ins: Wenn die Kipi-Plug-ins installiert sind, dann lassen sich Fotos auch mit diversen anderen Plattformen teilen.

Fotos betrachten und weitergeben

Natürlich dient Digikam nicht nur zur Verwaltung Ihrer Aufnahmen. Sie können direkt aus der Software heraus Diashows und Präsentationen gestalten. Diese Funktionen finden Sie im Menü „Ansicht“. Dazu wählen Sie zunächst die Alben oder Bilder aus, die Sie verwenden wollen, und legen danach Übergänge fest oder fügen auch Beschriftungen ein. Über „Extras“ produzieren Sie Galerien im HTML-Format oder gestalten einen individuellen Kalender. Dank zahlreicher Plug-ins können Sie Fotos auch mit externen Plattformen teilen. Dazu müssen Sie in der Paketverwaltung die sogenannten Kipi-Plugi-ns nachinstallieren. ■

Neue Software

Kleine und große Programme aus der Open-Source-Szene verlangen Aufmerksamkeit: Das Zeichenprogramm Krita geht in Version 4.0, Free CAD macht Fortschritte und Bitwarden ist ein Passwortmanager, der auch auf dem eigenen Linux-Server läuft.



VON DAVID WOLSKI

Open-Source-Projekte haben den Ruf, in Sachen Entwicklung besonders umtriebig zu sein. Zwar gibt es zwischen Versionsnummern oft nur etliche kleine Änderungen. Meist sind es Dutzende bis Hunderte kleiner Verbesserungen und Bugfixes, die dann in der Summe den Satz auf eine neue Versionsnummer nötig machen. So legen viele prominente Entwicklungen dank vieler beteiligter Programmierer eine enorme Geschwindigkeit vor, die Linux-Distributionen mit ihren offiziellen Paketquellen oft nicht mitkommen lässt.

In den folgenden Vorstellungen neuer Software rund um Linux geben wir deshalb auch stets mit an, wo man fertige Pakete eines Programms bekommt. Oft spielt dieser Aspekt auch schon bei der Vorauswahl einer Vorstellung eine Rolle. Denn es erscheint einfach nicht mehr zeitgemäß, größere Softwarepakete selbst zu kompilieren. Mehr und mehr populäre Anwendungen wie Krita werden von deren Entwickler deshalb routinemäßig in fertige Appcontainer gepackt, etwa in Snaps, Flatpaks oder Appimages.

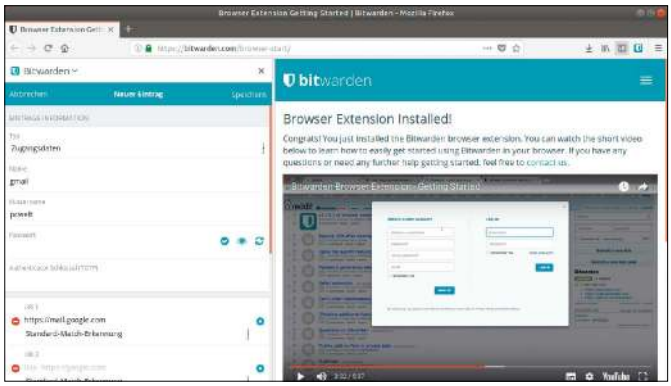
GNU Time lässt sich Zeit

Eine hohe Frequenz regelmäßiger Veröffentlichungen gibt es aber nur bei den spannenden Projekten, die auch mal für Furore sorgen können. Diese gut sichtbaren Projekte wie etwa der Linux-Kernel und Containertechnologien wie Docker, über die häufig berichtet wird, können sich über mangelnde Teilnahme durch IT-Industrie und individuelle Entwickler nicht beklagen. Bei anderen Open-Source-Technologien, ohne die keine Linux-Distribution funktioniert, ist die Lage nicht so rosig. So bewegen sich einige Programme aus dem Umkreis der GNU Coreutils nur mehr mit der Geschwindigkeit eines Gletschers. Das Schlusslicht ist mit langem Abstand das Kommandozeilentool GNU Time: Zwischen Version 1.7 und der Anfang des Jahres erschienenen Version 1.8 liegen nicht weniger als 21 Jahre (!). Das ist sogar für ein wenig bewegtes Shell-Werkzeug eine lange Zeit und dürfte den längsten Zeitraum zwischen zwei Punkt-Releases markieren. Den Rekord zwischen Veröffentlichungen hält aber Open Xanadu: Diese Hypertext-Software zur Visualisierung von Querverweisen war als Vorläufer des World Wide Web gedacht, wurde von diesem aber schließlich überholt. Zwischen dem Prototypen Xanadus im Jahr 1960 und dem schließlich veröffentlichten Open Xanadu (*http://xanadu.com/xanademos/MoeJusteOrigins.html*) vergingen 54 Jahre. Immerhin hat Xanadu in der Zwischenzeit erfolgreichere Unternehmungen wie Wikipedia inspiriert.

Bitwarden 1.1

Passwortsafe für Browser, Desktop, Smartphones
https://bitwarden.com

Seit bekannt ist, dass Firefox Sync mit dem als unsicher eingestuften Algorithmus SHA-1 verschlüsselt, suchen Anwender Alternativen. Eine Lösung für Anspruchsvolle, die im LAN oder Web Passwörter speichern, ist Bitwarden mit Plug-ins für Chrome/Chromium, Firefox, Safari, Edge, Opera, zudem iOS- und Android-Apps. Die optionale Serverkomponente ist Open Source und als Docker-Container verfügbar (*https://help.bitwarden.com/article/install-on-premise*).

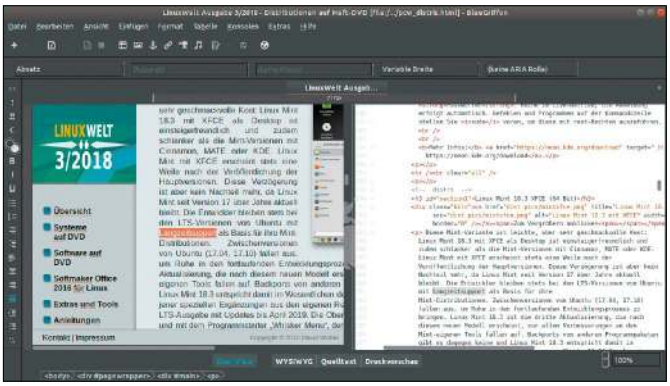


Hosten oder hosten lassen: Der Online-Passwortsafe Bitwarden ist mit vielen Browser-Add-ons eine sichere Alternative zu Firefox Sync.

Blue Griffon 3.0.1

Visueller HTML-Editor
http://bluegriffon.org

Blue Griffon erstellt HTML-Dokumente und statische Webseiten. Eine Vorschau zeigt das Ergebnis in der Gecko-Engine des Firefox. Eine Seitenleiste blendet einen CSS-Editor ein, der auch externe Stylesheets lädt. Blue Griffon liegt als DEB-Paket für Ubuntu auf der Projektwebseite vor. Das Programm steht unter Open-Source-Lizenzen, jedoch sind Funktionen für Epub-Dokumente und responsives Design in kostenpflichtige Plug-ins ausgelagert (ab 75 Euro).

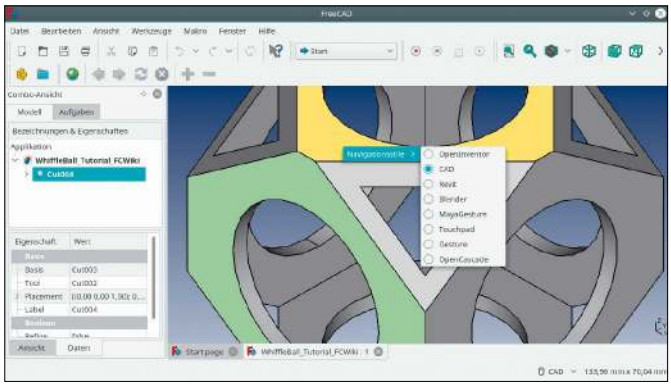


Vorschau sofort: Stärke des HTML-Editors Blue Griffon ist die Vorschaufunktion, die auf einem älteren Firefox basiert.

Free CAD 0.17

Freies CAD-Programm im Stil von Auto CAD
http://librecad.org/cms/home.html

Freie CAD-Programme sind rar, daher verdient Free CAD trotz kleiner Versionsnummer Beachtung. Die 3D-CAD-Software ist für technische Konstruktionen und Architektur geschaffen, kann 2D-Pläne erstellen und hat einen Arbeitsbereich für technische Zeichnungen sowie einen Add-on-Manager. Es versteht neben dem eigenen Format auch DXF. In aktuellen Linux-Distributionen ist Free CAD 0.17 nicht zu finden, aber die Webseite liefert ein universales Appimage.

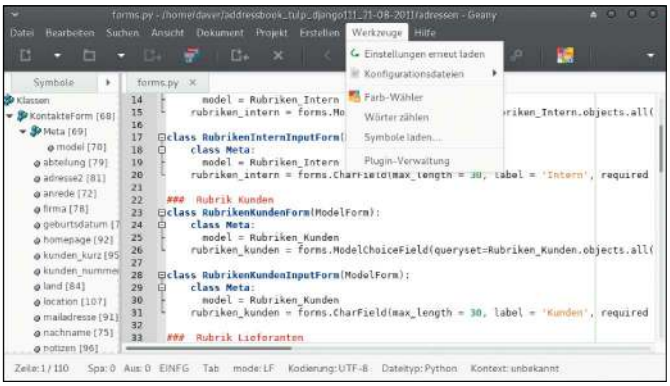


Gekonnt konstruiert: Die 3D-CAD-Software Free CAD mit Python-Schnittstelle nutzt die bewährten Open-Cascade-Bibliotheken.

Geany 1.33

Texteditor für Scripts und mehr
www.geany.org

Geany ist ein Klassiker, da er als einfacher Texter wie als mächtiger Codeeditor taugt. Das Open-Source-Programm macht nach dem Wechsel zu GTK3 auf modernen Linux-Desktops eine hervorragende Figur, zumal Version 1.33 die Darstellung auf Hi-DPI-Bildschirmen verbessert. In den Optionen gibt es die neue Möglichkeit, Dateien bei Änderungen automatisch neu zu laden. Pakete für viele Distributionen gibt es auf *www.geany.org/Download/ThirdPartyPackages*.

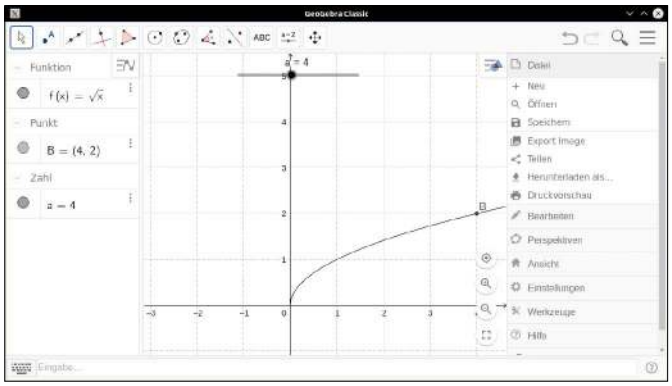


Eleganter Editor: Geany ist neben Linux auch für Windows sowie Mac-OS verfügbar und im zwölften Jahr seiner Entwicklung.

Geogebra Classic 6.0

Software für Algebra und Geometrie
www.geogebra.org

Die Universität Salzburg entwickelt Geogebra zur Berechnung und Darstellung von mathematischen Graphen. Zielgruppen sind Schüler, Studenten, Dozenten, die eine dynamische Geometriesoftware (DGS) ohne hohe Einstiegshürde suchen. Geogebra verlangt im Gegensatz zu Matlab oder Wolfram keine Programmierkenntnisse. Teile von Geogebra stehen unter der GNU Public License, andere sind proprietär. Die Nutzung im Unterricht ist aber kostenlos.

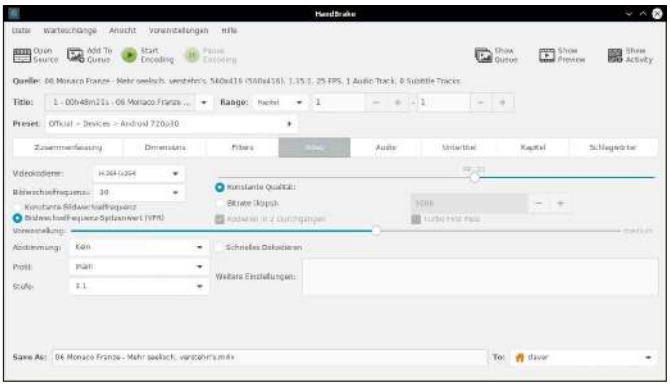


Euklidische Geometrie war noch nie so einfach: Geogebra zeichnet Graphen und geometrische Körper nach Gleichungen und Funktionen.

Handbrake 1.1

Videokonverter mit Jobverwaltung
https://handbrake.fr

Handbrake, das vor 14 Jahren für Be-OS erschien und später auf Linux, Windows und Mac-OS portiert wurde, vereinfacht die Videokonvertierung enorm. Im Hintergrund arbeiten mächtige Transcoder wie Libav. Sinnvolle Voreinstellungen, zu welchen auch Formate für Youtube und Vimeo gehören, bringen Videos unkompliziert ins Zielformat. Handbrake 1.1 gibt es für Ubuntu/Mint über das PPA *https://launchpad.net/~stebbins/+archive/ubuntu/handbrake-releases*.

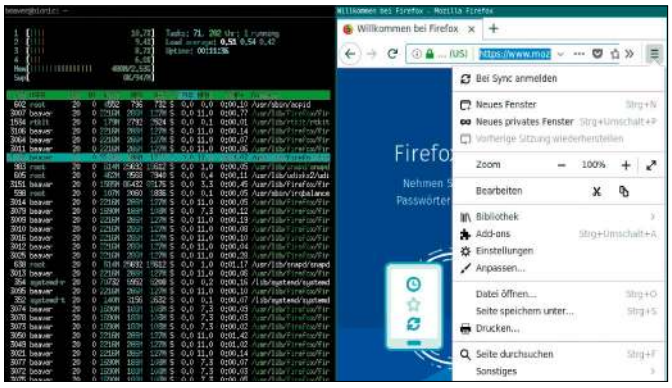


Komfortabel konvertieren: Handbrake nutzt Bibliotheken wie Libav und Ffmpeg, um Videocontainer verschiedener Formate zu schreiben.

i3 4.15

Kachelnder Fenstermanager
https://i3wm.org

Neben den bekannten Desktops gibt es eng spezialisierte Linux-Oberflächen. Der Window-Manager i3 bringt eine gekachelte Darstellung geöffneter Programmfenster auf den Bildschirm und ist auf Tastaturbedienung ausgerichtet. Die Maus wird nur innerhalb von Programmen wichtig. Auf PCs mit textbasierten Programmen ist mit i3 und etwas Übung sehr effizientes Arbeiten möglich. In Debian Sid und Ubuntu 18.04 gibt es neues i3 über apt-get.

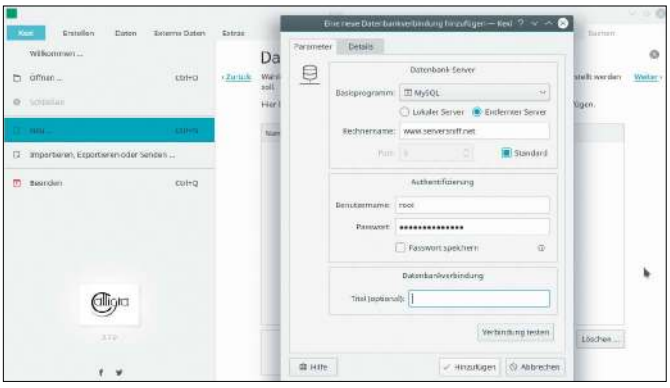


Ein Desktop, der beinahe ohne Maus auskommt: Im Fenstermanager i3 steht effiziente Tastatursteuerung im Vordergrund.

Kexi 3.1

Grafisches Werkzeug für Datenbankabfragen
www.kexi-project.org

Die Abfrage von Datenbanken muss nicht kompliziert sein. Kexi ist von Microsoft Access inspiriert und erlaubt Abfragen und Dateieingaben in Datenbanken (Maria DB, My SQL, Sqlite, Postgresql) mittels Formularen, für die Kexi einen visuellen Editor bereitstellt. Die Datenbankschnittstelle ist in KDE-Bibliotheken ausgelagert, damit auch andere Programme die Schnittstelle nutzen können. Kexi 3.1 findet sich in den Paketquellen von Ubuntu 18.04 sowie KDE Neon.

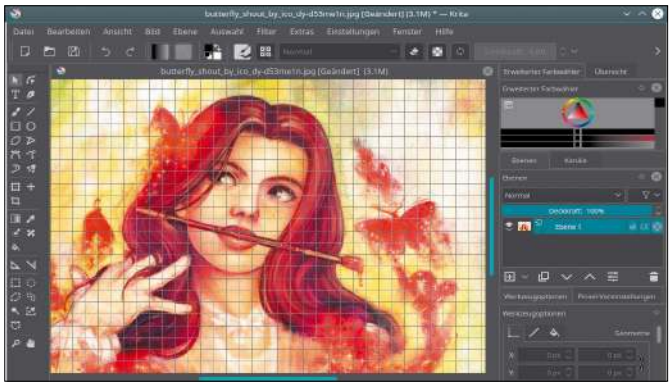


Sexy Kexi: Der Formulareditor von Kexi vereinfacht Abfrage und Eingabe von Datensätzen in verschiedenen Datenbanken.

Krita 4.0

Anspruchsvolles Zeichenprogramm
https://krita.org

Für Illustrationen und Zeichnungen ist das Open-Source-Grafikprogramm Krita geschaffen. Es spricht anspruchsvolle bis professionelle Benutzer an und hat seit Version 2 viele Lorbeeren erhalten. Ausgabe 4.0 ersetzt das Vektorgrafikformat durch SVG und verwirft ODG. Alte Dateien kann Krita 4.x zwar öffnen, neue Krita-Dateien sind aber nicht mehr abwärtskompatibel. Die Entwickler bieten ein PPA für Ubuntu, ein universelles Appimage sowie ein Flatpak.



Kunstfertiges Krita: Version 4 des Zeichenprogramms wechselt bei Vektorgrafiken zum SVG-Format und lernt die Script-Sprache Python.

Open RA 2018-02-18

Neu aufgelegtes Echtzeit-Strategiespiel
www.openra.net

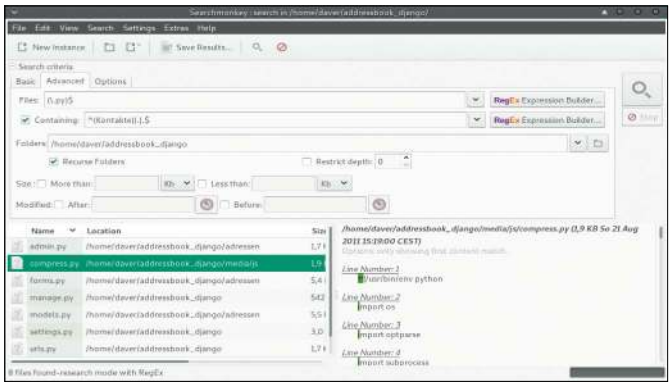
Open RA ist ein Nachbau von Command & Conquer: Red Alert, das Mitte der 90er-Jahre Kultstatus besaß und bis heute seine Fans hat. Open RA steht unter der GNU Public License und nutzt eine eigene Spieleengine mit vielen Erweiterungen gegenüber dem Original. Es gibt einen Single- und Mehrspielermodus. Grafik und Sound bezieht das Spiel aus der Freewareversion des Originals. Zur Installation liefert die Webseite fertige Pakete in den Formaten DEB und RPM.

Alarmstufe Rot: Auf Basis der als Freeware freigegebenen Vollversion von Command & Conquer erfindet Open RA den Klassiker neu.

Searchmonkey 3.2.0

Volltextsuche mit regulären Ausdrücken
http://searchmonkey.embeddediq.com/index.php

Searchmonkey ist das ideale Suchwerkzeug in ausufernden Programmier- und Webprojekten mit Bergen an Quellcode. Die Volltextsuche unterstützt reguläre Ausdrücke in Perl-Syntax. Clou des Programms sind übersichtliche Menüs zum Bau komplexer Suchabfragen. Kriterien und Ergebnisse kann Searchmonkey zur späteren Verwendung speichern. Searchmonkey liegt als plattformübergreifende Java-Anwendung vor, für Linux auch als GTK-Programm.

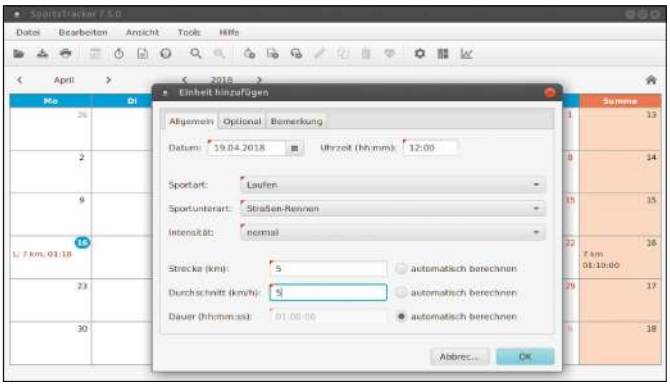


Grafischer Ersatz für Grep: Searchmonkey findet mit regulären Ausdrücken und Platzhaltern jede Zeichenkette in Textdateien.

Sportstracker 7.5

Auswertung sportlicher Aktivitäten
www.saring.de/sportstracker

Das Java-Tool Sportstracker 7.5 zeichnet Sportaktivitäten auf und importiert Protokolle von Herzfrequenzmesser und GPS-Empfänger. Die Sportarten sind beliebig und werden in einen Kalender eingetragen. Neben Herzfrequenz analysiert der Sportstracker Streckensteigung und Kalorienbedarf. Das Programm unterstützt GPX-Dateien zur Streckenvisualisierung sowie Daten von Garmin, Polar, Timex und Suunto. Ein DEB-Paket für Ubuntu gibt es über die Webseite.



Tagebuch zum Training: Der Sportstracker errechnet Statistiken aus den eingetragenen Aktivitäten und importiert GPS- und Tracker-Dateien.

Netflix und Amazon Prime Video mit Kodi

Kodi und der Raspberry Pi tauchen in der Liste der von Netflix und Amazon Prime offiziell unterstützten Geräte nicht auf. Über Kodi-Erweiterungen lassen sich die Streamingdienste dennoch einbinden.

VON THORSTEN EGGELING

Offiziell unterstützen Netflix und Amazon Prime Video Android- und iOS-Geräte sowie Smart-TVs, einige Spielekonsolen und Windows 10 jeweils über Apps. Am PC lassen sich die Videos auch im Webbrowser abspielen, was bei Mozilla Firefox und Google Chrome auch unter Linux funktioniert. Wer Kodi als Medienzentrale nutzt, kann die Streamingdienste über Add-ons auch hier nutzen.

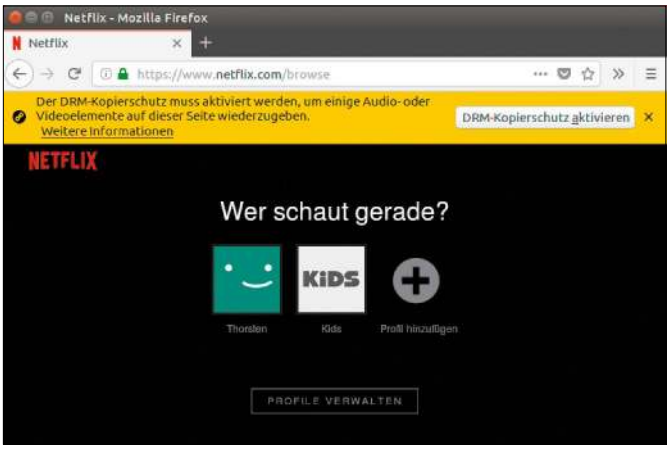
1. DRM-geschützte Inhalte unter Linux abspielen

Netflix und Amazon Prime Video setzen auf Widevine-DRM (Digital Rights Management) und das zugehörige Content Decryption Module (CDM) von Google. Bei Firefox und Google Chrome ist auch unter Linux die dafür nötige Bibliothek „libwidevinecdm.so“ bereits vorhanden oder sie wird automatisch eingerichtet, sobald Sie DRM-geschützte Inhalte abrufen. Firefox blendet einen Hinweis und eine Schaltfläche ein, über die Sie den DRM-Kopierschutz aktivieren.

Google bietet die DRM-Bibliothek für die meisten Betriebssysteme zum direkten Download an, jedoch nicht für ARM-CPUs. Die benötigte Datei für Amazon Video ist aber in den Wiederherstellungsabbildern von Google Chromebooks enthalten. Aus lizenzrechtlichen Gründern darf sie nicht frei zum Download angeboten werden. Sie müssen sich allerdings nicht selbst um den Download kümmern. Das erledigt das Amazon-Add-on für Kodi automatisch. Die Bibliothek lässt sich dann auch für Netflix verwenden. Zur Zeit funktioniert hier aber noch eine ältere Widevine-Version, die sich direkt herunterladen lässt (siehe Punkt 4).

2. Kodi für Netflix oder Amazon Video verwenden

Die kommende Kodi-Version 18 enthält ein Add-on mit dem Namen „InputStream Adaptive“. Damit lassen sich Videostreams durch ein Entschlüsselungsprogramm schicken und der decodierte Inhalt erscheint auf dem Bildschirm. Aktuell befindet sich Kodi 18 noch in der Testphase, ist aber stabil genug für den Alltagseinsatz. Es gibt jedoch einige Einschränkungen: Die Decodierung benötigt zusätzliche CPU-Leistung und



Verschlüsselte Streams: Damit Firefox unter Linux ein Video von Netflix oder Amazon Prime abspielen kann, müssen Sie das Widevine-DRM-Plug-in aktivieren.

die Hardwarebeschleunigung des Grafikchips kann nicht genutzt werden. Linux-PCs oder Notebooks sind in der Regel schnell genug, beim Raspberry Pi 3 müssen Sie jedoch auf HD-Videos verzichten. Maximal 720 p sind möglich. Die SD-Karte sollte mindestens 16 GB Speicherplatz bieten. Bei nur acht GB kann es knapp werden, weil die Widevine-Installation vorübergehend bis zu zwei GB auf der Karte ablegt.

Netflix und vor allem Amazon ändern regelmäßig die Aufbereitung und Struktur der ausgelieferten Daten oder es ist eine neuere Version von Widevine-DRM erforderlich. Es ist daher damit zu rechnen, dass die Add-ons nach einiger Zeit nicht mehr funktionieren, bis ein Update verfügbar ist. Meist arbeiten die Entwickler jedoch relativ schnell, so dass Sie nur kurze Zeit auf die Streamingdienste verzichten müssen. In den deutschsprachigen Kodinerds-Foren *www.pcwelt.de/r9kweT* (Amazon) und *www.pcwelt.de/nPrQWh* (Netflix) können Sie sich über die Entwicklung informieren.

Kodi auf dem Raspberry Pi: Richten Sie zuerst Libre Elec 8 mit Kodi 17 auf der SD-Karte ein. Danach installieren Sie Version 18 von Kodi als Update.

3. Kodi 18 installieren

Auf der Kodi-Downloadseite *https://kodi.tv/download* klicken Sie das gewünschte Betriebssystem an, beispielsweise Linux, Android, Windows oder Raspberry Pi, und gehen dann auf die Registerkarte „Pre release“ oder „Development Builds“. Es gibt Schaltflächen wie „Guide“, die auf Artikel mit Anleitungen im Kodi-Wiki verweisen.

Ubuntu/Mint-Nutzer können alternativ ein Launchpad-PPA einbinden und Kodi 18 darüber installieren:

```
sudo add-apt-repository ppa:team-xbmc/xbmc-nightly
sudo apt-get update
sudo apt-get install kodi
```

Beim Raspberry Pi benötigen Sie zuerst eine reguläre Libre-Elec-Installation mit Libre Elec 8/Kodi 17, die Sie anschließend auf die Version 18 aktualisieren.

Wenn Kodi bereits installiert ist, sollten Sie ein Backup der SD-Karte erstellen, damit Sie bei Problemen schnell zur vorherigen Version zurückkehren können (siehe Kasten „SD-Karte unter Linux sichern“).

Ist Libre Elec noch nicht installiert, laden Sie das Setuptool „LibreELEC USB-SD Creator“ von *https://libreelec.tv/downloads* herunter und kopieren das System auf die SD-Karte. Legen Sie die Karte in den Raspberry Pi ein, starten Sie das Gerät und folgen Sie den Anweisungen des Einrichtungsassistenten. Aktivieren Sie die Dienste „Samba“ und „SSH“. Sie können dann mit anderen PCs über das Netzwerk auf das Libre-Elec-System zugreifen.

Danach aktualisieren Sie Kodi auf die Version 18. Gehen Sie in die Einstellungen (Zahnradsymbol) und auf „LibreElec“. Unter „System“ stellen Sie bei „Aktualisierungen“ hinter „Automatische Aktualisierungen“ den Wert „manuell“ ein. Aktivieren Sie „Benutzerdefinierte Kanäle anzeigen“. Bei „Benutzerdefinierter Kanal 1“ tippen Sie

```
http://milhouse.libreelec.tv/builds/master/RPi2
```

ein. Beachten Sie die Groß-Klein-Schreibung. Bei „Update Kanal“ stellen Sie „Milhouse-9.0“ ein und bei „Verfügbare Versionen“ wählen Sie die höchste Versionsnummer. Anschließend bestätigen Sie das Update mit „Ja“. Das Update wird heruntergeladen und installiert. Der Raspberry Pi startet dabei mehrfach neu.

4. Netflix- und Amazon-Add-ons einrichten

Die folgende Anleitung gilt sinngemäß für alle Installationen von Kodi 18 beziehungsweise Libre Elec 9.0 unabhängig vom Betriebssystem.

Gehen Sie in den „Einstellungen“ auf „System → Addons“. Hier aktivieren Sie „Unbekannte Quellen“ und bestätigen mit „Ja“. Zurück zu den „Einstellungen“ gehen Sie auf „Addons → Benutzer-Addons → Videoplayer InputStream Addons“ und aktivieren „InputStream Adaptive“.

SD-KARTE UNTER LINUX SICHERN

Vor der Aktualisierung eines bestehenden Kodi 17 auf Version 18 empfehlen wir ein Backup des bisherigen Systems. Legen Sie dazu die Karte in den Kartenleser eines Linux-Rechners. Hier ermitteln Sie im Terminal mit lsblk den Pfad der SD-Karte und hängen diese dann mit umount aus. Für das Backup verwenden Sie dann diese beiden Befehlszeilen:

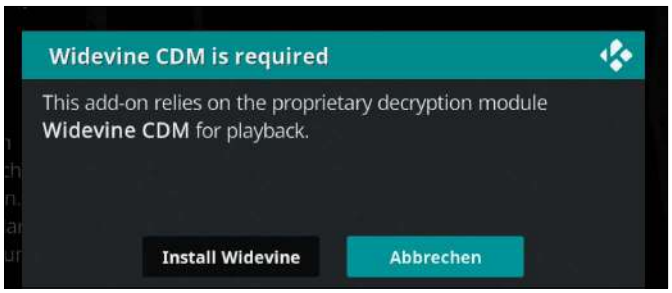
```
sudo apt-get install pv
sudo dd if=/dev/sd[X] | pv | gzip -c > ~/LibreElec20180529.img.gz
```

Das optionale Tool pv sorgt dafür, dass eine Fortschrittsanzeige für dd erscheint. Den Platzhalter „[X]“ ersetzen Sie durch die zuvor ermittelte Laufwerksbezeichnung. Bei Bedarf schreiben Sie das Backup mit diesen Befehlen:

```
gunzip -c ~/LibreElec20180529.img.gz | pv | sudo dd of=/dev/sd[X]
sync
```

wieder zurück.

Kodi erweitern: Nach der Installation der Kodinerds-Erweiterung haben Sie Zugriff auf zusätzliche Repositorien, über die Sie das Netflix- und Amazon-Add-on installieren.



DRM-Bibliothek: Das Amazon-Add-on fordert automatisch Widevine an, sobald Sie auf das Filmangebot zugreifen. Das Netflix-Add-on verwendet diese Datei ebenfalls.

In der Konfiguration des Add-ons sollte beim Raspberry Pi hinter „Max. Resolution secure decoder" der Wert „720p" eingestellt sein. Auf einem leistungsfähigeren Rechner wählen Sie „Max".

Öffnen Sie am PC die Adresse *www.pcwelt.de/uZnemE* im Browser. Klicken Sie auf „Download", um die Datei „repository.kodinerds-6.0.0.zip" herunterzuladen. Kopieren Sie die Datei über das Netzwerk (smb oder ssh/sftp) auf den Raspberry Pi, beispielsweise in den Ordner „/storage/downloads". Am Raspberry Pi gehen Sie in den Einstellungen auf „Addons → Aus ZIP-Datei installieren". Wählen Sie den Ordner, in den Sie die ZIP-Datei kopiert haben – beispielsweise „Home-Ordner → downloads". Gehen Sie auf „Aus Repository installieren → kodinerds Add-on → Addon-Repository". Aktivieren Sie „Netflix Addon Repository" und „Sandmann79s Repository" (Amazon). Installieren Sie das Amazon-Add-on auch dann, wenn Sie nur Netflix verwenden, weil darüber der Download der aktuellen Widevine-Bibliothek erfolgt.

Amazon Prime: Navigieren Sie zurück zu „Aus Repository installieren" und gehen Sie auf „Sandmann79s Repository → Video-Addons". Installieren Sie das Add-on „Amazon". Es lädt die Filmtitel in eine lokale Datenbank, die Kodi automatisch alle zwei Tage aktualisiert. Das kostet zwar etwas Speicher auf der SD-Karte, dafür navigieren Sie so schneller durch das Videoangebot. Alternativ können Sie auch das Add-on „Amazon VOD" verwenden, das ohne Datenbank auskommt. In der Konfiguration des Amazon-Add-ons stellen Sie unter „Allgemein" bei „Wiedergabemethode" den Wert „Input Stream" ein. Über „Verbindung → Anmelden" melden Sie sich bei Ihrem Amazon-Prime-Konto an, sofern Sie eines besitzen.

Gehen Sie zurück zum Kodi-Startbildschirm und auf „Addons". Wählen Sie „Amazon", und öffnen Sie dann ein beliebiges Video. Sie erhalten eine Meldung über den erforderlichen Download der Widevine-Bibliothek. Folgen Sie den Anweisungen auf dem Bildschirm. Ohne Amazon-Konto erhalten Sie ab und zu Meldungen über die fehlgeschlagene Anmeldung und landen bei der Add-on-Konfiguration. Schließen Sie das Fenster einfach. Sie können das Add-on dann nach dem Download deaktivieren.

Netflix: Navigieren Sie zurück zu „Aus Repository installieren", gehen Sie auf „Netflix Addon Repository → Video-Addons" und installieren Sie das Add-on „Netflix". Rufen Sie es über den Kodi-Startbildschirm unter „Addons" auf. Beim ersten Zugriff werden die Anmeldeinformationen angefordert.

Hinweis: Die ältere Widevine-Bibliothek für Netflix lässt sich zur Zeit (April 2018) auch auf einem anderen Weg installieren. Verwenden Sie diese Methode aber nicht, wenn Sie auch Amazon nutzen. Öffnen Sie auf Ihrem Linux-PC ein Terminalfenster und stellen Sie eine SSH-Verbindung zu Libre Elec auf dem Raspberry Pi her:

```
ssh root@libreelec
```

Das Standardpasswort ist „libreelec". Mit diesen Befehlen

```
wget http://nmacleod.com/public/
  libreelec/getwidevine.sh
sh getwidevine.sh
```

installieren Sie dann die Bibliothek. ■

STREAMINGDIENSTE: ÜBERSICHT UND KOSTEN

Netflix (*www.netflix.com*) und Amazon Prime Video (*https://www.amazon.de/amazonprime*) sind ab 7,99 Euro pro Monat erhältlich. Amazon Prime kostet bei jährlicher Zahlungsweise 69 Euro (5,75 Euro im Monat) und enthält auch den Gratis-Premiumversand sowie den Zugriff auf Songs bei Amazon Music. Im Amazon-Abo sind nicht alle verfügbaren Videos enthalten. Es gibt auch Angebote, für die Sie extra zahlen müssen.

Maxdome (*www.maxdome.de*) orientiert sich beim Preis an der Konkurrenz (7,99 Euro). Wie bei Amazon sind einige Filmtitel nicht im Abo enthalten und kosten extra.

Bei **Sky Ticket** (*https://skyticket.sky.de*) erhalten Sie Serien für 9,99 und Spielfilme für 14,99 Euro pro Monat. Sport-Tickets kosten ab 9,99 Euro pro Tag.

Außerdem gibt es noch **iTunes** (für iOS-Nutzer, *https://www.apple.com/de/itunes*), **Videoload** (*www.videoload.de*) und **Videobuster** (*www.videobuster.de*). Eine Flatrate gibt es bei diesen Diensten nicht. Sie zahlen hier pro Filmtitel.

Netzkino (*www.netzkino.de*) finanziert sich über Werbung und vor allem viele ältere Filme sind gratis. Sie können sich Videos im Browser mit installiertem Adobe-Flash-Plug-in ansehen. Neuere Filme gibt es im Abo ab 4,99 Euro.

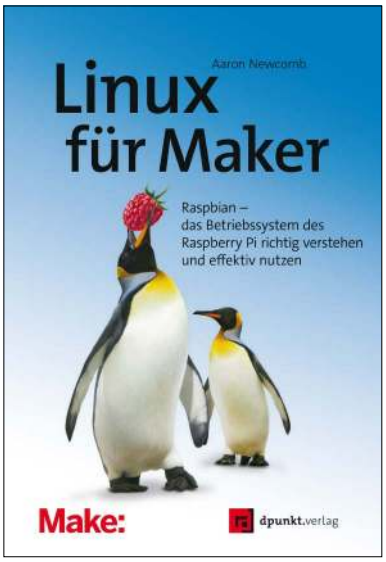
Neben den in diesem Artikel genannten Kodi-Add-ons für Netflix und Amazon Video gibt es auch Erweiterungen für Maxdome, Sky Ticket und Netzkino, die sich ähnlich einrichten lassen. Zum Ausprobieren verwenden Sie am besten den kostenlosen Probemonat bei Netflix, Amazon oder Maxdome. Alle Abodienste lassen sich monatlich kündigen.

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 des Buches »Linux für Maker« aus dem dpunkt.verlag.

Linux für Maker



Raspbian – das Betriebssystem des Raspberry Pi richtig verstehen und effektiv nutzen
Aaron Newcomb, Volker Haxsen (Übersetzung)
Oktober 2017, 254 Seiten, komplett in Farbe, Broschur, dpunkt.verlag
ISBN: 978-3-86490-511-7, 22,90 €

Die Vorliebe für Raspbian kommt bei Makern nicht von ungefähr und es gehört inzwischen dazu wie Schraubendreher und Hammer in der Werkstatt. Linux ist so leistungsfähig, dass Sie sich vielleicht sogar dazu entschließen, es für Ihre täglichen Aufgaben am Computer einzusetzen!
Das Buch befasst sich mit Linux speziell im Hinblick auf die Bedürfnisse von Makern. Die vermittelten Grundlagen helfen Ihnen, Ihre Projekte weiterzuentwickeln und Neues zu entdecken.

Aus dem Inhalt:
- Raspbian und andere populäre Linux-Distributionen installieren
- Code für Scripts schreiben, um Hardware und Arduino zu steuern
- Linux-Befehle, -Systeme und -Prozesse kennenlernen
- GPIO-Pins auf Ihrem Raspberry ansteuern
- ein IFTTT-Applet und andere Clouddienste nutzen
- einen virtuellen Raspberry Pi unter Windows, Mac-OS oder Linux betreiben

PLUS: Gratisheft für alle Teilnehmer

SO FUNKTIONIERT'S:

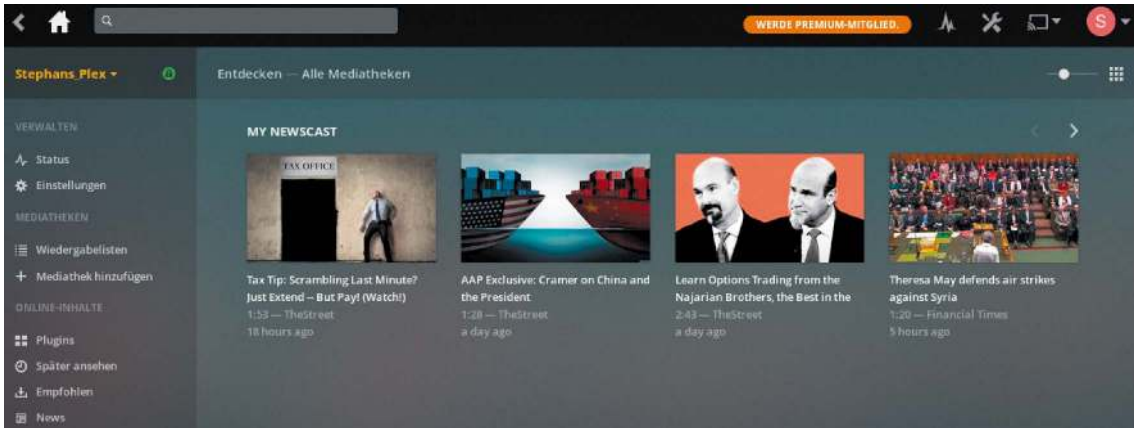
Auf *www.pcwelt.de/lin* gelangen Sie direkt zu unserer Leserbefragung und nehmen automatisch an der Verlosung teil. Von der Verlosung ausgenommen sind Mitarbeiter des Verlags und deren Angehörige. Der Rechtsweg ist ausgeschlossen.
Einsendeschluss für das Gewinnspiel in LinuxWelt 4/2018 ist der 24.7.2018.
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 XXL 1/2018 »Tipps-Handbuch 2018« als PDF (ohne Datenträger).

Sie finden den Link zum Download des Hefts am Ende der Leserbefragung.

Plex-Server auf Raspberry Pi

Wer seine Mediensammlung komfortabel im Heimnetz verteilen will, braucht einen Streamingserver, der Musik und Filme an die angeschlossenen Clients verteilt. Plex ist ein bewährter Server, der auch auf einem Raspberry betrieben werden kann.



Plex-Streamingserver: Alle Optionen und die Medien sind übersichtlich über die Weboberfläche des Servers zu erreichen.

VON STEPHAN LAMPRECHT

Dank seiner Masse an Funktionen gehört der Plex-Server zu den bekanntesten und beliebtesten Lösungen, wenn es um Abspielen und Verwalten von Medien im Netzwerk geht. Was Open-Source-Puristen eher stört, ist für andere Anwender ein Argument für den Einsatz der Lösung: Plex wird als Freemium-Modell vertrieben. Die kostenlosen Basisfunktionen reichen vielen Nutzern bereits aus und wer mehr möchte, schaltet die Funktionen durch eine kostenpflichtige Mitgliedschaft frei. Vorteil des Geschäftsmodells sind regelmäßige Updates und eine Vielzahl an unterstützten Plattformen für die Clients.

Voraussetzungen und Vorbereitung

Als Server verwaltet Plex nicht nur die Mediendateien, stellt also Kataloge und Playlisten bereit, sondern übernimmt auch die Transcodierung. Das System kümmert sich also automatisch darum, dass an die Clients passende Formate verteilt werden, die dort abgespielt werden können. Liegt ein Film zum Beispiel als WMV-Datei vor und soll auf einem iPhone abgespielt werden, wird während des Streamings das Signal in das von iOS erwartete Format konvertiert. Das erfordert einiges an Ressourcen. Aber selbst ohne Transcoding stoßen ältere Generationen des Ein-Platinen-Computers rasch an ihre Grenzen, wenn eine Reihe von Clients gleichzeitig Medien fordern. Ein Plex-Server auf einem älteren Raspberry Pi 2 ist also möglich, aber spaßfrei.

Neben dem Raspberry wird ein externer Datenträger benötigt, der ausreichend Platz für die Mediensammlung bietet. Wenn Sie erst mit dem Aufbau einer Mediensammlung beginnen, achten Sie unbedingt darauf, eine externe Festplatte anzuschaffen, die mit einer externen Stromversorgung arbeitet. Grundsätzlich kann der Raspberry zwar externe Datenträger über den USB-Anschluss mit Strom versorgen, jedoch reicht die Leistung für einen zuverlässigen Dauerbetrieb von Festplatten nicht immer aus. Für die Ersteinrichtung ist außerdem der Anschluss von Tastatur, Maus und externem Bildschirm notwendig. Die spätere Verwaltung geschieht hingegen über einen beliebigen PC im Netzwerk im Browser.

Als Systembasis soll der Raspberry ein Raspbian erhalten. Sofern noch nicht geschehen, installieren Sie es zum Beispiel über Noobs (*www.raspberrypi.org/downloads/noobs/*), das Ihnen ja die Wahl lässt, noch weitere Systeme auf dem gleichen Computer einzusetzen. Ist ein installiertes Raspbian bereits seit einiger Zeit im Betrieb, ist es zu empfehlen, das System vor der Einrichtung des Plex-Servers auf den neuesten Stand zu bringen. Das erledigen Sie schnell in einem Terminal:

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

Um während der Installation sicher zu sein, mit dem korrekten Server zu kommunizie-

ren, soll eine HTTPS-Verbindung genutzt werden. Installieren Sie deswegen zur Sicherheit das entsprechende Paket:

```
sudo apt-get install apt-transport-
  https
```

Ist es bereits eingerichtet, erhalten Sie nach dem Aufruf des Kommandos nur die Rückmeldung, dass die Software bereits vorhanden ist. Dann brauchen Sie nichts weiter zu tun.

Plex-Server herunterladen: Die Plex-Macher bieten den Server für eine ganze Reihe von Plattformen an. Dazu gehören die drei großen Betriebssysteme für den PC, auch viele NAS-Systeme, allerdings nicht direkt der Raspberry Pi und dessen Prozessor. Der Entwickler Jan Friedrich stellt jedoch eine installierbare Variante für ARM-Prozessoren und Distributionen zur Verfügung, die auf Debian basieren. Dank seiner Arbeit kann der Plex-Server dann auf Raspberry und auf Odroid-Platinen laufen. Damit die Installation klappt, muss sein Repository als Paketquelle eingerichtet werden. Auch das erledigen Sie auf der Konsole. Zunächst fügen Sie den öffentlichen Schlüssel für die Paketquelle hinzu.

```
sudo su wget -O - https://dev2day.
  de/pms/dev2day-pms.gpg.key | apt-
  key add -
```

Sollten Sie hier eine Fehlermeldung erhalten, dann kann es sein, dass das Programm wget auf Ihrem System fehlt. Holen Sie das einfach per *apt install wget* nach. Jetzt wird das Repository eingerichtet. Im Terminal geben Sie dazu

```
echo "deb https://dev2day.de/pms/
  stretch main" | sudo tee /etc/apt/
  sources.list.d/pms.list
```

ein. Damit ist die Paketquelle eingerichtet. Statt „stretch“ funktioniert auch noch die ältere Vorgängerversion „wheezy“. Damit Sie die neue Quelle auch über den Paketmanager nutzen können, müssen Sie die Quellen auch mit

```
sudo apt-get update
```

aktualisieren.

Den Plex-Server installieren

Nachdem Sie alle Voraussetzungen abgeschlossen haben, können Sie an die eigentliche Einrichtung gehen. Führen Sie in der Konsole das Kommando

```
sudo apt install plexmediaserver-
  installer
```

aus. Sie erleichtern sich die spätere Arbeit bei der Konfiguration und Wartung des Systems, wenn Sie in den Optionen des Servers ein bereits vorhandenes Benutzerkonto des Raspberry als Administratorkonto hinterlegen. Öffnen Sie auf der Konsole mit dem Editor Nano die entsprechende Datei:

```
sudo nano /etc/default/
  plexmediaserver
```

Suchen Sie dort nach der Zeile mit dem Eintrag „PLEX_MEDIA_SERVER_USER=plex“ und ändern Sie „plex“ auf einen anderen Benutzernamen ab. Sie können auch den Standardbenutzer „pi“ verwenden. Dieser ist auf jedem Raspberry direkt nach der Installation des Betriebssystems vorhanden. Dann sollten Sie aber unbedingt dessen Standardpasswort verändern. Speichern Sie die Datei und beenden Sie Nano. Jetzt können Sie den installierten Server mit

```
sudo service plexmediaserver
  restart
```

neu starten.

Feste IP-Adresse zuweisen: Die Verwaltung des gesamten Systems erfolgt über das Netzwerk im Browser. Dafür ist es praktisch, wenn Sie sich nur eine IP-Adresse merken müssen, um das System zu erreichen. Eine feste Adresse können Sie sowohl Raspberry selbst oder in den Einstellungen des Routers hinterlegen. Letztgenannte Methode ist übersichtlicher, vor allem wenn Sie für mehrere Geräte feste Adressen verwenden. In der Fritzbox gehen Sie dazu auf „Heimnetz → Heimnetzübersicht → Alle Geräte“. Mit einem Klick auf „Details“ neben dem Eintrag des Raspberry rufen Sie den notwendigen Dialog auf. Hier aktivieren Sie einfach die Option „Diesem Netzwerkgerät immer die gleiche IPv4-Adresse zuweisen“.

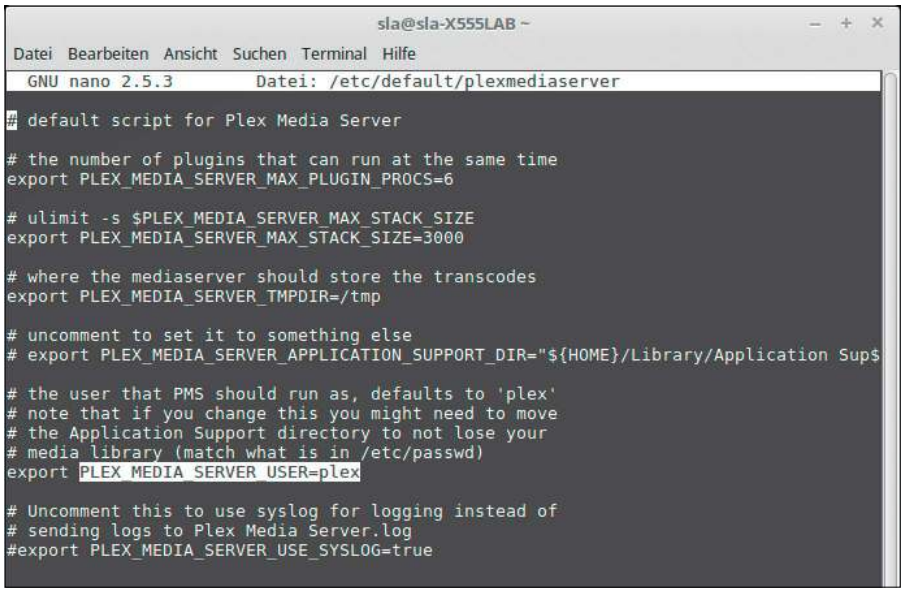
Wenn Sie die Adresse lieber auf dem Raspberry festlegen, öffnen Sie ein Terminal. Dort geben Sie

```
hostname -I
```

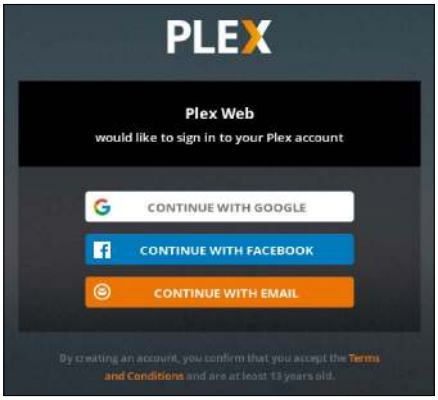
ein. Die angezeigte Adresse notieren Sie sich und öffnen mit

```
sudo nano /boot/cmdline.txt
```

die maßgebliche Konfigurationsdatei. An deren Ende fügen Sie eine neue Zeile nach dem Muster „ip=IP-Adresse“ ein – also etwa „ip=192.168.178.25“. Nach Speichern der Datei starten Sie mit „sudo reboot“ den Minirechner neu.

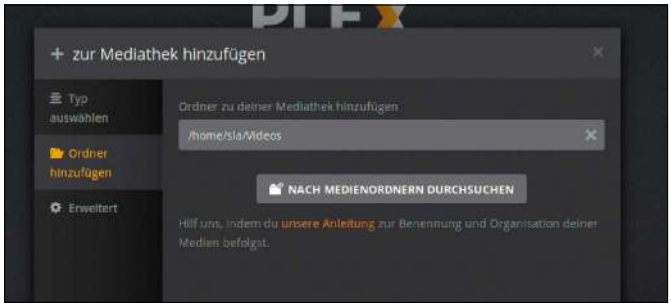


Um Komplikationen bei der Einrichtung zu vermeiden, ändern Sie den Nutzer in dieser Datei auf ein bereits bestehendes Konto des Raspbian-Systems ab.



Anmeldung ist Pflicht. Sie können ein Konto bei einem sozialen Netzwerk verwenden oder ein klassisches lokales Konto mit Benutzernamen und Passwort einrichten.

Weisen Sie dem Server einen individuellen Namen zu. So finden Sie ihn später einfacher in Ihren Abspielgeräten im Netzwerk.



Mediatheken entsprechen Verzeichnissen auf dem lokalen System. Treffen Sie Ihre Wahl und binden Sie eventuelle Netzwerkquellen vorher ein.

Den Plex-Server einrichten

Verbinden Sie die USB-Festplatte mit dem System, bevor Sie sich daran machen, eine Sammlung in Plex anzulegen. Es können auch Netzwerkfreigaben genutzt werden, allerdings müssen diese in das lokale Dateisystem des Raspbian-Systems eingebunden werden (entweder bei Bedarf manuell oder durch Einträge in die Datei „fstab").

Zur Konfiguration des Medienservers rufen Sie mit dem Browser die Oberfläche des Servers mit „http://IP-Adresse:32400/web/" auf. Wie Sie sehen, nutzt der Plex-Server den Port 32400. Falls Sie sich von einem Rechner in Ihrem Heimnetzwerk nicht anmelden können, blockiert wahrscheinlich die im Router eingebaute Firewall den Zugriff. In diesem Fall müssen Sie noch eine Portweiterleitung für diesen Port einrichten, die dann auf die IP-Adresse des Raspberry zeigt. Sie werden jetzt von der Startseite des Systems begrüßt. Sie können sich ein Konto per E-Mail-Adresse und Passwort einrichten oder Sie nutzen ein bestehendes Konto bei Google oder Facebook. Nach der Anmeldung gibt es eine kurze Anleitung und den Hinweis auf die Premiumfunktionen des Systems. Der Plex-Server funktioniert aber auch ohne die Freischaltung von kostenpflichtigen Funktionen. Ob Ihnen diese die Gebühr wert sind, können Sie später immer noch entscheiden. Der Einrichtungsassistent bittet Sie noch um die Eingabe eines Namens für den Server. Darüber können Sie ihn später in den zugreifenden Clientgeräten einfacher identifizieren.

Danach beginnen Sie damit, die Mediathek einzurichten, indem Sie auf „Mediathek hinzufügen" klicken. Entscheiden Sie sich für eine der angezeigten Kategorien und eine Sprache. Die Sprache ist insofern wichtig, als sich Plex ausgehend von den gefundenen Dateien und Titeln auf die Suche nach Metainformationen zu den Elementen der Sammlung macht. Außerdem können Sie den verschiedenen Mediatheken auch individuelle Namen zuweisen. Mit einem Klick auf „Weiter" gelangen Sie dann zur Auswahl des Medienordners, in dem sich die Stücke befinden. Sie können so viele Mediatheken (Ordner) anlegen, wie Sie möchten. Danach beginnt der Server, die Medieninhalte zu indizieren. Das kann, abhängig von der Menge der Medien, relativ lange dauern.

Wenn der Server nicht über das Netzwerk zu erreichen ist, müssen Sie noch eine Portweiterleitung einrichten. In den Optionen bietet das System auch gleich das passende Werkzeug an.

Fernzugriff einrichten

Für fast jedes Betriebssystem und auch für Minicomputer gibt es Clients für Plex, die sich mit dem Server verbinden, um Inhalte abzurufen. Klicken Sie auf das Werkzeugsymbol in der oberen Leiste, um die Einstellungen aufzurufen. Anschließend wechseln Sie in den Bereich „Server". Im lokalen Netzwerk ist der Client damit bereits mit der Plex-Mediathek des Servers verbunden und zeigt dessen Inhalte an. Im linken Menü finden Sie den Abschnitt „Fernzugriff". Eventuelle Probleme damit erkennen Sie an einem Ausrufezeichen neben dem Menüeintrag. Versuchen Sie bei Zugriffsproblemen zunächst, die Option „Öffentlichen Port manuell definieren" zu aktivieren. Danach klicken Sie auf „Erneut versuchen". Führt das nicht zum Erfolg, müssen Sie die Portweiterleitung im Router prüfen und dort UPnP aktivieren und Anfragen auf den Port weiterleiten. Die Besitzer aktueller Fritzboxen sind hier im Vorteil: In den Details eines Geräts in der „Heimnetzübersicht" gibt es eine Option, die selbständige Portfreigaben von Geräten erlaubt. Das sollte dann bereits genügen. Steht der Fernzugriff, steht dem Streamingvergnügen nichts mehr im Weg. ■

PC-WELT

Windows 10
Heimnetz ganz einfach!

Sonderheft
für nur
4,90 €

Gratis-Paket auf DVD:
120 Top-Programme
für das Heimnetz

Jetzt bestellen unter
www.pcwelt.de/windows 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 Windows 10 Heimnetz 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

Raspberry Pi als WLAN-Verstärker

Bei schwächelndem WLAN lässt sich die Reichweite des Funksignals vergrößern. Dafür gibt es Repeater und Access Points, jedoch kann diese Aufgabe auch ein Raspberry Pi mit dem Betriebssystem Raspbian erledigen.

Raspberry als Repeater oder Access Point: Der Raspberry 3 bringt einen WLAN-Chip schon mit. Bei älteren Modellen verwenden Sie einen WLAN-Stick am USB-Port.

VON THORSTEN EGGELING

Eine gute Verbindung zum WLAN-Router gibt es nur bei zentraler Aufstellung in Haus oder Wohnung. Massive Wände oder Metallteile können das Signal jedoch so weit dämpfen, dass es nicht in jeden Raum gelangt. Abhilfe schafft ein Raspberry Pi als WLAN-Verstärker, mit dem Sie die Abdeckung verbessern. Das bedeutet etwas Konfigurationsaufwand, den wir aber mit diesem Service deutlich reduzieren: **Alle Kommandozeilen und den Inhalt der Konfigurationsdateien** können Sie über *www.pc-welt.de/AEjbDf* herunterladen.

Repeater oder Access Point

Ein WLAN-Repeater empfängt Datenpakete vom Router und sendet diese per WLAN an andere Geräte weiter. Gemäß WLAN-Standard darf pro Kanal immer nur ein Teilnehmer senden. Deshalb kann der Repeater nicht gleichzeitig Daten an den Router und den Client übermitteln, wodurch sich die Transferrate halbiert. Sie werden die Reduzierung kaum bemerken, wenn es nur um Internetsurfen oder E-Mails geht. Beim Videostreaming oder dem Transfer großer Dateien sind die Einschränkungen jedoch spürbar. Mit zwei WLAN-Adaptern, die auf unterschiedlichen Kanälen mit 2,4 und fünf GHz arbeiten, kann es schneller gehen. Bei zahlreiche Funknetzen in der Nachbarschaft erhöht sich die Geschwindigkeit aber auch dadurch nicht deutlich. Bei der von uns vorgeschlagenen Konfiguration für den Raspberry Pi setzen wir daher nur einen WLAN-Adapter ein.

Ein WLAN-Access-Point ist per Ethernet-Kabel mit dem Router verbunden und leitet die Datenpakete per WLAN weiter. Hier steht immer die maximale WLAN-Leistung zur Verfügung. Der Nachteil: Sie müssen ein Ethernet-Kabel vom DSL-Router zum Raspberry Pi verlegen.

Raspberry Pi vorbereiten

Ein neuerer Raspberry Pi 3 ist für den Einsatz als Repeater oder Access Point geeignet, weil er von Haus aus WLAN und Ethernet mitbringt. Bei anderen Modellen schließen Sie einen WLAN-Adapter an den USB-Port an. Im Handel finden Sie den offiziellen Raspberry Pi USB Wi-Fi Dongle für knapp 20 Euro. Es funktionieren aber auch viele andere WLAN-USB-Adapter. Eine Übersicht lesen Sie unter *https://elinux.org/RPi_USB_Wi-Fi_Adapters*.

Raspbian installieren Sie – wenn noch nicht geschehen – am schnellsten über Noobs (*www.raspberrypi.org/downloads*). Eine ausführliche Anleitung liefert Ihnen *www.pc-welt.de/2261394*.

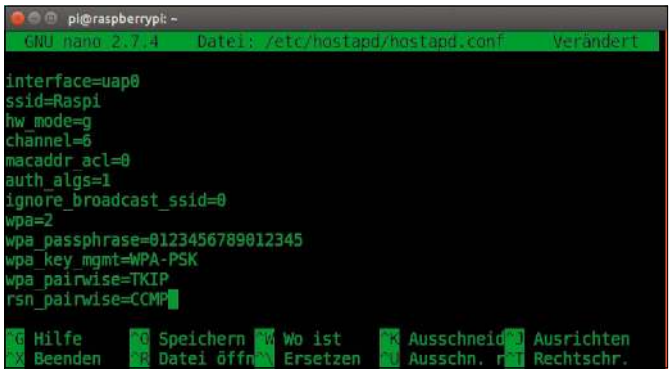
Prüfen Sie die Netzwerkkonfiguration des Raspberry Pi im Terminal:

```
ip address show
```

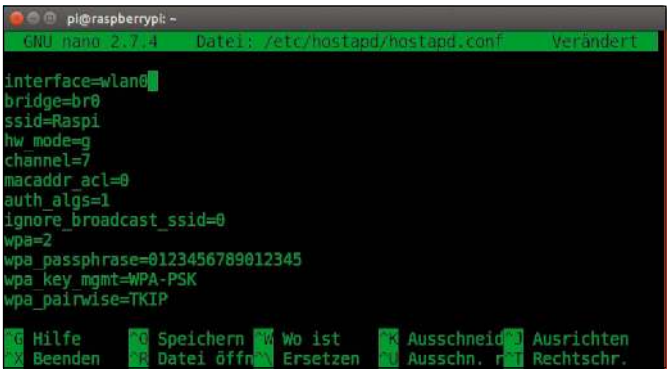
In der Ausgabe sollte neben dem Ethernet-Adapter „eth0“ auch der WLAN-Adapter „wlan0“ auftauchen. Abhängig von der Installationsart können die Bezeichnungen auch anders lauten. Verwenden Sie die ermittelten Namen für die nachfolgende Konfiguration.

Konfiguration eines WLAN-Repeaters

Die Basiskonfiguration des Netzwerks erfolgt bei Raspbian Stretch über die Datei „/etc/dhcpcd.conf“ und das Startsystem systemd. Die in früheren Versionen genutzte Konfigurationsdatei „/etc/network/interfaces“ ist noch vorhanden, hat aber keine Funktion mehr. Für unsere Zwecke ist es nötig, die bisherige Methode der Konfiguration zu verwenden, weil sie mehr Optio-



Konfiguration als Repeater: In der „hostapd.conf“ legen Sie SSID, den WPA-Schlüssel, die Netzwerkschnittstelle und andere Verbindungsparameter fest.



Konfiguration als Access Point: Die „hostapd.conf“ für unterscheidet sich nur beim Namen der Schnittstelle und durch den zusätzlichen Eintrag „bridge=br0“.

nen bietet. Installieren Sie in einem Terminalfenster zuerst die erforderlichen Pakete:

```
sudo apt install hostapd dnsmasq
```

Danach führen Sie die folgenden zwei Befehlszeilen aus:

```
sudo mv /etc/dnsmasq.conf /etc/
 dnsmasq.conf.orig
sudo nano /etc/dnsmasq.conf
```

Tragen Sie im Editor diese Zeilen ein:

```
interface=lo,uap0
no-dhcp-interface=lo,wlan0
dhcp-range=192.168.2.100,192.168.
 2.200,12h
```

Damit richten Sie einen DHCP-Server ein, der an die WLAN-Clients IP-Nummern aus dem hinter „dhcp-range“ definierten Bereich vergibt. Speichern Sie die Änderungen (Strg-O) und verlassen Sie dann den Editor mit (Strg-X).

Erstellen Sie die Konfigurationsdatei für hostapd folgendermaßen

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

und tragen Sie die zwölf Zeilen ein, wie sie in der Abbildung oben zu sehen sind. Beachten Sie die Variablen „ssid=“ (Name für das WLAN) und „wpa_passphrase=“ (Zugangspasswort), die Sie nach eigenen Vorstellungen anpassen müssen.

Danach bearbeiten Sie die Netzwerkkonfiguration „/etc/network/interfaces“. Tragen Sie dort diese acht Zeilen ein:

```
auto eth0
iface eth0 inet dhcp
auto wlan0
iface wlan0 inet dhcp
wpa-conf /etc/wpa_supplicant/wpa_
 supplicant.conf
auto uap0
iface uap0 inet static
address 192.168.2.1/24
```

Die Datei „/etc/wpa_supplicant/wpa_supplicant.conf“ sollte vorhanden sein, wenn Sie bereits den Schlüssel für eine WLAN-Verbindung bei der Nutzung über den Desktop festgelegt haben. Andernfalls erstellen Sie die Datei mit folgendem Inhalt:

```
ctrl_interface=DIR=/var/run/wpa_
 supplicant GROUP=netdev
update_config=1
country=DE
network={
ssid="OpenWrt_2"
psk="1234567890123456"
}
```

Hinter „psk=“ tragen Sie das Passwort für Ihr WLAN ein.

Erstellen Sie eine Datei für die Konfiguration und den Start der Dienste:

```
sudo nano /usr/local/bin/
 hostapdstart
```

Dort tippen Sie diese sechs Zeilen ein:

```
iw dev wlan0 interface add uap0 type
 __ap
service dnsmasq restart
sysctl net.ipv4.ip_forward=1
iptables -t nat -A POSTROUTING -s
 192.168.2.0/24 ! -d 192.168.2.0/24
 -j MASQUERADE
ifup uap0
hostapd /etc/hostapd/hostapd.conf
```

Machen Sie die Datei ausführbar:

```
sudo chmod 667 /usr/local/bin/
 hostapdstart
```

Bearbeiten Sie die Datei „/etc/rc.local“ und tragen Sie die Zeile

```
hostapdstart >1&
```

vor der Zeile „exit 0“ ein.

Abschließend deaktivieren Sie die unnötigen Dienste hostapd und dhcpcd:

```
sudo systemctl disable hostapd
sudo systemctl disable dhcpcd
```

Starten Sie dann den Raspberry neu (*sudo reboot*). In Ihrem Netzwerk ist jetzt das neue WLAN zu sehen, Sie können das Internet nutzen und auf Freigaben zugreifen.

Access Point konfigurieren

Bei einem Access Point ist die Konfiguration einfacher, weil sich hier eine Netzwerkbrücke nutzen lässt. Installieren Sie diese Pakete:

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

Deaktivieren Sie dhcpcd für „eth0“ und „wlan0“. Dazu öffnen Sie die Konfigurationsdatei

```
sudo nano /etc/dhcpcd.conf
```

und tragen am Ende der Datei diese zwei Zeilen nach:

```
denyinterfaces eth0
denyinterfaces wlan0
```

Führen Sie diese vier Befehle aus:

```
sudo systemctl stop hostapd
sudo brctl addbr br0
sudo brctl addif br0 eth0
sudo nano /etc/network/interfaces
```

Tragen Sie im Editor nano nun die folgenden drei Zeilen ein:

```
auto br0
iface br0 inet manual
bridge_ports eth0 wlan0
```

Erstellen Sie dann die Konfigurationsdatei „/etc/hostapd/hostapd.conf“ mit dem gleichen Inhalt wie im vorherigen Punkt beschrieben, aber mit diesen Änderungen:

```
interface=wlan0
bridge=br0
```

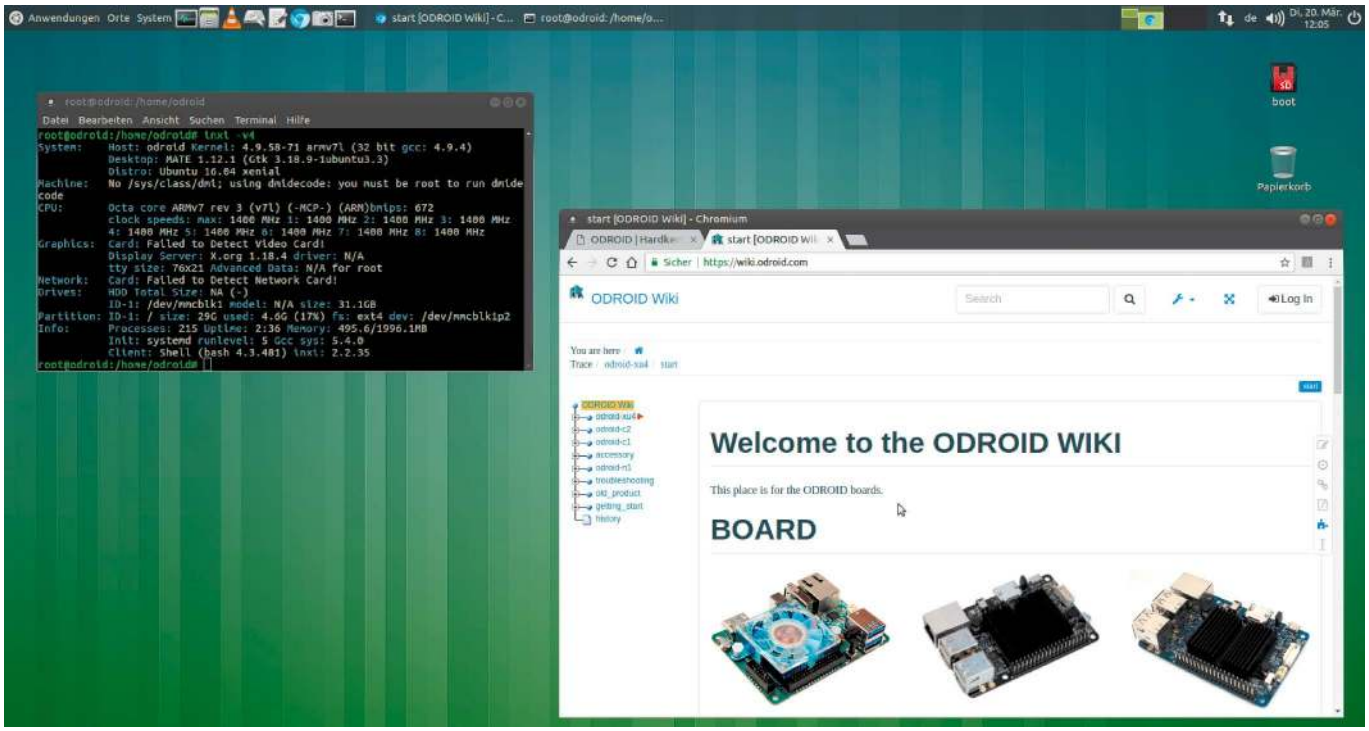
Damit der hostapd-Dienst die Datei berücksichtigt, tragen Sie in die Datei „/etc/default/hostapd“ diese Zeile ein:

```
DAEMON_CONF="/etc/hostapd/
 hostapd.conf"
```

Starten Sie das System neu. Der neue WLAN-Access-Point steht anschließend in Ihrem Netzwerk zur Verfügung. ■

Die Odroid-Miniserver

Seit fünf Jahren versuchen zahlreiche Platinenrechner, sich neben dem erfolgreichen Raspberry Pi zu positionieren. Die Odroid-Familie war und ist dabei besonders umtriebig. Dieser Beitrag bringt einen Überblick über die Minirechner aus Südkorea.



VON HERMANN APFELBÖCK

Wer meint, die koreanische Firma Hardkernel mit ihren diversen Odroid-Produkten („Open Droid") sei ein typischer Raspberry-Trittbrettfahrer, liegt mindestens teilweise falsch. Die Firma gibt es schon länger und ihr erster Platinenrechner „Odroid-PC" datiert aus dem Jahr 2011, also ein Jahr vor dem ersten Raspberry Pi. Richtig ist aber, dass Hardkernel früh und umtriebig auf den Erfolg des Raspberry Pi reagiert hat und seit 2012 die komplette Produktpalette als Raspberry-Konkurrenz ausrichtet. Der Raspberry-Boom veranlasste Hardkernel zur Fokussierung auf Miniserver und Platinenrechner. Die an sich vernünftige Kernstrategie war offenbar immer, für moderat höhere Preise deutlich mehr Leistung anzubieten als der Raspberry Pi. Die zahlreichen Odroid-Varianten der Jahre 2012 bis 2015 zeugen allerdings von hektischer Betriebsamkeit, die beim Konsumenten eine gewisse Ratlosigkeit hinterlässt, inwiefern sich die Produkte unterscheiden. Nachhaltigkeit und Weitblick war hier nicht zu erkennen und diverse Odroid-Projekte kamen und starben wie Eintagsfliegen: Die sehr lange Spalte „Obsolete products" auf der Herstellerseite *www.hardkernel.com/main/products/prdt_info.php* spricht für sich. Inzwischen hat Hardkernel seine Produktpalette konsolidiert.

Der Durchblick ist heute einfacher, verlangt aber immer noch genaueres Hinsehen. Dies sollen die nachfolgenden Seiten leisten. Die aktuell noch gepflegten Odroid-Platinen verdienen diese Übersicht, da sie qualitativ und zumeist auch in der Komponentenzusammensetzung überzeugen. Eine Produktübersicht des Herstellers bietet die oben genannte Hardkernel-Webseite. Deutscher Vertreiber für alle Odroid-Platinen und Odroid-Zubehör ist Pollin (*www.pollin.de*).

Odroid XU4: Das aktuelle Spitzenmodell

Die Platine Odroid XU4 ist nicht nur das aktuelle Spitzenmodell der Hardkernel-Palette, sondern zugleich die Basis für die Varianten HC1, HC2 und MC1. Der Achtkerner arbeitet mit zwei Quadcore-CPUs, wobei je nach Auslastung der Vierkerner Cortex A15 mit zwei GHz oder der sparsamere Vierkerner Cortex A7 mit 1,4 GHz zum Zuge

Quelle: pollin.de

Odroid XU4 mit und ohne Lüfter: Die flexible Platine bleibt mit Netzteil und Gehäuse knapp unter 100 Euro. Wer einen lautlosen Job erwartet, greift zur XU4Q-Variante mit passivem Kühlkörper.

Quelle: pollin.de

Odroid HC1 („Home Cloud"): HC1 und HC2 können am SATA-Port genau eine Festplatte aufnehmen. Wo dies genügt, bieten die HC-Platinen ein aufgeräumtes Mini-NAS.

kommt. Mit zwei GB DDR3-RAM ist die Platine für den Serverbetrieb mehr als ausreichend bestückt.

Entscheidender noch für den Datendurchsatz ist die stimmige Kombination von USB 3.0 (zweimal) mit echtem Gigabit-Ethernet. Die damit theoretisch möglichen 1000 MBit/s (125 MB/s) erreicht die Platine zwar nicht, aber 80 bis 90 MB/s sind maximal möglich. Damit gerät auch das Hantieren mit ISO-Abbildern und Filmen zur flotten Aufgabe. Als Boot- und Systemmedium kommen sowohl die typische Micro-SD-Karte als auch eine eMMC-Karte infrage. Die Auswahl des Mediums erfolgt über einen kleinen Schalter auf der Platine. Für Erweiterungen und Bastellösungen gibt es zwei Pin-Anschlüsse (30 plus 12), die allerdings nicht Raspberry-kompatibel sind und daher eigene Produktlösungen benötigen. Die Platine verbraucht unter Volllast bis zu 11 Watt, im Normalbetrieb etwa vier bis acht Watt.

Odroid XU4 als Desktop: Mit den genannten Spezifikationen ist die Platine ein idealer Datenserver für das private Netzwerk und Home Office. CPU, RAM, Mali-GPU T628 MP6 und HDMI-Port scheinen auch zum Einsatz als Desktop-Zweitrechner einzuladen, aber hier muss man nach unserer Erfahrung einige Einschränkungen akzeptieren. Das von uns getestete Ubuntu Mate 16.04.3 ist als Ersatzsystem durchaus akzeptabel, läuft aber nicht wirklich flüssig. Die Ladezeiten von großen Programmen wie Browser oder Libre-Office-Komponenten sind unbefriedigend. Alles, was mit grafischen Fenstern zu tun hat, reagiert etwas zäher als vom PC gewohnt, mit gelegentlichem Verschwinden des Mauszeigers und sporadischen Artefakten am Bildschirm. Selbst der deutlich schwächere Raspberry schlägt sich hier besser. Da die Hardware des Odroid XU4 an sich eine bessere Leistung verspricht, liegt es vermutlich an der mangelhaften Treiberanpassung.

Lüfter oder Kühlkörper: Das Kühlkonzept des Odroid XU4 wurde seit seinem Erscheinen 2015 vielfach kritisiert. Von Platinenrechnern erwarten die Kunden lautlosen, lüfterlosen Betrieb. Der XU4 kommt aber standardmäßig mit einem Lüfter, der seine kleinen Maße mit hoher Drehzahl ausgleicht. Im Serverbetrieb läuft er vor allem bei größeren Datentransfers und beim Booten, im Desktopbetrieb sehr häufig. Der Lüfter ist nicht laut, aber aufgrund der hohen Frequenz unüberhörbar. Beim Einsatz als Medienserver im Wohnzimmer kann das je nach Anspruch durchaus stören.

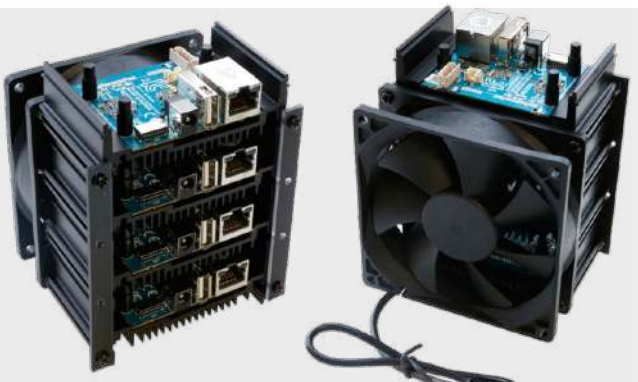
Hardkernel hat inzwischen doppelt reagiert: Erstens gibt es für Neukunden die Variante Odroid XU4Q mit einem passiven Kühlkörper („Q" für „quiet"). Die ist etwas günstiger als die Variante mit Lüfter, aber etwas leistungsärmer, weil die XU4 hier häufiger auf die schwächere A7-CPU schaltet. Wer bereits einen XU4 besitzt, kann den Lüfter durch den passiven Kühlkörper ersetzen, der mittlerweile als Einzelzubehör für etwa acht Euro verkauft wird.

X86 UND ARM: CPU-VERGLEICH AM BEISPIEL ODROID XU4

Die Octacore-CPU des Odroid XU4 mit 2 GHz klingt nach mächtig viel Leistung. Jedoch handelt es sich um zwei Quadcore-ARM-Einheiten, die je nach Anforderung zur schnelleren oder stromsparenderen umschalten. Vor allem aber darf man generell die Taktraten und die Kernzahlen von ARM-Prozessoren nicht annähernd den x86-CPUs von PCs und Notebooks gleichsetzen. Die kleine Tabelle zeigt, dass die Intel-Atom-CPU eines zehn Jahre alten Netbooks immer noch knapp vor der ARM-Quadcore-CPU eines Raspberry 3 liegt. Die Platine Odroid XU4 lässt diese Netbook-CPU zwar deutlich hinter sich, kommt aber nicht annähernd an Notebook- und PC-Prozessoren heran. Unser Vergleich wurde mit Sysbench auf der Kommandozeile ausgeführt.

Gerät	CPU-Architektur	Prozessor	Sysbench*
PC	x86	Intel i7-2600 Quad (3,4 GHz)	2,46
Neueres Notebook	x86	Intel i5-3320 Dual (2,6 GHz)	3,12
Älteres Notebook	x86	AMD Phenom Dual (3,0 GHz)	10,34
Odroid XU4	ARM	Cortex A7/A15 Octo (1,4/2,0 GHz)	24,24
Altes Netbook	x86	Intel Atom N270 (1,6 GHz)	45,26
Raspberry Pi 3	ARM	Cortex A53 Quad (1,2 GHz)	46,43
Raspberry Pi 2	ARM	Cortex A7 Quad (0,9 GHz)	77,23

* kleiner ist schneller



Quelle: hardkernel.com

Odroid MC1 („My Cluster One“):
Es handelt sich um vier gestapelte, abgespeckte XU4-Platinen, die durch Clustersoftware zu einer Recheneinheit gekoppelt werden.

Quelle: hardkernel.com

Odroid N1 ab Sommer 2018:
Dieser Minirechner übertrifft das bisherige Spitzenmodell XU4 noch einmal in allen Komponenten. Zudem gibt es zwei schnelle SATA-3-Anschlüsse.

Preis und Ausstattung: Der Odroid XU4 kostet etwa 80, der lüfterlose XU4Q circa 75 Euro (*www.pollin.de*). Das sind Preisangaben, die allerdings so nicht realistisch sind: Denn dafür gibt es nur die pure Platine ohne Netzteil, ohne Gehäuse. Mit Gehäuse (acht Euro) und Netzteil (zehn Euro) liegt man dann bei knapp 100 Euro Gesamtkosten.

Odroid HC1/HC2: Kleine Homeserver

„HC“ steht für „Home Cloud“. Diese beiden Odroid-Varianten basieren auf dem Modell XU4 und sind hinsichtlich CPU, GPU, RAM und Gigabit-Ethernet identisch ausgestattet. Als Betriebssystem kommt daher alles in Betracht, womit auch der XU4 läuft. Statt schnellem USB 3.0 (nur einmal USB 2.0) gibt es eine SATA-3-Schnittstelle für eine Festplatte oder SSD, die ähnlich typischen NAS-Geräten direkt in das Alugehäuse eingeschoben und dadurch angeschlossen wird. HC1 und HC2 fokussieren ganz klar auf einen kleinen, schnellen Netzwerkspeicher für private Zwecke: Klein, weil nur ein SATA-Anschluss vorliegt – schnell, weil die Kombination SATA und Gigabit-LAN noch etwas mehr Tempo liefert als die Kombination mit USB 3.0. **Achtung:** HC1 und HC2 haben kein HDMI oder sonstigen Monitoranschluss: Das System kann nur über das Netzwerk mit SSH oder Nginx/Apache-Server (etwa mit dem NAS-System Open Media Vault) erreicht und verwaltet werden.

Preis und Ausstattung: Die lüfter- und lautlosen HC1 und HC2 kosten circa 60 und 65 Euro. Der einzige Unterschied der beiden Varianten ist das Alugehäuse, das beim kleinen HC1 nur ein 2,5-Zoll-Laufwerk, beim HC2 auch eine größere 3,5-Zoll-Festplatte aufnimmt. Das Gehäuse ist im Preis inbegriffen, das unentbehrliche Netzteil (circa acht Euro) beim Hauptvertreiber Pollin hingegen nicht.

Odroid MC1: Rechenknecht ohne Schnittstellen

„My Cluster One“ (MC1) ist kein Produkt für Normalverbraucher. Das Gehäuse mit großem Lüfter stapelt vier abgespeckte Odroid XU4 zu einem Rechnercluster. Die vier Platinen besitzen lediglich Gigabit-Ethernet und einmal USB 2.0. Damit ist weder ein Serverdienst realistisch noch ein Monitoroutput möglich. Zum Rechnercluster wird MC1 nicht direkt über Gehäuseanschlüsse, sondern über das Netzwerk. Dabei übernimmt eine Platine die Masterrolle, die drei übrigen dienen als Nodes. Anleitungen zur nicht trivialen Einrichtung bietet unter anderem das hauseigene Odroid-Magazine (*https://magazine.odroid.com/article/odroid-mc1-docker-swarmgetting-started-guide*). Der circa 260 Euro teure vier-Platinen-Cluster kann dann etwa komplexe mathematische Berechnungen erledigen, und dies schneller als vergleichsweise teure x86-CPUs.

Odroid N1: Das künftige Spitzenmodell

Mit einem Sechskerner, der noch leistungsstärker ausfällt als die CPU des XU4, ferner

NEU: DER RASPBERRY PI 3 B+

Quelle: pollin.de

Mitte März hat der Raspberry ein Upgrade erhalten. Das Modell Raspberry Pi 3 B+ ist im einschlägigen Elektronikhandel bereits erhältlich, zum üblichen Preis von knapp 40 Euro. Der Takt des Quadcore-Prozessors ist von 1,2 auf 1,4 GHz erhöht. Entscheidender sind aber die Neuerungen beim Funkmodul und beim Ethernet-Port: Der Raspberry funkt nun schneller nach dem aktuellen 802.11ac-Standard und neben dem bisherigen 2,4-GHz- auch im 5-GHz-Frequenzbereich. Ebenso bemerkenswert ist der neue Gigabit-Ethernet-Port: Das ist zweifellos die Komponente, die sich Raspberry-Kunden seit Jahren am meisten wünschen. Allerdings handelt es sich um einen Kompromiss, der nicht alle zufriedenstellen wird: Da die Daten vom Ethernet-Anschluss über die USB-2.0-Schnittstelle laufen, ist der Durchsatz von 1000 MBit/s auf die maximalen 320 MBit/s von USB 2.0 gedrosselt. Im Alltag wird der Raspberry mit dieser Konstellation erfahrungsgemäß kaum mehr als 250 MBit/s schaffen, also etwa 30 MB/s. Das ist gegenüber dem bisherigem Fast Ethernet mit 100 MBit/s (etwa 12,5 MB/s) ein signifikanter Schub, aber natürlich nicht das erhoffte Gigabit-LAN. Echtes Gigabit-Ethernet wird es frühestens beim Raspberry 4 geben, der voraussichtlich 2019 erscheinen wird.

Quelle: pollin.de

Odroid C1+: Für diese Platine sind die Tage wohl gezählt, nachdem das jüngste Raspberry-Modell 3 B+ leistungstechnisch praktisch gleichzieht.

mit vier GB RAM, einer neueren Mail-GPU (T860MP4) und zwei SATA-3-Anschlüssen ist das nächste Spitzenmodel Odroid N1 angekündigt. Die beiden USB-3.0-Ports und das Gigabit-Ethernet wie beim Odroid XU4 wird diese Platine ebenfalls mitbringen und damit weiter Richtung Highspeed-NAS gehen. Die SATA-Ports sollen einen Durchsatz von mehr als 400 MB/s erreichen, was dann allerdings nur den Transfer zwischen zwei angeschlossenen Platten optimieren wird, denn via Gigabit-Ethernet ist ja bei 125 MBit/s Schluss. Mit Netzteil und Gehäuse wird der Odroid N1 etwa 120 Euro kosten. Die Platine kommt demnächst, voraussichtlich Juni/Juli 2018, auf den Markt.

Odroid C1+ und C2: Die Raspberry-Konkurrenz

Die größeren C-Varianten verstehen sich als etwas leistungsstärkere Raspberry-Konkurrenten, können aber spätestens jetzt neben dem eben erschienenen Raspberry 3 B+ kaum noch bestehen. Odroid C1+ hat bei CPU (Quadcore, 1,5 GHz), GPU (Mali 450) und RAM (1 GB) keine überzeugenden Vorteile gegenüber dem Raspberry und der Wert des Gigabit-Ethernet wird durch die vier USB-2.0-Ports relativiert, die den Durchsatz auf 25 bis 30 MB/s ausbremsen. Die I/O-Leistung ist damit vergleichbar mit dem jüngsten Raspberry (siehe Kasten auf Seite 98). In dieser Situation wird man besser zum Original greifen. Der Odroid C2 hat zwar einen moderneren Prozessor (Cortex-A53) und zwei GB RAM, die Einschränkungen bei der I/O-Leistung gelten aber auch hier.

Preis und Ausstattung: Odroid C1+ und C2 kosten 45 und knapp 60 Euro. Diese Preise bei Pollin beinhalten weder Netzteil (fünf Euro) noch Gehäuse (sieben Euro).

Odroid C0: Nackte Bastlerplatine

Odroid C0 ist ein extrem reduzierter C1+ und systemkompatibel mit diesem. Anders als der C1+ richtet sich die kleinste C-Variante aber ausschließlich an Elektronikbastler. Abgesehen vom HDMI-Ausgang ist die Platine praktisch unbestückt. Ethernet gibt es nicht, USB-Ports und GPIO-Pins können von Bastlern bei Bedarf manuell nachgerüstet werden. Die 16-Gramm-Platine bietet für circa 35 Euro praktisch nur die CPU (ARM Cortex-A5, Quadcore mit 1,5 GHz), Mali-GPU, HDMI-Port und einem GB DDR3-RAM.

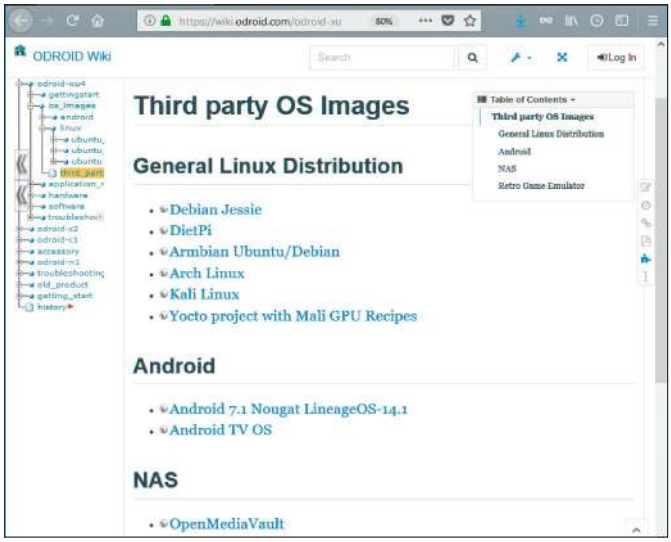
Alle Odroids: WLAN gibt es nur als Extra

Falls Sie bei obigen Beschreibungen den Hinweis auf WLAN vermisst haben: Die Odroid-Platinen haben tatsächlich allesamt keinen Funkchip an Bord. Das ist letztlich konsequent, weil die typischen Serveraufgaben eines XU4 oder HC1 nur mit Ethernet Sinn machen. Wer trotzdem Wi-Fi benötigt, muss dies über einen Wi-Fi-USB-Dongle nachrüsten. Die Hardkernel-eigenen Sticks sind allerdings in Deutschland kaum zu bekommen und müssten direkt aus Südkorea bestellt werden. Jedoch werden die Platinen auch jeden anderen Linux-kompatiblen Wi-Fi-USB-Dongle wie den Edimax EW-7811UN, Asus N10 Nano oder CSL 300 akzeptieren. Der uns zufällig vorliegende Hercules 300 N mini funktionierte ebenfalls auf Anhieb.

Auswahl der Betriebssysteme

Für alle Odroid-Platinen gibt es ordentliche Auswahl an Linux- und Android-Betriebssystemen, die Sie nur herunterladen und mit den üblichen Werkzeugen auf Micro-SD schreiben müssen (Etcher, dd, Win 32 Disk Imager). Der Weg zu den passenden Systemen ist aber nicht optimal organisiert, weil man auf der Hersteller-Hauptseite *www.hardkernel.com* nicht fündig wird. Anlaufstelle ist vielmehr das Wiki *https://wiki.odroid.com*, das auch über die Hauptseite erreichbar ist (wenn man weiß, wo man hinmuss).

Hier finden Sie in der linken Spalte die Platinenmodelle, unter dem einzelnen Modell jeweils den Eintrag „os_images“. Hier erscheinen dann die offiziellen Android- und Linux-Images, ferner inoffizielle „Third party OS images“. Mit den Hardkernel-Images sind Sie auf der sicheren Seite, jedoch lohnt sich unbedingt auch die Durchsicht der inoffiziellen Systeme: Darunter befinden sich interessante Spezialsysteme wie Libre Elec, Open Media Vault, Volumio, Kali Linux oder Diet Pi. ■



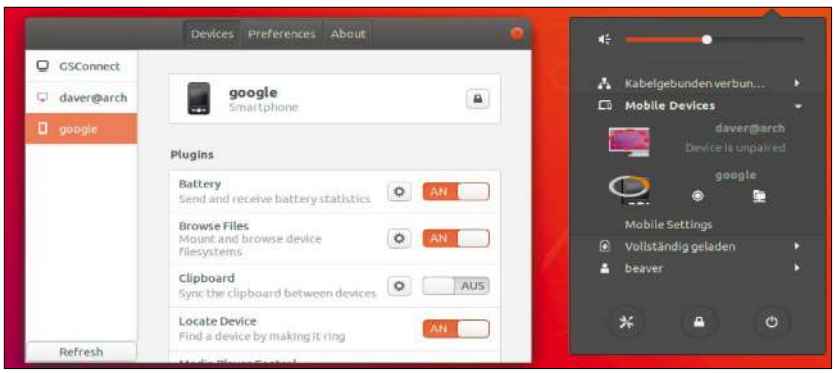
Betriebssysteme für Odroid-Platinen: Der schnellste Weg zum passenden System führt über das Wiki *https://wiki.odroid.com*.

Tipps zu Gnome, KDE, Mate & Co.

Nachdem Ubuntu 18.04 Gnome als primäre Arbeitsumgebung präsentiert, bekommt Gnome wieder viel Aufmerksamkeit: KDE-Connect, die Schnittstelle zur Anbindung von Android-Smartphones, kommt nun mit neuen Erweiterungen auf den Gnome-Desktop.

Smartphones: KDE Connect für Gnome

Die Anbindung von Android-Smartphones über KDE Connect hat der KDE-Desktop anderen Arbeitsumgebungen voraus. Aber nicht jeder will wegen des einfacheren Zugriffs auf Android-Geräte gleich zu KDE wechseln. Das ist inzwischen auch nicht mehr unbedingt nötig: Eine Erweiterung für Gnome holt die Funktionen von KDE Connect auf den Gnome-Desktop.



Verbindung zu Android-Geräten unter Gnome: Die Erweiterung Gsconnect bindet Smartphones und Tablets mit KDE-Connect ein und vereinfacht den Dateiaustausch per WLAN.

Während sich die KDE-Bibliotheken von KDE Connect auch unter Gnome um die Verbindung zum Android kümmern, integriert die neue Gnome-Erweiterung Gsconnect in die Desktopumgebung. Der Aufbau verlangt etwas Bastelei, läuft dann aber zuverlässig. Zu beachten ist, dass bei der Installation von KDE-Connect unter Gnome zahlreiche zusätzliche Pakete als Abhängigkeiten nötig sind. Die folgende Anleitung zeigt die Einrichtung im neuen Ubuntu 18.04:

1. Die grundlegenden KDE-Bibliotheken installiert folgendes Terminalkommando:

```
sudo apt-get install
  kdeconnect
```

Der Umfang der neuen Pakete umfasst rund 190 MB.

2. Die Gnome-Erweiterung Gsconnect liegt im offiziellen Verzeichnis unter *https://extensions.gnome.org/extension/1319* bereit. Bevor man hier aber etwas tun kann, ist es nötig, den Webbrowser in Ubuntu 18.04 fit für die Installation von Gnome-Extensions zu machen. Zuerst verlangt Firefox nach der Installation des angebotenen Firefox-Add-ons von *https://extensions.gnome.org* oder auch von *https://addons.mozilla.org/en-US/firefox/addon/gnome-shell-integration*. Damit nicht genug: Der Gnome-Desktop selbst braucht auch noch die neue Komponente chrome-gnome-shell als Ergänzung: Mit

```
sudo apt-get install
  chrome-gnome-shell
```

im Terminal ist die Bibliothek aber schnell nachgerüstet. Nach einem Neustart des Firefox ist der Extensions Service uneingeschränkt benutzbar und die Aktivierung einer Gnome-Erweiterung wie Gsconnect gelingt dort per Klick auf den angezeigten Kippschalter.

Zwingend nötig ist der Zugang via Firefox jedoch unter Ubuntu 18.04 nicht mehr: Gsconnect und andere Gnome-Erweiterungen sind auch im Softwarecenter (gnome-software) unter „Erweiterungen → Shell-Erweiterungen“ zu erreichen.

3. Auf dem Android-Gerät muss die zugehörige App von KDE-Connect installiert sein. Diese gibt es ganz offiziell über Google Play (*https://goo.gl/vM5ERh*).

4. Im oberen Gnome-Panel richtet sich Gsconnect mit einem neuen Symbol ein und zeigt dort sein Untermenü „Mobile Devices“ an. Zuerst muss der Linux-Rechner mit dem Android-Gerät im WLAN verbunden werden. Dazu schickt man in der Android-App eine Anforderung an den PC und bestätigt diese dort.

5. Nachdem die Verbindung per WLAN zum Android-Gerät steht, arbeiten die Funktionen von KDE-Connect über Gsconnect. Es handelt sich um einzelne Module, die man über einen Klick auf das Gerätesymbol in der Erweiterung aktiviert: Das Modul „Share“ kann Dateien zwischen Linux-PC und Android-Gerät empfangen und senden. Der Punkt „Browse Files“ öffnet eine Verbindung zum Smartphone im Dateimanager Nautilus. Außerdem gibt es eine Batterieanzeige, eine Klingelfunktion zum Finden verlegter Smartphones, eine gemeinsame Zwischenablage und eine Fernsteuerung des Mauszeigers vom Touchscreen des Android-Geräts aus. **-dw**

Anwendungsmenü: Öffnen per Windows-Taste

Einige Desktopumgebungen wie KDE und Mate öffnen auf den Druck der Windows-Taste („Super"-Taste) ihr Anwendungsmenü. Standard ist das jedoch nicht: Die Desktopumgebungen XFCE und LXDE reagieren beispielsweise nicht auf die Windows-Taste.

Einige Desktopumgebungen liefern keine eigene Möglichkeit, das Anwendungsmenü mit der Windows-Taste zu öffnen. Das kleine Programm Ksuperkey hilft weiter.

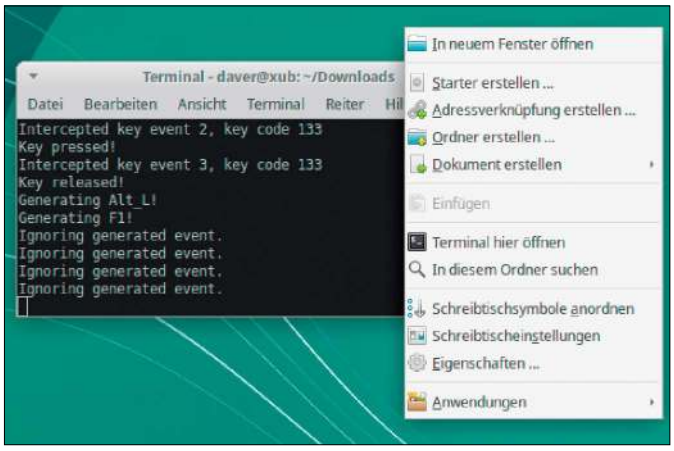
Ursprünglich war das Tool nur als Ergänzung für KDE gedacht. Es funktioniert aber mittlerweile zusammen mit allen tonangebenden Linux-Desktops. Für alle wichtigen Linux-Distributionen gibt es fertige inoffizielle Pakete, so dass die Installation nicht schwerfällt. Die Paketquellen für die verschiedenen Distributionen sind unter *https://www.linux-apps.com/p/1081256* aufgelistet.

Für die Varianten von Ubuntu 18.04 gab es zum Redaktionsschluss noch keine Pakete, allerdings funktioniert das Paket für Version 16.04 auch noch in der neuen Ubuntu-Version. Nach dem Download des passenden Pakets von *https://launchpad.net/~mehanik/+archive/ubuntu/ksuperkey/+packages* für 32 Bit oder 64 Bit installiert es dann im Terminal folgender Befehl:

```
sudo apt install ./
  [Paketname].deb
```

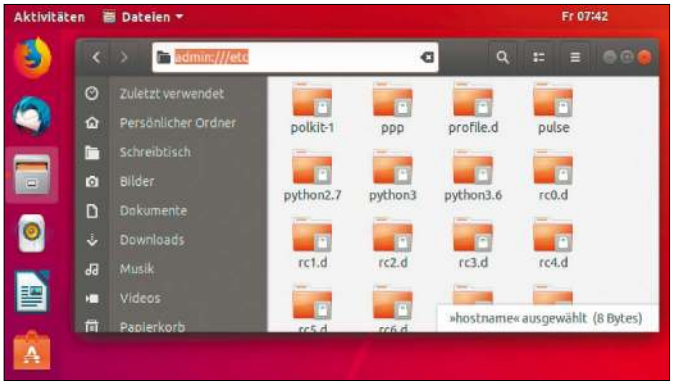
Diese Installation über apt sorgt dafür, dass eventuell vorhandene Abhängigkeiten zu anderen Paketen erfüllt werden. Damit apt lokal abgelegte DEB-Pakete installiert, erwartet es immer eine Pfadangabe vor dem Paketnamen, die in diesem Fall mit „./" das aktuelle Verzeichnis angibt.

Ksuperkey ist ein Hintergrundprogramm, das auf Tastatureingaben wartet und in der Standardkonfiguration den Druck auf die Windows-Taste abfängt und als Kombination Alt-F1 an den Desktop weitergibt. Denn diese Tastenkombination öffnet das Anwendungsmenü in den meisten Desktopumgebungen. Um Ksuperkey in Gang zu setzen, rufen Sie das Tool über den Ausführen-Dialog oder im Terminal mit *ksuperkey* auf. Soll das Programm stets zusammen mit dem Desktop starten, benötigt es einen Autostart-Eintrag. In XFCE unter Xubuntu sind eigene Autostart-Einträge über „Einstellungen → Sitzungen und Startverhalten → Automatisch gestartete Anwendungen" definierbar. LXDE unter Lubuntu hat unter „Einstellungen → Default applications for LXSession → Autostart" einen entsprechenden Konfigurationsdialog. **-dw**



Ksuperkey in Aktion: Das kleine Tool läuft im Hintergrund und fängt einen Druck auf die Windows-Taste ab, um hier in XFCE das Anwendungsmenü zu öffnen.

Gnome: Grafische Programme als root



Gnome-Programme mit root-Recht: Das neue Präfix „admin://" dient im Dateimanager, im Texteditor Gedit und in Dateidialogen zum Öffnen von Systemdateien.

Der Wechsel zu Wayland als Displayserver von Gnome bringt auch einige Änderungen in der Bedienung. So gibt es in Gnome einen neuen Weg, den Dateimanager Nautilus und den Texteditor Gedit mit root-Rechten zu starten.

Läuft Gnome unter Xorg, wie das in Ubuntu 18.04 noch einmal der Standard ist, dann funktioniert weiterhin der Aufruf grafischer Anwendungen mittels sudo über ein Terminalfenster. Das Kommando

```
sudo -H gedit
```

öffnet beispielsweise Gedit mit root-Berechtigungen und erlaubt die Bearbeitung von Konfigurationsdateien des Systems. Wo jedoch Wayland als Displaymanager läuft (wie unter Fedora bereits Standard und in Ubuntu optional auf dem Anmeldebildschirm wählbar), dann funktioniert sudo bei grafischen Anwendungen nicht mehr. Dafür haben Gnome-Programme aber eine neue Funktion bekommen. Ab Gnome 3.24 gibt es das neue Präfix „admin:///" in Dateidialogen, das ein Öffnen von Dateien und Verzeichnissen mit root-Rechten erlaubt.

Im Dateimanager Nautilus drückt man dazu die Tastenkombination Strg-L, um auf die editierbare Adresszeile umzuschalten. Hier verwenden Sie nun das Präfix „admin://" gefolgt vom gewünschten Verzeichnis, um an diesen Ort als root in das Dateisystem zu gehen. Beispielsweise öffnet

```
admin:///etc/
```

das Verzeichnis „/etc". Folgerichtig verlangt Nautilus dabei noch die Eingabe des sudo-Passworts in einem eingeblendeten Dialog. Ganz genauso kann der Texteditor Gedit mit dem neuen Präfix umgehen: Nach einem Klick links oben auf „Öffnen" und auch im Dateidialog (Strg-O) lädt beispielsweise die Angabe

```
admin:///etc/hosts
```

die Konfigurationsdatei „/etc/hosts" mit root-Berechtigungen in den Editor.

Die so geöffneten und modifizierten Dateien kann Gedit auch wieder speichern. **-dw**

Ubuntu: Fenster per Klick minimieren

Der Gnome-Desktop der neuen Ubuntu-Ausgabe verfügt bereits über einige Gnome-Erweiterungen, die den Wechsel von Unity vereinfachen. Eine der Erweiterungen ist die seitliche Leiste im Stil von Unity, die Programmverknüpfungen und laufende Programme anzeigt.

Im neuen Dock startet ein Klick auf ein Symbol die zugehörige Anwendung und ein weiterer Klick auf laufende Programme bringt dies in den Vordergrund, minimiert die Programmfenster aber nicht, wie das bei anderen Desktopumgebungen der Fall ist.

Eine versteckte Einstellung kann dieses Verhalten aber einschalten. Dazu dient folgendes Kommando in einem Terminalfenster:

```
gsettings set org.gnome.
  shell.extensions.dash-
  to-dock click-action
  'minimize'
```

Diese Änderung ist sofort wirksam. Ab jetzt kann ein Klick auf ein Programmsymbol im Dock dessen Fenster maximieren und minimieren, so wie es in KDE, Mate, XFCE und auch anderen Desktopumgebungen Standard ist. **-dw**

Programme per Klick minimieren: Diese Anpassung einer versteckten Einstellung des neues Docks macht die Fensternavigation in Ubuntu 18.04 bequemer.

Ubuntu: Gnome im alten Gewand

Anwendern, die vom Gnome-Desktop zwar insgesamt angetan sind, aber ohne traditionelle Bedienelemente nicht auskommen, kommt der Modus „Flashback" entgegen. Die Arbeitsfläche startet dann mit einer traditionellen Taskleiste zum Umschalten zwischen laufenden Programmen sowie einem ausklappenden Anwendungsmenü links oben. Dieser Modus steht in Ubuntu 18.04 aber zunächst nicht zur Verfügung.

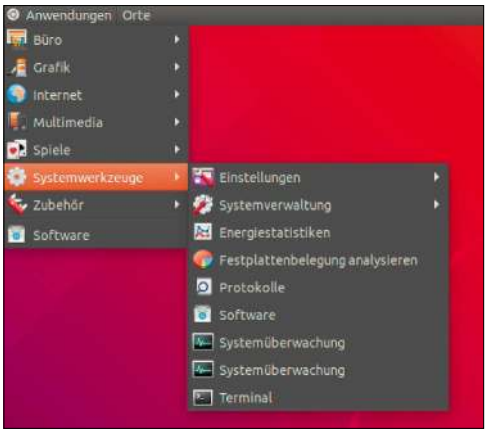
Tatsächlich gibt es auch im neuesten Ubuntu noch den Flashback-Modus für Gnome 3, der einen Desktop im Stil von Gnome 2 präsentiert (ähnlich wie Mate).

Dieser Modus kann parallel zum vorhandenen Gnome-Desktop nachinstalliert werden und steht dann auf der Anmeldeseite nach einem Klick auf das Zahnradsymbol unterhalb des Passwortfeldes bereit.

Zur Installation ist in Ubuntu 18.04 nur die Eingabe von

```
sudo apt-get install
  gnome-session-flashback
```

in einem Terminalfenster nötig. Der Befehl installiert alle weiteren benötigten Pakete, deren Größe sich auf rund 90 MB beläuft. Anschließend ist ein Neustart des Systems nötig, damit der zusätzliche Punkt „GNOME Flashback (Metacity)" im Sessionmenü der Anmeldung auftaucht. **-dw**



Altbekannt: Gnome läuft hier im Modus „Flashback", der das Aussehen von Gnome 2 imitiert. Dieser Modus lässt sich problemlos über ein Paket in Ubuntu 18.04 installieren.

Verschiedene Sessions bei der Anmeldung an Ubuntu 18.04: Die nachinstallierte Sitzung „GNOME Flashback (Metacity)" steht zur Auswahl unter dem Zahnradsymbol bereit.

KDE Plasma 5: Andere Farben für root

Wer hin und wieder grafische Programme unter KDE mit root-Recht starten will, etwa um Konfigurationsdateien mit einem grafischen Editor zu bearbeiten, tut dies am besten mittels kdesu. Ein eigenes Farbschema kann zudem als root gestartete Programme optisch von den anderen Programmfenstern unterscheiden.

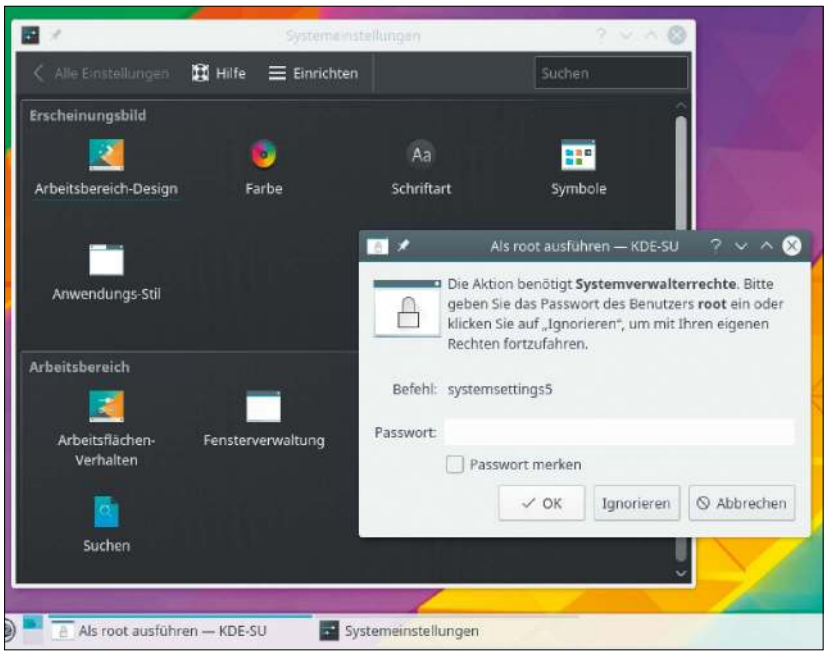
Unter KDE darf das übliche für Shell-Befehle konzipierte sudo generell keine grafischen Programme starten, denn der grafische X-Server verweigert die Verbindung zum Programmfenster. Stattdessen gibt es hier das Werkzeug kdesu, das in den typischen KDE-Distributionen wie Open Suse bereits vorinstalliert ist. Es kümmert sich auch darum, dass als root ausgeführ-

te Programme nicht einfach ihre Einstellungen in das Home-Verzeichnis des Benutzers schreiben, sondern in das Verzeichnis „/root“.

Damit aus Unachtsamkeit keine Fehler unterlaufen, wenn ein Programm als root läuft, kann man in KDE Plasma 5 den Programmfenstern ein anderes Aussehen geben. Dazu startet

```
kdesu systemsettings5
```

im Ausführen-Dialog die Systemeinstellungen. In der Ubuntu-Variante Kubuntu und KDE Neon lautet der Name des grafischen sudo-Befehls nicht „kdesu“ sondern „kdesudo“. Nach der Passworteingabe im angezeigten Dialog, die auf einigen Systemen das root-Passwort verlangt, gehen Sie in den Systemeinstellungen auf „Erscheinungsbild → Farben“ und legen dort die gewünschten Farben für Anwendungen fest, die mit root-Rechten aufgerufen werden. Regulär gestartete Programme bleiben bei ihrem bisherigen Farbschema. **-dw**



Auffällige Farben: Programme, die unter KDE Plasma 5 über kdesu mit root-Recht starten, lassen sich über die Systemeinstellungen mit einem besonderen Farbschema versehen.

Mate: Fenstergrößen leichter ändern

Mate ist eine schlanke Desktopumgebung geblieben, hat aber in den letzten Jahren speziell unter Ubuntu Mate (auf Heft-DVD) beachtliche Fortschritte gemacht. Ein Problem bleibt: Mit hohen Bildschirmauflösungen kann Mate zwar besser umgehen, aber es ist dann nicht ganz einfach, die Größe eines Fensters mit der Maus auf die gewünschten Dimensionen zu ziehen: Die Fensterrahmen sind unter Mate sehr dünn geraten.

Da es nicht immer einfach ist, den nur wenig Pixel breiten Fensterrahmen mit der Maus zu treffen, gibt es weitere Methoden zur bequemeren Größenänderung eines Fensters:

Tastenkombination und Maus: Hält man die Tasten Alt-F8 gedrückt, dann lässt sich das aktuelle Programmfenster durch Ziehen der Maus auf die gewünschte Größe anpassen.

Rechtsklick in die Titelleiste: Nicht bequem, aber ohne Tastaturbenutzung ist der Weg über einen Rechtsklick auf die Titelleiste eines Fensters, dessen Menü den Punkt „Größe ändern“ zeigt.

Fenstergrößen in Mate: Der Desktop erlaubt eine einfachere Anpassung von Fenstergrößen mit Tastatur und Maus per selbst definierten Hotkeys.

Selbst festgelegte Tastenkombination: Statt Alt-F8 ist es auch möglich, eine eigene Tastenkombination zur Größenänderung zu verwenden. Dazu gehen Sie in den Mate-Einstellungen auf „Tastenkombination“ und in der Liste auf „Fenstergröße ändern“. Nach einem Klick darauf lässt sich für diese Funktion eine eigene Tastenkombination festlegen. **-dw**

Shell-Spezialitäten

Der Befehl less zur Anzeige von Textdateien kann mehr, als er auf den ersten Blick verraten will. Ein Webterminal für SSH geht durch strikt konfigurierte ausgehende Portfilter hindurch und ein cleveres Tool zeigt Bilder im Terminal an.

Catimg: Bildbetrachter in der Shell

Das Terminal will so ganz und gar nicht als ein geeigneter Ort zum Betrachten von Bildern erscheinen. Um sich auf einem Webserver in einem Verzeichnis mit Bildern einen Überblick zu verschaffen, kann ein Tool zum Anzeigen von Grafiken in der Shell aber durchaus nützlich sein.

Ein originelles Kommandozeilentool zur stilisierten Anzeige von Grafiken im Terminal ist das Programm catimg.

Der Name hat nichts mit Katzen zu tun, sondern orientiert sich am bekannten Tool cat zur Anzeige von Textdateien in der Shell. In den Distributionen Ubuntu (ab 18.04), Fedora, Arch Linux und Debian Sid liegt das Paket „catimg" in den Standard-Repositories und ist flott eingerichtet.

Die Verwendung ist denkbar einfach:

```
catimg [Bilddatei]
```

zeigt im Terminalfenster eine heruntergerechnete Version des Bilds mit Unicode-Zeichen an. Je nachdem, ob das Terminal 265 Farben (TERM=xterm-256color) oder nur 16 Farben unterstützt, ist die Ausgabe mehr oder weniger detailliert. **-dw**

Nicht nur eine originelle Idee: Das Programm catimg stellt Bilddateien im Terminal mit Unicode dar und verschafft auf Webservern schnell einen Überblick zu Dateiinhalten.

Logs: Änderungen verfolgen

Auf dem eigenen Linux-Server im Internet oder auf dem Rasberry Pi im lokalen Netzwerk gehört die Überprüfung von Logs zu den regelmäßigen Aufgaben, um hin und wieder nach dem Rechten zu sehen. Üblicherweise dient der Befehl tail zur kontinuierlichen Anzeige von Logdateien. Mit less gibt es aber eine bequemere Lösung.

Auf einem Linux-System zeigt das Kommando

```
tail -F [Logdatei]
```

die zehn neuesten Zeilen in der angegebenen Logdatei an und aktualisiert dabei laufend die Ausgabe bei neuen Einträgen. Das Kommando

```
less +F [Logdatei]
```

kann dies auch, bietet dabei aber ein paar Funktionen mehr: Die Tastenkombination Strg-C verlässt die kontinuierliche Darstellung und springt zur scrollbaren, durchsuchbaren Anzeige der gesamten Datei. Ein Druck auf Taste F kehrt zurück zur fortlaufenden Anzeige. **-dw**

Logdateien im Blick: Der Befehl less verfolgt Änderungen, hier an einer Apache-Logdatei. Allerdings dient less auch als komfortabler Textbetrachter mit Suchfunktion.

SSH: Ausgehende Portfilter ausgetrickst

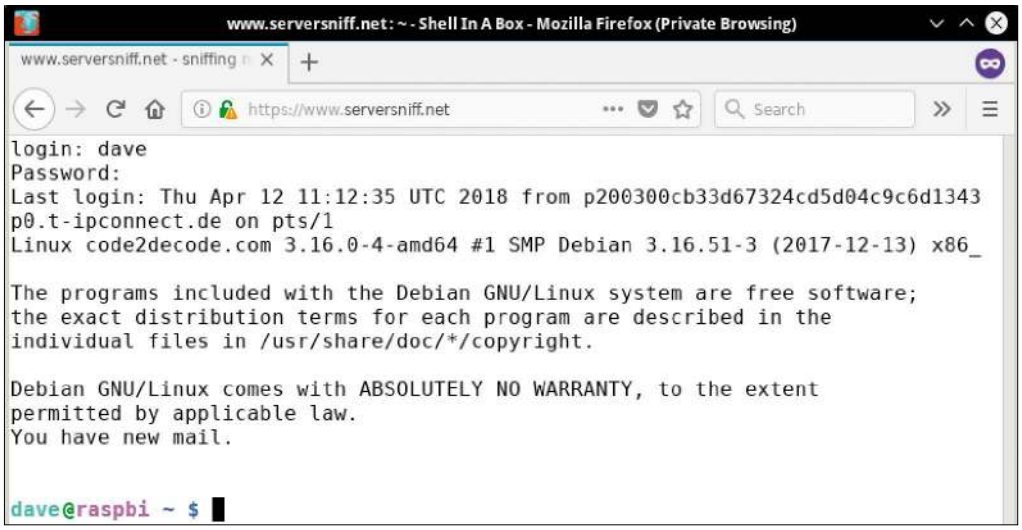
Viele 4G/LTE-Router, öffentliche Access Points und Firmenfirewalls blockieren ausgehende Ports und erlauben nur Port 80 für HTTP, Port 443 für HTTPS und einige Ports für den Mailverkehr über POP und SMTP. Linux-Anwender, die sich auf Port 22 mit einem SSH-Server im Internet verbinden möchten, haben bei dieser restriktiven Konfiguration erst einmal Pech.

Generell kann ein SSH-Server nach einer Konfigurationsanpassung auch auf einem anderen Port als dem Standardport 22 lauschen. Um ausgehende Portfilter auszutricksen, eignen sich beispielsweise die Portnummern 443 (HTTPS), 465 (SMTPS), 993 (IMAPS) und 995 (POP3S). Alle diese Ports sind für TLS-verschlüsselte Verbindungen gedacht. Die meisten Firewalls werden auf diesen Ports deshalb auch ausgehenden SSH-Traffic durchlassen, sofern der Port zu anderen Servern grundsätzlich offen ist. Es empfiehlt sich, vor Reisen oder Terminen vorsorglich schon mal auf dem eigenen SSH-Server einen weiteren Port für SSH zu öffnen. Im Notfall gibt es aber auch eine weitere Möglichkeit, auf ein Webgateway für SSH auszuweichen.

Möglichkeit 1: Um weitere Ports zum SSH-Dienst hinzuzufügen, ist nur eine kleine Anpassung der Konfigurationsdatei „/etc/ssh/sshd_config" nötig. Dazu entfernen Sie in der Zeile „#Port 22" das Kommentarzeichen # und tragen mit der weiteren Zeile

```
Port 995
```

den zusätzlichen Port 995 ein (falls verfügbar). Danach ist ein



SSH-Log-in im Browser: Shellinabox öffnet auf beliebigen Ports ein Webterminal für den SSH-Zugriff. Dabei generiert Shellinabox automatisch ein selbst signiertes SSL-Zertifikat.

Neustart des SSH-Dienstes mit

```
sudo service sshd restart
```

nötig. Jetzt lauscht der SSH-Server auf den Ports 22 und 995 und mit dem Kommando

```
ssh -p 995 [Serveradresse]
```

kann man sich nun mit dem SSH-Server verbinden. Falls auf dem SSH-Server ansonsten kein Webserver läuft, können Sie auch Port 443 (HTTPS) statt der 995 angeben.

Möglichkeit 2: Eine clevere Lösung, einen SSH-Log-in in den Webbrowser zu bekommen, ist das Tool Shellinabox. Zwar ist die Einrichtung etwas aufwendiger, aber nachdem es sich um ein Webterminal handelt, das jeden Traffic über Port 443 entgegennehmen kann, wird diese Lösung auch bei sehr strikten Firewalls funktionieren. Shellinabox ist ideal für Server, auf welchen kein Webserver läuft und folglich Port 443 noch frei ist. Allerdings kann Shellinabox keine Dateien per SSH übertragen, es handelt sich um ein reines Terminal.

Die Installation ist nicht kompliziert, da die meisten Distributionen ein fertiges Paket in ihren Repositories haben. In Ubuntu/Debian/Raspbian ist das Paket mit dem Befehl

```
sudo apt-get install
  shellinabox openssl
```

schnell eingerichtet. Zur Konfiguration dient die Datei „/etc/default/shellinabox“. In ihr legt die Zeile „SHELLINABOX_PORT=“ fest, auf welcher Portnummer der Dienst erreichbar ist. Standardmäßig ist hier „4200“ eingetragen. Damit Shellinabox auf dem freien Port 443 verfügbar ist, tauschen Sie diese Nummer gegen 443 aus und starten den Dienst mit

```
sudo service shellinabox
  restart
```

neu. Jetzt begrüßt den Besucher der URL „https://[Serveradresse]“ ein SSH-Log-in im Browserfenster. Shellinabox erstellt selbständig ein selbst signiertes SSL-Zertifikat beim Start, damit die Verbindung sicher verschlüsselt ist. Wie bei selbst signierten Zertifikaten üblich, muss man dieses im Browser erst noch als Ausnahme akzeptieren.

Möglichkeit 3: Wenn man spontan SSH-Zugriff auf einen Server durch eine strikte Firewall hindurch benötigt, so gibt es als Notnagel noch ein Webgateway unter *https://tools.bartlweb.net/webssh*. Aus Sicherheitsgründen sollten die Log-in-Daten und Passwörter auf dem Server nach der Verwendung dieses Gateways geändert werden, da der Betreiber theoretisch den Traffic mitlesen könnte. **-dw**

„Zeit“: Grafisches Cron-Front-End

Cron ist der Taskplaner unter Linux, der eingetragene Befehle zur bestimmten Zeiten oder im gewünschten Intervall ausführt. In alter Unix-Tradition erfolgt die Erstellung und Verwaltung von Tasks in der Kommandozeile, über den Befehl crontab -e. Die Syntax zur Angabe der Zeitintervalle für einen Eintrag ist nicht in allen Fällen einfach.

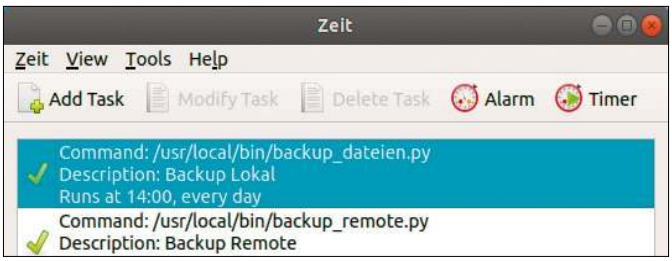
Für Einsteiger wird die Verwaltung von Cronjobs mit dem grafischen Front-End „Zeit“ viel einfacher. Außerdem kann das Programm auch über den Dienst at einmalig Programme oder Scripts zu bestimmten Zeiten ausführen. Zwar liegt das Programm noch nicht in den Paketquellen populärer Linux-Distributionen, aber ein PPA (inoffizielles Repository) für Ubuntu gibt es bereits. In Ubuntu und seinen Varianten nimmt das Kommando

```
sudo add-apt-repository
  ppa:blaze/main
sudo apt-get update
```

auf und

```
sudo apt-get install zeit
```

installiert das Programm, das auf Github im Quelltext vorliegt (*https://github.com/loimu/zeit*). Nach dem Start mittels *zeit* im Ausführen-Dialog zeigt das Tool in seiner englischsprachigen Oberfläche die derzeit eingerichteten Cronjobs an. Ein Klick auf „Add Task“ fügt einen neuen Cronjob über ein eingeblendetes Menü hinzu, das die Einstellung des Zeitintervalls einfach macht. Derzeit kann das Programm nur die Tasks des angemeldeten Benutzers bearbeiten, aber über den Menüpunkt „View → System Mode“ die Tasks des root-Kontos zumindest anzeigen. **-dw**



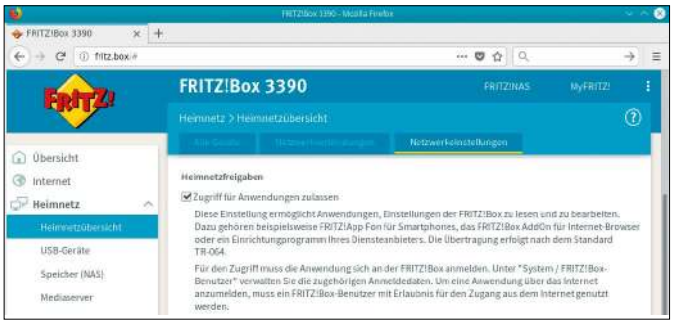
Cronjobs grafisch: „Zeit“ ist am Desktop eine Alternative zur Kommandozeile und erlaubt in englischsprachigen Menüs die Auswahl der gewünschten Zeiten.

Entspanntes Equipment

Diesmal geht es um bockiges Netzwerkequipment, das hin und wieder einen automatisierten Neustart erwartet. Weitere Tippthemen sind das unechte Raid vieler Hauptplatinen und die Wiederherstellung eines Chromebooks mit Linux.

AVM-Router: Automatisch neu starten

Bekanntes Gerät mit kaum bekannten Fähigkeiten: Die Fritzbox bietet ab Firmware-Version 6.x eine Fernsteuerung über das Netzwerk mit dem TR-064-Protokoll.



Fernsteuerung freischalten: Damit die Fernsteuerung einer AVM Fritzbox funktioniert, muss auf der Administrationsoberfläche der Punkt „Zugriff für Anwendungen zulassen“ aktiviert werden.

Eine einzelne AVM Fritzbox läuft meist ohne Verbindungsprobleme wochenlang stabil und verlangt selten nach einem Neustart. Anders verhält sich eine Kombination von Fritzbox mit weiteren AVM-Repeatern, um ein Funknetzwerk weiter zu spannen. Es kommt vor, das ein WLAN mit mehreren Repeatern erst nach einem Neustart der AVM Fritzbox wieder korrekt funktioniert.

AVM arbeitet mittels Firmwareupdates weiterhin daran, das Zusammenspiel von Router und Repeater im WLAN zu verbessern. So ist im Changelog der Firmwareversion 6.93 vom Anfang des Jahres mehrmals von „Stabilitätsverbesserung“ die Rede (*http://download.avm.de/labor/IQ17.2/1750E/info.txt*). Oft hilft trotzdem nur ein Routerneustart.

Einen regelmäßigen automatischen Neustart setzt man idealerweise zu jener Tageszeit an, wenn Router und WLAN nicht intensiv genutzt werden. Dabei kommt AVM findigen Anwendern und Admins entgegen: Zur Fernsteuerung von außen unterstützen Fritzboxen das herstellerübergreifende Protokoll TR-064. Bei der AVM Fritzbox (alle Modelle) eröffnet dieses Protokoll die Möglichkeit, den Router per Script von einem Linux-Rechner im lokalen Netzwerk aus zu Wunschzeiten neu zu starten.

1. Der erste Schritt ist die Aktivierung von TR-064 in der Fritzbox. Die Einstellung dazu verbirgt sich in der Konfigurationsoberfläche unter „Heimnetz → Heimnetzübersicht → Netzwerkeinstellungen“. Dort muss man einen Haken vor den Punkt „Zugriff für Anwendungen zulassen“ setzen und dann den Neustart der Fritzbox abwarten. Danach kann man testweise im Browser die URL *http://fritz.box:49000/tr64desc.xml* öffnen, auf der sich die Fritzbox per TR-064 vorstellt.

2. Ein unkompliziertes Script zum Neustart der Fritzbox stammt vom Linux-Anwender Nico Hartung, der es auf Github veröffentlicht hat (*https://git.io/vxzWG*). Das Script befindet sich auch als Datei „fritzbox-reboot.sh“ auf Heft-DVD. Zur Verwendung kopieren Sie es in ein beliebiges Verzeichnis auf den Linux-Rechner und machen es mittels des Befehls

```
chmod +x fritzbox-reboot.sh
```

ausführbar.

3. Damit das Script mit der eigenen Fritzbox zusammenarbeitet, sind zwei bis drei Ergänzungen nötig. Hinter die Zeile „IPS=“ kommt in Anführungszeichen die IP-Adresse oder der Hostname der Fritzbox, beispielsweise:

```
IPS="fritz.box"
```

Darunter muss hinter „FRITZUSER=“ der Log-in-Name für die Anmeldung an der Administrationsoberfläche angegeben sein, falls einer vergeben wurde. Ansonsten bleibt die Angabe einfach leer. Zuletzt erwartet die Zeile „FRITZPW=“ noch die Angabe des Passworts der Administrationsoberfläche.

4. Um das Script in einem gewünschten Intervall auszuführen, nutzt man auf dem Linux-Rechner den Taskplaner Cron. Im Terminal öffnet das Kommando

```
crontab -e
```

die Cron-Verwaltung im voreingestellten Texteditor. Die Zeile

```
0 5 */3 * * /home/user/fritzbox-reboot.sh
```

würde beispielsweise das Script „/home/user/fritzbox-reboot.sh“ alle drei Tage um fünf Uhr früh aufrufen und damit die Fritzbox neu starten.

fritzbox-reboot.sh: Bash-Script zum Neustart einer AVM Fritzbox per TR-064. Auf Heft-DVD, Download unter *https://git.io/vxzWG*. **-dw**

Raid: Besser ohne Hauptplatine

In den Firmware/Bios-Einstellungen vieler Hauptplatinen ist in der SATA-Konfiguration eine Option zum Betrieb mehrerer Festplatten im Raid-Verbund zu finden. Die Installer von Linux-Distributionen können aber bei dieser Einstellung kein Raid und oft auch gar keine Festplatten finden.

Bei der Raid-Option von Hauptplatinen handelt es sich um kein betriebssystemunabhängiges Hardware-Raid mit tatsächlichem Raid-Controller. Stattdessen ist es ein Software-Raid, das über die Windows-Treiber des Mainboardherstellers eine Kombination gleicher SATA-Festplatten als Raid-Verbund einbindet.

Eine unkomplizierte Möglichkeit, diese Raid-Kombination unter Linux zu nutzen, gibt es mangels Treibern nicht. Ein weiterer Nachteil: Dieser Raid-Verbund ist stets an das Modell der Hauptplatine beziehungsweise an den SATA-Controllerchip gebunden und kann bei einem Austausch der Platine gegen ein anderes Modell nicht mal mehr gelesen werden.

Es ist in jedem Fall performanter und zuverlässiger, aber auch teurer, ein echtes Hardware-Raid zu verwenden: Der Controller LSI MegaRAID SAS 9260-8I (*https://amzn.to/2Jw2VMI*) mit SATA/SAS-Ports ist ab 160 Euro zu haben und wird von Treibern für Linux und Windows unterstützt.

Die zweitbeste Lösung ist ein Software-Raid mit Hilfe des Linux-Kernels über das Tool MDADM (*https://pcwelt.de/1845119*). Der Vorteil ist, dass dieser Weg mit jeder Linux-Distribution funktioniert und unabhängig von Hauptplatine oder Controller ist. Die Leistung ist geringer als jene eines Hardware-Raids, da es keinen eigenen Prozessor und Cachespeicher auf einer Controllerkarte gibt. Allerdings ist die Performance keineswegs schlechter als die eines Onboard-Raids und außerdem ist ein Software-Raid mit Linux an keine obskure Hardware oder an eine bestimmte Linux-Distribution gebunden. **-dw**

Kein echtes Raid: SATA-Controller vieler Hauptplatinen bieten eine Raid-Option. Das ist aber nur eine Softwarelösung, die der CPU die gesamte Arbeit überlässt.

Chrome-OS: Recovery mit Linux

Zwar handelt es sich bei Chrome-OS um ein Linux-System, das von Gentoo abstammt. Google liefert das Betriebssystem zur Neuinstallation von Chrome-OS auf Chromebooks aber nicht einfach in Form von Imagedateien aus. Zur Erzeugung eines bootfähigen USB-Sticks mit Chrome-OS ist eine Chrome-App nötig (*https://goo.gl/JEfG27*), die aber nur unter Windows und Mac-OS läuft.

Aufgrund der erheblichen Unterschiede zwischen Chromebooks, die es sowohl mit ARM-Prozessor als auch mit Intel-CPU gibt, ist für jedes Chromebook-Modell ein spezielles Recovery-Image von Chrome-OS nötig.

Die Aufgabe der Chrome-App besteht im Wesentlichen darin, das richtige Image für das gewählte Modell herunterzuladen und auf einen USB-Stick zu schreiben. Wenn kein Mac- oder Windows-PC in Reichweite ist, hilft ein Script-basiertes Linuxtool bei der Erstellung eines Recoverysticks für das Chromebook. Mit wget können Sie es abholen (eine Befehlszeile!)

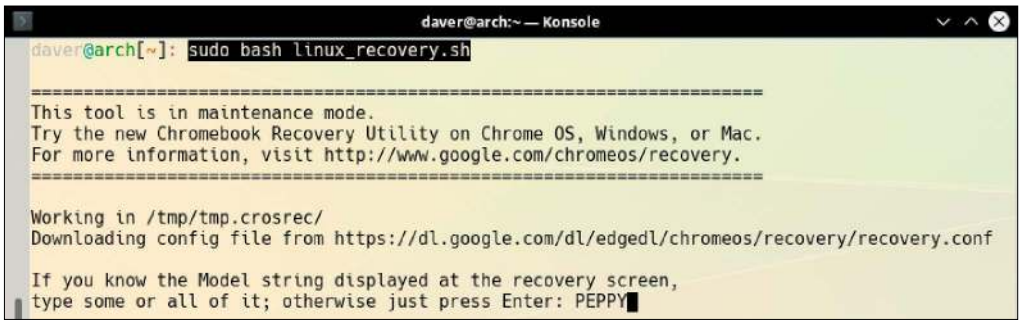
```
wget --no-check-
  certificate https://
  dl.google.com/dl/edgedl
  /chromeos/recovery/
  linux_recovery.sh
```

und danach im Terminal mit

```
sudo bash linux_recovery.
  sh
```

starten. Zur Identifizierung des Chromebooks ist dann der Codename des Geräts hilfreich. Eine Liste findet sich unter *https://www.chromium.org/chromium-os/developer-information-for-chrome-os-devices*.

Ansonsten kann das Script auch ein umfangreiches Menü zur Auswahl des Modells im Terminal anzeigen. Nach dem Download verlangt das Script nach einem angesteckten USB-Stick mit mindestens zwei GB Kapazität, um das Image zu übertragen. **-dw**



USB-Stick mit Chrome-OS erstellen: Die offizielle Recovery-App gibt es zwar nur für Windows und Mac-OS X, aber unter Linux hilft ein Script der Chrome-OS-Entwickler.

Softwarefinessen

Nach dem Datenskandal bei Facebook macht Mozilla mit Multi-Account-Containern Werbung für Firefox, um Facebook im Browser abzuschotten. Außerdem geht es in den Softwaretipps um Schriftarten und verwaiste Pakete auf Debian-Systemen.

ISO-Dateien: Einhängen oder bearbeiten

Aus einer Imagedatei im ISO- oder einem anderen Imageformat für optische Medien wird eine Datei benötigt, aber der Rechner hat kein DVD-Laufwerk. Notfalls geht es auch ohne Hardware: Der Isomaster kann ISO-Dateien und auch Imagedateien anderer Formate als Verzeichnis einhängen. Dabei kann Isomaster im Falle von ISO-9960 auch löschen oder hinzufügen.

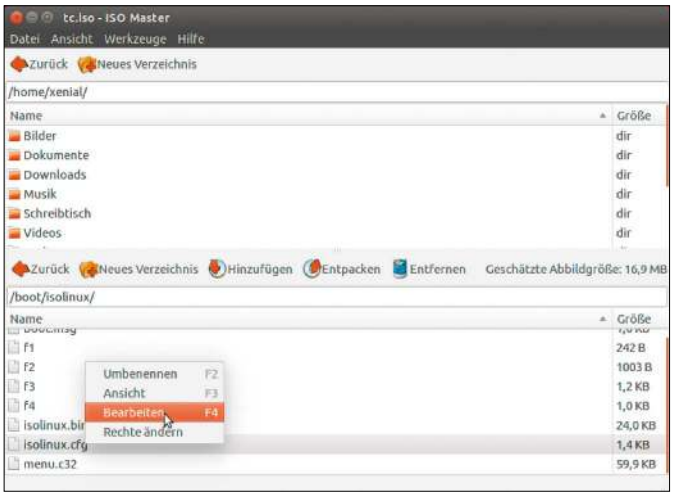
Isomaster beherrscht Dateien vom Typ ISO, aber auch die selteneren Formate NRG und MDF. Speichern will das Open-Source-Programm geänderte Inhalte aber nur im gebräuchlichen ISO-Format. Erfreulicherweise ist Isomaster inzwischen in den Standard-Paketquellen aller populären Linux-Distributionen zu finden und im jeweiligen Paketmanager schnell installiert. In Ubuntu/Debian genügt dazu beispielsweise das Kommando

```
sudo apt-get install
  isomaster
```

und schon ist Isomaster einsatzbereit.

Nach dem Aufruf des Programms zeigt es ein zweigeteiltes Fenster im Stil eines Dateimanagers. Der obere Teil zeigt die Verzeichnisse und Dateien auf dem lokalen Datenträger. Über den Menüpunkt „Datei → Öffnen“ wählt man in einem Dateibrowser das gewünschte Image aus, dessen Inhalt dann im unteren Fensterteil aufgelistet wird.

Einzige Einschränkung: Es gibt kein Drag & Drop. Stattdessen ist für Dateioperationen ein Rechtsklick auf Dateien oder Verzeichnisse oder auf die Menüleiste zwischen den Fensterteilen nötig. „Datei → Speichern unter“ erzeugt ein neues ISO-Image mit den Änderungen. **-dw**



Isomaster kann Images im Format ISO, NRG und MDF nicht nur wie ein Verzeichnis öffnen, sondern die ISO-Inhalte auch ändern und wieder zurückschreiben.

Isomaster 1.3.14: Open-Source-Programm (GPL) zum Öffnen und Bearbeiten von ISO-Images, Download des Quellcodes unter *www.littlesvr.ca/isomaster*.

Editoren: Überall die gleichen Stile

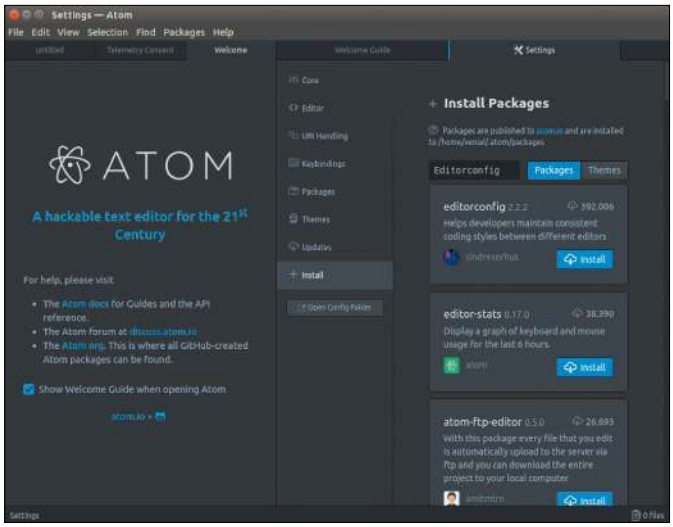
Quellcode wird mit einigen grundlegenden Formatierungen wie Einrücken, definierte Tabulatorbreite und Zeilenendzeichen im Editor gleich viel übersichtlicher. Am besten ist es, wenn dabei alle verwendeten Editoren die gleichen Formatierungen verwenden.

Das Projekt „Editorconfig“ ist ein cleveres Werkzeug, einheitliche Stile in mehrere verschiedene Editoren zu bringen, ohne dazu die Einstellungen jedes einzelnen Programms manuell anzupassen. Editorconfig definiert ein Metaformat, um Stile einheitlich in einer Konfigurationsdatei zu beschreiben. Dazu liefert Editorconfig Plug-ins für zahlreiche populäre Editoren aus, um diese Dateien in die Konfiguration einzulesen.

Der Vorteil: Anwender müssen die Formate nur einmal definieren. Unterstützung per Plug-ins bekommen dabei die Programme Geany, Atom, Brackets, Vim, Eclipse, Gedit, Notepad++, Sublime Text, Visual Studio Code und noch einige mehr. Eine Handvoll IDEs unterstützen Editorconfig sogar direkt, ohne Plug-in. dazu gehören Visual Studio, Komodo, Intellij Idea, BBEdit und andere. Die komplette Liste von Editoren ist auf *http://editorconfig.org/#download* zu finden.

Ein Wermutstropfen: Leider ist es bei einigen Programmen nicht ganz einfach, das angebotene Plug-in zu installieren. Meist liegt es nur im Quellcode vor. Folgendes Beispiel zeigt ganz praktisch die Verwendung von Editorconfig anhand der Editoren Vim und Atom:

1. Für den Editor Vim gibt es für Editorconfig ein kompaktes Plug-in auf Github (*https://git.io/vpYAK*), das keine Zusatzpakete benötigt und deshalb in allen Linux-Distributionen funktioniert. Die angebotene ZIP-Datei enthält das Verzeichnis



Editorconfig in Atom einrichten: Für das populäre Editorprogramm von Github gibt es ein fertiges Plug-in für Editorconfig, das über den enthaltenen Add-on-Manager schnell installiert ist.

„vim-editorconfig-master“, dessen Inhalt man in den Ordner „~/.vim“ im Home-Verzeichnis entpackt. Falls es dieses Verzeichnis noch nicht gibt, muss es noch mit dem Befehl

```
mkdir ~/.vim
```

erstellt werden.

2. Der Editor Atom hat seinen eigenen Plug-in-Manager und ein Erweiterungsverzeichnis im Stil eines Webbrowsers. Im Menü „Edit → Preferences → Install → Install Packages“ gibt es eine komfortable Suchfunktion, die das Plug-in „editorconfig“ mit wenigen Klicks installiert.

Editorconfig erlaubt die Definition von Stilen in einem Projekt. Öffnet man eine Quellcode- oder Script-Datei, zu der es im gleichen Ordner oder im übergeordneten Projektverzeichnis eine Datei namens „.editorconfig“ gibt, dann nutzen Vim und Atom die dort festgelegten Stile. Eine kurze, aber sehr nützliche Beispieldatei zeigt die Seite *http://editorconfig.org/#example-file*. **-dw**

Libre Office Calc: Zellen in Klammern setzen

Die Nachbearbeitung von langen Tabellen ist ein monotones Missvergnügen. Es gibt Hilfe: Geschickte Formeln können Zellen ergänzen, zusammenführen und mit temporären Hilfsspalten am Anfang und Ende Zeichen ergänzen. Noch mächtiger sind „reguläre Ausdrücke“ in der Suchen-und-Ersetzen-Funktion von Libre Office Calc.

Gerade URLs und Mailadressen verlangen oft eine Nachbehandlung in Form von Klammern, welche die Adresse in einer Zeile einfassen. Falls diese Adressen in einer eigenen Spalte untergebracht sind, ist die nachträgliche Klammerung nur ein kleines Problem: Vor und hinter dieser Spalte fügt man jeweils eine Hilfsspalte ein. In die erste Spalte, hier beispielsweise C2, kommt eine geöffnete eckige Klammer „[“ und in die hintere Spalte E2 eine geschlossene.

Um aus allen drei Spalten eine zu machen, dient in diesem Beispiel eine weitere Hilfsspalte mit der Formel:

```
=C2&D2&E2
```

Dies fasst die Inhalte von C2, D2 und E2 zusammen. Die Formel lässt sich über die ganze Spalte ausdehnen, indem Sie die erste Zelle per Klick markieren und dann bei gedrückter linker Maustaste nach unten ziehen. Die Zellbezüge sind relativ, das heißt, Calc wird in jeder Zeile die Zelladressen anpassen.

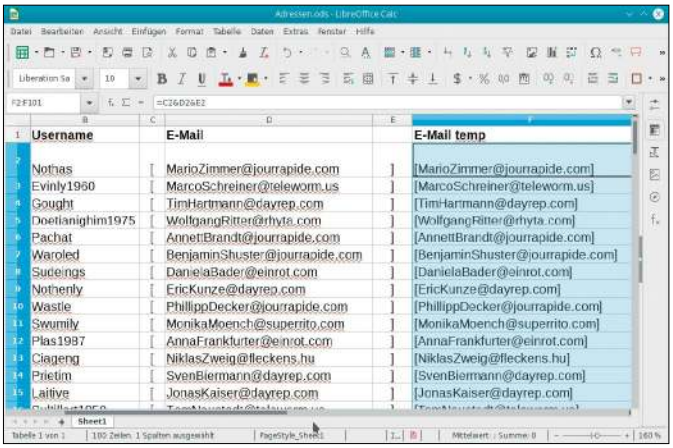
Falls die Mailadressen nicht einzeln in einer Spalte stehen, muss eine trickreichere Lösung helfen: Im Dialog „Bearbeiten → Suchen und Ersetzen“ aktivieren Sie „Weitere Optionen → Reguläre Ausdrücke“. In das Feld „Suchen“ kommt dann der Ausdruck

```
[a-zA-Z0-9._%+\-]+@
  [a-zA-Z0-9.\-]+\.[a-z]
  {2,6}
```

und in das Feld „Ersetzen“ dieser Platzhalter:

```
[&]
```

Ein Klick auf „Alle ersetzen“ wird sämtliche Mailadressen im Format „name@domain.tld“ in eckige Klammern setzen. **-dw**



Username	E-Mail	E-Mail temp
Nothas	MarioZimmer@jourrapide.com	[MarioZimmer@jourrapide.com]
Evinly1960	MarcoSchreiner@teleworm.us	[MarcoSchreiner@teleworm.us]
Gought	TimHartmann@dayrep.com	[TimHartmann@dayrep.com]
Doetlanighim1975	WolfgangRitter@rhyta.com	[WolfgangRitter@rhyta.com]
Pachat	AnnetBrandt@jourrapide.com	[AnnetBrandt@jourrapide.com]
Waroled	BenjaminShuster@jourrapide.com	[BenjaminShuster@jourrapide.com]
Sudeings	DanielaBader@einrot.com	[DanielaBader@einrot.com]
Nothenly	EricKunze@dayrep.com	[EricKunze@dayrep.com]
Wastle	PhillippDecker@jourrapide.com	[PhillippDecker@jourrapide.com]
Swumily	MonikaMoench@superrito.com	[MonikaMoench@superrito.com]
Plas1987	AnnaFrankfurter@einrot.com	[AnnaFrankfurter@einrot.com]
Ciageng	NiklasZweig@fleckens.hu	[NiklasZweig@fleckens.hu]
Prietim	SvenBiermann@dayrep.com	[SvenBiermann@dayrep.com]
Laitive	JonasKaiser@dayrep.com	[JonasKaiser@dayrep.com]

E-Mail-Adressen in eckigen Klammern: In Libre Office Calc gelingt dies mit zwei Hilfsspalten, hier C und E, oder mit Hilfe eines regulären Ausdrucks über „Suchen und Ersetzen“.

Firefox Send: Dateien per Link teilen

Schon vor einer Weile hat die Mozilla Foundation einen kostenlosen Filesharing-Service ins Leben gerufen: „Firefox Send“. Nur war nicht sofort klar, ob es sich dabei nicht um eine Eintagsfliege handelt. Nun ist der Dienst, der vor über sechs Monaten an den Start ging, schon ein gutes Stück arrivierter und deshalb einen Blick wert.

Die Mozilla Foundation ist eine Non-Profit-Organisation und wird deshalb keinen Filesharing-Dienst im Stil von Dropbox stemmen. Stattdessen geht es bei Firefox Send um einen ganz unkomplizierten Dateiaustausch über das Web für Dateien bis zu einem Gigabyte. Als Hoster dient Amazons Simple Storage Service S3. Nach 24 Stunden erlischt nicht nur der Downloadlink, auch die Datei verschwindet im Nirwana. Ebenso nach einem Download. Firefox Send eignet sich also nur für kurzfristiges Ad-hoc-Filesharing, um eben einen Link per Messenger oder Mail an einen Empfänger zu schicken.

Der Dienst ist nicht an den Firefox-Browser gebunden, son-

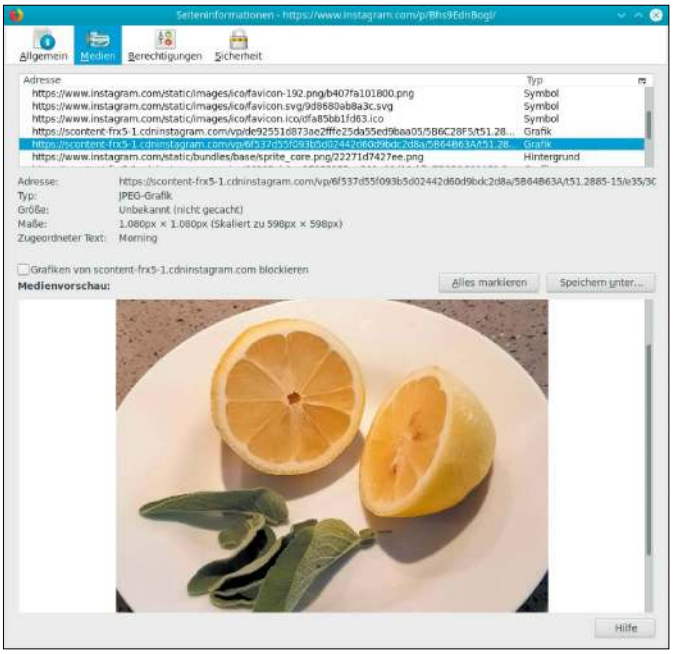
dern funktioniert auch mit Chrome/Chromium und allen anderen Browsern mit Unterstützung der Web Crypto API. Nach einem Besuch von *https://send.firefox.com* zieht man die gewünschte Datei ins Browserfenster, woraufhin die Datei noch im Browser vor dem Upload per AES verschlüsselt wird. Man erhält dann einen Link, der sich auch noch mit einem Passwort schützen lässt. Die Besonderheit an Firefox Send ist, dass dessen kompletter Quellcode Open Source und auf Github veröffentlicht ist (*https://github.com/mozilla/send*). **-dw**

Instagram: Bilder herunterladen

Die Webseite von Instagram (*https://www.instagram.com*) sieht nicht vor, dort veröffentlichte Bilder eines Accounts herunterzuladen. Auch der Rechtsklick auf ein Bild funktioniert nicht zum Speichern der Grafik. Mit einem Trick geht es trotzdem, egal in welchem Browser.

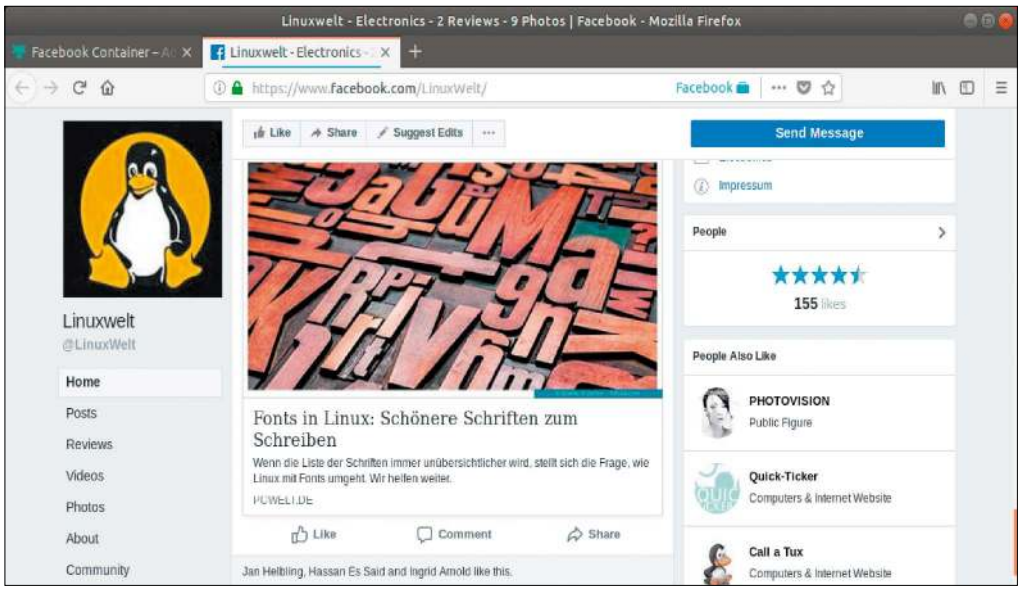
Im Browser Firefox zeigt der Menüpunkt „Extras → Seiteninformationen" alle Grafiken einer geladenen Webseite in der Liste „Medien" an.

Dank einer Vorschaufunktion ist es auch kein Problem, ein Bild schnell in der Liste zu identifizieren und dann per „Speichern unter" lokal abzulegen. In Chrome/Chromium funktioniert dies über die Entwicklertools (Taste F12) über die Unterseite „Network" in der Seitenleiste. Nach einem Klick auf „Img" lädt man die Seite mit der Taste F5 neu und erhält in der Seitenleiste dann ebenfalls eine Liste aller geladenen Grafiken mit Vorschau. **-dw**



Nützlich zum Speichern von Bildern: Die Seiteninformationen von Firefox (auch per Strg-I aufrufbar) zeigen alle geladenen Grafiken einer Seite mit Vorschau an.

Firefox: Facebook im Container



Ein eigener Container für Facebook: Die Firefox-Erweiterung „Facebook Container" verhindert bei konsequenter Nutzung die Trackingaktivitäten des sozialen Netzwerks im Browser.

Vielen Anwendern von Facebook ist die Datensammelwut des sozialen Netzwerks inzwischen bewusst. Mozilla zeigt mit einer Firefox-Erweiterung, wie sich Facebook im Browser isolieren lässt.

Hinter der Erweiterung „Facebook Container" stehen die Multi-Account-Container, die Mozilla bereits 2017 vorgestellt hat. Sie erlauben mehrere abgeschottete Browserinstanzen, um sich beispielsweise an einem Dienst mit mehreren Identitäten anzumelden. Das neue Add-on ist speziell für Facebook gemacht und verlangt keine weitere Konfiguration mehr. Nach der Installation der Erweiterung über *https://addons.mozilla.org/de/firefox/addon/facebook-container* löscht Firefox automatisch alle Facebook-Cookies und meldet den Anwender von Facebook ab. Beim nächsten Besuch von Facebook verwandelt sich der Browsertab in Firefox in einen Contai-

ner, was auch am blauen Symbol in der Adresszeile zu sehen ist. Von anderen Aktivitäten auf Webseiten ist der Facebook-Account jetzt abgeschottet. Eine (erwünschte) Nebenwirkung ist, dass Like- und Share-Schaltflächen sowie Facebook-Formulare außerhalb des Containers nicht mehr funktionieren. **-dw**

Facebook Container 1.3.1: Erweiterung für Firefox, die Facebook automatisch in einem abgeschotteten Browser-Container lädt *(https://addons.mozilla.org/de/firefox/addon/facebook-container)*.

Fontfinder: Fonts finden und installieren

Eine Linux-Distribution für den Einsatz auf dem Desktop liefert eine ansehnliche Sammlung an Schriftarten für etliche Sprachen mit. Trotzdem verlangen Illustrationen oft die Suche nach weiteren Schriften.

Der Fontfinder macht es einfache, Schriftarten aus dem großen freien Archiv der Google Fonts zu suchen und zu installieren. Das Open-Source-Programm, das für den Gnome-Desktop als Flatpak zur Installation bereitsteht, listet dabei verfügbare Fonts nicht einfach nur auf, sondern präsentiert auch gleich einen Beispieltext. Mit Klick auf „Install" richten Sie eine gewünschte Schriftart unter dem eigenen Benutzerkonto ein.

Zur Installation in Ubuntu, das im Auslieferungszustand nicht mit Flatpaks umgehen kann, sind diese Vorbereitungen nötig: Das Kommando

```
sudo apt install flatpak
```

installiert die Flatpak-Umgebung und

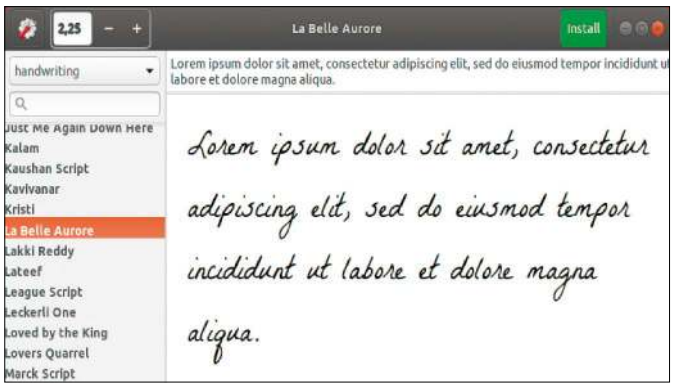
```
flatpak remote-add --if-
  not-exists flathub
  https://flathub.org/
  repo/flathub.
  flatpakrepo
```

richtet *https://flatpak.org* als Repository ein. Jetzt kann der Befehl

```
flatpak install flathub
  io.github.mmstick.
  FontFinder
```

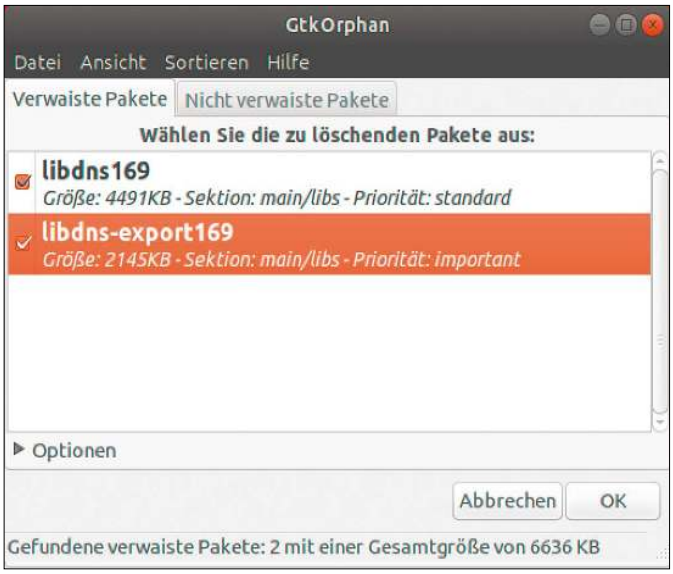
Fontfinder installieren. In Fedora und Linux Mint ist nur dieser letzte Befehl nötig, da Flatpak in diesen Linux-Distributionen schon eingerichtet ist. **-dw**

Fontfinder 1.3.2: Bietet Schriftarten aus dem Google-Fontarchiv zur Installation an.
Das Tool ist Open Source, Installation als Flatpak über *https://flathub.org/apps/search/FontFinder.*



In Schriftarten stöbern: Fontfinder präsentiert die Fonts aus dem öffentlichen Google-Fonts-Verzeichnis zur Installation. Diese Schriftarten wurden unter freie Lizenzen gestellt.

Ubuntu/Debian: Verwaiste Pakete



Obsolete Pakete, die kein anderes Programm mehr braucht: gtkorphan listet auf Debian-basierten Systemen verwaiste Bibliotheken auf, die gefahrlos deinstalliert werden dürfen.

Eine gut abgehangene oder durch Experimente gebeutelte Linux-Installation beherbergt oft eine Menge überflüssiger Bibliotheken und Zusatzpakete, die keinen Nutzen mehr haben, da das dazugehörige Programm längst deinstalliert ist. Ein Linux-System wird dadurch nicht langsamer, aber auf SSDs und kleinen SD-Karten ist der Platz oft nicht üppig und ein paar Bibliotheken weniger machen sich angenehm bemerkbar.

Wer Debian, Ubuntu oder Raspbian auf dem Raspberry Pi einsetzt, kann verwaiste Pakete mit einem Tool ausfindig machen: Das Kommandozeilenprogramm deborphan, das sich mit

```
sudo apt-get install
  deborphan
```

aus den Standard-Paketquellen nachrüsten lässt, zeigt eine Liste von Paketen, die keine Abhängigkeiten mehr erfüllen. Diese Situation entsteht, wenn ein Programm A ein zusätzliches Paket B als Voraussetzung mitinstalliert, später aber entfernt wird.

In den meisten Fällen bleibt dann Paket B weiterhin auf dem System, auch wenn es kein anderes Programm mehr benötigt. Das Tool hat auch ein grafisches Gegenstück namens gtkorphan, das mit

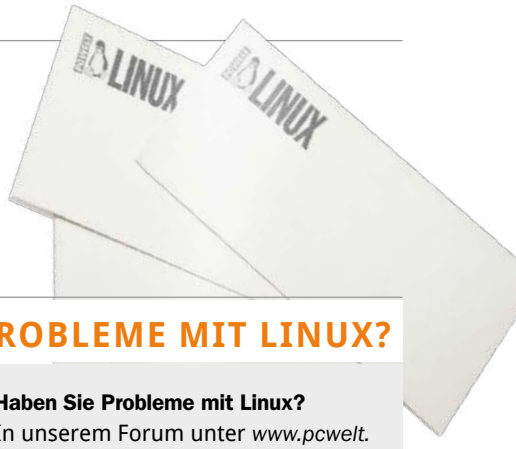
```
sudo apt-get install
  gtkorphan
```

zu installieren ist. Anders als deborphan verlangt gtkorphan beim Aufruf nach root-Berechtigungen. Im Terminal gibt das Kommando

```
sudo -H gtkorphan
```

dem Programm die verlangten Berechtigungen. Dieser Weg funktioniert allerdings nur unter Xorg, nicht im neuen Anzeigeserver Wayland. Gegebenenfalls müssen Sie sich, im Falle von Gnome auf einer aktuellen Linux-Distribution, zunächst abmelden und auf der Anmeldeseite eine Sitzung ohne Wayland auswählen.

Gtkorphan listet im Fenster „Verwaiste Pakete" übrig gebliebene Bibliotheken auf. Das grafische Tool bietet dabei gleich an, die gefundenen Pakete zu deinstallieren. **-dw**



Leserbriefe

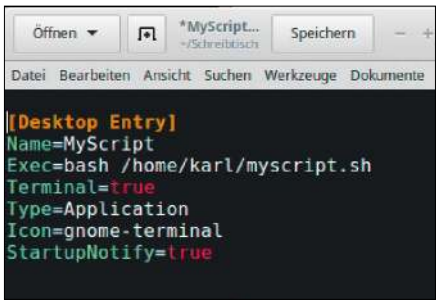
Haben Sie Fragen zum Heft oder möchten Sie uns Ihre Meinung dazu mitteilen? Schreiben Sie bitte an *linux@it-media.de* oder per Post an Redaktion LinuxWelt, IT Media, Gotthardstr. 42, 80686 München. Von den vielen Zuschriften können wir nur eine Auswahl veröffentlichen. Sinnwahrende Kürzungen behalten wir uns vor.

Desktoplink zum Shell-Script

Ich habe mir ein praktisches Shell-Script gebastelt, das im Terminal einwandfrei läuft. Aber wie kann ich das Script jetzt noch einfacher durch einen Link am Desktop auslösen? Versuche mit dem Dateimanager Nautilus und mit dem Kommando „ln“ schlugen fehl.

Karl R., per Mail

Mit einer symbolischen Dateiverknüpfung funktioniert das nicht. Sie benötigen dafür am Desktopordner eine Datei mit der Endung „.desktop“, die Sie mit jedem Texteditor schreiben können und die mindestens folgende Angaben enthalten muss:



Entscheidend ist die Angabe „Exec=...“, deren Pfad Sie natürlich anpassen müssen, so dass er zu Ihrem Shell-Script zeigt. Nach dem ersten Start durch Doppelklick muss die Verknüpfung zunächst als „vertrauenswürdig“ bestätigt werden. Danach ändert sie ihren Dateinamen und zeigt den Namen wie in der Datei als „Name=“ angegeben. Künftig startet nach Doppelklick das verlinkte Script.

Plank-Dock mit Defizit?

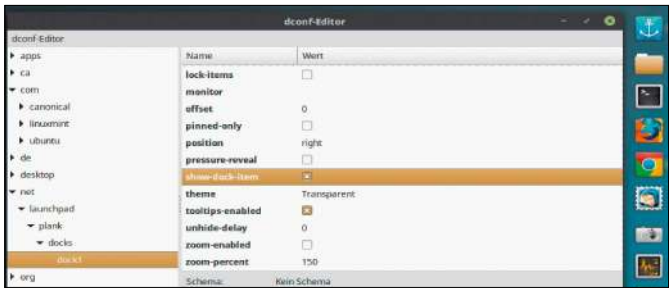
Das simple Starterdock Plank gehört bei mir am Linux-Desktop zur Standardausrüstung. Auf meinem aktuellen Linux Mint 18.3 zeigt es allerdings sein eigenes Icon im Dock nicht an. Wie komme ich an die Konfigurationseinstellungen des Docks?

Leon P., per Mail

Der Entwickler hat sich in neueren Versionen entschlossen, den Platz für das Einstellungsicon einzusparen. Mit dem Befehl

```
plank --preferences
```

kommt man aber jederzeit an die Plank-Konfiguration. Ganz bequem ist das nicht, aber es gibt auch noch einen komfortablen interaktiven Weg: Klicken Sie bei gedrückter Strg-Taste mit rechter Maustaste auf ein beliebiges Dockicon, so erscheint die einschlägige Option „Einstellungen“. Wenn Ihnen das Plank-eigene Icon im Dock trotzdem unentbehrlich erscheint, kann auch noch der dconf-editor aushelfen: Unter „net → launchpad → plank → docks → dock1“ finden Sie den Wert „show-dock-item“, den Sie per Optionskästchen auf „true“ setzen.



Wer das Plank-eigene Symbol (blauer Anker) im Dock vermisst, kann das mit einer dconf-Einstellung korrigieren.

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

Einsendungen: Für unverlangt eingesandte Beiträge sowie Hard- und Software übernehmen wir keine Haftung. Eine Rücksendegarantie geben wir nicht. Wir behalten uns das Recht vor, Beiträge auch auf anderen Medien, etwa auf DVD oder online, zu veröffentlichen.
Copyright: Das Urheberrecht für angenommene und veröffentlichte Manuskripte liegt bei der IT Media Publishing GmbH & Co. KG. Eine Verwertung der urheberrechtlich geschützten Beiträge und Abbildungen, insbesondere durch Vervielfältigung und/oder Verbreitung, ist ohne vorherige schriftliche Zustimmung des Verlags unzulässig und strafbar, soweit sich aus dem Urheberrechtsgesetz nichts anderes ergibt. Eine Einspeicherung und/oder Verarbeitung der auch in elektronischer Form vertriebenen Beiträge in Datensysteme ist ohne Zustimmung des Verlags unzulässig.
Haftung: Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Die Veröffentlichungen in der LinuxWelt erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Auch werden Warennamen ohne Gewährleistung einer freien Verwendung benutzt.
Bildnachweis: 123rf – naddi; sofern nicht anders angegeben: Anbieter

Anzeigenrepräsentanz
IDG Tech Media GmbH
Lyonel-Feininger Str. 26
80807 München,
Tel. 089/36086-210
Fax 089/36086-263
E-Mail: *media@pcwelt.de*
Gesamtanzeigenleitung:
Sebastian Wörle (-113)
(verantwortlich für den Anzeigenteil)
Digitale Anzeigenannahme – Datentransfer: Zentrale E-Mail-Adresse: *AnzeigendispoPrint@pcwelt.de*
Digitale Anzeigenannahme – Ansprechpartner: Walter Kainz (-258)
E-Mail: *wkainz@idg.de*

Anzeigenpreise: Es gilt die Anzeigenpreisliste 34 (1.1.2017).

Bankverbindungen:
Deutsche Bank AG
Konto 666 22 66, BLZ 700 700 10
Postbank München,
Konto 220 977-800, BLZ 700 100 80
Anschrift für Anzeigen:
siehe Anzeigenabteilung
Erfüllungsort, Gerichtsstand:
München
Verlagsrepräsentanten für Anzeigen in ausländischen Publikationen:
Europa: Shane Hannam
29/31 Kingston Road, GB-Staines, Middlesex TW 18 4LH
Tel.: 0044-1-784210210

Vertrieb
Vertrieb Handelsauflage:
MZV GmbH & Co. KG, Ohmstraße 1
85716 Unterschleißheim
Tel. 089/31906-0
Fax 089/31906-113
E-Mail: *info@mzv.de*
Internet: *www.mzv.de*

Druck: Mayr Miesbach GmbH
Am Windfeld 15, 83714 Miesbach
Tel. 08025/294-267

Verlag
IT Media Publishing GmbH & Co. KG
Gotthardstr. 42, 80686 München
Tel. 089/3398052-10,
Fax 089/3398052-70
E-Mail: *info@it-media.de*
www.it-media.de
Sitz: München, Amtsgericht München, HRA 104234

Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949:
Alleinige Gesellschafterin der IT Media Publishing GmbH & Co. KG ist die **IT Media Publishing Verwaltungs GmbH,** Sitz: München, Amtsgericht München, HRB 220269

Geschäftsführer: Sebastian Hirsch

ISSN 1860-7926

Anzeigen-Hotline Print:
Sven Schrader
E-Mail: *schrader@it-media.de*
089/3398052-41

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 5/2018 erscheint am 27.7.2018

Aus Aktualitätsgründen können sich Themen ändern.

Ubuntu 18.04 LTS optimieren

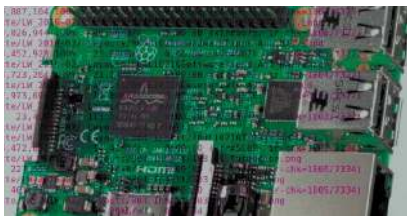
System- und Desktoptuning: Die nächste LinuxWelt wird dem brandneuen Ubuntu 18.04 LTS tiefer unter die Karosserie blicken, als dies in diesem Heft aus Zeitgründen möglich war. Hauptthemen sind optimale Systemleistung, Beseitigung von Mängeln und Defiziten, Ergänzung durch unentbehrliche Systemtools sowie die Optimierung der diversen Ubuntu-Desktops. Dabei kommen alle „Flavours" zu Wort, also neben den großen Gnome-, KDE-, Budgie-Desktops auch die sparsamen Ubuntus mit Mate, XFCE und LXDE.

Linux-Probleme systematisch lösen

Troubleshooting bei Systempannen: Die Artikelsammlung bringt Lösungen für verbreitete, andererseits nicht triviale Probleme beim Linux-System. Bootloader-Pannen oder vergessene Kennwörter sind ebenso im Portfolio wie gelöschte Daten, streikende X-Server oder Zugriffshindernisse durch mangelnde Dateirechte. Netzwerkprobleme kommen ebenfalls zu Wort, soweit sie im engeren Zusammenhang mit Linux-Servern und Clients stehen. Bei der Hardware geht es um fundamentale Fehler wie stumme Soundkarten oder unzugängliche USB-Laufwerke.

Raspberry & Co. als Backupserver

Automatische Datensynchronisierung: Ein permanent laufender Platinenrechner kann im Heimnetz das lästige Thema der Datensicherung weitgehend automatisieren. Ohne strategische Überlegungen und Ersteinrichtungsaufwand geht es aber nicht: Wenn der Backupserver die Daten automatisch abholen soll, muss er auf entsprechende Netzfreigaben treffen. Wenn umgekehrt die Clients die Daten selbst an den Server verschicken sollen, entsteht ebenfalls etlicher Konfigurationsaufwand an den einzelnen Netzwerkrechnern. Der Beitrag erklärt die unterschiedlichen Strategien und die möglichen Hindernisse.



Datenschutz mit Veracrypt

Basisbedienung und Komfortfunktionen von Veracrypt: Der Truecrypt-Nachfolger gewinnt unversehens an Bedeutung, nachdem die offizielle Ubuntu-Familie ab sofort, die Derivate (Linux Mint, Elementary OS, Zorin, Bodhi Linux, Bunsenlabs etc.) demnächst auf die Home-Verschlüsselung mit Ecrypt FS verzichten. Der Beitrag erläutert die Funktionsweise des nicht so ganz intuitiv zugänglichen Veracrypt und zeigt Komforttipps und Kommandooptionen, die sichere Datenverschlüsselung mit komfortabler Bedienung kombinieren.

PC-WELT

Sonderheft-Abo

Für alle Sonderausgaben der PC-WELT

Sie entscheiden, welche Ausgabe Sie lesen möchten!

Die Vorteile des PC-WELT Sonderheft-Abos:

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

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

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

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

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

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

BEZAHLEN

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

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PWSJO14130

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

Unterwegs-Power

Die ultramobilen Linux-Workstations von TUXEDO Computers

Erleben Sie jetzt die leistungsfähigsten TUXEDO Notebooks aller Zeiten

Dank neuester Intel® Core™ i-Prozessoren, bis zu 32 GB Arbeitsspeicher und flexibel wählbarem Festplatten- und SSD-Speicher sind Ihnen keine Grenzen gesetzt. Mit integriertem 4G LTE Modem und bis zu 24h Akkulaufzeit sind Sie "always on".

Immer die Leistungsfähigkeit im Blick haben wir ultramobile Begleiter geschaffen, die dank flacher Bauweise und leichter Materialien ideal für den Einsatz unterwegs sind.

Das alles funktioniert durch sorgfältig ausgewählte und aufeinander abgestimmte Komponenten zu 100% mit Linux und Windows - *garantiert!*

Direkt zum Vorzugspreis sichern!

Konfigurieren Sie jetzt Ihr TUXEDO Notebook individuell und sparen dabei exklusive 3% mit dem Rabattcode "LXWELTIB13" - *aber nur für kurze Zeit!*

TUXEDO COMPUTERS

tuxedocomputers.com