Multiboot-DVD mit 6 Top-Systemen

5/2018
August/September

4 196691 608505 05
Deutschland 8,50 €
Schweiz 16,90 sfr · Österreich + Benelux 9,45 €

LINUX WELT

Top-Linux Manjaro

Schlankes System mit Rolling Releases, grafischem Installer und großer Software-Auswahl

Profi-Hacks ganz einfach

So geht's: System patchen, Desktop aufbohren, Schutzfunktionen nachrüsten

- Schwächen beim Desktop beseitigen
- Eigenen Passworttresor bauen
- Terminalbefehle schnell finden
- Alle Optionen von Veracrypt nutzen
- Aktiven Backup-Server einrichten

Einfache Geräteortung

Mit Prey Notebooks, Smartphones und Tablets wiederfinden

Neu: Gimp 2.10

Einfache Bedienerführung, hohe Farbtiefe für Bilder, schnellere Render-Engine, Auto-Recovery u.v.m.

Perfekter Sound mit Linux

Nie mehr Tonprobleme: Linux-Sound-Server richtig einstellen

20 SEITEN SPECIAL

NEU: Das beste Linux!

Mint 19 und Ubuntu 18.04: Das bieten die Upgrades
PLUS: Die neuen Versionen im Praxis-Einsatz

Tipps & Tricks fürs Netzwerk

- TV-Server im Eigenbau
- Heimautomatisierung ganz einfach
- Server-Update ohne Neustart

MULTIBOOT-DVD

Linux Mint 19 & Ubuntu 18.04

Open Suse Leap 15
Manjaro Cinnamon 17.1.10
Fedora Workstation 28
Ubuntu Server mini.iso 18.04

LinuxWelt Digital XXL
Das komplette Handbuch
303 Seiten Linux-Profi-Wissen

Auf DVD: Mint 19 und Ubuntu 18.04

PLUS: Open Suse Leap, Manjaro Cinnamon u.v.m.

NEU: 10 Video-Workshops

- Vergessenes Passwort zurücksetzen
- Wiederherstellungspunkt einrichten
- Grafiktreiber unter Mint installieren
- Linux-System selbst zusammenstellen u.v.m.

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

PC-WELT

Sonderheft-Abo

Für alle Sonderausgaben der PC-WELT

Sie entscheiden, welche Ausgabe Sie lesen möchten!

Die Vorteile des PC-WELT Sonderheft-Abos:

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

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

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

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

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

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

BEZAHLEN

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

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PWSJO14130

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

Microsoft kauft Github

Microsoft kauft die Entwickler-Plattform Github (*www.github.org*) für 7,5 Milliarden Dollar. Auf Github veröffentlichen Millionen Entwickler ihre Open-Source-Projekte. Open Source steht für Transparenz, Offenheit und Sicherheit – Werte, die viele Entwickler nicht mit Microsoft in Verbindung bringen. Entsprechend groß war bei einigen der Unmut über den Kauf von Microsoft.

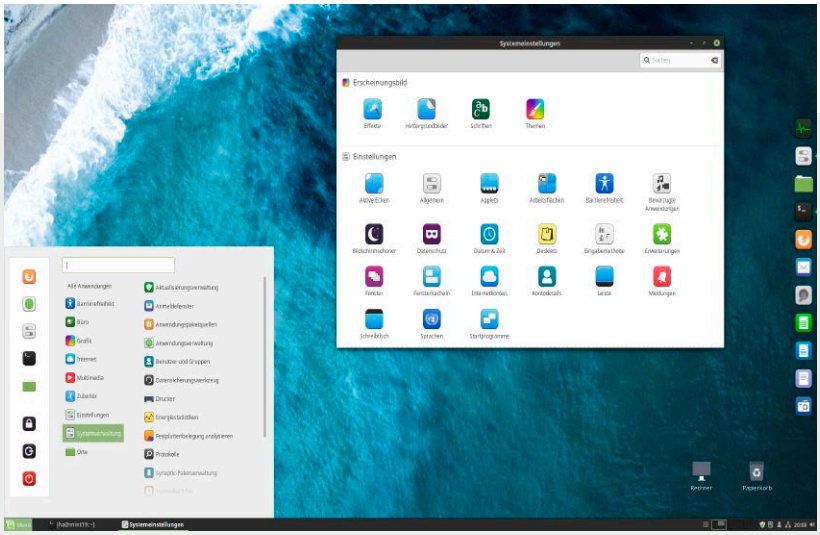
Kritiker fürchten, dass Microsoft nun ausspionieren kann, was 27 Millionen Software-Designer auf Github entwickeln – und sich dann die Ideen einverleibt. Hinzu kommen Ressentiments gegen Microsoft als früher Linux-feindliche Software-Schmiede.

Doch es gibt auch andere Stimmen: Optimisten hoffen, dass sich Microsoft selbst in weiten Teilen zu einem Open-Source-Unternehmen entwickeln wird. Schließlich ist Microsoft schon bisher das Unternehmen mit den meisten Projekten und Entwicklern auf Github.

Die LinuxWelt wünscht sich von Microsoft, dass das Unternehmen weiter auf die Open-Source-Community und Linux zugeht, Open Source weiter mit seinen Ressourcen unterstützt und für mehr Transparenz, Offenheit und Sicherheit sorgt, als das in der Vergangenheit des Unternehmens der Fall war.

Herzlichst, Ihr

Arne Arnold
Redakteur
aarnold@it-media.de



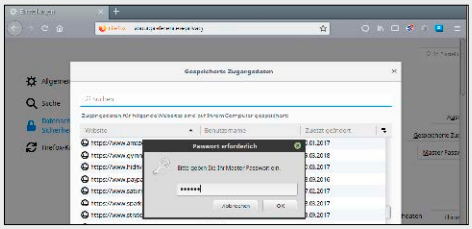
Profi-Hacks ganz einfach

Schwächen bei Cinnamon & Co. beseitigen, **S. 16** • Eigenen Passworttresor bauen, **S. 54** • Terminalbefehle schnell finden, **S. 105** • Alle Optionen von Veracrypt nutzen, **S. 68** • Aktiven Backupserver einrichten, **S. 88**

Passwörter

Kennwörter, Schlüssel, Strategien: Mit diesem Special haben Sie Ihre Authenifizierungsdaten im Griff.

S. 42 ff.



Passwortsafes

Passwortmanager machen die Inflation der Kennwörter beherrschbar. **S. 50**

Grundlagen

Special 1 – Tipps & Tuning für Ubuntu 18.04

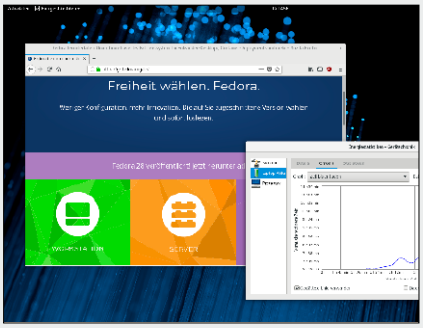
Special 2 – Passwörter, Schlüssel, Zertifikate

Die Highlights auf der DVD

Ungewöhnliche Dichte an Desktopneuheiten: Neben den Platzhirschen Ubuntu 18.04 (Budgie-Variante auf DVD) und Linux Mint 19 (Cinnamon-Hauptedition auf DVD) startet die Heft-DVD die brandaktuellen Versionen von Fedora, Open Suse und Manjaro. Auch diese drei Distributionen gehören zur Desktopprominenz unter Linux, richten sich aber vornehmlich an erfahrene Nutzer.

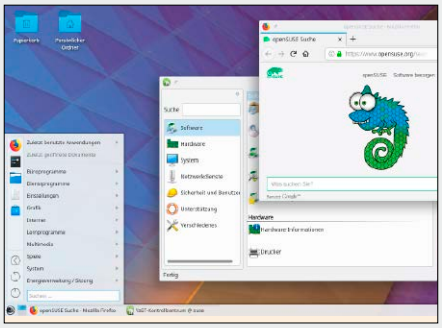
Fedora Workstation 28

Interessant für den Einsatz auf Notebooks: Fedora 28 investiert in die Stromsparmechanismen und verlängert die Akkulaufzeiten signifikant.



Open Suse Leap 15

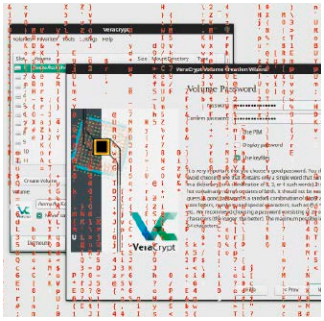
KDE-Desktop und bewährte Yast-Konfiguration: Trotz Tendenz zum Serversystem mit BTRFS bleibt Open Suse ein Kandidat für den PC-Desktop.



Manjaro 17.1.10

Derzeit hoch im Kurs: Das Arch-Derivat Manjaro ist ein Rolling Release mit Vor- und Nachteilen – immer aktuell mit gelegentlichem Korrekturbedarf.

Software & Distributionen



Netzwerk & Server

Praxis

Standards

Sechsmal Linux

Für Einsteiger und Experten

Linux Mint 19 (64 Bit)
Highlight dieser Ausgabe ist das einsteigerfreundliche Linux Mint 19 mit Cinnamon-Desktop. Ein neuer Willkommensbildschirm stellt das System vor und hilft bei der Ersteinrichtung. Mit dem vorinstallierten Programm Timeshift gibt es eine Snapshotfunktion. Das Installationsprogramm von Linux Mint ist dem Installer von Ubuntu sehr ähnlich, unterstützt aber weiterhin die Verschlüsselung des Home-Verzeichnisses. Das System liegt auch als ISO-Datei zur Übertragung auf USB-Sticks auf Heft-DVD.

Fedora 28 Workstation (64 Bit)
Das von Red Hat unterstützte und mitentwickelte Fedora bleibt eine Distribution, die technisch weit vorauseilt, um neugierigen Anwendern ein System mit den neuesten Linux-Entwicklungen zu zeigen. So verbessert Fedora 28 mit Gnome 3.28 die Akkulaufzeit auf Notebooks. Die Ausgabe auf Heft-DVD (auch als ISO-Datei vorhanden) wurde im Juni mit neuen Paketen aktualisiert.

Ubuntu Budgie 18.04 (64 Bit)
Zu einer beliebten Alternative zum regulären Ubuntu mit Gnome-Desktop ist Ubuntu Budgie geworden. Bei Budgie handelt es sich um eine Abspaltung von Gnome, die traditionelle Bedienkonzepte zurückbringt und sich mit Panels gut anpassen lässt. Dies ist eine offizielle Ubuntu-Variante mit drei Jahren Support. Das System liegt auch als ISO-Datei auf Heft-DVD.

Manjaro 17.1.10 Cinnamon Minimal (64 Bit)
Cinnamon ist als Desktopumgebung nicht nur unter Linux Mint zu Hause, wie Manjaro in dieser Version zeigt. Das installierbare Livesystem erleichtert den Einstieg in Arch Linux mit dem komfortablen grafischen Installationsassistenten Calamares und seiner grafischen Paketverwaltung. Hier handelt es sich um die Minimalvariante Manjaros, die nach der Installation mit den gewünschten Programmen ergänzt werden muss. Das System liegt auch als ISO-Datei auf Heft-DVD.

Open Suse Leap 15 (64 Bit)
Wieder als Livesystem: Open Suse Leap zeigt sich mit neuem Versionsschema, das die enge Verwandtschaft zum Suse Linux Enterprise Server signalisiert. Das Linux-System arbeitet mit dessen Systembasis und übernimmt viele Pakete des Servers. Auf DVD liegt Open Suse Leap 15 mit KDE-Desktop, sowohl direkt bootfähig als auch als ISO-Datei für UEFI-Installationen. Der bekannte Installer Yast kann auch andere Desktopumgebungen als KDE einrichten.

Ubuntu Server (mini.iso) 18.04 (64/32 Bit)
Dies sind keine Livesysteme, sondern bootfähige textbasierte Installer in 32 und 64 Bit, die Ubuntu 18.04 als Server oder auch mit Desktopumgebungen einrichtet. Der Installer stammt von Debian. Eine Paketauswahl nach Gruppen erlaubt die individuelle Zusammenstellung des Ubuntu-Systems. Gleichzeitig ist dieser Installationsweg weiterhin eine Option, alle offiziellen Varianten Ubuntu auf 32-Bit-Hardware einzurichten, obwohl es keine Livesysteme mehr mit 32 Bit von Ubuntu gibt.

Extras & Tools

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

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

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

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

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

Software auf DVD

Imgburn 2.5.8.0
Kompaktes deutschsprachiges Brennprogramm für alle Windows-Versionen, um Imagedateien auf CDs/DVDs zu schreiben. Werbefinanzierte Freeware.

Unetbootin 6.61
Das nützliche Tool mit grafischer Oberfläche transferiert mit wenigen Klicks die ISO-Images von Ubuntu und seinen Abkömmlingen wie Linux Mint sowie einige Distributionen mehr auf USB-Stick oder Speicherkarten und macht diese mit einem eigenen Bootmenü startfähig. Auf DVD finden sich 32-Bit und 64-Bit-Ausgabe für Linux (alle Distributionen), aber auch eine Version für Windows und Mac-OS.

Putty 0.70
Putty ist ein Terminalclient für SSH und Telnet, der für alle Windows-Systeme geeignet ist. Putty liegt als ausführbare EXE-Datei vor, die keine Installation erfordert. Das Open-Source-Programm ist englischsprachig.

Kitty 0.70.0.2
Als Abspaltung von Putty ist Kitty ebenfalls ein Terminalclient für SSH, allerdings mit einigen ergänzten Funktionen. 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.

Tresore.txt
Passworttresor selbst gebaut: Begleitend zu einem Artikel im Heft (Seite 54) zeigt diese Script-Sammlung, wie sich mit sehr einfachen Möglichkeiten unter Linux ein Passwortsafe selbst bauen lässt. Die Textdatei versammelt sechs verschiedene Scripts.

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 5/18
Nachsehen und Nachlesen: 303 Seiten Linux-Wissen umfasst die aufgefrischte PDF-Datei dieser LinuxWelt. Zum Nachschlagen sind neben Grundlagenthemen auch Teile der Specials aus den letzten Heften vertreten. Ergänzend zum aktuellen Ubuntu-Special sind die Ubuntu-Beiträge zum neuen Ubuntu 18.04 der letzten Ausgabe enthalten. Neue Beiträge in der Rubrik „Distributionen“ stellen Linux-Systeme vor und die Kategorie „Netzwerk und Internet“ bietet Praxis zu Linux Server im LAN und Internet.

EXTRA: VIDEOTUTORIALS

Die Heft-DVD enthält diesmal zehn Videotutorials des Youtubers Dominik Zerbe. Das Spektrum reicht von Einsteigerthemen bis zu einer Betrachtung von Free BSD und Slackware. Insgesamt ist der Ton aber kurzweilig und leicht gehalten. Der Youtube-Kanal „DominikSoftware“ findet sich unter https://*www.youtube.com/channel/UCnDo8BSkAEdJbVrjFlYUxyw*. Alle Videos liegen werbefrei im MP4-Format auf Heft-DVD im Unterverzeichnis „Videos“. Als Player kommt der VLC in Frage oder Gnome Videos mit H264-Codec.

WEITERE INFOS

Die Vorstellung der Systeme auf DVD beginnt ab Seite 10. Zu Linux Mint 19 gibt es detaillierte Einzelartikel auf den Seiten 14–21. Zusätzliche Anleitungen und Hinweise zu den Distributionen liefert die Übersicht auf Heft-DVD, die Sie über die Datei „index.html“ in einem Browser öffnen. In diesem Heft gibt es zwei Specials: Das erste dreht sich ab Seite 30 um Tipps, Problemlöser und Ergänzungen für Ubuntu 18.04. Im Special ab Seite 42 geht es um den praktischen Umgang mit Passwörtern, Passwortsafes, Zertifikaten und Schlüsseln, die zur sicheren Kommunikation unerlässlich sind.

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

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

Sagen Sie uns Ihre Meinung – und gewinnen Sie!

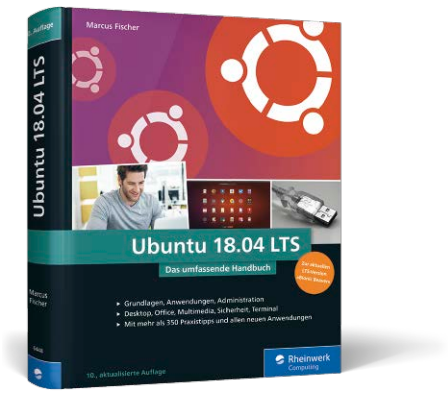
Wir möchten Linux-Hefte machen, die ganz Ihren Bedürfnissen und Interessen entsprechen. Dabei können Sie uns helfen! Füllen Sie einfach unseren Fragebogen im Internet aus. Das Beantworten der Fragen dauert nur rund zehn Minuten.

Unter allen Teilnehmern verlosen wir 3 Exemplare des Buches „Ubuntu 10.04 LTS“ aus dem Rheinwerk Verlag.

Ubuntu 18.04 LTS

Das umfassende Handbuch

Grundlagen, Anwendungen, Administration, Desktop, Office, Multimedia, Sicherheit, Terminal. Mit mehr als 350 Praxistipps und allen neuen Anwendungen



Marcus Fischer, September 2018, 100 Seiten, gebunden, Rheinwerk Verlag
ISBN: 978-3-8362-6448-8, 49,90 €

Ohne Unity, aber mit vielen neuen Ideen kommt die Ubuntu-Version „Bionic Beaver“ daher. Und dieses Handbuch macht Sie zum Ubuntu-Allrounder und bietet Ihnen alles, was Sie für den Linux-Alltag brauchen: vom neuen Gnome-Desktop, der Paketverwaltung mit Snap und apt bis hin zu fortgeschrittenen Themen wie Virtualisierungstechniken und Netzwerkkonfiguration. Zusätzlich gibt es über 350 bewährte Tipps und Tricks aus der Praxis sowie eine umfassende Kommandoreferenz, damit Sie sich schnell zum Ubuntu-Experten spezialisieren können.

Aus dem Inhalt:
• Installation und Einsatz des Livesystems • Upgrade von früheren Versionen • Konfiguration des Systems • Der neue GNOME-Desktop • Libre Office • Multimedia • Netzwerk • Dateiserver • Einsatz externer Geräte • Desktop- und Servervirtualisierung • Arbeiten mit der Shell • Kommandoreferenz • zahlreiche Praxistipps und Schritt-für-Schritt-Anleitungen • 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 5/2018 ist der 25.9.2018.**

Datenschutz: Wenn Sie gewinnen, schicken wir Ihnen den Preis per Post zu. Deshalb fragen wir Sie auch nach Ihrer Adresse.

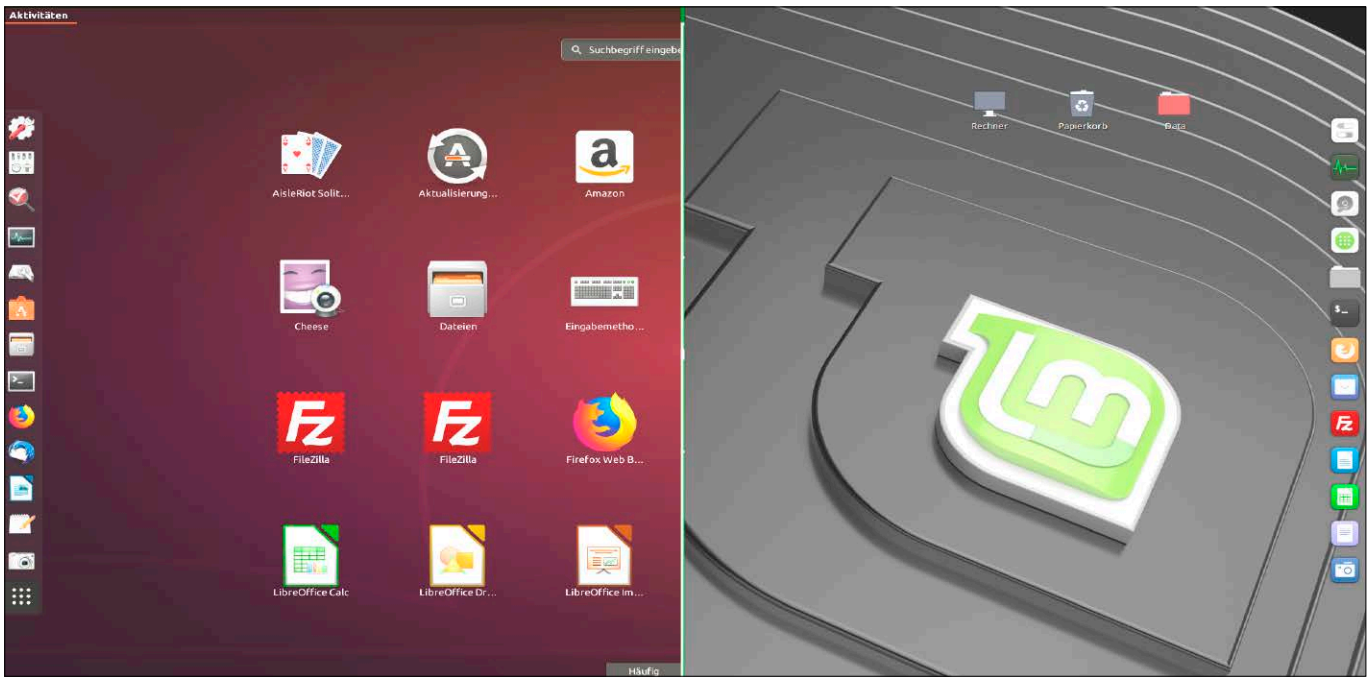
Datenschutzerklärung: Alle auf unserer Webseite erhobenen Daten werden entsprechend den Vorschriften des Bundesdatenschutzgesetzes (BDSG) und des Informations- und Telekommunikationsdienstegesetzes (IuTDG) behandelt. Eine Weitergabe der Daten an Dritte ohne ausdrückliche Einwilligung des Betroffenen erfolgt nicht. Weitere Infos finden Sie unter *www.pcwelt.de/datenschutz*

Jeder Teilnehmer bekommt als Dankeschön die LinuxWelt XXL 2/2018 „Das Handbuch 2018“ als PDF (ohne Datenträger).

Sie finden den Link zum Download des Hefts am Ende der Leserbefragung.

Desktop-Weltmeister

Das brandneue Linux Mint 19 aktualisiert pflichtgemäß seinen Systemunterbau auf Ubuntu 18.04, hält aber nebenbei noch einige Überraschungen parat. Es lässt keinen Zweifel, dass es am Desktop gegenüber Ubuntu das engagiertere Projekt ist.



VON HERMANN APFELBÖCK

Im Juli 2018 wurde nicht nur der Fußballweltmeister 2018 ermittelt, sondern auch der Desktop-Weltmeister 2018. So richtig spannend sind die Duelle am Linux-Desktop aber aktuell nicht. Die Rangliste am Linux-Desktop wird immer eindeutiger, weil sich Canonical mit Ubuntu zunehmend zurückzieht. Ubuntu hat manches Talent gefördert, aber nach plötzlichen Taktikwechseln auch wieder fallengelassen (Unity, Mir, Wayland).

Ubuntu 18.04 LTS vom April ist solide, aber keinesfalls ambitioniert. Bei der Rückkehr zu Gnome hat man selbigen zwar aufgepeppt, aber Gnome bleibt ein externer Spieler, dessen Entwicklung Canonical nicht selbst in der Hand hat. Der Wayland-Displayserver, sofern man sich an Ubuntu-LTS-Versionen hält, bleibt weitere zwei Jahre bis zur nächsten LTS-Ausgabe 20.04 auf der Auswechselbank. Der Ubuntu-Installer bringt zwar eine neue „Minimal"-Option, lässt aber andererseits die viel wichtigere Home-Verschlüsselung unter den Tisch fallen. Unterm Strich bleibt die Integration der Snap-Pakete in den grafischen Paketmanager die Maßnahme des letzten Entwicklungsjahres, die dem Ubuntu-Anwender den größten Komfortgewinn bringt.

Linux Mint auf der anderen Seite hat keine Ressourcen für technische Visionen. Es spielt opportunistisch und pragmatisch mit einer ausgeliehenen Ubuntu-Basis und etlichen externen Ergänzungsspielern wie neuerdings Timeshift. Die Mannschaft um den einzigen Star Cinnamon im Zentrum scheint zusammengewürfelt, harmoniert aber inzwischen in jedem Detail. Das kleine Mint-Team darf für sich in Anspruch nehmen, mit der jüngsten Version 19 das bestmögliche Linux für den PC-Endbenutzer anzubieten. Statt Desktopirrungen gibt es ein unverdrossen weitergeschliffenes Cinnamon. Zur Fokussierung wurde KDE abgeworfen, XFCE und Mate laufen ohne große Investionen für ältere Hardware mit. Um den Aufwand für XFCE und Mate weiter zu minimieren, hat Mint die desktopunabhängigen X-Apps (Xed, Xplayer, Xviewer) entwickelt.

Die Strategie von Linux Mint ist pragmatisch und langfristig: Abhängigkeiten von Ubuntu werden vermieden. Beim Trend zur vereinfachten Softwareverteilung mit Containernpaketen greift Linux Mint daher lieber zum Flatpak-Format als zum Canonical-Format Snap. Und nebenher pflegt man noch eine komplette Ersatzmannschaft mit der Linux Mint Debian Edition, die eine Zukunft des Cinnamon-Desktops notfalls auch ganz ohne Ubuntu-Hilfe garantiert.

Ubuntu 18.04 und Linux Mint 19

Wir sind der Ansicht, dass an Linux Mint mit Cinnamon derzeit keine Ubuntu-Edition heranreicht. Aber das kann jeder Nutzer selbst entscheiden und Gnome-, KDE- oder Budgie-Fans haben sicher auch gute Argumente. In diesem Heft sind daher beide Distributionen gut vertreten: Ab Seite 30 gibt es ein Ubuntu-Special, das sich mit System- und Desktopoptimierung, mit Snap-Paketen und der Servereinrichtung befasst. Zu Linux Mint 19 finden Sie ab Seite 14 eine Vorstellung der aktuellen Version, gefolgt von einer ausführlichen Praxiseinführung. Die Heft-DVD begleitet diese Desktopthemen mit der Mint-Standardedition und der Ubuntu-Variante Budgie.

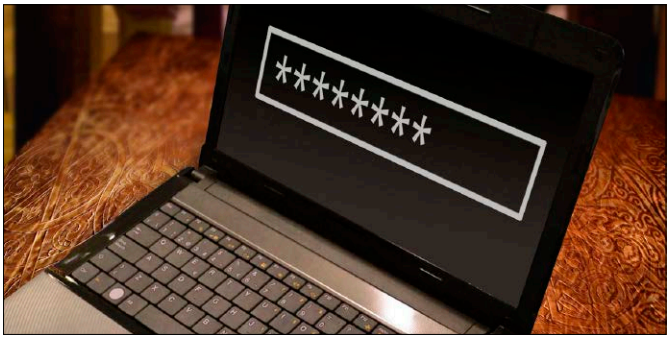
Alles zum Thema „Passwörter“

Das große Special in dieser Ausgabe dreht sich ab Seite 42 um „Passwörter“ aller Art. Hier geht es um Kennwortstrategien, um die unterschiedliche Sensibilität von Passwörtern und um eine möglichst komfortable und sichere Aufbewahrung aller Kennwörter. Daher kommen neben einem gut geschützten Browsertresor auch universelle Passwortverwaltungen zu Wort, die nicht nur die Onlinedaten verwahren. Und wer sich mit externen Passwortmanagern nicht anfreunden will, erhält praktische Anleitungen für einen selbst gebauten Kennworttresor. Der Schwerpunkt liefert ferner technische Grundlagen zu System-, SSH-, Samba-Passwörtern, Schlüsseldateien, Zertifikaten, zur Luks-Datenträgerverschlüsselung und zu speziellen Sicherheitsmaßnahmen wie die Zwei-Wege-Authentifizierung.

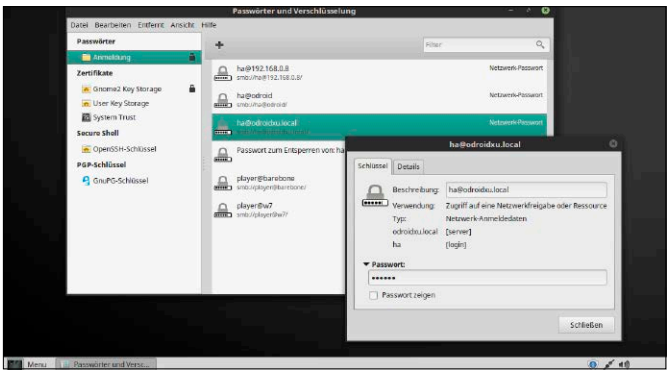
Die Heft-DVD

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 sowie beliebigen Aktionen im Livesystem bleiben Ihre Festplatte und das dort installierte Betriebssystem komplett unberührt. Erst mit der optionalen Installation aus dem Livesystem heraus ändern Sie die Partitionierung Ihrer Festplatte.
Die meisten Systeme liegen auch als ISO-Image auf der Heft-DVD (im Verzeichnis „/Image-Dateien“). Damit haben Sie die Möglichkeit, die Systeme selbst auf CD/DVD oder USB-Stick zu schreiben. ■

Alles über Passwörter, Schlüssel und Zertifikate: Welche Kennwörter sind sensibel, welche nicht? Das Heftspecial gibt strategische Ratschläge.



Passwortverwaltung und einschlägige Tools: Der Browser versammelt Onlinekennwörter, für andere Passwörter gibt es Spezialisten oder Script-Lösungen.



AUF DVD

10 Fedora Workstation 28 *(64 Bit)*
Das neue Red-Hat-Desktopsystem

11 Open Suse Leap 15 *(64 Bit)*
KDE-Desktop auf BTRFS-Dateisystem

12 Manjaro Cinnamon *(64 Bit)*
Arch-Derivat mit Mint-Desktop

13 Ubuntu Budgie 18.04 LTS *(64 Bit)*
Ubuntu-Variante mit Budgie-Desktop

13 Ubuntu Server 18.04 *(32/64 Bit)*
Bootfähiger Ubuntu-Installer

14 Linux Mint 19 Cinnamon *(64 Bit)*
Hauptausgabe von Linux Mint 19

Extras und Tools
Boothelfer und Hardwareanalyse: Supergrub, Memtest, HDT, DBAN

Software für Linux und Windows
Tools für Imagedateien: Unetbootin, Imgburn, Win 32 Disk Imager, 7-Zip

LinuxWelt Digital XXL (PDF)
303 Seiten technische Grundlagen

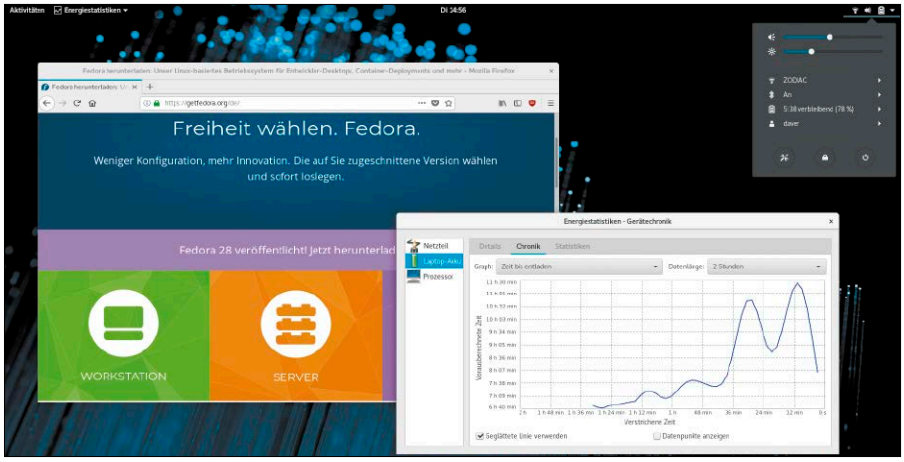
„Wahl-O-Mat“
Informationssystem zur Auswahl der passenden Linux-Distribution

Linux-Videos: Praxis und Distributionen
Linux-Tutorials vom Youtube-Kanal *www.youtube.com/channel/UCnDo8BSkAEdJbVrjFIYUxyw*

Fedora 28 Workstation

Unerhört: Fedora brach mit der eigenen Tradition und erschien ausnahmsweise pünktlich. Auch sonst macht die Workstationausgabe (in 64 Bit auf Heft-DVD) vieles anders als die Vorgängerversion, um bei Desktopanwendern wieder zu punkten.

VON DAVID WOLSKI



Läuft auf Anhieb als Gast in Virtualbox: Fedora 28 bringt Treiber für Virtualbox mit. Auch Wayland – schon eine Weile der Standard in dieser Distribution – funktioniert reibungslos in der VM.

Eine Weile sah es so aus, als sei der Linux-Desktop dem Branchenriesen Red Hat, der als Sponsor hinter Fedora steht, nicht mehr besonders wichtig. Geld wird schließlich im Serverbusiness verdient. Nun zeigt aber Fedora 28 Workstation eine Reihe an Verbesserungen, die vor allem Desktopanwender nützlich finden werden. Denn es gibt eine unübersehbare Gruppe von Entwicklern und Administratoren, die gerne auch privat mit einer bekannten Linux-Distribution arbeiten. Fedora will dabei jenen professionellen Anwendern gefallen, die Red Hat Enterprise Linux oder Cent-OS auf Servern verwenden und auf dem Arbeits-PC eine ähnliche Linux-Distribution bevorzugen. Gleichzeitig ist Fedora ein Schaufenster für die maßgeblichen Linux-Entwicklungen. Grundsätzliche Neuerungen halten in Fedora meist zuerst Einzug, bevor sie mit Verzögerung von anderen Distributionen adaptiert werden.

Maßnahmen gegen den Strom

Wie angekündigt haben sich Red-Hat-Entwickler um weitere, oft ungenutzte Stromsparfunktionen des Linux-Kernels gekümmert. Auf Notebooks mit Intel-Chipsätzen hält Fedora 28 Workstation merklich länger mit einer Akkuladung durch. SATA-Schnittstellen imitieren jetzt das Verhalten von Windows, um Laufwerke länger in den Schlaf zu versetzen. Auch für Soundchips und USB-Bluetooth-Chips sind Energiesparmodi aktiviert. In der Summe kann Fedora 28 so im Idealfall 1,5 bis 2,3 Watt einsparen. Der Vergleich auf einem Tuxedo Infinitybook Pro 13 belegt dies empirisch und zeigt einen recht deutlichen Unterschied: 4,5 Watt verlangt das Notebook beim Betrieb von Fedora 28 mit Gnome-Desktop ohne geöffnete Programme. Mit Ubuntu 18.04 sind es in der gleichen Konstellation 6,4 Watt. Diese Messungen hat das Tool powerstat vorgenommen, das direkt die Werte aus der Energieverwaltung des Kernels ausliest. Ein externes Repository mit diesem Tool für Fedora 28 findet sich über *https://pkgs.org/download/powerstat*.

Gnome: Erweiterungen optional

Der Desktop der Workstationausgabe ist bei Gnome 3.28 angekommen, der Version, die auch in Ubuntu 18.04 arbeitet. Allerdings läuft Gnome in Fedora standardmäßig unter Wayland und ist immer in seiner puren Form ohne Erweiterungen enthalten. Einige beliebte Erweiterungen wie die von Ubuntu bekannte Seitenleiste „Dash to Dock“ liegen als schnell installiertes Paket in den Paketquellen vor.

Zur weiteren Softwareinstallation gibt es „Gnome Software“, das jetzt auf Wunsch auch selbständig ein paar externe Paketquellen mit Zusatzsoftware aktiviert. So gibt es Chromium, proprietäre Nvidia-Treiber, den Steam-Client und die Entwicklungsumgebung Pycharm mit wenigen Klicks. In der Gnome-Ausgabe ist der Fedora Installer deutlich einfacher geworden, da die Benutzererstellung erst nach dem ersten Bootvorgang erfolgt. Wer Fedora 28, das es nur in 64 Bit gibt, mit anderen Desktops betreiben möchte, bekommt das installierbare Livesystem unter *https://spins.fedoraproject.org/de* auch mit KDE, Cinnamon, Mate, XFCE, LXQT und LXDE.

Schöpft aus fremden Quellen: Gnome Software bietet in Fedora jetzt an, weitere Paketquellen zu aktivieren, beispielsweise für proprietäre Nvidia-Treiber.

Mehr Infos zu Fedora
Website: *https://getfedora.org*
Dokumentation: *http://docs.fedoraproject.org*

Open Suse Leap 15

Open Suse Leap verblüfft mit einer Änderung der Versionsschemas. Hinter der Versionsnummer 15 steht eine Annäherung an die Serverausgabe der Distribution. Auf Heft-DVD liegt Open Suse als installierbares Livesystem mit KDE-Desktop.

VON DAVID WOLSKI

Das Maskottchen der Open-Suse-Distribution ist ein Chamäleon. Und genauso wandlungsfähig hat sich das Linux-System über die Jahre gezeigt: Aus einem Linux-System, das mit dem grafischen Administrationswerkzeug Yast zunächst Einsteigern entgegenkam, ist eine Distribution für ambitionierte Anwender geworden. Open Suse Leap, das erstmals wieder als installierbares Livesystem vorliegt, unterscheidet sich in seinen Schwerpunkten deutlich von anderen Linux-Systemen.

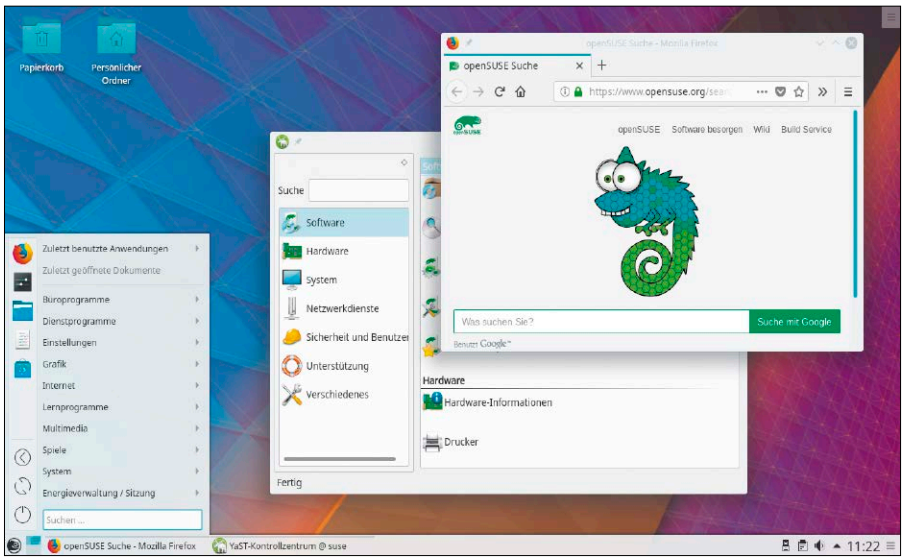
Servermerkmale für den Desktop

Open Suse Leap setzt schon seit einigen Jahren auf das Dateisystem BTRFS, das einmal als neues Standarddateisystem für Linux im Gespräch war und Snapshots auf Dateisystemebene ermöglicht. Das ist nicht nur für Server interessant, sondern auch für Desktops mit hohen Sicherheitsansprüchen. Als Verwaltungswerkzeug dient weiterhin Yast, das nicht nur eine grafische Oberfläche bietet, sondern auch mit textbasierten Menüs auf der Kommandozeile funktioniert.

Die Besonderheiten in der Konfiguration Open Suses bildet Yast gut ab und dient damit der Orientierung, wo sich welcher Schalter findet. Denn die Wege der Administration verlaufen hier oft ganz anders als in Debian/Ubuntu- oder in Red-Hat-Systemen. Wer sich bereits mit Open Suse beschäftigt hat, findet in Yast die vertrauten Einstellungen, aber auch einen verbesserten Partitionierer und ein neues Menü zur Konfiguration des Paketfilters „Firewalld“, der von Fedora übernommen wurde.

Aufgefrischte Software

Auf dem Desktop dient KDE in der Version 5.12 als Standardoberfläche. Der Installer des Livesystems bietet aber auch weitere



Mehr als nur Zahlenspiele: Open Suse Leap, hier mit KDE, trägt jetzt die gleiche Versionsnummer wie der Suse Linux Enterprise Server und teilt sich mit diesem denselben Systemunterbau.

Arbeitsumgebungen an: Es gibt Gnome 3.26 mit dem Displayserver Wayland als zweite prominente Option, in den benutzerdefinierten Paketgruppen aber auch die schlanken Umgebungen Mate, XFCE, LXQT und LXDE.

Bei der Softwareausstattung setzt das System auf bewährte Schwergewichte: Firefox 60 ESR mit Langzeitsupport ist der Standardbrowser, Libre Office 6.0.1 dient als Bürosuite und Gimp liegt noch in Version 2.8 vor. Bei seinem Kernel setzt das System auf Kernel 4.12, den Suse-Entwickler auf eigene Faust pflegen und mit Backports gegen die Lücken Spectre und Meltdown ausgestattet wurde. Insgesamt wird Open Suse Leap 15 drei Jahre mit Aktualisierungen versorgt werden und dabei jährlich ein größeres Update bekommen, das auch die Softwareversionen auf einen neueren Stand bringen kann.

Open Suse Leap 15 spricht vor allem jene Anwender an, die ein sorgfältig zusammengestelltes Linux-System auf dem Desktop oder dem eigenem Server wünschen und

Kann nicht nur KDE: Der Installer des Livesystems bietet jetzt auch andere Desktopumgebungen an sowie die Einrichtung von Serversystemen.

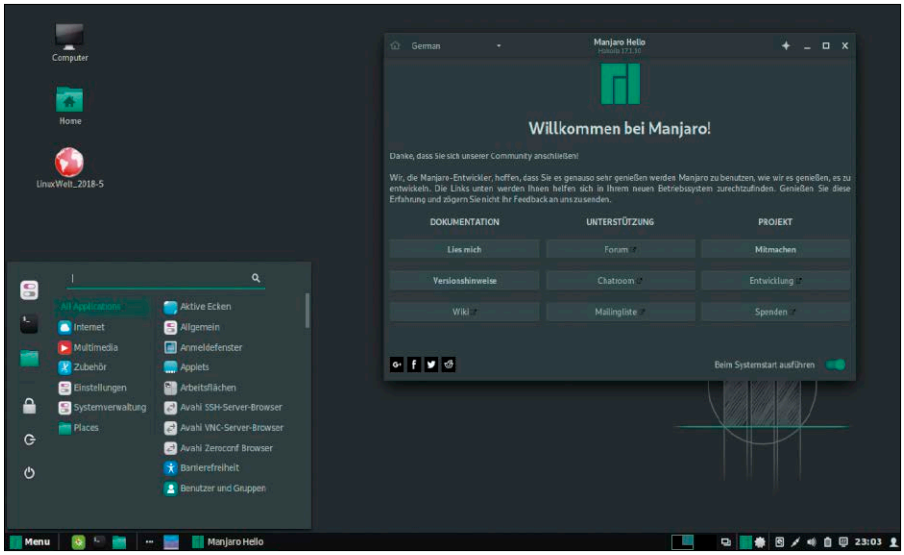
schon über fundierte Linux-Kenntnisse verfügen. Eine ausgesprochen einsteigerfreundliche Distribution ist Open Suse nicht, dafür aber ein Aushängeschild für vielversprechende Linux-Technologien wie BTRFS.

Mehr Infos zu Open Suse
Website: *www.opensuse.org*
Dokumentation: *https://doc.opensuse.org*

Manjaro 17.1.10 Cinnamon

Der Cinnamon-Desktop ist nicht nur in Linux Mint zu Hause. Auch der Arch-Linux-Abkömmling Manjaro hat diese Arbeitsoberfläche adoptiert. Das System auf Heft-DVD (64 Bit) installiert ein minimales System zur eigenen Ergänzung mit Programmen.

VON DAVID WOLSKI



Cinnamon mal anders: Manjaro pflegt zahlreiche Desktops in seinen Communityausgaben. Ein grafischer Installer richtet den Arch-Abkömmling schnell und komfortabel ein.

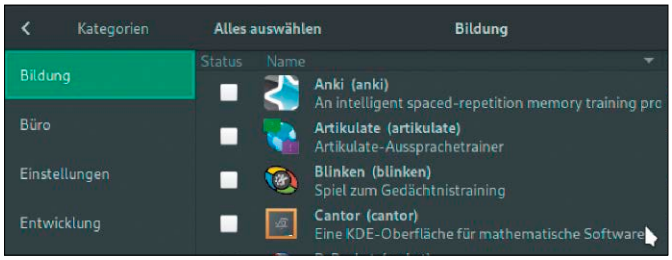
Der Weg zu einem optimal eingerichteten Arch Linux muss nicht lang und steinig sein, wie Manjaro seit fünf Jahren mit seinen Installationsmedien zeigt. Tatsächlich ist Manjaro aus seinem installierbaren Livesystem heraus mit dem Installer Calamares schnell und komfortabel eingerichtet. Der Ablauf orientiert sich an der Ubuntu-Installation. Das darf aber nicht darüber hinwegtäuschen, dass Manjaro genauso wie pures Arch Linux im Dauerbetrieb als Rolling Release immer wieder Überraschungen parat hat (siehe auch den Beitrag ab Seite 66). Deren Lösungen finden sich meist über eine hartnäckige Onlinerecherche in den Supportforen von Arch und erscheinen mit wachsender Erfahrung weniger obskur.

Auf Heft-DVD liegt Manjaro mit dem Cinnamon-Desktop, dessen Aufmachung von Linux Mint inspiriert ist. Anders als Linux Mint ist Manjaro in dieser Version aber eine sehr schlanke Minimalversion. Es gibt alle wichtigen Tools, aber große Softwarepakete wie Libre Office, Firefox, Chromium, Gimp sind nicht vorinstalliert. Diese Manjaro-Variante verlangt nach einer Einrichtung mit Programmen über „Systemeinstellungen → Software hinzufügen/verwalten“ oder mit dem Arch-Paketmanager pacman in der Kommandozeile.

Arch ohne Krach

Manjaro ist kein Einsteigersystem, sondern eine Linux-Distribution für Enthusiasten, die sich aktuelle Pakete wünschen und ein möglichst leistungsfähiges System – und dabei noch eine Menge über Linux lernen möchten. Manjaro entschärft die Situation allerdings durch eigene Repositories, in welchen Arch-Pakete etwas länger liegen bleiben, um mögliche Probleme bei großen Updates zumindest durch eine Karenzzeit zu entschärfen. Erfahrungsgemäß ist es bei Arch-Installationen alle paar Monate nötig, manuell die Konfiguration anzupassen, Paketkonflikte zu beheben oder neue Paketsignaturen einzulesen. Anwender von Manjaro haben immerhin die Sicherheit, dass diese Probleme bereits dokumentiert sind, wenn die neuen Pakete auf den Rechner kommen. Nach dem obligatorischen Warnhinweis, für wen ein Arch-Linux-Abkömmling wie Manjaro gemacht ist, zu den vielen Vorzügen: Die Aktualität der beständig aktualisierten Programmversionen lässt andere Linux-Distributionen alt aussehen.

Zugriff auf AURs: Die Benutzer-Repositories „AURs“ (Arch User Repositories) liefern für Arch wie Manjaro eine riesige Auswahl weiterer Software. Das Build-System von Arch kann aus diesen Repositories passend für das eigene System weitgehend automatisch Pakete kompilieren. Genau diese Fähigkeit macht Arch und Arch-basierende Systeme wie Manjaro besonders und bei fortgeschrittenen Anwendern beliebt. Das empfohlene Kommandozeilentool Trizen für den Zugriff auf AURs ersetzt das ältere und nicht mehr aktiv entwickelte Tool Yaourt und liegt zur Installation in den Manjaro-Paketquellen.



Gut eingerichtet: Auf DVD liegt Manjaro mit Cinnamon in einer Minimalversion. Der grafische Paketmanager hat die benötigten Programme aber schnell nachinstalliert.

Mehr Infos zu Manjaro

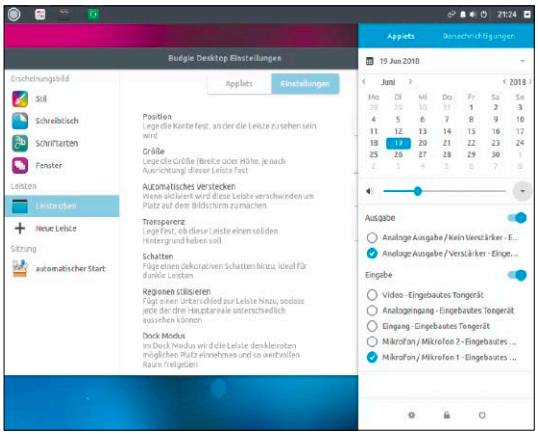
Website: *http://manjaro.org*

Dokumentation: *http://wiki.manjaro.org*

Ubuntu Budgie 18.04

VON DAVID WOLSKI

Wer sich mit dem gewöhnungsbedürftigen Gnome-Desktop von Ubuntu 18.04 nicht anfreunden will, bekommt mit Ubuntu Budgie eine neue Alternative (64-Bit-Version auf DVD). Erst vor einem Jahr ist aus einer experimentellen Ubuntu-Version mit dem Budgie-Desktop, welcher in der unabhängigen Distribution Solus entstand, ein offizielles Ubuntu geworden. Dieser Neuzugang hat nach dem Wechsel des primären Ubuntu-Desktops zu Gnome schnell viele Anhänger gefunden, zumal Budgie auch schon länger als ausgereift gilt. Es gibt links oben ein klassisches ausklappendes Anwendungsmenü, das Programme auch per Volltextsuche findet. Das obere Panel, das man auch am linken oder unteren Bildschirmrand festmachen darf, dient als Dock, das Favoriten sowie laufende Programme als Symbol zeigt. Eine weitere großzügige Seitenleiste für Kalender und Applets klappt sich bei Bedarf nach einem Klick auf das Pfeilsymbol im Infobereich des Panels aus.



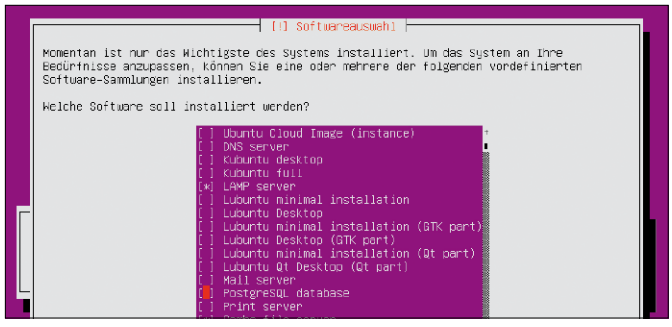
Die Softwareausstattung ist ähnlich wie jene von Ubuntu mit Gnome, allerdings dient Chromium statt Firefox als Standardbrowser. Der Anmeldebildschirm ist weiterhin von Lightdm und nicht von Gnome. So wie die reguläre Ubuntu-Variante mit Gnome präsentiert der Installer die Option, Ubuntu Budgie 18.04 als „Minimale Installation“ einzurichten. In diesem Fall verzichtet die Distribution darauf, Programme wie Libre Office einzurichten, und begnügt sich mit einer kleinen Auswahl. Die restliche Einrichtung bleibt dann dem Nutzer überlassen, der die Programme über den grafischen Paketmanager Gnome Software installieren kann.

Mehr Infos zu Ubuntu Budgie
Webseite: *https://ubuntubudgie.org*
Dokumentation: *https://wiki.ubuntu.com/BionicBeaver/ReleaseNotes*

Ubuntu Server 18.04 (mini.iso)

VON DAVID WOLSKI

Adieu, 32 Bit? Nicht ganz: Obwohl sich die reguläre Ausgabe von Ubuntu 18.04 für Desktop und Server die Installationsmedien für 32-Bit-Prozessoren gespart hat, ist die Plattform nicht ganz gestrichen. Weiterhin sind nahezu sämtliche Pakete in den Ubuntu-Repositories auch in 32 Bit verfügbar (i386-Plattform). Zur Installation dienen jetzt aber nur noch diese minimalen Installationsmedien, die im Textmodus starten und dann alle Pakete direkt aus dem Repository herunterladen.
Auf diese Weise kann Ubuntu 18.04 für Server oder mit beliebigen Desktops auf 32-Bit-Rechnern installiert werden, zu denen auch gar nicht so alte PCs mit Intels Atom-CPU gehören. Im Gegensatz zu den üblichen Ubuntu-Varianten, die als Livesystem vorliegen, booten diese Medien ein Installationsprogramm im Stil von Debian in 32/64 Bit. Auf Wunsch kann das Installationsprogramm gleich auf Deutsch umgeschaltet werden. Es gibt einen Partitionierer, der wie das grafische Pendant verschlüsselte Partitionen über den Logical Volume Manager (LVM) einrichtet, ein Software-Raid konfiguriert oder iSCSI-Targets aufnimmt.

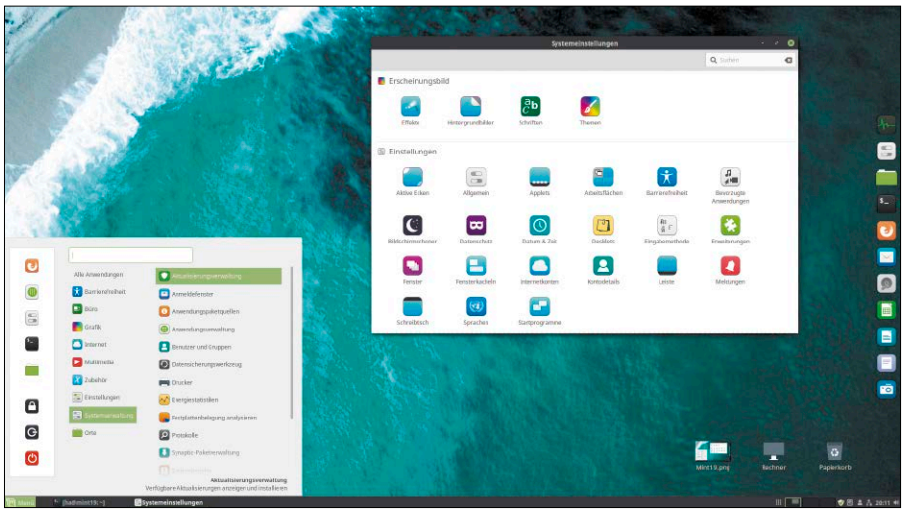


Die Größe vorhandener Partitionen kann der Partitionierer auch ändern. Eine Paketauswahl nach Gruppen erlaubt die individuelle Zusammenstellung des Ubuntu-Systems. Wer möchte, kann fertige Paketgruppen für bestimmte Serveraufgaben installieren, um beispielsweise einen kompletten Lamp-Stack (Linux, Apache, My SQL, PHP) aufzusetzen. Es gibt aber auch die Möglichkeit, ein grafisches System mit den üblichen Desktops von Gnome bis LXDE einzurichten.

Mehr Infos zu Ubuntu Server
Website: *www.ubuntu.com/download/server*
Dokumentation: *https://help.ubuntu.com/community/Installation/MinimalCD*

Neu und schnell: Linux Mint 19

Angekündigt war Version 19 als reine Pflichtübung, um den Cinnamon-Desktop und die Mint-Tools auf den Unterbau des aktuellen Ubuntu 18.04 zu setzen. Aber für einige Überraschungen ist Linux Mint immer gut.



VON HERMANN APFELBÖCK

Das auf Ubuntu basierende Linux Mint stellt sich mit Version 19 „Tara“ wieder auf die aktuellste Ubuntu-Systembasis mit Kernel 4.15 und liefert frische Softwarepakete mit – unter anderem Firefox 60, VLC 3.0 und Libre Office 6.0. Wie Ubuntu 18.04 erhält Mint 19 Langzeitsupport für fünf Jahre bis April 2023. Dies gilt für alle drei verbleibenden Mint-Editionen: Nachdem sich das Mint-Team kürzlich von KDE verabschiedet hat, bleiben noch die Varianten mit Cinnamon, Mate und XFCE.

Das von Heft-DVD startende 64-Bit-Livesystem ist die Standardedition mit dem angestammten Cinnamon-Desktop. Cinnamon ist das Aushängeschild von Linux Mint und ursprünglicher Anlass, überhaupt eine neue Linux-Distribution zu begründen. Hier liegt der Hauptehrgeiz des Mint-Teams und auch das jüngste Cinnamon 3.8 bringt wieder einige Neuerungen. Die Mate- und XFCE-Edition enthalten die allgemeinen Neuerungen an der Systembasis, die beiden Desktops selbst zeigen aber keine Änderungen gegenüber Mint 18.3. Linux Mint 19 mit Mate oder XFCE können Sie wie gewohnt über die Projektseite *https://linuxmint.com* beziehen, die zu den Spiegelservern für den Download führt.

Linux Mint 19 mit Home-Verschlüsselung

Ein auffälliger Unterschied zur Systembasis Ubuntu 18.04 ist die Installeroption „Meine persönlichen Daten verschlüsseln beim Anlegen des ersten Benutzerkontos (im Fenster „Wer sind Sie?“). Die Ubuntu-Entwickler hatten diese Verschlüsselung des Home-Verzeichnisses mit Ecryptfs ersatzlos gestrichen. Die Gründe sind nicht ganz von der Hand zu weisen, wie im Artikel ab Seite 34 angesprochen wird. Dennoch hat sich das Mint-Team entschlossen, dies in den Ubiquity-Installer zurückzubauen.

Aus Anwendersicht ist diese Situation durchaus heikel: Man kann die Mint-Entscheidung begrüßen, die Bedenken der Ubuntu-Entwickler als paranoid zurückweisen und unter Mint weiterhin die Home-Verschlüsselung nutzen. Wer sich hingegen der Einschätzung Canonicals anschließt, wird wie bei Ubuntu auf Alternativen zurückgreifen müssen. In Frage kommt die Datenträgerverschlüsselung (Luks) während der Installation oder nachinstalliertes Veracrypt, das in diesem Heft ab Seite 68 ausführlich zu Wort kommt.

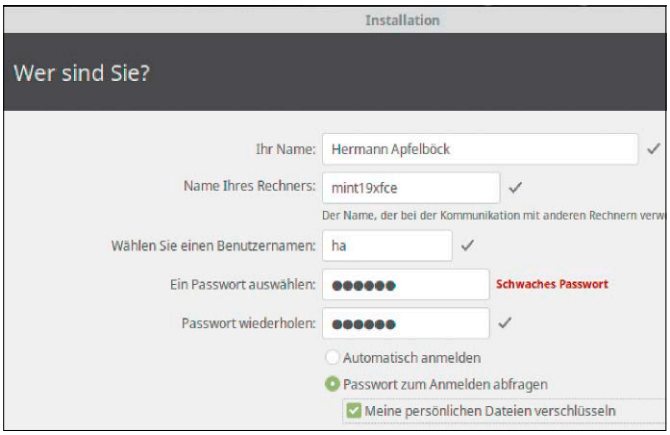
Systemaktualisierung & Timeshift

Die Snapshotsicherung mit Timeshift wurde mit Linux Mint 18.3 eingeführt, erhält aber in Version 19 eine ungleich zentralere Rolle. Die beginnt schon am automatisch startenden Willkommen-Bildschirm an oberster Stelle bei „Erste Schritte“. In der wichtigen „Aktualisierungsverwaltung“ erscheint ein farbig hervorgehobener Hinweis, die „Systemschnappschüsse“ einzurichten, falls dies noch nicht geschehen ist. Im Gegenzug verzichtet Mint 19 aber auf das jahrelang geltende Stufenkonzept, das systemnahe Updates standardmäßig nicht installiert hat – nur auf ausdrücklichen Wunsch des Nutzers. Das Stufenkonzept ist in der „Aktualisierungsverwaltung“ unter „Einstellungen → Ebenen“ zwar noch existent, Linux Mint 19 lässt jetzt aber auch „sensible“ Updates der Stufe 4 auf das System. Absicherung im Falle des Falles sollen eben jene Timeshift-Snapshots gewähren, die Mint 19 allerorts anbietet. Technisch hat sich bei Timeshift gegenüber der Mint-Version 18.3 nichts geändert: Bevorzugte Methode wird die Sicherung mit rsync bleiben, da die Alternative mit BTRFS dieses

Dateisystem voraussetzt, aber eine Standardinstallation weiterhin Ext4 bevorzugt. Nebenbei kommen nun alle Kernel-Updates als Metapakete. Bekanntlich werden alte Kernel-Versionen nach Kernel-Updates aus Sicherheitsgründen archiviert. Dies fordert Speicherplatz und verlängert die Liste des Bootmanagers beim Systemstart. Durch den Einsatz von Metapaketen können alte Kernel ab sofort bequem mit dem allgemeinen

```
sudo apt autoremove
```

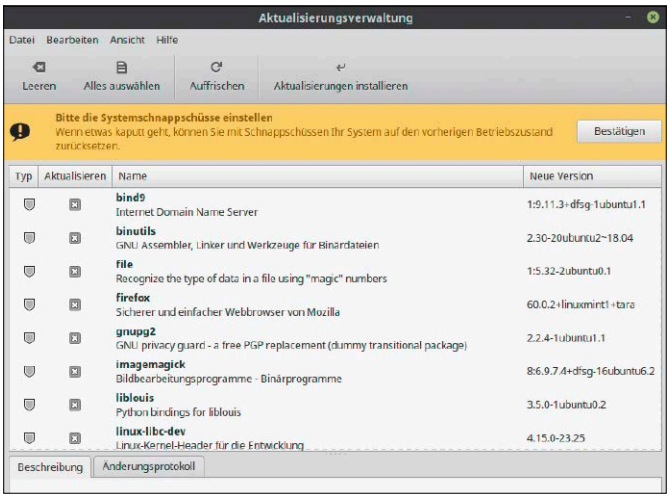
gelöscht werden, sofern sich ein Kernel-Update als problemlos erwiesen hat.



Linux Mint hält an der Home-Verschlüsselung fest: Der Nutzer muss entscheiden, ob er der Ubuntu- oder der Mint-Einschätzung zu Ecryptfs folgen will.

Kleine Verbesserungen für alle Mint-Editionen

Willkommen-Dialog: Mintwelcome hat erheblich gewonnen und avanciert zur praktischen Einstiegshilfe vor allem für Linux-Anfänger. Wirklich praxisnah ist die Rubrik „Erste Schritte“, die Anfängern sofort die wichtigsten Systemzentralen nahebringt.
Dateimanager: Nemo hat ein kleines, aber hübsches Feature erhalten: Eine Dateisuche kann durch Klick auf das kleine Sternchen im Suchfeld dauerhaft gespeichert werden. Diese Suche ist durch Rechtsklick auf das Sternchen später jederzeit wieder abrufbar. Nicht mehr benötigte Suchjobs werden durch normalen Klick auf das Sternchen wieder gelöscht.
Texteditor: Die X-App Xed erhält einen wesentlich klareren Einstellungsdialog, der statt Registerkarten eine Navigationsspalte verwendet. Der Optionsumfang hat sich, abgesehen von einem Plug-in zur Wortergänzung (unter „Erweiterungen“) nicht geändert.
HiDPI: Die Unterstützung hochauflösender Bildschirme wurde in allen Editionen verbessert. Das Standardthema Mint-Y bietet außerdem extragroße Symbole, um die Darstellung bei HiDPI zu optimieren.
USB-Stick-Formatierer: Mintstick erweitert die bisher unterstützten Dateisysteme (FAT32, NTFS und Ext4) um das Microsoft-Dateisystem exFAT.



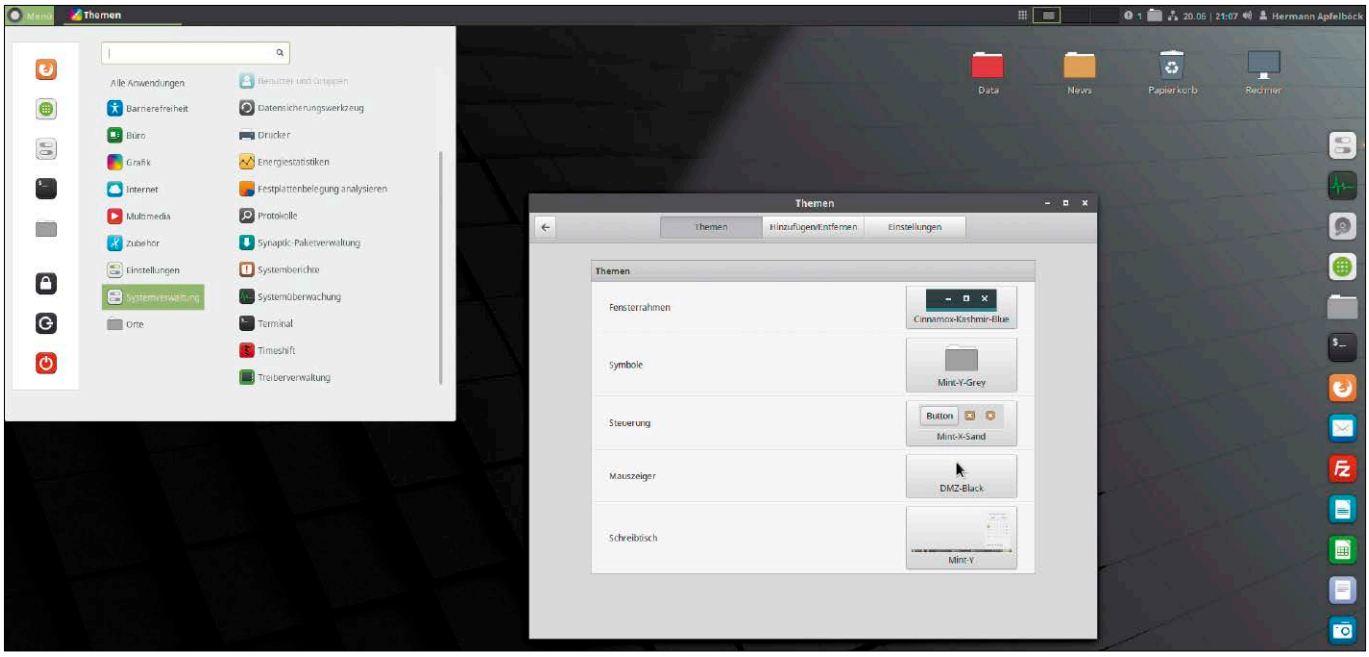
Linux Mint stellt das externe Timeshift in den Mittelpunkt: Timeshift-Schnappschüsse werden an mehreren Stellen dringend empfohlen bis angemahnt.

Der Desktop Cinnamon in Version 3.8

Cinnamon 3.8 wurde schon vor einigen Monaten abgeschlossen, interessierte Anwender mussten sich jedoch bis zum Erscheinen seiner Stammdistribution gedulden. Die Liste der Neuerungen ist tatsächlich lang, wirklich Spektakuläres lässt sie aber vermissen. Am spannendsten sind sicher die nicht sichtbaren Investitionen in die grafischen Fähigkeiten des Desktops, die zu schnellerer Fensterdarstellung und einer fühlbar flüssigeren Systemleistung führen sollen.
In der Tat zeigt sich Cinnamon enorm reaktionsschnell und Tasks wie Nemo, Systemeinstellungen, VLC, Xed, Terminal, Filezilla sind auf einem schnellen PC praktisch nach dem Mausklick eingabebereit, Firefox, Thunderbird oder Gimp nach ein, zwei Sekunden.
Die übrigen Verbesserungen sind zahlreich, aber unscheinbar: So zeigt das Applet „Klang“ in den „Systemeinstellungen“ im Register „Einstellungen“ nun einen Schieberegler, der die maximale Lautstärke zwischen 0 und 150 Prozent skaliert. Das hilft nicht nur, das Soundsystem zu überdrehen, sondern auch in die andere Richtung, um unabhängig von der Playereinstellung die Laustärke sinnvoll zu begrenzen.
Desklets werden häufig durch Vollbildanwendungen oder andere Fenster verdeckt: Wer Desklets benutzt, kann diese jetzt mit der Tastenkombination Super-Alt (oder Super-S) in den Vordergrund bringen. Die Systembenachrichtigungen in der Systemleiste bieten eine neue Schaltfläche zum Schließen. Die Anzahl der Benachrichtigungen von Anwendungen wird außerdem limitiert. Cinnamon überprüft bei Notebooks, ob eine externe Maus angeschlossen ist. Ist das nicht der Fall, aktiviert es selbsttätig das Touchpad des Geräts.
Unter „Einstellungen → Energieverwaltung“ erscheint in den „Zusätzlichen Optionen“ der Eintrag „Sofort herunterfahren“. Diese Option kann für das Drücken des Netzschalters gewählt werden.
Beim Zubehör hat sich Cinnamon einerseits von manchen Dauergästen verabschiedet, andererseits neue eingeladen: Der in der Tat nicht mehr ganz so popläre Messenger Pidgin ist nicht mehr an Bord. Andererseits ist der Gnome-Kalender jetzt Standard. Der erlaubt bekanntlich die Verknüpfung zum Google-, Facebook-, Microsoft- oder auch zum Nextcloud-Konto. ■

Linux Mint 19: Einrichtung & Tipps

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



VON HERMANN APFELBÖCK

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

Infos zu Linux Mint

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

1. Die Mint-Editionen und ihre Ausrichtung

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

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

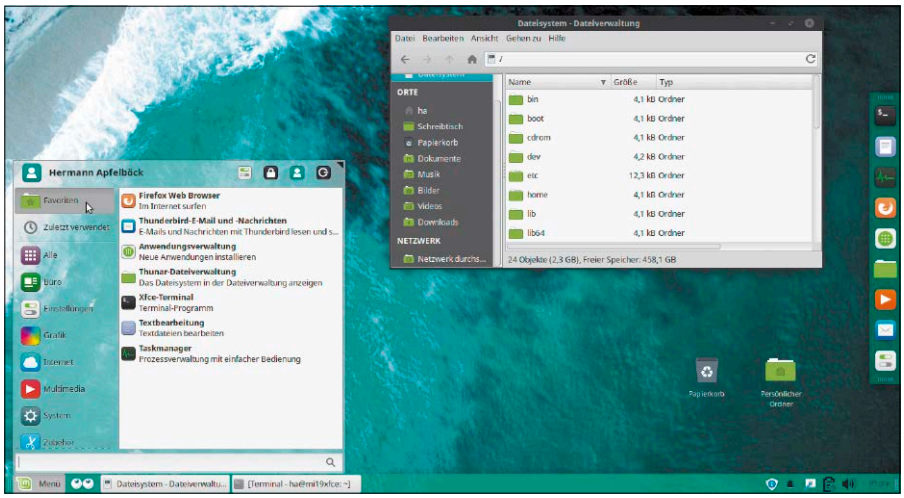
her auch startfähig auf Heft-DVD und belegt in der vorliegenden 64-Bit-Ausführung 700 bis 800 MB ab Anmeldung. Es sollte mindestens zwei GB RAM antreffen, besser vier. Der schicke Cinnamon-Desktop benötigt einen Grafikchip mit 3D-Beschleunigung, was aber bei Intel/AMD/Nvidia seit mehr als zehn Jahren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

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

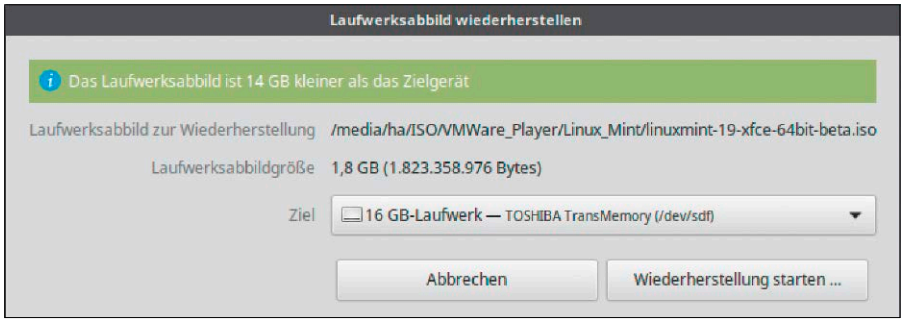
Linux Mint 19 Mate eignet sich für ebenfalls ältere Rechner und liegt beim Speicherbedarf zwischen XFCE und Cinnamon. Objektiv hat die Mate-Edition zwischen den sehr ähnlichen Desktops Cinnamon und XFCE wenig Argumente: Wer ein möglichst sparsames System sucht, greift besser zum noch schlankeren XFCE-Desktop.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

2. Vorbereitungen für eine Neuinstallation

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



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



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

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

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

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

AUSBLICK AUF LMDE 3: DAS ZWEITE LINUX MINT

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

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

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

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

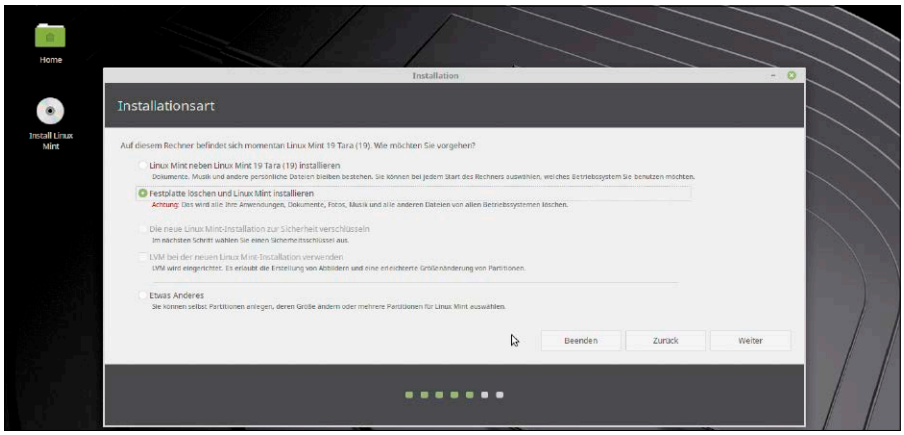
3. Installation mit Ubiquity-Installer

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

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

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

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



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

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

D. Die Option „Etwas Anderes“ erfordert manuelles Partitionieren. Dies ist unvermeidlich, wenn Sie das neue System auf USB installieren oder von bereits installierten Systemen ein ganz bestimmtes ersetzen möchten. Danach suchen Sie in der Liste das Laufwerk (also das physische Medium) und die Partition, wohin Sie Mint installieren möchten. Im Unterdialog „Partition erstellen“ ist oben die Gesamtgröße der Partition voreingestellt. 100 GB sollte ein längerfristig genutztes Desktop-Linux mindestens erhalten, zum Ausprobieren reichen auch 20 GB. Als „Typ der neuen Partition“ wählen Sie „Primär“, wenn Ihnen vier Partitionen auf diesem Datenträger ausreichen. Position ist am „Anfang dieses Bereichs“, Dateisystem vorzugsweise „Ext4“. Neben „Einbindungspunkt“ klappen Sie die Drop-down-Liste aus und wählen „/“. Wieder zurück im Hauptdialog „Installationsart“ steht die letzte wichtige Entscheidung unter „Gerät für die Bootloader-Installation“ an – also der Ort, wo der Grub-Bootloader eingerichtet werden soll. Voreingestellt ist die erste interne Festplatte („/dev/sda“). Das ist in Ordnung, wenn Sie Linux Mint auf eine interne Festplatte installieren, und zwar auch dann, wenn das System auf eine andere Platte, etwa nach „/dev/sdb1“ installiert wird. Das ist jedoch nicht in Ordnung, wenn Sie auf einen externen USB-Datenträger installieren. In diesem Fall muss der Bootloader ebenfalls auf das USB-Medium.

Nach der Partitionierung (A, B, C oder D) erscheint noch der wichtige Dialog „Wer sind Sie?“: Hier richten Sie den Erstbenutzer ein, der mit sudo-Berechtigung ausgestattet wird (für Systemaktualisierung, Installationen). Anders als Ubuntu bietet Linux Mint hier wie gehabt die Home-Verschlüsselung mit Ecryptfs. Alles Wesentliche dazu steht im voranstehenden Beitrag (Seite 14). Die Abwägung „Luks oder Ecryptfs?“ ist nicht einfach: Luksist technisch komplexer, aber datenschutztechnisch kompromisslos. Für stationäre PCs genügt Ecryptfs allemal, auf Notebooks, die viel unterwegs sind, spricht viel für Luks.

4. Das Upgrade von 18.x auf Version 19

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

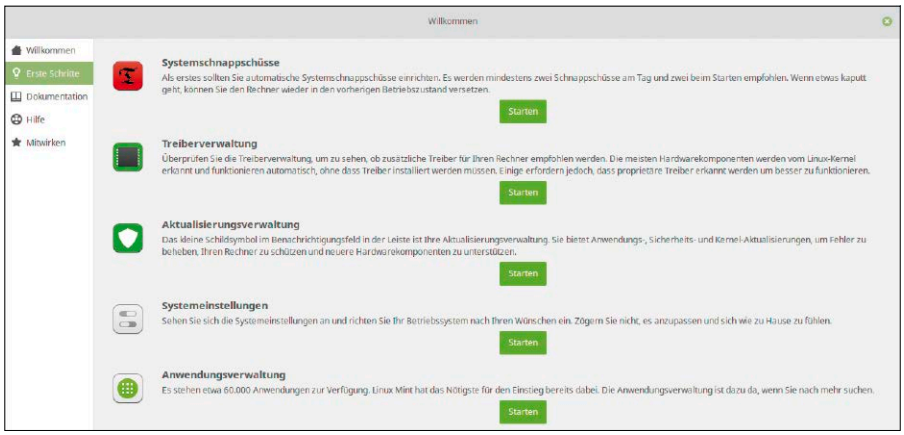
```
sudo apt-get update
sudo apt-get dist-upgrade
```

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

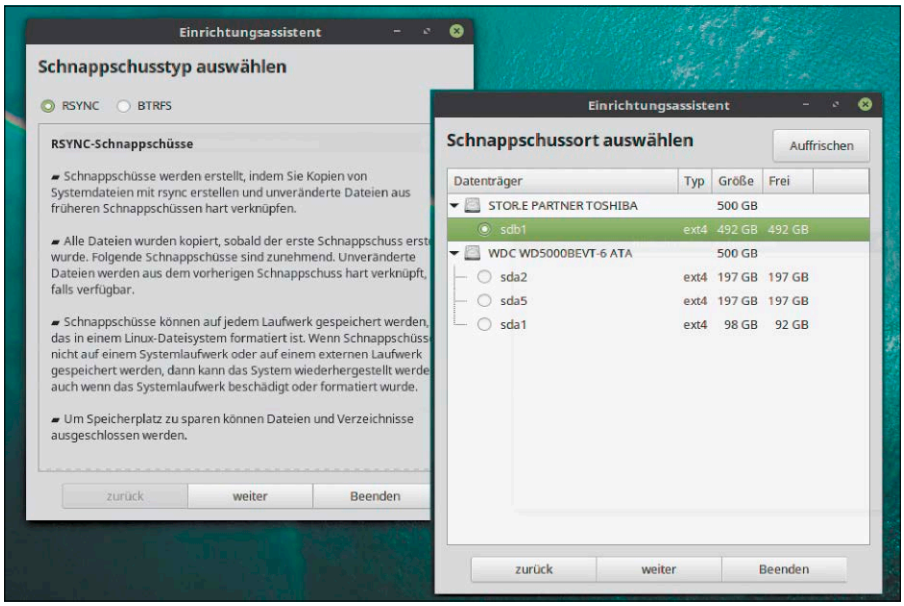
5. Systempflege nach der Installation

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

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



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



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

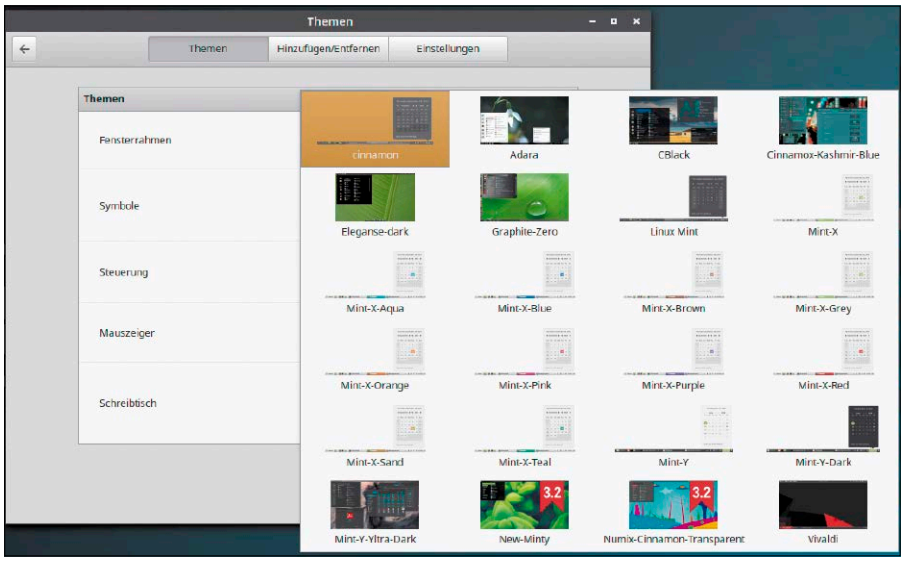
Systemsicherung mit Timeshift: Linux Mint 19 stellt für die Systemsicherung das Werkzeug Timeshift ins Zentrum. Der erste Sicherungspunkt (Snapshot) ist immer ein komplettes Backup der Systemverzeichnisse. Weitere Snapshots fallen dann deutlich kleiner aus, da Timeshift nur noch die geänderten Dateien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

Starten Sie Timeshift über „Systemverwaltung/Systemwerkzeuge → Timeshift“. Timeshift fordert das sudo-Kennwort. Beim ersten Start wird der „Schnappschusstyp“ abgefragt. Übernehmen Sie das voreingestellte „RSYNC“, sofern Sie Linux Mint mit Ext4-Dateisystem installiert haben (Standard). Im nächsten Schritt geht es um den „Schnappschussort“, also um den Zieldatenträger der Sicherung. Timeshift bietet alle Partitionen mit Linux-Dateisystem an. Standardziel, wenn nur eine Festplatte vorliegt, ist das Wurzelverzeichnis, wo der zusätzliche Ordner „timeshift“ entsteht. Optimal ist jedoch ein unabhängiger zweiter Datenträger als Ziel, allerdings muss dieser immer zur Verfügung stehen, wenn Sie einen automatisierten Zeitplan verwenden. Für manuelle Sicherung eignet sich auch ein USB-Laufwerk. Im letzten Schritt definieren Sie optional einen Zeitplan („Schnappschussebenen“) und die Menge der gespeicherten Systempunkte. Die automatische Sicherung ist bequem, aber nicht zwingend: Schnappschüsse lassen sich jederzeit manuell über „Erstellen“ im Timeshift-Fenster auslösen.

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

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

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



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

Wichtig: Die Wiederherstellung mit Timeshift ist notfalls mit der Basissyntax

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

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

6. Tuning für den Cinnamon-Desktop

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

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

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

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

TUNING FÜR DEN XFCE-DESKTOP

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

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

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

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

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

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

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

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

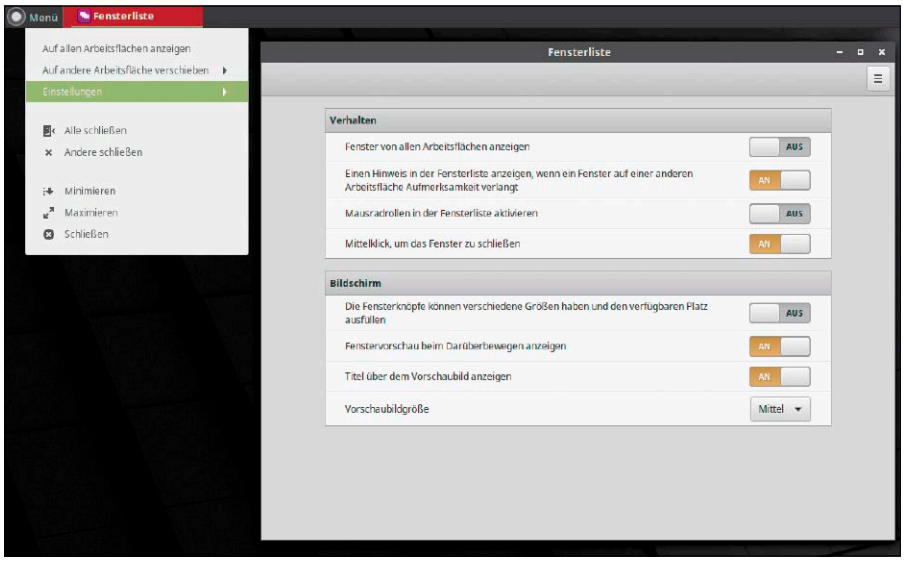
Sie lassen sich komplett deaktivieren, was die schnellste und ökonomischste Lösung ist. Wer möchte, kann die Effekte aber unter „Anpassen“ differenziert einstellen hinsichtlich Effekttyp und Effektdauer.

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

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

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

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



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

TUNING FÜR DEN MATE-DESKTOP

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

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

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

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

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

DSGVO für Blogger

Fast jeder, der eine Homepage oder einen Blog betreibt, ist von der neuen Datenschutz-Grundverordnung betroffen. Die DSGVO skaliert nicht – sie gilt praktisch überall. Damit Sie nicht mit dem Gesetz in Konflikt geraten, müssen Sie einiges beachten.

VON THORSTEN EGGELING

Quelle: © dlyastokiv – Fotolia.com

Die Datenschutz-Grundverordnung der EU, kurz DSGVO, betrifft fast jeden, der selbst im Internet aktiv ist. Betreiber etwa von Blogs, Foren oder Onlineshops sollten spätestens jetzt prüfen, ob ihre Internetpräsenz den aktuellen Vorschriften entspricht. Aktuell herrscht vor allem bei kleinen, nicht kommerziell orientierten Inhalteanbietern große Verunsicherung. Erst die nächsten Monate wird sich zeigen, ob die DSGVO das eigentliche Ziel, die großen globalen Datensammler zu bändigen, im Fokus behält, oder ob eine Abmahnwelle über kleine Blogs, Händler oder Vereinsseiten rollt.

Ziele und Inhalte der DSGVO

Datenschutz sowie Rechte und Pflichten im Internet waren in Deutschland auch bisher schon gesetzlich geregelt. Einzelheiten dazu finden sich seit 2007 beispielsweise im Telemediengesetz (*https://dejure.org/gesetze/TMG*). Die DSGVO (PDF-Download unter *www.pcwelt.de/yGzi4G*) soll jetzt einen einheitlichen europäischen Standard beim Datenschutz schaffen. Die Verordnung gilt in den Mitgliedsstaaten unmittelbar, kann aber in einzelnen Punkten durch die nationale Gesetzgebung ausgestaltet werden. In Deutschland geschieht das beispielsweise durch das Bundesdatenschutzgesetz (*https://dsgvo-gesetz.de/bdsg-neu*).

Das Kernziel der DSGVO: Sie soll die Grundrechte und Grundfreiheiten jeder natürlichen Person schützen – allen voran das Recht auf informationelle Selbstbestimmung. Die DSGVO gilt auch für Anbieter außerhalb der EU, sobald sie Daten von EU-Bürgern verarbeiten. Wie schon bisher dürfen personenbezogene Daten nicht ohne Zustimmung erhoben, verarbeitet oder gar an andere Unternehmen weitergegeben werden. Es ist jetzt aber genauer geregelt, wie die Einwilligung erfolgen muss. Das stillschweigende Einverständnis genügt nicht mehr. Der Nutzer etwa eines Onlineangebots muss der Datenspeicherung explizit zustimmen. Außerdem erhält er das Recht, die Einwilligung jederzeit zu widerrufen, Informationen über die gespeicherten Daten zu erhalten oder die Daten löschen zu lassen.

Daten dürfen nur zweckgebunden erhoben und weiterverarbeitet werden – auch das galt bisher schon. In der DSGVO ist jetzt zusätzlich vorgeschrieben, dass Nutzer in verständlicher Form über den genauen Zweck der jeweiligen Datenerhebung informiert werden müssen. Daten, die nicht mehr für einen konkreten Zweck notwendig sind, muss der Anbieter löschen und den Nutzer über die Fristen aufklären. Datenpannen müssen jetzt innerhalb von 72 Stunden gemeldet werden. Gelangen persönliche Daten in falsche Hände, besteht unter Umständen ein Schadensersatzanspruch.

Wer gegen die EU-Datenschutzgrundverordnung verstößt, muss mit Geldbußen bis zu 20 Millionen Euro oder vier Prozent des weltweiten Umsatzes des Unternehmens rechnen (der höhere Wert entscheidet). Laut BDSG kann eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe verhängt werden, wenn ein Unternehmen beispielsweise personenbezogene Daten einem Dritten übermittelt.

Für wen gilt die DSGVO?

In der DSGVO heißt es: „Diese Verordnung gilt nicht für die Verarbeitung von personenbezogenen Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten

und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit vorgenommen wird." (Punkt 18, Seite 3). Wie schon bisher, etwa bei der Impressumspflicht, gilt diese Einschränkung des Anwendungsbereichs nur für sehr wenige Websites. Sobald Sie in Ihren Blog Werbung einbauen oder es einen beruflichen Bezug gibt, ist die Website nicht mehr ausschließlich privat. Wenn ein Bäckermeister beispielsweise in seinem Blog Backrezepte veröffentlicht, ist ein Bezug zur beruflichen Tätigkeit gegeben und somit gelten für diesen Blog die Regeln der DSGVO.

Welche Maßnahmen sind erforderlich?

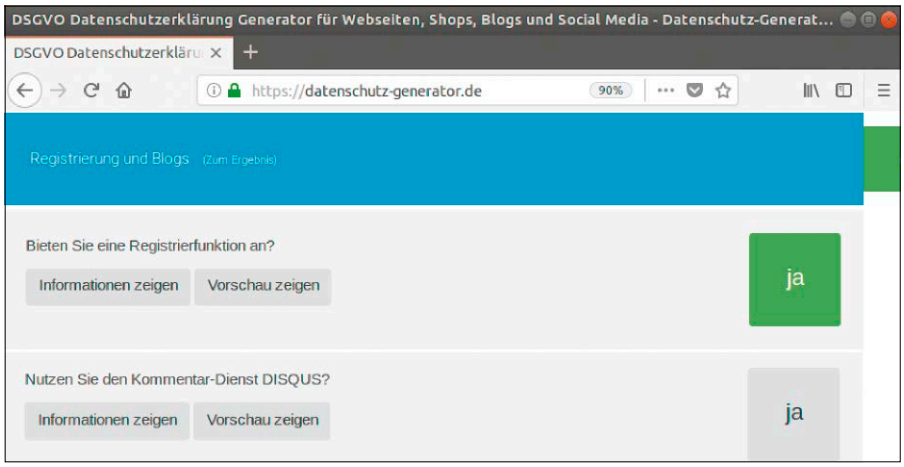
Für Ihren Blog benötigen Sie eine Datenschutzerklärung, die Sie beispielsweise über *https://datenschutz-generator.de* erzeugen können. Die Nutzung ist für Privatpersonen und Kleinunternehmen (Brutto-Umsatz nicht höher als 17 500 Euro im Jahr) kostenlos. Sehen Sie sich alle Rubriken an und klicken Sie jeweils dort auf „Ja", wenn Sie eine der genannten Funktionen in Ihrem Blog verwenden. Als Ergebnis erhalten Sie einen Text, den Sie in Ihre Website einbauen und an einer gut sichtbaren Stelle verlinken, etwa als „Datenschutzerklärung" in der Hauptnavigationsleiste.

Wenn Sie Benutzerdaten abfragen, etwa in einem Kontaktformular oder der Kommentarfunktion, müssen die Daten SSL-verschlüsselt übertragen werden. Sollte Ihre Website noch nicht über „https://" erreichbar sein, installieren Sie ein kostenloses Zertifikat von Let's Encrypt (*www.pcwelt.de/2189443*).

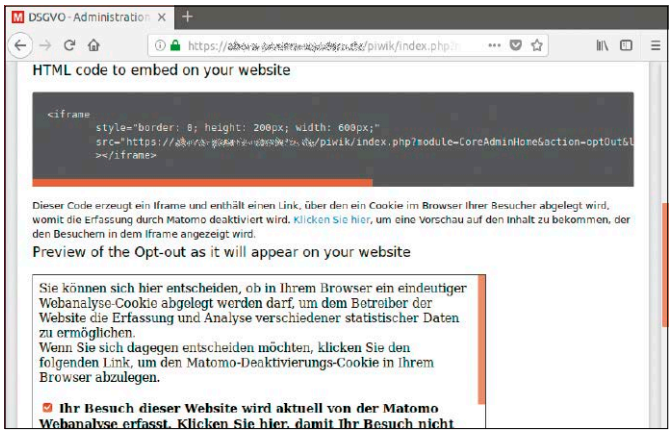
Problematisch sind alle Wordpress-Plugins, die Daten an andere Onlinedienste weiterleiten. Sie müssen sicherstellen, dass auch diese gemäß DSGVO arbeiten. Im Zweifelsfall deaktivieren Sie das Plug-in vorsichtshalber. Eine Liste mit Einschätzungen zur DSGVO-Konformität verbreiteter Plugins finden Sie beispielsweise unter *https://wp-ninjas.de/wordpress-plugins-dsgvo*.

In der Regel müssen Sie einen Vertrag zur Auftragsdatenverarbeitung abschließen, etwa wenn Sie Google-Analytics verwenden. Informationen dazu finden Sie unter *https://support.google.com/analytics/answer/3379636*. Wenn möglich, sollten Sie Analysetools wie beispielsweise Matomo bevorzugen (*https://matomo.org*). Hier bleiben die Daten auf Ihrem eigenen Server und damit unter Ihrer Kontrolle. In den Matomo-Einstellungen legen Sie unter „Privatsphäre" Optionen für die Anonymisierung fest. Außerdem finden Sie hier Informationen, wie Besucher Ihrer Website das Matomo-Tracking deaktivieren („users opt-out") oder ihr Einverständnis erklären können („Asking for consent").

Auch Namen und Bilder erfordern strikte Kontrolle: Sie sollten auf Ihrer Website prüfen, ob Sie das Einverständnis aller Personen besitzen, die dort namentlich erwähnt werden oder auf Fotos abgebildet sind. Im Zweifelsfall sollten Sie alle Personen auf Abbildungen unkenntlich machen, um rechtliche Risiken zu vermeiden. ■



Datenschutzerklärung: Den Text der Erklärung erstellen schnell über *https://datenschutz-generator.de*. Gehen Sie alle Rubriken durch und beantworten Sie Zutreffendes mit „Ja".



Websiteanalysen: Matomo bietet alle Optionen für eine Nutzung gemäß DSGVO. Bauen Sie den angezeigten HTML-Code ein, damit Benutzer sich gegen die Datenerfassung aussprechen können.

SPEICHERUNG VON IP-ADRESSEN

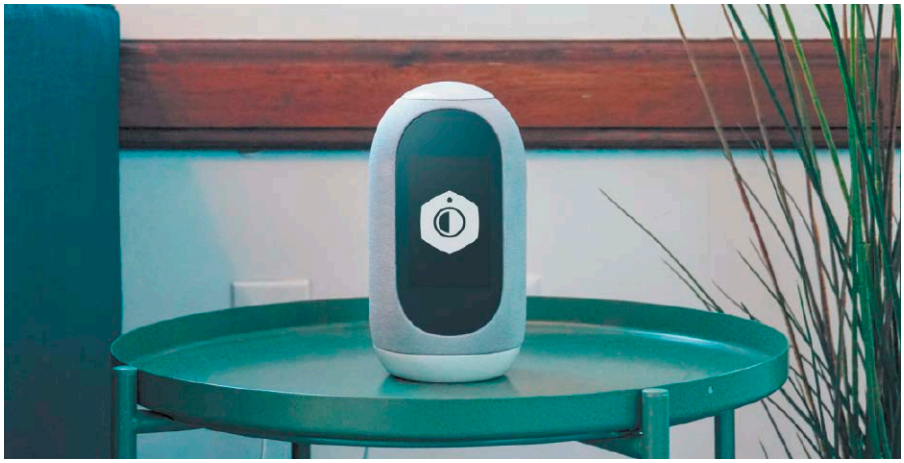
Auch IP-Adressen gelten als personenbezogene Daten. Meist ist es jedoch erforderlich, die IP-Adressen der zugreifenden Nutzer zumindest für einige Zeit zu speichern, beispielsweise wenn Sie Ihren Server mit Fail2Ban schützen (*www.pcwelt.de/2062825*). Die IP-Adressen helfen auch bei der Spamabwehr in Kommentaren und der Aufklärung missbräuchlicher Nutzungen der Kommentarfunktion. Sie können sich bei der Datenspeicherung auf „berechtigte Interessen" laut DSVO Artikel 6, Absatz 1 berufen, wenn Sie die Serverlogs beispielsweise alle sieben Tage löschen oder wenigstens die IP-Adressen in den archivierten Logs anonymisieren.

Welche Schritte im Einzelnen notwendig sind, hängt von der Serverinstallation ab. Webhoster bieten in der Konfigurationsoberfläche in der Regel Optionen, über die Sie die Anonymisierung und Dauer der Logarchivierung festlegen können.

Künstliche Intelligenz unter Linux

Bei künstlicher Intelligenz denkt man an Computer, die Schachgroßmeister in die Knie zwingen, vielleicht auch an „HAL“ in Kubricks „Odyssee im Weltraum“. Doch KI kann heute unter jedem Linux ganz praktische Alltagsaufgaben erledigen.

VON STEPHAN LAMPRECHT



So soll demnächst ein smartes KI-Gerät aussehen, das per Kickstarter finanziert wurde und auf Mycroft basiert.

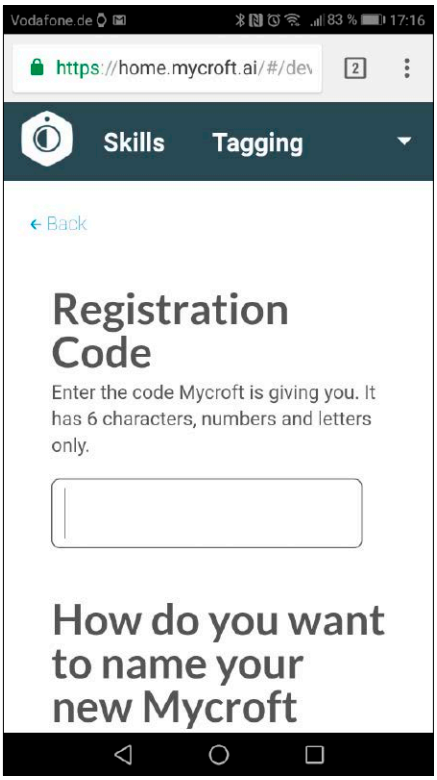
„Künstliche Intelligenz“ klingt sehr beeindruckend. Doch Publikumsmedien erwecken mit ihren Berichten oft falsche Erwartungen. Denn „Intelligenz“ darf nicht mit „Bewusstsein“ verwechselt werden. Erschwert wird das Verständnis durch eine wenig trennscharfe Verwendung des Begriffs. Informatiker verstehen darunter eine ganze Reihe von verschiedenen Techniken und Ansätzen. KI-Systeme können sich (derzeit noch in sehr begrenzten Umfang) Wissen selbständig aneignen und werden im Laufe der Zeit immer besser in der Erfüllung der an sie gestellten Aufgabe. Positiv ausgedrückt sind aktuelle KI-Systeme hochgradig spezialisiert. Die KI, die perfekt Go spielt, wird allerdings den Unterschied zwischen einer Giraffe oder eine Maus nicht erkennen. Und eine Bilderkennung wird mit dem Eröffnungszug beim Schach überfordert sein. Negativ formuliert, handelt es sich bei KI-Systemen um das, was wir umgangssprachlich als „Fachidioten“ bezeichnen. In Spezialdisziplinen ist es für den Menschen schwer, an die Maschinen heranzukommen. Wer Spaß am Anpassen und Entwickeln eigener Scripts hat, kann KI inzwischen auch im Rahmen eigener Projekte nutzen.

Der eigene intelligente Lautsprecher

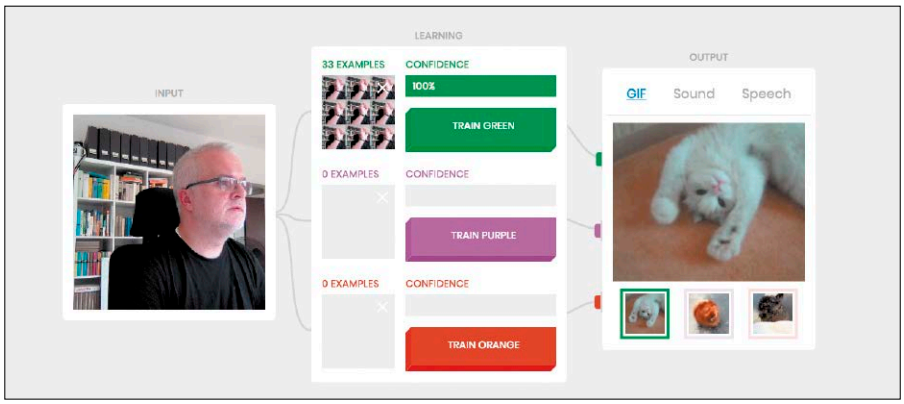
Eine Disziplin der künstlichen Intelligenz ist die Mustererkennung. Ob Handschriften während der Eingabe übersetzt werden müssen oder die Sprache während eines Diktats: Die Erkennungsraten verbessern sich, weil die dahinterstehenden Programme in der Lage sind, selbständig zu lernen. Mycroft ist eine auf Open Source basierende Spracherkennung, die eine Alternative zu Amazons Alexa oder Apples Siri sein will. Tatsächlich ist es den Machern gelungen, auf Kickstarter erfolgreich eine Kampagne durchzuführen, die den Bau eines von Mycroft angetriebenen Lautsprechers finanzieren soll. Wer selbst mit der Alternative zu kommerziellen Assistenten experimentieren will, kann das mit einfachen Mitteln. Dazu benötigen Sie einen Raspberry Pi (am besten die dritte Generation), einen passiven Lautsprecher, an den keine besonderen Ansprüche gestellt werden, sowie ein Mikrofon für die USB-Schnittstelle. Das Ganze funktioniert mit Picroft (*https://github.com/MycroftAI/enclosure-picroft*), einer Distribution für den Raspberry Pi, die Mycroft bereits an Bord hat.

Die Einrichtung ist typisch einfach, indem Sie die Imagedatei mittels Etcher oder einem anderen Werkzeug auf die SD-Karte kopieren. Dann verbinden Sie den Rechner per Ethernet-Kabel mit dem heimischen Netzwerk und verbinden alle anderen Komponenten. Für die ersten Schritte mit dem System ist es empfehlenswert, Monitor und Tastatur anzuschließen. Wie bei den kommerziellen Assistenten stammt die Intelligenz aus der Cloud. Deswegen ist ein Pairing zwischen dem Gerät und dem Server der Betreiber notwendig.

Die Vorgehensweise dazu zeigt Picroft direkt auf dem Monitor an. Über ein anderes Gerät (das kann auch ein Smartphone sein) verbinden Sie sich mit dem lokalen Netzwerk „MyCroft“ und rufen darüber die URL „start.mycroft.ai“ auf. Auf der nachfolgenden Seite werden dann die Zugangsdaten für das WLAN-Netzwerk des eigenen Routers eingetragen. Derzeit werden aber noch keine Netzwerke im Fünf-GHz-Modus unterstützt. Der Raspberry startet anschließend neu und das Gerät ist bereits einsatzbereit.



Eine Methode, Mycroft zu initialisieren, ist das vom Rechner aufgespannte WLAN zu benutzen, um den angezeigten Code in der Cloud zu hinterlegen.



Auf unterhaltsame Weise erklären die Entwickler von Tensorflow die Grundlagen des maschinellen Lernens und stellen Codebeispiele zur Verfügung.

Bevor Programme Objekte erkennen oder damit interagieren können, ist erst einmal ausführliches Training angesagt.

Fragen Sie doch spontan mal nach dem Wetter: „Hey Mycroft, how's the weather in Hamburg?". Tatsächlich versteht und „spricht" Mycroft experimentell auch bereits die deutsche Sprache. Dazu ist aber etwas Handarbeit an den Einstellungsdateien notwendig. Das wird aber von den Entwicklern sehr gut im Wiki erklärt (*https://mycroft.ai/documentation/language-support/german/*). Und selbstverständlich können Sie nach dem erfolgreichen Pairing Monitor und Tastatur vom Raspberry entfernen. Da es sich um ein auf Debian basierendes System handelt, genügt ein SSH-Terminal, um die Konfiguration des Systems zu verändern.

Maschinelles Lernen für (fast) jeden

Während sich Mycroft dank seiner Umsetzung für den Raspberry Pi sehr zugänglich zeigt, erfordern andere KI-Projekte vom Nutzer etwas mehr Durchhaltewillen. Sie sind nicht weniger beeindruckend als die Spracherkennung, bieten aber keine eigenen Anwendungen an. Wer sie nutzen will, sollte also Kenntnisse in der Programmierung mitbringen, um die künstliche Intelligenz einsetzen zu können. Sicherlich eines der herausragenden Projekte ist Tensorflow (*www.tensorflow.org/*), das von Google gefördert und auch in eigenen Anwendungen genutzt wird. Es handelt sich um ein Framework, das vielseitig eingesetzt werden kann. Die Logik für das maschinelle Lernen läuft auf dem Server, aber eingebunden werden muss sie dann über eine passende Programmiersprache.

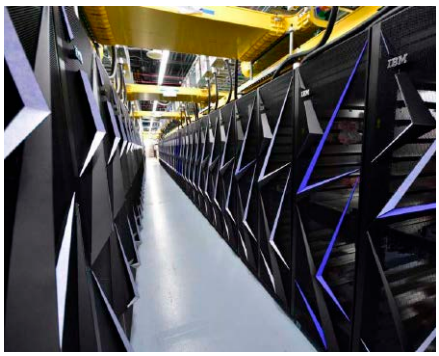
Bei Redaktionsschluss noch frisch gebackenes Mitglied der Tensorflow-Familie ist Tensorflow.js. Die Bibliotheken wurden ursprünglich unter dem Namen Deeplearn.js entwickelt. Wie der Name verrät, können damit Programme in Javascript um maschinelles Lernen erweitert werden. Der Einsatz der Methoden wird nicht nur in einer umfangreichen Dokumentation erklärt. Es steht auch eine ganze Reihe von Demoanwendungen zur Verfügung. Diese haben ihren Schwerpunkt in der Bilderkennung. So lernen Sie hier auf spielerische Weise mehr über das Training bei der Bilderkennung. Denn bevor ein System Daten automatisiert auswerten kann, muss es zunächst mit jeder Menge Daten gefüttert werden. Da auch der Code der Demos heruntergeladen werden kann, erfahren Sie hier, wie beispielsweise anhand von Fotos die Lage von Personen auf einem Bild identifiziert wird oder wie die Bild- oder besser Mustererkennung in der Praxis funktioniert.

Schon solche erste Schritte sind sehr lehrreich, denn man kann dann erst ermessen, wie viel Arbeit hinter aktuellen Apps wie der visuellen Suche von Google oder Microsoft auf dem Handy steckt. Bevor ein Programm das scheinbar offensichtliche Muster eines Regenschirms erkennt, muss es vorher jede Menge Bilder von Regenschirmen ausgewertet haben. Und da gibt es natürlich auch jede Menge Falscherkennungen, die der Programmierer noch korrigieren muss. Wer Python als Programmiersprache bevorzugt, kann die KI von Tensorflow auf jedem System einsetzen, für das Python zur Verfügung steht. Installationsanleitungen stehen für Ubuntu, Mac-OS und Windows parat. Einfach loslegen!

Nicht wenige Medienberichte suggerieren, dass die düsteren Visionen aus der Filmreihe „Terminator" bald Wirklichkeit werden könnten. Wer bei diesem Thema mitreden will, kann mit Projekten wie Tensorflow die ersten Gehversuche mit KI unternehmen. Vermutlich wird man danach seine eigenen Schlüsse ziehen. ■

Schnellster Superrechner mit Red Hat

Nachdem China lange Zeit die leistungsfähigsten Superrechner der Welt für sich reklamieren konnte, gibt es nun am Oak Ridge National Laboratory in den USA den mächtigsten Rechner. Mit 122,3 Petaflops steht der von IBM gefertigte Supercomputer „Summit" derzeit auf Platz eins der Weltrangliste. Der Riesenrechner kombiniert Power9-Prozessoren von IBM und Volta-100-GPUs von Nvidia zu einem System, das mit Red Hat Enterprise Linux betrieben wird. (*https://www.top500.org*) ■



Quelle: Oak Ridge National Laboratory

Ubuntu 18.10 wird ein Tintenfisch

Zur nächsten Ausgabe von Ubuntu, die voraussichtlich im Oktober erscheint, hat das Entwicklerteam die ersten Pläne veröffentlicht: Cosmic Cuttlefish („Kosmischer Tintenfisch") ist der Name von Ubuntu 18.10. Als Oberfläche soll Gnome 3.30 und der Kernel in Version 5.0 mit dabei sein. Die Gnome-Erweiterung „Gsconnect" wird vorinstalliert sein: Es handelt sich um eine Schnittstelle zu KDE Connect, um Android-Smartphones einfach per Netzwerk anzubinden. ■

Quelle: Hans Dappen; Lizenz: CC BY 3.0 (*https://bit.ly/2emh4gS*)

Ubuntu: Zahlen bitte!

Ubuntu sammelt Daten. Die unvermeidliche Kritik kontert Canonical offensiv mit der Veröffentlichung dieser Daten.

Wie angekündigt hat Canonical die ersten Zahlen aus der umstrittenen Erhebung von Systemdaten bei der Installation von Ubuntu 18.04 veröffentlicht. Erstaunlich ist vor allem die Teilnahmequote, die trotz gesetzlich vorgeschriebener Opt-out-Option bei der Installation bei fast 70 Prozent liegt.

Die Datenerhebung sendet anonymisiert RAM-Menge, CPU-Anzahl, Bildschirmauflösung, Partitionslayout, gewählte Installationsoptionen, den ungefähren Standort durch die gewählte Lokalisierung und die Installationsdauer an Canonical. Demzufolge sind vier und acht GB die häufigsten RAM-Kapazitäten, die am weitesten verbreitete Bildschirmauflösung ist 1920 × 1080 (1080 p), die PCs der meisten Anwender haben eine CPU und die durchschnittliche Dauer der Installation beträgt 18 Minuten. Die schnellste Installationszeit ist bei circa acht Minuten. Etwa 30 Prozent der Ubuntu-Anwender verwenden eine automatische Anmeldung. 50 Prozent wollen proprietäre Pakete bei der Installation und 15 Prozent nehmen die neue Option der minimalen Installation wahr. ■

Resultat der Datenerhebung von Ubuntu: Die Karte zeigt die Verteilung der Ubuntu-Installationen ab 18.04 nach Ländern anhand der gewählten Lokalisierung.

Quelle: Canonical

Vorschau auf Kernel 4.18

Kurz nachdem Linus Torvalds den Kernel 4.17 Anfang Juni freigegeben hatte, ist zwei Wochen später der erste Release Candidate des Kernel 4.18 erschienen. Die folgenden zwei Monate dienen dem eingespielten Entwicklerteam üblicherweise zu Tests und etlichen Korrekturen im Detail. Die nächste Kernel-Version wird die begonnenen Aufräumarbeiten unter den obsoleten Technologien fortsetzen und voraussichtlich etwas kleiner ausfallen als die Vorgänger. Das liegt an einigen entfernten Treibern für nie realisierte Hardware sowie an der vorübergehenden Verbannung des Clusterdateisystems „Luster" aus dem Kernel-Quellcode.

Eine der größeren Aufgaben ist die Umarbeitung zahlreicher Systemaufrufe, um diese für das Jahr 2038 sicher zu machen. Das Jahr-2038-Problem betrifft die in Sekunden gezählte Unix-Zeit, die ab diesem Datum einen 32-Bit-Integerwert überschreiten wird und dann einen ungültigen negativen Wert annimmt. In näherer Zukunft wird der Kernel ab 4.17 die Nvidia-Grafikchips Volta unterstützen sowie AMD Vega 20. Das Dauerthema Energieverwaltung bekommt systemweite Stromsparzustände, die Gerätegruppen zusammenfassen. Gamer können sich auf die Unterstützung des Steam-Controllers freuen. USB 3.2, das in den nächsten Monaten marktreif wird, erhält seine ersten Linux-Treiber. ■

Alle News von David Wolski

Quelle: Tuxedo

Tuxedo: Infinitybook Pro 14

Darf es etwas mehr sein? Tuxedo vergrößert seine Modellserie von Linux-Notebooks um das Infinitybook Pro 14, das mit einem 14-Zoll-Bildschirm ausgestattet ist und damit für Büroeinsatz besser geeignet scheint als das kleinere Infinitybook Pro 13. Das IPS-Display bietet eine Full-HD-Auflösung (1920 × 1080 Pixel), natürlich matt und entspiegelt, wie es sich für Businessnotebooks gehört. Das Gehäuse, aus einer silberfarbenen Aluminiumlegierung gefertigt, wiegt bis zu 1,4 Kilogramm – je nach Ausstattung, die sich auf der Shopwebseite Tuxedos individuell anpassen lässt. Der Rechner hat neben einem Gigabit-Ethernet-Port auch einen Typ-C-Thunderbolt-Port und kann mit bis zu 32 GB RAM bestückt werden. Die optional verfügbaren CPUs reichen bis zu Intel Core i7-8550U. Tuxedo entwickelt angepasste Ubuntu-Systeme mit Treibern für die Intel-Hardware, die für optimale Akkulaufzeiten sorgen. Das Linux-Engagement des Herstellers schlägt sich allerdings im Preis nieder: Der Einstiegspreis des Infinitybook Pro 14 liegt bei 995 Euro (*www.tuxedocomputers.com*). ■

SICHERHEITSNEWS

Docker-Images mit Malware

Nicht weniger als 17 öffentlich zugängliche und installierbare Docker-Images haben die Betreiber der offiziellen Docker-Plattform *https://hub.docker.com* entfernen müssen, weil die Images mit versteckten Komponenten zum Mining von Cryptowährungen versehen waren. Das wirft ein schlechtes Licht auf die Docker-Plattform, deren hochgeladene Images offensichtlich keiner stringenten Prüfung unterworfen waren. Ein ähnliches Problem trat im Mai auf Canonicals Snap Store für Ubuntu auf, auf der ebenfalls ein Snap-Paket mit Miningsoftware versehen war. Canonical will dem mit einem Bewertungssystem begegnen, das Quellen von Snaps transparent einstuft. Per se sind Miningprogramme nicht destruktiv, stehlen aber Rechenleistung auf Zielsystemen und fallen deshalb in die Kategorie dreiste Malware.

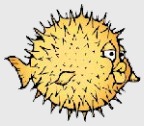
TL Bleed: Gesprächige Intel-CPUs

Kein Ende der Sicherheitslücken bei den einst hochgelobten Intel-Prozessoren: Per Seitenkanalangriff haben IT-Sicherheitsforscher bewiesen, dass es möglich ist, auf einem CPU-Kern die Grenzen von Hyperthreading zu umgehen und dabei andere Prozesse auszulesen. Die vollständigen Ergebnisse und Demomaterial wird der Entdecker von der Vrije Universiteit Amsterdam auf der Konferenz Blackhat 2018 vorstellen. Die neue Prozessorlücke hat schon den Namen „TL Bleed“ bekommen, weil der Translation Lookaside Buffer (TLB) des CPU-Caches eine tragende Rolle bei diesen Angriffen spielt.

Firebase: Ungesicherte Datenbanken

Ungeschützte Datenbanken im Internet sind ein gefundenes Fressen für Hacker, ein Alptraum aller Administratoren und oft der Grund für das abrupte Ende von IT-Unternehmen. Nun wurde bekannt, dass Tausende Installationen der Datenbank Firebase, die vornehmlich serverseitig für Smartphone-Apps eingerichtet werden, keinerlei wirksamen Zugriffschutz hatten. Firebase ist ein Dienst von Google für Entwickler von iOS- und Android-Apps. Wie sich zeigt, ist hier vielen Entwicklern Datensicherheit ein Fremdwort. Pentester der Firma Appthority fanden laut eigenen Angaben bei einer Studie über 2,7 Millionen Apps mehr als 2000 unsichere Firebase-Datenbanken und hätten auf 113 GB Kundendaten zugreifen können, inklusive Passwörtern, API-Keys, Rechnungsdaten und Kontaktadressen (*http://info.appthority.com/-q2-2018-mtr-download-Firebase-vulnerability*).

Open BSD ohne Hyperthreading



So ganz trauen die Entwickler von Open BSD, das als BSD-Variante Sicherheit in den Vordergrund stellt, den Veröffentlichungen Intels zu Sicherheitslücken in den modernen Prozessoren nicht mehr. Kurzerhand hat man sich bei Open BSD entschieden, Hyperthreading auf Intel-CPUs bis auf Weiteres abzuschalten. Grund ist die Bekanntgabe der neuen Sicherheitslücke „TL Bleed“ (siehe oben). Es gibt aber auch prinzipielle Bedenken, die auf eine Studie aus dem Jahr 2005 zurückgehen, welche nachweist, dass Hyperthreading generell risikobehaftet ist. Hyperthreading erlaubt Betriebssystemen die Verteilung von Prozessen auf wesentlich mehr virtuelle Prozessorkerne, als tatsächlich physikalisch vorhanden sind, und kann dank der Parallelisierung die Gesamtleistung steigern. Die Open-BSD-Entwickler erwarten aber eine Reihe weiterer Sicherheitslücken durch Cache-Timing-Attacken, die fremde Prozesse auslesen könnten.

Warndienst: Firefox Monitor

Bin ich schon gehackt? Diese Frage stellen sich die meisten Anwender viel zu spät. Vielen Usern wären mit der grundsätzlichen Annahme „Verdammt, ja!“ durchaus geholfen. Die Mozilla Foundation will jetzt mithelfen, dass solche Annahmen zur Gewissheit werden, wenn Zugangsdaten bereits in Crackerdatenbanken und auf Webseiten veröffentlicht werden. In einer Partnerschaft mit dem Dienst „Have I Been Pwned“ will der Firefox-Browser bald vor gehackten Zugängen zu Webdiensten aller Art warnen. Aufgrund der strengen DSVGO-Regularien wird dieser nützliche Dienst namens „Firefox Monitor“ europäischen Nutzern aber aus rechtlichen Gründen nicht so bald zur Verfügung stehen können.

UPDATETELEGRAMM

Raspbian 2018-06-27
Das Quasi-Standardsystem für den Raspberry Pi erhielt Ende Juni ein umfangreiches Update. Die Debian-Variante, die speziell für den Ein-Platinen-Computer angepasst ist, zeigt nach dem ersten Boot einen grafischen Setupassistenten an. Das herunterladbare Image ist um 200 MB kleiner geworden, weil optionale Programme in das neue Menü „Recommended Software“ ausgelagert wurde (*www.raspberrypi.org/downloads*).

Peppermint-OS 9
Der leichtgewichtige Ubuntu-Abkömmling aktualisiert seine Betriebssystembasis auf Ubuntu 18.04 und liefert etliche Tools für die Arbeit in Clouddiensten wie Microsoft Office Online, Google Docs sowie Dropbox. Chromium ersetzt Firefox als vorinstallierten Browser und XFCE-Komponenten ersetzen die älteren LXDE-Bestandteile des Desktops. Peppermint-OS 9 gibt es weiterhin in 32 Bit und 64 Bit (*https://peppermintos.com*).

AV Linux 2018.6.25
Um Audio- und Videoproduktion geht es im Debian-Derivat AV Linux. Zur vorinstallierten Software gehören der Multitracker Ardour, der Effektmixer Calf Studio Gear, der Drumcomputer Hydrogen und das Notationsprogramm Musescore. Unter den Videotools sind Cinelerra, Kdenlive und Openshot vertreten. AV Linux liefert einen Echtzeit-Kernel für möglichst geringe Latenzen bei der Signalverarbeitung und den Soundserver Jack (*www.bandshed.net/avlinux*).

Suse Linux Enterprise 15
Nach der Veröffentlichung von Open Suse Leap 15 (auf Heft-DVD) zog auch die Serverausgabe Suse Linux Enterprise nach und bringt seine Versionsnummer mit der freien Ausgabe in Einklang. Das neue Versionsschema soll die nahe Verwandtschaft der beiden Systeme signalisieren, die sich eine gemeinsame Basis teilen. Open Suse Leap kann jetzt direkt zur Enterpriseversion migriert werden. Eine Testversion gibt es ohne Abo unter *www.suse.com/de-de/download-linux*.

Fuchsia: Linux-Apps willkommen

Google baut für zukünftige Mobilgeräte schon seit zwei Jahren an einer Linux-Alternative namens „Fuchsia“, einem alternativen Micro-Kernel namens „Zircon“ aus eigener Entwicklung. Dies sei kein Linux-Abkömmling, machte Google schon im April klar, sondern ein eigener Ansatz. Der Quellcode zu Fuchsia ist unter *https://fuchsia.googlesource.com* einsehbar, zudem gibt es gibt bereits Demosysteme. Relativ neu ist die Ankündigung, dass Fuchsia diverse Linux-Anwendungen über die Virtualisierungsschnittstelle Virt IO unterstützen und möglichst nahtlos integrieren will. Wenn dies gelingt, hätte Google einen Ersatz für den Linux-Kernel in Android und in Chrome-OS. Die Lizenzpolitik der GNU Public License wird Fuchsia aber weiträumig umgehen. ■

Mint Box Mini 2

Quelle: Compulab

Gleichzeitig mit der Veröffentlichung der neuen Mint-Version 19 (auf Heft-DVD) haben die Hardwarespezialisten von Compulab den neuen Super-Mini-PC Mint Box Mini 2 vorgestellt. Der Name ist Programm, denn das Gerät wird mit Linux Mint 19 vorinstalliert ausgeliefert. Es handelt sich bereits um die vierte Generation der kleinen, passiv gekühlten Computer, deren Aufbau mit solidem Kühlkörper von den Industrie-PCs des Herstellers abstammt. Der Rechner basiert jetzt auf Intels Apollo Lake mit einem Celeron J3455 und vier GB RAM. Eine Pro-Version mit acht GB ist ebenfalls verfügbar. Der mitgelieferte Datenträger ist eine M.2-SSD mit 64 GB Kapazität. Der Preis liegt für das Grundmodell bei 299 Dollar plus MwSt. Wer mehr ausgeben möchte, kann sich auf *https://fit-iot.com/web* ein Wunschgerät anhand der verfügbaren Erweiterungsmodule selbst zusammenstellen. Ein fixer Betrag von fünf Prozent des Kaufpreises geht automatisch an die Entwickler von Linux Mint. ■

Google: Platin-Partner der Linux Foundation

Ende Juni hat Google seine Mitgliedschaft in der Linux Foundation, die sich um die Kernel-Entwicklung kümmert, vom Status „Silver“ auf „Platinum“ angehoben. Für rund 500 000 Dollar Jahresbeitrag gibt es dafür in der recht bodenständigen Linux Foundation einen Sitz im Direktorium. Liebe, Hassliebe oder Mittel zum Zweck? Klar ist, dass Google und deren Holding Alphabet ohne Linux heute nicht dort wäre, wo sie gegenwärtig ist: Alphabet hat eine Marktkapitalisierung von 763 Milliarden US-Dollar und liegt damit knapp hinter Amazon als das zweitwertvollste Unternehmen der Welt an der Börse. Alphabets Server laufen zumeist mit Linux, Android nutzt den Linux-Kernel und es ist anzunehmen, dass die meisten Mitarbeiter mit einem PC arbeiten, auf dem Debian oder Ubuntu läuft.

Trotzdem zeichnet es sich ab, dass Alphabet im Hardwaregeschäft einige Probleme mit Linux hat, denn die GNU Public License des Kernels gilt unter Hardwarepartnern als pures „Gift“: Die Lizenzklauseln verlangen eine frei zugängliche Dokumentation aller abgeleiteten Formen des Kernels. Auch deshalb dürfte Alphabet gerade an der Alternative „Fuchsia“ arbeiten, die unter der freizügigeren MIT-Lizenz steht. In den nächsten Jahren bleibt Linux aber eine wichtiger Motor im System von Alphabet und seiner Infrastruktur sowie hinter deren Marke Google und den Produkten. ■

Blender versus Youtube

Eine echte Internetposse spielte sich zwischen der Blender Foundation und Youtube ab, nachdem der Kanal der Blender-Entwickler mit den Demovideos des 3D-Animationsprogramms gesperrt wurde. Schon Ende 2017 waren einige Blender-Videos nicht mehr verfügbar, weil die Macher des Open-Source-Programms die damit erstellen Clips nur ohne Anzeigen auf Youtube veröffentlichen wollten.
Google forderte von Blender aufgrund der Popularität des Youtube-Kanals die Monetarisierung der Videos. Ein Versehen, wie der Youtube-Support im Juni beteuerte und fast alle Videos wieder freischaltete. Die Blender-Foundation möchte aber bis jetzt nicht alle neuen Geschäftsbedingungen seitens Youtube für europäische Videopublisher akzeptieren und prüft derzeit Alternativen. ■

Ubuntu: Intel NUCs mit Zertifizierung

Die siebte Generation von Intels Mini-PC-Familie Intel NUCs (Next Unit of Computing) hat von Canonical eine Ubuntu-Zertifizierung erhalten. Damit garantiert Canonical, dass Ubuntu einwandfrei auf dieser Hardware funktioniert. Diese umfasst Intels Kaby-Lake-Prozessoren vom Typ i3, i5 und i7. Wichtig ist eine Zertifizierung für Industrieanwendungen und Firmenkunden, die Ubuntu im großen Stil einsetzen möchten. Eine für Intel NUCs angepasste Ausgabe von Ubuntu 16.04.4 mit allen benötigten Treibern steht zum Download bereit (*www.ubuntu.com/download/iot/intel-nuc-desktop*). ■

Quelle: Intel

LINUXWELT-DVD MIT VIDEOTUTORIALS

Die Entwicklung um Open Source und Linux sowie primär der praktische Einsatz erzeugt eine ungeheure Vielfalt an Dokumentation, Onlinediskussionen – und Publikationen wie die LinuxWelt. Es geht aber auch ohne allzu viel Text und Lesestoff. Eine Schar von Linux-Fans produzieren, mal mit Kostenerstattung, mal unbezahlt, einen großen Schatz an Podcasts, Videos und Videotutorials. Die meisten Produktionen sind in englischer Sprache, doch nicht alles: Für die DVD-Inhalte dieser Ausgabe hat uns der Youtuber Dominik Zerbe zehn seiner Videotutorials überlassen – und das natürlich werbefrei. Die Videos finden sich auf Heft-DVD im Unterverzeichnis „Videos“ und liegen im MP4-Format vor, mit dem beispielsweise VLC klarkommt. Der komplette Youtube-Channel von Dominik Zerbe mit vielen weiteren Open-Source-Themen findet sich unter *https://www.youtube.com/user/dominiksoftware*.

UPDATETELEGRAMM

Tails 3.8
Das Livesystem mit vorkonfiguriertem TOR-Client zu Teilnahme am anonymisierenden TOR-Netzwerk aktualisiert die Programmkomponenten für die Open-PGP-Verschlüsselung. Die Korrekturen in den Paketen Thunderbird und der Verschlüsselungserweiterung Enigmail richten sich gegen die Sicherheitslücke „Efail“, die im Mai bekannt wurde und PGP durch HTML-Anhänge brechen kann (*https://tails.boum.org*).

VR180 Creator
Überraschung von Google: Das frisch vorgestellte Programm namens VR180 Creator, das Videoaufnahmen mit einem Bildwinkel von 180 Grad bearbeiten und in andere Formate exportieren kann, erscheint für Mac-OS und den Linux-Desktop – allerdings nicht für Windows. Das Tool konvertiert Fischauge-Aufnahmen auf eine rektanguläre Projektion, die in beliebigen Schnittprogrammen bearbeitet werden kann. Das fertige Video kann VR180 Creator wieder mit VR-Metadaten versehen (*https://vr.google.com/vr180/apps*).

Krita 4.1
Das erfolgreiche Mal- und Illustrationsprogramm für professionelle Ansprüche ist in der Version 4.1 in seinem Funktionsumfang um ein Multimonitor-Setup erweitert, das den Arbeitsbereich optimal auf mehrere Bildschirme verteilt. Arbeitssitzungen mit geöffneten Dateien kann Krita nun speichern und wiederherstellen. Auch die Animationswerkzeuge haben die Entwickler ausgebaut und verbessert (*https://krita.org*).

Firefox 61
Schneller als ursprünglich geplant hat Mozilla die Entwicklung des neuen Firefox Quantum abgeschlossen. Schnelligkeit steht insgesamt bei diesem Release im Vordergrund: CSS-Definitionen kann Firefox jetzt in mehreren CPU-Threads berechnen. Der kommende Verschlüsselungsstandard TLS 1.3 bekommt erstmals Unterstützung in Firefox (*www.mozilla.org/de/firefox*).

Ubuntu-Optimierung

Ubuntus neue LTS-Version von April ist noch taufrisch und längst nicht ausgelotet in allen technischen Vorzügen – und Defiziten. Die folgenden Beiträge helfen bei der Systemoptimierung und Mängelbeseitigung.

VON HERMANN APFELBÖCK

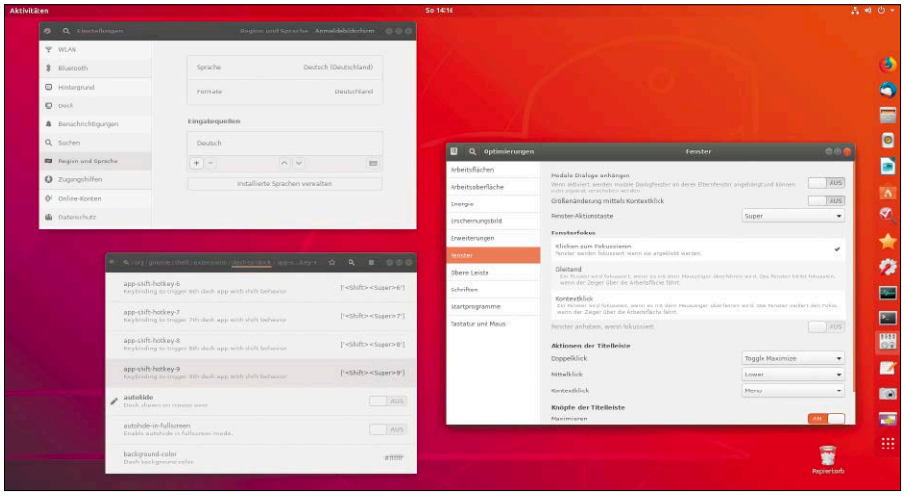
Das Ubuntu-Special zur aktuellen LTS-Version setzt die Artikelsammlung der letzten LinuxWelt 4/2018 fort. Die Themen sind Desktoptuning mit Fokus auf die Gnome-Hauptedition, ferner allgemeines Troubleshooting, Snap-Container und optimale Servereinrichtung. Beachten Sie, dass wir die im letzten Heft gelegten Grundlagen zur Desktopwahl, Installation, Ersteinrichtung mit Systemaktualisierung, Sprachunterstützung und Treiberoptimierung nicht wiederholen. Auch einfacheres Desktoptuning (Dock, Gnome-Erweiterungen, Onlinekonten, Tastatur, Benutzerverwaltung) und Hinweise auf die Optimierungstools Gnome-Tweaks und Dconf-Editor finden Sie im letzten Heft.

Das letzte Heft haben Sie nicht? Doch – jedenfalls alles, was Ubuntu 18.04 betrifft: Das E-Book „LinuxWelt 2018-05“ auf Heft-DVD (unter „/Ebook“) enthält alle Ubuntu-Beiträge der letzten Ausgabe (Startartikel unter der Rubrik „Distributionen“).

Diverse Autostarts abschalten

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

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



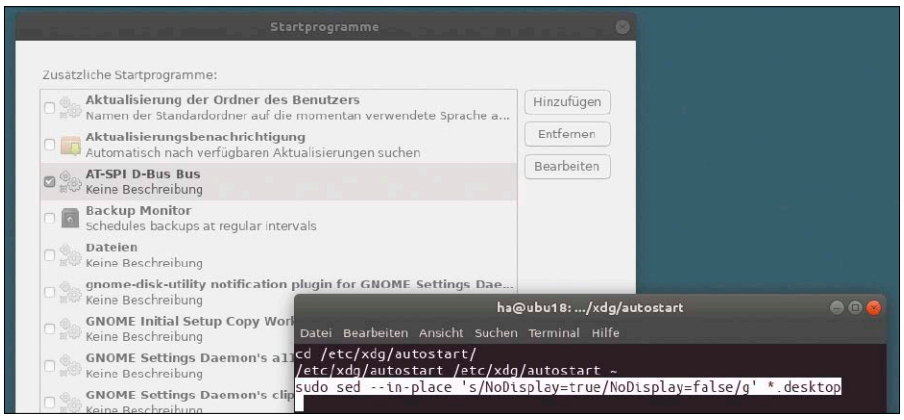
Nun zeigt „Startprogramme“ alle Komponenten. Theoretisch können Sie fast alles deaktivieren außer D-Bus und den Sicherheitsdienst. Damit ist Ubuntu auf deutlich unter ein GB RAM zu verschlanken, ohne Cache auf unter 700 MB (siehe *free -m*).

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

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

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

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



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

„org.gnome.desktop.privacy“ abschalten („report-technical-problems“).

Leistung und Speicher optimieren

Wenn ein Rechner mit acht GB RAM und mehr so gut wie nie „swappen“ muss (siehe „Systemüberwachung → Ressourcen“), sind Optimierungsmaßnahmen weder nötig noch erfolgversprechend. Auf einem zäh laufenden System bietet der Linux-Kernel aber die Möglichkeit, das Swapverhalten zu beeinflussen. Der „Swappiness“-Wert darf zwischen 10 und 100 liegen, Standard ist „60“. Je höher der Wert, desto intensiver schreibt der Kernel Speicherseiten aus dem RAM in die Swappartition. Ein niedriger Wert wie „10“ kann bei guter RAM-Ausstattung, aber langsamer mechanischer Platte vorteilhaft sein. Umgekehrt kann ein hoher Wert die Systemleistung verbessern, wenn der Speicher eher knapp ist, aber die Swappartition auf einer schnellen SSD liegt. Denn dann bleibt den laufenden Programmen mehr RAM, andererseits bremst die Auslagerung auf SSD das System kaum aus. Um den Wert temporär zu erhöhen, geben Sie im Terminal dieses Kommando ein:

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

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

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

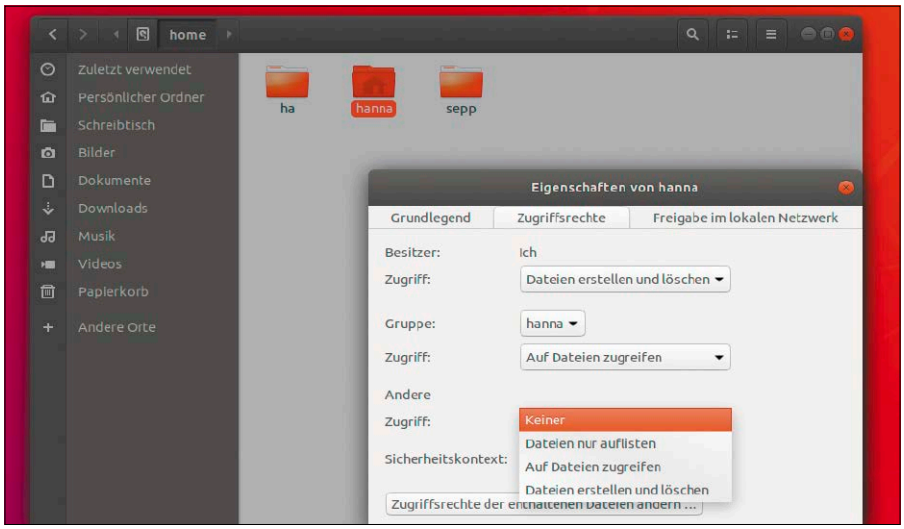
Suchen Sie „vm.swappiness“ und ändern Sie den Wert. Wenn der Eintrag fehlt, fügen Sie einfach folgende Zeile am Ende der Datei hinzu:

```
vm.swappiness=90
```

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

Schnellen Spiegelserver festlegen

Für alle Installationen und Updates benötigen Sie einen Spiegelserver, der die Ubuntu-Paketquellen bereitstellt und möglichst schnell ausliefert. Je schneller Ihre Internetverbindung ist, desto mehr profitieren Sie von einem richtig schnellen Spiegelserver. Ubuntu kann den geeignetsten deutschen Server selbst ermitteln: Dazu gehen Sie auf „Anwendungen & Aktualisierungen“ (software-properties-gtk). Auf der ersten Registerkarte „Ubuntu-Anwendungen“ ist ein Server voreingestellt. Diesen können Sie anklicken und „Andere“ auswählen, wonach Sie im Unterfenster die Option „Besten Server auswählen“ antreffen. Diese erledigt einige Verbindungstests und schlägt dann einen Server vor. Für Deutschland immer eine gute Wahl ist netcologne.de, das Sie auch direkt manuell auswählen können.



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

Das Home-Verzeichnis im Multiuserbetrieb

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

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

DIESE ZUSATZSOFTWARE BRAUCHEN SIE

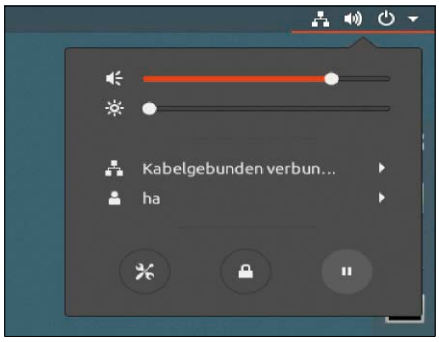
Wie bereits in der letzten LinuxWelt empfohlen (siehe LinuxWelt XXL auf Heft-DVD) brauchen Sie für bessere Kontrolle der Gnome-Oberfläche die zusätzlichen Tools **Gnome-Tweaks** („Optimierungen“) und **Dconf-Editor**, die mit gleichnamigen Paketnamen schnell nachinstalliert sind. Der Dconf-Editor wird auch in einigen Tipps dieses Artikels vorausgesetzt. Desgleichen lohnt sich die Durchsicht der zahlreichen **Gnome-Erweiterungen** in der Software-Zentrale „Ubuntu-Software“ unter „Erweiterungen → Shell-Erweiterungen“. Installierte Erweiterungen können Sie über Gnome-Tweaks bequem verwalten.

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

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

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

Ein dringender Installationskandidat auf Notebooks ist nach dem Wegfall der Home-Verschlüsselung die Software **Veracrypt**. Alles, was Sie zu Veracrypt wissen müssen, erfahren Sie in diesem Heft ab Seite 68.



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

Das System in „Bereitschaft“ versetzen

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

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

```
systemctl suspend
```

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

Die Bildschirmdarstellung optimieren

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

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

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

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

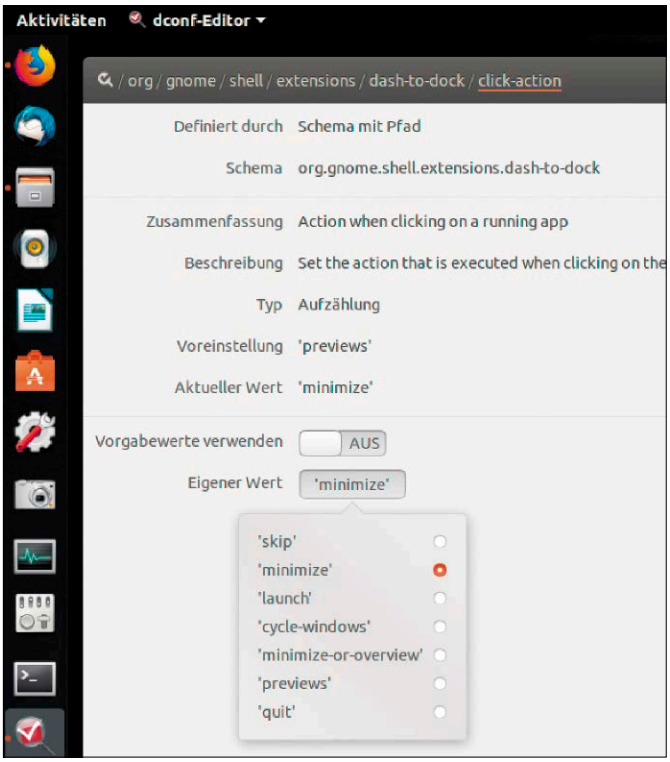
```
xrandr --output DVI-0 --scale
 1.2x1.2
```

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

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

Mit Dconf das Starterdock optimieren

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



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

drückter Umschalttaste bei einem bereits laufenden Programm eine zweite Instanz startet (nützlich etwa beim Terminal, Editor oder Dateimanager). Die Einstellung unter „org.gnome.shell.extensions.dash-to-dock“ lautet „shift-click-action“.

Voreinstellungen, die wir weniger optimal finden, gelten für „click-action“ und „middle-click-action“ – beides bezogen auf bereits laufende Programme. Für „click-action“ gilt die Aktion „previews“, was gar nichts hermacht. Hier ist „minimize“ eine gute Wahl: Das Programmfenster wird dann beim Klick auf sein Dock-Icon minimiert oder wiederhergestellt.

Für „middle-click-action“ ist „launch“ voreingestellt, was schon der normale Mausklick erledigt. Eine überlegenswerte Alternative für den Klick auf das Mausrad ist „quit“ – das schließt alle Instanzen eines laufenden Programms.

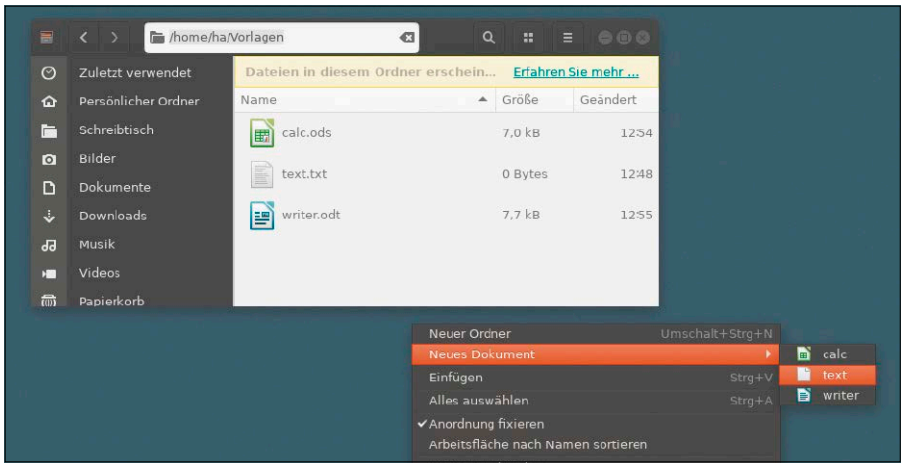
Erweiterungen für den Dateimanager

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

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

Die Auswahl aus den Erweiterungen, mit *sudo apt install* ... und den angezeigten Paketnamen leicht zu installieren, sollte aber dosiert erfolgen, um das Kontextmenü übersichtlich zu halten. Standardmäßig installiert ist „nautilus-extension-gnome-terminal“, das als Kontextoption „In Terminal öffnen“ erscheint. Ein wichtiger Kandidat ist „nautilus-admin“ mit dem Angebot („Als Administrator öffnen“ für Verzeichnisse Weitere Empfehlungen sind „nautilus-extension-brasero“ zur direkten Bearbeitung von Imagedateien sowie „seahorse-nautilus“, das eine sehr bequeme Option „Verschlüsseln“ für alle Dateien in Nautilus integriert. Die Erweiterungen „nautilus-compare“ (Dateien vergleichen), „nautilus-hide“ (Dateiobjekte über eine zusätzliche Datei „.hidden“ verstecken), „nautilus-wipe“ (Plattenplatz sicher überschreiben) bieten einfache Dateioperationen.

Andere Erweiterungen wie „nautilus-owncloud“, „easytag-nautilus“ oder „nitroshare-nautilus“ sind zum Teil recht speziell und nur Nutzern zu empfehlen, die in der angesprochenen Software (Owncloud, Nitroshare, Easytag) zuhause sind.



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

Das ehemalige Tool Nautilus-Actions, mit dem Sie Nautilus individuell mit eigenen Befehlen ausbauen können, ist in Ubuntu 18.04 nur noch über ein PPA beziehbar

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

und nennt jetzt sich nach der Installation „fma-config-tool“.

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

Kleine Anpassungstipps

Modale Dialoge: Es handelt sich um abhängige Unterfenster, die das Elternfenster solange blockieren, bis der Unterdialog wieder geschlossen wird. Ein Beispiel ist etwa der Dialog „Eigenschaften“ im Dateimanager. Standardmäßig ist Gnome so eingestellt, dass es Unter- und Elternfenster als ein Fenster zusammenfasst: Verschiebt man das Unterfenster, wandert das deaktivierte automatisch mit. Das ist gewöhnungsbedürftig und in Fällen wie dem Dateimanager auch unpraktisch, weil der Inhalt des Hauptfensters verdeckt und nicht zu lesen ist. Die Einstellung ist über Gnome-Tweaks („Optimierungen“) aber leicht zu ändern, indem Sie die Option „Fenster → Modale Dialoge anhängen“ deaktivieren.

Aktive Ecke: Die „Aktivitäten“ mit dem Suchfeld, der Fenster- und Arbeitsflächenübersicht sind sowohl durch die Super/Windows-Taste als auch durch Klick auf „Aktivitäten“ auszulösen. Seit je gibt es aber auch noch die Option einer aktiven Ecke (links oben), die beim Anfahren des Mauszeigers die „Aktivitäten“ startet. Diese Ecke ist standardmäßig inaktiv, aber im Dconf-Editor unter „org.gnome.shell“ mit der Einstellung „enable-hot-corners“ leicht scharfzuschalten.

Nachtmodus: Dieses relativ junge Angebot der Gnome-Shell ist ganz regulär in den „Einstellungen“ unter „Geräte → Anzeigegeräte“ zugänglich. Hier können Sie den Anteil der wärmeren Rotfärbung gegenüber hartem Blau per Regler selbst bestimmen. Wann der Nachtmodus gelten soll, überlassen Sie entweder dem System oder definieren die Zeiten manuell.

Dconf zurücksetzen: Der Dconf-Editor kann durch zahlreiche Anpassungen grafische oder auch bedientechnische Probleme in der Gnome-Shell auslösen. Wenn Sie dann nicht mehr zielsicher die maßgebliche Option aufsuchen können, hilft immer noch großzügiges Zurücksetzen auf die Standards. Dazu markieren Sie einen Überpunkt wie „gnome“ und verwenden nach Rechtsklick die Option „Rekursiv zurücksetzen“. ■

Problemlöser für Ubuntu 18.04

Auch LTS-Versionen von Ubuntu mit Langzeitsupport sind nicht frei von kleineren Lästigkeiten oder auch Versäumnissen der Entwickler. Die folgende Sammlung zeigt häufige Probleme und deren Lösungen in Ubuntu 18.04 LTS und Varianten.

VON DAVID WOLSKI

Kaum eine andere Distribution bekommt bei jeder Ausgabe so viel Aufmerksamkeit wie Ubuntu. Die Entwicklung von Ubuntu und die einzelnen Softwarepakete sind weiterhin eng mit Debian GNU/Linux verbunden, da dies die Basis für Ubuntu stellt. Auch im Entwicklerteam gibt es einige personelle Überschneidungen. Die Größe der Ubuntu-Community erlaubt eine Veröffentlichung alle sechs Monate und eine Ausgabe mit Langzeitsupport von fünf Jahren im Zweijahresrhythmus. Die praktische Erfahrung seit April hat gezeigt, dass Ubuntu 18.04 zwar deutlich weniger Probleme macht als die letzte LTS-Version 16.04. Trotzdem gibt es immer wieder die Notwendigkeit, Bugs im Zusammenspiel mit Hardware zu lösen oder Pakete und die Systemkonfiguration zu ergänzen. Die folgenden Themen behandeln Schwierigkeiten, die uns in der Redaktion selbst bei der Arbeit mit Ubuntu 18.04 begegnet sind, ferner Probleme, für welche auf der Frage-Antwort-Webseite *https://askubuntu.com* besonders häufig Lösungen gesucht werden.

Installer: Abstürze bei Hi-DPI

Monitore mit sehr hoher Auflösung sind nun wahrlich keine Seltenheit mehr und Gnome 3.28, der Standarddesktop Ubuntus, kann prinzipiell dank automatischer Skalierung gut mit Hi-DPI-Bildschirmen umgehen. Der Installer im Livesystem macht dennoch oft Ärger und stürzt bei diesen Auflösungen gerne ab.

Lösung: Bis der Bug in Ubuntu 18.04.1 gelöst wird, muss das installierbare Livesystem mit Gnome, das seine Desktopelemente automatisch ab 192 DPI vergrößert, erst wieder herunterskaliert werden. Dies gelingt in Gnome über die Einstellungen und dort unter „Geräte → Anzeigegeräte → Skalieren → 100 %“. Nach gelungener Installation können Sie diesen Wert wieder höhersetzen.

Zur Installation herunterskaliert: Das Installationsprogramm funktioniert in Ubuntu 18.04 nicht zuverlässig, wenn die Menüelemente bei hohen Auflösungen automatisch vergrößert wurden.

Alte Karten neu gemischt: Für betagte Nvidia-Karten wie diese Geforce 7100 gibt es keine proprietären Treiber mehr. Wer diese unbedingt benötigt, muss bei Ubuntu 16.04 bleiben.

Energieverwaltung: ASPM abschalten

Auf brandneuen Notebooks mit Intel-Chipsatz und NVMe-Laufwerken gerät schon im Livesystem die Energieverwaltung aus dem Tritt: Die Installation scheitert dann an Zugriffsfehlern, die sich in einem Terminalfenster über den Aufruf *dmesg* in den Kernel-Meldungen zeigen. Typische Fehlermeldungen lauten hier „PCIe Bus Error“ und treten meist so zahlreich auf, das sie kaum zu übersehen sind.

Lösung: Schuld an diesem Fehler sind die Stromsparfunktionen des „Active State Power Management“ (ASPM), das in Ruhephasen Geräte am PCIe-Bus mit weniger Strom versorgt. Das funktioniert in Ubuntu 18.04 aber nicht mit allen Laufwerken und es droht sogar Datenverlust. Abhilfe schafft der Kernel-Parameter

```
pcie_aspm=off
```

der beim Start des installierbaren Livesystems ergänzt wird. Dazu drücken Sie beim Bootbildschirm des Ubuntu-Livesystems die Taste F6 und fügen dann an die eingeblendete Zeile den genannten Kernel-Parameter an, um danach mit der Eingabetaste zu booten. Bei einem bereits installierten System muss der Parameter in die Datei „/etc/default/grub“ eingetragen werden, die man auf der Kommandozeile mit

```
sudoedit /etc/default/grub
```

öffnet. Dort kommt der Parameter mit in die Zeile „GRUB_CMDLINE_LINUX_DEFAULT“:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet
  splash pcie_aspm=off"
```

Damit die Änderung wirksam ist, müssen Sie anschließend die Grub-Konfiguration mit dem Befehl

```
sudo update-grub
```

aktualisieren.

AMD: Flackernde Bildschirme

Bei einigen AMD-Grafikchips wie dem RX480 und dem RX580 kommt es vor, dass der Bildschirm stark flackert. Das Problem tritt mit dem neuen Open-Source-Treiber AMDGPU für Radeon-Chips auf.

Lösung: Bis mit dem Point Release Ubuntu 18.04.1 eine neue Kernel-Version erscheinen wird, die die Kompatibilität mit einigen AMD-Grafikkarten verbessert, hilft vorläufig der Kernel-Parameter

```
amdgpu.dc=0
```

Dieser wird genauso, wie vorher beim ASPM-Problem beschrieben, als Standard-Bootparameter in die Datei „/etc/default/grub“ eingetragen:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet
  splash amdgpu.dc=0"
```

Auch dieser Eingriff muss mit *sudo update-grub* abgeschlossen werden, damit Grub diese Änderungen in das tatsächliche Bootmenü aufnimmt.

Nvidia: Keine Treiber für alte Karten

Wer noch Nvidia-Grafikkarten der Serie Geforce 6 und 7 im Einsatz hat, wird über die Treibersuche unter „Anwendungen & Aktualisierungen → Zusätzliche Treiber“ keine passenden proprietären Nvidia-Treiber mehr finden.

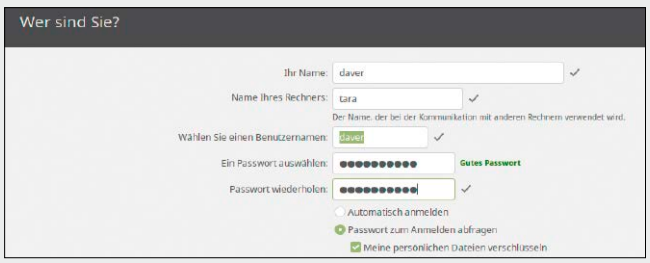
Lösung: Nvidia hat die Unterstützung für alte Karten aus aktuellen Treibern entfernt. Die letzte Treiberversion für Chips vom Typ Geforce 6 und 7, die durchaus noch in etlichen Bürorechnern arbeiten, waren die Nvidia-Treiber 304.x. Genau dieses Treiberpaket ist aber in Ubuntu 18.04 nicht mehr vorhanden. Es gibt zwar ein PPA für ältere Nvidia-Treiber, aber dies funktioniert im neuen Ubuntu nicht mehr. Dort ist die einzige Lösung, ältere Karten mit dem quellof-

VERSCHLÜSSELUNG: ECRYPTFS UND UPGRADES

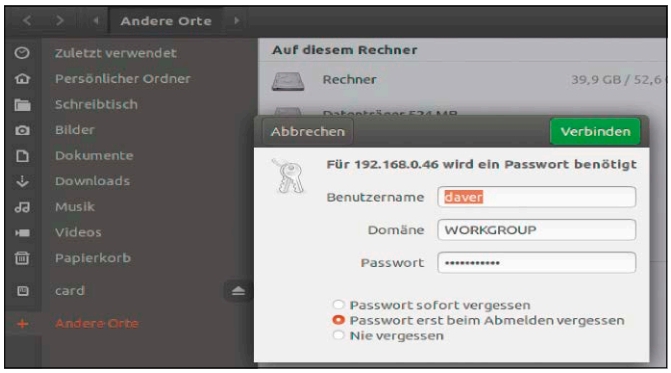
Ab Ubuntu 18.04 gibt es im Installationsprogramm beim Anlegen des Erstbenutzers die Option „Meine persönlichen Daten verschlüsseln“ nicht mehr.

Im Gegensatz zu nach wie vor vorhandenen Komplettverschlüsselung des Systems, die ganze Partitionen chiffriert (Luks), schützte diese Art der Verschlüsselung mit dem Programm Ecryptfs nur das eigene Verzeichnis auf Ordnerebene. Ecryptfs ist nicht komplett aus Ubuntu entfernt – es findet sich weiterhin in den Ubuntu-Paketquellen. Das Paket „ecryptfs-utils“ ist vom Repository „Main“, das offiziell gepflegt wird, in das weniger gut gepflegte Community-Repository „Universe“ gewandert. Es wird derzeit nicht mehr aktiv weiterentwickelt, nachdem der zuletzt dafür zuständige Entwickler das Projekt verlassen hatte. Es gibt keine Bugs, die einen Einsatz auf Ubuntu 18.04 unmöglich machen. Aber Kritiker weisen darauf hin, dass diese Verschlüsselungsmethode nicht besonders sicher ist, da temporäre Dateien auch außerhalb von Home entstehen und dann nicht verschlüsselt sind. Wer ein bestehendes Ubuntu 17.10/16.04 auf die neue LTS-Ausgabe aktualisiert, hat trotzdem nichts zu befürchten: Bei einem Update auf Ubuntu 18.04 installiert das System Ecryptfs automatisch mit und kann das verschlüsselte Home-Verzeichnis weiterhin öffnen. Ein vorheriges (unverschlüsseltes) Backup der persönlichen Daten sollten Sie in dieser Situation trotzdem anlegen.

Linux Mint 19 hat die Ecryptfs-Verschlüsselungsoption für das Home-Verzeichnis im Installer übrigens rekonstruiert.



Ab jetzt ein Merkmal von Linux Mint: Ubuntu 18.04 kann zwar verschlüsselte Home-Verzeichnisse bei einer Aktualisierung übernehmen, der Installer bietet diese Option aber nicht mehr an.



Wege ins Windows-Netzwerk: Aufgrund einer neuen Samba-Version ist der Browser für das Windows-Netzwerk kaputt. Man kann aber Hosts direkt mit Name oder IP-Adresse öffnen.

fenen Treiber Nouveau zu betreiben. Die Liste unter *http://www.nvidia.com/object/IO_32667.html* zeigt, welche Karten davon betroffen sind.

Netzwerk: Das Tool ifconfig fehlt

Der Aufruf *ifconfig* zur Anzeige der eigenen IP-Adresse im Netzwerk ist vielen Anwendern schon ins Muskelgedächtnis eingegangen. Ubuntu 18.04 kennt diesen Befehl jedoch nicht mehr.

Lösung: *ifconfig* ist schon eine ganze Weile auf dem Weg auf das Abstellgleis und wird seit 2009 nicht mehr gepflegt, weil es mit IPv6-Adressen nicht gut umgehen kann. So ist es wenig überraschend, dass es in den neuen Ausgaben wichtiger Distributionen gar nicht mehr enthalten ist, sondern von folgendem Aufruf

```
ip a
```

ersetzt wurde. Wer sich noch nicht umgewöhnen will, kann in Ubuntu 18.04 mit diesem Terminalbefehl

```
sudo apt install net-tools
```

das gewohnte Tool *ifconfig* nochmal nachinstallieren.

Freigaben: Kein Windows-Netzwerk

In Ubuntu kümmert sich der Dienst Samba um die Verbindung zu Freigaben im Windows-Netzwerk über das SMB-Protokoll. Ubuntu 18.04 liefert nach einigen Sicherheitslücken in SMB mit Samba 4.7.4 eine neue Version des Dienstes mit geänderter Standardkonfiguration aus. Diese verhindert die Verbindungsaufnahme zu Windows-Netzwerken im Dateimanager, um Hosts und Freigaben aufzulisten.

Lösung: In der aktuellen Version des SMB-Protokolls, das beispielsweise von Windows 10 und aktuellen Linux-Hosts genutzt wird, ist das automatische Durchsuchen des Windows-Netzwerks nach Servern und Freigaben nicht mehr vorgesehen. Stattdessen muss man sich neuerdings direkt mit einem Host anhand dessen Hostnamen oder der IP-Adresse verbinden. Im Dateimanager Nautilus öffnet die Tastenkombination Strg-O ein Feld, das sich mit der Eingabe

```
smb://[Adresse]
```

zum gewünschten Server verbindet.

Codecs: Fehlende Gstreamer-Plug-ins

Es kommt selten vor, dass Ubuntu mit Mediendateien nichts anfangen kann. MP3-Dateien sind schon lange kein Problem mehr, wenn im Installer die Option „Installation von Drittanbieter-Software für Grafik und WLAN-Geräte, Flash, MP3 und andere Medien“ angeklickt wurde. Trotzdem gibt es immer wieder mal Formate, die Ubuntu zunächst nicht erkennt.

Lösung: Die von einigen Gnome-Programmen angebotene Suche nach Codecs in den Paketquellen ist nicht immer erfolgreich. Zuverlässiger und schneller ist, gleich nach der Ubuntu-Installation alle häufig benötigten Codecs in einem Terminalfenster mit diesem Befehl

```
sudo apt install ubuntu-restricted-extras gstreamer1.0-plugins-bad gstreamer1.0-plugins-ugly
```

nachzurüsten.

Film-DVDs: Codec installieren

Ein Codec zum Abspielen von DVDs ist in Ubuntu 18.04 wie schon im Vorgänger aus

SYSTEMUPGRADE: AB UBUNTU 18.04.1 FÜR ALLE

Einer der großen Vorzüge Ubuntus ist das Distributionsupgrade, das ein bestehendes System ohne Neuinstallation auf die nächste Ubuntu-Ausgabe bringt.

Die Aktualisierungsverwaltung blendet einen Hinweis ein, sobald eine neue Version vorliegt, und startet auf Wunsch den Wechsel auf das neue Ubuntu. Wer mit einer Ubuntu-Zwischenversion wie 16.10, 17.04 oder 17.10 gearbeitet hat, wird den Hinweis bereits erhalten haben, dass 18.04 bereitliegt. Nicht so jene Anwender, die noch mit der letzten LTS-Ausgabe Ubuntu 16.04 arbeiten: Die Aktualisierungsverwaltung bietet das automatische Update erst an, wenn die ersten Kinderkrankheiten ausgestanden sind. Das ist erfahrungsgemäß rund drei Monate nach der Veröffentlichung der LTS-Version der Fall. Ist der Hinweis der Aktualisierungsverwaltung bisher ausgeblieben, so ist in den Systemeinstellungen ein Besuch bei den „Anwendungen & Aktualisierungen“ nötig. Unter „Aktualisierungen → Über neue Ubuntu-Versionen benachrichtigen“ muss „Für Langzeitunterstützungsversionen“ ausgewählt sein.

Tipp: Generell lässt sich ein Systemupgrade zur nächsten LTS-Version auch vor dem Ablauf der drei Monate erzwingen. Der Befehl

```
sudo update-manager -d
```

startet die Aktualisierungsprozedur auf die neue LTS-Ausgabe, falls vorhanden.

Hinweis: Der Installer vom Ubuntu-Livemedium bietet übrigens keine Aktualisierung mehr an, weil Fehler im Paket „apt-clone“ in der Vergangenheit zu unbrauchbaren Systemen führten.

Von Ubuntu 16.04 zu 18.04: Es dauert üblicherweise drei Monate bis zum ersten Point Release, bis die Aktualisierungsverwaltung die neue LTS-Version anbietet.

patentrechtlichen Gründen nicht enthalten. Es gibt auch kein fertiges binäres Paket in den Ubuntu-Paketquellen zum Nachrüsten mehr.

Lösung: Es bleibt weiterhin die Möglichkeit, den Codec für DVDs aus einem Quellcodepaket selbst zu kompilieren. Ubuntu 16.04 vereinfacht diesen Weg mit einem Installations-Script, das im Terminal mit

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

installiert wird. Den eigentlichen DVD-Codec baut dann das Kommando

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

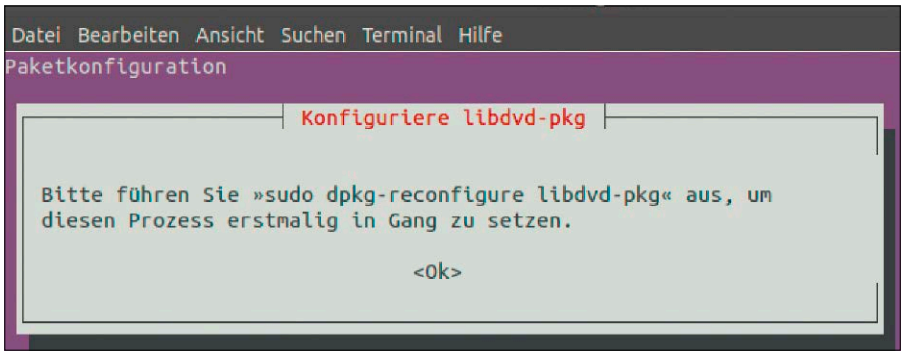
zusammen und installiert anschließend das fertige Paket.

Alte Rechner: Ubuntu für 32 Bit

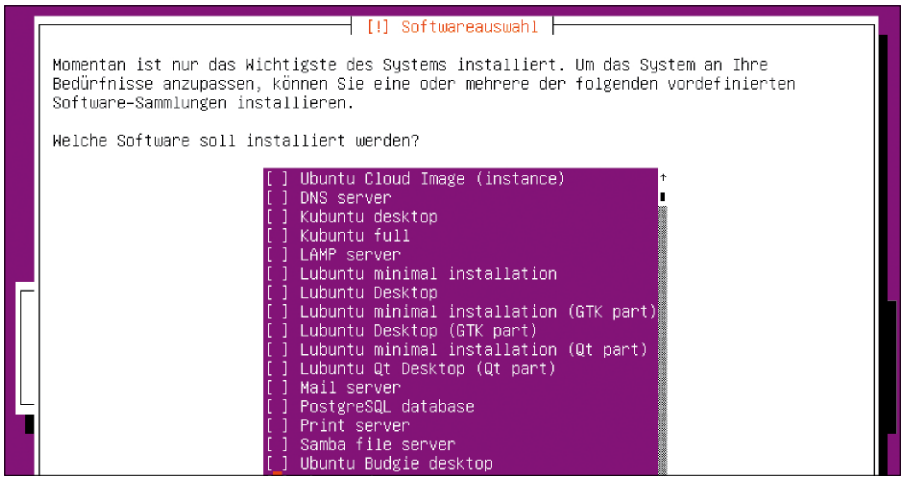
Schon in der letzten Version ließ Ubuntu in seiner Hauptedition mit Gnome-Desktop eine Installation für 32-Bit-Rechner unter den Tisch fallen. Die geringen Downloadzahlen der 32-Bit-Ausgabe rechtfertigten nicht mehr den Aufwand, so die Macher der Distribution. Trotzdem ist Ubuntu mit Gnome-Desktop auch für 32-Bit-Rechner noch verfügbar, nur die Installationsmethode hat sich geändert.

Lösung: Die Installation des regulären Ubuntu 18.04 in 32 Bit gelingt nach wie vor mit den minimalen Installationsmedien für eine Serverinstallation. Diese finden sich bootfähig auf der Heft-DVD dieser Ausgabe und starten die von Debian bekannte textbasierte Installation. Gegen Ende des Installationsprozess gibt es dann die Möglichkeit, gewünschte Paketgruppen auszuwählen. Die Gruppe „Ubuntu desktop“ richtet die reguläre Ubuntu-Arbeitsumgebung mit Gnome ein. ■

Hier fehlt etwas: Die von Gnome mitgelieferten Player greifen im Hintergrund auf das Gstreamer-Gerüst zurück. Weitere Codecs dafür liegen in den Standard-Paketquellen.



DVDs abspielen: In Ubuntu 18.04 gibt es zwar keinen DVD-Codec, aber ein Metapaket, das über einen kurzen Umweg ein passendes Paket baut und installiert.



Zurück zu 32 Bit: Ubuntu 18.04 bietet zwar kein Livesystem mehr für 32 Bit an, aber eine 32-Bit-Installation ist weiterhin über den textbasierten Serverinstaller möglich (auf Heft-DVD).

UNITY 7: DER GEWOHNTE DESKTOP

Eine Menge Arbeit ging in den Gnome-Desktop Ubuntus, damit dieser dem nicht mehr weiterentwickelten Desktop Unity möglichst ähnlich sieht.

Die Gnome-Erweiterung Dash-to-Dock ersetzt das seitliche Panel und ist Programmstarter und Fensterleiste zugleich. Das Fensterverhalten beim Umschalten zwischen Anwendungen ist in Gnome aber trotzdem ein anderes und die Suche nach Programmen führt nun immer über die „Aktivitäten“. Wer den gewohnten Unity-Desktop vermisst, bekommt noch einmal die Möglichkeit, die Pakete ganz regulär aus den Standard-Paketquellen nachzuinstallieren. Dazu dient in einem Terminalfenster dieser Befehl:

```
sudo apt-get install ubuntu-unity-desktop
```

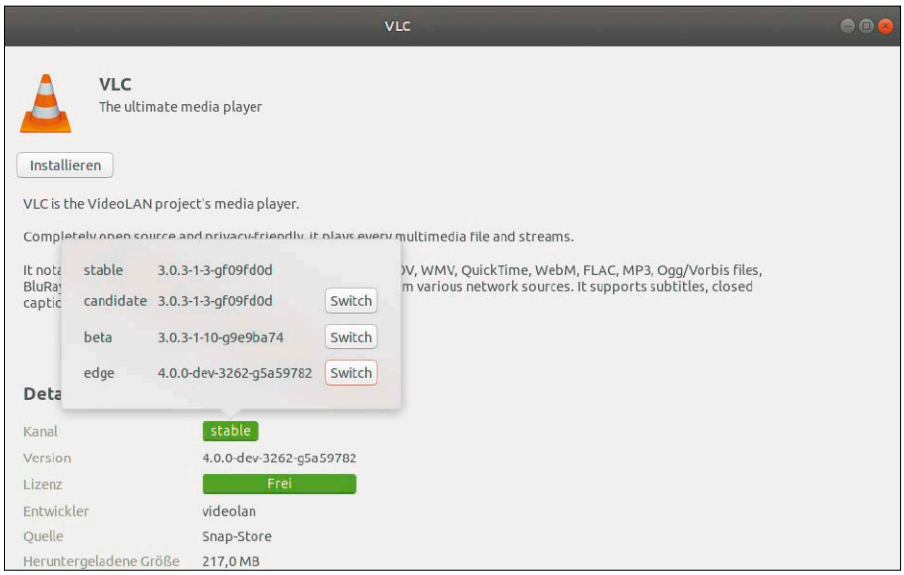
Der Download beträgt etwa 180 MB. Zum Schluss erscheint noch eine Abfrage, ob Gdm3 oder Light DM als Anmeldebildschirm verwendet werden soll. Beide funktionieren und es ist letztlich nur eine Geschmacksfrage, welchen man verwenden möchte.

Gewohnter Anblick: Unity 7 ist nicht ganz verschwunden, sondern liegt noch einmal in den Standard-Paketquellen bereit. Es lässt sich auch parallel zu Gnome installieren.

Snap-Apps in Ubuntu 18.04

Snap-Container enthalten eigenständige Anwendungen, die unabhängig vom restlichen System laufen. Das ermöglicht die einfache Installation neuerer Programmversionen.

VON THORSTEN EGGELING



Frische Software für Ubuntu: Snap-Apps lassen sich bequem über den Paketmanager Ubuntu-Software installieren. Für neuere Versionen wählen Sie einen anderen Updatekanal.

Wer sich für eine Langzeitversion wie Ubuntu 18.04 LTS entscheidet, kann das System fünf Jahre lang ohne größere Änderungen nutzen. Allerdings gibt es dann – bis auf wenige Ausnahmen wie etwa Mozilla Firefox und Thunderbird – auch keine neuen Programmversionen.

Über Updates werden lediglich Fehler behoben und Sicherheitslücken geschlossen. Das sorgt für ein stabiles System, schneidet den Nutzer jedoch von der aktuellen Softwareentwicklung ab.

Einen Ausweg bieten Snap-Apps (kurz: Snaps), über die sich neue Programme oder aktuellere Versionen installieren lassen, ohne die Stabilität des Systems zu gefährden. Das Verfahren ist zwar nicht neu, aber Version 18.04 ist das erste Ubuntu, bei dem bereits einige kleinere Programme in Snap-Containern vorinstalliert sind: gnome-calculator, gnome-characters, gnome-logs und gnome-system-monitor.

Klassische Software und Snap-Apps

Ein Softwareentwickler muss sein Programm genau mit der Ubuntu-Version erstellen, auf der es später laufen soll. Nur so ist sichergestellt, dass die nötigen Bibliotheken bereits vorhanden sind oder nachinstalliert werden können. Dafür sorgen Informationen über Abhängigkeiten, die in jedem DEB-Paket für die Installation unter Ubuntu enthalten sind. Wer ein Programm oder eine Programmversion benötigt, die es für die genutzte Ubuntu-Version nicht gibt, kann meist auf PPAs (Personal Package Archive) zurückgreifen. Das ist jedoch nicht ganz ohne Risiko, weil die angebotenen Pakete nicht immer ausreichend getestet sind und andere Programme beeinträchtigen können.

So funktionieren Snap-Apps: Snap-Apps sind Imagedateien mit der Dateinamenserweiterung „.snap“, die im Ordner „/var/lib/snapd/snaps“ liegen. Es handelt sich um Squashfs-Container, ein komprimiertes und schreibgeschütztes Format, die das System beim Start in Ordner unterhalb von „/snap“ einhängt. Jeder Container enthält einen Verzeichnisbaum, in dem alle Dateien liegen, die ein Programm benötigt. Alleine damit ist es jedoch noch nicht lauffähig. Für alle Snap-Apps gemeinsam ist noch das Basissystem Ubuntu Core erforderlich, das unter „/snap/core“ eingehängt ist. Es ist entpackt etwa 270 MB groß und bietet nur eine minimale Ausstattung. Laufzeitumgebungen wie Perl oder Java muss die Snap-App selbst mitbringen. Snap-Images können daher relativ groß werden. Es ist deutlich mehr Platz auf der Festplatte erforderlich als bei DEB-Paketen, der Hauptspeicherbedarf steigt und die Programme starten langsamer. Angesichts großer Festplatten und schneller CPUs ist das auf aktuellen PCs jedoch kaum spürbar.

Snap-Apps installieren und verwalten

Snap-Apps lassen sich wie herkömmliche Softwarepakete über das Tool Ubuntu-Software installieren. Verwenden Sie die Suchfunktion oder stöbern Sie in den Kategorien, um das gewünschte Programm zu finden. Wenn Sie beispielsweise nach dem Mediaplayer VLC suchen, taucht dieser im Ergebnis zweimal auf. Unter „Details“ se-

hen Sie jeweils, um welche Version es sich handelt. Steht hinter „Quelle“ die Angabe „Snap-Store“, handelt es sich um eine Snap-App. Hinter „Kanal“ können Sie auf „stable“ klicken. Es öffnet sich ein Fenster, in dem Sie zwischen den Kanälen umschalten können. Bei „beta“ oder „edge“ finden Sie meist höhere Versionsnummern, die Software ist aber nicht ausreichend getestet und kann noch etliche Fehler enthalten.

Klicken Sie auf „Installieren“, wenn Sie ein Programm verwenden möchten. Der Start einer Snap-App erfolgt über eine Suche nach einem Klick auf „Aktivitäten“ im Panel links oben. Das Verzeichnis „/snap/bin“ – hier liegen die Verknüpfungen zu den installierten Snaps – ist auch in der Umgebungsvariablen „PATH“ enthalten. Daher lassen sich die Programme auch von einem Terminal aus starten.

Sind unterschiedliche Versionen eines Programms installiert, beispielsweise der VLC sowohl als DEB-Paket als auch als Snap-App, dann wird es unübersichtlich. Die Suche über „Aktivitäten“ liefert für VLC zwei Ergebnisse, Beschriftung und Icon unterscheiden sich jedoch nicht. Hier hilft nur ausprobieren, welche Version sich hinter welchem Icon verbirgt.

Updates installieren: Ubuntu 18.04 prüft viermal täglich, ob Updates für Snap-Apps verfügbar sind. Die Installation erfolgt automatisch. Wer möchte, kann in einem Terminalfenster das Update manuell einleiten:

```
sudo snap refresh
```

Bei Updates oder nach einem Wechsel des Kanals werden die bisherigen Versionen nicht entfernt, sondern nur deaktiviert. Mit dem Befehl

```
snap list --all
```

lassen Sie sich alle installierten Snap-Apps inklusive Versions- und Revisionsnummern anzeigen. Um zu der vorherigen Version zurückzukehren, verwenden Sie den Parameter „revert“:

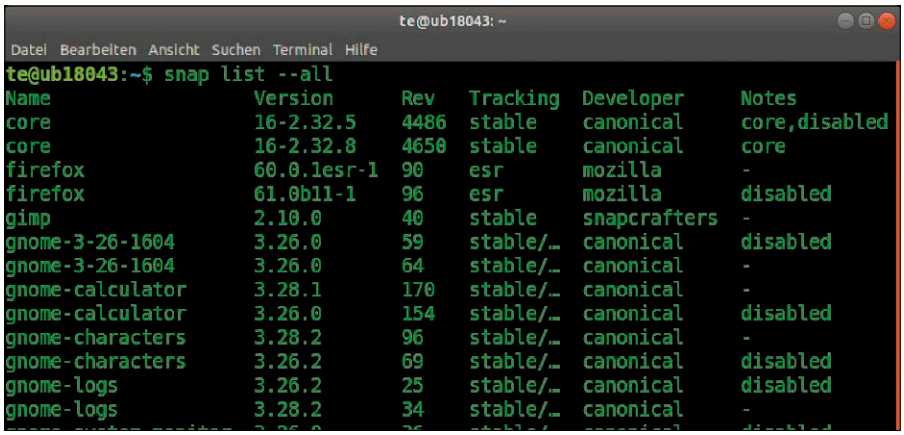
```
sudo snap revert gnome-calculator
```

Um etwa eine ältere Revision 154 von gnome-calculator (Taschenrechner) zu löschen, nutzen Sie diese Befehlszeile:

```
snap remove --revision 154 gnome-
  calculator
```

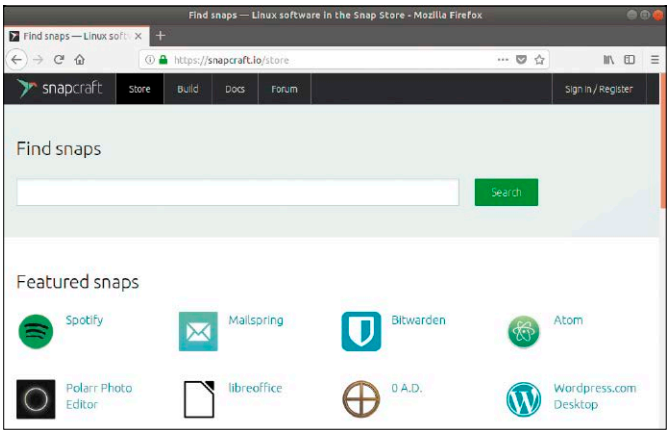
Dieser Schritt ist jedoch endgültig, weil sich ältere Versionen nicht aus dem Snap-Store installieren lassen.

Wenn Sie eine neuere Version ausprobieren möchten, wechseln Sie den Update-Kanal, für VLC beispielsweise so:



Snaps verwalten: *snap list --all* gibt Auskunft über die installierten Snaps. Nach Updates bleiben ältere Versionen erhalten, die Sie bei Gelegenheit aber entfernen können.

Im Store von *https://snapcraft.io* finden Sie neue Snap-Apps. Die Installation kann per Mausklick über Ubuntu-Software erfolgen oder über die Kommandozeile.




```
sudo snap switch --edge vlc && sudo
  snap refresh vlc
```

Zurück zur Version aus dem „stable“-Kanal geht es natürlich auch:

```
sudo snap switch --stable vlc &&
  sudo snap refresh vlc
```

Mit dem Tool snap können Sie auch Snap-Apps suchen (*snap find [Suchbegriff]*) und installieren (*snap install [snap-app]*).

Tipp: Eine direkte Anlaufstelle für Snaps ist die Webseite *https://snapcraft.io/store*. Hier suchen Sie gezielt nach Snap-Apps. Per Klick auf „Install“ und „View in Desktop-Store“ erfolgt die Installation über Ubuntu-Software. Wenn Sie auf „All Versions“ klicken, sehen Sie die passenden Kommandozeilen für die Installation aus den verfügbaren Updatekanälen. ■

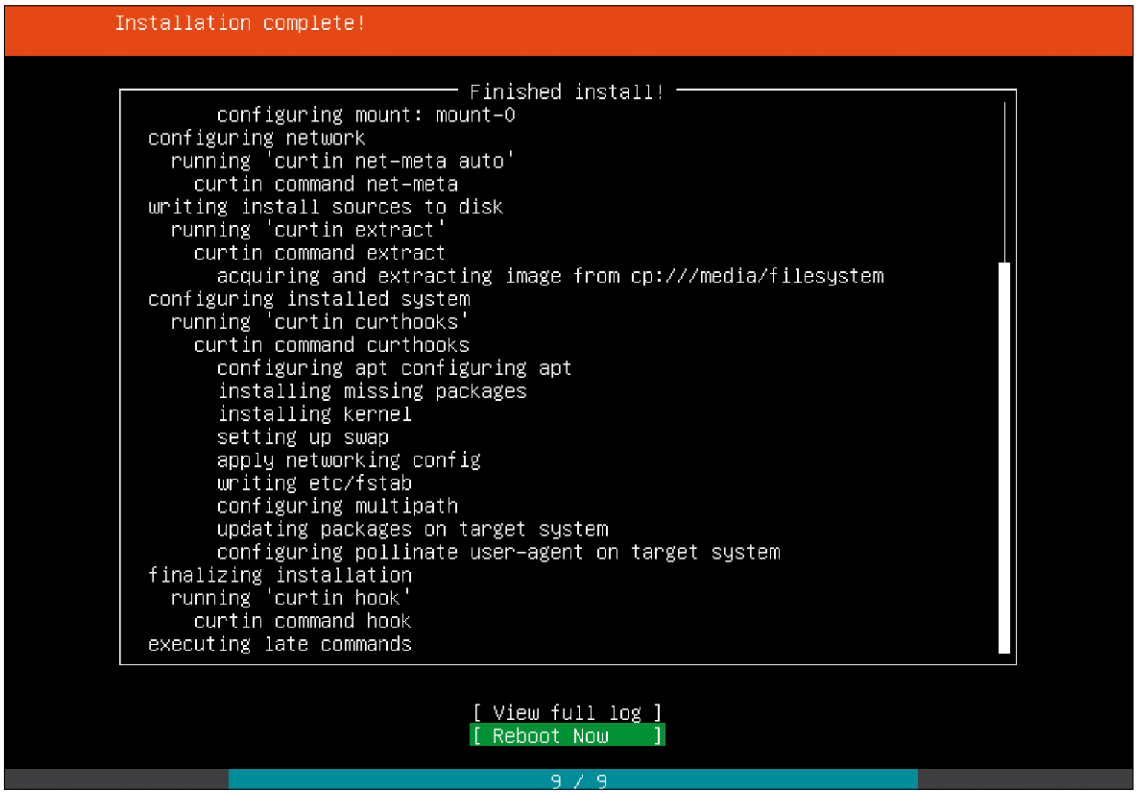
ZUGRIFFSRECHTE FÜR SNAP-APPS FESTLEGEN

Snap-Apps laufen weitestgehend in einer Sandbox. Vom installierten System nutzen sie nur wenige Dateien und der Lese- und Schreibzugriff ist nur im Home-Verzeichnis des jeweiligen Benutzers erlaubt. Es lassen sich aber weitere Berechtigungen vergeben. Sobald die Installation einer Snap-App über Ubuntu-Software abgeschlossen ist, klicken Sie auf „Berechtigungen“. Was sich einstellen lässt und was bereits aktiviert ist, hat der Entwickler vorgegeben. Aktivieren Sie beispielsweise „Lese/Schreibe auf mobilen Datenträger“, wenn die App auf USB-Geräte zugreifen soll, die unter „/media“ eingehängt sind.

Der Zugriff auf Netzwerkfreigaben ist bisher nicht möglich. Im „Öffnen“-Dialog beispielsweise tauchen nach Klick auf „Andere Orte“ keine Netzwerke auf. Sie können Dateien in Snap-Apps daher nur lokal speichern oder öffnen.

Ubuntu 18.04 Server

Das runderneuerte Setuptool von Ubuntu 18.04 Server ermöglicht eine schnelle Installation, eignet sich aber nicht für jeden. Es gibt jedoch alternative Installationsoptionen.



Ubuntu Server 18.04 installieren: Der neue Installer ermöglicht eine schnelle Ersteinrichtung, bietet aber nur wenige Funktionen und installiert Software, die viele nicht benötigen.

VON THORSTEN EGGELING

Mit Ubuntu 18.04 Server lässt sich ein stabiler Datei- oder Webserver für das eigene Netzwerk einrichten. Die Basis der Server- und Desktopvariante ist mehr oder weniger identisch.

Es gibt jedoch Unterschiede bei der Installation und bei den standardmäßig eingerichteten Paketen. Ubuntu Server ist ein Minimalsystem ohne grafischen Desktop. Konfiguration und Wartung erfolgen in der Regel von einem anderen Netzwerkrechner aus in einem SSH-Terminal. Für die Installation sollten jedoch Monitor und Tastatur angeschlossen sein. Bei Bedarf können Sie auch eine Desktopumgebung nachinstallieren.

Vorbereitungen für die Serverinstallation

Für Ubuntu Server gibt es mehrere ISO-Dateien. Der Hersteller Canonical bietet unter *www.ubuntu.com/download/server* die Datei „ubuntu-18.04-live-server-amd64.iso“ zum standardmäßigen Download an. Hier ist das neue Setuptool mit dem Namen Subiquity enthalten. Das Tool ist sehr übersichtlich, eignet sich aber nur für die Installation auf einer leeren Festplatte. Es lassen sich zwar neue Partitionen in frei wählbarer Größe erstellen, die Einrichtung auf einer vorhandenen Partition oder neben einem anderen Betriebssystem ist nicht vorgesehen. Raid-Arrays, LVM (Logical Volume Manager) oder erweiterte Netzwerkeinstellungen kennt Subiquity ebenfalls nicht. Wir raten jedoch aus anderen Gründen von diesem ISO-Image ab: Bei der Installation wird standardmäßig das Paket „cloud-init“ (Ubuntu Cloud Image) eingerichtet. Damit lassen sich mehrere Server automatisch konfigurieren, was längst nicht jeder Nutzer wirklich benötigt, zumal cloud-init oft den Bootvorgang verlangsamt und die Netzwerkkonfiguration verkompliziert.

Wer nur einen Server für den Hausgebrauch einrichten will, greift besser zu einer ISO-Datei mit dem traditionellen Debian-Installer. Den Download der Datei „ubuntu-18.04-server-amd64.iso“ (ohne den Zusatz „live“) finden Sie unter *http://cdimage.ubuntu.com/releases/18.04/release*. ISO-Dateien stehen nur noch für die 64-Bit-Architektur zur Verfügung. Wer ein 32-Bit-System installieren möchte, verwendet ein Netboot-Image (auf Heft-DVD und

unter *http://cdimage.ubuntu.com/netboot/18.04*). In der Regel sollten Sie aber die 64-Bit-Version wählen. Das Setuptool mit traditionellem Installer lädt alle Pakete über das Internet herunter. Dabei ist eine kabelgebundene Netzwerkverbindung erforderlich; WLAN wird nicht unterstützt. Sie können auch aus einer der ISO-Dateien einen USB-Stick für die Installation erzeugen. Dazu verwenden Sie das Kommandozeilentool dd. Weitere Infos finden Sie auf *www.pcwelt.de/2089747*.

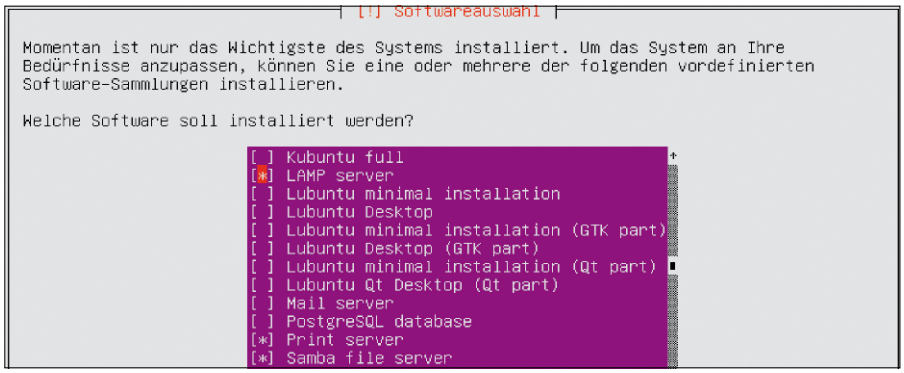
Die Installation von Ubuntu 18.04 Server

Die Serverinstallation läuft unterschiedlich ab, je nachdem, von welcher ISO-Datei Sie den PC booten.

Subiquity-Installer: Im ersten Schritt wählen Sie die gewünschte Sprache aus. Der Installer zeigt zur Zeit allerdings nur englischsprachige Meldungen. Bei Schritt 3 wählen Sie „Install Ubuntu“. Danach übernehmen Sie die DHCP-Netzwerkkonfiguration oder stellen nach Auswahl des Netzwerkadapters eine statische IPv4- und IPv6-Adresse ein. In Schritt 6 wählen Sie „Manual“, wenn Sie die Partitionierung selbst durchführen wollen. Andernfalls überlassen Sie das dem Installer mit „Use An Entire Disk“. Danach wählen Sie die gewünschte Festplatte aus und bestätigen den Partitionierungsvorschlag mit „Done“. Jetzt müssen Sie nur noch den Benutzernamen, Servernamen sowie Passwort eintragen und mit einem abschließenden „Done“ übernehmen. Ist die Installation abgeschlossen, gehen Sie auf „Reboot Now“.

Debian-Installer: Beim Start des Installationssystems vom Netboot-Image (auf Heft-DVD) oder dem alternativen ISO-Abbild sehen Sie den traditionellen Installer. Folgen Sie einfach den Anweisungen auf dem Bildschirm. Die Schritte entsprechen in etwa denen bei einer Standardinstallation von Ubuntu Desktop und sind weitestgehend selbsterklärend. Der Installer unterstützt Raid, LVM (auch verschlüsselt mit Luks) und die Parallelinstallation.

Im Fenster „Softwareauswahl“ können Sie vorbereitete Paketgruppen wählen. Es ist in jedem Fall sinnvoll, „Basic Ubuntu server“ und „OpenSSH server“ auszuwählen. Alles Weitere hängt vom Einsatzgebiet ab. Soll der PC als Dateiserver für Linux und Windows dienen (siehe *www.pcwelt.de/1903700*), wählen Sie „Samba file server“. Sind Webanwendungen geplant, aktivieren Sie den „LAMP server“ (Linux, Apache, My SQL, PHP, siehe *www.pcwelt.de/1607540*). Wenn Sie einen Desktop bevorzugen, wählen Sie den gewünschten aus – beispielsweise „Xubuntu desktop“ (XFCE).



Serverdienste: Der Debian-Installer bietet Ihnen eine Softwareauswahl an. Aktivieren Sie beispielsweise „LAMP server“ für einen Webserver oder „Samba file server“ für einen Dateiserver.

Erste Schritte nach der Installation

Nach dem Start des Ubuntu-Servers sehen Sie die Textkonsole, bei der Sie sich mit Benutzernamen und Passwort anmelden. Wenn Sie den Subiquity-Installer verwendet haben, hatten Sie keine Möglichkeiten zur Softwareauswahl. Verwenden Sie das Tool apt, um die gewünschten Pakete einzurichten. Die Basiseinrichtung gelingt jedoch einfacher mit tasksel. Installieren und starten Sie das Tool mit diesen drei Zeilen:

```
sudo apt update
sudo apt install tasksel
sudo tasksel
```

Die Softwareauswahl erfolgt – je nach Verwendungszweck – wie oben beim Debian-Installer beschrieben.

Das Netzwerk konfigurieren

Ubuntu 18.04 verwendet jetzt Netplan zur Konfiguration der Netzwerkschnittstellen. Bei der Installation über den Debian-Installer wird „/etc/netplan/01-netcfg.yaml“ erstellt, beim Subiquity-Installer „/etc/netplan/50-cloud-init.yaml“. Wenn Sie beispielsweise eine statische IP-Adresse verwenden möchten, tragen Sie die Zeilen ein, wie in der Abbildung dargestellt. Wichtig: Erstellen Sie die Einrückungen mit Leerzeichen und passen Sie die IP-Adresse für Ihr Netzwerk an. Im oberen Bereich sehen Sie die auskommentierten Einstellungen für DHCP. Wenden Sie die Änderungen mit

```
sudo netplan --debug apply
```

an. Sollten dabei Fehler auftreten, zeigt das Tool diese an. ■

LIVEPATCH-DIENST BESEITIGT KERNEL-SICHERHEITSLÜCKEN

Ein Server soll im optimalen Fall ohne Unterbrechungen laufen. Linux integriert normale Softwareupdates, ohne dafür neu starten zu müssen. Ausnahmen sind Änderungen am Linux-Kernel: Spätestens nach einem Kernel-Update wird ein Neustart unerlässlich. Um auch solche Unterbrechungen zu reduzieren, bietet Canonical neuerdings einen Livepatch-Dienst an. Damit lassen sich kritische Sicherheitslücken temporär im laufenden Kernel und ohne Neustart beseitigen. Der Neustart kann folglich verschoben werden bis zu einem günstigen Zeitpunkt. Wer diese Funktion nutzen möchte, muss sich über *https://auth.livepatch.canonical.com* einen „Live Patch Token“ besorgen. Dafür ist eine Registrierung erforderlich. Der Dienst ist für bis zu drei Rechner kostenlos. Anschließend führen Sie diese Befehle aus:

```
sudo snap install canonical-livepatch
sudo canonical-livepatch enable [Token]
```

Den Platzhalter „[Token]“ ersetzen Sie durch den Schlüssel, den Sie von Canonical erhalten haben.

Strategien für Passwörter

Alles über Passwörter! Dieser Artikel ist der Auftakt zum Heftschwerpunkt rund um System- und Onlinepasswörter, Passwortverwaltung und Zertifikate. Hier geht es zunächst um einfache Einschätzungen, welche Kennwörter besonders sensibel sind.

VON HERMANN APFELBÖCK

Foto: © adiruch na chiangmai - Fotolia.com

Viele Nutzer von PCs und Mobilgeräten sind sich nicht bewusst, wie viele und welche Zugangsdaten sie im Alltag verwenden. Ein Log-in samt Passwort ist schnell vergeben und schnell wieder vergessen: Betriebssystem, Browser, Mail- oder FTP-Programm speichern Log-in-Namen und Passwörter und tragen sie automatisch ein, sobald ein bestimmtes Ziel angefordert wird. Wer sich ganz auf die Software verlässt, hat aber theoretisch mehrere Probleme: Die Kontrolle über die Qualität der Passwörter geht verloren. Wenn die Software fehlt, sind Sie ausgesperrt. Und nicht zuletzt: Ist der Ort der Passwortsammlung im Browser, FTP-, Mailclient wirklich sicher (insbesondere auf mobilen Rechnern)?

Welche Passwörter wofür?

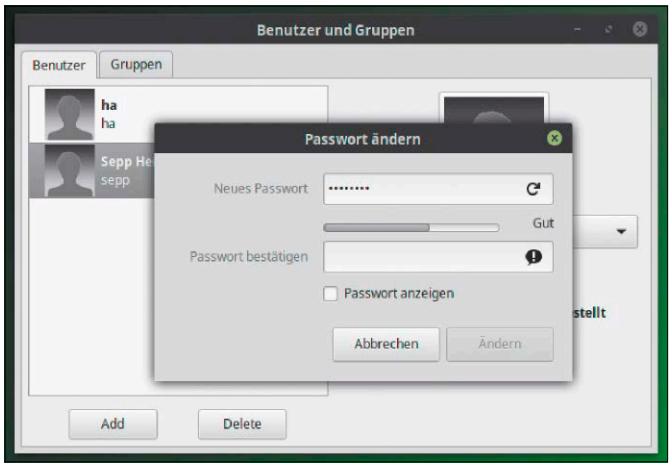
Im Heimnetz sind System-Log-ins, Netzfreigaben, Verwaltungsoberflächen (Router, Access Points, Apache-Dienste) nicht sonderlich sicherheitskritisch. Hier ist es vertretbar, sich die Log-ins für mehrere Zugänge mit einem gemeinsamen Kennwort zu vereinfachen, das noch nicht mal hohe Komplexitätsansprüche erfüllen muss. Eine wichtige Ausnahme ist nur das WLAN-Passwort, das den Zutritt Fremder ins Heimnetz verhindern muss: Dieses muss und darf komplex ausfallen, zumal es auf jedem Clientgerät nur einmal eingegeben werden muss.

Einfache Passwörter sind aber nur zulässig, solange Daten und Geräte das Haus nicht verlassen: Jede Öffnung nach außen via Portfreigabe im Router erfordert für dieses Gerät sichere Passwörter und jedes Notebook, das das Haus verlässt, verdient einen gut abgesicherten Systemzugang und Verschlüsselungsmaßnahmen.

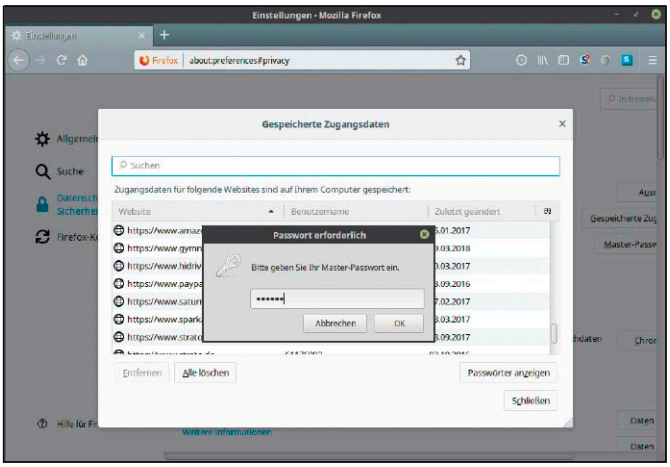
Onlinekennwörter sind ebenfalls nicht über einen Kamm zu scheren: Der Zugang zu einer Vereinshomepage ist unkritisch. Hier kann man auch ein Standardpasswort für verschiedene Zugänge nutzen. Sensibel ist hingegen das Mailkonto: Ein gehacktes Mailkonto legt nicht nur die private Korrespondenz offen (bei IMAP unter Umständen die Korrespondenz über Jahre), sondern ermöglicht zudem den Zugriff auf weitere Online-Log-ins: Denn bei den meisten Diensten genügt die Mailadresse, um sich („Kennwort vergessen?“) einfach ein neues Passwort zu beschaffen, das dann an das gehackte Mailkonto geschickt wird. Ebenfalls sensibel sind Bank-, Paypal- und Onlineshop-Log-ins, wo die Kreditkartendaten hinterlegt sind. Letztere sind die fast heikelsten Kandidaten, denn für Transaktionen beim Onlinebanking ist in der Regel eine zusätzliche TAN nötig und bei Paypal lässt sich ebenfalls eine Zwei-Wege-Authentifizierung einrichten.

Voreingestellte Standardpasswörter

Viele Spezialsysteme für Platinenrechner, Router, Access Point, NAS-Speicher werden zunächst mit Standardpasswörtern ausgeliefert. Das heißt, dass der Zugang zur Konfigurationsoberfläche bei diesen Geräten und damit deren Verwaltung mehr oder weniger jedermann offensteht. Das ist im Privathaushalt kein ernstes Problem, solange solche Geräte nicht für das Internet geöffnet werden (etwa Internetzugriff in der



Viele Passwörter verlangen eine Mindestlänge oder das eine oder andere Sonderzeichen. Wichtig ist Komplexität bei Banking, Mail, Portfreigaben und Händlerdatenbanken mit Kreditkartendaten.



Mobile Notebooks mit Firefox-Masterpasswort: Das ist eine Mindestmaßnahme, um die Browserpasswörter zu schützen. Im Optimalfall ist das ganze System Luks-verschlüsselt.

Fritzbox, Portfreigabe für NAS-Gerät). Trotzdem ist es überall zu empfehlen, in Firmen sowieso, typische Standards wie „pi“ und „raspberry“, „admin“ und „admin“ (auch „0000“, „1234“ oder ganz leer) durch eigene Passwörter zu ersetzen.

Wo sind die Kennwörter gespeichert?

Die Komplexität von Passwörtern spielt – scheinbar – keine Rolle, weil sich die Software die Kennwörter merkt: So landen etwa die Zugangsdaten für lokale Netzfreigaben im gnome-keyring, in Filezilla ist ein FTP-Serverzugang nur einmal samt Kennwort einzutragen, Browser wie Firefox oder Chrome speichern auf Nachfrage die Login-Daten von Onlinediensten.

Sich auf die Software zu verlassen, hat aber Nachteile und erhöht die Komplexität: Wer nur einen PC oder ein Notebook nutzt, fährt damit bequem. Bei mehreren Geräten muss man dafür sorgen, dass dieselbe Software überall bereitsteht und die Passwörter kennt. Richtig bequem ist das nur beim Browser, sofern Sie sich bei Firefox Sync oder Chrome Sync anmelden und die Passwörter synchronisieren. Dabei übermittelt der Browser die Passwörter an Mozilla oder Google. Dies geschieht verschlüsselt, schafft aber Abhängigkeit vom jeweiligen Browser.

Wer mobile Notebooks nutzt, sollte wissen, dass sich alle Passwörter unter „Einstellungen → Sicherheit → Gespeicherte Zugangsdaten“ (Firefox) oder „Einstellungen → Erweiterte Einstellungen → Passwörter verwalten“ (Chrome/Chromium) auslesen lassen. Chrome fordert dabei unter Windows das Windows-Kennwort, unter Linux stehen die Kennwörter hingegen offen. Auch Filezilla-Daten oder die Mailkennwörter unter Thunderbird lassen sich auslesen. Firefox und Thunderbird sind aber gut zu schützen, indem man das zusätzliche Masterpasswort einrichtet.

Schlüsseldateien und Security Tokens

Anstatt Passwörter einzugeben, können Zugangsberechtigungen auch in Schlüsseldateien abgelegt werden. Das ist sehr verbreitet bei der SSH-Fernwartung von Linux-Servern, wobei auf dem zugreifenden Client mit dem Tool ssh-keygen ein Schlüssel erstellt wird und der öffentliche Teil desselben dann zum Server kopiert wird. Im Prinzip ist diese Art der Legitimierung einfacher (keine Eingabe) und sicherer (abhörsicher und komplex). Bei physischem Fremdzugriff auf den Client kehrt sich der Sicherheitsvorteil aber ins Gegenteil.

Ein weiteres Beispiel, das optional Schlüsseldateien vorsieht, ist die Verschlüsselungssoftware Veracrypt, auf welche der Artikel ab Seite 68 genauer eingeht. Dort ist die Schlüsseldatei jedoch ein zweiter Nachweis neben dem Passwort, also ein zusätzlicher Schutz gemäß der Zwei-Wege-Authentifizierung (dazu mehr ab Seite 58). Schlüsseldateien erhöhen in jedem Fall die Komplexität: Dass man nach einem Zugangskennwort gefragt wird, ist jederzeit nachvollziehbar. Dass man sich hingegen aktuell nicht anmelden kann, weil man am falschen Rechner sitzt oder weil eine Schlüsseldatei verloren ging, kann Kopfzerbrechen über die Ursache auslösen.

Gute Kennwörter

Wer die unterschiedlichen Sensibilitätsstufen berücksichtigen will, kann sich Passwortstrategien nach folgendem Muster zurechtlegen: Ein einfaches Standardpasswort dient für die meisten lokalen Anmeldungen im Heimnetz. Ein anderes einfaches Kennwort nutzen Sie für unkritische Onlineanmeldungen (Forum, Schule, Verein, Stadtwerke). Für kritische Zugänge verwenden Sie komplexe Passwörter. Um es sich einfacher zu machen, kann ein variiertes Masterkennwort herhalten. Das könnte so aussehen: wien+bonn-kiel=ltrn – wobei „wien+bonn-kiel=“ das Masterkennwort wäre und „ltrn“ jeweils den 2., 4., 6. und 8. Buchstaben der Anmelde-URL von elster-online.de übernimmt (als Beispiel). Ein solches Schema ist bei jeder Anmelde-URL jederzeit ohne Softwarehilfe rekonstruierbar. Zweifellos ist es aber noch sicherer, für jedes kritische Konto ein unabhängiges, komplexes Kennwort zu nutzen.

Komplexe Kennwörter sind aber kein Allheilmittel: Immer wieder werden die Datenbanken von Händlern und Webdiensten inklusive aller Zugangsdaten gehackt. Dann ist das Passwort in fremden Händen – sei es schwach oder stark.

Daher ist es so wichtig, für eine halb private Vereinsseite oder einen kleinen Onlineshop, die keine anspruchsvolle Sicherheitsadministration erwarten lassen, ein anderes Kennwort zu verwenden als beim Google- oder Mailkonto. ■

Sichere Zertifikate

Die besten Passwörter nützen wenig, wenn diese im Klartext übertragen werden. Es ist ein großes Tabu, im Internet mit unverschlüsselten Log-in-Daten zu arbeiten. SSL-Zertifikate schützen die Übertragung zum eigenen Webserver.

VON DAVID WOLSKI

Für Administratoren von Webservern gehört die Einrichtung von SSL-Zertifikaten seit jeher zu den Routineaufgaben. Inzwischen sind Zertifikate für die Verschlüsselung des Traffics von und zu Webservern auch für die Betreiber kleiner Server im Web wichtig. Viele Anwender scheuten den Aufwand eines Zertifizierungsprozess für die eigene Domain und wichen deshalb aus Prinzip auf selbst generierte Zertifikate ohne CA aus. Diese werden vom Browser zwar erst nach einer manuell gesetzten Ausnahmeregelung akzeptiert, verschlüsseln den Verkehr zur eigenen Site aber ebenso wirkungsvoll. Selbst signierte Zertifikate haben deshalb in Sonderfällen auch keineswegs ausgedient, wie der Beitrag zeigt.

Let's Encrypt für alle

Für öffentliche Server im Web mit einer regulär registrierten Domain gibt es mittlerweile einen besseren Weg, Zertifikate zu bekommen: Seit Dezember 2015 bietet die Initiative „Let's Encrypt" (getragen unter anderem von Mozilla, Akamai und Cisco) kostenlose Zertifikate an, die sich vergleichsweise einfach beantragen und installieren lassen. Auch waren die Zertifikate von Let's Encrypt dank breiter Unterstützung durch IT-Riesen schnell von allen wichtigen Browsern anerkannt. Let's Encrypt arbeitet mit Domainvalidierung und prüft damit nur, ob der Antragsteller auch der Domaininhaber ist. Die restlichen Informationen zu einer Person oder einem Unternehmen werden nicht verifiziert. Dafür ist der Vorgang weitgehend per Scripts automatisiert und die Installation eines allseits anerkannten SSL-Zertifikats dieser CA dauert nur ein paar Minuten.

Let's Encrypt ist immer noch ein junger Dienst und die Scripts zur Einrichtung eines Zertifikats unterliegen immer wieder Änderungen. Zahlreiche Anleitungen aus der Anfangsphase des Dienstes sind deshalb nicht mehr gültig oder funktionieren nur für sehr allgemeine Serverkonfigurationen. Besser ist es, mit einer universellen Methode zu arbeiten, die nicht an einen bestimmten Webserver gebunden ist. Zunächst braucht man dazu die aktuelle Version des Certbot, eine Sammlung an Python-Scripts von Let's Encrypt. Dazu muss zuerst das Paket Git installiert werden, etwa mit

```
sudo apt-get install git
```

unter Debian/Ubuntu. Anschließend holt das Kommando

```
git clone https://github.com/
  letsencrypt/letsencrypt
```

die Certbot-Scripts in das neue Unterverzeichnis „letsencrypt". Nach einem Wechsel in diesen Ordner beenden Sie den Webserver temporär (im Beispiel: Apache auf einem Debian/Ubuntu-System):

```
systemctl stop apache2
```

Der Certbot soll nun selbst vorübergehend als Webserver auftreten und das Zertifikat mit Let's Encrypt aushandeln. Dazu starten Sie das Script mit dem Aufruf

```
sudo certbot certonly --standalone
  --preferred-challenges http -d
  meineseite.de
```

wobei „meineseite.de" der Platzhalter für den tatsächlichen Domainnamen ist. Der Certbot fragt einige Daten wie die Mailadresse ab und legt dann das ausgestellte Zertifikat im Pfad „/etc/letsencrypt/live/example.com" ab. Es umfasst die Dateien „cert.pem", „chain.pem", „fullchain.pem" und „privkey.pem". Wer noch nie Apache für SSL konfiguriert hat, findet unter Debian/Ubuntu eine Beispielkonfiguration in der Datei „/etc/apache2/sites-available/default-ssl" und eine Anleitung unter *https://linux-scout.de/webserver/apache2-ssl-zertifikat-installieren*.

privkey.pem: Der private Schlüssel des Webservers darf nie abhandenkommen. In einer Apache-Konfiguration wird diese Datei mit vollem Pfad hinter „SSLCertificateFile“ angegeben.

cert.pem: Dies ist die eigentliche Zertifikatsdatei. Sie muss in Apache hinter „SSLCertificateFile“ referenziert werden.

chain.pem: In dieser Datei ist die Vertrauenskette angegeben, damit ein Client das Zertifikat zurück zur CA verfolgen kann. Sie muss in Apache hinter „SSLCertificateChainFile“ angegeben sein.

Nach getaner Arbeit startet

```
systemctl start apache2
```

wieder den Webserver. Die Zertifikate von Let's Encrypt sind 90 Tage gültig, deshalb sollte man mit dem Befehl

```
sudo crontab -e
```

gleich einen wiederkehrenden Cronjob auf dem Linux-System einrichten. Der Cronjob

```
00 7 * * * systemctl stop apache2;
 letsencrypt renew; systemctl start
 apache2
```

überprüft beispielsweise jeden Tag um 7 Uhr morgens, ob ein neues Zertifikat fällig ist, und übernimmt dazu auch den Neustart des Webservers.

Selbst signierte Zertifikate

SSL-Zertifikate von einer CA wie Let's Encrypt bekommt man nur für Server und Domains, die einem selbst gehören. Dynamische Domainnamen von Diensten wie No-IP (*https://www.noip.com*) oder Free DNS (*http://freedns.afraid.org*) gehören einem aber nicht und ein selbst signiertes Zertifikat ist hier die einzige Möglichkeit, mit SSL zu arbeiten. Auf einem Linux-System erstellt der Befehl

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

das selbst signierte Zertifikat und dessen Dateien, wobei noch das angezeigte Frageformular mit beliebigen Angaben ausgefüllt werden darf.

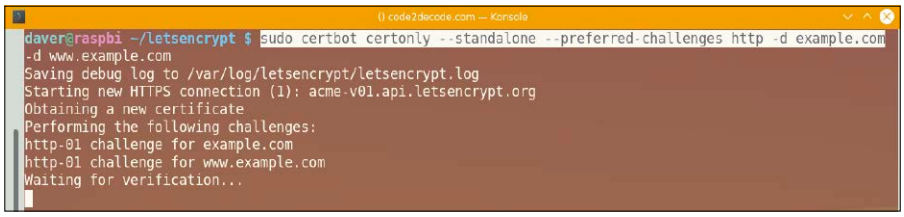
Die wichtigen Angaben in der Apache-Konfiguration sind nun

```
SSLCertificateFile /etc/apache2/
 ssl/apache.crt
```

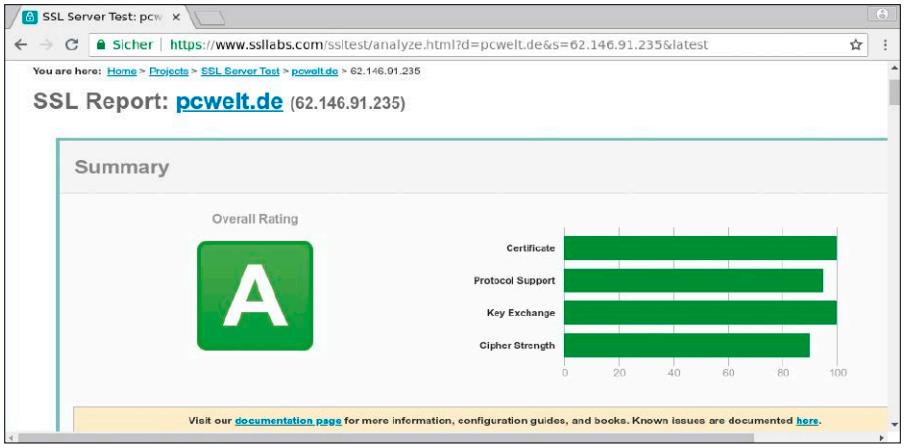
für das selbst signierte Zertifikat sowie

```
SSLCertificateKeyFile /etc/
 apache2/ssl/apache.key
```

für den privaten Schlüssel. Eine Zertifikatskette gibt es nicht, weil keine CA existiert.



Certbot in Aktion: Es ist zuverlässiger, den Webserver temporär abzuschalten und den Scripts von Let's Encrypt die Aushandlung des SSL-Zertifikats zu überlassen.



Zertifikat und Ciphers mit Ssllabs überprüfen: Die Site spürt Probleme bei SSL-Zertifikaten und Konfigurationsmängel auf. Die Ergebnisse werden genau aufgeschlüsselt.

Beim ersten Aufruf dieser Site zeigt der Browser einen Warnhinweis zu einem ungültigen Zertifikat an. In den üblichen Browsern muss man dann eine Ausnahme für das eigene Zertifikat einmalig für den genutzten Domainnamen festlegen.

Cipher: Verschlüsselung sicher machen

Ein gültiges SSL-Zertifikat allein ist noch keine Garantie, dass die Verbindung sicher ist. SSL/TLS ist ein fortschreitender Standard, der schon aus Kompatibilitätsgründen eine Menge Verschlüsselungsalgorithmen unterstützt, genannt Cipher. Ein Onlinecheck, welche Ciphers auf einem Webserver funktionieren, zeigt die Site *https://www.ssllabs.com/ssltest*. In der Auswertung vergibt die Site auch Noten von A+ (hervorragend) bis F (mangelhaft) für die SSL-Konfiguration eines Webservers. Ein Check der eigenen Site nach der ersten Installation eines SSL-Zertifikats ist eigentlich Pflicht. Mittlerweile gibt es nach dem verbreiteten Standard TLS 1.1 und 1.2 erschreckend wenige wirklich sichere Cipher-Kombinationen. Aktuell bewährt sich in der Apache-Konfiguration die Angabe

```
SSLCipherSuite ECDH+AESGCM:DH+AESG
 CM:ECDH+AES256:DH+AES256:ECDH+AE
 S128:DH+AES:!aNULL:!MD5:!DSS
```

sehr gut. ■

BESSER ALS PASSWÖRTER: LOG-INS PER ZERTIFIKAT

Wo hohe Sicherheit gefragt ist und die Anmeldung per Benutzername und Passwort nicht ausreicht, kommen Clientzertifikate zum Einsatz. Zusätzliche Zertifikate bedeuten mehr Sicherheit, da sich jemand auch mit einem gestohlenen Passwort noch nicht an einem Dienst anmelden kann. Üblicherweise liegen Clientzertifikate im Format „PKCS#12“ und der Endung PFX vor. Unter anderem arbeitet die Steuersoftware Elster mit dieser Art von Zertifikaten, desgleichen auch Clientanmeldungen an Webgateways. Es empfiehlt sich, von wichtigen PFX-Dateien eine Sicherheitskopie zu verwahren.

Systempasswörter & Systemverwaltung

Linux ist ein Mehrbenutzersystem. Jeder Benutzer besitzt ein eigenes Konto, bei dem er sich mit Namen und Passwort anmeldet. Das Passwort des Systemverwalters ist außerdem für administrative Aufgaben nötig.

VON THORSTEN EGGELING

Standardmäßig erstellen Sie bei der Ubuntu-Installation ein Benutzerkonto, das administrative Rechte besitzt. Dieses Systemverwalterkonto kann höhere Rechte anfordern, etwa für Updates, Software-Neuinstallationen oder um weitere Benutzerkonten zu erstellen. Es gibt zwar auch bei Ubuntu ein Administratorkonto für den Benutzer „root“, bei dem melden Sie sich aber nicht direkt an und es besitzt auch kein Passwort.

Bei Ubuntu genügt das Systemverwalterpasswort für administrative Aufgaben, das Sie auch für die Anmeldung beim System verwenden. Anwendungen und Einstellungen fordern Sie zur Passworteingabe auf, wenn es erforderlich ist. Sie können Programme aber auch manuell mit höheren Rechten starten, etwa um Konfigurationsdateien des Systems zu ändern.

Regeln für Systempasswörter

Für das bei der Installation vergebene Benutzerpasswort gelten keine besonderen Regeln. Das Setuptool weist Sie zwar auf ein zu kurzes Passwort hin, Sie können es nach einer Bestätigung aber trotzdem verwenden. Sobald Sie ein neues Benutzerkonto über „Informationen → Benutzer“ (Ubuntu 18.04) erstellen, gelten aber strengere Regeln. Das Passwort muss mindestens acht Zeichen lang sein und darf nicht aus einfachen Sequenzen wie „12345678“ bestehen.

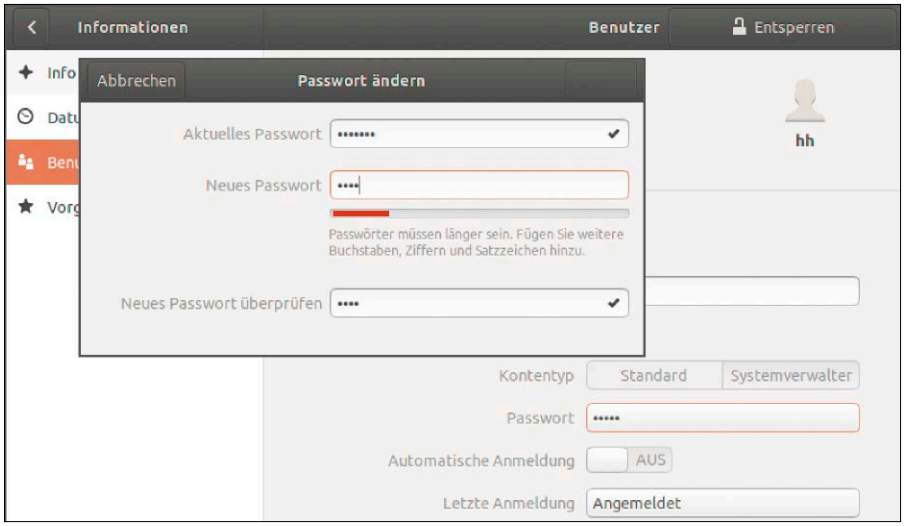
Mehr Sicherheit durch Passwörter? Wer den PC nur privat zu Hause nutzt, benötigt in der Regel keine besondere Passwortsicherheit. Passwörter bieten ohnehin kaum Schutz, wenn Angreifer Zugang zum Rechner erhalten können. Über das Ubuntu-Recoverysystem oder eine Live-DVD lassen sich Daten ganz einfach kopieren, was sich nur durch Verschlüsselung vermeiden lässt (siehe Luks ab Seite 48 und Veracrypt ab Seite 68). Außerdem lässt sich über ein Zweitsystem das Passwort löschen, was dem Nutzer im Notfall aber auch selbst helfen kann (siehe *www.pcwelt.de/2010638*).

Wenn Sie für mehr Komfort einfachere Passwörter verwenden wollen, aktivieren Sie die Option „Bei der nächsten Anmeldung Passwort wählen“, wenn Sie ein neues Benutzerkonto erstellen. Im Terminalfenster setzen Sie das Passwort mit

```
sudo passwd [Konto]
```

Den Platzhalter „[Konto]“ ersetzen Sie durch den Benutzernamen (mehr zu „sudo“ im nächsten Abschnitt). Geben Sie das Passwort des Systemverwalterkontos ein und danach das Passwort sowie die Passwortbestätigung für den neuen Benutzer, was Sie jeweils mit der Eingabetaste bestätigen. Dabei erscheinen keine Zeichen auf dem Bildschirm. Sie geben den Text also blind ein. Besondere Regeln für das Passwort gibt es nicht, es muss nur aus mindestens einem Zeichen bestehen. Auf dem gleichen Weg können Sie auch die Passwörter bereits vorhandener Benutzerkonten vereinfachen.

Durch Aufruf von *passwd* ohne sudo und ohne weiteren Parameter kann jeder Benutzer sein eigenes Passwort ändern. Er gibt zuerst das bisherige Passwort ein und dann das neue (zweimal). Das Passwort muss mindestens sechs Zeichen lang sowie nicht zu einfach sein und dem vorherigen nicht zu ähnlich.

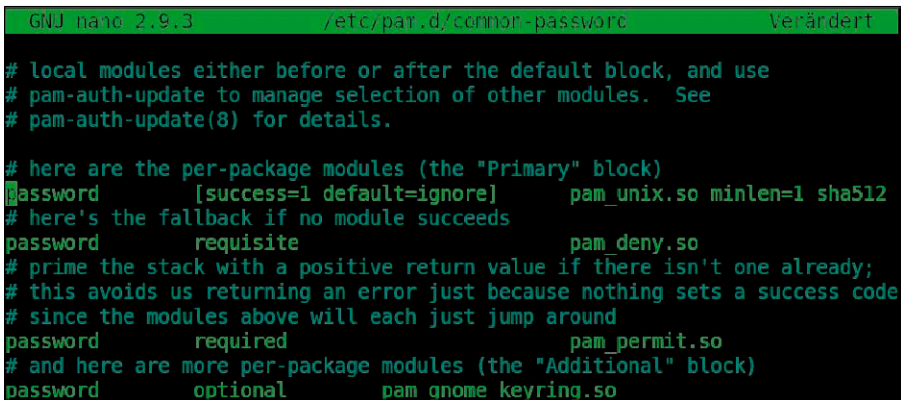


Minimallänge: Passwörter, die Sie über „Informationen → Benutzer“ ändern oder neu erstellen, müssen bestimmten Ansprüchen genügen. Minimal sind acht Zeichen erforderlich.

Regeln ändern: Wie ein Benutzerpasswort aussehen muss, ist in der Datei „/etc/pam.d/common-password“ festgelegt. Entfernen Sie in der Zeile, die „pam_unix.so“ enthält, den Wert „obscure“ und setzen Sie stattdessen

```
minlen=1
```

ein. Damit deaktivieren Sie den Komplexitätstest und erlauben Passwörter mit nur einem Zeichen. Bitte beachten Sie, dass diese Regeln nur im Terminal für passwd gelten, nicht aber für „Informationen → Benutzer“ in den grafischen Einstellungen.



Passwortregeln: Wenn Sicherheit keine Rolle spielt, legen Sie in der Datei „/etc/pam.d/common-password“ die Minimallänge auf „1“ fest. Der Wert gilt aber nur für das Tool passwd.

Programme mit root-Rechten starten

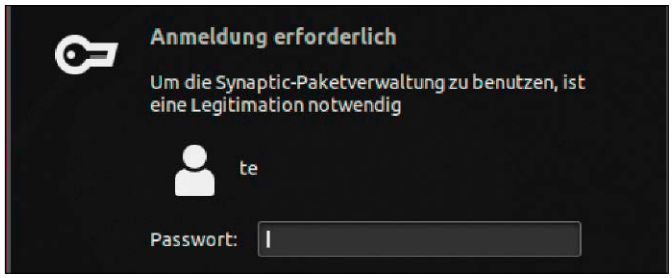
Systemverwalter gehören bei Ubuntu mindestens zur Gruppe „sudo“, wovon Sie sich über den Befehl *groups* in einem Terminalfenster überzeugen können. In der Datei „/etc/sudoers“ ist festgelegt, dass Mitglieder der Gruppe „sudo“ beliebige Programme mit erhöhten Rechten ausführen dürfen. In einem Terminalfenster geht das beispielsweise mit

```
sudo -i
```

Tippen Sie Ihr Passwort ein, um eine Anmeldeshell als Benutzer „root“ zu öffnen. Alle Befehle, die Sie dann in dieser Shell absetzen, führt das System mit administrativen Rechten aus. Sie besitzen daher Lese- und Schreibrechte für alle Dateien und Ordner. Wenn Sie ein bestimmtes Programm als root starten möchten, verwenden Sie beispielsweise

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

Damit öffnen Sie den Editor nano und die Datei „/etc/fstab“ zum Bearbeiten mit root-Rechten.



Mehr Rechte: Wenn root-Rechte für Programme oder Einstellungen nötig sind, bestätigen Sie das mit dem Kennwort des Systemverwalters.

Programme mit grafischer Oberfläche starten

Ubuntu 18.04 verwendet das Tool pkexec, um Programme mit grafischer Oberfläche mit erhöhten Rechten zu starten. Bisher kamen dafür Tools wie gksudo oder kdesudo zum Einsatz. Ähnlich wie sudo sorgen sie für die Passwortabfrage und führen ein Desktopprogramm mit maximalen Rechten aus. Mit pkexec ist eine genauere Rechtevergabe möglich, die Konfiguration ist jedoch aufwendig. Die meisten Programme benötigen pkexec jedoch nicht. Aktuelle Software startet fast immer im Kontext des Benutzers. Das Systemverwalter-Passwort geben Sie erst beim Aufruf von Funktionen ein, die das erfordern.

Bei Bedarf lassen sich unter Ubuntu 16.04 oder 18.04 auch Programme für die grafische Oberfläche per sudo von einem Terminalfenster aus starten.

Für den Dateimanager beispielsweise verwenden Sie

```
sudo -H nautilus
```

Über den Dateimanager können Sie dann Systemdateien in einem Editor öffnen und ändern.

Hinweis: Bei Systemen mit Wayland-Anzeigeserver (optional bei Ubuntu 18.04) funktioniert die sudo-Methode aus Sicherheitsgründen nicht.

Tipp: Installieren Sie das Paket „nautilus-admin“ und starten Sie Linux neu. Im Dateimanager Nautilus finden Sie jetzt im Kontextmenü von Ordnern „Als Administrator öffnen“ und bei Textdateien „Als Administrator bearbeiten“. ■

WINDOWS-UAC UND SUDO IM VERGLEICH

Die Benutzerkontensteuerung (UAC, User Account Control) erfüllt unter Windows ähnliche Aufgaben wie sudo/pkexec unter Linux. Allerdings genügt für höhere Rechte ein Klick auf „Ja“, etwa bei der Installation neuer Software. Ein Passwort müssen Sie nicht eingeben, wenn Sie mit einem Administratorkonto arbeiten. Nur Standardbenutzer benötigen das Passwort eines Admin-Kontos, was dem Verhalten von pkexec unter Linux entspricht.

Eine Eingabeaufforderung oder Powershell starten Sie mit administrativen Rechten bei Windows 8.1 oder 10 am schnellsten über das Win-X-Menü. Auf der Kommandozeile lassen sich auch Programme für die grafische Oberfläche starten, beispielsweise der Editor Notepad, wenn Sie Systemdateien bearbeiten möchten. Alternativ können Sie in einer Powershell, die Sie nicht als Administrator gestartet haben, diese Befehlszeile ausführen:

```
Start-Process Notepad -Verb RunAs
```

Bestätigen Sie die Abfrage der Benutzerkontensteuerung mit „Ja“. Standardbenutzer müssen das Passwort eines Admin-Kontos eintippen. Bei sudo wird Standardkonten dagegen generell der Zugang verweigert.

Luks-verschlüsselte Laufwerke

Vertrauliche Daten auf externen Medien und Notebooks verlangen nach besonderen Schutz, da sie leicht abhandenkommen. Luks ist eine Methode, ganze Partitionen sicher zu verschlüsseln, verlangt aber nach einer Notfallstrategie.

VON DAVID WOLSKI

Wenn Laufwerke oder ganze Arbeitsrechner verloren gehen, ist der Hardwareverlust ärgerlich bis teuer. Noch schwerer wiegt der Verlust von Geschäftsunterlagen, Log-ins und persönlichen Daten. Eine umfassende Verschlüsselung für komplette Datenträger und ganze Linux-Systeme bietet das „Linux Unified Key Setup", kurz Luks. Damit ein verschlüsseltes Linux-System nicht zum Datengrab wird, wenn das System einmal nicht mehr bootet, sollte man im Notfall eine Strategie haben, mit einem Livesystem die verschlüsselten Partitionen zu öffnen. Ist das Passwort bekannt, gibt es immer Möglichkeiten, Luks-Partitionen zu öffnen.

Die Komplettverschlüsselung

Viele Programme speichern temporäre Daten in den Ordnern „/tmp" und „/var/tmp" und bei RAM-Knappheit auch im Auslagerungsbereich (Swap). Ist also nur das Home-Verzeichnis oder ein externer Datenträger verschlüsselt, dann können geöffnete Dateien in unverschlüsselter Form an anderer Stelle landen. Gegen diese Datenschutzlecks hilft die Einrichtung eines Linux-Systems mit kompletter Verschlüsselung per Luks. Auf dem so geschützten Linux-Rechner liegt nur noch die zum Start notwendige Partition „/boot (/dev/sda1)" mit dem Bootloader Grub 2, initialer Ramdisk und dem Kernel im Klartext auf der Festplatte. Zum Systemstart kümmern sich die Cryptsetup-Scripts auf der Ramdisk um die Abfrage des festgelegten Passworts. Erst dann können die verschlüsselten Partitionen gemountet werden. Gut geeignet ist diese Methode für Notebooks, bei denen immer ein höheres Risiko besteht, dass das Gerät samt Daten abhandenkommen. Aktuelle Linux-Distributionen geben Luks den Vorzug vor anderen, containerbasierten Verschlüsselungsmethoden. Sie machen die komplette Systemverschlüsselung über Optionen im Installer auch recht einfach.

Ubuntu: Im Installer gibt es im Schritt „Installationsart" die Option „Die neue Ubuntu-Installation zur Sicherheit verschlüsseln". Dabei wird automatisch der Punkt „LVM" für den „Logical Volume Manager" aktiviert, der Luks bei einer Vollverschlüsselung als Unterbau dient.

Linux Mint: Den Installer hat Linux Mint von Ubuntu übernommen und die Verschlüsselungsoption mittels LVM ist deshalb auch dort in identischer Form vorhanden.

Manjaro: Im Installationsprogramm Calamares gibt es eine Verschlüsselungsoption dann, wenn im Partitionierer der Punkt „Parallel dazu installieren", „Ersetze eine Partition" oder „Festplatte löschen" ausgewählt ist. Manjaro arbeitet ohne LVM.

Fedora: Wird ein Fedora-System mit dem Standard-Partitionsschema eingerichtet, so erledigt die Option „Meine Daten verschlüsseln" eine Vollverschlüsselung mit oder wahlweise auch ohne LVM-Unterbau. Der Partitionierer Blivet bietet beim Anlegen neuer Partitionen ebenfalls die Option „Encrypt" an.

Notfallzugriff per Livesystem

Was tun, wenn sich das System mal nicht mehr booten lässt, weil etwa der Bootsektor überschrieben, ein Notebook defekt ist oder das Linux-System aus anderen Gründen nicht mehr startet? Keine Panik, wenn die verschlüsselte Partition intakt und das Luks-Passwort bekannt ist, dann kann auch ein gestartetes Linux-Livesystem noch auf die Luks-Partitionen zugreifen. Eine bequeme Möglichkeit sind die installierbaren, bootfähigen Livesysteme von Linux Mint 19 und Ubuntu Budgie 18.04 (auf Heft-DVD). Ebenfalls funktionieren das kleine GRML (*https://grml.org*, 600 MB) und das umfangreiche Knoppix (*www.knopper.net/knoppix*. 4,4 GB) als traditionelle Reparatursysteme. Für die Datenträger spielt es keine Rolle, ob ein Livesystem in der 32-Bit- oder 64-Variante zur Verwendung kommt.

So funktioniert das Entschlüsseln und Einhängen per Livesystem: Zuerst muss man sicherstellen, dass im Livesystem das Kernelmodul „dm-crypt" zum Öffnen verschlüsselter Datenträger geladen ist. Das erledigt de rfolgende Befehl in einem Terminalfenster:

```
sudo modprobe dm-crypt
```

Die Dateimanager aktueller Linux-Distributionen, etwa Dolphin unter KDE oder Nau-

tilus, Nemo sowie Caja unter Gnome-affinen Desktops, erkennen verschlüsselte Partitionen. Bei einem Klick darauf bieten die Dateimanager einen Dialog zur Passworteingabe an und hängen die Partition dann ein.

Das funktioniert bei komplexen Partitionsschemata und LVM-Volumen aber nicht immer automatisch. In diesem Fall ist ein Exkurs in die Kommandozeile nötig. Zunächst gilt es, mit dem Kommando

```
sudo blkid
```

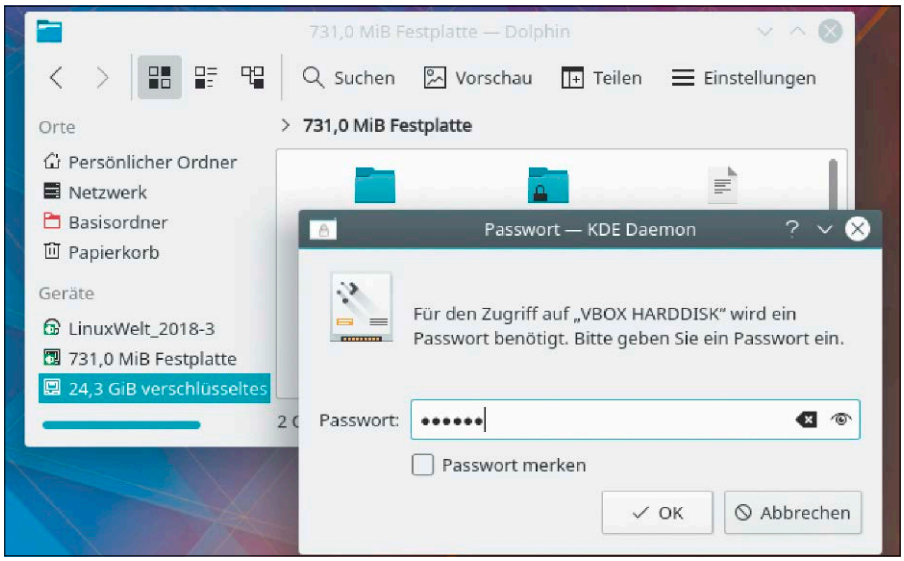
die Kennung der verschlüsselten Partitionen herauszufinden. Luks-Partitionen sind über die Ausgabe „TYPE=crypto_Luks“ in der angezeigten Liste leicht zu erkennen. Diese verschlüsselten Partitionen kann der Befehl mount nicht auf gewohnte Weise einhängen, da die Partitionstabelle selbst chiffriert ist. Stattdessen bereitet das Kommandozeilentool cryptsetup den Zugriff vor, in diesem Beispiel für die verschlüsselte Partition „/dev/sda5“:

```
sudo cryptsetup luksOpen /dev/sda5
 partition
```

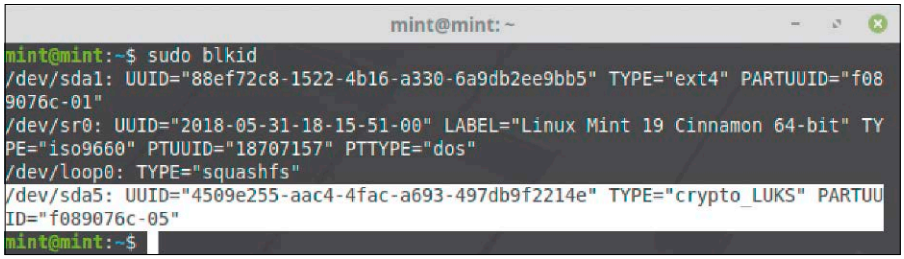
Der Befehl fragt dann das Passwort zur Entschlüsselung der Partition ab. Falls es sich um eine einzelne verschlüsselte Partition ohne LVM handelt, dann hängt nun das folgende Kommando die entschlüsselte Partition nach „/mnt/“ ein:

```
sudo mount /dev/mapper/partition /
 mnt/
```

Verwendung von LVM: Wenn das verschlüsselte System den Logical Volume Manager (LVM) nutzt, was in Ubuntu, Linux Mint und Fedora der Standard bei Vollverschlüsselung ist, dann kann mount noch nichts ausrichten. Stattdessen weisen Sie mit folgendem Befehl LVM an, alle Volumes der Partition aufzulisten:



Einfach einhängen: Der KDE-Dateimanager Dolphin erkennt genauso wie Gnome-Dateimanager Luks-verschlüsselte Datenträger und hängt sie nach der Passworteingabe ein.



Wo steckt die verschlüsselte Partition? In einem Livesystem, hier Linux Mint 19, ist der Befehl *sudo blkid* nützlich, um die Gerätekennung der gesuchten Luks-Partition anzuzeigen.

```
sudo vgscan --mknodes
sudo vgchange -ay
```

Die beiden Befehle finden die Volume-Gruppe auf der Luks-Partition und geben deren Namen aus, beispielsweise „ubuntu-vg“ bei einem Ubuntu-System. Das Kommando

```
sudo lvdisplay
```

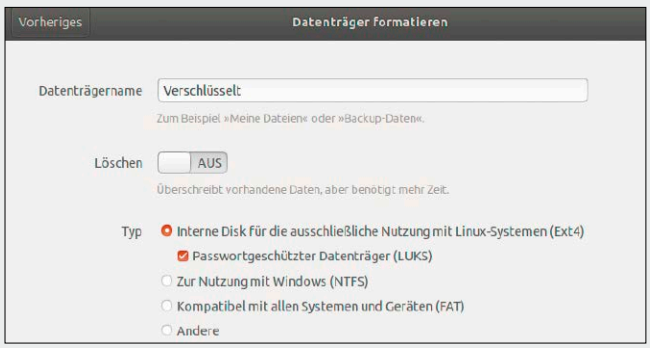
listet jetzt alle Volumes mit exaktem Pfad auf, der im nächsten Schritt wichtig ist: Um bei einem Ubuntu-System die Wurzelpartition „root“ in der Volume-Gruppe einzuhängen, sind diese zwei Befehle nötig:

```
sudo mkdir /mnt/ubuntu
sudo mount /dev/ubuntu-vg/root /
 mnt/ubuntu
```

Der Gerätepfad hinter „/dev/“ ist bei unterschiedlichen Distributionen abweichend, wird aber stets von lvdisplay angezeigt. ■

DATENTRÄGER: LUKS FÜR EXTERNE MEDIEN

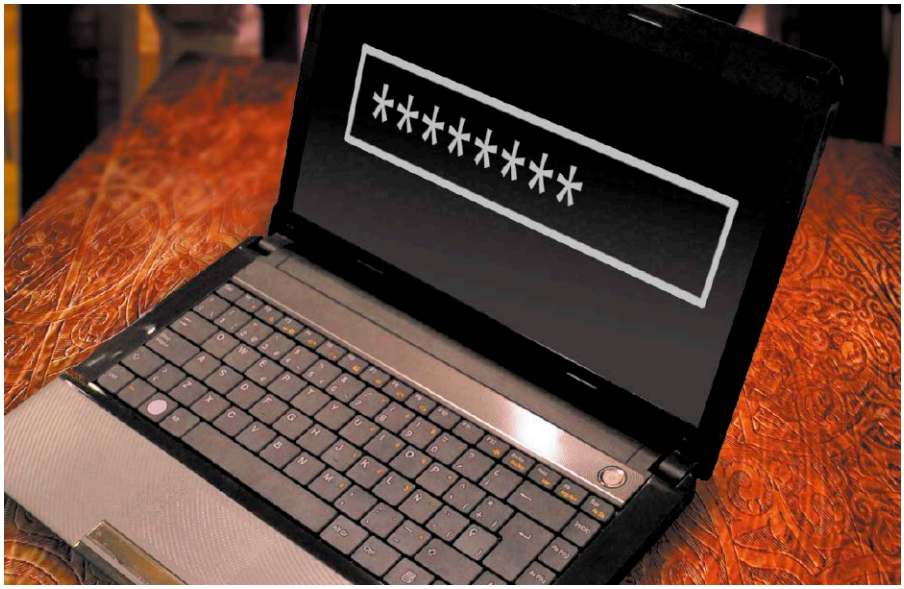
Luks-Partitionen sind auch auf externen Datenträgern wie SD-Karten und USB-Sticks gut aufgehoben. Das Programm Gnome-Disks („Laufwerke“ in der Gnome-Programmübersicht), das in Ubuntu, Linux Mint, Fedora und anderen Gnome-affinen Distributionen vorinstalliert ist, kann verschlüsselte Partitionen ganz komfortabel erstellen. Nach einem Klick auf einen freien Datenträgerbereich geht es auf das Plus-Zeichen zum Erstellen einer neuen Partition. Nach der Definition der gewünschten Größe zeigt der nächste Schritt den Punkt „Passwortgeschützter Datenträger“ an, als Unteroption des Menüpunkts „Interne Disk für die ausschließliche Nutzung mit Linux-Systemen“.



Passwörter sicher verwahren

Benutzernamen, Kennwörter, PINs: Das alles lässt sich nicht mehr im Kopf aufbewahren, zumal Passwörter komplex sein und sich selten wiederholen sollen. Passwortsafes versprechen, Zugangsdaten sicher und komfortabel zu verwalten.

VON DAVID WOLSKI



Wenn gehackte Datenbanken mit Benutzer-Log-ins in die falschen Hände fallen, sind vor allem jene Anwender gefährdet, die identische Log-ins über mehrere Onlinedienste hinweg verwenden. Hacks der Superlative sind gar nicht mehr so selten: Yahoo hat 2014 die Anmeldedaten von 500 Millionen Usern an Hacker verloren, Ebay musste im gleichen Jahr eingestehen, dass die Daten von 145 Millionen Anwendern gestohlen wurden. Letztes Jahr schlug Equifax Alarm, nachdem im Sommer 2017 die Daten von 150 Millionen Zugängen durch eine Sicherheitslücke einsehbar waren.

Pro Dienst ein eigenes Passwort

Wenn jeder Zugang mit einem individuellen Passwort geschützt ist, hält sich das Risiko für die betroffenen Anwender nach einem Hack in Grenzen. Pro Konto ein eigenes, womöglich regelmäßig geändertes Passwort: Diese Regel macht die Nutzung von Onlinediensten sicherer, trägt aber auch zu einer enormen Menge an Log-ins bei, die es zu verwalten gilt. Tatsächlich kommt kaum mehr jemand daran vorbei, sich die wachsende Zahl an Log-ins irgendwie zu notieren. Dann aber bitte sicher und komfortabel zugleich: Browser wie Firefox und Chromium bieten von sich aus an, Web-Log-ins zu sichern. Aber Browser sind nicht der richtige Ort für die zusätzliche Zahl an Linux-Log-ins, SSH-Anmeldungen und Datenbankpasswörtern, die ein Hobby-Admin immer wieder parat haben muss.

Der Beitrag nimmt sich deshalb sicher verschlüsselte Passwortsafes vor, die unter einer Open-Source-Lizenz stehen und mit vertretbarem Aufwand unter populären Linux-Distributionen wie Debian, Ubuntu, Linux Mint eingerichtet sind. Und natürlich am besten auch unter anderen Systemen wie Windows, Mac-OS und Android. Ein kurzer Steckbrief gibt an, was ein Programm neben Linux noch so abdeckt. Der Punkt „Kompatibilität" gibt an, von welchen anderen Safes ein Programm die Daten importieren kann.

Keepass XC: Neu aufgelegt

„Keepass XC" ist kein Druckfehler: Es handelt sich nicht um das bekannte Programm Keepass X, sondern um eine neuere Abspaltung. Diese war nach Ansicht einer kritischen Masse von Entwicklern nötig, weil es um Keepass X zu still geworden war. Bugreports und Funktionswünsche blieben monatelang liegen. Die Nutzergemeinde um die Open-Source-Software hat deshalb die Variante Keepass XC ins Leben gerufen, die Änderungen und Verbesserungen schneller aufnimmt.

Das Open-Source-Programm (GPL) erstellt eine lokale Datenbank, die mit AES-256 oder Twofish verschlüsselt ist. Die Oberfläche ist intuitiv und folgt im Aufbau der Keepass-Familie. Ein Rechtsklick auf einen Eintrag kann die dort hinterlegten Daten wie Benutzernamen und das Passwort in die Zwischenablage kopieren; dort bleibt die Zeichenkette aus Sicherheitsgründen nur zehn Sekunden lang, wonach Keepass XC die Zwischenablage automatisch leert. Eine andere Möglichkeit, Log-ins auf Web-

seiten automatisch auszufüllen, nennt sich „Autotype“. Dazu hinterlegen Sie in einem Datenbankeintrag im Feld „URL“ die Webadresse des Anmeldeformulars.

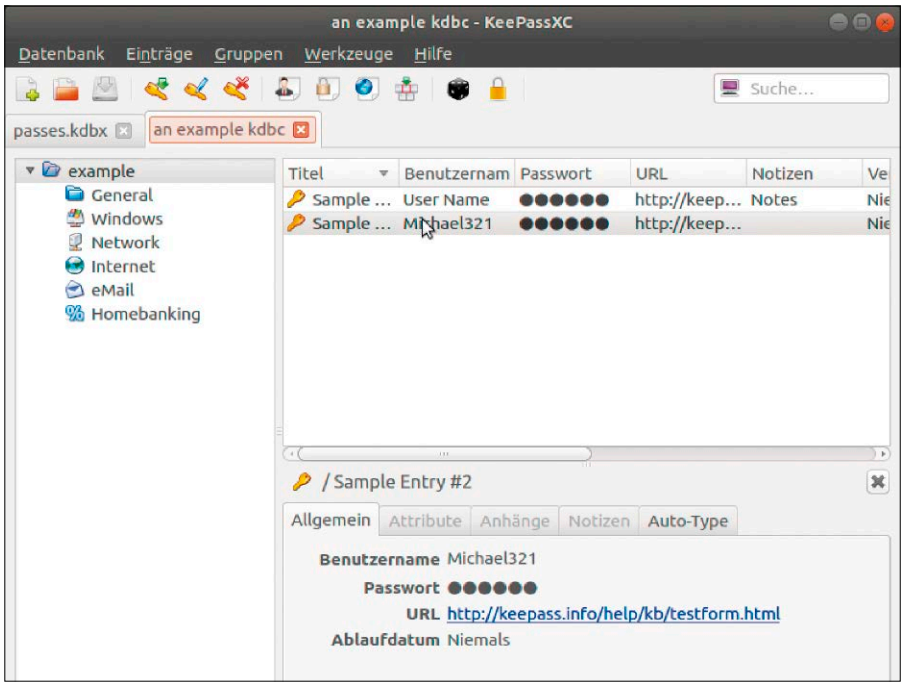
Systeme: Linux, Windows, Mac-OS

Besonderheiten: Die Abstammung von der Keepass-Familie hat ihre Vorteile: Der Umstieg von den populären Vorgängern Keepass 2 und Keepass X ist ohne Umgewöhnung möglich – perfekt für Desktopanwender.

Installation: *https://keepassxc.org*, die Projekt-Webseite, liefert fertige Pakete für Debian, Ubuntu, Linux Mint, Fedora, Open Suse Leap, Cent-OS, Arch Linux und Gentoo.

Browserintegration (für Firefox, Google Chrome/Chromium und Opera/Vivaldi): Die Funktion „Autotype“ sucht alle Browserfenster nach der in der Passwortdatenbank hinterlegten URL ab und gibt dann selbständig die Log-in-Daten ein.

Kompatibilität: Keepass XC liest unverschlüsseltes CSV ein und beherrscht lesend wie schreibend die KDBX-Dateien von Keepass X. Auch ältere KDB-Datenbanken können importiert werden.



Würdiger Erbe der Keepass-Familie: Der Allrounder ist eine Empfehlung für Anwender, die Passwörter lokal speichern und die Datenbank manuell auf andere Systeme übertragen.

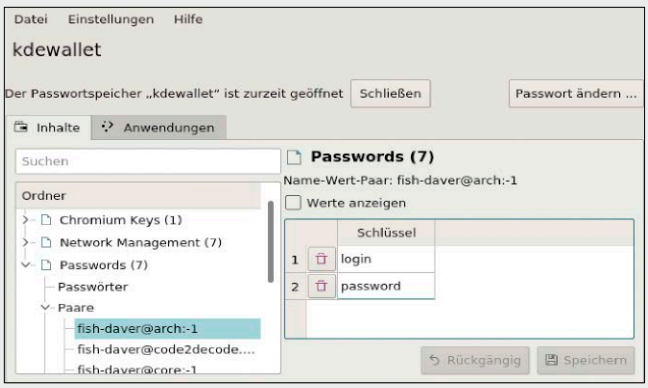
Bitwarden: Ein Griff in die Cloud

Warum nur lokal eine verschlüsselte Passwortdatenbank speichern? Die meisten Anwender benötigen Passwörter auf mehr als einem System. Bitwarden ist erst einmal nur ein Client, der sich in Form einer Desktopapp oder in Webbrowsern installiert. Statt in einem Programm mit lokaler Datenbank sind hier die Daten in der Cloud gespeichert. Es gibt Bitwarden nicht nur als Browsererweiterung, sondern auch als Desktopapp, aber auch diese verbindet sich mit dem Bitwarden-Server, um dort die verschlüsselte Datenbank zu speichern. Das wäre für misstrauische Nutzer ein Ausschlusskriterium. Aber Bitwarden ist eine hybride Lösung:

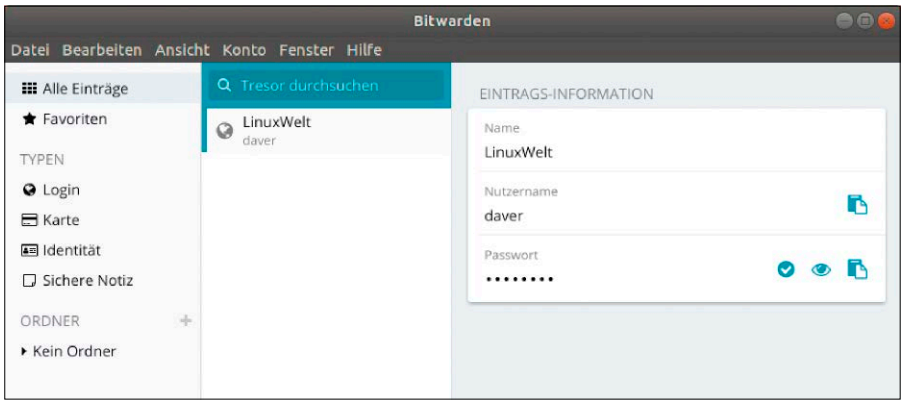
Besonders bequem ist Bitwarden als Dienst, der ein fremd gehosteter Ersatz für eine Browsersynchronisierung wie Firefox Sync ist. Weniger bequem, aber dafür komplett unter eigener Kontrolle arbeitet Bitwarden als Server für verschlüsselte Passwortdatenbanken auf einem eigenen Linux-Server im LAN oder im Internet. Dazu ist Bitwarden als freie (GPL) Serverkomponente in Form eines Docker-Containers verfügbar (*https://help.bitwarden.com/article/install-on-premise*) und kann auf einem eigenen Linux-System gehostet werden. Das ist die Variante für anspruchsvolle Anwender, die keiner Cloud trauen und lieber ihren eigenen netzwerkfähigen Passwortsafe im lokalen Netzwerk haben. Davon abgesehen erledigt Bitwarden die Ver- und Ent-

KDE-WALLET: PASSWÖRTER FÜR KDE

Die Programme von KDE sind kontaktfreudig. Allein über die KIO-Slaves, die auf entfernte Dateisysteme über SMB, SSH, Web DAV und FTP zugreifen können, ergibt sich häufig die Nachfrage, ob man wiederkehrende Log-in-Daten speichern will, um sie bei Bedarf wieder abzurufen zu können. KDE-Programme wie Dolphin und Krusader schlagen bei der ersten Eingabe eines Passworts von sich aus vor, diese Log-in-Daten sicher im KDE-Wallet zu speichern. Für die Verwaltung anderer Log-in-Daten außerhalb von KDE-Programmen ist das Programm nicht geeignet. KDE-Wallet ist mit dem Programmaufruf „kwalletmanager5“ einsehbar und die gespeicherten Daten lassen sich dort nach der Entsperrung mittels „Datei → XML exportieren“ in eine unverschlüsselte XML-Datei sichern. Ein chiffriertes Austausch- und Backupformat bietet die Funktion „Datei → Verschlüsselt exportieren“.



Passwortsafe in KDE: KDE-Wallet stellt KDE-Programmen einen geschützten Speicher bereit. Bei der ersten Verwendung muss ein Masterpasswort festgelegt werden.



Desktopapp von Bitwarden: Obwohl Bitwarden eher ein Dienst als eine Anwendung ist, gibt es inzwischen auch Programme für den Desktop, die außerhalb des Webbrowsers laufen.

schlüsselung der Datenbank auf dem eigenen Rechner und überträgt sie erst dann an den Server im Netzwerk.

Besonderheiten: Bitwarden ist einerseits ein Clouddienst, anderseits ein Open-Source-Server (GPL). Die Serversoftware lässt sich dank Docker-Images aber auch im LAN oder auf dem eigenen Server einrichten. Es gibt die Möglichkeit einer Zwei-Faktor-Authentifizierung. Bitwarden finanziert sich als Dienst über einen kostenpflichtigen Premiumdienst.

Installation: Auf der Website *www.bitwarden.com* gibt es neben Browsererweiterungen auch ein Desktopprogramm, das selbst eine Verbindung zum eigenen Server oder zur Cloud von Bitwarden aufbaut. Für Linux gibt es diese Desktopapp als universelles Appimage.

Systeme: Linux, Windows, Mac-OS

Browserintegration: Alle prominenten Browser werden unterstützt.

Kompatibilität: Bitwarden beherrscht den Import von mehr als zwei Dutzend bekannter Passwortmanagern, dazu auch den Import von Passwörtern aus Firefox und Opera.

Password Gorilla: Das Urgestein

Völlig unterschätzt ist der Passwortmanager Gorilla, zumal es in der Zielsetzung des Programms wenig zu verbessern gibt. Password Gorilla speichert eine Datenbankdatei lokal ab, mit Masterpasswort verschlüsselt. Es ist das einfachste Programm mit grafischer Oberfläche in dieser Aufstellung. Benötigt man einen Log-in, dann muss man diesen per Copy & Paste in das entsprechende Feld eintragen. Der Charme von Password Gorilla ist die Portabilität: Das Open-Source-Programm hat keine Ansprüche und ist plattformunabhängig. Das Masterpasswort dient zur Chiffrierung aller Einträge. Die Verschlüsselung arbeitet mit Twofish und SHA256-Cipher für das Masterpasswort.

Die Programmoberfläche ist schlicht und gibt nach der Erstellung einer Passwortdatenbank deren Inhalt nur über den eingebauten Texteditor preis. Bei Brute-Force-Angriffen verlängert Password Gorilla automatisch die Reaktionszeit in Intervallen und erschwert damit Wörterbuchangriffe. Wer nur wenige Passwörter und Log-ins verwalten muss, diese aber mit möglichst wenig Aufwand sicher verschlüsseln und eine Datenbank zwischen unterschiedlichen Systemen austauschen möchte, ist mit dem Password Gorilla gut beraten.

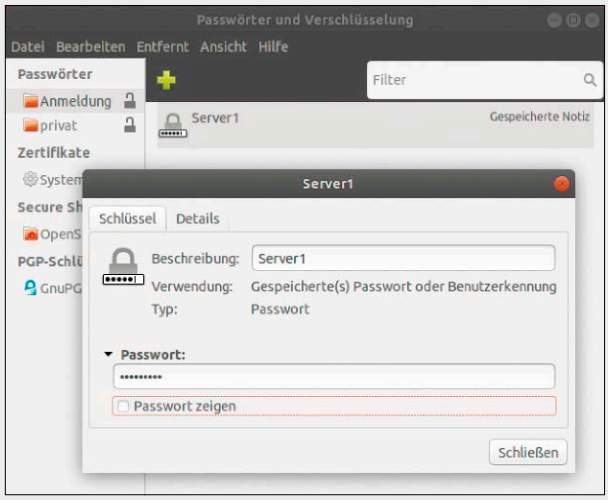
Besonderheiten: Password Gorilla kann mit mehreren Passwortdatenbanken umgehen. Er liegt als Binary vor und eignet sich damit für den portablen Einsatz auf USB-Sticks. Eine Browseranbindung fehlt.

Installation: Die Seite *https://github.com/zdia/gorilla* liefert neben dem Quellcode

GNOME: DER GNOME-KEYRING

In Gnome, Unity, Cinnamon, XFCE und Mate kümmert sich im Hintergrund der Dienst Gnome-Keyring um die Verwahrung von Passwörtern. Anders als KDE-Wallet hält sich der Gnome-Keyring dezent im Hintergrund, fragt nicht nach einem initialen Masterpasswort, sondern nutzt das Log-in-Passwort des Anwenders als Kennwort. Diese Übereinstimmung ist nicht zwingend, aber bequem, denn sonst würde der Gnome-Keyring nach der Anmeldung nochmal nach dem gewählten Passwort zum Entsperren der Passwortdatei fragen.

Gnome-Keyring ist ein Hintergrunddienst, der mit der Desktopumgebung Gnome sowie mit Programmen interagiert, die für diesen Dienst entwickelt wurden. Es gibt aber die Möglichkeit, mit dem Programm Seahorse den Gnome-Keyring zu öffnen und einzusehen. Prinzipiell wäre es möglich, mit Seahorse weitere Passwörter manuell im Gnome-Keyring zu speichern, denn über das Menü „Datei -> Neu → Gespeichertes Passwort“ könnten Sie beliebige neue Log-ins anlegen. Das wäre aber eine Zweckentfremdung des Gnome-Keyrings, der sich vornehmlich um Passwörter innerhalb der Desktopumgebung kümmert und mit Seahorse nur eine rudimentäre Passwortverwaltung zulässt.

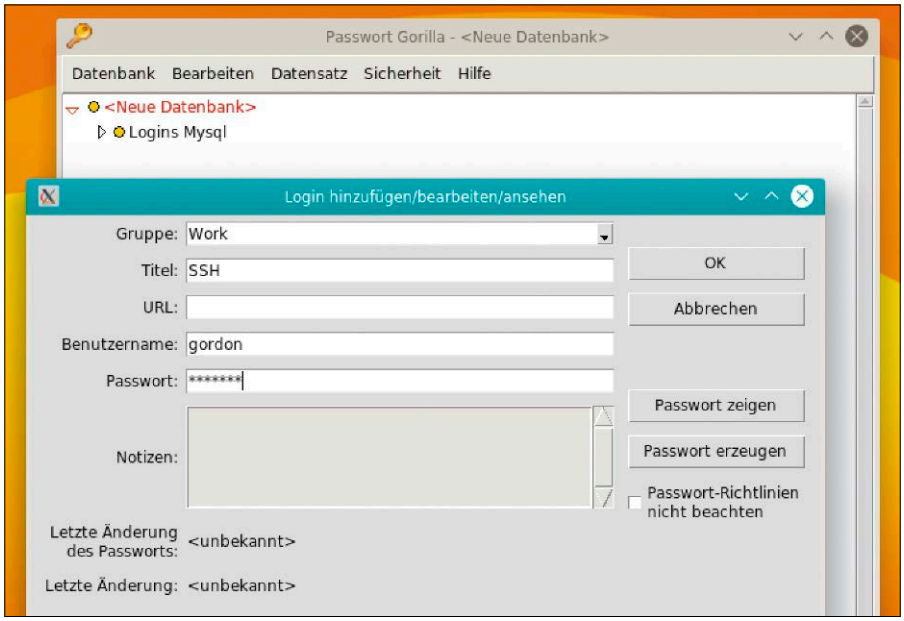


Seahorse: Der Gnome-Keyring arbeitet unbemerkt im Hintergrund und interagiert mit Programmen, nicht mit dem Anwender. Das Programm Seahorse dient zur Einsicht und Verwaltung.

eine ausführbare Binary, die unter allen Linux-Systemen funktioniert.
Systeme: Linux, Windows, Mac-OS
Browserintegration: keine, einfaches Copy & Paste
Kompatibilität: Password Gorilla ist ein eigenes Tier: Es gibt keine Import- oder Exportmöglichkeiten, die mit anderen Passwortsafes harmonieren.

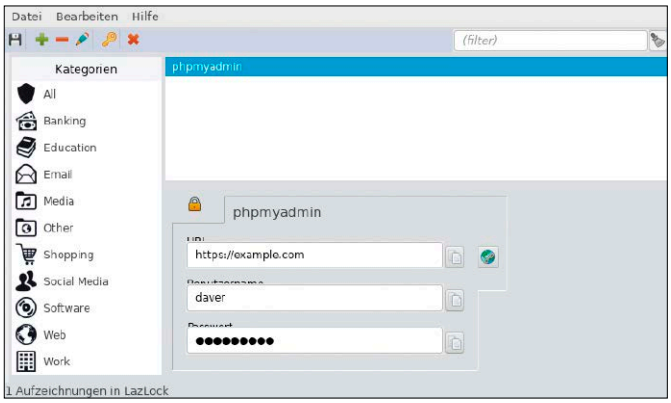
Lazlock: Nimm mich mit

Auch Lazlock liegt für Linux als ausführbare Binary vor, die unter allen verbreiteten Linux-Systemen läuft. Die Oberfläche ist ausschließlich englischsprachig. Das Programm ist Open Source (MIT-Lizenz) und noch portabler als alle anderen Passwortmanager. Die Verschlüsselung des Safes ist mit AES-128 vorgegeben und damit elaborierten Angriffen nicht gewachsen, aber sicher genug für den Hausgebrauch. Und nur dafür ist Lazlock gemacht. Das Programm zeigt eine intuitive Oberfläche ohne jedwede Rätsel, wie der Safe funktioniert: Beim ersten Aufruf wird ein Passwort verlangt, das dann als Masterpasswort zur Chiffrierung der Datenbank dient. Die Passworteinträge sind nach Kategorien sortiert und es gibt eine Exportfunktion, die alle Einträge als unverschlüsselte Textdatei exportiert. Der Funktionsumfang in Lazlock ist überschaubar – es geht nur um die manuelle Passwortverwaltung. Browsererweiterungen gibt es keine. Anwender müssen sich mit Copy & Paste begnügen.
Besonderheiten: Eine solide Lösung für gespeicherte Passwörter auf Wechseldatenträgern, die zwischen Windows und Linux ausgetauscht werden. Lazlock kann immer nur mit einer Passwortdatenbank umgehen.
Installation: Auf der Seite *https://cpunk-security.com/lazlock.html* liegt Lazlock in Form ausführbarer Binaries für Linux vor; eine Installation ist nicht nötig. Das Programm bietet zwei Varianten, einmal mit dem Toolkit GTK (Gnome & Co), ferner mit Qt (KDE) und sollte passend zur Desktopumgebung gewählt werden.
Systeme: Linux, Windows
Browserintegration: keine, einfaches Copy & Paste
Kompatibilität: Lazlock verwendet sein eigenes Format. Die Datenbank kann lediglich als unverschlüsselte CSV-Datei exportiert werden. ■



Die Oberfläche des Password Gorilla: Ausgewählte Passwörter kopiert das Programm bei Bedarf in die Zwischenablage. Eine Browserintegration über Addons gibt es nicht.

Besticht durch Einfachheit: Lazlock ist ein Passwortmanager, der unter Linux portabel und ohne Installation auf einem USB-Stick laufen kann.



ZUGANGSDATEN IN FIREFOX: ZWEIFEL AM MASTERPASSWORT

Firefox war einer der ersten Browser, der einen integrierten Passwortsafe für Formulardaten anbot – erst als lokaler verschlüsselter Speicher auf dem jeweiligen Rechner, später in Zusammenspiel mit der Sync-Funktion, mit der sich Firefox via Mozilla-Server auf mehreren Geräten abgleicht. Von großen Hacks auf die lokalen Firefox-Datenbanken oder gar auf die zentrale Sync-Datenbank, die ein echter Jackpot wäre, war über die Jahre nichts Beunruhigendes zu hören. Die Mozilla Foundation macht ihren Job offenbar gewissenhaft.
Aber es wurden inzwischen Zweifel laut, wie Firefox die lokalen Passwortdaten mit dem optionalen Masterpasswort absichert: Der Add-on-Entwickler Wladimir Palant fand im Quellcode von Mozilla Firefox eine Verschlüsselungsfunktion mit SHA-1. Die nutzt der Browser seit neun Jahren unverändert, obwohl SHA-1 mittlerweile als schwach gilt. Eine Stellungnahme der Mozilla Foundation steht noch aus (Stand Juli 2018). Ganz Vorsichtige werden daher auf Linux-Rechnern mit wichtigen Log-ins eine Verschlüsselung des Datenträgers mittels Luks verwenden, die Ubuntu, Linux Mint und Fedora bei der Installation anbieten.

Die eigene Passwort-zentrale

Für komfortables Surfen ist die Browsersynchronisierung von Passwörtern die einfachste Lösung. Browser berücksichtigen aber nur die Onlinepasswörter. Für eine komplette Synchronisierung aller Passwörter müssen Sie selbst aktiv werden.

VON HERMANN APFELBÖCK

Mit einem Cloudspeicher wie Dropbox oder einem stets erreichbaren FTP-Server auf einem Firmenrechner oder auf der eigenen Homepage bedeutet es nur geringen Aufwand, alle Passwörter und sonstige Zugangsdaten selbständig synchron zu halten. Wir erklären das Prinzip und bieten einige konkrete Script-Varianten, die Sie allesamt in der Datei „/Software/Tresore.txt“ auf der Heft-DVD sowie unter *https://paste.ubuntu.com/p/hnxB2mfBw8/* einsehen und abholen können. Etwas Script-Erfahrung setzen wir bei der Umsetzung voraus. Im Benutzeralltag ist ferner Disziplin erforderlich, da Sie bei einer eigenen Script-Lösung auf allen Rechnern konsequent mit diesen Scripts arbeiten müssen. Der Lohn ist eine flexible Datenzentrale, die neben den Passwörtern auch sonstige Daten wie Adressen und Notizen aufnehmen kann.

1. Das Prinzip und die erforderlichen Schritte

Das Prinzip einer eigenen Passwortzentrale folgt dem der Browsersynchronisierung: Die Daten liegen auf einem Server und der Browser holt diese beim Start dort ab. Wenn sich Passwörter oder Lesezeichen in der aktuellen Browsersitzung ändern, wird der geänderte Stand auf den Server zurückgespeichert. Das Abholen und Zurückschreiben der Daten muss bei einer selbst gestrickten Lösung durch ein Script geschehen. Dafür gibt es einschlägige Tools wie wget, wput oder curl, die auf jedem Linux-System standardmäßig vorliegen und unter Windows leicht nachzuinstallieren sind.

Außerdem muss eine Datei mit so hochsensiblen Inhalten natürlich verschlüsselt sein, egal wo im Internet Sie diese Datei hinterlegen: Selbst in einem geschützten Bereich der eigenen Homepage ist Verschlüsselung zu empfehlen, da mindestens der Admin des Webhosters mitlesen kann. Nachdem die Datei auf Server oder Cloud abgelegt ist, ergeben sich für das alltägliche Script insgesamt maximal fünf Schritte:

1. Abholen der Datei vom Server mit curl oder wget
2. Entschlüsseln der Datei mit einem Kommandozeilenprogramm (z. B. 7-Zip)
3. Öffnen der Datei mit dem Programm oder Editor Ihrer Wahl
4. Verschlüsseln der Datei mit einem Kommandozeilenprogramm (z. B. 7-Zip)
5. Zurückkopieren der Datei zum Server mit curl oder wput

Unter Umständen muss das Script aber nur einen Teil dieser Pflichten erledigen. Das Verschlüsseln kann eventuell der Editor selbst übernehmen, wonach Schritt 2 und 4 entfallen. Den Transport der Datei kann eine Cloudsoftware übernehmen, womit Schritt 1 und 5 entfallen.

2. Passwortdaten im Sync-Ordner einer Cloud

Dropbox, Hidrive, Onedrive, Google Drive u. a. bieten lokale Synchronisierungsordner, die dort abgelegte Dateien automatisch zum Cloudserver hochladen. Wenn für Verschlüsselung gesorgt ist (Keepassxc? Office? Dazu mehr im nächsten Punkt), dann können Sie Ihren Passworttresor einfach in diesem Sync-Ordner speichern, dort nutzen und bearbeiten. Für Upload und Download sorgt der Automatismus.

Diese komfortable Variante hat aber ihre Kehrseiten – nicht nur, dass Sie die Passwörter eventuell ungern bei US-Servern abladen: Der Synchronisierungsdienst müsste nämlich auf jedem benutzten Rechner installiert sein. Selbst wenn Sie diese Mühe nicht scheuen, scheitert dies unter Linux zum Teil an fehlender Clientsoftware. Lediglich für Dropbox und Strato Hidrive (kostenpflichtig) gibt es native Sync-Lösungen.

3. Verschlüsselung per Software

Um sich die Verschlüsselungspflicht zu vereinfachen, können Sie für den Passworttresor einen Editor verwenden, der selbst verschlüsselt. Eine gute Wahl ist das im vorangehenden Artikel beschriebene Keepassxc (Downloads für Linux, Windows und Mac-OS unter *https://keepassxc.org/download*). Die zugehörigen KDBX-Dateien mit den Daten sind standardmäßig sicher verschlüsselt, das Öffnen dieser Datenbankdateien erfordert immer die Eingabe des Masterpassworts.

Keepassxc ist außerdem als Passwortmanager spezialisiert und ermöglicht über die Zwischenablage einfaches Kopieren der Daten, mit „Auto-Type" auch automatisches Ausfüllen mehrerer Felder.

Nach dem Download vom Server würde der unter Punkt 1 genannte Schritt 3 („Öffnen der Datei mit dem Programm oder Editor Ihrer Wahl") im Falle von Keepass XC folgendermaßen aussehen:

```
keepassxc --keyfile [pfad]/[name].
  kdbx
```

Die Abbildung auf dieser Seite (rechts oben) zeigt ein konkretes Beispiel-Script für Keepassxc während der Ausführung.

Sofern Sie Keepassxc bisher nicht genutzt haben und noch keine KDBX-Datenbank vorliegt, dann muss diese in Keepassxc Eintrag für Eintrag neu erstellt werden. Wem dies zu mühsam ist, wird auf der Suche nach einer breiter angelegten Software, die aber gleichwohl verschlüsseln kann, schnell fündig: Libre Office und Microsoft Office können in Textverarbeitung oder Tabellenkalkulation auch unstrukturierte Daten aufnehmen und diese schützen („Speichern unter → Mit Kennwort speichern" oder „Speichern unter → Tools"). Wenn auf verschiedenen Rechnern beide Office-Suiten genutzt werden, empfehlen wir das Format DOCX oder XLSX. Wo nur Libre Office zum Einsatz kommt, ist natürlich dessen natives odt/ods-Format die beste Wahl.

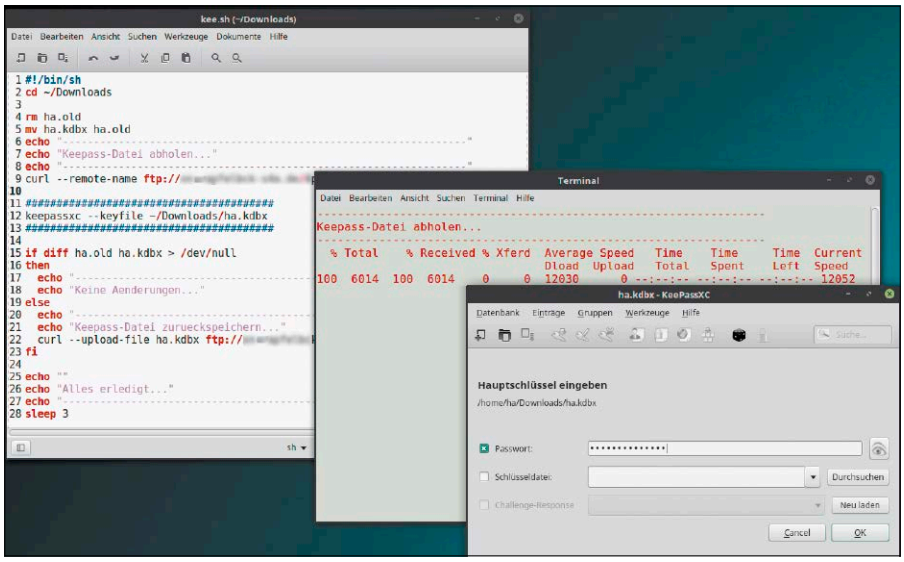
Hinweis: Der Start des jeweiligen Editors – sei es Keepassxc, Libre Office oder ein Texteditor – muss so ausfallen, dass das Script so lange pausiert, bis der Editor wieder beendet wird. Im Shell-Script unter Linux führt im Falle von Libre Office die Script-Zeile

```
libreoffice --calc [Datei]
```

zum Erfolg, während unter Windows folgender Befehl

```
start /wait [Datei]
```

zu empfehlen ist.



Keepassxc mit Datendatei vom Server: So ist gewährleistet, dass Sie auf allen Rechnern den aktuellsten Stand vorfinden. Für Verschlüsselung sorgt die Software selbst.

Variante mit 7-Zip-Verschlüsselung: Während des Schrittes „Bearbeiten" suchen oder ändern Sie Einträge in der Passwortdatei. Diese geht anschließend aktualisiert zurück zum Server.

4. Verschlüsselung per Script

Während die Varianten unter Punkt 2 und 3 die selbst gebaute Passwortsynchronisierung durch geschickte Wahl der Software oder/und durch Cloudeinsatz vereinfacht haben, können Sie auch alles selbst in die Hand nehmen. Das ist ein Stück komplizierter, bringt aber einige Vorteile:

1. Die Anzeige- und Bearbeitungssoftware der Passwortdatei kann ein beliebiger Standardeditor sein (Gedit, Notepad); somit entfällt die mehrfache Einrichtung einer Software wie Keepassxc oder Libre Office.
2. Auf stationären PCs können Sie das Verschlüsselungspasswort für den Tresor direkt in das Script eintragen und sich dadurch die Eingabe ersparen (auf mobilen Notebooks ist das nicht ratsam).
3. 7-Zip verschlüsselt mit einem komplexen Kennwort mindestens so sicher wie Libre/Microsoft Office oder Keepassxc.

Das knappe Fünf-Schritte-Prinzip sieht dann so aus:

```
curl --remote-name ftp://[server.
  de]/[ordner]/datei.7z --user
  [ftpuser]:[ftpkennwort]
7z x -p"geheim" -o"." datei.7z
## Öffnen der Passwortdatei
gedit -w datei.txt
## Script fährt nach Schließen fort
7z a -p"geheim" datei.7z datei.txt
curl -upload-file file.7z ftp://
  [server.de]/[ordner]/file.7z
  --user [ftpuser]:[ftpkennwort]
```

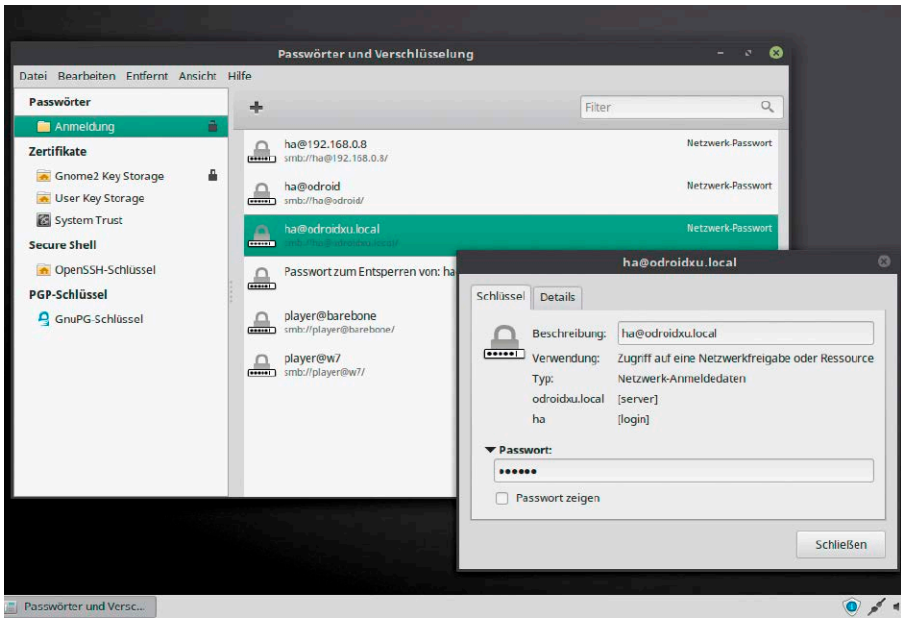
Den wesentlich ausführlicheren Beispielcode für Linux und Windows finden Sie in der Datei „Tresore.txt" unter „/Software" auf der Heft-DVD. Dort sind auch alle Beispiel-Scripts für die einfacheren Varianten mit Keepassxc und Libre/Microsoft Office (Punkt 3). Zusätzlich erhalten Sie die komplette Script-Sammlung auch im Web unter *https://paste.ubuntu.com/p/hnxB2mfBw8/*.

Spezielle Passwörter

Passwörter haben unterschiedliche Funktionen und unterschiedliche Speicherorte. Nachlässiger Umgang mit Passwörtern kann daher harmlose, lästige oder katastrophale Folgen haben. Dieser Beitrag hat einige spezielle Kennworttypen im Fokus.

VON HERMANN APFELBÖCK

Neben Onlinepasswörtern gibt es Funknetzschlüssel, System- und SSH-Konten, Netzwerkkennwörter, Verschlüsselungspasswörter, Passwörter für Weboberflächen, Masterkennwörter für Browser oder Passwortmanager. Die folgenden zwei Seiten geben eine Kurzcharakterisierung über Bedeutung und Sensibilität sowie jeweils eine Kurzempfehlung. Die allgemeine Empfehlung lautet, dass schon ein Heimnetz ohne Protokollierung der Anmeldedaten nicht mehr auskommt. Ob das in einem Passwortmanager geschehen muss oder ob eine Textdatei genügt, ist Ermessensfrage.



Erinnerungshilfe Seahorse: Das Tool zeigt gespeicherte Kennwörter im Klartext an, kann aber eine Sammlung aller System-, Samba-, Log-in- und Onlinedaten nicht ansatzweise ersetzen.

Log-ins auf Router, NAS, Access Point

Alle Netzwerkgeräte wie Router, Repeater, Access Point, Netzdrucker stellen heute eine Konfigurationsoberfläche mit Anmeldung bereit. In der Regel wird empfohlen, die Vorgabestandards durch ein persönliches Passwort auszutauschen. Pflicht ist dies, wenn Netzgeräte per Portfreigabe für den Internetzugriff geöffnet werden.

Empfehlung: Geänderte Passwörter von Netzgeräten müssen Sie dringend in einem Passwortmanager oder anderweitig speichern. Da sich oft monatelang keine Ursache ergibt, die Gerätekonfiguration aufzusuchen, werden Passwörter bald vergessen. Ohne Erinnerungshilfe bleibt schlimmstenfalls nur ein harter Reset auf die Werksvorgaben unter Verlust aller eigenen Einstellungen.

Kennwort für Luks-Festplattenverschlüsselung

Sowohl Systemdatenträger als auch externe Datenträger können mit Linux Unified Key Setup komplett verschlüsselt werden (siehe dazu ab Seite 48). Der Systemstart oder die Benutzung des externen Datenträgers ist dann nur noch nach korrekter Eingabe des Passworts möglich. Dieses Passwort ist an keiner Stelle gespeichert oder reproduzierbar.

Empfehlung: Da Zweifel beim Luks-Passwort irreparable Schäden auslösen, sollte man das Kennwort in jedem Fall an sicherer Stelle verwahren. Da Luks immer nur drei Eingabeversuche zulässt, ist es außerdem ratsam, auf abgeschaltetes Capslock und Numlock zu achten.

System-, SSH- und Samba-Passwörter

System- und SSH-Authentifizierung benutzen gleichermaßen die Systemkonten und somit dieselben Passwörter. Vergessene Systempasswörter sind allerdings nicht rekonstruierbar, allenfalls in der verschlüsselten Ablage der Datei „/etc/shadow“ (nach dem Kontonamen) manuell zu löschen. Neue Passwörter kann auch das Kommando passwd vergeben. Samba-Netzfreigaben haben hingegen ein unabhängiges User- und Passwortkonzept.

Sofern Samba-Netzfreigaben und SSH-Server mit dem grafischen Dateimanager und der Anweisung betreten wurden, die Zugangsdaten zu speichern, kann Seahorse („Passwörter und Verschlüsselung“) die Passwörter des aktuell angemeldeten Kontos anzeigen. Windows hat unter „Systemsteuerung → Anmeldeinformationsverwaltung“ ein vergleichbares Tool. Diese Programme können zwar einige Passwörter in Erinnerung rufen (für andere Rechner), helfen aber nicht bei ernsten Anmeldeproblemen. Mit allem, was hier steht, verbindet sich der Rechner problemlos.

Empfehlung: Wer mehrere Rechner betreut, tut gut daran, Systemkonten und Passwörter in einem Passwortmanager oder in einer verschlüsselten Datei zu si-

chern. Bei Samba-Freigaben empfiehlt sich, die Daten des Systemkontos auch für das Samba-Konto und -Passwort zu übernehmen. Das ist ein Stück unsicherer, aber deutlich übersichtlicher.

Das WLAN-Kennwort

Jeder, der Besucher in sein WLAN lässt, und sei es auch durch verdeckte Passworteingabe, gibt das Passwort dauerhaft nach außen. Auf Smartphones können WLAN-Kennwörter nach Rooten des Geräts ausgelesen werden.

Auf Notebooks und PCs ist es überhaupt kein Problem, alle Kennwörter der bisherigen WLAN-Verbindungen zu ermitteln. Linux zeigt die Kennwörter in der Datei „/etc/NetworkManager/system-connections“ (für root). Unter Windows reichen Benutzerrechte, um zunächst mit

```
netsh wlan show profile
```

alle gespeicherten Funknetze aufzulisten und dann mit

```
netsh wlan show profile
  [Funknetzname] key=clear
```

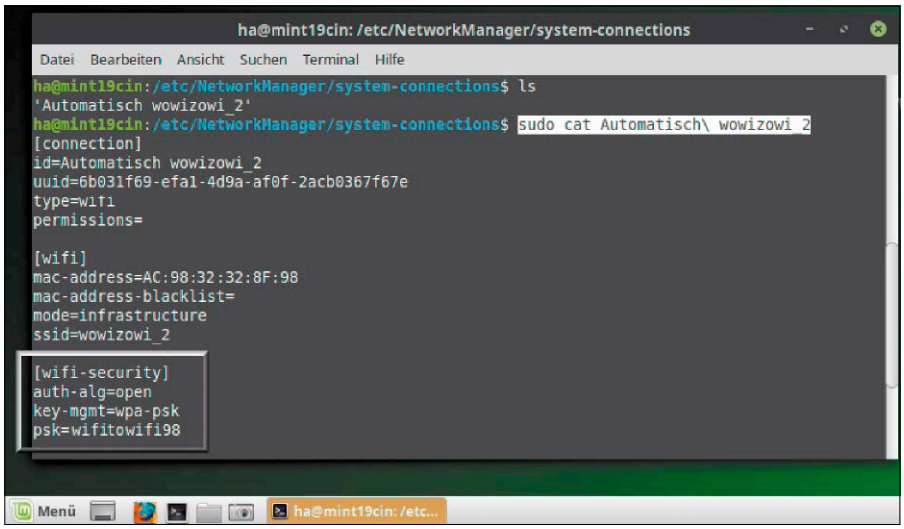
das Kennwort des gewünschten Netzes abzufragen.

Empfehlung: Für Besucher kann im Router mit wenig Aufwand ein WLAN-Gastfunknetz mit eigenem Passwort eingerichtet werden, das nur das Surfen erlaubt.

Manuelle Ad-hoc-Passwörter

Es gibt unzählige Verschlüsselungstools und Packer, die schnell mal einige Dateien in ein sicheres Archiv verschlüsseln. Wer hier mit wechselnder Software und schnellen Ad-hoc-Passwörtern hantiert, riskiert die eigene Aussperrung. Nach etlichen Monaten oder Jahren fehlen nämlich oft gleich zwei wesentliche Informationen – die Software und das Passwort.

Empfehlung: Verschlüsselung ist eine strategische Aufgabe, die Kontinuität bei Werkzeug und Schlüssel erfordert. Geänderte Kennwörter sollten in einem Passwortmanager oder in einer verschlüsselten Datei genau protokolliert werden.



Linux, Windows und gerootetes Android zeigen alle Daten von gespeicherten WLANs. Das ist nicht zu ändern, aber durch einen WLAN-Gastzugang zu entschärfen.

Das Passwort für die Chrome-Synchronisierung

Wer Onlinekennwörter (und weitere Daten wie Lesezeichen) nicht nur lokal speichert, sondern auf einem Server ablegt, um den Browser auf mehreren Geräten synchron zu halten, aktiviert dazu die Synchronisierung über ein Firefox- oder Google-Konto. Anders als bei Mozilla (Firefox) werden bei Google (Chrome/Chromium) aber nur die Kennwörter verschlüsselt. Den Rest kann Google lesen und auswerten. Jedoch bietet der Browser unter „Einstellungen → Erweiterte Synchronisierungseinstellungen“ die zusätzliche Option „Alle synchronisierten Daten [...] verschlüsseln“, bei der Sie ein Kennwort vergeben, das unabhängig vom Google-Kennwort ist. Der Komfortverlust ist nicht gravierend, da Sie dieses Kennwort auf jedem Gerät nur einmal eingeben müssen. Dies verschlüsselt alle Daten auf dem Google-Server, der Schlüssel verbleibt auf Ihrem Gerät.

Empfehlung: Es handelt sich um eine uneingeschränkt zu empfehlende Datenschutzmaßnahme gegen die Datenschnüffelei von Google. Die Maßnahme hilft aber nichts gegen Datenklau am lokalen Gerät. ■

DAS MASTERPASSWORT IN FIREFOX UND THUNDERBIRD

Firefox fragt wie jeder Browser bei einer Webanmeldung, ob die Zugangsdaten gespeichert werden sollen. Dann kann Firefox bei künftiger Anmeldung auf dieser Seite Name und Passwort automatisch übergeben. Das bedeutet aber, dass jeder, der Zugriff auf Ihr Gerät hat, auch Ihre persönlichen Zugänge nutzen kann, und unter „Einstellungen → Sicherheit → Gespeicherte Zugangsdaten“ lassen sich sämtliche Kennwörter bequem auslesen. Zum Schutz dieser Zugangsdaten bietet Firefox das Masterpasswort („Einstellungen → Sicherheit → Master-Passwort verwenden“), das alle Kennwörter verschlüsselt. Das Masterpasswort wird pro Firefox-Sitzung nur einmal abgefragt.

Thunderbird kann sämtliche Mailzugangsdaten offenlegen: Nach Einblenden des klassischen Menüs mit Alt-Taste gibt es unter „Extras → Einstellungen → Sicherheit“ die Schaltfläche „Gespeicherte Passwörter“. Die Liste zeigt alle SMTP-, POP-, IMAP-Zugangsdaten, die Passwörter erst, wenn zusätzlich der Button „Passwörter anzeigen“ geklickt wird. Damit diesen einfachen Weg nicht jeder nehmen kann, der Ihr System bei Ihrer Abwesenheit oder nach einem Notebookverlust vor sich hat, hilft die Option „Master-Passwort verwenden“ unter „Extras → Einstellungen → Sicherheit“.

Empfehlung: Es handelt sich um den Schutz der lokal im Firefox- oder Thunderbird-Profil gespeicherten Daten. Im Büro bei häufiger Abwesenheit und offenem System ist die Maßnahme sinnvoll, bei mobilen Notebooks zu erwägen. Auf stationären PCs zu Hause ist dieser Schutz eher unnötig.

Zwei-Faktor-Authentifizierung

Wer nur ein Passwort für die Anmeldung bei Banken oder Shops verwendet, lebt gefährlich. Für mehr Sicherheit sollten Sie Onlinekonten mit einem zusätzlichen Code schützen.

© vege – Fotolia.com

Onlinekonten schützen: Bei der Zwei-Faktor-Authentifizierung melden Sie sich mit Benutzernamen und Passwort sowie einem zusätzlichen Code an, den Sie etwa per SMS erhalten.

VON THORSTEN EGGELING

Bei sozialen Netzwerken, Onlineshops oder E-Mail-Diensten melden Sie sich mit einem Benutzernamen und Passwort an. Sicherheitsexperten raten, nicht bei allen Diensten das gleiche Passwort zu verwenden und die Passwörter regelmäßig zu ändern. Wenn Sie den Browser die Daten speichern lassen, müssen Sie sich immerhin nicht jedes Passwort merken. Trotzdem steigt der Verwaltungsaufwand bei häufigen Passwortwechseln, insbesondere wenn Sie viele Onlinedienste nutzen. Die Zwei-Faktor-Authentifizierung (2FA) sorgt für eine deutliche Verbesserung der Sicherheit bei nur geringen Einschränkungen des Komforts.

So funktioniert die Zwei-Faktor-Authentifizierung

Bei der Zwei-Faktor-Authentifizierung benötigen Sie neben dem Passwort einen weiteren Nachweis, der von einem anderen Gerät oder Medium stammt. Der Vorteil: Das Passwort muss nicht besonders kompliziert sein und wenn es in falsche Hände geraten sollte, dann spielt das kaum eine Rolle. Der Zugang zum Konto wird erst gewährt, wenn Sie sich mit einem zusätzlichen Schlüssel ausweisen. Bei einer 2FA-Anmeldung sollten mindestens zwei der drei folgenden Elemente zum Einsatz kommen:

- Wissen: etwas, das nur der Nutzer weiß (Passwort, PIN)
- Besitz: etwas, das nur der Nutzer besitzt (Mobiltelefon, Kartenlesegerät)
- Inhärenz: etwas, das der Nutzer ist (Fingerabdruck, Gesichtserkennung)

Als „Besitz" kommt beispielsweise eine ausgedruckte Liste, eine SMS, eine Smartphone-App oder ein Nummerngenerator in Betracht. Die Kombination aus „Wissen" und „Besitz" ist am leichtesten umzusetzen, weil dafür nur meist schon vorhandene Hardware nötig ist, etwa ein Smartphone. „Inhärenz" kommt noch selten zum Einsatz, weil die technischen Verfahren etwa bei der Gesichtserkennung noch nicht als völlig ausgereift gelten.

Je nach Konfiguration wird neben dem Passwort der Sicherheitsschlüssel bei jeder Anmeldung oder sicherheitsrelevanten Aktion angefordert oder er gilt dauerhaft für ein bestimmtes Gerät beziehungsweise den verwendeten Browser. Unbefugte Personen, die Ihr Passwort in Erfahrung gebracht haben, benötigen daher in jedem Fall zusätzlich auch noch den Sicherheitsschlüssel. Sie haben Ihr Notebook oder Smartphone verloren oder es wurde gestohlen? Sollte eine fremde Person Zugang zum Gerät erhalten, sind Ihre Onlinekonten in Gefahr, wenn der zweite Faktor nicht mehr abgefragt wird. Einige Onlineanbieter fordern den Sicherheitsschlüssel erneut an, wenn der Internetzugang über einen bisher nicht verwendeten IP-Adressbereich oder aus dem Ausland erfolgt. Darauf verlassen können Sie sich aber nicht. Geht ein mobiles Gerät verloren, sollten Sie schnellstmöglich alle Passwörter ändern.

Absicherung bei Onlinebanking und Shopping

Überweisungen oder Änderungen der persönlichen Daten sind beim Onlinebanking seit langem per Zwei-Faktor-Authentifizierung abgesichert. Zum Einsatz kommen ausgedruckte TAN-Listen, TANs per SMS oder TAN-Generatoren. Hingegen bieten die meisten Banken in Deutschland bisher keine Zwei-Faktor-Authentifizierung bei der

Onlineanmeldung an. Das wird sich aber ab 2019 ändern, weil bis dahin die EU-Richtlinie 2015/2366 wahrscheinlich auch in Deutschland umgesetzt ist. Die Richtlinie will verpflichtend eine „starke Kundenauthentifizierung" beim Onlineshopping oder bei Bankgeschäften einführen. Das Passwort alleine wird dann nicht mehr für den Kontozugriff genügen. Auch Kreditkartenzahlungen sind betroffen, für die in Onlineshops in der Regel die Angaben auf der Kreditkarte ausreichen.

Eine Übersicht mit Banken, Onlineshops und anderen Diensten, die bereits Zwei-Faktor-Authentifizierung anbieten, finden Sie unter *https://twofactorauth.org*.

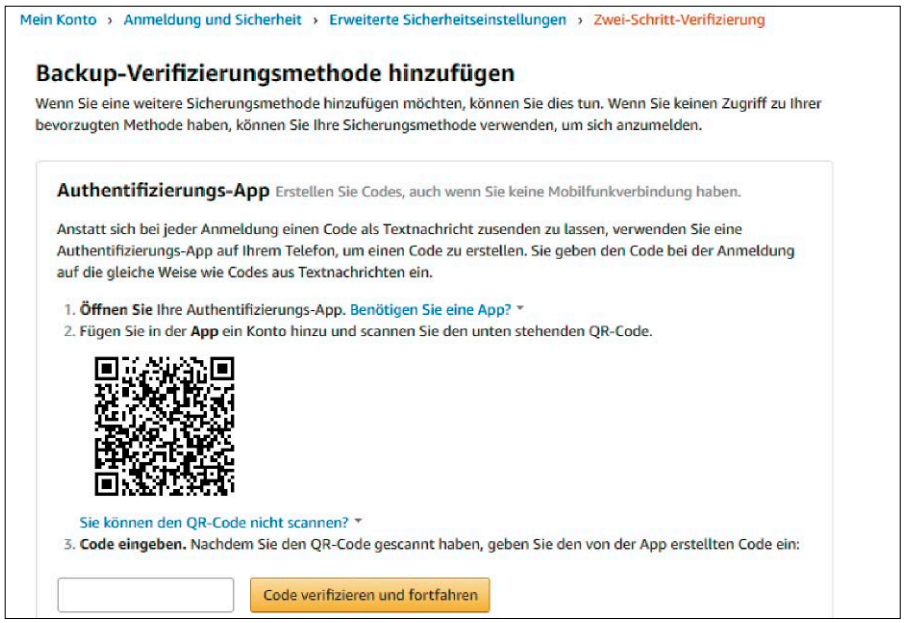
Zwei-Faktor-Authentifizierung bei Webdiensten

Zu den bekannten Webdiensten mit Zwei-Faktor-Authentifizierung gehören Google, Microsoft, Amazon, Dropbox, Facebook, Paypal und Whatsapp.

In den Kontoeinstellungen finden Sie die Optionen dafür meist in Rubriken wie „Sicherheit" oder „Anmeldeeinstellungen" mit Bezeichnungen wie „Bestätigung in zwei Schritten" oder „Zweistufige Überprüfung". In der Regel werden mehrere Verfahren angeboten, etwa SMS und per App generierte Sicherheitsschlüssel. Dazu zwei Beispiele:

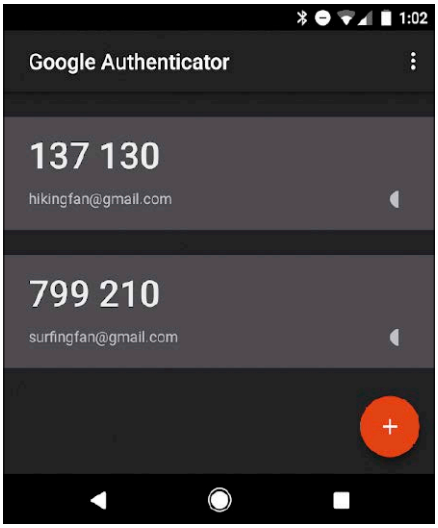
Google: Melden Sie sich bei Google an, öffnen Sie die Webseite *https://myaccount.google.com/security*, klicken Sie auf „Bestätigung in zwei Schritten" und auf „Jetzt starten". Geben Sie das Google-Passwort ein und klicken Sie auf „Weiter". Tippen Sie dann Ihre Telefonnummer ein und wählen Sie die Option „Telefonanruf" (Festnetz) oder „SMS". Nach einem Klick auf „Weiter" geben Sie den Code ein, den Sie erhalten haben, und klicken auf „Aktivieren".

Bestätigungscodes per SMS sind bereits aktiviert. Zusätzlich sollen Sie unter „Authenticator App" auf „Einrichten" gehen, zwischen „Android" und „iPhone" wählen und auf „Weiter" klicken. Installieren Sie die Authenticator App auf Ihrem Smartphone. Den Link zum Play Store beziehungsweise App Store sehen Sie im Fenster. Im Google Authenticator tippen Sie auf „+" und dann auf „Barcode scannen". Scannen Sie den auf dem PC-Bildschirm angezeigten QR-Code. Die App erzeugt etwa alle 30 Sekunden einen neuen Schlüssel, den Sie beim zweiten Schritt der Google-Anmeldung verwenden. Im Browser lassen Sie das Häkchen vor „Auf diesem PC nicht mehr fragen" gesetzt, damit Sie den Schlüssel nicht erneut eingeben müssen.



Code per App generieren: Scannen Sie den QR-Code ein, um das Konto einer Authentifizierungsapp bekannt zu machen. Den erzeugten Code geben Sie zur Bestätigung ein.

Amazon: Melden Sie sich bei Amazon an, gehen Sie auf „Mein Konto" und klicken Sie auf „Anmelden und Sicherheit". Klicken Sie bei „Erweiterte Sicherheitseinstellungen" auf „Bearbeiten" und dann auf „Erste Schritte". Tragen Sie Ihre Festnetz- oder Handynummer ein, wenn Sie die Codes per Telefon erhalten möchten. Alternativ wählen Sie die Option „Authentifizierungs-App", scannen den Barcode mit Google Authenticator (suchen Sie danach im App Store) und tippen dann den in der App angezeigten Code zur Bestätigung ein. Bei der Anmeldung bei Amazon können Sie ein Häkchen setzen vor „In diesem Browser nicht mehr nach Codes fragen". ■



Authentifizierungsapp: Der Google Authenticator benötigt keine Internetverbindung und hilft dabei, SMS-Kosten zu sparen.

PROGRAMME OHNE 2FA-FÄHIGKEIT NUTZEN

Nicht jede Anwendung kann mit der Zwei-Faktor-Authentifizierung umgehen. Mailprogramme wie Thunderbird fragen nur nach dem Passwort, aber nicht nach einem Sicherheitsschlüssel. In diesem Fall benötigen Sie ein eigenes Passwort für das Programm. Bei Google beispielsweise (*https://myaccount.google.com/security*) klicken Sie auf „App-Passwörter" und bei „App auswählen" auf „Andere (benutzerdefinierter Name)". Tippen Sie beispielsweise „Thunderbird auf meinem Linux-PC" ein und klicken Sie auf „Generieren". Sie erhalten ein 16-stelliges Passwort, das Sie bei der Kontoeinrichtung in Thunderbird angeben. Lassen Sie Thunderbird das Passwort speichern, damit Sie es nicht erneut eintippen müssen.

LINUX WELT

Mini-Angebot!

3x LinuxWelt

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

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

Satte **33 %** gespart!

+ BestChoice Gutschein*

oder 10,- € Geldprämie**

Jetzt testen:

3 x LinuxWelt als Heft frei Haus mit Gratis-DVD +

3 x LinuxWelt direkt aufs Smartphone & Tablet mit interaktivem Lesemodus +

10,- € BestChoice- oder BestChoice Entertainment-Gutschein* oder 10,- **€** Geldprämie**

=17,- € **(33 % gespart!)**

Jetzt bestellen unter

www.pcwelt.de/linuxwelt oder per Telefon: 0711/7252233 oder ganz einfach:

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

Ja, ich bestelle das LinuxWelt Mini-Angebot für 17,- € und erhalte 3 Ausgaben inkl. Prämie

○ BestChoice-Gutschein ○ BestChoice Entertainment-Gutschein ○ 10,- € Prämie

Möchten Sie die LinuxWelt anschließend weiter lesen, brauchen Sie nichts zu tun. Sie erhalten die LinuxWelt für weitere 6 Ausgaben zum aktuellen Jahresabopreis von z.Zt. 51,- EUR. Danach ist eine Kündigung zur übernächsten Ausgabe jederzeit möglich.

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

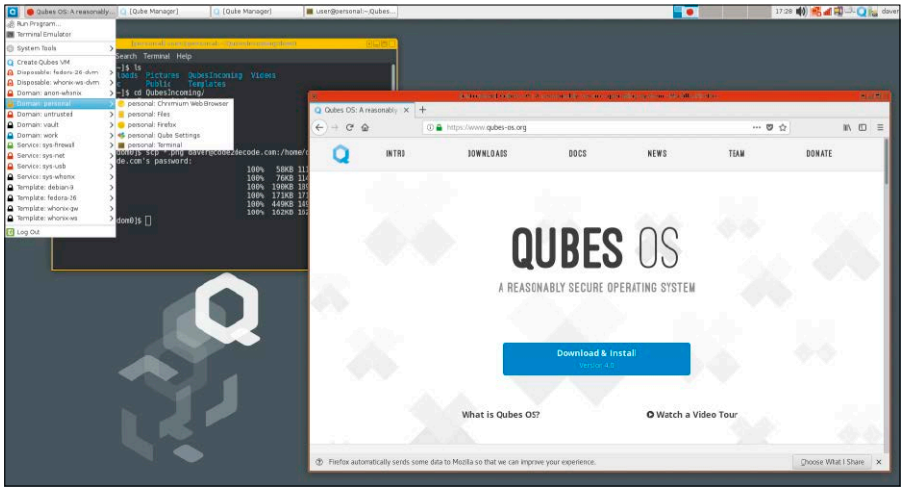
LWPM062018

*die BestChoice Gutscheine werden per Mail an den Kunden geschickt sobald die Zahlung eingegangen ist. ** wird mit Abo-Preis verrechnet

Qubes-OS: Supersicher mit Xen

Ein bemerkenswerter Vertreter unter den Linux-Distributionen, die sich dem Thema Sicherheit verschrieben haben, ist Qubes-OS. Es arbeitet mit der Virtualisierung von Xen, um einzelne Anwendungen in abgeschottete Container zu sperren.

VON DAVID WOLSKI



Der Desktop in Qubes-OS: Was aussieht wie eine fast normale XFCE-Oberfläche, beherbergt eine Paravirtualisierung mit Xen, die Programme in abgeschotteten Domänen startet („Qubes“).

Als besonders sichere Maßnahme hat sich im Alltag die strikte Trennung von Systemen und deren Anwendungen nach ihren Einsatzbereichen erwiesen: Auf privaten Systemen, auf denen man eventuell etwas mehr Dinge „anstellt“, laufen in der Regel keine hochwichtigen Programme mit nicht mehr beizubringenden Daten. Doch gut abgeschottete Systeme werden sich, auch nach Bedienfehlern, Nachlässigkeiten, missglückten Experimenten oder Hacks, gegenseitig weniger gefährlich. Zwar ist diese stringente Trennung und Abschottung von physikalischen Systemen nach ihren verschiedenen Einsatzzwecken eine einleuchtende Sicherheitsmaßnahme – aber auch reichlich umständlich in der Realisierung. Für jeden Anwendungsbereich ein eigenes Notebook oder einen separaten PC zu verwenden, erscheint wenig praktikabel. Im Alltag ist es dann doch zumeist so, dass man auf einem Arbeitsrechner auch mal persönliche Dokumente öffnet, sodass sich Privates und Geschäftliches vermischen.

Abschottung mit Xen

Komfortabler gelingt die Abschottung von Systemen und deren Anwendungen mittels Virtualisierung. Ein leistungsstarker PC kann mit einem Programm wie Virtualbox mehrere virtuelle Maschinen gleichzeitig stemmen. Sicherheitsbewusste Anwender haben so mehrere separate Systeme auf ihrem Rechner, brauchen aber nicht mit unterschiedlicher Hardware zu hantieren, sondern haben immer noch alles auf einem Rechner und Bildschirm. Diesen Ansatz greift das Linux-System Qubes-OS auf, das mit der Virtualisierungstechnik Xen arbeitet, die eng mit dem Linux-Kernel verzahnt ist und deren Entwicklung unter der Ägide der Linux Foundation steht. Xen ist kein kompletter Virtualisierer wie beispielsweise Vmware oder Virtualbox, sondern betreibt eine Paravirtualisierung.

Anders als bei der Komplettvirtualisierung bildet die Paravirtualisierung kein komplettes System mit virtueller Hardware ab. Qubes-OS nutzt den effizienten Ansatz mit Xen, um Anwendungen in ihrer eigenen Xen-Maschine (genannt „Xen-Domäne“ oder einfach „Qube“ in Qubes-OS) laufen zu lassen und auf einem Desktop nahtlos nebeneinander darzustellen.

Sichere und unsichere Domänen

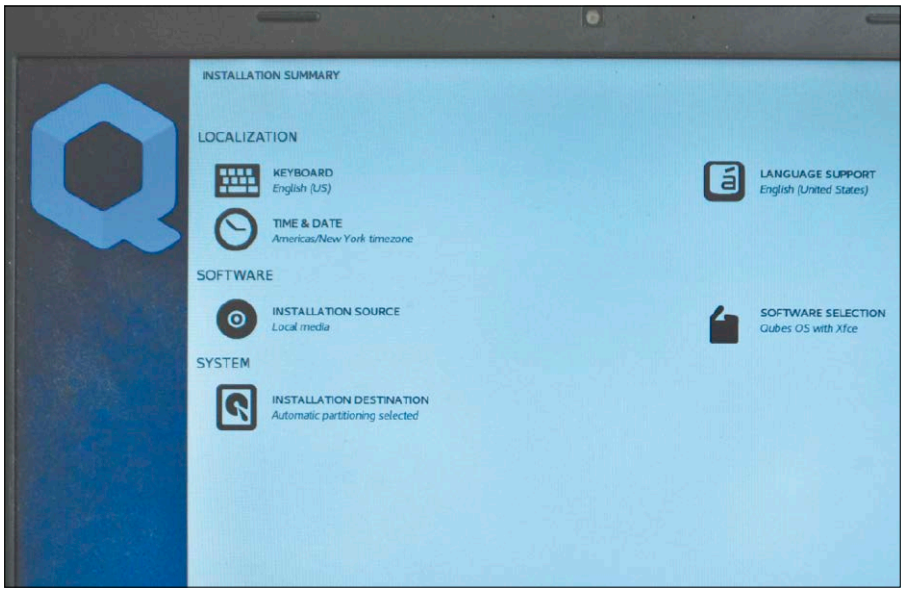
In Qubes laufen nicht alle Anwendungen in ihrer eigenen Xen-Domäne, denn das wäre eine übertriebene Maßnahme. Stattdessen liefert Qubes-OS mehrere vorkonfigurierte Domänen mit, die diverse Anwendungen nach Aufgaben zusammenfassen. So gibt es Xen-Domänen für die Arbeit, für Privates und für definitiv unsichere Tätigkeiten gibt es Wegwerf-Domänen, die generell keine Benutzerdaten speichern. Zur Abschottung voneinander erhalten die Domänen ein eigenes Dateisystem sowie eine eigene IP-Adresse in einem virtuellen Netzwerk unter Qubes, das die Domänen über NAT bei Bedarf ans eigentliche Netzwerk anbindet. Dabei kann Qubes verschiedene Netzwerkadapter nutzen, um beispielsweise eine Domäne mit einem Firmennetzwerk über Ethernet zu verbinden und eine andere per WLAN in ein privates Netzwerk einzuloggen. Firewallregeln gibt es getrennt für jede einzelne Domäne. Die Kommunikation zwischen Domänen ist damit eingeschränkt

und kontrolliert. Auch Dateien können nicht direkt zwischen Domänen ausgetauscht werden, sondern nur über einen externen Dateiserver oder über ein internes, von Qubes bereitgestellten Transfertool.

Fedora im Hintergrund

Das Management von Xen ist komplex und wäre auf Desktopsystemen mit den Linux-Bordmitteln allein überaus umständlich. Deshalb liefert Qubes einige hilfreiche grafische Verwaltungstools mit, die den Start und das Erstellen von Xen-Domänen erleichtern. Außerdem gibt es so eine einfachere Möglichkeit, Domänen mit PCI-Geräten per PCI-Passthrough zu verbinden oder einen Netzwerkadapter verfügbar zu machen. Die übergreifende Xen-Domäne (dom0) dient nur zur Verwaltung aller Xen-Domänen und des Basissystems, aber nicht zur eigentlichen Arbeit, damit das Basissystem immer isoliert von den Anwendungen bleibt.

Qubes-OS erschien erstmals 2012 und wurde von der bekannten VM-Spezialistin und Hackerin Joanna Rutkowska ins Leben gerufen. Schnell fanden sich rund ein Dutzend Mitstreiter, die das System heute weiterentwickeln. Es wurde 2014 für den „Access Innovation Price" 2014 nominiert und hat von Berufsparanoikern wie Edward Snowden viele Lorbeeren bekommen. Mittlerweile liegt Qubes-OS in Version 4.0 vor und lädt zum Ausprobieren und Experimentieren ein. Das Basisbetriebssystem mit der übergreifenden Xen-Domäne baut auf Fedora auf, bringt aber auch Domänen mit einem Debian-Gastsystem mit. Als Desktop kommt ein schlichtes englischsprachiges XFCE zum Einsatz.



Das Installationsprogramm: Qubes-OS basiert auf einer älteren Ausgabe von Fedora und übernimmt dessen Installer. Dieser überprüft die Kompatibilität der CPU mit Qubes-OS.

Installation: Keine kleine Hürde

Der Weg zur Installation beginnt mit dem Download der ISO-Datei von *https://www.qubes-os.org/downloads* (4,3 GB), die auf eine DVD oder einen USB-Stick ab acht GB Kapazität passt. Zur Übertragung eignet sich das Linux-Kommandozeilentool dd, die Installation ist unter *https://www.qubes-os.org/doc/installation-guide* im Detail be-

QUBES-OS 4.0: DIE VORAUSSETZUNGEN

Als überaus wählerisch zeigt sich Qubes-OS 4.0 bei der Installation, die schon aufgrund der Hardwarevoraussetzungen keine leichtzunehmende Hürde ist.

Aus diesem Grund haben die Entwickler unter *https://www.qubes-os.org/hcl* eine tabellarische Übersicht mit getesteter Hardware als erste Orientierung veröffentlicht. Ein Überblick zu den Anforderungen:

Generell: In Sachen Hardwareanforderungen ist Qubes-OS kein Leichtgewicht. Xen ist eine Linux-Technologie aus dem Serverbereich – an RAM und CPU-Leistung gibt in diesem Anwendungsbereich wenig Mangel. Entsprechend großzügig sollte die Hardwareausstattung eines Test-PCs für Qubes-OS sein. Dabei ist aber auch darauf zu achten, dass die Hardware nicht zu neu ist. Auf einem brandneuen System mit Intels achter Core-i7-Generation gab es Probleme mit der Hardwareerkennung. Besser geeignet sind etwas ältere, leistungsfähige Rechner der letzten drei bis fünf Jahre.

Speicher: acht GB Minimum

Festplattenplatz: 30 GB Minimum, schnelle SSD empfohlen

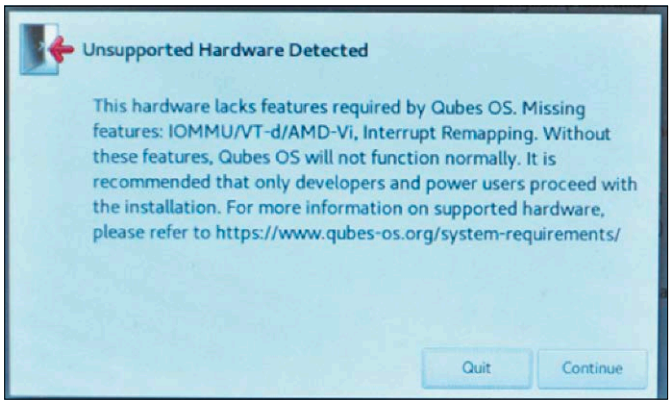
Prozessor: leistungsfähige CPU ab vier Kernen und Virtualisierungserweiterungen (Intel-VT-x, AMD-V)

Keine virtuellen Maschinen: In einer virtuellen Maschine läuft Qubes prinzipiell gar nicht oder doch nur sehr eingeschränkt, weil Qubes-OS mit Xen-Domänen arbeitet.

Diese Virtualisierungsmethode verlangt nach exklusivem Zugriff auf den Prozessor und die Hardware, denn eine verschachtelte Virtualisierung mit Xen unter einer VM ist schwierig zu realisieren. Mit Virtualbox funktioniert es gar nicht, mit Vmware Workstation und Player kann die Installation funktionieren, aber es sind weitere Probleme mit dem Netzwerkzugriff zu erwarten. Qubes-OS ist für einen speziell dafür geeigneten, leistungsfähigen PC gemacht, eine Installation auf eine extern angeschlossene SSD/Festplatte ist dank des flexiblen, von Fedora übernommenen Installers möglich und zum Einstieg empfehlenswert.

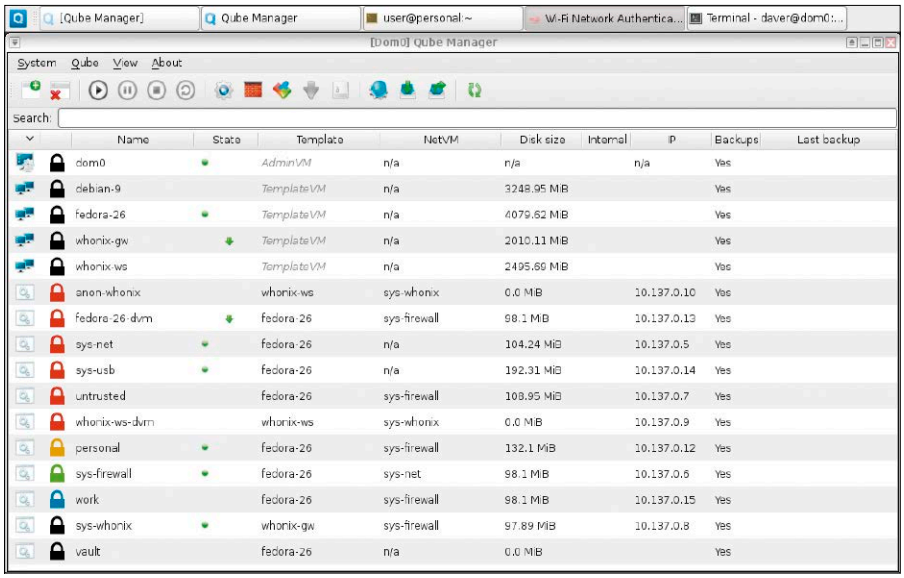
Download: Die ISO-Datei zur Übertragung auf einen USB-Stick ab acht GB Speicherplatz liegt unter *https://www.qubes-os.org/downloads* zum Download bereit (4,3 GB). Das installierbare System ist kein Livesystem, sondern startet den Fedora-Installer Anaconda in englischer Sprache.

Dokumentation: *https://www.qubes-os.org/faq*



Keine Installation möglich: Qubes-OS ist wählerisch bezüglich der Hardware, auf der es laufen will. Diverse Virtualisierungserweiterungen moderner CPUs sind Voraussetzung.

Netzwerk verbinden: Erst nachdem ein physikalischer Netzwerkadapter der Domäne „sys-net" zugewiesen ist, kann das System über das Symbol rechts oben ins Netzwerk.



Schaltzentrale: Der Qube Manager ist eine grafische Anwendung im Stil eines Taskmanagers, der alle vorhanden und laufenden Domänen anzeigt, startet, anhält und verbindet.

schrieben. Nach dem Booten auf dem ausgewählten Rechner startet Qubes-OS kein Livesystem, sondern einen Installer, der in weiten Teilen von Fedora 25 übernommen ist. Weil Qubes selbst mit Virtualisierung arbeitet, verlangt das System nach realer, leistungsfähiger Hardware. Diese muss zudem einige anspruchsvolle Voraussetzungen erfüllen (siehe Kasten „Qubes-OS 4.0: Die Voraussetzungen"), wobei man immerhin bei der Installation nicht lange rätseln muss. Der Installer spuckt umgehend eine Fehlermeldung aus, wenn die gewählte Hardware ein zwingend benötigtes Merkmal nicht mitbringt. Auf dem Datenträger verlangt das System mindestens 32 GB, wobei es sich empfiehlt, schon im Vorfeld mit dem Partitionierer Gparted Platz zu schaffen, weil der Partitionierer des Installationsprogramms reichlich umständlich zu bedienen ist. Nach der Auswahl der Zielfestplatte unter „Installation destination" erstellt ein Klick auf „Begin Installation" das Standard-Partitionslayout, das übrigens mit Luks-Verschlüsselung der Datenträger arbeitet und die Vergabe eines Passworts zum Systemstart verlangt. Während die Installation läuft, erstellt man noch unter „User creation" einen Benutzer und dessen Passwort zur Anmeldung am System. Nach dem ersten Booten fragt das System, welche Standarddomänen es erstellen soll. Für den Einstieg können Sie einfach die Vorauswahl übernehmen.

Erster Start und Orientierung

Qubes-OS präsentiert dem Anwender einen XFCE-Desktop, in dessen Anwendungsmenü links oben allerdings keine Anwendungen im Vordergrund stehen, sondern die vorkonfigurierten Xen-Domänen („Qubes"). Unterhalb jedes der Qubes klappen sich die darin vorhandenen aufrufbaren Programme aus. So finden sich beispielsweise unterhalb von „Domain: personal" die Einträge für den Firefox-Browser, den Dateimanager und das Terminal. Ein Klick darauf startet diese Xen-Domäne und das darin aufgerufene Programm – mit einem farbigen Fensterrahmen deutlich von anderen Programmen in den fremden Domänen abgesetzt.

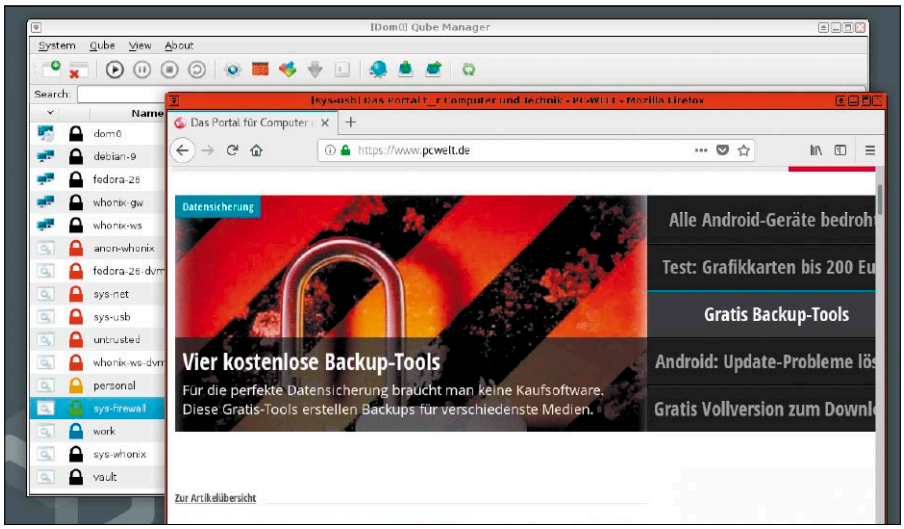
Bevor man etwa in Firefox in einer der Domänen loslegen kann, gilt es aber erst, für Netzwerkkonnektivität zu sorgen. Das ist keine triviale Aufgabe, denn Netzwerke sind für Qubes-OS grundsätzlich ein Einfallstor für Risiken von außen. Das Networkmanager-Icon rechts oben in XFCE ist deshalb auch nicht der richtige Weg ins Netzwerk. Stattdessen läuft die Netzwerkverbindung nur in die Xen-Domäne „sys-net", die das Netzwerk dann wiederum über „sys-firewall" oder direkt an eine der anderen Domänen weitergibt. Dieses Zusammenspiel wird klarer, wenn man den „Qube Manager" über „System Tools" im Anwendungsmenü startet. Die tabellarische Übersicht im Stil eines Taskmanagers zeigt die verfügbaren Qubes, deren Namen, den Status sowie in der Spalte „NetVM" de-

ren Netzwerkverbindung untereinander. Um jetzt die Domäne „sys-net“ ins Netzwerk zu bringen, klicken Sie diese im Qube Manager rechts an und wählen „Qube settings“. Unter „Devices“ wählen Sie links unter den PCI-Geräten den gewünschten Netzwerkadapter aus und befördern diesen mit dem Pfeil-Symbol in das rechte Feld „Selected“. Umgekehrt wirft der umgekehrte Pfeil unerwünschte PCI-Geräte aus der Spalte „Selected“ wieder heraus. Nach einem Klick auf „OK“ startet im Qube Manager der Kontextmenüeintrag „Restart qube“ die Domäne „sys-net“ neu. Erst dann kann das Netzwerksymbol in der XFCE-Systemleiste die Verbindung konfigurieren.

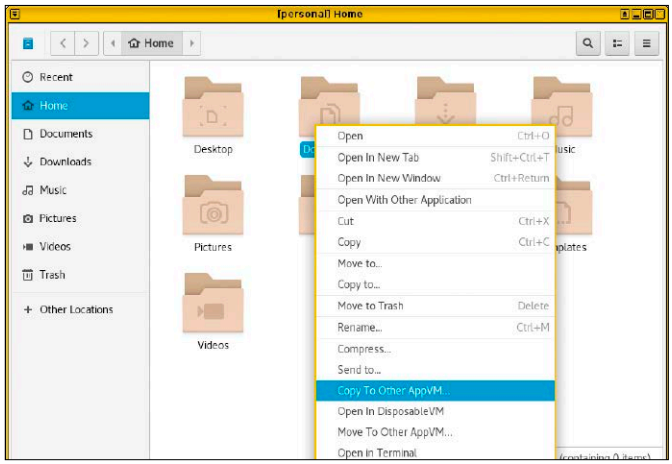
Domänen und Programme

Ein dann gestartetes Programm, beispielsweise ein Firefox in „Domain:personal“, hat nun die Internetverbindung. Diese Domäne merkt sich auch solche Änderungen und speichert Dateien in ihrem eigenen Dateisystem. Zur Arbeit mit Dateien dient in der „Domain:personal“ der Eintrag „personal: Files“. Dieser startet nicht den gewöhnlichen Dateimanager, sondern eine modifizierte Variante, die bei einem Rechtsklick auf Dateien und Ordner die Punkte „Copy to Other AppVM“ und „Move to Other AppVM“.anzeigt. Nur über diese Programmpunkte können Dateien in andere laufende Domänen kopiert beziehungsweise verschoben werden. Dort landen die Dateien stets im Unterverzeichnis „QubesIncoming“. Für den Anschluss eines USB-Sticks gibt es die Domäne „sys-usb“, zu der man Dateien erst transferieren muss und dann erst auf das USB-Laufwerk bekommt.

Neben den festen Domänen gibt es Einwegtemplates, die bei Bedarf eine frische Domäne erstellen und beim Schließen wieder komplett löschen. Diese Domänen finden sich im Anwendungsmenü unter „Disposable: fedora-26-dvm“ und „Disposable: whonix-ws-dvm“. Dort steht auch ein vorkonfigurierter TOR-Browser zur Verfügung. Zwar ist die Auswahl der vorinstallierten Programme nicht gerade üppig, aber doch bei Bedarf erweiterbar. Xen-Domänen selbst sind nicht direkt veränderbar, wohl aber deren Templates, die das virtuelle Dateisystem enthalten. Um beispielsweise „Domain:personal“ mit dem Chromium-Browser zu erweitern, starten Sie im Anwendungsmenü erst „Template:fedora-26 → fedora-26:Terminal“ und geben dort



Abgeschotteter Firefox: Geöffnete Programmfenster auf dem Desktop bekommen stets eine Rahmenfarbe, welche die Domäne signalisiert.



Aufgebohrter Dateimanager: Der Datenaustausch zwischen den virtuellen Domains ist nur über spezielle Kontextmenüs im Thunar-Dateimanager möglich.

`sudo dnf install chromium`

ein. Nach der Installation wartet die „Domain: personal“ im Qubes Manager per Rechtsklick und „Restart Cube“ auf ihren Neustart, um ihr Dateisystem zu aktualisieren. Soll Chromium im Anwendungsmenü auftauchen, geht man im Kontextmenü auf „Qube Settings → Applications“ und holt dort mit dem Pfeilsymbol den Eintrag „Chromium Web Browser“ in die rechte Spalte.

Die Betriebssysteme in den Templates müssen regelmäßig aktualisiert werden. Dazu klicken Sie ein Template im Qube Manager rechts an und wählen „Update qube“.

Fazit: Sicherheit mit hohem Aufwand

Eine Binsenweisheit aus dem Umfeld der IT-Sicherheit besagt, dass Komfort im umgekehrten Verhältnis zur tatsächlichen Sicherheit steht. Leider ist auch Qubes-OS hier keine Ausnahme von dieser Regel. Wer das System wirklich produktiv einsetzen will, muss bereits über einen soliden Wissensstand zur Xen-Paravirtualisierung mitbringen. Eine hohe Hürde ist, dass Qubes-OS extrem wählerisch bezüglich der Hardware ist, mit der es ausschließlich zusammenarbeiten kann. Eine Menge offener Bugs in der aktuellen Version Qubes-OS 4.0 versprechen zudem intensive Recherchen nach Lösungen auf der Projektwebseite, wobei die meisten Bugs im Zusammenspiel mit Hardware- und Bios-Problemen auftreten. Als Experimentalsystem ist Qubes-OS für eine Gruppe bewanderter Linux-Anwender ein interessanter Blick auf Xen. Normalsterbliche werden sich weiterhin mit virtuellen Maschinen in Virtualbox oder Vmware leichter tun, da diese weitaus intuitiver bedienbar sind als Qubes-OS. ■

Manjaro Linux: Eine echte Alternative

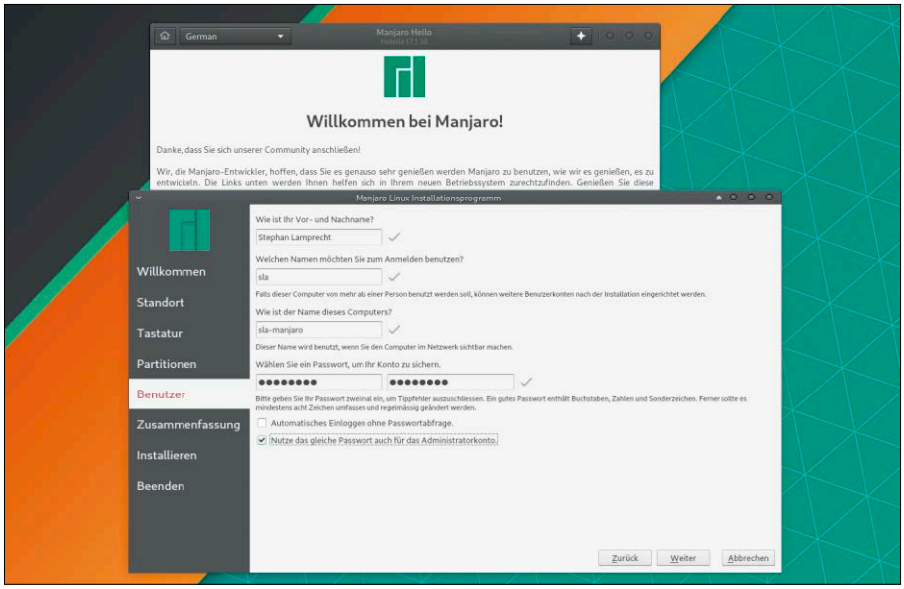
Auch Linux-Distributionen sind Moden unterworfen. So wurde dem einst in Deutschland herrschenden Suse Linux von Ubuntu der Rang abgelaufen. Neuerdings avanciert laut Distrowatch Manjaro Linux zur beliebtesten Distribution.

VON STEPHAN LAMPRECHT

Viele Entscheidungen der Ubuntu-Entwickler haben die Anwender etwas ratlos zurückgelassen. War die Unity-Oberfläche noch eher kosmetischer Natur, hat der Wechsel zu einem eigenen Init-System Administratoren vor erhebliche Herausforderungen gestellt. Das führte in der Konsequenz dazu, dass die Nutzer sich nach Alternativen umsehen – und immer häufiger bei Manjaro Linux landen. Einer der wesentlichen Vorteile von Arch Linux und damit auch von Manjaro liegt darin, dass es sich um ein Rolling Release handelt. Andere Distributionen machen vor der Veröffentlichung einen harten Schnitt bei den mitgelieferten Paketen.

Das birgt die Gefahr, dass dann die Programme bei der Veröffentlichung der Distribution bereits veraltet sind. Bei einem Rolling Release ist das nicht der Fall. Die Software ist sozusagen ganz nebenbei immer auf dem aktuellsten Stand.

Manjaro basiert auf Arch, das auf dem Linux-Desktop eine untergeordnete Rolle spielt. Arch ist schlank und nicht nur bei der Installation schnell, stellt aber Einsteiger vor erhebliche Hürden, da sich viele Einstellungen nur auf der Befehlszeile erledigen lassen. Und mit dem Terminal stehen Anfänger in aller Regel auf dem Kriegsfuß. Manjaro erleichtert den Arch-Einstieg durch einen grafischen Installer à la Ubuntu.



Manjaro-Installer: Anders als bei purem Arch Linux führt ein grafischer Assistent den Benutzer durch den Einrichtungsprozess. Probleme sind hier keine zu erwarten.

Eine nahezu perfekte Installation

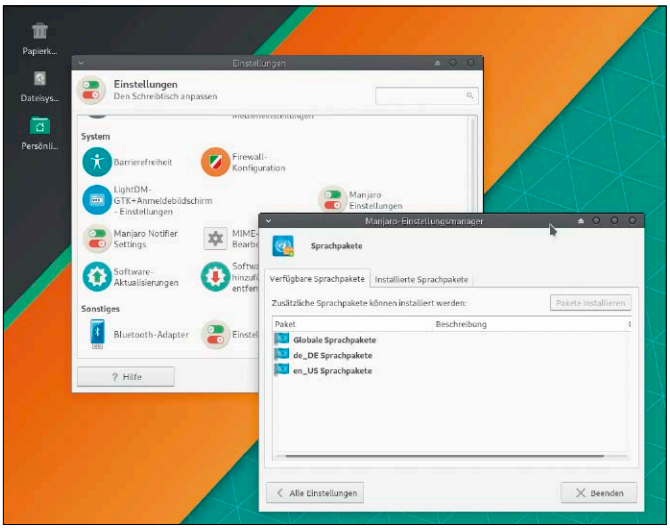
Auf der Webseite des Projekts (*https://manjaro.org/*) finden Sie unter „Download" die Distribution in mehreren Varianten. Die offiziellen Manjaro-Editionen bieten die Desktopumgebungen XFCE, KDE und Gnome. Community-Editionen erweitern das Angebot um Cinnamon, Mate, Budgie, LXDE, um nur die wichtigsten zu nennen. Von der auf DVD oder USB kopierten ISO-Datei starten Sie dann Ihren Computer.

Der Dialog des Bootmanagers erfordert etwas Umsicht. Achten Sie darauf, dass Sie mit den Pfeiltasten sowohl die deutsche Tastenbelegung als auch die deutsche Sprache für die Oberfläche auswählen. Mit einem Druck auf die Eingabetaste startet das System dann durch. Dies war dann auch schon der komplizierteste Schritt während des Einrichtungsprozesses. Direkt über den Begrüßungsdialog erreichen Sie den grafischen Installer des Systems.

Das Prozedere unterscheidet sich kaum von einer Ubuntu-Installation. Nach der Auswahl von Sprache und Zeitzone muss die Tastaturbelegung definiert werden. Dann folgt die Partitionierung. In diesem Dialog können Sie auch die (Luks-)Verschlüsselung der gesamten Festplatte aktivieren. Eine letzte Besonderheit gibt es bei der Anlage des Benutzers. Denn dort tragen Sie nicht nur den Benutzernamen und das Passwort ein, sondern haben die Wahl, ein abweichendes Kennwort für den Zugriff auf Admin-Rechte einzutragen. Es folgt die Zusammenfassung der gewählten Optionen und die Einrichtung des Systems beginnt.

Unmittelbar nach dem Start wird Sie das System über neue Updates informieren. In der Übersicht der Aktualisierungen mar-

kieren Sie entweder alle Einträge oder wählen gezielt einzelne Pakete aus, um diese auf den neuesten Stand zu bringen. Ist dieser Schritt abgeschlossen, ist es außerdem zu empfehlen, noch fehlende Sprachpakete zu installieren. Klicken Sie dazu auf die Menüschaltfläche mit dem Manjaro-Symbol und wechseln Sie anschließend in den Bereich „Einstellungen". Dort finden Sie das Programm „Einstellungen" und hier wiederum die „Manjaro-Einstellungen". Im nachfolgenden Fenster markieren Sie unter „Sprachpakete" den Eintrag „Deutsch". Das hat den Vorteil, dass auch andere Anwendungen, zum Beispiel Firefox oder Thunderbird mit deutschsprachiger Oberfläche starten.



Erste Schritte nach der Installation: Ratsam ist die sofortige Nachrüstung der weiteren Sprachpakete. Dann sind wichtige Programme ebenfalls deutsch lokalisiert.

Pralles Softwareangebot

Zur Beliebtheit von Manjaro trägt das Archtypische, umfangreiche Softwareangebot bei. Dessen Besonderheit besteht darin, dass es für Entwickler besonders einfach ist, die Anwendungen zu aktualisieren. Daher ist die Software in den Paketquellen von Manjaro respektive Arch Linux in der Regel aktueller als bei anderen Distributionen. Während Sie bei Ubuntu unter Umständen noch eine Betaversion über eine externe Paketquelle einbinden müssen, steht in Arch vielleicht schon die finale Version zur Verfügung. Unmittelbar nach der Installation enthält Manjaro alles, was zum Arbeiten und zur Internetnutzung notwendig ist. Gearbeitet wird mit Libre Office, als Browser ist Firefox an Bord, für Mails Thunderbird und auch Gimp für die Fotobearbeitung ist bereits installiert. Das ist nicht ungewöhnlich, aber es gibt auch Überraschungen: In der Rubrik „Büro" sind auch die Onlineausgabe von MS Office sowie Skype vorhanden. Spieler werden sich darüber freuen, dass es auch einen Eintrag für „Steam" gibt.

Manjaro verwendet weder das von Debian und Ubuntu bekannte Deb-Format noch das RPM-Format für seine Pakete. Über „Software hinzufügen / entfernen" greifen Sie auf einen grafischen Paketmanager zu. Die Pakete sind in thematische Kategorien unterteilt. Über die Suchfunktion finden Sie rasch, was Sie brauchen.

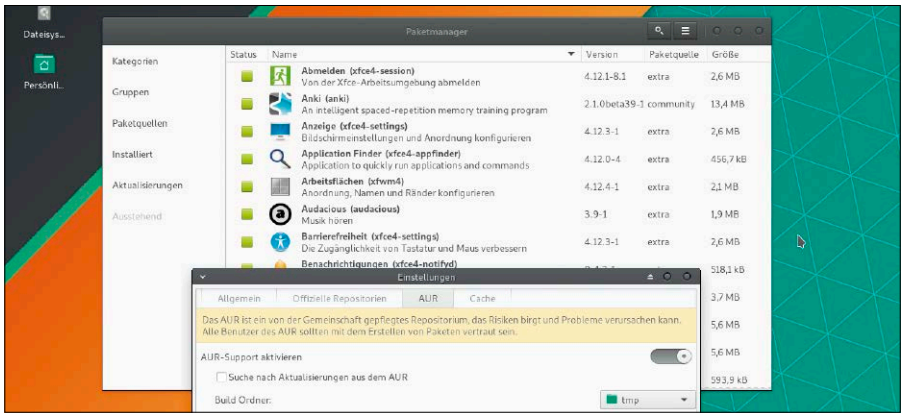
Flink und stimmig, aber kein echtes Arch

Manjaro ist eine überzeugende Distribution. Als Empfehlung darf die schlanke Variante mit dem XFCE-Desktop gelten. Alles greift ineinander und der Umstieg von anderen Linux-Varianten fällt leicht.

Das ergibt in der Summe ein stimmiges und wirklich flottes System, das auch der Hardware aus der Vorsaison eine zweite Chance gibt. Dank des Rolling-Release-Modells bleibt das System stets auf dem neuen Stand. Die von anderen Distributionen bekannte „Upgrade"-Prozedur auf die nächste Version und damit auf neuere Programme entfällt.

Eine für fortgeschrittene Nutzer interessante Funktion verbirgt sich im Paketmanager. Mit einem Klick auf die Menüschaltfläche können die „Einstellungen" geöffnet werden. Dort gibt es ein Register mit der Bezeichnung „AUR" - die „Arch User Repositories". Diese erweitern die Zahl der Programme noch einmal und bieten auch Zugriff auf brandaktuelle Versionen. Hinter einem solchen Repository stecken aber keine fertigen Pakete. Im Kern handelt es sich um Bauanleitungen, aus denen der Paketmanager entnehmen kann, welche Komponenten er benötigt, um die Anwendung aus dem Quellcode zu kompilieren. Wie jeder Ikea-Kunde indes weiß, kann jede noch so gute Anleitung etwas tückisch sein. Deswegen sollten diese Quellen wirklich nur Anwender freischalten, die so tief in die Linuxwelt eingetaucht sind, dass sie mit Rückmeldungen des Systems auch etwas anfangen können.

Die AUR-Repositories sind eigentlich für Arch gedacht. Die Pakete sind zwar brandaktuell, können aber mit anderen Bibliotheken unerwünschte Nebenwirkungen auslösen. Manjaro erleichtert den Einstieg, vermittelt aber wenig Wissen über die inneren Zusammenhänge des Systems. Die Manjaro-Community ist freundlich und hilfsbereit, aber bei Bauproblemen oder der Einrichtung wenig verbreiteter Anwendungen muss der Nutzer die Bereitschaft und das Wissen mitbringen, sich selbst zu helfen. ■



Paketquellen „Arch User Repositories": AUR sollten nur die Anwender aktivieren, die sich mit Linux auskennen und denen die umfangreiche Softwareauswahl nicht ausreicht.

Datenschutz mit Veracrypt

Truecrypt und der Nachfolger (Fork) Veracrypt sind faszinierende Verschlüsselungssoftware und beste Wahl für mobile Rechner und Datenträger. Dieser Beitrag erklärt den Umgang und plädiert für das KISS-Prinzip („Keep it simple, stupid“).

VON HERMANN APFELBÖCK

Die jüngsten Versionen von Ubuntu und allen Abkömmlingen haben die Nachfrage nach einer zuverlässigen Verschlüsselungssoftware wieder schlagartig erhöht. Seit das Home-Verzeichnis nicht mehr standardmäßig ab Installation durch Ecryptfs geschützt werden kann, muss vor allem auf mobilen Notebooks eine Alternative her. Auch USB-Datenträger, die persönliche Daten enthalten und viel unterwegs sind, brauchen Verschlüsselungsschutz. Der Truecrypt-Nachfolger Veracrypt ist hierfür allererste Wahl.

Veracrypt im Kurzporträt

Veracrypt ist Open-Source-Software und kann daher keine geheimen Hintertüren für Geheimdienste verbergen. Es eignet sich für große und sehr große Datenmengen, allerdings nicht für den Transfer in die Cloud, da auch bei geringen Datenänderungen immer der Transport eines gesamten Volumes („Container“) notwendig wäre. Die Verschlüsselungstechniken und nebenbei auch die Benutzeroberfläche stehen überwiegend auf der Basis des eingestellten Vorgängers Truecrypt, der als praktisch unüberwindbar eingestuft wurde. Das mysteriöse Ende von Truecrypt im Jahr 2014 wurde damals mit angeblichen Sicherheitslücken begründet, die jedoch nie nachgewiesen wurden. Dies lässt bis heute Gerüchte blühen, dass Truecrypt keineswegs fehlerhaft, sondern im Gegenteil zu gut war, um noch länger von staatlicher Exekutive und/oder Wirtschaft geduldet zu werden. In der Tat geht der Anspruch von Truecrypt und dem Nachfolger Veracrypt deutlich über so harmlose Datenschutzmotive hinaus, Mitarbeiteradressen oder Gehaltstabellen zugriffssicher zu verschlüsseln. Truecrypt/Veracrypt haben das Potenzial, auch die Daten von strafrechtlich oder politisch Verfolgten zu schützen, die mit professionellen Computerforensikern als Gegner rechnen müssen.

Für „normale“ Nutzer mit legitimen Ansprüchen auf Privatsphäre ist diese Komplexität von Veracrypt durchaus ein Problem: Container, Volume, Partition, Standard/Versteckt, Verschlüsselungsalgorithmus, Hash-Algorithmus, Passwort, PIM, Keyfiles, Dateisysteme, Headerdaten, Cachedaten – das sind anspruchsvolle und in Veracrypt überall präsente Begriffe.

Da muss man erst den Überblick gewinnen, was nun wirklich relevant ist oder doch eher in die Paranoia-Ecke gehört. Der Nutzer sollte sich auf das für ihn Notwendige konzentrieren. Wer mit Veracrypt-Optionen leichtfertig spielt, erzielt schnell maximalen Datenschutz – indem er sich selbst aussperrt.

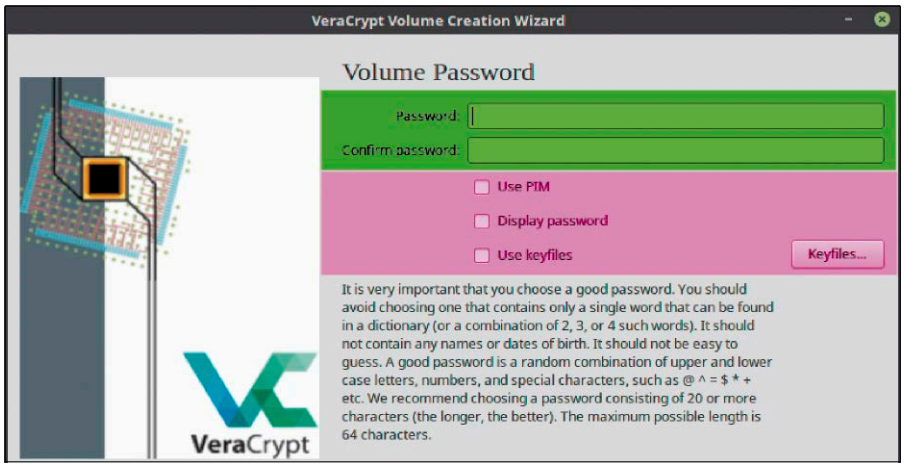
Wie jede Software ist auch Veracrypt nicht fehlerfrei. 2016 wurde ein Bug bekannt, durch den sich versteckte Volumes nachweisen lassen (zu versteckten Volumes siehe gleichnamigen Kasten). Dieser Bug ist seit Version 1.18a behoben, aktuell ist Version 1.22. Eine weitere Anfälligkeit ist akademisch und betrifft außerdem ausschließlich die Komplettverschlüsselung von Festplatten oder sogar der Systempartition (nur in der Windows-Variante). Die theoretische Lücke kann bei physischem Zugriff einer Fremdperson nach einer Speicheranalyse die Passwortlänge preisgeben.

Weitere theoretische Angriffsszenarien sind nicht spezifisch, sondern gelten generell für jedes kryptografische Verfahren: Die Kennworteingabe kann auf kompromittierten Rechnern durch Keylogger bespitzelt werden. Ferner beherrschen Forensiker Kaltstartattacken, bei welchen nach einem Neustart mit einem Minimalsystem der RAM-Speicher ausgelesen wird, der für kurze Zeit noch den gesamten Inhalt inklusive Kennwörter preisgeben kann.

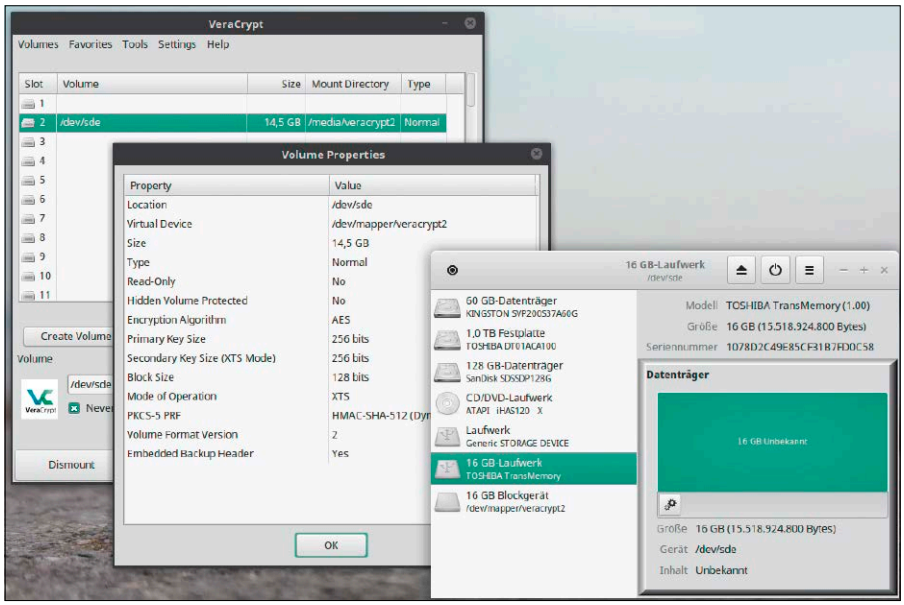
Noch zwei allgemeine Hinweise:

1. Der Einsatz von Veracrypt erfordert immer wieder Geduld: Das Laden („Mount"), mehr noch das Entladen („Dismount") ist häufig zäh, sollte Sie aber keinesfalls veranlassen, den Vorgang durch ein „Auswerfen" des Datenträgers mit Betriebssystem-Werkzeugen oder durch schlichtes Abziehen eines USB-Mediums zu unterbrechen.

2. Beim Hantieren mit Veracrypt-Containern werden Sie zusätzlich zum Containerpasswort auch nach dem sudo-Kennwort gefragt werden, das mit dem Veracrypt-Passwort nichts zu tun hat und vermutlich anders lautet.



Im Veracrypt-Assistenten: Anfänger sollten sich an die einfachen Optionen halten, Standards übernehmen und elaborierte Möglichkeiten erst mal ignorieren (hier „PIM" und „Keyfiles").



Verschlüsselter USB-Stick: Das Systemtool Gnome-Disks (rechts) zeigt an, dass es mit diesem Datenträger nichts anfangen kann. Nur Veracrypt kann ihn mounten.

Plattformen und Installation

Anlaufstelle ist die Projektseite *https://www.veracrypt.fr/en/Downloads.html*. Veracrypt gibt es für Linux (auch Free BSD, Raspbian), Windows und Mac-OS. Somit steht einer plattformübergreifenden Nutzung nichts im Wege. Für Windows gibt es sogar neben der installierbaren eine portable Variante, was die Mitnahme der Veracrypt-Software parallel zu den verschlüsselten Daten auf USB ermöglicht. Generell ist Veracrypt für Windows nochmal deutlich komplexer, da es auch Systempartitionen verschlüsselt und für externe Datenträger eine In-Place-Verschlüsselung anbietet – also die Verschlüsselung bestehender Datenträger ohne Datenverlust.

Unter Mac-OS ist neben Veracrypt das zusätzliche Osxfuse erforderlich, um Veracrypt-Container mit Benutzerrechten laden zu können. Unter Ubuntu, Mint & Co. ist die Installation über die genannte Webseite zwar möglich, der deutlich bequemere Weg führt jedoch über das PPA:

```
sudo add-apt-repository
  ppa:unit193/encryption
sudo apt-get update
sudo apt-get install veracrypt
```

Im Unterschied zur Windows-Version bietet Veracrypt unter Linux keine deutsche Übersetzung, weswegen wir uns bei den nachfolgenden Menübezeichnungen an die englischsprachigen halten.

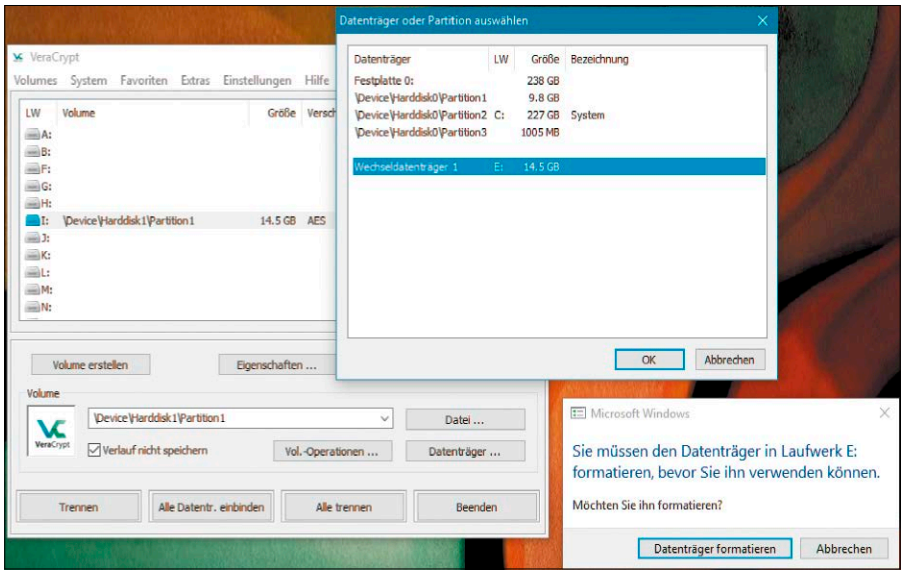
Veracrypt ist ein Tool für PCs und Notebooks. Smartphone und Tablets mit Android und iOS werden nicht direkt unterstützt. Die nachfolgend der Vollständigkeit halber genannten Apps sollten zumindest das Öffnen und Lesen von Veracrypt-Volumes ermöglichen. Mit technischen Limits und Komforteinschränkungen ist jedoch überall zu rechnen. Für Android finden Sie im Google Play Store das Tool EDS (Encrypted Data Store) in einer kostenlosen Lite-Version: (*goo.gl/Ce6wmg*) und der Vollversion für 7,49 Euro (siehe *goo.gl/1gsakw*). Die Lite-Version hat gravierende Beschränkungen (siehe *http://www.sovworks.com*). Für iOS gibt es den Crypto Disks & File Explorer (*goo.gl/vT4yNJ*) und Disk Decipher (*goo.gl/QGdkdq*) für je einen Euro.

Datencontainer oder Datenträger?

Veracrypt für Linux kann mit verschlüsselten Containerdateien arbeiten oder komplette (externe) Datenträger verschlüsseln. Die erste Variante ist die technisch einfachere und auch vom Assistenten („Creation Wizard") die stets empfohlene.

Datenträgerverschlüsselung: Da Veracrypt unter Linux einen Datenträger oder eine Partition komplett löschen und neu formatieren muss, um ihn danach verschlüsselt anzubieten, gibt es nur einen

Dateisysteme: Sollen Veracrypt-Daten unter Linux wie Windows funktionieren, ist ein kompatibles Dateisystem wichtig – einmal für den Datenträger, zum andern für den Container.



Ob Sie Container oder Datenträger mounten wollen, müssen Sie selbst wissen. Hier ist es ein USB-Stick („Datenträger“) unter Windows, mit dem Windows selbst nichts anzufangen weiß.

nennenswerten Grund für die Komplettverschlüsselung interner oder mobiler Laufwerke: Der Datenträger soll sich wie ein unformatiertes Laufwerk verhalten. Ein Veracrypt-Laufwerk präsentiert sich unter Linux nämlich als unbekanntes Dateisystem und Windows will es umstandslos sofort formatieren. Nur Veracrypt selbst kann das Laufwerk laden.

Ist dies gewünscht, dann verwenden Sie im Veracrypt-Assistenten nach „Create Volume“ die Option „Create a volume within a partition/drive“, danach „Standard VeraCrypt volume“ und wählen dann mit „Select Device“ den Datenträger. Das Gerät selbst, etwa „/dev/sdc“, können Sie nur verwenden, wenn der Datenträger im Rohformat ohne jede Partition vorliegt. Typischerweise ist eine Partitionsangabe wie „/dev/sdc1“ die richtige Wahl. Wenn nur eine Partition vorliegt, ist das Resultat von „/dev/sdc“ und „/dev/sdc1“ dasselbe. Wenn der Datenträger keine unverschlüsselte Partition enthalten soll, sorgen Sie vorab mit Gparted oder Gnome-Disks dafür, dass keine oder nur eine Partition vorliegt. Alle weiteren Optionen der Einrichtung unterscheiden sich nicht vom Anlegen eines einfacheren Containers, das nachfolgend genauer beschrieben ist. Für das Mounten verschlüsselter Datenträger verwenden Sie im Veracrypt-Hauptfenster statt „Select File“ (für Container) die Schaltfläche „Select Device“.

Datencontainer: Um eine neue Containerdatei anzulegen, klicken Sie im Hauptfenster auf „Create Volume“, dann auf „Create an encrypted file container“ und auf „Standard VeraCrypt volume“. Hier geben Sie Pfad und Namen einer **bisher nicht existierenden** Datei an. Unter „Encryption Options“ belassen Sie alles auf den Standardvorgaben. Danach geben Sie die Größe der Containerdatei an. Diese sollte großzügig ausfallen, weil die Kapazität nicht mehr zu ändern ist. Veracrypt verwaltet auch sehr große Container mühelos, andererseits bedeuten viele kleine Container erhöhten Verwaltungsaufwand und die Gefahr, Einstellungen und Passwörter zu vergessen.

Danach kommt die Passwortvergabe. Speziellere Optionen bei diesem Schritt sind im nächsten Punkt beschrieben. Für die meisten Szenarien ist ein komplexes Passwort völlig ausreichend. Die anschließenden „Format Options“ gelten für das innere Dateisystem des Containers und sind wichtig: Wählen Sie am besten FAT oder NTFS, wenn Sie die Daten auch unter Windows brauchen. Mit anderen Worten: Ein USB-Stick, den Sie unter allen Systemen nutzen möchten, muss nicht nur selbst ein allgemein kompatibles Dateisystem haben, sondern auch der Veracrypt-Container muss mit einem solchen formatiert sein.

Im Allgemeinen kann man bei der Containerformatierung mit NTFS nichts falsch machen. FAT genügt auch, sofern der Container keine Dateien größer als vier GB aufnehmen muss.

Die nächste Option lautet „Cross-Platform Support“. Hier muss die obere Einstellung aktiviert werden, wenn ein Container auch in anderen Betriebssystemen genutzt werden soll („I will mount the volume on other platforms“). Beachten Sie aber, dass es sich hier nur um ein zusätzliches Containerflag handelt, das nichts nützt, wenn das Dateisystem des Datenträgers plus das Dateisystem des Containers nicht kompatibel sind (siehe oben).

Zur Schlüsselerstellung auf Basis des Passworts erwartet Veracrypt danach Mausbewegungen im eigenen Fenster. Schließen Sie den Vorgang am Ende mit „Format“ ab. Damit ist der Container einsatzbereit.

Um Container zu verwenden, navigieren Sie mit „Select File“ im Hauptdialog zur Containerdatei. Mit Klick auf „Mount“ wird diese im Dateimanager geöffnet (falls nicht, lässt sich das unter „Preferences → System Integration“ einstellen). Linux mountet Container nach „/media/veracrypt[nummer]“, Windows auf freie

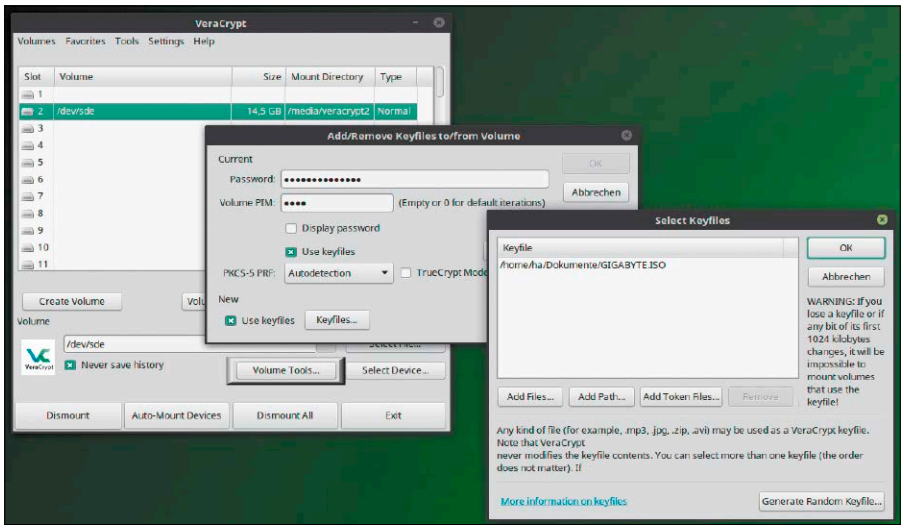
Laufwerkbuchstaben.Auf diesen Datenträgern lesen und arbeiten Sie wie auf einem normalen Laufwerk. Mit „Dismount“ im Hauptdialog entladen Sie den Container, der somit wieder geschützt ist.

Anspruchsvollere Passwortoptionen

Bei der Passwortvergabe haben wir im vorangehenden Abschnitt zwei Optionen übergangen, weil wir sie für die Basisbenutzung von Veracrypt nicht empfehlen. Interessant sind sie durchaus, aber sie erhöhen Komplexität und Verwaltungsaufwand.

Container mit Passwort und PIM: Beim Erstellen des Containers gibt es im Dialog der Passwortdefinition die zusätzliche Option „Use PIM“. Hier kann eine Zahl eingetragen werden. Geschieht dies, so genügt das richtige Kennwort zum Öffnen dieses Containers nicht mehr. Hier ist dann zusätzlich die exakte PIM-Zahl erforderlich. Vereinfacht gesagt, handelt es sich um ein zusätzliches Kennwort für deutlich erhöhten Schutz. Technisch definiert der Personal Iterations Multiplier die Anzahl der Wiederholungen von Hashfunktionen, die dann beim genauen angegebenen PIM-Wert den Entschlüsselungsheader generieren. Beachten Sie, dass ein hoher PIM-Wert den Mountvorgang eines Volumes deutlich verzögert. Das einmal geladene Volume ist dann aber so schnell wie gewohnt.

Container mit Passwort und Keyfile: Der Passwortdialog hält noch eine weitere interessante Möglichkeit parat – nämlich die „Keyfiles“, Schlüsseldateien. Dabei kann es sich um eine beliebige Datei handeln, die Veracrypt zum Öffnen des Containers zusätzlich zum Passwort benötigt. Entscheidend für die Schlüsselfunktion dieser Datei sind deren erste 1024 Bytes, nicht Pfad oder Dateiname. Das heißt, dass sich der Inhalt dieser Schlüsseldatei keinesfalls ändern darf, das Verzeichnis oder der Dateiname jedoch durchaus. Ideale Kandidaten für Schlüsseldateien sind Binärdateien, PDFs oder ISO-Images, die normalerweise nie geändert werden. Ein Keyfile ist wie die PIM-Zahl additiv: Es ersetzt nicht das Passwort, sondern muss zusätzlich vorliegen. Es ist ein guter Schutz gegen Keylogger, weil das Kennwort alleine nicht mehr ausreicht. Das Keyfile kann ferner auch ein schwächeres Kennwort rechtfertigen und die Kennworteingabe verkürzen. Für mobile USB-Laufwerke ist die Keyfilemethode nicht geeignet. Möglich wäre aber ein geschützter USB-Stick, für welchen das Keyfile sowohl zu Hause wie im Büro vorliegt – aber keinesfalls auf dem Stick selbst.



Nachträgliche Änderungen: Mit „Volume Tools“ können Passwort, PIM und Schlüsseldateien eines Containers neu definiert werden.

Schaltfläche „Volume Tools“: Für einen geladenen Container lassen sich alle bisherigen Einstellungen auch nachträglich ändern (unter Windows muss der Container ausgewählt, darf aber nicht geladen sein). Das erledigen Sie im Hauptfenster über „Volume Tools“. Sie können ein neues Passwort vergeben oder Keyfiles hinzufügen oder entfernen. Beachten Sie, dass die Aktion in jedem Fall noch einmal eine korrekte Anmeldung mit den bisherigen Daten erfordert (obwohl der Container bereits gemountet ist).

Durchaus kompliziert ist etwa die Definition einer neuen Schlüsseldatei („Add/Remove Keyfiles“). Dazu müssen Sie nämlich für die Anmeldung „Use keyfiles“ aktivieren und die bisherige Datei angeben, unter „New“ erneut „Use keyfiles“ aktivieren und dort die neue definieren. ■

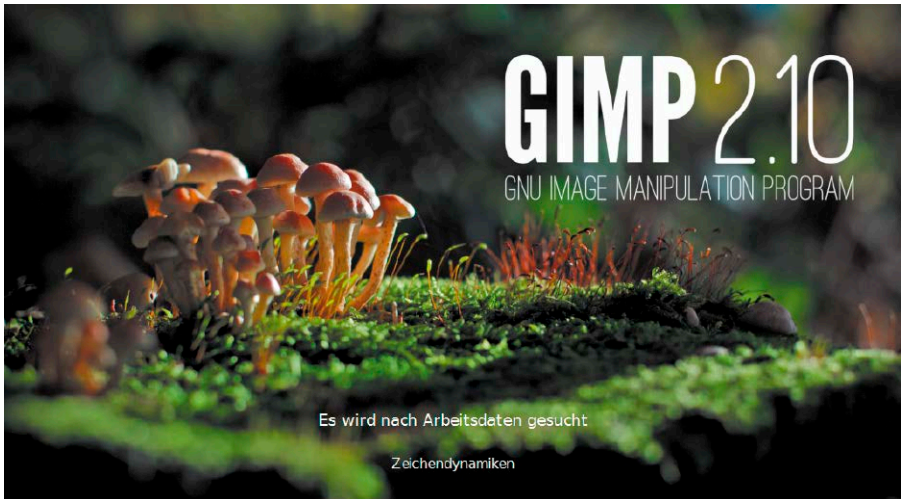
VERSTECKTE VERACRYPT-VOLUMES

Im zweiten Fenster des Assistenten kann man mit „Hidden VeraCrypt Volume“ einen versteckten Container innerhalb eines sichtbaren Containers anlegen. Der Vorgang beginnt zunächst mit dem „Outer Volume“. Nach Erstellung, Kennwortvergabe und Bestückung mit Dateien (was auch später geschehen kann) führt der Assistent automatisch weiter zum „Hidden Volume“, das im äußeren Container untergebracht wird. Wichtig ist, dass dieser zweite Container ein völlig anderes Kennwort erhält. Nutzt man beim späteren Mounten der Containerdatei das erste Kennwort, so öffnet sich das äußere Volume. Gibt man hingegen das zweite Kennwort ein, öffnet dies das innere, versteckte Volume. Laut Hersteller ist das innere Volume auch bei geöffnetem äußeren Volume und genauer Datenanalyse nicht nachweisbar.

Natürlich sind versteckte Container eine reichlich paranoide Methode, wenn es nur um den Datenschutz einiger Tabellen oder Texte geht. Das Prinzip „Plausible Deniability“ (glaubhafte Abstreitbarkeit) soll dem Datenbesitzer unter Erpressung oder Folter die Möglichkeit geben, ein Passwort preiszugeben – aber eben nicht das entscheidende. Wer tatsächlich mit einer solchen Situation rechnen muss, sollte im sichtbaren „Outer Volume“ zumindest scheinbar interessante Daten bereithalten.

Das neue Gimp 2.10

Die Entwickler haben Gimp mit Version 2.10 einen neuen Unterbau spendiert, der für mehr Geschwindigkeit und Komfort sorgt. Außerdem gibt es etliche neue und spannende Funktionen.



VON THORSTEN EGGELING

Gimp, das GNU Image Manipulation Program (*www.gimp.org*) ist neben Libre Office und Firefox eines der wichtigsten Open-Source-Großprojekte für den Desktop. Die Bildbearbeitung genügt auch professionellen Ansprüchen bei der Erstellung, Gestaltung und Bearbeitung von Grafikdateien. Es eignet sich für alle Nutzer, die unter Windows beispielsweise Adobe Photoshop verwenden, auch wenn Gimp dessen Funktionsumfang noch nicht erreicht. Nach sechsjähriger Entwicklungszeit steht Gimp 2.10 nun zum Download bereit. Sechs Jahre sind eine lange Zeit, entsprechend üppig fallen auch die Neuerungen gegenüber der Vorgängerversion aus.

1. Gimp 2.10.2 installieren

Es gibt mehrere Wege, Gimp unter Linux einzurichten. Wenn Sie Gimp über ein herkömmliches DEB-Paket neu installieren wollen, verwenden Sie ein PPA (Personal Package Archive). Ist Gimp bereits installiert, lässt sich das Programm damit aktualisieren. Die bisherige Version steht dann nicht mehr zur Verfügung. Führen Sie die folgenden drei Befehlszeilen aus:

```
sudo add-apt-repository ppa:otto-
  kesselgulasch/gimp
sudo apt-get update
sudo apt-get install gimp
```

Flatpak: Die Gimp-Entwickler empfehlen die Installation als Flatpak. Dabei handelt es sich um Softwarepakete, die eine eigene Laufzeitumgebung unabhängig vom installierten Betriebssystem verwenden. Der Vorteil: Sie können bei Bedarf auch die ältere Gimp-Version aus dem Repositorium der Distribution weiterverwenden und Sie erhalten schneller Updates. Neben Gimp müssen für Flatpak jedoch zahlreiche Pakete der Laufzeitumgebung eingerichtet werden, was insgesamt etwa ein GB Speicherplatz auf der Festplatte belegt. Flatpack-Apps benötigen zumindest für den ersten Start etwas länger und belegen mehr Systemressourcen. Ein weiterer Nachteil: Da Flatpak-Apps abgeschottet in einer Sandbox laufen, ist der Datenaustausch mit anderen Programmen nicht möglich, beispielsweise beim Import von RAW-Dateien (siehe Punkt 4).

Flatpak ist beispielsweise in Fedora seit Version 25 oder in Linux Mint seit 18.3 standardmäßig installiert. Bei Ubuntu 16.04 oder 18.04 fehlt die Software. Für die Installation führen Sie in einem Terminalfenster diese drei Befehle aus:

```
sudo add-apt-repository
  ppa:alexlarsson/flatpak
sudo apt update
sudo apt install flatpak
```

Bei Ubuntu 18.04 können Sie zusätzlich mit

```
sudo apt install gnome-software-
  plugin-flatpak
```

Flatpak in Ubuntu-Software integrieren und Flatpak-Pakete dann auch über die grafische Oberfläche installieren oder wieder entfernen. Die aktuelle Gimp-Version – zur Zeit 2.10.2 – installieren Sie dann mit dieser Zeile:

```
flatpak install https://flathub.
  org/repo/appstream/org.gimp.
  GIMP.flatpakref
```

Beantworten Sie alle Fragen mit „y“ und bestätigen Sie mit der Eingabetaste.

Installation als Snap-App: Ab Ubuntu 16.04 sind die für Snap erforderlichen Komponenten bereits vorinstalliert. Snap-Apps funktionieren ähnlich wie Flatpak-Pakete und haben die gleichen Vor- und Nachteile (mehr zu Snaps siehe Seite 38). Für die Installation starten Sie Ubuntu-Software, suchen nach Gimp und klicken auf den ersten Eintrag im Suchergebnis. Unter „Details“ steht hinter „Quelle“ die Angabe „Snap-Store“. Wenn nicht, haben Sie die Seite für die Installation aus dem Ubuntu Repositorium aufgerufen („Quelle: ubuntu-bionic-universe“, zur Zeit Version 2.8.22-1). In diesem Fall blättern Sie zu Seite mit dem Suchergebnis zurück und wählen einen anderen Eintrag.

Klicken Sie hinter „Kanal“ auf die Schaltfläche „stable“. Sie sehen dann, welche Versionen verfügbar sind. Bei Fertigstellung dieses Artikels ließ sich die aktuellste Version „2.10.2“ hinter „edge“ per Klick auf

„Switch“ auswählen. Klicken Sie anschließend auf „Installieren“. Nach Abschluss der Installatiown klicken Sie auf „Berechtigungen“. Aktivieren Sie „Dokumente ausdrucken“ und „Lese/Schreibe Dateien auf mobilen Datenträgern“, wenn Sie diese Funktionen nutzen möchten.

Bei unseren Tests Ende Juni 2018 fehlte der Snap-App von Gimp mindestens eine Funktion: Es war nicht möglich, „heic“-Dateien zu öffnen, weil die dafür nötige Programmbibliothek fehlte (siehe Kasten „Unterstützung für Apples HEIF-Bildformat“). Das Problem wird aber wahrscheinlich durch eins der nächsten Updates behoben.

Gimp aufrufen: Starten Sie Gimp über eine Suche im Dash (Ubuntu 16.04) oder in den „Aktivitäten“ (Ubuntu 18.04). Sollte die Suche direkt nach der Installation nicht fündig werden, melden Sie sich bei Ubuntu ab und wieder an.

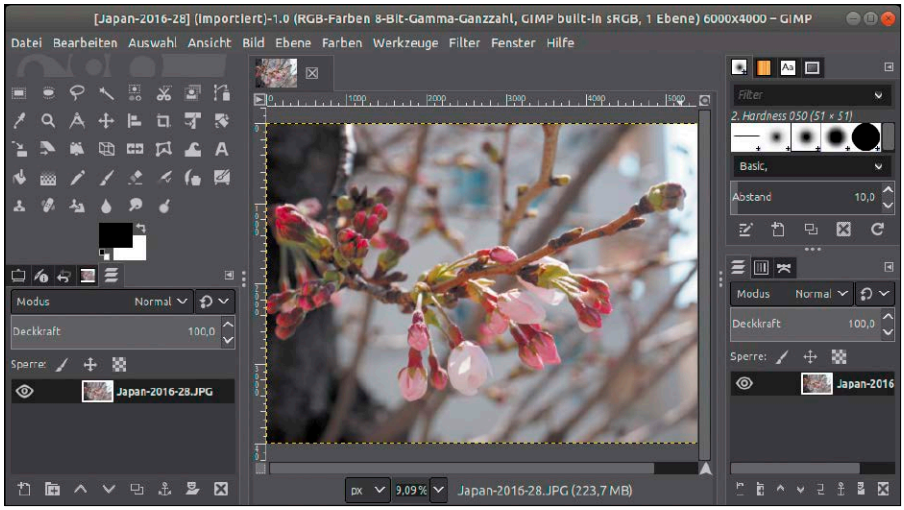
2. Änderungen bei Oberfläche und Bedienung

Gimp zeigt nach dem Start eine weitestgehend deutschsprachige Oberfläche. Vereinzelt stoßen Sie auf englischsprachige Beschriftungen. Über „Bearbeiten → Einstellungen“ können Sie im Bereich „Oberfläche“ auch eine andere Sprache oder „English [en_US]“ einstellen. Das kann hilfreich sein, wenn Sie englischsprachige Gimp-Tutorials nachvollziehen wollen.

Standardmäßig startet das Programm im Einzelfenster-Modus. Wenn Sie frei positionierbare Fenster bevorzugen, entfernen Sie das Kreuzchen unter „Fenster → Einzelfenster-Modus“. Bei der Aufteilung der Gimp-Benutzeroberfläche gibt es keine grundlegenden Änderungen, außer dass jetzt ein graues statt einem weißen Thema zum Einsatz kommt. Gimp versucht für hochauflösende Monitore die optimale Einstellung zu finden, damit die Elemente gut sichtbar sind. Über „Bearbeiten → Einstellungen“ können Sie unter „Oberfläche → Thema“ die Darstellung ändern und auch ein helles Thema auswählen. Unter „Oberfläche → Symbol Thema“ stellen Sie die dafür passenden Icons ein und ändern bei Bedarf die Symbolgröße. Für einige Abbildungen in diesem Artikel haben wir das Thema „System“ und das Symbolthema „Legacy“ aktiviert.

Wer sich in Gimp bereits auskennt, wird die neue Suchfunktion zu schätzen wissen, die sich über das Menü „Hilfe → Einen Befehl

Versionsauswahl: Die Paketverwaltung Ubuntu-Software bietet mehrere Gimp-Versionen als Snap-Apps an. Per Klick auf „Switch“ wählen Sie die gewünschte Version.



Gimp im neuen Gewand: Standardmäßig zeigt sich Gimp in Schwarz und Grau. Wem das nicht gefällt, kann in den Einstellungen ein anderes Thema wählen.

UNTERSTÜTZUNG FÜR APPLES HEIF-BILDFORMAT

Mit iOS 11 und Mac-OS High Sierry (10.13) hat Apple ein neues Containerformat für Bilddateien eingeführt. Es trägt den Namen High Efficiency Image File Format (HEIF). Die Dateien tragen die Endung „.heic“. HEIF basiert auf mehreren Standards, etwa ISO 14496-12 für strukturierte Datenabschnitte in Dateicontainern und ISO/IEC 23008-12 für die Bild- und Videokomprimierung nach dem Standard HEVC/H.265. Das Format bietet eine effizientere Komprimierung als das bisherige JPEG-Format und kann mehrere, bei Bedarf auch animierte Bilder sowie Audiospuren im Container unterbringen.

Gimp kann dieses Apple-Dateiformat ab Version 2.10.2 öffnen. Gehen Sie einfach auf „Datei → Öffnen“ und wählen Sie die gewünschte Datei aus. Dateien mit der Endung „.heic“ waren bei unseren Tests unter Ubuntu 18.04 aber noch nicht mit Gimp verknüpft. Um das zu ändern, klicken Sie im Dateimanager eine „heic“-Datei mit rechter Maustaste an, wählen „Eigenschaften“ und gehen auf die Registerkarte „Öffnen mit“. Wählen Sie in der Programmliste „GNU Image Manipulation Program“ und klicken Sie dann auf „Als Vorgabe festlegen“.

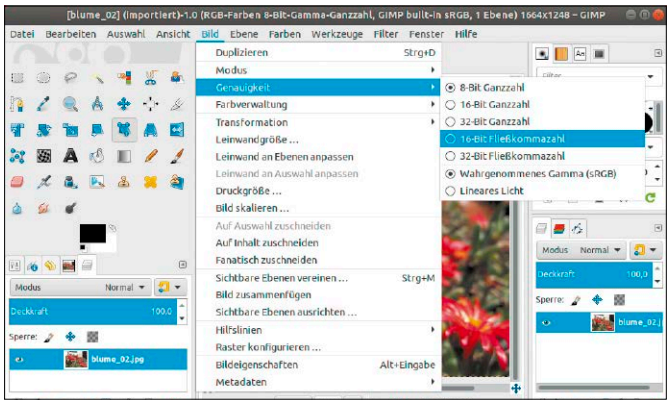
suchen und ausführen“ aufrufen lässt. Tippen Sie einen Suchbegriff ein, beispielsweise „Transform“. Per Doppelklick auf ein Suchergebnis in der Liste gelangen Sie sofort zur gewünschten Funktion, etwa zum neuen Werkzeug „Vereinheitlichte Transformation“ (siehe Punkt 5). Die Ergebnisliste passt sich dynamisch an. Häufig genutzte Funktionen erscheinen weiter oben.

3. Die neue GEGL-Grafikbibliothek

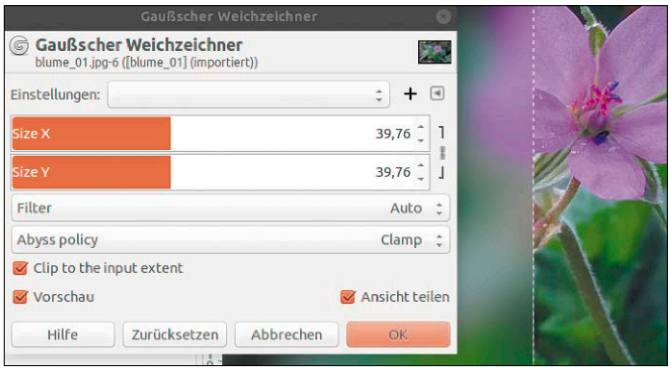
Zu den wichtigsten Neuerungen von GIMP 2.10 zählt die GEGL Image Processing Engine. Die Engine führt Pixelberechnungen deutlich schneller und genauer durch und ermöglicht neue Funktionen. Gimp 2.8 konnte nur mit acht Bit pro Farbkanal rechnen, bei Gimp 2.10 sind es bis zu 32 Bit. Es ist daher jetzt möglich, HDR-Formate wie PSD, TIFF, PNG, EXR und RGBE zu öffnen und zu exportieren. Über „Bild → Genauigkeit“ können Sie bei einem geöffneten Foto die Farbtiefe einstellen, beispielsweise auf „32-Bit-Fließkommazahl“. Importierte RAW-Fotos besitzen in der Regel dieses Format (siehe Punkt 4). Durch Umwandeln wird ein Standardbild mit 8 Bit natürlich nicht besser, aber mit 32 Bit lassen sich feinere Details herausarbeiten, etwa wenn Sie Filter anwenden.

Eine weitere Beschleunigung erreicht Gimp durch verbessertes Multithreading, wobei Aufgaben auf mehrere Prozessorkerne verteilt werden. Das kommt zwar nicht bei allen Gimp-Funktionen zum Einsatz, wird aber teilweise durch GEGL und Programmcode in Gimp realisiert. Zur Verbesserung der Leistung kann Gimp auch den Prozessor der Grafikkarte (GPU) verwenden. Die Optionen dafür finden Sie über „Bearbeiten → Einstellungen“ unter „Systemressourcen“. Passen Sie die Anzahl der Threads bei Bedarf an und setzen Sie für die Nutzung der GPU unter „Hardware-Beschleunigung“ ein Häkchen vor „OpenCL verwenden“.

Ein weiterer Vorteil von GEGL ist, dass Sie jetzt im linearen RGB-Farbraum und auch im an die Wahrnehmung angepassten Farbraum arbeiten können. Sie sehen das beispielsweise, wenn Sie für Farbanpassungen auf „Farben → Kurven“ gehen. In der Zeile hinter „Kanal:“ gibt es die zwei neuen Schaltflächen „Adjust curves in linear light“ und „Kurve nach Wahrnehmung anpassen.“ Dank GEGL sehen Sie jetzt nicht nur ein kleines Vorschaubild, etwa bei „Filter → Weichzeichnen → Gaußscher Weichzeichner“, sondern Gimp wendet die Einstellungen im Filter direkt auf das Bild an. Sehr praktisch ist in diesem Dialog auch „Ansicht teilen“. Wenn Sie hier ein Kreuzchen setzen, teilt eine vertikale Linie das Bild. Sobald Sie die Werte für den Weichzeichner ändern, erscheint im linken Bildbereich eine Vorschau der Einstellung, die Sie direkt mit dem unveränderten rechten Teil des Bildes vergleichen können. Die Vorschaufunktion und „Ansicht teilen“ gibt es auch in anderen Dialogen, die GEGL verwenden, beispielsweise „Farben → Farbabgleich“, „Farben →Belichtung“ oder „Filter → Licht und Schatten → Schlagschatten“.



Höhere Farbtiefe: Gimp kann jetzt auch mit 16- und 32-Bit-Farbtiefe umgehen. Dadurch lassen sich hochauflösende Bilder bearbeiten und Korrekturen mit weniger Fehlern durchführen.



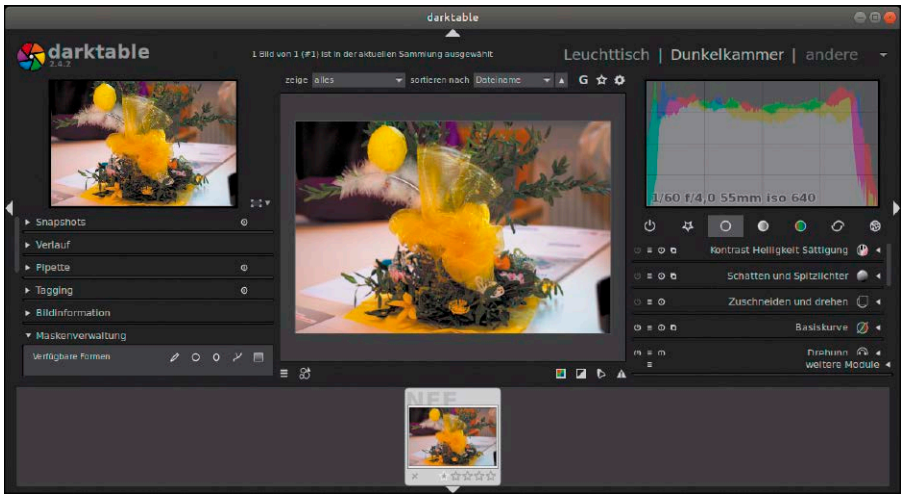
Bessere Vorschau: Dank GEGL zeigt Gimp 2.10 jetzt sofort im geöffneten Bild an, wie sich die Einstellungen etwa eines Filters auswirken.

4. Bilder im RAW-Format öffnen

Bilder im RAW-Format lassen sich in Gimp weiterhin nicht direkt öffnen. Hierzu muss Darktable ab Version 1.7 oder Rawtherapee ab Version 5.2 aushelfen. Sie finden beide Programme über den Paketmanager Ihrer Linux-Distribution. Ist beispielsweise Darktable installiert, gehen Sie in Gimp auf „Datei → Öffnen“ und wählen die gewünschte RAW-Datei. Die Datei öffnet sich in Darktable und Sie bearbeiten das Bild nach Ihrem Geschmack. Wenn Sie Darktable schließen, öffnet sich das Bild automatisch in Gimp. Bei unseren Tests funktionierte die Zusammenarbeit mit Darktable nur bei der PPA-Version von Gimp (siehe Punkt 1). Das ist auch nicht weiter verwunderlich, da Snap- und Flatpak-Apps keinen Zugriff auf die Daten anderer Programme haben. Die Installation von Darktable als Snap- oder Flatpak-App ändert daran erwartungsgemäß nichts. Eine denkbare Lösung wäre es, dass die Entwickler Gimp und Darktable zusammen in einem Paket ausliefern.

5. Neue Tools für die Bildtransformation

Unter „Werkzeuge → Transformationen“ finden Sie Funktionen, um eine Ebene, eine Auswahl oder einen Pfad zu verändern. Ein typisches Beispiel zeigt das Bild auf der nächsten Seite mit dem Notebook. So wie das Gerät steht, laufen in der Perspektive die Linien schräg nach hinten auf einen Fluchtpunkt zu. Im fertigen Bild soll das Notebook einen anderen Inhalt auf dem Bildschirm zeigen als im Original. Dazu öffnen Sie das Bild mit dem Notebook in Gimp und dann über „Datei → Als Ebenen öffnen“ das Bild, das Sie einbauen möchten. Sollte es zu groß oder klein sein, bringen Sie es zuerst über „Werkzeuge → Transformationen → Skalieren“ ungefähr auf die passende Größe. Danach rufen Sie die neue Funktion



RAW-Fotos über Umweg: Gimp öffnet Bilder im RAW-Format zuerst in Darktable. Wenn Sie das Programm schließen, lädt Gimp das konvertierte Bild und zeigt es an.

über „Werkzeuge → Transformationen → Vereinheitlichte Transformation“ auf. Über die großen Quadrate an den Ecken und die etwas kleineren am Rand lassen sich Höhe und Breite ändern (skalieren). Die auf der Spitze stehende Quadrate am Rand stellen das Bild schräg (scheren, kippen) und wenn Sie die kleinen Quadrate innerhalb des größeren an den Ecken ziehen, ändern Sie die Perspektive. Das Symbol am Mauszeiger ändert sich abhängig von der Funktion.

Das hört sich kompliziert an, aber letztlich müssen Sie es nur schaffen, das Bild so zu verzerren, dass die Ecken des Bildes genau auf den Ecken des Notebookbildschirms liegen. Die richtige Perspektive ergibt sich dabei automatisch. Wenn Sie mit dem Ergebnis zufrieden sind, klicken Sie auf „Transformation“.

Der Punkt „Werkzeuge → Transformationen → Gitter Transformation“ ist ebenfalls neu. Die englischsprachige Bezeichnung „Handle Transform Tool“ beschreibt die Funktion etwas genauer. Per Mausklick setzen Sie einen Handle, also einen Anfasser, beispielsweise an der linken Seite in das Bild. Wenn Sie diesen mit der Maus ziehen, verschieben Sie das Bild. Klicken Sie mit der Maustaste weiter rechts in das Bild. Wenn Sie den zweiten Anfasser ziehen, skalieren oder drehen Sie es. Mit einem dritten Anfasser lässt sich das Bild scheren.

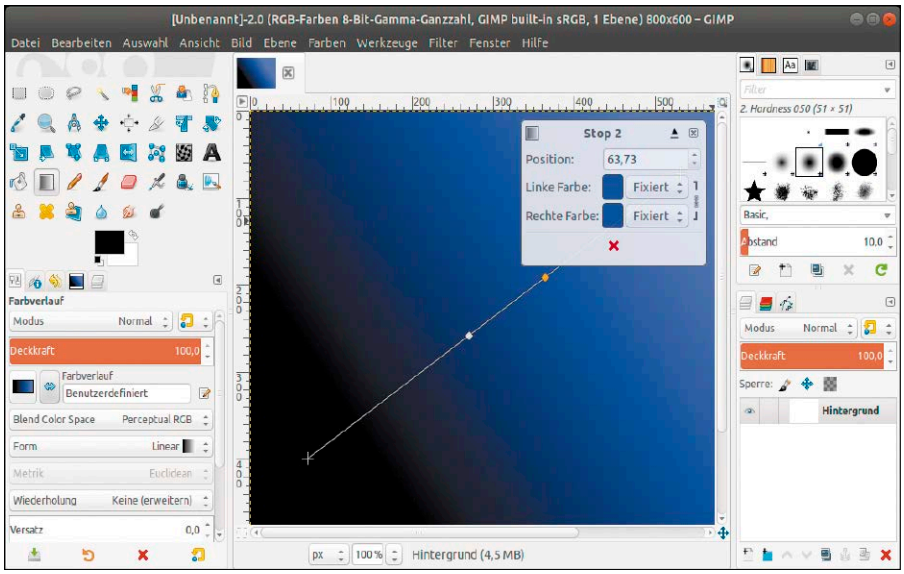
6. Verbesserungen bei den Farbverläufen

Eine der wichtigsten Neuerungen ist eine bessere Bearbeitung des Farbverlaufs. Bisher konnten Sie einen Farbverlauf nur einfach zwischen zwei Punkten aufziehen und Gimp hat das Bild oder die Auswahl sofort mit dem eingestellten Verlauf gefüllt. In Gimp 2.10 gibt es mehr Optionen, um Farbverläufe besser und auch nachträglich anzupassen.

So nutzen Sie die neue Funktion: Laden Sie zuerst das zu bearbeitende Foto in Gimp und duplizieren Sie die Ebene über „Ebene → Ebene duplizieren“. Fügen Sie eine neue Ebene über „Ebene → Neue Ebene“ hinzu und wählen Sie dabei in den Eigenschaften der Ebene den Modus „Weiche Kanten“ und als Füllung „Transparenz“. Danach klicken Sie diese Ebene auf dem Reiter „Ebenen“ an und verwenden in der Werkzeugkiste den „Farbverlauf“. Alternativ drücken Sie die G-Taste. Ziehen Sie den Farbverlauf über den gewünschten Bereich – von der einen zur anderen Ecke – und betrachten Sie das erste Ergebnis. Wenn Sie das Werkzeug anwenden, sehen Sie den Dialog „Farbverlauf“, in dem Sie die Parameter ändern können, beispielsweise die Vordergrund- und die Hintergrundfarbe des Farbverlaufs. Sollte der Dialog nicht erscheinen, blenden Sie ihn per Doppelklick auf das Werkzeug „Farbverlauf“ ein.

Durch Bewegen der beiden Kreuze im Bild lässt sich der Farbverlauf individuell anpassen. Darüber hinaus können Sie per Mausklick auf die Verlaufslinie eine beliebige Anzahl von Stopp-Punkten setzen. Damit legen Sie den Farbverlauf für einen Abschnitt des Bildes fest. An jedem Stopp-Punkt sind neue Definitionen für die Vorder- und Hintergrundfarbe möglich, außerdem lassen sich die Stopp-Punkte auf der Farbverlaufslinie beliebig hin- und herschieben. ■

Bildelemente einpassen: „Vereinheitlichte Transformation“ unterstützt Sie bei der Anpassung der Bildgeometrie. Das Ergebnis ist rechts unten zu sehen.

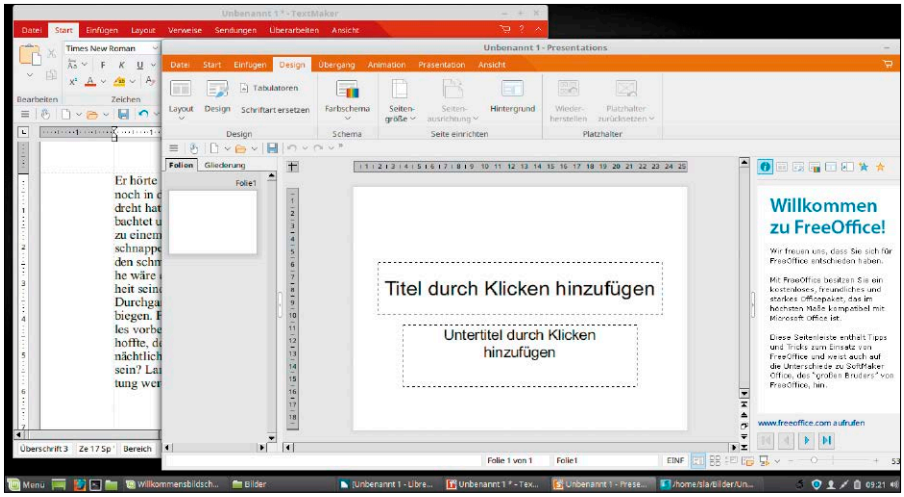


Farbverlauf bearbeiten: In Gimp 2.10 lassen sich Anfang und Ende eines Farbverlaufs verschieben und Sie können über Stopp-Punkte die Farben für einzelne Abschnitte festlegen.

Konkurrenz für Libre Office

Mit Libre Office gibt es seit vielen Jahren ein bewährtes Office-Paket. Free Office will sich als weitere kostenlose Alternative bewähren. Dahinter steckt mit fast vollständigem Funktionsumfang das kommerzielle Softmaker Office.

VON STEPHAN LAMPRECHT



Die Programmsammlung wird unter *www.freeoffice.com* zum kostenlosen Download angeboten und umfasst die Textverarbeitung Textmaker, ein Präsentationsprogramm sowie die Tabellenkalkulation Planmaker. Das entspricht weitestgehend dem Softmaker Office Standard für circa 70 Euro. Im Wesentlichen wurden aus Free Office nur die Rechtschreibprüfung herausgenommen sowie die Fähigkeit, die älteren Microsoft-Formate DOC, XLS, PPT zu speichern (Lesen, Bearbeiten und Konvertieren ist möglich). Daneben gibt es aber noch eine Reihe scheinbar kleinerer Limitierungen, die aber je nach Anspruch kritisch ausfallen können.

Angeboten wird die Office-Suite in verschiedenen Paketformaten sowie einer Version mit einem eigenen Installationsprogramm. Diese Variante sollten Sie etwa nutzen, wenn Sie ein Arch Linux einsetzen. Der Download erfordert die Angabe einer gültigen Mailadresse, an welche der Aktivierungscode gesendet wird. Die Installation dauert länger, als von anderen Programmen gewöhnt, weil hierbei Theme-Dateien der Desktops erweitert werden. Den Ansatz, auf allen Plattformen die gleiche Oberfläche anzubieten, erreicht Softmaker durch die Nutzung einer eigenen Umgebung für das Rendering der Bildschirmelemente.

Gute Textverarbeitung für Gelegenheitsschreiber

Die meist wichtigste Komponente eines Office-Pakets ist die Textverarbeitung. Direkt nach dem Start bietet Textmaker die Option an, die von Microsoft bekannten Ribbon-Menüs und Kommandos zu aktivieren. Wer es lieber schlichter mag, kann auch klassische Menüs wählen.

Die Arbeitsgeschwindigkeit von Textmaker ist gut, auch Schnellschreiber werden keine Latenz bei der Reaktion der Schreibmarke bemerken.

Die Schlacht um die Vorherrschaft bei den Textformaten ist längst geschlagen: Ein Büropaket, privat oder beruflich genutzt, muss heutzutage die Office-Formate von Microsoft beherrschen. Das ist bei Textmaker der Fall. Die getesteten Dokumente wurden problemlos geöffnet und dargestellt. Lediglich spezielle Formatierungen des Microsoft-Formats bereiteten gelegentlich Probleme. Der auf einem Tablet per Stift bearbeitete Testtext war aber auch für Libre Office eine unlösbare Herausforderung. Ältere Office-Formate („DOC“) können lediglich gelesen, aber nicht gespeichert werden. Das gilt auch für das Hausformat von Libre Office. Wer eine Datei erstmals in Textmaker speichert, muss sich entscheiden, ob er das Textmaker-Format oder das jüngere Microsoft-kompatible Format als Standard verwenden möchte.

Anwender aktueller Word-Versionen werden sich im Ribbon-Menü von Textmaker & Co. schnell zurechtfinden. Für den schnellen Arbeitsbeginn bietet das Programm eine ganze Reihe von Vorlagen. Vom klassischen Brief über den Lebenslauf bis zur Telefonliste sind hier viele Anwendungsfälle abgedeckt. Gegenüber der kommerziellen Ausgabe, die es in verschiedenen Varianten und Lizenzmodellen gibt, sind aber einige Einschränkungen zu beachten. Davon wiegen einige schwerer als andere. So lassen sich mit Free Office etwa keine Serienbriefe schreiben. Auch der Druck von Aufklebern oder Umschlägen aus einer verbundenen Datenbank ist der kommerzi-

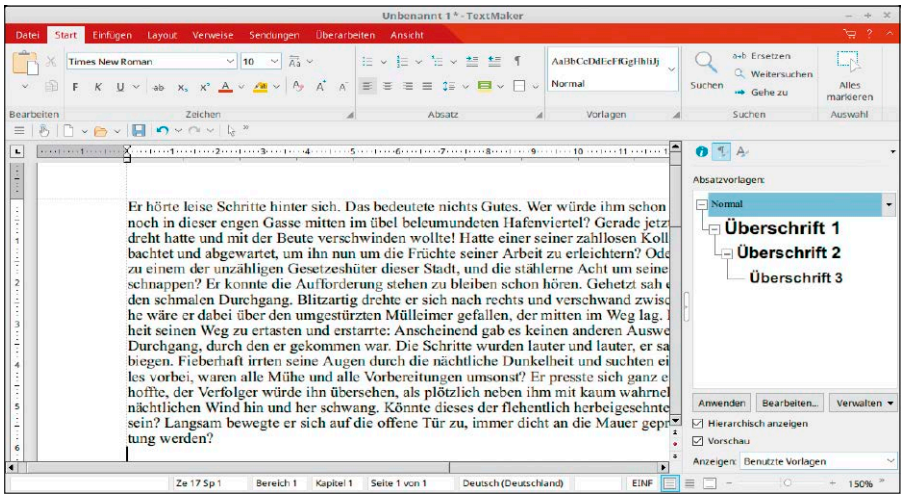
ellen Ausgabe vorbehalten. Wer ein wissenschaftliches Dokument oder eine Studienarbeit schreiben will, braucht auch die kommerzielle Lizenz. Denn Fußnoten, Querverweise, Bibliographien und Diagramme fehlen ebenfalls. Professionelle Anwender werden mit dieser Textverarbeitung nicht glücklich werden.

Schön präsentieren mit Presentations

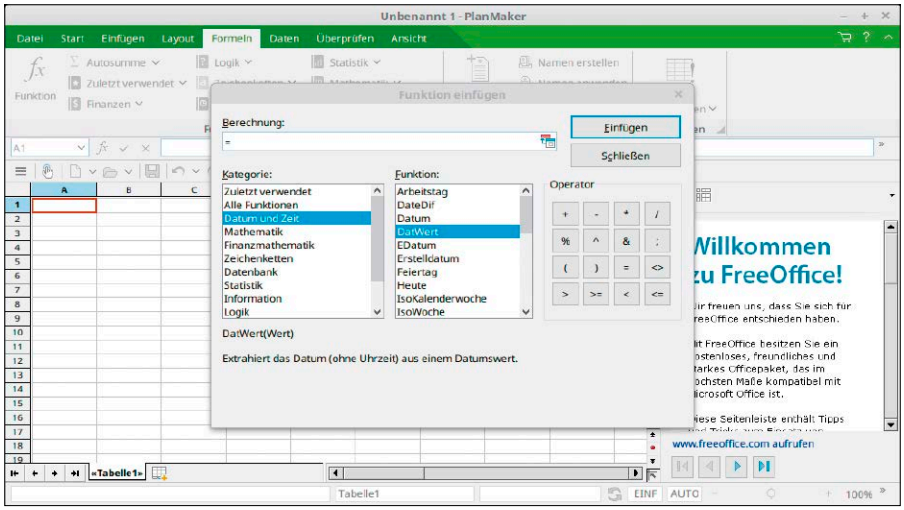
Auch das Präsentationsprogramm Presentations ähnelt in seiner Gestaltung und der Aufteilung der Menüs seinem Microsoft-Pendant. Powerpoint-Nutzer kommen damit auf Anhieb zurecht. Auch hier hat Softmaker eine Reihe von optisch ansprechenden Vorlagen hinzugefügt, die schnelle Ergebnisse erzielen. Aktuelle Microsoft-Formate können gelesen und geschrieben werden, ältere Formate nur geöffnet. Die Arbeit ist intuitiv und macht Spaß. Insgesamt wirkt Presentations vom gesamten Auftritt geschlossener und harmonischer als Impress aus Libre Office. Die funktionalen Unterschiede zur Kaufversion fallen beim Präsentationsprogramm geringer aus als bei der Textverarbeitung. Auch hier fehlt die Option, Diagramme einzufügen. Diagramme müssten also mit einem externen Programm vorbereitet und dann als Grafik integriert werden. Damit verzichtet der Nutzer dann aber auch gezwungenermaßen auf besondere Effekte bei der Darstellung der Diagramme. Den fehlenden Export von Diashows als Videos oder HTML-Dateien dürften wahrscheinlich nur wenige Anwender vermissen. Bedauerlich ist in dem Zusammenhang dagegen, dass für die Referentenansicht, wie sie aus Powerpoint und Impress bekannt ist, ebenfalls die Kaufversion erworben werden muss.

Das kleine Excel Planmaker

Ob sich eine Tabellenkalkulation auf dem Niveau vom Microsoft Excel befindet, dem Standard bei Controllern in Unternehmen, ist eher eine akademische Frage. Die Argumente pro und contra drehen sich meist um Funktionen, die ein durchschnittlicher Anwender ohnehin nie benutzt. Grundsätzlich ist Planmaker ein brauchbares Rechenprogramm. Gefühlt ist es aber das schwächste Glied in der Programmsammlung und auch etwas stiefmütterlich präsentiert. Denn außer einem Fahrten- und Haushaltsbuch sowie einer Zeiterfassung



Die Textverarbeitung: Textmaker ist ein flottes Schreibprogramm, verzichtet aber in der kostenlosen Version auf eine ganze Reihe von Profifunktionen.



Die Tabellenkalkulation: Bei der Arbeit mit Planmaker beim Einfügen von Formeln bietet die Software diesen Funktionsassistenten.

gibt es nur zwei weitere Vorlagen. In Sachen Bedienung gibt sich der Rechenknecht aber keine Blöße. Das Einfügen und Verknüpfen von Formeln wird wie bei Calc oder Excel von einem Assistenten begleitet. Wer die kostenlose Variante nutzt, muss gegenüber der kommerziellen Variante auf einige Komfortfunktionen verzichten, die den Umgang mit umfangreicheren Tabellenkonstrukten erleichtern. So fehlen etwa das Entfernen von leeren oder doppelten Zeilen oder das Aufteilen von Texten auf Spalten. Dies sind Funktionen, die Anwender zu schätzen wissen, die eine Tabellenkalkulation als Alternative zu einer Datenbank einsetzen und häufiger mit Texten arbeiten. Das größte Manko ist sicherlich das Fehlen von Szenarien, die im betriebswirtschaftlichen und statistischen Umfeld häufiger gebraucht werden. Hier hat Softmaker eindeutig nur den privaten Nutzer im Blick.

Schlanke Lösung (nur) für Privatanwender

Gegenüber der preiswertesten Variante von Softmaker Office sparen sich die Nutzer von Free Office 70 Euro beziehungsweise knapp sieben Euro Monatsgebühr. Funktional kann diese Office-Suite mit Libre Office nur bedingt mithalten. Auf der anderen Seite hat die Beschränkung aber auch Vorteile: Die Oberfläche wirkt frischer und ist eng an Microsoft Office angelehnt. Und weil Free Office sich auf die Funktionen fokussiert, die bei privaten Anwendern im Vordergrund stehen, schleppt das Paket wenig Ballast mit. ■

Pulseaudio im Griff

Die Klangausgabe von Linux-Systemen erfolgt heute fast ausnahmslos über Pulseaudio, das als Soundserver Anwendungen eine standardisierte Schnittstelle bietet. Der Beitrag zeigt Problemlösungen und nützliche Extras rund um Pulseaudio.

VON DAVID WOLSKI

Pulseaudio hat den Ruf, einerseits im Funktionsumfang sehr mächtig, andererseits aber auch widerspenstig zu sein. Dieser Ruf geht auf ein misslungenes, verfrühtes Debüt des Soundservers unter Ubuntu 8.04 zurück, der aus dem gleichen Entwicklerbüro stammt wie das anfangs umstrittene Init-System Systemd. In der einstigen Ubuntu-Version war die mitgelieferte Konfiguration unvollständig und unvermeidliche Bugs taten ihr Übriges, Anwendern den Hörnerv zu rauben. Jetzt, zehn Jahre später, ist Pulseaudio ausgereift und fällt weder in Ubuntu noch in anderen Linux-Distributionen im alltäglichen Betrieb durch unbehagliche Stille auf. Das Zusammenspiel mit wechselnden Ausgabegeräten verlangt aber weiterhin Aufmerksamkeit.

Pavucontrol: Mixer für Pulseaudio

Inzwischen beherrschen die Mixer-Applets der verbreiteten Desktopumgebungen wie Gnome, KDE, Mate und XFCE das Zusammenspiel mit Pulseaudio. Das ist nur konsequent, weil Pulseaudio die desktopspezifischen Bibliotheken ESD (Gnome) und Arts (KDE) ersetzte und die Schnittstellen standardisierte. Für die Fehlersuche und fortgeschrittene Funktionen sind die eigenen Tools des Soundservers aber immer noch die beste Wahl, weil dann Eigenheiten von Desktopumgebungen keine Rolle spielen. Das wichtigste Programm von Pulseaudio ist der grafische Mixer Pavucontrol, der in den meisten Linux-Distributionen noch auf seine nachträgliche Einrichtung wartet:

```
sudo apt-get install pavucontrol
```

Der Aufruf *pavucontrol* im Ausführen-Dialog oder im Terminal öffnet diesem systemnahen Mixer. Die Registerkarten „Wiedergabe“ und „Aufnahme“ zeigen jeweils aktive Anwendungen an, die mit Pulseaudio verbunden sind. „Ausgabegeräte“ und „Eingabegeräte“ listen die verfügbaren Geräte mit dem jeweiligen Ausgabeport und Reglern auf. Die wichtigste Einstellung verbirgt sich unter „Konfiguration“. Dort aktivieren oder deaktivieren die auswählbaren Profile externe Ports wie beispielsweise HDMI.

HDMI: Ausgabe umschalten

Wer ein TV-Gerät per HDMI anschließt, will meist auch das Audiosignal dahin umleiten. Die Auswahl des Audiogeräts, das zur Soundausgabe dienen soll, erfolgt wieder über das grafische Programm pavucontrol. Dort zeigt das Auswahlfeld „Konfiguration → Profil“, welche Ports zur Verfügung stehen, und dort tauchen auch die HDMI-Ports auf. Um den richtigen herauszufinden, schließen Sie das externe HDMI-Gerät an und sehen in dieser Liste nach, welcher der Einträge „Digital Stereo (HDMI)-Ausgabe“ nicht mit „(unplugged)“ markiert ist.

Wichtig: In einigen Desktopumgebungen wie XFCE ist es notwendig, einen angeschlossenen HDMI-Monitor erst noch in den Einstellungen unter „Anzeige“ beziehungsweise „Bildschirme“ zu aktivieren. Ansonsten erkennt auch Pulseaudio den HDMI-Port nicht.

Schnell in der Shell: Das gewünschte Profil und den aktiven Ausgabeport kann man auch in der Kommandozeile ohne pavucontrol umschalten. Der Befehl

```
pacmd list-cards | grep "active profile"
```

zeigt das gerade verwendete Profil. Gibt das Kommando beispielsweise

```
active profile: <output:hdmi-stereo-extra1>
```

für den gerade aktiven HDMI-Port aus, dann kann das Kommando

```
pacmd set-card-profile 0 output:hdmi-stereo-extra1
```

dieses Profil später bei Bedarf wieder aktivieren.

Equalizer: Klangbild anpassen

Auf Notebooklautsprechern, günstigen TV-Geräten und Kopfhörern klingt der Sound oft nicht berauschend und verlangt nach

einem Equalizer. Einen grafischen Equalizer hat Pulseaudio selbst im Angebot, diese Softwarelösung will aber erst eingerichtet werden. In Debian, Ubuntu und Linux Mint installiert das Kommando

```
sudo apt-get install pulseaudio-
  equalizer
```

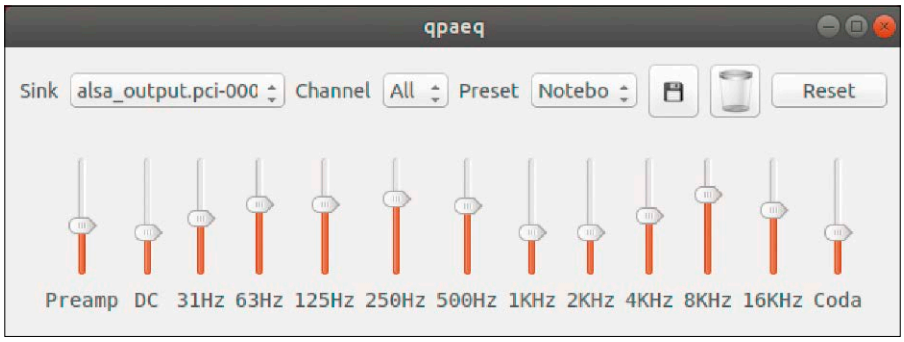
das nötige Paket. Danach öffnen Sie die Datei „/etc/pulse/default.pa“ beispielsweise mit

```
sudo nano /etc/pulse/default.pa
```

und fügen am Ende der Datei diese beiden Zeilen

```
load-module module-equalizer-sink
load-module module-dbus-protocol
```

ein. Nach dem Speichern und einem Neustart des Systems ruft *qpaeq* im Ausführen-Dialog den Equalizer auf, der sich die Position der Regler merkt und über das Diskettensymbol auch mehrere Presets speichern kann.

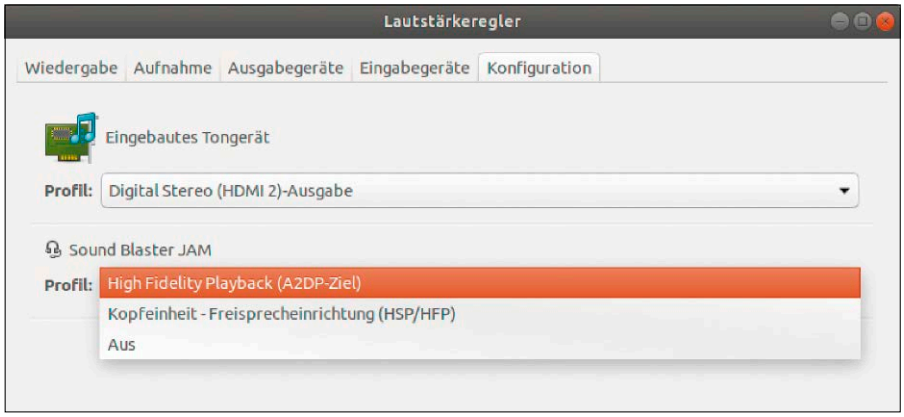


Softwareequalizer: Der Equalizer für Pulseaudio ist in den meisten Linux-Systemen über den Paketmanager installierbar, verlangt aber eine Anpassung der Pulseaudio-Konfiguration.

Kopfhörer: Hi-Fi per Bluetooth

Ein Kopfhörer ist mit einem Linux-System schnell über das Bluetooth-Symbol der Systemleiste eingebunden, bleibt aber zunächst einmal still.

Nach dem Aufruf *pavucontrol* zeigt die Registerkarte „Konfiguration“ den Status aller verbundenen Audiogeräte. Im Feld „Profil“ eines Bluetooth-Kopfhörers steht üblicherweise „Aus“. Erst die Auswahl des Profils „High Fidelity Playback (A2DP-Ziel)“ für dieses verbundene Gerät lässt die Soundausgabe in Hi-Fi-Qualität zu. Das Profil „Headset Head Unit (HFP/HSP)“ liefert dagegen nur mindere Qualität und ist für Musik unbrauchbar. Der Mixer speichert diese Einstellung übrigens permanent. ■



Soundqualität für Bluetooth-Headsets einstellen: Die meisten Linux-Distributionen sprechen Bluetooth-Geräte zunächst nur in Radioqualität an, was sich in pavucontrol ändern lässt.

KEIN SOUND: SYSTEMATISCHE FEHLERSUCHE

Pulseaudio selbst ist nur ein Soundserver für Anwendungen, setzt aber wiederum auf das hardwarenahe Alsa („Advanced Linux Sound Architecture“) des Linux-Kernels auf. Wenn die Klangausgabe stumm bleibt, gilt es auch, die Einstellung dieser Kernel-Komponente zu kontrollieren.

1. Gibt es nach einer Neuinstallation oder einem umfangreichen Update eines Linux-Systems gar keinen Sound, sollte ein Blick in die grundlegenden Alsa-Einstellungen erfolgen:
Der Befehl

```
alsamixer -c0
```

zeigt im Terminal alle Einstellungen von Soundquellen und Inputschnittstellen an, auf die Pulseaudio aufsetzt. Ist hier eine Ausgabe auf stumm gestellt, etwa „Master“, dann wird auch Pulseaudio keinen Sound ausgeben. Die Taste „M“ ändert die Stummschaltung, die Pfeiltasten stellen den Pegel ein und wechseln zwischen den Reglern.

2. Der häufigste Fehler ist schlicht ein falsch ausgewähltes Profil zur Soundausgabe. Ein Blick in pavucontrol unter „Konfiguration → Profil“ hilft weiter. Das dort ausgewählte Ausgabegerät ist stets das Standardgerät. Linux-Systeme sollten zwar beim Verbinden oder Abziehen von HDMI-Geräten das Profil automatisch anpassen, dies funktioniert aber nicht immer.

3. Ebenso wichtig ist die individuelle Zuweisung von Audiogeräten zu Anwendungen in pavucontrol unter „Wiedergabe“. Ein Klick auf die Schaltfläche rechts neben einer aktiven Anwendung erlaubt die Zuweisung eines Geräts pro Audiostream. Es stehen hier die Audiogeräte (Tongeräte) zur Auswahl, die unter „Konfiguration → Profil“ ausgewählt sind.

4. Gibt es Probleme mit der Konfiguration oder der Soundkartenerkennung, können die Statusmeldungen von Pulseaudio bei der Fehlersuche im Web weiterhelfen. Um eine Logdatei zu generieren, öffnen Sie die Datei „/etc/pulse/client.conf“ mit root-Recht in einem Texteditor und fügen unten diese Zeile ein:

```
extra-arguments = -vvvv --log-target=newfile:/tmp/
  pulseaudio.log --log-time=1
```

Nach einem Neustart zeigt die Datei „/tmp/pulseaudio.log“ alle Meldungen des Soundservers.

Neue Software

Zwölf ausgewählte Softwareneuerscheinungen und Updates zeigen, welche Highlights die letzten Monate an frischen Open-Source-Programmen hergegeben haben. Neben bekannten Schwergewichten sind auch kleine clevere Tools vertreten.

VON DAVID WOLSKI

Zur größten und bekanntesten Online-Codeverwaltung mit Versionierungssytem ist in den letzten zehn Jahren der Dienst Github mit 28 Millionen Nutzern und 70 Millionen öffentlichen Repositories aufgestiegen. Das dort genutzte „Git" war in der Open-Source-Szene bereits verbreitet und geschätzt, nachdem es 2003 von Linus Torvalds für die Entwicklung des Linux-Kernels ins Leben gerufen wurde.

Geld hat Github trotz Reichweite und Bekanntheitsgrad mit seinem Geschäftsmodell von kostenlosem Codehosting und kostenpflichtigen Enterprisediensten allerdings nicht verdient: Noch 2016 musste Github 66 Millionen Dollar Verlust abschreiben.

Einhorn in Schwierigkeiten

Obwohl Github Inc. im Silicon Valley schnell zu einem der Lieblinge (Einhörner) unter den Start-up-Unternehmen aufstieg und auf eine Marktbewertung von zwei Milliarden US-Dollar kam, wollten die Probleme bei Github nicht aufhören. Anhaltende Wechsel in der Unternehmensführung von Github Inc. nach Belästigungsvorwürfen gegen einen seiner Gründer und die stetige Suche nach frischem Investorenkapital machten Github schließlich reif für eine Übernahme.

Soweit keine Überraschung, überraschend ist aber der Käufer: Microsoft erhielt Anfang Juni 2018 den Zuschlag, Github Inc. für 7,5 Milliarden US-Dollar zu kaufen. Vorausgegangen waren wochenlange Verhandlungen, auch mit Google. Man kann davon ausgehen, dass es hinter den Kulissen ein Bietergefecht zwischen Google und Microsoft gab, das den Übernahmepreis in enorme Höhen trieb.

Gitlab wächst leicht

Für Microsoft ist die Github-Übernahme Teil einer bereits anhaltenden Verjüngungskur, die CEO Nadella dem Konzern nach dem Abgang Steve Ballmers verordnet hat. Die Windows-Sparte wird verkleinert, Clouddienste und Angebote für Entwickler, speziell Open-Source-Entwickler, bekommen Priorität.

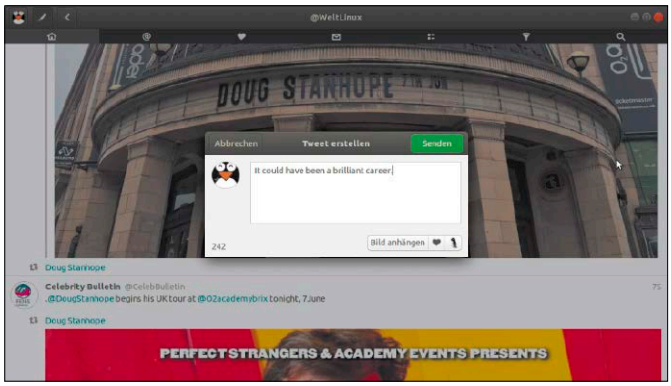
Open-Source und Microsoft – keine Liebe auf den ersten Blick, nachdem Microsofts letzter CEO noch 2001 in einer sehr unglücklichen Wortwahl Linux als „Krebsgeschwür" bezeichnete. Mittlerweile ist aber klar, dass sich Microsofts Haltung gegenüber Linux und Open Source in den letzten 17 Jahren gründlich geändert hat.

Es gab deshalb nur einen verhaltenen Aufschrei in der Entwicklergemeinde zur Übernahme von Github durch den Softwareriesen – zumal die Suche nach einer Alternative nicht schwerfällt: Mit Gitlab (*https://about.gitlab.com*) gibt es einen kleineren, jüngeren Mitbewerber mit einem ähnlichen Werkzeugkasten um Git. Nach der Microsoft-Übernahme wechselten rund 250 000 Projekte zu Gitlab.

Corebird 1.7.

Twitter-Client für Desktops
http://corebird.baedert.org

Der komfortable Twitter-Client Corebird für Linux hat sich in den letzten zwei Jahren viele Freunde gemacht. Corebird ist ein GTK-Programm und fügt sich gut in Desktops ab Gnome 3.20 ein. Hashtags und Mentions sind jetzt anklickbar, die Tweetlänge ist auf 280 Zeichen erhöht und das Editorfenster hat eine Auswahl an Emojis. Corebird ist in den aktuellen Ausgaben von Ubuntu- und Linux Mint per Paketmanager installierbar. Für Fedora gibt es ein Flatpak. ■



Gut getwittert: Corebird unterstützt mehrere Accounts und bietet viele Funktionen, welche der Weboberfläche von Twitter schlicht fehlen.

Flightgear 2018.1.1

Aufwendige Flugsimulation
http://home.flightgear.org

Der Flugsimulator Flightgear setzt auf Realismus und erfüllt im Multimonitorbetrieb höchste Ansprüche. Das Physikmodell stammt von der NASA. Neben den Flugzeugtypen im Basispaket gibt es 500 weitere Flugzeuge frei zum Download. In den 20 Jahren der Entwicklung haben Grafikqualität und Detailtreue enorm zugenommen. Flightgear liegt in den Paketquellen der meisten Linux-Distributionen und umfasst im Basispaket rund 1,5 GB. ■

Große Portion Realismus: Wie andere anspruchsvolle Flugsimulationen verlangt Flightgear vor dem Abheben lange Einarbeitung.

Gerbera 1.2

Streamingserver nach dem UPnP-Protokoll
http://gerbera.io

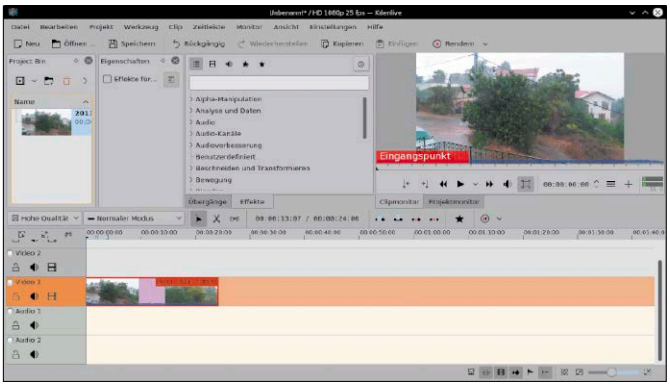
Der Medienserver Mediatomb war ein beliebter Mediaserver für UPnP (Universal Plug and Play), wird aber nicht mehr weiterentwickelt. An seine Stelle ist Gerbera getreten. Installation und Konfiguration erfolgen wie bei Mediatomb über das Terminal und Konfigurationsdateien. Eine Weboberfläche ist dann auf dem Port 49152 verfügbar und erlaubt die Auswahl von Mediadateien. Gerbera ist bereits für Ubuntu 18.04 und Linux Mint 19 verfügbar. ■

Schöner streamen mit neuer Weboberfläche: Gerbera tritt die Nachfolge des kompakten UPnP-Servers Mediatomb an.

Kdenlive 18.04.1

Videoschnittprogramm für gehobene Ansprüche
www.kdenlive.org

Der Open-Source-Videoeditor nutzt die MLT Video Rendering Engine und kommt auf den enormen Funktionsumfang professioneller Videoschnittprogramme. Die aktuelle Version bringt viele Verbesserung der Stabilität sowie der Oberfläche, um Frames zu zentrieren und Text zu platzieren. Außerdem gibt es Kdenlive jetzt zur einfacheren Installation als systemunabhängiges Appimage, als Flatpak, sowie als Snap für Ubuntu (*https://kdenlive.org/en/download*). ■

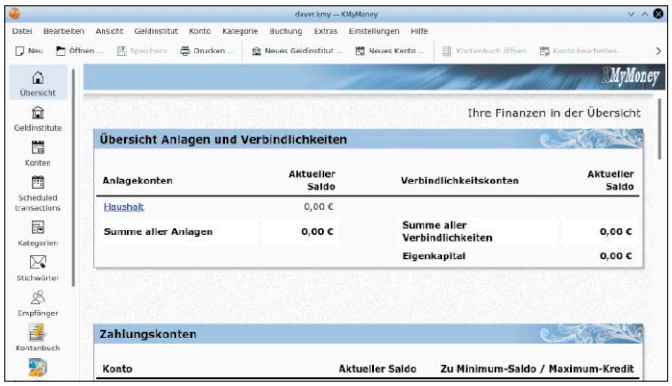


Guter Schnitt: Das Programm Kdenlive für den nicht-linearen Videoschnitt sitzt jetzt fest im Sattel und liefert beständig neue Versionen.

Kmymoney 5.0

Persönliche Finanzverwaltung
www.kmymoney.org

Mit Kmymoney bietet KDE eine Verwaltung für Konten, Aktien und Planung von Einnahmen und Ausgaben. Die Entwickler haben das Open-Source-Programm auf die neuen KDE Frameworks 5 portiert. Kmymoney kann QIF-Dateien einlesen und sich per HBCI/OFX mit Onlinekonten verbinden und Überweisungen einlesen. Überweisen kann Kmymoney aber noch nicht, das muss manuell geschehen. In Ubuntu 18.04 liegt das Programm bereits in den Paketquellen. ■

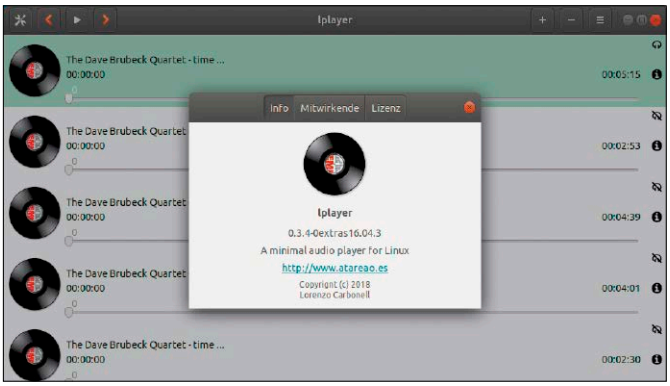


Einnahmen und Ausgaben: Kmymoney kann per HBCI/PFX Transaktionsdaten per Onlinebanking einlesen, jedoch keine Überweisungen ausführen.

Lplayer 0.3.4

Minimalistischer Audioplayer
https://github.com/atareao/lplayer

An Audioplayern herrscht auf dem Linux-Desktop kein Mangel, aber es sind ausgerechnet die Standardplayer Amarok und Rhythmbox der großen Desktops, die nicht recht überzeugen: behäbig, zu viele Funktionen, großer Ressourcenbedarf. Lplayer ist ein Minimalist mit optionalen Funktionen wie Equalizer. Mit seiner GTK3-Oberfläche ist der Player gut für Gnome-affine Desktops. Fertige Pakete für Ubuntu liefert ein PPA (*https://github.com/atareao/lplayer*). ■

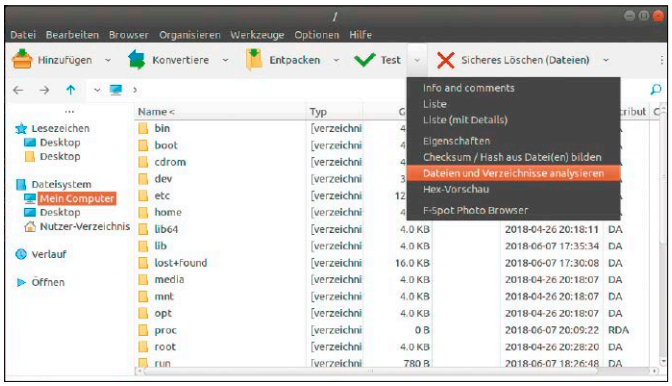


Hier spielt die Musik: Lplayer ist ein kompakter Player für MP3, OGG, Flac und M4A. Ein Equalizer lässt sich einblenden.

Peazip 6.6

Packer-Suite für Fortgeschrittene
http://peazip.sourceforge.net

Ein Packprogramm wie Ark (KDE) oder Fileroller (Gnome) hat jede gut sortierte Linux-Distribution dabei. Das plattformübergreifende Open-Source-Programm Peazip unterstützt aber deutlich mehr Formate (mehr als 150), beispielsweise auch RAR und 7Z. Auch mit Archiven wie JAR sowie Libre-Office-Dateien kommt Peazip klar. Auf der Projektseite steht es für Linux als DEB und RPM bereit sowie als ausführbare Binary, die keine Installation voraussetzt. ■

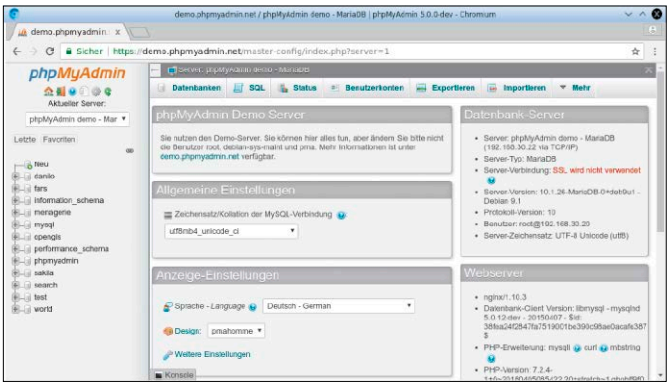


Kann einpacken: Peazip ist ein Meister der Packformate, bietet einen Dateimanager, Verschlüsselung und eine neue Duplikatssuche.

Phpmyadmin 4.8.1

Datenbankverwaltung im Browser
www.phpmyadmin.net

Bei der Arbeit an Datenbanken (My SQL, Maria DB), für Backups und Reparaturen ist Phpmyadmin mit seiner Browseroberfläche eine veritable Hilfe. Die Oberfläche unterstützt nun zur Anmeldung Zwei-Faktor-Authentifizierung und läuft auf Mobilgeräten – ideal für Notfälle, die unterwegs gelöst werden müssen. Phpmyadmin 4.8.x ist die letzte Version, die PHP 5 unterstützt. Eine Demo der neuen Version gibt es unter *https://demo.phpmyadmin.net/master-config*. ■

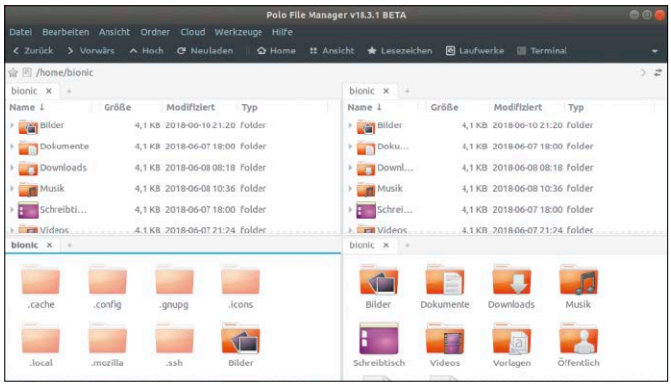


Datenbanken im Griff: Phpmyadmin läuft jetzt nicht nur auf dem Desktopbrowser, sondern auch unterwegs auf Smartphones und Tablets.

Polo 18.3.1

Dateimanager für Poweruser
https://github.com/teejee2008/polo/releases

Meist geht es bei Dateioperationen darum, Verzeichnisse und Dateien von A nach B zu bringen. Dateimanager mit zwei Fenstern erfüllen dies am besten. Polo erlaubt die Aufteilung seiner Fenster in bis zu vier Teile. Dort zeigt der Dateimanager lokale Ordner, SSH-, FTP-, SFTP und Samba-Verbindungen. Cloudspeicher wie Dropbox und Google kann Polo über Rclone einbinden. Das PPA *https://launchpad.net/~teejee2008/+archive/ubuntu/ppa* bietet Pakete für Ubuntu.

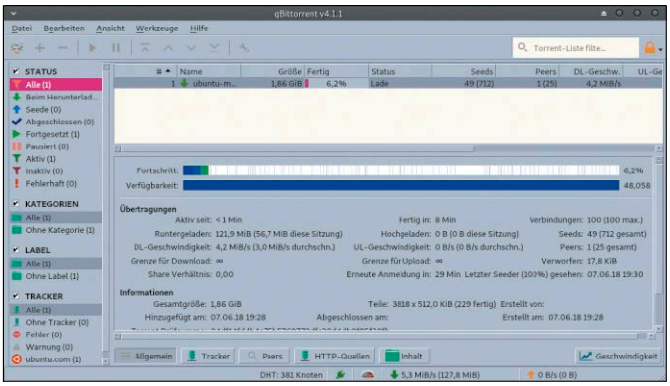


Vierteilen! Der Dateimanager Polo ist mit seinem Funktionsumfang trotz Betastatus bereits eine gute Ergänzung für den Gnome-Desktop.

Qbittorrent 4.1

Bittorrent-Client mit Weboberfläche
www.qbittorrent.org

Bittorrent-Downloads können eine langwierige Sache sein, daher sind Bittorrent-Programme gut auf einem sparsamen Server aufgehoben. Qbittorrent mit Weboberfläche ist eine gute Wahl: Das Tool kann auf dem Server im Hintergrund laufen und per Browser bedient werden. Qbittorrent liegt in den Paketquellen verbreiteter Distributionen. Für Ubuntu gibt es zudem das PPA *https://launchpad.net/~qbittorrent-team/+archive/ubuntu/qbittorrent-stable*.

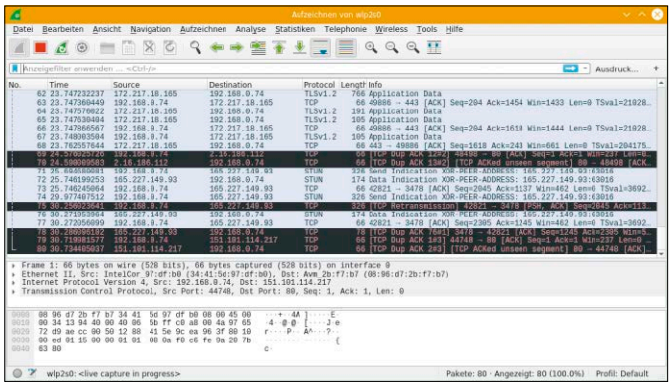


Bittorrent par excellence: Qbittorrent fühlt sich als Downloadclient auf Linux-Servern wohl und lässt sich per Weboberfläche steuern.

Wireshark 2.6

Netzwerksniffer und Paketanalyse
www.wireshark.org

Der Netzwerksniffer lauscht an beliebigen Netzwerkschnittstellen, zeichnet Netzwerkpakete auf und stellt sie in einer Tabelle dar. Zur Auswertung gibt es Filter- und Dekodierungsfunktionen. Die aktuelle Version baut ihre Unterstützung für Netzwerkprotokolle aus, vereinfacht die Filterfunktionen und ist die letzte Ausgabe mit GTK-Oberfläche. Künftig wird Wireshark nur noch mit Qt-Toolkit ausgeliefert. Wireshark 2.6 liegt bereits in den Paketquellen Fedoras.

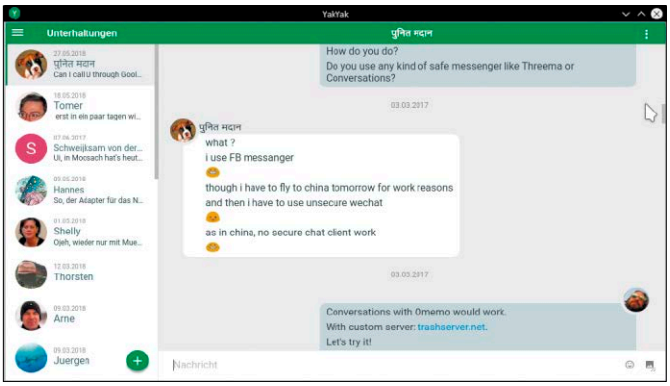


Blick auf den Netzwerkverkehr: Wenn der private Schlüssel vorliegt, kann Wireshark SSL/TLS-verschlüsselte Protokolle dechiffrieren.

Yak Yak 1.5.1

Client für Google Hangouts
https://github.com/yakyak/yakyak

Die offizielle App für Google Hangouts verlangt stets nach einem laufenden Chrome/Chromium. Eleganter stellt Yak Yak eine Verbindung zu den Google Hangouts her. Es handelt sich um eine Electron-App mit eigener Browserkomponente, die sich wie ein natives Linux-Programm verhält. Yak Yak zeigt Benachrichtigungen über Nachrichten, hat mehrere Farbschemata und kann sein Fenster verstecken. Die Github-Seite liefert fertige DEB- und RPM-Pakete.



Proper parlieren: Yak Yak bringt Google Hangouts als Electron-App auf den Linux-Desktop. Es liegt auch als Snap und Flatpak vor.

IPTV-Server für das Heimnetzwerk

Im Heimnetz lassen sich mehrere Geräte mit Fernsehprogrammen versorgen. Ein TV-Server stellt dafür die Streams bereit und ermöglicht auch den Mitschnitt von Sendungen.

Fernsehen mit Kodi: Die Mediacentersoftware Kodi bringt auch TV-Kanäle auf den Bildschirm. Dafür ist aber ein eigener IPTV-Server im Netzwerk erforderlich.

VON THORSTEN EGGELING

Die Programme der Fernsehsender können auf unterschiedlichen Wegen auf Ihre Geräte gelangen. Die klassische Methode sind Tuner in Fernsehern oder TV-Receivern, die per Koaxialkabel von einer Satellitenschüssel, einer Antenne oder einem Kabelnetzanbieter versorgt werden. Eine Alternative oder Ergänzung ist Streaming über das Internet. Smart-TVs bieten über Apps beispielsweise Zugriff auf die Mediatheken der öffentlich-rechtlichen Sender und auf kommerzielle Streamingdienste. Ein eigenes Multimedia-Netzwerk können Sie sich aber auch selbst aufbauen. Unterschiedliche Empfangswege wie Fernsehen über Satellit, Antenne oder Internet lassen sich unter einer einheitlichen Oberfläche zusammenfassen und mit weiteren Streamingangeboten kombinieren. Über WLAN oder Ethernet-Kabel verteilen Sie das Angebot an alle Geräte im heimischen Netzwerk.

1. Fernsehen über Kabel, Satellit, Antenne und Internet

Beim Fernsehempfang kommt es auf den Wohnort und die verfügbare Infrastruktur an. In Ballungsräumen ist meist TV über das Kabelnetz (DVB-C/C2) verfügbar. Die zusätzliche „2“ bei diesem und auch den anderen DVB-Standards (Digital Video Broadcasting) weist auf eine weiterentwickelte Technik mit verbesserter Qualität und meist auch höherer Auflösung hin. Aktuelle Geräte unterstützen sowohl das ältere DVD-C als auch DVB-C2. Sie müssen für die Bereitstellung ein Nutzungsentgelt zahlen – auch für sonst frei empfangbare Sender. Wie hoch es ist, hängt von Wohnort und Anbieter ab.

DVB-S beziehungsweise DVB-S2 sind überall verbreitet, wo die Montage einer Satellitenschüssel kein Problem ist. Das Signal erhalten Sie für die frei empfangbaren Sender kostenlos per Satellit, was in Europa über die Astra-Satellitenflotte so gut wie flächendeckend möglich ist. Privatsender gibt es manchmal nur in SD-Qualität gratis, die öffentlich-rechtlichen Sender auch in HD.

Das als Überall-Fernsehen beworbene DVB-T (seit April 2017 DVB-T2) kommt über die Antenne, bietet aber nur ein eingeschränktes Programmangebot. Die öffentlich-rechtlichen Sender gibt es kostenlos. Privatsender sind verschlüsselt und nur nach Abschluss eines Abos zu empfangen (siehe *www.pcwelt.de/2158822*).

Für alle genannten DVB-Techniken benötigen Sie einen Tuner im Fernseher oder ein externes Gerät. Für den PC gibt es Steckkarten oder USB-DVB-Sticks.

TV aus dem Internet: Die meisten öffentlich-rechtlichen Sender streamen das Liveprogramm kostenlos ins Internet. Allerdings wird der Livestream unterbrochen, wenn die Internetlizenz für den Inhalt fehlt, was bei fast allen fremdproduzierten Filmen der Fall ist. International ist die Menge der Streaminganbieter fast unüberschaubar. Eine Google-Suche etwa nach „iptv playlist“ führt Sie zu zahlreichen Adresslisten. Einiges davon ist allerdings wohl halblegal, beispielsweise Server, die aktuelle

Satelliten-TV: Für Astra reicht meist schon eine kleine SAT-Schüssel, wenn Sie freien Blick auf den Satelliten haben. Die wichtigsten deutschsprachigen Sender können Sie kostenlos sehen.

DVB-T2: Terrestrisches Fernsehen kann man über Antenne auch unterwegs auf dem Smartphone nutzen. Der TV-Empfang ist jedoch noch nicht in allen Regionen möglich.

IPTV-Server: Der Telestar Digibit R1 verfügt über vier DVB-S2-Tuner und kann daher gleichzeitig vier Geräte über das Netzwerk mit TV-Programmen versorgen.

Sportereignisse übertragen und dafür wahrscheinlich keine Lizenzen besitzen.

2. Hardware für den eigenen TV-Streamingserver

Für den TV-Empfang am PC benötigen Sie eine TV-Steckkarte oder einen TV-Stick mit dem passenden Tuner. Oft gibt es Kombinationen von DVB-C2/DVB-T2 oder Geräte, die nur DVB-S/S2 empfangen können. Für einen TV-Server sind die Geräte für den PC allerdings kaum empfehlenswert. Nicht jedes Modell lässt sich unter Linux problemlos in Betrieb nehmen. Außerdem steigen CPU-Belastung und Leistungsaufnahme. Wer es trotzdem probieren möchte, findet auf *https://linuxtv.org* Informationen zur den unterstützten Geräten und Hinweise zur Installation.

Besser geeignet sind Netzwerk-TV-Tuner (IPTV-Server), die als unabhängige Geräte DVB im Netzwerk bereitstellen. Die Vorteile: Sie benötigen keinen Treiber, da der Datenaustausch über standardisierte Netzwerkprotokolle erfolgt. Der Betrieb ist auch unabhängig vom PC möglich, etwa mit einer App auf dem Smartphone. Es lassen sich so viele Clients versorgen, wie DVB-Tuner im Gerät stecken.

Bei IPTV-Servern für DVB-S gibt es ein breites Angebot. Eine Übersicht finden Sie auf *www.satip.info*. Es gibt Geräte, die eher für die Montage auf dem Dachboden in der Nähe der Satellitenschüssel gedacht sind, beispielsweise Telestar Digibit Twin mit zwei Tunern (etwa 110 Euro, *https://telestar.de*). Telestar Digibit R1 (etwa 180 Euro, vier Tuner) und Digital Devices Octopus NET V2 S2/2 (etwa 299 Euro, zwei Tuner) sind von der Bauweise her für die Wohnung geeignet. Wo immer Sie die Geräte auch unterbringen, in jedem Fall benötigen Sie ein eigenes Koaxialkabel für jeden DVB-S2-Tuner, das von der Satellitenschüssel zum IPTV-Server führt. Bei DVB-C2 reicht ein einzelnes Koaxialkabel. Die Verteilung kann über einen einfachen Zweigeräteadapter erfolgen. Die Ausgänge im Octopus Net dienen zur Versorgung nachgeschalteter Geräte wie Fernseher oder Set-Top-Box. Für DVB-T2 genügt in Ballungsräumen eine Zimmerantenne mit oder ohne Antennenverstärker. Ist der Sender zu weit entfernt, benötigen Sie eine Dachantenne. Informationen zu den Empfangsgebieten erhalten Sie auf *www.dvb-t2hd.de/empfangscheck*.

Die Verbindung zum Netzwerk erfolgt über ein Ethernet-Kabel. Alternativ sind auch Power-LAN-Adapter oder Ethernet/WLAN-Adapter möglich. Beachten Sie, dass das Netzwerk bei gleichzeitigem Zugriff auf zwei Tunern ungefähr 16 Megabit/s (SD) oder 32 Megabit/s (HD) stabil transportieren muss. Das ist für Fast-Ethernet (100 MBit/s) kein Problem und erst recht nicht für das mittlerweile verbreitete Gigabit-Ethernet (1000 MBit/s). Bei Power-LAN und vor allem bei WLAN kann es unter ungünstigen Bedingungen jedoch knapp werden. Die Folge sind Bildausfälle oder der IPTV-Server ist nicht mehr erreichbar. Sorgen Sie daher für eine optimale WLAN-Abdeckung und Geschwindigkeit.

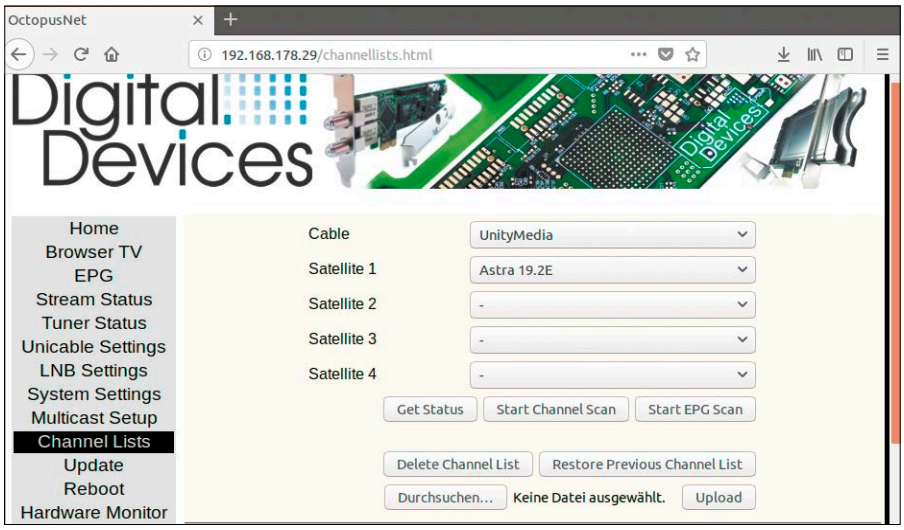
3. IPTV-Server konfigurieren und testen

Nach Inbetriebnahme des Gerätes rufen Sie dessen Weboberfläche mit „http://[IP-Adresse]“ auf. Den Wert für „[IP-Adresse]“ bekommen Sie sie über die Weboberfläche Ihres DSL-Routers oder Kabelmodems heraus, die Sie im Browser beispielsweise über „http://192.168.0.1“ oder

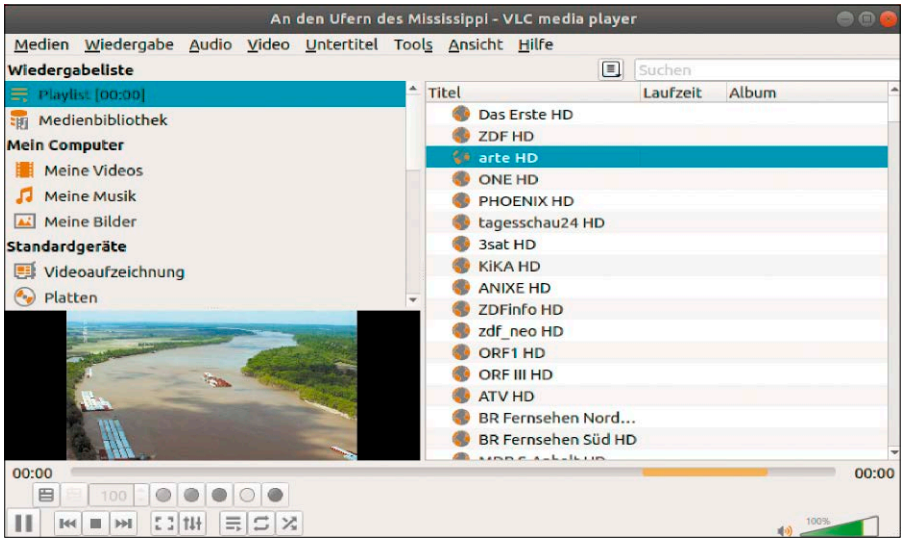
STREAMINGCLIENTS FÜR PC, TV-GERÄT UND SMARTPHONE

Kodi (*https://kodi.tv*) ist eine gut bedienbare Multimedia-Oberfläche mit vielen Funktionen. Sie finden die Software über die Paketverwaltung der meisten Linux-Distributionen und für Android bei Google Play. Für den Raspberry Pi empfiehlt sich die für das Gerät optimierte Distribution Libre Elec, die Kodi enthält. Eine Installationsanleitung finden Sie unter *www.pcwelt.de/2301815*.

Für Tvheadend benötigt Kodi ein Add-on, das Sie unter Linux über das Paket „kodi-pvr-hts“ installieren. Auf dem Raspberry Pi oder unter Android installieren Sie das Add-on „Tvheadend HTSP Client“. In die Konfiguration des Add-ons tragen Sie die IP-Adresse des Tvheadend-Servers ein. Geben Sie Benutzernamen und Passwort des bei Tvheadend angelegten Benutzers an oder lassen Sie die Felder leer, wenn Sie den anonymen Zugriff erlaubt haben (Benutzer „*“). Im Hauptmenü starten Sie die Fernsehwiedergabe über „TV“, indem Sie nach einem Klick auf „Kanäle“ oder „Guide“ zum gewünschten Kanal navigieren. Laufende Sendungen nehmen Sie mit der „Aufnehmen“-Schaltfläche auf. Über den „Guide“ lassen sich Aufzeichnungen auch planen, um sie später in Kodi anzusehen.



IPTV-Server konfigurieren: Die Einstellungen für das Gerät nehmen Sie über die Weboberfläche vor. Sie lassen nach Kanälen suchen, die dann als m3u-Kanalliste abrufbar sind.



VLC als TV-Empfänger: Öffnen Sie die m3u-Kanalliste in VLC. Über die Wiedergabeliste wählen Sie den gewünschten Kanal aus und ein Vorschauvideo erscheint im Fenster.

„http://192.168.178.1" (Fritzbox) erreichen. Suchen Sie in den Einstellungen den DHCP-Server. In diesem Bereich finden Sie meist auch die DHCP-Client-Liste. Bei einer Fritzbox finden Sie die Liste unter „Heimnetz → Heimnetzübersicht".

Die Einrichtung eines IPTV-Servers läuft im Prinzip immer gleich ab. Sie erzeugen auf dem Gerät eine Kanalliste, die dann später die Clients über die IP-Adresse und die verfügbaren Tuner und Kanäle informiert.

Bei einem Octopus Net beispielsweise gehen Sie in der Weboberfläche auf „Channel List", wählen hinter „Cable" (DVB-C) oder „Satellite 1" bis „Satellite 4" (DVB-S) den gewünschten Anbieter aus und klicken auf „Start Channel Scan". Nach Abschluss des Scans laden Sie die m3u-Datei über den Link hinter „Channel List:" herunter. Da es sich um einfache Textdateien handelt, können Sie die m3u-Dateien in einem Editor öffnen und bearbeiten. Entfernen Sie Zeilen mit Sendern, die Sie nicht benötigen, und passen Sie bei Bedarf die Senderbezeichnungen an. Am besten erstellen Sie eine neue m3u-Datei, in die Sie die Zeilen für alle gewünschten SD-, HD- und Radiosender kopieren.

IPTV-Server ausprobieren: Die m3u-Datei öffnen Sie beispielsweise im VLC Mediaplayer. Gehen Sie auf „Ansicht → Wiedergabeliste". In der Liste sehen Sie alle Einträge der Playliste, der Kanal lässt sich per Doppelklick wechseln.

4. Streamingserver Tvheadend installieren

In Ihrem Netzwerk läuft jetzt zwar schon ein IPTV-Server, dem aber ein paar wichtige Funktionen fehlen. Wenn Sie TV-Sendungen auch aufzeichnen wollen und erfahren möchten, was gerade im Fernsehen läuft, benötigen Sie weitere Software.

Tvheadend (*https://tvheadend.org*) ist ein Streamingserver für Linux, der alle verbreiteten DVB-Standards unterstützt. Die Konfiguration erfolgt über eine Weboberfläche im Browser.

Tvheadend läuft unter den meisten Linux-Distributionen, ist aber in der Regel nicht in den Standard-Repositorien enthalten. Wer keinen stromhungrigen PC für den Server verwenden möchte, installiert Tvheadend auf einem Raspberry Pi. Die Installation verläuft bei Raspbian und Ubuntu ähnlich.

Raspberry Pi (Raspbian): Wir gehen davon aus, dass Sie auf dem Raspberry Pi das aktuelle Raspbian Stretch installiert haben (*www.raspberrypi.org/downloads/raspbian*). Führen Sie im Terminal die folgenden fünf Befehle aus:

```
sudo apt install dirmngr apt-
  transport-https
sudo apt-key adv --keyserver hkp://
  keyserver.ubuntu.com:80 --recv-
  keys 379CE192D401AB61
sudo echo "deb https://dl.bintray.
  com/mpmc/deb raspbianstretch
  stable-4.2" | sudo tee -a /etc/apt/
  sources.list
sudo apt update
sudo apt install tvheadend
```

Sie werden aufgefordert, Benutzername und Passwort für den Administrator festzulegen. Diese Daten gelten nur für die Erstinstallation.

Ubuntu 18.04: Bei Ubuntu verwenden Sie diese fünf Befehlszeilen:

```
sudo apt-get install dirmngr
wget -qO- https://doozer.io/keys/
  tvheadend/tvheadend/pgp | sudo
  apt-key add -
sudo echo "deb http://apt.
  tvheadend.org/unstable bionic
  main" | sudo tee -a /etc/apt/
  sources.list.d/tvheadend.list
sudo apt update
sudo apt install tvheadend
```

Geben Sie den Benutzernamen und das Passwort des administrativen Benutzers ein, wenn Sie dazu aufgefordert werden.

5. Tvheadend konfigurieren

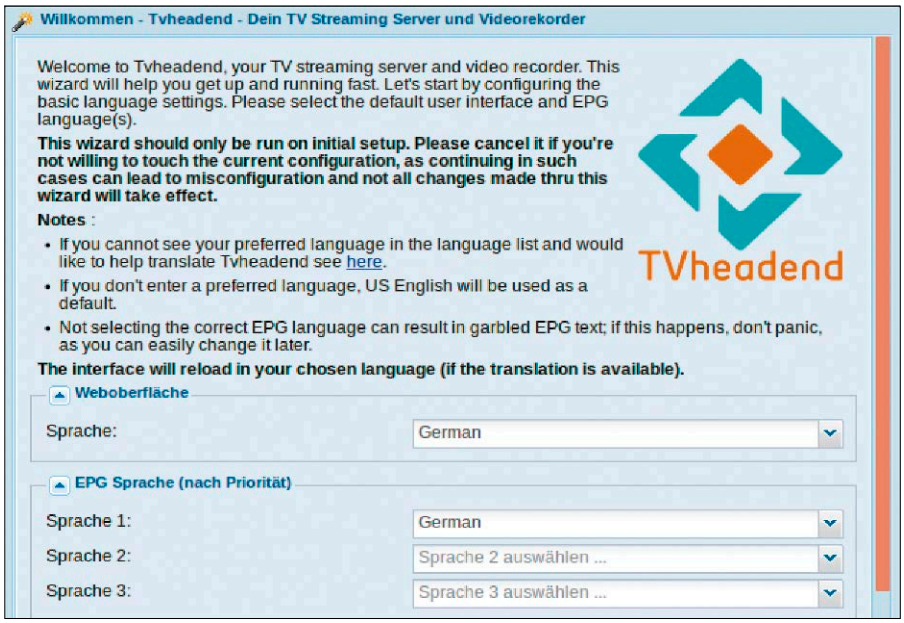
Öffnen Sie im Browser die Adresse „http://[ip-adresse]:9981“. Den Platzhalter „[ip-adresse]“ ersetzen Sie durch die IP-Nummer Ihres Raspberry Pi oder Ubuntu-PCs. Melden Sie sich bei Tvheadend an. Ein Assistent führt durch die nötigen Schritte. Zuerst stellen Sie die Sprache ein und legen dann Benutzernamen und Passwörter für den administrativen Benutzer und einen Standardbenutzer fest. Beim Standardbenutzer verwenden Sie für beides jeweils „*“ (ohne Anführungszeichen), wenn keine Anmeldung erforderlich sein soll. Klicken Sie auf „Save & Next“.

Im Fenster „Netzwerkeinstellungen“ wählen Sie bei „Netzwerk 1“ den Eintrag „IPTV Automatisches Netzwerk“ aus der Liste und klicken auf „Speichern & Weiter“. Tippen Sie die URL ein, über die sich die m3u-Liste vom IPTV-Server herunterladen lässt (siehe Punkt 3), und klicken Sie auf „Speichern & Weiter“. Danach scannt Tvheadhend die verfügbaren Kanäle. Sollte das Programm nichts finden, kann es wahrscheinlich die Liste nicht vom Server abholen. In diesem Fall kopieren Sie die in Punkt 3 heruntergeladene m3u-Datei nach „/home/hts“, beispielsweise unter dem Namen „channels.m3u“. Blättern Sie im Tvheadend-Assistenten zurück und tippen Sie als „URL“

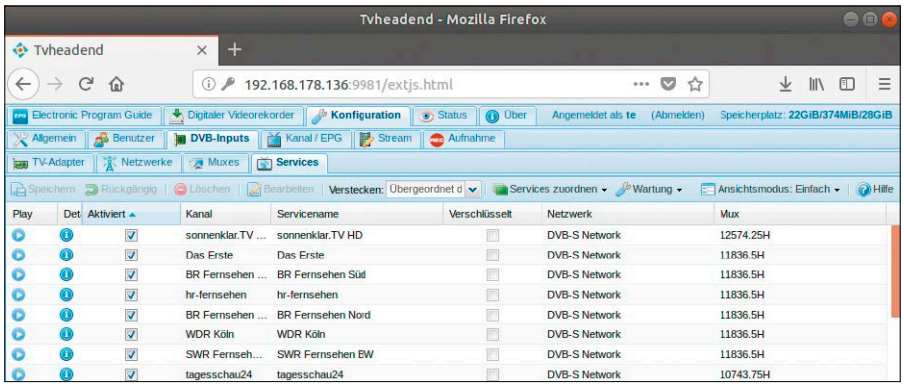
```
file:///home/hts/channels.m3u
```

ein. Wenn Sie jetzt erneut auf „Speichern & Weiter“ klicken, sollte es funktionieren. Sie sehen dann eine Fortschrittsanzeige, die bei DVB-S2 mehrere Hundert Muxes finden sollte. Klicken Sie auf „Speichern & Weiter“, wenn der Vorgang abgeschlossen ist. Im Fenster „Service Mapping“ setzen Sie keine Häkchen, sondern klicken nur auf „Speichern & Weiter“ und danach auf „Fertigstellen“.

Gehen Sie auf „Konfiguration → DVB-Inputs → Services“. Klicken Sie auf „Services zuordnen → Alle Services zuordnen“. Entfernen Sie das Häkchen hinter „Verschlüsselte Services einschließen“ und setzen Sie eines hinter „Verfügbarkeit testen“. Klicken Sie auf „Services zuordnen“. Die Prüfung dauert eine Weile. Danach gehen Sie auf „Konfiguration → Kanal/EPG“. Entfernen Sie die Häkchen in der Spalte „Aktiviert“ bei allen Sendern, die Sie nicht sehen wollen, und klicken Sie auf „Speichern“. In die Spalte „Nummer“ lässt sich nach einem Doppelklick eine Ziffer eintragen und damit die Sortierung der Sender ändern.



Ersteinrichtung: Tvheadend startet mit einem Assistenten, der Sie bei der Konfiguration unterstützt. Es sind nur wenige Schritte nötig, die Kanalsuche dauert jedoch einige Zeit.



Kanalvielfalt: Über DVB-C2 und DVB-S2 empfangen Sie Hunderte von Sendern. Verschlüsselte Angebote lassen sich herausfiltern, für mehr Übersicht sollten Sie die Kanalliste bearbeiten.

6. TV-Streams aus dem Internet einbinden

Streamingangebote aus dem Internet lassen sich ähnlich in Tvheadend einbinden wie die m3u-Liste eines lokalen IPTV-Servers. Eine Übersicht mit Anbietern wie 3sat, Das Erste und ZDF finden Sie über *www.pcwelt.de/IPTV*.

Gehen Sie in der Tvheadend-Weboberfläche auf „Konfiguration → DVB-Inputs → Netzwerke“. Klicken Sie auf „Hinzufügen“, wählen Sie „IPTV Netzwerk“ und tippen Sie eine Bezeichnung ein, beispielsweise „IPTV-Sender“. Klicken Sie auf „Anlegen“. Wechseln Sie dann zur Registerkarte „Muxes“, und klicken Sie auf „Hinzufügen“. Wählen Sie das eben angelegte Netzwerk „IPTV-Sender“. Tragen Sie in das Feld hinter „URL:“ eine Adresse ein, beispielsweise

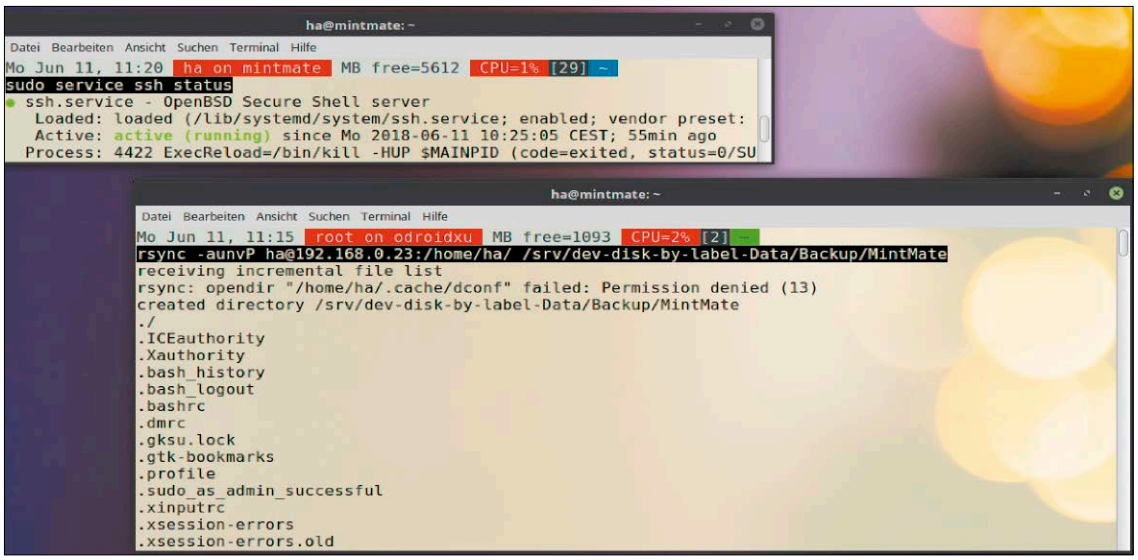
```
https://zdf1314-lh.akamaihd.
  net/i/de14_v1@392878/master.m3u8
```

für das ZDF („hohe Qualität“, 1280 x 720). Bei den Feldern „Mux-Name:“ und „Servicename:“ tippen Sie jeweils eine aussagekräftige Bezeichnung ein, etwa „ZDF-IPTV“. Klicken Sie auf „Anlegen“. Wechseln Sie auf die Registerkarte „Services“, suchen Sie dort den eben hinzugefügten Servicenamen und klicken Sie ihn an. Gehen Sie auf „Ausgewählte zuordnen → Gewählte Services zuordnen“.

Wechseln Sie danach auf „Kanal /EPG → Kanäle“. Der neue Sender ist hier zu sehen und Sie können ihm in der Spalte „Nummer“ eine Kanalnummer zuweisen. Der externe IPTV-Server erscheint bei den Clients genauso wie die Kanäle des eigenen IPTV-Servers. ■

Aktiver Backupserver

Für einen Backupserver im Heimnetz genügt ein Platinenrechner wie der Raspberry. Besser ist eine Alternative mit Gigabit-Ethernet (Odroid, Cubieboard). Wer einen solchen Server für die Datensicherung nutzt, hat die Wahl: „Push“ oder „Pull“?



Aktives Pull-Backup über SSH: Wenn auf dem Linux-Client der SSH-Server läuft (oben), genügt auf dem Backupserver ein Rsync-Befehl zur Sicherung.

VON HERMANN APFELBÖCK

Die sehr unterschiedlichen Methoden, die Daten von PCs und Notebooks auf einen Server zu sichern, sind den meisten PC-Nutzern gar nicht bewusst: Typischerweise bietet der Server Netzwerkfreigaben an und die Sicherungsdaten werden von den Clients dorthin kopiert („Push“).

Je nach Umfeld einfacher oder eleganter ist der umgekehrte Weg („Pull“): Hier ist der Backupserver der aktive Spieler und holt sich die Dateien von den Netzclients (Linux, Windows, Mac-OS). Wobei der Begriff „Clients“ hier genau genommen nicht zutrifft: Es findet ein Rollentausch statt, bei dem der Backupserver zum zugreifenden Client wird.

Push oder Pull: Die Vor- und Nachteile

Die Vorteile von „Pull“? Das Backupgeschäft ist hier zentral in einer Hand und nicht mehr von der Disziplin oder von Automatismen diverser Clients und Clientbenutzer abhängig. Das macht die Sache mit einem einheitlichen Werkzeug wie Rsync oder Tar einfacher, übersichtlicher und vor allem zuverlässiger.

Auf den Clientrechnern muss man sich nach einer einfachen Grundeinrichtung um nichts mehr kümmern. Da die Clients gar keinen eigenen Zugriff auf das Serverbackup haben, ist auch das Einschleusen von Netzwürmern unterbunden. Natürlich können auch Backupdaten Viren enthalten, die aber der Linux-Backuprechner nicht ausführen wird.

Nachteile gibt es natürlich auch: Der Client (-Benutzer) verliert die alleinige Kontrolle über seine Daten, da der Backupserver (und dessen Administrator) Zugriff hat. Ferner hat er auch seine Backups nicht mehr selbst in der Hand. Wenn er nach Datenverlust Backupdateien benötigt, muss er sich an den Administrator des Backupservers wenden. Daher ist die „Pull“-Methode am besten für ein kleines oder privates Netzwerk geeignet. Gar keine Gegenanzeigen ergeben sich, wenn Sie die Pull-Methode nur für mehrere eigene Rechner einsetzen.

Pull-Backups von Linux- und Mac-Rechnern

Beim Ziehen von Backupdaten hat der Backupserver bei Linux- und Mac-Rechnern leichtes Spiel, sofern er dort auf einen Open-SSH-Server trifft. Beim Mac muss in den Systemeinstellungen nur die „Entfernte Anmeldung“ aktiviert sein, damit der SSH-Server läuft. Bei Linux-Desktopsystemen ist der Open-SSH-Server meistens nicht Standard, aber mit

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

auf Debian/Ubuntu/Mint schnell nachinstalliert und damit sofort dauerhaft aktiv. Für die Anmeldung per SSH etwa mit

```
ssh ha@192.168.0.23
```

ist bekanntlich ein Systemkonto (hier „ha“) und dessen Passwort erforderlich. Es ist Ermessensfrage, wie umfassend der Backupserver per SSH auf den Desktoprechner zugreifen darf und soll. Im einfachsten Fall verwendet der Desktopbenutzer genauso

wie der Backupserver per SSH den bei der Installation eingerichteten Erstbenutzer, was dann via sudo-Recht Vollzugriff auf alle Daten bedeutet.

Sicherungen erfolgen dann mit einem einzigen Rsync-Befehl, der die SSH-Shell direkt nutzen kann:

```
rsync -auvP ha@192.168.0.23:/home/
  ha /srv/backup/mint19mate
```

In diesem Beispiel ist 192.168.0.23 die IP-Adresse des Desktoprechners, der gesichert werden soll. Die Sicherung soll sich auf das Home-Verzeichnis des Benutzers „ha“ beschränken. Dies ist zugleich das Konto, mit dem sich der Backupserver verbindet („ha@...“) und dessen Passwort abgefragt wird, bevor die Sicherung starten kann. Gesichert wird auf einen Datenträger „backup“, der unter „/srv“ gemountet ist. Das Zielverzeichnis „mint19mate“ kennzeichnet das gesicherte Desktopsystem. Der Rsync-Schalter „a“ sorgt für rekursive Sicherung, „u“ für Überspringen vorhandener Dateien (schneller), „v“ und „P“ machen die Ausgabe gesprächiger.

Ein Befehl wie der obige ist mächtig, aber zunächst nur interaktiv möglich, weil Sie auf dem Backupserver manuell arbeiten und das Systempasswort eingeben müssen. Um die Sicherung weitgehend (Alias) oder vollständig (Crontab-Eintrag) zu automatisieren, müssen Sie die Passworteingabe vermeiden und die manuelle Anmeldung durch eine Schlüsseldatei ersetzen. Der folgende Befehl erstellt den Schlüssel auf dem Backuprechner:

```
ssh-keygen -t rsa -b 4096
```

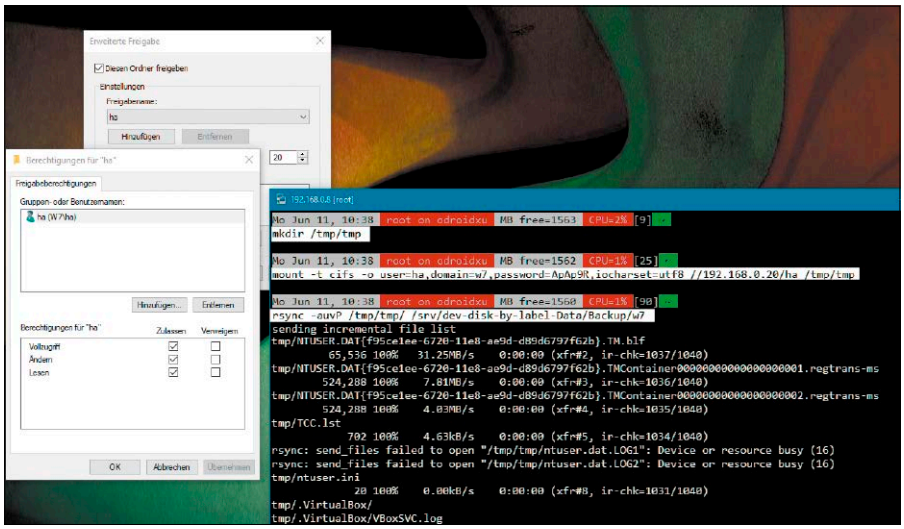
Bestätigen Sie die Standardvorgabe für die Schlüsseldatei („~/.ssh/id_rsa“) mit der Eingabetaste. Mit dem zweiten Befehl

```
ssh-copy-id -i ~/.ssh/id_rsa.pub
  [User]@[IP-Adresse]
```

kopieren Sie dann den öffentlichen Teil des Schlüssels zum Desktoprechner („IP-Adresse“). Ab der nächsten SSH-Anmeldung des Backuprechners dieses Users auf dieser IP-Adresse ist kein Passwort mehr erforderlich.

Pull-Backups von Windows-Rechnern

Wie schon bei SSH mit Linux-Clients erfordern auch Pull-Backups von Windows-Rechnern vertauschte Rollen: Der Backupserver wird – wie bei SSH – zum zugreifenden Client und das Clientgerät quasi zum Dateiserver. Da Windows sich dem Thema SSH gerade erst öffnet (Beta) und die Serverkomponente noch nicht alltagstauglich ist, muss hier eine Netzfreigabe auf dem Windows-Rechner als Brücke dienen.



Pull-Sicherung eines Windows-Rechners: Hier ist eine passende Freigabe erforderlich, damit der Backuprechner jederzeit die Daten abholen kann.

Wir gehen hier beispielhaft davon aus, dass das Userverzeichnis des Hauptbenutzers (quasi „home“) als Sicherungsquelle ausreicht. Dazu müssten Sie zunächst auf dem Windows-Rechner dieses Verzeichnis freigeben – etwa „\users\ha“. Dazu verwenden Sie nach Rechtsklick auf dieses Verzeichnis und „Eigenschaften“ das Register „Freigabe → Erweiterte Freigabe“, aktivieren oben die Freigabe und navigieren über „Berechtigungen“ zum zutreffenden Benutzerkonto (hier „ha“). Diesem geben Sie „Vollzugriff“ für die Netzfreigabe. Da dieser User in seinem „Home“ auch die lokalen Dateirechte hat, sind Rechteprobleme auszuschließen. Auf der Seite des Backupservers muss dann für jede Sicherung Folgendes geschehen:

1. Sie mounten die Windows-Freigabe irgendwo ins lokale Dateisystem (hier unter „/tmp/tmp“):

```
mkdir /tmp/tmp
mount -t cifs -o user=ha,domain=w10
  'password=xyzxyz'iocharset=utf8
  //w10/ha /tmp/tmp
```

2. Danach sichern Sie vorzugsweise wieder mit Rsync vom Mountpunkt der Freigabe zum eigentlichen Backupziel:

```
rsync -auvP /tmp/tmp/
  /srv/backup/w10
```

Hinweise: Zum Mounten von Windows-Freigaben muss unbedingt das Paket „cifs-utils“ installiert sein. Das ist oft, aber nicht überall Standard. Die Mountoption „iocharset=utf8“ ist dringend zu empfehlen, um Sonderzeichenprobleme in Dateinamen zu vermeiden.

In der Mountoption „domain=“ kann statt des Hostnamens des Windows-Rechners (im Beispiel „w10“) auch die Netzwerkgruppe angegeben werden – standardmäßig „workgroup“, sofern nichts anderes definiert wurde. ■

RSYNC MIT TESTLAUF

Rsync, das Tool der Wahl für Backups, kann bei falschen Quell- oder Zielverzeichnissen beträchtliche Datenmassen an falscher Stelle produzieren. Und es wird, wenn Sie den Schalter „--delete“ für 1:1-Spiegelsicherung verwenden (also nicht mehr vorhandene Quelldateien im Backupziel löschen) bei falschen Ordnerangaben zur Massenvernichtungswaffe. Daher müssen alle Backupbefehle vor einer Automatisierung getestet werden. Dazu dient der Schalter „--dry-run“ oder abgekürzt „-n“:

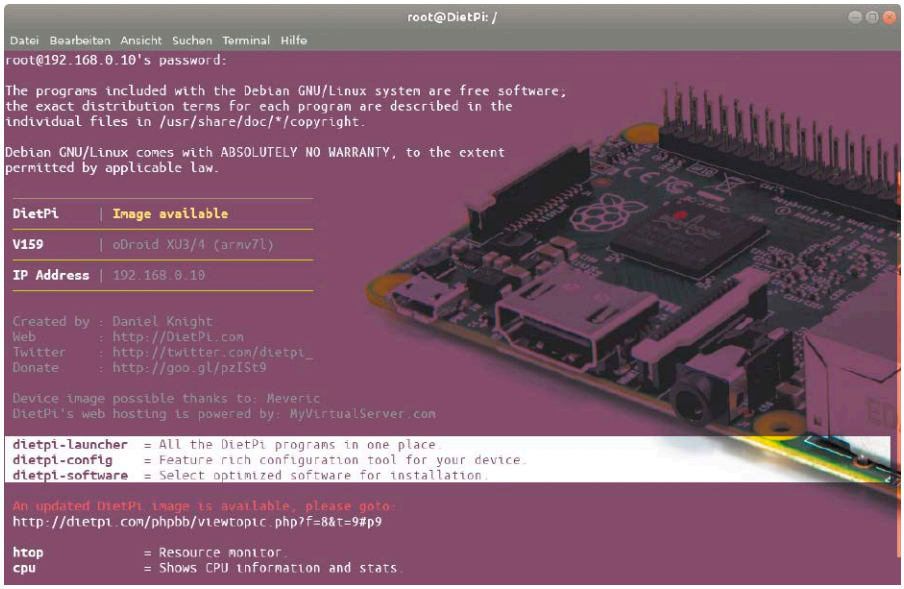
```
rsync -auvP --delete --dry-run /tmp/tmp /srv/backup/w10
```

Der Durchlauf mit „--dry-run“ zeigt alle zu erwartenden Aktionen, ohne sie tatsächlich auszuführen.

Diet Pi: Raspberry Pi auf Diät

Distributionen für den Raspberry Pi gibt es inzwischen reichlich, doch Diet Pi setzt hier neue Maßstäbe. Denn alles an dieser Zusammenstellung ist auf Geschwindigkeit bei minimaler Größe getrimmt.

VON STEPHAN LAMPRECHT



Wer seinen Raspberry ohne externen Speicher betreiben will, muss mit dem Platz auf der SD-Karte geizen. Viele Serveranwendungen können direkt per Browser konfiguriert werden, da braucht es keinen schwergewichtigen Desktop. Von Raspbian gibt es zwar bereits eine Lite-Ausgabe, aber Diet Pi zeigt sich hier sogar noch schlanker. Die Distribution ist extrem leichtgewichtig, was sich positiv beim RAM- und Speicherplatzverbrauch auswirkt. Das ist mit harten Zahlen nachzuweisen: Die Entwickler haben sich auch die Mühe gemacht, ihr Werk mit der Lite-Variante von Raspbian zu vergleichen (siehe Tabelle auf Google Docs: *goo.gl/PE9WmG*).

Installation standardmäßig ohne Desktop

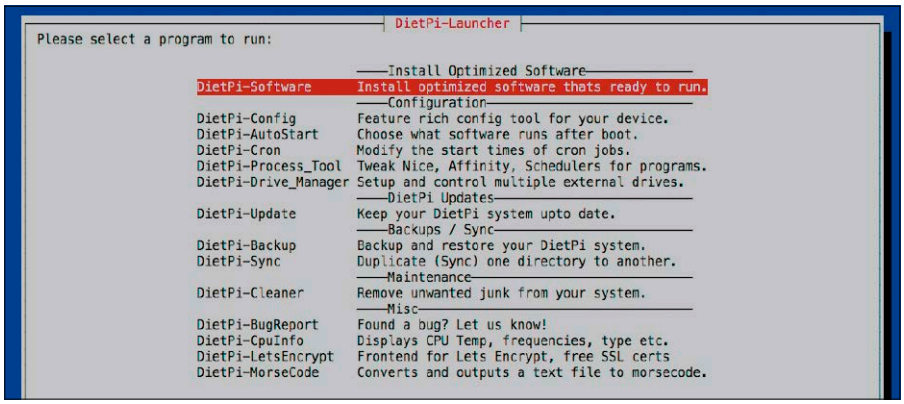
In der Rubrik „Downloads" auf der Startseite des Projekts (*https://dietpi.com/*) laden Sie sich zunächst die für den Pi gedachte Version herunter. Diet Pi gibt es in einer ganzen Reihe von Varianten auch für andere Platinenrechner sowie Imagedateien für Virtualisierer. Die ersten Schritte der Installation unterscheiden sich nicht von anderen Distributionen für den Raspberry. Entpacken Sie den Inhalt des Archivs. Wenn Sie unter Windows arbeiten, müssen Sie sich noch den Packer 7-Zip besorgen (auf Heft-DVD, Download unter *www.7-zip.de*). Das Archiv enthält die obligatorische IMG-Datei, die auf SD-Karte geschrieben werden muss. Das erledigen Sie unter Linux im Terminal mit dd, unter Windows mit dem Win 32 Disk Imager (auf Heft-DVD, Download unter *http://sourceforge.net/projects/win32diskimager*). Oder Sie verwenden unter Linux wie Windows den plattformunabhängigen Etcher (*https://etcher.io/*).

Ist das System aufgespielt, legen Sie die SD-Karte in den Raspberry ein, verbinden das Gerät per Ethernet-Kabel mit dem lokalen Netzwerk und versorgen es mit Strom. Warten Sie einen Moment, bis der erste Startvorgang erfolgreich abgeschlossen ist. Sie können Diet Pi natürlich per Tastatur und Monitor bedienen. Nötig ist das aber nicht: Diet Pi verwendet nach der Installation sofort einen SSH-Server, der auf Eingaben wartet, also nicht erst aktiviert werden muss. Für den Zugriff benötigen Sie nur die vom Router zugewiesene IP-Adresse. Diese ermitteln Sie am bequemsten am Router selbst. Auf der Fritzbox finden Sie eine Übersicht der Geräte unter „Heimnetz". Öffnen Sie auf einem Linux-PC ein Terminal und geben Sie dort ein:

```
ssh root@[IP_Adresse]
```

Standardpasswort für root ist zunächst „dietpi". Das System begrüßt Sie mit einem kurzen Hinweis. Danach beginnt es mit einer Aktualisierung. Im Rahmen der Einrichtung fragt das System nach, ob Sie die Standardpasswörter ändern wollen. Das ist auf jeden Fall empfehlenswert. Wählen Sie mit den Pfeiltasten also „OK" aus und geben Sie anschließend die neuen Passwörter ein. Um die Nutzung von Diet Pi zu verbessern, bitten die Entwickler Sie darum, Informationen zu Ihrem System zu übertragen. Welche Daten übermittelt würden, wird ebenfalls dargestellt. Treffen Sie in dem Dialog Ihre Auswahl und bestätigen Sie. Danach ist die

Einrichtung abgeschlossen und Diet Pi startet neu. Warten Sie einen Moment, bis das System wieder hochgefahren ist. Wahrscheinlich hat der Router dem Gerät wieder dieselbe IP-Adresse zugewiesen. Sie können sich also mit dem gleichen Kommando anmelden, jetzt aber bereits mit dem neuen Passwort. Um nicht in eine Endlosschleife zu verfallen, lehnen Sie diesmal die Änderung der Passwörter ab. Damit gelangen Sie zur Oberfläche von dietpi-software. Diese startet bei der ersten Anmeldung automatisch. Sie können Sie aber später jederzeit im Terminal mittels *dietpi-software* aufrufen.



Der dietpi-launcher ist die Hauptzentrale: Sie versammelt alle Systemprogramme unter einem Dach. Auch ein Partitionsmanager und ein Aufräumtool sind im Angebot.

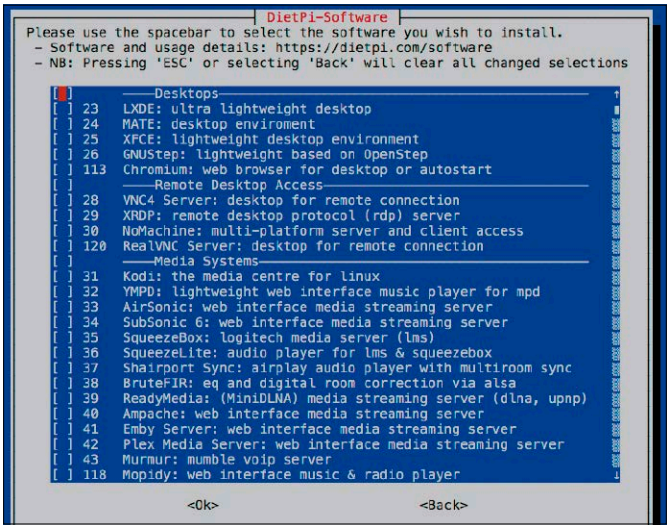
Diet Pi einrichten und Software installieren

Diet Pi ist gut organisiert: Mit dem Kommando *dietpi-config* rufen Sie ein Programm zur weiteren Anpassung des Systems auf. Dort können Sie bei Bedarf die Netzwerkschnittstellen einrichten, die Sprache wechseln, aber auch die notwendige Software installieren, wenn der Pi auf Netzwerkfreigaben zugreifen soll. Das Programm bedienen Sie ausschließlich mit den Pfeiltasten. Die Esc-Taste bringt Sie immer wieder zum Ausgangspunkt zurück.

Viel interessanter sind aber die beiden Einträge „Software Optimized“ und „Software Additional“. Unter „Additional“ finden Sie Programmpakete, die nur für Spezialaufgaben notwendig sind und meist für die Fälle gedacht sind, in denen Sie direkt vor dem kleinen Computer sitzen wollen, um damit zu arbeiten. So finden Sie hier etwa den Dateimanager Midnight Commander.

Unter „Software Optimized“ sind die Pakete enthalten, die für die Plattform angepasst sind. Die Anwendungen sind nach Szenarien organisiert. Sie finden eine breite Auswahl an verschiedenen Medienservern wie Kodi, Emby Server, Ampache oder Plex. Es stehen Pakete zur Auswahl, um den Raspberry als Downloadmaschine für das Filesharing einzurichten, aber auch Anwendungen für die Nutzung als Syncserver über die Cloud. Gelungen sind aber auch die Zusammenstellungen für den Einsatz als Web- oder VPN-Server und sogar der Home Assistant für das Smart Home ist hier mit an Bord.

Mit den Pfeiltasten bewegen Sie sich durch die Liste. Einen Eintrag, den Sie interessant finden, markieren Sie mit der Leertaste. Haben Sie Ihre Auswahl abgeschlossen, navigieren Sie mit Tab zum Schalter „Ok“ und



Im Tool dietpi-software: Die Dienste und Anwendungen sind nach Kategorien geordnet. So wird aus der Platine schnell ein Medienserver oder eine Plattform für die Datensynchronisation.

bestätigen. Sie gelangen jetzt wieder zur ersten Seite von dietpi-offware zurück und dort navigieren Sie zum Eintrag „Go“. Das System blendet Ihnen eine Zusammenfassung ein. Bestätigen Sie diese, um mit der Installation zu beginnen. Dies kann, je nach Umfang der Paketauswahl, eine ganze Weile dauern. Im Terminal können Sie jederzeit den Fortschritt verfolgen. Serveranwendungen konfigurieren Sie dann anschließend über den Browser. Dazu konsultieren Sie am besten die Anleitungen der Entwickler, die Sie auf den Projektseiten des jeweiligen Programms finden. Über dieselbe Oberfläche können Sie Anwendungen auch wieder entfernen. Dazu wählen Sie den Menüpunkt „Uninstall“ aus und dann das betreffende Paket.

Alle Optionen zentral versammelt

Diet Pi ist eine Empfehlung für Platinenbastler, die einen kleinen Server ohne grafischen Desktop betreiben wollen. Wenngleich das System unter „dietpi-software → Software Optimized“ auch LXDE oder XFCE anbietet, ist Diet Pi mit seinen vorbildlichen Zentralen auf die SSH-Verwaltung ausgerichtet. Gerade Hobby-Admins mit geringer Linux-Erfahrung profitieren von diesen Zentralen, die alle wichtigen Systemprogramme versammeln. Diese Zentralen zeigt Diet Pi bei jedem Systemstart und jeder SSH-Anmeldung an. Der Diet Pi Launcher ist die übergeordnete Instanz, die sämtlichen Diet-Pi-Programme anbietet, inklusive Paketmanager, Updater, Backup und Cronjobmanager.

Die Zentrale dietpi-config, die auch über den dietpi-launcher erreichbar ist, enthält die fundamentalen Hardware- und Netzwerkkonfiguration. Dietpi-software ist der Paketmanager zum Installieren und Deinstallieren. Damit hat man jederzeit das Wichtigste an der Hand, ohne die dahinterstehenden Terminalkommandos beherrschen zu müssen. ■

Geräte verfolgen mit Prey

Das Überwachungstool Prey eignet sich dazu, den Ort von PCs, Notebooks und Smartphones zuverlässig zu bestimmen. Interessant aus Linux-Perspektive: Die Clientkomponente von Prey ist Open Source und läuft auch unter Linux.

VON DAVID WOLSKI

Wo ist das Notebook abgeblieben? Das Tracking- und Fernsteuerungstool Prey kann mit einiger Vorbereitung und einer Portion Glück in Notfällen ein Gerät orten, auf dem es installiert ist. Vorausgesetzt, jemand startet das System, auf dem Prey installiert ist, und geht damit online. Das Programm arbeitet als freundlicher Trojaner als Hintergrunddienst und stellt über eine Internetverbindung in regelmäßigen Abständen den Kontakt zu einem zentralen Server her, dem es seine Position meldet.

Wenn der rechtmäßige Besitzer das Gerät als verloren gemeldet hat, sendet Prey in kurzen Intervallen Informationen über den Standort des Gerätes, den darauf laufenden Anwendungen und optional sogar Webcam-Fotos. Bildschirmfotos können bei der Identifizierung des jetzigen Nutzers helfen. Diese Infos schickt Prey entweder verschlüsselt per HTTPS an den Server des Softwareanbieters von Prey oder an einen eigenen Mailserver.

Bis zu drei Geräte pro Account sind kostenlos: Nach der Installation zeigt das Programm Log-in und Registrierung an, um den Rechner als überwachtes Gerät am Prey-Server anzumelden.

Tracking per Internetverbindung

Prey sammelt die Standardinformationen bei Notebooks über die IP-Adresse der Internetverbindung, was heute erstaunlich präzise funktioniert. Damit das jedoch alles perfekt abläuft, müssen einige günstige Umstände zusammentreffen: Jemand, der ein Notebook entwendet hat, muss sich auf dem bestehenden System anmelden und online gehen, anstatt die Festplatte gleich zu formatieren, ein Livesystem zu starten oder ein neues System aufzusetzen. Die Wahrscheinlichkeit, dass genau dies passiert, ist bei einem Linux-System natürlich geringer als bei einem Windows-System. Außerdem sollte man ein Lockvogel-Konto ohne Passwort anbieten, damit sich tatsächlich jemand arglos an einem präparierten System anmeldet. Als Diebstahlsicherung ist Prey deshalb auf Smartphones und Tablets sinnvoller installiert (siehe Kasten „Android und iOS: Prey für Mobilgeräte“) als auf Notebooks.

Für den Hausgebrauch ist Prey trotzdem auch auf Linux-Notebooks nützlich, um einen umfangreichen Gerätepark im Blick zu behalten. Der Hinweis, wo man zuletzt mit einem Notebook online war, ist ein wichtiger Hinweis darauf, wo ein verlegter mobiler Computer abgeblieben ist.

Installation und Einrichtung

Prey besteht aus einer Client- und einer Serverkomponente. Während die Macher von Prey den Server kommerziell als Freemium-Dienst betreiben, ist der Client kostenlos. Nicht nur das: Der Client ist Open Source, steht unter der GPL 3 und ist im Quelltext auf Github veröffentlicht (*https://github.com/prey/prey-node-client*).

Andernfalls wäre die Installation eines Trojaners wie Prey auch keinesfalls empfehlenswert. Prey ist inzwischen in Node.js komplett neu geschrieben und die Installation auf den verbreiteten Linux-Distributionen kein Problem.

Für DEB-basierende Linux-Systeme wie Debian, Ubuntu und Linux Mint liefern die Entwickler ein fertiges Paket auf *https://www.preyproject.com/download* in 32 Bit und 64 Bit. Für seine Zusatzfunktionen verlangt der Prey-Client nach ein paar Abhängigkeiten, die ein Doppelklick auf das DEB-Paket und die Installation über die Paketmanager Gdebi oder Gnome Software auflöst. Alter-

nativ kann auch apt in der Kommandozeile mit dem Aufruf

```
sudo apt install ./[Paketname].deb
```

alle Abhängigkeiten installieren.

Auf anderen Linux-Distributionen gelingt die Installation des Prey-Clients über den internen Paketmanager von Node.js. Dazu muss man im Terminal als root angemeldet sein, sudo funktioniert in diesem Fall nicht.

```
npm install -g prey
```

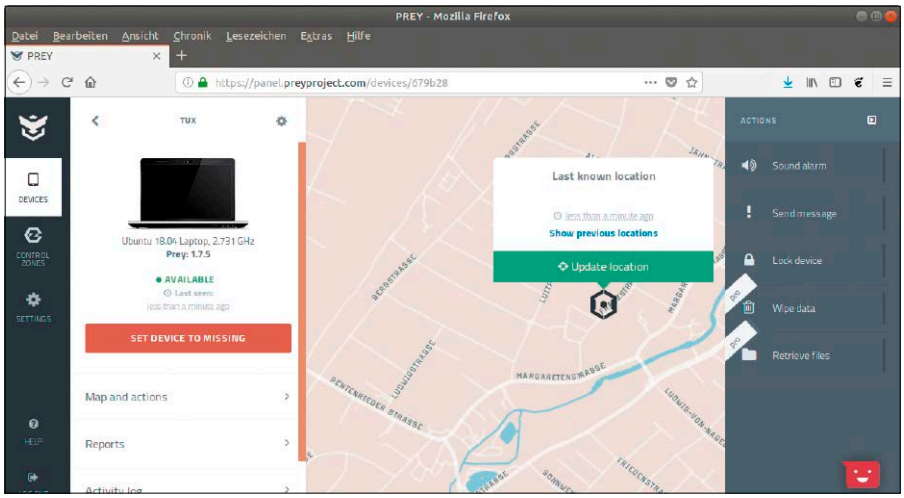
Weniger empfehlenswert ist die Installation von Prey über den jeweiligen Paketmanager der Distribution: Zwar ist der Open-Source-Client fast überall in den Standard-Paketquellen vertreten, doch meist handelt es sich um sehr alte Versionen.

Nach der Installation startet das englischsprachige Konfigurationsprogramm von Prey, das sich ansonsten unter „/usr/lib/prey/versions/1.7.5/lib/conf/gui/linux/prey-config.py“ findet. Es verlangt die Registrierung als neuer Benutzer anhand einer gültigen Mailadresse oder die Anmeldung mit einer bestehenden Adresse. Die Firma, die den zentralen Server für Prey bereitstellt, verdient ihr Geld mit dem Tracking von mehreren Geräten je Kunde. Die Anmeldung von maximal drei Geräten pro Mailadresse ist kostenlos. Nach der Registrierung mit den gewünschten Daten legt Prey die Konfigurationsdatei „/etc/prey/prey.conf“ an und startet den Systemd-Dienst prey-agent.service. Dieser Dienst läuft im Hintergrund, egal welcher Benutzer auf dem Linux-System angemeldet ist.

Kontrolle per Weboberfläche

Auf *https://panel.preyproject.com* gelangt man nach dem Log-in zur Übersichtsseite mit allen Geräten eines Accounts. Der Klick auf ein Gerät in der Spalte links aktualisiert den Standort, vorausgesetzt der Prey-Dienst kommt ins Internet. Die Position ist auf einer Open-Streetmap-Karte in der Mitte zu sehen. Auf der rechten Seite gibt es zum aktuell gewählten Gerät einige Aktionen: „Sound Alarm“ spielt einen Alarmton ab, dank dessen sich ein verlegtes Gerät im Haus leicht wiederfinden lässt. Der Punkt „Send Message“ blendet einen Nachrichtentext auf dem Bildschirm ein und „Lock Device“ sperrt den Bildschirm mit einem Passwortschutz.

Eine automatische Überwachung beginnt, wenn der Gerätestatus mit „Set device to missing“ auf verloren gesetzt wird. Dann wird Prey im Zehn-Minuten-Takt versuchen, den Standort zu ermitteln und diese Info an die hinterlegte Mailadresse zu schicken – auch mit Screenshots und einem aktuellen Bild der Webcam. Besonders nützlich für Mobilgeräte, die schnell mal verloren gehen, sind die „Control Zones“. Dort kann man auf der Karte einen Bereich definieren, der eine Mailbenachrichtigung auslöst, sobald ein Gerät diese Zone betritt oder verlässt. ■



Standort finden und Aktionen ausführen: Die Weboberfläche von Prey nutzt Open Streetmaps zur Darstellung der Position. Notebooks werden anhand der Internet-IP-Adresse geortet.

ANDROID UND IOS: PREY FÜR MOBILGERÄTE

Ein gestohlenes Notebook mit Prey wiederzufinden, ist sicherlich Glückssache. Auf Mobilgeräten wie Smartphones arbeitet die Ortung zuverlässiger, da diese Geräte über den Mobilfunkprovider häufiger online sind und präzise ihre GPS-Koordinaten mitteilen können.

Prey für Android und Apple iOS ist als App ebenfalls kostenlos und Open Source. Links zu den Apps auf Google Play beziehungsweise dem Apple App Store finden sich auf *www.preyproject.com/download*. Prey für Android wird nach der Installation per hinterlegten Zugriffsrechten vor der Deinstallation geschützt und die Weboberfläche kann zudem das Symbol auf dem Home-Screen ausblenden. Die Appkonfiguration auf dem Smartphone/Tablet kann den Powerbutton deaktivieren, damit das Gerät nicht abgeschaltet wird. Außerdem gibt es die Möglichkeit, auch ohne Internetverbindung aus der Ferne einige vordefinierte Aktionen per SMS auszulösen. Dazu gehören beispielsweise eine Bildschirmsperre, Alarmton und die Abfrage des Standorts. Prey kann damit bei der Standortbestimmung etwas mehr als der offizielle Google-Dienst unter *www.google.com/android/find* zum entfernten Sperren und Löschen von Android-Geräten.

Android-App von Prey: Auf diesen Geräten kann sich Prey über Android-Zugriffsrechte vor einer einfachen Deinstallation schützen und den Powerbutton blockieren.

Systeme für Smart Home unter Linux

Offene Systeme versprechen die Herstellergrenzen zwischen Geräten für das Smart Home zu überwinden. Wie bei den Lösungen wird auch die Auswahl bei den Plattformen größer. Der Artikel zeichnet ein Kurzporträt der wichtigsten Plattformen.

VON STEPHAN LAMPRECHT

Bei der Heimautomatisierung gibt es zwei mögliche Richtungen. Einfach wird es, wenn man sich für die Gerätewelt eines Herstellers entscheidet. Hier passt alles zusammen und mittels App oder Sprachsteuerung können dann die Komponenten gesteuert werden. Der Ansatz bereitet keine Probleme, ist aber auch am teuersten. Stellt man sich hingegen ein buntes Feld an Geräten verschiedener Hersteller zusammen, lassen die sich zwar problemlos nebeneinander betreiben, jedoch gibt es wenig integrative Ansätze. Der Haus-Admin jongliert dann zwischen den verschiedenen Apps und Steuerungsmöglichkeiten. Zentrale Verwaltungsplattformen schaffen hier Abhilfe und die gibt es auch in kostenfreien und offenen Varianten. Bei unserer Auswahl haben wir Projekte ausgewählt, die sich durch eine aktive Community auszeichnen, viele aktuelle Produkte auf dem deutschen Markt unterstützen und einen möglichst einfachen Einstieg bieten.

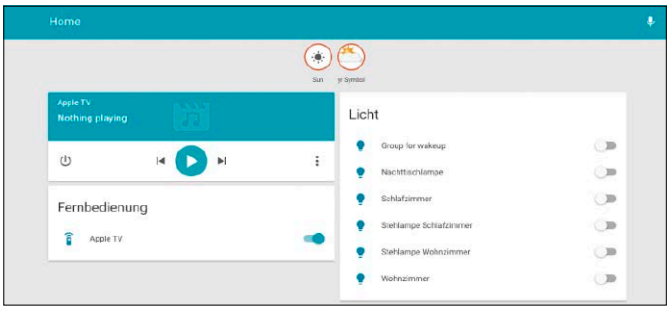
Der Home Assistant

Das Projekt Home Assistant (*https://www.home-assistant.io/*) verwandelt den Raspberry Pi in eine Steuerungszentrale für das Smart Home. Es wird ein fertiges Image zum Download angeboten. Entsprechend einfach gestaltet sich die Installation. Mit Etcher oder dem Win 32 Disk Imager wird der Inhalt des Archivs auf eine SD-Karte übertragen. Soweit die Theorie – etwas störend dabei: Zu Redaktionsschluss unterstützt das Projekt („Hassio“) noch nicht das neueste Modell des Raspberry Pi (3). Hassio basiert auf Resin-OS. Wenn es also mal klemmt, sind Foren und FAQ-Seiten zu diesem System hilfreich. Wer einen Raspberry 3 nutzen will, muss auf das Projekt „Hassbian“ ausweichen. Und wie der Name andeutet, bildet hier Raspbian die Grundlage, entsprechend muss man sich bei Problemen etwas umorientieren. Sicherlich wird es für diese unbefriedigende Situation in absehbarer Zeit eine Lösung geben.

Soll der kleine Rechner unmittelbar nach dem ersten Booten auf das heimische WLAN zugreifen, muss noch einmal Hand angelegt werden. Die Vorgehensweise ist zwar in beiden Fällen nahezu identisch, allerdings liegen die Konfigurationsdateien in verschiedenen Verzeichnissen. Das erklären die Entwickler aber in ausführlichen englischsprachigen Dokumentationen. Nach dem erfolgreichen Booten ist das System dann per Browser im lokalen Netzwerk über Port 8123 zu erreichen: „http://[IP-Adresse]:8123“.

Hass.io ist modular erweiterbar: Die Installation von Add-ons ergänzt die Fähigkeiten des Systems. So gibt es beispielsweise eine Erweiterung, die das Bearbeiten der Konfigurationen auch per Web ermöglicht. Eine besondere Erweiterung, die den Einstieg vereinfacht, kümmert sich um die automatische Erkennung von Geräten, die das WLAN verwenden. Die Einrichtung der einzelnen Geräte gestaltet sich mal mehr, mal weniger kompliziert. Viele grundlegende Konfigurationen, wie die Definition von Gruppen oder auch Schaltzyklen, werden über eine zentrale Konfigurationsdatei erledigt, die manuell, aber auch mit jedem beliebigem Texteditor bearbeitet werden kann. Typischerweise geschieht das mit einer SSH-

Verbindung und dem Standardeditor Nano. Das Einbinden von Bridges und Controllern unterscheidet sich herstellerabhängig erheblich. In der Konfiguration von Home Assistant wird die Basiskomponente, zum Beispiel ein Zigbee-Switch, hinterlegt. Das Anlernen der damit verbundenen Geräte wird dabei nach Anleitung des Herstellers erledigt. Hat das funktioniert, kann der Home Assistant dann auch die entsprechenden Geräteeinheiten (Entities) darstellen und Schaltungen ermöglichen. Unterstützt werden auch die in Deutschland beliebten Produkte, die auf „Homematic“ basieren.



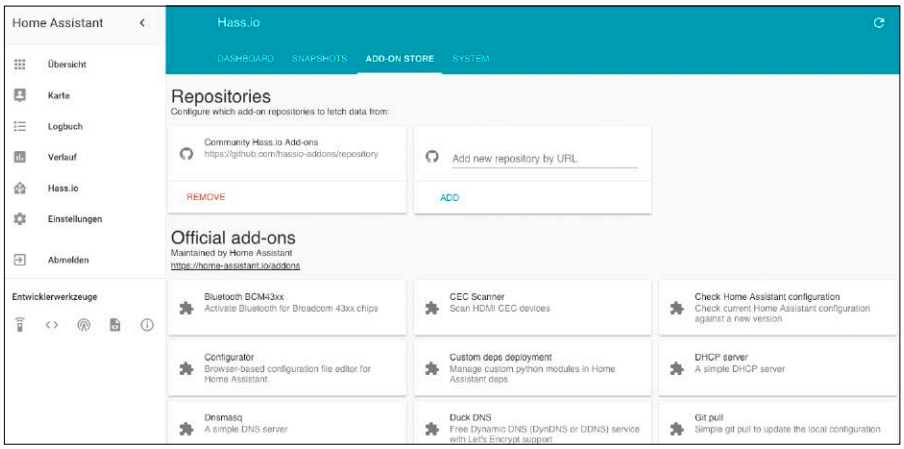
Durch die integrierte Funktion „Auto Discovery“ bietet Home Assistant gleich nach dem Start schon die ersten Geräte zum Schalten.

Home Automation mit Domoticz

Domoticz wird in Paketen für unterschiedliche Betriebssystem-Plattformen angeboten (*www.domoticz.com*). Unter den unterstützten Systemen sind auch Windows und Mac-OS anzutreffen. Auf dem Raspberry Pi erledigen Sie die Installation am einfachsten mittels des Befehls

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

Deutlich anspruchsvoller und mit längeren Wartezeiten verbunden ist das Kompilieren direkt aus den Quellen.



Die Funktionalität des Home Assistant ist modular erweiterbar: Add-ons ergänzen die Software selbst, erweitern aber auch die steuerbaren Geräte.

Ist die Software installiert, bietet auch sie eine Weboberfläche, die mit jedem Browser im lokalen Netz abrufbar ist. In diesem Fall ist Port 8080 voreingestellt („http://[IP-Adresse]:8080“). Domoticz hat eine sehr aktive Entwicklergemeinde und entspre-

AUF GERÄTESTANDARDS ACHTEN

Wer sichergehen will, dass die Komponenten reibungslos miteinander vernetzt werden können, sollte sich auf den Projektseiten der Steuerungszentralen vor der Anschaffung der Geräte darüber informieren, welche Modelle unterstützt werden.

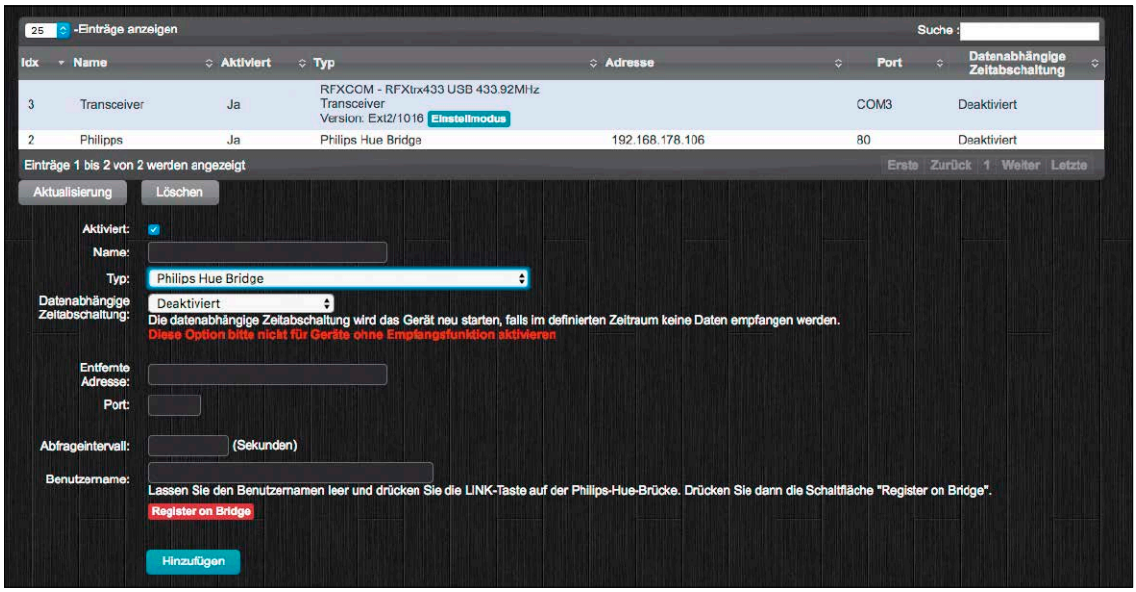
Denn der Markt ist unübersichtlich. Zwar nutzen die kabellosen Produkte alle die gleichen Frequenzbänder (434 MHz oder 868 MHz), verständigen sich aber auf unterschiedliche Weise. Zu allem Überfluss gibt es dann auch noch herstellereigene Initiativen und Kommunikationsprotokolle, um die Geräte miteinander zu vernetzen. Derzeit gibt es drei Standards mit größerer Verbreitung:

Z-Wave ist in den USA verbreiteter als in Deutschland, zählt aber weltweit zu den Marktführern. Mehr als 200 Hersteller setzen dieses Protokoll in ihren Geräten ein. Genutzt wird die Frequenz von 868 MHz. Per Z-Wave vernetzte Geräte leiten Mitteilungen untereinander weiter. Das erhöht die Reichweite des gesamten Systems. Zu den bekannteren Herstellern in Deutschland, die auf diesen Standard setzen, gehören Devolo, Hauppauge und Fibaro.

Zigbee wird ebenfalls als internationaler Standard stark genutzt. Philips verwendet Zigbee beispielsweise in seinen Hue-Lampen. Die Geräte sind drahtlos über das sogenannte WPAN-Protokoll vernetzt. Das funktioniert ganz ähnlich wie WLAN, wurde aber speziell für die Überbrückung deutlich kürzerer Distanzen entwickelt. Allerdings sind Geräte, die Zigbee nutzen, nicht automatisch miteinander kompatibel. Denn der Standard erlaubt auch die Verwendung von herstellereigenen Komponenten.

Home Kit wurde von Apple entwickelt. Es setzt auf iOS auf und ermöglicht so den Anwendern, das Smart Home mit iPhone oder iPad zu steuern. Typisch für Apple gestaltet sich die Einrichtung der Geräte und Steuerung extrem einfach. Home Kit bildet den Rahmen zwischen verschiedenen Apps und Geräten unterschiedlicher Hersteller, wie etwa von Elgato. Brücken zu anderen Standards sind möglich, erfordern aber eine zusätzliche Hardwarekomponente.

DECT vernetzt die Komponenten über eine Abwandlung des DECT-Standards, wie er in kabellosen Telefonen zum Einsatz kommt. Hier ist AVM besonders umtriebig. Das Unternehmen verwandelt so seine Fritzbox-Router zur Zentrale für das Smart Home. Damit ist die zentrale Hardware schon mal vorhanden, andererseits ist der Markt an Geräten aber noch recht überschaubar.



Auch in Domoticz richten Sie Geräte über vorgegebene Dialogmasken ein. Das sieht einfacher aus, als es tatsächlich ist, und erfordert häufig den Blick in das Wiki der Entwickler.

chend umfangreich sind die Wiki-Seiten, die kompatible Geräte auflisten. Nicht gelistete Komponenten können zwar durchaus auch funktionieren, sofern sie das gleiche Übertragungsprotokoll nutzen (siehe Kasten „Auf Gerätestandards achten"), tun es dann aber oftmals nur nach reichlich Handarbeit. Die Einrichtung von Geräten, die das WLAN für die Kommunikation zwischen Aktoren und Sensoren nutzen, ist auch für Einsteiger ohne Probleme machbar. Die IP-Adresse des Hubs oder der Bridge ist alles, was Sie wissen müssen. Unter „Einrichtung, Hardware" wählen Sie dann unter „Typ" die passende Geräteklasse aus, beispielsweise den Hub der Hue-Beleuchtung. Domoticz meldet sich dann dort an, nutzt also den gleichen Mechanismus wie eine externe App. Ist die Kopplung erfolgreich, können Sie über „Einrichtung → Geräte" die von der Bridge angesteuerten Elemente mit Domoticz bekanntmachen.

Spannen die Hubs eigene Netze auf oder soll das 433-MHz-Band verwendet werden, braucht es einen zusätzlichen Transceiver. Dieser wird per USB-Kabel mit dem Rechner verbunden. Über „Einrichtung → Hardware" sollte die Schnittstelle dann als mögliches Element auftauchen. Über eine Suchfunktion in der Liste auf dem Frequenzband funkender Geräte können Sie diese dann der Konfiguration hinzufügen. Dank der Einrichtung per Browser ist Domoticz auch für Einsteiger geeignet. „Homematic"-Geräte werden zwar im Prinzip unterstützt, deren cloudbasierter Standard (IPv6) allerdings noch nicht.

Smart Home mit IO Broker

Das offene Projekt IO Broker wählt technisch einen völlig anderen Ansatz, denn die Steuerung ist in Node.js programmiert. Da die Einstiegshürden in Javascript nicht besonders hoch sind, dürfte sich das positiv auf die potenzielle Zahl von aktiven Entwicklern auswirken. Apropos Einstiegshürden: Unter allen aktuellen Frameworks zur Automatisierung des Smart Homes dürfte IO Broker wahrscheinlich die sein, mit der sich Einsteiger am schnellsten anfreunden dürften. Script-Kenntnisse sind gut, aber keine zwingende Voraussetzung.

Zur Ansteuerung für Komponenten verwendet die Anwendung sogenannte „Adapter", die bereits in einer beeindruckenden Zahl zur Verfügung stehen, darunter auch die Homematic-Welt.

Im Downloadbereich des Projekts (*www.iobroker.net/docu/?page_id=2563&lang=de*, siehe auch die gut verständliche deutsche Einführung unter *www.iobroker.net/docu/?page_id=6317&lang=de*) stehen eine ganze Reihe von Images für verschiedene Ein-Platinen-Rechner zur Verfügung, darunter auch für alle Raspberry-Modelle, Tinker Board, Cubietruck, Banana Pi. Das System kann aber auch auf einem Windows-Rechner oder Mac installiert werden.

Bedient wird das gesamte System wieder per Browser über das Netz. In diesem Fall genügt der Aufruf von „http://IP-Adresse:8081". In der Konfigurationsoberfläche wechseln Sie dann in den Abschnitt „Adapter". Über die Eingabezeile suchen Sie nach einem zur Hardware passenden Adapter, zum Beispiel „Hue". Mit einem Klick auf das Pluszeichen wird dann der Adapter installiert. Die Konfiguration erledigen Sie über das Register „Instanzen". Über die IP-Adresse wird die Bridge des Systems angesprochen. Mit „Erstelle User" und Drücken der entsprechenden Taste auf der Bridge wird „Hue" mit dem System bekanntgemacht. Ist das erfolgreich verlaufen, werden unter „Objekte" sowohl die angemeldeten Geräte als auch die Schaltzustände der Bridge sichtbar.

Zum Schalten und zur Gestaltung von Raumplänen besitzt die Software eine eigene Visualisierungsansicht, die über die Adresse „http://[IP-Adresse]/vis" erreichbar ist. Allerdings muss dafür ein Lizenzschlüssel erworben werden. Dieser ist für private Nutzer kostenlos, setzt aber eine Registrierung voraus. Über diese besondere Oberfläche richten Sie dann die Schalter ein, die auf die erkannten Objekte reagieren. Das klingt zunächst kompliziert, ist aber dank der Dokumentation der Entwickler nicht schwierig. Auch die Anbindung an Amazons Alexa ist möglich. Allerdings ist dazu die Nutzung eines Cloudkontos von IO Broker nötig, da die Kommunikation zwischen System und Amazon über die Cloud erfolgt. Auch dafür ist eine Registrierung beim Anbieter Voraussetzung.

Der Home Automation Bus (Open HAB)

Schon 2010 konnte die allererste Version des in Java entwickelten Open HAB (*www.openhab.org*) beeindruckend viel. Allerdings

war die Software alles andere als einfach zu installieren und in Betrieb zu nehmen. Wer mit Open HAB etwas erreichen wollte, musste nicht nur eine Portion Begeisterung für das Smart Home mitbringen, sondern auch für Linux. Das änderte sich mit Version 2, die deutlich zugänglicher ist. Open HAB gibt es ebenfalls für zahlreiche Plattformen, darunter ein Image für den Raspberry, das die Einrichtung sehr angenehm macht. Einmal auf die SD-Karte gebracht, muss die Platine nur noch gestartet werden. Danach dürfen sich die Nutzer erst einmal eine ausgiebige Kaffeepause gönnen. Denn die vollständige Installation und der erste Start des Systems dauern zwischen 15 und 45 Minuten.

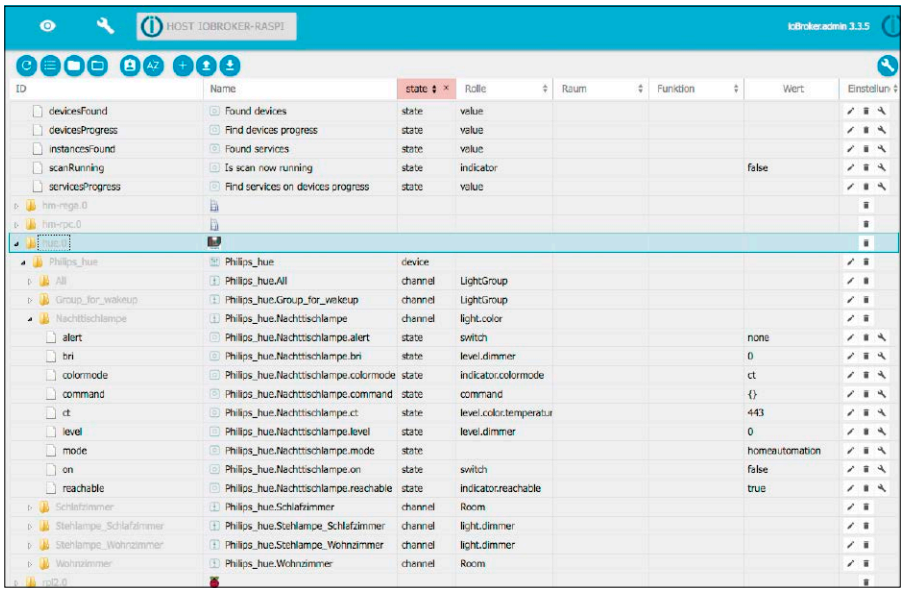
Danach kann die Konfiguration über den Browser gestartet werden. Auch hier benötigen Sie nur die IP-Adresse des Systems und die Angabe der Portnummer 8080. In der Konfigurationsoberfläche wird der Anwender dann von einem Setup begrüßt. Empfehlenswert ist die Nutzung des Standardsetups. Ist das erfolgreich durchlaufen, bietet der Server mit seiner „Paper UI“ eine übersichtliche Schnittstelle zur Konfiguration von Geräten und Aktionen. Die Anbindung der verschiedenen Komponenten erfolgt mittels sogenannter Bindings. Bevor ein Gerät, zum Beispiel ein Dash-Button, eingebunden werden kann, muss die Schnittstelle erst installiert werden. Über „Add-Ons“ können Sie nach einem Binding suchen und es dann auch gleich installieren. Die neue Schnittstelle landet dann in der „Inbox“.

Nach der Auswahl sucht das Hilfsprogramm dann nach steuerbaren Elementen. Das können andere Server und Komponenten im Netzwerk sein (Network Binding) oder Bridges und Controller. Über den „Home Builder“ gibt es ein grafisches Tool, um aus Geräten und Bindings eine optische Entsprechung des eigenen Heims zu formen. So wird es auch übersichtlicher, Szenarien und Aktionen miteinander zu verknüpfen. Die Entwickler haben im Rahmen des Setups eine Demokonfiguration eingebaut, die als Inspiration und Vorlage für die Einrichtung eigener Szenarien genutzt werden kann.

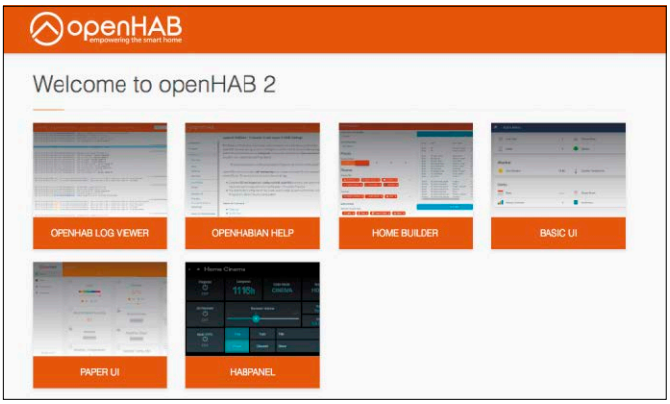
Fazit und Einschätzung

Ausgesprochen zugänglich auch für Einsteiger präsentieren sich IO Broker und Open HAB (in der Version 2). Steiler ist die Lernkurve beim Home Assistant, da hier noch der grafische Zugang für die Einrichtung von Szenarien und Geräten fehlt. In der Mitte liegt das Konzept von Domoticz.

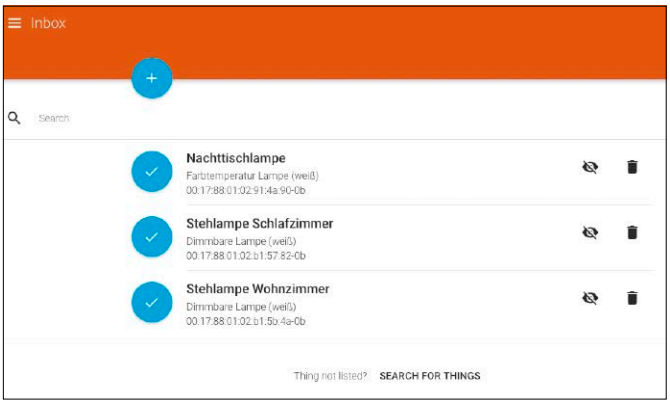
Eine generelle Empfehlung für das eine oder andere Konzept gibt es indes nicht, denn die Entscheidung steht und fällt mit den Geräten, die aktuell und in Zukunft verwendet werden sollen. Klassiker wie Hue oder Ikea Tradfri lassen sich in allen Systemen rasch einrichten. Wer auf Homematic und kompatible Geräte setzt, sollte vorab nachlesen, wie weit die Unterstützung derzeit reicht. ■



IO Broker ist in weiten Teilen intuitiv und ansprechend gestaltet. Die hier abgebildete Objektliste versprüht aber eher den Charme einer Datenbank.



Open HAB ist dank der neuen Oberfläche zugänglicher geworden. Bei den ersten Schritten ist aber dennoch das Handbuch hilfreich.



Hat Open HAB „Dinge“ und „Objekte“ gefunden, landen diese in der „Inbox“. Danach folgen die weitere Einrichtung und die Kombination von Szenarien.

Drucker unter Beschuss

Drucker haben eine Evolution von einfachen Peripheriegeräten zu kompletten netzwerkfähigen Druckservern gemacht. Das Thema Sicherheit kam dabei meist zu kurz. Das Python-Tool Pret klopft Drucker auf Sicherheitslücken ab.

VON DAVID WOLSKI

Im Idealfall ist der Drucker im Netzwerk ein unauffälliger Arbeitsknecht oder eine fleißige Papierschleuder, was bei Drucken mit Linux immer noch keinesfalls selbstverständlich ist. Schlimmstenfalls ist ein netzwerkfähiger Drucker aber noch um einiges mehr: Ein verwundbarer Printserver im Netzwerk, der Attacken aus dem Netzwerk schutzlos ausgeliefert ist. Nun sind unsichere Server in einem privaten Netzwerk sicher kein großes Problem, schließlich sind die Netzwerkteilnehmer vertrauenswürdig und in ihrer Zahl überschaubar. In Büro- und Firmennetzwerken sind verwundbare Drucker aber ein Risiko, da sie sich eventuell manipulieren, ausspähen, sabotieren oder sogar beschädigen lassen. Im Rahmen einer viel beachteten Masterarbeit an der Ruhr-Uni Bochum des IT-Sicherheitsspezialisten Jens Müller entstand 2016 das Python-Tool „Pret" (Printer Exploitation Kit), das eine vereinheitlichte Befehls-Shell für die diversen Druckersprachen bereitstellt, um Angriffe auf Drucker zu testen. Pret hat sich seitdem auf Github beständig weiterentwickelt (*https://github.com/RUB-NDS/PRET*) und gilt heute als das Standardtool, um Druckern auf den Zahn zu fühlen. Das Tool führt keine automatisierten Scans durch, sondern ist für manuelle Checks gemacht. Der Beitrag zeigt einige typische Angriffe, die Pret gegen den eigenen Drucker starten kann.

Drucker: Unterschätzte Gefahren

Bei einem Dateiserver im Netzwerk wären sich alle einig, dass diese Systeme ausreichend sicher konfiguriert sein müssen und deren Serversoftware regelmäßige Updates verlangt. Drucker stehen dagegen selten im Zentrum der Aufmerksamkeit von Administratoren und erhalten entsprechend selten Firmwareupdates, sofern der Gerätehersteller solche überhaupt noch anbietet. Auch die Druckbefehls- und Beschreibungssprachen Postscript, Printer Command Language und Printer Job Language sind teilweise 40 Jahre alt, also aus einer Zeit, als es in der IT noch arglos zuging. Sicherheitsmechanismen gegen manipulierte Kommandos gibt es wenige – und auch nur, wenn sich der Druckerhersteller in seiner Firmware darum gekümmert hat. Das Ziel manipulierter Befehle können dabei simple Denial-of-Attacken sein, aber auch die Übernahme und Änderung fremder Printjobs. Buffer Overflows können eingeschleuste Befehle auf unsicheren Druckern in einem privilegierten Kontext ausführen oder den Inhalt von Speicher und Dateisystem preisgeben.

Pret in der Praxis

Pret verlangt neben einem Python-Interpreter der Version 2.7 nur nach wenigen zusätzlichen Python-Modulen und läuft damit auf nahezu jedem Linux-System. Die Vorbereitung ist die Installation von Git, Imagemagick, Ghostscript und Python-Pip aus den Paketquellen des Linux-Systems. Unter Debian/Ubuntu und Linux Mint dient dazu dieser Befehl:

```
sudo apt install git imagemagick
  ghostscript python-pip
```

Anschließend installiert der Paketmanager von Python einige benötigte Module lokal im Home-Verzeichnis des Anwenders:

```
pip install colorama pysnmp
```

Danach holt der Befehl

```
git clone https://github.com/RUB-NDS/PRET
```

das Python-Programm Pret von Github und legt es in einem gleichnamigen Ordner ab. Von dort aus startet man nun die Arbeit mit Pret. Über Name und Adresse der Drucker im Netzwerk braucht man nicht lange zu spekulieren. Der Aufruf

```
./pret.py
```

listet die erreichbaren Drucker mit IP-Adresse und Gerätenamen auf. Mit Pret gibt es mit den Schnittstellen „ps“, „pjl“ und „pcl“ drei Möglichkeiten, sich mit einem Drucker zu verbinden, je nachdem, was das Gerät unterstützt. Die Verbindungsaufnahme erfolgt über diesen Befehl:

```
./pret.py [Adresse]
 [Schnittstelle]
```

Konkret nimmt der Befehl

```
./pret.py 192.168.0.8 ps
```

beispielsweise Kontakt zum Drucker mit der IP-Adresse 192.168.0.8 mittels Postscript („ps“) auf. Es lohnt sich, immer alle drei Schnittstellen durchzuprobieren, denn die meisten Netzwerkdrucker verstehen zumindest eine dieser Sprachen. Pret öffnet eine Kommandoshell, die dann die gewünschten Befehle schickt und die Antwort auswertet. Die Eingabe „help“ zeigt die möglichen Befehle an, „quit“ beendet diese Shell wieder.

Denial of Service: Viele ältere Drucker lassen sich über Postscript (ps) oder Printer Job Language abschalten (pjl). Der Befehl in Pret dazu lautet „disable“. In Postscript (ps) gibt es dazu auch noch den gemeineren Befehl „hang“, der einen Papierstau simuliert. Vom Befehl „destroy“ (ps/pjl), der versucht, das NVRAM durch eine große Zahl von Schreibvorgängen zu beschädigen, sollte man besser die Finger lassen.

Zugriffsrechte übergehen: Bei einigen Druckern genügt schon der Befehl „reset“ (ps/pjl), gefolgt von „restart“, um das Gerät auf Werkeinstellungen zurückzusetzen. Ältere HP-Drucker sind dafür besonders über die Printer Job Language anfällig (pjl).

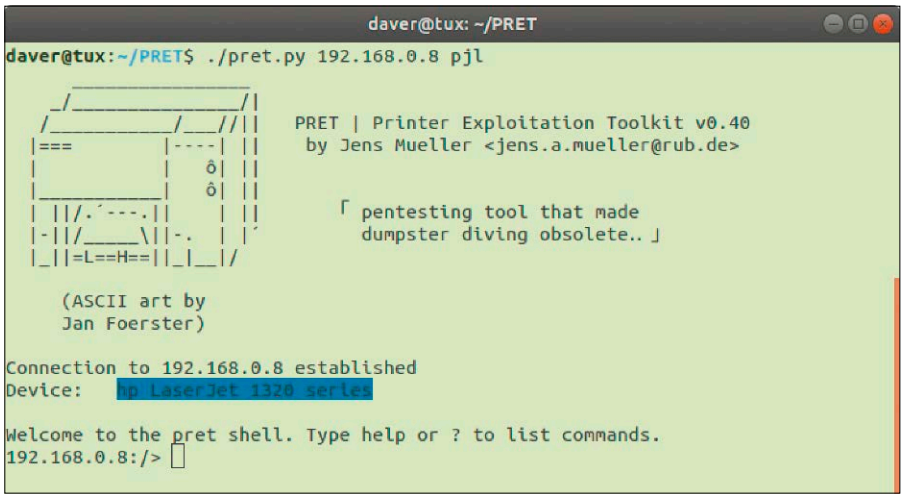
Auslesen von Jobs: Pret kann während der Verbindung (ps) zu einem Drucker mit dem Kommando „capture start“ Druckaufträge im RAM mitschneiden. Gelingt dies, so holt „capture fetch“ die mitgeschnittenen Daten als Postscript-Datei auf den Linux-Rechner.

Manipulation von Aufträgen: Mit Postscript (ps) kann Pret bei verwundbaren Druckern mit dem Befehl

```
overlay overlays/smiley.eps
```

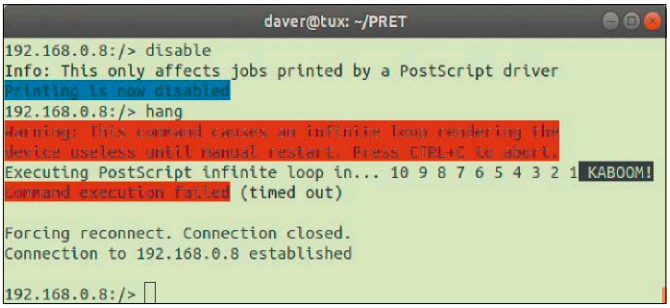
andere Druckaufträge mit der Grafik „smiley.eps“ aus dem PRET-Ordner versehen.

Diese Beispielbefehle von Pret zeigen nur einen kleinen Teil der Möglichkeiten des Printer Exploitation Kits. Zudem gilt es immer, die drei Schnittstellen Postscript (ps), Printer Command Language (pcl) und Printer Job Language (pjl) einzeln zu betrachten.



Pret stellt sich vor: Die in Python geschriebene Kommando-Shell ist eine universelle Eingabezeile für verständliche Befehle, die in die Sprachen ps, pjl und pcl übersetzt werden.

Es hat sich ausgedruckt: Ein älterer HP-Drucker wurde mit Postscript-Befehlen malträtiert und nimmt bis zum Neustart keine Druckaufträge mehr an – harmlos, aber nervig.



Wenn ein Drucker auf einer Schnittstelle unverwundbar ist, kann woanders dennoch eine Lücke bestehen.

Einen breit angelegten Einstieg und eine größere Übersicht zu interessanten Pret-Kommandos tragen IT-Spezialisten im englischsprachigen Wiki *https://hacking-printers.net* zusammen. ■

CHECKLISTE: DRUCKER ABSICHERN

Physischen Zugriff einschränken: In größeren Einrichtungen und Büros sollten Netzwerkdrucker nicht für alle Welt zugänglich aufgebaut sein, sondern hinter abschließbaren Türen.

Firmware aktuell halten: Für neuere Drucker gibt es seitens der Hersteller Firmwareupdates, die man zügig nach deren Veröffentlichung über die Treiber-Suite des Druckers einspielen sollte.

Alte Drucker nicht freigeben: Je älter ein Drucker, desto ergiebiger ist die Suche nach Lücken. Ein HP Laserjet 1320, gut 15 Jahre alt, zeigte sich besonders verwundbar. Solche alten, wenn auch funktional zuverlässigen Drucker sollten im Netzwerk nicht verfügbar sein, sondern nur noch lokal am PC betrieben werden.

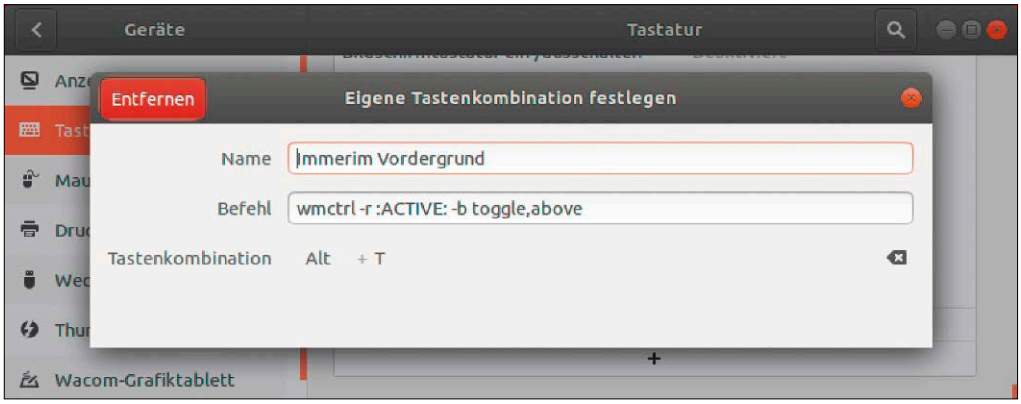
Drucker per Printserver abschotten: Generell ist es eine gute Idee, netzwerkfähige Drucker nicht direkt ins Netzwerk zu hängen, sondern an einen Printserver anzuschließen. Ein Beispiel, einen Raspberry Pi zu einem Druckserver zu machen, finden Sie unter *https://www.pcwelt.de/2190873*.

Desktop auf Kurs

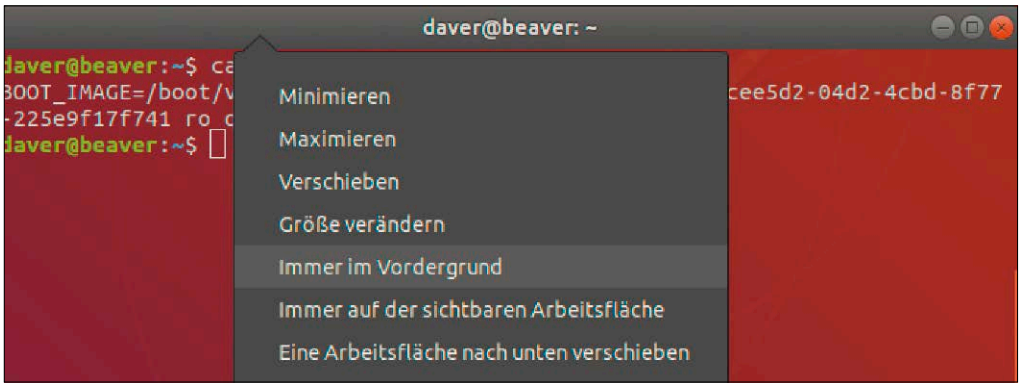
Unterschiedliche Zielsetzungen lassen die Linux-Desktops auseinanderdriften: Während es bei KDE um maximale Konfigurationsmöglichkeiten geht, will Gnome einfach und einheitlich sein. Ein paar Tricks bringen aber auch diesen Desktop auf Kurs.

Fenster: Per Tastendruck ganz oben

Programmfenster, aus welchen es etwas abzutippen gilt, hält man am besten aktiv im Vordergrund, über allen anderen Fenstern. Die meisten Linux-Desktops erlauben diese Einstellung nach einem Rechtsklick auf der Titelleiste der gewünschten Programme. In Gnome lautet der Kontextmenüpunkt dazu beispielsweise „Immer im Vordergrund“. Wer diese Funktion sehr oft braucht, dann kann sich eine eigene Tastenkombination dazu bauen.



Fenster nach oben holen: wmctrl steuert das Fensterverhalten auf dem X-Window-System und hält Fenster in den meisten Desktopumgebungen per Tastenkombination im Vordergrund.



Will immer oben liegen: Soll kein anderes Programm den Fensterinhalt verdecken, so hilft diese Funktion weiter, für die man sich auch eine Tastenkombination bauen kann.

Eine Zutat ist das Hilfsprogramm wmctrl, das die Eigenschaften von Programmfenstern auf dem X-Window-System beeinflussen kann und Fenster beispielsweise permanent in den Vordergrund holt. Es findet sich in den Paketquellen aller Linux-Distributionen. Mit dem Kommando

```
sudo apt-get install
  wmctrl
```

ist es in Debian, Ubuntu, Linux Mint und anderen Distributionen mit dem DEB-Paketsystem installiert. Anschließend stattet man in den Einstellungen der verwendeten Desktopumgebung den Tastenkombinationen einen Besuch ab. Die Einstellungen zu selbst definierten Tastenkombinationen finden sich in Gnome unter „Einstellungen → Geräte → Tastatur“ und in KDE unter „Systemeinstellungen → Arbeitsbereich → Kurzbefehle → Eigene Kurzbefehle“. Generell liefern alle Arbeitsumgebungen ein Menü zur Definition eigener Hotkeys.

Bei der Erstellung der Tastenkombination zum permanenten Anheben eines Fensters trägt man in das Feld „Befehl“ den Aufruf

```
wmctrl -r :ACTIVE: -b
  toggle,above
```

ein und vergibt dafür eine griffige Tasteneingabe wie Alt-T. Drückt man nun diese Tastenkombination, so ist das aktuelle Fenster immer im Vordergrund, bis Sie die Kombination erneut drücken. Eine Ausnahme ist Gnome, bei welchem man die Titelleiste rechts anklicken muss, um den Haken vor „immer im Vordergrund zu entfernen“.

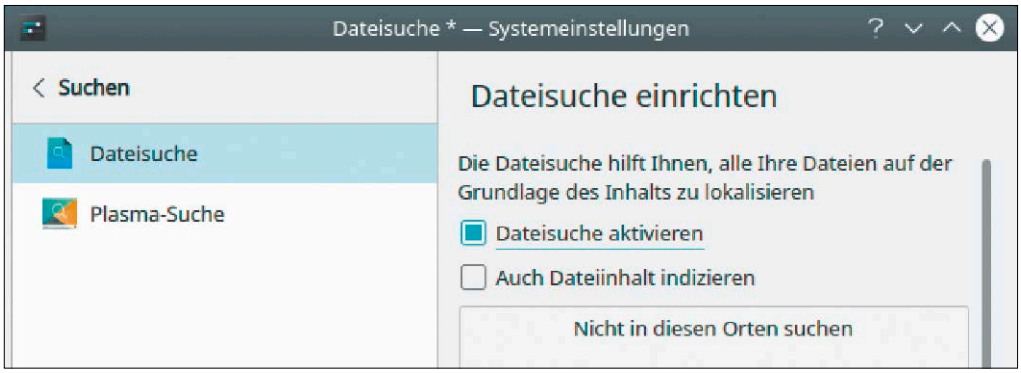
Hinweis: Das Tool wmctrl kann nur Fenster eines X-Window-Systems verändern. Mit dem neuen Displayserver-Protokoll von Wayland, das in Fedora 28 bereits Standard ist, funktioniert es noch nicht. **-dw**

KDE Plasma 5: Indexdienst abschalten

Mit KDE Plasma 5 hat die Desktopumgebung den notorisch speicherhungrigen Indexdienst im Hintergrund gegen den effizienteren Dienst Baloo ausgetauscht. Ein anderes Problem bleibt aber: Die Indexdateien werden wie bei anderen Volltext-Suchmaschinen wie Recoll und Tracker sehr groß – bei Texten ist der Index oft beinahe so umfangreich wie die Originaldateien. Wie groß der Index der gesammelten Daten von Baloo bereits ist, verrät ein Blick in das Verzeichnis „~/.local/share/baloo/". In diesem Unterordner des Home-Verzeichnisses speichert Baloo seine Indexdateien. Wenn der Platz auf einer kleinen SSD einfach zu schade ist, um ihn für einen Suchindex zu verbraten, oder falls der Indexprozess „baloo_file" auf einem langsameren Rechner immer wieder für zu hohe Prozessorauslastung sorgt, dann sollte man Baloo einfach abschalten. Die KDE-Entwickler haben dazu in KDE-Plasma in der Systemsteuerung den neuen Schalter „Suchen → Dateisuche aktivieren" untergebracht. Ist diese Option deaktiviert, dann läuft auch der Indexdienst nicht mehr. Den bereits erstellten, nicht mehr benötigten Index kann man manuell löschen – im Terminal

```
rm -rf~/.local/share/
  baloo/
```

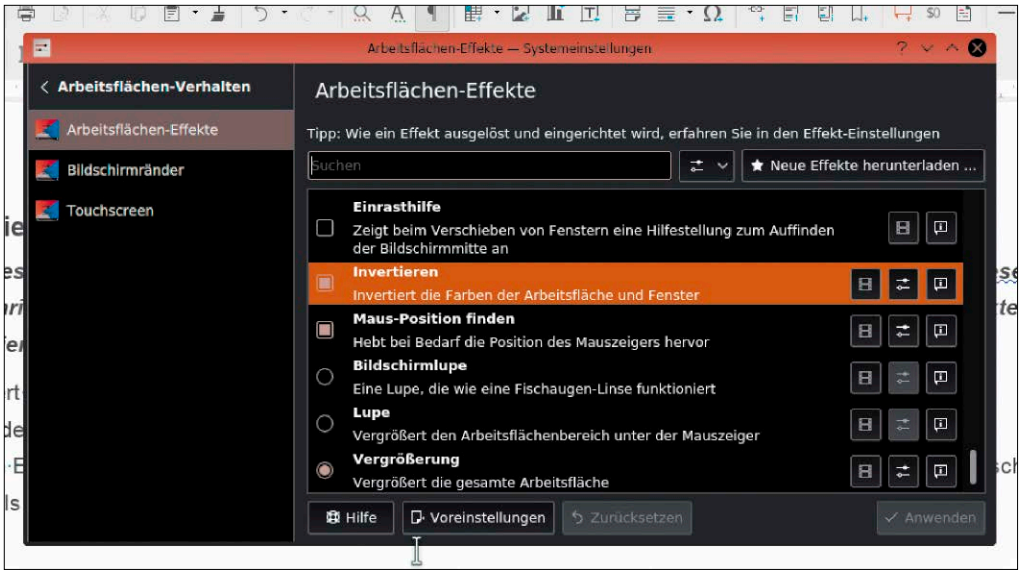
oder wahlweise auch mit dem Dateimanager. **-dw**



KDE Plasma 5 ohne Baloo: Mittlerweile hatten die KDE-Entwickler ein Einsehen und haben diesen Schalter in den Systemeinstellungen zum Deaktivieren des Indexdiensts ergänzt.

KDE Plasma 5: Fensterfarben invertieren

Helles Sonnenlicht produziert selbst auf den besseren, kontrastreichen Notebookbildschirmen schwer zu erkennende Suchbilder. Unter diesen Lichtverhältnissen Texte mit schwarzer Schrift auf weißem Grund zu lesen, bereitet kein Vergnügen. KDE Plasma 5 kann mit seinen Effekten gezielt die Farben einzelner Fenster invertieren und damit den Inhalt lesbarer machen. Zuerst muss der Effekt zur Invertierung aktiviert und schließlich mit der gewünschten Tastenkombination versehen werden. Die Einstellung der Fensterverwaltung Kwin und deren Effekte finden Sie in den KDE-Systemeinstellungen unter „Arbeitsbereich → Arbeitsflächen-Verhalten → Arbeitsflächen-Effekte". Dort schalten Sie den Effekt „Invertieren" ein. Die Standard-Tastenkombination zum Umkehren aller Farben auf dem Bildschirm ist Strg-I. Nur das aktuelle Fenster lässt sich mit Win-Umschalt-I farblich umkehren. Ein erneuter Druck der Tastenkombination stellt die gewöhnlichen Farben wieder her. Besonders nützlich ist der Kwin-Effekt bei schlecht lesbaren Terminalfenstern. **-dw**



Besser lesbar unter schwierigen Bedingungen: Der Invertierungseffekt für einzelne Fenster gehört zu den nützlichen Effekten in KDE Plasma 5. Allerdings muss man ihn erst einschalten.

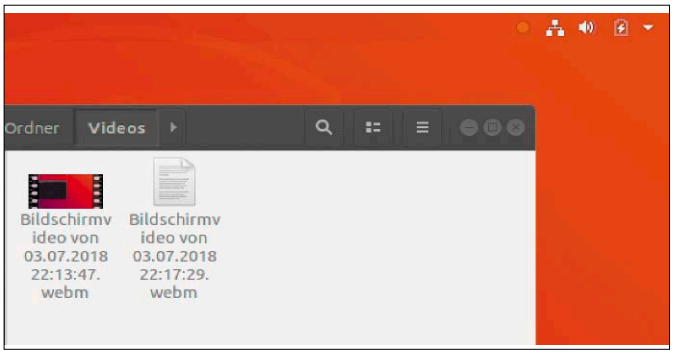
Gnome: Versteckter Videorecorder

Es muss nicht kompliziert sein, ein kurzes Video von den Aktivitäten am Bildschirm aufzunehmen. Das neue Gnome, das auch in Ubuntu 18.04 vorhanden ist, bietet eine versteckte Recorderfunktion. Nützlich sind Bildschirmaufnahmen beispielsweise, um kurze, anschauliche Anleitungen zu versenden oder zu veröffentlichen.

Auf eine Programmverknüpfung zum Gnome-Videorecorder verzichteten die Entwickler. Der Recorder lässt sich nur mit der Tastenkombination Strg-Alt-Umschalt-R starten und mit der gleichen Kombination dann auch wieder anhalten. Während der Recorder aufnimmt, zeigt sich in der rechten oberen Ecke des Gnome-Panels ein Aufnahmesymbol. Aufgenommen wird immer der komplette Desktop und das verwendete Format ist das quelloffene, zu den meisten Schnittprogrammen kompatible Format „Webm“. Die aufgenommenen Dateien legt Gnome im Ordner „Videos“ im Home-Verzeichnis ab. Die maximale Länge der Aufnahmen beträgt 30 Sekunden. Falls das nicht reicht, kann man auch noch etwas mehr Zeit herausholen: Der Befehl

```
gsettings set org.gnome.
  settings-daemon.
  plugins.media-keys max-
  screencast-length 50
```

verlängert die maximale Aufnahmedauer beispielsweise auf 50 Sekunden. **-dw**

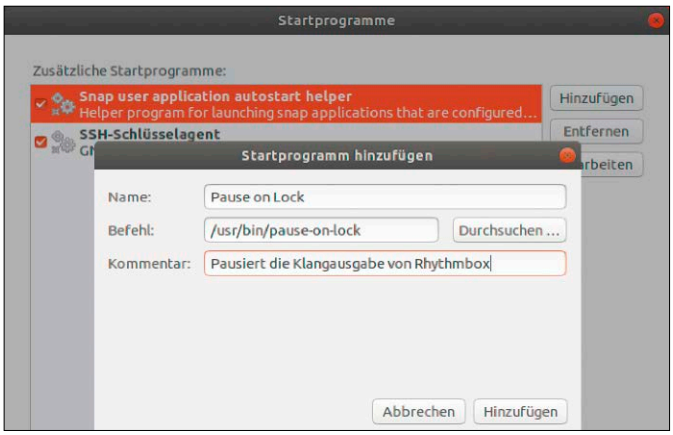


Aufnahme läuft: Ist der Videorecorder aktiv, so zeigt sich rechts oben ein Aufnahmesymbol. Die Videos landen im freien Webm-Format auf der Festplatte.

Gnome und Unity: Kein Sound bei Inaktivität

Das übliche Verhalten von Gnome und dem nahe verwandten Unity ist es, die Klangausgabe von Playern weiterlaufen zu lassen, auch wenn die Bildschirmsperre einsetzt. Das Verhalten lässt sich aber auch ändern, sodass der Player in Phasen der Inaktivität stoppt.

Für Debian, Ubuntu, Linux Mint und andere Debian-Ableger gibt es mit Pause on Lock ein Tool, das unterstützte Player automatisch während einer Bildschirmsperre anhält. Dieses Programm nutzt dazu die Schnittstelle D-Bus zur Kommunikation mit Mediaplayern. Folglich funktioniert Pause on Lock erst mal nur mit jenen Playern, die ein D-Bus-Interface haben. Das sind beispielsweise Rhythmbox und Spotify.



Rhythmbox und Spotify während der Bildschirmsperre anhalten: Pause to Lock hält die Player bei Inaktivität an. Der Entwickler arbeitet gerade an der Anbindung weiterer Player.

Die Installation des Tools gelingt in Debian und Ubuntu einfach über ein fertiges DEB-Paket des Entwicklers von dessen Github-Webseite *https://github.com/folixg/pause-on-lock/releases*. Das Paket installiert dann im Terminalfenster dieser Befehl:

```
sudo dpkg -i pause-on-
  lock_1.2-0ubuntu1_all.
  deb
```

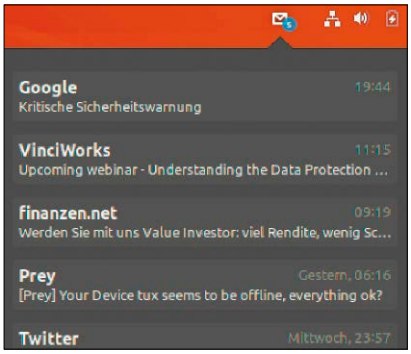
Aktiv wird das Tool aber erst, wenn es über den Ausführen-Dialog mit dem Befehl *pause-on-lock* gestartet oder zu den Autostart-Programmen hinzugefügt wird. Zu deren Konfiguration liefert Ubuntu weiterhin das Tool Startprogramme mit, das sich über die Aktivitäten-Übersichtsseite findet. Die dazu benötigte Pfad zur Programmdatei von Pause on Lock lautet „/usr/bin/pause-on-lock“.

Zum Testen des Tools müssen Sie nicht auf den Bildschirmschoner warten: Auch die Tastenkombination Win-L schaltet die Bildschirmsperre unter Gnome ein. **-dw**

Mailnag: Postfächer überprüfen

Es gibt eine Reihe von Möglichkeiten, sich über eingehende Mails benachrichtigen zu lassen, etwa über Browsererweiterungen. Das Tool Mailnag präsentiert dagegen Benachrichtigungen auf dem Desktop und unterstützt dabei in der aktuellen Version zahlreiche Arbeitsumgebungen.

Mailnag kann Postfächer über POP und IMAP überwachen sowie die Webmail-Dienste von Google, GMX und Web.de. An den Start ging das in Python geschriebene Tool vor sieben Jah-



Mailnag-Konfiguration: Das Programm bringt ein kleines Tool zur Einrichtung der Konten mit. Die Passwörter der Konten speichert es verschlüsselt im Gnome-Keyring.

Die neuesten Mails im Postfach: Mailnag arbeitet jetzt nicht nur unter Gnome, sondern auch in anderen Desktopumgebungen. Für Gnome gibt es als Extra diese Shell-Erweiterung.

ren zunächst als Erweiterung für Gnome 3. Der Entwickler ließ es aber nicht dabei, sondern hat Mailnag um breite Unterstützung mehrerer Desktopumgebungen erweitert.

Das Tool nutzt das standardisierte Benachrichtigungssystem „libnotify" für Meldungen über neue Mails in überwachten Postfächern und arbeitet damit unabhängig von Linux-Desktops.

In Ubuntu 18.04 ist Mailnag in den offiziellen Paketquellen in der aktuellen Version vorhanden und mittels

```
sudo apt-get install
 mailnag
```

schnell installiert. Auch Debian, Fedora und Open Suse kennen Mailnag in ihren Standard-Paketquellen. In der Grundausstattung arbeitet Mailnag unabhängig vom Desktop. Wer Gnome verwendet, kann im neuen Ubuntu zusätzlich noch mittels

```
sudo apt-get install
 gnome-shell-mailnag
```

eine Gnome-Shell-Erweiterung installieren.

Die erste Konfiguration von Mailnag ruft die Eingabe

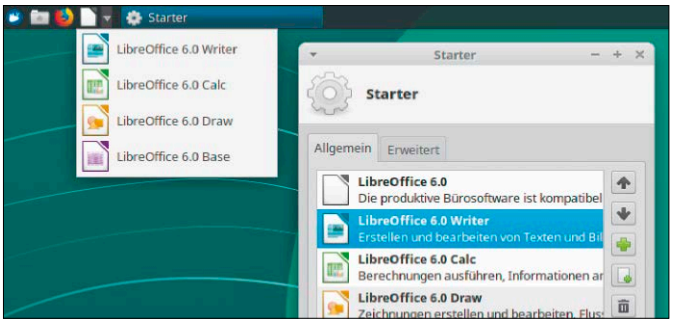
```
mailnag-config
```

im Ausführen-Dialog (Alt-F2) oder im Terminal auf. Dort richtet der Punkt „Konten" den Zugriff auf die zu überwachenden Postfächer ein. Das hinterlegte Password speichert Mailnag dabei übrigens nicht unverschlüsselt auf der Festplatte, sondern im sicheren Passwortspeicher von Gnome, dem Gnome-Keyring. Unter „Plugins" steht noch zur Auswahl, wie Mailnag über neue Mails informieren soll. Falls in Gnome die zugehörige Shell-Erweiterung installiert wurde, muss man sich zunächst einmal ab- und wieder anmelden. Anschließend kann man Mailnag für Gnome im Konfigurationswerkzeug „gnome-tweak" unter „Erweiterungen" aktivieren. **-dw**

XFCE: Multistarter in der Leiste

Die Leisten der Desktopumgebung XFCE können beliebige Starter mit Abkürzungen zu häufig benötigten Programmen ergänzen. Eine weniger bekannte Eigenschaft der Starter ist die Möglichkeit, mehrere Verknüpfungen unter einem Symbol im Panel unterzubringen.

Nützlich sind verschachtelte Starter, um mehrere Programmverknüpfungen aus Platzgründen oder aus logischen Gründen zusammenzufassen. So funktioniert es: Nach einem Rechtsklick auf das Panel und der Auswahl des Menüpunkts „Leiste → Neue Elemente hinzufügen" wählen Sie in der angezeigten Liste den Starter und platzieren diesen zunächst nur an der gewünschten Stelle auf der XFCE-Leiste. Danach lässt sich der neue Starter mit einem weiteren Rechtsklick darauf einrichten: Über „Eigenschaften → Allgemein" und das große Pluszeichen rechts holt man sich ein installiertes Programm in den Starter, der dann übrigens im Panel auch das Symbol dieser Anwendung annimmt. Aber es geht weiter: Jeder weitere Klick auf das Plus-Symbol kann ein weiteres Programm in den Starter holen. Der bekommt einen seitlichen Pfeil, der die zusätzlichen Symbole ausklappt. **-dw**



Schublade für weitere Verknüpfungen: Starter in der XFCE-Leiste können mehrere Programme aufnehmen und zu Gruppen zusammenfassen.

GNOME USAGE: EIN NEUER SYSTEMMONITOR

Ohne große Fanfaren hat Gnome 3.28, das in dieser Version der Standarddesktop von Ubuntu 18.04 wurde, einen neuen Systemmonitor zur Kontrolle der Systemauslastung und Festplattenbelegung bekommen. Das neue Systemwerkzeug namens „Gnome Usage" folgt in seinem schlichten, eleganten Design der Gnome-Philosophie, möglichst auf Menüelemente zu verzichten. In Fedora 28 und Ubuntu 18.04 liegt es zur Installation in den Paketquellen, vorinstalliert ist es allerdings nicht. In der Kommandozeile installiert

```
sudo apt-get install gnome-usage
```

den Systemmonitor im neuen Ubuntu. Eine nützliche Funktion ist die Suche nach Programmnamen über das Lupensymbol rechts oben auf der Unterseite „Speicher".

Ein Klick auf einen Prozessnamen kann diesen auf Nachfrage beenden. Der bisherige Systemmonitor, der gnome-system-monitor („Systemüberwachung") ist mit seiner differenzierten Prozessverwaltung aber noch nicht obsolet und bleibt vorerst das Standardprogramm unter Gnome. **-dw**

Systemressourcen im Blick: Der neue Systemmonitor von Gnome 3.28 zeigt sich schlicht und elegant. Er liegt in den Paketquellen von Ubuntu 18.04 bereit.

Kommandobrücke

Diesmal steht SSH im Zentrum der Konsolentipps: Die Möglichkeit, SSH-User auf die SFTP-Dateiübertragung einzuschränken und dabei in ihr Home-Verzeichnis einzusperren, gehört zu häufigen Konfigurationsszenarien für einen SSH-Server.

SSH: Nur Dateiübertragung erlauben

Das Protokoll SSH (Secure Shell) eignet sich nicht nur zur Fernwartung von Systemen per Shell-Zugang, sondern auch zur sicheren Dateiübertragung. Diese Aufgabe lässt sich weiter optimieren: Auf einem Linux-System, das dem Dateiaustausch dient, sollen ausgewählte Benutzer keinen Shell-Zugang erhalten und aus einem definierten Home-Verzeichnis nicht herauskommen. Lange brauchte es dazu einiger Tricks oder die Hilfe einer externen Pseudo-Shell wie RSSH (*www.pizzashack.org/rssh*). Mittlerweile hat Open SSH standardmäßig diese Funktion an Bord. Das folgende Beispiel zeigt, wie man den User „test" auf SFTP und einer Chroot-Konfiguration in dessen Home-Verzeichnis eingrenzt. Eine Shell-Anmeldung oder der Zugriff auf fremde Verzeichnisse per SFTP-Client ist dann nicht mehr möglich.

1. Der erste Schritt ist die Bearbeitung der SSH-Konfigurationsdatei „/etc/ssh/sshd_config" mit root-Berechtigungen. Kommentieren Sie die Zeile

```
Subsystem sftp /usr/lib/
  openssh/sftp-server
```

durch „#"-Zeichen am Zeilenanfang aus und tragen Sie darunter diese Zeile ein:

```
Subsystem sftp internal-
  sftp
```

2. Ganz ans Ende der Datei kommen für den User „test" diese vier Zeilen:

```
Match User test
ChrootDirectory %h
ForceCommand internal-
  sftp
AllowTcpForwarding no
```

Danach speichern Sie die Konfigurationsdatei starten mit

```
sudo systemctl restart
  sshd
```

den SSH-Dienst neu.

3. Das Home-Verzeichnis „/home/test" des gleichnamigen Users erhält jetzt root als Besitzer, denn sonst wird eine Anmeldung nicht gelingen. Dies erledigen diese beiden Befehle:

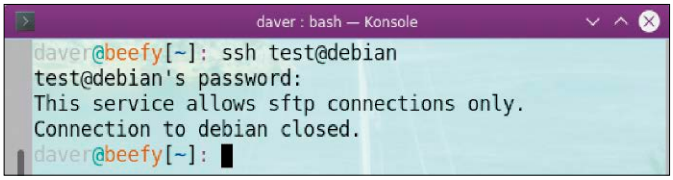
```
sudo chown root:root /
  home/test/
sudo chmod 0755 /home/
  test/
```

4. Damit der Benutzer „test" Dateien über SFTP weiterhin hoch- und herunterladen kann, benötigt dieser User jetzt noch einen beschreibbaren Unterordner im Home-Verzeichnis. Mit den Kommandos

```
sudo mkdir /home/test/
  daten
sudo chown test:test /
  home/test/daten
```

legt dazu das Unterverzeichnis „/home/test/daten" an.

5. Damit ist alles erledigt und der Benutzer „test" kann sich mit SFTP-Clients wie Filezilla oder dem Midnight Commander am System anmelden und das vorbereitete Verzeichnis zur Datenübertragung nutzen. Bei der SSH-Anmeldung auf der Shell zeigt der SSH-Server allerdings nur mehr die Meldung „This service allows sftp connections only" an.



Shell-Anmeldung unmöglich: Der Benutzer „test" darf sich nur zum Dateiaustausch per SFTP an diesem Linux-Server anmelden, aber keine Befehle ausführen.

Ist keine Anmeldung als „test" möglich, so liegt das meist an unpassenden Zugriffsrechten auf das Chroot-Verzeichnis „/home/test", das in diesem Fall root gehören muss. Reagiert der SSH-Server nicht auf Veränderungen an seiner Konfigurationsdatei, so fehlt meist nur der Neustart des SSH-Dienstes. **-dw**

SSH: Selbsttest vor Neustart

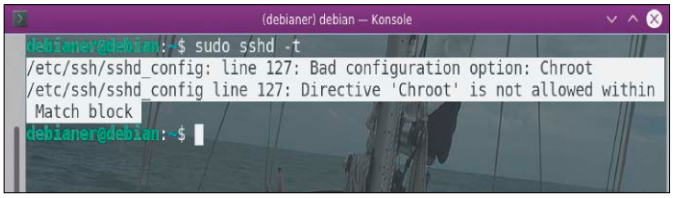
Auf einem entfernten System darf bei einem Neustart des Open-SSH-Servers mit veränderter Konfiguration nichts schiefgehen. Denn Syntaxfehler in der Konfigurationsdatei führen schlimmstenfalls dazu, dass der SSH-Dienst anschließend nicht mehr läuft und alle ausgesperrt sind.

Vor einem Neustart des SSH-Dienstes mit veränderter Konfiguration kontrolliert der Aufruf

```
sudo sshd -t
```

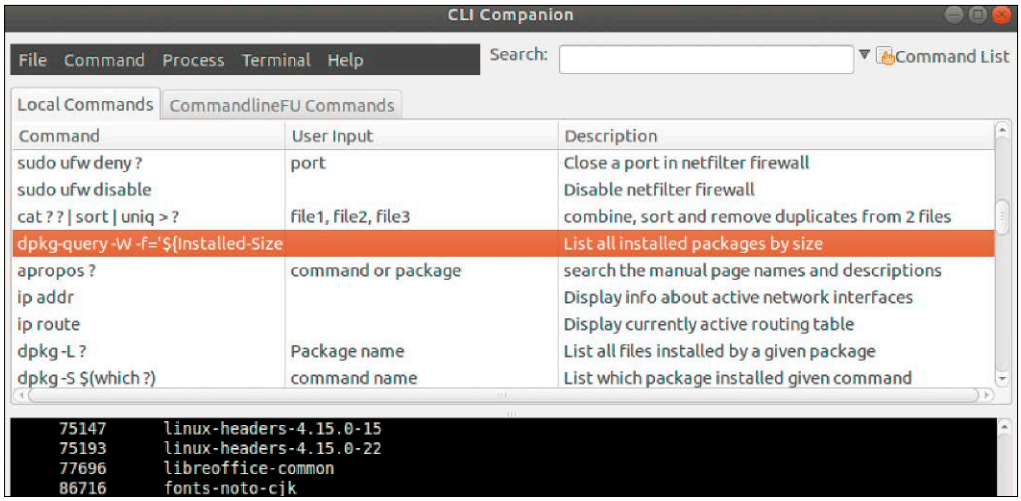
die Syntax der Datei „/etc/ssh/sshd_config".

Falls sich dieser Befehl ohne weitere Ausgabe beendet, passt deren Syntax. Sollte die Konfiguration aber Fehler enthalten, die den Neustart des SSH-Dienstes verhindern könnten, so wird das Kommando mit Zeilennummer und einem Auszug aus der Konfiguration darauf hinweisen. **-dw**



SSH-Fehler ausschließen statt aussperren: Nach Konfigurationsänderungen warnt dieser Aufruf vor fatalen Fehlern, die den SSH-Dienst lahm legen können.

CLI Companion: Eine Bibliothek für Befehle



Handliche Hilfestellung: Mit dem CLI Companion kann man sich eine eigene Sammlung nützlicher Shell-Kommandos aufbauen und diese nach Stichwörtern oder Befehlen durchsuchen.

Wie lautete eben wieder dieser nützliche, aber äußerst lange Befehl? Komplexe Kommandos sind schwer im Gedächtnis zu behalten. Der Befehlsverlauf der Shell ist eine gute Gedächtnisstütze, aber als Archiv für wichtige und interessante Kommandos nicht strukturiert genug.

Der CLI Companion ist eine erweiterbare Datenbank nützlicher Befehle und damit eine einsteigerfreundliche Hilfestellung für die ersten Schritte in der Shell. Das englischsprachige Programm für Debian/Ubuntu kombiniert ein Menü zur Verwaltung von Befehlen in einer Liste mit einem Terminalfenster. Das zweigeteilte Fenster zeigt oben die wichtigsten Kommandos für Einsteiger und unten das eingebettete Terminal. Der CLI Companion bringt eine durchsuchbare Liste praktischer Befehle zum Einstieg schon mit. Ideal ist das Programm aber auch, um sich nützliche und lange Befehle mit Kommentar zu notieren, sie schnell wiederzufinden und per Klick abzurufen.

Nicht ganz geradlinig ist die Installation des CLI Companion: Es gibt zwar unter *https://launchpad.net/clicompanion* ein fertiges DEB-Paket, aber in den Paketquellen Debians oder Ubuntus ist das Programm derzeit nicht zu finden. Den Download der Datei „clicompanion_1.3-1_all.deb" muss man also manuell erledigen. In Ubuntu kann der Punkt „Anwendungsinstallation" als ausgewählte Aktion für den Download im Browser die DEB-Datei gleich installieren und dabei eventuell vorhandene Abhängigkeiten auflösen. Mit

```
sudo apt install ./[DEB-Paket]
```

gelingt dies aber auch in der Kommandozeile mit dem Paketmanager apt. Das DEB-Paket muss dazu im aktuellen Verzeichnis liegen.

Nach dem Start zeigt der CLI Companion oben eine Tabelle der mitgebrachten Kommandos. Die Spalte links zeigt den Befehl, die mittlere Spalte „User Input" gibt an, welche Parameter bei der Eingabe noch gefragt sind, und ganz rechts findet sich noch eine englischsprachige Beschreibung. Zum Ausführen eines Befehls dient ein Doppelklick; eigene Kommandos kann ein Klick auf „Hinzufügen" ergänzen. Alle eingetragenen Befehle speichert der CLI Companion übrigens in der versteckten Datei „.clicompanion2" im Home-Verzeichnis. Um die Befehle zwischen Systemen auszutauschen, müssen Sie nur diese Datei auf andere Linux-Rechner kopieren. **-dw**

Wget: Mit angezogener Handbremse

Wo mehrere Anwender eine gemeinsame, eher langsame Internetverbindung gemeinsam nutzen, macht sich ein Download mit Wget drastisch bemerkbar, da Wget die Bandbreite gut ausschöpft. Abhilfe schafft ein spezieller Schalter.

Es gibt den Parameter „--rate-limit", der die genutzte Bandbreite von Wget begrenzt und das Tool bei geteilten Internetverbindungen sozialverträglicher macht. Mit folgendem Kommando

```
wget --limit-rate 200k http://[URL]
```

wird Wget beispielsweise nur bis maximal 200 KB/s gehen. Bei langsamen und instabilen Internetverbindungen sind zudem Parameter zum automatischen Wiederaufnehmen des Downloads empfehlenswert. Mit dem Aufruf

```
wget --tries=0 --continue
  --server-response
  --timeout=0 --retry-
  connrefused http://[URL]
```

lässt sich Wget auch bei zwischenzeitlich unterbrochenen Verbindungen nicht aus der Ruhe bringen lassen. Die Parameter sind mit „--rate-limit" kombinierbar und ideal für große Downloads. **-dw**

Langsam, aber unaufhaltsam: So arbeitet Wget mit langsamen 200 KB/s Downloadgeschwindigkeit, bleibt aber auch bei instabilen Verbindungen robust.

Hardware ahoi!

Die Hardwaretipps umsegeln das wachsende Kabelchaos auf dem Schreibtisch, betrachten aus der Ferne das Wetterradar im Fünf-GHz-Frequenzband und loten den erstaunlich seichten Pool der Zufallszahlen auf einem Raspberry Pi aus.

SSD: Temperatur auslesen

Viele moderne SSDs sind mit aufwendigen Kühlblechen ausgestattet. Diese sind nicht nur ein Designelement, sondern bei hoher I/O-Last tatsächlich nötig. Werden SSDs zu heiß, so drosselt der Controllerchip die Leistung, um die Temperaturen des Halbleiterspeichers im sicheren Bereich zu halten.

Ab etwa 70 bis 75 Grad Celsius ist bei SSDs mit einer automatischen Drosselung der Leistung („Thermal Throtteling“) zu rechnen.

Die aktuelle Temperatur eines Datenträgers zeigt unter Linux das Kommandozeilentool hddtemp aus dem gleichnamigen Paket an, das in Debian/Ubuntu mit dem Kommando

```
sudo apt-get install
  hddtemp smartmontools
```

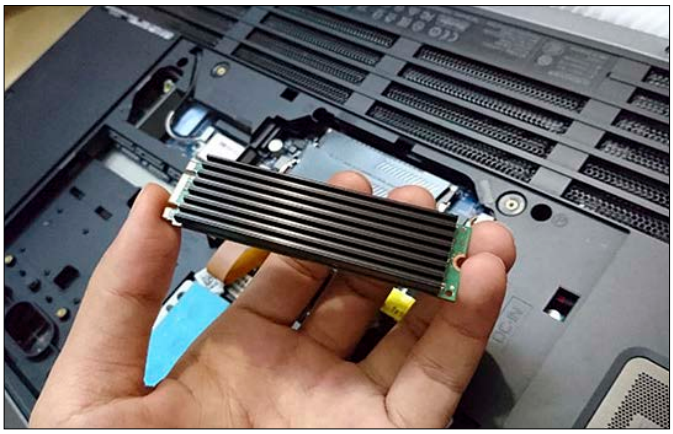
installiert ist. Der Abruf der Temperatur erfolgt mittels

```
sudo hddtemp /dev/sda
```

wobei „/dev/sda“ der Gerätepfad des abgefragten Laufwerks ist. Falls dieser nicht bekannt ist, so zeigt das Kommando *lsblk -d* die Gerätepfade aller Laufwerke an. Einige ältere SSDs von Intel enthalten keinen Temperatursensor. Falls hddtemp nichts anzeigt, so hilft bei den meisten SSDs noch diese Alternative:

```
sudo smartctl -a /dev/
  sda|grep -i temp
```

Falls eine SSD häufig heißer als 60–70 Grad wird, sollte man im PC-Gehäuse für eine bessere Belüftung sorgen. Falls genügend Platz ist, können auf M.2-Laufwerken nachträglich aufgeklebte Kühlkörper helfen.



Quelle: Electric Magic

Heiße Sachen: Werden M.2-Laufwerke im Dauerbetrieb über 70 Grad heiß, dann drosseln sie ihre Leistung. Zusätzliche Kühlbleche können aushelfen (*https://amzn.to/2J6v1lo*).

Tipp: Psensors aus den Ubuntu-Paketquellen ist eine bequeme Methode, um auf dem Desktop die Temperaturen von CPU, Festplatten und SSDs mit Sensor im Auge zu behalten. **-dw**

USB: Versenkter Schreibtisch-Hub

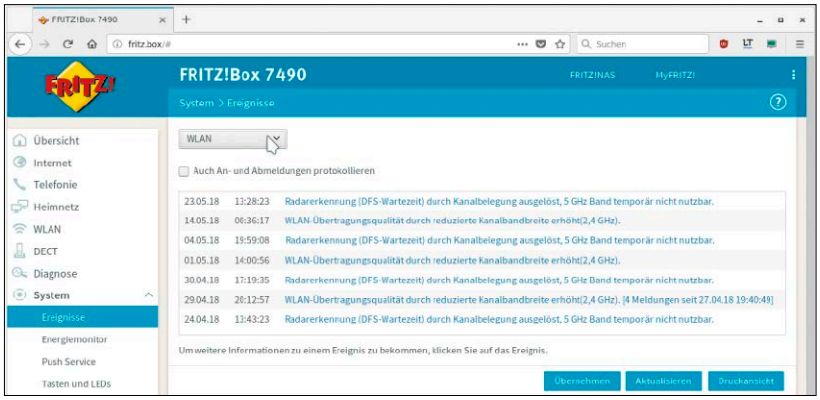
Smartphones und etliche externe Datenträger vom USB-Stick bis zur USB-Festplatte sind meist permanente Bewohner des Schreibtischs und verlangen nach immer mehr USB-Anschlüssen. Wenn der PC ganz klassisch unter dem Schreibtisch steht, wird die Menge von verlegten USB-Kabeln unübersichtlich und unansehnlich sowieso.

Abhilfe und Ordnung schaffen USB-Hubs für typische Büroschreibtische mit vorgebohrten Kabeldurchführungen, die üblicherweise einen Durchmesser von 60 mm haben. Es gibt inzwischen eine breite Auswahl an Hubs, die perfekt in diese Aussparung passen, damit in der Tischplatte versenkt sind, die nötigen Anschlusskabel zum PC reduzieren, an einem fixen Ort bleiben und nicht regelmäßig durch einen ungünstigen Zug am Kabel von der Schreibtischfläche fallen. Der Icy Box IB-Hub1403 liefert beispielsweise viermal USB 3.0 mit Typ-A-Anschlüssen und ist im Versandhandel für etwa 21 Euro zu haben (*https://amzn.to/2LcwpiT*). Vom gleichen Hersteller gibt es noch das Modell Icy Box IB-Hub1404, das USB-C, Kartenleser und ein eigenes Netzteil mitbringt, das Mobilgeräte auch dann laden kann, wenn der Rechner ausgeschaltet ist (ab 52 Euro, *https://amzn.to/2xyHpoY*). Eine günstigere Alternative dazu – ohne USB-C – ist der USB-Hub von Xystec mit vier USB-3.0-Ports, Audioanschlüssen und einem optionalen externen Netzteil (35 Euro, *https://amzn.to/2HdEe5i).e5i*). **-dw**

Quelle: Icy Box

Sauber versenkt: USB-Hubs für Schreibtisch-Kabeldurchführung verschiedener Hersteller passen genau in die runden standardisierten Aussparungen mit 60 mm Durchmesser.

AVM Fritzbox: WLAN mit Pausen



Dynamic Frequency Selection in Aktion: Wenn im Fünf-GHz-Band Störsender wie das Wetterradar liegen, sucht die Firmware der AVM Fritzbox selbständig nach einem freien Kanal.

Der WLAN-Standard 802.11n und das schnelle 802.11ac bewegen sich im Fünf-GHz-Spektrum. Nutzer einer AVM Fritzbox mit Unterstützung dieser WLAN-Standards müssen auf dieser Frequenz immer wieder mal minutenlange Aussetzer des Drahtlosnetzwerks beobachten.

Den Grund für diese Aussetzer liegt in den WLAN-Standards mit fünf GHz selbst: Funknetzwerke müssen sich in Europa dieses Frequenzband mit Wetterradar teilen. Damit sich die Sender nicht stören, muss ein Funknetzwerk bei der Erkennung eines Wetterradars innerhalb des Spektrums auf einen anderen Kanal ausweichen. Diese Technik nennt sich „Dynamic Frequency Selection" (DFS) und ist in den WLAN-Standards festgelegt. In regelmäßigen Abständen muss ein Access Point deshalb das Frequenzband auf Radarquellen überprüfen. Laut AVM kann dieser Suchlauf bei älteren Fritzbox-Modellen bis zu zehn Minuten dauern. In dieser Zeit ist das fünf-GHz-WLAN nicht erreichbar. Überprüfen kann man dieses Verhalten auf der Administrationsoberfläche der Fritzbox: Unter „System → Ereignisse" schaltet man im ausklappenden Menü zu den Kategorien oben links auf „WLAN". Die planmäßigen Aussetzer des Fünf-GHz-Frequenzbands sind dort mit dem Text „Radarerkennung (DFS-Wartezeit) durch Kanalbelegung ausgelöst, 5 GHz Band temporär nicht nutzbar" ausgewiesen.

Eine Lösung ist es, das Funknetz im Fünf-GHz-Band auf einen Kanal einzustellen, der von der Regelung nicht betroffen ist. Das gilt für die Kanäle 36, 40, 44 und 48. Für die Konfiguration des verwendeten Kanals gehen Sie auf „WLAN → Funkkanal", markieren dort „Funkkanal-Einstellungen anpassen" und wählen neben „Funkkanal im 5-GHz-Frequenzband" einen der angezeigten Kanäle aus.

Für experimentierfreudige Anwender hat AVM für die Modelle 7490 und 7590 der Fritzbox eine neue Betafirmware zum Testen vorgestellt, die DFS Wartezeiten im Fünf-GHz-Band deutlich verkürzt. Die Firmware steht unter *https://avm.de/fritz-labor/fritz-labor-fuer-fritzbox-7490-und-7590* zum Download bereit. **-dw**

Raspberry Pi: Bessere Zufallszahlen

Zufallsgenerator mit Hardwarehilfe: Der Raspberry Pi hat in seinem System-on-Chip einen Zufallsgenerator, der die Leistung von „/dev/random" und „/dev/urandom" verbessert.

Zufällige Zahlenreihen sind für die meisten Formen alltäglicher Kryptografie unentbehrlich. Der Linux-Kernel stellt mit „/dev/random" sowie „/dev/urandom" Zufallsgeneratoren bereit.

Generell gelten auf Computersystemen erzeugte Zahlenreihen nicht als zufällig genug, wenn die Entropie nur aus einer Quelle gespeist wird. Seit dem Kernel 3.16 fließen deshalb auch Daten von angeschlossenen Geräten in den Zufallsgenerator mit ein. Auf einem Raspberry Pi, der als kleiner Server dient, genügen im Dauerbetrieb die gesammelten Zufallszahlen meist nicht. Kryptografische Operationen werden damit sehr langsam beziehungsweise unzuverlässig.

Der System-on-Chip aller Raspberry Pis enthält einen hardwarebasierten Zufallsgenerator als Gerät „/dev/hwrng" als zusätzliche Quelle.

Weil dafür aber nicht von Anfang an Kernel-Treiber für den Raspberry Pi bereitstanden, ist dieser schnelle Zufallsgenerator auch in den aktuellen Ausgaben der offiziellen Debian-Distribution „Raspbian" nicht standardmäßig eingebunden. Abhilfe schafft das Paket „rng-tools", das in Raspbian mit dem Kommando

```
sudo apt-get install rng-tools
```

leicht nachinstalliert ist. Die Installation startet den Systemd-Dienst „rngd.service" automatisch, der ab jetzt „dev/random „und „/dev/urandom" zusätzlich mit Zufallszahlen des Generators „/dev/hwrng" füttert.

Tipp: Um dem Zufallsgenerator bei der Arbeit zuzusehen, eignet sich dieser Befehl:

```
dd if=/dev/random of=/
  dev/null bs=1024 count=1
  iflag=fullblock
```

Ohne das Paket „rng-tools" kommt das Kommando, das im Speicher eine zufällige Zahlenreihe von 1 KB Länge erzeugt, kaum zum Ende und muss mit Strg-C abgebrochen werden. Mit dem zusätzlichen Hardware-Zahlengenerator läuft der Befehl in wenigen Sekunden durch. **-dw**

Softwaretools & Tipps

Eine echte Perle im Meer der Open-Source-Software ist das OCR-Tool Ocrmypdf, das PDFs um eine Textebene ergänzt. Um Perl geht es dagegen im Tool Gprename, das Dateien reihenweise umbenennt und dazu reguläre Ausdrücke von Perl bietet.

PDF erstellen: Textebene ergänzen

Eingescannte Dokumente sind in einem PDF erst mal nicht durchsuchbar, da diese als Bilddatei vorliegen. Zum Ausdruck sind PDFs dieser Art völlig in Ordnung, aber in einem Archiv sind PDF-Dateien wertvoller, in welchen der Textinhalt als zusätzliche Textebene gespeichert ist, denn dadurch werden die Dokumente durchsuchbar.

Ein cleveres Linux-Programm fügt diese Textebene per OCR nachträglich hinzu: Ocrmypdf ist Open Source und dank der Texterkennungsengine Tesseract-OCR auch sehr zuverlässig. Einsteiger aufgepasst: Es handelt sich um ein Kommandozeilenprogramm. Allerdings ist die Bedienung nicht sonderlich kompliziert. In Debian, Ubuntu und Linux Mint liegt das Programm in den Standard-Paketquellen und ist von dort mit dem Befehl

```
sudo apt-get install
  ocrmypdf
```

in einem Terminalfenster mit allen Abhängigkeiten flott installiert. Für Tesseract-OCR muss zur Erkennung von deutschsprachigem Text noch eine zusätzliche Sprachdatei mit Erkennungsmuster installiert werden:

Pixel zu Buchstaben: Ocrmypdf nimmt sich PDFs mit eingescannten Bildern vor, lässt eine Texterkennung (Tesseract-OCR) darüberlaufen und ergänzt das PDF um eine Textebene.

```
sudo apt-get install
  tesseract-ocr-deu
```

Die Anwendung des Programms auf ein PDF ist dann nicht weiter kompliziert: Mit

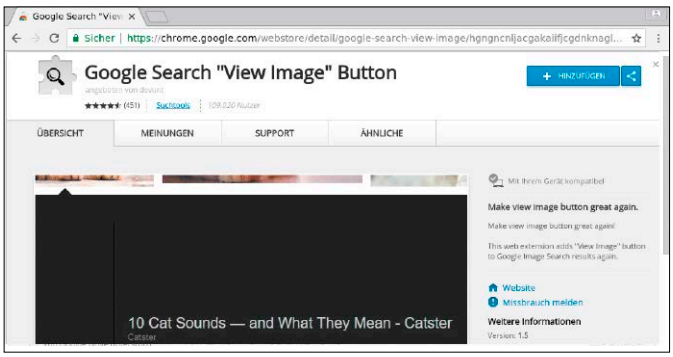
```
ocrmypdf -l deu beispiel.
  pdf txt_beispiel.pdf
```

ergänzt man ein PDF um eine zusätzliche Textebene. Der Schalter „-l deu“ gibt an, dass es sich um einen deutschsprachigen Text handelt. Bei einem englischen Text wäre Schalter „-l eng“ der richtige. **-dw**

Google Suche: Bilder wieder anzeigen

Die Bildersuche der Suchmaschine Google ist nahezu unschlagbar, hat aber eine nützliche Funktion eingebüßt. In den Suchergebnissen gibt es den Link „Bild anzeigen“ unter einem gefundenen Bild nicht mehr.

Firefox-Anwender können den Verlust der Funktion sicherlich verschmerzen, denn mit einem Rechtsklick auf ein Bild kann dieser Browser mit dem Punkt „Grafik anzeigen“ das Bild weiterhin isoliert zeigen. In Chrome/Chromium gibt es den Menüpunkt aber nicht. Aber hier kann eine Browsererweiterung aushelfen: Über „Weitere Tools → Erweiterungen“ finden Sie im Chrome Web Store das Tool Google Search View Image Button (*https://tinyurl.com/ybflcp9q*), das den fehlenden Link „View Image“ in den Google-Suchergebnissen nachrüstet.



Abkürzung zu Bildern: Eine Erweiterung für Chrome/Chromium ergänzt in diesen Browsern die Bildersuche von Google um einen direkten Link zur angezeigten Grafik.

Google Search View Image Button 1.5: Erweiterung für Chrome/Chromium, die in Suchergebnissen die Bilderanzeige wieder verfügbar macht. Installation über *https://tinyurl.com/ybflcp9q*. **-dw**

Gimp 2.10: Speichern statt Exportieren

Mit Gimp 2.10 gab es das wichtigste Update des Open-Source-Grafikprogramms seit den letzten sechs Jahren (siehe Beitrag im Heft ab Seite 72). Den Umgang mit Dateiformaten beim Speichern von Grafiken dürften viele Anwender verbesserungswürdig finden: Gimp 2.10 bevorzugt weiterhin das eigene Dateiformat XCF und bietet im gewohnten Speichern-Dialog kein anderes Format mehr an. Wer eine Grafik als JPG oder PNG sichern will, muss den Menüpunkt „Datei → Exportieren" (Strg-E) verwenden.

Zwar unterstützt das Gimp-Format XCF erweiterte Bildeigenschaften wie Ebenen, aber ein verbreitetes Format ist es nicht. Wer häufiger mit PNGs und JPGs zu tun hat, kann die Speicherfunktion soweit modifizieren, dass Gimp auch wieder fremde Formate sichert. Diese Modifikation bringt das Plug-in Save/Export Clean in Form eines neuen Menüpunkts.

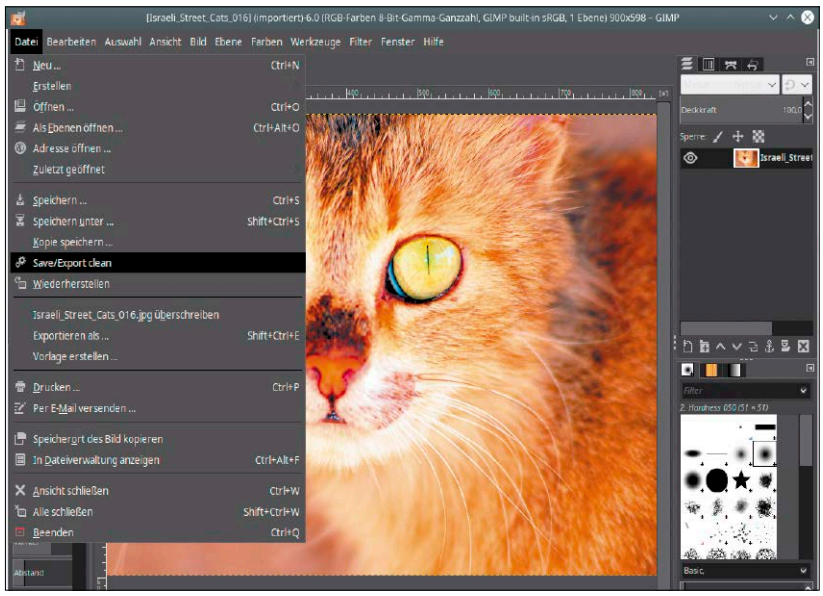
Zur Installation des Plug-ins geht man auf die Github-Seite des Entwicklers unter *https://raw.githubusercontent.com/akkana/gimp-plugins/master/save-export-clean.py* und speichert diese Datei lokal als „save-export-clean.py" ab. Anschließend macht man diese Datei ausführbar, was per Rechtsklick im verwendeten Dateimanager gelingt oder auch auf der Kommandozeile:

```
chmod +x save-export-
  clean.py
```

Anschließend verschiebt man das Script mit einem Dateimanager oder auch in der Shell in den neuen Plug-in-Ordner von Gimp 2.10, der unter „~/.config/GIMP/2.10/plug-ins" im Home-Verzeichnis liegt:

```
mv save-export-clean.py
  ~/.config/GIMP/2.10/
  plug-ins/
```

Exportunternehmen: Ein Plug-in für Gimp 2.10 rüstet den Menüpunkt „Save/Export clean" nach, der geöffnete Bilddateien ohne Umwege in Fremdformaten wie JPG und PNG speichert.



Nach einem Neustart von Gimp zeigt sich der neue Eintrag „Save/Export clean" im Menü „Datei", der Dateien ohne weitere Rückfragen im Originalformat speichert. Gimp fragt auch beim Schließen des Programms nicht mehr nach, ob Sie die geöffnete Dateien nochmal extra im XCF-Format sichern möchten, was bei exportierten Dateien sonst immer der Fall ist.

Damit das Plug-in jetzt auch noch auf die gewohnte Tastenkombination Strg-S reagiert, weisen Sie dem neuen Menüpunkt ein Tastenkürzel zu. Dazu dient in Gimp das Menü „Bearbeiten → Tastenkombination". Dort gibt man im Suchfeld mit „Save/E" die ersten Buchstaben des Plug-ins ein, wählen es in der Liste aus und klicken dann auf den Eintrag „Deaktiviert", um eine neue Tastenkombination zu definieren. Beachten Sie aber, dass die Funktion bereits vorhandene Dateien ohne Rückfrage überschreibt.

Save/Export Clean: Gimp-Plug-in mit alternativer Speicherfunktion, Download unter *http://shallowsky.com/software/gimp-save (2,5 KB, GPL)*. **-dw**

Webseiten: Einfügen immer erlauben

Es gehört zu den lästigeren Widrigkeiten im Web, wenn eine Webseite das gewohnte Copy & Paste im Browser unterbindet. Dieses Verhalten ist auf Seiten des Webseiten-Betreibers mit Javascript mit recht geringem Aufwand zu erreichen und viele Seiten wenden diese Einschränkung auf Passwort-Eingabefelder an – sehr zum Leidwesen vieler Anwender, die einen Passwortsafe wie Keepass XC verwenden.

Grundsätzlich alles, was Webseiten-Betreiber per Javascript auf der jeweiligen Seite anstellen, lässt sich im Browser auch wieder rückgängig machen oder unterbinden. Für Firefox, Chrome und Chromium gibt es schnell installierte Erweiterungen, die Copy & Paste auf ausgewählten Webseiten wieder erlauben.

Chrome/Chromium: Die Erweiterung „Don't Fuck With Paste" findet sich zur Installation im Chrome-Erweiterungsverzeichnis unter *https://tinyurl.com/qxz76lg*.

Firefox: Analog dazu liegt das Add-on für den Firefox-Browser im offiziellen Verzeichnis unter *https://addons.mozilla.org/en-US/firefox/addon/don-t-fuck-with-paste*.

In beiden Fällen legt die Erweiterungen in der Symbolleiste des jeweiligen Browsers ein neues Icon an. Ein Klick darauf öffnet einen Dialog, mit dem Sie die aktuelle Webseite in die Liste der erlaubten Webseiten aufnehmen. Das genügt: Danach ist das Einfügen aus der Zwischenablage möglich. Als Demo und zum Test der Erweiterung eignet sich die Seite *https://jsfiddle.net/aaronraimist/6qrnwcjp/28/show* mit ihrem Eingabefeld.

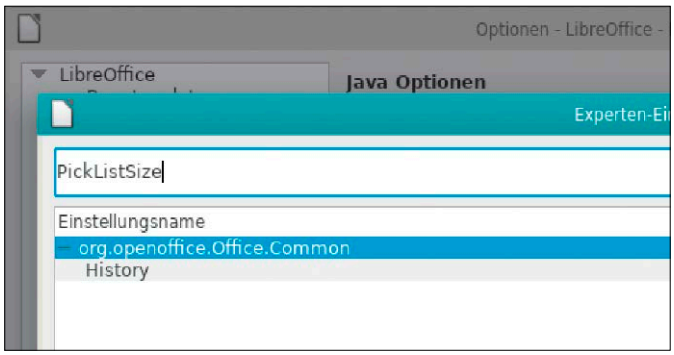
Don't Fuck With Paste: Browsererweiterung für Firefox (*https://addons.mozilla.org/en-US/firefox/addon/don-t-fuck-with-paste*) und Chrome/Chromium (*https://tinyurl.com/qxz76lg*), die auf Webseiten Copy & Paste wiederherstellt. **-dw**

Libre Office: Zuletzt verwendete Dokumente

Die Programme von Libre Office klappen im Dateimenü eine Liste der zuletzt benutzten Dokumente aus. Diese Liste haben die letzten Ausgaben von Libre Office von zehn Einträgen auf immerhin 25 erhöht. In Libre Office 6.x kann man nun die Anzahl der Einträge der Liste individuell erhöhen oder reduzieren.

Früher war es notwendig, zur Anpassung der Anzahl zuletzt verwendeter Dokumente die Erweiterung „HistoryMaster-1.1.1.oxt“ von *http://extensions.services.openoffice.org* zu installieren. Das ist jetzt keine Voraussetzung mehr, denn Libre Office hat seit den letzten Ausgaben einen Editor für seine internen Einstellungen erhalten. Dieser Editor ist unter „Extras → Optionen → LibreOffice → Erweitert“ über die Schaltfläche „Experteneinstellungen“ aufrufbar.

In der angezeigten, sehr umfangreichen Liste aller Einstellungen suchen Sie an im Feld oben nach dem Eintrag „PickListSize“. Nach einem Doppelklick auf den angezeigten Eintrag „History“ nimmt der Dialog die neue gewünschte Größe für die Dateiliste an. **-dw**



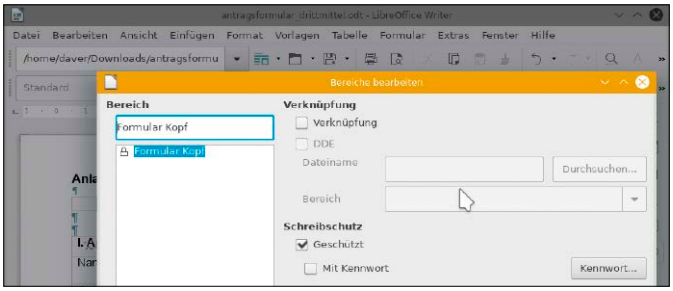
Große oder kleine Dateiliste: Den Umfang der Liste „Datei → Zuletzt verwendete Dokumente“ kann man in Libre Office nun in den Experteneinstellungen ändern.

Libre Office Writer: Bereiche schützen

In einem Dokument, das als Vorlage oder als Formular zum Ausfüllen weitergegeben wird, sollen nur bestimmte Bereiche editierbar sein. Andere definierte Abschnitte dürfen dagegen nicht geändert werden und Anwender sollen gar nicht erst in die Versuchung kommen, dort zusätzlichen Text zu schreiben.

Um Textbereiche in Libre Office Writer vor Änderungen zu schützen, markieren Sie den gewünschten Abschnitt und gehen in der Menüzeile auf „Einfügen, Bereich“.

Im angezeigten Dialogfenster kommt in das Feld „Neuer Bereich“ ein beliebiger, aussagekräftiger Name für den gerade markierten Bereich. Rechts aktivieren Sie mit der Klickbox „Schützen“ den Schutz vor Änderungen. Sollte jetzt jemand versuchen, in diesen Bereich zu schreiben, verweigert dies eine entsprechende Meldung. Natürlich kann ein Anwender den Schutz nach einem Rechtsklick auf den Bereich einfach über „Bereich bearbeiten“ wieder aufheben. Wollen Sie auch das verhindern, so markieren Sie zusätzlich die Checkbox vor „Kennwort“ und geben ein Passwort ein. Dieser Bereichsschutz bleibt auch bei dem Export in die Word-Formate DOC und DOCX erhalten. **-dw**



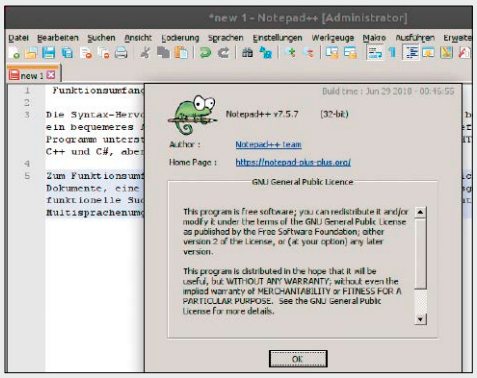
Hier bitte nicht schreiben: Werden Libre-Office-Dokumente als Vorlagen oder Formulare weitergegeben, so lassen sich dort Bereiche vor Änderungen schützen.

SNAP: NOTEPAD++ FÜR UBUNTU

An Texteditoren für jeden Zweck gibt es unter Linux keinen Mangel. Deshalb mutet es zunächst als Kuriosum an, dass die Ubuntu-Nutzergemeinde das Windows-Programm Notepad++ als Snap-Paket abgepackt hat. Interessant ist das einfach installierte Programm aber für Anwender, die von Windows zu Linux kommen und auf beiden Systemen denselben Editor nutzen möchten. Notepad++ ist Open Source und gehört zu den populärsten freien Programmen unter Windows. Das Snap-Paket für Ubuntu 16.04/18.04 liefert seine eigene Wine-Umgebung mit, um den Editor unter diesem Windows-Nachbau auszuführen. Die Installationsgröße beträgt deshalb rund 80 MB. Wer Notepad++ in Ubuntu ausprobieren möchte, öffnet einfach ein Terminalfenster und gibt dort

```
sudo snap install notepad-plus-plus
```

ein. Ohne weitere Konfiguration findet sich das Programm über die Aktivitätenübersicht in Gnome. In den Ubuntu-Desktop integriert sich das Windows-Programm erstaunlich gut. Unter „Settings → Preferences → General → Localisation“ steht sogar die deutsche Sprachdatei zur Verfügung. **-dw**

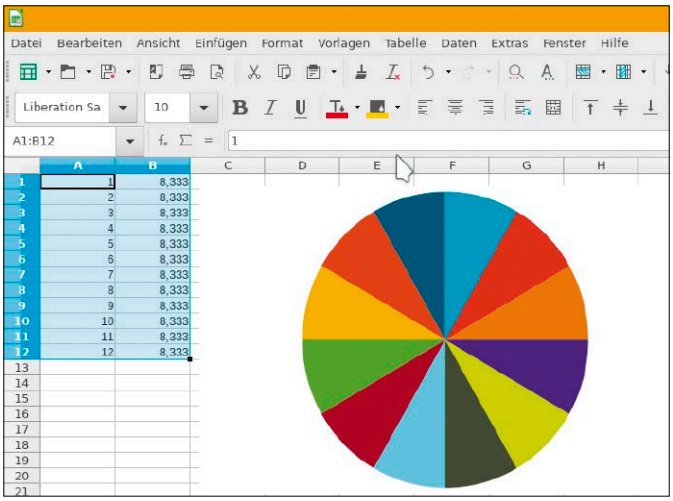


Bekanntes Gesicht: Das Windows-Programm Notepad++ ist jetzt unter Ubuntu als leicht zu installierendes Snap-Paket verfügbar – komplett mit eigener Wine-Umgebung.

Libre Office Calc: Kreisdiagramme korrigieren

In Libre Office gehen die Uhren manchmal anders. Wenn man in der Tabellenkalkulation Calc ein Kreisdiagramm über den Menüpunkt „Einfügen → Diagramm → Kreisdiagramm“ aus einem markierten Zellbereich erstellt, dann ordnet Calc die einzelnen Kreissegmente zunächst im umgekehrten Uhrzeigersinn an. Das Kreissegment für den ersten Wert erscheint also links neben der 12-Uhr-Position, links davon das zweite Segment.

Generell sind aber Kreisdiagramme mit Segmenten im Uhrzeigersinn üblich. Während der Erstellung des Diagramms kann man die gewünschte Richtung nicht angeben und viele Anwender suchen hier vergeblich nach der passenden Option. Nachträglich ist das aber sehr wohl möglich. Dazu klickt man die gesamte Diagrammfläche in Calc doppelt an und dann nochmal mit der linken Maustaste genau in das Kreisdiagramm. Nun sind die einzelnen Kreissegmente markiert. Ein Rechtsklick darauf bringt jetzt die Option „Datenreihe formatieren“ zum Vorschein. Dort markieren Sie unter „Ausrichtung“ die Option „Im Uhrzeigersinn“ und bestätigen dies mit „OK“. **-dw**



Libre Office Calc zieht seine Kreise: Die Tabellenkalkulation legt Kreisdiagramme mit den markierten Werten gegen den Uhrzeigersinn an. Ein Punkt im Kontextmenü kann die korrekte Anordnung herstellen.

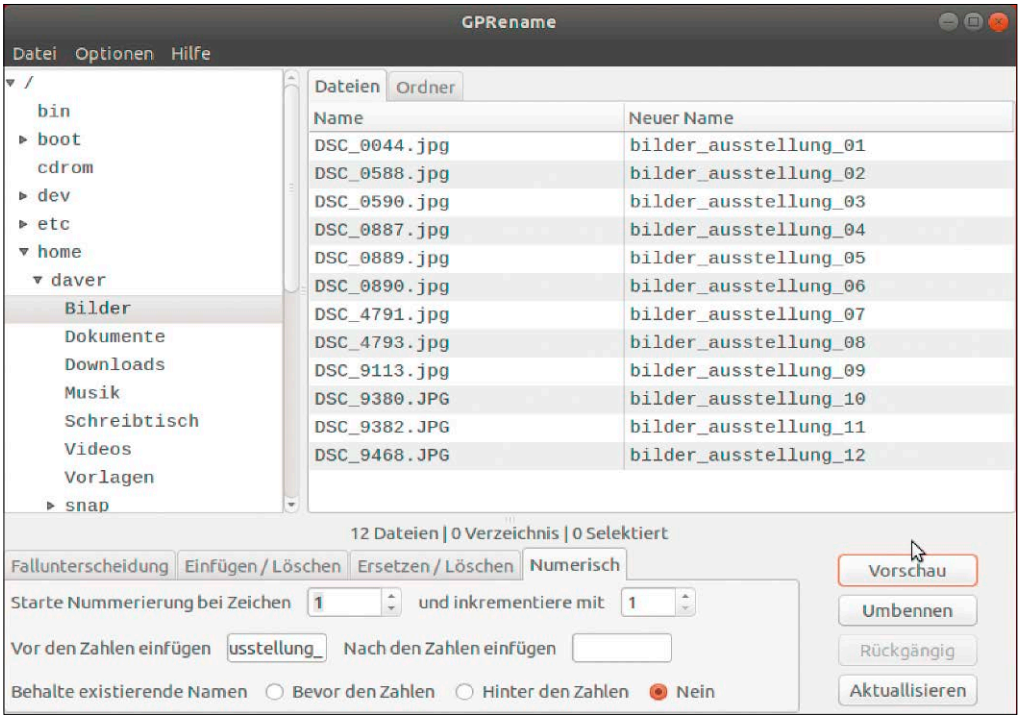
Gprename: Dateien reihenweise umbenennen

In Dateiarchiven aller Art dient es der besseren Organisation, Dateien einen aussagekräftigen oder nummerierten Namen zu geben. Die Desktopumgebung KDE verfügt mit dem Tool Krename über ein funktionsreiches Programm zum Umbenennen nach Mustern. In anderen Desktopumgebungen wie Gnome ist das Angebot nicht so üppig.

Gprename ist ein bewährtes grafisches Programm, das sich unter Gnome, Cinnamon und Mate und anderen GTK-basierten Desktops zum Umbenennen beliebig vieler Dateien nach definierbaren Mustern eignet. Das deutschsprachige Programm ist in den Standard-Paketquellen der populären Linux-Distributionen vertreten und in Debian, Ubuntu und Linux Mint beispielsweise mit dem Kommando

```
sudo apt-get install
  gprename
```

schnell eingerichtet. Nach dem Start zeigt Gprename in der Spalte links einen Ordnerbrowser und rechts davon die Dateiliste. Die Funktionen zum Umbenennen befinden sich in der Fußzeile. Neben ganz einfachen Schaltern wie „Alles klein“ gibt es unter „Ersetzen/Löschen“ eine Ersetzungsfunktion, die sogar reguläre Ausdrücke versteht. Diese folgen der gebräuchlichen Perl-Notation, die in vielen Programmen Standard ist und unter *http://www.mathe2.uni-bayreuth.de/perl/GK/regExp.htm* mit vielen Beispielen erklärt ist. **-dw**



Dateinamen ändern: Das Perl-Programm Gprename für Gnome, Cinnamon und Co. liefert häufig benötigte Rename-Aktionen per Mausklick sowie reguläre Ausdrücke für Fortgeschrittene.

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.

Ubuntu-Auslagerungsdatei anlegen

Ubuntu 18.04 genügt zwar eine Auslagerungsdatei, aber beim Upgrade der Ubuntu-Version 16.04 auf 18.04 übernahm das neue System die vorgefundene Auslagerungspartition des älteren Ubuntu. Ich würde meine Partitionierung gerne vereinfachen und die Swappartition durch eine Swapdatei ersetzen. Ist das nachträglich möglich?

Lion F., per Mail

Das geht und ist auch nicht allzu aufwendig. Zunächst legen Sie eine Datei gewünschter Größe (hier vier GB) für die neue Auslagerung an:

```
sudo fallocate -l 4G /mnt/swap.swap
```

Ordner und Name sind frei wählbar, sollten dann aber nicht mehr geändert werden. Die erstellte Datei müssen Sie dann als Swapspeicher formatieren:

```
sudo mkswap /mnt/swap.swap
```

Temporär für die aktuelle Sitzung können Sie die neue Swapdatei nun bereits mit

```
sudo swapon /mnt/swap.swap
```

nutzen. Für permanente Nutzung ist aber ein Eintrag in der Datei „/etc/fstab" notwendig. Öffnen Sie diese mit sudo-Recht in einen Editor und tragen Sie dort die Zeile

```
/mnt/swap.swap none swap sw 0 0
```

ein. Danach entfernen Sie die Zeile mit dem bisherigen Swapspeicher.

Starten Sie dann das System neu und prüfen Sie mit dem Befehl *swapon*, ob die Umstellung gelungen ist. Der Befehl sollte die neue Swapdatei melden, die frühere Swappartition hingegen nicht mehr. Ist dies der Fall, können Sie die nicht mehr benötigte Partition normal formatieren oder auch löschen und den Platz mit Gparted der Systempartition zuschlagen.

Hinweis 1: Aus Sicherheitsgründen werden die Befehle mkswap und swapon „Unsichere Zugriffsrechte" monieren. Ändern Sie die Dateirechte mit

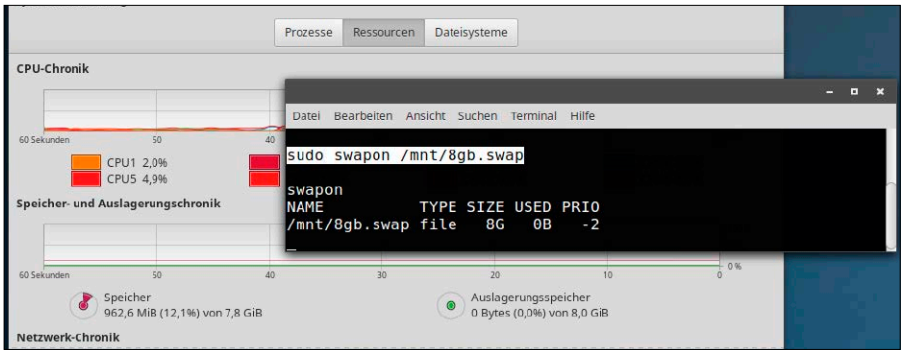
```
Sudo chmod 600 /mnt/swap.swap
```

dahingehend, dass zum Lesen der Swapdatei root-Recht erforderlich ist.

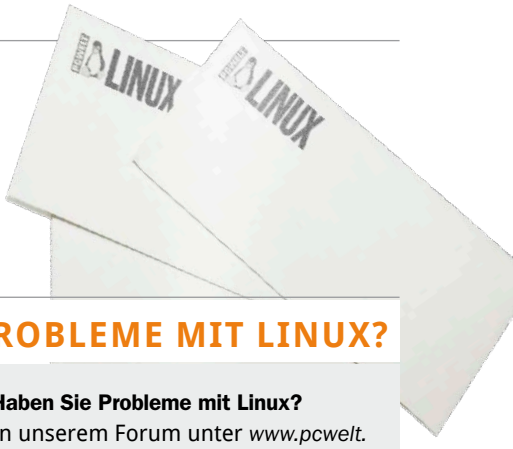
Hinweis 2: Die Größe der Swapdatei können Sie mit den genannten Schritten bei Bedarf neu definieren, je nachdem, was die Systemüberwachung zum Swapverhalten meldet. Dazu müssen Sie die Auslagerung nur vorbereitend mit

```
sudo swapoff -a
```

komplett abschalten.



Hantieren mit der Swapdatei: Diese ist unter Ubuntu/Mint leicht manuell zu erstellen, zu aktivieren oder auch abzuschalten.



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: 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

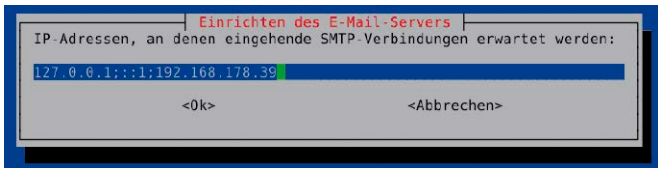
Sie können Ihr Abonnement jederzeit zur nächsten Ausgabe kündigen.
Bestellungen können innerhalb von 14 Tagen ohne Angabe von Gründen in Textform (zum Beispiel Brief, Fax, E-Mail) oder durch Rücksendung der Ware widerrufen werden.

LinuxWelt 6/2018 erscheint am 28.9.2018

Aus Aktualitätsgründen können sich Themen ändern.

Datenschutz für Ihre Mails

Heimischer Mailserver und Mailverschlüsselung: Egal ob IMAP oder POP – die Nachrichten liegen auf dem Server des Mailanbieters, bis Sie sie dort löschen. Und solange sie dort liegen, kann sie der Admin des Anbieters, schlimmstenfalls aber auch der Geheimdienst oder der Hacker lesen. Dagegen helfen drei Methoden: konsequentes Herunterladen und Löschen vom Server, Verschlüsselung der Nachrichten oder ein eigener Mailserver. Die kommende LinuxWelt erklärt alle drei Methoden ausführlich und praxisnah, sodass Sie diese direkt

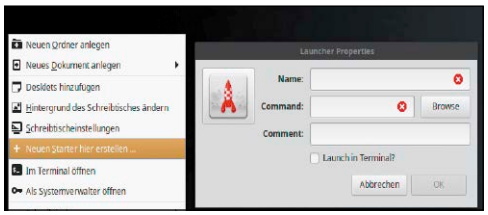


umsetzen können. Der anspruchsvollste Ansatz des eigenen Mailservers kombiniert diesen mit einem normalen externen Mailkonto, da viele Empfänger die Nachrichten von IP-Adressen privater Internetanschlüsse als Spam einstufen würden.

Alle Systeminfos im Griff

Eckdaten von Hardware und System abfragen: Im Betriebsalltag besteht immer wieder aktueller oder grundsätzlicher Infobedarf – bei Hardware wie CPU und Speicher, bei Datenträgern samt Belegung, Dateisystem und Mountpunkt, bei Systemdetails wie Kernel-, Distributions- und Desktopversion sowie bei den Netzwerkdaten der lokalen wie öffentlichen IP oder der MAC-Adresse. Auf grafische Infotools ist unter den zahlreichen Linux-Distributionen nur bedingt Verlass. Auf dem einen System liegen sie vor, auf dem nächsten nicht und bei der typischen Netzwerkadministration von Servern ist man sowieso auf Terminalwerkzeuge angewiesen. Da liegt es nahe, sich die nötigen Befehle in einer Script-Sammlung zurechtzulegen, die dann auf jedem Linux funktioniert.

Hardlinks, Softlinks und Starter



Technik und Einsatzmöglichkeiten von verlinkten Dateiobjekten: Eine wichtige Datei oder einen Ordner an mehreren Orten klickbereit zu haben, ist eine gängige Komfortpraxis unter allen Betriebssystemen. Typischer Einsatzzweck sind Starter für ausführbare Dateien. Hardlinks wiederum werden häufig unter der Haube als Stellvertreter genutzt, um den Plattenplatz inkrementeller Sicherungen signifikant zu verringern. Nicht zuletzt ist auch der geschickt gewählte Mountpunkt ein logischer Link zur gewünschten Ordnerhierarchie. Der Beitrag erklärt den Einsatz aller Verlinkungstechniken und die wichtigsten Motive für ihre Verwendung.

Das Surfsystem der LinuxWelt

Die LinuxWelt-DVD erweitert ihr Serviceangebot: Neben aktuellen und wechselnden Linux-Distributionen liefert die Heft-DVD stets einige Standardtools mit – so etwa die Super Grub Disk für den Notstart. Diese Standards erweitern wir ab Ausgabe 6/2018 durch ein schlankes Surfsystem, das Sie jederzeit schnell und sicher ins Internet bringt.
Als Basisdistribution dient das kompakte Porteus 4.0, das künftig in einer LinuxWelt-Edition mit Mate-Desktop und stets aktuellem Browser von der DVD bootet. Der neue DVD-Service wird im Heft durch einen Steckbrief zur Distribution Porteus und eine kurze Praxiseinführung begleitet.

PC WELT

350 Tipps & Tricks

Sonderheft
für nur
12,90 €

PLUS:
XXL-Toolkit 2018
auf DVD!

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

1. Formular ausfüllen **2. Foto machen** **3. Foto an shop@pcwelt.de**

Ja, ich bestelle das PC-WELT Sonderheft 350 Tipps & Tricks 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

InfinityBook Pro

32 GB
DDR4

Intel Core i7
Quad-Core

14h Akku
Maximale Laufzeit

IASANITYBOOK

32 GB
DDR4

Intel Core i7
Six-Core

GTX1070 Max-Q
NVIDIA GeForce

100%
Linux

5
Jahre
Garantie

Lifetime
Support

Gefertigt in
Deutschland

Deutscher
Datenschutz

Support
vor Ort

TUXEDO COMPUTERS

tuxedocomputers.com