Multiboot-DVD mit 6 Top-Systemen

1/2020
Dezember/Januar

4 196691 608505 01

Deutschland 8,50 €
Schweiz 16,90 sfr · Österreich + Benelux 9,45 €

LINUX WELT

18 SEITEN SPECIAL

Anti-Hacker-Paket *So kommt niemand an Ihre Daten*

Die besten Linux-Tools 2020

Diese Programme dürfen auf keinem PC fehlen!

Das große Komplett-Paket für
· System · Netzwerk · Office
· Dateien · Virtualisierung
· Desktop · Tuning · Server
· Raspberry Pi

Exklusiv!
LinuxWelt-Toolbox auf DVD

Die besten Terminal-Tricks

WLAN konfigurieren · Netzwerk überwachen · Daten kopieren

Raspberry Pi 4

Desktop-Ersatz · Heimserver · Streaming-Server und Dokumenten-Scanner

NEU! Ubuntu 19.10

Schneller Start, neue Funktionen, frische Software
Auf DVD: 3 x Ubuntu als Live-Systeme zum Ausprobieren

NEU!

Einsteiger-Tipps

Festplattenpflege: Schnellerer Zugriff, längere Lebensdauer

Linux Mega-Paket

· 8600 Seiten Linux-Know-how
· 6 Top-Systeme als Multiboot-DVD
· Exklusive LinuxWelt-Toolbox

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme


MACH, WAS WIRKLICH ZÄHLT.
#IT
FOLGE DEINER BERUFUNG.
bundeswehr
karriere.de
BUNDESWEHR

Neues von Snap

Canonical hat mal wieder zugeschlagen. In den neuen Ubuntu-Versionen 19.1 0 und 18.04.3 LTS gibt es den Browser Chromium nicht mehr als DEB-Paket, sondern nur noch als Snap-App. Diese Entscheidung ist umstritten, denn das Paketvertriebsmodell Snap wurden in den vergangenen Jahren oft kritisiert: Es verschwende Speicherplatz, umgehe die Kontrollen der Distributionen und habe ein schwieriges Sicherheitskonzept. Zudem steht der zentrale App-Store allein unter der Kontrolle von Canonical.

Besonders genervt reagierte Linux-Mint-Chefentwickler Clement Lefebvre. Denn Mint unterstützt Snap (noch) nicht. Da aber das für Dezember 2019 erwartete Mint 19.3 auf Ubuntu 18.04.3 aufsetzt, muss er entweder Snap übernehmen oder Chromium-Updates selbst in Mint einpflegen oder Canonical zum Umdenken bewegen …

Snap hat aber auch viele Vorteile: Snaps müssen für alle Plattformen nur einmal erstellt werden. Der Snap-Store liefert sie dann automatisch im Hintergrund aus. Das ist besonders bei Browsern wie Chromium mit ihren häufigen, sicherheitsrelevanten Updates wichtig.

Spannend ist jetzt, ob sich das Snap-Modell auch in anderen Distributionen stärker verbreiten wird. Weitere Informationen zu Ubuntu 19.10 und Snap finden Sie ab Seite 14 sowie im Ubuntu-Blog unter *www.pcwelt.de/CSgBZK*.

Herzlichst, Ihr

Arne Arnold
Redakteur
aarnold@it-media.de

Sicherheit und Verschlüsselung

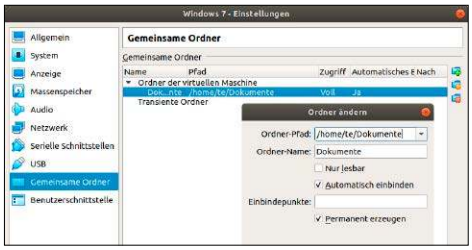
Bewährte und neue Methoden für Systemsicherheit und Datenschutz: Das Heftspecial startet mit Hardwarelösungen für sichere und bequeme Zwei-Wege-Authentifizierung.

S. 46

Die Toolbox

Softwarecenter der Redaktion: Die Toolbox bietet Empfehlungen, Praxisanleitungen und einfache Installation.

S. 28



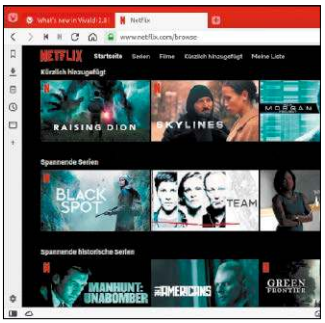
Win 7 virtuell

Nach dem Aus: So konvertieren Sie Windows 7 in ein virtuelles System.

S. 20

Grundlagen

Special I – Toolbox für Linux



Special II – Sicherheit & Verschlüsselung

Die Highlights der DVD

Auf Heft-DVD: Dreimal Ubuntu und drei Spezialdesktops

Die Heft-DVD berücksichtigt die neue Ubuntu-Version 19.10 mit drei Ausgaben: die Gnome-Hauptedition, ferner die genügsamen, aber ansprechenden Varianten mit XFCE (Xubuntu) und LXQT (Lubuntu). Ein echter Oldie-Spezialist ist Sparky Linux auf Debian-Basis. Endeavour und Slax sind unten knapp charakterisiert.

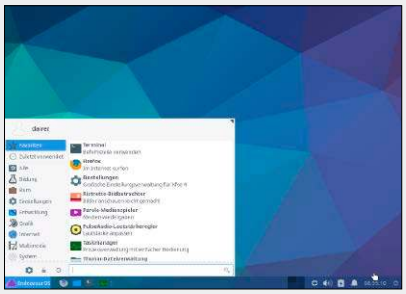
S. 10

Lubuntu 19.10

Das kleinste Ubuntu vollzog vor einem Jahr den Umstieg vom altbackenen LXDE-Desktop auf LXQT. Seitdem darf Lubuntu den Platz eines vollwertigen Desktopsystems beanspruchen.

Endeavour-OS 2019.10

Endeavour ist der Nachfolger von Antergos mit demselben Anliegen: Das schnelle, aber anstrengende Arch Linux soll mit Calamares-Installer und Desktop einsteigerfreundlich werden.



Slax 9.11

Slax ist kein installierbares Desktopsystem, sondern ein minimales Livesystem zum Surfen. Außer Browser, Terminal und VLC ist praktisch keine Software installiert.

Software

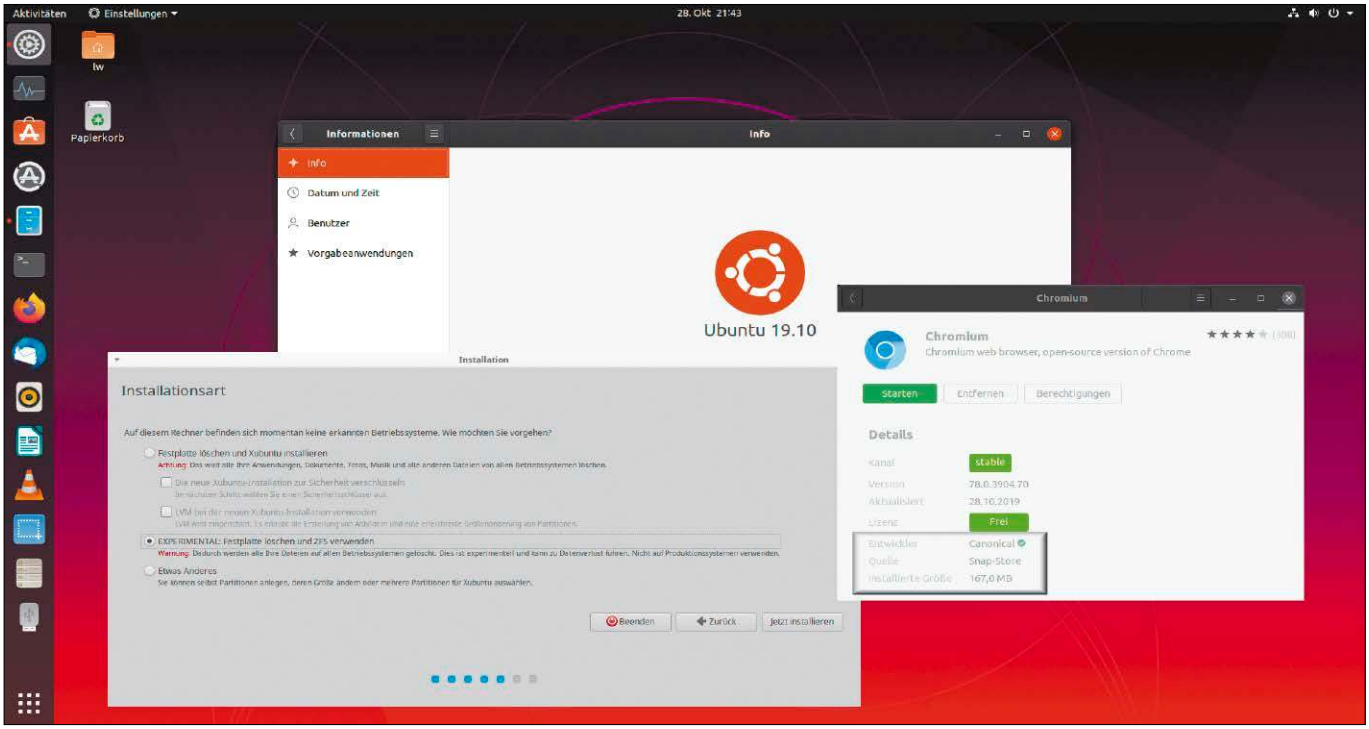
Server & Raspberry Pi

Standards

Praxis

Freundliches Ubuntu?

Ubuntu 19.10 sendet widersprüchliche Signale: Natürlich ist es ein Stück komfortabler, wenn der Nvidia-Grafiktreiber ab Installation läuft. Ob und wie man einem Desktopnutzer andererseits das ZFS-Dateisystem anbieten kann, steht auf einem anderen Blatt.



VON HERMANN APFELBÖCK

Ist Ubuntu noch benutzerfreundlich? Die letzten 15 Jahre haben Ubuntu und seine Derivate den Linux-Desktop durch diese Eigenschaft bestimmt. Die aktuelle Zwischenversion 19.10 ist kein eindeutiges Bekenntnis zum endbenutzerfreundlichen Desktopsystem. Der Anwender wird zwar die Kooperation mit Nvidia und manchen Gnome-Feinschliff von Canonical positiv verbuchen, aber die wichtigsten Änderungen in Ubuntu 19.10 sind strategisch und ökonomisch motiviert:

Den Chromium-Browser bietet das jüngste Ubuntu nur noch als Snap-Container. Das ist natürlich begründbar, weil dann statt mehreren DEB-Paketen für mehrere gültige Ubuntu-Versionen nur noch ein Snap-Paket gepflegt und aktualisiert werden muss. Für Ubuntu-Derivate wie Linux Mint heißt das dann aber, dass man sich notgedrungen auf die Snap-Laufzeitumgebung und auf den Snap Store einlassen muss – was bekanntermaßen beides von Ubuntu/Canonical stammt. Mint-Chef Lefèvbre hatte solche Abhängigkeit noch im Sommer 2019 strikt abgelehnt. Für den Anwender bringt die wunderbare Snap-Vermehrung zwar manch aktuellere Software, aber auch vergleichsweise gigantischen Plattenverbrauch im Vergleich zu schlanken DEB-Paketen.

Das ZFS-Dateisystem hat auf einem Desktoprechner oder Notebook eigentlich nichts verloren. Oracles ZFS ist zweifellos zukunftsweisend, gehört aber in den Serverschrank. Trotzdem wäre nichts einzuwenden gegen die jetzt eingeführte Installationsoption mit ZFS, wenn Ubuntu dies in irgendeiner Form anwendertauglich integriert hätte. Aktuell erfordert aber die Kontrolle und Konfiguration des Dateisystems, selbst das fundamentale Anlegen von Snapshots, den Einsatz sehr komplexer Kommandozeilentools. Ubuntu serviert damit dem normalen Desktopnutzer ein Angebot, das vermutlich auch professionelle Admins ins Schwitzen bringt. Anwenderfreundlich ist das nicht, sondern ein strategisches Statement für ein Serverdateisystem, dessen Einbau in den Linux-Kernel obendrein lizenzrechtlich umstritten ist. Es ist zu betonen: Anders als bei Open Suse, das sich vor Jahren für das ähnlich serveraffine Dateisystem BTRFS als Standard entschied, ist ZFS in Ubuntu noch eine freie Option: Sie dürfen – und sollten – in aller Regel ablehnen. Näheres zu Ubuntu 19.10 und ZFS lesen Sie ab Seite 14.

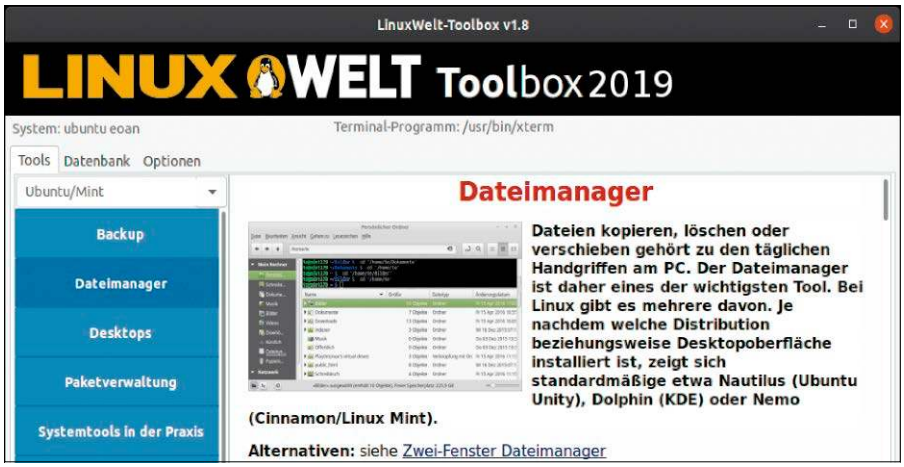
Themenschwerpunkte und fokussierte Ratgeber

Umfangtechnisch spielt das neue Ubuntu 19.10 als Zwischenversion nur eine kleine Rolle im Heft. Die beiden Schwerpunkte mit je sieben Einzelbeiträgen befassen sich mit der wichtigsten Software für den Linux-Desktop und für Linux-Server (ab Seite 28) und mit dem Thema Sicherheit inklusive Datenschutz und Verschlüsselung (ab Seite 46). Hier geht es unter anderem um neue Methoden der Zwei-Faktor-Authentifizierung und Strategien mit Luks und Veracrypt. Der eleganteste Weg, das auslaufende Windows 7 weiterzunutzen, ist die Umwandlung in ein virtuelles System. Der Ratgeber zu diesem Thema (Seite 20) leistet aktuelle Lebenshilfe, während der Praxisbeitrag zur Datenträgerpflege (Seite 90) systematische Grundlagen bietet. Und unter „Server & Raspberry Pi“ gehen wir auch der Frage nach, ob der neue Pi 4 desktoptauglich ist.

Multifunktionale Heft-DVD

Die Heft-DVD liefert aktuelle Livesysteme zum Ausprobieren und zur Installation. Sechsmal Linux können wir auf der 8,5-GB-DVD anbieten, obwohl die Livesysteme immer opulenter ausfallen. Im Zentrum steht das neue Ubuntu 19.10 mit drei Varianten. Ebenfalls installierbare Desktopsysteme sind Endevour-OS und Sparky Linux, während sich das minimale Slax als schnelles Live-Surfsystem eignet. Die Heft-DVD kann aber weit mehr, als diese Linuxsysteme zu booten: Die aktualisierte „LinuxWelt Toolbox“ ist das Softwarecenter der Redaktion, der „Distro-Wahl-O-Mat“ hilft bei der Auswahl der geeigneten Linux-Distribution und mit den Imagetools für Linux und Windows verarbeiten Sie die ISO- und IMG-Downloads. Hinzu kommen reichlich Handbücher im PDF-Format – neben dem aktualisierten LinuxWelt Digital XXL alle sechs LinuxWelt-Ausgaben 2019 sowie 33 Handbücher zu Administration und Sicherheit.

Die Benutzung der DVD ist einfach: Inhalte wie die PDF-Handbücher, den Wahl-O-Mat und die Softwaretools erreichen Sie unter jedem System nach Einlegen der DVD im Dateimanager. Um hingegen ein Livesystem zu starten, müssen Sie von DVD booten. Dazu rufen Sie beim Start per Tastendruck das Bios-Bootmenü auf und wählen das DVD-Laufwerk oder Sie ändern die Bootreihenfolge im Bios. Bei der Nutzung eines Livesystems bleiben Ihre Festplatte und das dort installierte System unberührt. Das ändert sich erst, falls Sie aus dem Livesystem den Installer starten. Die Heft-DVD bootet im Bios-Modus. Für das Ausprobieren der Livesysteme und für die Installation einer Distribution als alleiniges System spielt das keine Rolle. Wenn Sie aber ein System parallel neben einem bestehenden installieren möchten, das im Uefi-Modus läuft, müssen Sie dessen ISO-Abbild (auf DVD unter „Image-Dateien“) auf USB kopieren und dieses Medium im Uefi-Modus booten. ■



Das Softwarecenter der Redaktion: Die aktualisierte Toolbox 1.8 auf der Heft-DVD bietet Softwareempfehlungen, einfache Installation und grundlegende Anleitungen für die besten Linux-Programme.

AUF DVD

Distributionen

10 **Lubuntu 19.10** (64 Bit)
Ubuntu mit LXQT-Desktop

11 **Endevour-OS 2019.10** (64 Bit)
Arch Linux für Einsteiger

12 **Sparky Linux 5.9** (32 Bit)
Debian mit Calamares-Installer

13 **Slax 9.11** (32 Bit)
Mini-Surfsystem mit Chromium

14 **Ubuntu 19.10** (64 Bit)
Hauptedition mit Gnome

14 **Xubuntu 19.10 Core** (64 Bit)
Ubuntu mit XFCE (ohne Software)

Bootfähige Extras und Tools
Boothelfer & Analyse: Supergrub, Memtest, HDT, Plop-Bootmanager

LinuxWelt-Toolbox 1.8
LinuxWelt-Installer in neuer Version: Softwareauswahl, Empfehlungen, Infos und One-Click-Installation

LinuxWelt Digital XXL & vieles mehr
327 Seiten technische Grundlagenartikel plus Jahrgang 2019 der LinuxWelt 2019 (6 Ausgaben) plus 33 Handbücher (alle im PDF-Format)

6 x Linux
3 x Ubuntu 19.10

Ubuntu 19.10 (64 Bit)
Ubuntu 19.10 präsentiert ein blitzschnelles Gnome 3.34 auf dem Desktop, hat den Ubiquity-Installer um eine (noch) experimentelle Unterstützung für das Dateisystem ZFS ergänzt und liefert bereits auf den Installationsmedien die proprietären Nvidia-Treiber mit. Ubuntu 19.10 erhält neun Monate lang Unterstützung durch Updates und ist der letzte Schritt vor der nächsten Ubuntu-LTS-Version. Auch als ISO-Datei auf DVD.

Xubuntu Core 19.10 (64 Bit)
Hier arbeitet ein brandneues XFCE 4.14 als Desktop. Der Namenszusatz „Core" kennzeichnet ein zwar vollständiges Betriebssystem, das aber bei der Softwareausstattung stark reduziert bleibt. Xubuntu Core erwartet die Einrichtung der individuell gewünschten Software vom Benutzer. Auch als ISO-Datei auf DVD.

Lubuntu 19.10 (64 Bit)
Lubuntu gehört seit jeher zu den schlankeren offiziellen Ubuntu-Versionen, braucht sich aber nun optisch nicht mehr zu verstecken. Denn auf dem Desktop hat modernes LXQT in der letzten Version den alten LXDE-Desktop abgelöst. Dabei wirkt LXQT mit seinem Qt-Toolkit wie die kleine Schwester von KDE. Liegt auch als ISO-Datei auf DVD.

Endeavour-OS 2019.10.15 (64 Bit)
Vorhang auf für den Neuzugang Endeavour-OS, der die Arch-Linux-Variante „Antergos" ablöst: Endeavour-OS ist als Livesystem mit einem komfortablen grafischen Installer konzipiert. Als vorinstallierter Desktop dient der pragmatische XFCE 4.14. Liegt auch als ISO-Datei auf DVD.

Sparky Linux 5.9 (32 Bit)
Die emsig gepflegte Debian-Variante hat seine Paketquellen auf jene von Debian 10 „Buster" aktualisiert. Im laufenden Livesystem stehen zwei alternative Installer zur Auswahl. Der vorinstallierte Desktop ist ein sparsames Openbox, das auch noch auf richtig alten Rechnern gut läuft. Sparky liegt auch als ISO-Datei auf DVD.

Slax 9.11 (32 Bit)
Klein, schnell, aber sinnvoll erweitert: Slax ist eines der winzigsten Livesysteme und bringt in seiner originalen Ausgabe wenig mehr als den englischsprachigen Chromium-Browser mit. In dieser Version haben wir Slax für die LinuxWelt-DVD um Firefox und um deutsche Sprachpakete erweitert. Das Minisystem liegt auch als ISO-Datei auf DVD vor.

Extras & Tools

Super Grub Disk 2.0.4rc1
Das startfähige Tool Super Grub Disk 2 ist 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 Rechner-Bios 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 Prozessor, RAM, PCI-Geräte 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- und 64-Bit-CPUs und 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. Auf Flashspeichern wie SSDs und USB-Sticks ist das Tool wirkungslos.

Software auf DVD

Infrarecorder 0.53
Das Brennprogramm für ISO-Dateien hilft Windows-Nutzern, die mitgelieferten Imagedateien der Heft-DVD auf einen DVD-Rohling zu brennen. Der bewährte Infrarecorder 0.53 für alle Windows-Versionen liegt mit Installer und als portable Version vor.

Unetbootin 6.75
Das nützliche Tool mit grafischer Oberfläche transferiert mit wenigen Klicks die ISO-Images von Ubuntu und seinen Abkömmlingen wie Linux Mint sowie einigen 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 X.

Putty 0.76
Putty ist der klassische Terminalclient für SSH-Fernwartung (und Telnet) unter Windows. Putty liegt in Form einer portablen EXE-Datei vor, die ohne Installation unter allen Windows-Versionen läuft. Das Open-Source-Programm ist englischsprachig.

Kitty 0.72.0.6
Als Abspaltung von Putty ist Kitty ebenfalls ein Terminalclient für SSH, allerdings mit einigen ergänzten Funktionen und bequemen Features. Wie Putty wird es einfach über seine EXE-Datei gestartet.

Win 32 Disk Imager 1.0
Das kleine Windows-Programm überträgt ISO- und IMG-Dateien bootfähig auf externe Medien wie USB-Sticks und Speicherkarten. Das Programm liegt als ZIP-Archiv auf DVD, das nach dem Entpacken keine weitere Installation benötigt.

7-Zip 19.00
Das Open-Source-Programm 7-Zip für Windows ist eine leistungsfähige Alternative zu den Packern Winzip und Winrar. 7-Zip kommt nicht nur mit gängigen Formaten wie ZIP, CAB, RAR, ARJ zurecht, sondern auch mit typischen Linux-Formaten wie GZ.

Docsearcher 3.94.0
Das Java-Programm leistet eine Volltextsuche in vielen gebräuchlichen Dokumentformaten wie DOC, XLS, ODT, ODS, PDF und HTML. Dazu muss ein Index erstellt werden. Docsearcher verlangt eine Java-Runtime, etwa Open JDK, die alle verbreiteten Linux-Systeme zur Installation anbieten.

LinuxWelt Toolbox 1.8
In diesem Installer hat die LinuxWelt viele wichtige und unverzichtbare Utilitys unter einer bequemen Bedienerführung und mit ausführlichen technischen Infos zusammengefasst. Unter Ubuntu & Co. sowie Linux Mint installiert sich das jeweilige Programm mit einem Klick.

Wahl-O-Mat Distributionen
Der überarbeitete Fragebogen mit Informationssystem zur Wahl der passenden Linux-Distribution befindet sich auf der HTML-Oberfläche der Heft-DVD. Der interaktive Fragebogen braucht keine Onlineverbindung und ist komplett in Javascript (Jquery) realisiert.

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

Infotainment: Datenträger enthält nur Lehr- oder Infoprogramme

6 x LinuxWelt
Jahrgang 2019 als PDF

Nachlese: Als Service liegt diesmal der komplette Jahrgang 2019 der LinuxWelt auf Heft-DVD. Die sechs Ausgaben im PDF-Format bieten Lesestoff und Know-how der vergangenen Hefte. Mit dem Tool Docsearcher 3.94 (auf Heft-DVD) ist im Handumdrehen ein Archiv mit Volltextsuche aufgebaut.

Handbücher im PDF-Format

Noch mehr Linux-Know-how: 33 Handbücher auf der Heft-DVD zu Linux-Distributionen und Open-Source-Software bieten weiterführende Fachliteratur. Unter anderem sind aufgefrischte deutschsprachige Handbücher zu Linux Mint vertreten, die hervorragende technische Dokumentation von Tuxcadamy und englischsprachige Klassiker zu Bash, Python und Perl.

LinuxWelt XXL digital
Das komplette Handbuch 1/20

Die besten Ratgeber vergangener Ausgaben: Auf 327 Seiten sammelt das stets aktualisierte digitale „Handbuch" ausgewähltes Linux-Know-how. Neuzugänge sind diesmal Beiträge zu den verschiedenen Containerformaten, zur Paketverwaltung und zur Ubuntu-Installation. Außerdem kommen der Raspberry Pi 4 und dessen Odroid-Konkurrenz zu Wort. Ansonsten erfahren Sie im umfangreichen E-Book zeitlose Linux-Grundlagen, erhalten eine Distributionsübersicht verbreiteter Linux-Systeme und steigen in die Systemadministration ein.

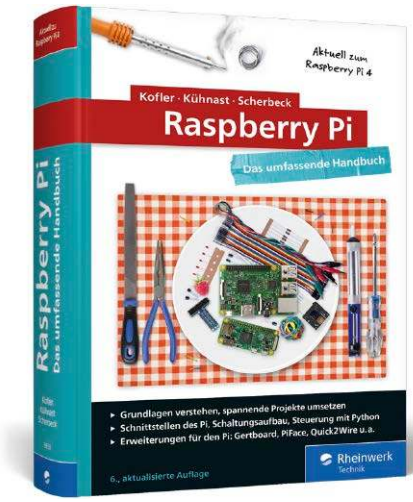
Weitere Infos

Die Vorstellung der sechs Linux-Systeme auf DVD beginnt auf Seite 10. Zusätzliche Anleitungen und Hinweise zu den Distributionen auf Heft-DVD liefert die dortige Übersicht, die Sie über die Datei „index.html" in einem Browser öffnen. Dieses Heft hat zwei Schwerpunkte: Ab Seite 28 geht es um die Linux-Welt-Toolbox mit der wichtigsten Software für Linux-Systeme. Das zweite Special ab Seite 46 hat Verschlüsselungstechniken und Datensicherheit zum Thema.

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 „Raspberry Pi – Das umfassende Handbuch“ aus dem Rheinwerk Verlag.
Das Standardwerk, jetzt auch zum Raspberry Pi 4.



Raspberry Pi

Das umfassende Handbuch

Autoren: Michael Kofler, Charly Kühnast, Christoph Scherbeck
Verlag: 1088 Seiten, 6., aktualisierte Auflage 2019, gebunden, in Farbe, 39,90 Euro
ISBN: Rheinwerk Computing, ISBN 978-3-8362-6933-9

Bücher zum Raspberry Pi gibt es viele. Aber keines ist wie dieser Bestseller in sechster Auflage. Die Raspi-Experten Michael Kofler, Charly Kühnast und Christoph Scherbeck bieten Ihnen auf über 1000 Seiten das komplette Wissen, damit Sie mit dem Raspberry Pi richtig durchstarten. Dieses Handbuch ist randvoll mit Grundlagen und Kniffen zu Linux, Hardware, Elektronik und Programmierung. Genau richtig für alle Maker und Tekkies. Legen Sie gleich los und lassen Sie Ihrer Kreativität freien Lauf!

Aus dem Inhalt: • Grundlagen verstehen • Spannende Projekte umsetzen • Schnittstellen des Pi • Schaltungsaufbau • Steuerung mit Python • Erweiterungen für den Pi: Gertboard, Pi Face u. a. in Hardwareprojekten einsetzen • Aktuell zu allen Modellen, inklusive dem neuen Raspberry Pi 4!

SO FUNKTIONIERT'S:

Auf *www.pcwelt.de/lin* gelangen Sie direkt zu unserer Leserbefragung und nehmen automatisch an der Verlosung teil. Von der Verlosung ausgenommen sind Mitarbeiter des Verlags und deren Angehörige. Der Rechtsweg ist ausgeschlossen.
Einsendeschluss für das Gewinnspiel in LinuxWelt 1/2020 ist der 28.01.2020.
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 das Digital Life Schritt für Schritt „Fritzbox“ 04/2019 (ohne Datenträger). Sie finden den Link zum Download des Hefts am Ende der Leserbefragung.

PLUS: Gratisheft für alle Teilnehmer

Lubuntu 19.10

Den Auftakt zur Heft-DVD macht diesmal Lubuntu 19.10 (in 64 Bit auf Heft-DVD), das als offizielle Ubuntu-Variante in den letzten Ausgaben die deutlichsten Fortschritte machte. Der Desktop ist hier seit einem Jahr das anpassungsfähige LXQT.

VON DAVID WOLSKI

Diese offizielle schlanke Ubuntu-Variante braucht sich in Sachen Aussehen und Desktop nicht mehr hinter den großen Ubuntu-Ausgaben zu verstecken. So wie KDE nutzt diese Desktopumgebung das Toolkit Qt und macht aus dem ehemals spartanischen Lubuntu eine neue Distribution. Insgesamt wirkt LXQT mit seinen Einstellungsmöglichkeiten und Desktopelementen wie die kleinere Schwester von KDE. Geplant war dieser Umbau zwar schon seit 2014, aber erst seit der letzten Version kam Lubuntu mit LXQT in die Gänge. Die Hardwareanforderungen fallen etwa wie jene von Xubuntu aus: Das System ist mit zwei GB RAM zufrieden und damit etwas speicherhungriger, als es Lubuntu mit LXDE war.

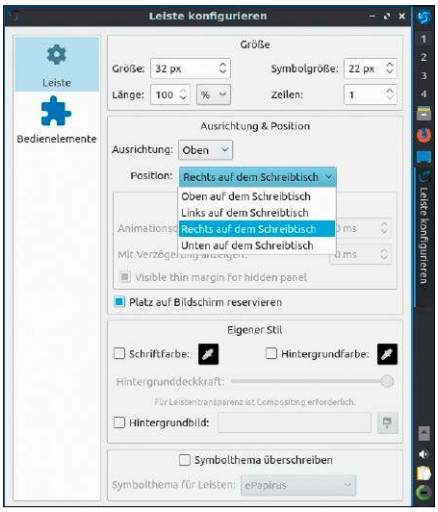
Äußerlich hat LXQT mit LXDE nicht mehr viel zu tun. Die Desktopumgebung entstand, als sich die Entwickler von LXDE und dem experimentellen Razor-Qt 2013 zusammentaten, um einen modernen Nachfolger für LXDE zu schaffen. Das war nötig, weil das Toolkit GTK2, das noch vom bereits eingestellten Gnome 2.32 stammte, schon auf dem Weg zum Abstellgleis war. Von Razor-Qt stammen einige Konfigurationswerkzeuge, die den Desktop nun ausgereifter wirken lassen als LXDE, das genauer besehen aus vielen Einzelteilen bestand. Aber auch LXQT leiht sich Komponenten von anderen Umgebungen. So arbeiten unter der Oberfläche einige KDE-Bibliotheken (KDE Frameworks). Einen eigenen Window-Manager hat LXQT auch nicht, sondern benutzt das schlanke Openbox.

Installer und Standardsoftware

Neben dem für alle Ubuntu-Ausgaben inzwischen üblichen Firefox und Libre Office 6.3 erhalten einige Qt-Programme den Vorzug. So gibt es die Qt-Variante des Videoplayers VLC 3.0 und des Dateimanagers Pcmanfm. Der grafische Paketmanager ist das von KDE bekannte Plasma Discover. Zur Installation gibt es wie bei KDE den grafischen Installer Calamares, der im Stil des Ubuntu-Installers gehalten ist und alle Einstellungen Schritt für Schritt inklusive der Partitionierung abfragt. Calamares ist ein distributionsübergreifendes Projekt, an dem sich Entwickler von Kubuntu, Fedora und Lubuntu beteiligen, um die Vorteile verschiedener Installer in einem möglichst einsteigerfreundlichen Setupprogramm zu vereinen. Auf die Option, das Dateisystem ZFS für die Systempartition zu nutzen, verzichtet Calamares. Dies bleibt ein Merkmal des Ubuntu-eigenen Installers. Lubuntu 19.10 wird neun Monate lang mit Updates versorgt und erscheint ab jetzt nicht mehr als 32-Bit-Ausgabe.

Als letzte Ubuntu-Version hat auch Lubuntu Abschied von 32 Bit genommen. Der Desktop LXQT bleibt mit kleinem Ressourcenhunger aber schlank genug auch für ältere Rechner.

Mehr Infos zu Lubuntu 19.10
Website: *https://lubuntu.me*
Dokumentation: *https://manual.lubuntu.me*
Auf Heft-DVD finden sich neben dem hier vorgestellten Lubuntu 19.10 auch die Hauptedition von Ubuntu 19.10 mit einem aufgefrischten Gnome-Desktop sowie Xubuntu Core 19.10. Eine detaillierte Vorstellung Ubuntus und seiner Neuerungen in Systemunterbau und bei den Desktops lesen Sie ab Seite 14.



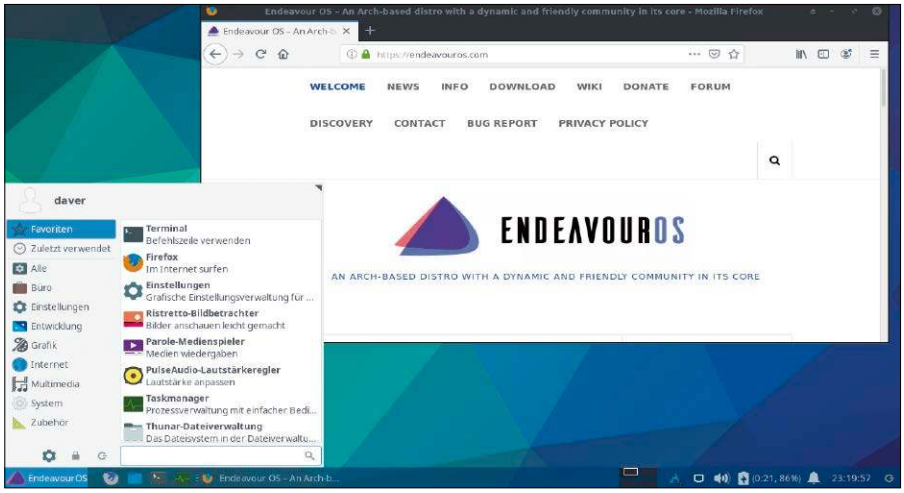
Viele Optionen: Der LXQT-Desktop kann Anwender begeistern, die ihre Arbeitsumgebung bis ins Detail konfigurieren möchten, und kommt damit KDE Plasma 5 nahe.

Endeavour-OS 2019.10.15

Der Vorhang fällt für Antergos und die junge Distribution Endeavour-OS folgt nach. Dieses System (64-Bit-Ausgabe auf DVD) hat den gleichen Anspruch, nämlich mit einem grafischen Installer einen einfacheren Zugang zu Arch Linux zu schaffen.

VON DAVID WOLSKI

Eine wachsende Schar von Linux-Spezialisten und ambitionierten Anwendern sammelte sich in den letzten Jahren um Arch Linux, denn diese Distribution erlaubt den Aufbau eines individuell konfigurierten Systems mit den neuesten Paketen. Generell bleibt Arch Linux mit seinem größtenteils manuellen Installationsprozess allerdings ein Hobby für Fortgeschrittene. Die neue Distribution Endeavour-OS entschärft den Installationsprozess mit dem grafischen Installationsprogramm Calamares, das inzwischen häufiger in Linux-Systemen anzutreffen ist. Es ist dem Installer von Ubuntu nachempfunden und vereinfacht viele Handgriffe.



Sanfter Einstieg in Arch Linux: Endeavour-OS ist keine eigenständige Distribution, sondern ein Livesystem zur bequemen Installation von Arch. Als Desktop dient XFCE 4.14.

Arch Linux in wenigen Schritten

Die neue Distribution entstand nach dem Ende von Antergos im Mai 2019 und will Arch Linux einem größeren Kreis von Anwendern bekannt machen. Nach dem Start des Livesystems zeigt ein Willkommensbildschirm mit „Start the Installer“ eine Verknüpfung zum Installationsprogramm Calamares. Der Desktop des Livesystems ist in Englisch, der Installer und das fertig installierte System sind aber komplett in Deutsch verfügbar. Für gerade erst zu Linux gekommene Einsteiger ist Arch Linux auch in dieser leichter verdaulichen Form von Endeavour-OS (noch) nicht das richtige Desktopsystem, denn die manuelle Ausstattung von Software und die Konfiguration des Linux-Systems erfolgen auf der Kommandozeile.

Im Unterschied zu Manjaro, das zum bekanntesten Arch-Abkömmling wurde, bleibt Endeavour-OS bei den originalen Paketquellen und bezieht Software nicht aus eigenen Quellen. Weitere Programme lassen sich über das inoffizielle Arch User Repository (kurz AUR) finden und kompilieren. Diese Quelle ist vergleichbar mit den PPAs für Ubuntu.

XFCE als Desktop

Endeavour-OS gilt als stabil, ist jedoch noch nicht auf dem Stand, den der Vorläufer Antergos nach seinen langen Jahren Entwicklungszeit erreicht hatte. So gibt es momentan noch keine Auswahl von verschiedenen Arbeitsumgebungen während der Installation. Derzeit ist nur ein – allerdings brandaktueller – XFCE-Desktop 4.14 erreichbar, der auch mit hochauflösenden Hi-DPI-Bildschirmen gut aussieht und seine Elemente passend skaliert.

Ein grafischer Paketmanager ist nicht vorinstalliert. Alle ersten Schritte zur kompletten Einrichtung mit der benötigten Software müssen im Arch-Linux-Stil auf der Kommandozeile mit dem Paketmanager pacman erledigt werden. Dafür sind Pakete aber stets wirklich aktuell, denn das Paketformat von Arch erlaubt den Entwicklern, fertige Pakete ohne großen Aufwand aus dem Quellcode von Programmen zu erzeugen. Als Rolling Release lässt sich die Distribution allein über den Paketmanager aktuell halten und bleibt, einmal installiert, über Jahre ohne aufwendige Neuinstallation frisch.

Mehr Infos zu Endeavour-OS
Website: *https://endeavouros.com*
Dokumentation: *https://wiki.archlinux.org*

Immer häufiger anzutreffen: Der Installer Calamares bringt Endeavour-OS auf die Platte, ist aber das Installationsprogramm von Lubuntu, Kubuntu und Sparky Linux.

Sparky Linux 5.9

In dieser sympathischen Distribution mit schlankem Openbox-Desktop steckt ein neues Debian 10 „Buster“, aber auch noch eine Menge mehr: Sparky Linux liefert zwei eigene Installer mit, welche direkt aus dem Livesystem heraus laufen.

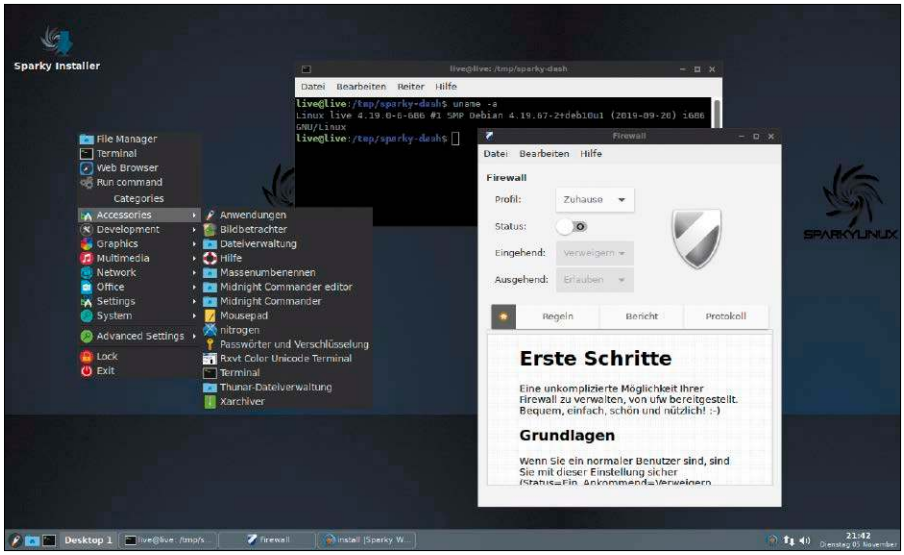
VON DAVID WOLSKI

Während Debian 10 wenig Neues bietet und sich brav um die Pflege der Programmversionen gekümmert hat, sind die ebenfalls aufgefrischten inoffiziellen Debian-Varianten immer einen genaueren Blick wert. Um ein solches System handelt es sich bei Sparky Linux 5.9. Es läuft in dieser superschlanken Ausgabe mit einem Openbox-Desktop und kommt mit wenig RAM aus. Ein älterer Rechner der letzten zehn Jahre ist für Sparky Linux ausreichend. Daher bietet die Heft-DVD bewusst die schlankere 32-Bit-Ausgabe des Systems.

Viele Desktops zur Auswahl

Sparky Linux ist ganz klar für Desktopanwender gemacht und wird daher mit einer ganzen Reihe von Arbeitsumgebungen angeboten. Davon profitiert auch das System auf Heft-DVD, selbst wenn dieses im Livesystem erstmal nur den wenig spektakulären Openbox-Desktop liefert. Denn die Besonderheit von Sparky Linux sind seine beiden Installer, die übrigens anders als in den offiziellen, unveränderten Debian-Systemen direkt aus dem Livesystem heraus starten. Die Verknüpfung auf dem Desktop ruft das komfortable Installationsprogramm Calamares auf, das dem Installer von Ubuntu ähnelt und auch von Lubuntu und Kubuntu verwendet wird. Über diesen Weg wird Sparky mit dem Openbox-Desktop eingerichtet.

Daneben gibt es aber über das Anwendungsmenü links unten mit dem Menüpunkt „Sparky (Advanced Installer)“ auch noch ein Script-basiertes Installationstool für Fortgeschrittene, welches in englisch- und deutschsprachigen Dialogfenstern die grundlegenden Einstellungen abfragt und gegen Ende des Einrichtungsprozesses eine Vielzahl an Desktopumgebungen zur Auswahl stellt.



Ein Debian mit Extras: Sparky Linux 5.9 ergänzt Debian 10 „Buster“ um nützliche Details. Der Desktop der Ausgabe auf DVD ist ein minimalistisches Openbox.

Wenig vorinstallierte Software

Sparky Linux liefert kaum vorinstallierte Software mit. Das muss der Nutzer über das Terminal oder mit dem grafischen Paketmanager Synaptic korrigieren. In Synaptic ist neben eigenen Paketquellen für angepasste Desktopumgebungen auch die Paketquelle *http://www.deb-multimedia.org* mit eingebunden, die etliche Player wie den VLC sowie alle wichtigen Codecs nachliefert, die einem puren Debian fehlen.

Sparky Linux wird solange gepflegt, solange auch Debian 10 aktuell bleibt, also mindestens die nächsten vier Jahre. Wie auch im aktuellen stabilen Debian ist der Kernel bei Version 4.19 angekommen. Bei der Installation kommt Libre Office 6.1.5 mit. Dies sind keine brandneuen Versionen, sondern jene ausgiebig getesteten Pakete, die der stabile Debian-Zweig liefert. Sicherheitssensible Browser wie Firefox und Chromium liegen aber auch in den Debian-Quellen stets in den neuesten Versionen zur Installation vor.

Mehr Infos zu Sparky Linux
Website: *http://sparkylinux.org*
Dokumentation: *http://sparkylinux.org/faq*

Hat eine Menge Desktops mehr auf Lager: Der alternative Installer von Sparky Linux bietet, anders als Calamares, eine große Auswahl von Desktopumgebungen.

Slax 9.11

Slax ist auf den Einsatz als komfortables, minimales Livesystem spezialisiert. Allerdings ist hier serienmäßig sehr wenig Software mit an Bord. Wir haben deshalb die Ausgabe auf Heft-DVD (32 Bit) um Firefox sowie Sprachpakete ergänzt.

VON DAVID WOLSKI

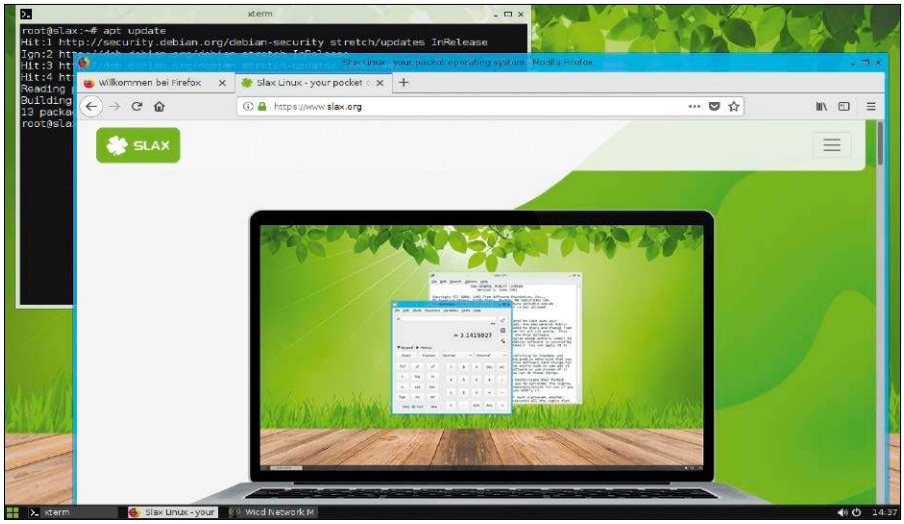
Slax basierte in seinen ersten Ausgaben auf Slackware, wurde von seinem Macher aber seit der Version 9 aus Debian-Komponenten komplett neu konzipiert, um die Entwicklung zu vereinfachen und zu beschleunigen. Slax ist als flottes kleines Linux auf einem USB-Stick das ideale Surfsystem, kann aber fortgeschrittenen Anwendern auch als minimales, leicht erweiterbares Notfallsystem dienen. Hier arbeitet mit Kernel 4.9 noch das ältere Debian 9 „Stretch“, das noch bis ins Jahr 2022 Bugfixes bekommt.

Ethernet- und WLAN-tauglich

Nach dem Start präsentiert das aktuelle Slax 9.11 einen sehr schlichten, aber ansehnlichen Desktop in englischer Sprache. Immerhin ist bereits ein deutsches Tastaturlayout aktiv, das sich bei Bedarf mit einem Rechtsklick auf den Desktophintergrund im angezeigten Menü „Keyboard Layout“ wieder ändern lässt.

Ein Klick auf das Starter-Symbol rechts unten blendet die verfügbaren Programme ein, inklusive des „Net Managers“ zum Aufbau einer WLAN-Verbindung. Dabei handelt es sich nicht um den üblichen Network-Manager von Gnome, denn dieser wäre mit seinen Abhängigkeiten zu umfangreich für dieses System. Stattdessen kümmert sich das Python-Programm Wicd um die Netzwerkverbindungen. Eine Ethernet-Verbindung wird automatisch aufgebaut, für die Teilnahme an einem WLAN sind aber noch ein paar Einstellungsschritte nötig: Für das gewünschte WLAN muss in den Verbindungsinformationen noch die verwendete Verschlüsselung (in den meisten Fällen „WPA2“) sowie das Passwort eingetragen werden.

Programme und Netzwerkkonfiguration in der Übersicht: Der Desktop von Slax ähnelt einem Smartphone-Homescreen und dient nur zum Start der wenigen Programme.



Extraklein und schnell: Slax gehört zu den winzigen Livesystemen, die kaum mehr als einen Browser mitliefern. Die Version auf Heft-DVD ist um Firefox und Sprachpakete erweitert.

Zusätzliche Programme

Die Software ist reduziert, aber ausreichend fürs Surfen und für Dateiaktionen. Als grafischer Dateimanager dient der schlanke Pcmanfm von LXDE und als Dateimanager im Terminal ist auch noch der Midnight Commander verfügbar. Terminal, Browser Chromium 73, Texteditor und Taschenrechner sind auch an Bord, zusätzlich gibt es Firefox in der ESR-Ausgabe 60.9, also die Browserversion mit Langzeitunterstützung.

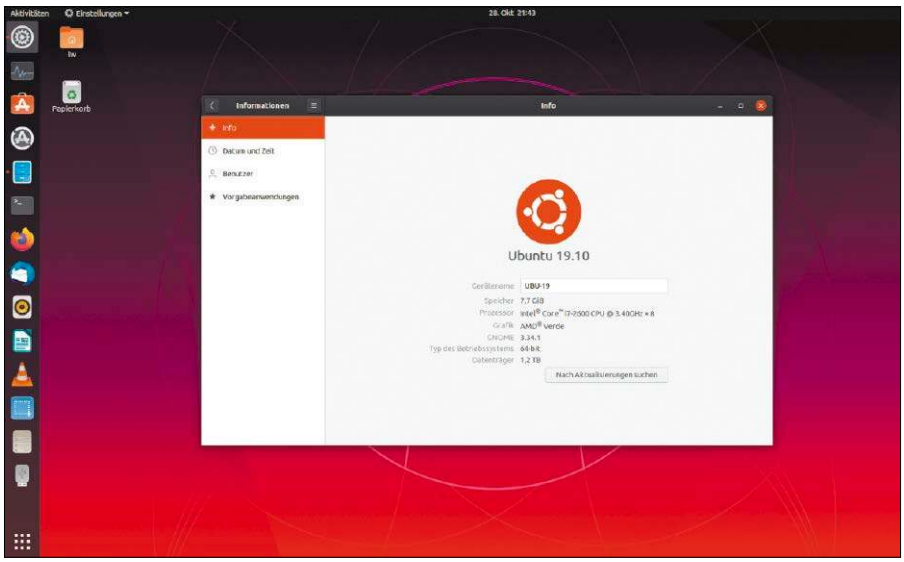
Slax ist eine gute Wahl als Livesystem auf USB-Stick, denn es ist mit seiner Debian-Abstammung für viele Anwender vertrautes Gelände und gut erweiterbar. Auf Heft-DVD liegt Slax 9.11 deshalb auch als ISO-Datei im Verzeichnis „Image-Dateien“. Die mitgelieferte ISO-Datei auf Heft-DVD dient zum Brennen von CDs/DVDs. Slax kann aber auch auf USB-Stick übertragen werden. Dazu muss die Datei „slax-32bit-9.11.0-lw.iso“ mit einem Entpacker oder Dateimanager geöffnet und auf einen leeren USB-Stick (mit Ext4 oder FAT32 formatiert) entpackt werden. Unter Linux kann beispielsweise der Packer Ark (unter KDE) oder Nautilus in Gnome eingesetzt werden. Auch 7-Zip in der Kommandozeile kann ISO-Dateien entpacken. Das mitgelieferte Script „bootininst.bat“ (Windows) beziehungsweise „bootinst.sh“ (Linux) im Unterverzeichnis „/slax/boot“ macht den Stick anschließend bootfähig. Das Script starten Sie direkt auf dem USB-Laufwerk.

Mehr Infos zu Slax
Website: *http://www.slax.org*
Dokumentation:
https://www.slax.org/introduction.php

Ubuntu 19.10

Ubuntu und die dahinterstehende Firma Canonical gehen wieder extravagante Sonderwege: Der Einbau des zukunftsweisenden Dateisystems ZFS ist die spektakulärste Maßnahme der neuen Ubuntu-Version 19.10 („Eoan Ermine“).

VON HERMANN APFELBÖCK



Das am 17. Oktober veröffentlichte Ubuntu 19.10 gewinnt in allen Editionen – nicht zuletzt durch die aktualisierten Desktops. Herauszuheben sind die Oberflächen Gnome (Hauptedition), XFCE (Xubuntu) und Mate (Ubuntu Mate) mit signifikanten Verbesserungen, während KDE (Kubuntu), LXQT (Lubuntu) und Budgie (Ubuntu Budgie) nur marginale Änderungen zeigen. Der Unterbau ist mit Kernel 5.3 ebenso aktualisiert wie die vorinstallierte Software inklusive Script-Interpreter und Compiler. Kontrovers diskutiert wird der Einbau des Dateisystems ZFS im Ubuntu-Installer – eine vorerst als „experimentell“ gekennzeichnete Option.

STS-Zwischenversion: Ja oder nein?

Die Ubuntu-Oktoberausgabe 19.10 ist eine STS-Zwischenversion (STS: Short Term Support) mit nur neun Monaten Support bis Juli 2020. Sie ist aber wie alle Zwischenversionen keine Sackgasse, sondern kann und sollte im Frühjahr 2020 auf die LTS-Langzeitversion 20.04 (LTS: Long Term Support, fünf oder drei Jahre) gehievt werden. Ungeachtet etlicher Neuheiten stellt sich bei kurzlebigen Ubuntu-Zwischenversionen immer als wesentlichste Frage, ob sich dieser temporäre Schritt tatsächlich lohnt. Dazu folgende Empfehlungen:

- Wer aktuell die Zwischenversion Ubuntu 19.04 installiert hat, **muss** auf das neue 19.10 upgraden, denn 19.04 läuft demnächst ab.
- Ubuntu-Neueinsteiger können ohne Bedenken zu Version 19.10 greifen, weil 2020 der problemlose Umstieg auf die nachhaltige LTS-Version möglich ist.
- Ubuntu-Fans werden Version 19.10 nicht auslassen wollen, weil es interessante Neuheiten bietet. Diese kommen allerdings vorrangig bei einer Neuinstallation zur Geltung, weniger beim Upgrade.
- Für Nutzer der Langzeitversion Ubuntu 18.04 gibt es in der Regel keine ausreichenden Gründe für das Upgrade. Auch die wie immer erweiterte Hardwareunterstützung durch den neuen Kernel (5.3) ist ein recht kurzlebiges Argument für Version 19.10, weil die aktuelle Langzeitversion 18.04 Anfang 2020 den Release Point 18.04.4 veröffentlichen wird. Somit wird 18.04 LTS voraussichtlich schon im nächsten Februar hardwaretechnisch auf dem Stand von 19.10 sein.

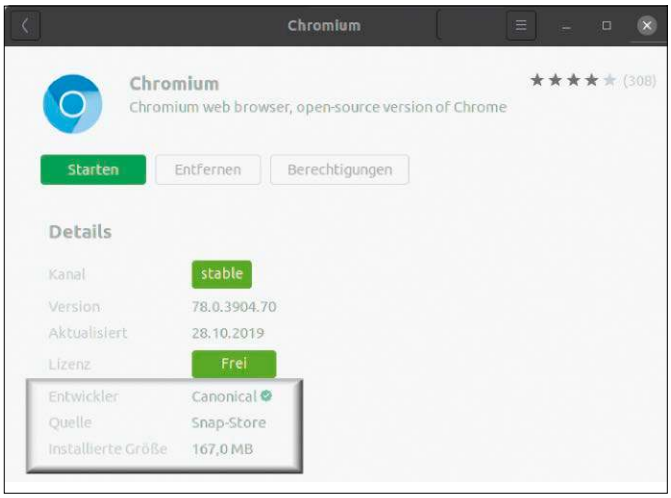
Kernel – Treiber – Software

Basis von Ubuntu 19.10 ist der aktuelle Linux-Kernel 5.3 vom September 2019. Die zahlreichen Änderungen im Kernel bieten unter anderem Leistungsverbesserungen für das Ext4-Dateisystem und für AMD- und Broadcom-Grafikchips. Die Tatsache, dass sich der Grafikhersteller Nvidia an der Kernel-Entwicklung so gut wie nicht beteiligen will, beantwortet Ubuntu jetzt mit dem Deal, den proprietären Nvidia-Treiber direkt auf dem Installationsmedium mitliefern zu dürfen. Benutzer von Nvidia-Grafikkarten müssen daher den Treiber nicht mehr manuell nachinstallieren. Das ist eine benutzerfreundliche Ubuntu-Geste, allerdings auch nicht mehr, weil das Nachladen des Treibers wenig Mühe bereitete. Strategisch ist dieser Deal aber durchaus bemerkenswert, weil Nvidia auf der Feindesliste der Linux-Gemeinde ganz weit oben steht.

Ebenfalls strategisch bewerten kann man die Entscheidung Canonicals, den beliebten Chromium-Browser nicht mehr als traditionelles DEB-Paket zu pflegen, sondern nur noch als Snap-Container auszuliefern. Canonical begründet dies technisch, nämlich mit dem erheblichen Aufwand, eine Software für mehrere gültige Ubuntu-Versionen (16.04, 18.04, 19.10) zu pflegen, die aus Sicherheitsgründen ständig aktualisiert werden muss. Das Snap-Paket ist hingegen versionsunabhängig und muss daher nur jeweils für x86- und ARM-Architektur aktuali-

siert werden. Diese plausible technische Begründung hat aber einen strategischen Nebenaspekt. Für den Ubuntu-Nutzer ist es kaum relevant, ob der Browser als Snap-Container oder normal installiert seinen Job erledigt. Für Ubuntu-Derivate wie Linux Mint ist Chromium als Snap hingegen ein technisches Problem, weil sie nun entweder das Snap-Format (von Canonical) integrieren oder den Browser selbst pflegen müssen.

Selbstverständlich bieten alle neuen Ubuntu-Editionen aktualisierte System- und Anwendungssoftware. Dazu gehören Libre Office 6.3, Firefox 69 und Thunderbird 68. Ubuntu Mate 19.10 verabschiedet sich von Thunderbird und VLC als Standardsoftware und übernimmt stattdessen das Mailprogramm Evolution und den Player Gnome MPV – beides weniger aus technischen, sondern aus optischen Gründen.



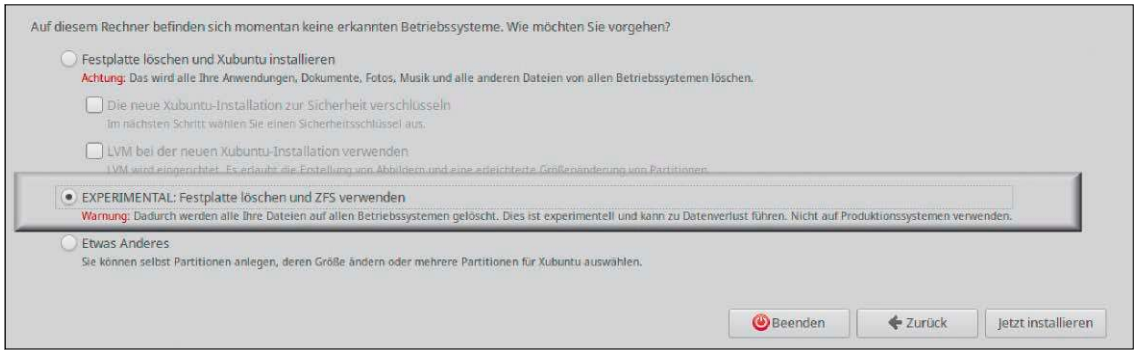
Ubuntu fördert sein eigenes Snap-Containerformat: Die Entscheidung, ab Version 19.10 den Browser Chromium nur noch als Snap anzubieten, ist vielleicht nur der Anfang.

Kaum relevante Bootoptimierung

Schon seit Version 18.10 startet Ubuntu mit komprimierten Bootmodulen, um das Laden vom Datenträger zu beschleunigen. An dieser Schraube wurde weitergedreht, um mit unterschiedlichen Kompressionsverfahren das Optimum zu erzielen. Das Ergebnis ist aber allenfalls messbar, nicht wirklich relevant oder spürbar. Wir haben Ubuntu 19.10 und den Vorgänger 19.04 nacheinander auf derselben Festplatte und Partition installiert. Auf dem relativ schnellen Rechner mit SSD messen wir Folgendes:

Ubuntu 19.04 11,45 Sekunden
Ubuntu 19.10 11,32 Sekunden

Man darf festhalten: Auf moderner Hardware bootet Ubuntu schon seit Versionen



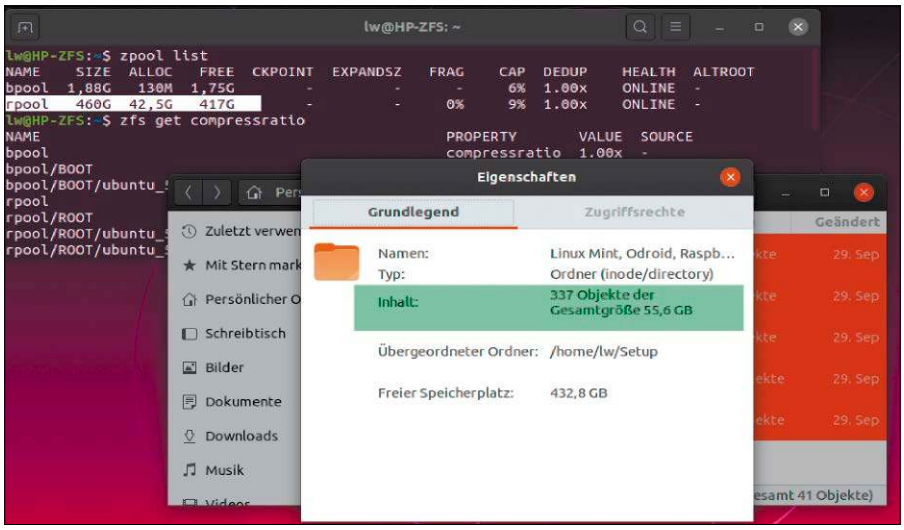
ZFS-Dateisystem im Ubuntu-Installer: Die spektakulärste Änderung zeigt der Ubiquity-Installer. Kubuntu und Lubuntu mit dem Calamares-Installer haben diese Option bislang nicht.

UBUNTU 19.10 AUF DVD UND ALS DOWNLOAD

Von den sechs offiziellen Ubuntu-Editionen finden Sie drei Ubuntus bootfähig als Livesystem mit Installationsoption auf der Heft-DVD. Es handelt sich um die Hauptedition, um das kleinere Lubuntu mit LXQT-Desktop und um das ebenfalls ressourcensparende Xubuntu. Letzteres enthält in der auf DVD vorliegenden Coreversion nur das Betriebssystem und den Desktop XFCE. Die beiden Spezialdistributionen Ubuntu Kylin (chinesisch) und Ubuntu Studio (ein Xubuntu mit Video-, Audio-, Grafikausstattung) bleiben hier außen vor.

Ubuntu 19.10 (Hauptedition mit Gnome)	*https://ubuntu.com/download/desktop* (auf Heft-DVD, Download 2,29 GB)
Kubuntu 19.10 (KDE)	*https://kubuntu.org/getkubuntu/* (Download 2,14 GB)
Xubuntu 19. 10 (XFCE)	*https://xubuntu.org/download* (auf Heft-DVD Xubuntu Core, Download 1,53 GB)
Lubuntu 19. 10 (LXQT)	*https://lubuntu.me/downloads/* (auf Heft-DVD, Download 1,56 GB)
Ubuntu Mate 19.10 (Mate)	*https://ubuntu-mate.org/download/*, dort unter „64 Bit“ (Download 2,10 GB)
Ubuntu Budgie 19.10 (Budgie)	*https://ubuntubudgie.org/downloads* (Download 2,0 GB)
Netboot-Installer	*http://cdimage.ubuntu.com/netboot/eoan/* (Download 73 MB, mini.iso, minimaler Installer mit manueller Desktop- und Softwareauswahl)

Beachten Sie bei geplanten Installationen, dass die Heft-DVD der LinuxWelt ausschließlich im Bios-Modus bootet (und folglich installiert). Für Multibootinstallationen im Uefi-Modus müssen Sie das gewünschte ISO-Abbild von der Heft-DVD (unter „Image-Dateien“) auf eigenen USB-Stick schreiben.



ZFS komprimiert ungefragt: Allein der Ordner „/home/lw/Setup“ enthält hier mehr als 55 GB. Trotzdem ist die komplette Partition inklusive Ubuntu-Betriebssystem nur mit gut 42 GB belegt.

richtig schnell und hat weitere Optimierung kaum nötig.

Auf älterer Hardware ist die Situation deutlich anders. Hier ist mit deutlich längeren Bootzeiten mit bis zu einer Minute zu rechnen, zumal sich Ubuntus Bootoptimierung hier kontraproduktiv auswirkt.

Auf diesen Zusammenhang hatten wir schon bei Einführung der Kompressionsmethode in Version 18.10 hingewiesen: Auf älteren Rechnern wird die CPU zum Flaschenhals, die die Module erst entpacken muss. Die geänderte Boottechnik begünstigt eindeutig aktuelle Rechner mit schnellen CPUs.

Das ZFS-Dateisystem

Die Ubuntu-Installation zeigt beim wichtigen Schritt „Installationsart“ die neue Option „EXPERIMENTAL: Festplatte löschen und ZFS verwenden“. Aus Termingründen hat Kubuntu diesen Einbau nicht realisiert, will dies aber in Version 20.04 nachholen. In Lubuntu fehlt die ZFS-Option ebenfalls, wobei hier aber nicht klar ist, ob dies Termingründe hatte oder ein bewusstes Veto bedeutet. Eine gerechte Bewertung von ZFS ist nicht einfach.

1. Psychologisch scheint es mehr als bedenklich, auf einem Endanwender-Desktop an dieser prominenten Stelle eine experimentelle und serveraffine Funktion anzubieten. Schon der unzureichend erklärte LVM (Logical Volume Manager) hat in diesem Dialog nach unserer Auffassung nichts verloren. Linux-Einsteiger und typische Desktopanwender sollten um beide Angebote einen großen Bogen machen, weil ZFS wie LVM die Komplexität deutlich erhöhen, ohne diesen Nachteil auf einem einfachen PC oder Notebook signifikant zu belohnen. Ausnahme ist die Option der Laufwerksverschlüsselung, die den LVM benötigt und diesen automatisch aktiviert. Auch für ZFS gibt es natürlich Motive, über deren Gewicht Sie aber selbst entscheiden müssen und im Zweifel skeptisch bleiben sollten.

2. ZFS ist ein Dateisystem von Sun Microsystems/Oracle, das nach heutigem Ermessen keine Größen- oder Mengenbegrenzungen kennt. Dazu besitzt es die Fähigkeiten eines Logical Volume Managers zur logischen Zusammenlegung von Festplatten, eines Raid-Controllers zur ausfallsicheren Mehrfachspeicherung, einer Snapshotsoftware zum Ablegen von Wiederherstellungspunkten und bietet ferner (um nur das Wichtigste zu nennen) automatische Fehlerkorrektur und eingebaute Daten-Komprimierung sowie eingebaute Datenverschlüsselung.

Mit solchen Eigenschaften gehört ZFS in erster Linie auf Server mit riesigen Datenmengen und höchsten Ansprüchen auf Ausfallsicherheit. Die Ubuntu-Firma Canonical, deren Ehrgeiz im kommerziellen Serverbereich liegen, fördert seit Jahren ZFS und setzt nun mit dem ZFS-Einbau in Ubuntu ein spektakuläres Zeichen.

Was bedeutet ZFS für den normalen Ubuntu-Nutzer? Beginnen wir mit den Nachteilen: In Ubuntu 19.10 fehlt noch jegliche Desktopintegration. Laufwerkstools wie Gnome-Disks zeigen die rpool-Partitionen von ZFS zwar immerhin an, können sie aber nicht bearbeiten.

Viele gewohnte Terminaltools wie lsblk oder df werden durch die komplexe ZFS-Partitionierung unübersichtlich bis unbrauchbar. Wer sich auf ZFS einlässt, kommt mittelfristig an den komplexen Terminaltools zfs und zpool nicht vorbei:

```
zpool list
```

leistet eine Übersicht und informiert über den Belegungszustand. Um mit

```
zfs snapshot [...]
```

einen Sicherungspunkt anlegen zu dürfen, sind erst entsprechende Rechte zu konfigu-

UPGRADE VON UBUNTU 19.04 AUF 19.10

Wer bislang die Zwischenversion Ubuntu 19.04 nutzt, sollte ab sofort auf 19.10 upgraden. Auch ein Upgrade der LTS-Version 18.04 ist möglich, aber in der Regel keine Empfehlung, zumal bald die nächste LTS-Version 20.04 demnächst nachfolgt (April 2020).

Vor dem Upgrade ist eine Systemaktualisierung Pflicht – entweder in der grafischen Aktualisierungsverwaltung oder im Terminal:

```
sudo apt update
```

Danach öffnen Sie „Anwendungen & Aktualisierungen“ und dort die Registerkarte „Aktualisierungen“. Damit die Zwischenversion 19.10 am Desktop angeboten wird, wählen Sie neben „Über neue Ubuntu-Versionen benachrichtigen“ die Option „Für jede neue Version“. Die Aktualisierungsverwaltung wird dann umgehend die aktuelle Version anbieten. Mit dem Terminalbefehl

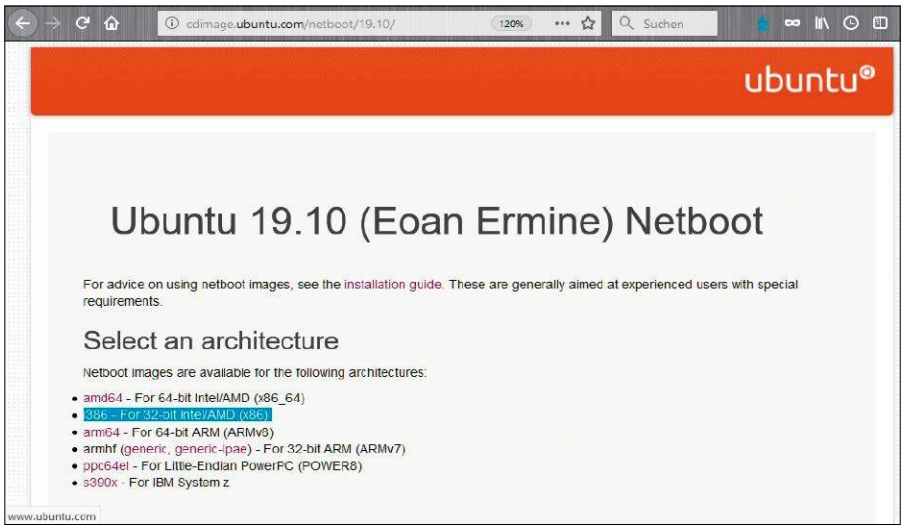
```
sudo do-release-upgrade -d
```

können Sie das Upgrade aber auch manuell anstoßen. Am besten starten Sie diesen Befehl nicht im grafischen Terminal, sondern in der virtuellen Konsole (Strg-Alt-F1). Die Vorgehensweise im nächsten Frühjahr beim fälligen Upgrade von 19.10 auf die LTS-Version 20.04 ist analog.

rieren. Von den sehr zahlreichen Subkommandos von zpool („zpool get […]“) und zfs („zfs create […]“, „zfs send […]“) wird man im Alltag nur wenige benötigen, aber eine Mindestausstattung ist unentbehrlich, solange Canonical die ZFS-Unterstützung nicht durch ein grafisches Front-End veredelt.
Ferner gilt ZFS als Speicherfresser, weil das Dateisystem eine großzügige Cacheverwaltung benötigt. Dieses Vorurteil ist aber zu relativieren, denn der RAM-Verbrauch hängt mit der verwalteten Festplattenkapazität zusammen: Pro TB Plattenkapazität sollte etwa ein GB RAM bereitstehen. Beim Einsatz auf einem Desktoprechner mit Ein-TB-Platte nimmt sich ZFS dann etwa ein GB RAM, was bei einer Ausstattung mit vier oder acht GB RAM keine Engpässe verursacht.
Natürlich hat dieses beeindruckende Dateisystem seine Vorteile. Der offensichtlichste Vorteil besteht darin, dass die interne Komprimierung erheblich Platz spart. Ohne jegliche Eingriffe werden Betriebssystem und Benutzerdaten je nach Format auf die Hälfte und kleiner geschrumpft. Die weiteren Vorteile ergeben sich durch Einsatz der angesprochenen Tools zfs und zpool (was den Rahmen dieser Versionsvorstellung definitiv sprengen würde).
Beachten Sie, dass sich das Dateisystem im Dateimanager ganz normal mit den Linux-üblichen Standardpfaden präsentiert. Lediglich die Geräteanzeige der Partitionen ist ungewöhnlich. Die Installation erledigt der Ubuntu-Installer Ubiquity vollautomatisch und im einfachsten Fall ohne Benutzerentscheidungen. Nur wenn mehrere Laufwerke als mögliches Installationsziel vorliegen, erscheint nach der Entscheidung für ZFS die Abfrage, auf welches Laufwerk installiert werden soll. Es ist also nicht so, dass ZFS einfach alle internen Platten übernimmt und als Pool zusammenfasst. Somit ist auch eine Multiboot-Installation mit ZFS möglich.

32 Bit ist so gut wie Geschichte

32-Bit-Systemarchitektur: Beim Standarddownload aller Ubuntu-Varianten gab es schon seit der letzten Version 19.04 keinen einzigen verbliebenen 32-Bit-Kandidaten mehr. Das gilt natürlich unverändert weiter für Version 19.10 und alle künftigen Ubuntus. Ein Geheimtipp für Nutzer, die ein sparsameres 32-Bit-Ubuntu bevorzugten, verblieb aber damals noch: der kleine Netboot-Installer (mini.iso), der für AMD64 (64 Bit) und i386 (32 Bit) vorlag. Dieser Installer, der alle Komponenten aus dem Internet zieht und dabei die Auswahl eines beliebigen Desktops erlaubt, ist auch für Ubuntu 19.10 unter *http://cdimage.ubuntu.com/netboot/eoan/* erhältlich. Die dort immer noch angezeigte Variante „i386 - For 32-bit“ führt aber ins Leere. Somit ist ein aktuelles 32-Bit-Ubuntu definitiv nicht mehr verfügbar.

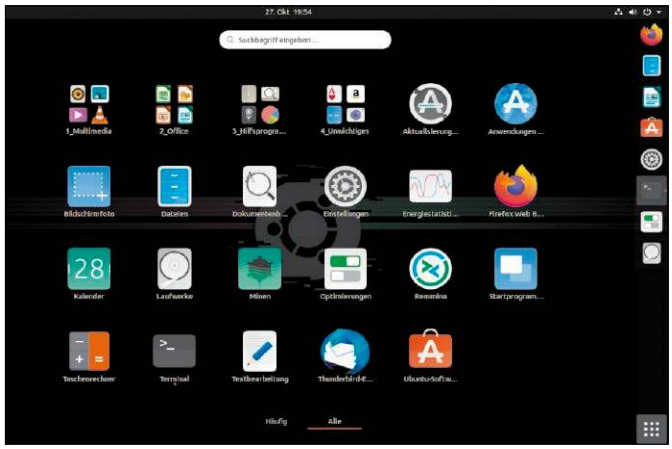


Schluss mit 32-Bit-Ubuntu: Auch der alternative Netinstaller liegt nur noch in 64 Bit vor. Der für Version 19.10 immer noch angezeigte Eintrag „i386“ ist irreführend und führt ins Nichts.

Die Gnadenfrist für 32-Bit-Ubuntu läuft aber immerhin bis April 2023, sofern man auf das nicht mehr ganz taufrische Ubuntu 18.04 LTS zurückgreift. Dazu ist es aber nötig, entweder die Ubuntu-Hauptedition zu wählen oder den besagten Netinstaller 18.04 (mit freier Desktopauswahl, siehe *http://cdimage.ubuntu.com/netboot/bionic/*), der ebenfalls bis 2023 Support erhält. Alle anderen Ubuntu-Editionen 18.04 laufen schon 2021 ab.
32-Bit-Software: Die Ubuntu-Firma Canonical wollte mit Version 19.10 nicht nur die 32-Bit-Distributionen (wie geschehen), sondern auch 32-Bit-Software komplett abschaffen. 64-Bit-Systeme können 32-Bit-Software nur ausführen, wenn die dafür erforderlichen 32-Bit-Bibliotheken vorliegen. Die Ankündigung, solchen 32-Bit-Support zu streichen, ist jedoch auf erheblichen Protest gestoßen – insbesondere von Entwicklern und Nutzern der Spieleplattform Steam und des Projekts Wine. Beide sind auf 32-Bit-Support angewiesen. Canonical hatte ein Einsehen: Die fundamentalen 32-Bit-Pakete werden innerhalb der 64-Bit-Distributionen weiterhin gepflegt und somit ist der Einsatz von 32-Bit-Software auch unter Version 19.10 gesichert.

Ubuntu 19.10 (Gnome-Hauptedition)

Die Hauptedition läuft mit dem Gnome-Desktop 3.34, der in Ubuntu-typischer Weise um einige Standards wie dem Favoriten-



Gruppierte Programme: In der Gnome-Anwendungsübersicht darf der Benutzer jetzt aufräumen. Die Sammelordner entstehen durch einfaches Drag & Drop.

Externe Medien im Ubuntu-Dock: Der kleine Service vereinfacht Zugriff und Auswerfen von USB-Medien und DVDs.

dock erweitert ist. Gnome und der Fenstermanager („Mutter“) haben weiteres Leistungstuning erfahren, das den Desktop flüssiger und – laut Entwickler – zugleich CPU-schonender macht.

Eine sichtbare Neuerung zeigt sich beim Anschließen von USB-Medien oder Einlegen von DVDs: Diese erscheinen jetzt standardmäßig als Icon im Favoritendock und bieten hier direkten Zugriff ohne vorherige Suche im Dateimanager. Cloudspeicher wie Google, Dropbox oder Onedrive erhalten hier ebenfalls ihr Icon. Nach Rechtsklick auf das Icon lassen sich die Medien „Auswerfen“.

Die bildschirmfüllende App-Übersicht nach Klick auf das Punkte-Symbol (oder Windows-A) gruppiert jetzt Programmicons durch Drag & Drop. Das spart Platz und räumt kaum benötigte Software aus dem Weg. So zusammengeworfene Programme landen in einem Sammelordner, der nach Rechtsklick passend benannt werden kann. Konsequent genutzt wird damit die App-Übersicht zu einem großflächigen Kategorienmenü. Falsch einsortierte Programme lassen sich jederzeit mit der Maus wieder aus dem Sammelordner ziehen. Das die Ubuntu-Optik bestimmende Yaru-Standardthema ist nicht nur verfeinert, sondern auch in drei Varianten verfügbar, um Titelleisten und Dialoge hell oder dunkel zu färben. Allerdings hält es Gnome nach wie vor nicht für nötig, solche Einstellungen selbst anzubieten. Erst das nachinstallierte Gnome-Tweaks („Optimierungen“) macht die Auswahl unter „Erscheinungsbild → Anwendungen“ möglich.

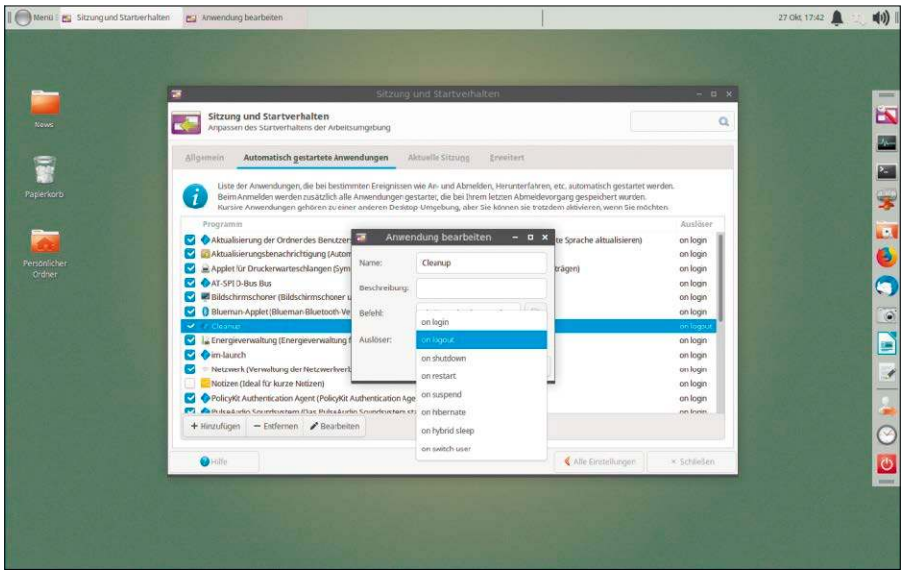
Die „Einstellungen“ (Gnome-Control-Center) bieten die bekannten Punkte, sind aber an einigen überarbeitet und aufgehübscht. So ist es bei der Auswahl des Hintergrundbildes sehr einfach, dieses für den Desktop, für den Anmeldebildschirm oder für beides festzulegen. Eine weitere Neuheit zeigt sich unter „Einstellungen → Freigabe“: Ubuntu 19.10 hat einen UPnP/DLNA-Server standardmäßig an Bord. Für das Streaming von Filmen vom Ubuntu-PC auf UPnP-fähige Clients wie Smart-TVs oder Medienplayer (VLC, Windows Media Player) ist nicht mehr erforderlich, als an dieser Stelle die „Medienfreigabe“ zu aktivieren.

Xubuntu 19.10 (XFCE)

Die altehrwürdige, aber exzellente Oberfläche XFCE hat sich vier Jahre für die neue Version 4.14 Zeit gelassen. In Xubuntu 19.10 ist dieser aktualisierte XFCE an Bord. Mit der Portierung auf GTK3 ist XFCE jetzt wieder zukunftstauglich und soll künftig auch wieder, ab Version 4.16, einen verlässlichen halbjährlichen Erscheinungszyklus erhalten. Der Window-Manager von XFCE 4.14 unterstützt nun Monitore mit hoher Auflösung (HiDPI) und Vsync, das Artefakte bei der Videowiedergabe unterbindet. In den „Einstellungen“ (xfce4-settings-manager) erscheint ein neuer Punkt „Farbprofile“ mit diversen vorgegeben Profilen, um Druck- und Scanergebnisse zu optimieren. Auf die Monitordarstellung hat dies keine Auswirkung. Optimiert wurde ferner der Punkt „Einstellungen → Anzeige“, der nun unter „Erweitert“ das Speichern der aktuellen Monitoreinstellungen als „Profil“ vorsieht. Damit wird es auf einem Notebook sehr einfach, zwischen mobilem und stationärem Betrieb in der Dockingstation Auflösungen und Frequenzen zu wechseln.

Das Einstellungsapplet „Sitzung und Startverhalten“ hat einiges dazugelernt. Eine interessante Option ist unter „Automatisch gestartete Anwendungen“ die freie Auswahl des Autostart-Zeitpunkts: Log-on, Log-out, Shutdown und jeder Ruhezustand kann vorher noch die gewünschte Aktion auslösen. Die Systemleisten erhalten dezentes Verhaltenstuning durch Animation, damit der (optionale) Vorgang des Ausblendens sichtbar wird. Im Dual-Monitor-Betrieb ist die Präsenz der Systemleisten auf primärem und sekundärem Display nach Wunsch zu regeln.

Neben dem XFCE-Desktop selbst erhalten auch die XFCE-eigenen Tools und Programme eine Menge an Fehlerkorrekturen und Verbesserungen: Thunar, der Standarddateimanager, erhält bei der Tastatursteuerung neue Standardhotkeys wie etwa Strg-+/- zur Skalierung der Dateiobjekte. Eine in



Xubuntu hat durch das erneuerte XFCE enorm gewonnen. Hier abgebildet ist das Systemapplet „Sitzung und Startverhalten“, das Autostarts für diverse Systemereignisse ermöglicht.

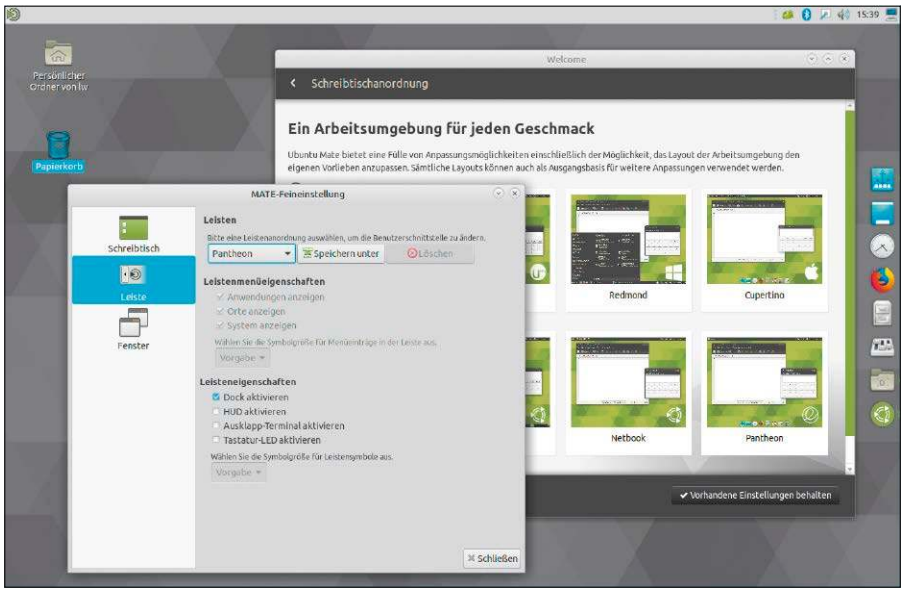
einem Dateiordner enthaltene Datei „folder.jpg“ zeigt Thunar als Ordnericon an. Der Mediaplayer Parole wurde mit einem platzsparenden „Mini-Modus“ ebenso verbessert wie der Bildbetrachter Ristretto, der nun auch den Desktophintergrund festlegen kann. Dies sind aber Marginalien, zumal die meisten Nutzer hier auf mächtigere Softwarekandidaten zurückgreifen werden.

Ubuntu Mate 19.10

Ubuntu Mate 19.10 hat am Mate-Desktop 1.22.2 zahlreiche kleinere Probleme beseitigt und neue Funktionen eingebaut. Spürbar angenehmer sind Größenänderungen von Programmfenstern, weil die Fensterecken zum Skalieren intern und unsichtbar vergrößert wurden. Ein neues Leistenapplet für Systemmeldungen erlaubt genaue Einstellungen über erwünschte und unerwünschte (abschaltbare) System- und Programminfos. Das „Notification Center” ist aktuell noch englischsprachig. Mit dem Tool Magnus gibt es eine neue Bildschirmlupe.
Die sehr nützliche, aber im Tool „Mate Tweak“ gut versteckte Option („Leiste“), das Leisten- und Desktoplayout mit einem Klick grundlegend umzustellen, ist jetzt ganz prominent in den „Willkommen“-Dialog gewandert. Die Option nennt sich „Schreibtischanordnung“ und lohnt in jedem Fall sorgfältige Auswahl.
Viele Mate-Themen wurden in die global genutzten Themen eingebaut, damit auch als Snap installierte Programme diese Themen nutzen können und sich optisch in den Gesamtdesktop integrieren. Gleichfalls aus optischen Gründen wurden zwei lange abonnierte Softwarekandidaten durch andere ersetzt: Statt Thunderbird kommt als Mailclient Evolution zum Einsatz und statt VLC der Player Gnome MPV. Beides sind Programme, die das grafische Toolkit GTK verwenden und sich mit Schriften und Klickelementen besser in den Mate-Desktop integrieren. Dabei räumen die Mate-Macher aber durchaus ein, dass der VLC der mächtigere Player ist, den der Nutzer natürlich jederzeit nachinstallieren kann.

Kubuntu 19.10 (KDE)

Kubuntu 19.10 mit KDE Plasma 5.16 zeigt kaum Veränderungen gegenüber dem direkten Vorgänger und verzichtet im Installer auch noch auf die neue ZFS-Unterstützung. Motiv für ein Upgrade liefern allenfalls einige aktualisierte KDE-Programme wie Kdenlive, Krita und Kdevelop. Der Einsatz des alternativen Fenstermanagers Wayland bleibt wie unter Gnome weiter experimentell.



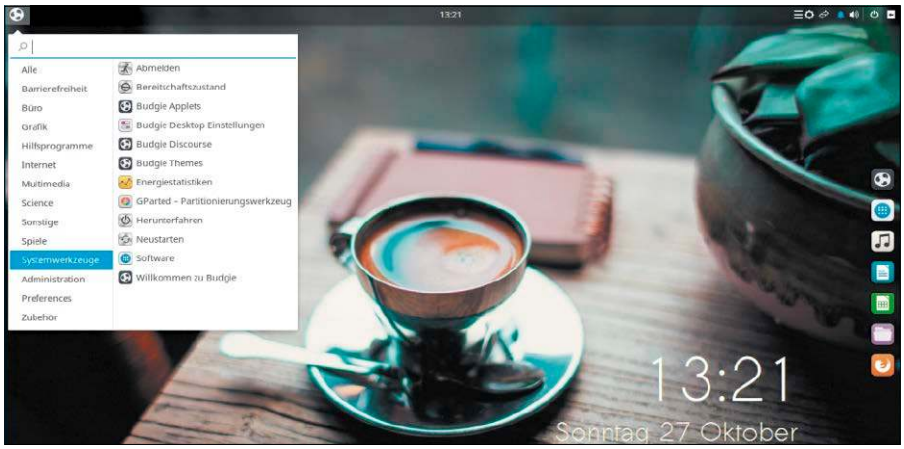
Die nützliche Funktion zum Umschalten des Leistenlayouts ging in Mate-Tweak etwas unter. Jetzt ist es zusätzlich und prominent mit Vorschaubildern im Welcome-Bildschirm integriert.

Lubuntu 19.10 (LXQT)

Lubuntu benutzt den unveränderten LXQT-Desktop 0.14.1 seines direkten Vorgängers und lässt – wie Kubuntu – die ZFS-Unterstützung im Installer vorerst vermissen. Hier gibt es also wie in Kubuntu lediglich einen frischeren Linux-Kernel und aktualisierte Programme.
Die LinuxWelt hat Lubuntu 19.10 dennoch in das Angebot der Heft-DVD aufgenommen, weil der erst jüngst vollzogene Wechsel von LXDE auf LXQT diese kleine Ubuntu-Edition erheblich aufgewertet hat. Eine kurze Lubuntu-Vorstellung finden Sie auf Seite 10.

Ubuntu Budgie 19.10

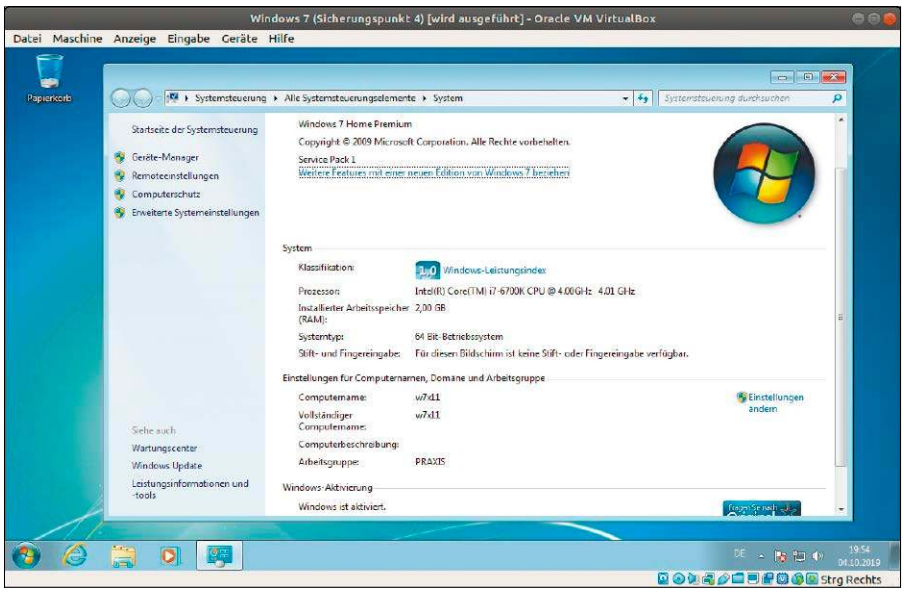
Diese Edition bleibt bei der Desktopversion Budgie 10.5 des Vorgängers, jedoch hat Budgie einige Verbesserungen vorzuweisen. So gewinnt die Desktopoberfläche jetzt Ordnerfunktionalität als Dateiablage und die Systemleiste erhält neue Applets wie einen Helligkeitsregler. Außerdem hat Budgie weiter an seinen Standardthemen Pocillo und Arc gefeilt, ohne seinen Fokus auf klare, kontrastive Optik aus den Augen zu verlieren. Bedientechnisch bleibt Budgie bei seinem Konzept mit Konfigurationszentralen statt intuitiver Kontextmenüs und ist damit ein – wenn auch schicker – Ubuntu-Exot. ■



Ubuntu Budgie 19.10: Die aufgeräumte Oberfläche hat ihre Anhänger. An der oft umständlichen Desktopkonfiguration über die Budgie-Zentralen hat sich aber nichts geändert.

Windows-7-System virtualisieren

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



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

VON THORSTEN EGGELING

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

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

1. Was das Ende des Supports bedeutet

Sobald Microsoft die Sicherheitsupdates einstellt, ist das System durch neu entdeckte Sicherheitslücken bedroht. Windows 7, 8 und 10 basieren teilweise auf demselben Quellcode, weshalb einige Sicherheitslücken wahrscheinlich in allen Systemen zu finden sind, bei Windows 7 jedoch nicht mehr behoben werden. Daher ist damit zu rechnen, dass Windows 7 ab Januar 2020 zum bevorzugten Ziel von Hackern wird. Das von Microsoft festgelegte Ende der

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

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

Nutzungsdauer bedeutet jedoch nicht das Ende der Nutzbarkeit. Windows 7 lässt sich auch nach dem 14. Januar 2020 starten, neu installieren und mit einem gültigen Produktschlüssel aktivieren.

Wenn Windows 7 ohne Verbindung zum Internet genutzt wird, darf dies als weitestgehend sicher gelten. Neu installierte Software muss allerdings sorgfältig geprüft werden und sollte nur aus vertrauenswürdigen Quellen stammen. Das Gleiche gilt für jede Art von Dateien, die Anwendungen unter Windows 7 öffnen und verarbeiten sollen. Programme wie PDF-Reader oder Office-Pakete sollte man solange wie möglich aktualisieren. Es ist jedoch damit zu rechnen, dass die meisten Softwarehersteller den Support für Windows 7 ebenfalls zeitnah einstellen werden.

2. Eingeschränkter Schutz durch Virtualisierung

Virtualisierungssoftware stellt einen virtuellen PC (virtuelle Maschine, VM) bereit, in dem sich ein weiteres Betriebssystem starten lässt. Sie können beispielsweise das installierte Linux nutzen (Hostsystem) und gleichzeitig bei Bedarf Windows 7 (Gastsystem) in einem Fenster oder auch im Vollbild starten.

Virtualisierungssoftware erlaubt keinen direkten Zugriff auf die PC-Hardware, mit Ausnahme von USB-Geräten. Die Gesamtleistung liegt daher etwas unterhalb eines herkömmlich installierten Systems auf dem gleichen PC und die virtuelle Grafikkarte eignet sich nur für Desktopanwendungen, aber nicht für aufwendige 3D-Spiele.

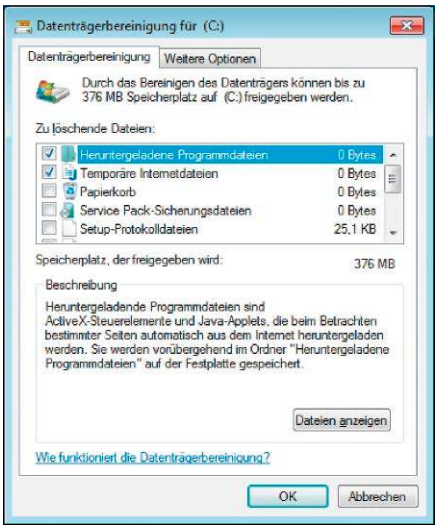
Ein mit Schadsoftware belastetes Windows kann jedoch eine Gefahr für das lokale Netzwerk darstellen. Über Freigaben können Viren andere Windows-PCs im Netzwerk infizieren. Das lässt sich vermeiden, indem Sie dem virtuellen PC nur Zugang zu schreibgeschützten Freigaben erlauben oder Daten auf einem anderen Weg austauschen (siehe Punkt 6).

3. Vorbereitungen für die Systemkopie

Der Transfer eines bestehenden Windows-Systems in eine virtuelle Maschine lässt sich deutlich beschleunigen, wenn Sie Windows vorher gründlich aufräumen. Löschen und deinstallieren Sie daher alles, was Sie nicht benötigen. Große Dateien verschieben Sie beispielsweise auf eine externe Festplatte. Nutzen Sie die Datenträgerbereinigung („cleanmgr.exe“), um überflüssige Dateien zu löschen.

Das Dateisystem sollte fehlerfrei und defragmentiert sein. Klicken Sie die Systemfestplatte im Windows-Explorer mit der rechten Maustaste an, wählen Sie „Eigenschaften“ und gehen Sie auf die Registerkarte „Tools“. Starten Sie die Fehlerüberprüfung und danach die Defragmentierung.

Windows-Tools: Damit Windows 7 in einer virtuellen Maschine startet, muss die Bootumgebung neu erstellt werden. Dafür benötigen Sie die ISO-Datei oder DVD des Installationsmediums von Windows 7. Ein Systemreparatur-Datenträger (Win-R, recdisc) funktioniert auch, muss aber unter einer Bios/MBR-Installation erstellt worden sein.



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

4. Windows-Partition mit Gparted kopieren

Die Festplatte mit der Windows-Partition muss in Virtualbox eingebunden werden. Das funktioniert jedoch nicht, wenn Linux von dieser Festplatte startet. In diesem Fall lesen Sie ab Punkt 5 weiter.

Schritt 1: Führen Sie die folgenden beiden Befehlszeilen aus:

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

Den Platzhalter „[User]“ ersetzen Sie durch Ihren Benutzernamen. Die Gruppenzugehörigkeiten ermöglichen den Zugriff auf Festplatten ohne administrative Rechte und auf USB-Geräte in Virtualbox. Danach starten Sie Linux neu.

Schritt 2: Öffnen Sie ein Terminal (Strg-Alt-T) und starten Sie

```
sudo parted -l
```

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

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

„/dev/sdb“ ersetzen Sie durch den zuvor ermittelten Laufwerkspfad. Sie erzeugen damit die virtuelle Festplatte „~/WinDisk.vmdk“, die auf das physikalische Laufwerk verweist.

Der Schritt kann entfallen, wenn Sie die Windows-Festplatte über einen SATA-USB-Adapter anschließen. Dafür muss das Oracle VM Virtualbox Extension Pack installiert sein (*www.virtualbox.org/wiki/Downloads*).

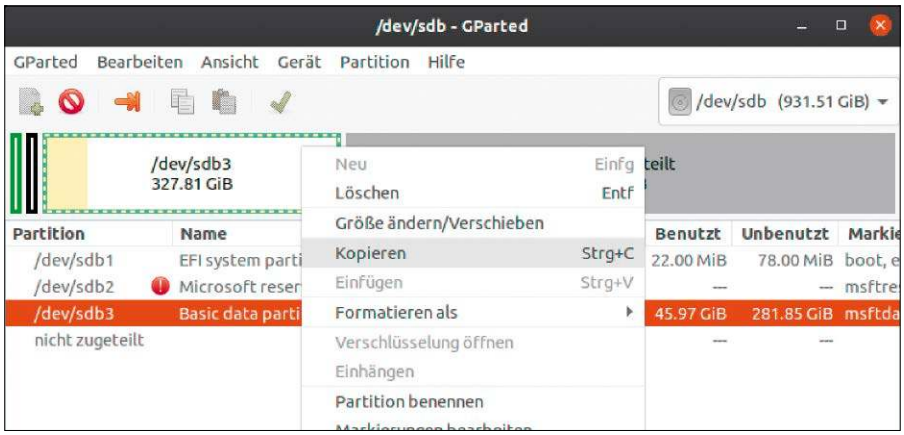
Schritt 3: Starten Sie Virtualbox und erstellen Sie eine neue VM für Windows 7. Erzeugen Sie über den Einrichtungsassistenten eine virtuelle Festplatte mit der

WINDOWS-BOOTUMGEBUNG REPARIEREN

Oft genügen die Computerreparatur-Optionen, um die Startumgebung von Windows 7 zu erzeugen. In manchen Fällen reicht das aber nicht aus. Booten Sie dann die virtuelle Maschine vom Windows-Installationsmedium und drücken Sie die Tastenkombination Umschalt-F10. In der Eingabeaufforderung geben Sie die folgenden vier Befehle ein:

```
bootrec /fixmbr
bootrec /fixboot
bootrec /rebuildbcd
bootsect /nt60 C: /mbr
```

Damit reparieren Sie die Bootumgebung und Windows 7 lässt sich danach in der virtuellen Maschine starten.



Windows umziehen: In einem Linux-Livesystem kopieren Sie mit Gparted die bisherige Windows-Partition und fügen diese in die virtuelle Festplatte ein.

Größe der bisherigen Windows-7-Partition oder größer.

Schritt 4: In den Einstellungen der virtuellem Maschine („Ändern“) gehen Sie auf „Massenspeicher“. Binden Sie als DVD-Laufwerk die ISO-Datei des Installationsmediums von Ubuntu 18.04 oder 19.10 (auf Heft-DVD) ein.

SATA-Festplatte: Klicken Sie „Controller: SATA“ mit der rechten Maustaste an, gehen Sie auf „Festplatte hinzufügen“ und klicken Sie auf „Vorhandene Festplatte auswählen“. Dann klicken Sie auf „Hinzufügen“, wählen die in Schritt 2 erstellte „vmdk“-Datei aus und bestätigen mit „Auswählen“ und „OK“.

USB-Festplatte: Bei einem USB-Laufwerk gehen Sie in der Navigation auf der linken Seite auf „USB“. Wählen Sie „USB-2.0-Controller (EHCI)“ oder „USB-3.0-Controller (xHCI), je nachdem, mit welchem USB-Port das Laufwerk verbunden ist. Klicken Sie auf die Schaltfläche mit dem „+“-Zeichen und wählen Sie das USB-Laufwerk. Klicken Sie auf „OK“, um die Änderungen zu speichern.

Schritt 5: Starten Sie die VM und darin das Ubuntu-Livesystem. Über „Aktivitäten“ suchen und starten Sie das Partitionierungstool Gparted. Das Auswahlfeld rechts oben zeigt zwei Festplatten: „/dev/sda“ ist die bisher leere virtuelle Festplatte und „/dev/sdb“ die bisherige Systemfestplatte.

Schritt 6: Wählen Sie „/dev/sda“, und gehen Sie im Menü auf „Gerät → Partitionstabelle erstellen“. Hinter „Neuen Partitionstabellentyp auswählen“ stellen Sie „msdos“ (MBR-Partitionstyp) ein und klicken auf „Anwenden“.

Es spielt keine Rolle, ob Windows 7 bisher auf einer Festplatte mit MBR-Partitionstyp installiert war oder GPT/Uefi verwendet. Da die Kombination Uefi/Windows 7 mit Virtualbox nicht funktioniert, muss Windows 7 in der VM im klassischen Bios/MBR-Modus starten.

Schritt 7: Wählen Sie „/dev/sdb“, klicken Sie die Windows-Partition mit der rechten Maustaste an und gehen Sie auf „Aushängen“. Danach wählen Sie im Kontextmenü „Kopieren“. Wechseln Sie zu „/dev/sda“, klicken Sie mit der rechten Maustaste in das Fenster, gehen Sie auf „Einfügen“ und klicken Sie auf die Schaltfläche „Einfügen“. Gehen Sie im Menü auf „Bearbeiten → Alle Vorgänge ausführen“ und bestätigen Sie mit „Anwenden“.

Nach Abschluss des Kopiervorgangs wählen Sie im Kontextmenü der eingefügten Partition „Markierung bearbeiten“, setzen ein Häkchen vor „boot“ und klicken auf „Schließen“. Fahren Sie das virtuelle System herunter.

Schritt 8: Im Hauptfenster „Oracle VM Virtualbox Manager“ klicken Sie auf „Ändern“ und ersetzen unter „Massenspeicher“ die ISO-Datei des Linux-Livesystems durch die ISO-Datei des Windows-7-Installationsmediums oder des Systemreparatur-Datenträgers. Über das CD/DVD-Icon lässt sich auch eine DVD im Laufwerk auswählen. Die in Schritt 4 hinzugefügte „vmdk“-Datei entfernen Sie aus der Konfiguration oder Sie deaktivieren unter „USB“ den Filter für USB-Geräte.

Schritt 9: Booten Sie das Windows-Installationssystem in der virtuellen Maschine. Klicken Sie auf „Weiter“ und dann auf „Computerreparaturoptionen“. Sobald Windows die Installation gefunden hat, klicken Sie auf „Reparieren und neu starten“. Sollte Windows 7 danach nicht booten, rufen Sie erneut die „Computerreparaturoptionen“ auf. Diesmal klicken Sie auf „Weiter“, dann auf „Systemstartreparatur“, „Fertig stellen“ und „Neu starten“. In einigen Fällen reicht das nicht aus, um Windows 7 zum Start zu überreden. Was Sie dann unternehmen müssen, lesen Sie im Kasten „Windows-Bootumgebung reparieren“.

5. P2V von Windows 7 über ein Backup

Sollten sich Windows 7 und Linux zusammen auf einer Festplatte befinden, erstellen Sie unter Linux ein Windows-Backup auf Dateisystemebene, das Sie danach auf die virtuelle Festplatte zurücksichern.

Installieren Sie unter Linux folgendermaßen zwei zusätzliche Pakete:

```
sudo apt install openssh-server
  wimtools
```

Der SSH-Server ermöglicht dem Gastsystem den Zugriff über das Netzwerk auf den Host und das Paket „wimtools“ enthält Programme, die sich für ein Windows-Backup unter Linux nutzen lassen.

Schritt 1: Ermitteln Sie über

```
sudo parted -l
```

den Gerätepfad der Windows-Installation, beispielsweise „/dev/sda3“. Sollte die Partition eingehängt sein, hängen Sie sie mit

```
te@Z77X: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
te@Z77X:~$ mkdir ~/Backup
te@Z77X:~$ wimcapture /dev/sda3 ~/Backup/windows7.wim "Windows 7"

Capturing WIM image from NTFS filesystem on "/dev/sda3"
Scanning "/dev/sda3"
171 MiB scanned (773 files, 123 directories)
Excluding "/$Recycle.Bin" from capture

Excluding "/hiberfil.sys" from capture

Excluding "/pagefile.sys" from capture
1244 MiB scanned (2954 files, 502 directories)
Excluding "/System Volume Information" from capture
15 GiB scanned (107668 files, 19681 directories)
Using LZX compression with 8 threads
Archiving file data: 5 GiB of 15 GiB (34%) done
```

Windows kopieren: Wimcapture erstellt ein platzsparendes Windows-Backup in einer WIM-Datei. In der virtuellen Maschine sichern Sie es dann auf die virtuelle Festplatte zurück.

```
sudo umount /dev/sda3
```

aus.

Schritt 2: Um das Backup zu erstellen, führen Sie die folgenden zwei Befehlszeilen aus:

```
mkdir ~/Backup
wimcapture /dev/sda3 ~/Backup/
  windows7.wim "Windows 7"
```

Im Ordner „Backup“ liegt danach die „wim“-Datei mit dem kompletten Systemabbild.

Schritt 3: Bereiten Sie eine virtuelle Maschine für Windows 7 vor. Erzeugen Sie über den Einrichtungsassistenten eine virtuelle Festplatte mit der Größe der bisherigen Windows-7-Partition oder größer. Binden Sie unter „Massenspeicher“ das ISO-Abbild einer Linux-Live-DVD ein, so etwa Ubuntu 19.10 (auf Heft-DVD). Unter „Netzwerk“ wählen Sie hinter „Angeschlossen an:“ den Eintrag „Netzwerkbrücke“, damit das Gastsystem Zugang zum lokalen Netzwerk erhält.

Schritt 4: Booten Sie das Linux-Livesystem in der virtuellen Maschine. Mit Hilfe von Gparted erstellen Sie auf „/dev/sda“ eine MS-DOS-Partition (siehe Punkt 4), die Sie mit dem Dateisystem NTFS formatieren. Setzen Sie über „Markierung bearbeiten“ die Option „boot“, damit die Partition aktiv und bootfähig ist.

Schritt 5: Führen Sie im Livesystem im Terminal die folgenden zwei Befehle aus:

```
sudo add-apt-repository universe
sudo apt install wimtools sshfs
```

Mit der Zeile

```
sudo sshfs -o allow_other [User]@
  [IP]:/home/[User]/Backup /mnt
```

hängen Sie den Backupordner aus Schritt 2 unter „/mnt“ in das Dateisystem ein. Den Platzhalter „[User]“ ersetzen Sie jeweils durch Ihren Benutzernamen, „[IP]“ ist die IP-Adresse oder der Name des Hostsystems.

Schritt 6: Kopieren Sie den Inhalt der „wim“-Datei auf die virtuelle Festplatte:

```
sudo wimapply /mnt/install.wim 1 /
  dev/sda1
```

Danach erstellen Sie die Windows-Bootumgebung, wie in Punkt 4 in den Schritten 8 und 9 beschrieben.

6. Windows 7 optimieren und absichern

Die Leistung eines virtuellen PCs lässt sich über die Gasterweiterungen verbessern, die Treiber etwa für die Maus und den virtuellen Grafikadapter enthalten. Zur Installation gehen Sie auf „Geräte → Gasterweiterungen einlegen“, öffnen im virtualisierten System das DVD-Laufwerk im Windows-Explorer und rufen das Programm

```
VBoxWindowsAdditions.exe
```

Auf. Folgen Sie den Anweisungen des Installationsassistenten und starten Sie Windows danach neu. Im Gastsystem stehen jetzt weitere Funktionen zur Verfügung. Der Windows-Desktop wird automatisch an die Größe des Fensters angepasst und der Mauszeiger löst sich automatisch, wenn Sie ihn aus dem Fenster ziehen.

Datenaustausch: Verwenden Sie im virtualisierten Windows 7 einen gemeinsamen Ordner mit dem Hostsystem. Das ist sicherer als der Zugang zu Netzwerkfreigaben.

Netzwerk und Datenaustausch: Eine virtuelle Maschine ist bei der Standardkonfiguration „NAT“ vom lokalen Netzwerk getrennt, hat aber Zugang zum Internet. Wenn Sie den virtuellen Netzwerkadapter als „Netzwerkbrücke“ konfigurieren, erscheint die VM auch im lokalen Netzwerk – das ist aus Sicherheitsgründen für Windows 7 nicht zu empfehlen.

Zur Datenübertragung zwischen Host- und Gastsystem verwenden Sie besser einen gemeinsamen Ordner. Gehen Sie im Fenster der virtuellen Maschine auf „Geräte → Gemeinsame Ordner → Gemeinsame Ordner“. Über die „+“-Schaltfläche bestimmen Sie einen Ordner für den Datenaustausch auf dem Hostsystem. Setzen Sie Häkchen vor „Automatisch einbinden“ und „Permanent erzeugen“. Unter Windows 7 erreichen Sie den Ordner im Windows-Explorer über „Netzwerk“ und „Vboxsrv“ oder den Laufwerksbuchstaben „Z:“

Im Fenster der virtuellen Maschine können Sie zwei weitere Optionen für den Datenaustausch aktivieren: „Geräte → Gemeinsame Zwischenablage → bidirektional“ und „Geräte → Drag und Drop → bidirektional“. Wenn Sie im Hostsystem beispielsweise einen Textabschnitt mit Strg-C kopieren, lässt er sich im Gastsystem in einem Editor mit Strg-V einfügen. Drag & Drop funktioniert bei Windows 7 nur in eine Richtung, etwa vom Linux-Dateimanager auf den Windows-Desktop. ■

WINDOWS IN DER VM AKTIVIEREN

Nach dem Umzug oder einer Neuinstallation in einer virtuellen Maschine läuft Windows 7 auf neuer Hardware. Die Aktivierung stellt in der Regel kein Problem dar und kann in der Systemsteuerung über „System → Windows aktivieren“ umstandslos erfolgen. Nach unseren Erfahrungen funktioniert die Aktivierung mit Produktschlüsseln der Vollversion sowie mit OEM/SB-Schlüsseln. Sollte das fehlschlagen, nutzen Sie die telefonische Aktivierung.

VMs lassen sich klonen oder auf andere Rechner kopieren. Solange die virtuelle Hardware sich nicht wesentlich verändert, bleibt die Aktivierung unabhängig vom jeweils genutzten PC erhalten. Wenn Sie nur eine Windows-7-Lizenz besitzen, dürfen Sie das System aber nur in der virtuellen Maschine starten und das bisher auf der Festplatte installierte System nicht gleichzeitig verwenden.

Noch 2019: Linux Mint 19.3

Nachdem die letzte Version von Linux Mint wegen Schwierigkeiten im Entwicklungsprozess um den Compositor und Window-Manager „Muffin“ etwas auf sich warten ließ, ist Linux Mint 19.3 trotz vieler Änderungen wieder auf Kurs. Die kommende Mint-Ausgabe wird auf Ubuntu 18.04.3 basieren, hat den Codenamen „Tricia“ bekommen und soll noch im Dezember erscheinen. Das .NET-Framework „Mono“ soll komplett getilgt werden, es gibt einen neuen Videoplayer namens „Celluloid“ und das Mint-Team wird ein neues Logo vorstellen. Die XFCE-Ausgabe wird das neue XFCE 4.14 mitbringen. ■

Internet Archive: 2500 freie DOS-Spiele

Das Internet Archive ist ein in San Francisco ansässiger gemeinnütziger Verein, der eine freie Bibliothek digitaler Werke pflegt. Auch die „Wayback Machine“, die alte Versionen großer Webseiten archiviert, wird von diesem Verein betrieben. Nun hat das Archiv 2500 DOS-Spiele aus den 90er-Jahren in die Bibliothek aufgenommen, die sich online in modernen Browsern in einem Emulator spielen lassen, der Webassemply nutzt. Unter anderem ist der Titel „Alone in the dark“ vertreten, Sierra-Spiele und viele Adventures von SSI. Die Übersicht findet sich auf *https://archive.org/details/softwarelibrary_msdos_games*. ■

Mozilla: Offlineübersetzer geplant

Der Browser Firefox soll eine Übersetzungsfunktion erhalten, die anders als die Dienste von Google und Bing auch offline funktionieren soll. Anstatt Clouddienste zur Übersetzung will Mozilla auf Deep-Learning-Algorithmen bauen, die komplett clientseitig im Browser laufen. Diese Entwicklung plante Mozilla schon länger, konnte das Projekt aber mangels Finanzierung nicht umsetzen. Nun hat sich die EU mit 3,35 Millionen US-Dollar an dem Projekt beteiligt, das unter einer Open-Source-Lizenz stehen wird. ■

Alle News von David Wolski

Kernel 5.4: exFAT und Sicherheitsmodule

Zum Redaktionsschluss war Kernel 5.4 noch nicht fertig, aber die Neuerungen sind bereits absehbar: Es wird einen offiziellen exFAT-Treiber geben sowie Sicherheitsmodule gegen Manipulationen durch den root-Account.

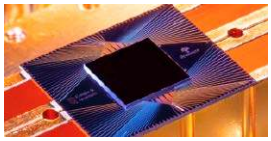
Linus Torvalds hat die Freigabe des neuen Kernels Ende November oder in der ersten Dezemberwoche angepeilt. Damit bleibt die Kernel-Entwicklung trotz nicht gerade kleiner Neuaufnahmen im Quellcode bei einer zweimonatlichen Frequenz. Eine Ergänzung, die Desktopnutzer freuen wird, ist die Aufnahme eines offiziellen Treibers für Microsofts Dateisystem exFAT, mit dem etliche Digitalkameras arbeiten. Bislang mussten sich Linux-Anwender mit einem externen Fuse-Modul behelfen. Bemerkenswert ist, dass die Neuaufnahme des exFAT-Treibers von Microsoft selbst vorangetrieben wurde, was einem Verzicht auf das Patent gleichkommt.

Der Kernel 5.4 zieht eine weitere Verteidigungslinie um den Kernel, um diesen mit „Lock-down“-Modulen vor Manipulationen und Neukonfigurierung zu schützen, auch wenn der root-Account das durchführen sollte. Diese Module können damit auch das Auslesen von Kernel-Informationen und Leistungsparametern unterbinden, die als vertraulich gelten können. Die neuen optionalen Sicherheitsfunktionen wurden lange kontrovers diskutiert, weil sie nicht nur IT-Abteilungen, sondern auch Hardwareherstellern eine einfachere Möglichkeit bieten, ein Linux-System signifikant zu vernageln. Wer sich aber nach günstigen oder besonders ausdauernden Linux-Notebooks mit ARM-Prozessor sehnt, darf sich auf die nächsten Kernel-Versionen freuen, denn mit Kernel 5.3 bekommt der Qualcomm Snapdragon 835 bessere Unterstützung und damit solche Notebooks wie das Asus Novago, HP Envyx2 und das Lenovo Miix 630. Die nächste Snapdragon-Generation 855 erhält auch die ersten Ergänzungen im Kernel. Den Intel-Prozessoren vom Typ Icelake die AMD-CPUs der Epyc-Serie und dem Ryzen 3000 entlockt der Kernel neue Funktionen. Bei den Dateisystemen fallen Ergänzungen der nativen Verschlüsselung von F2FS und EXT4 ins Auge, die vor allem von Google für Android-Geräte vorangetrieben werden. ■

Micron: Superschnelle Server-SSDs

Die derzeit schnellste Solid State HD stammt von Micron: Mit Transferraten bis zu neun GB pro Sekunde ist die Micron X100 SSD um den Faktor drei schneller als die bisher schnellsten SSDs. Die Latenz könnte ebenfalls neue Maßstäbe setzen: Bei gleichmäßigen Lese- und Schreibvorgängen liegt die Verzögerung unter acht Mikrosekunden. Andere NAND-SSDs würden laut Micron eine um den Faktor elf größere Latenz vorweisen. Das Speichermedium eignet sich laut Hersteller besonders für Big-Data-Anwendungen und Storageserver mit zeitkritischen Transaktionen. Die SSDs sind vornehmlich für Rechenzentren gedacht und bisher nur über ein Partnerprogramm zu haben. Angaben zum Preis machte Micron noch nicht. ■

Google: Erfolg mit Quantencomputer



Quelle: Google LLC

Das Prinzip des Quantenrechners ist schon länger bekannt. Man braucht, um ihn sinnvoll einsetzen zu können, gewissermaßen auch passende Probleme mit speziellen Eigenschaften: Ein Durchbruch ist Ingenieuren bei Google gelungen, die mit einem Quantencomputer in 200 Sekunden eine speziell formulierte Aufgabe gelöst haben, für die der derzeit schnellste Supercomputer angeblich 10 000 Jahre bräuchte. Konkret hat das Forscherteam damit die sogenannte „Quantenüberlegenheit" (Quantum Supremacy) gegenüber digitalen Computern belegt. Es gibt aber bereits Kritik und sogar Zweifel an den Forschungsergebnissen: John Preskill, Physiker am Caltech-Institut der Universität Kaliforniens und Schöpfer des Begriffs „Quantenüberlegenheit", kritisiert die sehr unscharf formulierte Aufgabe, deren Lösung nicht mal aufschlussreiche Ergebnisse liefere. Wissenschaftler von IBM zweifeln die Ergebnisse an und stellen die These auf, dass ein herkömmlicher Superrechner die gleiche Aufgabe innerhalb von zwei Tagen mit höherer Genauigkeit bewältigten könnte. Einig ist sich die Wissenschaft aber, dass Google einen wichtigen Schritt getan hat, Quantencomputer besser zu verstehen und zu kontrollieren. Der nächste Schritt, ein wirklich „nützliches Problem" zu lösen, liegt aber in weiter Ferne. ■

SICHERHEITSNEWS

DWLAN: Leidige Linux-Lücke

Der Treiber des Linux-Kernels für WLAN-Chips von Realtek kann einen Pufferüberlauf auslösen und Systeme zum Absturz bringen. Schlimmstenfalls ließe sich sogar ausführbarer Code einschleusen, so der Entdecker der Lücke, der diese gegen jede Netiquette auf Twitter veröffentlichte. Die Lücke war im Kernel-Code schnell gepatcht und Linux-Distributionen sind bereits mit Aktualisierungen versorgt. Die größere Gefahr sind jedoch Android-Geräte und Router, die beispielsweise mit Open WRT arbeiten. Auch diese Geräte sind Opfer des Bugs, falls der WLAN-Chip von Realtek stammt.

Verwundbar: Nginx mit PHP-FPM

In PHP gibt es immer wieder drastische Sicherheitslücken. Die im Oktober bekannt gewordene Lücke kam bei einem Hackingwettbewerb ans Licht und betrifft nur die Kombination des Webservers Nginx mit der PHP-FPM-Runtime. Dies ist keine seltene Kombination und wird etwa von Nextcloud aufgrund der guten Leistung empfohlen. Die Schwachstelle CVE-2019-11043 erlaubt das Ausführen von Code auf verwundbaren Servern. Beispielcode ist auf Github zu haben und führte zu massenhaften Angriffen auf Server. Ab den PHP-Versionen 7.3.11 und 7.2.24 ist die Lücke geschlossen.

Thunderbird: Eigene GPG-Funktion kommt

Für die sicher verschlüsselte Korrespondenz mit GPG/PGP ist Thunderbird bisher auf die Erweiterung Enigmail angewiesen. Ab 2020 soll Thunderbird GPG/PGP nativ beherrschen, denn wie Firefox wird auch Thunderbird die von Enigmail genutzte Erweiterungsschnittstelle gegen die neuen „Webextensions" austauschen. Der Austausch wird ab Thunderbird 68 erfolgen und damit wird diese Version auch die letzte sein, die Enigmail unterstützt.

Chrome/Chromium: Aus für gemischte Inhalte

Noch laden die Google-Browser gemischte Inhalte von Webseiten, also einen Mix an Ressourcen, die von unverschlüsselten HTTP- und verschlüsselten HTTPS-Ressourcen stammen. Gemischte Inhalte erlauben aber Angriffe durch Cross-Site-Scripting, das eine Webseite dazu bringt, weitere Ressourcen von fremden URLs zu laden. Bisher blockieren Chrome/Chromium bereits Scripts und iFrames. Ab Chrome 80 werden Audio- und Videodateien blockiert, die auf einer HTTPS-Seite nur per HTTP verfügbar sind. Chrome 81 wird dann auch Bilder blockieren, auf die das zutrifft.

Sudo: Bug erlaubt root-Recht

Ausgerechnet im allseits geschätzten Sicherheitstool Sudo zum Delegieren von root-Rechten fand sich ein Bug, der im schlimmsten Fall die Ausweitung von Benutzerrechten erlaubt. Damit der Fehler fatal wird, ist aber eine sehr ungewöhnliche Konfiguration nötig: Dazu muss in der „sudoers"-Datei ein Nutzer definiert sein, der mit den Rechten aller anderen Konten Befehle ausführen darf, nur nicht als root. Diese Konfiguration verlangt nach dem Statement „!root". Mit Version 1.8.28 hat Sudo den Fehler beseitigt.

Geminilake: Fehler in Intel-CPU

Das Entwicklerteam von Google Chrome hat in Intels CPU-Architektur Geminilake einen Bug entdeckt, der diverse Browser zum Absturz bringt. Der Bug wurde mit hoher Wahrscheinlichkeit nachträglich durch Microcode-Update lebendig. Geminilake ist in der Intel-Modellserie der Nachfolger von Apollolake und umfasst Celeron- und Pentium-Silver-CPUs, die seit 2017 in vielen Notebooks arbeiten. Eine vorübergehende Lösung sei es laut Google, auf den betroffenen Rechnern die 32-Bit-Pakete der Browser zu verwenden.

Apps: Torheiten mit TOR

Viele Android-Anwender nutzen unbemerkt das TOR-Netzwerk und setzen sich damit dem Risiko der Spionage aus, wie Sicherheitsforscher demonstrierten. Der Grund: Viele Apps nutzen TOR zur Übermittlung von Daten, da deren App-Entwickler davon ausgehen, dies sei ein Ersatz für ein VPN. Tatsächlich aber können Exit-Nodes den unverschlüsselten Datenverkehr mitschneiden. Die Sicherheitsforscher zeigten mit selbst aufgesetzten Exit-Nodes die unverschlüsselten persönlichen Daten wie GPS-Koordinaten, Adressen, Tastatureingaben von Millionen von Nutzern diverser Apps. Schätzungsweise übertragen 30 Prozent aller Android-Geräte aufgrund schlecht programmierter Apps Daten über TOR. Unter iOS ist das Problem geringer, tritt jedoch auch auf. Es fehlt generell an Aufklärung, dass das TOR-Netzwerk kein VPN ersetzt, sondern nur die Absender von Daten anonymisiert.

UPDATETELEGRAMM

Fedora 31

Knapp nicht mehr auf Heft-DVD: Fedora 31 erschien Ende Oktober mit fast schon traditioneller Verspätung. Die Distribution gilt als Vorzeige-System für Wayland und den Gnome-Desktop, der hier in der Gnome 3.34 ohne Veränderungen enthalten ist. Der Kernel ist bei Version 5.3 angekommen und wird voraussichtlich auch noch auf Version 5.4 aktualisiert. Das System wird auf der nächsten Heft-DVD liegen (*https://getfedora.org*).

Tails 4.0

Das Livesystem mit vorkonfiguriertem TOR-Client zur sicheren Teilnahme am anonymisierenden TOR-Netzwerk wurde aus den Paketquellen von Debian 10 „Buster“ neu gebaut. Die Aktualisierungen umfassen auch den Desktop, bei dem es sich um Gnome 3.30 handelt. Der TOR-Browser ist in Version 9.0 enthalten (*https://tails.boum.org*).

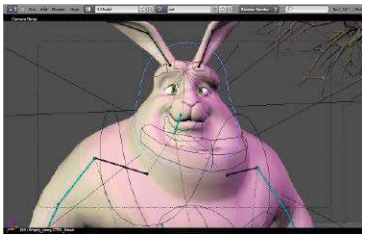
Jack Audio Server 1.9.13

Nach zwei Jahren Entwicklungszeit steht der Jack Audio Server, der mit seiner geringen Latenz professionelle Ansprüche der Studiotechnik bedient, in neuer Version bereit. Dieser Ersatz für Pulse Audio und Alsa stellt Verbindungen von Audio- und Midi-Daten zwischen Anwendungen und Hardware in Echtzeit her. Die neue Version versteht sich besser mit Systemd und hat eine neue Daten-API für Lizenzinformationen erhalten (*https://jackaudio.org*).

MPV 0.30

Der MPV Videoplayer erhielt in den letzten Jahren neben VLC viel Aufmerksamkeit, weil er sich mit weniger Systemressourcen begnügt. Zur Ausgabe nutzt MPV die Schnittstellen Open GL oder Vulkan, falls vorhanden, und holt damit mit Hardwarebeschleunigung das Optimum aus einem System. MPV selbst hat keine grafische Oberfläche, sondern nur minimale Steuerelemente (*https://mpv.io*).

Nvidia, Adidas und AMD: Alle für Blender



Die Blender-Foundation hat genügend Unterstützer gefunden, um die Entwicklung des 3D-Modellers und Renderers mit festangestellten Programmierern erheblich voranzubringen. Vor zwei Monaten hat Epic Games mit einer einmaligen Spende von 1,2 Millionen US-Dollar die Blender-Entwickler unterstützt. Jetzt folgen Nvidia, Adidas, AMD und Embark Studios als weitere Unterstützer. Blender erschien vor 16 Jahren erstmals unter einer freien Lizenz und ist heute das wichtigste Open-Source-Programm in seiner Sparte. Die Software ist nicht nur für eine große Anwenderbasis der Einstieg in die Thematik 3D-Modelling, CAD-Visualisierung und Rendering, sondern wird seit vielen Jahren von professionellen Studios eingesetzt (siehe auch ab Seite 66). ■

KDE-Connect für Windows

Die ursprünglich für KDE entwickelte Komponente, welche Android mit dem Desktop-PC über WLAN verknüpft, setzt ihren Siegeszug fort. KDE Connect erlaubt per App den Austausch von Dateien, Zwischenablage und die Anbindung von Android-Geräten zur Mediensteuerung und sogar als Eingabegerät. Von KDE kam die Komponente zunächst auf andere Linux-Desktops, dann auf Mac-OS X und jetzt sogar zu Windows. Noch gilt KDE Connect für Windows als Alphaversion, aber eine EXE-Datei steht für unkomplizierte Tests bereits zum Download bereit (*https://binary-factory.kde.org/view/Windows%2064-bit/job/kdeconnect-kde_Nightly_win64*, 78 MB, für Windows 10, 64 Bit). ■

Ubuntu 20.04 wird ein Raubtier

Quelle: „kellinahandbasket“, Lizenz: CC BY 2.0 (http://bit.ly/1QbME0k)

Kaum war Ubuntu 19.10 „Eoan Ermine“ veröffentlicht, begann auch schon die Entwicklungsphase der kommenden Version. Ubuntu 20.04 wird eine Ausgabe mit Langzeitunterstützung. Wie auf der Entwickler-Mailingliste bekanntgegeben wurde, bekommt Ubuntu 20.04 den Codenamen „Focal Fossa“. Das Fossa ist ein katzenähnliches Raubtier, auch „Frettkatze“ genannt, die auf Madagaskar vorkommt und eine bedrohte Tierart ist. Im Fokus wird bis zum geplanten Veröffentlichungstermin im April 2020 die Einbindung von Gnome 3.36 stehen, außerdem sollten Kernel 5.5 und PHP 7 bis dahin fertig sein. ■

50 Jahre Internet

Nicht nur Unix begeht dieses Jahr sein fünfzigjähriges Jubiläum, auch das Internet wird ein halbes Jahrhundert alt, sofern man den Vorläufer „Arpanet“ und dessen Nachfolger „Darpanet“ hinzuzählt. Am 29. Oktober 1969 loggte sich zum ersten Mal ein Student an der UCLA in einen Rechner am Hunderte Kilometer entfernten Stanford Research Institut ein. Aus diesem Netzwerk, das mit Paketvermittlung arbeitete und ursprünglich im Auftrag der US Air Force entstand, wurde nach 20 Jahren das öffentliche und teilkommerzielle Internet. ■

Streaming: Disney+ mag kein Linux

Der neue Streamingdienst Disney+ läuft wegen der sehr restriktiven DRM-Vorgaben nicht in Browsern unter Linux, wie Fedora-Entwickler vorab festgestellt haben. Zwar nutzt Disney+ wie die Konkurrenz von Netflix und Amazon auch das Widevine-Plug-in für das Rechtemanagement und als Kopierschutz, allerdings mit der höchsten von drei möglichen Sicherheitsstufen. Die höchste Stufe geht zu Lasten der Kompatibilität und wird auf vielen Endgeräten und einigen Betriebssystemen nicht funktionieren, unter anderem nicht auf Desktop-Linux. ■

Systemd: Konzepte für „Home“

Lennart Poettering, der maßgebliche Entwickler hinter dem Soundserver Pulse Audio und dem Init-System Systemd, hat in einer Präsentation eine mögliche Zukunft für die Verwaltung des Home-Verzeichnisses auf Linux-System formuliert. Unter dem Projektnamen „Systemd-Homed“ sollen Home-Verzeichnisse zu einer verschlüsselten portablen Containerdatei werden, die per Systemd eingebunden wird. Besonders IT-Manager und Admins werden sich für die Netzwerkfähigkeit dieser Lösung begeistern können. Systemd-Homed wird Home-Verzeichnisse von einem Server im Netzwerk beziehen können – im Stile eines Active-Directory-Servers. Dies soll nicht lange Theorie bleiben: Im aktuellen Entwicklungszyklus bekommt Systemd (Version 244) bereits erste Ergänzungen im Code. ■

Cent-OS: Es rollt!

Mit Cent-OS Stream hat Red Hat eine neue Linux-Distribution ins Leben gerufen, die als Rolling Release gepflegt werden kann, also fortwährend mit frischen Paketen versorgt wird. Bisher war Cent-OS als Klon von Red Hat Enterprise Linux vor allem auf Stabilität und lange Unterstützungszeiträume von bis zu zehn Jahren getrimmt. Dies brachte aber das Dilemma von alten Paketversionen mit sich, was bei Serverprogrammen und Rahmenwerken wie Node.JS und PHP nicht für jeden Einsatzzweck optimal ist. Server-Admins mussten hier oft auf das inoffizielle EPEL-Repository ausweichen, um in der Entwicklung mitzuhalten. Mit Cent-OS Stream wird es einfacher, frischere Pakete aus offiziellen Quellen zu installieren. Ein Ersatz für Fedora, das als Distribution als Trendsetter für Desktopanwender und experimentelle Server aufgestellt ist, wird Cent-OS Stream aber nicht sein. ■

Canonical: Zahlen, bitte!

Lubuntu ist als Distribution im Herbst 15 Jahre alt geworden. Die Entwicklerfirma Canonical hat mit der Veröffentlichung von Ubuntu 19.10 auch ihren Geschäftsbericht abgegeben. Aus dem Bericht geht hervor, dass Canonical nun 437 Angestellte beschäftigt, zehn mehr als im Jahr zuvor. Der Umsatz ist um vier Millionen US-Dollar auf 99 Millionen US-Dollar gestiegen, aber es bleibt ein operativer Verlust von neun Millionen US-Dollar. Das ist immerhin eine Verringerung des Verlusts um 14 Millionen US-Dollar zum Vorjahr. Canonical benötigt also weiterhin finanzielle Zuwendung durch seinen Gründer, den südafrikanischen Multimillionär Mark Shuttleworth. ■

UPDATETELEGRAMM

Firefox 70

Die zweimonatlichen Firefox-Updates verdienen wegen ihrer Häufigkeit eigentlich keine Erwähnung. Version 70 ist aber eine eindrucksvolle Version mit interessanten neuen Funktionen: Es gibt eine neue Sicherheitsübersicht zu HTTP-Seiten und einen Privatsphärenbericht, der auf Wunsch über die geblockten Tracker aufklärt. Außerdem gibt es einen neuen Manager für gespeicherte Zugangsdaten, der nun nicht mehr als Dialog erscheint, sondern in das Browserfenster integriert ist. Ein neues Logo gibt es auch (*www.mozilla.org/de/firefox/new*).

Free CAD 0.18.4

Das freie 3D-CAD-Programm fußt auf dem Rahmenwerk von Open Cascade, das seit 2013 Open-Source-Software ist. CAD-Programme für Linux sind rar, denn der Entwicklungsaufwand für Software dieser Art ist hoch. Deshalb verdient Free CAD immer eine Erwähnung, wenn eine neue Version vorliegt. Free CAD 0.18.4 behebt Fehler und verbessert die Berechnung von Bohr- und Schneidegeschwindigkeit für bekannte Materialien (*www.freecadweb.org*).

Ubuntu Touch OTA-11

Ubuntu Touch hält sich stabil als Gemeinschaftsprojekt und kommt sogar regelmäßig auf neue Versionen, die Ubuntu-Touch-Geräte direkt Over The Air (OTA) einspielen können. Ubuntu Touch OTA-11 basiert auf Ubuntu 16.04, behebt Probleme mit der Bildschirmtastatur und verbessert den Webbrowser Morph, der auf der Qt-Webengine von KDE aufbaut (*https://ubuntu-touch.io*).

Ubuntu 18.04.4

Die nach wie vor gültige Langzeitversion 18.04 LTS erhält Anfang Februar ihre vierte Erneuerung durch Release Point 18.04.4. Ähnlich den „Service Packs“ unter Windows fasst dieser Schritt alle bislang erschienenen Updates zusammen, bringt aber zusätzlich mit einem Kernel-Update das System auf den neuesten Treiberstand.

Toolbox für Ubuntu & Mint

Linux-Systeme bieten direkt nach der Installation eine umfangreiche Softwareausstattung. Weitere nützliche Programme empfehlen die nachfolgenden Artikel und bieten dazu mit der LinuxWelt-Toolbox ein komfortables Werkzeug.

VON THORSTEN EGGELING

Software lässt sich unter Linux schnell und sicher aus dem Software-Repositorium der jeweiligen Distribution installieren. Wer eine aktuellere Version oder spezielle Programme benötigt, kann in Ubuntu oder Linux Mint auch PPAs (Personal Package Archive) einbinden. DEB-Pakete für die bequeme Installation gibt es bei Bedarf auch auf den Webseiten von Softwareherstellern. Eine bequeme Alternative sind Containerformate wie Snap-Apps, Flatpak und Appimage.

Es ist allerdings eine Herausforderung, im unüberschaubaren Angebot das passende Tool für einen bestimmten Zweck zu finden. Oft gibt es mehrere Programme für die jeweilige Aufgabe, aber nicht jedes davon kann auch alle Ansprüche erfüllen. Auf den folgenden Seiten finden Sie daher die Beschreibungen nützlicher Anwendungen und Tools sowie Tipps zu deren Verwendung. Für die komfortable Installation haben wir das Programm LinuxWelt-Toolbox (auf Heft-DVD) erstellt. Hier finden Sie ausführliche Anleitungen und Internetlinks sowie Befehlszeilen oder Schaltflächen für die schnelle Installation. Die meisten Einträge beziehen sich auf Ubuntu und Linux Mint und gelten größtenteils auch für verwandte Systeme wie Debian.

1. Die LinuxWelt-Toolbox installieren

Die LinuxWelt-Toolbox erleichtert die Installation der in diesem und den sechs folgenden Artikeln genannten Programme. Entpacken Sie das Tool von der Heft-DVD aus dem

Bequeme Installationen: Die LinuxWelt-Toolbox zeigt Programmbeschreibungen und Infolinks. Für die Installation oder den Start der gewünschten Software genügt oft ein Mausklick.

Ordner „Software“ in das Home-Verzeichnis. Im Verzeichnis „LinuxWelt-Toolbox“ finden Sie die Datei „lwToolbox_x86_64“ für 64-Bit-Systeme, die Sie per Doppelklick starten. Nutzer eines 32-Bit-Systems verwenden „lwToolbox_i386“, für den Raspberry Pi eignet sich „lwToolbox_arm“.

Vorbereitungen: LinuxWelt-Toolbox läuft unter Ubuntu 16,04, 18.04 und 19.10, Linux Mint 18 und 19 sowie Raspbian Buster. Für den Download von Tooldatenbank und Updates muss libssl 1.0 oder libssl 1.1 installiert und die Dateien oder Symlinks „libssl.so“ und „libcrypto.so“ müssen vorhanden sein. Ob das der Fall ist, prüfen Sie in einem Terminalfenster mit den folgenden zwei Zeilen:

```
sudo ldconfig -v
ldconfig -pv | grep
 'libssl\.\|libcrypto\.'
```

Sollten in der Ausgabe beispielsweise nur „libssl.so.1.0.0“ und/oder „libssl.so.1.1“ auftauchen, aber nicht „libssl.so“, dann installieren Sie ein zusätzliches Paket:

```
sudo apt install libssl-dev
```

Nutzer von Ubuntu 19.10 müssen ein weiteres Paket installieren:

```
sudo apt install libgtk2.0-0
```

Für den Start von Programmen über die LinuxWelt-Toolbox ist außerdem bei allen Systemen xterm erforderlich und bei Ubuntu/Mint außerdem apturl für die Paketinstallation:

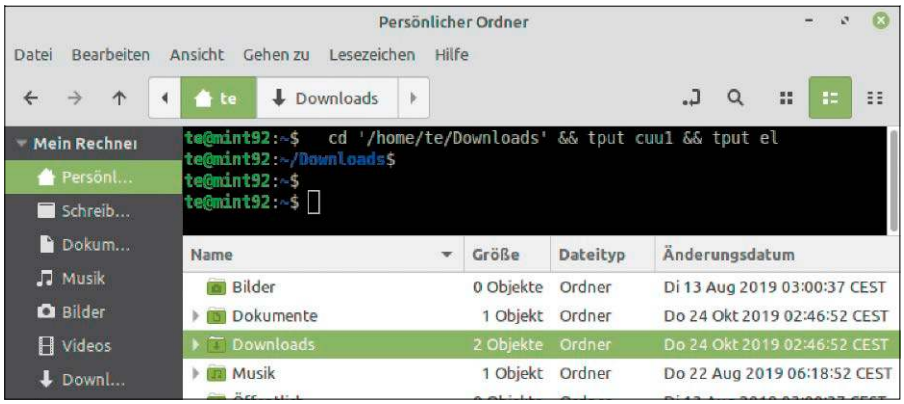
```
sudo apt install xterm apturl
```

Beim ersten Start der LinuxWelt-Toolbox erscheint ein Fenster, in dem Sie auf „Download“ klicken. Damit laden Sie die aktuelle Tooldatenbank herunter, die auf der Heft-DVD aus Aktualitätsgründen nicht mit dabei ist. Sie können das Programm

inklusive Tooldatenbank auch über *www.pcwelt.de/2Gtt1r* herunterladen.
Prüfen Sie auf der Registerkarte „Optionen“, ob die Toolbox das System richtig erkannt hat. Wichtig ist vor allem der Eintrag hinter „Codename“ (etwa „bionic“ für Ubuntu 18.04 LTS). Falls der falsche Codename auftaucht, tragen Sie den richtigen ein und klicken auf „Speichern“.
Eine Übersicht mit den Codenamen finden Sie auf *https://wiki.ubuntu.com/DevelopmentCodeNames*.

2. Softwarepakete suchen und installieren

Bei Ubuntu ist das Programm „Ubuntu Software“ die erste Anlaufstelle für die Suche nach neuer Software, Benutzer von Linux Mint nutzen die „Anwendungsverwaltung“. Fortgeschrittene Linux-Nutzer verwenden das Kommandozeilentool apt oder greifen zu Synaptic, das bei Linux Mint bereits vorinstalliert ist.
Sie finden Synaptic im Menü „Systemverwaltung → Synaptic-Paketverwaltung“. Das Tool ist schnell und ermöglicht vor allem eine gezieltere Paketauswahl. Meist genügt die Eingabe eines Suchbegriffs in das Eingabefeld unter „Schnellauswahl-Filter“. Oder Sie klicken auf die Schaltfläche „Suche“ und tippen den Suchbegriff ein. Über das Auswahlfeld darunter lässt sich der Bereich beispielsweise auf „Name“ oder „Beschreibung und Name“ eingrenzen. Per Klick auf „Einstellungen → Paketquellen“ gelangen Sie zum Fenster „Anwendungen & Aktualisierungen“. Auf der Registerkarte „Andere Programme“ lässt sich festlegen, welche Repositorien die Paketverwaltung berücksichtigt.
Installation: Wechseln Sie in der Linux-Welt-Toolbox über das Ausklappmenü in die Rubrik „Ubuntu/Mint“. Ubuntu-Nutzer installieren Synaptic nach Klicks auf die Schaltflächen „Paketverwaltung“ und „Synaptic installieren“.



Dateimanager erweitern: In Nemo können Sie unter Linux Mint ein Terminalfenster integrieren. Darüber lassen sich Befehle schnell im aktuellen Ordner absetzen.

3. Tools für die Dateiverwaltung

Dateien kopieren, löschen oder verschieben gehört zu den täglichen Handgriffen. Der Dateimanager ist daher eines der wichtigsten Tools. Bei Linux gibt es eine ganze Reihe: Je nachdem, welche Distribution und welcher Desktop installiert ist, zeigt sich standardmäßig etwa Nautilus (Ubuntu Unity), Dolphin (KDE) oder Nemo (Cinnamon/Linux Mint). Nautilus und Nemo bieten praktische Erweiterungen, etwa um die Größe von mehreren Bildern zu ändern oder Prüfsummen von Dateien zu berechnen. Außerdem lassen sich in beide Dateimanager Scripts einbinden und starten. Über das Kontextmenü können Sie dann etwa Ordner schnell packen oder Audiodateien konvertieren. Für Nemo gibt es eine Erweiterung, über die sich ein Terminalfenster im Dateimanager einblenden lässt, das automatisch in den jeweils geöffneten Ordner wechselt.
Installation: Nautilus, Nemo und Dolphin laufen unter allen Desktopumgebungen und Ubuntu-Varianten. Die nötigen Pakete sind in den Standardrepositorien enthalten. Über die LinuxWelt-Toolbox finden Sie alle relevanten Paketnamen und Funktionen für die schnelle Installation nach einem Klick auf „Dateimanager“. Weitere Alternativen gibt es in der Rubrik „Zwei-Fenster Dateimanager“.

DIE LINUXWELT-TOOLBOX NUTZEN

In der LinuxWelt-Toolbox sehen Sie links oben eine Auswahlliste, über die Sie die Rubrik einstellen.
Für diesen Artikel beispielsweise „Ubuntu/Mint“. Die Schaltflächen am linken Rand führen Sie jeweils zur Beschreibung eines oder mehrerer Tools. Die Programme sind teilweise in den Standardrepositorien von Ubuntu, Linux Mint oder Debian enthalten.
In diesem Fall gibt es blaue Schaltflächen am unteren Rand des Fensters, über die Sie ein Programm installieren und starten können. Teilweise sind auch im Text Schaltflächen für die Installation untergebracht.
Alternativ können Sie die Programme auf der Kommandozeile mit apt installieren. Die dafür nötige Befehlszeile kopieren Sie über die Schaltfläche „Kopieren (Strg-C)“ und fügen die Zeile in einem Terminalfenster mit Strg-Umschalt-V ein.

Bitte beachten Sie: Die Installationsanleitungen und Befehlszeilen beziehen sich auf den Stand der Entwicklung im Oktober 2019. Bei neuen Programmversionen kann es Abweichungen geben. Sollte ein Download oder eine Installation nicht funktionieren, informieren Sie sich auf der Webseite des Anbieters.
Die LinuxWelt-Toolbox verwendet XML-Dateien aus dem Unterverzeichnis „Tools“ als Datenbank. Über die Registerkarte „Datenbank“ können Sie die Inhalte bei Bedarf ändern und eigene Tools hinzufügen. Die Beschreibungstexte stammen aus den HTML-Dateien im Ordner „doc“. Diese lassen sich auch im Webbrowser aufrufen – eine Übersicht liefert die Datei „index.html“. Nach eigenen Anpassungen sichern Sie die Ordner „Tools“ und „doc“, damit diese bei einem Update nicht verloren gehen. Für Ihre individuelle Toolsammlung verwenden Sie die Rubrik „Benutzer“.

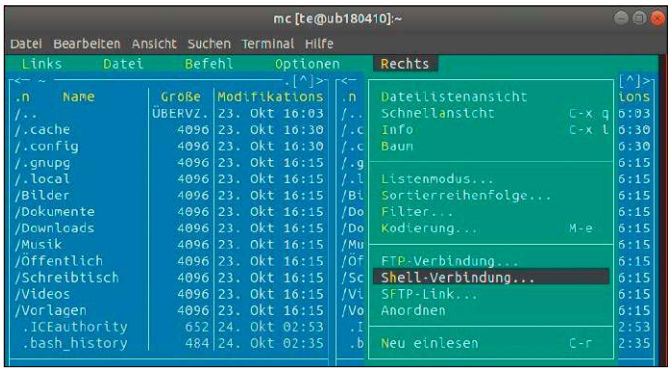
4. Dateimanager im Terminalfenster nutzen

Auch im Terminalfenster müssen Sie nicht auf einen komfortablen Dateimanager verzichten. Das bekannteste Tool heißt Midnight Commander und lässt sich mit dem Befehl „mc“ starten. Vor allem beim Fernzugriff über SSH auf Server oder PCs, wo kein Desktop zur Verfügung steht, zeigt dieses Tool seine Stärken.

Die wichtigsten Operationen lassen sich über die F-Tasten steuern, deren Bedeutung in der unteren Leiste zu sehen ist. F5 beispielsweise kopiert das aktuell markierte Element in das Verzeichnis des anderen Panels. Über F3 rufen Sie einen Dateibetrachter auf und über F4 einen Editor. Taste Esc gefolgt von der Eingabetaste setzt den gerade markierten Ordner- oder Dateinamen in die Kommandozeile ein.

Netzwerkfunktionen: Der Midnight Commander bietet in den Menüs „Links/Rechts“ Funktionen für den Zugriff auf SSH-, SFTP- und FTP-Server. Nach Auswahl etwa von „Shell-Verbindung“ geben Sie Servername oder IP-Adresse an, optional bereits mit dem gewünschten User (etwa „root@192.168.1.10“). Nach Eingabe des Kennworts zeigt der MC wieder seine beiden Fensterhälften und Sie kopieren bequem Dateien zwischen dem lokalen und dem entfernten System.

Installation: Der MC ist in allen Linux-Distributionen verfügbar. Die Installationsanleitung finden Sie in der LinuxWelt-Toolbox nach einem Klick auf „Dateimanager“.



Komfort im Terminal: Der Midnight Commander vereinfacht die Dateiverwaltung auf der Kommandozeile und ermöglicht auch den Datenaustausch über SSH und FTP.

Zwischenablage mit Copy Q: Das Programm hat einen großen Funktionsumfang und zeigt in seinem Verlauf auch Bilder an. Es steht auch für Windows und Mac-OS zur Verfügung.

5. Mehr Funktionen für die Zwischenablage

Einige Desktopumgebungen behandeln die Zwischenablage stiefmütterlich und überlassen deren Verwaltung dem X-Window-System. Dieses arbeitet mit einer empfindlichen Einschränkung: Kopiert man Inhalte aus einem Programm in das Clipboard und schließt dann das Programm, so verschwinden dessen Inhalte aus der Ablage.

Gpaste: Eine Zwischenablage mit lückenlosem Kurzzeitgedächtnis und einem permanenten Erinnerungsvermögen bietet das Gnome-Programm Gpaste. Es nimmt mehrere Bilder und Textausschnitte auf, die sich über das Symbol im Gnome-Panel auswählen lassen. Gpaste ist englischsprachig, aber einfach zu bedienen.

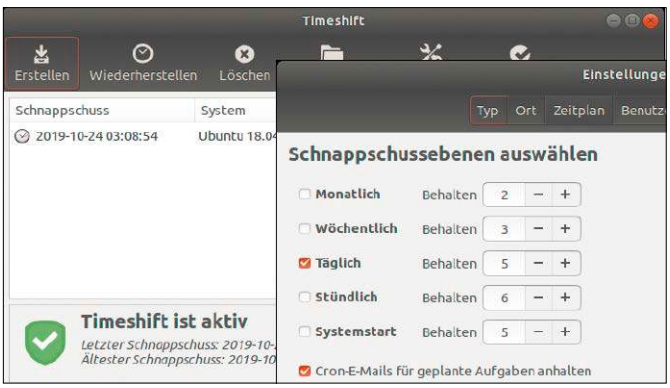
Gpaste ist in den Paketquellen der verbreiteten Linux-Distributionen mit Gnome-Desktop enthalten. Nach der Installation ist ein Neustart des Desktops nötig. Das Tool „Gnome-Tweaks“ (siehe Punkt 6) ist wichtig, um die Gnome-Shell-Erweiterung nach der Installation zu aktivieren.

Copy Q: Für Linux, Windows und Mac-OS gibt es das deutschsprachige Programm Copy Q. Es nimmt Bilder, Text und HTML-formatierten Text auf und kann diese auf Wunsch auch ohne Formatierungen einfügen. Die zwischengespeicherten Einträge lassen sich in einem Editor direkt bearbeiten und überstehen sogar einen Systemneustart.

Installation: Hinweise zu Installation und Benutzung von Gpaste und Copy Q finden Sie in der LinuxWelt-Toolbox nach einem Klick auf „Zwischenablage“.

6. Eigene Dateien und System sichern

Backups sind lästig, aber wichtig. Persönliche Dateien aus Ihrem Home-Verzeichnis sollten Sie regelmäßig sichern, das komplette System zumindest vor größeren Änderungen, etwa vor Distributionsupgrades. Für die persönlichen Daten ist bei Ubuntu standardmäßig ein Tool installiert, das Sie



Systembackup: Timeshift sichert das komplette Linux-System. Es eignet sich für regelmäßige und platzsparende Backups, weil nur geänderte oder neue Dateien berücksichtigt werden.

per Suche im Dash nach „Datensicherungen“ finden. Linux-Mint-Nutzer rufen ein ähnliches Tool über das Menü und „Systemverwaltung → Datensicherungswerkzeug“ auf. Für regelmäßige Backups empfehlen wir das Tool Timeshift (unter Linux Mint Standard). Es erstellt Momentaufnahmen des Dateisystems, die beim Zurückspielen einen vorherigen Zustand wiederherstellen. Home-Verzeichnisse sind standardmäßig ausgeschlossen, lassen sich aber über die „Einstellungen“ dem Backup hinzufügen. Der erste Sicherungspunkt ist immer ein komplettes Backup der Systemverzeichnisse und mit einigen Gigabyte recht groß. Weitere Wiederherstellungspunkte sind dann aber deutlich kleiner, da Timeshift nur noch die Unterschiede zum vorherigen Sicherungspunkt speichert.

Installation: Die Installationshinweise zu Timeshift finden Sie in der LinuxWelt-Toolbox nach einem Klick auf die Schaltfläche „Backup“.

7. Tuningtool für den Desktop

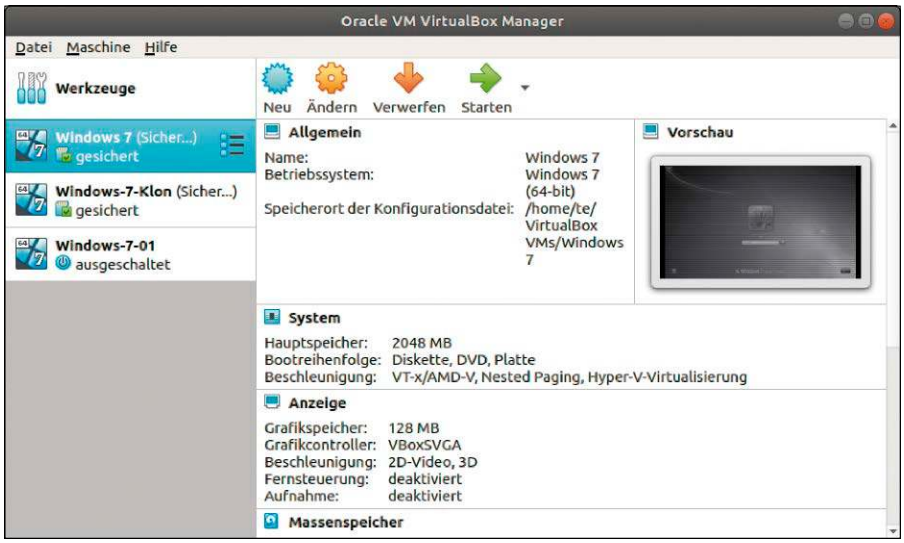
Erweiterte Einstellungsoptionen für Gnome bietet das Tool gnome-tweaks (früher gnome-tweak-tool, „Optimierungen“ auf deutschem System). Da die meisten Gnome-Nutzer das Tool für unentbehrlich halten und notfalls nachinstallieren, bringen einige Gnome-Distributionen das Programm bereits mit – Ubuntu allerdings nicht. Mit gnome-tweaks ist es möglich, den Desktop als Dateiablage zu verwenden, ferner Arbeitsflächen, Schriftbild, Fensterverhalten, Fensterschaltflächen und Fensteroptik genauer zu justieren.

Installation: Eine ausführliche Funktionsbeschreibung und Installationsanleitung liefert LinuxWelt-Toolbox nach einem Klick auf „Tweak-Tools“.

8. Nützliche Systemtools

Wie viel Speicher steckt im Rechner? Wo ist die Konfigurationsdatei für den Samba-Server? Wie beende ich ein eingefrorenes Programmfenster? Und wo ist das Mountverzeichnis für das eingehängte Netzlaufwerk? Antworten auf diese und viele weitere Fragen geben wir in einem längeren Beitrag, den Sie in der LinuxWelt-Toolbox per Klick auf „Systemtools in der Praxis“ aufrufen. Dabei kommen prominente grafische Programme unter den Desktopsystemen Ubuntu und Linux Mint zu Wort, aber den größeren Anteil erhalten die typischen Terminalprogramme. Diese haben nämlich zwei entscheidende Vorteile: Erstens funktionieren sie auf allen Linux-Distributionen, zweitens sind sie alternativlos, wenn ein Server per SSH im Terminal administriert wird. Ein Teil der genannten Tools ist bei Ubuntu oder Linux Mint standardmäßig installiert. Wenn nicht, finden Sie in der LinuxWelt-Toolbox eine Installationsanleitung.

Anpassungen mit Gnome-Tweaks: Viele wichtige Detaileinstellungen zum Aussehen und Verhalten des Desktops sind nur über dieses zusätzliche Werkzeug zugänglich.



Virtualisierung: Installieren Sie Betriebssysteme in einer virtuellen Maschine. Darin lässt sich Software gefahrlos ausprobieren und Sie können Windows-Anwendungen unter Linux starten.

9. Virtualisierung und Windows-Programme

Nicht immer steht eine benötigte Software auch für Linux zur Verfügung. Es bietet sich dann an, Windows in einer virtuellen Maschine zu verwenden und hier die jeweils gewünschte Software zu nutzen. Die Virtualisierungssoftware Virtualbox ist in den Standard-Paketquellen enthalten. Darüber lässt sich die Open-Source-Variante installieren, die aber meist nicht ganz aktuell ist und einige Funktionen vermissen lässt, beispielsweise die Unterstützung von USB-Geräten. Der Hersteller Oracle (*www.virtualbox.org*) stellt jedoch eigene Linux-Repositorien bereit, über die sich die aktuelle Version einrichten lässt.

Installation: Klicken Sie in der LinuxWelt-Toolbox auf „Virtualisierung“. Sie finden hier eine Schaltfläche für den Import der Oracle-PGP-Schlüssel, mit dem die Pakete digital signiert sind. Danach klicken Sie auf „Virtualbox installieren“. Die Befehlszeilen für die manuelle Installation sind darunter zu finden.

Alternative: Für den Start von vielen Windows-Programmen unter Linux eignet sich auch Wine, das Windows-Funktionen unter Linux nachbildet. Am einfachsten gelingt die Installation von Windows-Software über Playonlinux. Die Softwareauswahl für Wine ist jedoch begrenzt. Oft funktionieren nur ältere Programmversionen problemlos. Sehen Sie auf *www.playonlinux.com* nach, ob und wie gut die benötigte Software unterstützt wird.

Installation: Für die Einrichtung von Playonlinux, die automatisch die passende Wine-Version anfordert, klicken Sie in LinuxWelt-Toolbox auf „Virtualisierung“ und dann auf „Playonlinux installieren“. ■

Programme & Tools fürs Netzwerk

Linux fühlt sich im Netzwerk traditionell zu Hause. Das System ist als Datei- oder Webserver schnell eingerichtet und auch die Fernwartung über das Netzwerk stellt kein Problem dar.

VON THORSTEN EGGELING

Über den Dateimanager nutzen Sie Freigaben im lokalen Netzwerk, die auf einem Linux- oder Windows-Server liegen. Die Zugangsdaten können Sie dauerhaft speichern.

Was Sie für das Internet benötigen, ist bei allen gängigen Linux-Distributionen bereits vorinstalliert. Als Browser dient meist Firefox und für E-Mails gibt es Thunderbird. Der Zugriff auf Netzwerkfreigaben erfolgt über den Dateimanager. Serverdienste für Dateifreigaben oder SSH/SFTP sind standardmäßig oft nicht vorhanden, lassen sich aber schnell aus den Paketquellen nachinstallieren. Die Kommandozeilen aus diesem Artikel, Tipps, Beschreibungen, Internetlinks zu weiteren Informationen und Downloadlinks finden Sie in der LinuxWelt-Toolbox in der Rubrik „Netzwerk".

1. Zugriff auf Freigaben im Netzwerk

Linux, Windows und Mac-OS sprechen im Netzwerk eine gemeinsame Sprache: Das SMB/CIFS-Protokoll. Einen SMB-Client (für den Zugriff auf SMB-Freigaben) bringen alle Systeme mit: Mac-OS zeigt solche Windows-Freigaben im Dateimanager in einer eigenen Rubrik. Unter Linux Mint, Ubuntu & Co. finden Sie die Freigaben über „Andere Orte → Windows-Netzwerk" oder „Netzwerk" im Dateimanager – und ganz ähnlich auch im Windows-Explorer. Sofern es sich um eine Freigabe ohne den großzügigen „Gastzugriff" (Zugriff ohne Kontoinformationen) handelt, ist zum Öffnen eine Authentifizierung notwendig: Dazu benötigen Sie den Namen und das Kennwort eines Samba-Kontos. Diese Zugangsdaten kann sich jeder Client dauerhaft merken, sodass die spätere Nachfrage entfällt (Option „Nie vergessen" unter Ubuntu/Linux Mint).

Ab Ubuntu 18.04/Linux Mint 19 gibt es allerdings Probleme mit Windows-Freigaben. Diese werden im Dateimanager nicht angezeigt. Der Grund dafür: Aus Sicherheitsgründen ist das Protokoll SMB 1.1 deaktiviert, das aber für die Auflistung der Freigabenamen erforderlich ist. Bis die Distributoren diesen Fehler behoben haben, geben Sie den Pfad hinter „Mit Server verbinden" oder in der Adresszeile (Strg-L) in der Form

```
smb://Servername/Freigabename
```

ein. Für den künftigen schnelleren Zugriff legen Sie über das Hamburger-Menü (Icon mit den drei horizontalen Linien) ein Lesezeichen für die Freigabe an. Unter Mint verwenden Sie das Menü „Lesezeichen".

2. Freigaben für Windows- und Linux-PCs

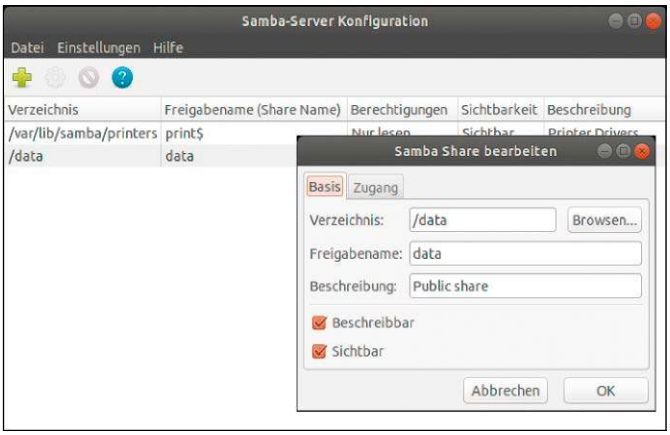
Für die Freigabe persönlicher Ordner verwenden Sie im Ubuntu-Dateimanager den Kontextmenüpunkt „Freigabe im lokalen Netzwerk" eines Ordners. Setzen Sie ein Häkchen vor „Diesen Ordner freigeben". Ist der Freigabedienst Samba noch nicht installiert, klicken Sie auf „Freigabedienst einrichten" und danach auf „Installieren". Anschließend melden Sie sich bei Linux ab und wieder an.

In Linux Mint 19 Cinnamon heißt der Kontextmenüpunkt „Freigabeoptionen". Bevor Sie ihn nutzen können, müssen Sie Samba installieren. Dazu verwenden Sie im Terminal die folgenden zwei Befehle:

```
sudo apt update
sudo apt install samba
```

Im Fenster „Ordner freigeben" können Sie ein Häkchen vor „Gastzugriff (für Nutzer ohne Benutzerkonto)" setzen. Damit erlauben Sie anderen PCs im Netzwerk ohne Anmeldung Lesezugriff auf den freigegebenen Ordner. Ansonsten gibt es Lesezugriff nach vorheriger Anmeldung nur für Nutzer, die ein Konto auf dem PC mit der Freigabe besitzen. Schreibzugriff ist möglich, wenn Sie ein Häkchen vor „Anderen erlauben, Dateien in diesem Ordner zu erstellen oder zu löschen" setzen. Damit die Anmeldung funktioniert, müssen Sie aber vorher den gewünschten Benutzerkonten ein Samba-

Ordnerfreigabe: Eigene Ordner lassen sich über das Kontextmenü „Freigabe im lokalen Netzwerk“ (Ubuntu) für gemeinsame Nutzung im Netz bereitstellen.



Samba-Server konfigurieren: Mit dem grafischen Tool aus dem Paket „system-config-samba“ erstellen Sie Freigaben für angemeldete Benutzer und Gäste.

Passwort zuweisen, denn Samba verwendet eigene Passwörter, die vom Systemkonto unabhängig sind:

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

Den Platzhalter „[User]“ ersetzen Sie durch die Bezeichnung des Benutzerkontos. Tippen Sie das Passwort ein und bestätigen Sie es. Das Passwort darf identisch mit dem Linux-Anmeldepasswort sein oder von diesem abweichen.

Es ist jedoch empfehlenswert, auf allen Linux- und Windows-PCs die gleiche Kombination von Benutzernamen und Passwörtern zu verwenden.

Samba konfigurieren: Für die Basiskonfiguration von Samba sowie systemweiter Freigaben empfiehlt sich bei Ubuntu 16.04, 18.04 sowie Linux Mint 18 und 19 die Installation des Pakets „system-config-samba“. Bei Ubuntu 19.10 ist es nicht mehr installierbar. Erstellen Sie zuerst eine Konfigurationsdatei:

```
sudo touch /etc/libuser.conf
```

Danach starten Sie das Tool mit

```
sudo -H system-config-samba
```

Über „Einstellungen → Server-Einstellungen“ legen Sie bei Bedarf die Arbeitsgruppe für den Samba-Server fest, wenn Sie in Ihrem Netzwerk etwas anderes als den Linux- und Windows-Standard „Workgroup“ verwenden.

Klicken Sie auf „Datei → Share hinzufügen“, um einen Ordner im Netzwerk freizugeben. Setzen Sie ein Häkchen vor „Sichtbar“ und auf der Registerkarte „Zugang“ wählen Sie die Option „Jedem Zugriff erlauben“. Alle Benutzer im Netzwerk haben dann über das Gastkonto anonymen Zugang zu dieser Freigabe. Ist auf der Registerkarte „Basis“ ein Häkchen vor „Beschreibbar“ gesetzt, ist auch anonymer Schreibzugriff möglich. Die Dateisystemrechte haben jedoch Priorität.

NETZWERKTOOLS FÜR DIE KOMMANDOZEILE

Im Terminalfenster lassen sich einige nützliche Tools starten, über die Sie die Netzwerkkonfiguration prüfen oder ändern können. Mit der Eingabe von

```
ip addr
```

ohne weitere Parameter erhalten Sie die physikalische MAC-Adresse des Netzwerkadapters, die lokale IP-Adresse und die Anzahl und Datenmenge der empfangenen (RX) und der gesendeten (TX) Datenpakete seit dem letzten Systemstart. Ethernet-Adapter tauchen mit Bezeichnungen wie „enp0s3“ auf, WLAN-Adapter etwa als „wlp5s0“. Bei der an erster Position angezeigten „lo“-Schnittstelle mit der IP-Adresse 127.0.0.1 handelt es sich um einen Loopback-Adapter, über den lokale Prozesse via TCP/IP miteinander kommunizieren. Gibt „ip addr“ eine IP-Adresse aus, die nicht im Bereich des Routers liegt, oder erscheint gar keine Adresse, ist die Netzwerkverbindung gestört. Mit Ping prüfen Sie Netzwerkverbindungen: *ping google.de* oder *ping 192.169.178.1* geben Zeilen mit Antworten aus, wenn das Netzwerk erreichbar ist. Andernfalls erscheint „Destination Host Unreachable“ oder ähnlich.

Das Programm Ethtool zeigt die Geschwindigkeit des Netzwerkadapters an. Sie rufen es beispielsweise mit folgender Befehlszeile auf:

```
ethtool enp0s3
```

Erscheint hinter „Speed“ der Wert „1000Mb/s“, nutzt der Adapter Gigabit-Ethernet. *ethtool -i enp0s3* gibt den Namen des Treibers aus, der für diese Schnittstelle verantwortlich ist.

Der Net-Befehl dient zur Kontrolle und Konfiguration eines Samba-Servers. Net ist vor allem praktisch, wenn Sie Samba-Freigaben auf einem Server ohne grafische Oberfläche oder aus der Ferne über SSH verwalten müssen. Folgende Befehlszeile gibt die vom aktuellen Benutzer erstellten Freigaben aus:

```
net usershare list
```

Eine neue Freigabe erstellen Sie mit dieser Zeile:

```
net usershare add sepp /home/sepp "" sepp:f
```

In diesem Fall wird „/home/sepp“ mit dem Freigabenamen „sepp“ für den gleichnamigen User im Netzwerk freigegeben. Über den Befehl *net usershare delete sepp* löschen Sie diese Freigabe.

Installation: Alle genannten Tools sind bei Ubuntu und Linux Mint standardmäßig vorhanden oder lassen sich nachinstallieren. Die Befehlszeile zur Installation finden Sie in der Linux-Welt-Toolbox nach einem Klick auf „Terminal-Tools“.

Ordner und Dateien im freigegebenen Verzeichnis müssen für den Gastzugriff mit Schreibrechten dem Benutzer „nobody“ und der Gruppe „nogroup“ gehören und ausführbar beziehungsweise beschreibbar sein. Das lässt sich in einem Terminalfenster beispielsweise durch folgenden Befehl erreichen:

```
sudo chown -R nobody:nogroup /
  freigegeben
sudo chmod -R 755 /freigegeben
```

Installation: In der LinuxWelt-Toolbox finden Sie nach einem Klick auf die Schaltfläche „Samba“ eine Schaltfläche für die Installation von „system-config-samba“. Folgen Sie den Links zu den weiterführenden Informationen. In der Rubrik „Raspberry Pi“ erfahren Sie nach einem Klick auf „Datenserver“, wie sich Samba über die Datei „/etc/samba/smb.conf“ konfigurieren lässt. Die Anleitung gilt nicht nur für Raspbian, sondern auch für andere Linux-Systeme wie Ubuntu 19.10.

3. Terminal und Dateitransfer über SSH

SSH (Secure Shell) ist ein Netzwerkprotokoll, über das Sie eine verschlüsselte Verbindung zu anderen Linux-PCs im Netzwerk herstellen. Es kommt vor allem bei der Fernwartung von Servern zum Einsatz. Der SSH-Client ist bei Ubuntu und Linux Mint Standard. Auf jedem Client-PC im Netzwerk können Sie über

```
ssh [User]@[Server][:Port]
```

Verbindungen aufbauen. Den Platzhalter „[User]“ ersetzen Sie durch das Systemkonto auf dem Server, „[Server]“ durch Name oder IP-Adresse des Open-SSH-Servers. Die Portangabe kann entfallen, wenn der Standardport (22) verwendet wird. Danach können Sie im Terminal so arbeiten, als ob Sie direkt vor dem entfernten PC sitzen würden.

Installation: Wenn Sie auf allen Rechnern im Netzwerk den Open-SSH-Server installieren, funktioniert die Verbindung in alle Richtungen. Ein SFTP-Server für den Dateitransfer wird dabei automatisch mit installiert. In der LinuxWelt-Toolbox finden Sie nach einem Klick auf „OpenSSH“ die Befehlszeile für die Installation, zusätzliche Informationen zum Dateitransfer per SFTP sowie über die Anmeldung mit einem Sicherheitsschlüssel statt mit einem Passwort. Weitere Infos zu SSH erhalten Sie nach einem Klick auf „Netzwerk-Tools“.

Fernwartung: In der LinuxWelt-Toolbox finden Sie alle Informationen zur Einrichtung des Open-SSH-Servers und zur optimalen Nutzung der SSH-Clients.

4. Webserver auf dem PC einrichten

Im eigenen Netzwerk lässt sich ein Webserver für ein Intranetportal nutzen, etwa mit einem Wiki für die Ideensammlung oder mit einem Teamkalender. Sie können außerdem Webanwendungen wie Wordpress, Joomla oder Magento installieren und die Konfiguration sowie Gestaltung der Weboberfläche ausprobieren.

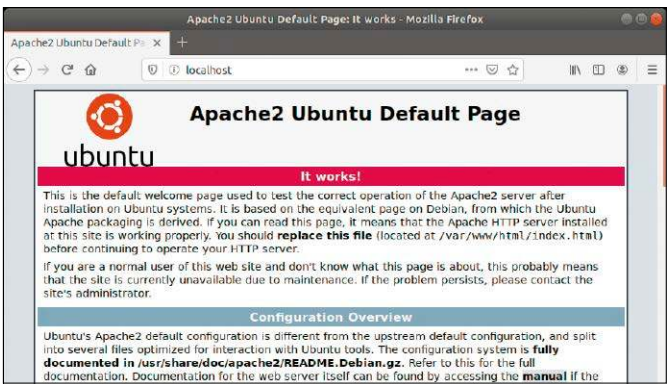
Der Webserver auf dem eigenen PC kann seine Dienste auch im Internet anbieten. Dazu müssen Sie in Ihrem DSL-Router die Portweiterleitung auf den Server-PC aktivieren. Wechselnde IP-Adressen, fehlende IPv4-Unterstützung durch den Internetprovider und eine geringe Uploadgeschwindigkeit lassen diese Lösung jedoch als wenig attraktiv erscheinen.

Für kleine Teams, die keinen Server im Internet mieten wollen, kann der heimische Webserver jedoch ausreichen. Sie sollten dann jedoch einen Dienst für dynamisches DNS nutzen, damit der Server stets über einen konstanten Domainnamen erreichbar ist. Wie sich dynamischem DNS einrichten lässt, lesen Sie in der LinuxWelt-Toolbox nach einem Klick auf „Nextcloud“ in der Rubrik „Raspberry Pi“.

Installation: In der LinuxWelt-Toolbox finden Sie nach einem Klick auf „Der eigene Webserver“ eine Installationsanleitung für den Apache Webserver zusammen mit Dokuwiki. Eine Alternative für Geräte mit limitierter Hardwareausstattung zeigen wir unter „Nginx-Webserver“.

5. Tipps & Tools für das Heimnetzwerk

Netzwerke sind hardwareseitig unglaublich flexibel und ausbaufähig. Linux wiederum ist für das Netzwerk geschaffen und macht als Netzwerkclient wie als Server eine glänzende Figur. In der LinuxWelt-Toolbox finden Sie nach einem Klick auf „Netzwerk-Tools“ einen Beitrag, der Basiswissen und



Webserver: Nach der Apache-Installation zeigt „http://localhost“ im Browser die Standard-Website „index.html“ aus dem Verzeichnis „/var/www/html/“.

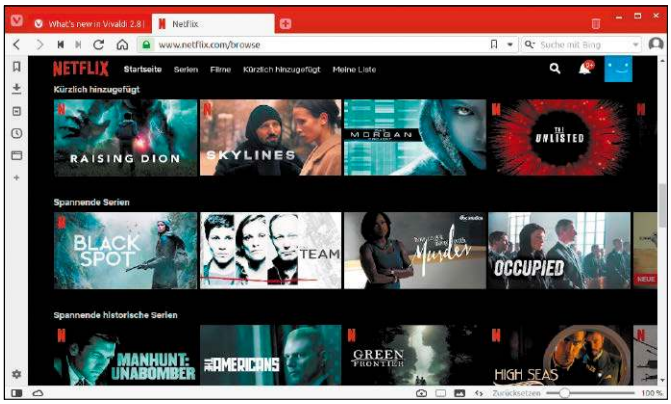
vertiefende Tipps für ein optimiertes Heimnetz liefert. Dabei geht es um das lokale LAN- und WLAN-Netz mit typischen Geräten, Kommunikationsprotokollen, Freigaben und Serververwaltung.
Alle genannten Tools wie ping, ifconfig, iwlist, arp oder nmap sind bei den meisten Linux-Systemen vorinstalliert oder sie lassen sich aus den Standardrepositorien nachinstallieren (siehe auch den Kasten „Netzwerktools“).

6. Frische Browser fürs Internet

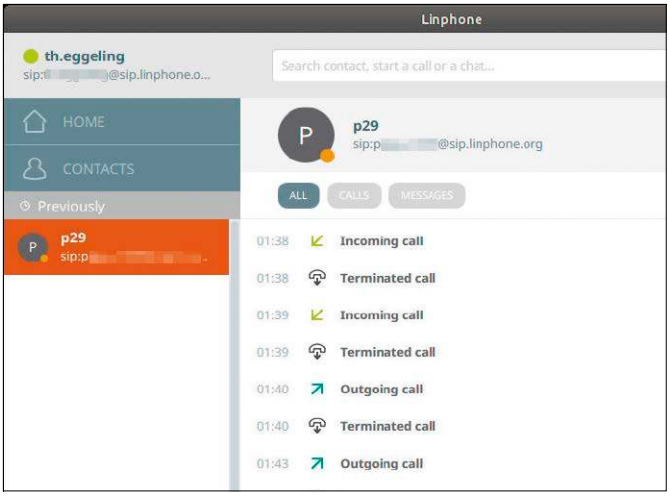
Firefox ist einer der beliebtesten Webbrowser und bei den meisten Linux-Distributionen bereits vorinstalliert. Der Browser glänzt vor allem durch seine Erweiterbarkeit über Add-ons. Firefox geht jedoch nicht besonders sparsam mit dem Hauptspeicher um, was vor allem bei vielen geöffneten Tabs das System ausbremsen kann. Chromium (*www.chromium.org*), ein Open-Source-Ableger von Google Chrome, hat einen geringeren Ressourcenverbrauch. Die Unterschiede von Chromium im Vergleich zu Google Chrome sind gering. Sie betreffen einige Einstellungen, Codecs sowie die Erweiterungen für Adobe Flash. Chromium ist in den Standard-Paketquellen von Ubuntu und Linux Mint enthalten. Streams von Amazon Video oder Netflix kann Chromium allerdings nicht wiedergeben. Dafür benötigen Sie Google Chrome (*www.google.de/chrome*) oder Firefox.
Eine weitere Alternative ist der Browser Vivaldi (*https://vivaldi.com*), der ebenfalls auf Chrome basiert und auch Videos von Amazon oder Netflix abspielen kann. Der Schwerpunkt bei Vivaldi liegt auf der Anpassungsfähigkeit. Tabs lassen sich in Tabgruppen organisieren, Sie können die Position von Tab- und Adressleiste festlegen, den Browser über konfigurierbare Kurzbefehle steuern und Notizen zu Webseiten erstellen.
Installation: In der LinuxWelt-Toolbox wählen Sie links oben die Rubrik „Netzwerk“ und klicken dann auf „Browser“. Sie finden hier Installationsanleitungen für alle genannten Webbrowser.

7. E-Mail und Kommunikation

Das verbreitete E-Mail-Programm Thunderbird ist bei Ubuntu und Linux Mint bereits vorinstalliert. Wenn Sie mehr Funktionen benötigen, sollten Sie sich Evolution ansehen. Dabei handelt es sich um ein Groupwarepaket, das neben Mail auch Kalender, Adressbuch, Aufgabenlisten und Notizen bietet.
Eine weitere Alternative ist Kmail, vor allem für Nutzer des KDE-Desktops. Der Funktionsumfang von Kmail entspricht in etwa dem von Thunderbird. Für Groupwarefunktionen installieren Sie das Metapaket mit dem Namen „kdepim“. Darin sind neben Kmail unter anderen auch ein Adressbuch, Aufgaben- sowie Terminplaner enthalten. Das Programm Kontact („Persönliche Informationsverwaltung“) kann als Zentrale für diese Anwendungen genutzt werden.
Wer lieber per Chat kommuniziert oder ein bewegtes Bild des Gegenübers sehen will, kann Skype installieren. Aktuelle DEB- und RPM-Pakete gibt es bei Microsoft zum kostenlosen Download (*www.pcwelt.de/P3BHbX*). Wenn Sie Open-Source-Software bevorzugen, dann installieren Sie die Messenger Pidgin oder KDE-Telepathy. Beide unterstützen Netzwerkprotokolle wie ICQ, MSN, Jabber und Google Talk. Als Alternative zu Whatsapp gibt es auch für Linux eine Desktop-App von Telegram (*https://telegram.org*).
Als VoIP-Lösung für Sprach- und Videotelefonate sowie Chats lässt sich bei Ubuntu 18.04/19.10 und Linux Mint 19 Linphone installieren. In den Standardrepositorien finden sich allerdings nur ältere Versionen, weshalb Sie besser die Flatpak-App von der Webseite des Herstellers verwenden (*www.linphone.org*). Linphone gibt es auch für Windows, Mac-OS, Android und iOS.
Über das Programm oder direkt auf der Seite *https://www.linphone.org/freesip/* erstellen Sie ein Konto, das die kostenlose Kommunikation mit anderen Linphone-Nutzern ermöglicht. Wer einen Festnetzanschluss oder ein Mobiltelefon anrufen möchte, benötigt ein kostenpflichtiges Konto bei einem SIP-Anbieter, beispielsweise *www.sipgate.de*.
Installation: Klicken Sie in der LinuxWelt-Toolbox unter „Netzwerk“ auf „Kommunikation“. Hier finden Sie Schaltflächen oder Links zur Installation der genannten Programme sowie Befehlszeilen für die manuelle Einrichtung der Software. ■



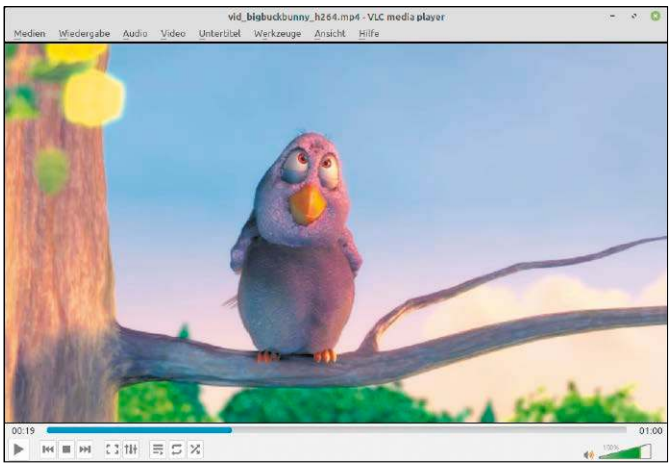
Schneller Browser: Vivaldi basiert auf Google Chrome und spielt auch Filme etwa von Amazon oder Netflix ab. Die Oberfläche lässt sich individuell anpassen.



Telefonieren mit Linux: Für die aktuelle Linphone-Version verwenden Sie eine Flatpak-App. Das Programm beherrscht Sprach- und Videotelefonate sowie Chats.

Tools für Audio, Video & Foto

Linux-Nutzer können mehrere Mediaplayer verwenden, je nach gewünschtem Funktionsumfang. Außerdem stehen zahlreiche Tools bereit, mit denen sich Multimedia-Formate bearbeiten oder umwandeln lassen.



Filme abspielen: Der VLC Mediaplayer gibt alle verbreiteten Audio- und Videoformate wieder. Nur für kopiergeschützte DVDs benötigen Sie eine zusätzliche Programmbibliothek.

VON THORSTEN EGGELING

Im Bereich Multimedia müssen Linux-Nutzer auf nichts verzichten. Abspielprogramme für Musik und Filme sind vorinstalliert und es gibt Bildbetrachter und Programme für die Fotoverwaltung. Wem die Standardprogramme nicht reichen, sollte sich die Alternativen ansehen. Alle in diesem Artikel erwähnten Programme lassen sich über die LinuxWelt-Toolbox installieren. Wählen Sie die Rubrik „Multimedia“ und steuern Sie mit der Schaltfläche darunter die gewünschten Tools an.

1. Mediaplayer für Linux

Bei Ubuntu taucht der Mediaplayer unter der Bezeichnung „Videos“ auf, Nutzer von Linux Mint finden im Menü unter „Multimedia“ die „Medienwiedergabe“. Ob die Player alle verbreiteten Audio- und Videoformate abspielen können, hängt davon ab, ob Sie bei der Installation die Option „Installation von Drittanbieterprogrammen“ aktiviert haben. Wenn nicht, installieren Sie diese Pakete nach:

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

Alternative Player: Der VLC-Player ist immer eine gute Wahl *(www.videolan.org)*, da er eigene Codecs mitbringt und alle gängigen Medienformate abspielt. Eine weitere Alternative ist Smplayer (*http://smplayer.sourceforge.net*). Dieses grafische Front-End für Mplayer hält den gesamten Funktionsumfang von Mplayer bereit. Wichtige Audio- und Videocodecs hat Smplayer ebenfalls an Bord.

Installation: In der LinuxWelt-Toolbox finden Sie Schaltflächen und Befehlszeilen für die Installation der Gstreamer-Plug-ins sowie von VLC und Smplayer per Klick auf „Mediaplayer“.

2. Videodateien bearbeiten und konvertieren

Mit Avidemux schneiden Sie Videodateien, recodieren in andere Formate oder verpacken Video- und Audiospuren ohne Qualitätsverlust neu (*http://fixounet.free.fr/avidemux*). In welchem Format das Ausgangsmaterial vorliegt, spielt keine Rolle, denn Avidemux kommt mit allen Formaten klar.

Videos konvertieren: Handbrake (*http://handbrake.fr*) wandelt Videos in das MKV- oder MP4-Container-Format mit h264- oder h265-Codec um. Eine umfangreiche Liste mit Konvertierungsprofilen für mobile Geräte und Internetplattformen erleichtert die Konfiguration. Bei Bedarf passen Sie auf den Registerkarten „Bild“ oder „Video“ die Einstellungen an. Mit Klick auf „Enkodierung starten“ beginnt die Konvertierung.

Installation: Avidemux gibt es als Appimage zum Download, das unter Ubuntu oder Linux Mint läuft. Handbrake ist im Standardrepositorium zu finden, neuere Versionen in einem PPA. Für die Installationen und weitere Infos klicken Sie in der LinuxWelt-Toolbox auf „Video bearbeiten“.

3. Videoeditoren für Ubuntu/Mint

Wer Videos nicht nur umwandeln, sondern bearbeiten möchte, kann das einsteigertaugliche Openshot verwenden (*www.openshot.org*). Schneiden und Trimmen sind intuitiv: Sie zerteilen einen Clip und löschen oder verschieben nach Rechtsklick auf den jeweiligen Teil den Abschnitt. Neben den Schnittfunktionen gibt es eine Reihe von Übergängen. Sie wählen den Effekt aus der Liste und ziehen ihn auf die entsprechende Spur. Über das Kommando „Datei → Video exportieren“ und Auswahl eines Profils schreiben Sie die geschnittene Fassung in eine neue Datei.

Weitere Videoeditoren für Linux sind Pitivi, Kdenlive und Cinelerra. Pitivi (*www.pitivi.*

org) ähnelt in Bedienung und Funktionsumfang Openshot. Kdenlive (*https://kdenlive.org*) und Cinelerra (*http://cinelerra.org*) bieten mehr Funktionen, benötigen aber Einarbeitungszeit.

Installation: Klicken Sie in der LinuxWelt-Toolbox auf „Videoeditoren“. Die Installation erfolgt über die zugehörige Schaltfläche meist aus den Standardrepositorien. Für neuere Versionen verwenden Sie die Downloadlinks oder Terminalbefehle.

4. Fotosammlungen verwalten

Für die Fotoverwaltung ist bei Ubuntu Shotwell vorinstalliert, bei Linux Mint Pix. Bilder lassen sich mit Stichwörtern versehen und es gibt einfache Bearbeitungsfunktionen. Wer mehr will, verwendet Digikam (*www.digikam.org*), das Fotos nach Alben, Tags, Stichwörtern sortieren und kategorisieren kann. Es enthält zahlreiche Tools für die Fotobearbeitung wie die Tonwert- oder Rote-Augen-Korrektur. Eine Unterstützung von RAW-Formaten ist vorhanden, jedoch ist Digikam kein Ersatz für Darktable und Rawtherapee.

Installation: Digikam, Darktable, Rawtherapee sind in den Paketquellen von Ubuntu und Mint enthalten. Zur Installation und für weitere Infos klicken Sie in der LinuxWelt-Toolbox auf „Fotos verwalten“.

5. Bilder unter Linux bearbeiten

Gimp (*www.gimp.org*) kann zwar auch Fotos bearbeiten, hat aber höhere Ansprüche – vergleichbar mit Photoshop. Gimp bietet Zeichenwerkzeuge, Ebenen, Masken, Automatikverbesserung und Filter. Sie können Fotos retuschieren, Bilder freistellen oder verfremden. Wie bei Photoshop erschließen sich die meisten Funktionen nicht auf Anhieb und bestimmte Effekte sind nur durch eine Kombination von Masken und Ebenen zu erreichen. Für Gimp gibt es aber viel Unterstützung – ein guter Einstieg ist die Dokumentation unter *www.gimp.org/docs*.

Installation: Gimp ist in den Standardrepositorien von Ubuntu und Linux Mint enthalten. Zur Installation und für weitere Infos klicken Sie in der LinuxWelt-Toolbox auf „Gimp“.

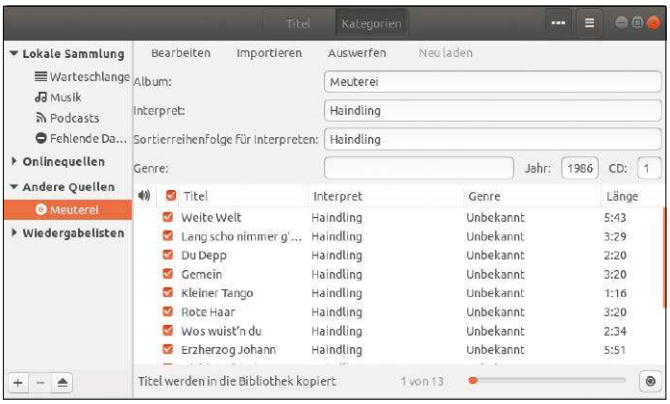
6. Tools für Audiodateien

Rhythmbox – Standard unter Ubuntu und Linux Mint – kann Musikdateien wiedergeben und verwalten. Über „Importieren“ lassen sich Audio-CDs nach MP3 umwandeln. Über „Bearbeiten → Einstellungen“ legen Sie auf der Registerkarte „Musik“ das Ausgabeformat fest. Das Tool ermittelt über eine Internetabfrage Infos zur eingelegten CD und benennt die Audiodateien entsprechend.

Audacity ist das Tool der Wahl zum Bearbeiten und Aufnehmen von Audiodaten. Auf beliebig vielen Spuren lassen sich Audiodateien mischen, bearbeiten, mit Effekten versehen oder Hintergrundgeräusche entfernen. Audacity eignet sich zum Digitalisieren von Schallplatten oder zur Nachvertonung eigener Videos.

Installation: Klicken Sie in der LinuxWelt-Toolbox auf „Audio-Tools“. Installieren Sie Audacity über die zugehörige Schaltfläche.

Avidemux: Das Programm beherrscht den verlustlosen Schnitt fast beliebiger Videodateien. Das Tool arbeitet sehr schnell, wenn die Recodierung entfallen kann.



Musik verwalten und abspielen: Rhythmbox gibt Audiodateien wieder und kann auch Audio-CDs importieren. Die Tracks werden nach einer CDDB-Abfrage passend benannt.

DVD- UND BLU-RAY-WIEDERGABE

Um Video-DVDs abzuspielen, müssen Sie unter Ubuntu/Mint ein zusätzliches Paket installieren. Im Terminalfenster verwenden Sie diesen Befehl:

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

Die angezeigten Meldungen bestätigen Sie mit „OK“ beziehungsweise „Ja“ und starten dann diesen Befehl:

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

Beantworten Sie die Frage in der ersten Meldung mit „Ja“. Wenn Sie DVDs im Standardplayer abspielen möchten, installieren Sie zusätzlich das Paket „gstreamer1.0-plugins-bad“. Alternativ verwenden Sie den VLC Player.

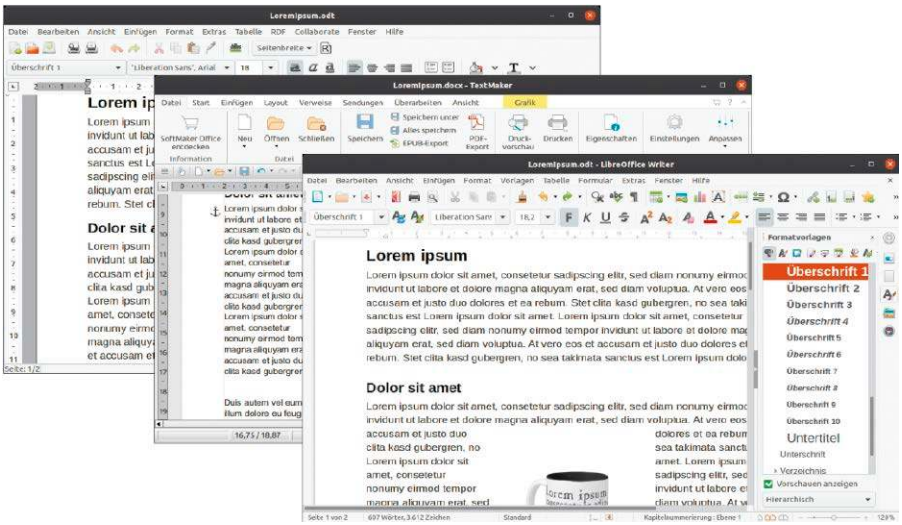
Zur Zeit gibt es für Linux-Nutzer keine einfache Möglichkeit, verschlüsselte Blu-ray-Disks abzuspielen. Die Anleitung unter *https://wiki.archlinux.org/index.php/Blu-ray* ist eine Chance, aber keine Garantie, dass sich jede Blu-ray wiedergeben lässt. Eine Anleitung zur Installation der Bibliotheken für die Wiedergabe verschlüsselter DVDs lesen Sie in der LinuxWelt-Toolbox nach einem Klick auf „DVD/Blu-ray“.

Office-Pakete und Produktivität

Bei den meisten Desktopdistributionen steht direkt nach der Installation ein umfangreiches Office-Paket zu Verfügung. Mit zusätzlichen Programmen und Tools lässt sich die Arbeitsumgebung weiter ausbauen und effizienter nutzen.

VON THORSTEN EGGELING

Libre Office bietet alles für typische Büroaufgaben: Textverarbeitung und Tabellenkalkulation, ein Präsentationsprogramm und ein Modul für Zeichnungen sind mit dabei. Ein Datenbankmodul lässt sich bei Bedarf ergänzen. Einige Distributionen, beispielsweise Lubuntu, setzen auf die leichtgewichtigere Kombination von Gnumeric (Tabellenkalkulation) und Abiword (Textverarbeitung). Welchen Funktionsumfang Sie tatsächlich benötigen, probieren Sie am besten selbst aus. Die meisten in diesem Artikel genannten Programme sind über die Paketverwaltung schnell installiert. Anleitungen und weiterführende Links finden Sie in der LinuxWelt-Toolbox unter „Office“.



Freie Wahl: Abiword, Textmaker Free und Libre Office Writer sind die beliebtesten Textprogramme unter Linux. Alle drei haben einen Funktionsumfang, der für die meisten Aufgaben ausreicht.

1. Office-Pakete für Linux

Der Funktionsumfang von Libre Office (*www.libreoffice.org*) reicht wahrscheinlich für die meisten privaten Nutzer aus. In der Textverarbeitung lassen sich Briefe professionell formatieren und die Tabellenkalkulation hilft bei Berechnungen. Probleme sind zu erwarten, wenn Sie häufig Dokumente mit Nutzern von Microsoft Office austauschen müssen. Die vollständige Übernahme der Formatierungen ist vor allem bei komplexeren Dokumenten nicht garantiert. Wer darauf angewiesen ist, nutzt unter Linux Microsoft Office in einer virtuellen Maschine. Informationen dazu gibt es in der LinuxWelt-Toolbox in der Rubrik „Ubuntu/Mint“ nach einem Klick auf „Virtualisierung“.

Mehr Kompatibilität zu Microsoft-Produkten verspricht Softmaker Office (*www.softmaker.de*). Die Importfilter sind besser als die von Libre Office. Wer das ausprobieren möchte, kann sich bei Softmaker eine kostenlose 30-Tage-Demo herunterladen. Die Vollversion Softmaker Office Standard 2018 kostet 69,95 Euro. Für 99,95 Euro gibt es Softmaker Office Professional 2018, das mit dem Duden-Korrektor eine leistungsfähige Rechtschreibprüfung enthält. Außerdem können Sie die Gratisversion Free Office (*www.freeoffice.com*) nutzen, die sich nur in Kleinigkeiten von der Kaufversion unterscheidet (siehe *https://www.freeoffice.com/de/vergleich*).

Installation: Libre Office ist in der Regel standardmäßig eingerichtet und steht in den Standard-Paketquellen bereit. Wer eine aktuellere Version installieren möchte, verwendet die Anleitung aus der LinuxWelt-Toolbox in der Rubrik „Office“.

2. Erweiterungen für Libre Office

Über Erweiterungen (*http://extensions.libreoffice.org*) erhält Libre Office zusätzliche Funktionen. Empfehlenswert ist die verbesserte Rechtschreib- und Grammatikprüfung Language Tool (*www.languagetool.org*). Die Installationsanleitung liefern wir Ihnen in der LinuxWelt-Toolbox (Schaltfläche „Office-Pakete“).

Sie können selbst Makros für Libre Office erstellen, um häufig wiederkehrende Arbeitsschritte zu automatisieren. Komplexere Programme, sogar mit einer eigenen Benutzeroberfläche, sind ebenfalls möglich, erfordern jedoch Programmierkenntnisse. Den Einstieg in die Makroprogrammierung erleichtert der Makrorecorder, mit dem Sie Menüklicks sowie Tastatureingaben aufzeichnen und später wiedergeben. Informationen zu Makros und einige nütz-

liche Beispiele haben wir in der LinuxWelt-Toolbox untergebracht (Schaltfläche „Makros für Libre Office“).

3. Alternative Office-Programme

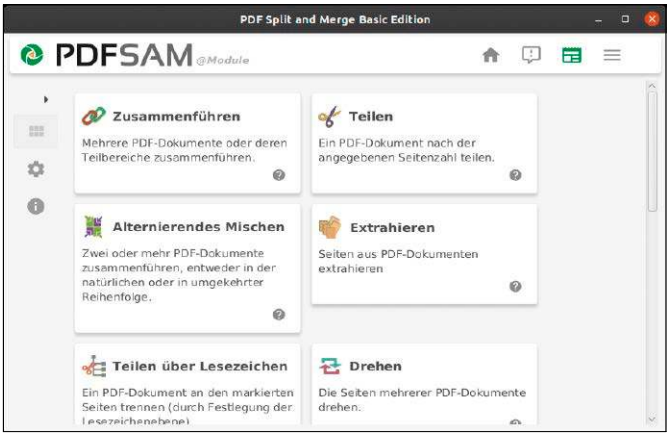
Wer ab und zu einen Brief schreibt, für den kann auch Abiword ausreichend sein (*www.abiword.org*). Die Bedienung ist einfach und orientiert sich an den Standards von Libre Office und Word 2003. Abiword benötigt kaum Systemressourcen und ist Standard bei leichtgewichtigen Linux-Distributionen. Das Gleiche gilt auch für die Tabellenkalkulation Gnumeric (*www.gnumeric.org*). Den Funktionsumfang von Excel erreicht das Programm nicht, dafür gibt es aber ausgefeilte finanzmathematische Funktionen und ein gut bedienbares Modul, mit dem sich Graphen erzeugen lassen.

Mit Scribus layouten Sie Broschüren, Zeitschriften und mehr (*www.scribus.net*). Das Programm beherrscht professionellen Textsatz und kann Dokumente so für den Druck vorbereiten, dass auch die Farben stimmen (CMYK-Farbseparation).

Calibre ist ein plattformunabhängiges Programm zur Verwaltung und Konvertierung von E-Books (*http://calibre-ebook.com*). Es kennt alle gängigen Formate wie Epub, LRF, Mobi und PDF. Außerdem lassen sich die Inhalte auf E-Book-Readern übertragen.

Installation: Informationen zu den genannten Tools finden Sie in der LinuxWelt-Toolbox über die Schaltfläche „Office-Programme“.

Anspruchsvolle Broschüren: In Scribus arbeiten Sie mit Text- und Bildrahmen, was ein professionelles Layout beispielsweise für Flyer, Zeitschriften und andere Druckwerke erlaubt.



Tools für PDFs: PDF Split and Merge kann PDF-Dateien bearbeiten. Sie können beispielsweise PDFs neu aufteilen, zusammenführen oder einzelne Seiten entnehmen.

4. Produktive Desktoptools

Die Dateimanager unter Ubuntu und Linux Mint bieten eine Suchfunktion, mit der Sie Ordner und Dateien über ihren Namen finden. Wenn Sie auch Dateiinhalte finden wollen, benötigen Sie ein Tool wie Docfetcher (*http://docfetcher.sourceforge.net*). Das Programm leistet eine Volltextsuche für Libre und Microsoft Office, Abiword, PDF, Epub sowie Textdateien aller Art. Docfetcher arbeitet mit einem Index, den Sie zunächst für das gewünschte Verzeichnis erstellen. Die Volltextsuche arbeitet mit logischen Operatoren und zeigt eine Vorschau der Fundstellen.

Das Tool Recoll (*www.lesbonscomptes.com/recoll*) leistet Ähnliches, bietet aber eine fortgeschrittene Abfragesyntax. Sie können Suchabfragen formulieren, die das Suchergebnis auf Metadaten wie Autorenname oder Schlüsselwörter eingrenzen. Recoll bringt außerdem einen eigenen Webserver mit, mit dessen Hilfe Sie anderen PCs im Netzwerk die Suche im Browserfenster zur Verfügung stellen.

Installation: Docfetcher ist ein portables Tool für alle Betriebssysteme und benötigt eine Java-Runtime (Paket: „default-jre“). Sie müssen es nur herunterladen und entpacken. Recoll lässt sich unter Ubuntu und Linux Mint direkt installieren. Lesen Sie dazu die Anleitung in der LinuxWelt-Toolbox nach einem Klick auf „Desktop-Tools“.

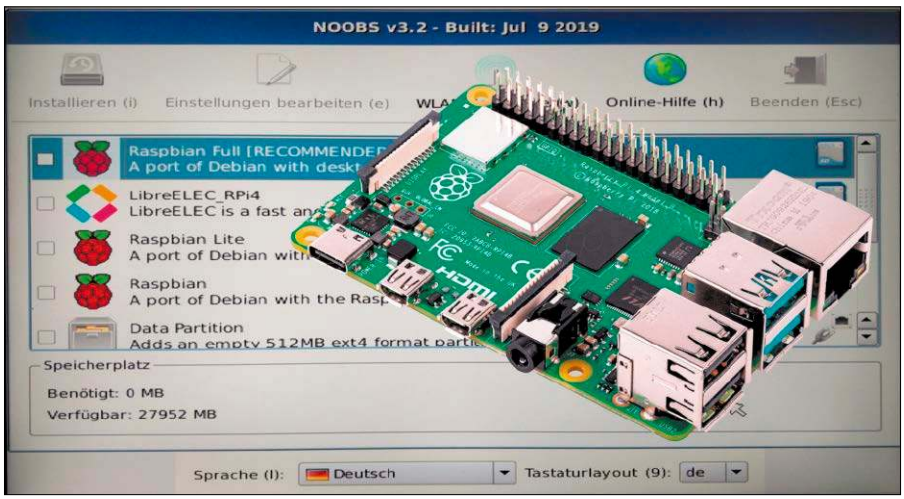
5. PDFs erstellen und bearbeiten

Mit den genannten Office-Paketen (siehe Punkt 1) lassen sich Dokumente im PDF-Format speichern. Libre Office kann PDFs auch öffnen und bearbeiten, mit Inkscape geht das ebenfalls, allerdings nur mit einzelnen Seiten. Da PDF ein Format für die Archivierung von Dokumenten und den Druck ist, sind der Nachbearbeitung Grenzen gesetzt. PDFs lassen sich jedoch ohne Problem aufteilen, Sie können einzelne Seiten extrahieren, hinzufügen, löschen oder drehen. Ein geeignetes Tool dafür ist PDF-Shuffler (Paket: „pdfshuffler“, Ubuntu 19.10: „pdfarranger“). Noch mehr Funktionen und eine ansprechende grafische Oberfläche bietet PDF Split and Merge (Paket: „pdfsam“). Es kann Dokumente zusammenfügen und zerteilen, Seiten drehen und umsortieren. Sie können Dokumente per Maus zusammenstellen und sehen dabei stets eine Vorschau des fertigen PDFs.

Installation: PDF-Shuffler ist in den Standardrepositorien enthalten. Aktuelle Versionen von PDF Split and Merge gibt es auf der Downloadseite des Herstellers. In der LinuxWelt-Toolbox finden Sie nach einem Klick auf „PDF-Tools“ eine Anleitung zu Installation und Downloadlinks. ■

Software für Platinenrechner

Der Erfolg des Raspberry Pi hat die Entwicklung von Mini-PCs vorangetrieben. Dank geringer Leistungsaufnahme eignen sich die Geräte hervorragend als Dateiserver oder Mediacenter am TV-Gerät.



Einfache Installation: Die Noobs-Dateien kopieren Sie auf eine FAT32-formatierte SD-Karte. Das gewünschte Betriebssystem wählen Sie dann direkt auf dem Raspberry Pi.

VON THORSTEN EGGELING

Mini-PCs gibt es in unterschiedlichen Preislagen und mit mehr oder weniger leistungsfähiger Hardware. Nicht jeder Platinenrechner eignet sich für beliebige Einsatzbereiche. Für Dateiserver sind Gigabit-Ethernet und USB 3.0 oder ein SATA-Adapter wünschenswert, für die Medienwiedergabe ein Grafikchip mit Hardwarebeschleunigung. Der Raspberry Pi 4 deckt die meisten Bereiche ab, weshalb wir uns hier auf dieses Gerät konzentrieren. Informationen zu anderen Mini-PCs, Downloadlinks und die Befehlszeilen aus diesem Artikel liefert die LinuxWelt-Toolbox in der Rubrik „Platinenrechner".

1. Systeme für den Raspberry Pi

Der Installer Noobs (*www.raspberrypi.org/downloads/noobs*) – „New Out Of Box Software" – ist für Raspberry-Einsteiger der einfachste und schnellste Weg für die Systeminstallation. Die Standardversion (2,4 GB) enthält bereits das Desktopsystem Raspbian („Full"), das auf Debian basiert und die Multimedia-Zentrale Libre Elec mitbringt. Sie können während der Installation auch Raspbian Lite ohne Desktopumgebung herunterladen. Bei der Noobs-Lite-Variante (38 MB) laden Sie das gewünschte System immer während der Installation herunter.

Entpacken Sie Noobs auf eine FAT32-formatierte SD-Karte mit mindestens acht GB Kapazität. Anschließend legen Sie die Karte in den Raspberry ein. Im unteren Bereich des Fensters wählen Sie als Sprache „Deutsch" und stellen bei „Tastaturlayout" den Wert „de" ein. Setzen Sie ein Häkchen vor dem gewünschten Betriebssystem, klicken Sie auf „Installieren" und folgen Sie den weiteren Anweisungen des Assistenten.

Wenn Sie mehrere Systeme wählen, muss die SD-Karte genug Platz bieten. Den benötigten und verfügbaren SD-Speicher zeigt Noobs an. Planen Sie Reserven ein, damit Updates und zusätzliche Software auf die SD-Karte passen. Beim Start wählen Sie im Bootmenü das gewünschte System, das zuletzt verwendete startet nach kurzer Wartefrist automatisch. Drücken Sie beim Start die Shift-Taste, sobald die Aufforderung dazu erscheint, um wieder auf die Noobs-Oberfläche zu gelangen. Hier können Sie die Systemauswahl ändern oder ein weiteres System installieren. Dabei wird ein bereits vorhandenes System allerdings überschrieben, was einer Neuinstallation entspricht.

Hinweis: Noobs kommt manchmal nicht mit SD-Karten größer 32 GB zurecht, auch wenn diese mit FAT32 formatiert sind und zumindest ab Raspberry Pi 3 auch Karten mit mehr als 256 GB funktionieren sollten. In diesem Fall laden Sie das Abbild des gewünschten Systems herunter und kopieren es auf die SD-Karte, wie in der LinuxWelt-Toolbox unter „Systeme für den Pi" beschrieben.

Noch mehr Systeme: Über *www.raspberrypi.org/downloads* finden Sie weitere Betriebssysteme für den Raspberry Pi, beispielsweise Ubuntu Mate, Ubuntu Server, das Mediacenter OSMC und Windows 10 IoT Core. Der Inhalt der heruntergeladenen Abbilddatei muss auf die SD-Karte kopiert werden. Detaillierte Anleitungen dazu finden Sie in der LinuxWelt-Toolbox („Systeme für den Pi").

Installation: In der LinuxWelt-Toolbox finden Sie in der Rubrik „Platinenrechner“ Downloadlinks und Beschreibungen wichtiger Betriebssysteme für den Raspberry Pi.

2. Raspberry Pi als Dateiserver

Wenn Sie einen Raspberry Pi als Datenspeicher im Netzwerk bereitstellen wollen, installieren Sie unter Raspbian das Programmpaket „samba“. Da Samba eine eigene Benutzerdatenbank verwendet, benutzen Sie folgenden Befehl, um für den Standardbenutzer „pi“ ein Passwort festzulegen:

```
sudo smbpasswd -a pi
```

Das genügt, um über einen Dateimanager unter Linux oder Windows eine Verbindung herzustellen. Standardmäßig ist das Home-Verzeichnis schreibgeschützt freigegeben. In Nautilus oder Nemo tippen Sie beispielsweise folgende URL in die Adresszeile ein (einblenden mit Strg-L).

```
smb://[Raspberry]/pi/
```

Den Platzhalter „[Raspberry]“ ersetzen Sie durch den Hostnamen oder die IP-Adresse des betreffenden Raspberry Pi. Sie haben dann Lesezugriff auf das Home-Verzeichnis des Benutzers „pi“.

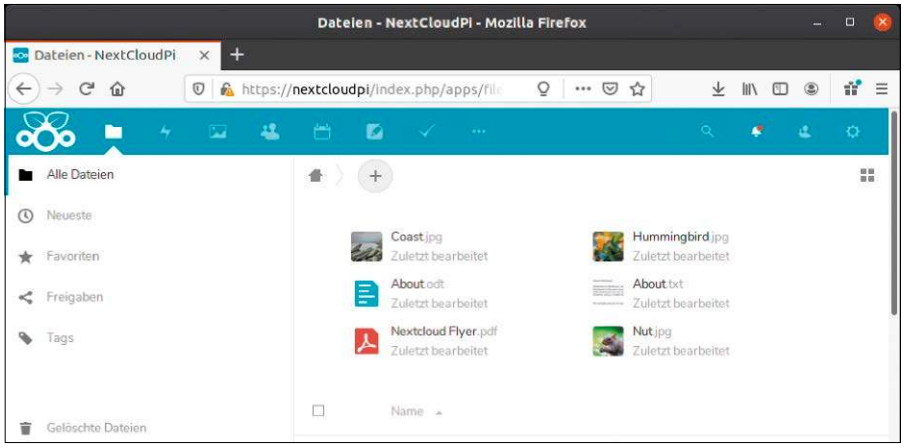
Installation: Die Befehlszeilen zur Installation und Konfiguration des Samba-Servers finden Sie in der LinuxWelt-Toolbox nach einem Klick auf „Datenserver“. Hier erfahren Sie auch, wie Sie den Lesezugriff auf das Home-Verzeichnis aktivieren und andere Ordner freigeben.

3. Raspberry Pi als Cloudserver

Nextcloud (*https://nextcloud.com*) bietet fast alles, was für den Datenaustausch über das lokale Netzwerk oder Internet erforderlich ist, beispielsweise Kalender, Adressbuch, Fotogalerie, Wiedergabe von und Musik und Videos sowie gemeinsames Arbeiten an Dokumenten. Über Plug-ins lassen sich die Funktionen noch erweitern. Der Zugriff erfolgt über eine Weboberfläche oder Sie verwenden eine Clientsoftware für Windows, Mac-OS, Linux, Android oder iOS, um einen lokalen Ordner mit dem Cloudserver zu synchronisieren.

Nextcloud lässt sich auf dem Raspberry Pi entweder als Neuinstallation fertig vorbereitet zusammen mit Raspbian oder nachträglich in einem laufenden Raspbian einrichten. Die erste Variante ist vorzuziehen, außer Sie betreiben bereits ein auch für andere Dienste konfiguriertes Raspbian. In der LinuxWelt-Toolbox finden Sie ausführliche Anleitungen für beide Wege. Soll der heimische Nextcloud-Server auch aus dem Internet erreichbar sein, richten Sie einen Dienst für dynamische IP-Adressen ein. Wie das geht, erfahren Sie in der LinuxWelt-Toolbox unter „Netzwerk → Portweiterleitung“. ■

Freigaben im Netzwerk: Samba verwandelt den Raspberry Pi in einen Dateiserver. Ohne weitere Konfiguration ist der Zugriff auf das Home-Verzeichnis des Benutzers „pi“ möglich.



Die eigene Cloud: Nextcloud vereinfacht den Datenaustausch über das lokale Netzwerk und das Internet. Der Funktionsumfang lässt sich über zusätzliche Apps erweitern.

BEISPIELPROJEKTE FÜR DEN RASPBERRY PI

In der LinuxWelt berichten wir regelmäßig über nützliche Raspberry-Pi-Projekte. Mit einem Stück Extrasoftware oder zusätzlicher Hardware lässt sich das Gerät vielfältig einsetzen. Ausführliche Anleitungen lesen Sie in der LinuxWelt-Toolbox in der Rubrik „Platinenrechner“.

Kontrolle per LCD: Oft verrichtet ein Raspberry Pi im Netzwerk ohne Monitor und Eingabegeräte seine Dienste – meist genügt ein gelegentlicher Besuch per SSH. Ein günstiges LCD zur Ausgabe von Systeminformationen macht die Platine aber gesprächiger.

Werbeblocker für das Netzwerk: Das Projekt Pi-Hole ist nicht nur ein schwarzes Loch für Werbung, sondern es blockiert auch Tracker, die Ihr Surfverhalten verfolgen und monetarisieren möchten. Die Software läuft auch auf dem Raspberry Pi, klinkt sich in Ihr Netzwerk ein und arbeitet auf DNS-Basis.

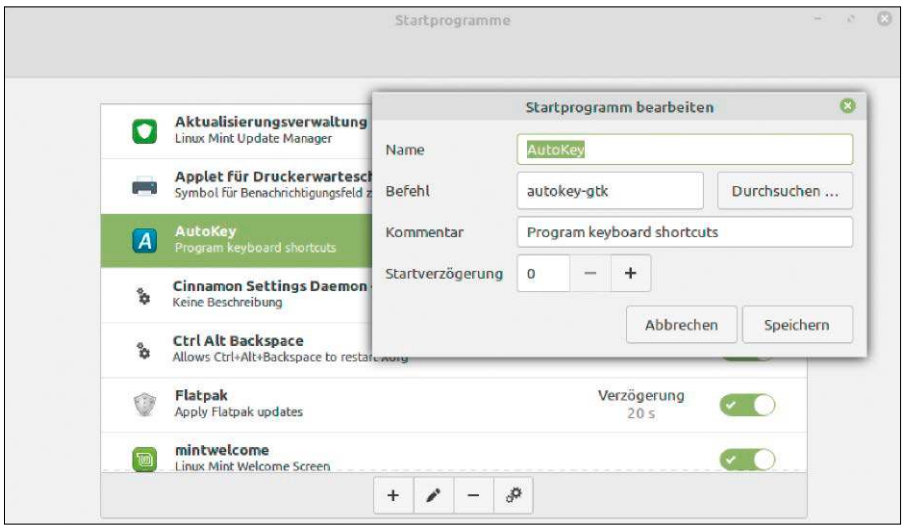
Pi als Webcam: Der Raspberry Pi lässt sich für etwa 30 Euro mit einer Kamera ausstatten. Per Script laden Sie Einzelbilder regelmäßig auf einen Webserver hoch. Wenn Sie Live-Videostreams bevorzugen, gibt es auch dafür eine Lösung. Das System lässt sich damit auch für die Raumüberwachung mit automatischer Bewegungserkennung einsetzen.

Streamingdienste einbinden: Um die Musiksammlung aus Streamingdiensten in den eigenen vier Wänden über Lautsprecher auszugeben, bietet sich der Raspberry Pi als einfache und preiswerte Lösung an.

Tools für die Linux-Automatisierung

Regelmäßige Aufgaben wie beispielsweise Backups lassen sich unter Linux automatisch durchführen. Mit Shell-Scripts und Zusatztools können Sie aber praktisch jedes Vorhaben automatisieren.

VON THORSTEN EGGELING



Programme automatisch starten: Soll ein Programm direkt nach der Anmeldung sofort zur Verfügung stehen, erstellen Sie dafür einen Eintrag mit „Startprogramme“.

Linux erledigt schon von Haus aus einige Aufgaben automatisch im Hintergrund. Das System erstellt beispielsweise Backups wichtiger Konfigurationsdateien, archiviert Logdateien und prüft auf Updates. Die Infrastruktur lässt sich für eigene Backup-Scripts oder andere regelmäßige Wartungsarbeiten nutzen. Automatisierung ist auch sinnvoll, wenn Sie mehrere Arbeitsschritte nacheinander häufig ausführen müssen. Dabei hilft ein einfaches Script für die Bash-Shell, das Sie manuell, zeitgesteuert oder per automatische Ordnerüberwachung starten. Hilfetexte und Befehlszeilen für die Installation von Automatisierungswerkzeugen finden Sie in der LinuxWelt-Toolbox in der Rubrik „Automatisierung“.

1. Programme automatisch starten

Bei der Anmeldung automatisch startende Programme gehören zum Repertoire jedes Desktopsystems. Zur Verwaltung suchen Sie unter Ubuntu über „Aktivitäten“ nach „Startprogramme“, bei Linux Mint gehen Sie im Menü auf „Einstellungen → Startprogramme“. Über „Hinzufügen“ beziehungsweise die Plus-Schaltfläche lassen sich Programme in den Autostart aufnehmen. Das ist bei einigen Systemtools nützlich (siehe Punkt 2), es kann sich aber um beliebige Programme handeln. In der Regel genügt hinter „Befehl“ der Programmname ohne Pfad. Mint-Nutzer können eine Startverzögerung einstellen, damit das System unmittelbar nach der Anmeldung nicht zu sehr belastet wird.

2. Textbausteine und Scripts mit Autokey

Das englischsprachige Autokey ist ein vielseitiges Tool für systemweite Textbausteine bis hin zu raffinierten Scripts. Sie legen damit Textbausteine an, die Sie über ein Kürzel oder eine Tastenkombination in einen Editor, die Textverarbeitung, das E-Mail-Programm oder das Terminalfenster einfügen. Autokey beherrscht außerdem Scripts, um komplexere Aufgaben der Automatisierung zu erledigen.

Autokey ist in den Paketquellen von Ubuntu 16.04, 18.04 und 19.10 enthalten (Paket: „autokey-gtk“). Das Programm lässt sich standardmäßig über ein Panel-Icon steuern, was bei Ubuntu 18.04 und 19.10 jedoch nicht erscheint, bei Linux Mint 19 sehen Sie es in der Leiste am unteren Bildschirmrand. Wie Sie Ubuntu dazu bringen, Autokey automatisch zu starten und das Panel-Icon anzuzeigen, lesen Sie in der LinuxWelt-Toolbox nach einem Klick auf „Autokey“. Hier finden Sie neben der Installationsanleitung auch Tipps zur Konfiguration und Beispiel-Scripts.

3. Zeitgesteuerte Tasks mit Cron

Auf Linux-Systemen läuft ein Crondienst, der Aufgaben zeitgesteuert ausführt. Cron nutzt eine systemweite Datei „/etc/crontab“, die für alle Benutzer gilt und im Terminal mit root-Recht bearbeitet werden kann:

```
sudo crontab -e
```

Zusätzlich kann jeder Benutzer in einer eigenen Crontab Programme laden, indem er *crontab -e* ohne „sudo“ aufruft. Crontab-Einträge benötigen fünf Zeitangaben (Minute, Stunde, Tag, Monat, Wochentag) mit Leerzeichen oder Tabulatoren getrennt, danach den Programmbefehl. Ein Backup, das täglich um 22:00 Uhr laufen soll, kann dann so aussehen:

```
0  22  *  *  *  rsync -av /home/sepp/
  /media/sepp/USB/backup
```

Der Asterisk (*) bedeutet wie üblich „alle“ an der betreffenden Stelle – hier also „an jedem Tag, jedem Monat und jedem Wochentag“. Um Formatfehler bei relativ einfachen Zeitangaben zu vermeiden, gibt es simplifizierende Variablen, die Sie anstelle der fünf Zeitangaben verwenden können (@hourly, @daily, @weekly, @midnight). So ist etwa die Variable „@midnight“ identisch mit der ausgeschriebenen Schreibweise „0 0 * * *“. Einen ausführlichen Beitrag zu Cron finden Sie in der LinuxWelt-Toolbox nach einem Klick auf „Cronjobs“.

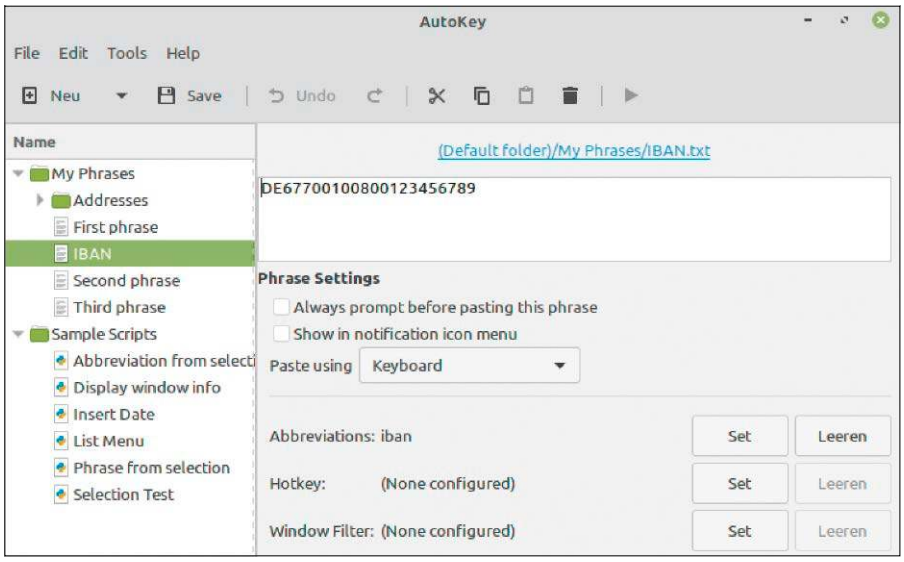
4. Crontab mit grafischen Tools bearbeiten

Bei Systemen mit KDE-Desktop (Kubuntu) installieren Sie das Paket „kde-config-cron“. In den „Systemeinstellungen“ lassen sich dann unter „Starten und Beenden → Aufgabenplaner“ Zeitpläne für den automatischen Start erstellen. Für Ubuntu und Linux Mint eignet sich das Tool Gnome-Schedule. Es ist jedoch nicht in den Paketquellen enthalten und es gibt auch kein PPA. Sie können das Tool aber selbst kompilieren. Die Anleitung dazu finden Sie in der LinuxWelt-Toolbox nach einem Klick auf „Aufgaben planen“.
Gnome-Schedule bietet auch eine Möglichkeit, definierte Aktionen über das Tool at einmalig zu einem bestimmten Zeitpunkt auszuführen. Die wichtigsten Intervalle wie „Jeden Tag“ finden Sie klickfertig vor und die „Vorschau“ bietet in der Form „An jedem Tag um 01:00“ eine gute Kontrolle.

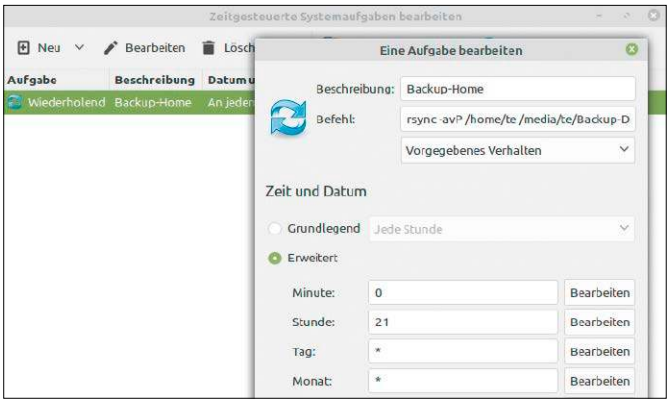
5. Automatische Datensicherung

Backups anzulegen ist unverzichtbar. Sie müssen die nötigen Vorkehrungen jedoch nur einmal treffen, den Rest übernimmt Linux automatisch. Das Kommandozeilentool rsync arbeitet zuverlässig und schnell und ist in allen verbreiteten Linux-Distributionen standardmäßig enthalten. Es lässt sich mit zahlreichen Schaltern und Optionen für jede Aufgabe anpassen, im Alltag genügen aber einige wenige.
Backups sollten immer auf unabhängige Datenträger erfolgen – etwa auf eine zweite interne Festplatte oder ein USB-Laufwerk. Für ein einfaches manuelles Backup des eigenen Home-Verzeichnisses auf eine USB-Festplatte genügt folgendes Kommando:

```
rsync -avP $HOME /media/$USER/
  [Laufwerks-ID]/backup
```



Textbausteine: Häufig genutzte Textabschnitte legen Sie in Autokey fest. Über ein Kürzel lässt sich der Text dann in jedem beliebigen Programm einfügen.



Automatisierte Aufgaben: In Gnome-Schedule erstellen Sie Cronjobs für einmalige oder wiederkehrende Aufträge. Das eignet sich etwa für regelmäßige Backups.

Die „Laufwerks-ID“ ist die Bezeichnung einer USB-Festplatte, die Linux automatisch unter „/media/$USER“ eingebunden hat. Ändern Sie den Pfad entsprechend Ihrer Systemkonfiguration. „$USER“ ist eine Standardvariable für den Namen des Benutzers, „$HOME“ für den Pfad zum Home-Verzeichnis. Das Ziel „backup“ erstellt rsync automatisch, wenn es noch nicht vorhanden ist.
Backup-Script für rsync: Klicken Sie in der LinuxWelt-Toolbox auf „Rsync“. Hier finden Sie ein Shell-Script für inkrementelle Backups und Infos zu erweiterten Funktionen sowie Backups über SSH. Über die Aufgabenplanung (siehe Punkt 3 und 4) erstellen Sie einen Zeitplan für regelmäßige Backups.

6. Scripts und Ordnerüberwachung

Shell-Scripts sind Textdateien, die interne Shell-Befehle und Programmaufrufe enthalten. Im einfachsten Fall bringen Sie in einem Script nur einen oder mehrere Programmnamen sowie die gewünschten Optionen oder Parameter unter. Variablen, Schleifen („for … do … done“) und Bedingungen („if … fi“) ermöglichen komplexere Programmstrukturen.
In der LinuxWelt-Toolbox finden Sie nach einem Klick auf „Shell-Scripts“ einige Beispiele. Diese zeigen, wie sich Audio- und Bilddateien konvertieren oder Screenshots erstellen lassen. Shell-Scripts rufen Sie bei Bedarf manuell auf oder zeitgesteuert über einen Cronjob.
Für einige Aufgaben ist auch der automatische Aufruf per Ordnerüberwachung sinnvoll. Wie Sie diese einrichten, erfahren Sie nach einem Klick auf „Incron“. Mit diesem eleganten, aber nicht ganz einfachen Mechanismus können Sie dann beispielsweise Audiodateien automatisch in ein anderes Format umwandeln, sobald diese in einem bestimmten Ordner landen. ■

Service- & Mobilsysteme

Linux-Systeme sind flexibel und starten von jeder Art Datenträger. Auf einem USB-Stick oder einer USB-Festplatte lässt sich schnell ein Zweit- oder Reparatursystem einrichten.

VON THORSTEN EGGELING

Aus der LinuxWelt-Redaktion stammen die LinuxWelt-Rettungs-DVD (Linux-Wartung), das LinuxWelt-Surfsystem und die PC-WELT-Rettungs-DVD (Windows-Tools).

Mit Linux-Livesystemen kommen Sie spätestens bei der Installation von Ubuntu oder Linux Mint in Kontakt. Beide lassen sich von einer DVD oder einem USB-Stick starten und bieten einen ersten Eindruck von der Gestaltung des Desktops. Enthalten sind viele Programme, die Sie später auch beim installierten Linux nutzen, beispielsweise Firefox und Libre Office. Sollte ein Tool fehlen, lässt es sich auch im Livesystem installieren. Der Datenträger ist jedoch schreibgeschützt, sodass zusätzliche Programme bei einem Neustart wieder verschwunden sind. Das ist in den meisten Fällen auch erwünscht, damit das System immer in einem definierten Zustand startet und nicht manipuliert werden kann. Livesysteme eignen sich daher gut als sichere Surfumgebung.

1. Livesysteme für jeden Zweck

Installations-DVDs etwa von Ubuntu (19.10 auf Heft-DVD) oder Linux Mint eignen sich für Reparaturen, wenn das Hauptsystem einmal streikt. Auf die Version kommt es nicht an. Mit neueren Linux-Versionen lassen sich auch ältere Systeme reparieren. Nur die Architektur sollte übereinstimmen (32 oder 64 Bit).

Sie können beispielsweise die Dateien aus Ihrem Home-Verzeichnis sichern oder die Bootumgebung reparieren. Livesysteme sind außerdem so konstruiert, dass sich temporär Reparaturtools oder Analysesoftware nachinstallieren lassen. Allerdings überdauern hinzugefügte Dateien keinen Neustart. Auf einem USB-Stick lässt sich Ubuntu/Mint jedoch so einrichten, dass Programme und Konfiguration erhalten bleiben.

In der LinuxWelt-Toolbox bieten die ersten vier Einträge in der Rubrik „Service/Mobil-Systeme“ eine Übersicht mit den wichtigsten Livesystemen. Sie erfahren, was Sie beim Umgang mit den heruntergeladenen ISO-Dateien und beim Transfer auf einen USB-Stick beachten müssen.

Außerdem finden Sie Tipps zur Auswahl eines für Ihre Zwecke geeigneten Systems, ausführliche Installationsanleitungen und Downloadlinks.

2. Linux mit Zweitsystem reparieren

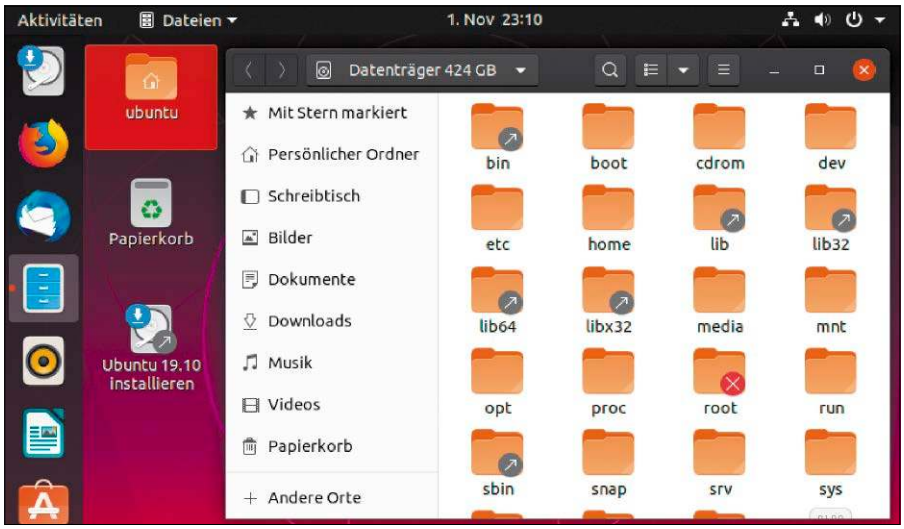
Über ein Livesystem erhalten Sie Zugriff auf die Partitionen eines installierten Betriebssystems. Das lässt sich nutzen, wenn Sie das Passwort vergessen haben, die Konfigurationsdateien bearbeiten oder den Bootmanager reparieren müssen.

Die LinuxWelt-Rettungssystem (*www.pcwelt.de/uqtBiY*) startet schnell und ist auf die Wartung von Linux-Installationen spezialisiert. Das System startet standardmäßig mit der grafischen Oberfläche XFCE und deutscher Tastaturbelegung. Im LinuxWelt-Rettungssystem sind der Dateimanager Thunar, Firefox und Filezilla installiert. Festplattenabbilder lassen sich mit Clonezilla erstellen, Partitionen verwalten Sie mit Gparted. Nach dem Start zeigt der Desktop automatisch ein Terminal mit root-Recht, in dem Sie die üblichen Linux-Tools für die Kommandozeile verwenden und beispielsweise Partitionen per mount-Befehl einhängen können. Als bequemer Dateimanager für das Terminalfenster ist außerdem der Midnight Commander (mc) installiert. Eine Anleitung mit praktischen Tipps erreichen Sie in der LinuxWelt-Toolbox per Klick auf „LinuxWelt-Rettungs-DVD“.

3. Windows mit Linux retten

Einige Windows-Probleme lassen sich nur über ein Zweitsystem beheben. Das ist beispielsweise nötig, wenn Windows nicht mehr startet und Sie nur einige wichtige Dokumente sichern wollen.

Die PC-WELT-Rettungs-DVD (*www.pcwelt.de/pcwrescue*) enthält spezielle Tools für Windows-Systeme, kann aber auch für Linux wertvolle Dienste leisten. Sie können den Browser Firefox für die Recherche im Internet nutzen, außerdem sind Clonezilla und Gparted an Bord. Nach einem Klick auf „Rettungswerkzeuge“ sehen Sie die Menüeinträge für Tools, mit denen Sie das Windows-Passwort löschen, gelöschte Dateien („QPhotorec“) wiederherstellen oder nach Schadsoftware („ClamAV“) suchen können. Wenn möglich, sollten Sie das PC-WELT-Rettungssystem von einem USB-Stick booten. Es startet dann schneller. Wie Sie die PC-WELT Rettungs-DVD auf einem USB-Stick einrichten – auch mit permanentem und verschlüsseltem Speicher – erfahren Sie in der LinuxWelt-Toolbox unter „PC-WELT Rettungs-DVD“.



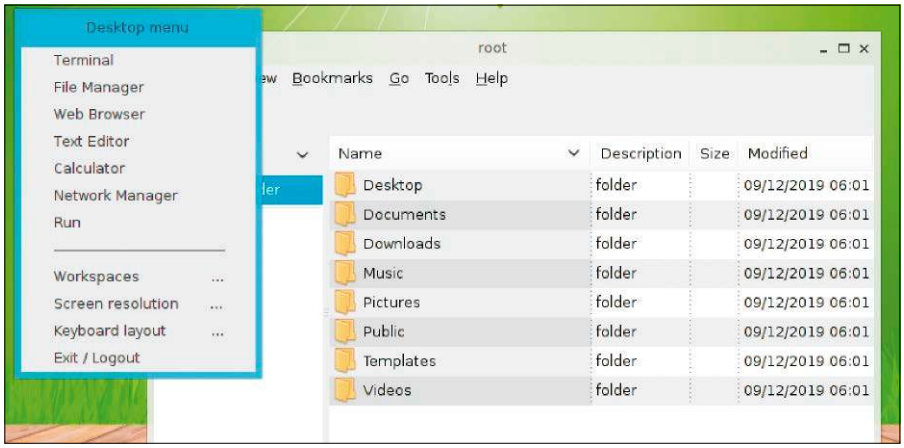
Das Ubuntu-Installationsmedium genügt für viele Reparaturen, Konfigurationsänderungen und die Datenrettung. Weitere Tools lassen sich nachinstallieren.

4. Mini-Linux- und Surfsysteme

Das LinuxWelt-Surfsystem bietet eine komfortable deutschsprachige Desktopumgebung. Es ist nur rund 500 MB groß und enthält die Browser Chromium, Firefox sowie Vivaldi. Außer den Browsern stehen im Livesystem der Partitionierer Gparted, der Mediaplayer Audacious sowie der Gnome Mplayer zur Verfügung. Zur Übertragung auf USB-Stick verwenden Sie im laufenden System das Tool unter „Applications → System Tools → create live USB“. Das dazu abgefragte root-Passwort lautet „toor“.

Slax gehört zu den wirklich kleinen und schnellen Livesystemen (264 MB): Viel mehr als ein Browser, Mediaplayer und ein rudimentärer Desktop ist nicht dabei. Über einen Rechtsklick auf den Desktophintergrund aktivieren Sie im Menü „Keyboard Layout → German“ das deutsche Tastaturlayout. Ein Klick auf das Starter-Symbol rechts unten blendet die verfügbaren Programme ein, inklusive dem „Net Manager“ zum Aufbau einer WLAN-Verbindung. Außerdem gibt es als grafischen Dateimanager den kleinen Pcmanfm von LXDE.

Neben dem Browser Chromium sind das Terminal, Texteditor und Taschenrechner dabei. Weitere Softwarepakete gibt es zum temporären Nachinstallieren über eine Internetverbindung mit apt-get im Terminal.



Minimales Livesystem: Slax ist klein und startet schnell. Es bietet eine einfache Oberfläche, über die sich beispielsweise Browser und Texteditor starten lassen.

Das Livesystem Tails erfüllt nur einen Zweck: Den unkomplizierten Zugang zum TOR-Netzwerk. Hinter dem Kürzel TOR steht das Netzwerk „The Onion Router“ – eine Verkettung anonymisierender Proxyserver. Dieses Proxynetzwerk erlaubt auch in Zeiten von rigoroser Überwachung des Netzwerkverkehrs ein hohes Maß an Anonymität.

Informationen zu den genannten Systemen inklusive Downloadlinks finden Sie in der LinuxWelt-Toolbox in der Rubrik „Service/Mobil-Systeme“. ■

FIRMWAREEINSTELLUNGEN FÜR LIVESYSTEME

Die meisten Linux-Systeme starten problemlos auf jedem Rechner. Wenn nicht, prüfen Sie die Bios-/Firmwareeinstellungen. Suchen Sie nach Optionen wie „CSM“, „Uefi and CSM“ oder „Uefi and Legacy“, die meist unter Menüs wie „Boot“ oder „Boot Order“ zu finden sind. Die Bios-Emulation CSM (Compatibility Support Module) sollte aktiviert sein, damit der PC sowohl im Uefi- als auch im Bios-Modus booten kann. Deaktivieren Sie Secure Boot. Die Funktion verhindert den Start der meisten Livesysteme. Ändern Sie außerdem die Bootreihenfolge, damit der PC vom DVD-Laufwerk oder USB-Stick bootet.

Mehr Schutz dank Sicherheitsschlüssel

Alleine mit einem Passwort sind Onlinedienste nicht optimal geschützt. Ein USB-Sicherheitsschlüssel verbessert den Schutz und kann auch die Linux-Anmeldung absichern.

VON THORSTEN EGGELING

Gefahr für Onlinekonten: Die Absicherung nur mit Benutzername und Passwort bedroht Ihre Onlineidentität. Sicher ist eine Zwei-Wege-Authentifizierung.

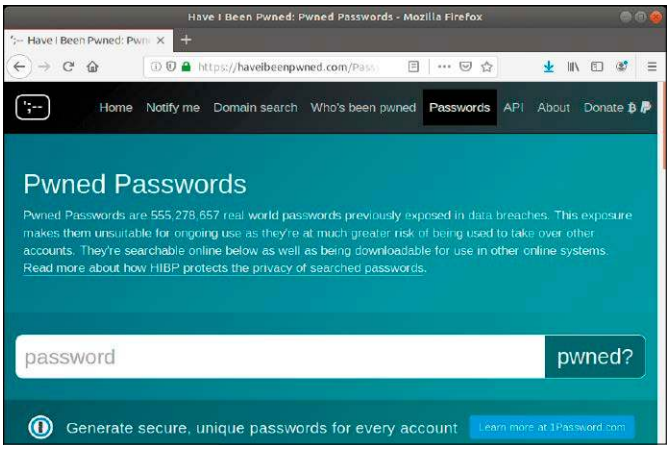
Die Anmeldung mit Benutzername und Passwort gilt seit langem als die größte Schwachstelle bei jeder Art von Authentifizierung. Einfache Passwörter lassen sich erraten oder ausprobieren und komplexe Passwörter überfordern den Benutzer. Zudem bietet auch das beste Passwort keinen Schutz, wenn es nach dem Einbruch in den Server eines Onlinedienstes in falsche Hände gerät. Onlinekonten und PCs lassen sich jedoch über eine Zwei-Wege-Authentifizierung effektiv absichern. Die Idee dahinter ist einfach: Bei der Anmeldung muss neben Benutzernamen und Passwort ein weiterer Faktor hinzukommen. Dafür gibt es unterschiedliche Verfahren. Die Identität lässt sich beispielsweise über einen Code prüfen, den Sie sich per SMS zusenden lassen, über eine App auf dem Smartphone oder mit Hilfe zusätzlicher Hardware. Nicht alle Methoden bieten die gleiche Sicherheit.

Service: Die Befehlszeilen, Scripts und Beispielkonfigurationen dieses Artikels sowie weitere Information zum Thema finden Sie über *www.pcwelt.de/5Wk1MZ*.

1. Das Problem mit den Passwörtern

Die Authentifizierung nur mit dem Benutzernamen und Passwort ist aus mehreren Gründen problematisch. Zu einfache Passwörter stellen eine Gefahr dar, weil Onlinekonten einfach durch Ausprobieren gekapert werden können. Aber auch bei komplexen Passwörtern gibt es keine vollständige Sicherheit.

Passwort und Benutzername sind beim Anbieter in einer Datenbank gespeichert. Gerät die Benutzerdatenbank nach einem Servereinbruch in falsche Hände, können Sie nicht sicher sein, ob fremde Personen Zugriff auf Ihr Konto haben. Die Anbieter informieren meist – aber nicht immer – per E-Mail und fordern Sie dazu auf, das Passwort zu ändern. Oft wird der Einbruch aber nicht sofort bemerkt. Deshalb gilt die Empfehlung, bei den diversen Onlinediensten stets unterschiedliche Passwörter zu verwenden. Das erhöht für Sie als Benutzer allerdings den Aufwand bei der Passwortverwaltung.



Datendiebstahl: Mailadressen und Passwörter können bei Servereinbrüchen in falsche Hände geraten. Ob Ihre Daten gestohlen wurden, lässt sich unter *https://haveibeenpwned.com* ermitteln.

Tipp: Ob Ihre E-Mail-Adresse oder das Passwort bei einem Servereinbruch kopiert worden sind, können Sie übrigens unter *https://haveibeenpwned.com* herausfinden.

2. Die Lösung: Zwei-Faktor-Authentifizierung

Mehr Sicherheit lässt sich durch die Kombination von Benutzernamen und Passwort mit einer weiteren Information erreichen. Der zusätzliche Faktor stammt im optimalen Fall von einem anderen Gerät oder Medium. Der Vorteil: Das Passwort muss dann nicht besonders kompliziert sein und wenn es in falsche Hände geraten sollte, dann spielt das keine Rolle. Der Zugang zum Konto wird erst gewährt, wenn Sie sich mit einem zusätzlichen Schlüssel ausweisen. Bei der Anmeldung sollten mindestens zwei der drei folgenden Elemente zum Einsatz kommen:

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

„Besitz" kann beispielsweise eine ausgedruckte Liste, SMS, Smartphone-App oder ein Nummerngenerator sein. Die Kombination aus „Wissen" und „Besitz" ist am leichtesten umzusetzen, weil dafür meist bereits vorhandene Hardware wie ein Smartphone genutzt werden kann.

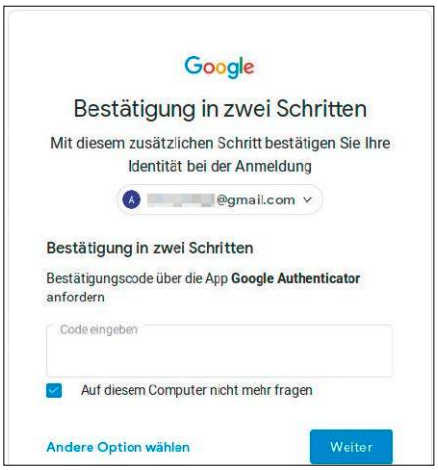
Je nach Konfiguration wird neben dem Passwort der Sicherheitsschlüssel bei jeder Anmeldung oder sicherheitsrelevanten Aktion angefordert oder er gilt dauerhaft für ein bestimmtes Gerät beziehungsweise den verwendeten Browser. Unbefugte Personen, die Ihr Passwort in Erfahrung gebracht haben, benötigen daher in jedem Fall zusätzlich den Sicherheitsschlüssel, wenn sie sich auf einem anderen PC anmelden.

3. Sicherheit von Einmalpasswörtern

Vor allem Banken haben in der Vergangenheit bei der Zwei-Wege-Authentifizierung auf Einmalpasswörter in Form einer TAN gesetzt (OTP: One Time Password). Die gab es zuerst als ausgedruckte Listen und dann per SMS. Im Prinzip wäre das sicher, wenn Bankingteilnehmer nicht immer wieder TANs über Phishingseiten preisgegeben hätten. SMS lassen sich durch Trojaner auf dem Smartphone abfangen oder beim Mobilfunkanbieter mitlesen. Banken sind aufgrund gesetzlicher Vorgaben dazu verpflichtet, die möglichen Risiken zu reduzieren. Beim Onlinebanking beispielsweise wurden Sie mit den geänderten Anforderungen wahrscheinlich schon konfrontiert. Die meisten Banken fordern inzwischen die zusätzliche Authentifizierung über eine Banking-App oder einen Chip-TAN/Smart-TAN-Generator an. Banking-Apps können als sicher gelten, solange PC und Smartphone nicht durch Schadsoftware kompromittiert sind oder Benutzername, Passwort und Smartphone nicht in falsche Hände geraten.

TAN-Generatoren arbeiten offline und sind daher vor Hackerangriffen geschützt. Zudem benötigen Sie Ihre Bankkarte, um eine TAN zu erzeugen. Diese gilt nur für einen bestimmten Auftrag, dessen Daten Sie auf dem Display des TAN-Generators prüfen sollten. Die Auftragsdaten lassen sich bei Geräten mit optischen Sensoren von einem Flickerbild auf dem PC-Monitor einlesen. Das Verfahren kann als sicher gelten, solange unbefugte Personen nicht in den Besitz von Bankkarte und Zugangsdaten gelangen. Wenn Sie den Verlust bemerken und die Karte sperren lassen, erzeugt der Generator keine gültigen TANs mehr.

Eine weitere Variante sind Passwörter, die nur eine Zeitlang gültig sind (TOTP: Time-based One Time Password). Weit verbreitet ist die Smartphone-App Google Authenticator, die von Google, Amazon, Paypal und weiteren Diensten unterstützt wird. Bei der Initialisierung, also bei der Einrichtung der Zwei-Faktor-Authentifizierung, wird ein geheimer Schlüssel erzeugt und auf dem Smartphone und auf dem Server gespeichert. Der Google Authenticator erstellt auf Basis dieses Schlüssels und der aktuellen Uhrzeit das Einmalpasswort, das aus sechs Ziffern besteht und für 30 Sekunden gilt. Die Uhren von Server und Client müssen ungefähr synchron sein, damit das Passwort akzeptiert wird. Die Schwachstelle von TOTP: Client und Server verwenden identi-



Zweiter Faktor: Viele Konten lassen sich über einen zusätzlichen Code sichern, der beispielsweise vom Google Authenticator auf dem Smartphone erzeugt wird.

ZUSÄTZLICHE TOOLS FÜR DEN YUBIKEY

Die im Artikel erwähnten Kommandozeilentools für den Yubikey sind allesamt in den Paketquellen aktueller Linux-Systeme enthalten. Wer möchte, kann sich aber auch Verwaltungstools für die grafische Oberfläche installieren. Führen Sie im Terminal diese zwei Befehlszeilen aus, um das Yubico-PPA hinzuzufügen:

```
sudo add-apt-repository ppa:yubico/stable
sudo apt-get update
```

Danach lassen sich per „sudo apt install [Paketname]" drei zusätzlich Pakete installieren.

yubikey-manager-qt: Das Programm bietet eine einfache grafische Oberfläche für die Konfiguration von FIDO2, OTP und PIV. Außerdem lassen sich damit einzelne Funktionen deaktivieren und wieder aktivieren.

yubikey-personalization-gui: Das Yubikey Personalization Tool dient ebenfalls zur Konfiguration des Yubikeys, bietet aber erweiterte Funktionen. Sie verwenden es vor allem, wenn Sie in einem Unternehmen mehrere Yubikeys konfigurieren möchten.

yubioath-desktop: Der Yubikey-Authenticator arbeitet ähnlich wie der Google Authenticator. Er generiert jedoch Einmalpasswörter, die über den Yubikey abgesichert sind.

sche Schlüssel. Sollte der Schlüssel in falsche Hände geraten, könnten ihn auch Phishingseiten verwenden.

4. Beste Absicherung über Hardwareschlüssel

Maximale Sicherheit versprechen Hardwaretokens für den USB-Port, auf denen ein privater Schlüssel gespeichert ist. Dieser Schlüssel lässt sich nicht auslesen und wird auch nicht an einen Onlinedienst übertragen. Bei der Einrichtung der Zwei-Wege-Authentifizierung übermittelt der USB-Token seinen öffentlichen Schlüssel an den Server des Onlineanbieters. Die Aktion muss der Nutzer am USB-Token per Knopfdruck bestätigen. Damit ist sichergestellt, dass die Information tatsächlich von der Hardware stammt und nicht per Software simuliert wird. Der weitere Datenaustausch wird dann über den USB-Token mit dem privaten Schlüssel signiert, was einer digitalen Unterschrift entspricht. Der Server prüft die Signatur mit dem ihm inzwischen bekannten öffentlichen Schlüssel. Passen Daten und Signatur zusammen, ist die Identität bestätigt.

Da der private Schlüssel sich beim USB-Token nicht auslesen lässt und der öffentliche Schlüssel nur dem Onlinedienst bekannt ist, gibt es hier kaum Angriffsflächen. Zudem speichern die USB-Token die URL der ursprünglichen Website und die Anmeldung funktioniert nur hier. Ein Angreifer müsste daher den Webserver des Onlinedienstes komplett unter seine Kontrolle bringen, damit ein Angriff Erfolg hat.

5. Hardwareschlüssel für Google & Co.

USB-Tokens für die Onlineauthentifizierung gibt es schon ab zehn Euro. Ein Beispiel ist Key-ID Fido U2F (*www.key-id.com*) für etwa 12 Euro. Der USB-Sicherheitsschlüssel ist nach Fido (Fast Identity Online, *https://fidoalliance.org*), zertifiziert und bietet daher Kompatibilität mit vielen Webdiensten. „U2F“ steht für Universal Second Factor, also Zwei-Wege-Authentifizierung. Zur Zeit werden unter anderem Google, Dropbox, Facebook und Wordpress.org unterstützt.

Mit gut 50 Euro ist der Yubikey 5 NFC deutlich teurer (*www.yubico.com*). Der Sicherheitsschlüssel bietet dafür aber auch zahlreiche Funktionen, unter anderem Fido, Fido2, Webauthn, Smart Card (PIV-kompatibel), OTP, TOTP und Open PGP. Entsprechend lang ist die Liste der unterstützten Onlinedienste, die Sie unter *https://www.yubico.com/works-with-yubikey/catalog/* finden. Mit Fido2 sind Sie auch für die Zukunft gerüstet. Bisher gibt es für den noch recht neuen Standard jedoch nur wenige Einsatzbereiche, etwa bei Microsoft für die Windows-10-Anmeldung ohne Passwort.

Unter Linux lässt sich der Yubikey für die Zwei-Wege-Authentifizierung in den Webbrowsern Firefox und Google Chrome nutzen. Dafür ist keine zusätzliche Software erforderlich. Es ist aber auch möglich, die Linux-Anmeldung mit dem Sicherheitsschlüssel zu schützen.

Sicherheitsschlüssel: Der Yubikey (50 Euro) unterstützt auch aktuelle Standards wie FIDO2. Key-ID (12 Euro) bietet den U2F-Standard, was für die meisten Onlinedienste ausreicht.

6. Zwei-Wege-Authentifizierung per USB-Token

Wir erläutern am Beispiel Google, wie sich eine Zwei-Wege-Authentifizierung mit einem Sicherheitsschlüssel einrichten lässt. Bei den meisten Onlinediensten läuft es ähnlich ab.

Schritt 1: Melden Sie sich auf dem PC bei Google an, öffnen Sie die Webseite *https://myaccount.google.com/security*, klicken Sie auf „Bestätigung in zwei Schritten“ und auf „Jetzt starten“. Geben Sie das Google-Passwort ein und klicken Sie auf „Weiter“.

Schritt 2: Es ist sinnvoll, die Benachrichtigung per SMS zu aktivieren. Sollte der Sicherheitsschlüssel gerade nicht verfügbar sein, können Sie sich über die alternative Methode anmelden. Wenn Sie das nicht wünschen, klicken Sie auf „Andere Option auswählen“ und „Sicherheitsschlüssel“ und fahren bei Schritt 4 fort. Andernfalls tippen Sie Ihre Telefonnummer ein und wählen die Option „Telefonanruf“ (Festnetz) oder „SMS“. Nach einem Klick auf „Weiter“ geben Sie den Code aus der SMS ein, klicken auf „Weiter“ und dann auf „Aktivieren“.

Schritt 3: Klicken Sie unter „Alternativen zweiten Schritt einrichten“ auf „Sicherheitsschlüssel“ hinzufügen und dann auf „Weiter“.

Key mit dem Konto verknüpfen: Aktivieren Sie in den Google-Einstellungen die „Bestätigung in zwei Schritten“. Danach registrieren Sie den Sicherheitsschlüssel.

Schritt 4: Danach verbinden Sie den Yubikey oder Key-ID-Schlüssel mit dem PC. Berühren Sie die Scheibe auf dem Yubikey oder drücken Sie bei Key-ID den Taster. Tippen Sie eine aussagekräftige Bezeichnung für den Schlüssel ein und klicken Sie auf „Fertig“.

Schritt 5: Melden Sie sich bei Google ab und mit Ihrem Passwort wieder an. Danach bestätigen Sie die Anmeldung am Sicherheitsschlüssel wie in Schritt 4. Auf der folgenden Seite ist standardmäßig ein Häkchen vor „Auf diesem Computer nicht mehr fragen“ gesetzt. Das ist zwar bequem, macht aber den zusätzlichen Schutz durch den Sicherheitsschlüssel zunichte, etwa wenn das Notebook verloren geht. Daher sollten Sie das Häkchen entfernen, bevor Sie auf „Weiter“ klicken.

Unsicherheitseinstellung: Bei Google ist standardmäßig „Auf diesem Computer nicht mehr fragen“ aktiviert. Für maximale Sicherheit sollten Sie das Häkchen entfernen.

7. Über den Yubikey bei Linux anmelden

Der Yubikey wird von Linux standardmäßig wie eine Tastatur behandelt und als „Human Interface Device“ erkannt. Die Konfiguration als Hardwaretoken für die Linux-Anmeldung erfordert jedoch höhere Rechte, die Sie über Udev-Regeln anfordern.

Schritt 1: Die erforderlichen „rules“-Dateien „69-yubikey.rules“ und „70-u2f.rules“ finden Sie unter *www.pcwelt.de/5Wk1MZ* im Ordner „yubikey“. Kopieren Sie beide Dateien in den Ordner „/etc/udev/rules.d“. Danach führen Sie die folgenden zwei Befehle in einem Terminalfenster aus.

```
sudo udevadm control --reload
sudo udevadm trigger
```

Starten Sie Linux neu.

Schritt 2: Installieren Sie die erforderliche Software:

```
sudo apt-get install libpam-yubico
 yubikey-personalization
```

Führen Sie danach diese drei Befehlszeilen aus:

```
ykpersonalize -2 -ochal-resp
 -ochal-hmac -ohmac-lt64 -oserial-
 api-visible
mkdir $HOME/.yubico
ykpamcfg -2 -v
```

Das erste Kommando konfiguriert den Yubikey für das Challenge-Response-Verfahren. Der Key besitzt zwei Konfigurationsspeicher. „Slot 1“ ist vom Werk aus für Yubico-OTP eingerichtet und liefert das Einmalpasswort für Onlineanmeldungen, wenn Sie die Schaltfläche kurz berühren. „Slot 2“ ist nicht belegt, was Sie über die Option „-2“ und das Tool ykpersonalize ändern. ykpamcfg sendet eine zufällige Zeichenfolge (Challenge) an den Yubikey, der einen mit seinem privaten Schlüssel erzeugten Hashwert zurückgibt (Response). Das Ergebnis wird in einer Datei im Ordner „$HOME/.yubico“ gespeichert. Bei der Authentifizierung wird erneut eine Challenge an den Yubikey gesendet. Wenn er korrekt antwortet, handelt es sich um denselben Schlüssel, der bei der Initialisierung mit dem PC verbunden war, und die Anmeldung ist erfolgreich.

Schritt 3: Jetzt müssen Sie die Anmeldung über den Yubikey noch in die Linux-Anmeldung einbauen. Erstellen Sie (als root) die Textdatei „/etc/pam.d/inc_yubikey“ mit diesen vier Zeilen:

```
auth required pam_yubico.so
 mode=challenge-response
auth [success=1 default=ignore]
 pam_unix.so    try_first_pass
auth requisite pam_deny.so
auth required pam_permit.so
```

Schritt 4: Probieren Sie die Konfiguration zuerst für „sudo“ aus:

```
sudo gedit /etc/pam.d/sudo
```

Mint-Nutzer verwenden „xed“ statt „gedit“. Setzen Sie ein Kommentarzeichen (‚#‘) vor die Zeile „@include common-auth“ und fügen Sie darunter die Zeile

```
@include inc_yubikey
```

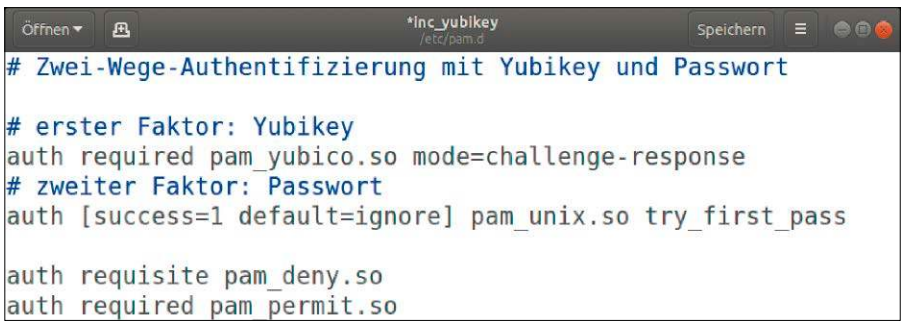
ein. Öffnen Sie dann ein weiteres Terminal, wo Sie diesen Befehl eingeben:

```
sudo -i
```

Der Wechsel zum Systemverwalterkonto funktioniert jetzt nur mit eingesteckten Yubikey und Passwort.

Schritt 5: Bauen Sie „@include inc_yubikey“ entsprechend in die Dateien „/etc/pam.d/gdm-password“ (Linux Mint 19: „/etc/pam.d/lightdm“) sowie „/etc/pam.d/polkit-1“ ein.

Damit sichern Sie die Anmeldung an der grafischen Oberfläche zusätzlich über den Yubikey ab. ■



Linux-Log-in absichern: Diese PAM-Konfiguration erlaubt die Linux-Anmeldung nur, wenn der Yubikey mit dem PC verbunden ist und Sie das richtige Passwort eingeben.

Verschlüsselung für Websites

Mit HTTPS verschlüsselte Webseiten sorgen für mehr Sicherheit bei der Übertragung sensibler Daten. Die dafür nötigen SSL-Zertifikate gibt es kostenlos von der Initiative „Let's Encrypt".

VON THORSTEN EGGELING

SSL-Zertifikate gratis: Die Initiative Let's Encrypt bietet kostenlose Zertifikate für „https://". Beantragung und Installation erfolgen über eine Clientsoftware auf dem Webserver.

Ob und wann Internetseiten gemäß DSGVO (Datenschutz-Grundverordnung) verschlüsselt sein müssen, ist Auslegungssache. Unstrittig ist, dass die Übertragung personenbezogener Daten wie Name oder Adresse verschlüsselt erfolgen sollte, etwa bei einem Kontaktformular. Wer sich rechtlich im sicheren Bereich befinden möchte, verschlüsselt einfach jede Datenübertragung. Das ist seit einiger Zeit kostenlos möglich und erfordert lediglich die Anpassung der Konfiguration des Webservers.

SSL-Zertifikate von Let's Encrypt

Seit Dezember 2015 bietet die Initiative Let's Encrypt (*https://letsencrypt.org*) kostenlose Zertifikate an, die sich einfach abrufen und installieren lassen. Einige Hostinganbieter haben Let's Encrypt bereits in ihr Angebot integriert. Es genügen dann wenige Mausklicks in der Konfigurationsoberfläche des Hostingpakets, damit die Domain zusätzlich oder ausschließlich mit einem vorangestellten „https://" aufrufbar ist. Eine Liste mit Shared-Hosting-Anbietern, die Let's-Encrypt-Zertifikate unterstützen, finden Sie unter *https://certbot.eff.org/hosting_providers*.

Wer einen voll ausgestatteten Root-Server gemietet hat, kann die Zertifikate oft ebenfalls bequem über eine Verwaltungsoberfläche aktivieren – sofern vorhanden. Andernfalls lassen sich Let's-Encrypt-Zertifikate über eine Clientsoftware auf dem Server einrichten. Die Zertifikate sind nach der Ausstellung 90 Tage lang gültig. Empfohlen wird eine Erneuerung nach 60 Tagen, was sich per Cronjob automatisieren lässt.

Ein Webserver zu Hause, der über DSL oder Kabelmodem angebunden ist, kann ebenfalls mit einem SSL-Zertifikat versorgt werden, wenn er über eine Domain von einem Anbieter für dynamisches DNS erreichbar ist. Allerdings limitiert Let's Encrypt die Anzahl der Zertifikate pro Second-Level-Domain und Zeiteinheit. Sollte die Zertifikatsausstellung nicht funktionieren, müssen Sie eine Woche warten, bevor Sie es erneut versuchen können.

Zertifikat auf dem Server installieren

Wir gehen davon aus, dass Sie erstens über einen Apache-Webserver verfügen, der über einen Domainnamen erreichbar ist, und dass Sie zweitens eine Root-Shell verwenden können. Unsere Anleitung gilt für Ubuntu, Linux Mint und verwandte Systeme. Information zur Installation für andere Webserver und Betriebssysteme finden Sie unter *https://certbot.eff.org*.

Die Installation der Let's-Encrypt-Clientsoftware erfolgt bei Ubuntu/Mint über ein PPA. Führen Sie in einem Terminalfenster die folgenden fünf Befehle aus:

```
sudo apt-get update
sudo apt-get install software-
  properties-common
sudo add-apt-repository
  ppa:certbot/certbot
sudo apt-get update
sudo apt-get install certbot
  python-certbot-apache
```

Anschließend starten Sie

```
sudo certbot --apache
```

und folgen den Anweisungen des Assistenten. Certbot legt zur Prüfung eine Datei unter „/var/www/html/.well-known/acme-challenge/" („HTTP-01 challenge") an, ruft das Zertifikat ab, aktiviert die Apache-Module „ssl" und „rewrite" und erstellt eine neue Konfigurationsdatei im Ordner „/etc/apache2/sites-available". Auf Wunsch enthält diese auch eine automatische Umleitung von „http://"-Aufrufen nach „https://".

Certbot aktiviert die SSL-Konfiguration automatisch und startet Apache neu. Sie können jetzt die Sicherheit der Serverkonfiguration und das SSL-Zertifikat beispielsweise über *www.ssllabs.com/ssltest* testen.
Bei der Certbot-Installation unter Ubuntu 18.04 oder Linux Mint 19 wird ein Systemd-Timer eingerichtet, der zweimal täglich mit „certbot -q renew" das Ablaufdatum prüft und das Zertifikat ungefähr 30 Tage vor Ablauf erneuert.

Zertifikate für alle Subdomains erstellen

Ein Let's-Encrypt-Zertifikat ist standardmäßig für die Domain inklusive Präfix „www" gültig. Für Subdomains müssen Sie eigene Zertifikate erstellen. Wenn Sie viele davon verwenden, lohnt sich ein Wildcard-Zertifikat. Die Prüfung muss dann allerdings über einen zusätzlichen TXT-DNS-Eintrag („DNS-01 challenge") erfolgen. Da sich der DNS-Eintrag bei der Zertifikaterneuerung ändern muss, ist meist keine automatische Aktualisierung möglich – außer, Sie verfügen über einen DNS-Server, der sich über API-Aufrufe konfigurieren lässt. Informationen dazu finden Sie unter *https://certbot.eff.org/docs/using.html#dns-plugins*.
Unabhängig vom verwendeten DNS-Server lässt sich ein Wildcard-Zertifikat manuell erstellen. Rufen Sie zuerst ein einfaches Domainzertifikat ab, wie im vorherigen Abschnitt beschrieben. Dann besitzen Sie bereits eine funktionstüchtige Apache-Konfiguration für SSL-Verbindungen.
Verwenden Sie folgenden Befehl (eine Zeile), um das Zertifikat anzufordern oder später zu erneuern:

```
certbot certonly --manual
 --preferred-challenges dns
 --server https://acme-v02.api.
 letsencrypt.org/directory
 --manual-public-ip-logging-ok -d
 "*.[Ihre.Domain]" -d [Ihre.
 Domain]
```

Die Platzhalter „[Ihre.Domain]" ersetzen Sie durch den gewünschten Domainnamen (ohne „www"). Danach erscheint eine Meldung wie diese:

```
Please deploy a DNS TXT record under
 the name
_acme-challenge.[Ihre.Domain] with
 the following value:
Rnsnq9ERBUgyQpBZ9hfK2ZiruMkKBZsLb
 zWwZP_YU9Q
```

Erstellen Sie den geforderten Eintrag über den DNS-Editor beim Hostinganbieter. Es kann einige Zeit dauern, bis die DNS-Einstellungen aktualisiert wurden. Prüfen Sie das in einem zweiten Terminalfenster mit

```
dig -t txt _acme-challenge.[Ihre.
 Domain]
```

Sobald der Eintrag erscheint, drücken Sie im Certbot-Terminal die Eingabetaste. Danach müssen Sie auf dem gleichen Weg einen weiteren TXT-DNS-Eintrag erstellen, da wir zwei Domains verwenden wollen – einmal mit und einmal ohne Wildcard.
Abschließend informiert Sie Certbot über den Pfad zu Zertifikat und privatem Schlüssel. Die SSL-Konfigurationsdatei der Domain aus dem Ordner „/etc/apache2/sites-enabled" sollte die Pfade bereits enthalten, da sich der Domainname nicht geändert hat. In Konfigurationsdateien für Subdomains tragen Sie die gleichen Pfade ein. ■

```
te@p5ql: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
Congratulations! You have successfully enabled https://d[redacted].de

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=d[redacted].de

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/d[redacted].de-0001/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/d[redacted].de-0001/privkey.pem
   Your cert will expire on 2020-01-08. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
```

Zertifikat abrufen: Das Tool Certbot läuft im Terminalfenster. Nach erfolgreichem Abschluss erhalten Sie Informationen zu den installierten Dateien und dem Ablaufdatum.

```
Öffnen   meinedomain_ssl.conf   Speichern
~/Dokumente
<IfModule mod_ssl.c>
<VirtualHost *:443>
    #Basic apache vhost configuration
    ServerName meinedomain.de
    ServerAdmin te@meinedomain.de
    ErrorLog /var/log/apache2/meinedomain_ssl.log
    LogLevel warn
    CustomLog /var/log/apache2/meinedomain_ssl.log combined
    ServerSignature on
SSLCertificateFile /etc/letsencrypt/live/meinedomain.de/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/meinedomain.de/privkey.pem
Include /etc/letsencrypt/options-ssl-apache.conf
</VirtualHost>
</IfModule>
```

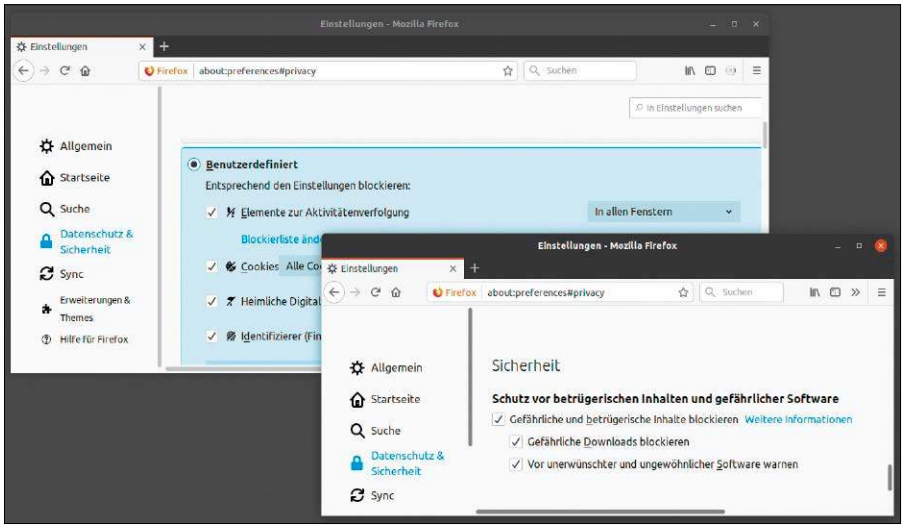
SSL aktivieren: Certbot erstellt automatisch eine Apache-Konfigurationsdatei. Enthalten sind die Pfade zur Zertifikatsdatei und zum privaten SSL-Schlüssel.

SO FUNKTIONIERT SSL-VERSCHLÜSSELUNG

Die meisten Websites verwenden HTTPS/SSL-Verschlüsselung, was Sie in Firefox am grünen Schloss-Symbol vor der Adresszeile erkennen. Beim Aufbau der gesicherten Verbindung sendet der Webserver an den Browser ein digitales Zertifikat, das eine Zertifizierungsstelle ausgestellt hat, die selbst ebenfalls zertifiziert ist. Die Gültigkeit des Zertifikats für die aufgerufene Internetdomain prüft der Browser anhand von Root-Zertifikaten, die zur Browserinstallation gehören. Webserver und Browser verwenden einen gemeinsamen SSL-Sitzungsschlüssel, über den die Nutzdaten verschlüsselt werden. Ist ein Zertifikat ungültig, etwa weil es abgelaufen ist, nicht zur Domain passt oder kein Vertrauen genießt, warnt der Browser und blockiert den Aufruf der Website. Firefox-Nutzer können auf „Erweitert" und dann auf „Risiko akzeptieren und fortfahren" klicken, um die Seite trotzdem aufzurufen.

Firefox-Sicherheit

Moderne Browser filtern das Web und schützen vor gefährlichen Webseiten und Downloads. Dieser Beitrag erklärt die Techniken für Sicherheit und Datenschutz im Mozilla-Browser Firefox.



VON HERMANN APFELBÖCK

Sicherheit im Browser hat zwei Aspekte: Das Wichtigste ist der Schutz vor betrügerischen Seiten und Schadsoftware. An zweiter Stelle steht der Datenschutz für Surfaktivitäten, Lesezeichen und Kennwörter. Der Artikel erklärt die Sicherheitsfunktionen von Firefox, der unter Linux mit Masterpasswort und besserem Script-Schutz (mit Noscript) weiter erste Wahl bleibt.

Das Masterpasswort

Firefox fragt bei einer neuen Webanmeldung, ob das Passwort gespeichert werden soll. Solches Speichern ist bequem, weil Sie sich das Passwort dann nicht länger merken müssen. Andererseits bedeutet das, dass jeder, der Zugriff auf Ihr Gerät hat, auch Ihre persönlichen Zugänge nutzen kann. Unter „Einstellungen → Sicherheit → Gespeicherte Zugangsdaten“ lassen sich alle Kennwörter sogar in Gesamtschau bequem auslesen. Dagegen hilft das Masterpasswort, das Sie unter „Einstellungen →Datenschutz & Sicherheit → Master-Passwort verwenden“ einrichten und das die Kennwörter verschlüsselt. Der Komfortverlust ist vertretbar: Das Masterpasswort wird pro Firefox-Sitzung nur einmal abgefragt, eventuell auch gar nicht, falls Sie keinen Zugriff auf die Kennwörter benötigen.

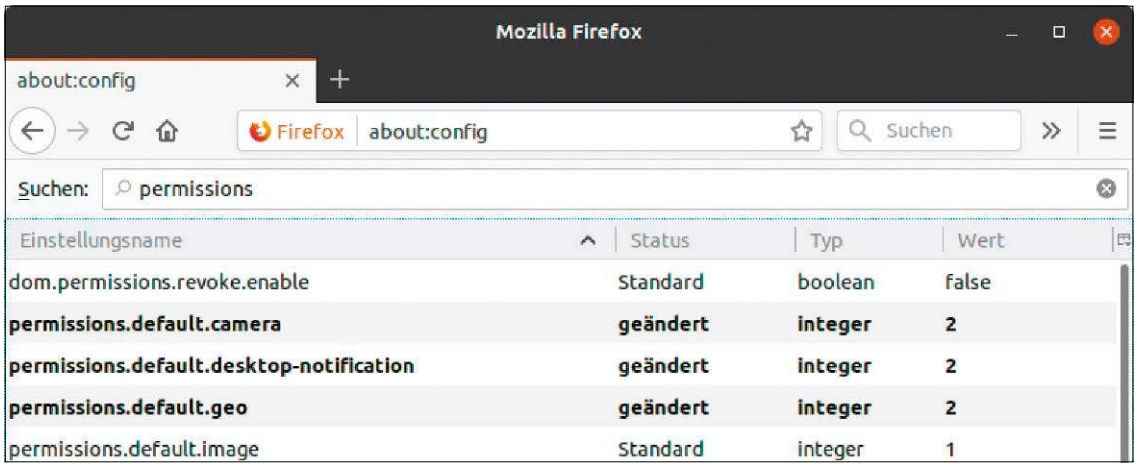
Die Firefox-Schutzmechanismen

Anlaufstelle ist der Punkt „Einstellungen → Datenschutz & Sicherheit“. Die wichtigsten Einstellungen zeigt Firefox ganz unten auf dieser Seite unter **„Schutz vor betrügerischen Inhalten…“.** Hier sollten alle drei Kästchen aktiviert sein, um gefährliche Webseiten und Downloads zu blockieren. Es handelt sich um einen Grundschutz, der auf der Basis einer Blacklist funktioniert, die ständig aktualisiert wird (alle 30 Minuten). Eine weitergehende Heuristik wie Chrome besitzt Firefox nicht. Das heißt: Firefox blockiert Downloads von bekannten betrügerischen Seiten. Den Virendownload von einer bisher unbescholtenen Webseite wird Firefox hingegen ohne Kommentar zulassen, während Chrome in gleicher Situation vor einem „ungewöhnlichen Download“ warnt. Allerdings ist dieser Chrome-Mechanismus relativ primitiv: Er schlägt dann an, wenn Dateiname und Signatur unbekannt sind und eine ausführbare Extension vorliegt (wie EXE oder DEB). Unter Linux ist solche Unterstützung kaum relevant.

Berechtigungen für Kamera und Mikro: Eine Webseite sollte niemals ungefragt Kamera oder Mikrofon Ihres Rechners benutzen dürfen. Auch der geografische Standort ist ein personenbezogener Fakt, der nicht ungefragt berichtet werden muss. Solche „Berechtigungen“ regelt der gleichnamige Punkt unter „Datenschutz & Sicherheit“. Mit der Schaltfläche „Einstellungen“ bestimmen Sie für Standort, Kamera, Mikrofon und Benachrichtigungen je einzeln, dass alle Webseiten (die nicht in der Liste stehen) nichts automatisch dürfen: Der Punkt lautet „Neue Anfragen […] blockieren“.

Ganz oben auf der Konfigurationsseite „Datenschutz & Sicherheit“ steht der Punkt **„Seitenelemente blockieren“.** Hier steht der Datenschutzaspekt im Vordergrund. Die Stufe „Standard“ genügt für den Schutz vor der Aktivitätenverfolgung von Trackern, die Surfdaten, Cookies und Fingerprints (errechnet aus Browser, Computer, Betriebssystem, Bildschirmauflösung u. a.) über mehrere Websites hinweg sammeln, sowie vor Krypto-Minern und schädlichen Scripts. Die Einstellung „Streng“ erzielt praktisch einen permanenten „Privaten Surfmodus“ (siehe unten). „Benutzerdefiniert“ ermöglicht gegenüber „Standard“ und „Streng“ kaum genauere Abstufungen, nur die Cookieakzeptanz können Sie hier noch restriktiver (als „Streng“) oder noch toleranter (als „Standard“) setzen.

Bei „strenger“ oder „benutzerdefiniert“ strenger Konfiguration ist es immer noch möglich, die Verbote für vertrauenswürdige Websites aufzuheben. Dies geschieht im Abschnitt „Seitenelemente blockieren“ ganz oben mit der Schaltfläche „Ausnahmen verwalten“.



Alternative Konfiguration: Einstellungen wie „Permissions“ (Berechtigungen) sind in der Firefox-Konsole „about:config“ leichter zu filtern als in den grafischen Einstellungen.

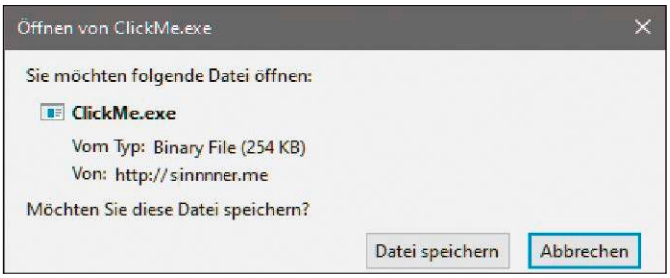
Das Surfen im „Privaten Fenster“

„Privates Surfen“ bietet keinen Schutz vor Schädlingen oder betrügerischen Seiten. Es anonymisiert weder die IP noch verschleiert es strafbaren Handlungen. Trotzdem sind „Private Fenster“ nützlich: Sie unterbinden den Großteil kommerzieller Trackingschnüffelei. Ein wichtiger Nebenaspekt ist ferner, dass Sie ohne Cookies und Webprotokolle unterwegs sind und neutrale Ergebnisse erhalten (gelegentlich wichtig bei Suchmaschinen und Onlineshops). In Firefox ist der Hotkey Strg-Umschalt-P der schnellste Weg zum privaten Fenster.

Neben dem privaten Modus bietet Firefox eine „Do Not Track“-Option. Dieser Info-Tag im Header der Browseranfrage sollte es der Gegenstelle verbieten, Nutzungsprofile über den Besucher anzulegen. Der Effekt ist aber fraglich, weil Websites nicht verpflichtet sind, der Bitte nachzukommen. „Do Not Track“ ist nicht standardmäßig aktiv. Sie finden die Option „Websites eine „Do Not Track“-Information senden“ unter „Einstellungen → Datenschutz & Sicherheit“.

Die Firefox-Synchronisierung

Browsersynchronisierung bedeutet für Nutzer mehrerer Geräte einen unschätzbaren Komfort. Sie benötigt allerdings ein kostenloses Konto auf *https://accounts.firefox.com* und hat den Nebenaspekt, dass viele persönliche Daten auf dem Mozilla-Server hinterlegt werden müssen – aus Bequemlichkeit meist auch die Passwörter („Zugangsdaten“). Der Umfang der Synchronisierung ist unter „Einstellungen → Sync“ im Detail einstellbar. Firefox verschlüsselt aber standardmäßig alle Daten, wobei der Schlüssel auf dem Gerät des Benutzers verbleibt. Die Mozilla Foundation ist grundsätzlich vertrauenswürdig und macht keine Geschäfte mit Benutzerdaten.



Schädliche Downloads: Firefox warnt nicht vor Downloads, wenn die betreffende Website bislang nicht als bösartig gemeldet wurde.

Sicherheitsrelevante Erweiterungen

Firefox hat seine Stärken bei der Erweiterbarkeit und dies gilt auch für den Sicherheitsaspekt: Firefox-Erweiterungen suchen und installieren Sie über „Add-ons → Erweiterungen“.

Noscript: Das Add-on verhindert, dass Firefox Javascript, Java oder andere ausführbare Inhalte automatisch startet. Noscript ist unbequem, aber der Schädlingsstop schlechthin. Einmal erlaubte Sites landen in der Whitelist und müssen später nicht mehr einzeln bestätigt werden, aber zunächst müssen Sie auf vielen interaktiven Seiten diverse Scripts manuell erlauben. Dies geschieht über das Noscript-Symbol mit Klick auf das blaue „S“ mit kleiner Uhr (temporär) oder mit dem zweiten „S“-Symbol (dauerhaft). Falls eine als „Trusted“ bewertete Seite rot markiert bleibt, dann ist die Verbindung nicht HTTPS-verschlüsselt. Wenn dort nur HTTP funktioniert, müssen Sie die Rotfärbung akzeptieren. Das Umschalten auf „Grün“ (durch Klick auf das Schloss-Symbol) würde die Adresse wieder auf „Untrusted“ schalten, da „Grün“ HTTPS voraussetzt.

HTTPS Everywhere: Verschlüsseltes HTTPS ist bei allen Webanmeldungen, vor allem bei Bankgeschäften und Einkäufen unverzichtbar.

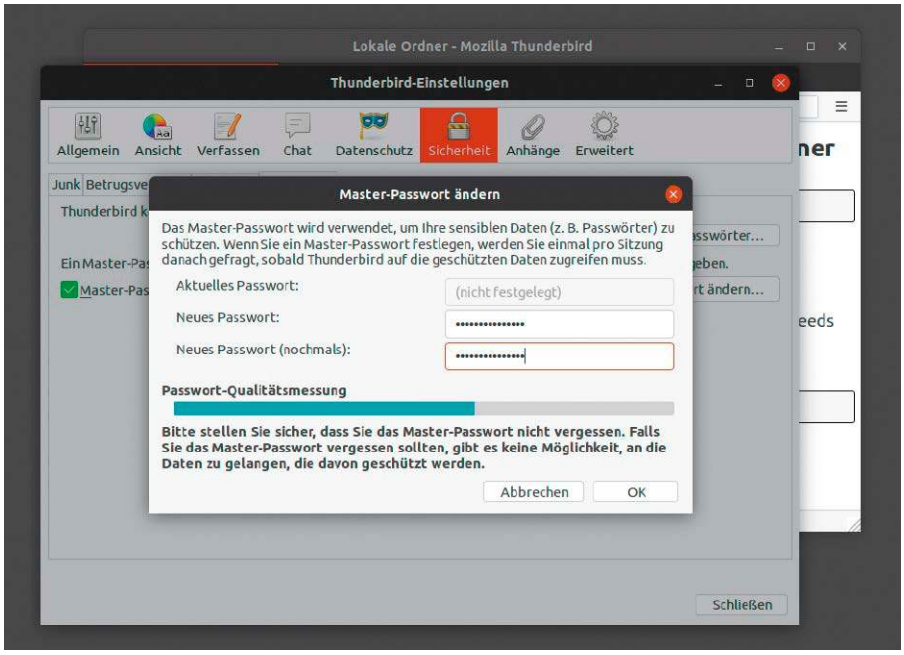
Der Browser zeigt verschlüsselte Verbindungen in der Adresszeile grün gefärbt. HTTPS Everywhere wählt, wo immer verfügbar, eine verschlüsselte HTTPS-Verbindung zu einer Website, auch wenn die Adresseingabe oder ein Link eine unverschlüsselte HTTP-Adresse anfordert. Die Bedeutung des Add-ons nimmt aber ab, je mehr HTTPS zum Standard wird. Beachten Sie außerdem, dass „grünes“ HTTPS zwar den Datenverkehr verschlüsselt, aber keine vertrauenswürdige Seite garantiert. Auch betrügerische Seiten nutzen heutzutage oft verschlüsselte Verbindungen.

Lastpass & Co.? Als Ersatz für den eingebauten Passwortmanager gibt es Alternativen wie das Add-on Lastpass. Dieser Manager benötigt ein Konto bei Lastpass und verspricht auf seinen Servern AES-Verschlüsselung aller Daten. Der Einsatz solcher Alternativen ist aber nicht recht nachvollziehbar: Das native Firefox Sync bietet neben der Synchronisierung der Kennwörter auch noch die von Lesezeichen und Einstellungen. Aus unserer Sicht gibt es kein Motiv, einen externen Passwortmanager zu verwenden. ■

Thunderbird-Sicherheit

Mails an sich sind nicht gefährlich. Aber sie sollten Mails bleiben, nicht ins Web gehen – und Mailanhänge von Fremden haben auf dem Rechner gar nichts verloren. Wenn Sie dann noch Ihre Zugangsdaten schützen, sind Sie auf der sicheren Seite.

VON HERMANN APFELBÖCK



Jüngst hatte ein Windows-Schädling Erfolg, der als Mailanhang in Form einer Word-Datei verschickt wurde. Die Nachricht forderte zum Lesen der Word-Datei auf, mit dem Hinweis, doch bitte beim Öffnen der Datei den Makrovirenschutz von Word zu deaktivieren. Dass viele Anwender dieser Aufforderung gehorcht haben, ist dümmer, als Windows und Word erlauben, beweist aber die Manipulierbarkeit und Naivität der meisten Internetnutzer. Gesundes Misstrauen ist unerlässlich und beginnt mit misstrauischen Softwareeinstellungen.

Die Notwendigkeit des Masterpassworts

Ein „gehacktes" oder den falschen Personen bekanntes Mailkonto (Benutzername und Kennwort) legt nicht nur die Korrespondenz offen, sondern ermöglicht den Zugriff auf weitere Log-ins: Denn bei den meisten Diensten genügt die Mailadresse, um sich („Kennwort vergessen?") einfach ein neues Passwort zu beschaffen. Trotzdem werden sich die meisten Nutzer den Komfort erlauben, die Zugangsdaten in der Thunderbird-Konfiguration zu hinterlegen. Thunderbird speichert dann die Daten im Profilordner in der Datei „logins.json", was die automatische Anmeldung am Mailserver ermöglicht. Dadurch ergeben sich folgende Datenschutzlücken:

1. Wer auf das laufende System mit Ihrem Benutzerkonto Zugriff hat, kann die Zugangsdaten in Thunderbird unter „Einstellungen → Sicherheit → Passwörter → Gespeicherte Passwörter → Passwörter anzeigen" auslesen. Das ist kein großes Problem, sofern Sie in einer Büroumgebung vor Verlassen des Arbeitsplatzes den Desktop sperren.

2. Kritisch sind verlorene Notebooks oder der Fremdzugriff auf PCs, auf denen Thunderbird die Zugangsdaten verwaltet. Auf den ersten Blick scheint das unproblematisch, denn die Zugangsdaten in der Datei „logins.json" sind verschlüsselt. Diese Verschlüsselung ist jedoch nicht mehr als Sichtschutz, um die Passwörter nicht im Klartext abzulegen. Es gibt Tools, um diese Zugangsdaten zu entschlüsseln. Noch umfassender ist der schlichte Umzug des Thunderbird-Profils mit Copy & Paste: Wer nach dem Boot mit einem Fremdsystem einfach den Profilordner („/home/[user]/.thunderbird/[xxxxxxxx]") auf USB-Stick kopiert und dann auf einem anderen Rechner in ein neu angelegtes Thunderbird-Profil einfügt, hat Zugangsdaten, Kennwörter und die komplette Mailkorrespondenz vorliegen.

Angesichts dieser Bedrohung gibt es für Notebooks, Mehrbenutzersysteme und leicht zugängliche Bürorechner nur zwei angemessene Antworten: Entweder man verzichtet auf das Thunderbird-Angebot, die Zugangsdaten zu speichern, oder man benutzt das Masterpasswort. Die Vergabe des Masterpassworts erledigen Sie unter „Bearbeiten → Einstellungen → Sicherheit → Passwörter → Master-Passwort verwenden". Dadurch werden die Zugangsdaten individuell verschlüsselt, sodass der Fremdzugriff auf Dateiebene erfolglos ist.

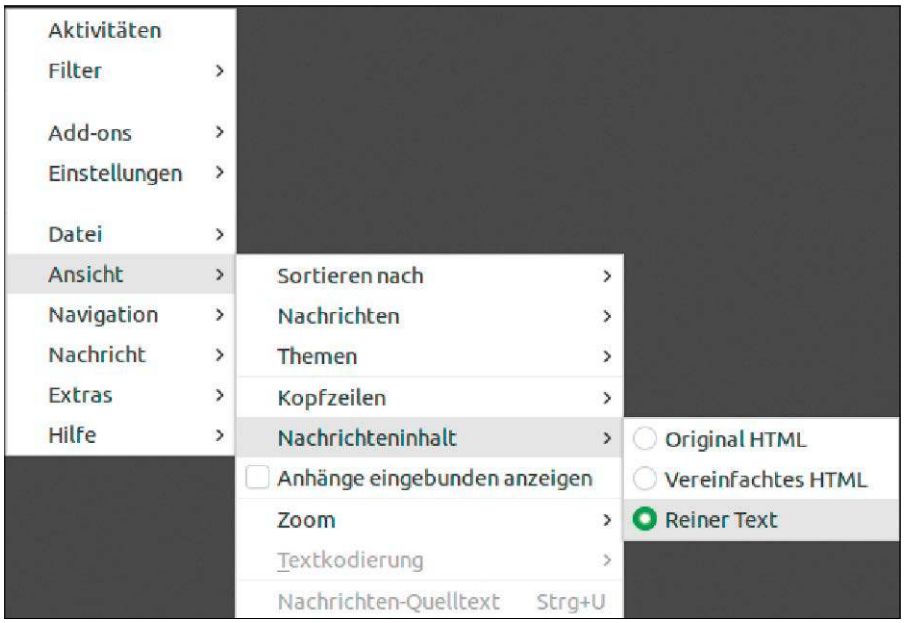
HTML-Format und externe Inhalte

HTML erlaubt hübsche Kommunikation mit Bildern, Links, Farben, Schriften. In Geschäftsmails mit Logos und Signaturen sind solche Formatierungen oft alternativlos. Auf der anderen Seite bietet HTML eine Plattform für Scripts und Tracking aller Art. Standardmäßig blockiert Thunderbird immerhin alle externen Inhalte, die nicht in der Nachricht selbst enthalten sind. Dafür sorgt die deaktivierte Option „Einstellungen → Datenschutz → Externe Inhalte in Nachrichten erlauben".

Schon das Anzeigen externer Elemente genügt, dem externen Webserver mitzuteilen, erstens dass überhaupt, zweitens wann und wo der Mailempfänger die Mail erhalten und gelesen hat. Das harmloseste Resultat ist daher der Nachweis, dass die Mailadresse existiert und genutzt wird. Beim Klick auf externe Inhalte kann aber darüber hinaus bereits ein Script ausgelöst werden, das Schadsoftware installieren will.

Externe Inhalte sollten deaktiviert bleiben. Man kann aber noch einen Schritt weitergehen und alle Nachrichten als reinen Text öffnen: Dazu genügt die globale Einstellung „Ansicht → Nachrichteninhalt → Reiner Text". Ein ästhetischer Kompromiss, der zumindest aktives Scripting aushebelt, ist die Einstellung „Vereinfachtes HTML". Ergänzend zu dieser Option sollte der Punkt „Ansicht → Anhänge eingebunden anzeigen" abgeschaltet werden. Dies unterbindet die Gefahr, dass ein Anhang schon beim Öffnen der Nachricht ein Script aktiviert.

Wer auf Formatierung und Bilder keinen Wert legt, kann seine eigenen Nachrichten als Reintext verschicken. Dies lässt sich unter „Einstellungen → Konten-Einstellungen" für jedes Konto mit „Verfassen & Adressieren" einzeln festlegen, indem Sie die Option „Nachrichten im HTML-Format verfassen" deaktivieren.



Nicht hübsch, aber hübsch sicher: Das Abschalten der HTML-Anzeige entschärft Links auf externe Websites und entzaubert manipulative Tarnoptik.

Maßnahmen gegen Phishing und Spam

Thunderbird kann betrügerisches Phishing und lästiges Spam („Junk") erkennen. Ob der Anti-Phishing-Filter aktiv ist (Standard), kontrollieren Sie unter „Einstellungen → Sicherheit → Betrugsversuche". Die Thunderbird-Regeln, gefälschte Nachrichten zu erkennen, sind hart codiert und nicht zu beeinflussen. Fundamentale Mechanismen erkennen falsche Web-URLs, die auf andere als die angezeigten Seiten führen, ferner gefälschte Bildverweise, die anders lauten als die URL der tatsächlichen Bildquelle. In solchen Fällen warnt Thunderbird: „Diese Nachricht könnte ein Betrugsversuch (Phishing) sein".

Beachten Sie, dass Sie der Gefahr, per unbedachten Klick auf eine gefälschte URL zu gelangen, kategorisch aus dem Weg gehen, wenn Sie Mails als „Reiner Text" anzeigen (siehe oben). Anderen Aufforderungen von Phishingbetrügern kann aber keine Technik, sondern nur der Verstand widerstehen: Die Abfrage von Bank- oder Kreditkartendaten macht kein Kreditinstitut per Mail und das Laden eines Anhangs unbekannter Absender verbietet sich von selbst.

Spam („Junk") ist in der Regel nur lästig, kann aber auch Stufe 1 zur Verifizierung des Mailkontos sein, dem dann Schlimmeres nachfolgt.

In den Einstellungen unter „Sicherheit → Junk" können Sie global bestimmen, ob Junknachrichten in den Junkordner verschoben werden sollen. Die Option, Spam automatisch zu löschen, ist meistens zu radikal, da Thunderbird wie jede Software gelegentlich irrt.

Anders als den Phishingfilter können Sie Thunderbird bei Spam individuell trainieren. Dazu markieren Sie jede Nachricht als Junk, die Sie als solche einstufen. ■

DER THUNDERBIRD-CHECK

- „Ansicht → Nachrichteninhalt → Reiner Text": Diese Einstellung ist nicht schön, denn sie unterbindet die Anzeige von HTML-Format, damit aber auch trügerische Tarnoptik und fatale Klicks auf Weblinks.
- „Einstellungen → Sicherheit → Betrugsversuche": Die einzige Option an dieser Stelle muss aktiviert sein, damit der Phishingfilter arbeitet.
- „Einstellungen → Sicherheit → Passwörter": Hier vergeben Sie das Masterpasswort. Wo und warum sich ein Masterpasswort empfiehlt, erklärt der Haupttext. Unter „Einstellungen → Sicherheit → Passwörter → Gespeicherte Passwörter" zeigt Thunderbird alle hinterlegten Zugangsdaten.
- „Einstellungen → Datenschutz": Folgende Option sollte aktiviert sein: „Websites mitteilen, meine Aktivitäten nicht zu verfolgen".
- „Einstellungen → Datenschutz": Folgende Option sollte auf keinen Fall aktiviert sein: „Externe Inhalte in Nachrichten erlauben".
- „Einstellungen → Erweitert → Allgemein → Konfiguration bearbeiten": Die Low-Level-Konfiguration zeigt Expertenoptionen, die über die Einstellungen der grafischen Oberfläche hinausreichen. Die meisten Direktiven sind allerdings nicht oder unzureichend dokumentiert. Das nicht risikolose Javascript können Sie durch Doppelklick beim Eintrag
  `javascript.enabled`
  auf „false" setzen und damit ausschalten.

Datenverschlüsselung mit Linux

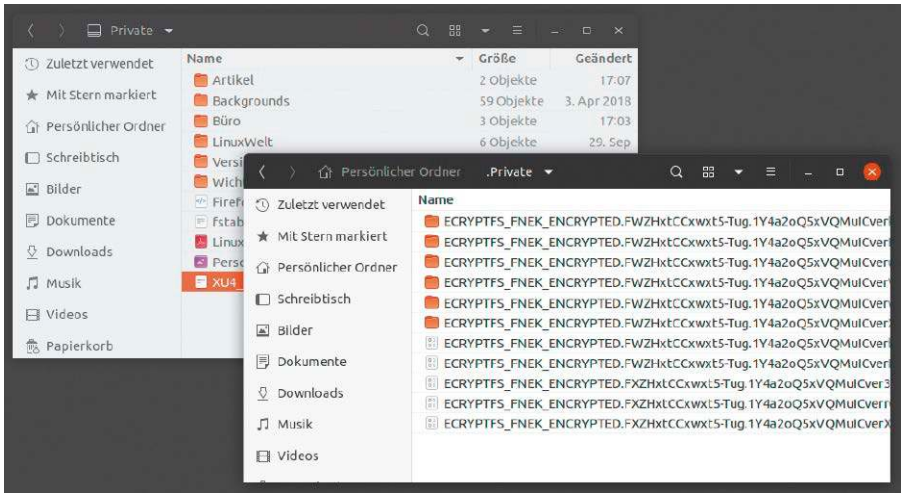
Wer sich den alleinigen Zugriff auf bestimmte Daten sichern will, muss diese verschlüsseln. Dabei stehen Geräte im Fokus, die besonders leicht in fremde Hände geraten, nämlich Notebooks und USB-Medien.

VON HERMANN APFELBÖCK

Verschlüsseln ist ein beeindruckender Vorgang: Aus standardisierten Tabellen-, Text- oder Bilddateien, die Milliarden Geräte und Personen lesen könnten, wird ein Binärcode, den nur noch Sie selbst lesbar machen. Die Motive, dies genau so zu wollen, müssen weder paranoid noch staatstragend noch kriminell oder schmuddelig sein: Ein verlorener USB-Stick kann unglaublich viel über Identität, Status, Arbeitgeber, Kontakte und Interessen verraten.

Linux-Werkzeuge zur Verschlüsselung

Wenn verschlüsselte Daten ausschließlich unter Linux genutzt werden, stehen zwei Methoden im Zentrum: Luks ist erste Wahl, zumal damit die Datenmenge dosierbarer ist, als es der Name „Datenträgerverschlüsselung“ nahelegt. Dazu unten mehr. Kleinere Lösungen bieten die sehr ähnlichen Werkzeuge Ecrypt FS und Enc FS. Aus Gründen der besseren Integration sehen wir hier klare Vorteile für Ecrypt FS, dessen Arbeitsweise wir unten kurz beschreiben. Andere Techniken können allenfalls als Adhoc-Lösung dienen, um schnell einen Dateianhang oder eine Clouddatei zu schützen. Ein Zukunftsversprechen, aber aktuell nicht praktikabel, ist die dateisystemeigene Ext4-Verschlüsselung. Diese von Google für Android entwickelte Ext4-Erweiterung hat unter Linux noch keinerlei Desktopintegration und bleibt auch im Terminal eine Zumutung. Da ist es komfortabler, etwa zum Packer 7-Zip zugreifen, der seine Archive mit Passwort verschlüsseln kann. Wenn Sie



Die kleine Ecrypt-FS-Lösung: Das Kryptotool richtet sehr bequem einen Ordner „~/Private“ ein, der bei der Systemanmeldung die Daten aus „~/.Private“ entschlüsselt.

nach Rechtsklick auf einer Datei „Komprimieren“ und das Format „7z“ wählen, gibt es unter „Erweiterte Einstellungen“ die Passwortoption. Mit

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

rüsten Sie 7-Zip bei Bedarf nach.

Ecrypt FS: Einfach und komfortabel

Ecrypt FS bietet transparente Verschlüsselung eines Ordners inklusive aller Unterordner. Wer mit den beiden vorgegebenen Standardordnern klarkommt („/home/[user]“ oder Untermenge „/home/[user]/Private“), kann sich über komfortabelste Bedienung freuen. Die Einrichtung ist einfach und Sie benötigen kein Extrakennwort, da Ecrypt FS durch die Systemanmeldung entschlüsselt. Die Sicherheit hängt daher vom Systempasswort ab.

1. Verschlüsseltes „Home“ des Erstbenutzers: Linux Mint 19.x bringt diese Möglichkeit nach wie vor im Installer mit. Mit der Option „Meine persönlichen Dateien verschlüsseln“ wird Ecrypt FS automatisch für das Home-Verzeichnis des Erstbenutzers eingerichtet. Bei Fremdzugriff auf das Gerät ist zwar der Großteil des Dateisystems lesbar, nicht aber der Inhalt von „/home/[user]“. Dieser liegt verschlüsselt unter „/home/.ecryptfs/[user]/.Private“. Die Dateien werden automatisch unverschlüsselt nach „/home/[user]“ geladen, sobald sich der Benutzer anmeldet. Aus Anwendersicht ändert sich nichts beim Umgang mit den Dateien.

2. Verschlüsseltes „Home“ für weitere Konten: Unter Ubuntu, Linux Mint & Co. ist es sehr einfach, weitere Konten mit Home-Verschlüsselung einzurichten. Falls Ecrypt FS nicht installiert ist, holen Sie dies zunächst mit

```
sudo apt install ecryptfs-utils
```

nach. Danach legt dieser Terminalbefehl

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

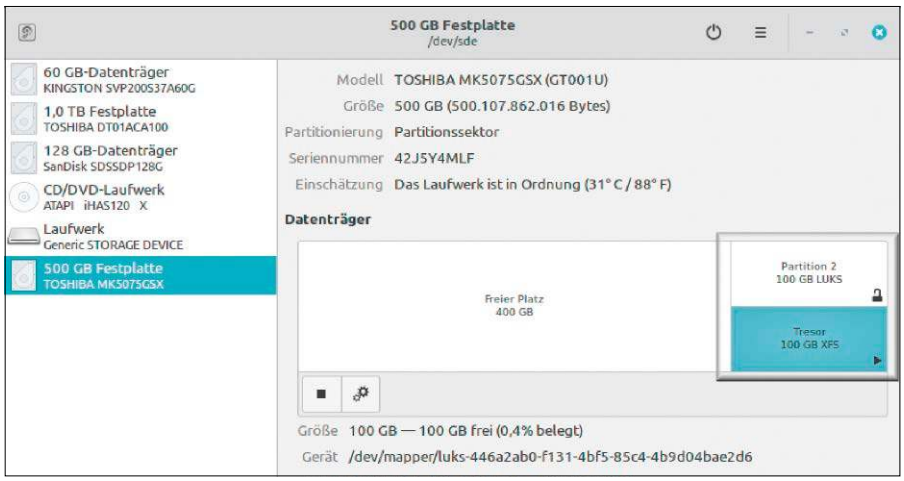
einen neuen Benutzer an. Das Passwort für den neuen Benutzer wird mit „Geben Sie ein neues UNIX-Passwort ein:“ abgefragt. Danach kann sich der neue Benutzer anmelden und das verschlüsselte Home-Verzeichnis nutzen. Das Mounten der verschlüsselten Daten erfolgt auch hier automatisch mit der Systemanmeldung.

3. Nur den Unterordner „~/Private“ verschlüsseln: Ecrypt FS kann jederzeit genutzt werden, um im eigenen „Home“ einen geschützten Unterordner anzulegen, der standardmäßig den Namen „Private“ erhält:

```
ecryptfs-setup-private
```

Das Kommando fordert zunächst die Eingabe des normalen Systemkennworts („loginpassphrase“). Danach erwartet das Werkzeug mit der „mount-passphrase“ den Schlüssel, mit dem die Daten codiert werden. Die „mount-passphrase“ müssen Sie bei der späteren Benutzung niemals interaktiv eingeben und sollte zur höheren Sicherheit komplex ausfallen. Nach der nächsten Anmeldung erscheint im Home-Verzeichnis der neue Ordner „~/Private“. Alle Dateien darin werden bei der Anmeldung automatisch aus dem versteckten Ordner „~/.private“ entschlüsselt und bei der Abmeldung dorthin verschlüsselt.

Gut integriertes Ecrypt FS: Ein knapper Befehl aktiviert den verschlüsselten „Private“-Unterordner. Ein komplett verschlüsseltes Home kann ein adduser-Befehl einrichten – aber nur für neue Konten.



Luks auf kleiner Partition: Die Verschlüsselung muss nicht mehr Platz einnehmen, als Sie für sensible Daten tatsächlich brauchen. Die übrige Laufwerkskapazität bleibt normal nutzbar.

Luks-Verschlüsselung: Transparent und flexibel

Luks (Linux Unified Key Setup) ist eine Datenträgerverschlüsselung ähnlich Bitlocker unter Windows. Gut organisiert leistet Luks aber mehr als die typische Komplettverschlüsselung des Systems.

1. Vollverschlüsselung ab Installation: Ubuntu-Distributionen bieten Luks bei der Systeminstallation. Im Dialog „Installationsart“ erscheint die Option „Die neue [...] Installation zur Sicherheit verschlüsseln“. Sobald Sie diese aktivieren, wird der weitere Punkt „LVM [...] verwenden“ aktiv. Der Logical Volume Manager ist notwendig, um neben der unverschlüsselten Bootpartition die Luks-formatierte Partition und die virtuelle LVM-Partition unterzubringen, die später – bei korrekter Kennworteingabe – unverschlüsselt ins Dateisystem geladen wird. Das Kennwort wird im nächsten Installerschritt abgefragt: Es sollte komplex, aber für tägliche Eingabe zumutbar sein: Das System startet später nur noch nach Kennworteingabe.

2. Luks auf USB: Luks kann auch USB-Laufwerke schützen. Mit dem Standardtool Gnome-Disks („Laufwerke“ unter Ubuntu und Linux Mint) ist das besonders einfach (ähnlich der „KDE Partition Manager“): Sie schließen das USB-Laufwerk an, hängen es im Dateimanager oder mit Gnome-Disks aus und löschen mit dem Laufwerkstool bestehende Partitionen mit dem Minus-Symbol unterhalb der Partitionsanzeige. Mit dem Plus-Symbol erstellen Sie auf dem freien Speicherplatz eine neue Partition mit Größenangabe. Mit „Nächstes“ geht es zum Folgedialog, wo Sie den „Datenträgernamen“ vergeben und als „Typ“ die Option „Andere“ wählen. Mit „Nächstes“ kommt dann der Dialog mit der Dateisystemwahl, der unten rechts den Eintrag „Passwortgeschützter Datenträger (LUKS)“ anzeigt. Nach Kennwortvergabe und Formatieren ist das Laufwerk präpariert. Bei späterer Verwendung verlangen Linux-Dateimanager automatisch das Kennwort und mounten den Datenträger bei korrekter Eingabe.

3. Partitionierungstipps: Luks-Verschlüsselung auf USB fordert keineswegs den kompletten Datenträger. Sie können den geschützten Bereich so klein oder groß definieren, wie Sie möchten. Wenn Sie etwa ein Zwei-TB-Medium mit einer Luks-Partition mit 400 GB einrichten, eine zweite unverschlüsselte Partition mit den restlichen 1600 GB, dann verhält sich diese zweite Partition unter Linux wie Windows standardmäßig: Beim Anstecken des Datenträgers wird die Partition im Dateimanager geladen (sofern ein kompatibles Dateisystem vorliegt). Die Luks-Partition sieht hingegen nur Linux und fragt nach dessen Kennwort. Bei korrekter Eingabe lädt Linux dann auch diese Partition. Die Reihenfolge der Partitionen – Luks-Partition am Anfang oder am Ende – spielt keine Rolle.

Was für USB-Laufwerke gilt, gilt auch für interne Festplatten. Durch Aufteilung der Systemfestplatte in System- und Luks-Partition erhalten Sie einen geschützten Bereich, den Sie im Dateimanager unter „Geräte“ per Klick bequem ein- und aushängen. Wer diese Konstellation nachträglich einrichten möchte, muss die Systempartition mit einem Livesystem und Gparted verkleinern, um im freien Platz eine Luks-Partition zu schaffen. ■

Verschlüsselte Veracrypt-Container

Veracrypt ist die beste Wahl, wenn verschlüsselte Daten auf unterschiedlichen Betriebssystemen genutzt werden. Die Software ist unter Linux, Windows und Mac-OS zwar nicht völlig funktionsgleich, aber die verschlüsselten Daten sind kompatibel.

VON HERMANN APFELBÖCK

Quelle: David Wolski

Veracrypt ist Open-Source-Software und kann keine geheimen Hintertüren für Geheimdienste verbergen. Es eignet sich für große Datenmengen auf Festplatten und mobilen USB-Datenträgern, weniger für den Transfer in die Cloud, da auch bei geringen Datenänderungen der Transport des gesamten Volumes („Container") notwendig wäre. Der technische Anspruch von Veracrypt geht deutlich über so einfache Motive hinaus, Mitarbeiteradressen oder Gehaltstabellen zugriffssicher zu verschlüsseln. Mit versteckten Volumes, diversen Verschlüsselungsalgorithmen, Zugangsmethoden über Passwort, PIM und Schlüsseldateien taugt das Werkzeug für politisch Verfolgte, vermutlich auch für strafrechtliche Verfolgte. Veracrypt ist komplex, wer sich jedoch auf das Wesentliche konzentriert, ist mit den Handgriffen zum Erstellen und Mounten von verschlüsselten Containern schnell vertraut.

Plattformen und Installation

Veracrypt gibt es auf der Projektseite *www.veracrypt.fr/en/Downloads.html* für Linux, Windows und Mac-OS. Generell ist Veracrypt auf Windows fokussiert und dort nochmal deutlich komplexer, da es auch Systempartitionen verschlüsselt und für externe Datenträger eine In-Place-Verschlüsselung bestehender Datenträger ohne Datenverlust anbietet. Unter Mac-OS ist neben Veracrypt das zusätzliche OSXFUSE erforderlich, um Veracrypt-Container laden zu können. Wenn Sie Veracrypt von der Projektseite auf Linux Mint installieren wollen, wählen Sie derzeit das DEB-Paket für Ubuntu 18.04. Alternativ funktioniert auf allen Ubuntu-basierten Distributionen auch die Einrichtung über ein PPA:

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

Im Unterschied zur Windows-Version ist Veracrypt unter Linux nicht Deutsch lokalisiert, weswegen wir uns bei den Menübezeichnungen an die englischsprachigen halten.

Die Datenträgerverschlüsselung

Da Veracrypt unter Linux einen Datenträger oder eine Partition komplett löschen und neu formatieren muss, um ihn zu verschlüsseln, gibt es nur einen nennenswerten Grund für die Komplettverschlüsselung: Der Datenträger soll sich wie ein unformatiertes Laufwerk verhalten. Ein Veracrypt-Laufwerk präsentiert sich unter Linux als unbekanntes Dateisystem und Windows will es umstandslos sofort formatieren. Nur Veracrypt kann das Laufwerk laden.

Ist dies tatsächlich so gewünscht, dann verwenden Sie im Veracrypt-Assistenten nach „Create Volume" die Option „Create a volume within a partition/drive", danach „Standard VeraCrypt volume" und wählen dann mit „Select Device" den Datenträger. Das Gerät selbst, etwa „/dev/sdc", können Sie nur verwenden, wenn der Datenträger im Rohformat ohne Partition vorliegt. Typischerweise ist eine Partitionsangabe wie „/dev/sdc1" die richtige Wahl. Wenn nur eine Partition vorliegt, ist das Resultat von „/dev/sdc" und „/dev/sdc1" dasselbe. Wenn der Datenträger keine unverschlüsselte Partition enthalten soll, sorgen Sie vorab mit Gparted dafür, dass keine oder nur eine Partition vorliegt. Alle weiteren Optionen der Einrichtung unterscheiden sich nicht vom Anlegen eines einfacheren Containers, das nachfol-

gend genauer beschrieben ist. Für das Mounten verschlüsselter Datenträger verwenden Sie die Schaltfläche „Select Device“.

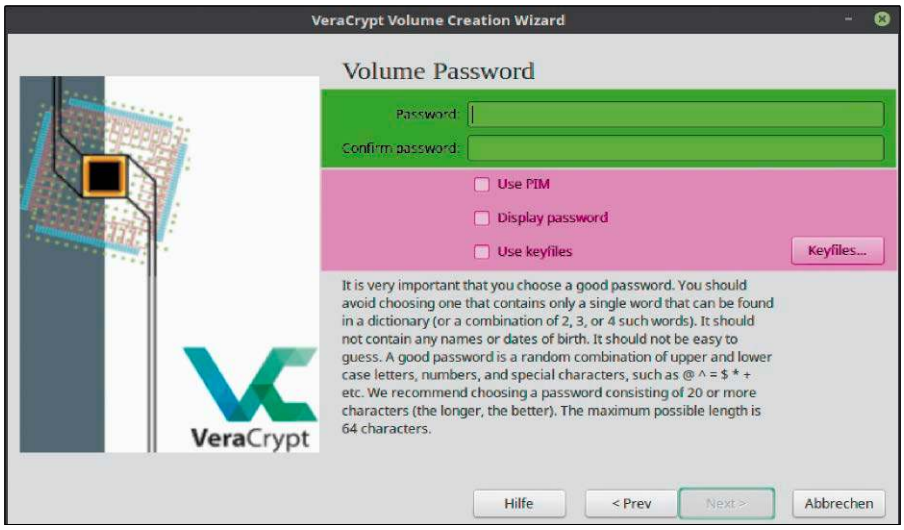
Die Containerverschlüsselung

Die Containerverschlüsselung ist technisch einfacher und die von uns wie auch vom Veracrypt-Assistenten empfohlene. Um eine Containerdatei anzulegen, klicken Sie im Hauptfenster auf „Create Volume“, dann auf „Create an encrypted file container“ und auf „Standard VeraCrypt volume“. Hier geben Sie Pfad und Namen einer bisher nicht existierenden Datei an. Unter „Encryption Options“ belassen Sie alles auf den Vorgaben. Danach geben Sie die Größe der Containerdatei an. Die sollte großzügig ausfallen, weil die Kapazität nicht mehr zu ändern ist.

Danach kommt die Passwortvergabe. Speziellere Optionen sind im nächsten Punkt beschrieben. Für die meisten Szenarien ist ein Passwort völlig ausreichend. Die anschließenden „Format Options“ gelten für das innere Dateisystem des Containers und sind wichtig: Wählen Sie NTFS, wenn Sie die Daten auch unter Windows brauchen. Ein USB-Medium, das Sie unter allen Systemen nutzen möchten, muss nicht nur selbst ein allgemein kompatibles Dateisystem haben, sondern auch der Veracrypt-Container muss mit einem solchen formatiert sein. Im Allgemeinen kann man wenig falsch machen, sowohl als Datenträgerformat als auch beim internen Containerformat NTFS zu wählen. FAT genügt nur, wenn der Container keine Dateien größer als vier GB aufnehmen muss.

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

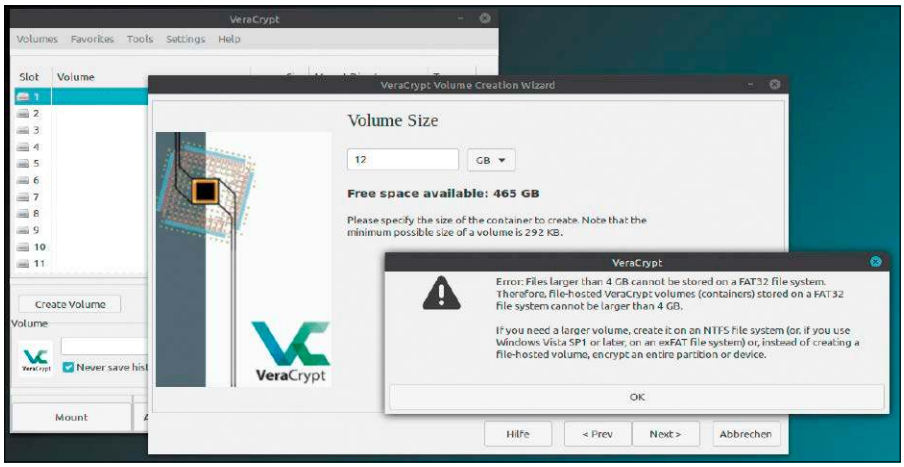
Zur Schlüsselerstellung auf Basis des Passworts erwartet Veracrypt Mausbewegungen im eigenen Fenster. Schließen Sie den Vorgang am Ende mit „Format“ ab. Damit



Veracrypt-Einsteiger halten sich besser an die einfache Passwortoption. Die erweiterten Möglichkeiten erhöhen die Komplexität (PIM, Keyfiles, Default Keyfiles).

VERACRYPT: PLUS UND MINUS

+ Veracrypt verschlüsselt sicher und kann als Open-Source-Software keine heimlichen Hintertüren für Geheimdienste enthalten.
+ Veracrypt ist plattformunabhängig und bester gemeinsamer Nenner, wenn verschlüsselte Daten zwischen Linux und Windows (und Mac-OS) ausgetauscht werden. Insbesondere Daten auf USB-Laufwerken können zuverlässig geschützt und auf verschiedenen Betriebssystemen verwendet werden.
+ Veracrypt-Daten können – mit gewisser Vorbereitung – auf einem zentralen Netzwerkserver von allen Systemen genutzt werden.
+ Veracrypt-Container sind flexibel: Anders als bei einer kompletten Datenträgerverschlüsselung ist die Größe beliebig skalierbar und genau auf die Menge der zu verschlüsselnden Daten abstimmbar. Außerdem gibt es keine Beschränkung für die Menge solcher Container.
+ – Die Basisbedienung ist relativ einfach, die Kenntnis aller Optionen jedoch anspruchsvoll.
+ – Veracrypt ist eine Software für PCs und Notebooks. Smartphones und Tablets mit Android und iOS werden nicht direkt unterstützt. Apps wie EDS Lite (Android) und Disk Decipher (iOS) sind unbefriedigend und bieten allenfalls Lesezugriff.
– Mit der bis zur Unsichtbarkeit reichenden Transparenz von Luks (Linux) und Bitlocker (Windows) kann Veracrypt nicht konkurrieren. Im Unterschied zu diesen Verschlüsselungsmethoden führt an der aktiven Benutzung der externen Veracrypt-Software kein Weg vorbei.
– Der Einsatz von Veracrypt erfordert gelegentlich Geduld: Das Laden („Mount“) und Entladen („Dismount“) ist öfter mal zäh, sollte Sie aber keinesfalls veranlassen, den Vorgang durch „Auswerfen“ des Datenträgers oder durch Abziehen eines USB-Mediums zu unterbrechen.
– Beim Hantieren mit Veracrypt-Containern werden Sie zusätzlich zum Containerpasswort stets auch nach dem sudo-Kennwort gefragt werden, das mit dem Veracrypt-Passwort nichts zu tun hat und vermutlich anders lautet. Unter Windows geschieht mit der Abfrage der Benutzerkontensteuerung im Prinzip technisch dasselbe, kann aber dort zu keinen Irritationen führen, weil kein Passwort verlangt wird.



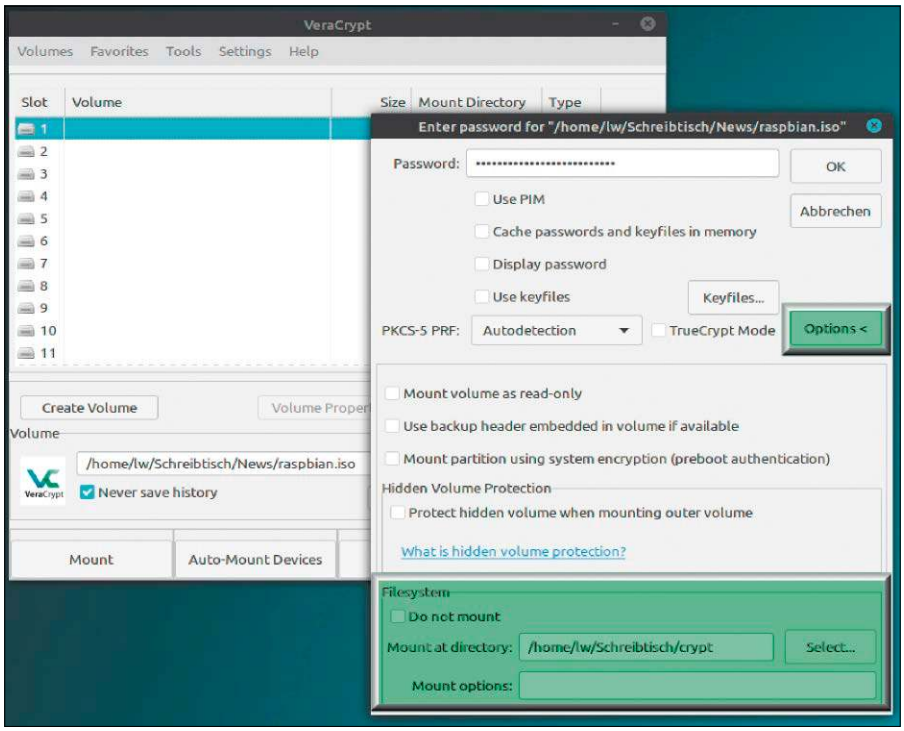
Im Zweifel NTFS: Die Auswahl eines kompatiblen Dateisystems ist zweimal wichtig – einmal für den Datenträger selbst (bei USB-Medien), zum andern für das interne Containerformat.

ist der Container einsatzbereit. Um den Container zu verwenden, navigieren Sie mit „Select File" im Hauptdialog zur Containerdatei. Mit Klick auf „Mount" wird diese im Dateimanager geöffnet. Linux mountet Container standardmäßig (aber nicht zwangsläufig) nach „/media/veracrypt [nummer]", Windows auf freie Laufwerksbuchstaben. Auf diesen Datenträgern lesen und arbeiten Sie wie auf einem normalen Laufwerk. Die Schaltfläche „Dismount" im Hauptdialog entlädt den Container, der somit wieder geschützt ist.

Optionen für erhöhte Sicherheit

Bei der Passwortvergabe haben wir bisher zwei Optionen übergangen. Interessant sind sie durchaus, aber sie erhöhen die Komplexität.

Container mit Passwort und PIM: Beim Erstellen des Containers gibt es im Dialog der Passwortdefinition die zusätzliche Option „Use PIM". Hier kann eine Zahl eingetragen werden. Geschieht dies, so genügt das Kennwort zum Öffnen dieses Containers nicht mehr. Zusätzlich ist die exakte PIM-Zahl erforderlich. Vereinfacht gesagt, handelt es sich um ein zusätzliches Kennwort für deutlich erhöhten Schutz. Technisch definiert der „Personal Iterations Multiplier" die Anzahl der Wiederholungen von Hashfunktionen, die beim Erreichen des genauen PIM-Werts den Entschlüsselungsheader generieren. Achtung: Ein hoher PIM-Wert (vier- und fünfstellig) verlangsamt den Mountvorgang deutlich.



Optionen ohne Ende: Manche interessante Veracrypt-Funktion erschließt sich erst beim zweiten Blick, so etwa, dass die Linux-Version einen Container in jeden beliebigen Pfad laden kann.

Container mit Passwort und Keyfile: Der Passwortdialog hält eine weitere Möglichkeit parat – nämlich die „Keyfiles" (Schlüsseldateien). Dabei kann es sich um eine oder mehrere beliebige Datei(en) handeln, die Veracrypt zum Öffnen des Containers zusätzlich zum Passwort benötigt. Entscheidend für die Schlüsselfunktion dieser Datei sind deren erste 1024 Bytes, nicht Pfad oder Dateiname. Der Inhalt der Schlüsseldatei darf sich also keinesfalls ändern, das Verzeichnis oder der Dateiname jedoch durchaus. Ideale Kandidaten für Schlüsseldateien sind Binärdateien, PDFs oder ISO-Images, die normalerweise nie geändert werden.

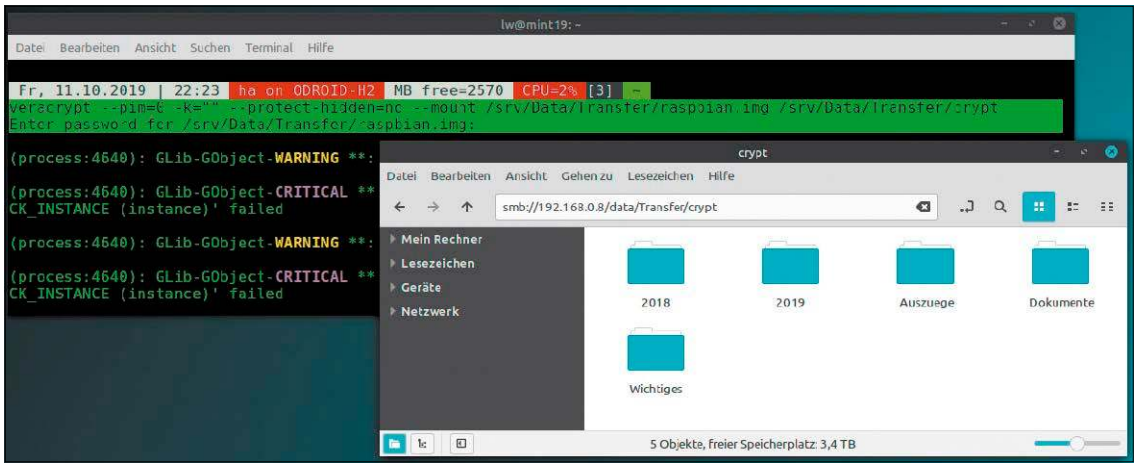
Ein Keyfile ist wie die PIM-Zahl additiv: Es ersetzt nicht das Passwort, sondern muss zusätzlich vorliegen. Das Keyfile kann ein schwächeres Kennwort rechtfertigen und die Kennworteingabe verkürzen.

Zum passenden Keyfile müssen Sie zum Öffnen eines Containers normalerweise über die Schaltfläche „Keyfiles" manuell navigieren. Jedoch gibt es auch die Option, über „Settings → Default Keyfiles" auf einem Rechner eine Standarddatei zu verwenden. Diese berücksichtigt Veracrypt dann automatisch – ohne manuelle Auswahl.

Schaltfläche „Volume Tools": Für einen geladenen Container lassen sich alle bisherigen Einstellungen nachträglich ändern. Das erledigen Sie im Hauptfenster über „Volume Tools". Sie können ein neues Passwort vergeben oder Keyfiles hinzufügen oder entfernen. Beachten Sie, dass die Aktion noch einmal eine korrekte Anmeldung mit den bisherigen Daten erfordert.

Container im Netzwerk

Verschlüsselte Daten im Netzwerk freizugeben, scheint paradox. Im privaten Heimnetz ist das aber nicht nur praktikabel, sondern auch komfortabel, weil die Veracrypt-Container dann an zentraler Stelle liegen und von Linux- wie Windows-Rechnern bearbeitet werden können. Im Prinzip gibt es zwei Möglichkeiten:



Veracrypt-Container im Netz: Wenn Veracrypt am Server läuft, kann dieser via SSH den Container auf eine Samba-Freigabe mounten. Im Heimnetz ist das sicher zu vertreten.

A. Der verschlüsselte Container liegt auf einer Samba- oder Windows-Freigabe des Servers und wird am Clientrechner mit Veracrypt gemountet.

Dies wäre die sicherste Möglichkeit, hat aber zu viele Einschränkungen. Unter Linux müsste dazu die komplette Samba-Freigabe vorher ordentlich ins Dateisystem gemountet werden. Und selbst wenn dabei alle Rechteprobleme ausgeräumt würden, könnte Veracrypt den Container nur für Lesezugriff laden.

B. Der verschlüsselte Container wird auf dem Server selbst mit Veracrypt gemountet, und zwar in einen Ordner auf einer bestehenden Samba-Freigabe. Diese zweite Möglichkeit ist unkomplizierter, hat keine Beschränkungen, ist aber auch unsicherer: Solange der Container auf die Freigabe gemountet ist, haben die Samba-Berechtigten auf die Daten Zugriff.

Es ist letztlich eine Frage der Netzwerkrechte und der Menge der Netzteilnehmer, ob diese Möglichkeit in Betracht kommt. Im Privatnetz sollte wenig dagegen sprechen. Die notwendigen Zutaten dieser Variante B sind folgende:

1. Als Server kommt nur Linux ernsthaft infrage: Sie benötigen nämlich SSH-Zugriff (also einen laufenden Open-SSH-Server) und eine Samba-Freigabe (Samba-Server). Das ließe sich mit Windows-Freigabe und Remotesteuerung auch realisieren, jedoch benötigt der Server außerdem ein installiertes Veracrypt. Und ungeachtet mancher Defizite der Linux-Variante hat Veracrypt unter Linux einen entscheidenden Vorteil: Es kann den Containerinhalt in jedes beliebige Verzeichnis mounten („Mount → Options → Mount at directory“ oder per Kommandozeile, siehe unten).

2. Den Veracrypt-Container erstellen Sie auf dem Server selbst oder kopieren einen existierenden auf den Server.

3. Sie mounten den Container bei Bedarf auf dem Server auf die Samba-Freigabe. Da sämtliche Veracrypt-Aktionen auch als Terminalkommando zu erledigen sind, geschieht das am einfachsten über SSH auf der Kommandozeile – im Prinzip:

```
ssh [server-ip]
veracrypt --mount [Containerdatei]
  [Mountpunkt_auf_Samba_Freigabe]
```

Achtung: Die Anmeldung am Server und das Mounten des Containers muss mit einem Systemkonto geschehen, das sowohl Zugriff auf die Samba-Freigabe besitzt als auch sudo-Berechtigung (notwendig zum Mounten von Veracrypt-Containern).

Der Befehl fragt allerdings auch weitere Zugangsmethoden wie PIM und Schlüsseldateien ab. Wenn nur ein Passwort genutzt wird, unterdrücken Sie alle weiteren Abfragen mit diesem Befehl (konkretes Beispiel):

```
ssh ha@192.168.0.8
veracrypt --pim=0 -k="" --protect-
  hidden=no --mount /srv/Data/
  crypt.iso /srv/Data/crypt
```

Nicht wundern: Während hier alle anderen Veracrypt-Schalter in der ausführlichen Form mit Doppelbindestrich geschrieben sind, benötigt der Keyfiles-Schalter offenbar die Kurzform „-k“. Der lange Befehl ist natürlich ein Kandidat für ein Bash-Alias, das die Sache abkürzt. Der Pfad „/srv/Data“ in diesem Beispiel wäre per Samba freigegeben und somit die Containerdaten anschließend im Unterverzeichnis „crypt“ für berechtigte Samba-Konten zugänglich.

4. Nach der Bearbeitung der verschlüsselten Daten entlädt der Befehl (wieder auf dem Server via SSH)

```
veracrypt --dismount
```

alle Veracrypt-Container. Ist ein Container gerade in aktiver Benutzung, erscheint womöglich eine Fehlermeldung. Dies können Sie mittels

```
veracrypt --force --dismount
```

zwar ignorieren, aber es empfiehlt sich, das betreffende zugreifende Programm (oft nur der Dateimanager auf einem Samba-Client) zu beenden und dann den normalen Entladebefehl aufzurufen. ■

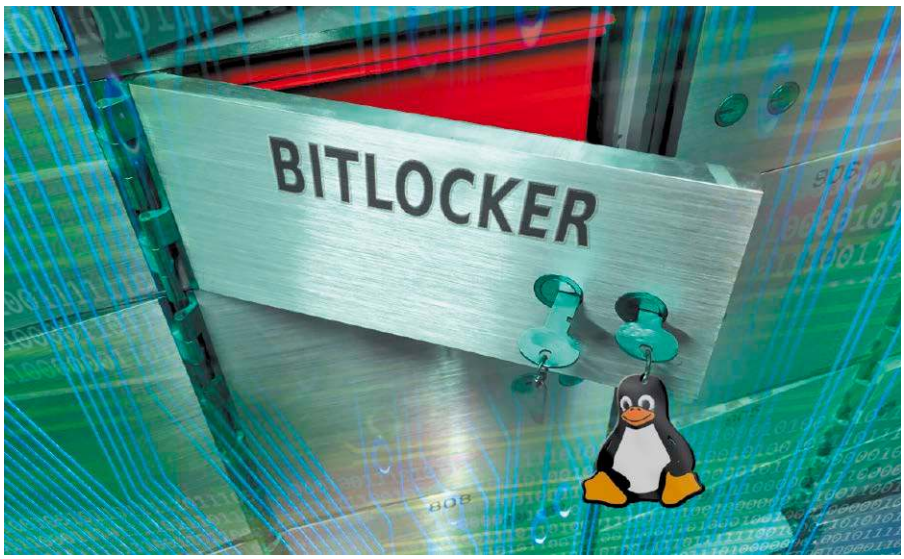
PARANOIA? VERSTECKTE VOLUMES!

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

Bitlocker unter Linux

Die Verschlüsselung von Partitionen erledigt in Windows-Systemen das Tool Bitlocker. Diese Verschlüsselungstechnik hat den Ruf, nur mit Windows zu funktionieren. Mit Dislocker kann aber auch Linux auf solche Partitionen zugreifen.

VON DAVID WOLSKI



© David Wolski

Die Bitlocker-Laufwerkverschlüsselung ist eine Windows-Funktion, die interne und externe Laufwerke vor fremden Zugriffen schützt. In den meisten Firmen ist die sichere Verschlüsselung von Datenträgern und die komplette Systemverschlüsselung von Laptops Pflicht. Bitlocker schützt auch vor Zugriffsversuchen mit einem Livesystem oder auf physisch entfernter Festplatte. Microsoft stellte Bitlocker erstmals in Windows Server 2008 vor, dehnte die Unterstützung dafür aber auf Windows Vista Ultimate sowie Enterprise aus, später auf die Professional-Versionen von Windows ab Version 7. Mit Bitlocker-To-Go gibt es seit Windows 7 außerdem die Möglichkeit, externe USB-Medien per Bitlocker zu verschlüsseln.

Der Verschlüsselungsalgorithmus von Bitlocker hat sich häufiger geändert, oft ohne ausführliche Erklärungen seitens Microsoft, und ist nun bei AES-XTS mit einer (optionalen) Schlüssellänge von 256 Bit angekommen. Auch wegen dieser Änderungen hat Bitlocker den Ruf, eine ganz und gar proprietäre Verschlüsselung zu sein, mit der außerhalb eines Windows-Dunstkreises wenig anzufangen ist. Das stimmt aber nicht ganz: Mit Dislocker gibt es ein Modul für den Userspace-Dateisystemtreiber Fuse, der das Einhängen von Bitlocker-Laufwerken mit dem korrekten Schlüssel auch unter Linux erlaubt.

Dislocker im Einsatz

Eine Einschränkung vorab: Dislocker arbeitet mit bescheidener Zugriffsgeschwindigkeit, bietet aber Lese- und Schreibrechte. Zum Entschlüsseln verlangt das Tool den bei der Bitlocker-Einrichtung erzeugten und (hoffentlich) gespeicherten Wiederherstellungsschlüssel, eine BEK-Datei mit Schlüssel oder bei Bitlocker-To-Go auch nur das vergebene Kennwort. Mit Dislocker können Linux-Systeme also nicht nur externe verschlüsselte Windows-Datenträger lesen, sondern auch Systempartitionen, falls das dort installierte Windows nicht mehr booten will. Dislocker ist mittlerweile in den Standard-Paketquellen der verbreiteten Linux-Distributionen vertreten und wie bei den anderen Dateisystemmodulen für Fuse erfolgt die Bedienung per Kommandozeile. Zur Installation genügt in Debian/Ubuntu (auch in Livesystemen) der

DISLOCKER MIT SCHREIBZUGRIFF

Um mit Linux auf Windows-Partitionen zu schreiben, ist es vorher unter Windows nötig, entweder die Schnellstart-Funktion abzuschalten oder – einfacher – das System komplett herunterzufahren. Die Windows-Funktion „Herunterfahren" tut dies nämlich nicht – und dann droht Datenverlust, wenn ein Linux-Livesystem oder ein parallel installiertes Linux auf die betroffene Partition zugreift. Immerhin erkennt der NTFS-Treiber unter Linux das Problem und wird sich dann weigern, die Partition im Schreibmodus einzuhängen.

Die Lösung lautet, Windows mit „Neu starten" zu beenden, was die Schnellstart-Funktion unterbindet. Auch der Kommandozeilenbefehl

```
shutdown /s /f
```

erledigt einen vollständigen Systemabschluss. Danach kann Dislocker wie folgt

```
sudo mount -o loop /mnt/bitlocker/dislocker-file /mnt/laufwerk
```

eine Bitlocker-Partition auch mit Schreibzugriff einhängen.

folgende Befehl

```
sudo apt-get install dislocker
```

und in Fedora, Cent-OS und Red Hat Linux dieser Befehl:

```
sudo dnf install dislocker
```

Der Quellcode von Dislocker findet sich auf Github unter *https://github.com/Aorimn/dislocker* zusammen mit recht detaillierten Anleitungen zum Kompilieren, um das Tool beispielsweise auch unter Mac-OS X einzusetzen.

Der erste Schritt ist es, im laufenden Linux-System die Bitlocker-Partition mit ihrer Partitionskennung zu identifizieren. Bei externen Laufwerken ist das üblicherweise kein Problem, bei internen (System-)Partitionen hilft die Eingabe von

```
lsblk -f
```

bei der Suche: Denn NTFS-Laufwerke mit Bitlocker-Verschlüsselung kann lsblk in seiner Auflistung kein Dateisystem zuordnen. Eine Identifizierung ist also durch Ausschluss möglich. Einfacher geht es mit dem grafischen Gparted, das verschlüsselte Partitionen mit dem Dateisystemtyp „Bitlocker" kennzeichnet. Ist die korrekte Partition gefunden, beispielsweise „/dev/sda3", dann kann der Befehl

```
sudo dislocker-metadata -V /dev/
  sda3
```

den Inhalt analysieren und wird zahlreiche Daten zur enthaltenen Bitlocker-Struktur anzeigen. Dies soll zur Bestätigung dienen, dass es sich auch um die richtige Partition handelt.

1. Zum Entschlüsseln und Einhängen der verschlüsselten Partition verlangt Dislocker zwei Verzeichnisse als Einhängepunkte. Diese erstellt man am besten unterhalb des Ordners „/mnt":

```
mkdir /mnt/bitlocker
mkdir /mnt/laufwerk
```

2. In das Verzeichnis wird zunächst mittels Dislocker die Bitlocker-Partition als entschlüsseltes NTFS-Image eingehängt. Dafür ist das Passwort einer Bitlocker-To-Go-Partition nötig beziehungsweise der Wiederherstellungsschlüssel („Recovery-Key") einer chiffrierten Windows-Partition, den ein Windows-System bei der ersten Erstellung eines Bitlocker-Laufwerks zur Sicherung anbietet. Das Kommando

```
sudo dislocker -v -V /dev/sda3 -p /
  mnt/bitlocker/
```

wird hier die Partition „/dev/sda3" entschlüsseln und dazu zunächst das sudo-Passwort und dann das Bitlocker-Kennwort beziehungsweise den Wiederherstellungsschlüssel mit 55 Stellen abfragen.

3. Ist das gelungen, so zeigt nun die Eingabe von

```
sudo ls /mnt/bitlocker/
```

die Datei „dislocker-file" im Zielverzeichnis an. Dieses Image muss jetzt als Loopback-Gerät eingehängt werden, zur Sicherheit im Nur-Lese-Modus. Denn meist ist das Windows-System zuletzt im Ruhezustand gewesen oder mit standardmäßig aktivierter Schnellstart-Option („Fast Startup"). In diesem Fall hängt Windows seine NTFS-Partitionen nicht sauber aus und ein Schreiben auf diese Laufwerke könnte schlimmstenfalls zu Datenverlust führen.

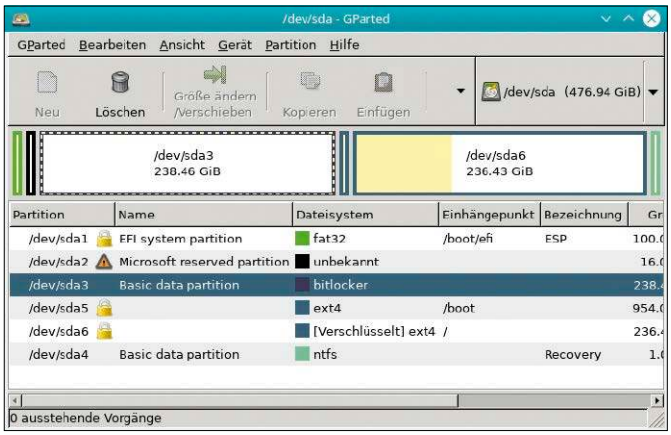
Das Kommando

```
sudo mount -o loop,ro /mnt/
  bitlocker/dislocker-file /mnt/
  laufwerk
```

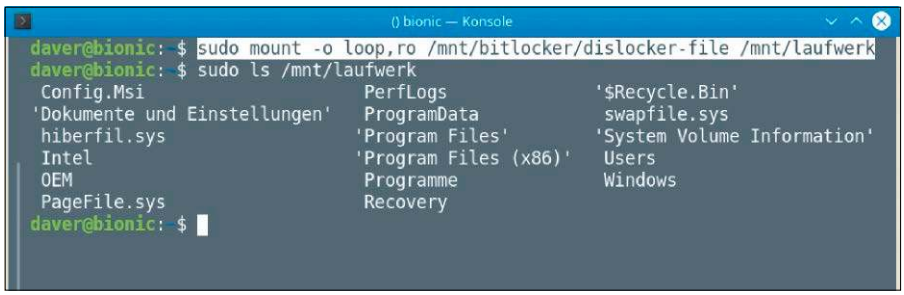
hängt das NTFS-Laufwerk in der Datei „dislocker-file" deshalb nur im Lesemodus nach „/mnt/laufwerk" ein („ro").

4. Jeder beliebige Dateimanager kann nun lesend auf den gesamten Inhalt der Bitlocker-Partition zugreifen. NTFS-Benutzerrechte ignoriert Linux dabei. Soll ein Bitlocker-Laufwerk im Lese- und Schreibmodus eingehängt werden, so muss zunächst Windows komplett beendet werden. Der Kasten „Dislocker: Lesen und Schreiben" gibt dazu Aufschluss. ■

Gparted macht es in seiner Übersicht besonders einfach, die Bitlocker-Partition(en) zu identifizieren. Die Laufwerkskennung wird dann für den Zugriff benötigt.



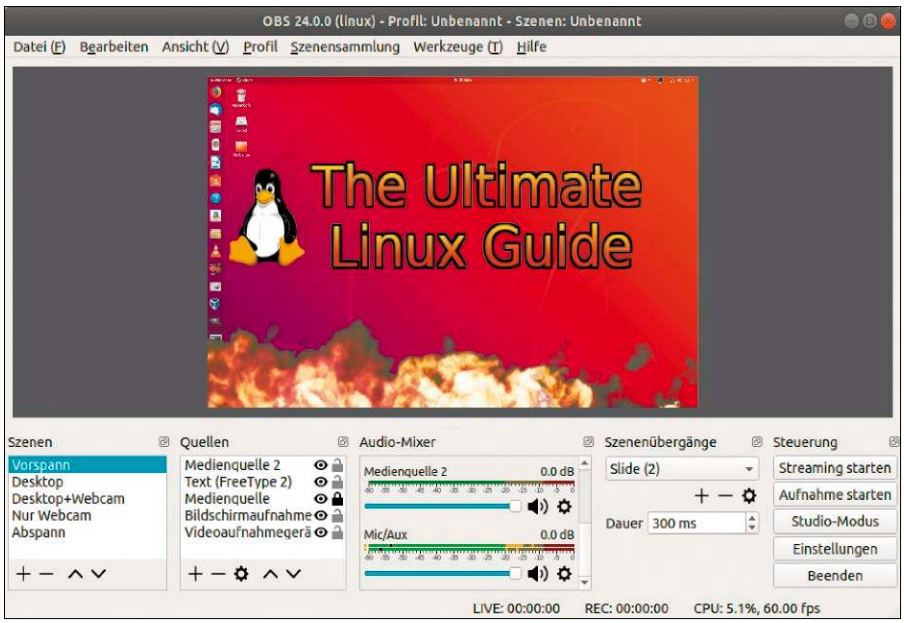
Entschlüsselt: Dislocker erwartet beim Zugriff auf eine verschlüsselte Windows-Partition den Wiederherstellungsschlüssel und zeigt dann die NTFS-Partition als Imagedatei.



NTFS-Partition einhängen: Das entschlüsselte NTFS-Dateisystem erscheint als Datei, die per Loopback eingehängt wird – in diesem Beispiel nur mit Lesezugriff.

Bildschirmaufnahmen für Youtube

Youtube-Videos lassen sich unter Linux bequem erstellen. Die dafür geeignete Software gibt es kostenlos. Für die optimale Qualität der Videos sollten Sie jedoch ein paar Euro in Hardware investieren.



Desktop aufnehmen: OBS Studio bietet viele Funktionen nach kurzer Einarbeitungszeit. Sie können den Desktop aufzeichnen und Bilder, Text sowie die Webcam einbinden.

VON THORSTEN EGGELING

Mit einem Upload von ungefähr 300 Stunden Videomaterial pro Minute ist Youtube die beliebteste Videoplattform im Internet. Viele Beiträge dienen eher der Unterhaltung, aber es gibt auch etliche Lehr- und Lernvideos zu Linux-Themen und Programmiersprachen. Wer selbst Youtube-Tutorials, etwa über die Bedienung eines Linux-Systems oder mit Tipps zu Software, erstellen möchte, benötigt für den Einstieg keine spezielle Ausrüstung. Die erforderliche Software gibt es gratis. Der Erfolg von Youtube-Videos steigt aber in der Regel mit der Qualität, und die ist nur mit zusätzlicher Hardware zu erreichen.

1. Die Hardwareausstattung

Im einfachsten Fall besteht das Video nur aus einer Aufnahme des Desktops. Eine Beschreibung dessen, was da zu sehen ist, kann man beispielsweise in einen Editor tippen, der ebenfalls im Video erscheint. Solche Tutorials sind auf Youtube gelegentlich zu finden, sind aber nicht besonders attraktiv.

Größere Aufmerksamkeit finden Videos mit Audiokommentar. Zur Aufzeichnung genügt das Mikrofon eines Notebooks oder ein Headset. Für eine bessere Audioqualität ist ein allerdings ein USB-Mikrofon mit Stativ, Antivibrationshalterung und Poppschutz empfehlenswert. Die entkoppelte Aufhängung in einer Halterung sorgt dafür, dass Umgebungsgeräusche und Vibrationen in der Aufnahme weniger zu hören sind. Der Poppschutz reduziert die Nebengeräusche beim Sprechen. Solche USB-Mikrofone inklusive Zubehör kosten zwischen 30 und 300 Euro. Die teureren Modelle bieten in der Regel optimale Qualität, die Anschaffung lohnt sich aber nur bei regelmäßiger Nutzung.

Videos erscheinen durch direkte Ansprache des Zuschauers lebendiger und interessanter. Wer persönlich im Video auftritt, wirkt außerdem kompetenter. Für die Aufnahme reicht eine Webcam, wie sie in den meisten Notebooks zu finden ist. Preisgünstige USB-Webcams für den PC gibt es ab etwa 30 Euro, wer bessere Qualität will, muss etwa 100 Euro ausgeben. Webcams für Videokonferenzen oder Livestreaming enthalten in der Regel auch ein Mikrofon. Die Aufnahmequalität liegt aber oft unter der von etwas teureren USB-Mikrofonen.

Eine weitere sinnvolle Anschaffung können Studioscheinwerfer sein, wie sie auch Fotografen verwenden (circa 50 Euro). Webcamaufnahmen lassen sich dann gleichmäßiger ausleuchten, was vor allem bei HD-Videos die Qualität verbessert. Ein Chromakey-Fotohintergrund (Greenscreen oder Bluescreen) vervollständigt die Videoausrüstung. Damit lässt sich der Hintergrund ausblenden und durch ein anderes Motiv ersetzen.

2. Die Softwareausstattung

Eine einfache Recordersoftware ist in Ubuntu und Linux Mint bereits enthalten. Drücken Sie die Tastenkombination Strg-Alt-Umschalt-R, um die Aufnahme zu starten. Ein roter Punkt im Panel am oberen Bildschirmrand (Linux Mint: unten rechts) signalisiert die laufende Aufnahme. Drü-

cken Sie erneut Strg-Alt-Umschalt-R, um die Aufnahme zu beenden. Die Videodatei liegt danach im Ordner „Videos“ oder (bei Linux Mint 19) im Home-Verzeichnis.

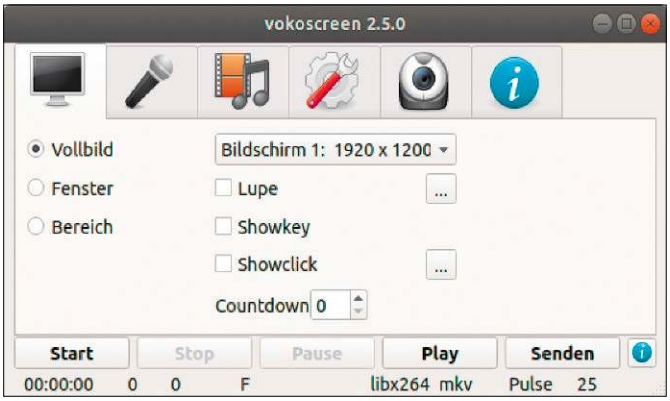
Ein weiterer Bildschirmrecorder, der auch Audio aufnehmen kann, ist **Recordmydesktop**. Das Programm ist in den Standard-Paketquellen enthalten und lässt sich über Ubuntu-Software oder Synaptic installieren (Pakete: „recordmydesktop“ und „gtk-recordmydesktop“). Die Aufzeichnung erfolgt im Theora/Vorbis-Format („ogv“-Datei).

Noch mehr Funktionen bietet **Vokoscreen**, das ebenfalls in den Standard-Paketquellen zu finden ist. Sie können damit den Desktop und Audio aufzeichnen sowie das Bild von einer Webcam in den Aufnahmebereich einblenden. Als Ausgabeformate stehen die Formate Matroska und MPEG-4 mit den Codecs „libx264“ oder „mpeg4“ zur Verfügung.

Das Profitool **OBS Studio** (Open Broadcaster Software, *https://obsproject.com*) bietet die meisten Möglichkeiten, ist aber nicht ganz einfach zu bedienen. Wie Sie mit der Software umgehen, erklären wir im nächsten Punkt.

Audio aufzeichnen: Wer auf die Audioqualität Wert legt, sollte ein hochwertigeres Mikrofon verwenden. Eine entkoppelte Aufhängung sowie Poppschutz sind empfehlenswert.

Bessere Videoaufnahmen: Gute Webcams gibt es für um die 80 Euro. Die meisten aktuellen Modelle, etwa die Logitech C922 Pro Stream, werden von Linux direkt unterstützt.



Übersichtlicher Screenrecorder: Vokoscreen kann den Desktop, ein Fenster oder einen Bereich aufzeichnen und bei Bedarf gleichzeitig den Stream einer Webcam darstellen.

3. OBS Studio einrichten und nutzen

OBS ist nicht in den Standard-Paketquellen enthalten, kann aber über ein PPA installiert werden. In einem Terminalfenster installieren Sie zuerst den Medienkonverter Ffmpeg:

```
sudo apt-get install ffmpeg
```

Danach fügen Sie das PPA hinzu und installieren OBS (drei Zeilen):

```
sudo add-apt-repository
 ppa:obsproject/obs-studio
sudo apt-get update
sudo apt-get install obs-studio
```

OBS konfigurieren: Nach dem Start des Programms gehen Sie auf „Datei → Einstellungen“ und dann auf „Ausgabe“. Unter „Aufnahme“ geben Sie hinter „Aufnahmepfad“ ein Zielverzeichnis an, beispielsweise „Videos“ in Ihrem Home-Verzeichnis. „Aufnahmequalität“ und „Aufnahmeformat“ sollten Sie unverändert lassen, außer es sind besondere Einstellungen für einen bestimmten Zweck erforderlich. Unter „Kodierer“ wählen Sie „Hardware (NVENC)“, sofern ein Nvidia-Grafikchip im PC steckt und der proprietäre Nvida-Treiber installiert ist. Das sorgt für eine geringere CPU-Belastung bei der Aufnahme.

Gehen Sie auf „Audio“ und konfigurieren Sie das Mikrofon. Unter „Video“ stellen Sie die gewünschte Bildschirmauflösung ein. Sie können die Standardauflösung des Desktops oder eine geringere Auflösung verwenden.

Aufnahme vorbereiten und starten: Klicken Sie links unten unter „Szenen“ auf die „+“-Schaltfläche und dann auf „OK“. Unter „Szenen“ versteht OBS eine Sammlung von Quellen. Klicken Sie unter „Quellen“ auf die „+“-Schaltfläche, wählen Sie „Bildschirmaufnahme (XSHM)“ und bestätigen Sie mit „OK“. Sie sehen ein Vorschaubild und hinter „Bildschirm“ lässt sich der gewünschte Monitor auswählen, wenn mehrere vorhanden sind. Klicken Sie auf „Okay“. Auf dem gleichen Weg fügen Sie ein „Videoaufnahmegerät (V4L2)“ zur Szene hinzu, wenn Sie den Videostream von einer Webcam in das Video einfügen möchten. Ziehen Sie den Eintrag unter „Quellen“ an die erste Position, damit das Bild der Webcam über der Desktopaufnahme liegt. Ziehen Sie den Bereich mit der Maus auf eine passende Größe.

Über „Medienquelle“ können Sie Bilder und andere Videos einbauen, über „Text (Free Type 2“) Titel und Beschriftungen. Wenn Sie diese Quellen in einer eigenen Szene verwenden, lassen sich damit beispielsweise Vorspann und Abspann realisieren. Bei Bedarf erstellen Sie Szenen für alle gewünschten Kombinationen, etwa nur für die Desktopaufzeichnung, Desktop plus Webcam oder die Webcam alleine.

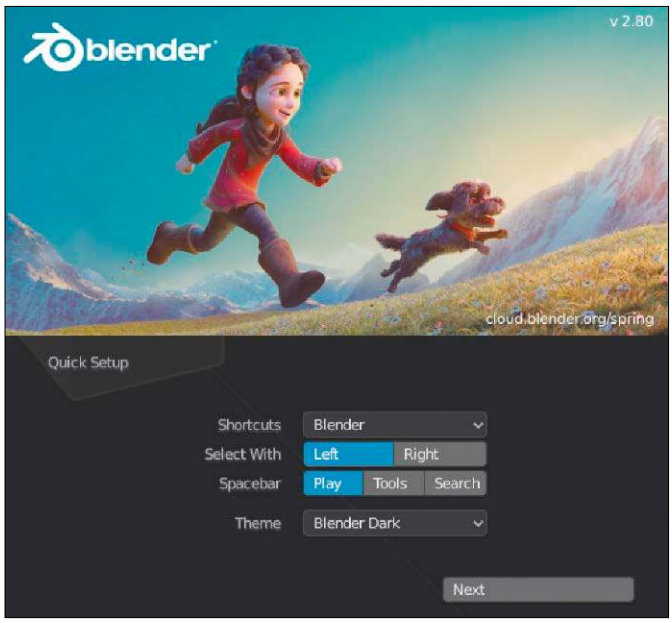
Klicken Sie auf „Aufnahme starten“ und zeichnen Sie das Video auf. Wenn Sie mehrere Szenen erstellt haben, klicken Sie die gewünschte unter „Szenen“ an, um die Darstellung zu ändern. Zum Abschluss klicken Sie auf „Aufnahme stoppen“. Das fertige Video laden Sie anschließend bei Youtube hoch. Die Uploadfunktion verbirgt sich hinter dem Kamerasymbol rechts oben. ■

Blender 2.8: Gutes wird noch besser

Die Entwickler der kostenlosen 3D-Rendering-Software Blender haben sich mit dem Update ordentlich Zeit gelassen. Nach rund zwei Jahren hat das Warten aber jetzt ein Ende. Wir stellen die neue Version mit ihren Änderungen vor.

VON STEPHAN LAMPRECHT

Wer nach einer kostenfreien Möglichkeit sucht, dreidimensionale Objekte und Landschaften zu gestalten, kommt seit vielen Jahren um Blender nicht herum. Seit über 15 Jahren verrichtet das Werkzeug auf unzähligen Computern seine Dienste. Jetzt liegt die neue Version 2.8 für Linux, Windows und Mac-OS vor. Wie gewohnt, genügt es, sich das Archiv von der Projektseite zu laden und zu entpacken. Gestartet wird Blender dann über die ausführbare Datei innerhalb des Pakets.



Erste Schritte in Blender: Bereits im Startdialog können Sie zwischen den neuen Tastenbelegungen, der neuen Optik und den Templates umschalten.

Die Optik: „Darkmode“ muss wohl sein

Eine der größten Neuerungen begegnet Ihnen direkt nach dem Programmstart. Denn Blender besitzt jetzt, wie viele andere Kreativprogramme, einen „Darkmode“. Die gesamte Oberfläche präsentiert sich somit in Schwarz und Weiß – das soll ja bekanntlich besser für die Augen sein.

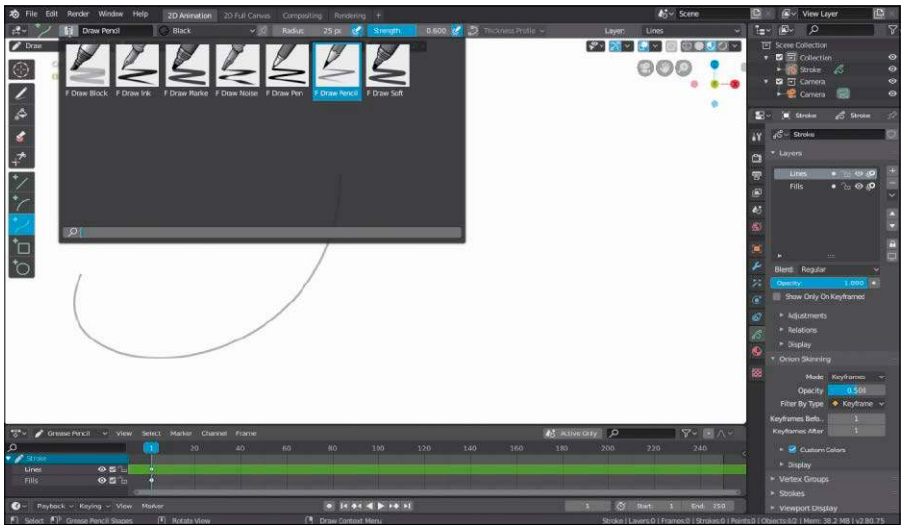
Das Programmfenster hat sich aber nicht nur optisch verändert. Neueinsteiger werden davon wenig bemerken, wer aber mit den Vorgängerversionen gearbeitet hat, muss sich erst einmal neu orientieren. Icons und Widgets dominieren das Programmfenster. Blender-Vertraute können sich aber auf die Hotkey-Bedienung verlassen. Das neue Bedienkonzept nutzt die Maus intensiver, aber Shortcuts gibt es immer noch reichlich. Da sich die Tastaturbelegung teilweise geändert hat, kann in den Einstellungen die Keymap der Vorgängerversion aktiviert werden. Dort finden Sie als dritte Variante auch noch ein Setting mit dem Titel „Industrial Standard“, das sich an anderen Kreativprogrammen orientiert. Die Einstellungen finden Sie ab sofort im Menü „Edit“.

Wer sich für die neue Standardbelegung entscheidet, kann sich in Hinblick auf die Bedienung über eine weitere Neuerung freuen. Denn jetzt funktioniert die Auswahl von Objekten auch mit der linken Maustaste. Neu ist auch das Konzept der „Workspaces“. Diese finden sich in der oberen Navigationsleiste und orientieren sich an typischen Arbeitsschritten auf dem Weg zum gerenderten Produkt: Modellierung der Objekte – UV-Editing – Shading. Im Startdialog kann der Nutzer zudem zwischen Templates wählen. Diese stellen die Werkzeuge und Strukturen von Menüs sinnvoll für einzelne Aufgabenstellungen zusammen. Wird dort etwa „2D Animation“ ausgewählt, werden die Optionen für die dreidimensionale Darstellung ausgeblendet. Schön ist zudem, dass jetzt mit beliebig vielen Ebenen gearbeitet werden kann, die sich auch gruppieren lassen. Wohl lange auf der Wunschliste vieler Anwender dürfte auch das gleichzeitige Bearbeiten mehrerer Objekte gestanden haben.

Ausgebaute 2D-Animationen

Auch der 2D-Bereich wurde ausgebaut. Damit ist Blender auf dem Weg, ein universelles Werkzeug für die komplette Produktion von Animationsvideos zu werden. Der bisher funktional etwas bescheidene Grease Pencil wurde um viele Funktionen erweitert. Mit den neuen Werkzeugen, Paletten und dem Editiermodus können Konzept-

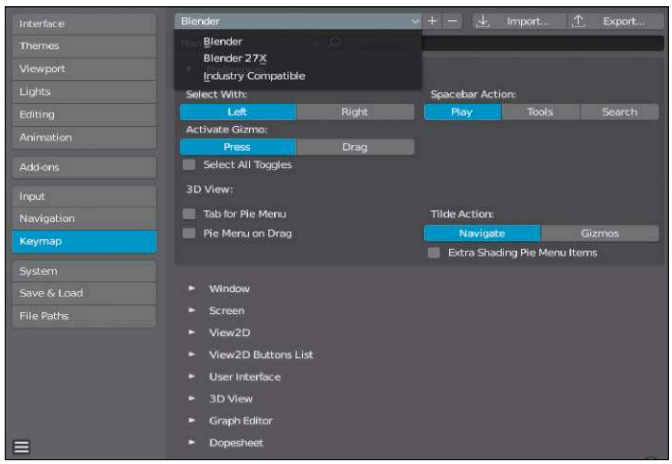
zeichnungen und Storyboards gezeichnet und animiert werden. Wer bereits mit anderen Vektorzeichenprogrammen gearbeitet hat, wird sich sofort heimisch fühlen. Bézierkurven, Linien, Primitive: Alles ist da und lässt sich intuitiv einsetzen. Spaß machen auch neue visuelle Effekte: „Pixelate" versieht das Objekt mit der Anmutung früherer Klötzchenspiele aus der Zeit eines C64. Kreatives Zeichnen am Computer per Maus bleibt aber auch in Blender eine Herausforderung. Die Investition in ein Zeichentablet lohnt sich.



Der 2D-Bereich mausert sich zu einem vollwertigen Zeichenprogramm. Jetzt können mit Blender auch Storyboards angelegt und animiert werden.

Noch mehr Realitätsnähe

Eine Herausforderung bei der Schaffung künstlicher Welten bleiben nach wie vor volumetrische Objekte wie Haare, Rauch oder auch Feuer. Für die High-End-Rendering-Maschine in Blender haben die Entwickler zwei neue Principled Shader gebaut. „Volume" eignen sich sowohl für Rauch als auch für Feuer. Die Daten erhält der Shader aus den Eigenschaften des Objekts, auf das er angewendet wird. Mit dem „Hair Shader" hält ganz viel Realismus Einzug in das Programm. Für die eher kreativeren Naturen bietet es sich an, die Farbe einfach direkt an der Figur zu setzen. Wer es noch realistischer will, kann sich über die Konzentration von Melanin in den Haaren eher eines naturwissenschaftlichen Ansatzes bedienen.



Hotkeys für Blender-Vertraute: In den Einstellungen, die in ein neues Menü gewandert sind, kehren Sie optional wieder zu den alten Tastenbelegungen zurück.

Neuerungen unter der Haube

Viele der geänderten Details liegen versteckt hinter der Programmoberfläche. Das neu geschriebene Coresystem soll die Arbeit beschleunigen und wurde für Mehrkern-Prozessoren optimiert. Es heißt aber auch Abschied nehmen: So verzichtet die aktuelle Version auf eine eigene Gamingengine. Als Ausblick liefern die Entwickler die bessere Anbindung an externe Engines wie das populäre Unreal. Weichen musste auch der „Blender Internal Renderer".

Insgesamt drei Renderingengines stehen jetzt zur Auswahl:

- Die Workbenchengine kommt während der Arbeit mit den Objekten zum Einsatz. Sie sorgt dafür, einen möglichst realistischen Eindruck zu gewinnen.
- Neu ist Eevee, die anstelle des bisherigen Internal Renderers tritt. Sie nutzt Open GL ab Version 3.3 und dürfte für die meisten Anwender auch bereits ausreichen, denn sie unterstützt Reflexionen, weiche Schatten und Darstellungen wie Feuer und Rauch. Durch die höhere Versionsnummer werden auch die Hardwareanforderungen etwas höher. Dennoch braucht es nicht unbedingt einen High-End-Boliden, um mit Blender flüssig zu arbeiten.
- Den Renderer Cycles setzen Anwender ein, die höchste Qualität erwarten und viel Zeit für das Rendering mitbringen können. Mit dieser High-End-Lösung kann dann auch in Spielfilmqualität produziert werden.

Das Update lohnt sich

Ein kleiner Sprung in der Versionsnummer, aber ein riesiger Schritt bei den Funktionen – so lässt sich die Blender-Version 2.8 am treffendsten zusammenfassen.

Die vielen neuen Möglichkeiten, Leistungsverbesserungen und die neue Renderingengine lohnen das Update. Da die Betaversion bereits sehr früh im Entwicklungszyklus als instabiles Release veröffentlicht wurde, konnten auch bereits viele Bugs behoben werden.

Blender 2.8 arbeitet stabil und macht Spaß. Geblieben ist dagegen die für Einsteiger nach wie vor hohe Lernkurve. Aber im Web stehen unzählige Videotutorials zur Verfügung, die nicht nur die neuen Funktionen erklären, sondern grundlegend in die Arbeit mit der Software einführen.

Tipp: Anwender, die Blender mit Add-ons ergänzt haben, sollten sich vor dem Update informieren, ob die Erweiterungen auch mit Version 2.8 zusammenarbeiten. Die Python-Schnittstelle hat sich geändert, was eine Portierung der Erweiterungen auf die neue Schnittstelle erforderlich macht. Gibt es für eine Erweiterung niemanden mehr, der sich für die Entwicklung verantwortlich fühlt, bedeutet das schlicht das Aus für die betreffende Erweiterung. ■

Pimp den Gimp

Aus Gimp wird kein zwar Adobe Photoshop, aber die Grafikbearbeitung ist neben Krita das mächtigste Open-Source-Programm für Illustrationen und Retusche. Mit cleveren und auch ganz erstaunlichen Erweiterungen lernt Gimp sogar noch dazu.

VON DAVID WOLSKI

Wenige professionelle Grafiker werden Gimp als vollwertigen Ersatz für Photoshop ansehen, denn dazu entwickelt sich Gimp zu langsam und ist in der Bedienung zu eigenwillig. Es gibt aber keinen Grund, auf Gimp herabzublicken. Die Grafikbearbeitung kann auch im professionellen Umfeld bestehen und macht Retusche und Bildmanipulation einfach. Dazu gibt es Erweiterungen, die Gimp benutzerfreundlicher machen und Filter und Algorithmen zur automatisierten Bildmanipulation hinzufügen, die selbst Profis verblüffen. Wir stellen die besten vier Erweiterungen vor – von nützlich bis abgefahren.

Dateien: Speichern statt exportieren

Gimp bevorzugt stets das eigene Dateiformat „XCF“ und bietet im gewohnten „Speichern“-Dialog kein anderes Format an. Wer als JPG oder PNG sichern will, muss die Datei mittels „Datei → Exportieren“ auf den Datenträger schreiben. In einem flotten Workflow sind die dafür nötigen Extra-Mausklicks durchaus lästig und der Umweg ist nicht intuitiv. Das muss aber nicht so bleiben: Das Plug-in Saver ergänzt eine unkomplizierte Funktion zum Speichern in beliebigen Dateiformaten. Zur Installation muss das Script von *https://github.com/akkana/gimp-plugins/blob/master/saver.py* heruntergeladen werden. Dazu klicken Sie auf der angegebenen Webseite auf den Link „Raw“ über dem angezeigten Quelltext und speichern die Datei als „saver.py“. Damit das Plug-in funktioniert, muss der Download ausführbar sein, was der Befehl

```
chmod 755 save-export-clean.py
```

auf der Kommandozeile erledigt. Jetzt muss die Datei noch per Dateimanager in das (versteckte) Plug-in-Verzeichnis von Gimp verschoben werden, das sich bei Gimp 2.10 im Home-Verzeichnis unter „.config/GIMP/2.10/plug-ins“ befindet. Nach einem Neustart von Gimp zeigen sich jetzt die neuen Einträge „Saver“ und „Saver as“ im Dateimenü, die jeweils eine Bilddatei ohne weitere Rückfragen mit der angegebenen Endung speichern. Gimp fragt dann auch beim Schließen des Programms nicht mehr nach, ob Sie geöffnete Dateien sichern möchten, was bei exportierten Dateien sonst immer der Fall ist.

Damit das Plug-in auf die gewohnte Tastenkombination Strg-S reagiert, ändert man in Gimp die zugewiesenen Tastenkürzel. Dazu geht man auf „Bearbeiten → Tastenkombination“ und gibt dort im Suchfeld „Saver“ ein, um das Plug-in anzuzeigen. Nach einem Klick auf den Eintrag in der Spalte „Tastenkombinationen“, der zunächst noch deaktiviert ist, definieren Sie dann die Tastenkombination Strg-S.

Das Add-on basiert auf Python und benötigt unter Debian, Ubuntu, Mint noch ein weiteres Paket, das in der Kommandozeile mittels

```
sudo apt-get install gimp-python
```

schnell nachinstalliert ist.

GMIC: Umfangreiche Filtersammlung

Die Filter- und Effektsammlung GMIC („Greyc's Magic Image Converter“) liefert über 400 Algorithmen zur Nachbearbeitung von Bildern. GMIC ist zwar auch als alleinstehende Anwendung konzipiert, aber erst die Integration der Filter in Gimp macht die Arbeit damit komfortabel. Der Entwickler der Filtersammlung GMIC hat deshalb auch an eine Schnittstelle zu Gimp gedacht, damit sich die Filter nahtlos und mit Vorschaufunktion in die Bildbearbeitung integrieren. Diese Schnittstelle ist in einer separaten Binary untergebracht, die in das Plug-in-Verzeichnis von Gimp installiert wird. Debian, Ubuntu und Mint liefern die Gimp-Ausgabe der Filtersammlung als fertiges Paket, das der Befehl

```
sudo apt install gimp-gmic
```

einrichtet. Nach einem Neustart der Bildverarbeitung Gimp zeigt sich im Menü „Filter“ ganz unten der Punkt „GMIC“ zum Abruf aller einzelnen Filteraktionen.

Resynthesizer: Bildelemente verschwinden

Es ist kein Problem, Objekte zu bestehenden Bildern so hinzuzufügen, dass alles weiterhin realistisch aussieht. Aber der umgekehrte Weg, ein Objekt zu entfernen, erweist sich als mühsam. Die Lösung heißt Textursynthese. Bei dieser Technik wird der umliegende Bildhintergrund eines markierten Bildbereichs analysiert und eine passende realistische Textur aus diesen Informationen erzeugt.

Das Gimp-Plug-in Resynthesizer bringt manuell markierte Objekte eines Bildes zum Verschwinden, indem es den Hintergrund anhand der umgebenden Bildbereiche nachbildet. Das Plug-in spart langwieriges Klonen einzelner Bildausschnitte und liefert passable Ergebnisse, die nach etwas Nachbearbeitung natürlich aussehen. Das Plug-in ist so populär, dass es in die offizielle Erweiterungssammlung von Gimp 2.10 aufgenommenen wurde, die in Debian, Ubuntu und Mint über das Paket „gimp-plugin-registry“ installiert wird:

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

Bei der Benutzung wählen Sie den gewünschten Bereich mit der Freihand-Auswahl aus (F-Taste). Die Auswahl muss nicht pixelgenau und sollte tendenziell größer sein. Um eine bestehende Auswahl zu erweitern, kann Gimp bei gedrückter Shift-Taste weitere Bereiche zur bestehenden Auswahl hinzufügen. Die automatische Synthese führt dann der Menüpunkt „Filter → Verbessern → Heal selection“ aus. Für noch bessere Ergebnisse sind manuelle Filtereinstellungen nötig, die über „Abbilden → Resynthesize“ möglich sind.

Weniger ist mehr: Intelligent verkleinern

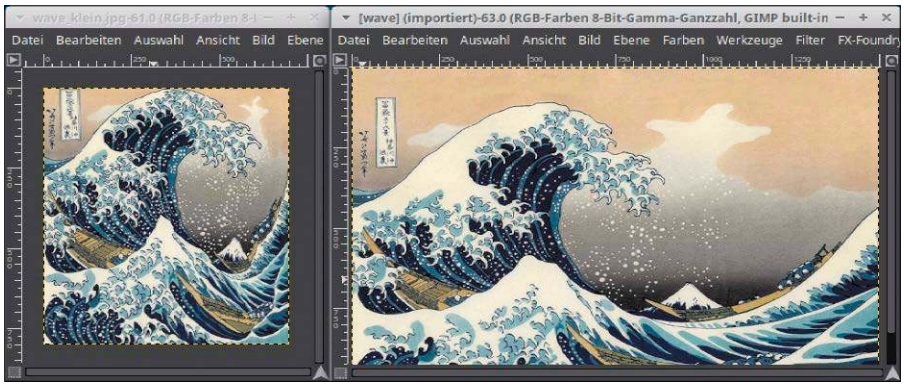
Es ist immer eine verlustreiche Angelegenheit, ein Bild zu verkleinern: Einen Weg der Verkleinerung ohne deutlichen Informationsverlust geht der Algorithmus Liquid Rescaling. Dies ist eine Mischung aus Skalieren und Zuschneiden, wobei der Algorithmus ein Motiv zuvor analysiert, um optisch wichtige Elemente unverändert zu behalten. Diese Erweiterung ist ebenfalls in der Sammlung „gimp-plugin-registry“ enthalten. Um es zu verwenden, lädt man das gewünschte Bild und geht in der Menüleiste des Bilderrahmens auf „Ebenen → Liquid Rescale“.

Der Menüpunkt öffnet einen neuen Dialog zum Plug-in. Im automatischen Modus genügt es, in den Feldern „Width“ und „Height“ die neuen Dimensionen einzugeben. Je nach Motiv erkennt das Plug-in Nahtstellen zwischen betonten Bildteilen. Richtig gut arbeitet die Skalierung aber erst, wenn Bereiche mittels Ebenen manuell markiert wurden. Dazu gehen Sie im Dialog des Plug-ins auf „Elementmasken → Elemente erhalten → New“. Auf dieser neuen Ebene markieren Sie alle wichtigen Motive mit dem Pinselwerkzeug und klicken dann auf „OK“, um die Skalierung auf die angegebene Breite und Höhe zu starten.

Ebenso kann man auch manuell eine Maske erstellen, deren markierte Bereiche bei der Skalierung verschwinden sollen. Dazu dient die Funktion „Feature discard selection“, welche die Markierung von unwichtigen Bildbereichen vor der Anwendung des Filters erlaubt. ■

Speichern statt exportieren: Ein Plug-in rüstet diesen Menüpunkt nach, der geöffnete Bilddateien ohne Umweg in Formate wie JPG und PNG speichert.

Bildteile entfernen: Der Resynthesizer-Algorithmus für Gimp überzeichnet markierte Objekte eines Bildes anhand der Strukturen der angrenzenden Pixel und lässt sie so verschwinden.



Ein Bild zerfließt: „Liquid Rescale“ erlaubt die Skalierung eines Bildes, bei der ausgewählte Bereiche unangetastet bleiben und irrelevante Flächen zusammengeschoben werden.

Apps für Heim-Admins

Wichtige Werkzeuge für Administratoren sind der SSH-Zugriff, Überwachungstools für Server, Zutritt auf Samba-Freigaben oder SFTP (SSH) und Kontrolle der WLAN-Stärke. All das gibt es auch als Android- oder iOS-Apps für Tablets und Smartphones.

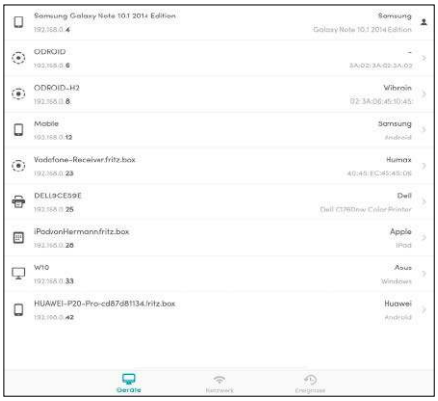
VON HERMANN APFELBÖCK

Termius: Mobiler SSH-Client

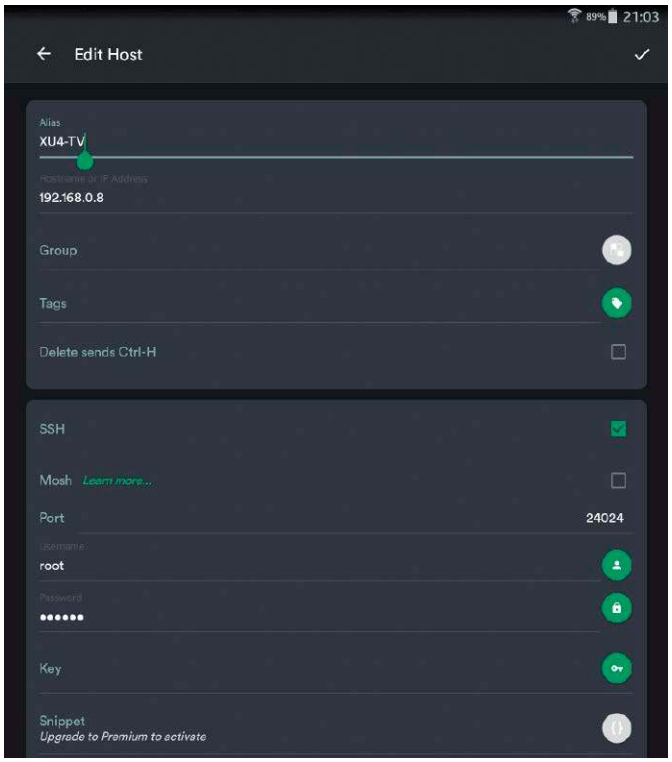
SSH-Terminals für Smartphones und Tablets gibt es etliche, die sich funktional nicht viel nehmen. Daher entscheiden letztlich Übersichtlichkeit, Bedienkomfort und Anpassungsfähigkeit – und hier ist Termius mit der beste Kandidat. Die englischsprachige App gibt es für Android und iOS. Unter „Host" legen Sie mit dem Plus-Zeichen einen Eintrag an („New host"). Im Prinzip genügt der Eintrag der IP-Adresse, falls der Server Standardport 22 für SSH nutzt. Man kann aber bei geringen Sicherheitsansprüchen im lokalen Netz auch gleich Konto und Kennwort direkt hinterlegen. Allgemeine Einstellungen zu Schriftgröße und Farben werden unter den „Settings" eingetragen, die dann für alle Hosts gelten. Um Einstellungen an einem bereits eingetragenen Server („Host") zu ändern, hilft längeres Drücken des Eintrags, was den Host markiert und in der kleinen Symbolleiste den Editierstift einblendet. Für eingetragene Hosts genügt ein Fingertipp, um die SSH-Verbindung zu starten.

Fing: Gute Netzwerkübersicht

Fing ist für Android wie iOS kostenlos, aber mit (relativ dezenten) Werbeeinblendungen verfügbar. Die App bietet auf der Seite „Geräte" einen guten Überblick über alle laufenden Netzwerkgeräte, der den Gang zum Netzwerkrouter erspart. Rechnername, IP-Adresse, MAC-Adresse, Domäne/Workgroup, UPnP-Dienste, Betriebssystem, Gerätehersteller gehören zu den Standardinfos. Über die Schaltfläche „Offene Ports finden" deckt Fing für das jeweilige Gerät die angebotenen Dienste auf – allerdings nur auf den Standardports zwischen 1 und 1000. An dafür konfigurierte Geräte (Netzwerkadapter, eventuell auch Bios) kann Fing mit „Aufwecken mit LAN" das „Magic Packet" schicken, um sie auf diesem Weg einzuschalten. Auf der Seite „Netzwerk" gibt es die Option „Internet-Geschwindigkeit". Ein zuverlässiger Providertest ist das allerdings nicht, sondern auf Smartphones und Tablets eher ein WLAN-Test.



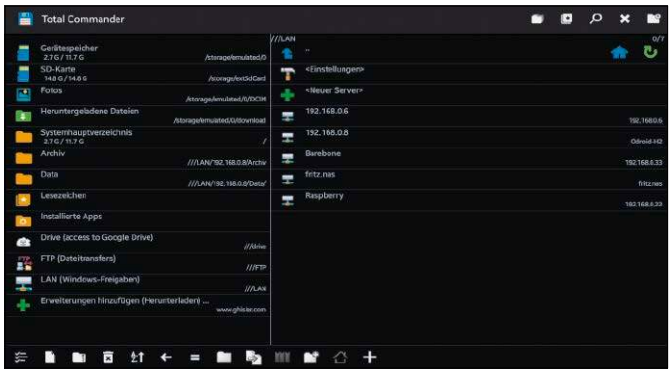
Fing liefert eine informative Gesamtschau des lokalen Netzwerks und bietet aktive Funktionen wie Portscanner, Wake-on-LAN und Tempomessung.



SSH-Client Termius für Android und iOS: Die englischsprachige App verwaltet beliebig viele Server übersichtlich und optisch ansprechend.

Total Commander: Android-Dateimanager

Für den Zugriff auf Netzfreigaben, FTP-Server und Cloudspeicher (Google, Dropbox, Onedrive) gibt es eine Android-App, die alles kann: den Total Commander. Funktionalität und Schnelligkeit entschädigen für konservative Bedienung. Der Total Commander benötigt Plug-ins für seine Netzwerkfähigkeiten, die Sie im Google Play Store über die Suche „total commander plugin" erreichen (FTP, Webdav, Google Drive, Onedrive, Dropbox). Unentbehrlich für Heim-Admins ist das „LAN (Windows network) Plugin" für



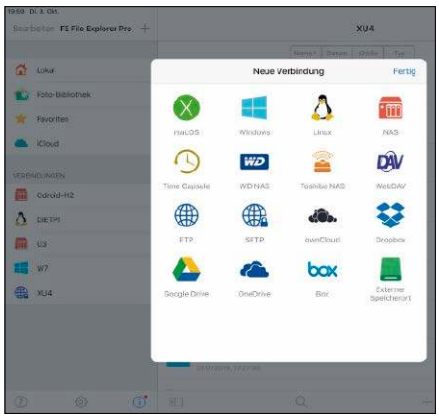
Total Commander mit Netz-Plug-ins: Funktional ist diese Android-App unschlagbar. Die Bedienung stammt allerdings von lange vor Smartphone-Zeiten aus den 90er-Jahren.

Windows- und Samba-Freigaben. Plug-ins erscheinen im Hauptverzeichnis des Total Commander. Egal, welches Plug-in Sie verwenden, funktioniert das Einrichten einer Ressource weitgehend analog. Mit „Neuer Server" oder „Neue Verbindung" richten Sie den Zugriff ein: Zunächst vergeben Sie einen Namen, darunter die Server- und Authentifizierungsdaten. Die Dateibearbeitung im Total Commander ist am übersichtlichsten, wenn Sie das Smartphone/Tablet horizontal nutzen. In vertikaler Lage sehen Sie von der klassischen Zwei-Spalten-Ansicht mit zwei Verzeichnissen stets nur eines und müssen mit den Pfeiltasten am Rand hin und her wechseln.

Alternative: Wer mit dem Bedienkonzept des Total Commander nicht klarkommt, kann auf die Android-App Network Places ausweichen. Die kostenlose Version ist jedoch auf einen einzigen Samba-Server limitiert. Ohne diese Einschränkung kostet die App 4,79 Euro.

FE File Explorer: Dateimanager für iPads und iPhones

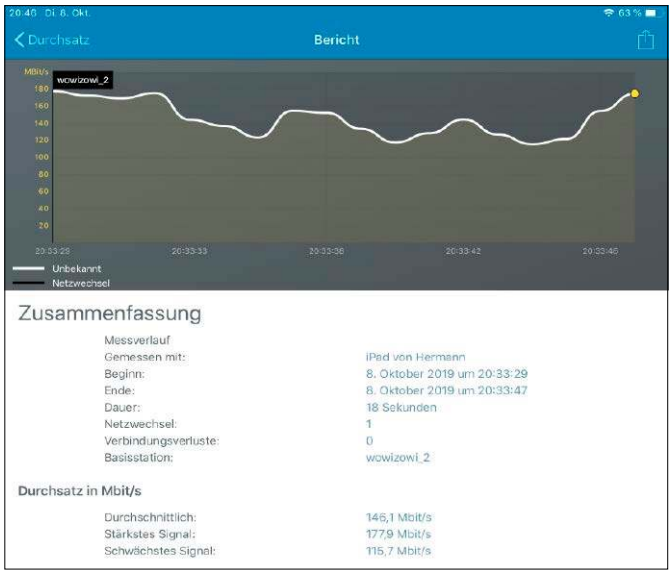
Für iOS-Geräte ist der FE File Explorer eine klare Empfehlung: Funktionsreich, schnell und attraktiv taugt dieser Dateimanager für Netzwerkressourcen aller Art. Neben Samba- und Windows-Freigaben hat er FTP, SFTP (SSH), Webdav und diverse Clouddienste im Portfolio. Die kostenlose Version ist allerdings arg beschränkt, sodass sich der Kauf der unlimitierten Versionen empfiehlt (5,49 Euro). Mit der „+"-Schaltfläche links oben über der Navigationsspalte ist eine neue Verbindung schnell eingerichtet.



Dateimanager für Samba, SFTP, FTP und Cloud: Auf Apple-Geräten ist der FE File Explorer erste Wahl.

Fritzapp WLAN oder Wifi Analyzer

Bei der Suche nach dem besten Standort und bei der Optimierung des eigenen WLANs sind Tablets oder Smartphones handlicher als Notebooks. Wer als Heimrouter eine Fritzbox besitzt, nimmt dafür am besten die Fritzapp WLAN, die es identisch für Android und iOS gibt. Neben Infos zum Router und zur lokalen und öffentlichen IP-Adresse liefert „WLAN messen" den Durchsatz am aktuellen Standort. Fritzbox-unabhängige Apps für diese Aufgabe gibt es natürlich auch: Unter Android bietet sich etwa der Wifi Analyzer an.



Fritzapp WLAN zeigt die Signalstärke am aktuellen Standort. Außerdem hilft die App beim Einrichten eines Repeaters und des WLAN-Gastzugangs.

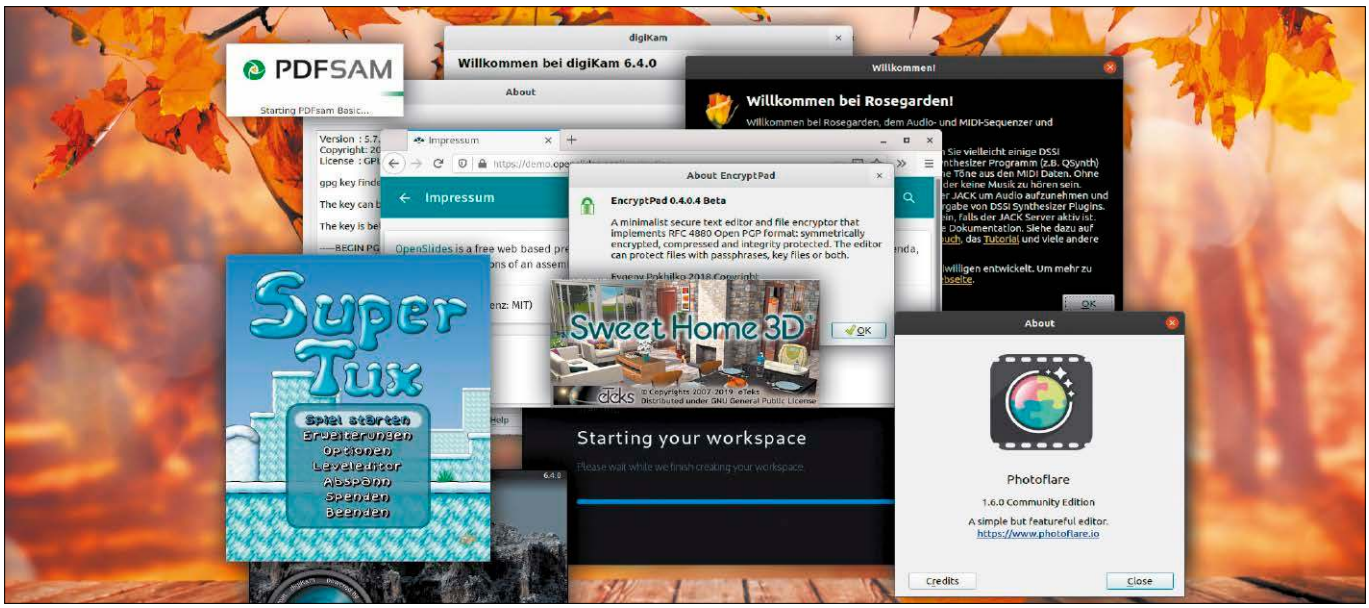
Anag/Easy Nag als Nagios-Monitor

Nagios ist an sich ein Profiwerkzeug zur Überwachung von Servern oder von ganzen Netzwerken. Mancher Heim-Admin vertraut aber auch bei der Kontrolle seiner Raspberry-Platinen auf Nagios. Dessen Serverkomponenten benötigen nur Apache und PHP und die Ausgabe der Statistiken erfolgt einfach über HTTP. Um diese Ausgabe am Mobilgerät abzufragen, gibt es die Android-App Anag und für iOS Easy Nag – beide kostenlos. Die englischsprachigen Apps können auch aktiv Warnmeldungen ausgeben, wenn Nagios kritische Serverereignisse an die App meldet. ■

Servermonitor für Android: Anag verbindet sich mit der Nagios-Installation auf einem Server, um die Leistungsdaten abzufragen.

Softwareperlen

Diesmal haben wir eine Menge kleinerer, aber sehr nützliche Utilitys im Blick, die das Leben auf dem Linux-Desktop und im IT-Umfeld leichter machen. Auch Digikam, ein Vorzeigeprojekt aus dem KDE-Umfeld, ist in einer neuen Version erschienen.



VON DAVID WOLSKI

Es gibt kaum IT-Unternehmen und Anwender, die keine Open-Source-Software einsetzen. Vor gut zwanzig Jahren war freie Software etwas Exotisches und meist auch nur an Unis und in Serverräumen für hoch spezialisierte Aufgaben anzutreffen – heute ist der Einsatz von Open-Source-Software eher die Regel als die Ausnahme. Zudem funktionieren große Teile von Netzwerkinfrastrukturen und maßgebliche Teile des Internets nur mit freier Software sowie mit Betriebssystemen wie Linux und BSD. Die Protagonisten einer freien Softwarekultur haben offensichtlich auf ganzer Linie gewonnen und die Industrie zog eifrig mit.

Müsste dann nicht auch das Geschäft für Entwickler brummen? Leider nicht. Zwar sind Softwareentwickler gefragt und kommen an gut bezahlte Jobs. Das nutzt den wichtigen, für das Internet sogar lebenswichtigen, dabei chronisch unterfinanzierten Open-Source-Projekten jedoch erst mal wenig. Im rauen IT-Alltag ist alles auf Effizienz und Profit getrimmt. Aber viele Programme, die an neuralgischen Stellen für den reibungslosen Betrieb des Internets sorgen, wären ohne den Idealismus ihrer Entwickler längst verwaist und schlimmstenfalls unsicher.

Hinzu kommt, dass Programmiergenies oft die ganz andersgeartete Kompetenz fehlt, auf sich aufmerksam zu machen. Tatsächlich sind Millionen von Internetnutzern und nicht wenige Internetgiganten davon abhängig, dass unbekannte Open-Source-Programmierer unentgeltlich arbeiten. Das ist eine gefährliche Schieflage, die für ganze Unternehmen bedrohlich wird. Denn unbezahlte Programmierer hören eventuell irgendwann plötzlich auf oder gehen in Rente. Oder es schleichen sich über Jahre böse Bugs in ein verbreitetes Softwarepaket ein, wie zuletzt in Open SSL im Falle des Heartbleed-Bugs, weil die Mittel für teure Audits nicht vorhanden waren.

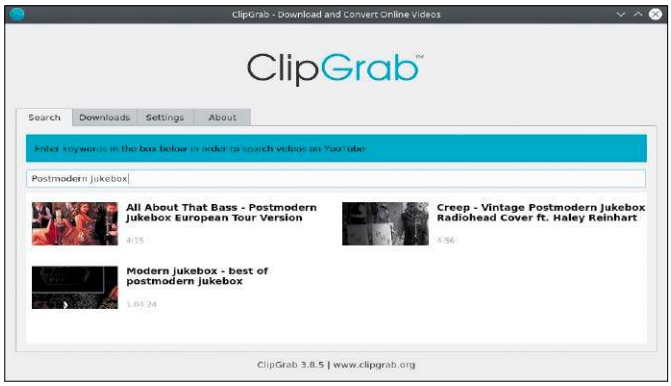
Es gilt, diesen Missstand zu beheben, bevor Entwickler wichtiger Programme die Lust verlieren oder in Rente gehen. Zu einer wichtigen Einnahmequelle sind Spenden geworden. Diese erhalten essenzielle Projekte wie Gnu PG und Open SSL am Leben und deren Entwickler im Geschäft. Diese beiden Projekte haben die Unterstützung einiger IT-Riesen wie Google und Facebook gewonnen.

Andere Entwickler wenden sich mit einer „Spenden"-Schaltfläche direkt an die Anwender. Ausgerechnet der vielversprechenden VPN-Technologie „Wireguard" wurde nun eine Spendenkampagne kurzzeitig zum Verhängnis: Google entfernte die Wireguard-App für Android von Google Play, weil ein „Spenden"-Button in der Open-Source-App gegen die Google-Richtlinien verstößt. Dieser Ausschluss zeigt exemplarisch, dass es noch dauern wird, bis sich das große IT-Geschäftsmodell und Open-Source-Projekte auf einen gemeinsamen Nenner geeinigt haben.

Clipgrab 3.8.5

Speichert Youtube-Videoclips
http://clipgrab.de

Die einst zahlreichen Webdienste zum Konvertieren und Speichern von Youtube-Videos werden rar. Es gibt aber noch eine andere zuverlässige Möglichkeit, Clips von Videos lokal zu speichern: Clipgrab gibt sich als Browser aus, um Videos herunterzuladen, und erwartet lediglich die URL zu einem Clip auf Youtube, Vimeo, Metacafe, Dailymotion. Verschiedene Abspielqualitäten sind möglich. Die Projektseite bietet den Quellcode und ein universelles Binärprogramm.

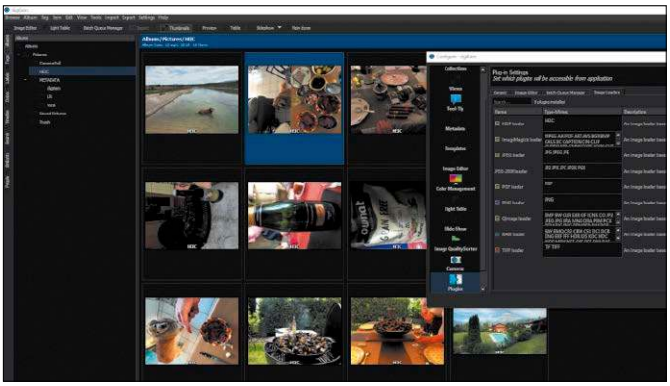


Clipgrab speichert und konvertiert Videoclips aus dem Web: Die aktuelle Version 3.8.5 versteht sich auf zahlreiche Video-Websites.

Digikam 6.4

Bringt Ordnung in das Fotoarchiv
www.digikam.org

Die Bildverwaltung Digikam entstammt dem KDE-Umkreis und ist auch für Windows und Mac-OS verfügbar. Die Open-Source-Perle hat mit ihrem Funktionsumfang wenig kommerzielle Mitstreiter. Fotos werden nach Datum, Tag, Gesichtserkennung oder Merkmalsuche organisiert. Es gibt einen neuen Bildeditor mit RAW-Import und ein Plug-in, das von der Kipi-API des KDE-Projekts stammt. Hinweise zur Installation fertiger Pakete liefert die Webseite.

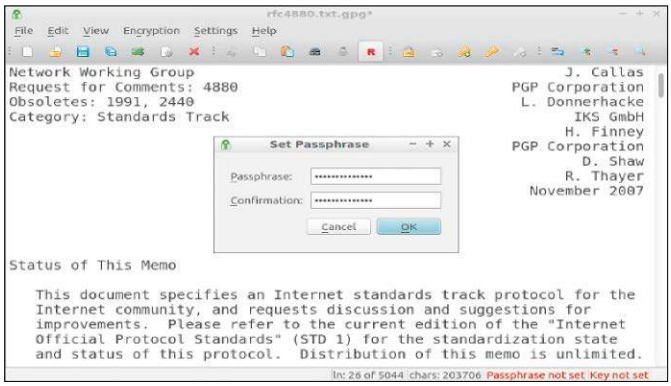


Organisationstalent: Digikam ist ein Vorzeigeprojekt unter den KDE-Anwendungen. Version 6.4 ergänzt den Bildeditor um einen RAW-Import.

Encryptpad 0.4.0

Verschlüsselter Notizblock für alle Systeme
https://evpo.net/encryptpad

Notizen sind nichtig, manche wichtig oder gar so wichtig und sensibel, dass sie besonderen Schutz erfordern. Die Arbeit mit dieser Art von Notizen macht Encryptpad einfacher. Es speichert in einem Dateiformat, das mit GPG symmetrisch per Password und Schlüssel chiffriert ist und dann auch in der Cloud gespeichert werden kann. Encryptpad ist Open Source und plattformübergreifend (Linux, Windows, Mac-OS). Die Website liefert Quellen für Linux-Pakete.

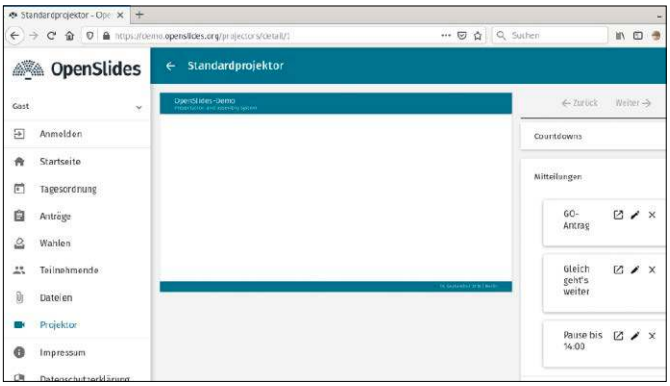


Für Geheimniskrämer und Datenschutzbewusste: Encryptpad speichert Notizen mit Open GPG in einer verschlüsselten Datei.

Openslides 3.0

Webbasierte Präsentationssoftware
https://demo.openslides.org

Openslides ist ein webbasierter Werkzeugkasten zum Erstellen öffentlicher Präsentation und zur Organisation dazugehöriger Meetings. Web – ist das zu unsicher? Openslides als freies Python-Programm (MIT-Lizenz) ist auch gut auf dem eigenen Server aufgehoben. Es gibt neben dem Zugriff per Browser auch einen Webclient mit responsivem Design für Smartphones. Version 3.0 bietet Anwesenheitslisten, Anfragen und neue Funktionen für Vereine.

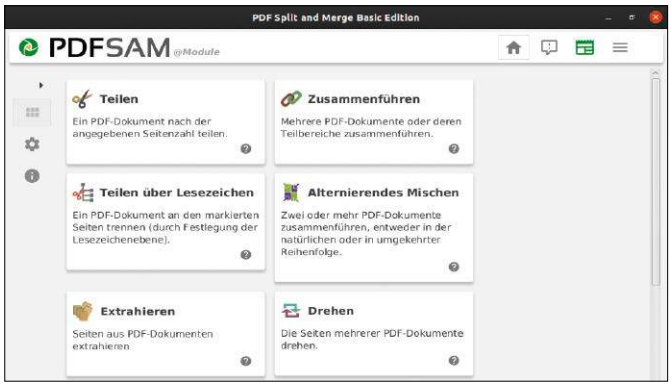


Präsentationen im Web: Openslides ist ein CMS für Präsentationen und Veranstaltungen. Es basiert auf Python und kann selbst gehostet werden.

PDF Sam Basic 4.0

Java-Programm zur PDF-Bearbeitung
https://pdfsam.com

PDF Split and Merge ist in Java geschrieben und bietet eine umfangreiche Oberfläche zum Zusammenfügen und Zerlegen von PDF-Dokumenten. PDF Sam kann Seiten drehen, umsortieren, einzeln abspeichern und einfügen. Der visuelle Editor zeigt eine Vorschau des neuen Dokuments. Bestehende PDFs zerlegt das Open-Source-Programm in Einzelseiten oder Kapitel. Version 4.0 hat seine Java-Runtime im Gepäck, läuft aber nur noch auf 64-Bit-Systemen. ■

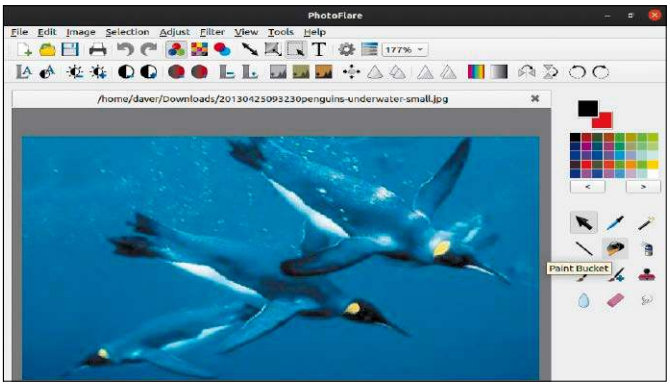


PDF-Bearbeitung: PDF Split and Merge bietet einen grafischen Editor, der Dokumente und Einzelseiten zu neuen PDFs zusammenfügt.

Photoflare 1.5.9

Grafikbearbeitung mit Batchfunktion
https://photoflare.io

Nicht für jeden lohnt sich der Einstieg in Gimp & Co. Photoflare ist für Gelegenheitsanwender gemacht und vom Windows-Programm Photofiltre inspiriert. Die Software hat Farbregler, Filter und typische Werkzeuge. Eine ganze Reihe von Bildern kann Photoflare im Batchmodus automatisiert bearbeiten, um Größe, Orientierung, Farben, Kontrast, Helligkeit anzupassen oder Filter anzuwenden. Fertige DEB-Pakete und ein Appimage liefert die Projektseite. ■

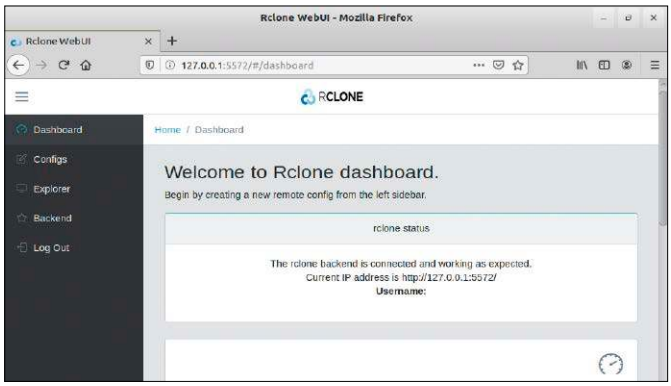


Bilder schnell in Form bringen: Photoflare ist für einfache Aufgaben ideal, kann Bilder aber im Batchmodus auch in Serie bearbeiten.

Rclone GUI 1.6

Kopiert Dateien zwischen Clouddiensten
https://mmozeiko.github.io/RcloneBrowser

Umzugsservice für die Cloud: Rclone Browser hilft beim Datenumzug von einem Cloudspeicher auf einen anderen und bei der Synchronisation zwischen Cloud und PC. Bemerkenswert ist die Zahl an Clouddiensten, die das Tool unterstützt. Insgesamt kann die aktuelle Version auf 45 Cloudanbieter zugreifen, darunter Google Drive, Dropbox, Microsoft Onedrive und Amazon 3. Die Projektwebseite bietet Pakete für Ubuntu und Arch Linux. ■

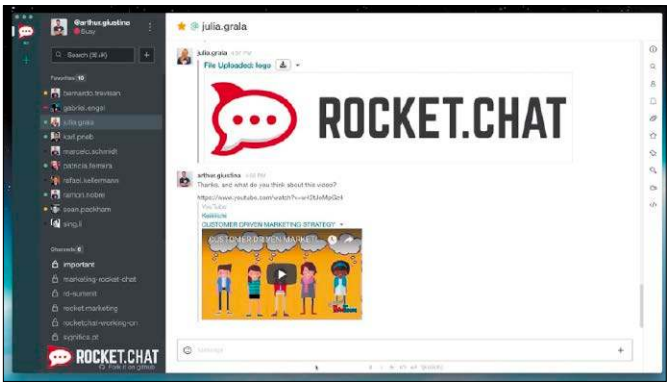


Clouddateien abgleichen: Einige Clouddienste können per Rclone die Dateien direkt austauschen, ohne Umweg über den lokalen PC.

Rocket Chat 2.1

Freier Chatserver im Stil von Slack
https://rocket.chat

Chatserver mit Apps für Smartphones sind für viele Teams eine perfekte Ergänzung. Allerdings erfordern Datenschutzauflagen oft das Hosting auf dem eigenen Server. Für diesen Zweck ist Rocket Chat ideal, das dem bekannten Slack nachempfunden und mit relativ wenig Aufwand auf dem Server eingerichtet ist. Rocket Chat ist Open Source, kostenlos und funktioniert mit Apps unter Android und iOS. Die Software ist in Node.JS programmiert. ■



Messenger- und Chatservice für den eigenen Server: Rocket Chat macht enorme Fortschritte und ist ideal für große Teams.

Rosegarden 19.06

Midi-Sequenzer und Notationsprogramm
www.rosegardenmusic.com

Der Sequenzer für kleine Studios mischt und bearbeitet Midi- und Audiodaten. Rosegarden kann Midi-Daten als Notensatz darstellen, verändern und ausdrucken. Ist kein Keyboard oder Synthesizer per Midi angebunden, so gibt es einen Softwaresynthesizer zur Klangerzeugung. Zum Abmischen unterstützt das Open-Source-Programm Filter und Effekte über die LADSPA-Schnittstelle. Die neue Version ist in den Paketquellen von Ubuntu 19.10 enthalten. ■

Sequenzer und Audiorecorder: Die Oberfläche von Rosegarden schreckt niemanden ab und die Fähigkeiten reichen für ernsthafte Tonproduktion.

Supertux 0.6

Jump & Run mit dem Pinguin
http://supertuxproject.org

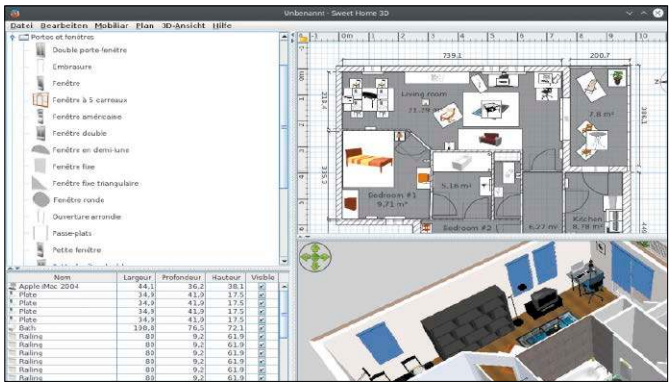
Das kurzweilige Spiel orientiert sich schamlos am Spielprinzip von Super Mario. Spielfigur ist das Linux-Maskottchen Tux, das mit Tasten oder Joystick durch Level gesteuert wird, wo diverse Monster und Gegner warten. Die neue Version optimiert die Grafikausgabe mit Open GL, damit diese auch auf älteren Ein-Platinen-Computern flott funktioniert. Zudem wurden einige Level und Grafiken neu gemacht. Supertux 0.6 liegt als auch universelles Appimage vor. ■

Springen, Rennen, Sammeln: SuperTux meldet sich mit einer neuen Version zurück, die für den Raspberry Pi optimiert ist.

Sweet Home 3D 6.2

Java-Programm zur Innenraumplanung
www.sweethome3d.com

CAD-Programme für Gelegenheitsnutzer sind rar. Umso erfreulicher ist die Entwicklung von Sweet Home 3D, das mit vertretbarem Aufwand Innenräume mit einer CAD-Oberfläche plant und mit Möbeln ausstattet. Die Planung beginnt mit dem 2D-Plan, wobei das deutschsprachige Java-Programm mit mehreren Dialogen assistiert. Ein Renderer gibt Ansichten als 3D-Szene aus. Sweet Home 3D läuft auf allen Distributionen mit Java-Runtime, wobei Open JDK ausreicht. ■

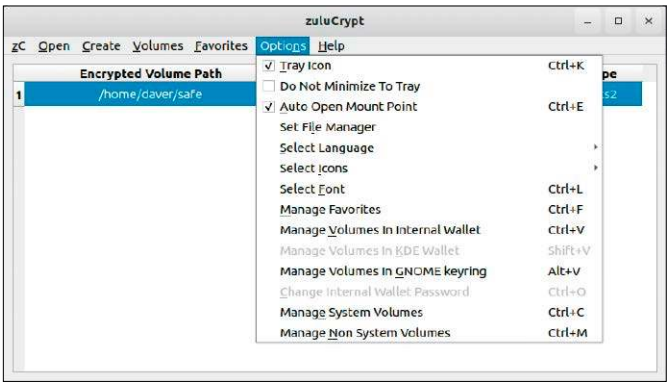


Sweet Home 3D erlaubt einfaches Planen von Räumen. Es nutzt sein eigenes Dateiformat, kann aber auch Fremdobjekte importieren.

Zulucrypt 5.7

Erstellt verschlüsselte Container
http://mhogomchungu.github.io/zuluCrypt

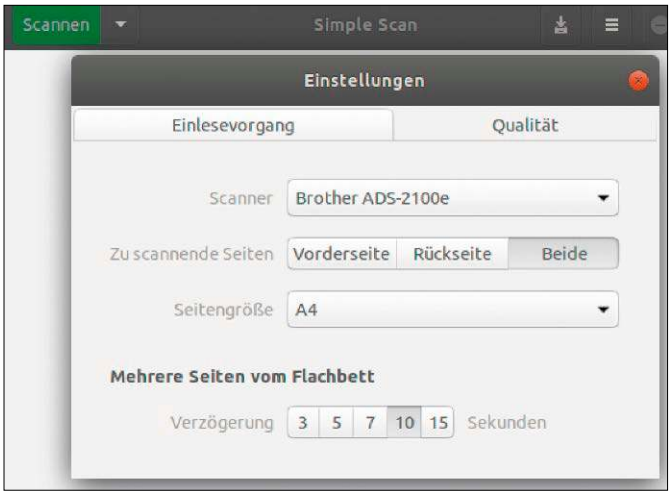
Verschlüsselte Container zur Verwahrung sensibler Daten gibt es in etlichen Formaten. Zulucrypt ist ein Front-End, das die Arbeit mit diesen Containern vereinfacht. Es kann die unter Linux gebräuchlichen Luks-verschlüsselten Datenträger öffnen, aber auch mit Veracrypt/Truecrypt umgehen. In Version 5.6 ist jetzt Bitlocker von Windows hinzugekommen. Zur Installation bietet die Projektseite Pakete für Ubuntu/Mint, Debian, Fedora und Open Suse. ■



Zulucrypt öffnet verschlüsselte Container und Partitionen: Das Programm beherrscht Veracrypt, Truecrypt, Luks-Partitionen und Bitlocker.

Netzwerkscanner dank Raspberry Pi

Die Netzwerkfähigkeit von Scannern lassen sich viele Hersteller mit einem Aufpreis bezahlen. Der Raspberry Pi macht auch USB-Scanner ohne Ethernet und WLAN zum zentral erreichbaren Netzwerkgerät.



Scanprogrammen wie Simple Scan ist es egal, ob das Scannergerät direkt am Rechner angeschlossen ist oder über das Netzwerk angesprochen wird.

VON STEPHAN LAMPRECHT

Für jeden Anspruch und jedes Budget gibt es im Handel Foto- und Dokumentenscanner. Vom einfachen Flachbettmodell bis zur High-End-Maschine, die beidseitig Papierstapel digitalisiert, werden die meisten Geräte via USB an einen Computer angeschlossen und sind damit an den jeweiligen Computer gebunden. Wenn Sie den Scanner auch mit anderen Geräten nutzen wollen, lässt sich das mit einem Raspberry komfortabel umsetzen.

Vorbereitende Arbeiten

Der Raspberry Pi sollte bereits mit Ihrem Heimnetz verbunden sein, ob per WLAN oder kabelgebunden, das spielt keine Rolle. Falls Sie einen besonders kompakten Scanner nutzen, der per USB auch mit Strom versorgt wird, ist es empfehlenswert, sich ein externes Netzteil für das Gerät anzuschaffen. Beim direkten Anschluss an den Raspberry könnte es bei voller Last zu einem Engpass kommen. Alternativ könnten Sie sich auch einen aktiven USB-Hub mit externem Netzteil anschaffen. Damit hätten Sie dann auch eine Ladestation für andere Geräte.
Während das Zusammenstecken der Hardware schnell erledigt ist, kann die Einrichtung der Software etwas aufwendiger werden. Damit die Konstruktion auch funktioniert, muss Ihr Scanner vom SANE-Projekt unterstützt werden. Dazu rufen Sie die offizielle Projektseite (*www.sane-project.org*) auf und suchen in der umfangreichen Modell- und Herstellerliste.
Sollte Ihr Gerät dort nicht auftauchen, bedeutet das noch nicht zwangsläufig das Ende für das Projekt. Jetzt kommt es nämlich darauf an, ob der Geräteproduzent möglicherweise eigenen Treiber für Linux entwickelt hat. Das ist beispielsweise bei vielen Modellen des Herstellers Brother der Fall. Zur Vorbereitung müssten Sie also zunächst diesen Treiber installieren. In der Regel handelt es sich dabei um klassische Pakete, die direkt über den Paketmanager installiert werden können.

Den Scanner einrichten

Schließen Sie den Scanner an den Raspberry per USB an und schalten Sie ihn ein. Anschließend bringen Sie die Pakete des Raspberry mit

```
sudo apt-get update
```

auf den aktuellen Stand. Anschließend installieren Sie das SANE-System. Dazu genügt folgender Terminalbefehl:

```
sudo apt-get install sane-utils
```

Das Scansystem benötigt keine eigene Oberfläche. Wenn Sie über den Desktop des Raspberry direkt scannen wollen, könnten Sie beispielsweise den grafischen Aufsatz XSANE installieren (Paketname „xsane“). Als root überprüfen Sie mittels lsusb, ob der Scanner an der USB-Schnittstelle korrekt erkannt wurde. Taucht das Gerät dort auf, geht es zur nächsten Frage:

```
sudo scanimage -L
```

Dieser Befehl zeigt, ob SANE den Scanner erkennt. Sollte auch nach der Installation eventuell angebotener proprietärer Treiber hier keine Ausgabe erfolgen, wird der Scanner mit großer Wahrscheinlichkeit nicht unterstützt. In diesem Fall bleibt Ihnen nur eine intensivere Webrecherche in den Foren des Herstellers, ob es trotzdem einen Weg gibt.

Netzwerkzugriff ermöglichen

Mit einem unterstützten Scanner haben Sie zunächst eine lokale Scannerlösung für den Raspberry Pi. Um nun den Zugriff auch von externen Geräten zu erlauben, sind weitere Konfigurationsarbeiten notwendig. Dazu gehört die Einrichtung des passenden Daemons auf dem kleinen Rechner sowie

eine Definition der IP-Adressen, von denen SANE Anfragen akzeptiert. Öffnen Sie auf dem Raspberry mit root-Recht mit einem Editor wie Nano die Datei „/etc/sane.d/saned.conf“. Hier suchen Sie den Abschnitt „Access list“ und fügen entweder einzelne IP-Adressen oder gleich einen ganzen Bereich ein. Welche IP-Adressen bei Ihnen zutreffen, erfahren Sie mit „ip address“ auf jedem Rechner oder in der Konfigurationsoberfläche des Routers. Mit einem Eintrag wie „192.168.178.6“ legen Sie beispielsweise fest, dass genau das Gerät mit dieser IP-Adresse zugreifen darf, während „192.168.178.0/24“ (sic!) die Anfragen aller Geräte des Adressraums 192.168.178.* erlaubt (1 bis 254).

Danach geht es noch an die Einrichtung des Daemons, der dafür zuständig ist, das System auf eingehende Scananfragen zu überwachen. Unter aktuellen Debian/Ubuntu-Versionen richten Sie mit

```
systemctl status saned.socket
```

den Socket zur Überwachung ein. Nach diesem Kommando sollte das System melden, dass es jetzt auf eingehende Anfragen wartet. Mittels

```
sudo systemctl start saned.socket
```

aktivieren Sie dann die Schnittstelle und ein letzter Befehl

```
sudo systemctl enable saned.socket
```

sorgt dafür, dass der Dienst stets automatisch beim Systemstart aufgerufen wird.

Die Clientrechner einrichten

Da SANE ein Linux-Dienst ist, fällt die Einrichtung von Linux-Rechnern besonders leicht. Voraussetzung wie bei allen Serverdiensten ist eine feste IP-Adresse für den Raspberry, die Sie diesem im Router zuweisen – in der Fritzbox unter „Heimnetz → Heimnetzübersicht“ mit der Option „Diesem Netzwerkgerät immer die gleiche IPv4-Adresse zuweisen“. Auf dem Clientgerät installieren Sie anschließend eine App wie Simplescan oder XSANE. Diese erwarten als Abhängigkeit das entsprechende SANE-System, das dabei gleich mitinstalliert wird. Ist die Installation erfolgreich, sollten Sie danach die Datei „/etc/sane.d/net.conf“ vorfinden. Im Abschnitt „saned hosts“ tragen Sie die feste IP-Adresse des Pi ein und speichern die Datei.

Geben Sie in einem Terminal danach

```
scanimage -L
```

ein, dann sollte der über das Netzwerk verfügbare Scanner in der Liste auftauchen.

```
sla@sla-X555LAB:~$ lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 004: ID 0bda:0129 Realtek Semiconductor Corp. RTS5129 Card Reader Control
ler
Bus 001 Device 003: ID 0bda:57b5 Realtek Semiconductor Corp.
Bus 001 Device 005: ID 04f9:037d Brother Industries, Ltd
Bus 001 Device 002: ID 046d:c043 Logitech, Inc. MX320/MX400 Laser Mouse
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
sla@sla-X555LAB:~$ sudo scanimage -L
[sudo] Passwort für sla:
device `brother4:bus1;dev2' is a Brother ADS-2100e USB scanner
sla@sla-X555LAB:~$
```

Das sieht gut aus. Das Gerät wird an der USB-Schnittstelle erkannt (lsusb) und SANE kennt das Modell des Scanners (scanimage).

Konfigurationsdatei „saned.conf“: Hier erlauben Sie den Zugriff einzelner IP-Adressen oder gleich des ganzen Adressraums Ihres Heimnetzes.

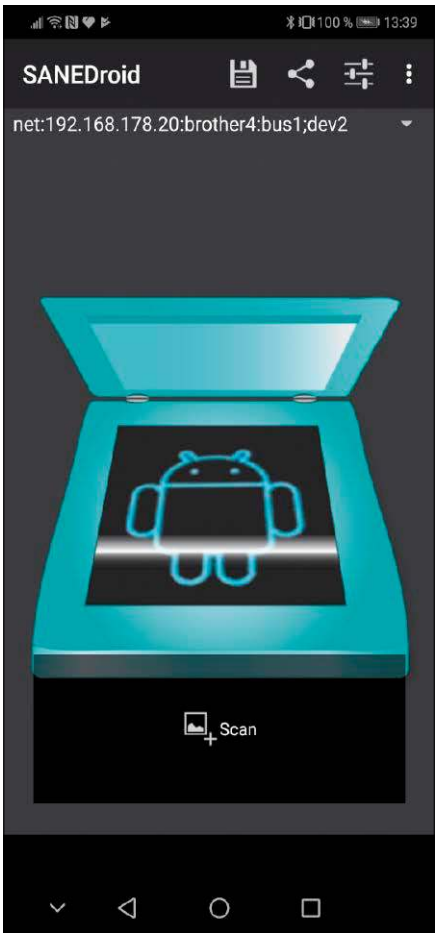
```
GNU nano 2.9.3                    /etc/sane.d/saned.conf

## Access list
#scan-client.somedomain.firm
#192.168.0.1
192.168.178.0/24
#[2001:db8:185e::42:12]
#[2001:db8:185e::42:12]/64

# NOTE: /etc/inetd.conf (or /etc/xinetd.conf) and
# /etc/services must also be properly configured to start
# the saned daemon as documented in saned(8), services(4)
# and inetd.conf(4) (or xinetd.conf(5)).
127.0.0.1
```

Dem Eintrag wird ein „net“ vorangestellt. Damit können Sie mit dem Scannen bereits beginnen, denn für die Scansoftware spielt es keine Rolle, ob der Scanner lokal oder per Netzwerk angeschlossen ist.

Um mit Windows auf den Scanner zugreifen zu können, benötigen Sie eine andere Software. Hier hilft ein wenig Experimentieren. Oft bewährt sich der Einsatz von Sane Twain (*https://sanetwain.ozuzo.net/*). Es verbindet SANE mit der unter Windows genutzten Twain-Schnittstelle, über die dort Scanner angesprochen werden. Sollte die von Ihnen genutzte Windows-Version darüber nicht auf den Scanner zugreifen können, gibt es mit SANE Win DS (*https://sourceforge.net/projects/sanewinds/*) eine Alternative. Beide Programme erwarten beim ersten Programmaufruf die Eingabe der IP-Adresse des Raspberry Pi.

Für Mac-Nutzer gibt es mit Twain SANE (*www.ellert.se/twain-sane*) eine ähnliche Anwendung, die den externen Scanner im Systemdialog von Mac-OS einbindet. Das neueste Mac-OS unterstützt dies allerdings nicht. Wenn Sie bereits auf Catalina gewechselt sind, können Sie das Programm nicht einsetzen.

Mit Smartphones auf Android-Basis können Sie Ihr SANE-System hingegen ansprechen. Möglich wird das mit der App SANEDroid (*https://play.google.com/store/apps/details?id=com.sane.droid*). ■

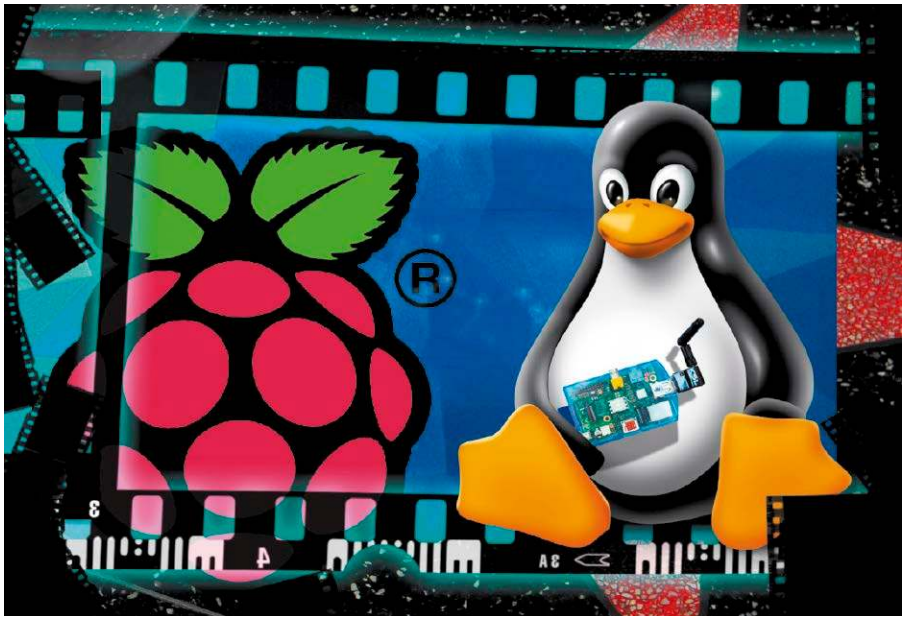


Sogar Android-Geräte können den Scanner benutzen. Dazu müssen Sie der Software nur die IP-Adresse des Raspberry Pi mitteilen.

Raspberry Pi statt Chromecast

Die diversen Chromecast-Modelle sind mit intuitiver Funktionsweise ein ansehnlicher Erfolg geworden. Ohne Google-Gerät gibt es auch die Möglichkeit, einen Streamingclient mit ähnlichen Funktionen mittels eines Raspberry Pi nachzubauen.

VON DAVID WOLSKI



© David Wolski

Mit der Vorstellung des ersten Chromecast-Modells vor sieben Jahren hat Google ganz offensichtlich einen Nerv getroffen. Die kleinen, erstaunlich leistungsfähigen Chromecast-Geräte mit HDMI-Anschluss binden sich perfekt in Google-Dienste und dank eines frühzeitig veröffentlichten SDK in Android-Apps ein. Mit dem Erfolg der Geräte sind Chromecast-Modelle auch auf dem Gebrauchtmarkt und auf Ebay erstaunlich preisstabil geblieben. Man braucht etwas Glück dazu, ein günstiges Chromecast zu erwerben oder zu ersteigern. Ein Google Chromecast der ersten Generation kommt immer noch auf 20 Euro, ein Gerät der zweiten Generation kostet oft mehr als 30 Euro.

Nachbau mit einfachen Mitteln

Was Open-Source-Freunde weniger von Google überzeugt (beziehungsweise „Google Home“, wie die Technologie auch heißt), ist die proprietäre Natur des Protokolls und des Chromecast-Betriebssystems. Das ist Motivation genug, einen Streamingclient mit ähnlichem Funktionsumfang nur mit Hilfe von Open-Source-Software und eines Raspberry Pi nachzubilden.

Der Beitrag zeigt die nötigen Zutaten, die Installation und die Fähigkeiten eines so aufgebauten Streamingclients. Als Voraussetzung kommt hier ein älterer Raspberry Pi 2 mit einem aktuellen Raspbian zum Einsatz. Es genügen dabei die Lite-Ausgabe von Raspbian und eine kleine SD-Karte mit nur vier GB. Anders als bei Google Chromecast braucht die Netzwerkverbindung nicht über WLAN hergestellt zu werden, denn der Raspberry Pi kann auch über den Ethernet-Port als Streamingclient angesprochen werden.

An Software benötigt der Raspberry Pi ein Clientprogramm wie den OMX Player, der dann Musik und Videos abspielt. Für die Anzeige von Bildern dient in unserem Fall Openmax Image Viewer. Diese Programme können für eine optimale Leistung die Hardwarebeschleunigung der bemerkenswerten Grafikchips der diversen Raspberry-Pi-Modelle nutzen. Als Steuerungs-App auf dem Tablet oder Smartphone kommt die App Raspicast von Google Play in Frage. Alle Komponenten zusammen bilden dann einen ähnlichen Funktionsumfang wie Googles Chromecast ab.

Software für den Raspberry Pi

Die benötigten Softwarekomponenten für den Raspberry Pi stehen nicht alle als fertige Pakete bereit. Den Player für Musik und Videos gibt es zwar in den Paketquellen, aber der Bildbetrachter mit Streamingfähigkeit muss manuell kompiliert werden.

1. Bildbetrachter: Nach dem Start und der obligatorischen Aktualisierung des Raspbian-Systems installiert man dazu erst noch die verlangten Pakete in der Kommandozeile

```
sudo apt-get install git make
  libjpeg8-dev libpng12-dev
```

und kann die Quellcodedateien von Openmax Image Viewer über das Kommando

```
git clone https://github.com/
  HaarigerHarald/omxiv.git
```

abholen. Danach geht es mit dem Befehl

```
cd omxiv
```

in das gerade angelegte Quellcodeverzeichnis, in welchem nun die beiden folgenden Befehle

```
make ilclient
make
```

den Bildbetrachter Open Max Image Viewer kompilieren. Ein vorangestelltes sudo ist hier noch nicht verlangt. Erst nachdem der Compiler fertig ist, brauchen wir sudo-Berechtigungen, um das Programm mit dem Kommando

```
sudo make install
```

auf dem Raspbian-System zu installieren. Ist alles gelungen, so kann der Aufruf

```
/usr/bin/omxiv -h
```

das frisch kompilierte Programm testen und dessen Hilfestellung in der Kommandozeile zeigen.

2. Streaming-Videoplayer: Das größere Paket, den OMX Video Player, braucht man nicht zu kompilieren. Mit

```
sudo apt install omxplayer
```

ist das Programm umstandslos aus den Raspbian-Paketquellen installiert.

Den Raspberry Pi einrichten

Die Fernsteuerung des Raspberry Pi wird mittels SSH erfolgen. Damit dies funktioniert, muss also dieser Dienst aktiviert sein. Falls dies noch nicht erfolgt ist, erledigen Sie das ganz unkompliziert in der Kommandozeile mit dem Konfigurationstool raspbi-config unter „Interfacing Options → P2 SSH“.

Auf der grafischen Oberfläche gibt es analog dazu das Tool Raspberry Pi Configuration im Anwendungsmenü.

Damit der Raspberry Pi als Streamingclient mit den installierten Programmen funktioniert, muss die grafische Benutzeroberfläche allerdings abgeschaltet sein. Diese Einstellung erledigen Sie ebenfalls mit dem Tool raspi-config, und zwar unter „Boot Option → Desktop/CLI” → Console“.

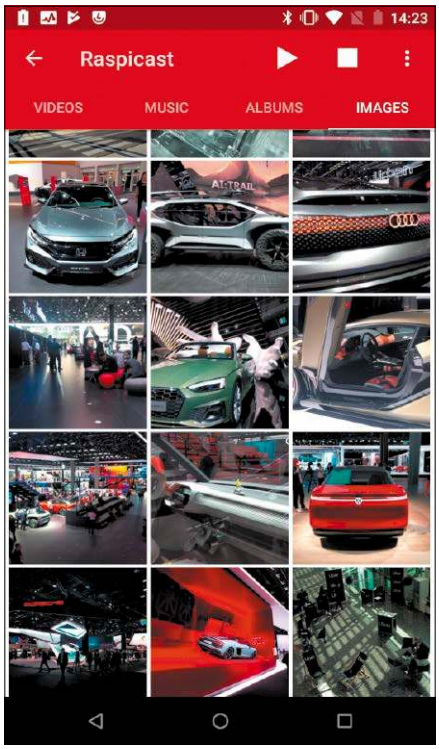
Zuletzt ist zur Kontaktaufnahme mit dem Raspberry Pi noch dessen IP-Adresse beziehungsweise Hostname im lokalen Netzwerk in Erfahrung zu bringen. Den Hostnamen zeigt der gleichnamige Befehl

```
hostname
```

an und dieser Befehl

```
hostname -I
```

liefert die lokale IP-Adresse des Raspberry Pi. In der Regel empfiehlt sich die Verbindung über die IP-Adresse (siehe unten).



Bilder als Stream: Die Auswahl und Übertragung von Bilddateien auf dem Android-Gerät an den Raspberry Pi mittels Raspbicast funktioniert deutlich besser als das Streaming per DLNA.

Die App Raspbicast konfigurieren: Wenn Bildbetrachter und der Video/Musikplayer auf dem Raspberry Pi installiert sind, funktioniert der Rest einfach per SSH-Verbindung.

Smartphone oder Tablet verbinden

Für den eigentlichen Streamingzauber sorgt nun die App Raspbicast für Android-Geräte, die auf Google Play unter der Adresse *https://play.google.com/store/apps/details?id=at.huber.raspicast&hl=de* zur Installation bereitsteht. Der Zauber besteht hier jedoch nicht aus geschützten Chromecast-Protokollen, sondern aus dem verschlüsselten SSH-Protokoll, das mit dem Open-SSH-Server auf dem Raspberry Pi Kontakt aufnimmt und dann die installierten Streamingclients über die App mit einigen Menübefehlen fernsteuert. Bei der App Raspbicast handelt es sich also im Wesentlichen um einen SSH-Client mit einem grafischen App-Front-End für den OMX Video Player und den OMX Bildbetrachter.

Nach dem ersten Aufruf der App verlangt diese noch die Eingabe der SSH-Verbindungsinformationen zum Raspberry Pi. In das Feld „Hostname oder IP“ kommen die IP-Adresse des Raspberry Pi und die Portnummer des SSH-Servers, darunter der Benutzername und das Passwort für die Anmeldung. Auf dem Raspberry Pi muss niemand angemeldet sein, Streaming wird von der Anmeldemaske im Textmodus aus funktionieren.

Die App kann nun mit „Dateien“ auf das Dateisystem des Raspberry Pi zugreifen und dort gespeicherte Mediendateien abspielen. Mit dem Menüpunkt „Cast“ kann die App Bilder, Filme und Musik vom Android-Gerät zum Raspberry Pi streamen, der diese dann ausgibt. Wo die Soundausgabe erfolgen soll, kann die App in den Optionen unter „Audioausgang“ festlegen. Mit „HDMI“ gibt der Raspberry Pi die Audiodaten über den angeschlossenen TV aus.

Kleinere Probleme und Lösungen

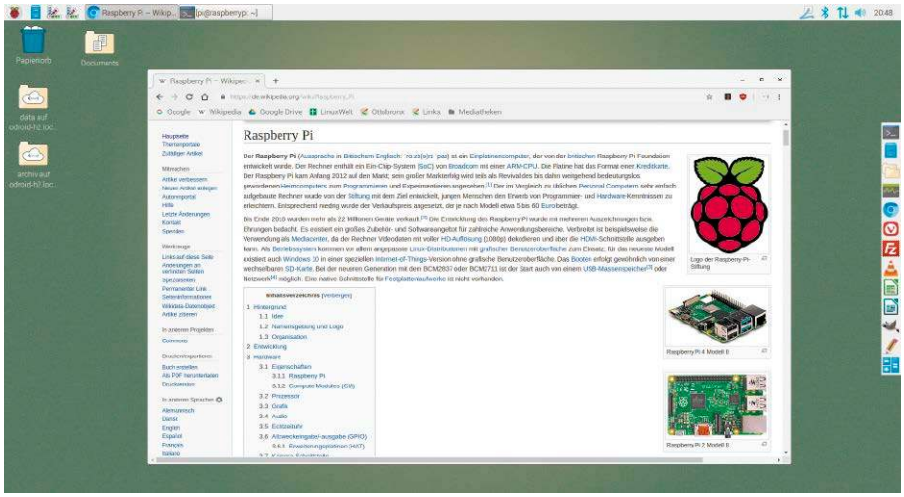
1. Zeigt die App nur einen sich ewig drehenden Kreis an, so scheiterte die SSH-Verbindung. Bei unseren Tests funktionierte nämlich die Identifizierung des Raspberry Pi per Hostnamen nicht. Mit der Angabe der IP-Adresse war das Problem behoben.

2. Es ist in der App nicht ersichtlich, wie das Streamen von Youtube-Videos funktioniert. In der Youtube-App dient das Symbol „Teilen“ dazu, die URL eines aufgerufenen Videos an Raspbicast zu senden. Dann spielt das Youtube-Video auch auf dem Raspberry Pi ab. ■

Raspberry Pi 4 als Desktop

Schon älteren Modellen des Raspberry Pi wurde Desktoptauglichkeit angedichtet. Dass der deutlich leistungsstärkere Pi 4 diese Rollendiskussion neu anheizt, war zu erwarten. Und in der Tat: Bei richtiger Konfiguration taugt der Pi 4 allemal als Zweitdesktop.

VON HERMANN APFELBÖCK



Eigentlich sollte es selbstverständlich sein, dass von einer kleinen Platine zum Preis von 50 oder 60 Euro keine echte PC-Leistung zu erwarten ist. Der Raspberry Pi wurde als Bastelplatine geboren und kann sich inzwischen uneingeschränkt als Dateiserver, Mediencenter oder HDMI-Zuspieler für das TV-Gerät bewähren. Nachdem der Pi 4 nun aber bis zu vier GB RAM und eine Quadcore-CPU mit 1,5 GHz mitbringt, wird er gerne mit älteren Notebooks und PCs ähnlicher Ausstattung verglichen, die ja ihrerseits als Hardware für den Desktopbetrieb konzipiert waren. Das verkennt aber die Tatsache, dass ARM-CPUs mit vergleichbarer Kernzahl und Taktung nicht annähernd die Leistung der x86-CPUs (von Intel und AMD) erreichen. Trotzdem ist der Einsatz des Raspberry 4 als Desktopsystem realistisch, sofern man diese Rolle eindeutig festlegt, seine Multitaskinganspruche nicht übertreibt – und vor allem das Betriebssystem auf eine schnelle SD-Karte schreibt.

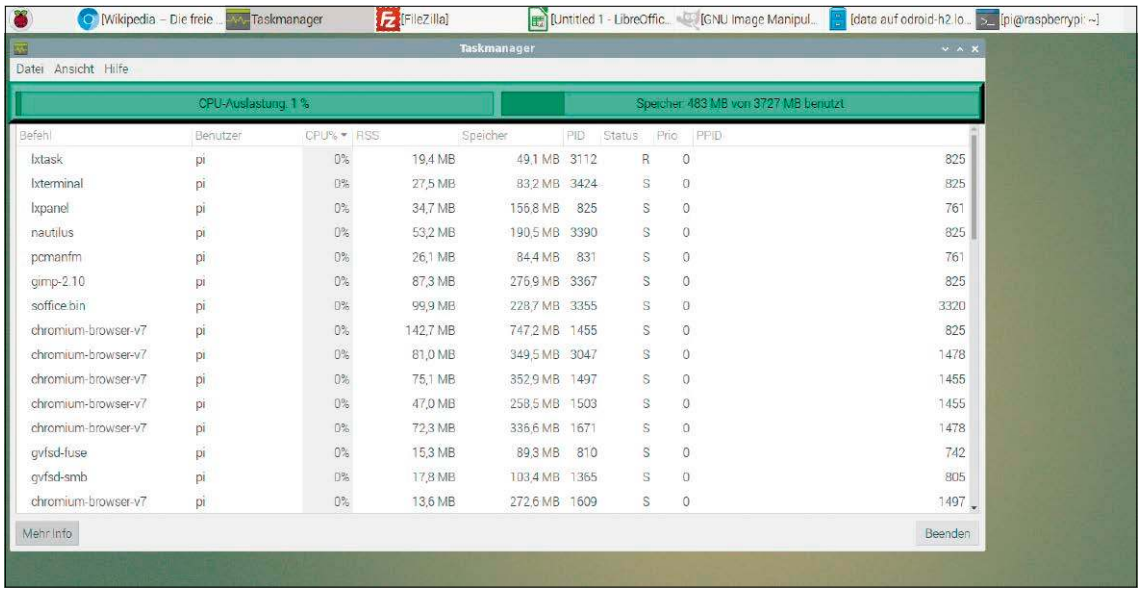
SD-Karte und Betriebssystem

Die eindeutig wichtigste Maßnahme für einen flüssigen Raspberry-Desktop ist eine richtig schnelle Micro-SD-Karte, die Lesegeschwindigkeiten von etwa 100 MB/s erreicht. Eingefrorene Fenster, langsamer Bootvorgang, zähe Installationen, für die man schnell den kleinen Raspberry Pi 4 verantwortlich machen könnte, sind allesamt Folgen einer unzureichenden SD-Karte. Der Leistungsunterschied des Pi 4 mit einem Raspbian auf einer Class-10-Karte (Class 10 ohne weitere Attribute bedeutet lediglich zehn MB/s) und einer Class-10-UHS-Karte (100 MB/s und mehr – UHS I, II und III) ist dramatisch. Die schnellsten SD-Karten beginnen mit Kapazitäten von 32 GB und tragen den Zusatz „SDXC“, „UHS“ oder „Ultra“. Eine Empfehlung sind etwa Sandisk-SDXC-Karten mit der Bezeichnung „Extreme“. Der Preis solcher SD-Karten kann je nach Kapazität dann allerdings den Preis der Raspberry-Platine erreichen.

Beim Betriebssystem gibt es derzeit noch kaum Alternativen: Das Raspbian „Buster“ (*www.raspberrypi.org/downloads*) mit seinem bescheidenen Desktop „Pixel“ dürfte aber so und so die angemessene Wahl bleiben, selbst wenn früher oder später Alternativen wie Ubuntu Mate bereitstehen. Wem der Pixel-Desktop zu karg ist, kann sich über Metapakete wie „mate-desktop-environment“ oder „lxqt“ auch in Raspbian immer noch einen anderen Desktop nachrüsten. Von den drei Raspbian-Varianten empfehlen wir „Raspbian Buster with desktop“, das mit Browser Chromium und VLC-Mediaplayer nicht viel, aber doch die wesentlichste Software mitbringt. Gezielte Nachinstallation sind jederzeit im Terminal über „apt install“ möglich, während das grafische Tool „Recommended Software“ (rp-prefapps) mit seinem sehr begrenztem Angebot eher überflüssig erscheint.

Mit einer flotten SD-Karte erzielt der Raspberry Pi 4 mit Raspbian respektable Bootzeiten: In 17 Sekunden sind wir beim Anmeldebildschirm und bei gewählter Auto-Anmeldung („Raspberry-Pi-Konfiguration → System → Automatisch Anmeldung“) dauert der Start bis zum vollständigen Desktop ganze 21 Sekunden.

Beim Desktopbetrieb mit Raspbian „Buster“ und typischer Anwendungssoftware wie Browser, VLC, Gimp, Libre Office ist es unwahrscheinlich, dass das System jemals mehr als ein GB RAM benötigt. Die Maximalausstattung des neuen Platinenmodells mit vier GB RAM ist daher definitiv nicht



Multitasking: Der neue Raspberry bedient mehrere aktive Prozesse flüssig und ohne Desktopaussetzer. Speicherengpässe sind auf dem sparsamen Raspbian-System generell kein Thema.

notwendig, schon die mittlere Variante mit zwei GB RAM bietet genügend Reserven.
Um den Desktopbetrieb zu optimieren, lohnen sich etliche Optionen und Kontrollen in der Systemkonfiguration: Unter „Einstellungen → Raspberry-Pi-Konfiguration“ muss unter „System“ der „Boot“ zum „Desktop“ erfolgen. Unter „Schnittstellen“ sollten, soweit möglich, alle Dienste deaktiviert sein und unter „Leistung“ können Sie den „GPU-Speicher“ auf 128 (MB) erhöhen. Wer die Platine konsequent auf den Desktopeinsatz fokussiert, wird außerdem auf die Installation von Serverdiensten wie Samba, Open SSH oder Apache verzichten.

Software und Desktop

Besondere Softwarediät müssen Sie dem Raspberry Pi 4 nicht auferlegen. Auch anspruchsvollere Software wie Libre Office oder Gimp ist in wenigen Sekunden gestartet. Der in Raspbian vorinstallierte Browser Chromium ist gegenüber dem etwas trägeren Firefox die vermutlich beste Wahl für den Raspberry. Nach dem Browserstart ist das Verhalten auch mit etlichen geöffneten Tabs jederzeit flüssig. Eine noch etwas flinkere Alternative wäre der Browser Vivaldi, von dem es auf *https://vivaldi.com/de/* auch ein DEB-Paket für die ARM-Architektur gibt. Das bleibt aber eher Geschmackssache ohne Not. Ein Ausweichen auf wirklich minimalistische Browser wie Midori hat der Raspberry Pi 4 definitiv nicht nötig, zumal solche Alternativen in der Regel nur RAM sparen, aber beim Seitenaufbau eher langsamer sind. Raspbians schlichter Pixel-Desktop bietet durchaus mehr Anpassungsmöglichkeiten als das Hauptmenü unter „Einstelllungen“ standardmäßig preisgibt. Es lohnt sich, dies mit dem „Main Menu Editor“ zu korrigieren. Hier finden Sie in der Kategorie „Einstellungen“ weitere Tools wie „Erscheinungsbild anpassen“ oder „Openbox Konfiguration Manager“, die standardmäßig deaktiviert sind, aber nach Klick auf das Kästchen „Anzeigen“ im Hauptmenü erscheinen.

Pi 4 als Desktop-PC: Das Fazit

Eben Upton, Gründer und Leiter der Raspberry Pi Foundation, hat die Frage, ob der neue Raspberry Pi 4 desktoptauglich sei, klipp und klar folgendermaßen beantwortet: „Yes, it is suitable for use as a general-purpose desktop PC“.
Der Raspberry Pi 4 als Allzweck-PC? Wir hatten erhebliche Zweifel, doch beim aktuellen Raspberry ist solche Nutzung in der Tat realistisch, vorausgesetzt, man spart weder bei der SD-Karte noch beim Gehäuse. Als Surfstation, als Zweitdesktop oder als Übungsrechner für Schulen ist die Platine uneingeschränkt zu empfehlen und absolviert sogar Multitasking mit Installationen oder Datentransfers neben laufendem Browser ohne Murren. ■

FLIRC LÖST DIE HITZEPROBLEME LAUTLOS

Neben allem Jubel über den Raspberry Pi 4 stand schnell die Sorge über eine allzu heiße neue Himbeere. Mit dem Kommando „vcgencmd measure_temp“ gemessene 70 Grad und darüber sind im Desktopbetrieb keine Ausnahme, sondern eher die Regel. Doch das Hitzeproblem ist mit kleiner Investition zu beheben – und zwar lautlos ohne lästige Lüfter: Das in der letzten LinuxWelt als Newsmeldung vorgestellte Aluminiumgehäuse „Flirc Raspberry Pi 4 Case“ (*www.welectron.com/Metallgehaeuse*, 20 Euro) konnten wir mittlerweile im Dauerbetrieb testen. Es sorgt dafür, dass der Raspberry Pi 4 auch bei Hochlast keine 70 Grad mehr erreicht und im Normalbetrieb bei etwa 55 bis 60 Grad bleibt. Das ist immer noch hübsch warm, aber tolerierbar. Das auch optisch ansprechende Gehäuse führt eine quadratische Einbuchtung im Deckel exakt auf SOC und CPU der Platine und kann damit die Abwärme großzügig auf die gesamte Deckelfläche ableiten. Diese einfache Maßnahme wirkt erwiesenermaßen effizienter als die kleinen Kühlkörper für das SOC, wie sie ebenfalls im Elektronikfachhandel angeboten werden.

Quelle: amazon.de

Server – ganz einfach!

Yunohost will Installation und Betrieb von Serveranwendungen vereinfachen. Mit der Software können Sie sich individuell die Komponenten zusammenstellen, die Sie benötigen. Das System läuft auch auf dem Raspberry Pi.

VON STEPHAN LAMPRECHT

Das Aufsetzen eines eigenen Web- oder Datenservers ist nicht immer ganz einfach, insbesondere wenn das System mehrere Dienste und Anwendungen anbieten soll. Yunohost tritt mit dem Versprechen an, die Einrichtung und Installation zahlreicher Serverdienste stark zu vereinfachen: Mit wenigen Klicks lassen sich etwa Wordpress oder Nextcloud in Betrieb nehmen.

Yunohost hier mit zwei Serverdiensten: Beim Aufruf des Yunohost finden eingerichtete Benutzer die Verknüpfungen zu den installierten Apps vor.

Yunohost stellt sich vor

Bei Yunohost handelt es sich um eine spezialisierte Debian-Distribution mit Webserver Nginx, Maria DB als Datenbank, Spamfilter, Mailserver und Firewall. Alle Module sind über eine einheitliche Weboberfläche für die Konfiguration zugänglich. Über diese Oberfläche stellt Yunohost dann offiziell unterstützte Anwendungspakete bereit, die einfach per Browser aktiviert werden können. Dazu gehören so populäre Serverdienste wie Dokuwiki, Wordpress, Nextcloud oder Baikal.

Rund um Yunohost ist eine Community aktiv, die weitere Anwendungen zusammenstellt. Auch diese Programme können Sie mit wenigen Mausklicks in Betrieb nehmen. Neben zahlreichen weiteren Hardwareplattformen (siehe Kasten) unterstützen die Entwickler auch den Raspberry Pi. Damit bietet sich eine sehr platz- und energiesparende Hostinglösung an. Ob der Raspberry tatsächlich auf Dauer die passende Plattform ist, hängt von der Last des Projekts ab. In Hinblick auf Arbeitsspeicher und Prozessorleistung ist der Ein-Platinen-Rechner limitiert. Ressourcenhungrige Dienste wie Nextcloud mit mehreren Anwendern werden den Raspberry schnell an seine Leistungsgrenzen bringen. In diesem Fall ist es vermutlich sinnvoller, Yunohost auf einen Server umzuziehen. Ein Dokuwiki oder Baikal-Kalender ist hingegen keine Herausforderung für die Pi-Platine.

Installation auf dem Raspberry Pi

Die Installation verläuft wie bei anderen Projekten auch: Sie laden sich von *https://yunohost.org/#/images* das aktuelle Image für den Raspberry Pi auf einen Rechner herunter (bei Redaktionsschluss wurde der neue Raspberry 4 noch nicht unterstützt). Sie benötigen eine SD-Karte mit wenigstens acht GB Speicherkapazität. Zum Kopieren der Imagedatei empfehlen wir das kostenlose Programm Etcher (*www.balena.io/etcher*), das auf jedem Betriebssystem funktioniert. Wenn Sie den Systemstart verfolgen wollen, schließen Sie Tastatur und Monitor an den Rechner an. Im laufenden Betrieb werden diese nicht mehr benötigt. Legen Sie die SD-Karte ein, verbinden Sie das System per Ethernet mit Ihrem Heimnetz und versorgen Sie die Platine mit Strom, um den Mini-PC zu starten.

Am Ende des Systemstarts werden Sie von einem unscheinbaren Log-in begrüßt. Hier finden Sie die vom System ermittelte IP-Adresse. Die weiteren Schritte können Sie dann bereits über den Browser durchführen – oder Sie nutzen das Terminal dafür. Wenn Sie den Browser verwenden, dann laden Sie in der Adresszeile die IP-Adresse des Raspberry, also beispielsweise „http://192.168.178.24“. Sie werden eine Fehlermeldung erhalten, die auf ein mangelndes Sicherheitszertifikat hinweist. Bei der ausschließlich internen Nutzung des Systems genügt das selbst ausgestellte Zertifikat. Dafür legen Sie im Browser eine Ausnahme für diese Site fest und fahren fort. Im nächsten Schritt geht es um die Definition des Passworts für den Admin, um die Administrationsoberfläche zu schützen.

Die Domain einrichten

Um nicht ständig mit einer IP-Adresse hantieren zu müssen und die Problematik mit der unsicheren Verbindung zu lösen, benötigen Sie eine Domain. In diesem Zusammenhang gibt es drei Szenarien:

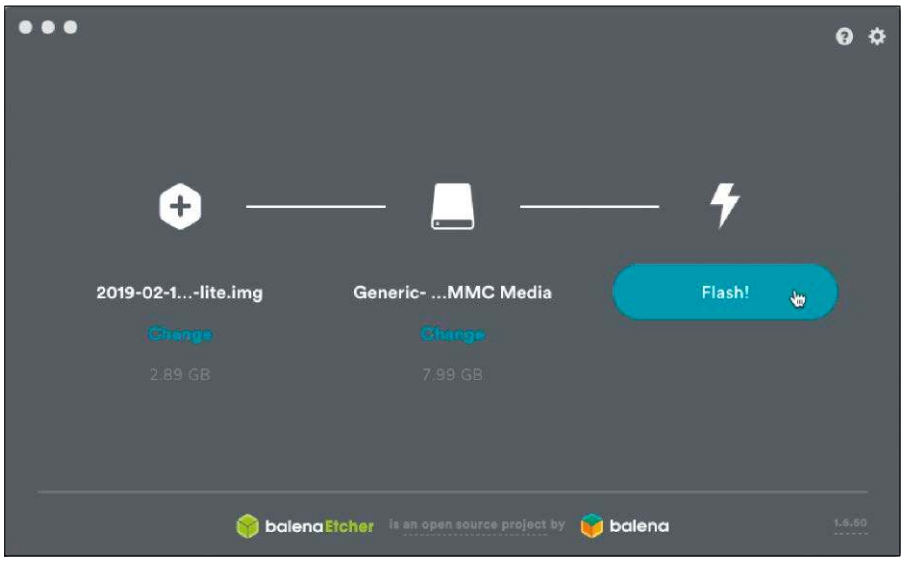
A. Wenn Sie das System nur im lokalen Netz einsetzen, genügt die Namensvergabe für eine lokale Domain.

B. Wird Yunohost auf einem virtuellen Server installiert, benötigen Sie Zugriff auf den DNS-Server des Anbieters, um dort eine eventuell bereits vorhandene Domain auf dem Server mit einem A-Record einzu-

tragen. Diese Arbeit sollte bereits vor der Einrichtung von Yunohost erledigt sein. Im A-Record in der DNS-Tabelle des Providers wird dann die Verbindung zwischen der (festen) IP-Adresse des Servers und der Domain hergestellt. Danach ist auch erst die Ausstellung eines Zertifikats sinnvoll zu erledigen.

C. Der komlizierteste Fall: Yunohost läuft auf dem Raspberry Pi im Heimnetzwerk, soll aber öffentlich zugänglich sein. In diesem Fall benötigen Sie eine Domain bei einem Anbieter für dynamische Domains, die dann externe Anfragen auf die Domain an den lokalen Anschluss weiterleiten. Rufen Sie die Admin-Oberfläche von Yunohost über die IP-Adresse auf. Sofern Sie noch keine Apps und keine Domain eingerichtet haben, sollten Sie immer auf der Verwaltungsseite landen. Sie erreichen diese auch immer über „[IP_Adresse]/admin“. Auf der Übersichtsseite wählen Sie „Domänen“ aus. Haben Sie bereits eine Domain registriert oder wollen Sie eine lokale Domain einrichten, dann wählen Sie „Ich habe schon eine Domain“ und tragen den entsprechenden Namen direkt ein. Mit „Hinzufügen“ übernehmen Sie den Eintrag.

Wenn Sie eine neue dynamische Domain aus dem übersichtlichen Angebot einrichten wollen, entscheiden Sie sich für die zweite Option. Das System begleitet dann durch die nächsten Schritte. Für alle Besitzer einer Fritzbox lautet unsere klare Empfehlung: Nutzen Sie die über „Internet → Freigaben“ erreichbare Funktion für Dyn DNS. Sie können damit komfortabel eine dynamische Domain bei einem bekannten Anbieter einrichten und müssen sich anschließend über „Freigaben“ nur noch um die Zuordnung der Ports kümmern, etwa den Port 80 auf Yunohost umleiten, wenn auf den Webserver zugegriffen werden soll. Ist die Domain final eingerichtet, richten Sie zur Absicherung direkt aus der Konfigurationsoberfläche heraus ein Zertifikat ein. Yunohost nutzt dabei der Dienste von Let's Encrypt. Über die Übersicht der eingerichteten Domains rufen Sie sich die Detailansicht auf. Im unteren Teil des Bildschirms finden Sie unter „Handlungen“ den Schalter „SSL-Zertifikat“. Sie haben an dieser Stelle zwei Optionen. Jederzeit können Sie das selbst signierte, aber von Browsern bemängelte Zertifikat erneuern. Ist die Domain mitsamt DNS-Eintrag korrekt eingerichtet, ist der Schalter „Let's Encrypt“ auswählbar.



Das übliche Prozedere, hier mit dem plattformunabhängigen Etcher: Vor Beginn des Raspberry-Hostings muss erst mal das Yunohost-Image auf eine SD-Karte.

Sprödes „Willkommen“: Wichtig ist aber nur die IP-Adresse, die Yunohost an dieser Stelle meldet.

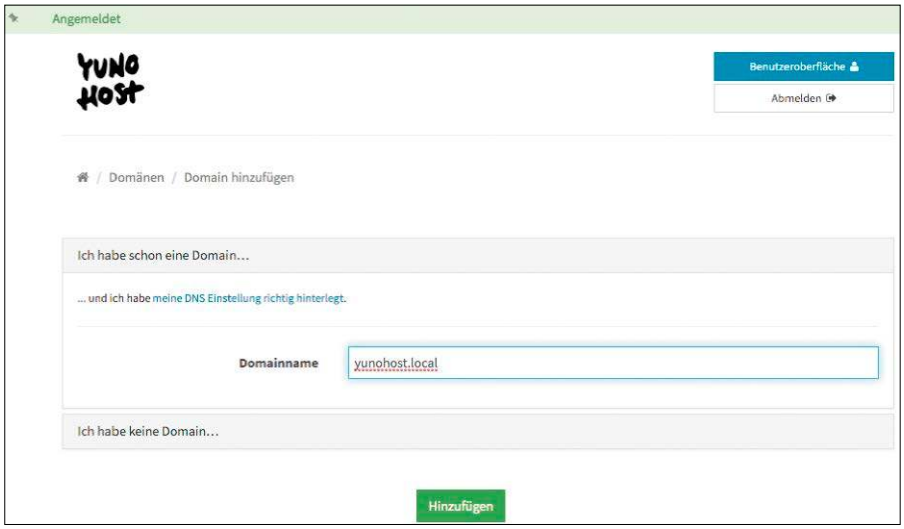
Mit einem Mausklick wird das Zertifikat dann ausgestellt und auch gleich installiert. Einfacher geht es kaum.

Benutzer anlegen und App installieren

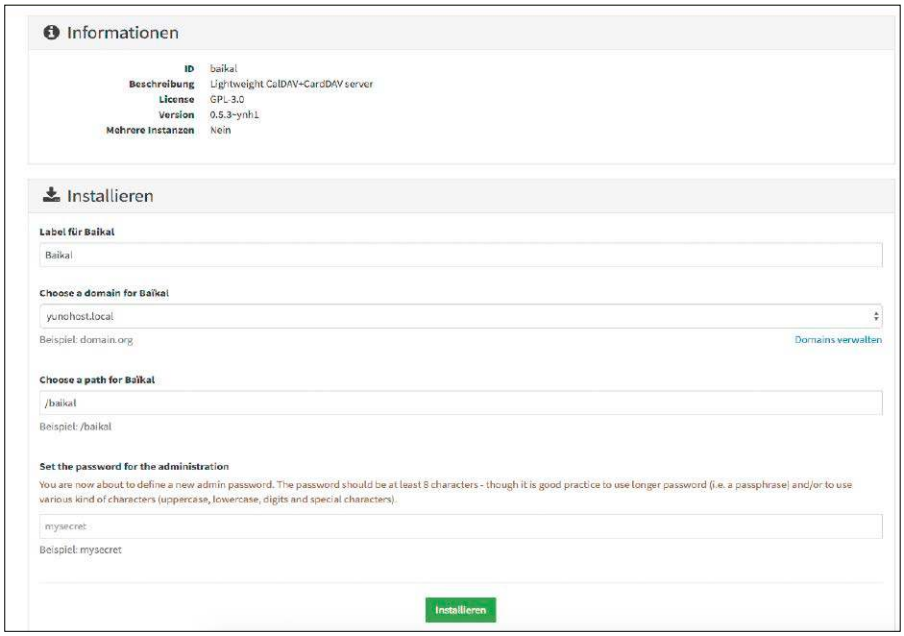
Über die Adminoberfläche sollten Sie im Bereich „Benutzer“ wenigstens ein Benutzerkonto für das Gesamtsystem anlegen. Denn während der Installation vieler Apps werden Sie in der Regel nach einem Benutzer mit Administrationsrecht gefragt. Ist ein Benutzer eingerichtet, wählen Sie diesen dann später einfach aus der Liste aus. Der Dialog zur Benutzereinrichtung ist übersichtlich: Sie vergeben einen Benutzernamen, den realen Namen und ein Passwort. Im Zentrum von Yunohost stehen die Dienste, die Sie installieren können. Besuchen Sie über die Verwaltungsoberfläche

YUNOHOST: NICHT NUR AUF RASPBERRY PI

Die Projektwebseite bietet eine Reihe weiterer Yunohost-Versionen. Angeboten werden ISO-Dateien für x86-Computer (32 und 64 Bit), eine Variante für den Orange Pi sowie fertige virtuelle Maschinen für Virtualbox. Auch an die Einrichtung auf einem virtuellen Host wurde gedacht. So ist eine ausschließlich in der Cloud laufende Installation zum Beispiel bei Amazons AWS möglich. Als Betriebssystem sollte dann am besten Debian eingesetzt werden. Ist die Installation abgeschlossen, unterscheiden sich die weiteren Schritte nicht von der Raspberry-Variante.



Eine lokale Domain ist mit der Angabe des Namens schnell angelegt. Für dynamisches DNS und den Zugriff über das Internet greifen Sie am besten auf vordefinierte Anbieter des Routerherstellers zurück.



Eine Installation – hier des Kalenderdienstes Baikal – ist rasch erledigt. In dem übersichtlichen Dialog passen Sie Optionen und Benutzer an Ihre Wünsche an.

den Abschnitt „Applikationen“. Mit Klick auf „Installieren“ erreichen Sie den beeindruckenden Katalog der verfügbaren Anwendungen.

Das kleine Listenfeld neben der Suchmaske am oberen Rand dient als Filter. Es gibt ein Rating bei den Apps, das beschreibt, wie gut die Anwendung in dem Gesamtkonstrukt arbeitet. Je weiter Sie die Qualität herabsetzen, umso größer wird das Angebot. Andererseits kann es dann bei der Arbeit mit dem System passieren, dass nicht alles reibungslos funktioniert. Das sollte Sie aber nicht davon abhalten, ganz nach Wunsch zu installieren, denn die Qualität der Anwendungen und des Gesamtsystems ist allgemein überzeugend.

Wenn Sie etwa Wordpress auf dem Raspberry einrichten wollen, suchen Sie zunächst nach dem passenden Eintrag in der Liste. Klicken Sie in der Übersicht dann auf „Installieren“. Sie gelangen damit stets auf die Detailseite der jeweiligen App. Je nach gewähltem Programm müssen Sie an dieser Stelle zusätzliche Angaben machen. Bei Wordpress ist dies überschaubar. Über den Dialog ändern Sie optional den Pfad für die Installation (und damit auch die Erreichbarkeit) und die Domain ab. Sie müssen das Benutzerkonto des Admins definieren und können häufig auch die Sprache der Installation verändern. Den Fortgang der Installation verfolgen Sie im Browser.

Jede installierte Anwendung ist direkt über die eigene (Sub-)Domain, den Serverpfad oder über eine Sammelseite zu erreichen. Wenn Sie die Domain des Yunohost direkt abrufen, gelangen Sie stets zur Anmeldungsseite (Single-Sign-on). Mit Konto und Passwort erreichen Sie dann die Übersicht der installierten Anwendungen, um diese von hier zu starten.

Die Anwendungen selbst, etwa ein Wordpress, verhalten sich so wie ihre Originale. Yunohost erleichtert die Installation von Wordpress & Co., ändert aber nichts an allen weiteren Optionen dieser Dienste. Auch Tutorials und Anleitungen können Sie uneingeschränkt umsetzen.

Wem die Standardauswahl immer noch nicht genügt, kann unter *https://github.com/YunoHost-Apps* stöbern. Hier sind weitere Pakete verfügbar.

Um solche Anwendungen zu installieren, benötigen Sie die URL des Programms von Github. Am Ende der Seite mit installierbaren Anwendungen finden Sie einen eigenen Bereich „Benutzerdefinierte Apps installieren“. Dort haben Experimentierfreudige die Möglichkeit, die URL zum Repository des Entwicklers einzutragen, um die Installation von dort aus durchzuführen.

Systempflege und Optionen

Als Admin lohnt es sich, regelmäßig die Verwaltungsoberfläche aufzusuchen, um grundlegende Arbeiten zu erledigen. Dazu gehört die Systemaktualisierung, die Sie per Browser starten können. Nach der Auswahl des entsprechenden Menüpunkts werden alle Pakete angezeigt, für die es neuere Versionen gibt. Per Mausklick führen Sie die Aktualisierung durch. Sofern es neuere Versionen der installierten Apps gibt, finden Sie diese in einem eigenen Bereich und können hier selektiv vorgehen. Unter „Dienste“ schalten Sie optional einzelne Dienste ab, pausieren diese oder sehen sich deren Logdateien an, beispielsweise von fail2ban, das bereits vorinstalliert ist, um Attacken auf das System abzuwehren. Der Bereich „Werkzeuge“ erlaubt das Herunterfahren oder den Neustart des Systems und informiert mittels „Überwachung“ über die Auslastung des Servers. ■

LINUX WELT

GESCHENKT!

Machen Sie sich selbst oder Freunden zum Jahresende eine Freude und legen Sie ein Abonnement der LinuxWelt unter den Weihnachtsbaum:

Jahres-Abo für mich oder zum verschenken

6 x pro Jahr – gedruckt und immer mit Heft-DVD oder unterwegs in unserer App!

6 Ausgaben pro Jahr
+ Digital-Zugang 51,- €

Studenten-Abo

6 Ausgaben pro Jahr
+ Digital-Zugang 45,90 €

Mini-Abo

3x LinuxWelt + Prämie
+ Digital-Zugang 17,- €

Bestellen Sie jetzt!

Hier geht's zum Shop: **www.pcwelt.de/linuxabo** oder per Telefon: 0711/7252233 (werktags Montag - Freitag von 08:00 - 17:00 Uhr) oder per Mail: LinuxWelt@zenit-presse.de

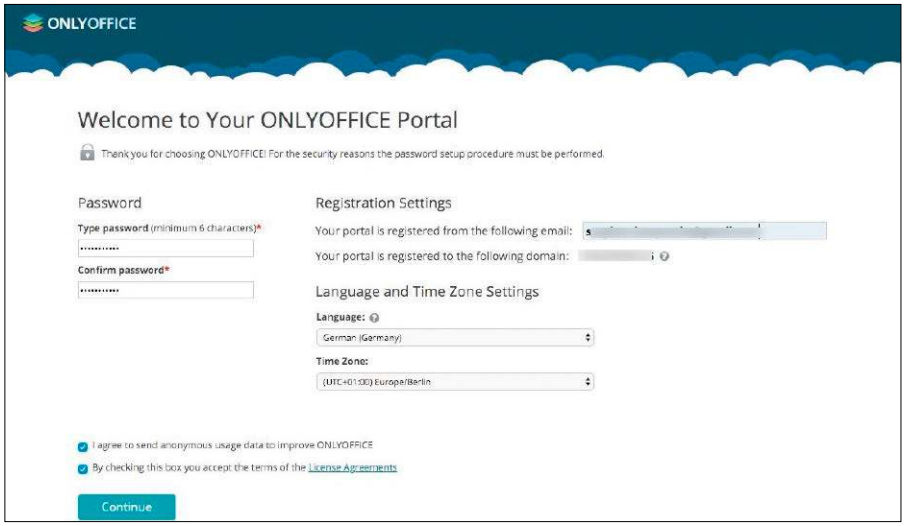
LinuxWelt erscheint im Verlag IT Media Publishing GmbH & Co. KG, Gotthardstraße 42, 80686 München, Registergericht München, HRA 104234, Geschäftsführer: Sebastian Hirsch.
Die Kundenbetreuung erfolgt durch ZENIT Pressevertrieb GmbH, Postfach 810580, 70522 Stuttgart, Geschäftsführer: Joachim John

Cloud-Office auf eigenem Server

Der Trend in die Cloud ist auch bei Büroanwendungen unverkennbar. Doch nicht jedes Unternehmen möchte Office 365 oder Google nutzen. Only Office ist eine interessante Alternative für kleinere Büros, Arbeitsgruppen und Vereine.

VON STEPHAN LAMPRECHT

Only Office ist eine kommerzielle Büroanwendung, die einen Dokumentenserver, ein Projektmanagement, ein CRM-System und Mailfunktionen umfasst. Die gesamte Anwendung kann beispielsweise auch in Nextcloud integriert werden, um die darin gespeicherten Dateien bearbeiten zu können. Wir zeigen Ihnen die Installation und den Betrieb des Dokumentenservers – ohne die Anbindung an eine andere Groupware. Wenn Sie solche Integration anstreben, weist Ihnen eine Recherche im Internet den Weg.



Erste Schritte in Only Office: Bereits die grundlegende Konfiguration des Systems kann im Browser über das Netzwerk erledigt werden.

Die Voraussetzungen schaffen

Es gibt verschiedene Wege, um Only Office auf einem Linux-Server zu installieren. Der etwas mühevollere Weg führt über die Einrichtung aller notwendigen Komponenten. Dazu zählen die Konfiguration eines Webservers (Nginx), einer Datenbank mit Postgre SGL und Node.js. Dieser Weg ist besonders für Serversysteme zu empfehlen, die über nur eingeschränkte RAM-Reserven verfügen. Hinweise zur Installation auf diesem Weg finden Sie im Supportbereich der Community-Edition.

Schnell, einfach und eleganter ist der Einsatz eines Docker-Images. Hier wird lediglich ein Script gestartet, das sich dann um die Einrichtung des Systems kümmert. Allerdings konsumiert Docker auch Ressourcen für sich selbst. Deswegen sollte der Rechner über mindestens vier GB RAM verfügen. Einer der größten Vorteile dieses Ansatzes liegt darin, dass Sie sich zahlreiche Einstellungsarbeiten wie das Anlegen von Datenbanknutzern ersparen können. In dieser Anleitung wählen wir daher diesen einfachen Weg. Erste Voraussetzung zur Installation ist also erst einmal die Einrichtung von Docker. Als Basis dient in diesem Beispiel Ubuntu. Mit

```
sudo apt update
```

bringen Sie das Paketmanagement zunächst einmal auf den aktuellen Stand. Damit die Repositories von Docker auch per gesicherter Verbindung erreicht werden können, nutzen Sie im Terminal dieses Kommando:

```
sudo apt install apt-transport-
  https ca-certificates curl
  software-properties-common
```

Dies installiert die Option der gesicherten Verbindung, ferner mit Curl einen Crawler für den Download. Im nächsten Schritt holen Sie sich den Schlüssel des Repositories:

```
curl -fsSL https://download.
  docker.com/linux/ubuntu/gpg |
  sudo apt-key add - Repositories
```

Jetzt fügen Sie das Repository als Paketquelle ein. Hier kommt ein leicht verändertes Kommando zum Einsatz als Sie es vielleicht bereits kennen:

```
sudo add-apt-repository "deb
  [arch=amd64] https://download.
  docker.com/linux/ubuntu $(lsb_
  release -cs) stable"
```

Die Variable „lsb_release“ liefert den Codenamen Ihrer Ubuntu-Version zurück. Somit landen Sie im passenden Datenspeicher und können jetzt Docker installieren. Das erledigen Sie mit diesem Befehl:

```
sudo apt install docker-ce
```

Unmittelbar nach der Installation sollte der Daemon von Docker bereits laufen, was Sie folgendermaßen

`sudo systemctl status docker`
kontrollieren können. Sollte der Daemon nicht laufen, holen Sie dies manuell mit
`sudo systemctl start docker`
nach und mit
`sudo systemctl enable docker`
sorgen Sie dafür, dass der Dienst künftig stets automatisch geladen wird. Damit ist die Vorbereitung abgeschlossen.

Die Community-Version von Only Office installieren

Jetzt können Sie die Community-Edition von Only Office installieren. Auch hier führen verschiedene Weg zum Erfolg. Die einfachste Option ist die Nutzung eines speziellen Installations-Scripts. Dies laden Sie sich lokal auf die Maschine herunter:

```
wget https://download.onlyoffice.
  com/install/opensource-install.
  sh
```

Wechseln Sie anschließend in das Verzeichnis des Downloads und sorgen Sie mit dem Dateimanager dafür, dass in den Eigenschaften der Datei das Attribut „ausführbar“ gesetzt ist. In unserem Szenario interessiert in erster Linie die Office-Funktionalität als Dokumentenserver.

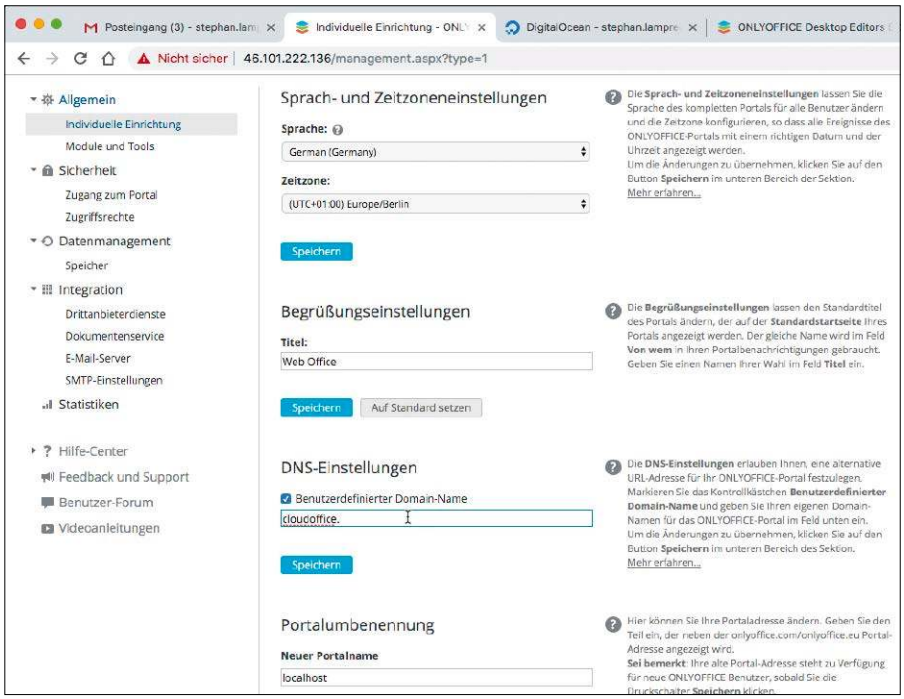
Wird das Script für die Installation ohne Parameter gestartet, richtet es alle Module von Only Office ein, so etwa den Mailserver, den wir nicht brauchen. Spezielle Schalter können dies verhindern:

```
sudo ./opensource-install.sh -ims
  false
```

Der Parameter „-ims“ schaltet die Installation des Mailservers aus. Ist die Installation der Programmdateien abgeschlossen, können Sie die restlichen Arbeiten bereits mit einem Browser durchführen.

Rufen Sie im Browser den Office-Server mit seiner IP-Adresse auf („http://[IP_Adresse]“). Im Begrüßungsdialog sind nur wenige Angaben erforderlich. Sie melden sich direkt nach der Installation als Administrator an. Deswegen müssen Sie zunächst ein Passwort für diesen wichtigen Benutzer einrichten. Außerdem ist es notwendig, eine gültige E-Mail-Adresse zu hinterlegen, über die das Konto erreicht werden kann. Schließlich legen Sie über die Listenfelder noch die gewünschte Sprache und die Zeitzone des Servers fest. Mit „Continue“ schließen Sie die Installation ab.

Sie werden vom Server eine Mail an die hinterlegte Adresse erhalten, die Sie bestätigen müssen. So ist sichergestellt, dass der Docker-Container: Ist Docker erfolgreich auf dem System installiert, ist die Einrichtung von Only Office zügig und unkompliziert erledigt.



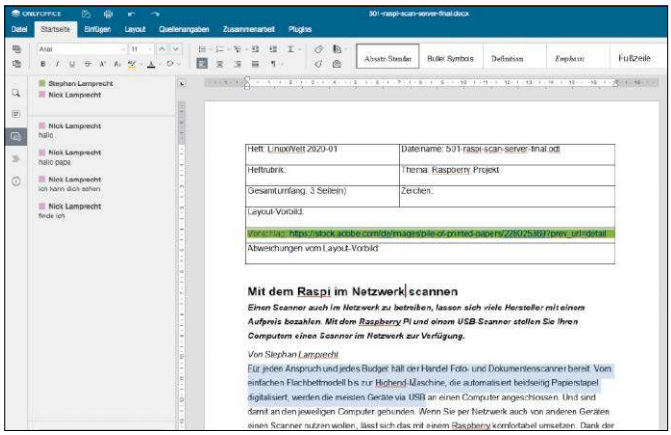
Als Administrator der Installation können Sie in den Optionen des Systems einen neuen DNS-Eintrag hinterlegen. Damit das funktioniert, muss die Domain allerdings konnektiert sein.

Administrator erreichbar ist. Auch der Admin gelangt nach dem Aufruf des Servers zuerst auf die Startseite des Portals. Die allgemeinen Einstellungen erreichen Sie nach einem Klick auf das Zahnrad. Hier ist die Option „DNS-Einstellungen“ von besonderem Interesse, wenn der Server via Internet über einen eigenen Domainnamen angesprochen werden soll. Damit das funktioniert, muss der Rechner extern erreichbar sein, etwa über einen entsprechenden dynamischen DNS-Eintrag.

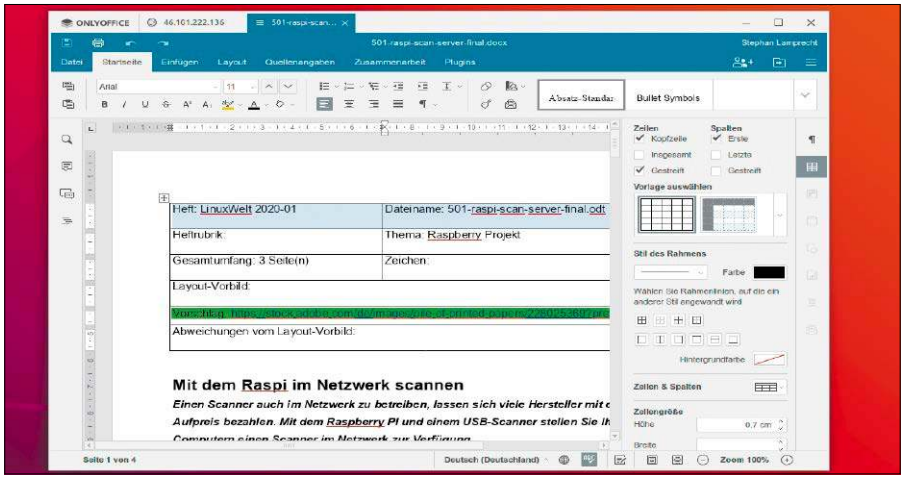
Ist die Verbindung zum Internet sichergestellt, hinterlegen Sie den Domainnamen in der Maske. Der Dokumentserver speichert die Daten im Normalfall lokal auf einem dem System zugänglichen Massenspeicher. Optional können Sie aber auch andere Datenquellen einbeziehen – dazu gehören unter anderem Dropbox, Google Drive und Onedrive. Einen solchen externen Speicher aktivieren Sie innerhalb des Menüs „Integration → Drittanbieterdienste“. Der Zugriff auf die externen Daten erfolgt allerdings nicht per Benutzernamen und Passwort, sondern über die von den Anbietern bereitgestellte API. Es genügt also nicht, nach dem Aktivieren von Google einfach den Benutzernamen und das Passwort einzutragen. Vielmehr müssen Sie erst den Erläuterungen folgen, die Sie über den kleinen Link am oberen Bildschirmrand erreichen. Die Hilfeseiten erklären für jeden Anbieter genau, wie Sie die API des gewünschten Dienstes aktivieren.

Arbeitsgruppe vergrößern und Dokumente bearbeiten

Zum jetzigen Stand haben Sie ein funktionierendes Online-Office, auf das Sie allerdings bisher nur allein zugreifen dürfen. Seinen Nutzen erhält das System natürlich erst dann, wenn Sie weitere Konten anlegen. Dies erfolgt über das Modul „Personen“, das Sie mit einem Klick auf den kleinen Pfeil am oberen linken Bildschirmrand erreichen. Die geringste Mühe macht die Einladung von weiteren Personen mittels eines Links. Auf der Übersichtsseite von „Personen“ klicken Sie auf den Schalter mit



Bearbeiten und besprechen: Während der parallelen Bearbeitung eines Dokuments können Sie mit den anderen Only-Office-Teilnehmern chatten.



Offlineclients: Mit optionalen Clients für Linux, Windows und Mac-OS greifen Sie nicht nur auf die Dokumente des Servers zu, sondern können Dateien auch offline anlegen.

den drei Punkten und wählen „Einladungslink“. Kopieren Sie den Link und senden Sie diesen per Messenger oder Mail an weitere Teammitglieder. Jeder Eingeladene richtet sich dann sein eigenes Konto ein, das er über eine E-Mail bestätigen muss. Als Admin können Sie die aktiven Benutzer zentral über die Personenverwaltung gruppieren, wenn mehrere Mitglieder an einem gemeinsamen Projekt arbeiten sollen, aber auch bei Bedarf wieder entfernen.

Unmittelbar nach dem Einloggen landet jeder Nutzer auf der Portalseite des Servers, über den die verschiedenen Module erreicht werden. Mit einem Klick auf „Dokumente“ betreten Sie die Office-Suite, über die linke Navigation gelangen Sie zum Dateimanagement. Dort haben Sie die Wahl zwischen den Dateien, die Sie selbst erstellt haben, die Ihnen also gehören, sowie Dokumenten, die andere Nutzer angelegt, aber für Sie freigegeben sind. Wenn Sie online an einer bereits existierenden lokalen Datei weiterarbeiten wollen, drücken Sie das Symbol für den Upload. Anschließend wählen Sie das Dokument aus, um es auf den Server zu laden.

Dabei gibt es die Besonderheit, dass Only Office alle Dateien in das aus MS-Office bekannte XML-Format konvertiert. Wenn Sie also eine ODT-Datei aus Open Office hochladen, wird diese automatisch zu einer DOCX-Datei. In Hinblick auf die Formatierungsoptionen stehen alle wesentlichen Möglichkeiten zur Auswahl. Das Einfügen von Diagrammen oder Bildern ist genauso möglich wie die Nutzung von Fußnoten oder Tabellen. Wurde ein Dokument als Basis hochgeladen, werden dessen Formatierungen weitestgehend übernommen.

Das gemeinsame und auch simultane Bearbeiten der gleichen Datei ist mit wenigen Mausklicks eingerichtet. Eine Freigabe erteilen Sie direkt aus dem Dokument heraus: Klicken Sie am oberen Rand der Datei auf das Icon mit dem symbolisierten Nutzer. Im nachfolgenden Dialog wählen Sie einen bestimmten Nutzer aus und erteilen ihm über das Listenfeld ein abgestuftes Recht auf die Datei. Sofern Sie gleichzeitig an einer Datei arbeiten, verfolgen Sie die Änderungen in Echtzeit.

Auch eine Chatfunktion ist integriert. Damit können sich die Bearbeiter über die Änderungen abstimmen. Insgesamt lässt sich mit allen drei Office-Modulen (Textverarbeitung, Tabellenkalkulation und Präsentationsprogramm) gut arbeiten. Wie bei allen Office-Suiten, die nicht direkt von Microsoft stammen, können sich Excel-Dateien als problematisch erweisen, wenn Formeln und Ausdrücke verwendet wurden, die nicht im Funktionsumfang der Drittanwendung enthalten sind.

Optionale Clients installieren

Ist die Verbindung zum Server nicht möglich oder unterbrochen, können Sie die Dokumente nicht via Browser bearbeiten. Um in solchen Situationen trotzdem produktiv arbeiten zu können, bietet das hinter Only Office stehende Unternehmen für Linux, Mac und Windows eigene Clients an. Deren Einsatz ist optional, denn Sie können unterwegs Ihre Dateien mit einem beliebigen Office-Programm bearbeiten, sofern Sie eine lokale Kopie angefertigt haben. Die Installation der Clients kann aber dennoch sinnvoll sein. Damit können Sie sich ebenfalls auf den Dokumentenserver einloggen, um online auf Dateien zuzugreifen oder lokale Kopien hochzuladen. Und Sie können damit auch offline Dateien anlegen und lokal bearbeiten. Beim Arbeiten mit dem Editor nutzen Sie automatisch nur solche Funktionen, die von Only Office verstanden und unterstützt werden.

Solche Clients gibt es auf der Homepage des Unternehmens (*www.onlyoffice.com*). Die Nutzung ist kostenlos. Für Linux werden fertige Binärpakete angeboten, die Sie direkt aus dem Paketmanager oder via Doppelklick im Dateimanager installieren. Nach dem Programmstart wählen Sie aus der Hauptnavigation den Eintrag „Verbindung zur Cloud“. Im nachfolgenden Dialog wählen Sie im Listenfeld zunächst die Art der Installation aus, in unserem Beispiel „Only-Office“. Außerdem tragen Sie die IP-Adresse oder die Domain der Installation ein. Nach einem Klick auf „Zusammenarbeit“ erwartet die Software dann noch den Benutzernamen und das Passwort. Anschließend gelangen Sie zu einer Oberfläche, die exakt wie die Browserversion aussieht. ■

PC-WELT

Die beste Software 2020

Sonderheft
für nur
9,90 €

Ausgewählte Top-Programme für Windows, Sicherheit, Netzwerk, Multimedia

Jetzt bestellen unter
www.pcwelt.de/sh-software 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 EXTRA 1/20 Software-Guide für nur 9,90 €.

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

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

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

Linux und die Datenträger

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

VON HERMANN APFELBÖCK

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

1. Partitionieren und Partitionsstil

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

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

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

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

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

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

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

```
sudo fdisk -l
```

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

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

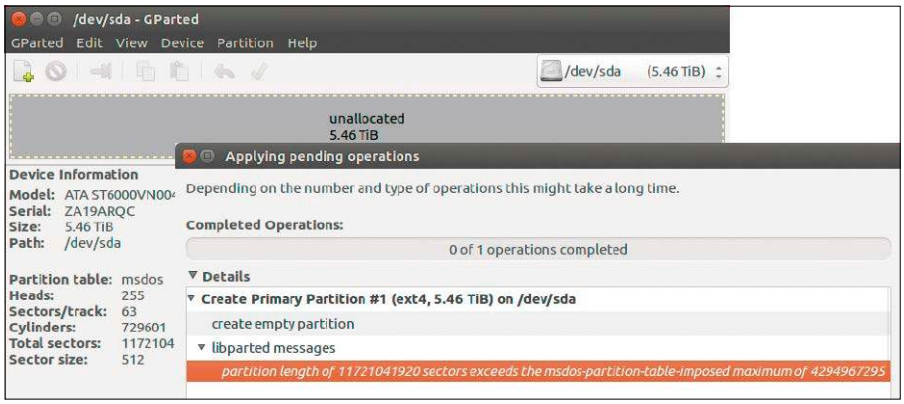
nach GPT oder

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

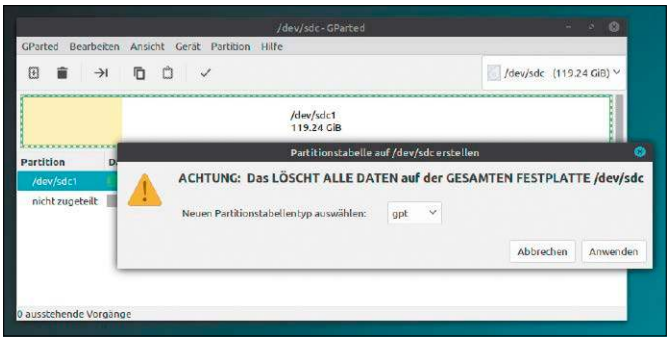
zum Schreiben einer MBR-Partitionstabelle. Ersetzen Sie dabei „[X]“ jeweils durch die richtige Kennung des Laufwerks. Bei reinen Datenpartitionen (nur Benutzerdaten) kann mit diesen Befehlen sogar eine Umwandlung des Partitionsstils ohne Datenverlust gelingen. Wir raten aber davon ab, sich darauf ohne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

2. Partitionen löschen und anlegen

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



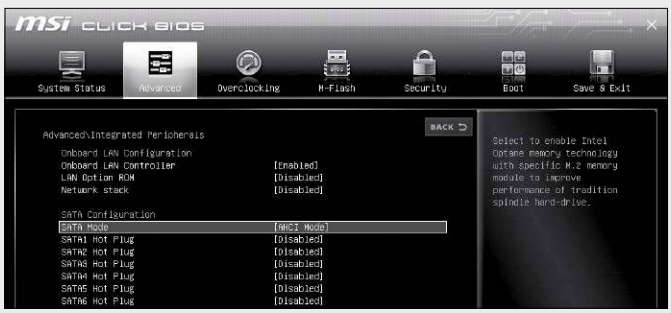
Auch große Festplatten lassen sich im MBR-Stil durch Partitionierung komplett nutzen. Jedoch scheitert der Versuch, große Festplatten (hier mehr als fünf TB) als eine Partition anzulegen.



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

AHCI-MODUS IM BIOS

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



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

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

3. Partitionsstil (MBR/GPT) und Multiboot

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

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

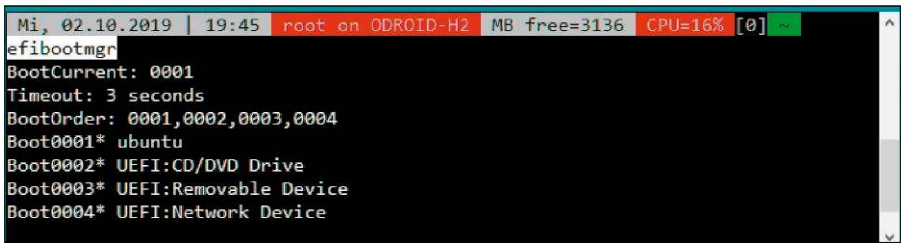
Ob das schon vorhandene System den Bios- oder Uefi-Modus verwendet, erfahren Sie unter Linux im Terminal durch Aufruf dieses Tools:

```
efibootmgr
```

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

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

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



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

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

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

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

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

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

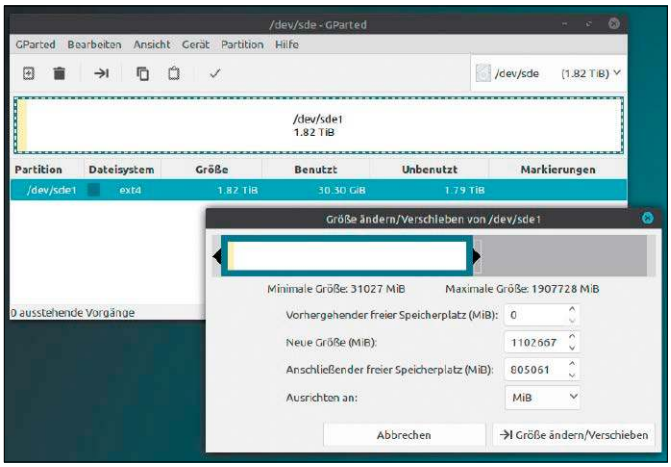
4. Partitionsgrößen nachträglich ändern

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

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

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

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



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

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

FESTPLATTEN ZUSAMMENLEGEN

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

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

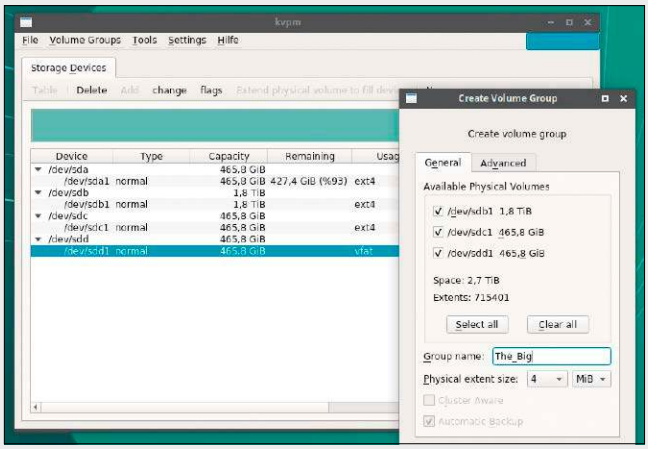
```
sudo apt install kvpm
```

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

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

```
sudo kvpm
```

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



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

5. Formatieren: Die Dateisysteme

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

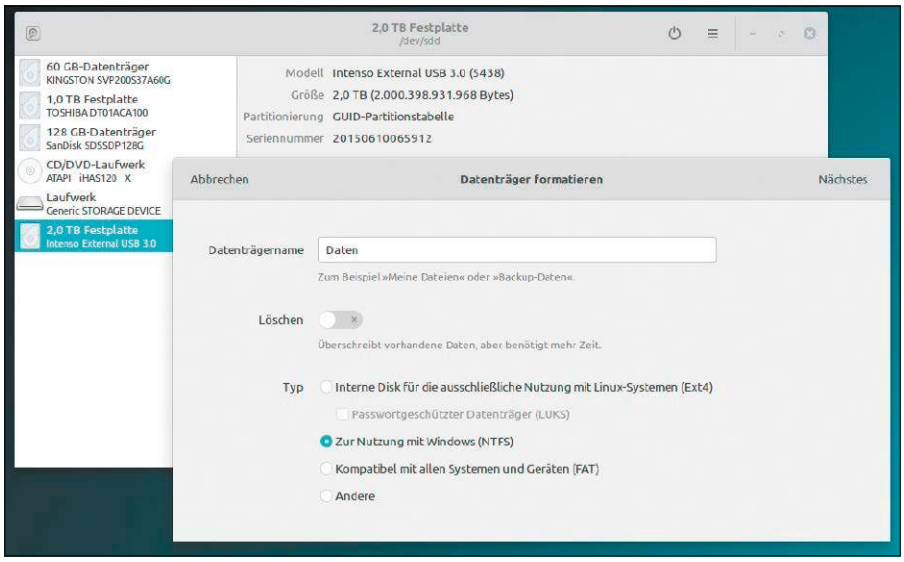
Trotz zahlreicher weiterer Dateisysteme wie F2FS, JFS, ZFS, ReiserFS, XFS ist die Wahl auf einem Desktopsystem nicht schwer: Für die Systempartition, aber auch für alle sonstigen Datenträger, die nur am Linux-System genutzt werden, ist Ext4 die solideste Wahl. Das gilt auch für Laufwerke, die Netzfreigaben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

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

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

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

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



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

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

```
te@teu160403: ~
te@teu160403:~$ mkfs.ntfs

Usage: mkntfs [options] device [number-of-sectors]

Basic options:
    -f, --fast                  Perform a quick format
    -Q, --quick                 Perform a quick format
    -L, --label STRING          Set the volume label
    -C, --enable-compression    Enable compression on the volume
    -I, --no-indexing           Disable indexing on the volume
    -n, --no-action             Do not write to disk

Advanced options:
    -c, --cluster-size BYTES        Specify the cluster size for the volume
    -s, --sector-size BYTES         Specify the sector size for the device
    -p, --partition-start SECTOR    Specify the partition start sector
    -H, --heads NUM                 Specify the number of heads
    -S, --sectors-per-track NUM     Specify the number of sectors per track
    -z, --mft-zone-multiplier NUM   Set the MFT zone multiplier
    -T, --zero-time                 Fake the time to be 00:00 UTC, Jan 1, 1970
    -F, --force                     Force execution despite errors
```

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

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

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

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

Nach „mkfs.“ folgt die Angabe des Dateisystems „ext4“, hinter „-L“ („Label“) geben Sie optional eine Bezeichnung an, anhand derer sich die Partition später im Dateimanager leichter identifizieren lässt. Den Platzhalter „[XY]“ ersetzen Sie durch die Laufwerksbezeichnung und Partitionsnummer, etwa „/dev/sdb1“ oder „/dev/sdc2“. Für andere Dateisysteme gibt es entsprechende Tools, beispielsweise mkfs.ntfs oder mkfs.vfat (FAT32).

6. Mounten: Statisch und dynamisch

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

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

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

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

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

```
lsblk -f
```

Ein Eintrag für die fstab sieht dann im Prinzip so aus

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

und im konkreten Beispiel etwa so:

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

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

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

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

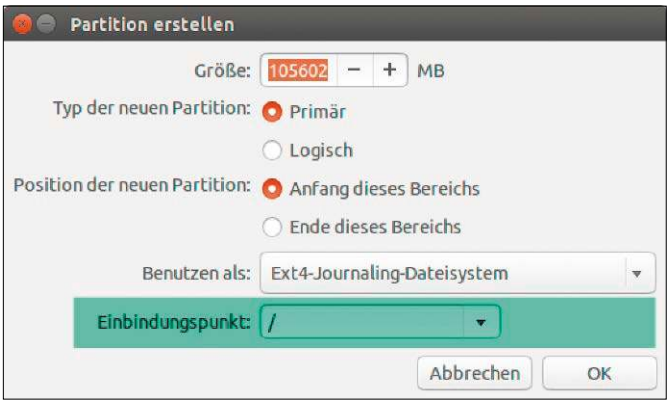
```
sudo mount -a
```

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

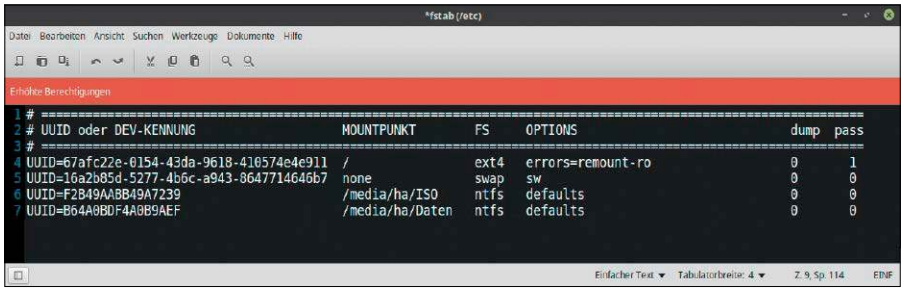
Dynamisches Mounten: Auf dem Linux-Desktop erledigt der grafische Dateimanager den Großteil des Mountgeschäfts. Wenn Sie ein USB-Laufwerk anschließen oder ein neues Laufwerk gerade neu formatiert haben, taucht dieses sofort in der Navigationsspalte des Dateimanagers auf. Nach einem Mausklick darauf erledigt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

- Benutzer mit administrativen Rechten (Systemverwalter) dürfen interne und externe Laufwerke über den Dateimanager ein- und aushängen.
- Auch Systemverwalter erhalten bei Linux-Dateisystemen wie Ext4, BTRFS und XFS nur Lesezugriff, Schreibzugriff gibt es auf FAT32- und NTFS-Partitionen..
- Standardbenutzer dürfen über den Dateimanager nur externe Geräte (USB-Sticks und Festplatten) ein- und aushängen. Auf FAT32- und NTFS-Partitionen gibt es Lese- und Schreibzugriff.
- Standardbenutzer werden bei einem Klick auf interne, nicht eingebundene Laufwerke zur Eingabe des Systemverwalter-Passworts aufgefordert. Bei FAT32 und NTFS räumt Ubuntu Lese- und Schreibzugriff ein, auf Linux-Dateisystemen gibt es nur Leserechte.

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



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



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

7. Zugriffsrechte im Dateisystem setzen

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

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

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

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

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

Diese Befehlszeilen erstellen ein Verzeichnis „/mnt/Data“ für den Datenaustausch. Es gehört der Gruppe „plugdev“, die Vollzugriff erhält. „chmod g+s“ bewirkt, dass das Gruppenattribut erhalten bleibt, wenn ein Benutzer neue Dateien oder Ordner anlegt. Mit setfacl setzen Sie die Standard-Zugriffsrechte, die auf alle enthaltenen und zukünftigen Elemente vererbt werden. Im Ergebnis erhalten alle Mitglieder der Gruppe „plugdev“ Lese- und Schreibzugriff. Zur Gruppe „plugdev“ gehören unter Ubuntu/Mint standardmäßig alle Benutzer.

8. Kapazitäten einfach erweitern

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

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

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

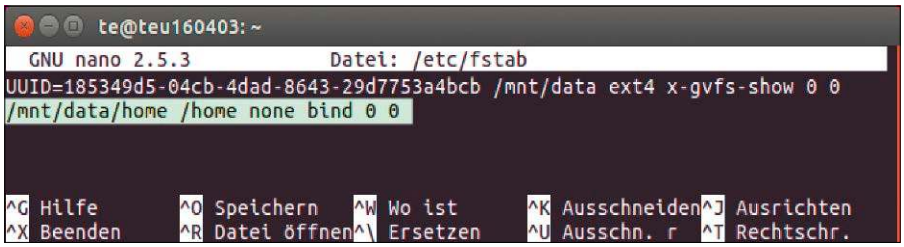
Beachten Sie beim rsync-Befehl den abschließenden Slash hinter „/home/“. Mit folgenden Befehlen erstellen Sie einen neuen Ordner „/home“ und hängen das Verzeichnis des neuen Laufwerks an dieser Stelle ein:

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

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

```
/mnt/data/home /home none bind 0 0
```

Mit Strg-Alt-F7 kehren Sie nun zur grafischen Oberfläche zurück und melden sich an. Ihr Home-Verzeichnis finden Sie so vor, wie Sie es verlassen haben – aber mit mehr Platz.



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

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

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

den neuen Datenträger direkt in das betreffende Verzeichnis:

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

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

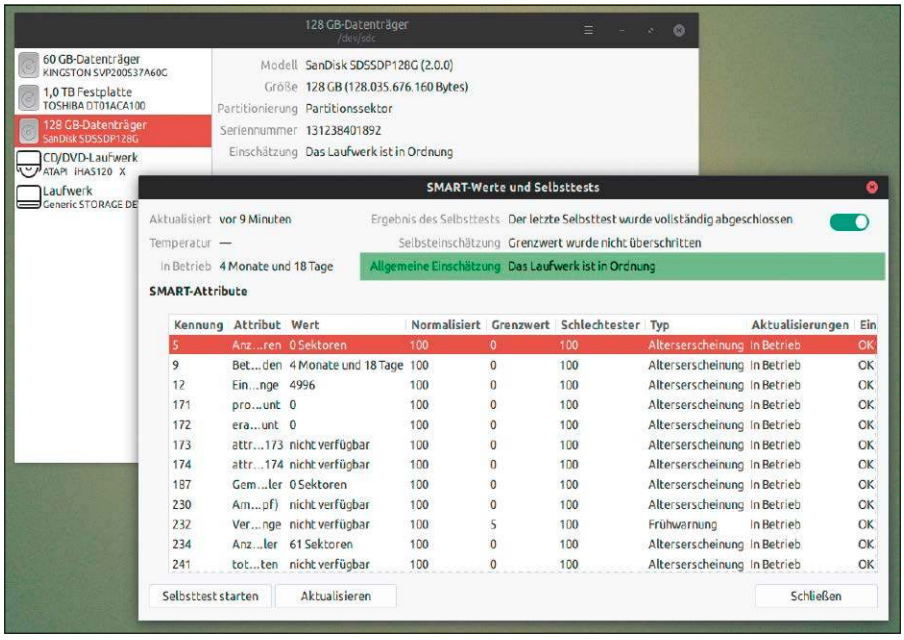
```
sudo chmod -cR 777 ~/Videos
```

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

9. Kontrolle des Datenträgerzustands (SMART)

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

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



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

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

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

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

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

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

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

10. Kontrolle der Festplattenbelegung

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

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

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

```
du -h
```

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

DATENTRÄGER IM BEREITSCHAFTSMODUS

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

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

```
blkid
```

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

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

Wenn das funktioniert, können Sie eine automatische Abschaltung festlegen:

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

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

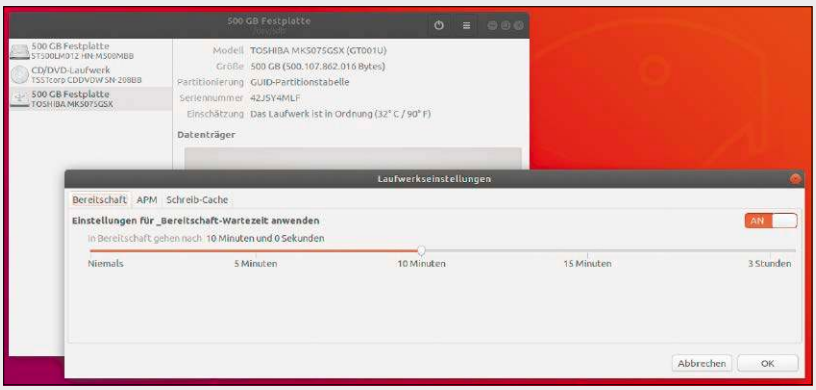
```
sudo nano /etc/hdparm.conf
```

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

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

Die UUID-Kennungen ermittelt das Kommando blkid.

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



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

Desktop de luxe

Hier geht es nicht nur um die Platzhirsche KDE und Gnome. Mit einer neuen Ausgabe von Xubuntu steht auch mal wieder das kürzlich aufgefrischte XFCE im Fokus. Wie immer gibt es aber auch Tipps, die für nahezu alle Desktopumgebungen geeignet sind.

Texpander: Arbeiten mit Textbausteinen

Niemand tippt gerne zu viel, aber im IT-Alltag und Büro wiederholen sich Textbausteine und Floskeln jeden Tag aufs Neue. Ein cleveres Shell-Script speichert Textbausteine und fügt sie systemweit per Abkürzung in beliebigen Programmen oder Eingabefeldern im Browser ein.

Das Script namens Texpander (*https://github.com/leehblue/texpander*) ist kein eigenständiges Programm wie der Makro-Rekorder Autokey, sondern macht im Hintergrund von den Tools Xsel, Xdotool und Zenity Gebrauch.

Textbausteine werden einfach als Textdatei gespeichert, die mit ihrem Namen auch gleich die Abkürzung für deren Abruf definieren. Einfacher geht es kaum, ein Powertool für den Linux-Desktop zu schreiben. So gehen Sie vor:

1. Das Bash-Script „texpander.sh“ von *https://raw.githubusercontent.com/leehblue/texpander/master/texpander.sh* speichern Sie im Home-Verzeichnis selbst oder dort in einem Unterverzeichnis und machen es mit

```
chmod +x texpander.sh
```

ausführbar. Außerdem erstellen Sie mit

```
~/.texpander
```

ein neues Verzeichnis für die künftigen Textbausteine.

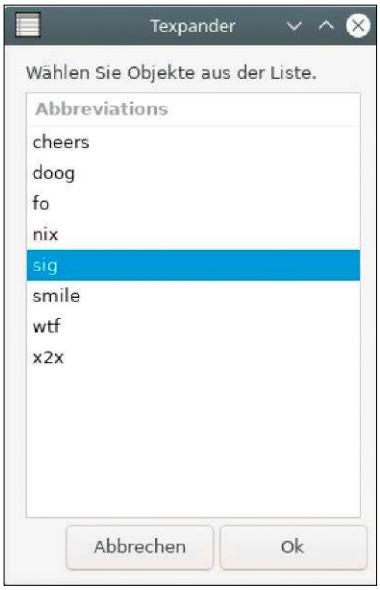
2. Nun werden die Hilfsprogramme benötigt. Über den jeweiligen Paketmanager der verwendeten Linux-Distribution installieren Sie die Pakte für Xsel, Xdotool und Zenity, in Ubuntu beispielsweise mit:

```
Sudo apt install xsel
  xdotool zenity
```

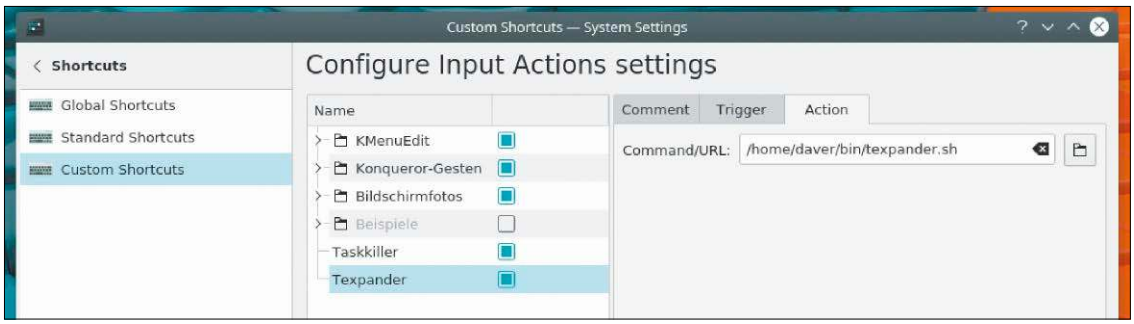
3. In der verwendeten Desktopumgebung gilt es nun, eine eigene Tastenkombination für den Aufruf von „texpander.sh“ zu definieren. In Gnome gelingt das beispielsweise in den Einstellungen mit „Geräte → Tastatur → Tastaturkürzel → Eigene Tastaturkürzel“. Als Befehl muss hier der komplette Pfadname zu „texpander.sh“ eingegeben werden. Die gewählte Tastenkombination sollte etwas Griffiges sein, aber auch nichts, das im Alltag in die Quere kommt. Strg-Leertaste käme etwa in Frage.

4. Jetzt sollte Texpander schon auf die eingerichtete Tastenkombination reagieren und sein Dialogfenster anzeigen, das aber noch leer ist. Nun füllen wir Texpander mit Textbausteinen und legen im zuvor erstellen Verzeichnis „~/.texpander“ eine Textdatei namens „sig“ an, die als Inhalt eine beispielsweise oft getippte Mailsignatur bekommt.

5. Damit ist der Texpander einsatzbereit. Nach dem Aufruf zeigt das Dialogfenster die Kürzel an, die sich mit der Maus auswählen lassen. Die in den Dateien hinterlegten Textbausteine fügt das Script im aktuell aktivieren Fenster ein. **-dw**

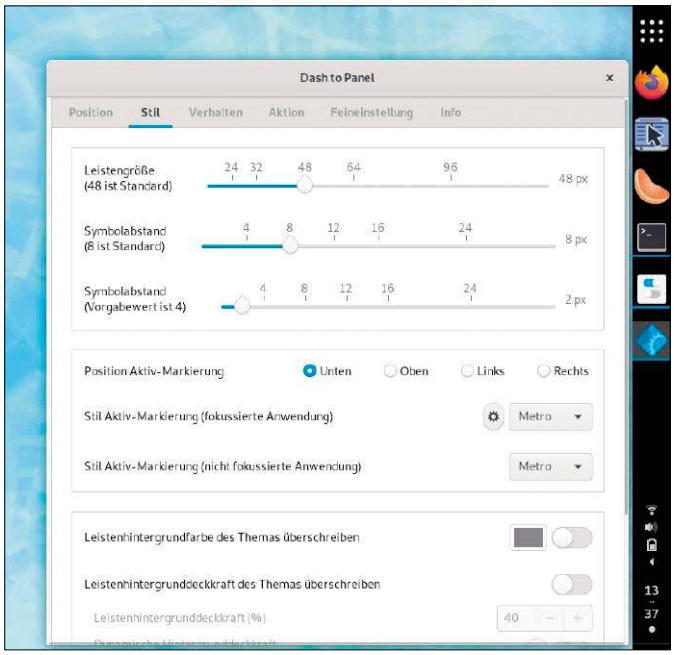


Textbausteine abrufen: Texpander listet die vordefinierten Textbausteine auf, die als Textdatei mit dem gleichen Namen wie die angezeigten Abkürzungen abgelegt werden.



Tastenkombination definieren: Damit die Script-Datei „texpander.sh“ in Aktion treten kann, bekommt die Script-Datei über die Desktopumgebung einen Hotkey zugewiesen.

Gnome: Panel auf der rechten Seite



Mit der passenden Erweiterung Dash to Panel kann Gnome die Systemleiste mit Aktivitäten und Programmfavoriten auf der rechten oder linken Seite des Bildschirms einblenden.

Eine der Gnome-Erweiterungen, auf die wir hier immer wieder hinweisen, ist Dash To Panel. Diese Erweiterung ergänzt Gnome um eine Leiste im Stil von Windows 10 und dürfte deshalb besonders Umsteigern entgegenkommen. Nun liegt eine neue Version vor, die sich an einen beliebigen Bildschirmrand anheften lässt.

Ein Standard-Gnome plus Gnome-Erweiterung Dash To Panel mit seinen neuen Optionen ähnelt der Gnome-Interpretation von Ubuntu (mit der Erweiterung Dash To Dock). Manche Anwender dürften Dash To Panel der Ubuntu-Lösung sogar vorziehen, weil Dash To Panel die Favoritenleiste mit dem normalen Systempanel platzsparend kombiniert. Und so gelingt die Einrichtung dieser und anderer Gnome-Erweiterungen über den vorinstallierten Browser Firefox:

1. Zuerst macht die Installation der angebotenen Firefox-Erweiterung von *https://extensions.gnome.org* oder auch von *https://addons.mozilla.org/en-US/firefox/addon/gnome-shell-integration* den Browser fit für die Gnome-Erweiterungen.

2. Gnome selbst braucht dann noch die neue Komponente „chrome-gnome-shell“, um Firefox einzubinden. Das gleichnamige Paket findet sich unter diesem Namen in den Standard-Paketquellen aller Linux-Distributionen mit Gnome und ist in Debian/Ubuntu beispielsweise mittels

```
sudo apt install chrome-gnome-shell
```

zu installieren.

3. Abschließend ist noch ein Neustart von Firefox notwendig, um ab jetzt die Gnome-Erweiterungen einfach per Klick von der Webseite *https://extensions.gnome.org/extension/1160/dash-to-panel* zu aktivieren. Nach der Installation von Dash To Panel können Sie die Erweiterung genauer konfigurieren.

Sonderfall Ubuntu: Falls Sie diese Lösung in Ubuntu (Gnome) integrieren, sollten Sie die andere, standardmäßig installierte Erweiterung deaktivieren. Dazu ist das Gnome-Optimierungswerkzeug nötig, das inzwischen in allen Distributionen schlicht Gnome-Tweaks („Optimierungen“) heißt und beispielsweise in Debian/Ubuntu mit dem Befehl

```
sudo apt-get install gnome-tweaks
```

installiert ist. In den Gnome-Tweaks gehen Sie dann auf „Erweiterungen“ und deaktivieren zunächst das „Dash to Dock“ mit einem Klick auf den Schalter. Anschließend gehen Sie auf das Zahnradsymbol neben „Dash to Panel“ und nutzen die Einstellungsmöglichkeiten. **-dw**

UBUNTU 19.10: CINNAMON ALS DESKTOP

Der Desktop Cinnamon ist nicht nur das Markenzeichen von Linux Mint, sondern hat über diese Distribution hinaus mit seinem klaren, klassischen Aufbau viele Freunde.

So gibt es eigene Ausgaben von Debian und Fedora mit Cinnamon-Desktop. Eine offizielle Ubuntu-Version mit Cinnamon fehlt allerdings.

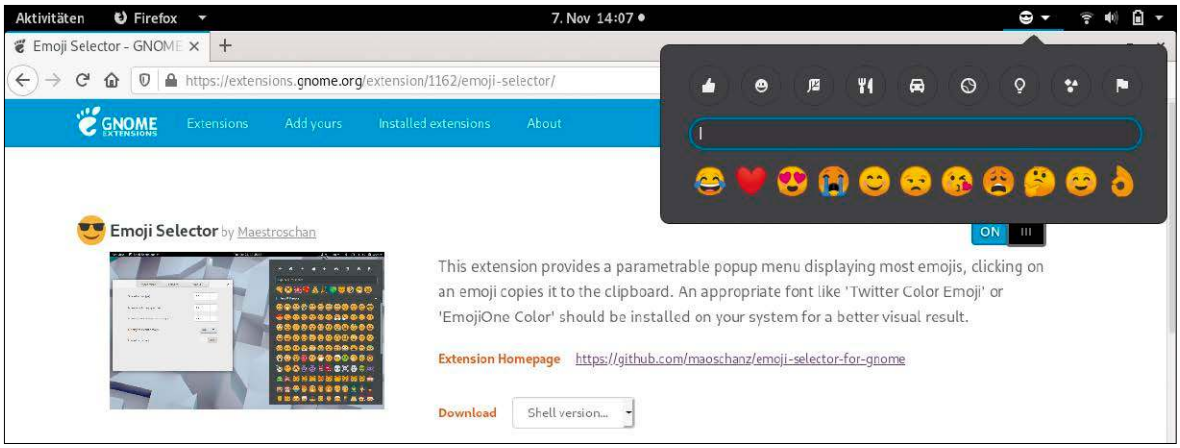
Wer Cinnamon anstatt des Gnome-Desktops im aktuellen Ubuntu 19.10 nutzen möchte, braucht nicht lange zu suchen. Das aktuelle Cinnamon 4.0 liegt in der Standard-Paketquelle „Universe“ zur nachträglichen Installation parallel zum Gnome-Desktop. Die Umgebungen kommen sich nicht in die Quere und stehen auf der Log-in-Seite zur alternativen Auswahl. In Ubuntu 19.10 installiert das Kommando

```
sudo apt install cinnamon-desktop-environment
```

die gesamte Desktopumgebung mit einigen Basisprogrammen, aber ohne die Mint-Tools, welche nur in den Mint-Paketquellen bereitstehen. Der zusätzliche Platzbedarf auf der Festplatte beträgt 1,3 GB und die Download-Datenmenge etwa 400 MB.

Cinnamon in Ubuntu 19.10: Die Standard-Paketquellen liefern Cinnamon in der neusten Version auch für Ubuntu. Mit dem installierten Gnome geraten die Pakete nicht in Konflikt.

Gnome: Emojis per Erweiterung



Bildchen im Überfluss: Auf dem Gnome-Desktop liefert der Emoji Selector die bunten Piktogramme in einer Bildschirmtastatur. Die Emojis funktionieren in den meisten Anwendungen.

Smileys in Ascii sind selten geworden. Stattdessen füllen bunte Emojis auch die Onlinekonversationen erwachsener Menschen. Wer einen Messenger, Twitter oder einen Client für andere soziale Netzwerke unter Linux verwendet, muss dem bunten Treiben nicht einfach nur zusehen, sondern kann per Gnome-Erweiterung massenhaft bunte Bildchen um sich werfen.

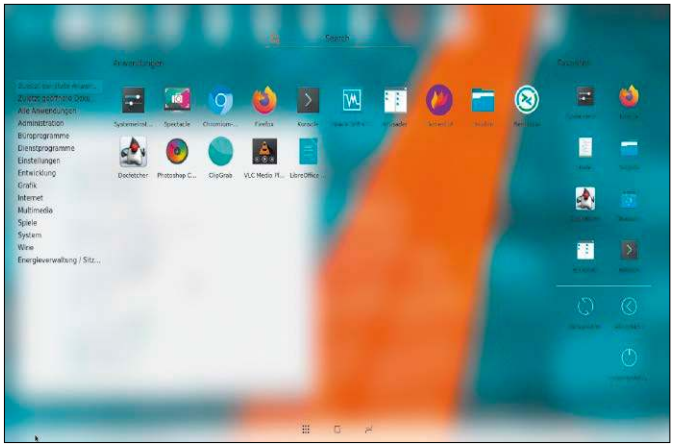
Die Erweiterung Emoji Selector für Gnome bringt eine kategorisierte und durchsuchbare Übersicht von Emojis im Stil von Whatsapp auf den Linux-Desktop. Wie auf einer Bildschirmtastatur lassen sich die bunten Piktogramme über die Zwischenablage in Texteditoren und Textfelder im Browser einfügen.

Vorbereitungen: Emojis sind im Zeichensatz UTF-8 enthalten und in den aktuellen Linux-Distributionen mit einem Font vertreten.

Dies lässt sich einfach testen. Ein Besuch der Webseite *http://eosrei.github.io/emojione-color-font/full-demo.html* präsentiert zur Demonstration eine Übersichtsseite in Firefox mit Emojis aus dem Font Emojione, der in vielen Linux-Systemen wie Ubuntu und Varianten (ab 18.04) vorinstalliert ist. Für andere Linux-Distributionen gibt es auf der Github-Webseite des Entwicklers unter *https://github.com/eosrei/emojione-color-font* ein „tar.gz"-Archiv für Linux, das ein Installations-Script („install.sh") und das dazugehörige De-Installations-Script („uninstall.sh") enthält. Klappt die Darstellung, so kann es zur Installation der Gnome-Erweiterung unter *https://github.com/maoschanz/emoji-selector-for-gnome* gehen. Wie sich in Firefox Gnome-Erweiterungen installieren lassen, zeigt der vorangegangene Tipp. Nach der Installation zeigt sich rechts oben im Panel ein Smiley, das die Emoji-Übersicht mit Suchfeld aufklappt. Ein Klick auf ein Emoji kopiert dieses in die Zwischenablage. **-dw**

KDE Plasma 5: Dashboard statt Menü

Auf kleineren Notebookbildschirmen erscheint das übliche Anwendungsmenü von KDE Plasma 5 klein und unübersichtlich. Das Plasma-Widget Navdexie für das KDE-Panel kann das Anwendungsmenü durch ein ganzseitiges Dashboard im Stil von Gnome ersetzen und dient zudem noch als Starter für konfigurierbare, häufig benötigte Anwendungen.



Übersichtsseite statt dem klassischen KDE-Menü: Das großzügige Dashboard von Navdexie macht sich auf kleineren Notebookbildschirmen besonders gut.

Ganz egal, welche Linux-Distribution zum Einsatz kommt, gelingt die Installation dieses KDE-Widgets ganz einfach über die KDE-Einstellungen. Nach einem Rechtsklick auf die KDE-Leiste geht es dort auf „Kontrollleiste-Optionen" und dann zu „Miniprogramme hinzufügen → Neue Miniprogramme holen → Neue Miniprogramme herunterladen". Dieser Menüpunkt stellt eine Verbindung zum Online-verzeichnis der KDE-Applets her und findet das Navdexie schnell über das Feld „Suchen".

Nach der Installation gehen Sie wieder zum Kontextmenüpunkt „Miniprogramme hinzufügen" der KDE-Leiste. In dessen Auswahl steht jetzt Navdexie zur Verfügung, das als eleganter Ersatz für das herkömmliche Menü dienen kann. Das erste Symbol zeigt ein Dashboard an, das zweite Symbol zeigt alle laufenden Anwendungen und das dritte Icon gibt den Blick auf den Desktop frei. Ein Rechtsklick erlaubt die weitere Konfiguration des Aussehens und Ergänzungen mit Programmverknüpfungen. **-dw**

XFCE: Zwischenablage mit automatischen Aktionen

Eine Spezialität der Desktopumgebung XFCE sind die Erweiterungen für das Panel, die der Arbeitsumgebung interessante Zusatzfunktionen und Abkürzungen entlocken. Eine der bemerkenswerten XFCE-Erweiterungen ist Clipman, eine Verwaltung für die Zwischenablage mit Automatisierungsfunktion.

Automatische Aktionen für die Zwischenablage können beispielsweise Programme ausführen oder den kopierten Inhalt der Zwischenablage umformen. Clipman kann dabei so konfiguriert werden, dass Aktionen durch eine erkannte Zeichenkette ausgelöst werden, die mittels regulären Ausdrücken definiert ist. Der mögliche Anwendungsbereich dieses Produktivitätswerkzeugs ist enorm breit und einfallsreiche Anwender werden nicht lange nach einem Einsatzzweck suchen müssen. Als ein Beispiel zeigen wir hier, wie Clipman dazu dient, Video-URLs zur Wiedergabe an den VLC-Player zu schicken.

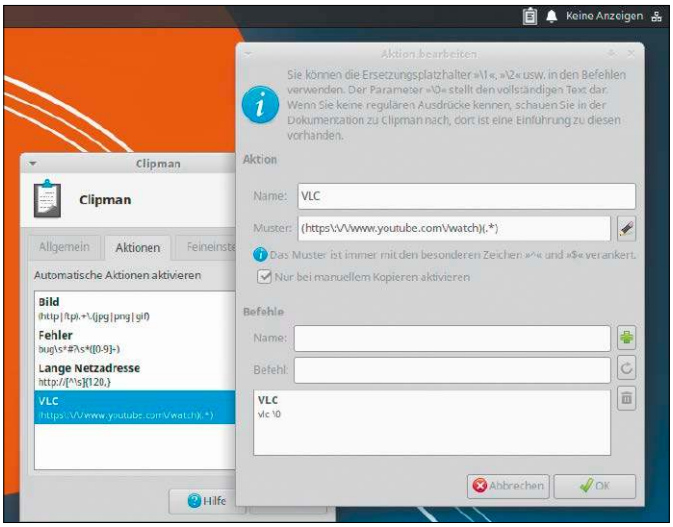
1. In Xubuntu und den meisten Linux-Distributionen ist Clipman nicht standardmäßig installiert. In Xubuntu rüstet das Kommando

```
sudo apt install xfce4-
  clipman
```

das nützliche Tool nach. Clipman muss zunächst manuell gestartet werden. Im XFCE-Menü ist es unter dem Namen „Zwischenablage“ vertreten.

2. Im Panel öffnet ein Rechtsklick auf das Clipboard-Symbol dessen Eigenschaften. Unter „Aktionen“ aktiviert der Schalter oben die gewünschten automatischen Aktionen, und das Plus-Zeichen erstellt eine neue Aktion, die wir im angezeigten Dialog gleich „VLC“ nennen. Vor die Option „Nur bei manuellem Kopieren aktivieren“ setzen wir einen Haken. In das Feld „Muster“ kommt dieser exakte Ausdruck:

```
(https\:\/\/www.youtube.
  com\/watch)(.*)
```



Clipman-Aktion: In diesem Beispiel tritt künftig beim Kopieren einer Youtube-URL in die Zwischenablage automatisch der VLC in Aktion.

Darunter muss nun im Abschnitt „Befehle“ in das Feld „Befehl“ jene Aktion, die ausgeführt werden soll. Hierhin kommt dieser Aufruf

```
vlc \0
```

und in das Feld „Name“ wiederum nur „VLC“. Ein Klick auf das untere Plus-Zeichen und dann auf „OK“ speichert die Aktion.

3. Sobald nun im Browser eine Youtube-URL mit Strg-C in die Zwischenablage kopiert wird, zeigt Clipman ein kleines Popfenster mit der Aktion „VLC“ an. Deren Auswahl startet den VLC-Player und spielt die kopierte Video-URL ab. **-dw**

XFCE: Screenshots vereinfachen

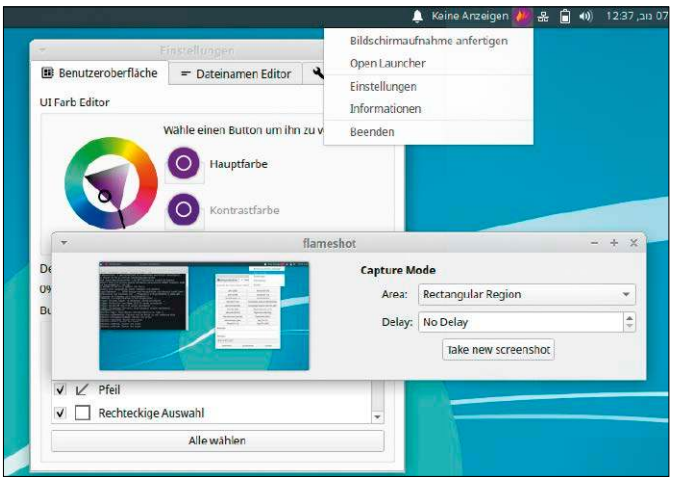
Unter XFCE holt die Druck-Taste das integrierte Screenshottool auf dem Bildschirm, das nur wenige Optionen und keine verzögerte Aufnahme mit Timer bietet. Wer häufiger Aufnahmen von Bildschirm und Programmfenstern macht, wird mit bei dieser stark vereinfachten Methode grundlegende Einstellungsmöglichkeiten vermissen.

Das Screenshottool Flameshot ist in den letzten Jahren zu einem der populärsten Programme dieser Art geworden und deshalb in den Paketquellen vieler Distributionen vorhanden. Der Vorteil von Flameshot ist, dass es ein eigenständiges Qt-Programm ist und unabhängig von der verwendeten Arbeitsumgebung ist.

Flameshot ist eines der wenigen Screenshot-Werkzeuge, die auch unter Wayland ihre Arbeit verrichten. Es kann den kompletten Bildschirm oder nur einen ausgewählten Teil davon aufnehmen und liefert einen Werkzeugkasten für Markierungen im Bild. In Debian (ab Version 10), in Ubuntu (ab Version 18.04), in Fedora und natürlich auch in Arch Linux ist Flameshot aus den Standardpaketquellen schnell installiert, in Debian/Ubuntu etwa mit diesem Kommando:

```
sudo apt install flameshot
```

Nach dem ersten Aufruf des Programms legt es ein Symbol in der Taskleiste der Desktopumgebung ab, das zur Steuerung und Konfiguration dient. Der Menüpunkt „Open Launcher“ ruft den Screenshotauslöser auf. **-dw**

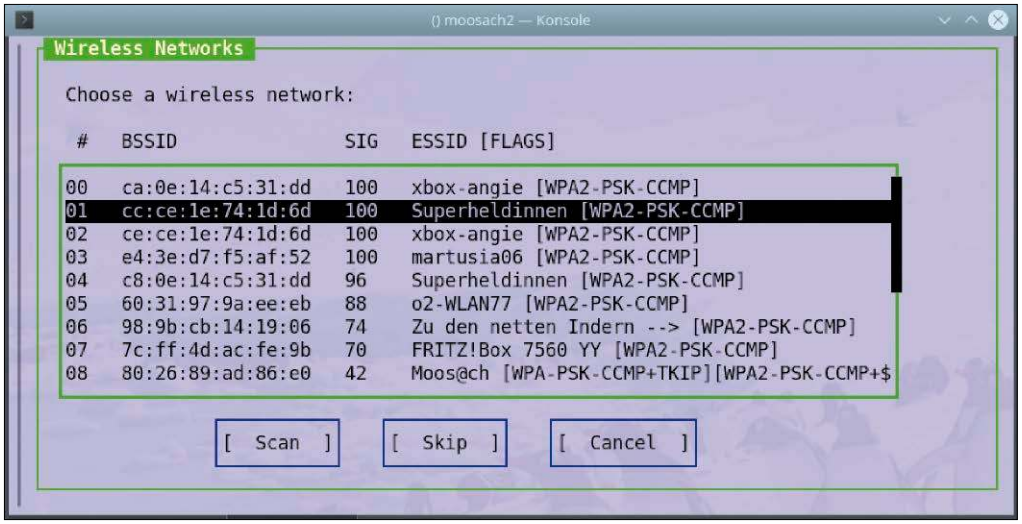


Bitte recht freundlich: Flameshot macht Bildschirmfotos komfortabel und kann auch mit dem neuen Displayserver Wayland unter Gnome und KDE umgehen.

Coole Konsole

Themen wie rekursives Umbenennen von Dateien und die Konfiguration eines WLAN in der Shell sind Dauerbrenner. Dazu stellen die Konsolentipps einen aufschlussreichen Netzwerkmonitor und ein Tool zum Stöbern in Verzeichnisbäumen vor.

Netzwerk: Verbindungen bearbeiten



Ab ins Netzwerk: Das textbasierte Ceni ist ein Konfigurationswerkzeug für Netzwerkschnittstellen und WLAN-Verbindungen auf Serversystemen ohne Desktop.

Auf Linux-Systemen wie dem Raspberry Pi, die vornehmlich als Server zum Einsatz kommen, läuft meist kein grafischer Desktop.
Während Ethernet-Verbindungen bei einem aktiven DHCP-Server im Netzwerk wenig mehr verlangen als ein angeschlossenes Netzwerkkabel, ist es ohne grafische Benutzeroberfläche kein Vergnügen, in der Kommandozeile eine WLAN-Verbindung aufzubauen. Einige textbasierte Tools helfen dabei, in wenigen Schritten ohne obskure Befehle ein Linux-System per Shell an einem WLAN anzumelden.
Mit Network-Manager: Auf einem Linux-System, das eigentlich für den Desktop gemacht ist, kümmert sich der Network-Manager um alle Netzwerkverbindungen.
Läuft die grafische Oberfläche nicht, so gibt es immer noch das textbasierte Tool

```
nmtui
```

zur Steuerung des Network-Managers über ein textbasiertes Menü in der Shell.
Ohne Network-Manager: Auf puren Linux-Serversystemen gibt es üblicherweise keinen Network-Manager. Die Kontrolle aller Netzwerkverbindungen erfolgt stattdessen über die Konfigurationsdatei „/etc/network/interfaces“ und das Start-Script „ifup“. Eine Konfiguration von WLAN-Verbindungen geht in dieser Konstellation viel einfacher mit dem Hilfsprogramm Ceni. Dieses Perl-Tool ist schon etwas älter, aber trotzdem erst kürzlich in die Paketquellen von Debian (Version 10) sowie Ubuntu (ab 19.04) aufgenommen worden und mit

```
sudo apt-get install ceni
```

installierbar. Danach startet

```
sudo ceni
```

das Programm zur Auswahl und Einrichtung der WLAN-Schnittstelle. Ceni erkennt übrigens, ob der Network-Manager läuft, und vermeidet damit einen Konflikt bei der Konfiguration der Netzwerkschnittstellen. `-dw`

Dateimanagement: Umfangreiche Kopieraktionen

Es scheint eine triviale Angelegenheit zu sein, große Mengen an Dateien mit mehreren Hundert GB Umfang unter Linux in einer Kopieraktion von einem Laufwerk A auf ein Laufwerk B zu schaufeln. Tatsächlich sind aber grafische Dateimanager der Aufgabe oft nicht gewachsen, wenn es um viele Tausend Dateien und Verzeichnisse geht. Am zuverlässigsten arbeitet immer noch ein alter Bekannter in der Kommandozeile.
Das Programm Rsync ist als Synchronisationswerkzeug für seine Netzwerkfähigkeiten bekannt, aber es arbeitet genauso gut mit lokalen Datenträ-

gern. Der Vorteil gegenüber anderen Befehlen und Programmen: Es macht auch bei größten Datei- und Datenmengen nicht schlapp, kann unterbrochene Kopieraktionen zu einem späteren Zeitpunkt wiederaufnehmen und – anders als die schlichten Kommandozeilentools cp oder mv – zeigt es auf Wunsch eine Fortschrittsanzeige. Letztes ist gerade bei lang andauernden Kopieraktionen ein Muss.

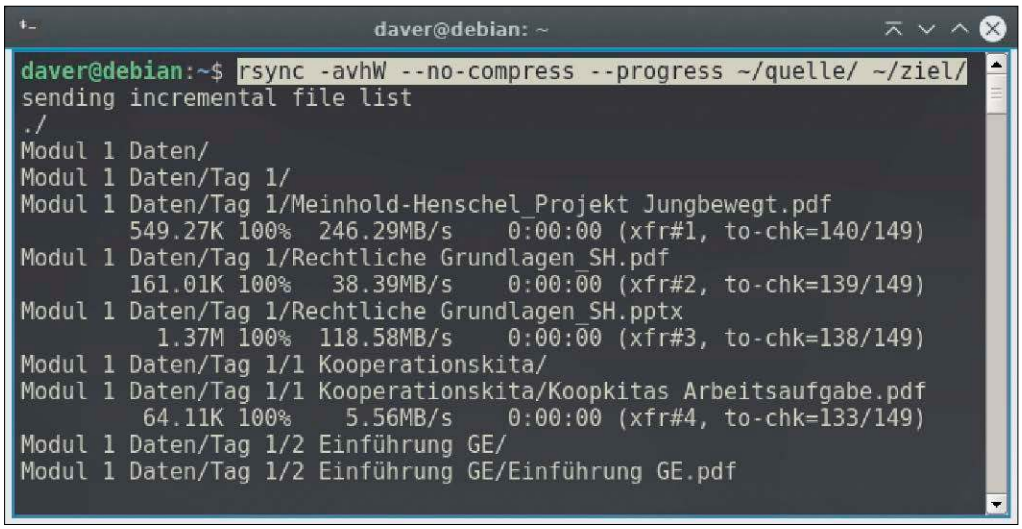
Die Befehlssyntax von Rsync unterscheidet sich beim Einsatz auf lokalen Datenträgern nicht erheblich von Aktionen über eine Netzwerkverbindung – statt einem Hostnamen und Datenträgerpfad werden einfach nur die Pfade von Quell- und Zielordner angegeben:

```
rsync [Optionen] [Quelle]
  [Ziel]
```

Soweit keine Überraschungen. Ausschlaggebend sind aber die angegebenen Optionen, damit Rsync als Kopierwerkzeug für ganze Verzeichnisbäume auch das tut, was es soll. Besonders wichtig ist dabei, mit der Option „--inplace" zu unterbinden, dass Rsync die Kopie einer übertragenen Datei zunächst als Kopie am Ziel anlegt. Dies wäre das Standardverhalten für den Einsatz im Netzwerk, führt aber bei sehr vollen Datenträgern zu Platzproblemen. Außerdem ist bei lokalen Operationen ein Komprimieren der Daten während der Übertragung unnötig. So ergeben sich insgesamt folgende Optionen:

```
rsync -avhW --no-compress
  --progress [Quelle]/
  [Ziel]/
```

Dies kopiert den Inhalt der Quelle samt aller Unterordner, Symlinks und Zugriffsrechten in das Zielverzeichnis. **-dw**



Korrekt kopiert: Rsync ist als Multitalent nicht nur zur Dateiübertragung im Netzwerk wichtig. Auch beim Kopieren umfangreicher lokaler Verzeichnisse ist es verlässlicher Helfer.

Iftop: Wohin geht die Brandbreite?

Lahmt ein Server im Netzwerk, so liegt das entweder an der Systemlast oder der Netzwerklast. Während eine hohe Systemlast und die dafür verantwortlichen Prozesse schnell ausgemacht sind, gelingt dies bei der Zuordnung der Netzwerkauslastung nicht so einfach.

Die Kombination zweiter Kommandozeilentools kann die Verursacher einer hohen Netzwerklast präzise ermitteln.

1. Wer oder was verantwortet die Auslastung? Welches Programm oder welcher Serverprozess auf einem Linux-System wie viel Netzwerkverkehr verursacht, entschlüsselt das Tool Nethogs. Es listet den Netzwerkverkehr pro laufendem Prozess auf und zeigt dazu Programmname und das jeweilige Benutzerkonto an, unter welchem der Prozess läuft. Nethogs beginnt ab dem Aufruf mit der Protokollierung und zeigt den aktivsten Prozess am Anfang der Auflistung an.

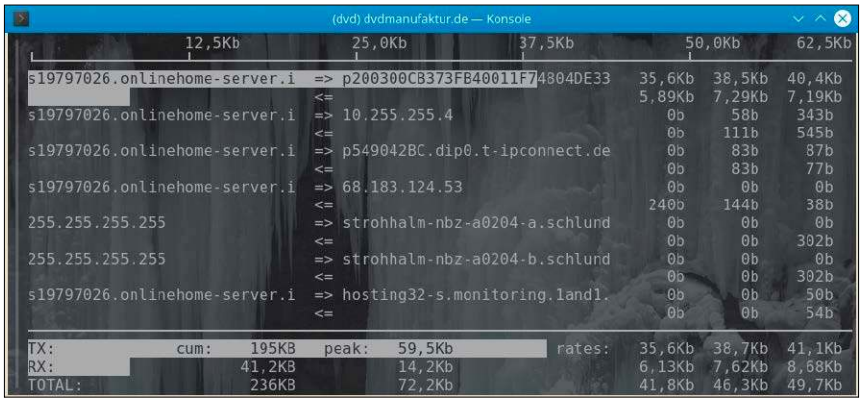
Das Tool ist unter Debian, Ubuntu und Fedora flott über den Paketmanager installiert und benötigt zum Aufruf auf der Kommandozeile root-Berechtigung oder ein vorangestelltes „sudo":

```
sudo nethogs
```

2. Woher kommt der Traffic, wohin geht er? Während Nethogs klärt, welcher Prozess Netzwerkpakete sendet und empfängt, ermittelt das Tool Iftop, welche IP-Adressen beziehungsweise Hostnamen den meisten Netzwerkverkehr erzeugen. Auf einem System im LAN ist dies eine lokale IP-Adresse, auf einem Server im Internet eine öffentliche Adresse. Das Programm liegt mit Paketnamen „iftop" in den Standard-Paketquellen nahezu aller Linux-Distributionen und wird mit root-Rechten

```
sudo iftop
```

gestartet. **-dw**



Verbindungen mit Iftop nach Adressen aufschlüsseln: Das Tool analysiert den Netzwerkverkehr und zeigt in der sortierten Liste an, welche Gegenstelle die meisten Daten überträgt.

Dateinamen: Alles klein gemacht

Die in Linux gebräuchlichen Dateisysteme unterscheiden alle zwischen Groß- und Kleinschreibung. Um die Sache zu vereinfachen, sind unter Linux generell Datei- und Ordnernamen in Kleinbuchstaben üblich, um die Sache zu vereinfachen. Dateien von FAT16/FAT32-Datenträgern, etwa von Digitalkameras, liegen aber meist in Großbuchstaben vor.
Es gibt in der Shell etliche Möglichkeiten, alle Dateien in Ordnern und Unterordnern umzubenennen und mit Namen in Kleinbuchstaben zu versehen. Eine besonders geradlinige Methode liefert das Kommandozeilenwerkzeug Convmv, das sich generell dazu eignet, Dateinamen von einem Zeichensatz in einen anderen zu konvertieren.
Es ist in den Paketquellen aller Linux-Distributionen vorhanden und in Debian/Ubuntu mit dem Befehl

```
sudo apt-get install
  convmv
```

schnell installiert. Um alle Datei- und Verzeichnisnamen im aktuellen Ordner und Unterordnern mit Kleinbuchstaben zu versehen, genügt der Aufruf

```
convmv --lower -r --notest
  .
```

Der abschließende Punkt ist die Pfadangabe für den aktuellen Ordner. Statt der Option „--lower“ kann „--upper“ auch Namen in Großbuchstaben erzeugen.
Fehlt die Angabe „--notest“, so macht das Tool keine aktiven Änderungen, sondern zeigt diese in einem Testlauf an. **-dw**

Texteditoren: Zeilennummern anzeigen

Die verbreiteten Editoren in der Shell sind Nano unter den Linux-Distributionen, die von Debian abstammen, sowie Vim unter Red Hat, Cent-OS und Fedora.
Nano hat den Ruf, leichter verständlich in der Bedienung zu sein, während Vim in den Händen gewandter Administrationen enorm effizient ist. Welchen Editor man in der Shell auch bevorzugt: Vieles wird einfacher mit eingeblendeten Zeilennummern.
Beide Editoren können Nummern vor den jeweiligen Zeilen einer geöffneten Textdatei einblenden. Allerdings wartet diese nützliche Ergänzung, welche die Orientierung in Dateien erleichtert, noch auf ihre Aktivierung.
Nano: In diesem Editor sind Zeilennummern bei Bedarf über eine Tastenkombination schnell ein- und ausgeschaltet. Nach dem Druck auf die Alt-Taste zusammen mit dem Zeichen „#“ zeigt Nano links am Rand Zeilennummern an und blendet sie über die gleiche Kombination auch wieder aus. Soll Nano immer mit aktivierten Zeilennummer starten, dann hilft eine zusätzliche Zeile in der Konfigurationsdatei des Editors. Der Befehl

```
nano ~/.nanorc
```

öffnet die Datei und die Zeile

```
set linenumbers
```

schaltet permanent Zeilennummern ein.
Vim: Als Urzeitwesen aus Unix-Tagen mit stetiger Evolution hat Vim (kurz für „Vi improved“) eine große Gefolgschaft gewonnen, obwohl der Editor alles andere als einsteigerfreundlich ist. In Linux-Distributionen für den professionellen Einsatz als Server ist Vim aber nach wie vor Standard. Zeilennummern zeigt Vim im Kommandomodus (Eingabe von „:“) über den Befehl

```
set number
```

an. Auch hier gibt es selbstverständlich die Option, diese Funktion permanent in einer Konfigurationsdatei zu setzen. Das Kommando

```
vim ~/.vimrc
```

öffnet beziehungsweise erstellt die Datei, in welcher dann die Zeile „set number“ die gewünschte Option dauerhaft setzt. **-dw**

Nummerierte Zeilen machen jeden Editor freundlicher: Sowohl der Klassiker Vim als auch Nano kennen eine Option, Zeilennummern einzublenden.

Dateisystem: Verzeichnisbäume mit Ytree

Wo ist was? Und wie viel ist hier gespeichert? In der Kommandozeile fällt die Orientierung im Dateisystem neuer oder fremder Systeme und auf üppig belegten Datenträgern nicht einfach. Das Tool Ytree sorgt im Handumdrehen für Übersicht.
Ausgehend vom aktuellen Verzeichnis zeigt das Konsolenprogramm Ytree die enthaltenen Ordner in einer Baumstruktur an. Diese erfolgt aber nicht als statische Ausgabe im Terminal, denn Ytree erlaubt die Navigation durch Verzeichnisbäume mit den Pfeiltasten. Das Programm ist, wie der Name nahelegt, an das altehrwürdige DOS-Programm xtree angelehnt. Es ist nützlich und intuitiv, aber in Linux-Systemen nicht vorinstalliert. Die verbreiteten Linux-Distributionen haben es aber in ihren Standard-Paketquellen, sodass es schnell nachinstalliert ist. In Debian, Ubuntu & Co erledigt das dieser Befehl

```
sudo apt-get install ytree
```

und in Fedora das folgende Kommando:

```
sudo dnf install ytree
```

Der Aufruf *ytree* ohne Parameter präsentiert die Verzeichnis- und Dateistruktur unterhalb des aktuellen Ordners. Ein Druck auf die Pfeil-auf- und Pfeil-ab-Tasten navigiert den Cursor durch die Unterverzeichnisse. Mit der Pfeil-nach-rechts-Taste öffnet man den aktuell markierten Unterordner. Über die Eingabetaste gelangt man in den Dateibrowser, der im unteren Drittel der Ausgabe zu sehen ist. Der Bereich rechts zeigt die Gesamtgröße der Dateien im Unterverzeichnis an. Die Dateioperationen am unteren Bildschirmrand erlauben über den Druck der hervorgehobenen Buchstaben das Kopieren, Verschieben, Umbenennen, Löschen und Änderung von Zugriffsrechen. Mit der Escape-Taste wechselt der Cursor zurück zur Navigation in den Verzeichnisbaum und Taste „Q“ beendet Ytree. **-dw**

Hilfen zur Hardware

In den Hardwaretipps geht es darum, Lenovo-Thinkpads die Zusammenarbeit mit Akkus fremder Hersteller beizubringen. Außerdem behandeln wir Probleme mit dem Nvidia-Treiber im neuen Ubuntu und leidige WLAN-Aussetzer, deren Ursache oft simpel ist.

Lenovo-Thinkpads: Alle Akkus akzeptieren

Auch optimale Behandlung eines Li-Ion-Akkus kann den Kauf eines Ersatzakkus nur aufschieben. Notebookakkus altern und verlieren über die Jahre stetig an Kapazität. Nach rund zwei bis drei Jahren oder rund 750 bis 1000 Lade-Entlade-Zyklen hat auch ein sorgfältig gepflegter Akku seine Lebenserwartung erreicht und wird kaum noch Energie speichern.

Für ältere Notebooks sind Originalakkus des Herstellers häufig sehr teuer, während Nachbauten recht günstig sind und oft sogar höhere Kapazitäten haben. Ausgerechnet bei einigen sehr beliebten Thinkpad-Modellen, auf welchen Linux tadellos läuft, lässt Lenovo über die Firmware nur originale Akkus zu.

Betroffen vom Ausschluss fremder Akkus per Firmware sind die Thinkpad-Modelle T430, T430s, T530, T530i, W530, X230, X230t, L430, L530 und E330. Nach dem Einlegen eines Akkus eines anderen Herstellers als Lenovo wird die Lade-LED des Thinkpads nur einen Batteriedefekt anzeigen. Langjährige Thinkpad-Fans, darunter viele Entwickler und IT-Profis, sind von dieser empfindlichen Einschränkung natürlich wenig begeistert. Ein Hardwareentwickler hat per Decompiler die Firmwaredateien der betroffenen Thinkpad-Modelle analysiert und jeweils einen Patch für die Firmware der Geräte entwickelt, welche unter anderem die Überprüfung auf erlaubte Originalakkus entfernen kann.

Der Patch funktioniert bei den Thinkpad-Modellen T430, T430s, T530, T530i, W530, X230 und X230t. Lenovo hat von diesem Patch natürlich Wind bekommen und in neueren Bios-Versionen weitere Hürden wie eine Codesignatur für die Firmware eingebaut, um Firmwarepatches zu unterbinden. Mit älteren Bios-Versionen (siehe Tabelle „Patch für Thinkpads: Erlaubte Bios-Versionen“) funktioniert der angebotene Patch in seiner jetzigen Ausgabe aber immer noch. Der Patch liegt auf Github und verlangt ein Linux-System zum Kompilieren der neuen Firmware, die dann als ISO-Datei auf einen bootfähigen USB-Stick kommt. Mit dem Booten des Sticks wird der Patch dann einfach als Firmwareupdate auf das Thinkpad aufgespielt.

Kein feiner Zug: Lenovo stattete die Firmware neuerer Thinkpads mit einer Liste erlaubter Akkus aus. Akkus fremder Hersteller werden von diesen Geräten nicht akzeptiert.

1. Zum Kompilieren verlangt das System einige Entwicklerpakete, die in Debian, Ubuntu, Linux Mint über den Befehl

```
sudo apt install build-
  essential git mtools
  libssl-dev
```

installiert werden. In Fedora und Cent-OS richtet das Kommando

```
sudo dnf install git
  mtools openssl-devel
sudo dnf group install "C
  Development Tools and
  Libraries"
```

alle benötigten Pakete ein.

2. Nun holt man die neueste Version des Quellcodes für den Patch mit

```
git clone https://github.
  com/hamishcoleman/
  thinkpad-ec
```

auf den eigenen Computer. Dabei legt der Git-Befehl ein neues Unterverzeichnis für alle Dateien an, in das nun das Kommando

```
cd thinkpad-ec
```

wechselt.

3. Eine Liste aller Thinkpad-Modelle, die der Patch unterstützt, zeigt hier der Befehl

```
make list_laptops
```

an. Der Patch für das Entfernen der Akkuliste ist standardmäßig nicht aktiv. Erst der Befehl

```
make patch_enable_battery
  clean
```

aktiviert diesen Teil des Patches.

4. Jetzt gilt es, den passenden Patch für das Thinkpad-Modell zu bauen. Handelt es sich bei dem Zielgerät beispielsweise um ein Thinkpad X230, so lautet das Kommando dafür

```
make patched.x230.img
```

5. Die resultierende IMG-Datei ist nun der bootfähige Firmwa-

PATCH FÜR THINKPADS: ERLAUBTE BIOS-VERSIONEN

Modell	Letzte patchbare Bios-Version
T430	Bios 2.81
T430s	Bios 2.81
T530,	Bios 2.76
T530i	Bios 2.76
W530	Bios 2.75

Modell	Letzte patchbare Bios-Version
X230	Bios 2.76
X230t	Bios 2.73
L430	kein Patch möglich
L530	kein Patch möglich
E330	kein Patch möglich

Unterstützte Thinkpads: Der vorliegende Patch funktioniert bei jedem Modell nur bis zu einer bestimmten Bios-Version, mit einem neueren Bios jedoch nicht mehr.

repatch für das ausgewählte Thinkpad-Modell. Diese Datei wird jetzt mit dd auf einen USB-Stick geschrieben:

```
sudo dd if=patched.x230.
  img of=/dev/sdc
```

Das Beispiel geht davon aus, dass der USB-Stick die Laufwerkskennung „/dev/sde“ hat. Hier darf kein Fehler passieren, um nicht versehentlich ein anderes Laufwerk zu überschreiben. Eine Liste aller Laufwerke zeigt der Befehl lsblk an.

6. Das Thinkpad wird nun mit dem USB-Stick gebootet und der Patch zeigt eine Informationsseite an, die auch den Abbruch erlaubt, falls das Modell wider Erwarten doch nicht passen sollte. Nach der Bestätigung, dass alles seine Richtigkeit hat, bootet das Thinkpad noch einmal und aktualisiert dann die Firmware. Danach akzeptieren die unterstützten Modelle auch Akkus von anderen Herstellern. **-dw**

Ubuntu: Probleme mit Nvidia-Treibern

Die Open-Source-Treiber für Nvidia-Chips im Linux-Kernel hinken leistungstechnisch den proprietären Nvidia-Treibern weit hinterher und reichen für Spiele nicht aus. Die meisten Anwender werden also zuerst die Nvidia-Treiber nachinstallieren, die in Ubuntu und Co. über die „Zusätzlichen Treiber“ unter „Anwendungen & Aktualisierung“ bereitstehen. Mit einigen Nvidia-Grafikkarten bleibt der Bildschirm ab dem Systemstart jedoch schwarz oder hängt in einer Schleife beim Laden des Log-in-Bildschirms fest.

Ab Ubuntu 19.04 kann schon der Installer die Nvidia-Treiber während der Installation einrichten, wenn dort die Option „Install third-party software for graphics and Wi-Fi hardware and additional media formats“ aktiviert ist

Ubuntu 19.10 liefert die Nvidia-Treiber sogar schon direkt auf den Installationsmedien mit, sodass zur Einrichtung der Treiber nicht mal mehr eine Internetverbindung notwendig ist.

Bei einigen Nvidia-Karten wird Ubuntu aber mit den proprietären Treibern seit Version 19.04 nicht mehr bis zum grafischen Desktop kommen. In diesem Fall ist es notwendig, das System stets mit der Kernel-Option „nomodeset“ zu booten:

1. Die Tastenkombination Strg-Alt-F2 springt von einem dunklen Bildschirm oder von der Log-in-Schleife auf die Textkonsole.

Hier gilt es nun, einen neuen Bootparameter in den Grub-Bootloader zu schreiben. Dazu öffnen Sie die Konfigurationsdatei „/etc/default/grub“ mit root-Privilegien, beispielsweise mit dem Editor nano:

```
sudo nano /etc/default/
  grub
```

2. In der Datei ist nur die Zeile „GRUB_CMDLINE_LINUX_DEFAULT=“ interessant, welche die Bootparameter angibt. Die vorhandenen Parameter in Anführungszeichen müssen um die Angabe „nomodeset“ ergänzt werden, sodass dort dann beispielsweise Folgendes steht:

```
"GRUB_CMDLINE_LINUX_
  DEFAULT="quiet splash
  nomodeset""
```

3. Damit ist die neue Option aber noch nicht aktiviert. Vor dem Neustart ist es noch nötig, den Bootloader mit dem Kommando

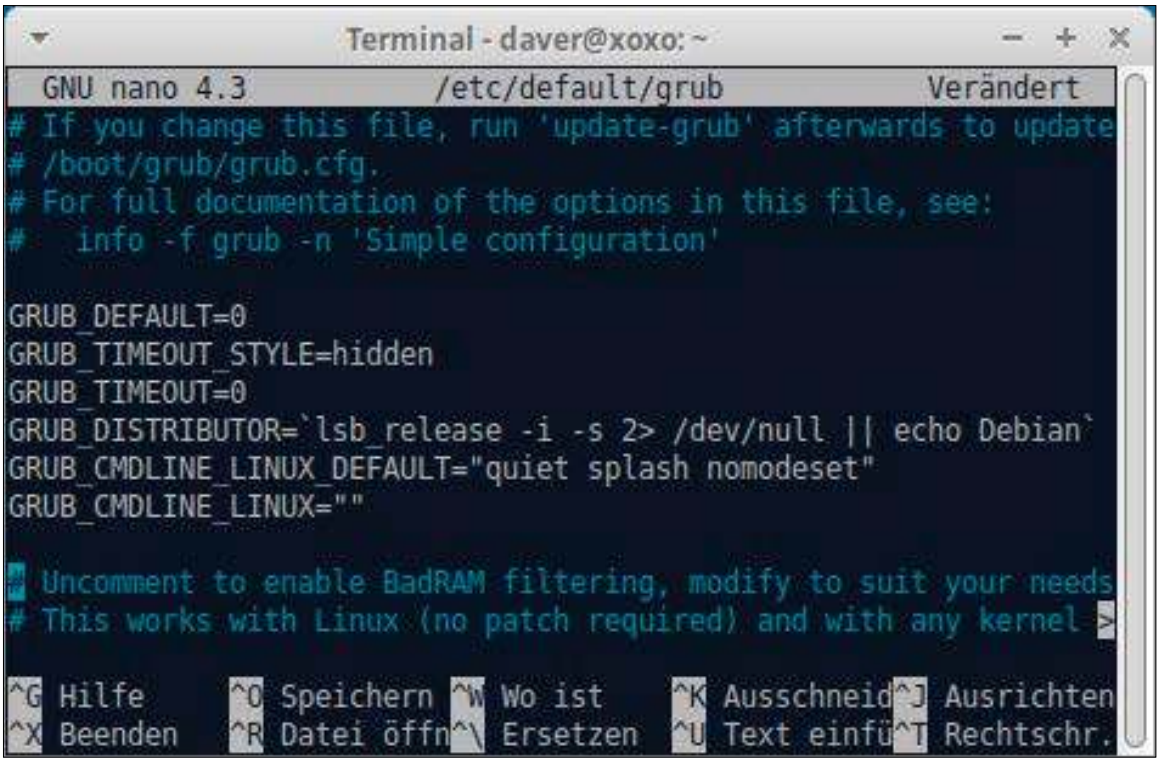
```
sudo update-grub2
```

zu aktualisieren.

4. Achtung Gnome!: Der Log-in-Manager GDM3 ist in Ubuntu 19.10 ebenfalls dafür bekannt, Probleme in der Kombination mit dem Nvidia-Treiber zu bereiten. GDM3 kann aber über den Paketmanager mit dem Befehl

```
sudo apt install lightdm
```

gegen den älteren und unproblematischen Lightdm ausgetauscht werden. **-dw**



Vorsicht mit proprietären Nvidia-Treibern: Bei einigen Nvidia-Grafikkarten startet Ubuntu 19.10 nicht mehr und verlangt die Ergänzung der Option „nomodeset“ in der Grub-Konfiguration.

Fehlersuche: Notebook ohne WLAN

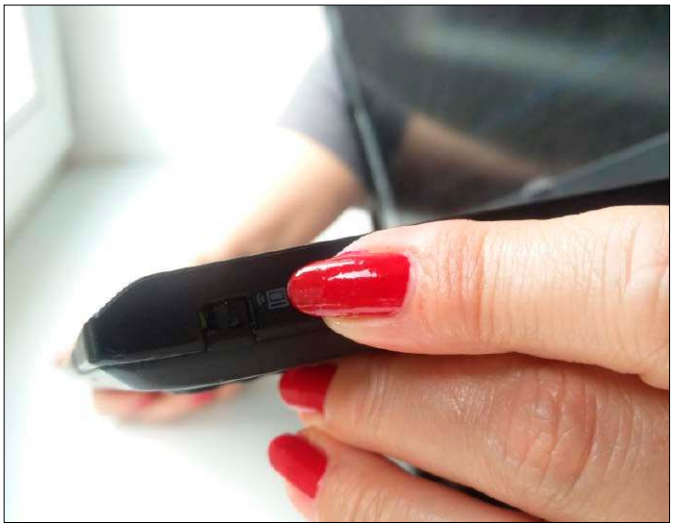
Dieses Problem ist ein echter Klassiker und sorgt immer wieder für Irritation: Unvermittelt scheint der WLAN-Chip eines Notebooks ausgefallen zu sein und der Network-Manager des Linux-Systems zeigt keine WLAN-Schnittstelle mehr an. Die Lösung ist oft trivial, wenn man an der richtigen Stelle sucht.

Alle Notebooks erlauben es, den WLAN-Sender abzuschalten, etwa um das Gerät auch an Bord eines Flugzeugs während Start und Landung zu betreiben. Moderne Notebooks bieten eine Tastenkombination, meistens in Verbindung mit einer der FN-Tasten, um den WLAN-Chip treiberseitig zu deaktivieren. Ältere Laptops und Notebooks für den professionellen Einsatz haben aber auch einen Hardwareschalter, der meist ganz unscheinbar an der Seite des Gehäuses untergebracht ist. Zuerst muss man im Fall eines unbekannten Notebooks das Gehäuse oder das Benutzerhandbuch nach einem WLAN-Schalter absuchen. Meist ist das Problem dann schon gelöst.

Es kommt bei wenigen WLAN-Chips vor, dass ein Abschalten per Hardwareschalter auch gleich ein Deaktivieren per Treiber nach sich zieht. Auch nach dem Einschalten bleibt der WLAN-Sender trotzdem softwaremäßig blockiert. Klarheit darüber, ob und wie ein WLAN-Chip blockiert ist, verschafft das Kommandozeilentool rfkill, das nach der Eingabe des Befehls

```
rfkill list all
```

in einem Terminalfenster den Status aller Sender (WLAN und Bluetooth) ausgibt. Es gibt dabei zwei Typen von Blockaden: Die häufigere „Soft blocked: yes“ bedeutet, dass der Sender per Software, etwa über den Network-Manager, abgeschaltet ist.



Es gibt mehr als eine Möglichkeit, den WLAN-Chip eines Notebooks lahmzulegen. Zunächst sollte immer nach einem unscheinbaren Hardwareschalter am Gehäuse gesucht werden.

Mit dem Kommando

```
sudo rfkill unblock all
```

können Sie diese Blockade für alle Sender aufheben. **-dw**

Bildschirmorientierung: Hardwaresensor aktivieren

Notebooks mit frei drehbarem Display sind keine Seltenheit mehr. Diese Geräte erlauben dann nicht nur den üblichen Einsatz als „Reiseschreibmaschine“, sondern auch als Tablet. Ein Hardwaresensor ermittelt dabei die Ausrichtung und dreht den Bildschirminhalt passend mit, wenn das Notebook wie ein Tablet hochkant gehalten wird. Das funktioniert mittlerweile auch mit Linux und dem Gnome-Desktop ganz ordentlich.

Damit das Linux-System die Bildschirmorientierung korrekt ermittelt und den Gnome-Desktop bei Bedarf passend zur Ausrichtung dreht, ist ein Treiber für den Hardwaresensor Voraussetzung. Dieser Treiber wird nicht automatisch in allen Linux-Distributionen beziehungsweise deren Ausgaben mitinstalliert. Das Paket „iio-sensor-proxy“ mit diesem Treiber findet sich aber in den Standard-Paketquellen aller verbreiteten Distributionen. In Debian und Ubuntu ist es mit

```
sudo apt install iio-
  sensor-proxy
```

nachgerüstet. In Fedora, das sich mit seinem stets sehr frischen Kernel und der aktuellen Gnome-Version ausgezeichnet für x86-Tablets eignet, lautet der Befehl so:

```
sudo dnf install iio-
  sensor-proxy
```

Anschließend aktiviert das Kommando

```
systemctl start iio-
  sensor-proxy.service
```

den Systemdienst zur Überwachung des Accelerometers zur Bildschirmorientierung. Einen Test, ob der Hardwaresensor erkannt wurde, erlaubt die Eingabe dieses Kommandos:

```
udevadm info --export-db
```

Linux mit Gnome auf x86-Tablets: Moderne Distributionen wie Fedora 31 machen sich gut auf Convertibles wie hier dem Lenovo Miix 320 und können auch den Bildschirm passend drehen.

Hier sollte dann eine Liste von Eigenschaften des Accelerometers erscheinen. **-dw**

Software, Tipps und Tools

Animierte GIFs, wie sie allenthalben als ironische Antwort auf Twitter zu sehen sind, kann das Programm Gifcurry bequem erstellen. Außerdem geht es um neue GPG/PGP-Schlüsselserver für Thunderbird und auch Libre Office kommt nicht zu kurz.

Grafikbearbeitung: Animierte GIFs erstellen

Das Format GIF stammt ursprünglich von Compuserve und wurde als gebräuchliches Grafikformat im Web längst von PNG-Dateien abgelöst. Es gibt aber eine Nische, in der sich GIFs weiterhin halten: Als animierte Grafiken auf Twitter sind GIFs weiterhin verbreitet. Unter Linux ist es auch kein großes Problem, solche Minianimationen zu erstellen.

Mit dem Open-Source-Programm Gifcurry, das als grafisches Front-End für Ffmpeg und Imagemagick arbeitet, sind animierte GIFs mit wenigen Klicks aus regulären Videodateien erstellt. Gifcurry erlaubt dabei die Angabe eine Anfangs- und Endpunkts, die Definition der Animationsqualität, der Auflösung und die Überlagerung mit einem Schriftzug. Generell sollten animierte GIFs klein bleiben und es empfiehlt sich, mit eher niedrigen Qualitätseinstellungen zu experimentieren.

Gifcurry ist ein kleines Tool, das im Hintergrund auf andere Programme für die Konvertierungsschritte setzt. Der Entwickler hat deshalb Gifcurry und alle Abhängigkeiten zu einem Appimage-Container zusammengebaut, der die Installation unter Linux sehr einfach macht. Die einzige Vorbereitung, die das Linux-System braucht, ist die Installation des Pakets „ffmpeg" aus dessen Paketquellen.

Bewegte Bilder: Animierte GIF-Dateien sind zwar kein effizientes Videoformat, dafür aber für kleine Clips auf Twitter und Co. ideal. Gifcurry erstellt solche GIFs aus Videodateien.

Universelles Appimage: Die stets neueste Version des Programms findet sich auf der Github-Seite des Entwicklers unter *https://github.com/lettier/gifcurry*. Das Appimage für Linux gibt es nur in 64 Bit. Nach dem Download der gewünschten Version macht das Kommando

```
chmod +x [Datei].AppImage
```

die Datei ausführbar und

```
./[Datei].AppImage
```

startet das Programm.

Snap-Installation in Ubuntu: Gifcurry ist auch im Snap Store angekommen und als Snap-Container in Ubuntu und seinen Varianten mittels

```
sudo snap install gifcurry
```

mit allen seinen Abhängigkeiten installiert.

Nach dem Start präsentiert das Programm eine (englischsprachige) Eingabemaske zur Auswahl der gewünschten Videodatei und spielt diese ab. Die Regler darunter sind die Schnittwerkzeuge zur Auswahl der Start- und Stoppzeit. Alle Einstellungen wie Größe („Size"), Bildausschnitt („Crop") und Ausgabedatei („File") befinden sich in der linken Seitenleiste.

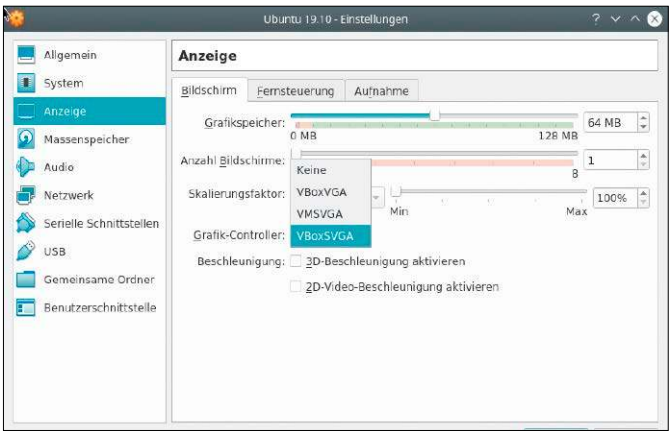
Gifcurry 6.0.0: Konvertiert Videos in animierte GIFs, Open Source, Download als universelles Appimage unter *https://github.com/lettier/gifcurry/releases* (40 MB). **-dw**

Virtualbox: Virtuelle Grafikkarte auswählen

Seit Version 6.x präsentiert der Hypervisor von Virtualbox drei Optionen, um einen virtuellen Grafikadapter zu emulieren: VMSVGA, Vbox VGA und Vbox SVGA. Der Menüpunkt dafür befindet sich in den Einstellungen einer virtuellen Maschine unter „Anzeige → Grafik Controller". Die Standardeinstellung „VMSVGA" ist nicht für alle Gastsysteme ideal.

Die Standardeinstellung „VMSVGA" bietet die beste Kompatibilität für alle älteren Betriebssysteme, egal ob Windows, Linux, BSD oder Exoten. Dieser

Grafikadapter ist für virtuelle Maschinen ideal, die von Vmware übernommen wurden und bereits die Vmware-Gasttreiber installiert haben. Allerdings sind die Leistung und die maximale Auflösung nicht die beste. Eine bessere Einstellung für alle frisch installierten Gastsysteme ab Windows 7 beziehungsweise für aktuelle Linux-Systeme ermöglicht der Grafikcontroller „VboxSVGA“. Denn dieser Controller erlaubt den Gastsystemen auch ohne Treiber höhere Auflösungen als 1024 x 786, arbeitet aber auch mit den optionalen Virtualbox-Gasttreibern („Guest Additions“) perfekt zusammen, um die Auflösung des Gasts auch dynamisch anzupassen. **-dw**



Grafikcontroller auswählen: Virtualbox kann mehrere Grafikkarten emulieren. Die Standardeinstellung ist für Linux-Gäste nicht ideal, „VboxSVGA“ macht sich oft besser.

Libre Office Calc: Aktuelles Datum markieren

In einer Tabelle mit chronologischen Kalenderdaten soll immer das aktuelle Datum hervorgehoben sein. Nützlich ist das beispielsweise für Anwesenheits- und Besucherlisten.

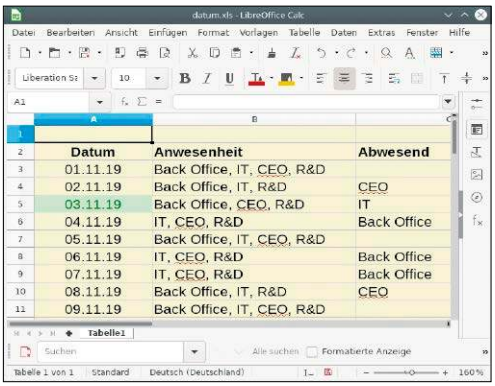
Zur Hervorhebung von Zellen anhand von Berechnungen oder dynamischer Daten dienen in Libre Office Calc die bedingten Formatierungen.

Der Abgleich einer Zeile mit Datumseinträgen mit dem aktuellen Datum zur Hervorhebung ist eine der einfacheren Übungen:

1. Mit der Maus markieren Sie die gesamte Datumsspalte oder Reihe, die vom Datentyp her als Datum ausgewiesen sind. Der Datentyp ist mit „Format → Zahlenformat → Datum“ schnell korrigiert – falls nötig.

2. Mit den weiterhin markierten Datumseinträgen geht es jetzt auf den Menüpunkt „Format → Bedingte Formatierung → Datum“.

3. Im angezeigten Dialog ist es jetzt einfach, Bedingungen zur Formatierung festzulegen. Als „Bedingung 1“ belässt man die vorgeschlagenen Kriterien bei „Datum ist“ und „heute“. Darunter bietet das Feld „Vorlage anwenden“ einige Formatierungen zur Hervorhebung, wenn die Bedingungen zutreffen. Ein Klick auf „Hinzufügen“ wendet dann die Bedingung auf den markierten Bereich an. **-dw**



Das Datum hervorheben: Ohne umständliche Formeln kann eine bedingte Formatierung bestimmte Werte in einer Tabelle einfärben, hier beispielsweise das jeweils aktuelle Datum.

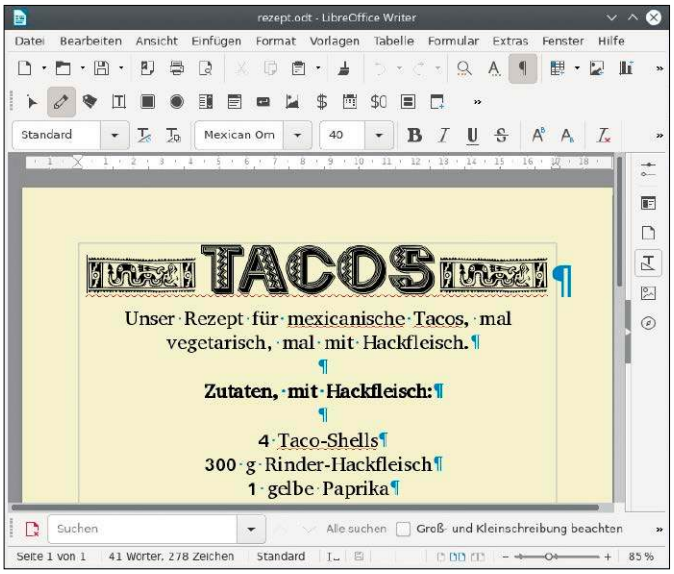
APP-CONTAINER ALLER ART: GESUCHT UND GEFUNDEN

Bisher waren zur Suche nach installierbaren Programmen und passenden Programmpaketen nur für die offiziellen und inoffiziellen Paketquellen eines Linux-Systems interessant.

Mit den Containerformaten Flatpak, Snap und Appimage gibt es noch einige Quellen mehr, die weitgehend unkompliziert viele populäre Programme in einem leicht installierbaren Format liefern und Linux-Anwendern die oft aufwendige Kompilierung sparen. Ein App Store, der die populären Snaps, Flatpaks und Appimages an einer zentralen Stelle präsentiert, ist jetzt mit dem App Outlet verfügbar (*https://app-outlet.github.io*). Das englischsprachige Tool ist im Stil eines grafischen Paketmanagers gehalten und liegt selbst als Appimage vor, aber auch als Snap-Paket und als DEB-Datei für Debian, Ubuntu und Linux Mint. Es gibt eine Volltextsuche, eine Navigation mittels kategorisierten Tags und Filter nach App-Containertyp. Die Installation eines Programms ist mit wenigen Klicks möglich.

Ein Paketmanager für App-Container: Das Programm App Outlet präsentiert installierbare Software in den Formaten Snap, Flatpak und Appimage in einem grafischen Paketmanager.

Libre Office: Schriften einbetten



Exotische Schriftarten: Bei Libre-Office-Dokumenten mit ausgefallenen Fonts empfiehlt es sich, die Schriftarten im Dokument mitzuliefern. Dort liegen sie dann auch als Datei vor.

Die Schriftarten in einem Dokument zeigt Libre Office nur dann genau wie im Originaldokument an, wenn diese auf dem Rechner installiert sind. Bei gewöhnlichen Textdokumenten sind Detailunterschiede bei Schriften nicht dramatisch. Wenn aber ungewöhnliche Fonts als Stilmittel verwendet wurden, dann zeigt das Dokument auf einem anderen PC erhebliche Unterschiede.

Soll das Austauschformat kein PDF sein, sondern ein weiterhin editierbares Libre-Office-Dokument, so kann Libre Office im Writer, in Calc, Impress und Draw die verwendeten Fonts direkt in die Dokumentdatei einbetten. Dieses Verfahren ist vor allem dann zu empfehlen, wenn eine Datei an andere Anwender zur Weiterbearbeitung gehen soll und dabei die Formatierung möglichst exakt erhalten bleiben muss. Alles ist dann in der Libre-Office-Datei enthalten. Voraussetzung ist natürlich, dass Libre Office auch bei den Empfängern verwendet wird.

Die Funktion dazu verbirgt sich im Menü „Datei → Eigenschaften“ auf der Registerkarte „Schrift“. Hier sorgt ein Häkchen vor der Optionen „Schriftarten ins Dokument einbetten“ dafür, dass die Fontdateien mit in die Dokumentdatei kommen.

Falls es nicht klappt: Es kommt vor, dass einige Versionen von Libre Office unter Linux die eingebetteten Schriften doch nicht anzeigen und nur eine Austausch-Schriftart als Platzhalter sichtbar ist.

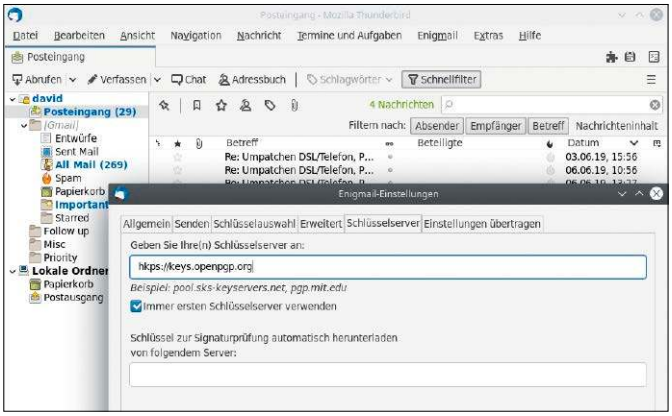
In diesem Fall bekommt man die mitgelieferten Schriftarten aber dennoch aus der Dokumentdatei heraus und kann diese immerhin manuell auf dem System installieren.

1. Bei Libre-Office-Dateien handelt es sich um ZIP-Archive, welche eine Ordnerstruktur mit den Dokumentbestandteilen enthalten. Um die Schriftarten zu extrahieren, gibt man der Dokumentdatei die Endung „.zip“ und öffnet sie mit einem Packprogramm wie zum Beispiel dem File-Roller unter Gnome oder Ark in KDE.

2. Im Packprogramm ist nun die Ordnerstruktur des Dokuments sichtbar. Die verwendeten Schriftarten liegen im Unterverzeichnis „Fonts“.

3. Nach dem Entpacken der Schriftdateien müssen diese noch auf dem Zielsystem installiert werden. Die unterschiedlichen Linux-Desktops bringen dafür jeweils eigene Hilfsprogramme zum Betrachten von Fontdateien mit, in welchen sich auch eine Funktion zur Installation der Schriftart findet. Nach einem Neustart von Libre Office sind die Schriftarten dort verfügbar. **-dw**

Thunderbird und Enigmail: Andere Schlüsselserver



Schlüsselserver austauschen: Die von Enigmail genutzten Standardserver zum Nachschlagen von GPG/PGP-Schlüsseln sind unbrauchbar und müssen in diesem Dialog ersetzt werden.

Die Erweiterung Enigmail bringt Thunderbird die Verschlüsselung mit GPG/PGP bei. Enigmail kann auch zu E-Mail-Adressen veröffentlichte Schlüssel auf sogenannten Schlüsselservern wie in einem Telefonbuch suchen. Der voreingestellte Schlüsselserver (*https://sks-keyservers.net*) liefert aber schon seit mehreren Monaten keine zuverlässigen Ergebnisse mehr. Es empfiehlt sich deshalb, zum Nachschlagen andere Schlüsselserver zu verwenden.

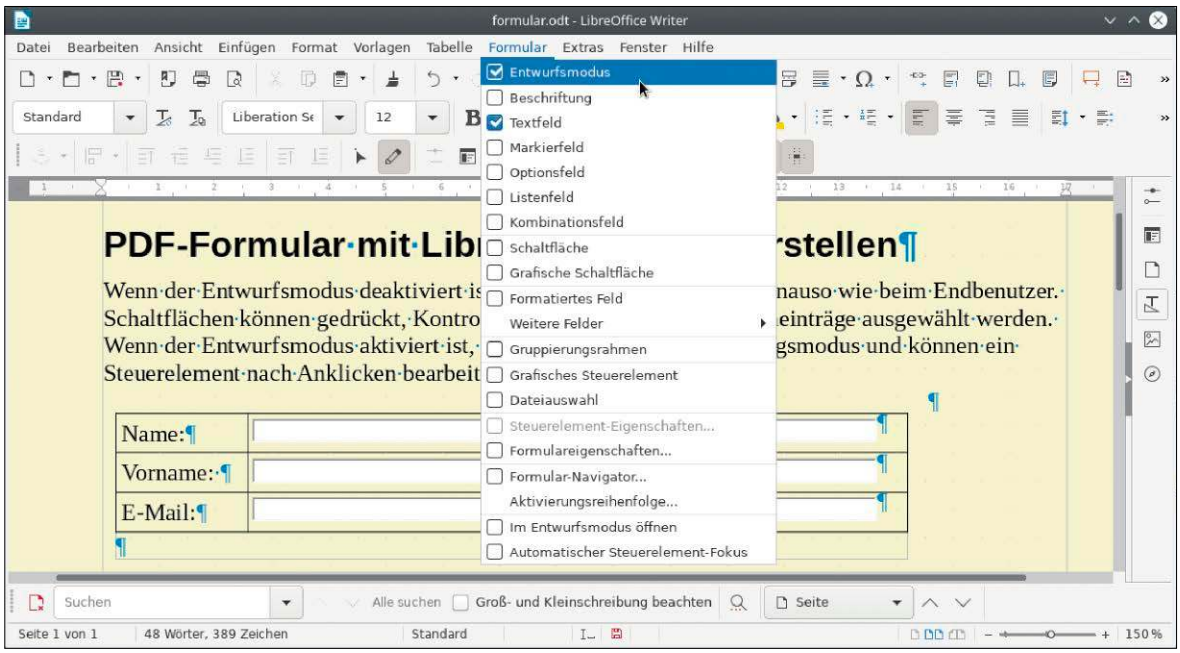
Seit Sommer 2019 sehen sich die öffentlichen Schlüsselserver des SKS-Pools einem Spamangriff ausgesetzt. SKS steht für „Synchronizing Key Server“ und ist ein Serververbund mit rund fünf Millionen GPG/PGP-Schlüsseln. Die Besonderheit ist, dass jeder auf diesen Servern Schlüssel veröffentlichen darf, bestehende Datensätze jedoch nicht löschen kann. Diesen Umstand nutzten nun Spammer aus, um die Server mit Hunderttausenden von ungültigen Schlüsselzertifikaten zu fluten. Die Serverbetreiber haben bisher keine Möglichkeit gefunden, dieses Treiben zu unterbinden. Das heißt: Das SKS-Key-Server-Netzwerk wurde mit Spam geflutet und es ist bisher kein Weg bekannt, diesen Spam auszusortieren. Die Betreiber des Netzwerks glauben selbst nicht mehr daran, dass die Server zu retten sind, und empfehlen daher, auf andere Auskunftsdienste auszuweichen.

Als Alternative zu dem bisherigen SKS-Key-Server-Netzwerk kommt der noch recht neue Open-PGP-Key-Server unter *https://keys.openpgp.org* infra-

ge. Wer auf dem dortigen Server einen PGP-Key zu einer Mailadresse eingibt, der erhält im Anschluss daran eine Bestätigungsmail an diese E-Mail-Adresse mit einem Link zur Verifizierung. Es können also nur Anwender einen Key dort einreichen, die auch wirklich Zugriff auf das zugehörige Postfach haben.

Ein Nachteil des neuen Servers: Die Anzahl der hinterlegten öffentlichen Schlüssel ist noch vergleichsweise gering. Das wird sich erst im Laufe der nächsten Jahre ändern. Wer den neuen Server von Thunderbird bereits mit Enigmail verwenden möchte, kann die Serveradresse wie folgt eintragen: In Thunderbird zeigt der Menüpunkt „Enigmail → Einstellungen → Experten-Optionen → Menüpunkte einblenden → Schlüsselserver“ im Feld „Schlüsselserver“ die bisherigen Adressen an, etwa „pool.sks-keyservers.net, keys.gnupg.net, pgp.mit.edu“. Diese Adressen ersetzen Sie durch den Eintrag „hkps://keys.openpgp.org“, welcher auf den neuen Open-PGP-Server verweist. Bei Abfragen kann es einige Momente dauern, bis der Server Antworten gibt. **-dw**

Libre Office Writer: PDF-Formular erstellen



Alles klar im Formular: Im Libre Office Writer sind PDF-Dokumente zum bequemen Ausfüllen sehr einfach erstellt. Rahmen und Tabellen helfen bei der sauberen Platzierung.

Formulare im PDF-Format sind praktisch, lassen sie sich doch mit einem PDF-Betrachter ausfüllen, ausdrucken und sogar abspeichern. Anwender brauchen dabei nur die vorgefertigten Felder auszufüllen und den Anweisungen zu folgen. Alles, was zum Erstellen solcher Formulare benötigt wird, ist in Libre Office enthalten.

Erfahrungsgemäß erhält man ein gut vorbereitetes, strukturiertes PDF-Formular viel schneller ausgefüllt zurück als einfache Dokumente.

Die meisten PDF-Reader wie auch Okular und Evince unter Linux können mit Formularen umgehen, diese PDFs ausfüllen und speichern.

1. Angefangen bei einem neuen leeren Textdokument in Libre Office Writer ist der erste Schritt die Struktur und Positionierung der Eingabeelemente. Ein guter Weg zur präzisen, sauberen Positionierung von Elementen ist die Anordnung in Rahmen und Tabellen.

2. Die Funktion „Einfügen → Rahmen → Rahmen interaktiv“ erlaubt das Ziehen und Positionieren eines Rahmen mit der Maus. Die standardmäßig eingeblendeten Ränder lassen sich über einen Rechtsklick über „Eigenschaften → Umrandung“ auch unsichtbar machen.

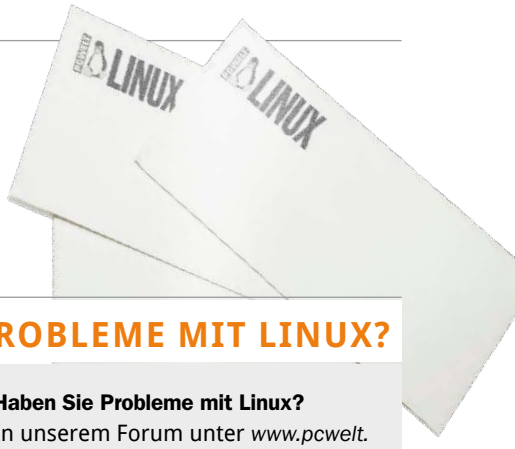
3. In den Rahmen setzt nun der Menüpunkt „Einfügen → Tabelle“ das Tabellenelement für die Eingabefelder. Soll das Formular beispielsweise drei Eingabefelder mit Beschriftung haben, so ist eine Tabelle mit zwei Spalten und drei Zeilen groß genug.

4. In die erste Spalte der Tabelle kommen nun die Beschriftungen zu den Eingabefehlern. Die zweite Spalte, welche die gedrückte Maustaste auf die gewünschte Größe zieht, nehmen die Eingabefelder auf.

5. Das Setzen der Eingabefelder, beispielsweise Textfelder, gelingt nach dem Einschalten des „Entwurfsmodus“ unter „Formular“. Die gewünschten Felder kommen in die zweite Spalte der Tabelle und werden wieder mit gedrückter Maustaste positioniert. Mit Kopieren und Einfügen sind Eingabefelder desselben Typs bei Bedarf schnell dupliziert.

6. Ein Doppelklick auf ein Formularfeld im Entwurfsmodus öffnet dessen Eigenschaften. Hier können Sie weitere Einstellungen wie die maximale Textlänge einer Eingabe festlegen und ferner Schriftart sowie Schriftgröße definieren, die beim Ausfüllen erscheint.

7. Nach dem Abschalten des „Entwurfsmodus“ sollten Sie das Formular erst noch einmal mit Eingaben testen. Danach erstellt der Punkt „Datei → Exportieren → Als PDF exportieren“ das fertige Dokument. Im Export-Dialog muss die Option „PDF-Formular erzeugen“ aktiviert sein, was standardmäßig der Fall ist. **-dw**



Leserbriefe

Haben Sie Fragen zum Heft oder möchten Sie uns Ihre Meinung dazu mitteilen? Schreiben Sie bitte an *linux@it-media.de* oder per Post an Redaktion LinuxWelt, IT Media, Gotthardstr. 42, 80686 München. Von den vielen Zuschriften können wir nur eine Auswahl veröffentlichen. Sinnwahrende Kürzungen behalten wir uns vor.

Heft-DVD: Startproblem mit Parrot-OS

Die DVD der letzten LinuxWelt 6/2019 enthielt das Livesystem Parrot-OS Home, das ich ausprobieren und eventuell installieren wollte. Das System startet aber nur zum Anmeldebildschirm und lässt dann keine Anmeldung zu.

Thorsten S., per Mail

Das Problem müssen wir bestätigen. Wir vermuten, dass das optische DVD-Medium in diesem besonderen Fall zu langsam ist, um bis zum Start der grafischen Oberfläche alle Dienste korrekt zu laden. Die automatische Anmeldung scheitert, die manuelle Anmeldung mit dem Standardkonto „user“ und dem Standardpasswort „toor“ ebenfalls. Diese Erfahrung lehrt uns, Parrot-OS künftig nicht mehr oder nur noch nach speziellen Testläufen anzubieten. Ganz verloren ist das System auf der letzten DVD damit allerdings nicht:

1. Eventuell könnte es helfen, den Log-in-Bildschirm etliche Minuten (!) abzuwarten und sich erst dann mit Kennwort „toor“ anzumelden.

2. Der Livebetrieb funktioniert, wenn Sie mit Strg-Alt-F1 in die virtuelle Konsole wechseln und die grafische Oberfläche mit dem Befehl *startx* laden. Dann ist das System zu benutzen, allerdings nicht zu installieren, da für den Live-„User“ offenbar keine sudo-Rechte existieren.

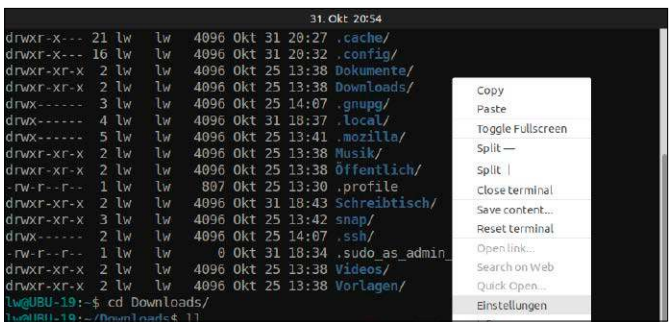
3. Installieren lässt sich das System aber dennoch, da es beim Booten eine Option anbietet, die Installation (ohne Livesystem) direkt zu starten. Das auf Festplatte installierte Parrot-OS hat derartige Probleme dann natürlich nicht mehr.

Terminal per Knopfdruck

Im Kubuntu-Dateimanager Dolphin kann man jederzeit mit F4 ein Terminal einblenden, das dann gleich im aktuellen Dolphin-Ordner startet. Gibt es Vergleichbares für Nautilus unter Ubuntu mit Gnome?

Heinz W., per Mail

Es gibt eine Python-Erweiterung („nautilus-terminal“) für den Dateimanager Nautilus, die wir allerdings nicht empfehlen, weil dieses Terminal weder optisch überzeugt noch anpassungsfähig ist. Bestes Einblendterminal, allerdings ohne Dateimanager-Integration, ist das Tool Guake (mit gleichnamigen Paketnamen). Guake blendet sich in einstellbarer Größe nach Hotkey F12 ein und bei Fokusverlust automatisch aus. Die „Einstellungen“ (nach Rechtsklick) bieten Transparenz, Animation, Farbthemen, Suchleiste und vieles mehr. ■



Terminal jederzeit mit F12: Guake ist das beste Einblendterminal für Gnome-affine Desktops.

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/linuxwelt-ipad-jahresabo-zukunft-ist-jetzt–2636

Verlag

IT MEDIA PUBLISHING GMBH & CO KG

IT Media Publishing GmbH & Co. KG
Gotthardstr. 42, 80686 München
Tel. 089/3398052-10
Fax 089/3398052-70
E-Mail: *info@it-media.de*
www.it-media.de

Chefredakteur: Sebastian Hirsch (v.i.S.d.P – Anschrift siehe Verlag)

Druck: Mayr Miesbach GmbH
Am Windfeld 15, 83714 Miesbach
Tel. 08025/294-267

Inhaber- und Beteiligungsverhältnisse: Alleinige Gesellschafterin der IT Media Publishing GmbH & Co. KG ist die IT Media Publishing Verwaltungs GmbH, München, Geschäftsführer Sebastian Hirsch.

WEITERE INFORMATIONEN

Redaktion

Gotthardstr. 42, 80686 München
Tel. 089/3398052-10
Fax 089/3398052-70
E-Mail: *info@it-media.de*
www.it-media.de
Chefredakteur: Sebastian Hirsch (verantwortlich für den redaktionellen Inhalt)
Stellvertretender Chefredakteur: Thomas Rau
Chef vom Dienst: Andrea Kirchmeier
Redaktion: Arne Arnold
Redaktionsbüro: MucTec (*hapfelboeck@googlemail.com*)
Freie Mitarbeiter Redaktion: Dr. Hermann Apfelböck, Thorsten Eggeling, Stephan Lamprecht, David Wolski
Titelgestaltung: Schulz-Hamparian, Editorial Design / Thomas Lutz
Freier Mitarbeiter Layout/Grafik: Alex Dankesreiter
Freie Mitarbeiterin Schlussredaktion: Andrea Röder
Freier Mitarbeiter digitale Medien: Ralf Buchner
Herstellung: Melanie Arzberger
Redaktionsassistenz: Manuela Kubon

Anzeigen

Anzeigenleiter:
Sven Schrader
Tel. 089/3398052-41
E-Mail: *schrader@it-media.de*

Vertrieb

Vertrieb Handelsauflage:
MZV GmbH & Co. KG, Ohmstraße 1
85716 Unterschleißheim
Tel. 089/31906-0
Fax 089/31906-113
E-Mail: *info@mzv.de*
Internet: *www.mzv.de*

Druck: Mayr Miesbach GmbH
Am Windfeld 15, 83714 Miesbach
Tel. 08025/294-267

Verlag

IT Media Publishing GmbH & Co. KG
Gotthardstr. 42, 80686 München
Tel. 089/3398052-10,
Fax 089/3398052-70
E-Mail: *info@it-media.de*
www.it-media.de
Sitz: München, Amtsgericht München, HRA 104234
Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949:
Alleinige Gesellschafterin der IT Media Publishing GmbH & Co. KG ist die **IT Media Publishing Verwaltungs GmbH,** Sitz: München, Amtsgericht München, HRB 220269
Geschäftsführer: Sebastian Hirsch
ISSN 1860-7926

KUNDENSERVICE

LinuxWelt-Kundenservice für Einzelheft-Käufer:
DataM-Services GmbH
Postfach 9161
97091 Würzburg
Tel.: 0931/4170-177
Fax: 0931/4170-497
(Mo bis Fr, 8 bis 17 Uhr)
E-Mail: *idg-techmedia@datam-services.de*

LinuxWelt-Kundenservice für Abonnenten: Fragen zum bestehenden Abonnement / Premium-Abonnement, zum Umtausch defekter Datenträger, zur Änderung persönlicher Daten (Anschrift, E-Mail-Adresse, Zahlungsweise, Bankverbindung) bitte an
Zenit Pressevertrieb GmbH
LinuxWelt-Kundenservice
Postfach 810580
70522 Stuttgart
Tel: 0711/7252-233
(Mo bis Fr, 8 bis 18 Uhr)
Fax: 0711/7252-333
E-Mail: *linuxwelt@zenit-presse.de*
Erscheinungsweise:
6x jährlich

Jahresbezugspreise LinuxWelt mit DVD: 51,00 € (D)
57,00 € (A, CH, Benelux)
inkl. Versandkosten

Bankverbindung für Abonnenten:
Postbank Stuttgart, IBAN
DE56 6001 0070 0029 0547 04, BIC PBNKDEFFXXX

Sie können Ihr Abonnement jederzeit zur nächsten Ausgabe kündigen.
Bestellungen können innerhalb von 14 Tagen ohne Angabe von Gründen in Textform (zum Beispiel Brief, Fax, E-Mail) oder durch Rücksendung der Ware widerrufen werden.

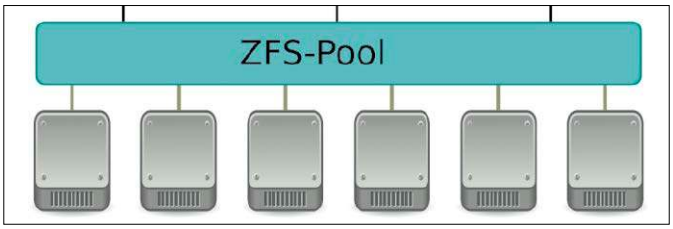
LinuxWelt 2/2020 erscheint am 31.1.2020

Aus Aktualitätsgründen können sich Themen ändern.

Die Macht der Schalter

Startparameter für Browser, Office, VLC & mehr: Startparameter sind kein Terminalprivileg. Was im Terminal unumgänglich ist, ist bei grafischen Programmen zwar nur optional, aber erstaunlich vielseitig. Die LinuxWelt filtert die Spreu der zahlreichen Debug- und Analyseschalter heraus und konzentriert sich auf die wirklich produktiven Startschalter. Im Zentrum steht dabei weitverbreitete Software wie Firefox, Chrome, Libre Office, VLC, Calibre, Bleachbit und andere. Sie werden staunen, wieviel Potenzial liegen bleibt, solange Sie auf diese meist kaum bekannten Optionen verzichten.

Ubuntu-Tuning



ZFS-Dateisystem und neue Desktopfunktionen: Das frische Ubuntu 19.10 bringt eine Reihe technischer Neuheiten. Das nächste Heft zeigt unter anderem, wo sich der Einsatz der neuen Installationsoption mit ZFS-Dateisystem lohnt und mit welchen Kommandos ZFS-Volumes zu kontrollieren und zu bearbeiten sind. Darüber hinaus geht es um das Einrichten und Optimieren der Ubuntu-Oberflächen, wobei die Desktops im Vordergrund stehen, die mit Version 19.10 die meisten Veränderungen erfahren haben (Gnome, Xubuntu, Mate).

Netzwerkhardware

Ratgeber für das optimale Heimnetz: Mit den richtigen Komponenten sind Heimnetzwerke und kleinere Büronetzwerke schnell aufgebaut. Dieser Grundlagenbeitrag zeigt alle wichtigen Geräte für den Aufbau von Ethernet-LAN und Powerline-Brücken, WLAN und Funknetzbrücken mit Repeater oder Access Points. Sie erhalten Tipps zum Ausbau einer bereits bestehenden Infrastruktur und zur optimalen Konfiguration von Router, Access Points, Repeater, Powerline, Netzwerkdrucker und Netzwerkergänzungen wie NAS, Platinenserver sowie Streaminghardware.

Fedora 31

Neue Version der Red-Hat-Workstation: Fedora 31 ist ein gesetzter Kandidat für die Heft-DVD der nächsten LinuxWelt. Die aktualisierte Gnome-Oberfläche verspricht flüssigeres Arbeiten und auch im Unterbau zeigt Fedora 31 einige Umbauten. Ein geändertes Kompressionsverfahren sorgt für eine schnellere Installation von Softwarepaketen. Die Details zu Fedora 31 lesen Sie in einer ausführlichen Vorstellung in der nächsten LinuxWelt.

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

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PWSJO14130

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

InfinityBook Pro 15

10h Akku
Maximale Laufzeit

64 GigaByte
DDR4 2666 MHz

Intel Core i7
Quad-Core

FullHD Display
15,6" IPS Panel

Thunderbolt 3
Mit Ladefunktion

Privatsphäre+
IntelME, Webcam, Audio abschaltbar

100% Linux

5 Jahre Garantie

Lifetime Support

Gefertigt in Deutschland

Deutscher Datenschutz

Support vor Ort

TUXEDO COMPUTERS

tuxedocomputers.com