



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

LINUX WELT



Einsteiger-Tipps: Ubuntu installieren

So startet das System auf jedem Rechner

Jubiläums- Paket

Über
8000
Seiten Linux-
Know-how!



Über 70 Hefte auf DVD

Plus: Mint 19.2

und vier weitere
Top-Systeme

15 Jahre LinuxWelt! Das große Jubiläums- Paket **15 Jahrgänge** auf DVD

Linux perfekt sichern

Security-Check mit Hacker-Tools

- Alle Schwachstellen am PC stopfen
- Einfallstore im Heimnetzwerk schließen
- Lücken im Heimserver aufdecken

PLUS
Alle Check-
Tools auf
Heft-DVD



Praxis-Workshop Linux Mint 19.2

Tipps zu schnellerem Desktop, neuer
Kernel-Verwaltung und verbesserten System-Programmen

PLUS:
Neue Mint-
Version auf
DVD!

30 geniale Systemtipps

Bootloader beschleunigen,
Preload für Programme,
Systemaufgaben automatisieren,
Datenmüll beseitigen u.v.m.

Tools richtig installieren

- Mehr Software-Quellen nutzen
- Installationsprobleme lösen
- Tools immer aktuell halten

Die besten Mini-PCs

Die neue Generation
mit mehr Leistung,
schnellerer Grafik und
Highspeed-Netzwerk



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 indg-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	Geburts- tag	TT	MM
	E-Mail			

BEZAHLEN	<input type="radio"/> Ich bezahle bequem per Bankeinzug.	<input type="radio"/> Ich erwarte Ihre Rechnung.
	Geldinstitut	
	IBAN	
	BIC	
	Datum / Unterschrift des neuen Lesers	

PWSJ014130

Alles Gute, LinuxWelt!

Vor 15 Jahren erschien die erste Ausgabe der LinuxWelt, damals noch als „Linux PC-WELT Extra“. Dieses Jubiläum feiern wir, indem wir Ihnen alle 15 Jahrgänge LinuxWelt auf die Heft-DVD packen. So lässt sich in über 70 Heften die tolle Mischung aus einfachen Schritt-für-Schritt-Anleitungen und Beiträgen mit Profi-Know-how nachlesen.

Ein Blick in das LinuxWelt-Archiv zeigt auch, wie nachhaltig Linux ist. Wer sich vor 15 Jahren mit der LinuxWelt die Grundlagen von Linux angeeignet hat, etwa die wichtigsten Befehle fürs Terminal, der konnte damit alle folgenden Linux-Versionen gleichermaßen gut bedienen. Denn das grundlegende Linux-Know-how veraltet kaum.

Trotzdem gibt es laufend spannende Neuigkeiten zu entdecken und aktuelle Entwicklungen zu besprechen. Zu den wichtigsten Linux-Themen heute zählt der Sicherheitsaspekt von Betriebssystem und Software. Darum bringen wir in dieser Ausgabe ein ausführliches Special zum Thema Linux und Sicherheit. So können Sie prüfen, ob Ihre Linux-Installation gut genug gegen Angreifer geschützt ist.

Viel Spaß beim Lesen!

Arne Arnold



Arne Arnold

Redakteur

aarnold@it-media.de

MINI-ABO LINUXWELT: EIN HALBES JAHR GEBALLTES LINUX-KNOW-HOW!

Wenn Ihnen die LinuxWelt gefällt, können Sie sich das Heft für sechs Monate per Mini-Abo einfach ins Haus schicken lassen. Sie sparen mit dem Mini-Abo 33 Prozent und erhalten noch einen Gutschein dazu.

Gratis-Versand: Mit dem Mini-Abo der LinuxWelt bekommen Sie drei Ausgaben der LinuxWelt ohne Versandkosten direkt nach Hause ge-

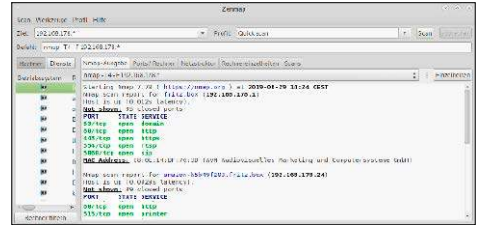
liefert. In der Regel treffen sie noch vor dem offiziellen Verkaufsstart bei Ihnen ein. **Digitaler Zugriff:** Als Ergänzung zum Mini-Abo der gedruckten Hefte bekommen Sie Ihre Ausgaben auch digital auf Ihr Mobilgerät.

33 Prozent sparen: Mit dem Mini-Abo sparen Sie satte 33 Prozent: Sie zahlen nur 17 statt 25,50 Euro! Und zusätzlich erhalten Sie eine Geld-

prämie oder einen Gutschein über 10 Euro.

Alle Infos: Das Mini-Abo können Sie ganz einfach über www.pcwelt.de/linux bestellen. Nach drei Ausgaben verlängert sich das Abo automatisch um ein Jahr (sechs Ausgaben LinuxWelt für zurzeit 51 Euro). Wenn Sie kein Abo möchten, kündigen Sie einfach vor Erhalt der dritten Ausgabe.

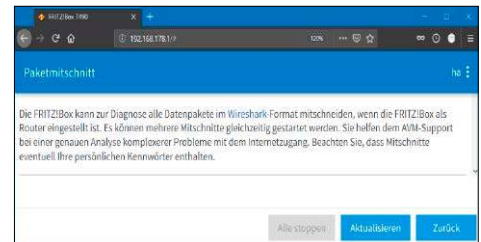




Nmap und Ports

Offene Türen: Nmap und Zenmap finden offene Netzwerkports und die verantwortlichen Dienste und Programme.

S. 26



Wireshark

Der Paketsniffer kann den kompletten Verkehr der Fritzbox kontrollieren.

S. 30

Raspberry und Alternativen

Anlässlich des neuen Raspberry lesen Sie einen ausführlichen Test und nachfolgend einen Überblick zu alternativen Odroid-Platinen und Intel-Mini-PCs sowie zum besten Platinenzubehör.

S. 54

■ Grundlagen

- 6 **Linux 2004 bis 2019**
15 Jahre LinuxWelt: Heutige Linux-Themen belegen den Fortschritt
- 8 **DVD-Übersicht**
Distributionen, Tools, Infos und alle 75 Ausgaben der LinuxWelt
- 10 **Distributionen auf DVD**
Steckbriefe von Manjaro XFCE, Parrot-OS, Q4-OS und Bionic Pup
- 14 **Linux Mint 19.2**
Vorstellung und Einstieg: Der Ubuntu-Ableger wird noch besser
- 20 **Systemschutzmaßnahmen**
Rückversicherung: Mit Timeshift, Clonezilla und Datenbackup arbeiten Sie pannersicher
- 22 **Linux-News**
Linux, Open Source und Sicherheit: Die jüngsten Trends, Updates und Sicherheitsnews

■ Special I – Sicherheitsanalysen

- 26 **Portscans mit Nmap**
Offene Türen erkennen: Nmap-Portanalysen zeigen, ob Ihr Netzwerk von außen erreichbar ist
- 28 **Server-Schwachstellen**
Spezialwerkzeug Nikto: Das Tool erledigt Tausende von Checks und erkennt Fehler und Schwachstellen
- 30 **Paketsniffer Wireshark**
Wireshark weiß, was im Netzwerk läuft: Das Profiwerkzeug liest alle Netzwerkprotokolle mit
- 32 **Burp-Suite-Proxy**
Analysetool für Webanwendungen: Der Mitschnitt des Client-Server-Verkehrs entlarvt vorhandene Sicherheitsmängel
- 34 **Dateisuche mit Dirbuster**
Dateien auf Webservern: Dirbuster findet nicht öffentliche Verzeichnisstrukturen und Dateien im Internet

- 36 **Pentesting**
Hacken Sie Ihr eigenes System: Metasploit kennt und attackiert Tausende von Sicherheitslücken
- 40 **Viren finden und beseitigen**
Heterogene Netze: Scannen Sie Linux-Rechner, wenn diese von Windows frequentiert werden



■ Special II – Software für Linux

- 42 **Software und Pakete**
Die Werkzeuge der Softwareinstallation aus den Paketquellen
- 46 **Software in Containern**
Snap, Flatpak, AppImage: Diese Formate haben Vor- und Nachteile
- 48 **Zusätzliche Paketquellen**
PPAs: Hier erhalten Sie die aktuellsten Softwareversionen
- 50 **Software für Umsteiger**
Mit diesen Programmen fällt der Windows-Umstieg leichter



■ Die Highlights der DVD

Auf Heft-DVD: Linux Mint 19.2 nebst spannenden Exoten

Das beliebte Linux Mint in neuer Version 19.2 ist eine Pflichtübung für unsere DVD. Seine Begleiter wird nicht jeder kennen: Parrot-OS etabliert sich als Desktopsystem, Q4-OS ist extrem sparsam, Manjaro zeigt den brandneuen XFCE-Desktop 4.14 und Bionic Pup ist ein aktualisiertes Puppy-Livesystem.

S. 10



Linux Mint 19.2 (Cinnamon)

Linux Mint ist ein Ubuntu-Derivat, das seinem Basissystem längst den Rang abgelaufen hat. Der Desktop Cinnamon überzeugt ebenso wie die Zentralen für Software und Aktualisierung.



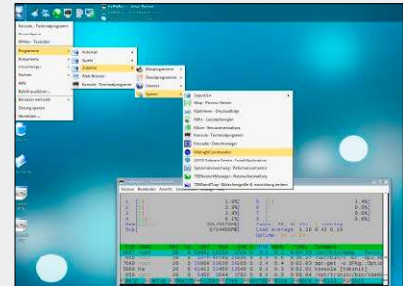
Parrot-OS Home 4.6

Das Sicherheitssystem Parrot-OS macht als „Home“-Variante Desktopkarriere. Mit sorgfältig konfiguriertem Mate ist Parrot-OS schlank und flott – auch auf schwächerer Hardware.



Q4-OS 3.8

Q4-OS definiert sich durch den genügsamen Trinity-Desktop. Da sich Trinity an älteren Windows-Versionen orientiert, ist Q4-OS ein guter Ersatz für Windows 7 auf älterer Hardware.



■ **Hardware**

- 54 **Der neue Raspberry Pi 4**
Alles, was Sie über den Pi 4 wissen müssen: Was er leistet und was Sie als Zubehör brauchen
- 58 **Die Odroid-Platinen**
Eine Übersicht inklusive den neuesten Modellen N2 und H2
- 62 **Mini-PCs: NUC und Zotac**
Schicke Wohnzimmerserver mit Intel-CPU und großer Preisspanne
- 65 **Zubehör für den Raspberry**
Kameras, Displays und Sensoren: Das sind die besten Ergänzungen

■ **Software**

- 68 **Videos konvertieren**
Platz sparen, Qualität bewahren: So reduzieren Sie den Speicherplatz Ihrer Filme mit Handbrake und Avidemux
- 72 **ISO-Bearbeitung**
ISO-Images anpassen: Mit dem Tool Xorriso bauen Sie individuelle Livesysteme
- 76 **Spieleklassiker unter Linux**
GOG („Good Old Games“) und mehr: Diese Quellen für Linux-Spiele sollten Sie kennen
- 78 **Samba im Terminal**
Das Tool Smbclient: So erhalten Sie im Terminal direkten Zugriff auf Samba-Freigaben

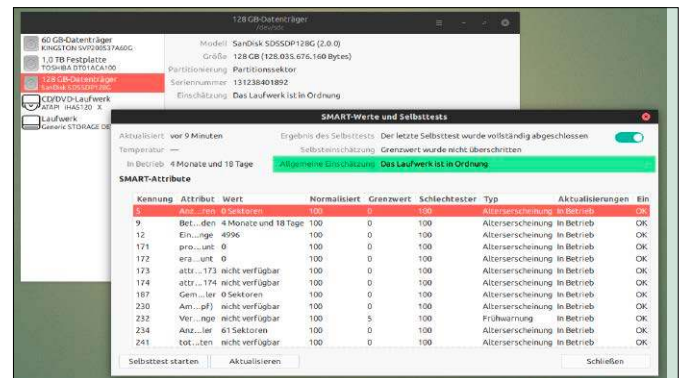
■ **Praxis**

- 86 **Ubuntu-Installationen**
Alle Varianten: Die Ubuntu-Installer können mehr, als Sie denken
- 90 **Die 30 besten Systemtipps**
Mit diesen Tipps gewinnt Ihr Linux-System an Leistung, Kontrolle und Bedienkomfort
- 98 **Desktoptipps**
Tipps & Tricks zu den Oberflächen Gnome, KDE, Cinnamon & Co.
- 102 **Terminaltipps**
Neue Bash- und Kommandotricks der Terminalprofis
- 105 **Hardwaretipps**
Hardwarekomponenten im Griff: Tools und Tricks, die sich lohnen
- 108 **Softwaretipps**
So bearbeiten Sie PDFs, laden Google-Apps als APK-Pakete und entfernen Snap-Container

■ **Standards**

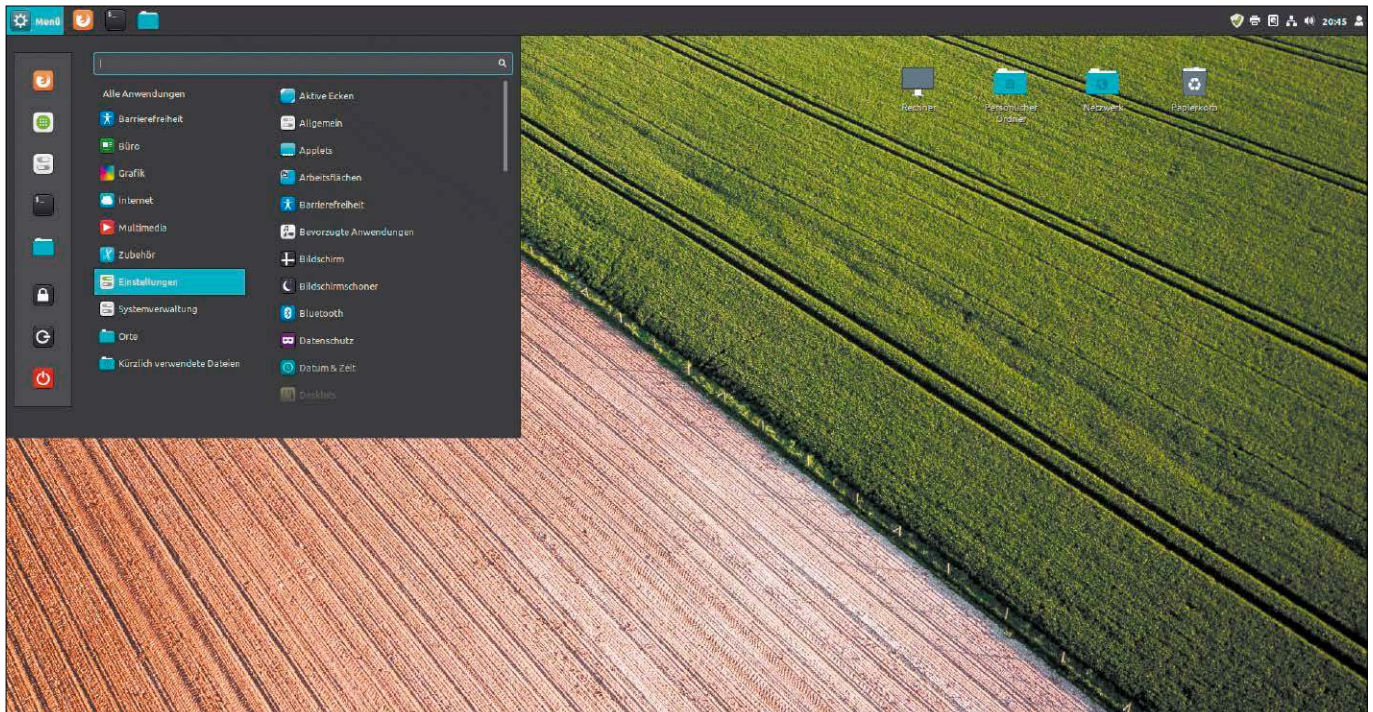
- 3 **Editorial**
- 9 **Leserbefragung**
- 112 **Leserbriefe/Service**
- 113 **Impressum**
- 114 **Vorschau**

- 80 **Neue Software**
12 Programme im Steckbrief: Neuheiten & Updates aus dem Umfeld von Linux & Open Source



Linux 2004 bis 2019

Ungeduldige mögen so manche innovationsarme Zwischenversion von Ubuntu & Co. als Stagnation beklagen. Wer aber mit etwas Abstand ein paar Jahre Linux-Entwicklung resümiert, reibt sich die Augen: Mal zäher, mal rasanter – aber stets geht es voran.



VON HERMANN APFELBÖCK

Grund unserer Rückschau ist ein kleines Jubiläum: Die LinuxWelt startete vor 15 Jahren im Frühjahr 2004. Das war noch vor dem ersten Auftreten des mittlerweile populärsten Desktop-Linux Ubuntu (inklusive Derivate). Ubuntu startete wenig später mit der Version 4.10 im Oktober 2004 und einer Versionsbezeichnung (nach Jahr und Monat), die bis heute gilt. Der Ubuntu-Start und das Folgejahr 2005 fand in der damaligen LinuxWelt noch kaum Niederschlag. 2006 wurde dann deutlich, dass mit Ubuntu der Desktopstar geboren war, der dem lange favorisierten Open Suse bald den Rang ablief. Noch weniger als die Aussicht auf Linux-Standards à la Ubuntu zeichnete sich in den

Nuller Jahren die Geräteklasse der Linux-affinen Miniserver ab, die der Raspberry Pi ab 2012 begründete. Der Raspberry legte im Laufe von sieben Jahren manches laue Modellupgrade hin, darf aber heute mit Modell 4 B als erwachsen gelten. Was beim Prototyp 2012 eher noch Vision und Versprechen war, ist 2019 Realität. Und wem der kleine Rechner für seine Serveransprüche trotzdem noch nicht reicht, findet Auswahl bei leistungsstärkerer Konkurrenz, die der Raspberry angestoßen hat.

Linux-affine und netzwerkfähige Minihardware ist aber längst nicht auf Platinenrechner beschränkt: Das Schlagwort IoT (Internet of Things) subsumiert eine Legion unzähliger Netzwerkgeräte der Hausautomatisierung, Kameraaufzeichnung, Messensorik, die vor zehn oder 15 Jahren nicht vorherzusehen war.

Nochmal 2004: Linux-Software gab es damals ausschließlich aus den Standardpaketquellen oder durch Kompilieren des Quellcodes. Die ersten Pflänzchen externer Softwareverteilung über PPAs oder Klick-Images (heute Appimage) starteten zwar etwa zu diesem Zeitpunkt, relevant wurden sie erst Jahre später. Die heute bekannten distributionsunabhängigen Containerformate Snap und Flatpak kamen erst 2014 und 2015 ins Rollen.

Die wichtigsten Themen im Heft

Die Themen der obigen kleinen Rückschau waren nicht zufällig gewählt: Es sind die Schwerpunkte im aktuellen Heft. Das beliebte Ubuntu-Derivat **Linux Mint 19.2** nutzt die fällige Systemerneuerung auf Releasepunkt 2 sowohl zur Desktopoptimierung (Cinnamon) als auch zu ansehnlichen

Detailverbesserungen bei einigen Systemtools (Aktualisierungs- und Anwendungsverwaltung). Version 19.2 ist ein moderater, aber ordentlicher Schritt nach vorne.

Den Quantensprung des **Raspberry Pi 4** hatten wir brandaktuell und entsprechend knapp bereits in der letzten Ausgabe, inzwischen aber die nötige Zeit, den Platinen-PC genauer zu inspizieren. Fast alles gefällt, aber er ist die bisher heißeste Himbeere. Da die Raspberry-Konkurrenz nicht untätig war, stellen wir Kandidaten vor, die neben dem neuen Raspberry Pi 4 bestehen können.

Wenn ein Raspberry, ein NAS, die Heizungs- oder Jalousiesteuerung ins Internet gehen, dann sollten Sie sicher sein, dass nicht jeder Ihre Daten liest oder Ihre Heizung steuert. Das **Sicherheitsspecial** zeigt den Umgang mit bewährten Analysetools, die offene Ports, Sicherheitslücken, Konfigurationsmängel und unfreiwillig öffentliche Daten entlarven.

Dass der **Softwarebezug 2019** unter Linux weit mehr Möglichkeiten bietet als früher, zeigt ein weiterer Schwerpunkt. Dieser erläutert die technischen Details zum klassischen Weg über die Distributions-Paketquellen und erklärt Vorteile und Nachteile alternativer Softwareauswahl durch Container, Appimages und PPAs.

Die Heft-DVD mit Distributionen und 75 LinuxWelt-Ausgaben

Die Liste rechts zeigt die auf Heft-DVD enthaltenen Systeme und Inhalte. Die Benutzung der DVD ist einfach: Das gesammelte Heftarchiv von 15 Jahren LinuxWelt, das obligatorische Zusatzheft LinuxWelt Digital XXL (PDF), den interaktiven Wahl-O-Mat, ferner Distributionsvorstellungen und Software erreichen Sie unter jedem System nach Einlegen der DVD im Dateimanager. Beachten Sie, dass auf der DVD auch die ISO-Dateien der Linux-Systeme zu erreichen sind – für die manuelle Weiterbearbeitung (siehe unten).

Um hingegen ein Livesystem zu starten, müssen Sie den Rechner 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 von der DVD 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 einen DVD-Rohling schreiben oder auf USB kopieren und dieses Medium im Uefi-Modus booten. ■



Raspberry Pi 4, Zubehör, Platinenkonkurrenz und Mini-PCs: Den Test des neuen Raspberry Pi 4 ergänzen weitere Beiträge, die empfehlenswertes Zubehör und alternative Hardware vorstellen.

AUF DVD

Distributionen

- 10 Manjaro XFCE 18.1** (64 Bit)
Arch-Linux mit neuestem XFCE
- 11 Parrot-OS Home 4.6** (64 Bit)
Deskoptaugliches Spezialsystem
- 12 Q4-OS 3.8** (64 Bit)
Schlanker Desktop für Altgeräte
- 13 Bionic Pup 8.0** (32 Bit)
Flexibles Zweit- und Minisystem
- 14 Linux Mint 19.2** (64 Bit)
Desktop-Linux in neuer Auflage

„Extras und Tools“

Boothelfer & Hardwareanalyse: Supergrub, Memtest, Hardware Detection Tool (HDT), Plop-Bootmanager
75 x LinuxWelt 2004–2019 (PDF)
 15 Jahre LinuxWelt: Zum Jubiläum sämtliche 75 Ausgaben der LinuxWelt im PDF-Format
LinuxWelt Digital XXL (PDF)
 326 Seiten technische Grundlagenartikel und Distributionsratgeber
LinuxWelt Wahl-O-Mat
 Interaktiver Fragebogen zur Auswahl der optimalen Linux-Distribution
Software für Linux und Windows
 Tools für Linux-Image-dateien



Fünf Linux-Systeme

Frisches Mint und bunte Exoten



Linux Mint 19.2 (64 Bit)

Etwas länger hat Linux Mint 19.2 auf sich warten lassen und kam wegen seines späten Erscheinungstermins nicht mehr in die letzte Ausgabe der LinuxWelt. Die Verzögerung hatte aber triftige Motive, denn die Mint-Entwickler ließen Verbesserungen in den Cinnamon-Desktop und den Window-Manager einfließen, die eine spürbare Beschleunigung im Aufbau von Menüelementen und Programmfenstern bringen. Das System liegt auch als originalgetreue ISO-Datei auf Heft-DVD.



Parrot-OS Home 4.6 KDE (64 Bit)

Das spezialisierte System ist nicht nur für Sicherheitsexperten und ambitionierte, sicherheitsbewusste Anwender interessant: Parrot-OS ist ein Debian-System aus dem Testingzweig, das sich auch als universelles Desktopsystem eignet. In dieser Ausgabe ist ein KDE Plasma 5.14 als Arbeitsumgebung vorinstalliert sowie typische Anwendungen für den täglichen Betrieb. Es gibt aber auch alle Sicherheitstools aus den Parrot-OS-Paketquellen zur nachträglichen Installation.



Q4-OS 3.8 (64 Bit)

Q4-OS kann als Ersatz für Windows 7 auf Bürorechnern dienen: Dieses Debian-System ist auf alte Hardware zugeschnitten und arbeitet mit dem besonders schlanken Desktop Trinity, der KDE 3.5 als Abspaltung am Leben erhält. Das Aussehen ist jenem von Windows 2000 nachempfunden. Q4-OS 3.8 ist ein Livesystem zum Ausprobieren und Installieren. Es liegt auch als ISO-Datei auf Heft-DVD.



Manjaro XFCE 18.1 (64 Bit)

Die enorme Auswahl an sehr aktuellen Desktopumgebungen aus den Arch-Linux-Paketquellen macht das Arch-basierte Manjaro immer wieder zu einem attraktiven Livesystem für die Heft-DVD. Aktueller Grund für dieses Manjaro ist die eben erschienene neue Version von XFCE 4.14, die vier Jahre in der Entwicklung war. Das Livesystem präsentiert den brandneuen Desktop und erlaubt die Installation über einen komfortablen Installer. Das System liegt auch als ISO-Datei auf Heft-DVD.



Bionic Pup 8.0 (32 Bit)

Linux-Systeme für richtig alte Computer, die kein 64-Bit-System stemmen, werden rar, sterben aber nicht aus. Diese Ausgabe von Puppy Linux ist ein kom-



paktes und ausbaufähiges Livesystem, das auf Ubuntu 18.04 „Bionic Beaver“ basiert – daher sein Name. Bionic Pup liefert einen Kernel 4.9 für betagte 32-Bit-Rechner mit.

Extras & Tools

Super Grub Disk 2.0.4rc1

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

Plop Bootmanager 5

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

Hardware Detection Tool 0.5.2

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

Memtest 86+ 5.01

Der aktuelle Memtest 86+ testet den Arbeitsspeicher und unterstützt auch moderne Intel-Chipsätze. Das Diagnoseprogramm läuft auf jedem PC und erkennt sowohl 32-Bit- als auch 64-Bit-CPU's sowie alle vorbereiteten RAM-Typen. Es beginnt sofort nach dem Start mit den Tests, die jederzeit unterbrochen werden können.

DBAN 2.3

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

Software auf DVD

InfraRecorder 0.53

Das Open-Source-Brennprogramm für Windows (u. a. zum Schreiben von Linux-Livesystemen) liegt auf Heft-DVD als installierbare und als portable Version vor.

Unetbootin 6.61

Das nützliche Tool mit grafischer Oberfläche transferiert mit wenigen Klicks die ISO-Images von Ubuntu und seinen Abkömmlingen wie Linux Mint sowie einige Distributionen mehr bequem 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 Linux-Distributionen), aber auch eine Version für Windows und Mac-OS X.

Putty 0.72

Der Terminalclient für SSH und Telnet ermöglicht Windows-Systemen seit vielen Jahren den Zugriff auf Linux-SSH-Server. Putty liegt in Form einer portablen EXE-Datei vor, die ohne Installation unter allen Windows-Versionen läuft. Das Open-Source-Programm ist englischsprachig.

Kitty 0.71.0.4

Diese Abspaltung von Putty ist ein weitgehend funktionsgleicher Terminalclient für SSH, allerdings mit einigen ergänzten Funktionen und bequemen Features. Wie Putty startet es einfach über seine EXE-Datei.

Win 32 Disk Imager 1.0

Das kleine Windows-Programm überträgt ISO-Images und IMG-Dateien bootfähig auf USB und SD-Speicherkarten und arbeitet analog einer Rohkopie mit dd unter Linux. Das Programm liegt als ZIP-Archiv auf Heft-DVD, das keine 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 mit gängigen Formaten wie ZIP, CAB, RAR, ARJ zurecht, sondern auch mit typischen Linux-Formaten wie GZ. Das Tool liegt in 64 Bit und 32 Bit auf Heft-DVD.

Wahl-0-Mat für Linux-Distributionen

Der überarbeitete Fragebogen und das 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



LinuxWelt

Sämtliche Jahrgänge seit 2004!

Die LinuxWelt (früher „PC-WELT Linux“) wird 15 Jahre alt. Als Service für unsere treuen Leserinnen und Leser liegen alle 75 Ausgaben von 2004 bis heute als PDF-Dateien auf der Heft-DVD. Beim Stöbern in jüngeren Jahrgängen gelten viele technische Anleitungen unverändert. Die ganz frühen Ausgaben haben eher historischen Zeugniswert und mancher Screenshot ist ein sehenswerter Nachweis für 15 Jahre Desktopentwicklung unter Linux.

LinuxWelt XXL digital

Das komplette Handbuch 6/19



Nachschub zum Nachschlagen in älteren Ausgaben:

Diesmal kommt das aktualisierte digitale „Handbuch“ als PDF-Datei mit ausgewähltem Linux-Know-how vergangener Ausgaben auf 326 Seiten. Einige ältere Beiträge sind entfernt und neue Artikelserien sind hinzugekommen. In den Grundlagen gibt es für Einsteiger eine systematische Anleitung zur Übertragung von ISO- und IMG-Dateien auf externe Medien. In der Rubrik „Software“ finden sich alle Beiträge zum Thema Virtualisierung aus der letzten LinuxWelt-Ausgabe. Neben der Kernel Virtual Machine (KVM), Qemu und Vmware erhält Oracles Virtualbox die meiste Aufmerksamkeit.

Weitere Infos

Die Vorstellung der fünf Systeme auf DVD beginnt ab Seite 10, wobei Linux Mint 19.2 eine großen eigenen Artikel ab Seite 14 erhält. 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. In diesem Heft gibt es zwei Schwerpunkte: Ab Seite 26 geht es um Sicherheitsanalysen im Netzwerk und auf Servern mit den wichtigen Linux-Tools. Das zweite Special „Software für Linux“ nimmt sich ab Seite 42 die Paketformate von Linux-Distributionen, externe Paketquellen, Containerformate sowie die Prinzipien der Softwareinstallation vor.

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 „Hacking & Security“ aus dem Rheinwerk Verlag.

Hacking & Security

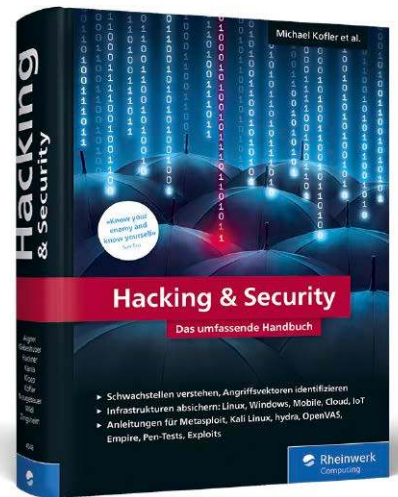
Das umfassende Handbuch

Autoren: Michael Kofler, André Zingsheim, Klaus Gebeshuber, Markus Widl, Roland Aigner, Thomas Hackner, Stefan Kania, Peter Kloep, Frank Neugebauer

Verlag: Rheinwerk Verlag, über 1000 Seiten, gebunden, 49,90 Euro
ISBN: 978-3-8362-4548-7

It's not a bug, it's an exploit! Nur wenn Sie verstehen, wie ein Angreifer denkt, können Sie Ihre Systeme auch wirklich sicher machen. Dieses Buch ist der Schlüssel dazu. Die Security-Profis rund um Bestsellerautor Michael Kofler vermitteln Ihnen das ganze Know-how, um Ihre Infrastrukturen vor Angriffen zu schützen – Praxisbeispiele und konkrete Szenarien inklusive. Hier werden Sie zum Security-Experten!

Aus dem Inhalt: • Kali Linux • Hackingtools (nmap, hydra, Metasploit, Open VAS) • Externe Sicherheitsüberprüfung • Penetration Testing (Client und Server) • Basisabsicherung für Linux und Windows, Active Directory und Samba • Cloudsicherheit (AWS, Nextcloud, Office 365) • Hacking und Security von Smartphone & Co. • Webanwendungen absichern und angreifen • Exploits (Buffer Overflows, Fuzzing, Heap Spraying) • IoT-Geräte und -Infrastruktur



PLUS:
Gratisheft
für alle
Teilnehmer

SO FUNKTIONIERT'S:

Auf www.pcwelt.de/lin gelangen Sie direkt zu unserer Leserbefragung und nehmen automatisch an der Verlosung teil. Von der Verlosung ausgenommen sind Mitarbeiter des Verlags und deren Angehörige. Der Rechtsweg ist ausgeschlossen.

Einsendeschluss für das Gewinnspiel in

LinuxWelt 6/2019 ist der 25.11.2019.

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 Telekommunikationsdienstestegesetzes (ItuTDG) 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 »Google Maps« 03/2019 als PDF (ohne Datenträger). Sie finden den Link zum Download des Hefts am Ende der Leserbefragung.



Manjaro 18.1

Manjaro ist eine der ersten Distributionen, die das neue XFCE 4.14 mitliefern (64-Bit-Version auf DVD). Die Pakete stammen von Arch Linux. In Manjaro gibt es aber einen komfortablen Installer zur Beseitigung von Einstiegshürden.

VON DAVID WOLSKI

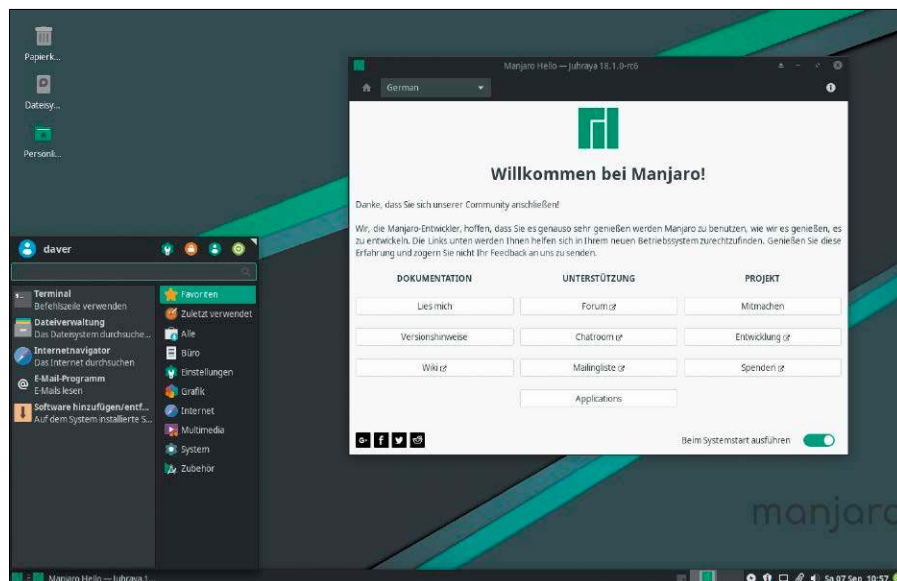
Es fällt Manjaro nicht schwer, immer besonders früh aktuelle Softwarepakete und Linux-Desktops zu präsentieren. Denn in Arch Linux, auf dem dieses System basiert, ist der Weg vom Quellcode zum fertigen Paket vergleichsweise kurz. Neue Softwareversionen kommen ohne Unterbrechung durch einen festen Entwicklungszyklus in die Paketrepositoryn.

Und so ist Manjaro 18.1 die erste Linux-Distribution, die das brandneue XFCE 4.14 zeigen kann, welches in anderen Systemen erst in einigen Monaten Einzug erhalten wird. XFCE lässt sich natürlich auch selbst kompilieren oder in Arch Linux jetzt schon installieren. Die Lernkurve dazu ist aber steil und schon die Einrichtung von Arch Linux eine Aufgabe für fortgeschrittene Anwender. Mit dem Arch-Abkömmling Manjaro gelingt ein entschärfter Einstieg: Diese Distribution bringt ein installierbares Livesystem und einen grafischen Installer, der die gewünschten Einstellungen Schritt für Schritt abfragt und im Stil von Ubuntu gehalten ist.

Manjaro ist ein Rolling Release, das sich dauerhaft über den Paketmanager auf dem neuesten Stand halten lässt. Manjaro ist kein pures Arch-System, da es seine Pakete nicht aus den originalen Arch-Repositories bezieht, sondern auf eigene Quellen zurückgreift. Für Anwender bedeutet das, dass Updates etwas später als unter einem echten Arch Linux erscheinen. Stichpunktartig durchlaufen die neuen Pakete in der Manjaro-Community weitere Tests.

XFCE holt wieder auf

Eine Weile sah es so aus, als wäre die Weiterentwicklung der schlanken Desktopumgebung XFCE beendet. Aber nun ist nach mehr als vier Jahren Entwicklungszeit Version 4.14 erschienen, die den Desktop fit



Neues XFCE: Als besonders aktueller Arch-Linux-Abkömmling hat Manjaro die aktuelle Version des schlanken Desktops als erste größere Distribution an Bord.

für die Zukunft macht. Die Desktopelemente sind dazu komplett nach GTK3 portiert, also dem Toolkit von Gnome 3.x, das auch die Skalierung von Programmen für hohe Auflösungen möglich macht.

Für den Einsatz mehrerer Monitore oder eines zusätzlichen TVs kann XFCE nun mehrere Einstellungen speichern und abrufen. Der weiterhin sparsame Desktop ist damit wieder eine Wahl für Anwender, die eine schlichte, sparsame, jetzt aber auch moderne Arbeitsumgebung suchen. In der XFCE-Ausgabe installiert Manjaro 18.1 eine Soft-

wareausstattung, wie sie für Gnome-affine Distributionen typisch ist: Firefox ist als Browser vorinstalliert, Thunderbird als Mailprogramm, Libre Office als Bürosuite und VLC als Videoplayer. Für die Paketverwaltung liefert Manjaro ein eigenes grafisches Front-End, um auch weniger versierten Anwendern und Arch-Neulingen etwas Komfort zu bieten. ■

Mehr Infos zu Manjaro

Website: <http://manjaro.org>

Dokumentation: <http://wiki.manjaro.org>

Nachträglich einrichten:

Auf DVD liegt Manjaro mit XFCE in der Minimalversion. Im grafischen Paketmanager sind die benötigten Programme schnell nachinstalliert.



Parrot-OS 4.6 Home

Nicht nur auf Sicherheits-Checks getrimmt: Das Debian-System hat auch auf dem Desktop viele Freunde gefunden, da die Entwickler einen Sinn für Ästhetik haben. Parrot-OS ist in 64 Bit und dem Desktop KDE auf Heft-DVD.

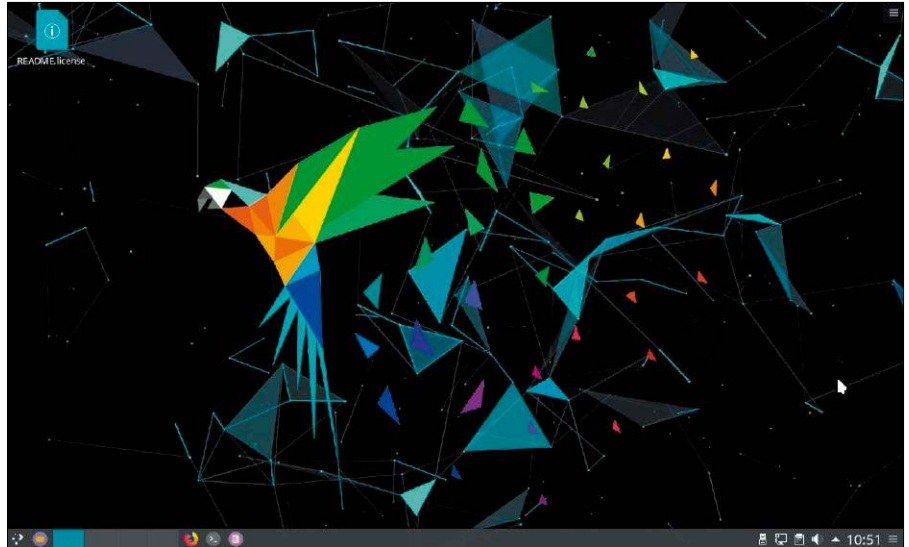
VON DAVID WOLSKI

Ursprünglich ist Parrot als (Un-)Sicherheits-Distribution mit vielen Hacking- und Pentestingtools entstanden und das bleibt auch sein Haupteinsatzzweck. Daneben hat sich aber auch eine Ausgabe von Parrot-OS für den universellen Desktopeinsatz etabliert, die mit Mate und wahlweise KDE Plasma 5 vorliegt und erst mal keine sicherheitsspezifischen Programme vorinstalliert. Aber keine Sorge: Diese lassen sich bei Bedarf nachinstallieren. Die Desktops von Parrot-OS, das mit Mate und KDE vorliegt, haben mit einer farnefrohen Aufmachung und sorgfältigen Zusammenstellung auch unabhängig vom Einsatzbereich dieser Sicherheitsdistribution viel Zuspruch erhalten.

Debian Testing mit Extras

Anwender fragten bei den Entwicklern nach, ob es diesen Desktop nicht auch einzeln mit dem vorgefertigten Aussehen gäbe. Auf diese konkreten Nachfragen hin entstand eine Desktopversion von Parrot-OS, das als installierbares Livesystem für den alltäglicheren Einsatz konzipiert ist und damit auch erst einmal zum unverbindlichen Test einlädt.

Es handelt sich um ein Debian-Derivat mit den Paketen aus dem Testingzweig, also um eine Distribution, die sich laufend aus den Paketquellen aktualisiert. Das bedeutet neuere Pakete in Debian, aber auch bisweilen einen höheren Administrationsaufwand, wenn größere Updates anliegen. Dann sind hin und wieder Nacharbeiten an der Konfiguration nötig. Dies ist der Preis von allen Linux-Systemen, die dem Modell eines Rolling Release folgen. Beim Einsatz von KDE Plasma 5, das in der Ausgabe auf Heft-DVD der Desktop ist, gibt es dabei aber den Vorteil, laufend Verbesserungen aus der schnell fortschreitenden Entwicklung dieser Arbeitsumgebung zu bekommen.



Farnefrohen: Parrot-OS Home, hier mit KDE Plasma 5, präsentiert sich als bunter Vogel. Die Sicherheitstools der Spezialdistribution warten in den Paketquellen.

Hürden bei der Installation

Zur Einrichtung auf Festplatte sind der grafische und der textbasierte Debian-Installer über das Bootmenü der Heft-DVD verfügbar. Bei diesem Installer ist es essentiell, die Festplatte eigenhändig mit dem einfachen Partitionierer des Installationsprogramms aufzuteilen und dabei eine Partition „/boot“ mit mindestens einem GB Größe einzurichten. Die vorgegebenen Standards bei einer geführten automatischen Partitionierung sind nicht ausreichend, um danach ein funktionierendes System zu erhalten. Die vorliegende Ausgabe mit KDE enthält ein KDE Plasma 5.14 und eine Auswahl an Programmen für den Desktopbetrieb wie Libre Office 6.1 und Firefox 68. Der Charme dieses System ist aber, dass sich auch die Sicherheitstools der regulären Parrot-Ausgabe installieren lassen. Dafür ist der grafische Paketmanager Synaptic enthalten. Eine komplette Systemaktualisierung muss in der Kommandozeile mit dem Befehl

```
sudo parrot-upgrade
```

durchgeführt werden, der eine komplette Systemaktualisierung aller Pakete mit „`apt-get dist-upgrade`“ durchführt, was bei Debian Testing der einzig empfohlene Weg ist. Insgesamt ist Parrot-OS Home eine anspruchsvolle Debian-Variante für ambitionierte Anwender mit Interessen an sicherheitsrelevanten Linux-Werkzeugen sowie für Sicherheitsexperten, die ein universelles Desktopsystem bevorzugen, das mehrere Rollen erfüllen kann. ■

Mehr Infos zu Parrot-OS

Website: <https://parrotlinux.org>

Dokumentation: <https://docs.parrotlinux.org>

```
daver: bash — Konsole
Datei Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe
[daver@parrot]-[~]
└─$ uname -a
Linux parrot 4.19.0-parrot4-28t-amd64 #1 SMP Parrot
parrot4.28t (2019-04-18) x86_64 GNU/Linux
[daver@parrot]-[~]
└─$
```

Ungewöhnliche Shell: Die Bash-Befehlszeile, relevant für die meisten Sicherheitstools und Scanner, hat in Parrot-OS ebenfalls ein buntes Gewand.

Q4-OS 3.8

Spezialist für ältere Rechner: In Q4-OS steht der Desktop Trinity im Mittelpunkt, der KDE 3.5 als schlanken, ansehnlichen Desktop im Stil von Windows XP/7 am Leben erhält. Q4-OS 3.8 (in 64 Bit auf DVD) aktualisiert den Unterbau auf Debian 10.

VON DAVID WOLSKI

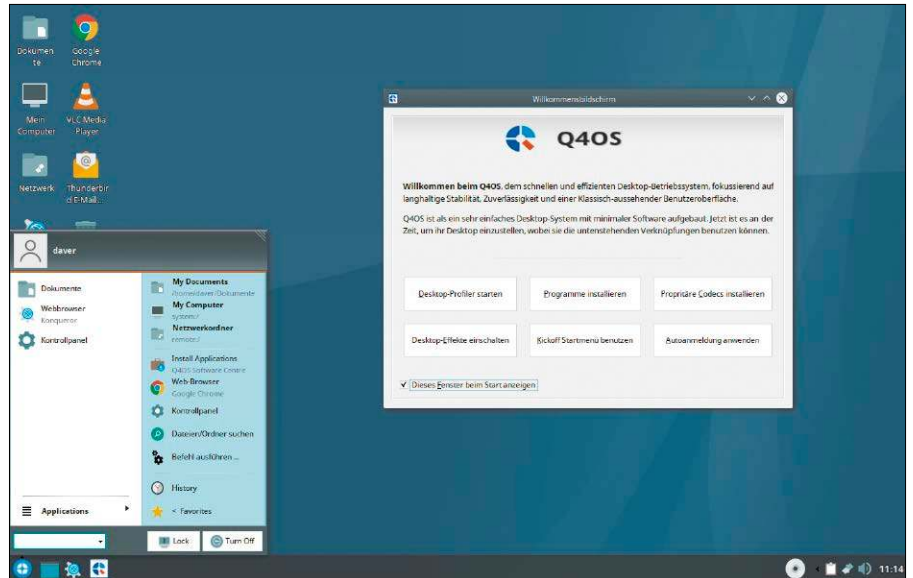
Für das neue Debian „Buster“ hatte unsere DVD aufgrund des Umfangs der neuen Installationsmedien kein Platz mehr, dafür aber für den modernisierten Debian-Ableger Q4-OS. Dieser ist für den Ersatz für das auslaufende Windows 7 auf älteren PCs interessant, die kein Windows 10 mehr stemmen können. Das schlanke Linux-System mit der soliden Debian-Basis läuft auf solchen PCs der letzten zehn Jahre meistens ausreichend flott.

Alt trifft neu: Desktop und Betriebssystem

Q4-OS steht ganz klar im Schatten der großen bekannten Linux-Distributionen, obwohl es seit sechs Jahren regelmäßig erscheint. Sein primärer Einsatzzweck ist auch speziell, denn Q4-OS geht es um geringe Hardwareanforderungen, die es mit einem traditionellen und schlanken Desktop kombiniert. Die Oberfläche mit dem Namen Trinity dürfte erfahrenen Anwendern ein alter Bekannter sein und Linux-Einsteigern eine vertraute Arbeitsumgebung bieten, die sich an Windows-Standards orientiert. Trinity ist aus KDE 3.5 entstanden, das zwar schon seit KDE 4 nicht mehr weiterentwickelt wird, aber in dieser Abspaltung weiterhin Fehlerbehebungen und kleine Ergänzungen bekommt. Deshalb funktioniert unter Trinity beispielsweise der aktuelle Networkmanager, der Hardwaremanager Udev und der Fenstercompositor Compton, der für dezente Effekte sorgt. Eine Menge älterer KDE-Programme wie das „Kontrollpanel“, der Dateimanager Konqueror und der Texteditor Kate sind in Trinity noch in ihrer einstigen Fassung vorhanden.

Pakete von Debian 10

Bei den Programmen für den Alltag setzt Q4-OS grundsätzlich auf neue Software



Q4-OS mit dem Desktop Trinity: Trinity lässt KDE 3.5 als Fork weiterleben. Das Resultat ist ein klassischer Desktop mit einer gewissen Ähnlichkeit mit alten Windows-Systemen.

und erleichtert Einsteigern die Einrichtung des Systems nach der Installation mit der Auswahl fertiger Softwaresets. Optional stehen Libre Office, Chromium als Browser, VLC als Videoplayer und Thunderbird als Mailprogramm zur Verfügung. Unter Debian immer gerne gesehen ist auch die Möglichkeit, Mediacodecs per Klick nachzurüsten. Zur Verwaltung einzelner Pakete ist Synaptic vorinstalliert.

Trinity ist kein Mainstreamdesktop und Unterstützung für Hi-DPI-Bildschirme darf man auch nicht erwarten. Q4-OS zeigt aber, dass die alte KDE-Fassung mit ergänzenden Zutaten und Modernisierungen noch nicht obsolet ist. Es handelt sich um einen stimmigen Desktop für konservative Anwender und Umsteiger, die bisher mit Windows 7 arbeiteten. Auf Heft-DVD ist Q4-OS diesmal in der 64-Bit-Ausgabe, denn nur für diese Architektur gibt es die Distribution noch als Livesystem, das einen Test von System und Desktop ohne Installation erlaubt. Auf der Projektwebseite gibt es das System für rich-

tig alte PCs auch noch als bootfähigen Installer in 32 Bit. Der Installer startet gleich in Deutsch und beruht auf dem Programm Calamares, das sich auch in Manjaro oder Kubuntu um die Installation kümmert. Q4-OS 3.8 soll die nächsten fünf Jahre Aktualisierungen bekommen, die zumeist von Debian 10 stammen. ■

Mehr Infos zu Q4-OS

Website: <http://q4os.org>

Dokumentation:

<http://q4os.org/documents.html>



Komfortabler Installer: Zur Einrichtung auf der Festplatte nutzt Q4-OS jetzt den grafischen Installer Calamares, der im Stil des Ubuntu-Installers gehalten ist.

Bionic Pup 8.0

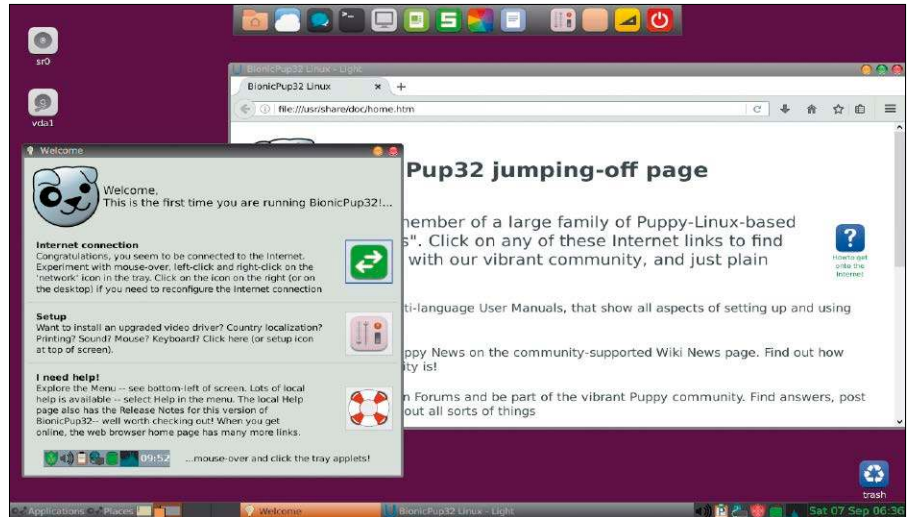
Nachwuchs aus der Puppy-Familie: Bionic Pup 8.0 (in 32 Bit auf Heft-DVD) ist als schnelles, nicht ganz minimales Livesystem aus den Paketen von Ubuntu 18.04 gebaut und kann zur Laufzeit Software aus dessen Quellen nachladen.

VON DAVID WOLSKI

Mit der schwindenden Zahl an 32-Bit-Distributionen bekommt Puppy Linux wieder etwas mehr Aufmerksamkeit. Bionic Pup 8.0 läuft als Livesystem mit Browser und großer Auswahl an zusätzlichen Paketen auch auf alten Rechnern mit 32-Bit-CPU. Bei Puppy Linux handelt es sich nicht um eine eigenständige Linux-Distribution, sondern um eine Methode, vorhandene Distribution zu einem möglichst kleinen Livesystem zu machen und auf das Wesentliche zu reduzieren. Während viele Projekte Linux-Systeme als Grundlage nehmen, die mit weiteren Ergänzungen ausgebaut werden, geht Puppy den umgekehrten Weg und entfernt zunächst viele Komponenten. Dazu dient das eigene Baukastensystem Woof-CE, das die Reduktion einer Linux-Distribution mit Scripts vereinfacht. Die Resultate sind Livesysteme mit eigener Bootumgebung und komfortablen Konfigurationstools, die auch auf sehr alter Hardware einen ansehnlichen Linux-Desktop starten.

Start als pures Livesystem

Alle offiziellen Puppy-Ausgaben gehen auf das gleiche Build-System zurück. Die Startprozedur ist recht ähnlich und führt im Nu zu einem einsatzfähigen Desktop, mit dem auch Anfänger trotz englischsprachiger Oberfläche gut zurechtkommen dürften. Nach dem Start kann man die gewünschte Bildschirmauflösung und die Tastenbelegung auswählen. Die vorliegende Version nutzt die äußerst schlanke Desktopumgebung JWM. Für WLAN-Verbindungen steht der Frisbee Network Manager bereit. Als Browser ist eine leichtgewichtige Version von Firefox 48 namens „Light“ vorinstalliert. Das gesamte System hat eine Größe von nur 325 MB und außer dem Webbrowser, der Illustrationssoftware Inkscape und einigen Playern sind keine größeren An-



Schnelles Livesystem: Wie in allen Puppy-Varianten ist in Bionic Pup ein Firefox-Webbrowser vorinstalliert. Auch der Partitionierer Gparted (Version 0.30) ist mit von der Partie.

wendungen vorinstalliert. Diese lassen sich bei Bedarf temporär zur Laufzeit des Livesystems aus den Paketquellen nachladen. Zur Paketverwaltung von Puppy gelangt man über das Paketsymbol im oberen Dock und dort über „Install Applications → Puppy Package Manager“.

Als Zweitsystem auf USB-Sticks

An gleicher Stelle über das Paketsymbol geht es zur Einrichtung von Bionic Pup auf USB-Laufwerk oder auf eine interne Festplatte. Eine schnelle Übertragung des Livesystems für Uefi-Systeme ist mit „Install Puppy → Bootflash USB Installer → UEFI USB Installer“ möglich. Ein angesteckter USB-Stick muss vorher mit FAT32 formatiert werden. Dies kann der Partitionierer Gparted im Livesystem erledigen. Für den Boot im Bios-Modus eignet sich dagegen „Install Puppy → Bootflash USB Installer → Create grub4dos USB“.

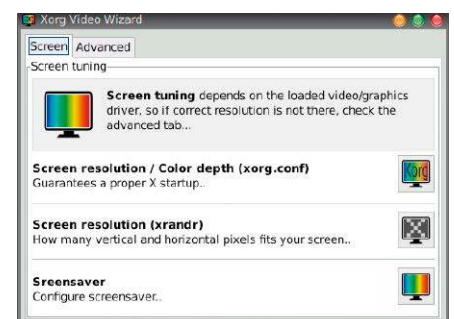
Generell ist Bionic Pup als Zweitsystem auf USB-Sticks gut aufgehoben, aber für besonders alte Rechner kann auch die Installation auf einem internen Datenträger interes-

sant sein. Dazu gibt es wieder einen separaten Installer unter „Install Puppy → Universal Installer“. Der Installer überträgt das System auf eine bereits existierende Partition mit Ext3- oder Ext4-Dateisystem. Eine parallele Installation zu anderen Linux-Systemen ist nicht möglich. ■

Mehr Infos zu Bionic Pup

Webseite: <http://puppylinux.com>

Dokumentation: <http://puppylinux.org/wikka/HomePage>



Bionic Pup nach dem Start konfigurieren: Falls die Bildschirmauflösung nicht passt, sind die Einstellungen schnell geändert.

Linux Mint 19.2 („Tina“)

Die letzte LinuxWelt konnte anhand der frühen Alphaversion über geplante Neuerungen im jüngsten Linux Mint 19.2 berichten. Seit Anfang August liegt das finale System vor. Dieser Artikel informiert ausführlich und die Heft-DVD liefert die Cinnamon-Edition mit.

VON HERMANN APFELBÖCK

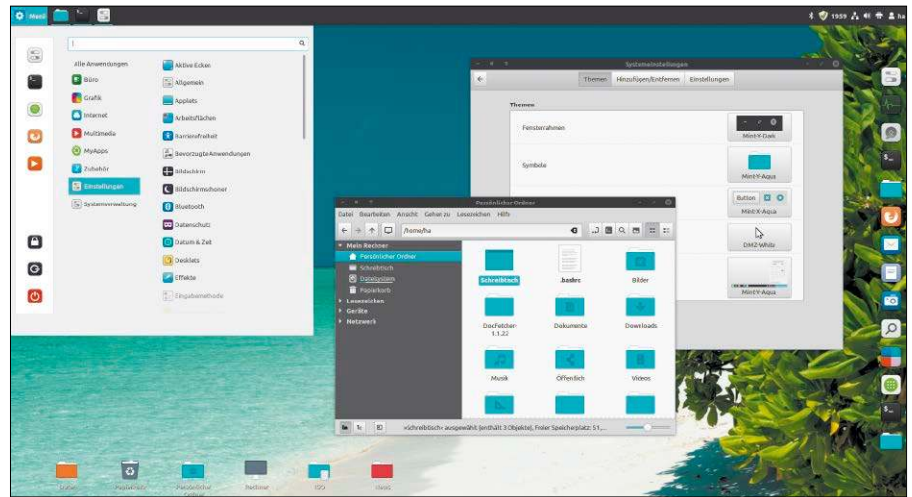
Wie gewohnt zieht Linux Mint seine Bahnen etliche Monate nach seiner Systembasis Ubuntu LTS. Dieses vollzog am 15. Februar 2019 seinen Schritt zum Release Point 18.04.2 LTS, dem Linux Mint Anfang August als Version 19.02 mit reichlich Verspätung nachfolgte. Damit steckt das Mint-Team sofort in der nächsten Aufgabe, denn ebenfalls Anfang August veröffentlichte Canonical bereits das nächste Release Point Ubuntu 18.04.3, dem Mint dann voraussichtlich im Spätherbst folgen wird.

Neben der Hauptedition mit Cinnamon-Desktop gibt es Linux Mint weiterhin mit einem leicht überarbeiteten Mate-Desktop 1.22 und mit XFCE, das mit Version 4.12 am Desktop unverändert bleibt. Alle Ausgaben erhalten Sie in 32- wie 64-Bit-Architektur über die Seite <https://linuxmint.com/download.php>, die zu diversen deutschen und internationalen Spiegeldern verlinkt (je circa zwei GB bei allen Varianten). Die nach unserer Meinung entscheidende Edition ist jene mit Cinnamon-Desktop, der den Wesenskern von Linux Mint ausmacht. Diese Hauptedition finden Sie in der 64-Bit-Ausführung bootfähig auf Heft-DVD.

Dieser Beitrag bietet einen Durchgang durch das neue System mit Fokus auf die neuen Funktionen. Da wir nicht davon ausgehen können, dass alle Leser die letzte LinuxWelt vorliegen haben (Artikel auf Basis der Alphaversion), nehmen wir einige Wiederholungen in Kauf.

Linux Mint 19.2: aktuell genug

Aufgrund seiner Produktionsweise kann Linux Mint bei Kernel, Unterbau und Softwareversionen niemals ein „Cutting Edge“-Trendsetter sein, zumal schon seine Systembasis Ubuntu dies nicht leistet. Version



19.2 hat daher einen relativ betagten Linux-Kernel 4.15 an Bord, dieser allerdings mit Langzeitunterstützung bis 2023. Auch die mitgelieferte Standardsoftware wie Libre Office oder Gimp datiert zumeist aus dem Jahr 2018. Geschadet hat diese bedächtige Erscheinungsweise diesem beliebtesten Ubuntu-Derivat allerdings nie: Der exzellente und stets mit Detailliebe weiterentwickelte Cinnamon-Desktop (jetzt Version 4.2) entschädigt den Anwender reichlich. Linux Mint 19.2 versteht sich als Langläufer und ist wie Ubuntu eine Langzeitversion, die bis 2023 unterstützt wird.

Frische Kernel: Für Nutzer aktueller Hardware, die jüngere Kernel mit neuen Treibern benötigen, hat Linux Mint 19.2 Lösungen parat: Die „Aktualisierungsverwaltung“ (mintupdate) kann in Version 19.2 über „Ansicht → Linux Kernel“ einen jüngeren Linux-Kernel 5.x installieren. Dies ist ein Systemeingriff, der zu Problemen führen kann, aber keineswegs muss – Ausprobieren hilft. Da der mit Linux Mint 19.2 mitgelieferte Kernel 4.15 weiter vorliegt, können Sie im Notfall im Grub-Bootmana-

ger zu diesem Kernel zurückkehren. Unter „Erweiterte Optionen für Linux Mint“ ist der ältere Kernel im Grub-Menü nach wie vor aufgeführt und kann gestartet werden. Den problematischen jüngeren Kernel können Sie in der Aktualisierungsverwaltung unter „Ansicht → Linux Kernels“ durch Markieren und „Entfernen“ auch wieder löschen, sodass dann standardmäßig wieder der ältere Kernel bootet.

Die Kernel-Verwaltung in der Aktualisierungsverwaltung unter „Ansicht → Linux-Kernel“ ist generell überarbeitet: Es wird angezeigt, wie lange der gerade aktive Kernel unterstützt wird. Außerdem gibt es die Option „Kernel entfernen“ mit einer Auswahl installierter Kernel-Versionen, wobei der aktive Kernel natürlich nicht gelöscht werden kann und auch nicht angeboten wird. Unter „Bearbeiten → Einstellungen → Automatisierung“ erscheint ferner eine Option, um veraltete Kernel automatisch zu löschen. Das bringt für ein Langlaufsystem, bei dem sich über die Jahre zahlreiche Kernel-Versionen ansammeln, deutliche Vereinfachung.

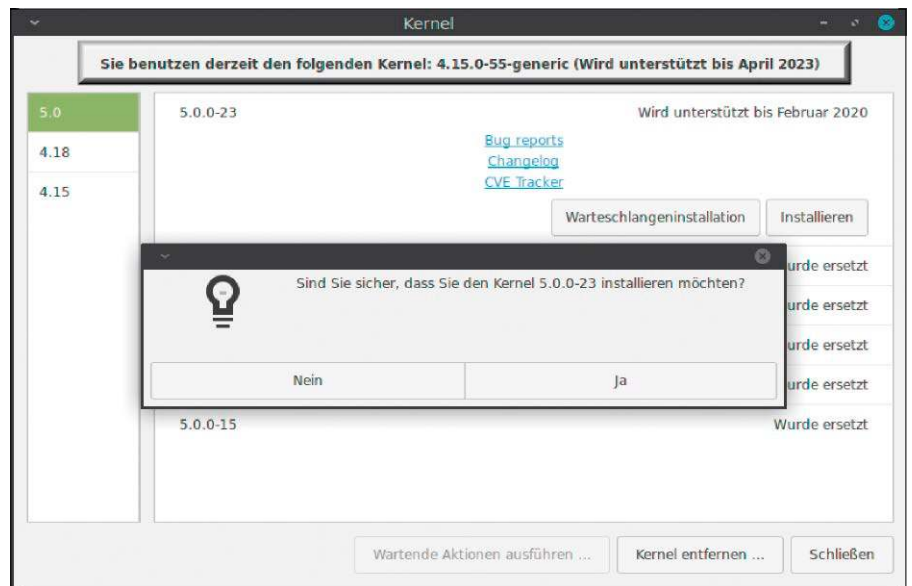
Frische Software: Anwender, die auf aktuellerer Software bestehen, sollten in der „Anwendungsverwaltung“ (mintinstall) die Sektion „Flatpak“ beachten. Dieses Containerformat liefert systemunabhängige Software aus, die alle Paketabhängigkeiten mitbringt und zum Teil weit aktueller ist als die vorinstallierten Programme. Flatpak-Container sind in der „Anwendungsverwaltung“ von Linux Mint schon seit Version 18.3 integriert. Die vergleichbaren hauseigenen Snap-Container von Ubuntu lehnt Linux Mint ab, da der Snap Store unter alleiniger Kontrolle von Ubuntu/Canonical steht. Beachten Sie beim Einsatz von Flatpak-Software, dass Sie die Systemunabhängigkeit der Programme mit erheblichen Download- und Installationsgrößen bezahlen müssen: Flatpaks sollten Sie nur bei Software wählen, bei der die aktuellere Version für Sie eine entscheidende Rolle spielt (eine Tatsache, die analog für die Ubuntu-Snaps gilt).

Linux Mint 19.2 installieren

Wie gewohnt starten Sie die Installation über das heruntergeladene und auf USB-Stick kopierte Livesystem. Für das Kopieren des ISO-Abbilds empfehlen wir unter Linux Mint das Tool „Laufwerke“ (Gnome-Disks, Option „Laufwerksabbild wiederherstellen“) und unter Windows den Win 32 Disk Imager (auf Heft-DVD). Einziger wesentlicher Unterschied zu den früheren Installations-ISO-Images ist das zusätzliche Tool „Boot-Repair“. Es ist in der Lage, die meisten Startkonfigurationsprobleme zu beheben. Das Tool findet sich im Livesystem im hier noch englischsprachigen Menü unter „Administration“. Boot Repair ist als Nothelfer im Livesystem oder als Vorbereitung der Mint-Installation gedacht. Beim installierten Linux Mint 19.2 ist es nicht mehr an Bord.

Weitere Installationshinweise ersparen wir uns an dieser Stelle, weil Sie in diesem Heft ab Seite 86 einen Ratgeber zu allen Ubuntu-Installationsvarianten finden. Dieser gilt identisch auch für Linux Mint 19.2, das bekanntlich den Standardinstaller Ubiquity von Ubuntu verwendet. Beachten Sie bei Parallelinstallationen, dass die Heft-DVD im Bios-Modus startet.

Für eine Parallelinstallation neben einem UEFI-System (Windows oder Linux) benötigen Sie ein selbst erstelltes Medium (DVD oder USB). Auch das ist im genannten Beitrag beschrieben.



Taufrisch ist der Kernel in Linux Mint nie, da erst einmal Ubuntu den aktualisierten Kernel einbauen muss. Über die Aktualisierungsverwaltung können Sie testweise jüngere Kernel installieren.

Ein verdientvoller Unterschied zum Ubuntu-Setup bleibt aber zu erwähnen: Wie bisher zeigt auch Version 19.2 im Installationsdialog „Wer sind Sie?“ (bei der Einrichtung des Erstbenutzers) die Option „Meine persönlichen Daten verschlüsseln“. Es handelt sich um die Verschlüsselung des Home-Verzeichnisses mit Ecrypt FS, welche Ubuntu seit Version 18.04 wegen Sicherheitsbedenken ersatzlos aus dem Installer gestrichen hat. Es gibt allerdings keine gravierenden Bugs, die den Einsatz von Ecrypt FS verbieten würden. Kritiker wiesen lediglich darauf hin, dass außerhalb von „/home/[user]“ temporäre Dateien entstehen können, die dann nicht verschlüsselt sind. Das Mint-Team hat diese Bedenken verworfen und diese Option im Installer wieder zurückgebaut.

Das via Installer aktivierte Ecrypt FS verschlüsselt alle Benutzerdateien des Erstbenutzers. Die Dateien und Ordner werden

durch die Systemanmeldung dieses Benutzers automatisch entschlüsselt.

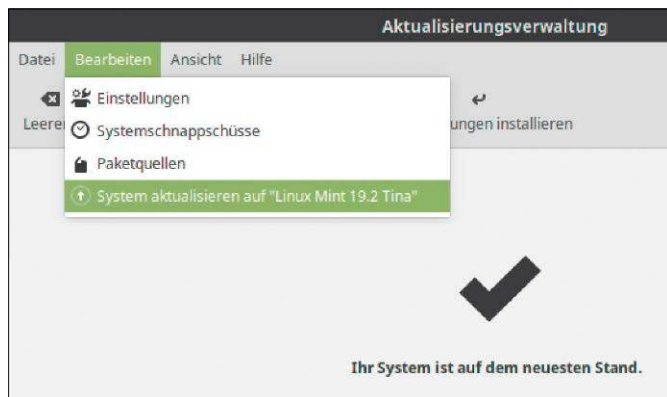
Das Upgrade von Version 19.1

Wer ein Linux Mint 19.1 laufen hat, muss natürlich nicht neu installieren, sondern kann unkompliziert upgraden und Dateien und Einstellungen erhalten. Das traditionell Upgrade-Skeptische Mint-Team empfiehlt vor dieser Aktion etliche Sicherheitsvorkehrungen. Nach unserer Erfahrung ist das Upgrade auf 19.2 eine harmlose Angelegenheit, dennoch geben wir die Empfehlungen der Entwickler hier weiter:

1. Ein manueller Snapshot mit Timeshift („Erstellen“) kann den aktuellen Systemzustand sichern und somit eine spätere Rückkehr zur Version 19.1 ermöglichen.
2. Ein eventuell genutzter Bildschirmschoner sollte deaktiviert werden („Systemeinstellungen → Bildschirmschoner“ mit Einstellung „Nie“). Wird dies versäumt, kann



Die Home-Verschlüsselung bleibt weiter erhalten: Diese nützliche Option hat das Mint-Team explizit wieder in den Ubuntu-Installer zurückgebaut.



der Upgradevorgang theoretisch in einen scheinbar abgestürzten Zustand geraten. Hier hilft es aber immer noch, mit Strg-Alt-F1 in die erste virtuelle Konsole zu wechseln und mit

```
pkill -f screensaver
```

jedigen Bildschirmschoner zu beenden und dann mit Strg-Alt-F7 zum Desktop zurückzukehren.

3. Das System sollte über die Aktualisierungsverwaltung (mintupdate) komplett auf den neuesten Stand von Version 19.1 gebracht werden, also mit den Optionen „Auffrischen“ und – falls Updates gemeldet werden – mit „Aktualisierungen installieren“. Insbesondere die Cinnamon Spices, also „Applets“, „Desklets“, „Erweiterungen“, „Themen“ (siehe „Systemeinstellungen“), sollten allesamt aktuell sein. Am sichersten ist das Upgrade, wenn nur die Standardmodule genutzt werden.

Nach diesen aus unserer Sicht eher übervorsichtigen Maßnahmen der Risikominimierung, starten Sie den Upgradevorgang in der Aktualisierungsverwaltung: Im Menü „Bearbeiten“ finden Sie den neuen Eintrag „System aktualisieren auf „Linux Mint 19.2 Tina““ – anklicken und los geht's.

Hinweis: Falls der Upgradeeintrag in der Aktualisierungsverwaltung trotz aktualisiertem System nicht auftaucht, kann man versuchen, die Aktualisierungsverwaltung manuell mittels

```
sudo apt install mintupdate mint-upgrade-info
```

auf den neuesten Stand zu bringen. Dies ist nach unserer Erfahrung aber nie notwendig.

Der gestartete Upgradeassistent zeigt zunächst einige Quellen im Web, die über die Neuheiten der neuen Version informieren. Vor dem eigentlichen Update erscheint noch eine Sicherheitswarnung. Wird diese

Upgrave von 19.1 auf 19.2: Nach der Aktualisierung des bisherigen Systems starten Sie auf diesem Weg das Upgrade.

bestätigt, beginnt der Download. Das Upgrade dauert nur wenige Minuten und endet mit der Aufforderung, den Rechner neu zu starten.

Erfreulich: Das neue Linux Mint meldet sich nicht nur im laufenden System („Systemeinstellungen → Systeminformation“) als Version 19.2, sondern auch schon im Grub-Bootmenü.

Cinnamon wird schlanker und schöner

Laut Mint-Chef Lefèbvre ist das neue Cinnamon 4.2.3 komplett überarbeitet. Der Desktop wurde entschlackt und der RAM-Bedarf um 30 Prozent reduziert. Außerdem wurde der darunterliegende Fenstermanager Muffin optimiert, um verzögerte Reaktionen der Oberfläche zu verringern. Auch das Anwendungsmenü reagiert schneller und unterscheidet jetzt Softwareduplikate. Wenn zwei Anwendungen denselben Namen tragen (etwa nach Doppelinstallation eines Programms als Deb-Paket und als Flatpak-Container), zeigt das Menü klärende Hinweise wie etwa den Zusatz „(Flat-

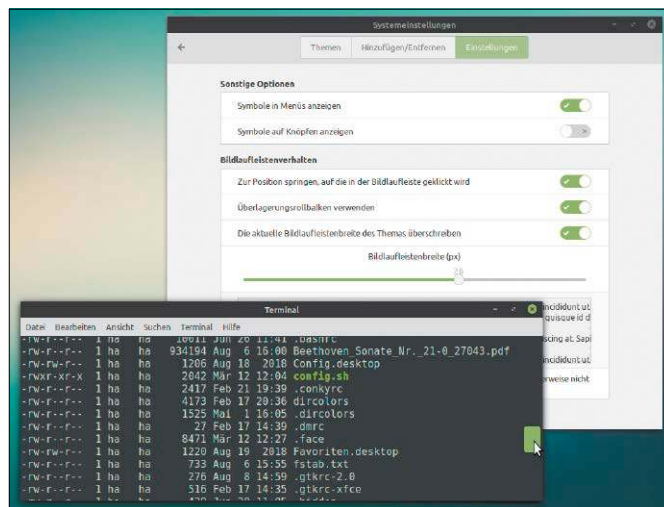
pack)“. Unter „Systemeinstellungen → Themen → Einstellungen“ gibt es die neue Option „Bildlaufleistenbreite des Themas überschreiben“. Sobald Sie dies aktivieren, erscheint darunter ein Schieberegler, mit dem Sie pixelgenau die gewünschte Breite definieren. Die Einstellung gilt für vertikale wie horizontale Laufleisten. Das Scrollen, insbesondere in Terminal und Dateimanager, wird dadurch wesentlich einfacher. Das Konfigurationstool für den Anmeldebildschirm („Systemeinstellungen → Anmeldefenster“) erhält unter „Benutzer“ eine neue Option.

Neben „Verzögerung...“ erscheint ein neues Feld, um eine Wartezeit in Sekunden für die automatische Benutzeranmeldung zu bestimmen. Dadurch wird es möglich, zwar einerseits den PC-Standardbenutzer automatisch anzumelden, andererseits aber die Option offenzuhalten, vorher ein anderes Konto auszuwählen.

Unter „Systemeinstellungen → Allgemein“ erscheint die Option „Vsync-Methode“. Es handelt sich um eine Videokorrektur, die störende Tearing-Artefakte beim Abspielen von Filmen verhindern kann. Während das Umschalten der Vsync-Methode früher einen Neustart des Desktops erforderte, können Sie im jüngsten Cinnamon unterbrechungsfrei damit experimentieren.

Weiterer Feinschliff an der Optik zielt primär auf den Cinnamon-Desktop, jedoch profitieren auch die Mate- und XFCE-Edition davon. Es handelt sich aber nur um minutiöse Feinheiten der Farbwerte, um die Kontraste zu optimieren. Im Alltag wird das keinem Anwender auffallen, da selbst beim direkten Vergleich mit dem Vorgänger ein sehr genauer Blick notwendig wird.

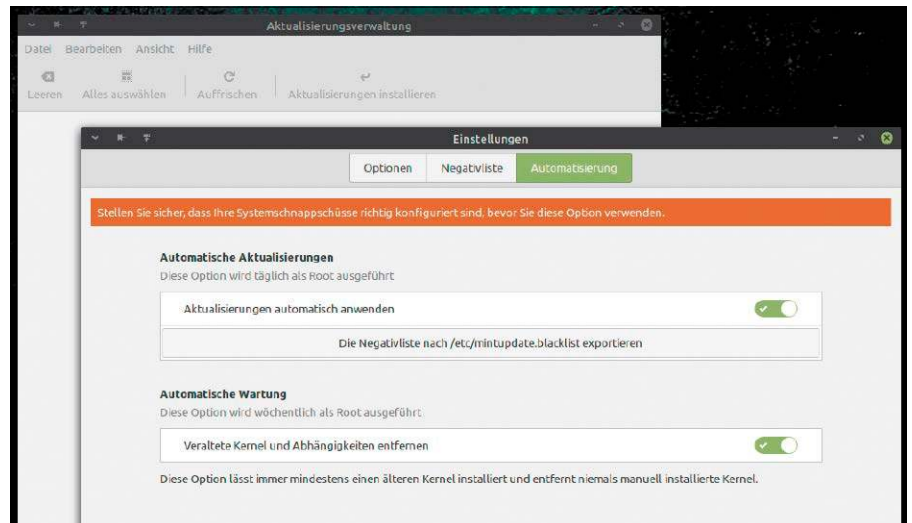
Scrollbar: Wenn Sie Bildlaufleisten in der Standardgröße zu dünn finden, können Sie diese jetzt breiter konfigurieren.



Verbesserte Aktualisierungsverwaltung

Der erste Schritt nach einer Neuinstallation ist immer eine Systemaktualisierung, da es seit Erscheinen von Version 19.2 schon wieder eine Reihe neuer Updates gibt. Daher gehen Sie in der „Aktualisierungsverwaltung“ auf „Auffrischen“ und danach auf „Aktualisierungen installieren“. Sorgen Sie über „Bearbeiten → Einstellungen → Automatisierung“ dafür, dass ab sofort Updates automatisch installiert werden. An gleicher Stelle können Sie auch die neue automatische Entsorgung veralteter Kernel aktivieren, die bereits eingangs dieses Artikels angesprochen wurde.

Die Aktualisierungsverwaltung wurde aber noch weiter verbessert: Sie ist einfacher, weil die neueste Version das langjährig gepflegte, aber eigensinnige Ebenenkonzept über Bord wirft. Ein neuer Service sorgt dafür, dass der Benutzer 90 Tage vor Ablauf eines Mint-Systems (Supportende) einen Warnhinweis erhält. Und bei neuen Versionen der wichtigen Aktualisierungsverwaltung selbst erhalten Sie ebenfalls



Überarbeitete Aktualisierungsverwaltung: Das Tool zeigt sich funktional deutlich erweitert (Kernel-Verwaltung, Automatisierung) und wurde im Gegenzug vereinfacht (ohne Ebenenkonzept).

umgehend eine Aufforderung, diese zu aktualisieren.

Die Systemschnapschüsse

Die Systemsicherung mit dem Tool „Timeshift“ ist in Linux Mint inzwischen mehr

oder weniger Pflicht. Solange Sie deren Einrichtung unterlassen, werden Sie in der Aktualisierungsverwaltung permanent dazu angemaht. Bei der Ersteinrichtung wählen Sie als „Schnapschusstyp“ „RSYNC“. Im nächsten Schritt geht es um den „Schnapp-

MINT 19.2 MIT MATE UND XFCE

Das Mint-Team macht bei den minimalen Hardwareanforderungen der drei Editionen keinen Unterschied: Ein, besser zwei GB RAM und 16 bis 20 GB Festplattenplatz sollten für jedes Mint-System ausreichen.

Tatsächlich sollte man aber bei der 64-Bit-Edition mit Cinnamon 800 MB RAM allein für System und Desktop einrechnen und für komfortablen Betrieb vier GB RAM veranschlagen. Wer es sparsamer haben will, kann auf Mate oder XFCE ausweichen – und dies eindeutig am sparsamsten mit einer 32-Bit-Ausführung. Diese Mint-Systeme stehen zwar in Konkurrenz zu den etwas aktuelleren Ubuntu-Editionen Ubuntu Mate und Xubuntu, bringen aber fast alle Mint-Tools mit. Folglich gelten die beschriebenen Neuheiten in der Aktualisierungsverwaltung, der Anwendungsverwaltung, den X-Apps, den Systemberichten und der Themenoptik auch für diese Editionen. Lediglich die Neuerungen beim Dateimanager Nemo fließen hier nicht ein, da Mate den eigenen Caja, XFCE den eigenen Thunar als Dateimanager benutzt.

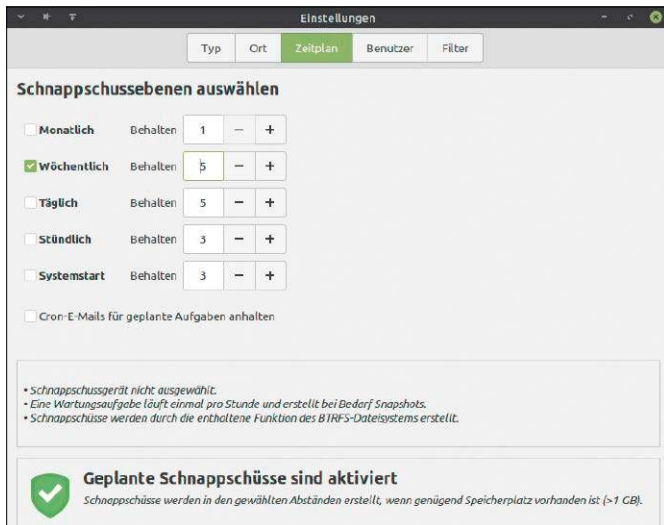
Linux Mint 19.2 XFCE ist in der 32-Bit-Variante äußerst genügsam und begnügt sich mit 250 MB RAM. Der ausgereifte Desktop XFCE ist weiterhin in Version 4.12 an Bord, bei dem sich seit 2015 nichts geändert hat. Der Desktop ist zwar etwas altmodisch, aber organisatorisch perfekt und bestens konfigurierbar. Kleiner Bug: Das wichtige Applet „Benutzer und Gruppen“ ist in den Systemeinstellungen nicht verlinkt und nur

über das Menü (unter „Systemverwaltung“) zu erreichen. Linux Mint 19.2 Mate ist in der 32-Bit-Variante ziemlich exakt genauso anspruchslos wie die XFCE-Variante. Daher bleibt die Wahl zwischen Mate und XFCE Geschmackssache.

Wir halten XFCE für den klareren Desktop, Mate wird aber andererseits aktiv weiterentwickelt. Linux Mint 19.2 zeigt die aktuellste Mate-Version 1.22 vom Frühjahr 2019. Hierfür wurde am Aussehen der Fenster- und Desktopwechsler gefeilt, für Autostart-Programme gibt es die neue Option der zeitlichen Verzögerungsintervalle, außerdem kamen neue Tastenkürzel für die Mediensteuerung hinzu.



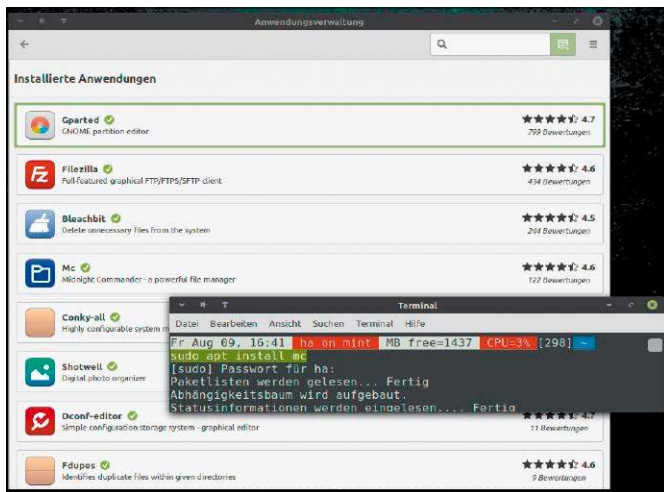
Hässlich ist anders: Der konservative, aber exzellente XFCE-Desktop ist immer erste Wahl für schwächere Hardware.



Timeshift-Zeitplan: An Timeshift kommen Mint-Benutzer kaum vorbei. Intervalle und Sicherungsmengen lassen sich aber beliebig steuern – hier nur wöchentlich und fünf Sicherungen.

Die Anwendungsverwaltung

Bislang fehlte der Softwarezentrale „Anwendungsverwaltung“ (mintinstall) eine wichtige Verwaltungsoption: Das Menü rechts oben mit der Option „Installierte Anwendungen anzeigen“ zeigte nur die installierte Software, die über die grafische Zentrale eingerichtet wurde. Dies hat sich in Linux Mint 19.2 geändert: Die Liste zeigt nun alle Programme an, die nicht zum Systemstandard gehören und vom Benutzer nachinstalliert wurden. Dazu vergleicht die Anwendungsverwaltung alle vorhandenen Pakete mit der Paketliste des ursprünglichen Installers (Ubiquity): Alles was abweicht, ist logischerweise vom Benutzer installiert, und auf welche Weise dies geschah, spielt für diese Analyse keine Rolle. In den **Anwendungspaketquellen** (mint-sources) gibt es im Abschnitt „Wartung“ zwei neue Schaltflächen. Die Option „Fehlende Schlüssel hinzufügen“ durchsucht alle aktiven Paketquellen und PPAs und lädt fehlende Schlüssel automatisch nach. Der weitere Punkt „Doppelte Einträge entfernen“ erkennt Duplikate in der Liste der Softwarequellen und löscht diese.



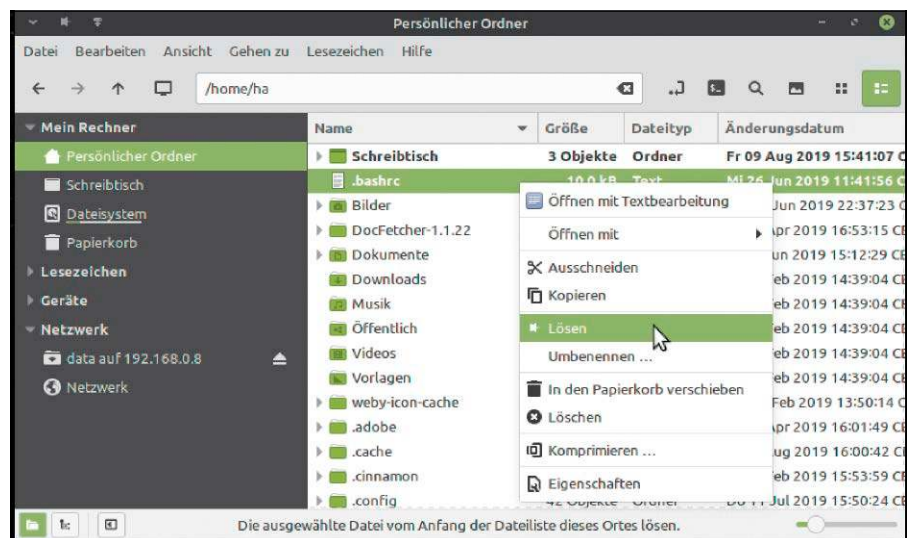
Verbesserte Anwendungsverwaltung (mintinstall): Die grafische Softwarezentrale zeigt jetzt auch installierte Software, die über das Terminal eingerichtet wurden.

Der Dateimanager Nemo

Im Dateimanager gibt es nach Rechtsklick das neue Kontextmenü „Anheften“. Dieses hält ein Dateibjekt ungeachtet der gewählten Sortierung immer ganz oben in der Liste. Die Option arbeitet sowohl in der Symbolansicht als auch in der Listen- und Kompaktansicht. Das ist praktisch, um wichtige Ordner und Dateien an erster Stelle zu

schussort“. Standardziel, wenn nur eine Festplatte vorliegt, ist das Wurzelverzeichnis, wo der zusätzliche Ordner „timeshift“ entsteht. Im letzten Schritt definieren Sie einen Zeitplan und die Anzahl der gespeicherten Systempunkte. Der vorgegebene Standard täglicher Snapshots ist sicher übertrieben. In vielen Fällen sollte es genügen, die Option „Wöchentlich“ zu aktivieren und von diesen Sicherungen etwa fünf Versionen zu „Behalten“. Beachten Sie, dass Sie vor riskanten Aktionen jederzeit manuell einen Schnapschuss im Timeshift-Fenster auslösen können („Erstellen“). Timeshift-Backups bestehen einfach aus unkomprimierten Ordnern und Dateien. Einzelne Dateibjekte oder der komplette frühere Zustand lassen sich daher mit jedem Livesystem aus dem Backupdatenträger unter „/timeshift/snapshots“ kopieren. Sofern das System noch funktioniert, schreiben Sie den gewünschten Sicherungspunkt mit Timeshift selbst und „Wiederherstellen“ zurück.

ungspunkt mit Timeshift selbst und „Wiederherstellen“ zurück.



Bevorzugte Dateibjekte in Nemo: Die mit „Anheften“ an oberste Stelle gesetzten Dateibjekte ignorieren die üblichen Sortierregeln. Mit „Lösen“ lassen sie sich wieder normal einsortieren.

halten – und sei es auch nur vorübergehend. Dergestalt bevorzugte Objekte markiert Nemo fett. Angeheftete Objekte sind mit dem Kontextmenü „Lösen“ jederzeit wieder normal eingereiht. Beachten Sie, dass sich angeheftete Dateien sogar der Standardsortierung unterhalb von Ordnern widersetzen: Sie erscheinen somit vor den Verzeichnissen.

Unter „Bearbeiten“ erscheint die neue Nemo-Option „Vollständiges Kontextmenü verwenden“. Damit kann man das Rechtsklickmenü erweitern oder – durch Abschalten – übersichtlicher halten. Ist der Punkt aktiviert, erscheinen die zusätzlichen Punkte „Verdoppeln“, „Verknüpfung anlegen“ und „Kopieren nach“ für alle Dateiobjekte. Bei „Verdoppeln“ entsteht einfach eine Kopie (von Datei oder Ordner) im selben Verzeichnis mit dem Hinweis „(Kopie)“ im Dateinamen.

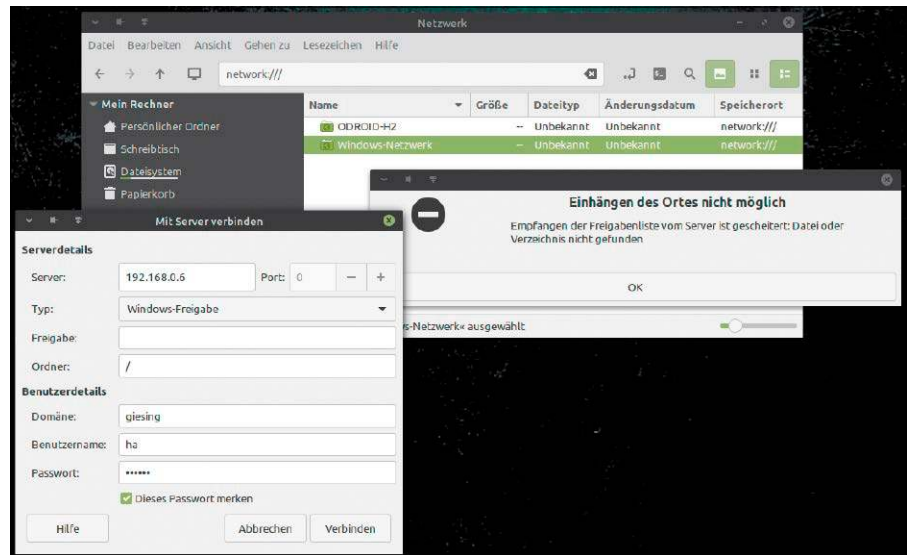
Samba und Nemo-Share

In Cinnamon sorgt das kleine Hilfstool nemo-share dafür, Samba und dessen Netzwerkfreigaben in den Desktop und in den Dateimanager zu integrieren. Zu den bisherigen Aufgaben von nemo-share gehörte die automatische Nachinstallation des Samba-Servers, sobald ein Benutzer etwas freigeben möchte, ferner der Eintrag dieses Nutzers zur Gruppe „sambashare“. In Linux Mint 19.2 verbessert nemo-share seine Fehlertoleranz: Die Samba-Nachinstallation wird durch passende Firewallregeln begleitet, ferner prüft das Tool, ob die lokalen Dateirechte einer Netzfreigabe widersprechen, und schließlich, ob Home-Verschlüsselung (Ecrypt FS) eine erfolgreiche Freigabe verhindern könnte. Letzteres wird das Problem nicht lösen, zeigt dem Anwender aber zumindest, woran es liegt.

Achtung Bug: Den von Ubuntu altbekannten Samba-Fehler erbt auch Mint 19.2 wieder: Die Übersicht im Dateimanager über das „Windows-Netzwerk“ scheitert. Ein wirkliches Problem ist das nicht, weil über „Datei → Mit Server verbinden“ (Cinnamon mit Nemo – in Caja und Thunar ähnlich) der Zugriff auf einzelne Samba-Server jederzeit funktioniert und dann dauerhaft als Lesezeichen abgelegt werden kann (Strg-D).

Zubehör und X-Apps

Xed, der Standard-Texteditor, unterstützt jetzt das Umschalten von Kommentaren und Kommentarblöcken. Die Funktion ist



Dieser – harmlose – Bug wartet weiter auf Ubuntu-Hilfe: Die Gesamtschau auf alle Samba-Server scheitert weiterhin und muss durch direkte Anmeldung kompensiert werden.

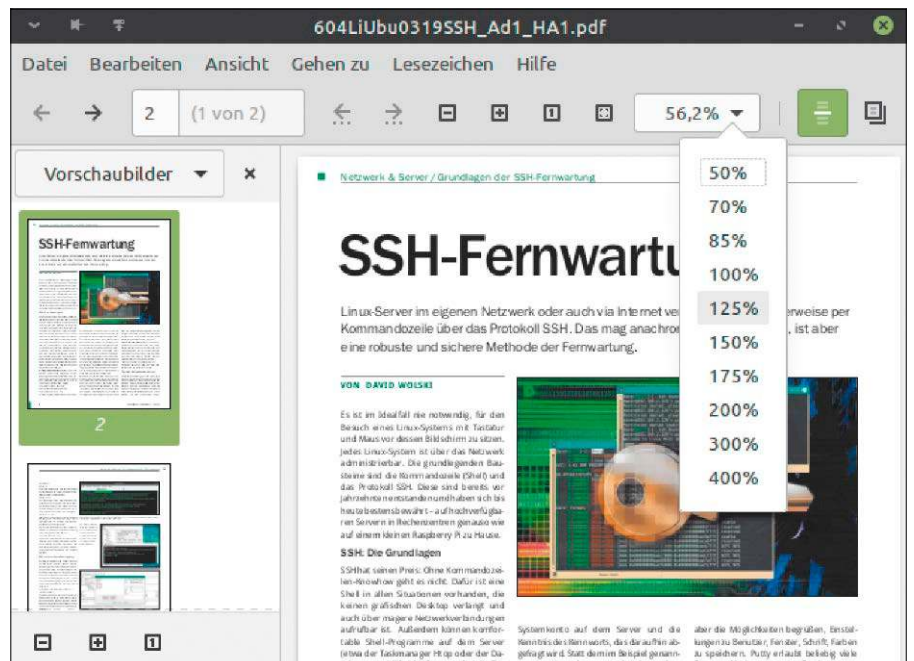
unspektakulär und nur für das Scripting relevant: Ein markierter Textblock kann mit Strg-Umschalt-/ auskommentiert und mit derselben Tastenkombination auch wieder aktiviert werden. Die Funktion ist auch im Menü „Bearbeiten“ als „Kommentar umschalten“ zu finden.

Das Tool **Systemberichte** (mintreport) wurde optisch überarbeitet und liefert einen gut lesbaren Überblick zur Hardware inklusive Temperatursensoren. Für Problemanalysen ist aber die zusätzliche Befragung der „Protokolle“ (gnome-logs“) unentbehrlich.

Xreader ist der Standardreader für PDF-Dateien. Über „Bearbeiten → Einstellungen“ kann der Werkzeuggestreife ein neues Control zum schnellen Umschalten des Vergrößerungsfaktors hinzugefügt werden.

Das Leistenapplet „Drucker“ für die Systemleiste ist als optionales Element neu hinzugekommen. Sie aktivieren es nach Rechtsklick auf die Leiste und „Applets zur Leiste hinzufügen“ über den Listeneintrag „Drucker“.

Das Applet ist nur eine Abkürzung zu „Systemeinstellungen → Drucker“.



Kleine Anpassung des PDF-Viewers: Xreader erhält ein Zoom-Control für die Werkzeuggestreife.

Die besten System- schutzmaßnahmen

Datensicherung ist unbeliebt, aber ein notwendiges Übel jeder großen wie kleinen IT-Infrastruktur. Mit den richtigen Tools kostet aber nur die erste Einrichtung oder die Kommandorecherche Zeit. Danach läuft das Meiste automatisch ab.

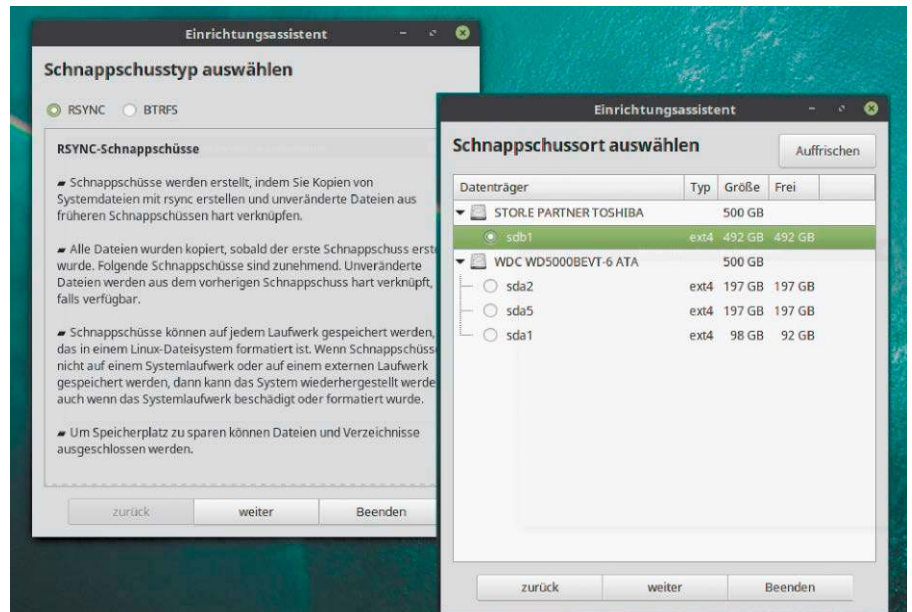
VON HERMANN APFELBÖCK

Mit Linux sind Sie gegen Schadsoftware so gut wie immun, doch mit Benutzerfehlern und Havarien müssen Sie auch hier rechnen. Versehentliches Löschen, Konfigurationsfehler, misslungene Upgrades oder Festplattendefekte verursachen Datenverluste. Dagegen hilft nur eine gesunde Redundanz: Sorgen Sie dafür, dass Sie alle wichtigen Dateien und Ordner ein zweites oder drittes Mal vorfinden.

Systemschutz (1): Timeshift

Das Sicherungswerkzeug Timeshift ist unter Linux Mint Standard. Es erstellt Momentaufnahmen des Dateisystems, die beim Zurückspielen einen früheren Zustand wiederherstellen. Unter Ubuntu ist es nicht Standard, aber eine empfehlenswerte Ergänzung. Timeshift liegt fast überall in den Standardpaketquellen und ist mit `sudo apt install timeshift` schnell nachinstalliert.

Der erste Sicherungspunkt ist ein komplettes Backup der Systemverzeichnisse. Weitere Wiederherstellungspunkte fallen dann viel kleiner aus, da Timeshift nur noch geänderte Dateien speichert. Der Rest wird per Hardlinks abgebildet. Folgesicherungen



Einrichten der Timeshift-Sicherung: Ein unabhängiger Datenträger ist als Backupziel ideal, der muss aber bei automatischer Sicherung nach Zeitplan immer verfügbar sein.

haben nur scheinbar den im Dateimanager angezeigten großen Speicherbedarf.

Die Einrichtung: Timeshift fordert beim Start immer das sudo-Kennwort, da es Zugriff auf alle Ordner benötigt. Beim ersten Start wird der „Schnappschusstyp“ abgefragt („RSYNC“). Im nächsten Schritt geht es um den „Schnappschussort“, also um den Zieldatenträger der Sicherung. Timeshift bietet alle Partitionen mit Linux-Dateisystem an (notwendig wegen der Hardlink-Technik). Besser als die Systempartition selbst ist ein unabhängiger zweiter Datenträger, der dann aber immer zur Verfügung stehen muss, wenn Sie einen automatisierten Timeshift-Plan verwenden. Im letzten Schritt definieren Sie einen Zeitplan („Schnappschussebenen“) und die Menge der gespeicherten Systempunkte. Auf einem normal genutzten Desktop sollten wöchentliche Sicherungen und drei bis fünf aufbewahrte Sicherungspunkte genügen, aber das lässt sich beliebig steigern. Getrof-

fene Einstellungen können Sie später jederzeit ändern. Mit der Schaltfläche „Erstellen“ können Sie auch jederzeit einen Sicherungspunkt manuell auslösen.

Wiederherstellen: Die Backups bestehen aus unkomprimierten Ordnern und Dateien unter „/timeshift/snapshots“. Einzelne Dateiobjekte oder der komplette frühere Zustand lassen sich daher mit jedem Live-System rekonstruieren, falls das primäre System nicht mehr funktioniert – im Prinzip auch ohne Timeshift. Noch bequemer geht's aber mit Timeshift selbst: Das Tool zeigt in seiner Liste alle Sicherungspunkte. Mit „Wiederherstellen“ schreiben Sie einen markierten Punkt zurück. Die Partitionsdaten werden im Fenster „Ziellaufwerk auswählen“ noch einmal explizit abgefragt.

Systemschutz (2): Clonezilla-Images

Mit Clonezilla erstellen Sie Abbilder von Festplatten oder klonen den Inhalt einer

Festplatte direkt auf eine zweite. Das Livesystem beziehen Sie über <http://clonezilla.org> (260 MB). Clonezilla ist textbasiert, hat aber eine pseudo-grafische Oberfläche. Mit den Pfeiltasten navigieren Sie im Menü und bestätigen die Auswahl mit Eingabetaste. Mit der Tabulator-Taste wechseln Sie zwischen Schaltflächen wie „OK“ und „Cancel“.

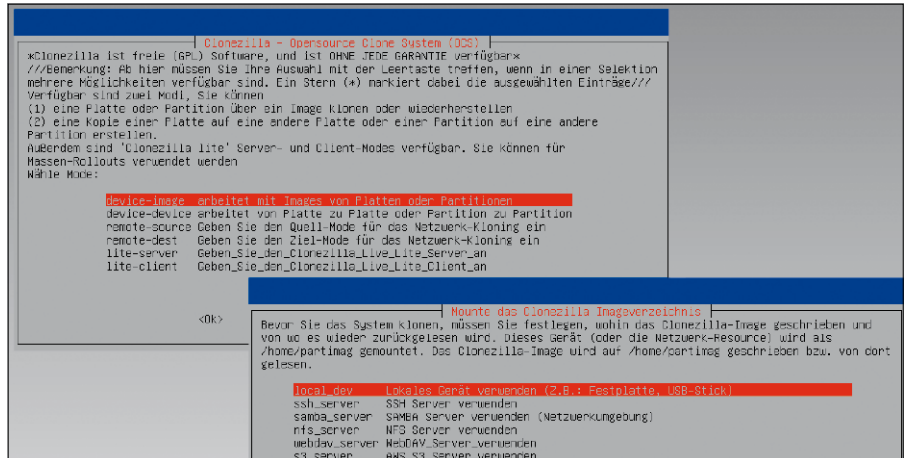
Soll die Sicherung auf eine USB-Festplatte erfolgen, schließen Sie diese vorher an. **Abbildsicherung:** Im gebooteten Clonezilla wählen Sie für ein Imagebackup die Option „device-image“ und danach „local_dev“. Geben Sie die Festplatte an und danach das Verzeichnis, wohin Sie das Abbild speichern wollen. Wählen Sie „Beginner“ und „savedisk“ und geben Sie einen Dateinamen für das Image an. Die spätere Wiederherstellung eines Abbilds läuft entsprechend ab. Nach „Beginner“ wählen Sie „restoredisk“, danach die gewünschte Abbilddatei und dann die Zielfestplatte.

Direktkopien: Für eine Direktkopie von einer Festplatte auf eine zweite wählen Sie „device-device“, danach „Beginner“ und „disk_to_local_disk“. Bestimmen Sie dann die Festplatte, die Sie kopieren möchten. Bei der Systemfestplatte handelt es sich in der Regel um „sda“. Nach „OK“ wählen Sie die Zielfestplatte. Wenn sich nur zwei Festplatten im PC befinden, ist dies „sdb“. Bestätigen Sie diese Auswahl und auch die nächsten beiden Meldungen mit der Eingabetaste. Sie erhalten dann eine zusammenfassende Meldung über die ausgewählten Festplatten. Prüfen Sie die Angaben genau, um ja nicht Quelle und Ziel zu verwechseln. Bei startfähigen Festplatten fragt Clonezilla automatisch, ob Sie auch die Startumgebung („boot loader“) kopieren möchten. Bestätigen Sie dies mit „y“ und Eingabetaste.

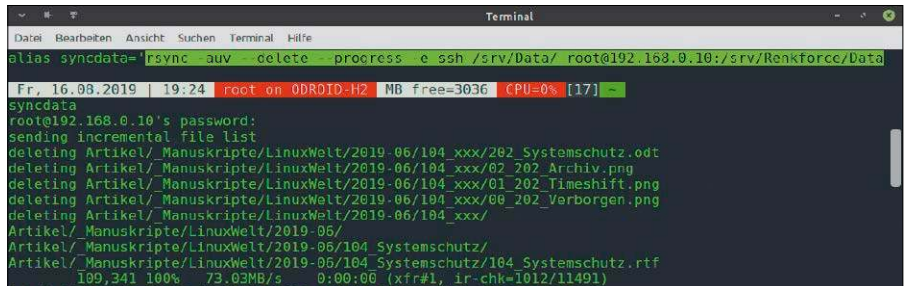
Hinweis: Bei einer Direktkopie muss die Zielfestplatte mindestens die Kapazität des Quelllaufwerks besitzen. Ist das Ziellaufwerk größer, sollten Sie nachträglich die Partitionsgröße ausdehnen, um die Festplatte komplett zu nutzen. Dies erledigen Sie am besten mit Gparted in einem Livesystem (etwa Linux Mint 19.2 auf Heft-DVD). Über „Größe ändern/verschieben“ lässt sich die Partition ausdehnen.

Datenbackups mit Rsync

Theoretisch kann Timeshift auch zur Sicherung der Home-Verzeichnisse eingesetzt werden („Einstellungen → Benutzer“). Dies



Klonprogramm Clonezilla: Die Menüs sind nicht hübsch, aber ganz gut erklärt. Typischerweise arbeiten Sie mit Images (Bild oben) und mit lokalen Datenträgern (Bild unten).



Spiegelsynchronisierung mit Rsync: Solche 1:1-Kopie mit Löschscharter ist nur zu empfehlen, wenn das Backupziel nie direkt bearbeitet wird (in der Abbildung eine Sicherung via SSH von Server zu Server).

halten wir aber bei großen Datenbeständen unter „/home“ für keine gute Idee, weil es den Zeitaufwand und die Schnapsschussgrößen für Timeshift erheblich aufbläht. Für Benutzerdateien sind Backups oder Synchronisierungen mit Rsync erste Wahl. Rsync sichert auf interne und externe Laufwerke, auf Freigabeordner, auf Netzwerk- oder Webserver, auf denen der SSH-Server läuft. Rsync hat reichlich Schalter zu bieten, doch fasst die Option „-a“ häufig benötigte Funktionen zusammen. Damit erreichen Sie rekursives Kopieren aller Unterverzeichnisse:

```
rsync -a /home/ha/ /media/ha/usb/backup
```

Das Beispiel geht davon aus, dass ein USB-Laufwerk mit dem Label „usb“ unter „/media/ha“ eingehängt ist. Dies ist das Ziellaufwerk der Sicherung. Das angegebene Verzeichnis („backup“) wird automatisch erstellt, sofern es noch nicht existiert. Das erste – nach den Schalteroptionen – angegebene Verzeichnis ist der Quellordner. Beachten Sie den abschließenden Slash (/). Nur so landen alle Sicherungsdaten direkt im Zielordner „backup“.

Von weiteren Rsync-Schaltern sind mindestens drei unentbehrlich: Mit `rsync -av --delete /home/ha/ /media/ha/usb/backup` erzeugen Sie bei periodischer Sicherung eine Mirror-Kopie. Was unter der Quelle „/home/ha“ seit dem letzten Kopiervorgang gelöscht wurde, wird auch auf dem Ziel gelöscht. Mit falschen Pfadangaben wäre das fatal. Ein Testlauf mit `rsync -av --delete --dry-run /home/ha/ /media/ha/usb/backup` zeigt alle zu erwartenden Aktionen, ohne sie tatsächlich auszuführen. Schalter „-u“ spart bei periodischen Sicherungen Zeit (`rsync -auv ...`), weil er bereits bestehende Dateien überspringt.

Sicherung via SSH: Rsync kann von jedem Rechner im Netzwerk Daten beziehen oder dorthin kopieren, wo ein SSH-Server läuft. Die Sicherung folgt diesem Schema `rsync -av -e ssh ha@192.168.0.66:/home/ha/Bilder/ /home/ha/Bilder` oder auch mit `rsync -auv --delete -e ssh /var/www/ root@192.168.0.8:/var/www/` in die andere Richtung. ■

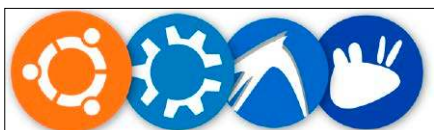
Linuxboot: Die Uefi-Alternative reift

Seit 2010 sind neu verkaufte Mainboards und Notebooks mit Uefi ausgestattet, um die Geräte fit für aktuelle Hardware und Betriebssysteme zu machen. Ursprünglich wurde die Uefi-Referenzimplementierung von Intel unter dem Namen „Tianocore“ unter der BSD-Lizenz entwickelt, was für Transparenz sorgen sollte. Mittlerweile sind die Uefi-Varianten der Hardwarehersteller aber alles andere als transparent, wenig vertrauenswürdig für sicherheitskritische Anwendungen und teils einfach fehlerhaft. Als Alternative steht der komplett offengelegte Uefi-Ersatz „Linuxboot“ in den Startlöchern, der gerade von Google-Mitarbeitern für verschiedene Betriebssysteme fit gemacht wird. Linuxboot kann nicht nur Linux, sondern auch Windows starten. Den Namen hat „Linuxboot“ von seiner Funktionsweise: Anstatt einer Uefi-Shell bootet diese Firmware ein Mini-Linux-System, welches dann das eigentliche Betriebssystem startet. ■



Ubuntu und Derivate: Version 18.04.3

Für die Ubuntu-Varianten 18.04 LTS (Langzeitsupport) sind neue Installationsmedien in der Version 18.04.3 erschienen. Diese dritte Aktualisierung der Medien bringt alle Updates mit, die seit der Veröffentlichung von Ubuntu 18.04 erschienen sind, und auch den Kernel 5.0. Wer ein Ubuntu dieser Version bereits installiert hat, braucht die Medien natürlich nicht, da der Paketmanager alle Updates liefern kann. Ubuntu mit Langzeitsupport wird sowohl in der Desktop- als auch in der Servervariante insgesamt fünf Jahre mit Aktualisierungen versorgt – in der Version 18.04 also noch bis April 2023. Kunden von Canonical mit Wartungsvertrag sollen sogar bis 2028 Sicherheitsupdates und Backports erhalten. ■



Alle News von David Wolski

Vorschau auf Kernel 5.3

Keine Sommerpause: Mitte September hat Linus Torvalds als maßgeblicher Kopf hinter den Kernel-Veröffentlichungen die Version 5.3 freigegeben. Sie enthält im Vergleich zu den vorangegangenen Kernel-Versionen umfangreichere Änderungen und Neuerungen.



Rund 12 600 Änderungen fließen in den Kernel 5.3 ein, die lediglich zwei Monate nach Version 5.2 erschienen ist. Die Geschwindigkeit ist bemerkenswert, da in der Anfangsphase eine vergleichsweise große Menge an inakzeptablem Code eingereicht wurde, die Linus Torvalds nicht akzeptierte. Der Hauptteil des neuen Codes stammt von AMD, betrifft den Grafiktreiber AMDGPU und insbesondere Neuerungen zur aktuellen AMD-Grafikkarte Radeon RX 5700. Mittlerweile ist das AMD-Subsystem mit Grafiktreibern der umfangreichste Treiber im Kernel, allerdings auch jener Teil mit dem schlechtesten Code, der größtenteils automatisch erzeugt ist.

Dennoch bekommt AMD schrittweise mehr und mehr Code in den Kernel, während es für Nvidia-Anwender nur den Nouveau-Treiber im Kernel gibt. Dieser unterstützt immerhin die Nvidia-Chips TU116 der Turing-Serie. Gleichzeitig verliert Nvidia mit seinem proprietä-

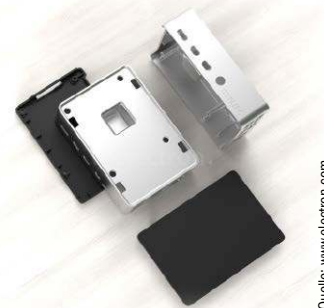
ren Treiber die Unterstützung im Kernel für IBM-Power-Architektur, weil die Kernel-Entwickler absichtlich einige Anknüpfungspunkte für diesen fremden Treiber entfernten, weil kein anderes Modul diese Punkte benötigte. Nun muss Nvidia erst neue Treiber für die Powerarchitektur erstellen.

Die Hoffnung hinter dem Schritt ist, dass sich Nvidia vielleicht doch noch engagierter in den Kernel-Quellcode einbringt. Intel hat derweil für seine bereits verfügbaren CPUs ab der Serie „Cascade-Lake“ die Methode „Intel Speed Select Technology“ beigesteuert, die eine feinere Abstufung von Taktfrequenzen pro CPU-Kern erlaubt und damit die Effizienz der Prozessoren verbessert.

Einen markanten Abschied gibt es auch: Der alte ISDN-Treiber „isdnl4linux“ ist entfernt worden, der für viele Router der ersten Stunde eine wichtige Komponente war. ISDN funktioniert aber mit dem neuen „mISDN“ weiterhin. ■

Raspberry Pi 4: Passiv gekühltes Gehäuse

Nach dem Erscheinen des Raspberry Pi 4 wurde schnell klar, dass die Platine mit dem Quadcore-ARM-SoC von Broadcom und 1,5-GHz-Takt recht heiß wird (siehe ab Seite 54). Aufgeklebte Kühlkörper reichen hier oft nicht mehr. Die übliche Lösung ist, einen aktiven Lüfter auf einem geeigneten Gehäuse zu montieren. Mit dem Aluminiumgehäuse Flirc gibt es jetzt eine lautlose Alternative: Das Gehäuse fungiert als großer Kühlkörper und hält den Raspberry Pi 4 auch ohne drehende Lüfter auf einer akzeptablen Temperatur. Flirc ist ab 20 Euro im Versandhandel erhältlich, beispielsweise bei Welectron (www.welectron.com/Flirc-Raspberry-Pi-4-Case). ■



Quelle: www.welectron.com

Owncloud: Großer Umbau

Es ist schon eine Weile her, dass sich Nextcloud mit den Gründern von Owncloud von diesem Projekt abspaltete: 2016 hat sich Nextcloud unvermittelt und auch für viele Mitarbeiter überraschend von Owncloud getrennt. Die Owncloud GmbH machte aber trotzdem weiter und holt nun Anlauf zu einem weiten Sprung. Das grundlegende Rahmenwerk, auf welchem Owncloud seinen Dateiaustausch- und Kollaborationsfunktionen aufbaut, soll von PHP auf die moderne Sprache Go portiert werden. Tatsächlich sehen Skeptiker die PHP-Basis als Nachteil, schließlich geht es bei Owncloud und Nextcloud nicht um ein paar Blogseiten, sondern um einen

zuverlässigen Dateispeicher zum Austausch unter mehreren Usern und zur Synchronisierung vieler Clients. Dieses Einsatzfeld ist weniger die Stärke von PHP, sondern von ausgewachsenen Programmiersprachen wie Python oder Go. Mit dem Umbau auf Go könnte sich Owncloud gerade im Firmenumfeld wieder gut aufstellen, nachdem das ursprüngliche Projekt hinter Nextcloud in den letzten Jahren zu einer Fußnote wurde. Der Umbau soll Ende 2019 abgeschlossen sein; mit der allgemeinen Verfügbarkeit der neuen Go-Version von Owncloud ist 2020 zu rechnen. ■



SICHERHEITSNEWS

Chrome/Chromium: Adieu, FTP

Das pure File Transfer Protokoll (FTP) ist aufgrund der unverschlüsselten Übertragung von Log-in-Daten unsicher und kommt im Internet kaum noch zum Einsatz. Die Browser Chrome und Chromium werden die Unterstützung deshalb in einer ihren nächsten Ausgaben komplett entfernen. Zwar kann FTP mit TLS verschlüsselt werden, aber diese Variante sei zu selten, so die Entwickler der Google-Browser, um noch viel Aufwand für diese raren Protokolle zu betreiben. In Zukunft werden Anwender dieser Browser also einen separaten Client wie Filezilla (<https://filezilla-project.org>) benötigen, um FTP zu nutzen.



Libre Office: Angriff per Dokument

In mehreren Versionen der freien Büro-Suite steckten Fehler, die einen Angriff auf das System per Dokument ermöglichten. Öffnen Anwender ein manipuliertes Dokument, so kann dies Python-Kommandos auf dem Zielrechner ausführen. Diese untergeordneten Befehle laufen dann im Kontext des Benutzers, der das Dokument öffnete, und können immerhin Unheil im Home-Verzeichnis anrichten. Ab Version 6.2.5 ist die Schwachstelle in Libre Office behoben. Für etliche Distributionen wie Debian, die eine ältere Version des Büro-Suite pflegen, stehen Backports bereit.



KDE: Einstellungen mit Fallen

Eine gut versteckte Funktion in KDE kann unter geschickter Ausnutzung einer jetzt entdeckten Lücke eingeschmuggelte Scripts ausführen. Das Problem steckt in der Behandlung von „.desktop“-Dateien unter KDE, die als Anwendungsverknüpfung dienen. Unter KDE bis hin zur neuesten Version 5.60 des KDE-Frameworks kann das Feld zum Laden eines Icons dazu missbraucht werden, stattdessen Code auszuführen. Anwender brauchen dazu nicht mehr zu tun, als einen Ordner mit dem KDE-Dateimanager zu öffnen, der eine Datei dieser Art beherbergt. Mittlerweile hat das KDE-Team die Lücke behoben und neue KDE-Pakete stehen für alle verbreiteten Linux-Distributionen bereit.



VLC: Attacken aus der Ferne

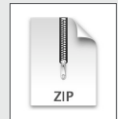
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat vor einer kritischen Schwachstelle in VLC gewarnt.



Es geht um die Gefahr von eingeschmuggeltem Code, der in manipulierten Videodateien stecken kann. Nach der Veröffentlichung des BSI meldeten sich einige Tage später die Macher des Mediaplayers VLC zu Wort: Der gefundene Fehler hat wenig mit dem VLC selbst zu tun, sondern mit einer veralteten Version einer Systembibliothek namens „libebml“, die schon seit über einem Jahr in korrigierter Version vorliegt. Das VLC-Team bezeichnete die Meldung des BSI daraufhin als „Fake News“. Das BSI hat die Einschätzung der Schwere der Lücke nun nach unten korrigiert.

ZIP: Ungebremst auf 4,5 Petabyte

ZIP-Bomben, die ein manipuliertes Archiv auf gigantische Datengrößen entpacken, stellen zwar kein hohes Risiko für Anwender und Administratoren dar, können aber eine ungebetene Überraschung sein, die lästige Aufräumarbeiten erfordert. Eine besonders explosive ZIP-Bombe hat der Open-Source-Entwickler David Fifield gebastelt: Mit Hilfe des ZIP64-Packalgorithmus kommt das entpackte Archiv bei einer Ausgangsgröße von 46 MB (!) auf 4,5 Petabyte! ZIP64 ist allerdings durch die fehlende Kompatibilität mit vielen Packprogrammen kein hohes Risiko. Gegen eine kleinere Variante dieser ZIP-Bomben, die mit dem üblichen Kompressionsalgorithmus immerhin auf 281 Terabyte kommt, haben die Packprogramme unter Linux bereits einen Schutz erhalten.



Logitech: Nur ein halber Patch

Das Unifying-Protokoll der Funkmäuse und Funktastaturen von Logitech leidet unter mehreren Fehlern, die ein Abhören von Eingaben erlauben. Ein Firmware-Update für die betroffenen Geräte machen das Protokoll nun ein Stück sicherer, lässt andere Lücken aber weiterhin offen: Nach wie vor können Angreifer den Pairingprozess der Logitech-Geräte mitschneiden und so an kryptografische Schlüssel gelangen. Das Pairing kann dabei gezielt durch einen Druck auf einen Knopf am Eingabegerät ausgelöst werden, wo zumindest physischer Zugriff auf das Equipment nötig ist. Logitech steht mit der Fehlerbehebung laut eigener Aussage vor Schwierigkeiten: Ein Patch sei nicht möglich, weil dann ältere Unifying-Geräte nicht mehr kompatibel wären.



UPDATETELEGRAMM

Endeavour-OS

Der Arch-Linux-Abkömmling Antergos ist Vergangenheit und wird nicht mehr erscheinen. Ein Nachfolgeprojekt steht mit Endeavour-OS schon bereit. Auch bei dieser Linux-Distribution geht es darum, ein Arch Linux mit einem flexiblen und komfortablen Installer auszustatten, um die Einstiegshürden zu senken (<https://endeavouros.com>).



Opsense 19.7

Das Free-BSD-System ist für den Betrieb auf Firewalls und Router zugeschnitten beziehungsweise verwandelt einen PC in ein solches Gerät. Der Free-BSD-Kernel ist für hohe Netzwerklast prädestiniert und das System ohne grafische Benutzeroberfläche liefert eine Administrationsoberfläche für das Web, um diffizile Filter- und Routingregeln für Netzwerkschnittstellen zu definieren (<https://opsense.org>).



Enlightenment 0.32

Zwei Jahre war vom Enlightenment-Desktop nichts zu hören, nachdem sich Samsung von seiner Open-Source-Sparte getrennt hatte, zu der zwischenzeitlich auch Enlightenment gehörte. Ohne Vorankündigung ist nun Enlightenment 0.32 erschienen, das den Desktop auf das neue Displayprotokoll Wayland bringt. Eine Installation in Linux-Distributionen ist nicht so einfach möglich, aber Arch Linux und Manjaro haben bereits die neuen Pakete (www.enlightenment.org/news/e23_release).



Kdenlive 19.08

Der Open-Source-Videoeditor nutzt die MLT Video Rendering Engine und kommt damit auf einen enormen Funktionsumfang, der sich mit professionellen Videoschnittprogrammen messen kann. Die Stabilität ließ aber zu wünschen übrig. Nun haben die Entwickler eine dreijährige Phase abgeschlossen, in der Kdenlive eine umfassende Umstrukturierung des Quellcodes gesehen hat. Die aktuelle Version bringt zudem ein erweitertes Schema an Tastenkürzeln (<https://kdenlive.org/de>).



KDE Connect für Mac-OS

Mit der KDE-Komponente KDE Connect bringt der Linux-Desktop eine solide Methode, Dateien mit Android-Geräten mittels einer App per WLAN auszutauschen oder diese sogar als Eingabegerät zu verwenden. Dies war zunächst eine Spezialität von KDE, hat aber aufgrund seiner komfortablen Funktionsweise viele Freunde über KDE hinaus gewonnen. Es gibt eine Portierung nach Gnome namens Gconnect, die in den nächsten Ubuntu zum Standardreperoire gehören soll. Jetzt kommt die Komponente auch auf ein Fremdsystem: Eine Version für Mac-OS X befindet sich in der Entwicklung und liegt unter https://binaryfactory.kde.org/view/MacOS/job/kdeconnect-kde_Nightly_macos bereits in Form von DMG-Archiven bereit. KDE Connect für den Mac verlangt mindestens nach Mac-OS X 10.14 „Mojave“ und ist im Funktionsumfang noch nicht gleichauf mit der Linux-Version. Zwei der wichtigsten Funktionen, der Dateiaustausch und die Desktopbenachrichtigungen, laufen aber bereits. ■



Linux: 32-Bit-Kernel kämpft mit Bugs

Zuverlässig, kaum schwere Bugs und schnelle Lösungen für sicherheitskritische Probleme: Diese Tugenden haben den Linux-Kernel groß gemacht. Der Kernel ist aber in verschiedenen Ausgaben für etliche Plattformen und Architekturen verfügbar und es sind keineswegs alle Kernel-Versionen einer Versionsnummer gleichauf. Der 32-Bit-Kernel für x86-CPU's macht keine gute Figur mehr und schiebt alte Probleme zu lange vor sich her, die in der 64-Bit-Version längst behoben sind. Die diversen Korrekturen der CPU-Schwachstellen „Meltdown“ und „Spectre“ kamen nicht nur Monate später in den 32-Bit-Zweig, sondern offenbarten noch weitere Bugs in dieser Prozessorarchitektur, die erst jetzt im Kernel 5.3 (32 Bit) eine zuverlässige Behandlung finden. Der Grund ist ein schwindender Anteil an Entwicklern, die sich um ältere 32-Bit-CPU's kümmern und neuen Kernel-Code akribisch auf diesen Plattformen testen. Gleichzeitig muss die 32-Bit-Schiene des Kernels aber unbedingt weitergepflegt werden, weil etliche Microcontroller und Industrie-PCs auf 32-Bit-CPU's von Intel und AMD beruhen und einen gut gepflegten Linux-Kernel brauchen. ■



Microsoft: ExFAT für den Kernel

Der Linux-Kernel wird bald Microsofts Dateisystem ExFAT nativ unterstützen, nachdem der IT-Konzern alle Unsicherheiten zu Patenten an ExFAT ausgeräumt hat. Das Dateisystem ExFAT erschien 2006 nicht unter einer Open-Source-Lizenz und war bis vor kurzem durch Patente geschützt. Für den Linux-Kernel gibt es Unterstützung für ExFAT, das vor allem auf externen Datenträgern und auf Digitalkameras zum Einsatz kommt, schon eine Weile in Form eines externen Moduls. Als Vorbild für das externe Modul diente ein Linux-Treiber für Android 3.0, den Samsung entwickelt hatte und zwangsläufig unter der GPL freigeben musste. Microsoft hat die technischen Spezifikationen für ExFAT jetzt freigegeben und der offiziellen Aufnahme des Treibers in den Kernel-Quellcode steht nichts mehr im Wege. ■



Kernel: Floppy Disks im Abseits

Die erste Linux-Version baute Linus Torvalds vor 28 Jahren für einen 386er mit Diskettenlaufwerk, das als Installations- und Bootlaufwerk diente. Auch später erstellten Linux-Anwender der ersten Stunden routinemäßig noch Notfall-Floppys zur Sicherung des Lilo-Bootloaders, um im Falle eines überschriebenen Bootsektors ein Linux-System wieder booten zu können. Mittlerweile ist die Floppy Disk im IT-Alltag nur mehr Geschichte. Auch der Kernel-Entwickler, der bis heute die Pflege des Kernel-Codes für Diskettenlaufwerke übernommen hatte, steht vor dem Problem sterbender Hardware und verfügt nun nicht mehr über alle nötigen Ausprägungen der Floppy, denn heutige noch verkaufte Diskettenlaufwerke werden als USB-Datenträger angeschlossen. Auch in virtuellen Maschinen gibt es emulierte Floppys, aber echte alte Hardware ist zu selten geworden. Linus Torvalds hat deshalb den Kernel-Unterzweig für altmodische Diskettenlaufwerke als „verwaist“ markiert. Möglich ist, dass Firmen mit großem Altbestand an laufender Hardware die Pflege übernehmen oder dass traditionelle Diskettenlaufwerke nur mehr in Form eines externen, nicht mehr weiterentwickelten Moduls Unterstützung erhalten. ■



Debian/Ubuntu: Ohne Python 2

Als Python 3 vor über zehn Jahren erschien, um Python 2.x zu ersetzen, waren nicht alle Nutzer der mächtigen Script-Sprache erfreut. Denn Python 3 enthält einige Änderungen, die den neuen Interpreter inkompatibel zum Vorgänger machten. Auch deshalb wurde der endgültige Abschied von Python 2.x immer wieder verschoben, zuletzt auf das Jahr 2020. Bis dahin ist es nun gar nicht mehr lange hin: Debian und Ubuntu gehen nun die Entfernung der alten Python-2-Pakete an. Bisherige Scripts sollen in der verbleibenden Zeit auf das neuere Python 3 portiert werden. ■

Nvidia: Hybride Treiber für Linux

Hybride Notebooks mit integriertem Grafikchip und externer Grafikkarte funktionieren auch mit verbreiteten Linux-Systemen über den proprietären Nvidia-Treiber. Dies soll ab jetzt noch einfacher werden und mit weniger Bastelei funktionieren: Ab Version 435.17 kann der Nvidia-Treiber unter dem Window-System Xorg einzelne Programmfenster mit Open GL oder Vulkan über die stärkere Nvidia-GPU darstellen. Ein PPA (inoffizielles Repository) für Ubuntu hält dazu ein gepatchtes Paket von Xorg für Ubuntu 18.04/19.10 bereit (<https://launchpad.net/~aplattner/+archive/ubuntu/ppa>). ■

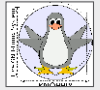
Slackware: Zukunft vorerst gesichert



Der Linux-Kernel ist im August 28 Jahre alt geworden. Nur zwei Jahre jünger ist die Distribution Slackware (www.slackware.com), die als älteste aktive Distribution gilt. Allerdings tat sich der Gründer mit der weiteren Pflege der Distribution zuletzt schwer, denn ein kommerzieller Erfolg wurde das System nie. Jetzt hilft aber eine Spendenaktion auf Patreon unter www.patreon.com/slackwarelinux weiter, das System weiter am Leben zu halten. Unter anderem basieren viele Livesysteme auf dem effizienten Slackware, beispielsweise das gut erweiterbare Livesystem Porteus (www.porteus.org). ■

UPDATETELEGRAMM

Knoppix 8.6



Das Linux-System ist eines der dienstältesten Livesysteme und erhält in seiner großen DVD-Ausgabe weiterhin regelmäßige Updates. Knoppix 8.6 aktualisiert seine Pakete auf den Stand von Debian 10 „Buster“, das im Juli 2019 erschienen war. Mit einer Größe von vier GB liefert Knoppix eine opulente Softwareausstattung mit (www.knoppix.org).

Kodi 18.4



Das beliebte Multimedia-Center Kodi behebt in der Version 18.4 wieder Fehler und aktualisiert den integrierten Encoder und Decoder Ffmpeg auf eine neuere Version. Damit folgen die Entwickler dem Rhythmus regelmäßiger Wartungsupdates. Neue Funktionen kommen in die zukünftige Ausgabe 19 von Kodi, deren Entwicklung bereits angelaufen ist (<https://kodi.tv>).

Glimpse 0.1



Die Grafikbearbeitung Gimp hat eine Abspaltung bekommen, die den Streit um den unglücklich gewählten Namen der Software beilegen soll. In vielen englischsprachigen Ländern ist „Gimp“ ein Schimpfwort und kein akzeptabler Name für ein seriöses Programm. Glimpse ändert aber nicht nur den Namen, sondern will sich auch um unbearbeitete Bugs kümmern. Auf Dauer ist eine enge Zusammenarbeit mit dem Gimp-Projekt geplant, damit Fehlerbehebungen zurück in den originalen Quellcode fließen (<https://getglimpse.app>).

XFCE 4.14



Kein Linux-Desktop schreitet gelassener voran als XFCE („X-Face“). Version 4.14 hat sich seit dem Vorgänger 4.12 mehr als vier Jahre Zeit gegönnt. Grund ist, dass diese konservative Oberfläche weitgehend perfekt ist, sofern man sie nicht neu definieren möchte. Hauptmotiv ist auch in Version 4.14 nicht neue Funktionalität, sondern der Umstieg des grafischen Unterbaus von GTK2 zu GTK3. Im Zuge dessen gibt es Dateiverbesserungen bei der Monitorkonfiguration und im Dateimanager Thunar.

Offene Türen im Netzwerk

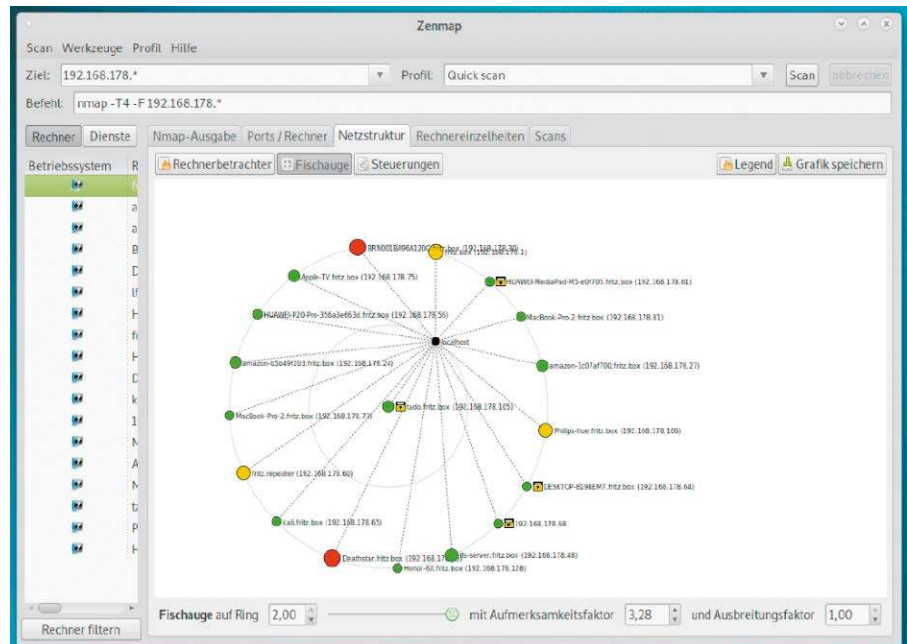
Viele Netzwerke haben offene Türen (Ports), über die sich heimische Computer über das Internet erreichen lassen. Das ist ein – kalkulierbares – Risiko, weil sie auch von Angreifern genutzt werden können. Nmap schafft Klarheit.

VON STEPHAN LAMPRECHT

Offene Ports sind unerlässlich, wenn man die auf einem heimischen NAS gespeicherten Daten über das Internet erreichen oder die Heizung vom Büro aus steuern will. Dann muss im Router mindestens ein Port geöffnet werden. Externe Anfragen werden dann intern an das gewünschte Gerät weitergeleitet. Ein solcher Zutrittspunkt wird aber auch schnell wieder vergessen und das ist bei schwacher Zugangssicherung (Kennwörter) fatal. Nmap ist ein seit vielen Jahren bewährtes Werkzeug, um sich über den Status von Netzwerkports zu informieren.

Wann Sie Nmap brauchen

Mit Nmap können Sie einen Rechner oder ein gesamtes Subnetzwerk auf offene Ports untersuchen. Das Werkzeug für die Kommandozeile hilft Ihnen herauszufinden, ob ein bestimmter Port auf dem Zielsystem geöffnet ist. Wie bei allen Sicherheitswerkzeugen gilt auch hier, dass Sie Ihre Untersuchungen auf eigene Systeme beschränken sollten. Im lokalen Netzwerk ist Nmap jederzeit erlaubt. Die nachfolgenden Beispiele verwenden aus diesem Grund ausschließlich lokale Adressen. Beachten Sie aber, dass der eigentlich sicherheitsrelevante Scan der Ihrer öffentlichen Adresse darstellt. Beschränken Sie sich beim Scannen öffentlicher IP-Adressen aber immer auf diejenige, die Ihr Router als Ihre eigene anzeigt (etwa die Fritzbox unter „Übersicht“), oder gegebenenfalls auf diejenige Ihres eigenen Webauftritts bei einem Internethoster. Beim Nmap-Scan fremder Adressen begehen Sie nicht nur einen unfreundlichen



Akt, sondern können sich strafbar machen. Linux-Nutzer finden Nmap in den Paketquellen der Distribution. Wer das Werkzeug unter Windows einsetzen will oder eine bestimmte Version aus dem Quellcode kompilieren möchte, muss die Projektseite aufsuchen (<https://nmap.org/download.html>). Nmap ist ein Kommandozeilenprogramm, es gibt aber mit Zenmap auch ein grafisches Front-End, das die Aufträge an Nmap weiterreicht und dabei auch über die Nmap-Syntax informiert.

Geöffnete Ports analysieren

Ein physikalischer Server kann verschiedene Dienste parallel anbieten. Das NAS im Wohnzimmer kann beispielsweise über ein Terminal erreicht werden (SSH-Sitzung) und

stellt eine Weboberfläche zur Verfügung (HTTP-Zugang). Damit sich die Datenpakete, die in der Regel über das gleiche Protokoll abgewickelt werden (heute in der Regel TCP/IP), nicht in die Quere kommen, werden die Dienste auf unterschiedlichen Ports bereitgestellt. Hier hat sich eine Reihe von Standards etabliert. Beispielsweise werden die Anfragen an einen Webserver üblicherweise über Port 80 abgewickelt, SSH über Port 22 und viele weitere (https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports).

Für eine erste Abfrage genügt der Terminalbefehl `nmap [Adresse/Adressraum]`, etwa: `nmap 192.168.178.10`
Wenn Sie Zenmap verwenden, tragen Sie Einzeladresse oder Adressraum in das Feld

„Ziel“ ein und drücken ohne weitere Veränderungen auf „Scan“. Statt der IP-Adresse können Sie auch den Hostnamen verwenden. Als Rückmeldung erhalten Sie eine Übersicht der geöffneten Ports mit der jeweiligen Nummer, dem Status und dem Service, der auf diesem Port aktiv ist. Falls Sie die Rückmeldung erhalten, dass das Zielsystem nicht erreichbar („Down“) ist, Sie aber sicher sind, dass der Rechner läuft, ergänzen Sie den Aufruf mit „-Pn“:

```
nmap -Pn 192.168.178.10
```

Damit unterdrückt Nmap seine Pingabfrage, denn manche Systeme sind so konfiguriert, dass sie auf Pings nicht antworten (auch bei Routern einstellbar). In der Ergebnisliste können Sie jetzt überprüfen, ob die geöffneten Ports wirklich benötigt werden. Vielleicht haben Sie im Router ja einmal einen Port für ein Onlinespiel oder eine Filesharing-Anwendung geöffnet, die Sie schon lange nicht mehr nutzen? Eine Internet-Portfreigabe im Router können Sie manuell schließen (Fritzbox: „Internet → Freigaben → Portfreigaben“), einen offenen Port im lokalen Netz nur dadurch, dass Sie das verantwortliche Programm beenden.

Nmap kann auch ganz gezielt nach einzelnen Ports oder einem Portbereich fahnden, wenn Sie den Schalter „-p“ verwenden:

```
nmap -p 22 192.168.178.10
```

Dieser Befehl ermittelt, ob auf dem Rechner der Standardport 22 für SSH aktiv ist. Danach erhalten Sie wichtige Hinweise auf den Status eines Ports:

Open: Ein Dienst ist bereit, auf diesem Port Datenpakete in Empfang zu nehmen. Es ist Hauptaufgabe von Nmap, solche offenen Ports zu finden, um danach nicht benötigte zu schließen oder benötigte gut zu sichern (Kennwort).

Closed: Es sind keine Verbindungen auf diesem Port möglich.

Blocked: Um Ports zu schützen, werden diese oft durch Firewalls und andere Sicherheitseinrichtungen geschützt. Der Scanner kann nicht feststellen, ob der Port geöffnet oder geschlossen ist.

Unblocked: Nmap kann nicht feststellen, ob der Port offen oder geschlossen ist. Der Port ist nicht durch eine Firewall geschützt.

Alle Netzwerkgeräte finden

Die Annäherung eines Hackers an ein unbekanntes Netzwerk beginnt in der Regel mit der Abfrage der darin vorhandenen Rechner. Für diese „Host Discovery“ gibt es

Mit der Untersuchung einer IP-Adresse stellen Sie schnell fest, ob Sie einen geöffneten Port vergessen haben oder welche Ports der Gerätehersteller standardmäßig öffnet.

Das grafische Zenmap ist nur eine Oberfläche für Nmap. Mit vordefinierten, klickbaren Standards ist es aber bequemer zu bedienen und hat obendrein die hübschere Ausgabe.

mit Nmap verschiedene Wege. Der unauffällige Listscan geht lediglich alle IP-Adressen in einem Netzwerk durch und nutzt die sogenannte Reverse-DNS-Abfrage. Standardmäßig setzt Nmap einen Pingbefehl auf die Zieladresse ab, der bemerkt werden könnte. Wird auf den Ping verzichtet, ergibt sich aus Sicht des Netzbetreibers nur „normaler“ DNS-Verkehr.

Schon eine solche einfache Liste kann Schwächen des Netzwerks zeigen. Denn bei der Installation eines Betriebssystems müssen die Anwender oft einen Hostnamen angeben. Wenn Sie diesen nicht editieren, wird dann ein vom Hersteller definierter Eintrag verwendet, der den Gerätetyp verrät. Viele Administratoren nutzen zur leichteren Orientierung auch den Hostnamen, um Hinweise auf die Verwendung des Systems zu geben. Die Abfrage mit

```
nmap -sL 192.168.1.*
```

fördert eine Liste der Rechner im Netz herbei. Wird die Abfrage um „-Pn“ ergänzt, unterbleibt der (für einen Hacker) verräterische Ping.

```

root@kali: ~
Datei Bearbeiten Darstellung Suchen Terminal Hilfe
root@kali:~# nmap 192.168.178.35
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-29 14:22 CEST
Nmap scan report for Deathstar.fritz.box (192.168.178.35)
Host is up (0.0065s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rcpbind
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
548/tcp   open  afp
873/tcp   open  rsync
2849/tcp  open  nfs
5000/tcp  open  upnp
5001/tcp  open  complex-link
MAC Address: 00:11:32:08:72:3B (Synology Incorporated)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
root@kali:~#

```

```

Zenmap
Scan Werkzeuge Profil Hilfe
Ziel: 192.168.178.* Profil: Quickscan
Befehl: nmap-T4 -F 192.168.178.*

Rechner Dienste Nmap-Ausgabe Ports/Rechner Netzstruktur Rechneinzelheiten Scans
Betriebssystem R
B
a
B
C
f
f
f
f
f
f
f
k
l
N
A
N
t
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-29 14:24 CEST
Nmap scan report for fritz.box (192.168.178.1)
Host is up (0.012s latency).
Not shown: 95 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
554/tcp   open  rtsp
5000/tcp  open  sip
MAC Address: C8:0E:14:BF:70:3D (AVM Audiovisuelles Marketing und Computer
Nmap scan report for amazon-b5b49f203.fritz.box (192.168.178.24)
Host is up (0.0029s latency).
Not shown: 99 closed ports
PORT      STATE SERVICE
8009/tcp  open  ajp13
MAC Address: 38:F7:3D:B9:A8:78 (Unknown)
Nmap scan report for amazon-1c07af700.fritz.box (192.168.178.27)
Host is up (0.014s latency).
Not shown: 99 closed ports
PORT      STATE SERVICE

```

Detailanalyse in einem Netzwerk

Ein komplexes Beispiel soll zeigen, wie mächtig Nmap ist. Dazu wird ein ganzes Netzwerk untersucht. Statt einer IP-Adresse wird ein ganzer Adressraum genutzt, um alle dort laufenden Rechner zu prüfen. Wieder wird die Pingabfrage unterbunden, also der Schalter „-Pn“ verwendet. Und hier soll Nmap außerdem ermitteln, welche Software hinter einem Port läuft (Schalter „-sV“). Für möglichst genaue Portinfos sorgt der Schalter „-version-all“. Der weitere allgemeine Parameter „-v“ macht Nmap insgesamt so gesprächig wie möglich:

```
nmap -Pn -sV --version-all -v
192.168.178.*
```

Ihre Geduld wird auf jeden Fall belohnt werden. Denn Sie erhalten nicht nur Hinweise darauf, welchen Status die Ports besitzen, sondern können ermitteln, welche Serversoftware eingesetzt wird. Das wiederum kann die Ausgangsbasis für weitere Analysen liefern, etwa um die Sicherheit der eingesetzten Programme genauer unter die Lupe zu nehmen. ■

Nikto findet Server-Schwachstellen

Cyberkriminelle haben es viel zu oft viel zu leicht. Falsch konfigurierte Webserver oder nicht behobene Sicherheitslücken bieten Möglichkeiten, um ein System zu kapern. Wir stellen Ihnen ein Werkzeug vor, das Webserver überprüfen kann.

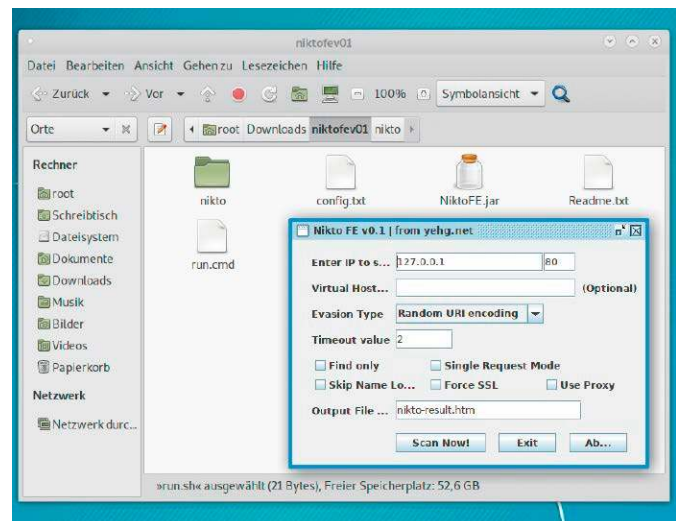
VON STEPHAN LAMPRECHT

Vertrauen ist gut, Kontrolle ist besser. Wer sein Blog oder seinen Webserver nicht auf einem eigenen Rechner betreibt, muss sich auf seinen Provider verlassen. Ob die aktuellste Version einer Anwendung eingesetzt wird, ist noch einfach zu überprüfen. Deutlich schwieriger wird die Beurteilung, wenn es tiefer in den Maschinenraum geht. Denn wie es mit Datenbanken, Serverkomponenten oder Script-Sprachen aussieht, erkennt der Nutzer nur dann, wenn er auf dem Server root-Rechte besitzt – und die sind eher den teureren Tarifpaketen vorbehalten. Mit Nikto besitzen Sie ein Werkzeug, das ein System gezielt auf Schwachstellen überprüft und auch veraltete Programmversionen entlarvt.

Wann Sie Nikto brauchen

Die Anwendung Nikto wurde dazu entwickelt, einen Webserver auf Sicherheitslücken zu analysieren. Das können beispielsweise falsch konfigurierte Erweiterungen für Apache sein. Aber auch veraltete Softwareversionen erweisen sich schnell als potenzielles Einfallstor für ungebetene Gäste auf dem Server. Nikto findet solche Lücken und ist leicht zu bedienen. Die Software ist ambivalent: Nikto kann für einen professionellen Angreifer eine wichtige Ergänzung zu nmap bei der Informationsbeschaffung über unbekannte Systeme sein. Während nmap zunächst die in einem Netzwerk vorhandenen Server ermittelt, dienen diese anschließend für Nikto als Angriffsziele. Nikto ist in den meisten Paketquellen aktueller Distributionen dabei. In der Regel

Nikto ist ein Programm für die Kommandozeile, es gibt aber auch grafische Oberflächen. Die Voreinstellungen für einen Scan lassen sich dann hier in Konfigurationsdateien definieren.



genügt also die Installation über den Paketmanager der Wahl. Sie können sich das in Perl geschriebene Programm aber auch direkt von der Projektseite herunterladen (<https://github.com/sullo/nikto/>). In der sehr guten Zusammenstellung von Kali Linux ist Nikto ebenfalls Standard. Die Spezialdistribution ist auch als Liveversion verfügbar. So können Sie schnell von jedem Rechner eine Analyse starten.

Was der Server über sich verrät

Bevor es losgeht, der obligatorische Hinweis, dass Sie Nikto nur auf Systeme loslassen dürfen, die Ihnen gehören. Bei der Überprüfung anderer Webserver machen Sie sich im Zweifel strafbar. Und die Nikto-Analyse könnte dort auch schnell auffallen, denn Nikto besitzt keinen Stealthmodus. Seine Analysen werden so schnell wie möglich ausgeführt: Auf dem Zielsystem tauchen eine Reihe von Anfragen auf, die

verdächtig erscheinen und ihre Spuren hinterlassen. Die einfachste Option, Nikto einzusetzen, besteht im Aufruf direkt im Terminal:

```
nikto -h
```

Es gibt für das in Perl geschriebene Programm auch eine Reihe grafischer Oberflächen, um damit zu arbeiten. Ob Sie darauf zurückgreifen wollen, ist letztlich Geschmackssache. Bei der Angabe des Zielrechners können Sie dessen URL, aber auch die IP-Adresse verwenden.

In diesem Zusammenhang sollten Sie sich vor Augen führen, dass je nach Aufruf der gleichen Maschine unterschiedliche Ergebnisse zurückgeliefert werden. Rufen Sie etwa einen virtuellen Host auf, beispielsweise „www.domain.tld“, werden die darunter angeordneten Verzeichnisse gefunden und untersucht. Beim Zugriff auf die IP-Adresse des Rechners sollten dabei die darunter angeordneten Verzeichnisse und

virtuellen Hosts ausgegeben werden. Ist ein fester Pfad Teil der Abfrage, wird Nikto auch nur innerhalb dieser Verzeichnisstruktur suchen. Nach der Bestätigung Ihrer Eingabe müssen Sie das System einen Moment seine Arbeit verrichten lassen. Wenige Sekunden nach dem Start tauchen dann erste Hinweise im Terminal auf. So erfahren Sie dort dann gleich, welche Serverversion eingesetzt wird, und können das Geschehen verfolgen. Es dauert eine Weile, bis die Software alle Tests abgeschlossen hat.

Wie Sie richtig auf die Analyse reagieren

Im Hinblick auf die gefundenen Schwachstellen zeigt sich Nikto sehr anwenderfreundlich. Einige der Meldungen sind unmittelbar verständlich, beispielsweise wenn die Analyse erbringt, dass die Lizenzdateien („license.txt“) der installierten Anwendungen offen zugänglich sind. Diese werden für die Ausführung der Programme nicht benötigt, enthalten aber Hinweise auf die installierte Version, was Angreifern wieder Rückschlüsse darüber erlaubt, wonach sie gezielt suchen müssen. Andere Meldungen erschließen sich dagegen nicht so ohne Weiteres. In den Ergebnissen fallen schnell die nummerierten Hinweise auf, zum Beispiel „OSVDB-3233“. Diese verweisen auf die Website des Projekts „Open Source Vulnerability Database“, das allerdings seine Dienste eingestellt hat.

Mit der Formulierung und dem exakten Zahlencode werden Sie in vielen Fällen durch eine Google-Anfrage Hinweise auf das Problem und dessen Lösung erhalten. Bei Schwachstellen, die auf SSL-Zertifikate oder Komponenten des Webservers hinweisen, besitzen Sie bei Nutzung eines Hostingpakets allerdings eher schlechte Karten, das Problem zu beseitigen. Denn der Zugriff auf die entsprechenden Komponenten ist von den Providern in der Regel verweigert. Erst beim Einsatz von dedizierten Servern, auf denen Sie root-Recht besitzen, können Sie die angemahnten Bibliotheken bearbeiten oder ersetzen.

Mit Nikto gezielt Schwachstellen aufstöbern

Je nach Größe der Installation, die geprüft wird, kann es eine Weile dauern, bis Nikto seine Arbeit beendet hat. Um dies abzukürzen, können Sie vorab auswählen, welche Tests durchgeführt werden sollen. Außer-

```

root@kali:~# nikto -h www.de
- Nikto v2.1.6
-----
+ Target IP:          134.119.57.68
+ Target Hostname:    www.de
+ Target Port:        80
+ Start Time:         2019-08-20 11:36:27 (GMT2)
-----
+ Server: Apache/2.4.39
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Root page / redirects to: https://www.de
+ Retrieved x-powered-by header: PHP/5.6.34
+ Uncommon header 'link' found, with contents: <https://www.de/wp-json/>; rel="https://api.w.org/"
+ Cookie wordpress_08d7990c266a2f37a7f1228eebaa3b5b created without the httponly flag
+ Cookie wordpress_sec_08d7990c266a2f37a7f1228eebaa3b5b created without the httponly flag
+ Cookie wordpress_logged_in_08d7990c266a2f37a7f1228eebaa3b5b created without the httponly flag
+ Cookie wp-settings-0 created without the httponly flag
+ Cookie wp-settings-time-0 created without the httponly flag
+ Cookie wordpressuser_08d7990c266a2f37a7f1228eebaa3b5b created without the httponly flag
+ Cookie wordpresspass_08d7990c266a2f37a7f1228eebaa3b5b created without the httponly flag
+ Cookie wp-postpass_08d7990c266a2f37a7f1228eebaa3b5b created without the httponly flag
+ All CGI directories 'found', use '-C none' to test none
  
```

Nach wenigen Sekunden liefert Nikto erste Informationen über den Server, wie in diesem Fall die fehlende Angabe eines MIME-Typs und dessen Konsequenzen.



Eine Recherche im Internet liefert in der Regel zu den jeweiligen Nikto-Ergebnissen detaillierte Informationen.

dem ist es möglich, sich das Ergebnis der Analyse auch in anderer Form zu speichern, um die Probleme in Ruhe nachzulesen und nacheinander zu bearbeiten. Um gezielt einen Bereich zu überprüfen, ergänzen Sie den Funktionsaufruf um den Parameter „-Tuning“, dem Sie dann den gewünschten Bereich als Ziffer folgen lassen. Um beispielsweise nach verräterischen Dateien zu suchen, nutzen Sie

```
nikto -h -Tuning 1
```

Das spart viel Zeit bei der Analyse. Für die Speicherung der Ergebnisse für spätere Verwendung ist ebenfalls ein Schalter beim Funktionsaufruf zuständig. Mittels „-Format“ definieren Sie das Ausgabeformat. Möglich sind etwa Text- und HTML-Dateien, aber auch die Weitergabe an Datenbanken

via CSV oder JSON. Eine Auflistung aller Parameter inklusive dieser Formate erreichen Sie mit diesem Befehl:

```
nikto -H
```

Zusätzlich definieren Sie den Namen der Ausgabedatei. Diese wird, sofern kein Pfad angegeben wird, in das Dokumentverzeichnis des aktuellen Benutzers geschrieben. Ein typischer Funktionsaufruf sieht dann folgendermaßen aus:

```
nikto -h -Format txt -o dateiname.txt
```

Der Schalter „o“ steht wie gewohnt für Output. Ihre eigentliche Arbeit beginnt dann am Ende der Analyse, wenn das Patchen der gefundenen Lücken beginnt oder neue Programmkomponenten installiert werden müssen. ■

Wireshark weiß, was im Netzwerk läuft

Immer mehr Geräte erfordern den Zugang zum Internet. Ob damit tatsächlich nur die Daten übertragen werden, die für das smarte Türschloss oder die Heizungsfernsteuerung notwendig sind, können Sie nur mit einem Spezialwerkzeug ermitteln.

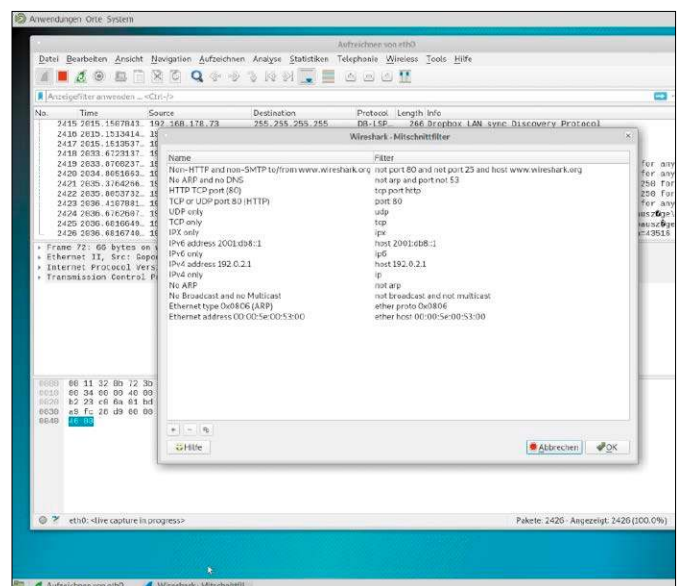
VON STEPHAN LAMPRECHT

Wir alle haben uns an den Komfort gewöhnt, dass sich unzählige Anwendungen auf unseren Computern automatisch aktualisieren. Und natürlich ist es komfortabel, wenn man auf dem Heimweg schon einmal Klimaanlage oder Heizung einschalten kann. Regelmäßig machen in diesem Zusammenhang Anwendungen Schlagzeilen, die zusätzliche Informationen über die angeschlossenen Systeme an einen Server des Herstellers senden. Ohne um Erlaubnis zu fragen, versteht sich. Wireshark hilft Ihnen dabei, unerwünschten Datenverkehr aufzuspüren. Der Paketsniffer ist allerdings ein Hardcoretool, das gute Kenntnisse über Netzwerkprotokolle voraussetzt.

Wozu setzen Sie Wireshark ein?

Der Sniffer Wireshark ist in allen Linux-Distributionen sowie für Windows und Mac-OS verfügbar. Das Programm kann den Datenverkehr aufzeichnen, wobei Sie sich den Inhalt eines Datenpakets ansehen können. Protokolliert wird dabei immer die IP-Adresse des Zielsystems. Mit Wireshark lassen sich beispielsweise Programme entlarven, die notorisch „nach Hause telefonieren“. Den gesammelten Datenverkehr können Sie auch statistisch auswerten, etwa nach besonders großen Paketen suchen oder sich Adressen herausuchen, die häufig aufgerufen werden. Eine Gegenprobe, wem eine solche IP-Adresse gehört, bringt Sie dann möglicherweise auf die Spur eines Angriffs. Wireshark protokolliert den Netzwerkverkehr der Schnittstellen des Systems, auf

Datenflut eingrenzen: Haben Sie ein bestimmtes Protokoll in Verdacht oder wollen sich die Darstellung übersichtlicher gestalten, setzen Sie einen der mitgelieferten Wireshark-Filter.



dem es installiert ist. Es kann also alle ein- und ausgehenden Verbindungen des jeweiligen Rechners untersuchen. Gleichzeitig empfängt es auch alle Datenpakete, die an alle Systeme im Netzwerk gesendet werden (Broadcasts).

Beim Router wird es schwieriger: Die Zentrale im Netzwerk kann Wireshark nicht direkt kontrollieren und protokollieren, es sei denn, der Router unterstützt dies selbst. Sofern vorhanden, liegt diese Protokollfunktion des Routers meistens tief vergraben in der Konfiguration. Bei der Fritzbox führt der Aufruf mit `fritz.box/support.lua` auf eine Supportseite, die „Paketmitschnitte“ anbietet. Die Seite ist auch auf der normalen Fritzbox-Oberfläche über den kleinen Link „Support“ links unten zu erreichen. Der Mitschnitt wird als Datei auf der Festplatte des PCs gespeichert, mit dem Sie die

Fritzbox bedienen. Das Dateiformat ist Wireshark-kompatibel und kann dem Sniffer direkt übergeben werden.

Achtung: Leider sind einige Fritzboxen (etwa die Kabel-Fritzboxen von Vodafone) funktionsreduziert und bieten diese Option nicht. Die technisch weit anspruchsvollere Alternative können wir hier nur ansprechen, aber nicht explizit ausführen: Sie besteht darin, den Router lediglich als Modem zu verwenden. Dahinter bauen Sie sich mit Open WRT und einem Raspberry Pi einen Router, den dort installiertes Wireshark dann komplett kontrollieren kann.

Netzwerkverkehr analysieren

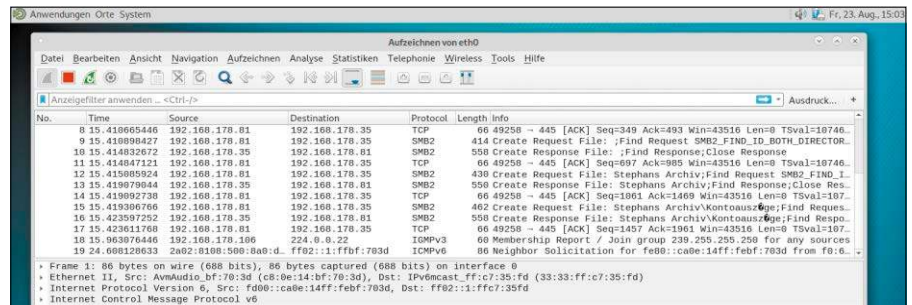
Vor der Analyse steht die Aufzeichnung. Nachdem Sie Wireshark gestartet haben, zeigt Ihnen die Software zunächst die Schnittstellen des Rechners an. In der

Übersicht markieren Sie den Eintrag der Schnittstelle, die überwacht werden soll. Mit einem Klick auf das Symbol einer Flosse in der linken oberen Ecke starten Sie die Aufzeichnung. Bereits während der Aufzeichnung können Sie einen Eintrag anklicken, um sich das Paket genauer zu betrachten. Arbeiten Sie wie gewohnt mit dem System weiter. Wenn es darum geht, unerwünschten Netzwerkverkehr zu entdecken, lässt sich ja nicht mit Bestimmtheit festlegen, wann ein Rechner seinen Zielhost aufruft. Übrigens können Sie zu einem späteren Zeitpunkt, wenn Sie ein Protokoll oder eine Zieladresse unter besonderem Verdacht haben, die Aufzeichnung des Datenverkehrs von Beginn an filtern. Im Menü „Aufzeichnen“ finden Sie dazu den Eintrag „Mitschnittfilter“.

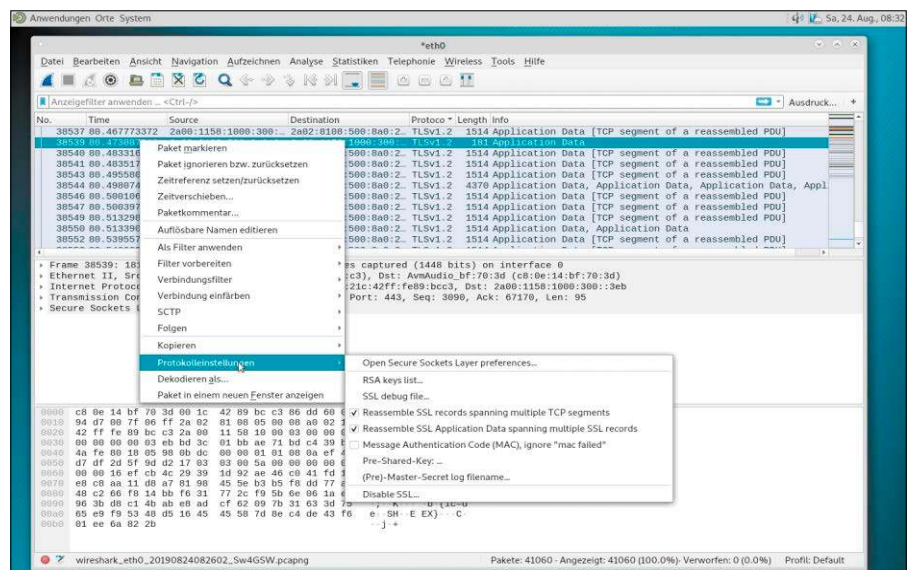
Aus dem nachfolgenden Dialog entscheiden Sie sich dann für eine der gezeigten Optionen. Über das Pluszeichen können Sie mit Unterstützung des Programms eigene Filter definieren. Praktisch ist die Funktion, sich die schnell angewachsene Liste mittels eines Autofilters (Icon mit farbigen Balken) zu organisieren. So werden die Pakete desselben Protokolls besser sichtbar. Bei der Analyse werden Sie wahrscheinlich häufiger auf Protokolle stoßen, die Ihnen im Alltag noch nicht häufig begegnet sind. Recherchieren Sie dann über das Internet, was es damit auf sich hat und wozu es genutzt wird.

Netzwerkprobleme finden

Verzögerungen beim Aufruf von Netzwerkressourcen oder der Eindruck, dass die Verbindung zu langsam ist, sind ein Klassiker bei Netzwerkproblemen. Wenn eine Geschwindigkeitsmessung direkt am Router (per Ethernet-Kabel und direkt an einer Ethernet-Schnittstelle) ergibt, dass die Bandbreite nicht dem gebuchten Tarif entspricht, sollte zusätzlich der DNS-Server überprüft werden. Häufiger haben Provider gerade in den Abendstunden damit ein Problem. Sofern möglich, tragen Sie im Router einen öffentlichen DNS ein, etwa von Google oder Oracle, und prüfen, ob sich das Problem damit lösen lässt. Falls nicht, kann Wireshark beim Eingrenzen helfen. Bei geringem Durchsatz liegt der Verdacht nahe, dass die Schnittstelle von einem Dienst belegt wird, der viele oder große Datenpakete versendet. Solche Analysen lassen sich mit den Statistikfunktionen des Programms



Sie können jedes einzelne Paket inspizieren: Über die Kommandos unter „Navigation“ verfolgen Sie Schritt für Schritt die Verbindung zu einem Internethost.



Bei jedem Element zeigt das Kontextmenü die Eigenschaften des jeweiligen Protokolls. So finden Sie für SSL die Option, den verwendeten Schlüssel einzutragen.

durchführen. Nutzen Sie das Kommando „Endpunkte“, um eine Liste der Zieladressen der Pakete abzurufen. Mit einem Klick auf die Spaltenübersichten sortieren Sie diese Einträge dann nach der Häufigkeit. So fallen Ihnen auch Endpunkte außerhalb Ihres Netzwerks schnell auf. Mittels Whois-Abfragen ermitteln Sie dann, wer hinter den entsprechenden IP-Adressen steckt. Falls es sich um den Provider handelt, dessen Hardware Sie einsetzen, kann ein Blick in die Pakete möglicherweise Aufschluss darüber geben, was dorthin übertragen wird. Stellt sich heraus, dass die IP-Adresse nicht eindeutig zugeordnet werden kann, sondern aus dem Adressraum eines anderen Zugangsproviders stammt, ist besondere Vorsicht geboten. Dahinter könnte dann ein Angriffsversuch stecken. Dann ist es sinnvoll, den Rechner auf Schädlinge und Rootkits zu untersuchen. Wireshark führt Sie nicht direkt zum potenziellen Täter, aber es verrät viel darüber, was im Netzwerk läuft.

Die Beurteilung, ob das mit rechten Dingen zugeht, müssen Sie aber selbst treffen.

Die SSL-Verschlüsselung

Sniffer wie Wireshark haben ein Problem: Um den Inhalt eines Pakets einsehen zu können, muss es unverschlüsselt vorliegen. Bei einer abgesicherten Verbindung taucht zwar das Paket mit der Zieladresse auf, der Inhalt lässt sich aber nicht kontrollieren. Die gute Nachricht: Wireshark kann auch verschlüsselten Datenverkehr entschlüsseln. Die Einschränkung: Das funktioniert nur dann, wenn man den verwendeten Schlüssel in Wireshark einlesen kann. Das ist allerdings anspruchsvoll: Die Wireshark-Entwickler haben im offiziellen Wiki eine Anleitung verfasst, die das grundsätzliche Vorgehen beschreibt, um beispielsweise SSL-Verbindungen zu analysieren, die von Firefox aufgebaut werden (https://wiki.wireshark.org/TLS?action=show&redirect=SSL#TLS_dissection_in_Wireshark). ■

Traffic-Kontrolle mit Burp-Suite

Bei jedem Medienbericht über Kundendatenbanken, die öffentlich im Netz auftauchen, fragen sich Betroffene, wie es dazu kommen kann. Ein mächtiges Werkzeug kann Schwachstellen und schlampige Programmierung rechtzeitig entlarven.

VON STEPHAN LAMPRECHT

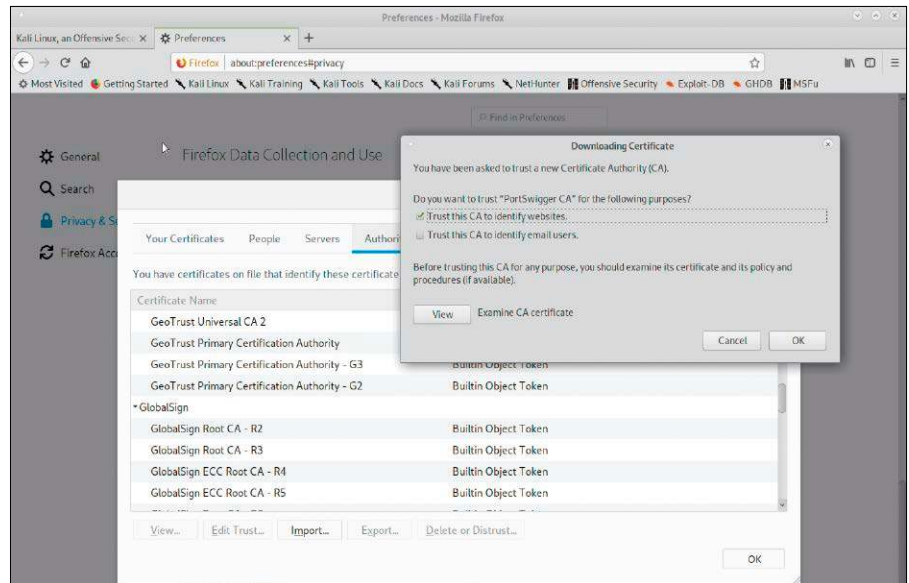
Das Sicherheitswerkzeug Burp-Suite ist in Java geschrieben. Der Hersteller bietet eine kostenlose Community-Version sowie eine kommerzielle Variante mit größerem Funktionsumfang an. Die kostenlose Version können Sie sich beim Hersteller herunterladen (<https://portswigger.net/burp/communitydownload>). Bei Kali Linux gehört die Burp-Suite bereits zum vorinstallierten Standardinventar.

Die Burp-Suite ist wie alle Werkzeuge dieser Art ein ambivalentes Tool: Sie können und dürfen damit Ihre eigenen Webdienste kontrollieren, beim Analysieren fremder Server benötigen Sie meist die Genehmigung des Besitzers.

Wie die Software funktioniert

Die Burp-Suite arbeitet als lokaler Proxyserver – als Zwischenstation, auf welche sämtlicher Netzverkehr zwischen Browser und Serveranwendung umgeleitet wird. So kann die Software den kompletten Datenverkehr abfangen und aufzeichnen. Auf diesen Weg lassen sich gezielt Lücken einer Anwendung finden und testen, indem beispielsweise Zeichenketten für Scripts gezielt manipuliert werden.

Damit Burp-Suite den Datenverkehr analysieren kann, starten Sie zunächst das Programm. Benutzen Sie im Assistenten einfach das angebotene temporäre Projekt und belassen Sie es bei den vorbereiteten Einstellungen. Das Prinzip des Programms wird sofort deutlich, wenn der Burp-Proxy auf dem gleichen Rechner wie der Browser läuft. Nachdem die Burp-Suite gestartet ist,



Vorbereitungen: Damit SSL-Verbindungen (HTTPS) ohne Störungen hergestellt werden können, muss im Browser das Zertifikat der Burp-Suite hinterlegt werden.

rufen Sie den Browser auf und wechseln dort in dessen Einstellungen. Aktivieren Sie dort einen Proxyserver, etwa unter Firefox über „Einstellungen → Allgemein → Netzwerk-Proxy“. Hier schalten Sie auf „manuelle Konfiguration“ und verwenden als Adresse „localhost“ mit dem Port 8080. Im Register „Proxy → Intercept“ der Burp-Suite deaktivieren Sie „Intercept ist on“.

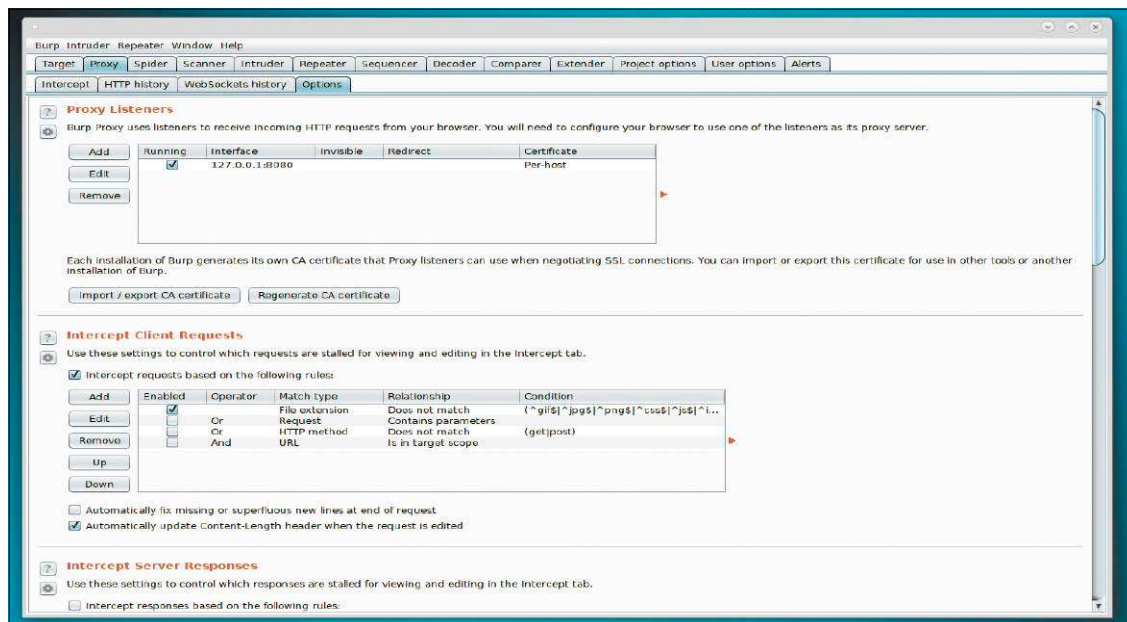
Rufen Sie mit dem Browser jetzt eine Seite im Internet auf. Wahrscheinlich erhalten Sie die Rückmeldung, dass die Verbindung nicht sicher ist. Da die meisten Onlineangebote inzwischen SSL-gesicherte Verbindungen anbieten (HTTPS), stört der Proxy die sichere Kommunikation. Deswegen installieren Sie zunächst ein von Burp ausgestelltes Zertifikat im Browser.

Rufen Sie dazu „http://burp“ auf (dabei muss die Burp-Suite laufen). Klicken Sie auf „CA Certificate“ und speichern Sie die Datei. In Firefox importieren Sie das Zertifikat mit „Einstellungen → Datenschutz & Sicherheit“. Über „Zertifikate anzeigen“ können Sie im Reiter „Zertifizierungsstellen“ über „Importieren“ das Zertifikat einbinden. Danach sollte der Abruf von HTTPS-Seiten gelingen. Jetzt schalten Sie in der Burp-Suite wieder auf „Intercept ist on“, wenn Sie die Datenpakete vor der Weiterleitung untersuchen wollen.

Netzwerkverkehr mitschneiden und prüfen

Die Burp-Suite ist eine ganze Sammlung von Werkzeugen, wobei der Proxyserver

Komplexe Oberfläche:
Über das Register
„Proxy“ im Programm
schalten Sie das Mit-
schneiden und Anhalten
des Datenverkehrs an.



die Grundlage bildet. Wer etwa Schwachstellen von Anwendungen herausfinden will, sucht sich zunächst alle Parameter zusammen, die der Browser an den Server schickt. Anschließend kann er damit experimentieren. Beispielsweise verlassen sich Entwickler oft darauf, dass sie nur gültige Werte bei Abfragen erhalten. Sie sparen sich die Mühe, genau zu definieren, welche Angaben zulässig sind. So können Angreifer dann etwa Code in eine Abfrage einschleusen, die in der Datenbank Änderungen vornimmt.

Bei der Durchsicht des Datenverkehrs fallen Informationen auf, die als „hidden“ in einem Formular markiert wurden, aber übermittelt werden. Rufen Sie in solchen Fällen die Zieladresse in Ihrem Browser auf. Sie stellen fest, dass sich die Website nicht sofort vor Ihnen aufbaut. Sie wechseln zum Fenster der Burp-Suite und müssen im Register des Proxys erst auf „Forward“ klicken, damit die Anfrage tatsächlich übermittelt wird. Er wird in der Liste am unteren Rand des Bildschirms dargestellt. Darin könnten Sie vor dem Absenden gezielt Werte verändern oder solche Eingaben an die weiteren Werkzeuge schicken.

Konkretes Beispiel: Passwörter oder Benutzernamen erraten

Wie funktionieren die in den Registern angeordneten Werkzeuge im Zusammenspiel? Ob durch einen Zufall oder gezielt könnte ein Angreifer mit einem Tool wie Dirbuster und Nmap herausgefunden ha-

ben, dass auf einem Server eine Instanz von Owncloud installiert ist. Im Anschluss aktiviert er die Burp-Suite und den Proxyserver, lässt die Datenpakete aber passieren, deaktiviert also die Option „Intercept“. Bei einer bekannten Anwendung wie Owncloud ist es nicht schwer herauszufinden, über welche URL die Benutzeranmeldung aufgerufen wird. Genau das würde ein Angreifer jetzt tun. Damit hinterlässt er in der Burp-Suite in der Historie einen Eintrag in der Liste im Abschnitt „Proxy“. Diesen Request klickt er mit der rechten Maustaste an und nutzt aus dem Kontextmenü den Eintrag „Send to Intruder“.

Der „Intruder“ (Eindringling) stellt in seinen Registern alle Funktionen zur Verfügung, mit der sich per „Brute Force“ Dateneingaben erzwingen lassen. Im Register „Position“ kann bei Bedarf die Stelle innerhalb des Requests verändert werden, an der der Benutzername an den Server übertragen werden soll. Ein Eingreifen ist aber häufig gar nicht notwendig. Für die Attacke benötigt der Intruder natürlich noch „Munition“. Diese wird innerhalb des Registers „Payload“ zusammengestellt. Darin ist praktischerweise auch eine Schablone, um Benutzernamen auszuprobieren. In den Optionen wird abschließend noch definiert, welche Rückmeldungen des Servers gespeichert werden.

Sind die Rahmendaten definiert, kann die Attacke gestartet werden. Bei einem solchen Angriff kommt es aus Sicht des Angreifers nun auf das Verhalten der Anwen-

dung an. Diese reagiert unterschiedlich auf einen gänzlich unbekanntem Nutzer und einen bekannten Nutzer, der nur sein Passwort falsch eingetragen hat. Über diesen Unterschied kann der Angreifer, nachdem er erst einmal den Benutzernamen herausgefunden hat, versuchen, das Passwort zu ermitteln.

Uns geht es an dieser Stelle nur um die Wirkungsweise der Werkzeuge. Denn der beschriebene Beispielangriff ist relativ primitiv. Brute-Force-Attacken auf Passwörter können Sie als Administrator recht einfach durch eine automatische Sperrung des entsprechenden Benutzerkontos nach einer bestimmten Zahl an Versuchen einschränken. Und eine erfolgreiche Brute-Force-Attacke läuft komplett ins Leere, wenn für die eigentliche Anmeldung eine Zwei-Faktor-Authentifizierung eingerichtet wurde.

Automatische Analyse für Premium-Nutzer

Zur Burp-Suite gehört zusätzlich das Werkzeug „Scanner“, mit dem sich Serveranwendungen gezielt auf Schwachstellen untersuchen lassen. Doch dieser Service hat seinen Preis. Die Funktion ist eine Premium-Funktion, für die pro Jahr 350 Dollar fällig werden. Die Anschaffung lohnt sich aber für Firmen, die regelmäßig eigene Anwendungen für das Web entwickeln. Denn der Scanner setzt die Burp-Suite quasi in den automatischen Modus, um beispielsweise Lücken aufzudecken, die das Einschleusen von schädlichem Code erlauben. ■

Dateien aufspüren mit Dirbuster

Auf den ersten Blick ist ein Webserver eine Blackbox. Niemand scheint wissen zu können, wie die Dateien darauf strukturiert sind. Es gibt aber ein Tool, das viel mehr verrät, als sich der Webmaster das vorstellt.

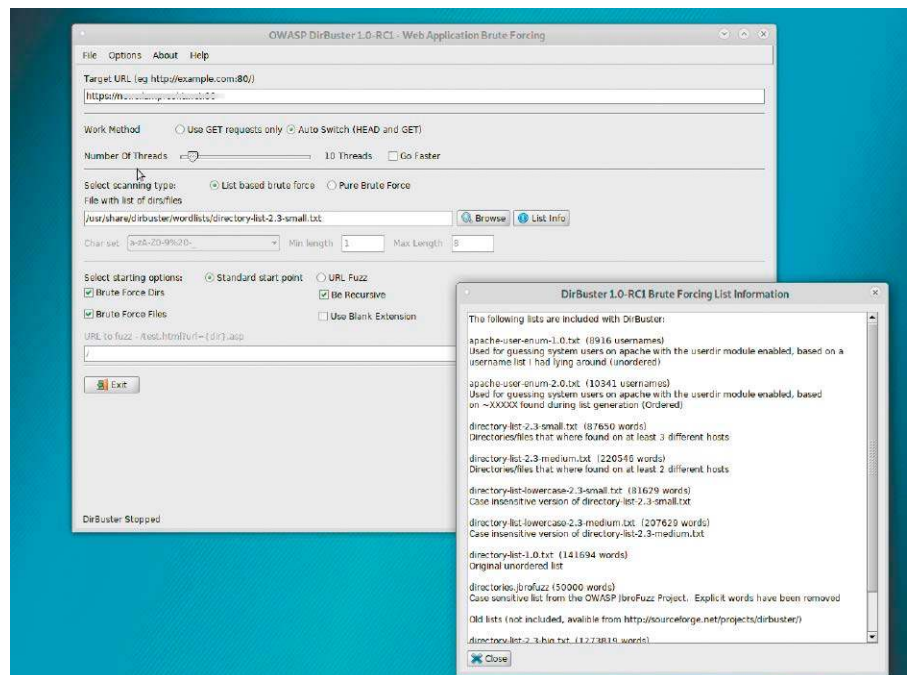
VON STEPHAN LAMPRECHT

Kein Angreifer schlägt einfach darauf los. Er wird sich zunächst möglichst viele Informationen über das System beschaffen, um danach zu entscheiden, an welcher Stelle ein Angriff möglicherweise erfolgreich ist. Und dafür sind Informationen über die Verzeichnisstruktur des Systems wertvoll. Umgekehrt können Administratoren herausfinden, was ein Angreifer ohne Mühe über den Server herausfindet. So können gezielt Barrieren eingebaut werden. Mit Werkzeugen wie Nikto oder Nmap lassen sich Informationen über die in einem Netz verfügbaren Computer und mögliche offene Ports gewinnen.

Ist erst einmal bekannt, welche Systeme vorhanden und erreichbar sind, kann im nächsten Schritt versucht werden, sich die Verzeichnisse und Dateien darauf genauer anzusehen. Genau das erledigt das Java-Programm Dirbuster.

Was Dirbuster herausfindet

Die Software arbeitet nach einem verblüffend einfachen Prinzip. Sie stellt an einen Webserver in kürzester Zeit eine Reihe von Anfragen, um Dateien und Verzeichnisse abzufragen. Für diese Requests benötigt das Programm entsprechende „Munition“. Diese bezieht es aus Wörterbüchern, in denen Namen von Dateien und Ordnern gespeichert sind, die als Basis für Attacks genutzt werden können. So ist das Verzeichnis „admin“ einer Webanwendung für einen Angreifer immer interessant. Die Methode des wilden Erratens von Dateien wird als „Brute Force“ bezeichnet. Da in recht



Fahndung nach Verzeichnissen und Dateien auf Webservern: Vor einer Abfrage mit Dirbuster legen Sie das Ziel fest, definieren die Zahl der Prozesse und entscheiden sich für eine Wortliste.

kurzer Zeit jede Menge Anfragen an das Zielsystem gestellt werden, setzen Sie sie legalerweise nur auf einem eigenen Server ein. Bei ihren Abfragen wertet die Software die von einem Server zurückgemeldeten Codes aus. Der bekannteste Fehler, den Nutzer aus dem Alltag kennen, ist die Meldung „404“ – eine Datei wurde also nicht gefunden. Aber längst nicht jedem Nutzer ist auch bewusst, dass der Server auch zurückmeldet, wenn eine Datei vorhanden ist. Der Code „200“ besagt, dass die gewünschte Ressource vorhanden ist. Ein Code „403“, also „forbidden“, weckt natürlich weitere Neugier. Denn damit wurde nicht nur be-

stätigt, dass es die Datei oder den Ordner gibt, sondern dass der Betreiber verhindern möchte, dass diese einfach abgerufen werden kann.

Dirbuster ist in Kali Linux standardmäßig vorhanden. Da es sich um eine Java-Anwendung handelt, können Sie sich das Archiv aber auch über die Projektseite <https://sourceforge.net/projects/dirbuster/support> besorgen. Gestartet wird die Anwendung dann über das im Archiv enthaltene Shell-Script.

Dirbuster wird zwar seit einiger Zeit nicht mehr aktiv weiterentwickelt, funktioniert aber nach wie vor ohne Probleme.

Verzeichnisstruktur eines Servers ermitteln

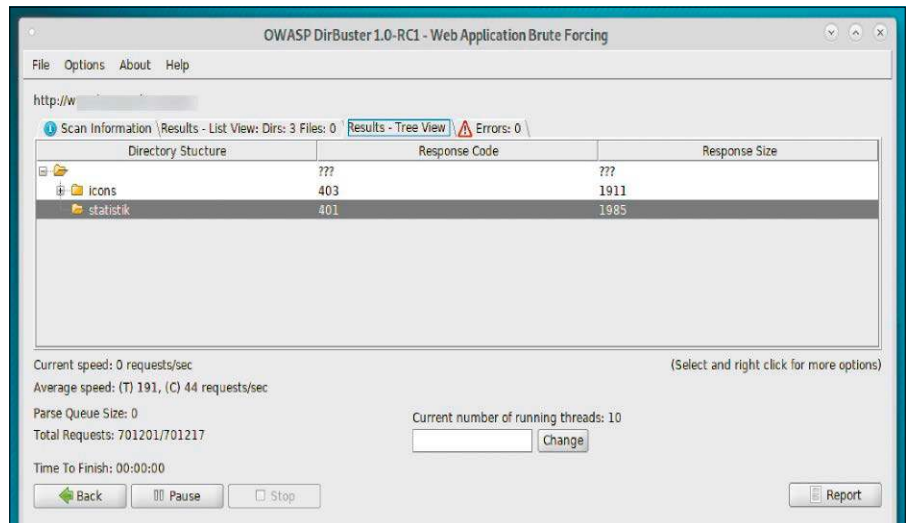
Um einen Webserver zu untersuchen, tragen Sie die URL nach dem Programmstart in das Feld „Target URL“ ein. Ergänzen Sie den Aufruf um den Port für das Protokoll. Bei einem Webserver wird das in der Regel Port 80 sein, als dann beispielsweise „http://www.meineseite.de:80“. Im nächsten Schritt müssen Sie eine Wortliste aussuchen, die Dirbuster verwenden soll. Eine kurze Beschreibung der mitgelieferten Listen erhalten Sie, wenn Sie auf den Schalter „List Info“ klicken.

Eine Webrecherche wird Sie optional zu einer ganzen Reihe von zusätzlichen Wörterbüchern führen. Mit „Browse“ wechseln Sie in das Verzeichnis der gewünschten Liste. Die von Dirbuster mitgelieferten Wörterbücher finden Sie üblicherweise im Verzeichnis „/usr/share/dirbuster/wordlists“. Bevor Sie die Untersuchung starten, legen Sie über den Schieberegler noch die Anzahl der parallelen Anfragen („Threads“) fest. Je größer die Anzahl, umso schneller sind Sie natürlich fertig. Andererseits wollen Sie mit dem Rechner wahrscheinlich noch weiterarbeiten. Hier müssen Sie also abwägen. Bereits 20 Prozesse können die Leistung etwas schwächerer Hardware ordentlich belasten. Mit einem Klick auf „Start“ beginnt die Abfrage.

Im Anschluss verfolgen Sie den Fortgang der Anfragen. Auch wenn das spannend ist, lohnt es sich eher, eine oder mehrere Tassen Kaffee zu kochen. Denn die Untersuchung kann sich über einige Stunden hinziehen. Interessant sind die Ergebnisse im Register „Results-Tree View“. Hier sehen Sie, wie sich langsam eine Verzeichnisstruktur des untersuchten Servers vor Ihnen aufbaut. Was für den normalen Seitenbetrachter unsichtbar ist, zeigt Dirbuster. Am Ende eines vollständigen Scans sehen Sie sich die Ergebnisse in den verschiedenen Registern an. Um später jederzeit darauf zurückgreifen zu können, lassen sich die Daten in Form eines Reports exportieren. Dazu klicken Sie am Ende auf den Schalter „Report“. Dabei haben Sie die Wahl, sich auf die gefundenen Verzeichnisse oder Dateien zu beschränken.

Wie Dirbuster die Sicherheit erhöht

Mit den Ergebnissen aus Dirbuster wüsste ein Angreifer jetzt also bereits viel über die



Während der Durchsicht baut Dirbuster langsam, aber sicher die Ordnerstruktur des Servers auf. Dabei sind die gemeldeten Codes des Servers interessant.



Dirbuster-Export: Damit Sie sich später die Ergebnisse in Ruhe ansehen können, ist das Speichern in Form eines Reports zu empfehlen.

Struktur des fremden Servers. Diese Informationen helfen aber auch dem Seitenbetreiber, den Einstieg möglichst zu verhindern und die Sicherheitsstrategie zu überprüfen. Achten Sie etwa auf die Codes des Servers und die Namen der Verzeichnisse. Bei Webanwendungen ist es immer ratsam, administrative Verzeichnisse und die darin liegenden PHP-Dateien vor einem externen Zugriff zu schützen. Das erreichen Sie mit einer „htaccess“-Datei. Eine Webrecherche erklärt Ihnen schnell, wie diese aufgebaut sein muss, um den externen Zugriff zu unterbinden.

Dirbuster ist aber auch hilfreich, wenn es darum geht, Sicherheitslücken zu schließen, die sich durch längst vergessene Installationen ergeben. Vielleicht haben Sie vor lange Zeit eine Software zum Teilen von Fotos ausprobiert? Oder testweise eine Anwendung wie Wordpress benutzt, dann aber nie produktiv genutzt? Wenn sich sol-

che PHP-basierten Anwendungen dann vielleicht sogar eine Datenbank mit anderen Programmen teilen, kann das brandgefährlich sein. Auch Dateien wie „Change-logs“ oder „Readme“ verraten Details zu Programmen, die auf dem Webserver laufen. Sie haben nach der Installation keine Funktion mehr und können in der Regel entfernt werden. Das trägt ebenfalls zu mehr Sicherheit bei.

Beim Löschen von Dateien und Verzeichnissen müssen Sie stets umsichtig agieren. Bei allen Dateien, von denen Sie nicht sicher sind, ob diese tatsächlich gelöscht werden können, machen Sie es sich am besten zur Gewohnheit, diese zunächst nach einem sprechenden Schema umzubenennen – etwa mit dem Zusatz „.old“.

Testen Sie danach Ihren Webserver mit allen Diensten. Erst dann, wenn alles nach wie vor reibungslos läuft, entfernen Sie diese Dateien endgültig. ■

Hacken Sie Ihre eigenen Systeme!

Wer Angriffe auf einen Computer oder ein Netzwerk ausführt, ist ein bössartiger Hacker – oder? Nicht ganz, denn mit gezielten Angriffen auf eigene Systeme versuchen Administratoren in aller Welt, ihre Infrastruktur sicherer zu machen.

VON STEPHAN LAMPRECHT

In der Medizin macht die Dosis das Gift, in der Computerforensik macht die Absicht des Angreifers den Unterschied. Ein Penetrationstest, kurz Pentest, ist der Versuch, gezielt Schwachstellen eines Systems auszunutzen oder zu protokollieren, wie sich das Ziel bei einem solchen Angriff verhält. Diese Methode befürwortet sogar das Bundesamt für Sicherheit in der Informationstechnik (BSI) und legt Unternehmen nahe, solche Tests durchzuführen (https://www.bsi.bund.de/DE/Publikationen/Studien/Pentest/index_htm.html).

Die Grenzen des Erlaubten

Ein Pentest ist genau unter zwei Voraussetzungen erlaubt:

1. Sie bombardieren ein System, das Ihnen gehört und von Ihnen betrieben wird. Diesen Bereich verlassen Sie bereits, wenn Sie einen Webserver testen, der bei einem Provider steht. In den meisten günstigeren Tarifen teilen Sie sich einen physikalischen Rechner mit einer ganzen Reihe von anderen Kunden. Ein Pentest könnte dann auch deren Systeme beeinträchtigen. Wir raten Ihnen also, sich auf Geräte zu beschränken, die bei Ihnen zu Hause stehen.



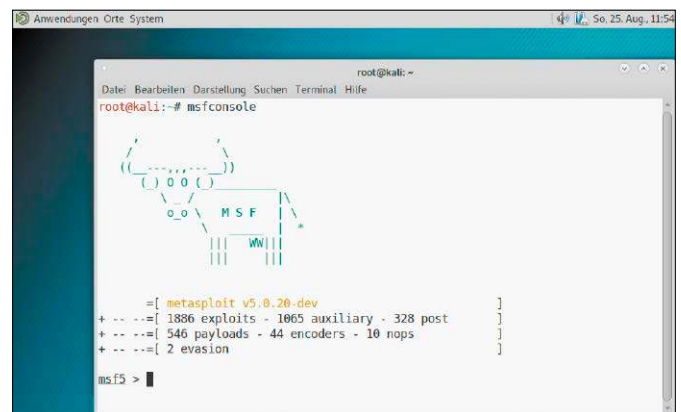
2. Sie haben vom Inhaber und Betreiber einer Infrastruktur den offiziellen Auftrag erhalten, einen solchen Test durchzuführen. Auf den nächsten Seiten zeigen wir Ihnen, wie Sie mit einem Framework handwerklich eigene Pentests planen und durchführen.

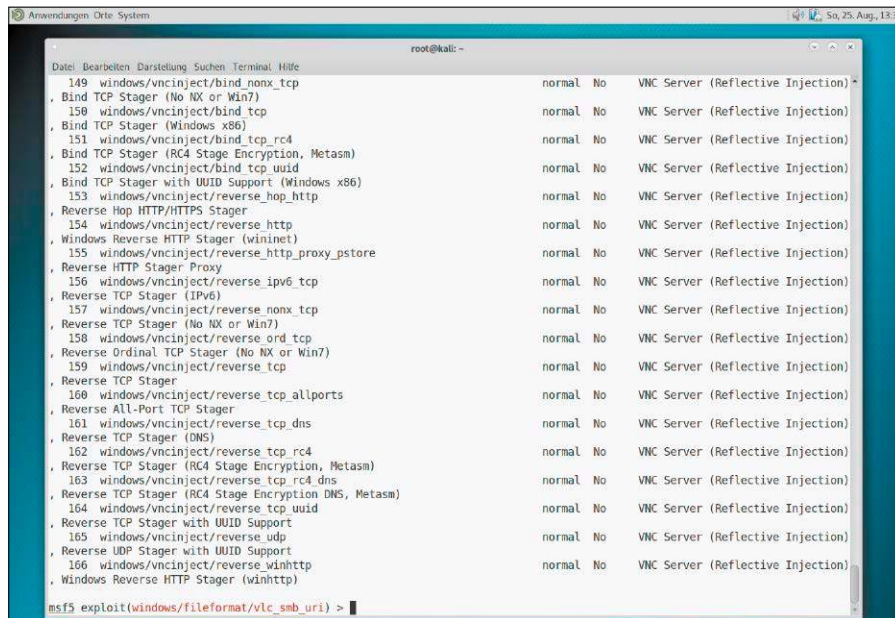
Metasploit stellt sich vor

Ein Framework sammelt verschiedene Werkzeuge rund um eine Aufgabenstellung. Zu dieser Kategorie gehört Metasploit, das unter einer Oberfläche verschiedene

Tools versammelt, die für Pentests benötigt werden. Dazu gehören Programmkomponenten zur Informationsbeschaffung und auch die sogenannten Exploits. Das sind Programmbestandteile, mit denen sich bekannte Sicherheitslücken eines Systems ausnutzen lassen. Metasploit ist eine kommerzielle Anwendung. Es gibt aber eine kostenlose Version, die für Linux, Windows und Mac-OS angeboten wird und die Basisfunktionen zur Verfügung stellt. Das kommerzielle Produkt ist zusätzlich mit einer

Wer ohne grafische Oberfläche auskommt, kann die Community-Edition von Metasploit nutzen. Zentrales Element ist die eigene Konsole.

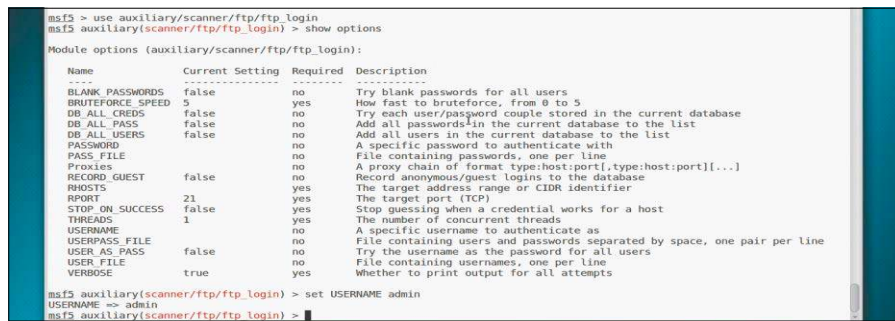




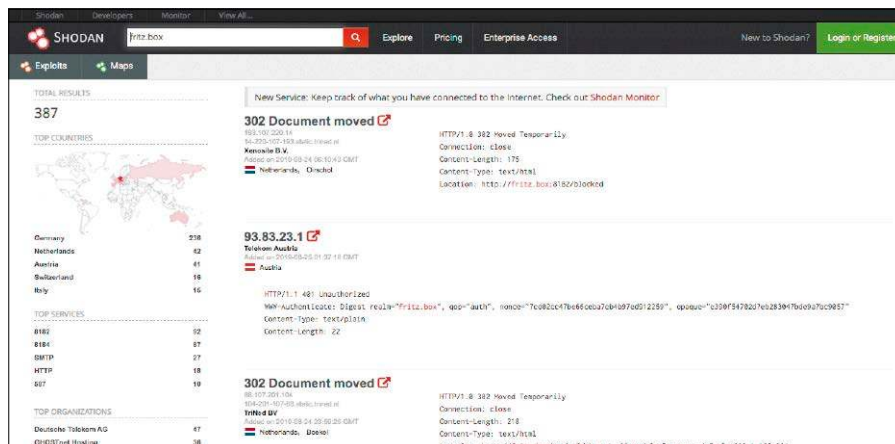
Die geänderte Farbe des Metasploit-Prompts signalisiert, dass Sie sich in einem Modul befinden. Mit Targets und Payloads sehen Sie sich Module an, die auf die Lücke angesetzt werden können.

wenn die notwendige Voraussetzung auf der Gegenseite gar nicht vorhanden ist, läuft der Angriff in Leere. Payloads sind Kommandos, die beim Angriff mitgeschickt werden, also sich beispielsweise im Zielsys-

tem festsetzen. Haben Sie das Ziel definiert, führt „run“ dann den Angriff aus. Ist er erfolgreich, werden Sie dies direkt im Terminal sehen. Läuft er ins Leere, was bei einer Sicherheitsprüfung ja ein gutes Zeichen ist,



Der integrierte Scanner prüft die FTP-Zugänge auf einem Server. Wir probieren es hier mit dem Konto „admin“.



Suchmaschine der besonderen Art: In Shodan (www.shodan.io) liefert eine einfache Abfrage nach „Fritz.box“ erstaunlich viele Treffer für offene AVM-Router.

probieren Sie einen anderen Exploit. Neben den konkreten kleinteiligen Exploits gehören zum Framework hilfreiche Zusatzprogramme. Mit diesen Scannern überprüfen Sie beispielsweise ein Log-in auf zu triviale Passwörter. So gibt es nach wie vor viele Router, die gemäß Auslieferungszustand dem Benutzer „admin“ das Passwort „admin“ zuordnen.

Wenn Sie sich außerhalb von Metasploit einen Überblick über die vorhandenen Scanner, Exploits und andere Module verschaffen wollen, können Sie dies direkt im Dateisystem tun. Unter „/usr/share/metasploit-framework/modules/“ sind die einzelnen Gruppen und Komponenten aufgelistet.

Nun zurück zur Suche nach trivialen Passwörtern. NAS-Systeme, Webserver und teilweise auch Router, die Filesharing anbieten, nutzen einen FTP-Zugang und besitzen in aller Regel ein Benutzerkonto für den Nutzer „admin“. Wie Sie gleich sehen werden, ist es immer günstig, wenn Sie einen eigenen Benutzer mit einem eigenen Namen einrichten, der über die Admin-Rechte verfügt. Denn mit Metasploit können Sie gezielt das Admin-Konto attackieren, um sich durch Brute Force Zugang zum System zu verschaffen. Dazu benötigen Sie nur eine Textdatei, in der sich die Passwörter befinden, die allesamt ausprobiert werden sollen. Über das Internet werden Sie schnell passende Wörterbücher finden können, wenn Sie nicht selbst eine solche Datei erzeugen wollen. Wie die Suche nach `search type:auxiliary path:scanner` oder der Blick in die Dateistruktur ergibt, gibt es eine Erweiterung mit dem Namen „ftp_login“, die im Verzeichnis „ftp“ liegt. Dieses Modul nutzen Sie mittels `use auxiliary/scanner/ftp/ftp_login`

Rufen Sie sich mit „show options“ die Parameter dazu auf. Mit „set USERNAME admin“ legen Sie den Admin-Account fest. Setzen Sie dann, wie bereits gezeigt, die IP-Adresse des Zielsystems und den Port. Die Datei, die im Stammverzeichnis von Metasploit liegen muss, definieren Sie mit `set PASS_File bsp.txt`

Jetzt können Sie mittels „run“ ermitteln, ob Sie sich mit Trivialpasswörtern oder dem Passwortmaterial aus der Dateiliste Zutritt zum System verschaffen können. Verblüffend simpel! Da Sie die wesentlichen Kommandos von Metasploit jetzt bereits kennen, können Sie das System weiter erkunden.

Ihnen wird ohne Zweifel eine ganze Reihe von weiteren Tests für Ihre Geräte einfallen.

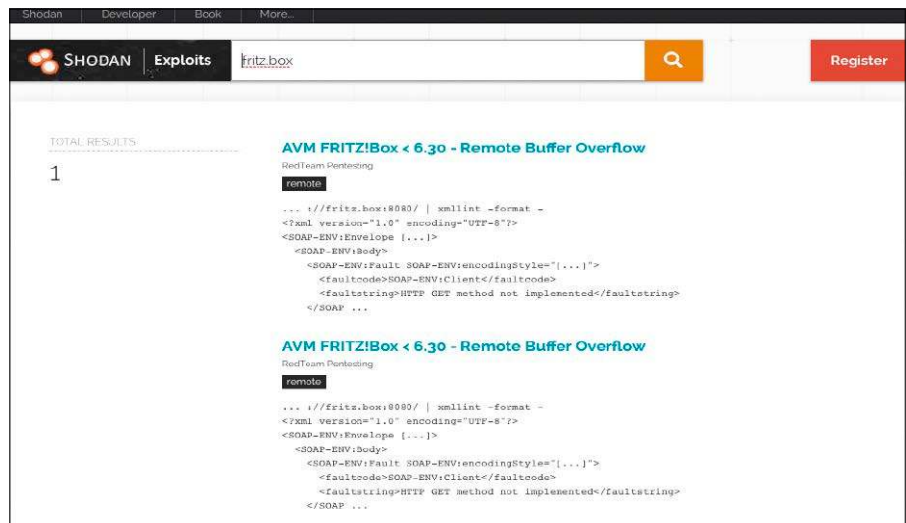
Mit Shodan verwundbare Geräte aufspüren

Fernseher, Beleuchtungssysteme, sogar Staubsauger erhalten heute von ihren Herstellern das Etikett „smart“. Es scheint fast, als könnten selbst Alltagsgegenstände nicht mehr ohne Verbindung mit dem Internet verkauft werden. Die Entwickler der Systeme versprechen den Konsumenten mehr Komfort und neue Möglichkeiten. Die Konnektivität ist auch meist rasch entwickelt. Oft zu schnell, denn häufig wird auf die Absicherung der Geräte kein Wert gelegt. Das belegen die vielen Schlagzeilen rund um Datenlecks und gekaperte Systeme, wenn beispielsweise Überwachungskameras von Dritten ferngesteuert und ihre Bilder ausgewertet werden können.

Grundsätzlich wollen es die Hersteller den Nutzern möglichst einfach machen. Sie werden mit Standardbenutzernamen und einfachen Passwörter ausgeliefert, ohne Aufforderung, ein sicheres Passwort zu vergeben. Ein weiteres Problem besteht oft auch darin, dass ein weniger komplexes Protokoll wie UDP verwendet wird, damit das Gerät schneller über einen anderen Computer gefunden wird.

Die Suchmaschine Shodan, die wohl eher wenigen Nutzern bekannt sein dürfte, sammelt Informationen zu offenen Systemen (<https://www.shodan.io>). Im Prinzip arbeitet Shodan wie Google, nimmt aber in seinen Index Systeme und Geräte auf, die über das Internet erreichbar sind. Wer in die Welt dieses besonderen Suchdienstes etwas tiefer eintaucht, wird schnell feststellen, dass es hier fast nichts gibt, was sich damit nicht finden lässt: Überwachungskameras, Router, Heizungsanlagen, Drucker, sogar Ampeln oder Stromzähler.

Wahrscheinlich fragen Sie sich jetzt, ob der Betrieb und die Nutzung eines solchen Systems überhaupt legal sind. Klare Antwort: ja. Es ist nicht illegal, das Internet nach öffentlich erreichbaren Systemen zu durchsuchen und das Ergebnis festzuhalten. Und es ist auch nicht illegal, sich darüber zu informieren. Verboten ist es allerdings, die Ergebnisse danach für einen Penetrationstest zu verwenden. Es sei denn, es handelt sich um Ihren eigenen Drucker oder Router. Hinter der Suchmaschine steckt auch ein Geschäftsmodell. Denn anders als bei



Der Angriff kann starten: Shodan nennt Ihnen „netterweise“ auch gleich noch die passenden Exploits zu einem offenen System.

Google sind nicht alle Funktionen kostenlos. Wer die Suchergebnisse mittels Filtern einschränken will, wird in der Regel auf die kostenpflichtige Variante hingewiesen. Wenn Sie Shodan besuchen, sehen Sie dort die klassische Eingabemaske. Geben Sie hier zum Test etwa „fritz.box“ ein.

Auf einer kleinen Karte sehen Sie anschließend die geografische Verteilung der Treffer. Mit einem Klick auf die Überschrift eines Eintrags bekommen Sie nun weitere Informationen zum gefundenen Gerät. Dazu zählen etwa Hostnamen, die gefundenen (offenen) Ports und die unterstützten Protokolle. Mit dem Symbol des Pfeils in der Überschrift bringt Sie Shodan dann sogar zu Anmeldemaske des Geräts. Mit den an einen registrierten Account geknüpften weiteren Filtern können Sie die Suche noch weiter eingrenzen:

Fritz.box country:DE city:Hamburg

Hier zeigt Shodan alle AVM-Router aus der Hansestadt, die öffentlich gefunden werden. Auch die Eingabe einer Ortschaft allein ist möglich. Oder probieren Sie einmal den Namen eines bestimmten Herstellers von Webcams aus. Sie werden überrascht sein, wie oft Sie dann ohne weiteres Zutun die Aufnahmen direkt abrufen können.

Klicken Sie nach der Suche nach einem Gerät auf das Kommando „Exploit“, liefert die Suche bekannte Lücken zum jeweiligen System zurück, die nachweislich bereits dazu verwendet worden sind, sich Zutritt zu schaffen. Shodan liefert alle Informationen, die Sie dazu benötigen, um einen gezielten Angriff zu planen und durchzuführen.

Kali Linux: Der komplette Werkzeugkasten

Es gibt Linux-Distributionen für jeden Geschmack. Die Programmzusammenstellungen berücksichtigen die Wünsche von Musikern, Lehrern oder Kreativen. Warum also nicht eine Distribution entwickeln, die sich in erster Linie der Computerforensik und Sicherheit widmet? Das war die Idee der beiden Initiatoren von Kali Linux, als sie ihr System vor rund sieben Jahren erstmals vorstellten. Kali Linux (www.kali.org) basiert auf Debian und stellt unter einem Desktop eine umfangreiche Sammlung von Sicherheitswerkzeugen zusammen: Nikto, Nmap, Wireshark, Burp Suite, Metasploit – alle diese Programme sind dort versammelt.

Das Startmenü des Desktops präsentiert die Programme übersichtlich nach deren Einsatzgebiet. Dort finden Sie die Rubriken „Schwachstellenanalyse“, „Informationsbeschaffung“ oder auch „Social Engineering“. Normale Programme wie der Internetbrowser oder das Terminal treten in den Hintergrund und sind unter „Useful Applications“ abgelegt.

Der größte Vorteil von Kali liegt im Zeitgewinn beim Einsatz der Tools. Diese sind startfähig installiert, alle Konfigurationsarbeiten entfallen somit. Und rund um Kali gibt es auch zahlreiche Tutorials, die den Einsatz der Programme genau erklären. Damit ist Kali ideal für alle, die Pentesting und Hacking einmal ausprobieren wollen, zumal Kali auch ohne Installation als Live-system arbeitet. ■

Viren finden und beseitigen

Die Bedrohungslage ist bei Linux mehr als entspannt. Aufgrund der Architektur und seiner deutlich geringeren Verbreitung haben Virentwickler mit dem System ihre Mühe. Das bedeutet aber nicht, dass Viren für Linux-Anwender gar keine Rolle spielen.

VON STEPHAN LAMPRECHT

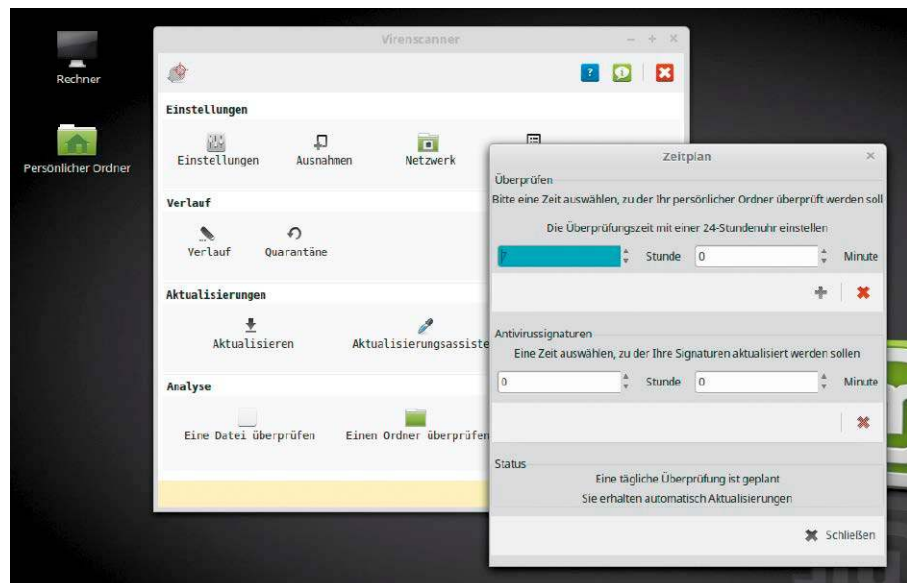
Windows-Schädlinge können Linux nichts anhaben oder nicht beschädigen. Aber natürlich können sie auch unter Linux vorkommen. Auf einem Linux-NAS in einer gemischten Netzwerkkumgebung können früher oder später auch Windows-Viren liegen, die sich beim Abruf der infizierten Datei auch auf andere Clients verbreiten. Deswegen ist es ratsam, Linux-Server regelmäßig auf Viren zu überprüfen, sofern dort auch Windows-Rechner zugreifen.

Das Linuxsystem regelmäßig scannen

Der Klassiker für diese Aufgabe ist Clam-AV. Der Scanner wird auch für Linux angeboten. Das Programm ist in den Paketquellen aller bekannten Distributionen vorhanden und mit wenigen Klicks installiert. Wie bei allen Virens Scannern gilt auch hier, dass die Signaturdateien regelmäßig aktualisiert werden müssen. Das übernimmt ein spezielles Programm, das Sie in einem Terminal mittels des Befehls

```
sudo freshclam
```

manuell aufrufen. Üblicherweise wird aber ein Daemon installiert und gestartet, der in regelmäßigen Abständen automatisch nach neuen Signaturdateien Ausschau hält. Clam-AV ist so flexibel, dass es eine ganze Reihe von Möglichkeiten gibt, das Scannen zu automatisieren und zu steuern. Auch die Einbindung in eigene Anwendungen ist möglich. Hier hilft ein Blick in die umfangreiche Dokumentation des Projekts, die auch die zahlreichen Optionen beim Funktionsaufruf erklärt. Denn das Programm



Das Open-Source-Programm Clam-AV, für das es auch grafische Oberflächen gibt, ist der meistverbreitete Virens Scanner unter Linux.

kann wahlweise den Nutzer nur über gefundene Viren informieren oder betroffene Dateien auch verschieben.

Ein einfacher und schneller Weg, den Prozess zu automatisieren, besteht im Anlegen eines Shell-Scripts, das lediglich aus dem Funktionsaufruf des Programms besteht. Dieses Script können Sie dann in die Crontabelle des Systems im gewünschten Intervall eintragen. Der Aufruf selbst könnte dann so aussehen:

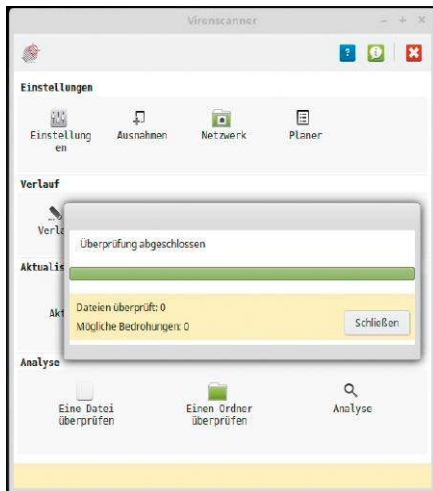
```
sudo clamscan -r --move=VERZEICHNIS0  
VERZEICHNIS1 VERZEICHNIS2
```

In diesem Fall untersucht die Software die Ordner „Verzeichnis1“ und „Verzeichnis2“ rekursiv (Schalter „-r“), also inklusive aller Unterordner. Jede verdächtige Datei wird in das Verzeichnis verschoben, das Sie hin-

ter „--move=“ angeben. Es gibt auch einen Schalter, um eine Datei automatisch zu löschen. Damit sollten Sie aber vorsichtig sein, da ja Fehlalarme nicht immer auszuschließen sind.

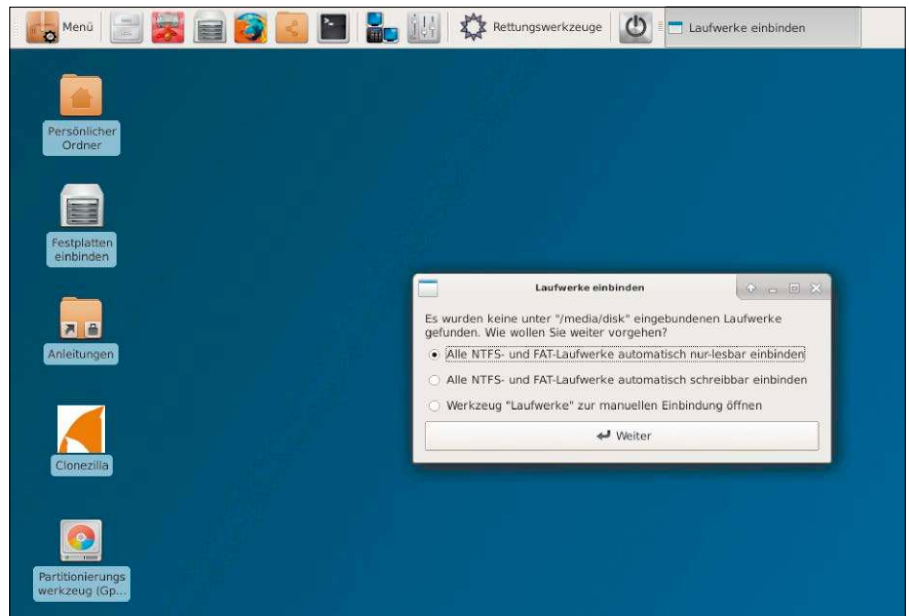
Linux als Windows-Helfer

Linux ist auch die perfekte Unterstützung, wenn es darum geht, Windows-Systeme zu untersuchen und im Notfall erste Maßnahmen zu ergreifen. Spätestens wenn Clam-AV einen Virus auf dem Linux-Dateiserver findet, ist es Pflicht, sämtliche Windows-Clients genauer unter die Lupe zu nehmen. Hier greifen Sie am besten auf ein Rettungssystem zurück, wie sie viele Hersteller von Sicherheitslösungen zum Download anbieten.



Die Prüfung mit Clam-AV lässt sich automatisieren und ist empfehlenswert, wenn das System etwa als Dateiserver für Windows-Clients genutzt wird.

Die LinuxWelt-Redaktion bietet ebenfalls ein solches Rettungssystem, das Sie kostenlos nutzen können (www.pcwelt.de/downloads/PC-WELT-Notfall-DVD-3890747.html). Der Unterbau solcher Systeme und auch dieses Rettungssystems ist ein Linux, das im Livebetrieb ausgeführt wird. Mit dem unabhängigen Notfallsystem können Sie den Windows-Rechner aus unkompromittierter Quelle nach Viren durchsuchen, Benutzerdateien auf andere Datenträger retten oder Reparaturen erledigen, falls ein Windows-System nicht mehr startet. Die Vorgehensweise ist bei allen Datenrettern ähnlich. Sie starten den Computer über DVD- oder USB-Medium. Dazu müssen Sie im Bios meist die Reihenfolge beim Systemstart verändern oder Secure Boot abschalten. Das Livesystem wird Sie dann dazu auffordern, ein WLAN auszuwählen, falls der Computer nicht per Ethernet mit dem Internet verbunden ist. Meist erfolgt anschließend die Aktualisierung der Programme und der Virensignaturen. Unter Linux können Sie nur auf Datenträger zugreifen, die in das Linux-Dateisystem eingehängt sind. Das gilt auch für Rettungssysteme. Um also gezielt die interne Festplatte oder besser eine Partition zu untersuchen oder zu bearbeiten, müssen Sie die Platte des Windows-Rechners erst anmelden. Im Notfallsystem der LinuxWelt/PC-Welt gibt es dafür das Leistsensymbol „Festplatten einbinden“. Über die weitere Schaltfläche „Rettungswerkzeuge“ erreichen Sie dann mehrere Antivirenprogramme – neben Clam-AV auch Avira oder Sophos.



PC-Welt-Rettungs-DVD: Unser Linux-Spezialsystem für Windows-Pannen kann nach Viren scannen und Benutzerdateien retten oder das Windows-Passwort zurücksetzen.

„Reparatur“ ist selten erfolgreich

Und wenn ein Virus gefunden wird? Die meisten am Markt befindlichen Schutzprogramme versprechen, einen Virenbefall reparieren zu können. Was unter dieser Reparatur zu verstehen ist, definieren die Hersteller aber sehr verschieden. Häufig wird die entsprechende Datei nur lokalisiert und automatisch in ein besonderes Verzeichnis verbannt („Quarantäne“). Wenn es sich um die ausführbare Datei eines Windows-Programms handelt, lässt sich dieses dann nicht mehr starten.

Nach unserer Einschätzung sind die Versuche, einen Virus tatsächlich physikalisch aus einer befallenen Binärdatei zu entfernen, selten von Erfolg gekrönt. Bevor Sie sich auf zweifelhafte Rettungsaktionen einlassen, ist es sicherer, den befallenen Rechner vollständig neu aufzusetzen. Dazu gehören die vollständige Formatierung der Speichermedien, die Installation des Betriebssystems aus einer vertrauenswürdigen Quelle und die Wiederherstellung der gespeicherten Benutzerdateien aus einem Backup. Wichtige Benutzerdateien können Sie mit dem Rettungssystem aber auch vom infizierten System auf einen anderen Datenträger kopieren und dadurch retten. Die Gefahr, dass Office-, Text- und Mediendateien Schadsoftware enthalten und diese durch einen Software-Interpreter wie Excel, Adobe Reader oder VLC ausgelöst werden, ist nicht völlig auszuschließen, aber sehr gering.

Rootkits sind für Linux gefährlich

Es gibt durchaus ein Bedrohungsszenario für Linux-Systeme, das Sie ernst nehmen sollten. Das Konto root darf unter Linux alles und Rootkits, deren Namen sich inzwischen auch für ähnliche Schädlinge für andere Systeme eingebürgert hat, sind Werkzeugsammlungen eines Angreifers, die sich erfolgreich vor der Entdeckung von Virenskannern tarnen. Ein solches Rootkit eröffnet dem Angreifer die Option, sich auf dem kompromittierten System anzumelden, Netzwerkverkehr zu überwachen oder Programme zu starten. Häufig werden solche erfolgreich auf verschiedenen Systemen installierten Kits für konzertierte Attacken genutzt.

Ein Programmpaket, das beim Aufspüren solcher Rootkits hilft, ist „chkrootkit“, das in den Paketquellen aller Distribution zu finden ist. Es wird in einem Terminal mit root-Recht gestartet (`sudo chkrootkit`), um das System zu untersuchen. Um sicher zu sein, dass das eigene System und damit das Programm chkrootkit nicht seinerseits kompromittiert ist, ist es ratsam, chkrootkit von einer unabhängigen Live-CD zu verwenden. Möglicherweise hat der Angreifer sein Rootkit gegenüber der Software getarnt, deswegen kann es nicht schaden, eine zweite Meinung etwa mit dem Programm rkhunter einzuholen. Auch dieses Tool ist in allen Distributionen über die Paketquellen zu beziehen. ■

Software und Paketverwaltung

Neue Anwendungen und Updates beziehen Sie unter Linux in der Regel aus dem Software-Repository der jeweiligen Distribution. Für die Verwaltung gibt es mehrere Tools mit unterschiedlichen Funktionen.

VON THORSTEN EGGELING

Fast alle Linux-Distributionen verwenden eine zentrale Paketverwaltung, über die Sie die gewünschte Software beziehen, installieren und aktualisieren. Die Vorteile: Sie erhalten geprüfte und virenfreie Programmpakete, die reibungslos mit dem Betriebssystem zusammenarbeiten. Sicherheitsupdates gibt es automatisch für jedes installierte Programm.

Es gibt aber auch Nachteile. Bei Distributionen wie Ubuntu, Linux Mint oder Debian sind Sie in der Regel auf die Programmversionen festgelegt, die zur jeweiligen Version des Betriebssystems gehören. Neuere Versionen gibt es erst beim nächsten Upgrade der Distribution. Ausnahmen sind beispielsweise Firefox und Thunderbird. Wer aktuellere Programme benötigt oder in der Paketverwaltung nicht fündig wird, kann jedoch zusätzliche Paketquellen einbinden oder Software auf anderen Wegen installieren (siehe Artikel ab Seite 46 und 48).

Für die Paketverwaltung bieten Ubuntu und verwandte Distributionen mehrere Tools für unterschiedliche Zielgruppen und mit unterschiedlichen Funktionen. Teilweise ist es Geschmackssache, welchem Programm der Vorzug zu geben ist. Es gibt aber auch Aufgaben, die sich nur mit einem bestimmten Tool erledigen lassen.

1. Programme und Bibliotheken

Ausführbare Programmdateien enthalten unter Linux in der Regel nicht alle nötigen Komponenten. Meist ist zusätzlich wenigstens eine Standardbibliothek erforderlich, die Funktionen für in der Programmier-



sprache C geschriebene Programme enthält. Genauere Informationen liefert beispielsweise diese Befehlszeile:

```
ldd /bin/bzip2
```

In der Ausgabe sehen Sie alle Programmbibliotheken, die das Komprimierungstool bzip2 benötigt. Darunter ist die Standardbibliothek „libc.so.6“ zu finden, „linux-vdso.so.1“ stellt einige Kernel-Funktionen bereit und „ld-linux-x86-64.so.2“ ermöglicht es, Bibliotheken bei Bedarf zu laden („dynamic

shared“). Die Komprimierungsfunktion ist in der Bibliothek „libbz2.so.1.0“ zu finden, die auch andere Programme nutzen können. Programme benötigen genau die Bibliotheken, mit denen sie erstellt wurden, oder eine höhere, abwärtskompatible Version. Das Konzept der dynamisch ladbaren, gemeinsam genutzten Bibliotheken verringert die Größe der Programmdateien und ermöglicht eine effiziente Hauptspeicherung.

Abhängigkeiten: Die meisten Programme benötigen zusätzliche Bibliotheken. Die Paketverwaltung sorgt für die automatische Installation der abhängigen Pakete.

```
te@ub180407: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
te@ub180407:~$ ldd /bin/bzip2
        linux-vdso.so.1 (0x00007fff225e9000)
        libbz2.so.1.0 => /lib/x86_64-linux-gnu/libbz2.so.1.0
        (0x00007f197c183000)
        libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x0000
        7f197bd92000)
        /lib64/ld-linux-x86-64.so.2 (0x00007f197c59d000)
te@ub180407:~$
```

2. Das Debian-Paketformat

Bei Installation oder Update lädt die Paketverwaltungssoftware bei Debian/Ubuntu-Systemen eine „deb“-Datei herunter. Es handelt sich um ein gepacktes Archiv, das ausführbare Dateien, Bibliotheken und Konfigurationsdateien enthalten kann, die bei der Installation in das Dateisystem kopiert werden. Ebenfalls enthalten sind meist einige Scripts, über die sich beim Setup beispielsweise Konfigurationsdateien anpassen oder Systembenutzer erstellen lassen. Ein weiterer Bestandteil ist eine Textdatei mit Informationen über die Abhängigkeiten von anderen Paketen sowie optionalen Empfehlungen für zusätzliche Pakete.

3. Die Paketverwaltung bei Ubuntu

Bei der Softwareinstallation muss die Paketverwaltung die ausführbaren Dateien auf die Festplatte kopieren und dafür sorgen, dass alle benötigten Bibliotheken und Tools vorhanden sind. Bei komplexeren Programmen ergibt sich ein verzweigter Baum von Abhängigkeiten („dependency tree“) und die Paketverwaltung installiert mehrere Pakete.

Wer es genauer wissen möchte, kann mit dem Befehl

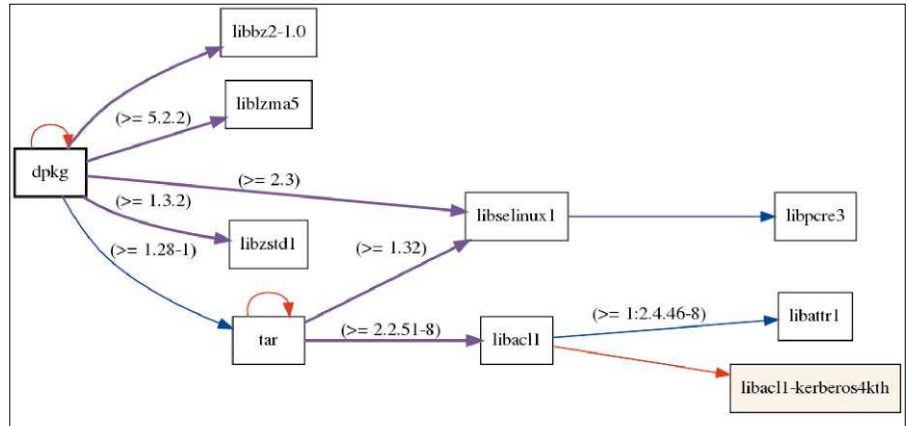
```
debtree [Paketname] | dot -Tpng > bild.png
```

eine grafische Darstellung der Abhängigkeiten eines Pakets erstellen. Die Pakete „debtree“ und „graphviz“ müssen dafür installiert sein.

Das zentrale Programm zur Paketverwaltung heißt unter Ubuntu und verwandten Systemen dpkg. Es verwendet Datenbanken, in denen verfügbare und installierte Pakete gespeichert sind. dpkg lädt jedoch keine Paketdateien herunter und prüft keine Abhängigkeiten. Deshalb werden Sie das Tool nur selten direkt nutzen (siehe auch ab Seite 48). Stattdessen verwenden Sie eines der Programme, die wir in den nächsten Punkten beschreiben.

4. Die Standard-Paketverwaltung von Ubuntu

Anwendungen für die grafische Oberfläche lassen sich in Ubuntu mit Ubuntu-Software installieren, entfernen und aktualisieren. Sie starten es über das Icon in der Starterleiste. Auf der Registerkarte „Alle“ zeigt das Tool Kategorien wie „Audio und Video“ und „Grafik und Fotografie“. Klicken Sie eine



Dependency Tree: Damit ein Linux-Programm läuft, sind meist zusätzliche Tools und Bibliotheken ab einer bestimmten Version erforderlich. Welche das sind, lässt sich mit debtree ermitteln.

Kategorie an und stöbern Sie in der Liste nach für Sie interessanten Anwendungen. Wenn Sie den Namen eines Programms

kennen, können Sie auch die Suchfunktion verwenden (Lupensymbol auf der Startseite). Empfehlenswert ist auch ein Blick in die

Programme installieren: Ubuntu-Software ermöglicht eine komfortable Programmauswahl. Das Angebot ist hier aber nicht vollständig und enthält beispielsweise keine Terminaltools.



PAKETVERWALTUNG IN ANDEREN DISTRIBUTIONEN

Bei allen verbreiteten Linux-Distributionen erfolgt die Paketverwaltung ähnlich wie bei Debian/Ubuntu. Es gibt jedoch andere Paketformate und Tools für deren Verwaltung. Bei Fedora dient Gnome-Software als Standardtool, das auch die Basis von Ubuntu-Software bildet. Nutzer des KDE-Desktops nutzen Plasma Discovery. Im Terminalfenster kommt hier dnf, der Nachfolger von yum, zum Einsatz. dnf ähnelt in der Bedienung apt. Für die Installation beispielsweise verwendet man

```
sudo dnf install [Paketname]
```

Als Paketformat verwendet Fedora RPM (RPM Package Manager, früher Red Hat Package Manager). RPM wird auch von Open Suse genutzt, zur Paketverwaltung dient hier Yast2 und auf der Kommandozeile Zypper.

Auch Gentoo Linux kennt eine Softwareverwaltung, die allerdings etwas anders funktioniert. Das Tool emerge greift auf einen täglich aktualisierbaren Portage-Tree zu, in dem Infos zu Quelltextarchiven und Abhängigkeiten hinterlegt sind. Bei der Installation werden die Binärdateien aus dem Quelltext erstellt. Das ermöglicht sehr aktuelle Softwareversionen, birgt aber auch ein hohes Fehlerpotenzial. Letztlich ist der Benutzer selbst dafür verantwortlich, dass alles reibungslos zusammenpasst.

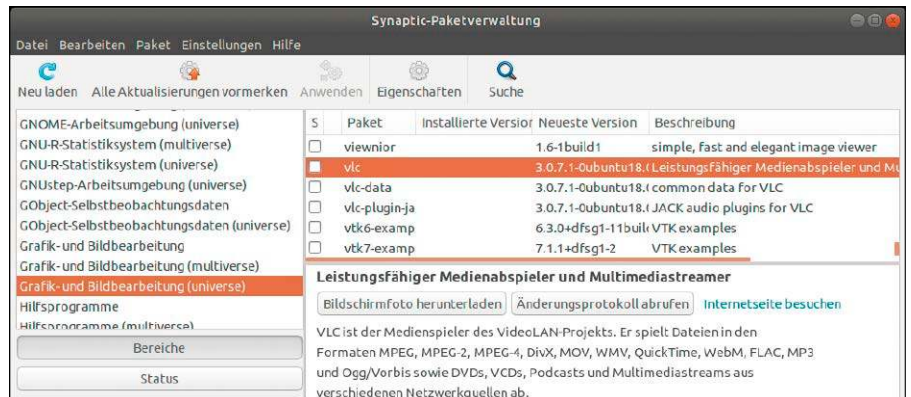
Kategorie „Erweiterungen“. Hier finden Sie neue Schriftarten und nützliche Shell-Erweiterungen.

Ein Klick auf das Programmsymbol führt zu weiteren Informationen (häufig mit Screenshot), Beschreibungen und Rezensionen. Unter „Details“ erfahren Sie jeweils, um welchen Pakettyp es sich handelt. Wenn hinter „Quelle“ beispielsweise „ubuntu-bionic-universe“ oder ähnlich steht, handelt es sich um ein herkömmliches „deb“-Paket. Sollte die Angabe „Snap-Store“ lauten, dann handelt es sich um einen Snap-Container (siehe ab Seite 46).

Klicken Sie auf „Installieren“, um eine Software einzurichten. Sollte diese bereits vorhanden sein, sehen Sie die Schaltflächen „Starten“ und „Entfernen“. Die Registerkarte „Installiert“ (Startseite) zeigt Ihnen eine Liste der installierten Anwendungen, per Klick auf „Entfernen“ können Sie ein Programm deinstallieren. Auf der Registerkarte „Aktualisierungen“ sehen Sie die verfügbaren Updates. Klicken Sie auf die Schaltfläche links oben im Fenster, um die Paketdatenbank zu aktualisieren.

5. Softwarepakete mit Synaptic verwalten

Synaptic ist bei Linux Mint 19 bereits vorinstalliert, Ubuntu-Nutzer können das Tool über Ubuntu-Software nachinstallieren. Synaptic bietet eine Suchfunktion und



Alles installieren: Synaptic bietet eine schnelle Suche nach allen verfügbaren Anwendungen, Tools und Bibliotheken. Software lässt sich außerdem über „Bereiche“ auswählen.

mehrere Filter, über die sich die Ansicht auf die gewünschte Software einschränken lässt. Das Tool ist im Vergleich zu Ubuntu-Software etwas unübersichtlicher, dafür liefert aber die Suche schnellere Ergebnisse. Anders als mit Ubuntu-Software lassen sich mit Synaptic alle verfügbaren Programme installieren, also auch Tools für die Kommandozeile, Bibliotheken und Entwicklerpakete.

Nach dem Start von Synaptic klicken Sie zuerst auf „Neu laden“, um die Paketdatenbank zu aktualisieren, und danach auf die Schaltfläche „Suche“. Tippen Sie einen Suchbegriff ein und klicken Sie auf „Suchen“. Sie können den Namen eines Programms verwenden oder einen Begriff, der

in der Beschreibung vorkommen sollte. Synaptic kann auch alle verfügbaren Programme aus einer Kategorie anzeigen. Dazu klicken Sie auf „Bereich“ und wählen beispielsweise „Grafik- und Bildbearbeitung“. In der Regel ist alles aus dieser Kategorie bereits installiert. Weitere Software gibt es unter „Grafik- und Bildbearbeitung (universe)“ sowie „Grafik- und Bildbearbeitung (multiverse)“. Programme aus dem Bereich „multiverse“ unterliegen lizenzrechtlichen Einschränkungen, was beispielsweise für Multimedia-Codecs gelten kann. In der Kategorie „universe“ ist freie Software ohne solche Einschränkungen zu finden. Für Endanwender in Deutschland hat diese Unterscheidung jedoch keine Konsequenzen. Sie können alle installierbaren Programme uneingeschränkt und kostenlos nutzen. Es kann jedoch Länder oder Einsatzbereiche geben, die Programme aus dem Bereich „multiverse“ nicht erlauben.

Software installieren und entfernen: Wenn Sie fündig geworden sind, klicken Sie das gewünschte Paket mit der rechten Maustaste an und wählen „Zum Installieren vormerken“. In der Regel öffnet sich ein Fenster, das eine Liste mit weiteren erforderlichen Paketen anzeigt. Klicken Sie auf „Vormerken“ und danach in der Synaptic-Symboleiste auf „Anwenden“. Das Fenster „Zusammenfassung“ zeigt Ihnen die anstehenden Änderungen. Klicken Sie auf „Anwenden“, um die Installation anzustoßen. Für die Deinstallation wählen Sie im Kontextmenü eines Pakets „Zum Entfernen vormerken“ und klicken danach auf „Anwenden“. Prüfen Sie im Fenster „Zusammenfassung“ die Angaben unter „Zu entfernen“. Hier sollten nur das gewählte Paket und wenige weitere Pakete aufgeführt sein.

PROBLEME BEI DER INSTALLATION BEHEBEN

Bei der Vielzahl der Softwarepakete ist nicht ausgeschlossen, dass es bei Installationen oder Updates zu Fehlern kommt. Meist sind nur Pakete betroffen, die selten installiert werden und nicht ausreichend gepflegt sind. Die Installation kann beispielsweise fehlschlagen, wenn eine Abhängigkeit besteht, die nicht erfüllt werden kann. Das Problem lässt sich meist mit

```
sudo apt-get -f install
```

lösen. Dabei wird das defekte Paket entfernt. Sollte das nicht funktionieren, verwenden Sie

```
sudo dpkg -r [Paketname]
```

Damit löschen Sie das Paket ohne Prüfung der Abhängigkeiten.

Bei Problemen mit Abhängigkeiten können Sie nur darauf warten, dass der Paketbetreuer den Fehler behebt. Oder Sie suchen nach einer alternativen Quelle für die Software (siehe ab Seite 48).

Eine häufige Fehlermeldung bei der Verwendung von apt ist „Konnte Sperre /var/lib/dpkg/lock-frontent nicht bekommen“ oder ähnlich. Ursache dafür ist meist ein automatisches Update im Hintergrund. Warten Sie einige Zeit, bis das Update abgeschlossen ist, und versuchen Sie es dann erneut. Die Meldung erscheint auch, wenn ein anderes Tool die Paketverwaltung gesperrt hat (beispielsweise Synaptic) oder wenn Sie apt ohne vorangestelltes „sudo“ starten.

Ist die Liste sehr lang, besteht die Gefahr, dass wichtige Pakete dabei sind, und die Deinstallation die Funktionen des Betriebssystems beeinträchtigt. In diesem Fall sollten Sie die Deinstallation besser abbrechen. Bei systemrelevanten Programmen gibt Synaptic ohnehin eine Warnmeldung aus. Die Frage „Sind Sie sicher, dass Sie das tun wollen?“ sollte Sie immer alarmieren und ist besser mit „Nein“ zu beantworten. Im Kontextmenü gibt es außerdem den Punkt „Zum vollständigen Entfernen vormerken“. Damit entfernen Sie Programmdateien inklusive Konfiguration. Verwenden Sie diese Funktion, wenn Sie ein Programm auch in Zukunft nicht mehr verwenden wollen oder wenn Sie Fehler in der Konfiguration vermuten, die sich auch nach einer Neuinstallation auswirken können. Synaptic löscht jedoch nur die systemweite Konfiguration. Konfigurationsdateien in den Benutzerverzeichnissen unter „/home“ müssen Sie manuell entfernen.

6. Softwarepakete im Terminalfenster verwalten

Bei der SSH-Fernwartung eines Servers im Netzwerk sind Sie auf Kommandozeilentools angewiesen. Diese leisten aber auch auf einem Arbeitsrechner gute Dienste, weil Installationen über die Kommandozeile schneller und bequemer ablaufen als über die Tools für die grafische Oberfläche. Meist werden Sie unter Ubuntu, Linux Mint oder Debian das Tool apt einsetzen. Starten Sie es in einem Terminalfenster ohne weitere Optionen, um einen kurzen Hilfetext zu erhalten. Für die Installation einer Software verwenden Sie

```
sudo apt update
sudo apt install [Paketname]
```

Die erste Zeile aktualisiert die Paketdatenbank, die zweite installiert das im Platzhalter „[Paketname]“ angegebene Paket. Sie können auch mehrere Paketnamen hintereinander verwenden – durch schlichtes Leerzeichen getrennt. Für die Deinstallation verwenden Sie

```
sudo apt remove [Paketname]
```

Auch hier sollten Sie vorsichtig sein, wenn apt mehr als ein Paket entfernen möchte. apt gibt jedoch eine deutliche Warnung aus, wenn Sie versuchen, systemrelevante Pakete zu entfernen. Wenn bei der Deinstallation unnötige Pakete zurückbleiben, gibt apt eine Liste unter „Die folgenden Pakete wurden automatisch installiert und

```
te@ub180407: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
te@ub180407:~$ apt
apt 1.6.11 (amd64)
Aufruf: apt [Optionen] befehl

apt ist ein Paketmanager für die Befehlszeile und bietet Befehle für die Suche und Verwaltung von Paketen sowie für die Abfrage von Informationen zu diesen Paketen.
Es stellt die gleiche Funktionalität zur Verfügung wie die spezialisierten APT-Werkzeuge apt-get und apt-cache, aber seine Optionen sind eher passend für die interaktive Nutzung.

Meist verwendete Befehle:
list - Pakete basierend auf dem Paketnamen auflisten
search - Paketbeschreibungen durchsuchen
show - Paketdetails anzeigen
install - Pakete installieren
remove - Pakete entfernen
autoremove - alle nicht mehr verwendeten Pakete automatisch entfernen
update - Liste verfügbarer Pakete aktualisieren
```

Schnelle Paketverwaltung: apt ist im Terminal einfach zu verwenden und bietet den meisten Komfort, wenn Sie mehrere Programme auf einmal einrichten wollen (apt install [Paketnamen]).

werden nicht mehr benötigt.“ aus. Diese Pakete lassen sich mit

```
sudo apt autoremove
```

entfernen. Diesen Befehl sollten Sie in regelmäßigen Abständen verwenden, besonders nach mehreren Kernel-Updates. Wenn der aktuelle Kernel stabil läuft, entfernen Sie damit alte Kernel-Pakete, was Platz auf der Festplatte einspart. Mit dem Befehl `apt list [Suchmuster]` können Sie nach Softwarepaketen suchen. Verwenden Sie für den Platzhalter „[Suchmuster]“ beispielsweise `*gimp*`. apt gibt dann alle Paketnamen aus, in denen „gimp“ an beliebiger Stelle vorkommt. Entsprechendes leistet

```
apt search [Suchmuster]
```

für die Suche in den Paketbeschreibungen. Das Kommandozeilentool apt-get bietet alle für apt beschriebenen Funktionen und noch ein paar mehr. Es gibt beispielsweise „purge“ für die vollständige Entfernung von

Paketen und „download“, wenn Sie ein „deb“-Paket vorerst nicht installieren, sondern nur herunterladen wollen. Ebenfalls nützlich ist dieser apt-Befehl:

```
sudo apt-get clean
```

Dies löscht den Paketcache und räumt damit Festplattenplatz frei.

Wer eine Paketverwaltung mit Menüsteuerung im Terminal bevorzugt, kann aptitude installieren. Das Menü rufen Sie per Strg-T auf. Alternativ verwenden Sie Tastaturkürzel, die aptitude bei den einzelnen Menüpunkten anzeigt. Drücken Sie die Taste „/“, um nach Paketen zu suchen, und die Taste „N“ für „Weitersuchen“. Mit der Plus-Taste („+“) markieren Sie ein Paket für die Installation, dann drücken Sie die Taste „G“ für eine Vorschau der Änderungen und noch einmal die Taste „G“, um die Installation durchzuführen. Über die Minus-Taste („-“) lassen sich Pakete für die Deinstallation auswählen. ■

```
te@ub180407: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
Aktionen Rückgängig Paket Auflöser Suchen Optionen Ansichten Hilfe
C-T: Menü ?: Hilfe q: Beenden u: Update g: Vorschau/Herunterladen/Inse
aptitude 0.8.10 @ ub180407 Datenträger: -17
--\ graphics Anzeigen und Bearbeiten von Bildern und Grafiken (16)
--- main Die Debian-Distribution (13)
--\ universe Unsupported Free Software. (3)
i gimp 2.8.22-1 2.8.22-1
i A gimp-data 2.8.22-1 2.8.22-1
i A graphviz 2.40.1-2 2.40.1-2
-- httpd Webservers and their modules (3)
-- interpreters Interpretersprachen (5)
GNU Image Manipulation Program
GIMP ist ein hochentwickelter Bildeditor. Sie können ihn verwenden, um #
Fotos und Scans zu bearbeiten, zu verbessern und zu retuschieren sowie
```

Alternative fürs Terminal: aptitude ist nicht besonders übersichtlich, bietet aber im Terminal eine menügeführte Paketverwaltung mit Programinfos und eine Suchfunktion.

Container statt Pakete

Wer neuere Programmversionen nutzen oder ausprobieren möchte, verwendet Software im Container. Seit Version 16.04 ist Ubuntu dafür standardmäßig vorbereitet. Linux Mint bevorzugt das Flatpak-Format.

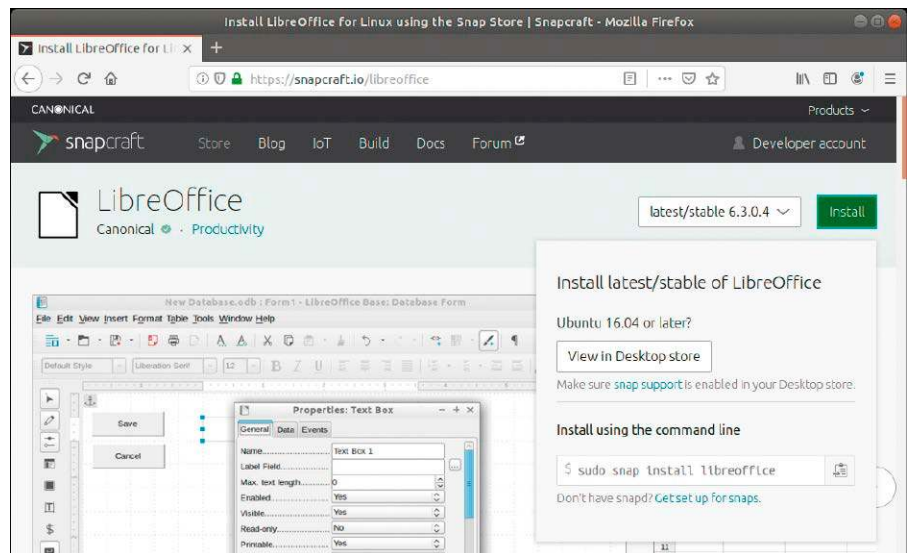
VON THORSTEN EGGELING

Linux-Programme laufen nur unter genau der Distribution problemlos, für die sie erstellt wurden. Das schränkt die Verbreitung aktueller Programmversionen stark ein und fortlaufende Anpassungen für andere Distributionen sowie Systemversionen erhöhen den Entwicklungsaufwand erheblich. Software lässt sich aber auch zusammen mit allen nötigen Komponenten in einen eigenständigen Container packen. Programme in Containern arbeiten weitestgehend unabhängig vom installierten Betriebssystem und können andere Anwendungen nicht beeinträchtigen. Es gibt aber auch Nachteile bei der Verwendung von Containerformaten.

Programme für alle Linux-Distributionen

Softwarecontainer enthalten neben dem eigentlichen Programm auch alle nötigen Bestandteile des Betriebssystems sowie Bibliotheken. Im Idealfall läuft eine Anwendung im Container unter jedem Linux-System. Auf diesem Weg können Sie neuere Versionen verwenden, auch parallel zu einem herkömmlich als „deb“-Paket installierten Programm.

Ubuntu setzt seit Version 16.04 das von Canonical entwickelte Format Snap-Apps (kurz: Snaps) ein. Seit Ubuntu 18.04 sind bereits einige Snap-Apps vorinstalliert, beispielsweise die Systemüberwachung und der Taschenrechner. Als Nutzer merken Sie davon nichts, außer dass die Programme eventuell etwas langsamer starten als gewöhnlich. Zentrale Anlaufstelle für die Suche nach Snap-Apps ist <https://snapcraft.io/store>. Hier finden Sie auch Informationen zur Installation der Snap-Software für alle unterstützten Distributionen, wenn diese auf Ihrem System noch nicht vorhanden ist.



Snap-Apps suchen: Über <https://snapcraft.io/store> finden Sie Programme schnell und bequem. Ein Klick auf „View in Desktop store“ führt direkt zur Installation über Ubuntu-Software.

So funktionieren Snap-Apps

Lassen Sie sich in einem Terminalfenster mit dem Befehl

```
mount
```

die eingehängten Dateisysteme anzeigen. Sie sehen unter Ubuntu 18.04 etliche eingehängte Squashfs-Container, beispielsweise „/var/lib/snapd/snaps/gnome-calculator_406.snap“. Snap-Apps sind Image-Dateien mit der Dateinamenserweiterung „.snap“, die im Ordner „/var/lib/snapd/snaps“ liegen und in das Dateisystem unterhalb des Ordners „/snap“ eingehängt sind. Bei Squashfs-Containern handelt es sich um ein komprimiertes und schreibgeschütztes Format. Jeder Container enthält einen Verzeichnisbaum, in dem alle Dateien liegen, die ein Programm benötigt.

Alle Snap-Apps nutzen gemeinsam die Basissysteme Ubuntu Core und Base mit minimaler Ausstattung, die unter „/snap/core“ beziehungsweise „/snap/core18“ eingehängt sind. Laufzeitumgebungen wie

Perl oder Java muss der Snap-Container selbst mitbringen. Es ist daher deutlich mehr Platz auf der Festplatte erforderlich als bei „deb“-Paketen – der Speicherbedarf steigt und die Programme starten langsamer. Angesichts großer Festplatten und schneller CPUs ist das auf aktuellen PCs jedoch zu tolerieren.

Snap-Apps in Ubuntu installieren

Nutzen Sie die Suchfunktion in Ubuntu-Software oder stöbern Sie in den Kategorien, um das gewünschte Programm zu finden. Wenn Sie beispielsweise nach dem Mediaplayer VLC suchen, taucht dieser im Ergebnis zweimal auf. Unter „Details“ sehen Sie, um welche Version es sich handelt. Steht hinter „Quelle“ die Angabe „Snap-Store“, handelt es sich um eine Snap-App. Hinter „Kanal“ klicken Sie auf „stable“. Es öffnet sich ein Fenster, in dem Sie zwischen den Kanälen umschalten können. Bei „beta“ oder „edge“ finden Sie

meist höhere Versionsnummern. Die Software ist aber nicht ausreichend getestet und kann Fehler enthalten.

Klicken Sie beim gewünschten Programm auf „Installieren“ und danach auf „Starten“. Später verwenden Sie für den Programmstart eine Suche über die „Aktivitäten“. Sind unterschiedliche Versionen eines Programms installiert, beispielsweise VLC sowohl als „deb“-Paket als auch als Snap-Container, dann wird es unübersichtlich. Die Suche liefert für VLC zwei Ergebnisse, Beschriftung und Icon unterscheiden sich jedoch nicht. Hier hilft nur ausprobieren, welche Version sich hinter welchem Icon verbirgt.

Alternative: Suchen Sie ein Programm über <https://snapcraft.io/store>. Wählen Sie rechts oben im Fenster die gewünschte Version, klicken Sie auf „Install“, auf „View in Desktop store“ und dann auf „Link öffnen“. Installieren Sie die App in Ubuntu-Software wie oben beschrieben.

Snap-Apps verwalten

Ubuntu prüft viermal täglich, ob Updates für Snap-Apps verfügbar sind. Die Installation erfolgt automatisch. Im Terminalfenster lässt sich das Update auch folgendermaßen manuell einleiten:

```
sudo snap refresh
Mit dem weiteren Befehl
snap list --all
```

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

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

Um etwa eine ältere Revision 260 von gnome-calculator (Taschenrechner) zu löschen, nutzen Sie diesen Befehl:

```
snap remove --revision 260 gnome-calculator
```

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

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

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

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

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

Mit Hilfe des Tools snap können Sie auch nach Apps suchen (mit `snap find` [Suchbe-

Mehrere Versionen: Über Ubuntu-Software können Sie auch Beta- oder Vorabversionen von Snap-Apps installieren. Sollten diese nicht gut funktionieren, kehren Sie zum Kanal „stable“ zurück.

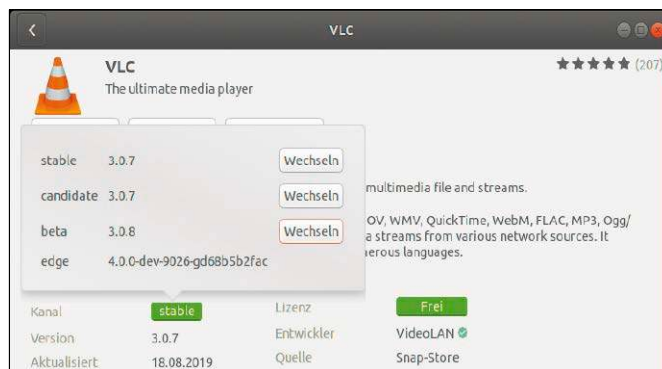
Snap-Apps dürfen nicht alles. In Ubuntu-Software legen Sie bei der jeweiligen App nach einem Klick auf „Berechtigungen“ fest, was erlaubt ist und was nicht.

griff)) und diese installieren (`snap install [snap-app]`).

Zugriffsrechte für Snap-Apps festlegen

Aus Sicherheitsgründen haben Snap-Apps nur Zugriff auf das Home-Verzeichnis. Das führt zu Irritationen, wenn Linux den Zu-

griff beispielsweise auf einen Wechseldatenträger verweigert. Deshalb sollten Sie direkt nach der Installation über Ubuntu-Software auf „Berechtigungen“ klicken. Aktivieren Sie „Lese/Schreibe Dateien auf mobilen Datenträgern“, wenn die App auf USB-Geräte zugreifen soll, die unter „/media“ eingehängt sind. ■



WEITERE CONTAINERFORMATE NUTZEN

Nicht alle Programme sind als Snap-App verfügbar. Einige Entwickler bevorzugen Flatpak, wieder andere das Format Appimage. Flatpak-Container funktionieren ähnlich wie Snaps. Bei Linux Mint 19 ist Flatpak bereits vorinstalliert, Ubuntu-Nutzer installieren die Software mit

```
sudo apt install flatpak
```

Flatpak-Apps finden Sie über <https://flathub.org/apps>, in Linux Mint auch über die „Anwendungsverwaltung“ in der Kategorie „Flatpak“.

Bei Appimage handelt es sich um portable Apps für Linux. Zusätzliche Software für die Verwaltung ist nicht erforderlich. Die heruntergeladene Datei enthält alles Nötige. Programme finden Sie beispielsweise über <https://appimage.github.io/apps>.

Nach dem Download machen Sie die Datei ausführbar („Eigenschaften → Zugriffsrechte“ im Dateimanager). Das Programm lässt sich dann per Doppelklick starten. Ein weiteres Containerformat ist Docker (www.docker.com). Es wird hauptsächlich für Serveranwendungen ohne grafische Oberfläche eingesetzt. Informationen zu den verfügbaren Programmen und Installationsanleitungen finden Sie unter <https://hub.docker.com>.

Zusätzliche Paketquellen verwenden

Die Standard-Paketquellen von Ubuntu stellen die wichtigsten Programme bereit. Sollten Sie hier etwas nicht finden, binden Sie weitere Paketquellen ein oder Sie installieren Pakete manuell.

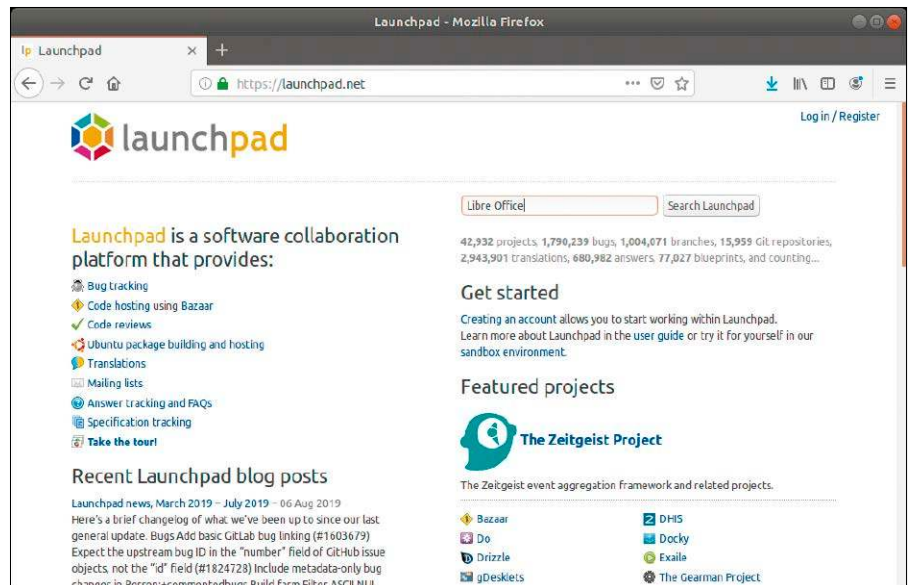
VON THORSTEN EGGELING

Die Softwareinstallation über die Ubuntu-Paketverwaltung aus den Standardrepositorien ist der bequemste und sicherste Weg. Manchmal fehlt jedoch das gewünschte Programm oder es gibt nur eine veraltete Version. Sie sind jedoch nicht auf das angewiesen, was der Distributor bereitstellt. Für neue Software lassen sich weitere Paketquellen konfigurieren oder deb-Pakete manuell installieren.

Service: Eine Textdatei mit allen Befehlszeilen aus diesem Artikel laden Sie über <http://www.pcwelt.de/mQYUqt> herunter.

Zusätzliche Paketquellen einbinden

Sie können jede Paketquelle einbinden, die ein Repository im Ubuntu/Debian-Format betreibt und für Ihre Systemversion passende Software bereitstellt. Beim Update der Paketdatenbank prüft die Paketverwaltung die Gültigkeit der GPG-Schlüssel von Paketquellen und Paketlisten. In den Paketlisten sind Hash-Werte der „deb“-Pakete hinterlegt, die ebenfalls berücksichtigt werden. Sollte der GPG-Schlüssel einer Softwarequelle nicht vorhanden oder ungültig sein, lässt sich die Paketquelle nicht ver-



Neue Softwarepakete: Was Sie in den Ubuntu-Paketquellen nicht finden, gibt es wahrscheinlich bei Launchpad. Binden Sie für Installation und Updates die gewünschte Paketquelle ein.

wenden und die darüber angebotene Software nicht installieren.

Am einfachsten ist die Installation von Fremdpaketen über ein Launchpad-PPA (Personal Package Archive). Die Website <https://launchpad.net> wird vom Ubuntu-Distributor Canonical betrieben und ist die bevorzugte Plattform für Entwickler, die Softwarepakete für Ubuntu und verwandte Distributionen bereitstellen möchten. Verwenden Sie die Suchfunktion auf der Startseite, um herauszufinden, ob es ein PPA für die gewünschte Software gibt. Die Suche beispielsweise nach „Libre Office“ und Klick auf den Link „LibreOffice Packaging in Launchpad“ führt zu einer Übersichtsseite. Unter „Personal package archives“ klicken Sie auf „LibreOffice 6.3.x“, wenn Sie die zurzeit aktuellste Version von Libre Office installieren möchten. Unter „Overview of published packages“ öffnen Sie hinter „Published in:“ eine Liste mit den Ubuntu-Versionen, für die Pakete verfügbar sind. Bei diesem PPA ist die älteste

Version „Bionic“ (Ubuntu 18.04). „LibreOffice 6.2.x“ gibt es dagegen auch für Xenial (Ubuntu 16.04). Wenn die Version passt, verwenden Sie im Terminalfenster die Befehlszeile unter „Adding this PPA to your system“, beispielsweise

```
sudo add-apt-repository
```

```
ppa:libreoffice/libreoffice-6-3
```

Bestätigen Sie mit Eingabetaste, dass Sie das PPA verwenden wollen. Es wird dann über die Textdatei „/etc/apt/sources.list.d/libreoffice-ubuntu-libreoffice-6-3-bionic.list“ als neue Paketquelle eingebunden, der zugehörige GPG-Schlüssel ist unter „/etc/apt/trusted.gpg.d“ zu finden. Abweichend von der Ubuntu-Dokumentation aktualisiert add-apt-repository bei Ubuntu 18.04 die Paketdatenbank automatisch. Sollte das bei Ihnen nicht der Fall sein (oder unter einer älteren Ubuntu-Version), dann verwenden Sie diesen Befehl:

```
sudo apt update
```

Da Libre Office wahrscheinlich bereits installiert ist, genügt dann

```
sudo apt upgrade
```

für das Upgrade. Andernfalls verwenden Sie folgende Zeile

```
sudo apt install libreoffice
```

für unser Beispiel.

Paketquellen manuell einbinden

Sollte es kein Launchpad-PPA für die gewünschte Software geben, finden Sie bei Anbietern von Linux-Software oft Adressen für deren eigene Repositorien. Der Ablauf ist immer der gleiche: Zuerst importieren Sie den GPG-Schlüssel und konfigurieren dann die neue Paketquelle.

Wer beispielsweise Google Chrome verwenden möchte (siehe auch den übernächsten Punkt), importiert zunächst den Schlüssel:

```
wget -q -O - https://dl-ssl.google.com/linux/linux_signing_key.pub | sudo apt-key add -
```

Mit folgendem Befehl erzeugen Sie eine Textdatei für die neue Paketquelle:

```
echo deb [arch=amd64] http://dl.google.com/linux/chrome/deb/stable main | sudo tee /etc/apt/sources.list.d/google_chrome.list
```

Danach verwenden Sie

```
sudo apt update
sudo apt install google-chrome-stable
```

für die Installation der Software.

Paketquellen wieder entfernen

Paketquellen, die Sie nicht mehr benötigen, sollten Sie entfernen. Die darüber installierte Software bleibt erhalten und muss manuell deinstalliert werden (`apt remove [Paketname]`). Verwenden Sie diesen Befehl:

```
sudo add-apt-repository -r
ppa: [Launchpad-Nutzername/PPA-Name]
```

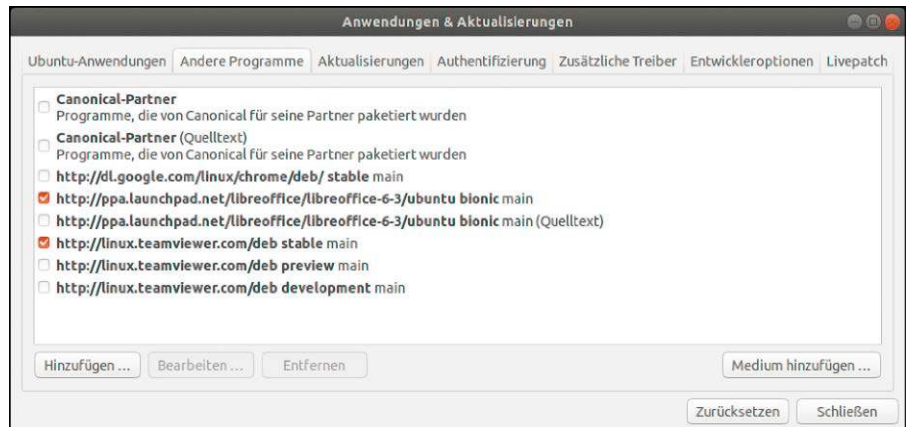
Den Platzhalter ersetzen Sie durch die Angaben, die Sie auch bei der Installation verwendet haben. Sie können auch das grafische Tool „Anwendungen & Aktualisierungen“ nutzen, das Sie über „Aktivitäten“ finden. Gehen Sie dort auf die Registerkarte „Andere Programme“, entfernen Sie das Häkchen vor der Paketquelle und klicken Sie auf „Entfernen“.

Alternativ verwenden Sie das Tool `ppa-purge`, das Sie mit

```
sudo apt install ppa-purge
```

installieren.

Mit dem Befehl



Paketquellen verwalten: Paketquellen lassen sich mit Hilfe von „Anwendungen & Aktualisierungen“ entfernen. Die installierte Software müssen Sie selbst deinstallieren.

```
sudo ppa-purge ppa: [Launchpad-
```

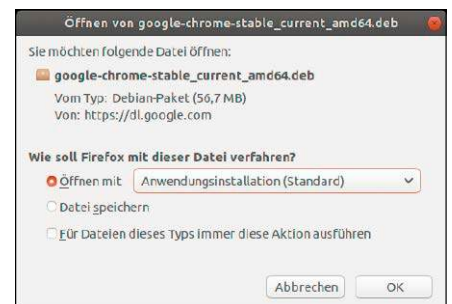
```
Nutzername/PPA-Name]
```

deaktivieren Sie die PPA-Quelle. Sollte eine andere Version der Software in den offiziellen Quellen zu finden sein, wird diese automatisch als Ersatz installiert.

Das ist beispielsweise der Fall, wenn Sie Libre Office über das PPA auf die Version 6.3.x aktualisiert haben wie zuvor beschrieben. `ppa-purge` richtet dann erneut die Vorgängerversion ein. Ist das Paket über die Standard-Paketquellen nicht installierbar, bleibt es erhalten und Sie deinstallieren es manuell.

Heruntergeladene „deb“-Pakete installieren

Ubuntu-Software kann auch Pakete installieren, die Sie aus dem Internet herunterladen. Ein Beispiel ist Google Chrome (www.google.de/chrome). Beim Download über Firefox ist hinter „Öffnen mit“ standardmäßig „Anwendungsinstallation“ eingestellt. Nach einem Klick auf „OK“ öffnet sich Ubuntu-Software und Sie klicken auf „Ins-



Pakete installieren: „deb“-Dateien, die Sie über den Browser herunterladen, öffnen Sie gleich mit Ubuntu-Software („Anwendungsinstallation“) und klicken auf „Installieren“.

tallieren“. Das Chrome-Paket weist eine Besonderheit auf: Es richtet eine neue Paketquelle für den Google-Browser ein und installiert den Google-GPG-Schlüssel. Sie erhalten daher auch regelmäßig Updates für den Browser. Einige „deb“-Pakete aus dem Internet bieten diesen Komfort eventuell nicht. Für ein Update installieren Sie dann – wenn verfügbar – eine neue Version des „deb“-Pakets. ■

FREMPAKETE KÖNNEN DAS SYSTEM GEFÄHRDEN

Grundsätzlich ist jede Softwareinstallation immer Vertrauenssache. Die GPG-Schlüssel dürfen nicht kompromittiert und die Downloadserver müssen sicher sein. Bei den offiziellen Ubuntu-Servern können Sie von professioneller Wartung und umfangreichen Sicherungsmaßnahmen ausgehen. Launchpad (<https://launchpad.net>) wird zwar ebenfalls von Ubuntu-Distributor Canonical betrieben, Software kann hier jedoch jeder einstellen. Die Wahrscheinlichkeit, dass Schadsoftware frühzeitig entdeckt und gemeldet wird, ist aber sehr hoch. Launchpad darf daher als ausreichend sicher gelten. „deb“-Dateien aus dem Internet sollten Sie nur vertrauen, wenn diese von bekannten Anbietern stammen. Alles andere ist als unsicher anzusehen und das Risiko bei der Installation müssen Sie selbst verantworten.

Programme für Umsteiger

Wer unter Windows Firefox und Libre Office nutzt, muss sich beim Wechsel auf Linux kaum umgewöhnen. Trotzdem ist einiges anders und nicht für jede bisher genutzte Anwendung gibt es eine gleichwertige Alternative.

VON THORSTEN EGGELING

Wie gut der Umstieg von Windows auf Linux gelingen kann, hängt auch von der bisher genutzten Software ab. Das Spektrum beginnt beim gelegentlichen PC-Nutzer, der hauptsächlich den Browser und ab und zu eine Bildbearbeitung für die Urlaubsfotos verwendet. Auf dem typischen Büro-PC wird ausgiebig von Textverarbeitung und Tabellenkalkulation Gebrauch gemacht, hinzu kommen eventuell noch Buchhaltungsprogramme oder Software für die Steuererklärung. Der Poweruser bearbeitet Bilder mit Adobe Photoshop, schneidet Videos mit Adobe Premiere und installiert Unmengen von Software, die sich für Windows aus dem Internet herunterladen lässt.

Windows hat für alle genannten Nutzergruppen etwas Passendes zu bieten, Linux nur teilweise. Außerdem sind die Zielgruppen andere. Linux eignet sich eher für Personen, die auch ohne spezielle Software auskommen, die bereit sind, sich umzugewöhnen, oder die sich einfach gerne mit Linux beschäftigen möchten. Auf der anderen Seite stehen Benutzer, die Serverdienste (SSH, Apache, Samba) benötigen, und die dann bei Linux besser aufgehoben sind als bei Windows.



Schlüsselfertiges Betriebssystem: Linux-Distributionen richten die wichtigsten Anwendungen bereits bei der Erstinstallation ein. Textverarbeitung und Bildverwaltung sind schon dabei.

Wer unter Windows vor allem Open-Source-Software einsetzt, sollte auch mit Linux keine Probleme haben. Die unterschiedlichen Softwareangebote für Linux und Windows sind ansonsten nur schwer vergleichbar. Am einfachsten ist es, die Linux-Anwendungen einfach auszuprobieren und sich dann zu entscheiden.

1. Programme für alle Benutzer

Linux-Distributionen wie Ubuntu oder Linux Mint bieten direkt nach der Installation die wichtigsten Anwendungen für die meisten Benutzer. Als Office-Paket ist Libre Office vorhanden (siehe Punkt 2), Firefox ist der Standard-Webbrowser und für E-Mail gibt es Thunderbird.

Umsteiger von Windows auf Ubuntu 18.04 haben unter Umständen Probleme, die installierten Anwendungen überhaupt zu finden. Die Starterleiste am linken Bildschirmrand zeigt nur Icons beispielsweise für Firefox, Libre Office Writer, Rhythmbox und den Dateimanager. Ein Klick auf „Aktivitäten“ ermöglicht die Suche nach Anwen-

dungen und Tools, deren Namen man kennt. Das unscheinbare Symbol in der Starterleiste ganz unten hilft weiter. Nach einem Klick darauf zeigt Ubuntu die Icons der häufig genutzten Programme und nach einem Klick auf „Alle“ jede installierte Anwendung für die grafische Oberfläche. Es lassen sich dann beispielsweise die Tabellenkalkulation Libre Office Calc, die Fotoverwaltung und Fotobearbeitung Shotwell (siehe Punkt 3) oder der Player Videos starten. Ist ein Programm aktiv, sehen Sie sein Icon in der Starterleiste. Nach einem rechten Mausklick erscheint ein Menü, in dem Sie auf „Zu Favoriten hinzufügen“ gehen können. Das Programmsymbol bleibt dann in der Leiste und die Anwendung lässt sich darüber später schneller starten. Linux Mint 19 bietet eine ähnliche Ausstattung. Das Startmenü erinnert an Windows 7 und führt Umsteiger wie gewohnt zu den gewünschten Programmen. Firefox, Thunderbird und Libre Office sind vorinstalliert. Unter „Zubehör“ finden Sie Taschenrechner, Screenshottool und Textbearbeitung.

2. Programme für den Büro-PC

Libre Office bietet einen großen Funktionsumfang, der für die meisten privaten Anwender ausreicht. Die Suite enthält die Textverarbeitung Writer, die Tabellenkalkulation Calc, das Präsentationsprogramm Impress und das Zeichenprogramm Draw. Das Datenbankmodul Base lässt sich über die Paketverwaltung nachinstallieren.

Die Bedienung über Menüs und der Funktionsumfang erinnern an Microsoft Office 2003. Microsoft Office 365 sieht im Vergleich moderner aus, auch wenn die Bedienung über das Menüband nicht nach jedermanns Geschmack ist. Komfortfunktionen wie „Designs“ mit Livevorschau im aktuellen Dokument gibt es beispielsweise in Libre Office Writer nicht und der Tabellenkalkulation fehlen etliche Rechenoptionen von Excel.

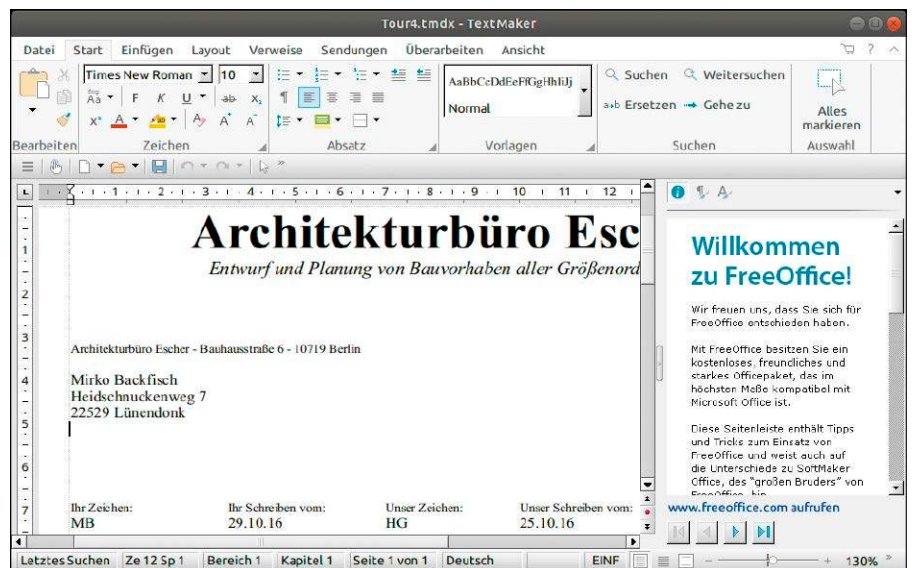
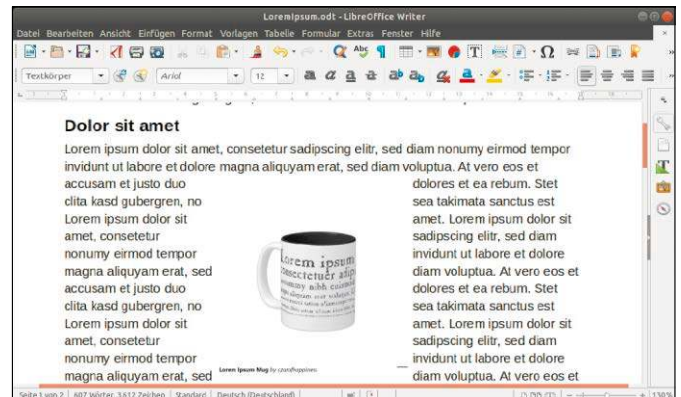
Wer gelegentlich einen Brief schreibt oder Finanzberechnungen macht, wird in Libre Office kaum etwas vermissen. Probleme sind zu erwarten, wenn Sie häufig Dokumente mit Nutzern von Microsoft Office austauschen müssen. Die Import- und Exportfilter werden zwar ständig verbessert, die Übernahme aller Formatierungen ist vor allem bei komplexeren Dokumenten jedoch nicht garantiert.

Mehr Kompatibilität zu Microsoft-Produkten verspricht Softmaker Office (www.softmaker.de). Die Importfilter sind besser als jene von Libre Office, wenn auch nicht perfekt. 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 2016, das mit dem Duden Korrektor eine besonders leistungsfähige Rechtschreibprüfung enthält.

Außerdem können Sie die Gratisversion Free Office nutzen, die aber keine Microsoft-XML-Formate speichern kann (www.freeoffice.com). Die Speicherformate „.doc“ und „.xls“ stehen jedoch für den Datenaustausch zur Verfügung.

Wer Broschüren oder Zeitschriften layouten möchten, greift unter Windows zu Adobe InDesign oder Quark Xpress. Vergleichbare Desktop-Publishing-Programme gibt es für Linux nicht. Für den Hobbylayouter genügt aber Scribus (www.scribus.net), das sich über die Paketverwaltung installieren lässt. Das Programm beherrscht den professionellen Textsatz und kann Dokumente

Office-Paket: Libre Office Writer kann zwar nicht ganz mit Microsoft Word mithalten, bietet aber für die meisten privaten Nutzer ausreichende Funktionen.



Textmaker: Softmaker Office gibt es auch in einer kostenlosen Version. Leistungsfähige Importfilter für die Microsoft-XML-Formate bietet aber nur die Bezahlversion des Programms.

so für den Druck vorbereiten, dass auch die Farben stimmen (CMYK-Farbseparation).

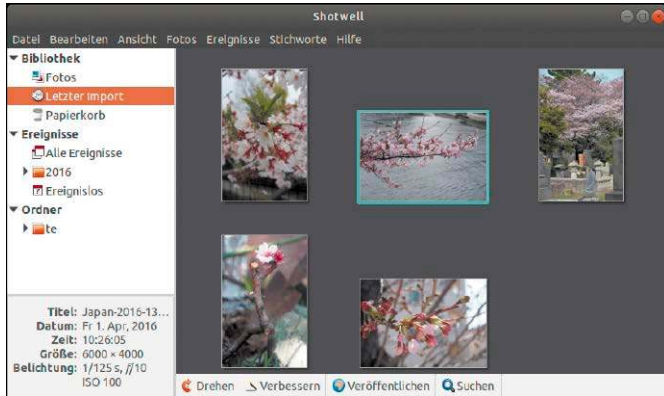
3. Fotoverwaltung und Bildbearbeitung

Das bei Ubuntu standardmäßig installierte Shotwell ist eine einfache Fotoverwaltung.

Bilder lassen sich mit Stichwörtern versehen und bewerten, was die Basis für die schnelle Anzeige von Bildern aus der gleichen Kategorie und für Ansichtsfiler bildet. Shotwell bietet einfache Bearbeitungsfunktionen wie „Zuschneiden“ oder „Rote-Augen-Effekt“.

WINDOWS-PROGRAMME UNTER LINUX NUTZEN

Wer spezielle Windows-Programme benötigt, kann eine Windows-Installation im Dualboot neben Linux auf dem gleichen PC verwenden. Eine bessere Lösung bietet jedoch Virtualisierungssoftware wie Virtualbox. Windows-Programme stehen damit jederzeit zur Verfügung, ohne dass Sie den PC neu starten müssen. Der Nachteil: Auch für ein virtualisiertes Windows benötigen Sie einen Lizenzschlüssel von Microsoft. Wer Windows nur gelegentlich startet, verwendet die Enterprise-Version von Windows 10 kostenlos für einen 90-Tage-Test (www.pcwelt.de/k2mNT9). Welche Voraussetzungen Ihr PC erfüllen muss, wie Sie die aktuelle Virtualbox-Version unter Linux installieren und Windows 10 darin einrichten, lesen Sie unter www.pcwelt.de/2111217.



Mit Digikam lassen sich Fotos (www.digikam.org) nach Alben, Tags oder Stichwörtern sortieren beziehungsweise kategorisieren. Es stehen zahlreiche Tools für die Fotobearbeitung zur Verfügung, etwa Tonwertkorrektur, Rote-Augen-Korrektur oder Rahmenbearbeitung. Auch eine Unterstützung von Fotos in RAW-Formaten ist vorhanden: Digikam kann nicht nur die eingebettete Vorschau anzeigen, sondern RAW-Dateien in der Vorschau öffnen. Wer Fotos im RAW-Format bearbeiten möchte, greift zu Darktable oder Rawtherapee. Alle genannten Programme lassen sich über die Paketverwaltung installieren.

Die Zielgruppe von Gimp (www.gimp.org) sind Benutzer, die unter Windows Photoshop einsetzen. Das Programm bietet Malwerkzeuge, Ebenen, Masken, Automatikverbesserung und etliche Filter. Sie können damit Fotos retuschieren, Bilder freistellen oder verfremden. Wie bei Photoshop erschließen sich die meisten Funktionen nicht auf Anhieb. Bestimmte Effekte sind nur durch eine geeignete Kombination von Masken und Ebenen zu erreichen.

Da Gimp jedoch weit verbreitet ist und viel genutzt wird, finden Sie im Internet ausreichend Unterstützung.

Ein guter Startpunkt ist die Dokumentation unter www.gimp.org/docs. Gimp ist in den Standard-Repositories von Ubuntu und Linux Mint enthalten. Neuere Versionen lassen sich unter Ubuntu als Snap-App installieren (siehe Artikel ab Seite 46).

4. Player für Audio & Video

Bei Ubuntu heißt der Videoplayer „Videos“ (Totem Video Player), bei Linux Mint „Medienwiedergabe“ (Xplayer). Den Programmen ist gemeinsam, dass sie das Multimedia-Framework Gstreamer benutzen. Gstreamer stellt eine Infrastruktur zur Verfügung, über die sich Audio- und Videodateien abspielen beziehungsweise codieren und decodieren lassen.

Anwender müssen sich um die Details in der Regel nicht kümmern. Sobald Sie eine Multimedia-Datei über den Dateimanager öffnen, startet der passende Player. Wenn Ubuntu oder Linux Mint das Dateiformat bisher unbekannt ist, fordert der Player die

Fotos verwalten: Shotwell bietet ausreichende Funktionen für die Organisation von Urlaubsbildern. Mit Tools wie „Drehen“ oder „Anpassen“ lassen sich die Fotos auch bearbeiten.

Installation der nötigen Gstreamer-Module (Codecs) automatisch an.

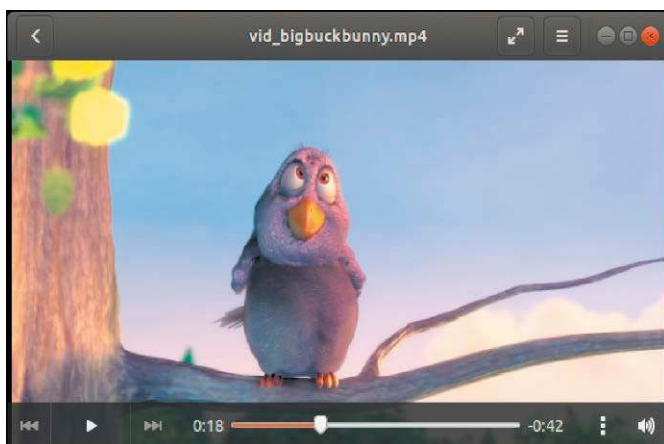
Wenn Ihnen diese Standardplayer nicht gefallen oder der Funktionsumfang nicht ausreicht, installieren Sie den verbreiteten VLC Media Player (www.videolan.org). Das Programm bringt eigene Codecs mit und spielt alle gängigen Medienformate ab. Eine weitere Alternative ist Smplyer (<http://smplyer.sourceforge.net>). Dieses grafische Front-End für Mplayer hält den gesamten Funktionsumfang von Mplayer bereit. Wichtige Audio- und Videocodecs hat Smplyer ebenfalls bereits mit an Bord. Beide Programme sind in den Standard-Repositories von Ubuntu und Linux Mint zu finden.

5. Videoeditoren für Linux

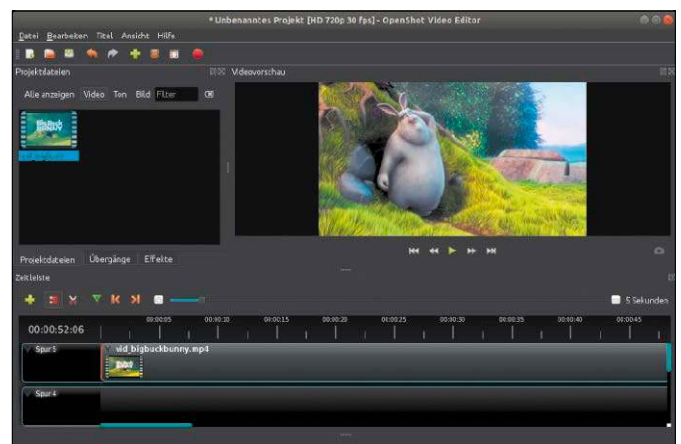
OpenShot ist ein funktionsreicher und trotzdem für Einsteiger verständlicher Videoeditor (www.openshot.org). Sie importieren das ungeschnittene Rohmaterial zunächst in eine Projektdatei. Aus der Liste der Projektelemente ziehen Sie dann die einzelnen Bestandteile auf die Zeitleiste. Das Schneiden und Trimmen ist intuitiv gelöst. Sie zerteilen einen Clip und können dann nach Rechtsklick auf den jeweiligen Teil über das Kontextmenü den Abschnitt löschen oder verschieben.

Neben den Schnittfunktionen stehen eine Reihe von Übergängen zur Verfügung. Sie wählen den gewünschten Effekt aus der Liste und ziehen ihn auf die entsprechende Spur. Über das Kommando „Datei → Video exportieren“ und die Auswahl eines Profils geben Sie die geschnittene Fassung in eine neue Datei aus.

Weitere Videoeditoren für Linux sind Pitivi und Kdenlive. Pitivi (www.pitivi.org) ähnelt in



Filme ansehen: Die Standardplayer von Ubuntu und Linux Mint bieten nur Basisfunktionen. Wer mehr will, greift zum VLC Media Player oder Smplyer.



Videos bearbeiten: OpenShot schneidet Videos. Es gibt mehrere Spuren und Sie können Videotitel und Übergänge erzeugen sowie Effekte einbauen.

Bedienung und Funktionsumfang OpenShot. Kdenlive (<https://kdenlive.org>) bietet mehr Funktionen, benötigt dafür aber auch mehr Einarbeitungszeit.

Alle genannten Programme lassen sich über die Paketverwaltung in Ubuntu und Linux Mint installieren. Auf den Seiten der Hersteller gibt es auch neuere Versionen – in der Regel als AppImage, Snap-App oder Flatpak (siehe Artikel ab Seite 46). Wer Videos nur in andere Formate umwandeln möchte, verwendet dafür Handbrake oder Avidemux. Ausführliche Infos dazu finden Sie ab Seite 68.

6. Software für das Internet

Firefox ist einer der beliebtesten Browser und glänzt vor allem durch seine Erweiterbarkeit über Add-ons. Das Programm geht jedoch nicht besonders sparsam mit dem Hauptspeicher um, was vor allem bei vielen geöffneten Tabs das System ausbremsen kann. Der Browser schneidet bei Geschwindigkeitstests gut ab, aber andere können es noch besser – beispielsweise Chromium (www.chromium.org), der Open-Source-Abfolger von Google Chrome. Der Ressourcenverbrauch ist geringer als bei Firefox, die Geschwindigkeit in einigen Bereichen höher. Die Unterschiede von Chromium im Vergleich zu Google Chrome sind gering.



Schlanker Browser: Wer auf Firefox-Add-ons verzichten kann, findet in Chromium einen schnellen Webbrowser, der sparsamer mit den Systemressourcen umgeht.

Sie betreffen einige Einstellungen, Codecs sowie die Erweiterungen für Adobe Flash und PDF. Chromium ist in den Standard-Paketquellen von Ubuntu und Linux Mint enthalten. Es gibt jedoch auch Gründe, Google Chrome zu installieren (www.google.de/chrome). Einer davon ist das Angebot von Amazon Video, das HTML5-Videos nur in Google Chrome, aber nicht in Chromium anzeigt. Google bietet ein eigenes Repository für Ubuntu-Systeme an (siehe Artikel ab Seite 48).

Wer gerne per Chat kommuniziert oder ein bewegtes Bild des Gegenüber sehen will, kann auch unter Linux Skype installieren. Aktuelle „deb“- und RPM-Pakete sowie eine Snap-App gibt es bei Microsoft zum kostenlosen Download (www.pcwelt.de/P3BHbX). Wenn Sie Open-Source-Software bevorzugen, installieren Sie die Messenger Pidgin oder KDE-Telepathy. Beide unterstützen Netzwerkprotokolle wie ICQ, MSN, Jabber und Google Talk und lassen sich direkt über die Paketverwaltung installieren. ■

SOFTWARE AUS DEM QUELLTEXT KOMPILIEREN

Ein Kompilat aus dem Quelltext ist nur erforderlich, wenn es kein PPA oder eine andere Downloadquelle für die gewünschte Software gibt.

Dank App-Image, Snap-Apps und Flatpak ist das inzwischen nur noch selten erforderlich. Ein eigener Build kann jedoch weiterhin aus Sicherheitsgründen wünschenswert sein. Nur so stellen Sie sicher, dass eine Software tatsächlich dem Quelltext entspricht und nicht manipuliert wurde.

Sie benötigen keine Programmierkenntnisse, aber den souveränen Umgang mit der Kommandozeile und unter Umständen ausreichende Englischkenntnisse für die Lektüre der Dokumentation.

Ein allgemeines Rezept für die Erzeugung von Binärdateien aus dem Quellcode gibt es nicht, unser Beispiel für Ubuntu 18.04 zeigt jedoch einige grundsätzlichen Schritte.

Wer die Verschlüsselungssoftware VeraCrypt (www.veracrypt.fr) selbst kompilieren möchte, installiert zuerst die nötigen Entwicklertools

```
sudo apt install git build-essential yasm libfuse-dev
pkg-config libgtk2.0-dev libcxxunit-dev
libwxgtk3.0-dev make
```

Welche Entwicklerpakete („*-dev“) erforderlich sind, ermitteln Sie in der Beschreibung der jeweiligen Software. Danach erstellen Sie ein Arbeitsverzeichnis, laden den Quellcode herunter und starten den Buildvorgang (sechs Zeilen):

```
mkdir ~/src
cd ~/src
wget -q -O - https://github.com/wxWidgets/wxWidgets/releases/download/v3.0.4/wxWidgets-3.0.4.tar.bz2
tar xvjf -
git clone https://github.com/veracrypt/VeraCrypt.git
cd ~/src/VeraCrypt/src/Build
sudo ./build_veracrypt_linux.sh
```

Nach Abschluss des Buildvorgangs liegen die Installerpakete im Ordner „~/src/VeraCrypt/src/Setup/Linux“. Zur Installation starten Sie in diesem Verzeichnis diesen Befehl:

```
sudo ./veracrypt --CustomEFI-setup-gui-x64
```

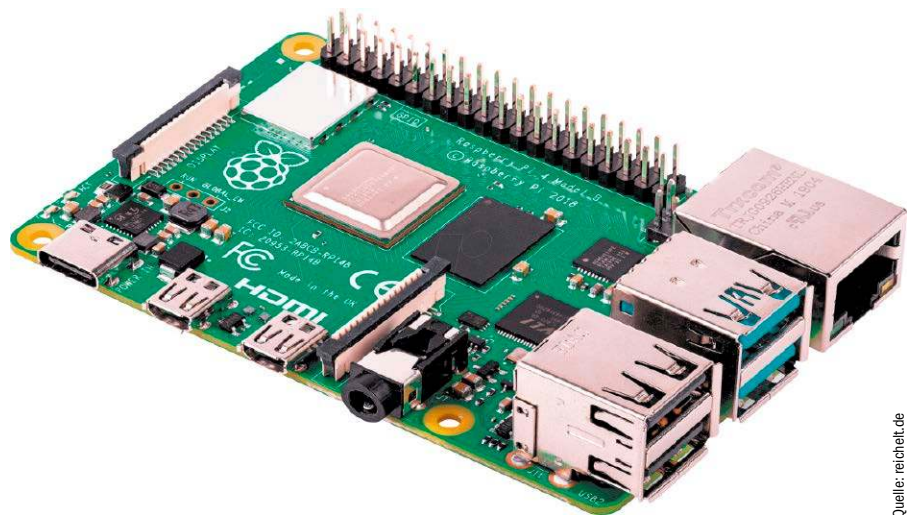
Ganz typisch ist die Vorgehensweise bei VeraCrypt nicht. Die meisten Entwickler bieten kein spezielles Build-Script an. Meist gibt es das Script „configure“, das die Voraussetzungen prüft. Mit `make` wird das Programm kompiliert und danach mit `sudo make install` installiert.

Der neue Raspberry Pi 4

Platinenrechner sind nicht teuer. Trotzdem ist es ein Fehler, jeden Platinen hype mitzumachen. Den Raspberry Pi 4 kann man aber guten Gewissens jedem empfehlen – Neueinsteigern und Freaks, die schon etliche Platinen im Haushalt haben.

VON HERMANN APFELBÖCK

Viele, vielleicht die Mehrzahl der Rollen, die begeisterte Bastler dem Raspberry Pi seit 2012 abverlangten, waren der Leistung der frühen Modelle schlicht nicht angemessen. Es ist ein Unterschied, ob die kleine Platine als Controller für eine Kamera und Wetterstation oder als Daten- und Medienserver arbeiten soll. Letzteres wird eigentlich erst mit dem brandaktuellen Modell 4 überzeugend funktionieren. Der Raspberry Pi 4 hat in allen Belangen aufgerüstet – die Vierkern-CPU dezent von 1,4 auf 1,5 GHz, den Arbeitsspeicher auf Wunsch deutlich bis zu vier GB, den Grafikprozessor zum Typ Videocore VI, USB 3.0 gibt es auf immerhin zwei der vier Ports, ferner echtes Gigabit-Ethernet und zwei Videoports (Micro-HDMI). Im Prinzip hat sich außer dem WLAN-Chip und dem Audio-Output alles verbessert und dies zum Teil signifikant. Weitgehend unverändert sind Maße und Bauweise der Platine sowie der Basispreis



Quelle: reichelt.de

für die kleinste Variante mit einem GB RAM (knapp 40 Euro, die Varianten mit zwei und vier GB RAM circa 50 und 60 Euro). Aufgrund des konstanten Formfaktors und der unveränderten 40-Pin-GPIO-Leiste ist das meiste Platinenzubehör der älteren Raspberry-Modelle weiterhin zu verwenden. Einige Ausnahmen gibt es und diese sind am besten schon beim Kauf zu berücksichtigen.

Die nackte Platine genügt nicht!

Absolut unentbehrliches Zubehör ist das neue Raspberry-Netzteil für acht bis neun Euro. Die Netzteile der älteren Pi-Modelle passen nicht. Das originale, rot-weiße Gehäuse für vier bis fünf Euro ist optional, aus Belüftungsgründen vielleicht nicht einmal optimal (siehe unten), es bietet der Platine aber Staubschutz und gibt ihr ein aufgeräumtes Aussehen. Gehäuse der Vorgänger sind aufgrund der geänderten Videoports und des Stromanschlusses unbrauchbar. Wer mit purer SSH-Fernwartung des Rasp-

berry nicht auskommt oder diesen sogar als Desktop nutzen will, benötigt mindestens einen kleinen Zwischenstecker von Micro-HDMI auf HDMI. Der ist für gut zwei Euro zu haben, allerdings vielleicht nicht die ideale Lösung: Der Pi 4 hat ja zwei solcher Micro-HDMI-Ports direkt nebeneinander. Zwei solcher Zwischenstecker haben aber wegen ihrer Breite keinen Platz. Etwa ab sieben Euro gibt es Direktkabel vom Micro-HDMI-Anschluss des Raspberry zum HDMI-Port des Monitors. Wirklich notwendig werden zwei solcher Kabel aber nur, wenn der Minirechner tatsächlich zwei Monitore versorgen soll.

Für das Betriebssystem brauchen Sie eine Micro-SD-Karte mit mindestens acht GB. Wer den Leistungsschub des neuen Raspberry nicht durch den Flaschenhals einer langsamen Geizhals-Karte verschenken will, wird bei der Standardempfehlung einer „Class-10“-Karte nicht stehenbleiben: Die schnellsten Karten beginnen mit Kapazitätä-



Quelle: reichelt.de

Das originale Netzteil (circa 8,50 Euro): Dieses Zubehör muss sein, da die Netzteile der Vorgänger spannungs- und anschlusstechnisch nicht passen.



Zwischenstecker für Micro-HDMI auf HDMI: Für einen Monitor genügt diese einfache Lösung. Zwei solcher Adapter haben jedoch keinen Platz.



Micro-HDMI auf HDMI: Zwei solcher Kabel benötigen Sie, wenn der Raspberry zwei Monitore versorgen soll.

ten von 32 und 64 GB und tragen den Zusatz „SDXC“ oder „UHS“. Der Preis solcher Karten kann je nach Kapazität dann allerdings den einer Raspberry-Platine erreichen.

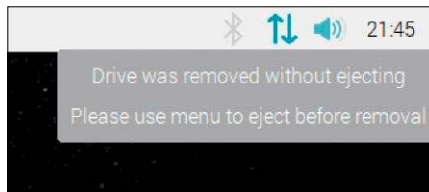
Hinweis: Ein Betriebssystem auf Micro-SD-Karte ist aktuell die einzige Möglichkeit, den Raspberry 4 zu starten. Die Fähigkeit des Vorgängers, von USB oder über das Netzwerk zu booten, bietet das neue Modell (noch) nicht.

Gigabit-Ethernet und USB 3.0

Die Kombination von ungedrosselter Gigabit-Schnittstelle und USB 3.0 lässt vom Raspberry Pi 4 hervorragende Serverleistungen erwarten. Was beim Modell 3 noch durch USB 2.0 auf etwa 30 MB/s gebremst wurde, kann nun theoretisch bis zu einem Durchsatz von 125 MB/s durchrauschen. Realiter werden Sie mit der neuen Platine gute, aber nicht diese Werte erreichen, was aber nicht am Raspberry und seinen Schnittstellen liegt. Netzwerkswitch, Netzwerkprotokoll, Festplattenleistung, Dateigrößen spielen zusammen und bremsen den Idealdurchsatz.



Hübsch aufgeräumt, aber heiß: Das Gehäuse haben wir geöffnet, um den Raspberry um etliche Celsius-Grade abzukühlen.



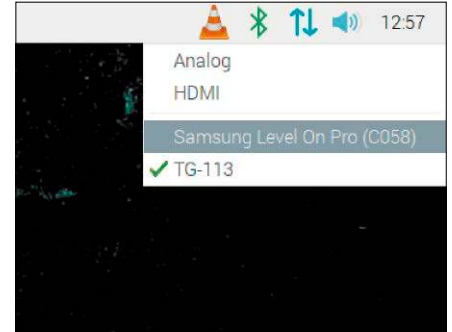
Mehr als eine Festplatte kann der Raspberry Pi 4 nicht mit ausreichend Strom versorgen.

Der von uns getestete Raspberry Pi 4 erreicht im Bestfall knapp 100 MB/s, meistens aber liegt der Durchsatz bei 55 bis 60 MB pro Sekunde. Das ist beim Raspberry nicht anders als bei anderen Gigabit-Schnittstellen in PCs oder alternativen Platinen und absolut alltagstauglich. Wichtig ist beim Serverbetrieb mit dem Raspberry (wie auf allen Platinen), dass die Daten über schnelles USB 3.0 und externe Festplatten laufen. Netzfreigaben auf der Micro-SD-Karte selbst sind kontraproduktiv, weil zu langsam.

Die zwei schnellen (blauen) USB-3.0-Anschlüsse eignen sich für schnelle Festplatten, während die beiden USB-2.0-Ports sich für Maus oder Tastatur anbieten. Allerdings müssen Sie – wie schon bei den Vorgängern – vermeiden, zwei externe USB-Festplatten ohne eigene Stromversorgung über die Raspberry-Ports zu versorgen. Das geht zuverlässig schief: Die Datenträger schalten mangels ausreichender Stromversorgung spontan ab und es drohen Datenverluste. Der Raspberry Pi 4 kann nur eine USB-Festplatte selbst zuverlässig betreiben. Auf der sicheren Seite sind Sie mit einem aktiven USB-Hub, der die Laufwerke mit Strom versorgt.

WLAN und Bluetooth

Für alle serverähnlichen Aufgaben ist verkabeltes Gigabit-Ethernet alternativlos. Doch hat der Raspberry für mobilere Aufgaben schon seit Modell 3 einen WLAN-



Klappt nicht immer, aber immer öfter: Zwei von drei getesteten Bluetooth-Geräten akzeptierte der Raspberry Pi 4 ohne Murren.

Chip (802.11ac für 2,4- und Fünf-GHz-Band), an dem sich beim neuen Modell nichts geändert hat. Dessen Leistung ist nicht überragend, aber alltagstauglich und erreicht bis zu zehn MB/s beim Versenden von Daten, beim Empfang etwa bis zu sechs MB/s. Das ist mehr als genug für das Senden einiger Wetterdaten und reicht auch noch zum ruckelfreien Abspielen durchschnittlicher Filmqualität.

Bluetooth (5.0) ist in Raspbian über das Leistungssymbol unkompliziert zu bedienen. Unabhängig von der Raspberry-Hardware zeigt es aber die unter Linux allgemein bekannten Tücken: Von drei Versuchen waren in unserem Fall immerhin zwei erfolgreich. Der Anschluss eines Sony-Bluetooth-Lautsprechers scheiterte daran, dass der Raspberry das Gerät nicht erkannte und folglich nicht anzeigte.

Ein weiterer No-Name-Lautsprecher sowie ein Samsung-Kopfhörer ließen sich hingegen problemlos verbinden und dann über das Sounddapplet der Systemleiste als Soundgerät nutzen. Im Falle, dass Sie mit einem Gerät Pech haben, ist Bluetooth-Troubleshooting unter Linux eine eher heikle Aufgabe.

Heizkörper mit Himbeere?

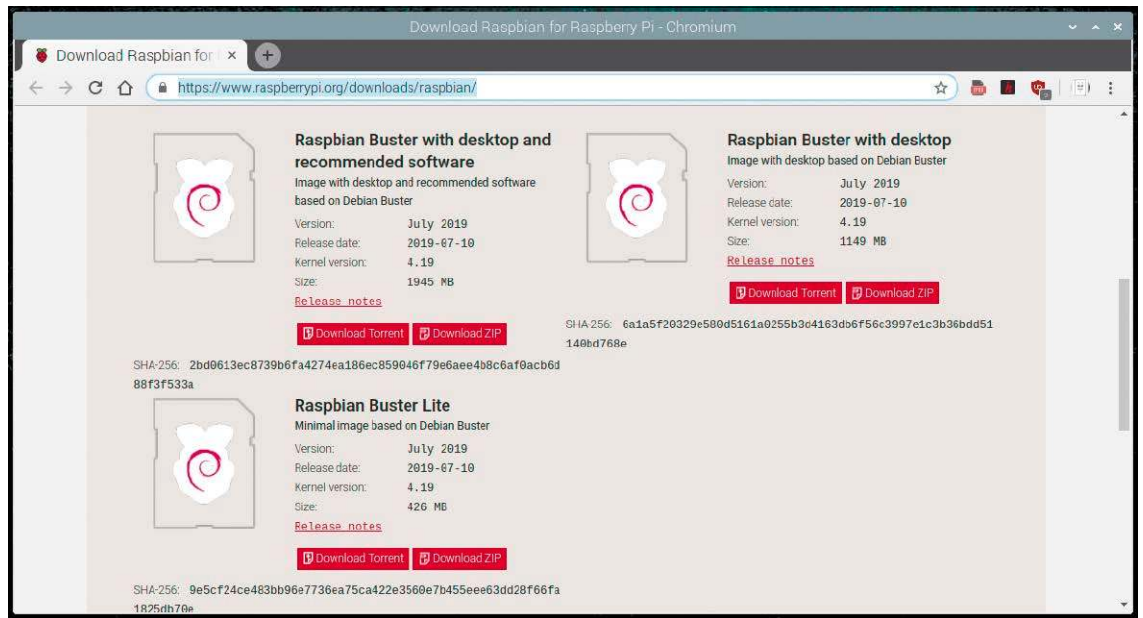
Kurz nach Erscheinen des Raspberry Pi 4 gab es sofort kritische Stimmen zur Temperaturentwicklung beim SOC inklusive CPU. Zu messen ist die Temperatur des System-on-Chip mit einem Tool, das Raspbian standardmäßig mitliefert:

```
vcgencmd measure_temp
```

Tipp: Das Werkzeug kann deutlich mehr als nur dies, wie die Abfrage `vcgencmd commands` zeigt.

Nach typischen Faustregeln gelten Temperaturen bis 50 Grad als kühl, bis 60 Grad als

Das Standardsystem für den Raspberry Pi: Mit Raspbian „Buster“ kann man nichts falsch machen. Bei Redaktionsschluss gab es auch noch kaum Alternativen.



warm, aber unproblematisch. Bei 70 Grad wird es zumindest ungesund und ab 80, 90 Grad schädlich, sofern diese Temperaturen als Zustand anhalten. Kurzzeitige Spitzen bis 90 Grad verträgt allerdings jede CPU. Im Dauerbetrieb des Raspberry 4 ist festzustellen, dass der Kleinrechner im geschlossenen Gehäuse auch bei geringer Auslastung 60 Grad und mehr meldet. Das Abnehmen des Gehäusedeckels oder der komplette Verzicht auf ein Gehäuse bringt annähernd drei Grad Besserung, der Einsatz kleiner passiver Kühlkörper macht sich nur minimal bemerkbar. Ob der relativ große, ebenfalls passive RPI COOL 40X30 (etwa bei *reichelt.de* für 2,40 €) mehr ausrichtet, haben wir nicht getestet.

In kühler Ecke ohne Sonnenlicht und ohne Gehäusedeckel sollte der Pi 4 mit Werten um die 60 Grad zu betreiben sein, mit Temperaturspitzen bis 70 Grad. Das ist hübsch warm, aber nicht wirklich problematisch. Ähnliche Werte konnten wir beim Odroid XU4 auslesen, der dies nachweislich über Jahre vertrag. Mit etwas Optimismus ist ferner davon auszugehen, dass der Raspberry Foundation die Wärmeentwicklung des neuen Pi 4 bekannt ist und diese im Dauerbetrieb getestet wurde.

Hinweis: Im Standardbetriebssystem Raspbian lässt sich die grafische Oberfläche wie gewohnt über die „Raspberry-Pi-Konfiguration“ (`rc_gui`) bequem abschalten, falls der Pi 4 als Controller oder Server dient. An den Temperaturen ändert diese Maßnahme allerdings nichts.

Minimaler Stromverbrauch

Die hohen Betriebstemperaturen lassen höheren Stromverbrauch des Raspberry Pi 4 vermuten. Tatsächlich bleibt die Platine aber legendär sparsam: Für die pure Platine ohne angeschlossene Datenträger messen wir im Leerlauf 3,7 Watt, etwas mehr also als beim Modell 3, aber immer noch äußerst ökonomisch. Erstaunlicherweise ist der neue Raspberry auch unter Hochlast kaum über fünf Watt zu bringen. Wir haben uns mit Filmwiedergabe aus dem Netz plus ISO-Download aus dem Web, Terminalaktion und Mausaktivität alle Mühe gegeben und messen als Spitzenwert lediglich 5,2 Watt. Allerdings zeigt die Platine unter extremer Last Aussetzer am Desktop oder bei anderen am Multitasking beteiligten Aufgaben. Der Pi 4 taktet offenbar vor drohender Überlastung herunter. Zwischen 3,7 bis 4,5 Watt – in diesem engen Bereich bleibt die Platine praktisch kontinuierlich. Den Verbrauch von angeschlossenen Datenträgern müssen Sie gegebenenfalls hinzurechnen: Ein aktiver USB-3.0-Hub mit zwei sparsamen 2,5-Zoll-USB-Festplatten ist mit weiteren 3,5 Watt zu veranschlagen. Das ergibt in diesem Beispiel insgesamt ein äußerst genügsames Serversystem, das kaum acht Watt fordert (und im 365-Tage-Dauerbetrieb ganze 20 Euro Stromkosten verursacht).

Raspbian „Buster“ für den Pi 4

Auf den unverhofften Auftritt des neuen Raspberry 4 werden bis Erscheinen dieses

Magazins diverse Spezialdistributionen mit angepassten Versionen reagieren. Bis Redaktionsschluss Anfang September war davon noch nicht viel zu sehen: Das eiligst fertiggestellte Raspbian auf Basis von Debian 10 „Buster“ war das einzige Allzwecksystem, das vorlag. Der bekannte Noobs-Installer bot zu diesem Zeitpunkt wiederum nur besagtes Raspbian „Buster“ sowie die Spezialdistribution Libre Elec mit dem Mediencenter Kodi. Libre Elec bekannte sich zu diesem Zeitpunkt noch zu einem Zustand der Betaphase und war uns außerdem zu spezialisiert.

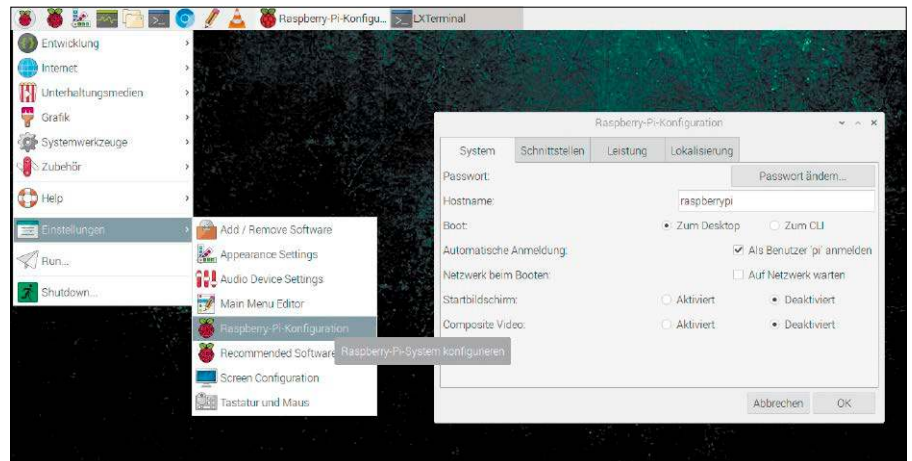
Die gewohnte Seite www.raspberrypi.org/downloads/ bietet neben den offiziellen Distributionen Raspbian und Noobs die Links zu weiteren Raspberry-Systemen wie Ubuntu Mate oder Ubuntu Server. Verwenden Sie diese Images für den neuen Raspberry aber nur, wenn die Beschreibung ausdrücklich Modell 4 nennt. Bis Redaktionsschluss war dies nicht der Fall.

Das offizielle Standardsystem Raspbian „Buster“ stammt von der Raspberry Pi Foundation selbst und sollte die beste Abstimmung mit der Platinenhardware gewährleisten. An der Installation des neuen Raspbian hat sich nichts geändert. Das System gibt es unter www.raspberrypi.org/downloads/raspbian/ in drei Varianten, deren mittelgroße mit etwa 1,1 GB wir empfehlen: „Raspbian Buster with desktop“ bringt den bekannten, einfachen Desktop „Pixel“ mit sowie eine Software-Basisausstattung inklusive Chromium-Browser. Der

Download ist ein ZIP-Archiv, das Sie nach dem Entpacken zum deutlich größeren IMG-Abbild mit den üblichen Werkzeugen auf Micro-SD kopieren. Unter Ubuntu eignet sich dafür Gnome-Disks („Laufwerksabbild wiederherstellen“), unter Windows der Win 32 Disk Imager (auf Heft-DVD) oder auf allen Plattformen Etcher (www.balena.io/etcher). Mit so bestückter und eingelegerter ist der Raspberry dann sofort startklar.

Raspbian „Buster“ mit Pixel-Desktop ist ein schlankes und agiles System, das kaum 200 MB Eigenbedarf hat. Daher sollte für Raspbian die Raspberry-Variante mit zwei GB RAM für alle Aufgaben und Rollen locker ausreichen. Als erste Aktion nach dem allerersten Booten wird das Dateisystem auf der SD-Karte auf die gesamte Kapazität erweitert. Dies erfolgt automatisch und danach startet der Pi neu. Die Bootzeit zum klickbereiten Desktop liegt selbst mit preiswerter Discount-SD-Karte unter 30 Sekunden. Der Ersteinrichtungs-Assistent bietet dann an, das Raspbian-System auf Deutsch umzustellen, das Passwort (voreingestellt ist „raspberrypi“) des Standardkontos „pi“ zu ändern, sich optional am WLAN anzumelden und die jüngsten Updates einzuspielen.

Spätere Systemaktualisierungen erledigen Sie mit „Systemwerkzeuge → Paketaktualisierung“. Die wichtigsten Systemeinstellungen versammelt Raspbian unter „Einstellungen → Raspberry-Pi-Konfiguration“ (rc_gui). Unter „Schnittstellen aktivieren Sie per Klick wichtige Dienste wie SSH oder VNC. Samba muss allerdings manuell installiert



Raspbian-Konfigurationszentrale: Hier bestimmen Sie über die Desktoprolle des Minirechners und über entscheidende Dienste wie SSH. Samba muss manuell eingerichtet werden.

und konfiguriert werden. Unter „System“ gibt es die schon erwähnte Einstellung, ob das System zum Desktop oder zur Konsole („CLI“) starten soll. Beim Start zur Konsole können Sie mit dem Befehl *startx* den Desktop jederzeit manuell laden.

Ungeachtet des stabilen und performanten Eindrucks von Raspbian „Buster“ zeigt das System auch einige Bugs, die wohl der relativ hektischen Fertigstellung geschuldet sind. Netzpasswörter für Samba oder SSH vergisst das System gerne, auch wenn das Gegenteil gefordert wurde.

Der Dateimanager will Dateien und Ordner bei Doppelklick umbenennen statt öffnen, was sich vorläufig durch Markieren und Eingabetaste umgehen lässt. Auch die deutsche Lokalisierung ist an vielen Stellen unvollständig.

Der Raspberry Pi 4 als Desktop?

Die Tauglichkeit als Desktopsystem wurde auch schon einigen Vorgängern des Modells 4 angedichtet. Der aktuelle Raspberry kommt solchem Anspruch immerhin näher. Einen Film mit VLC ansehen **oder** mit Chromium ins Web gehen **oder** mit dem Writer von Libre Office arbeiten – das alles geht flüssig von der Hand. Wer aber von einem Desktopsystem flexibles Multitasking erwartet, wird mit dem Raspberry Pi 4 nicht glücklich. Im Hintergrund eine Systemaktualisierung zu erledigen und gleichzeitig zu arbeiten oder Medien zu nutzen, überfordert den Minirechner. Dann bleibt schon mal ein Fenster ohne Rückmeldung und die Reaktion auf den Mausclick bleibt aus. Ein Multitasking-Desktop ist auch der neue Raspberry nicht. ■

MINI-BENCHMARK MIT RASPBERRY PI 4

Wer misst, misst Mist. In der Tat halten wir den empirischen Alltag, wie flott ein Rechner startet, wie schnell er die Daten im Netzwerk transportiert, wie flüssig sich der Desktop verhält, für aussagekräftiger als numerische Benchmarks. Einen kleinen Vergleich mit der simplen arithmetischen Iteration

```
time $(i=0; while (( i < 9999999 )); do (( i ++ )); done)
```

haben wir auf etlichen Geräten dennoch ausgeführt. Die primitive Methode haben wir gewählt, weil auf den diversen Geräten eine andere einheitliche Methode ohne großen Aufwand nicht realisierbar war. Über die Aussagekraft dieses Primitivbenchmarks lässt sich gewiss streiten, aber die Rangfolge deckt sich erstaunlich exakt mit unserer praktischen Alltagserfahrung mit diesen Geräten. Den Raspberry Pi 4 finden Sie im Mittelfeld und das ist mehr als respektabel, da es sich um das mit Abstand preisgünstigste Gerät handelt.

CPU-„BENCHMARK“ MIT RASPBERRY PI 4

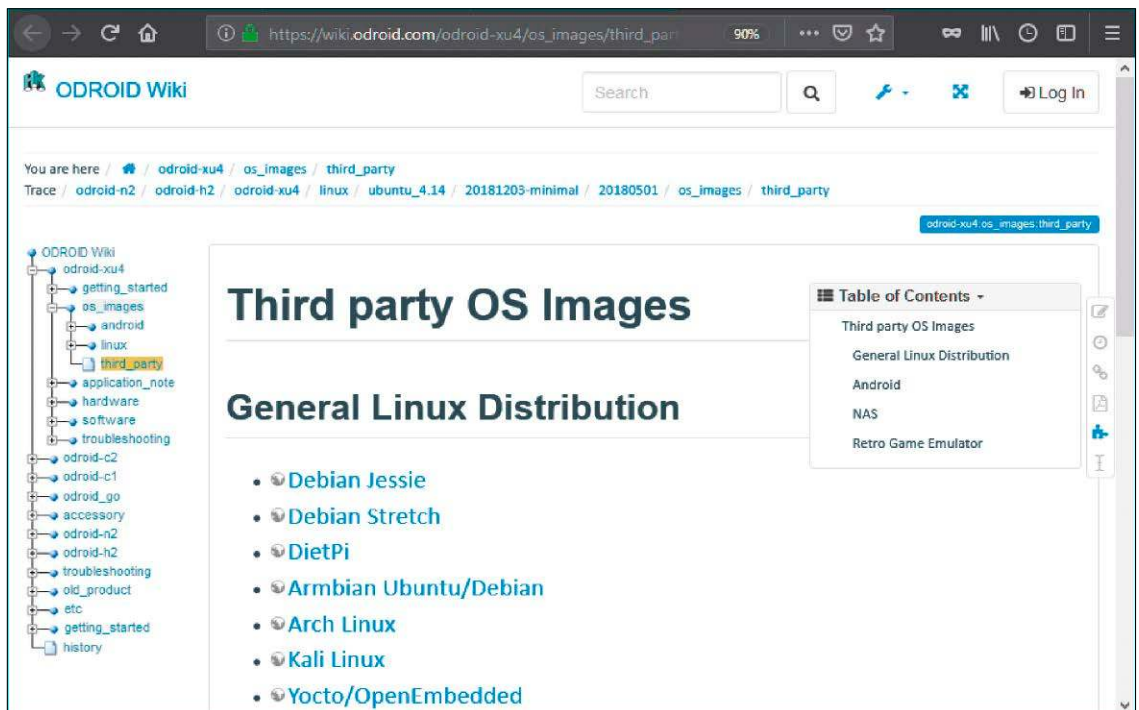
Gerät	Prozessor	Architektur	Zeit*
PC	Intel i7 (3,4 GHz)	x86	25,56
Odroid H2	Intel Celeron J4105 (2,5 Ghz)	x86	41,28
Älteres Notebook	AMD Phenom Dual (3,0 GHz)	x86	55,94
Odroid N2	Amlogic (1,8 GHz) / A53 (1,9 GHz)	ARM	71,71
Raspberry Pi 4	Cortex A53 (1,4 GHz)	ARM	113,11
Odroid XU4	Cortex A7/A15 (1,4/2,0 GHz)	ARM	144,86
Odroid U3	Exynos 4 (1,7 GHz)	ARM	216,30
Raspberry Pi 3	Cortex A53 (1,2 GHz)	ARM	317,33
Netbook	Intel Atom N270 (1,6 GHz)	x86	356,90

*kleiner ist schneller (Angabe in Sekunden)

Odroid-Mini-PCs

Keine Frage: Der neue Raspberry Pi 4 wird die meisten Konkurrenzplatinen vom Markt fegen und auch die Odroid-Familie wird nicht verschont bleiben. Dieser Artikel zeigt, was diese Minirechner leisten und ob sie weiterhin punkten können.

Odroid-Geräte sind ARM-basiert und benötigen ein angepasstes Linux, das Sie über <https://wiki.odroid.com> erreichen. Ausnahme ist der Odroid H2 mit Intel-CPU, der beliebige Systeme ermöglicht.



VON HERMANN APFELBÖCK

Verträgt der südkoreanische Hersteller Hardkernel, der die Odroid-Geräte baut, noch mehr Konkurrenz? Die Odroid-Platinen kannibalisieren sich nämlich bereits ordentlich untereinander. Die zahlreichen Odroid-Varianten der Jahre 2012 bis 2019 beweisen viel innovatives Potenzial, aber keine nachhaltige Strategie. Der nächste Odroid in der jeweiligen Preisklasse ist quasi immer der Killer des letzten Odroid. Aber vielleicht ist das ja die Strategie – und beim Raspberry ja auch nicht anders. Im Unterschied zum Raspberry skalieren die Odroids aber gewaltig und bieten eine Auswahl für unterschiedliche Leistungsansprüche. Außerdem hat uns bislang jede Odroid-Hardware qualitativ und in der Komponentenzusammensetzung über-

zeugt. Ein eventueller Schwachpunkt ist die Systemsoftware.

Die Odroids: Allgemeine Vorbemerkungen

Für alle Odroid-Platinen gibt es eine Reihe von Linux- und Android-Betriebssystemen, die Sie herunterladen und mit den üblichen Werkzeugen auf Micro-SD schreiben. Anlaufstelle ist das Wiki <https://wiki.odroid.com>, das auch über die Hauptseite erreichbar ist (www.hardkernel.com). Sie finden in der linken Spalte die aktuellen Platinenmodelle und unter dem einzelnen Modell jeweils den Eintrag „os_images“. Hier erscheinen dann die offiziellen Android- und Linux-Images, ferner unter „third party“ weitere inoffizielle, aber beachtenswerte Systeme wie etwa Diet Pi oder Open Media Vault. Die Auswahl an Systemen ist insgesamt nicht üppig, aber jederzeit ausrei-

chend: Ein ausbaufähiges LTS-Ubuntu, oft mit Mate-Desktop, ist für alle Platinen im Angebot. Problematischer als die Systemauswahl ist die Tatsache, dass ständig neue Odroid-Geräte die älteren verdrängen und diese dann softwaretechnisch nicht mehr gepflegt werden. So wird etwa der ältere, sehr brauchbare Odroid U3 längst nicht mehr verkauft und auch nicht mehr gepflegt. Über das zuletzt aktuellste Ubuntu 16.04.6 (mit Updatesupport bis 2021) auf dieser Platine wird daher wohl keine jüngere Version mehr hinausführen. Eine ähnliche Entwicklung ist für alle Odroids (außer H2) zu bedenken: Unter Umständen muss dann das Gerät ohne Updates weiterlaufen, was beim lokalen Heimserver kein ernstes Problem ist, aber jede Öffnung für den Internetzugriff verbietet.

Eine weitere Einschränkung gilt für alle Odroids: Die Platinen haben allesamt kei-

nen WLAN/Bluetooth-Funkchip an Bord. Das ist letztlich konsequent, weil ein H2, N2, XU4 oder HC1 für Serveraufgaben prädestiniert ist, die nur mit verkabeltem Ethernet Sinn machen. Wer zusätzliches WLAN oder Bluetooth benötigt, muss dies über einen WLAN- oder Bluetooth-USB-Stick nachrüsten. Die Firma Hardkernel bietet dafür eigene Dongles, jedoch funktionieren auch alle anderen Linux-kompatiblen Dongles wie Edimax EW-7811UN, Asus N10 Nano oder CSL 300. Deutscher Vertreter für sämtliche Odroid-Platinen und Zubehör ist Pollin (www.pollin.de). Das Meiste finden Sie auch bei Reichelt (www.reichelt.de) und Amazon.

Odroid H2: Ein Ausbau-Barebone

Der Odroid H2 wurde Ende 2018 erstmalig angeboten, war nach zwei Tagen ausverkauft und dann erst wieder ab Juli 2019 verfügbar. Das in mehrfacher Hinsicht außergewöhnliche Gerät gehört nicht wirklich in die Kategorie der Platinenrechner, sondern ist ein Ausbau-Barebone, der eher mit Zotac-Boxen oder Intel-NUCs konkurriert. Dies zeigt sich schon an der Größe der Platine (elf mal elf Zentimeter) und an der Tatsache, dass die typische GPIO-Leiste mit den programmierbaren Pins für Bastelprojekte fehlt. Der Odroid H2 ist ganz klar als Barebone für Heimserver oder Zweitdesktops konzipiert.

Intel-CPU: Mit dem Intel Processor J4105 (Quadcore mit 1,5 bis 2,5 GHz) verlässt der Odroid H2 die sonst übliche ARM-Plattform. Diese Celeron-CPU auf der 130-Euro-Platine ist natürlich kein Gamingrenner, kann aber mit älteren AMD-Phenom/Athlon- oder schwächeren Intel-i3-CPUs mithalten und ist jederzeit deskoptauglich. Aufgrund der x86-CPU gibt es keinerlei Einschränkungen hinsichtlich des Betriebssystems: Windows kann ebenso installiert werden wie jede Linux-Distribution. Angemessen ist ein leichtgewichtiges Ubuntu, mit dem sich der Odroid H2 geradezu spielt.

DDR4-RAM: Der Arbeitsspeicher kann je nach Bedarf auf zwei Bänken auf bis zu 32 GB bestückt werden (DDR4 SO-DIMM). Für eine der Platine angemessene Rolle als Daten- oder Medienserver sollten aber vier oder allenfalls acht GB allemal ausreichen.

Anschlüsse: Für Serverrollen ist der Odroid H2 auch sonst bestens gerüstet: Zwei SATA-3.0-Ports und zweimal USB 3.0 (ferner zwei-



Kein Platinenrechner, sondern eher ein Ausbau-Barebone mit Intel-CPU: Der Odroid H2 ist flexibel mit RAM, eMMC-Karte oder NVME-SSD bestückbar, bootet aber auch via USB oder SATA.

mal USB 2.0) sorgen für schnellen Datentransfer auf angeschlossenen Festplatten. Für den Netztransport sind zwei schnelle Gigabit-Ethernet-Anschlüsse vorhanden, die auch einen Einsatz als Netzwerkbrücke zwischen zwei lokalen Netzen oder als Hardwarefirewall hinter dem Router anbieten. Unter halbwegs idealen Umständen messen wir bis zu 115 MB/s, die der Rechner als Samba-Server ausliefert, was sich dem theoretischem Maximum von Gigabit-Ethernet nähert.

Der Rechner besitzt ein Uefi-Bios wie ein PC und kann sein Betriebssystem von SATA, USB, eMMC-Karte oder NVMe-Express-SSD booten. Ein Micro-SD-Einschub wie auf typischen Platinenrechnern ist nicht vorhanden und auch nicht nötig. Die Installation eines Betriebssystems erfolgt wie auf ei-

nem PC über ein Linux-Livesystem via USB-Stick oder über ein DVD-Laufwerk am USB-Anschluss. Für Monitoranschluss sind ein HDMI-Ausgang und ein Display-Port 1.2 (4K) vorhanden.

Neben der Soundausgabe via HDMI gibt es auch noch analoge Aus- und Eingänge für Klinenstecker.

Mit solcher Ausstattung kann die Platine locker mehrere Rollen erledigen: In unserem Fall arbeitet sie mühelos als zentraler Samba- und SSH-Server, als Apache-Server für eine Dokumentenzentrale und als Kodi-Mediencenter für das TV-Gerät via HDMI.

Lautlos: Die lüfterlose Platine macht keinerlei Betriebsgeräusche und zeigt trotz passiver Kühlung moderate Temperaturen zwischen 40 und 55 Grad. Die Leistungsaufnahme liegt höher als bei Raspberry & Co.

Systeminfo	14:38
Info	CPU: Intel(R) Celeron(R) J4105 CPU @ 1.50GHz CPU-Temperatur: 49°C CPU-Geschwindigkeit: 2158 MHz System CPU-Auslastung: CPU0: 1.9% CPU1: 3.9% CPU2: 1.9% CPU3: 1.9%
Speicherplatz	Gesamter Speicher: 3766MB Freier Speicher: 2957MB
Netzwerk	
Grafik	
Hardware	
PVR-Dienst	
Datenschutzerklärung	
System CPU-Auslastung: CPU0: 1.9% CPU1: 3.9% CPU2: 1.9%...	Versionsinfos: Version: kodi from Debian 7.6 Debian package version Kompiliert: 2:17.6+dfsg1-1ubuntu1
System Speicher-Auslastung: 809MB / 3766MB - 21%	

Odroid H2 mit Kodi: Der Rechner zeigt hier unter einem schlanken Linux mit Mediencenter Kodi, dass er diese Aufgaben leicht bewältigt. CPU, RAM, Temperatur – überall sind Reserven.

Quelle: pollin.de, hardkernel.com



Odroid N2 auf großem Kühler: Das Beste an dieser Hardware sind Sechs-Kern-CPU, Coolness und geringer Stromverbrauch. Die Input/Output-Leistung ist nicht besser als beim Odroid XU4.

bei etwa fünf Watt im Leerlauf, sieben bis acht Watt bei Last und gelegentlichen Spitzen bis zu 12 Watt.

Preise: Der Preis von 130 Euro darf nicht täuschen: Dafür gibt es nur die nackte Platine ohne Netzteil, ohne RAM, ohne Gehäuse, ohne Bootmedium, ohne Kabel. Um das Barebone-ähnliche Ausbauboard zum Laufen zu bringen, sind folgende Ergänzungen einzuplanen: ein Netzteil (circa 14 Euro), ein Gehäuse (circa 12 Euro), vier GB RAM (DDR4-SO-DIMM, circa 50 Euro), eMMC-Karte mit 64 GB (circa 55 Euro), eventuelle Kabel wie Displayport nach HDMI (zehn Euro), SATA-Kabel (fünf Euro).

Es ist ratsam, den Kauf der Komponenten so abzusichern, dass am Ende alles passt. Der Vertrieb Pollin.de kann da manche Zweifel beseitigen, insofern er das H2-taugliche Zubehör direkt anzeigt. Der Gesamtpreis geht dann schnell Richtung 300 Euro, wobei die angeführten Beispiele bei RAM und eMMC sowohl nach oben wie nach unten zu skalieren sind. Eine schnelle eMMC-Karte ist optimal, aber optional, da der Odroid H2 auch reichlich andere Bootoptionen besitzt.

Odroid N2: Coole Platine

Nimmt man den beschriebenen Odroid H2 aus den genannten Gründen aus der Rechnung, ist der Odroid N2 das aktuelle Spitzenmodell der Odroid-Platinenrechner. Der seit Frühjahr 2019 erhältliche Odroid N2 versteht sich mit 40-poliger GPIO-Leiste auch als Bastelplatine, ist aber in erster Linie als Heimserver oder Zweitdesktop konzipiert. Auffällig ist das Kühlkonzept der relativ breiten Platine, die komplett auf einem ebenso großen passiven Kühlkörper sitzt.

Sechs-Kern-CPU: Die Platine kombiniert sechs ARM-Kerne – zwei kleine Kerne (Cortex A53 mit 1,9 GHz) und vier große (Cortex A73 mit 1,8 GHz). Die Leistung ist spürbar, aber nicht dramatisch besser als beim neuen Raspberry. Mit dieser CPU und dem Mali-Grafikchip G52 liefert der Odroid N2 einen nahezu flüssigen Desktop. Beim Einsatz als Zweitdesktop ist die Hardware dem Raspberry Pi 4 eindeutig überlegen.

Anschlüsse: Der Odroid N2 bietet kein SATA, aber viermal USB 3.0. Für den Netzverkehr gibt es einen Gigabit-Ethernet-Anschluss, womit der Rechner als Samba-Server bis zu 110 MB/s liefert. Weniger erfreulich ist die Leistung der USB-Ports, die sich per internen Hub einen USB-3.0-Kanal teilen. Dies führt beim lokalen Austausch zwischen diesen USB-Laufwerken zu eher enttäuschendem Durchsatz. Eine große Datenfestplatte ist daher die klügere Ausstattung als mehrere kleine, zumal diese einen zusätzlichen Hub erfordern.

Alternativ zur Micro-SD-Karte kann das Betriebssystem auch von einer schnelleren eMMC-Karte gebootet werden. Die Auswahl des Bootmediums erfolgt über einen kleinen Schalter auf der Platine. Zur Soundausgabe gibt es neben dem typischen HDMI-Ausgang (Standardgröße) einen analogen Ausgang für Klinkestecker. Außerdem ist ein Infrarotempfänger an Bord.

Lautlos und kühl: Die mit zehn mal neun Zentimetern relativ breite Platine auf dem großen passiven Kühler arbeitet lüfterlos und somit absolut lautlos. Das Kühlkonzept scheint überzeugend, da die Platine im Leerlauf nur 35 Grad meldet und unter Last kaum über 45 Grad zu heizen ist. Das ist auch haptisch anhand der offenen Platine leicht zu verifizieren, während man beim

Raspberry Pi 4 die Finger besser weglässt. Das Gerät bestätigt seine Coolness auch beim Stromverbrauch: Nur zwei bis drei Watt fordert der Leerlaufbetrieb und bei Last geht es maximal Richtung fünf Watt. Für die Stromversorgung externer 2,5-Zoll-USB-Festplatten über die USB-Ports gilt Ähnliches wie beim Raspberry: Zwei Laufwerke sind bereits zu viel, spätestens dann, wenn die Laufwerke Arbeit bekommen. Ohne zusätzlichen aktiven USB-Hub geht es also auch hier nicht.

Preise: Die Platine gibt es mit zwei oder vier GB DDR4-RAM für circa 80 beziehungsweise 95 Euro. Wenn Kabel für HDMI und eine SD-Karte vorhanden sind, ist der Odroid N2 damit bereits vollständig ausgestattet. Das optionale Gehäuse für etwa sieben Euro ist eigentlich nur eine Abdeckung, die in die Schiene des Lüftersockels geschoben wird.

Odroid XU4: Das Auslaufmodell

Bis Ende 2018 noch Spitzenmodell, gerät der Odroid XU4 durch die hauseigene Konkurrenz und den Raspberry Pi 4 zum Auslaufmodell. Die Platine hat gegen den Pi 4 nur noch schwache Argumente und wem dieser nicht genügt, kann zum Odroid N2 greifen. Das ist fast bedauerlich, denn der XU4 hat sich im Server-Dauerbetrieb als äußerst robust und zuverlässig erwiesen. Solche Nachhaltigkeit als unermüdlicher Rechenknecht muss der Odroid N2 erst noch nachweisen. Deskoptauglich ist der XU4 allerdings im Unterschied zum N2 definitiv nicht. Die besten Chancen hat die XU4-Hardware eventuell noch in ihren spezialisierten Varianten HC1 und HC2, die ebenfalls auf Odroid XU4 basieren (siehe unten).

CPU und RAM: Der Achtkerner arbeitet mit zwei Quadcore-CPU, wobei je nach Auslastung der Vierkerner Cortex A15 mit zwei GHz oder der sparsamere Vierkerner Cortex A7 mit 1,4 GHz zum Zuge kommt. Mit standardmäßig zwei GB DDR3-RAM ist die Platine für den Serverbetrieb ausreichend bestückt.

Anschlüsse: Entscheidend für den Datendurchsatz ist die Kombination von USB 3.0 (zweimal) mit Gigabit-Ethernet. Die theoretischen 125 MB/s erreicht die Platine zwar nicht, aber 80 bis 90 MB/s sind maximal möglich. Als Boot- und Systemmedium kommt sowohl die typische Micro-SD-Karte als auch eine eMMC-Karte infrage. Die Auswahl des Medium erfolgt über einen kleinen Schalter auf der Platine. Für Erweite-

rungen und Bastellösungen gibt es zwei Pin-Anschlüsse (30 plus 12).

Mit und ohne Lüfter: Das Kühlkonzept des Odroid XU4 wurde seit seinem Erscheinen 2015 vielfach kritisiert. Von Platinenrechenern erwarten die Kunden lautlosen Betrieb. Der XU4 hat einen aktiven Lüfter, der seine kleinen Maße mit hoher Drehzahl ausgleicht. Das Geräusch ist nicht laut, aber aufgrund der hohen Frequenz unüberhörbar. Beim Einsatz als Medienserver im Wohnzimmer kann das durchaus stören. Daher hat Hardkernel den Odroid XU4Q mit passivem Kühlkörper nachgeschoben („Q“ für „quiet“). Die Variante ist etwas preiswerter, aber etwas leistungsärmer, weil die Platine hier häufiger auf die schwächere A7-CPU schaltet. Wer einen XU4 besitzt, kann den aktiven Lüfter auch durch den passiven Kühlkörper ersetzen, der als Einzelzubehör für etwa acht Euro verkauft wird.

Stromverbrauch: Der Odroid XU4 kommt im Idle-Betrieb auf etwa vier Watt und fordert bei Last und laufendem Lüfter bis zu zehn Watt.

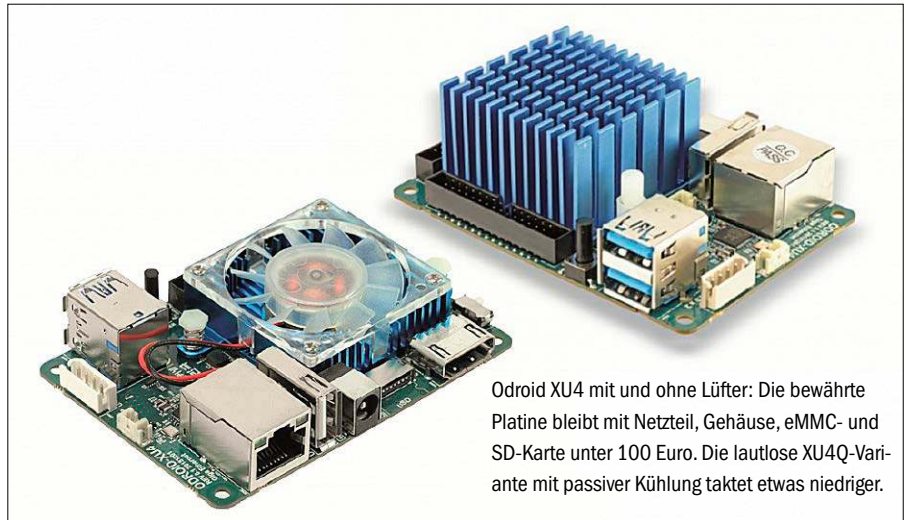
Preise: Die Preise für die Platine dürften demnächst purzeln. Bislang kostet er immer noch etwa 80 Euro, als lüfterloser XU4Q circa 75 Euro (www.pollin.de). Aktuelle Bundles liegen aber bereits unter 100 Euro und liefern Gehäuse, Netzteil, SD- und eMMC-Karte mit.

Odroid HC1/HC2: Kleine Heimserver

„HC“ steht für „Home Cloud“. Die beiden Odroid-Varianten basieren auf XU4 und sind hinsichtlich CPU, GPU, RAM und Gigabit-Ethernet identisch ausgestattet. Statt USB 3.0 (nur einmal USB 2.0) gibt es hier eine SATA-3-Schnittstelle für genau eine Festplatte oder SSD, die in das Alugehäuse eingeschoben wird. HC1 und HC2 fokussieren auf einen kleinen, schnellen Netzwerkspeicher für private Zwecke.

HC1 und HC2 haben kein HDMI oder sonstigen Monitoranschluss: Das System kann nur über das Netzwerk mit SSH erreicht und verwaltet werden.

Preise: Die lüfter- und lautlosen HC1 und HC2 kosten circa 60 und 65 Euro. Der einzige Unterschied der beiden Varianten ist das Alugehäuse, das beim HC1 nur ein 2,5-Zoll-Laufwerk, beim größeren HC2 wahlweise eine 2,5- oder 3,5-Zoll-Festplatte aufnimmt. Das unentbehrliche Netzteil kostet circa acht Euro.

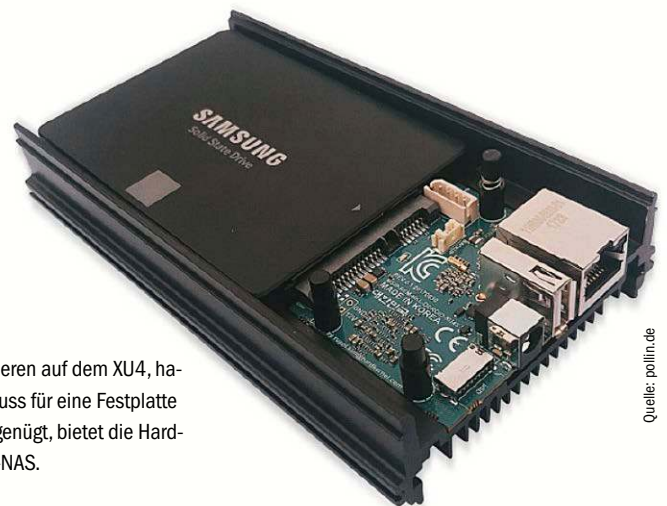


Odroid XU4 mit und ohne Lüfter: Die bewährte Platine bleibt mit Netzteil, Gehäuse, eMMC- und SD-Karte unter 100 Euro. Die lautlose XU4Q-Variante mit passiver Kühlung taktet etwas niedriger.

Odroid C1/C2: Obsolet

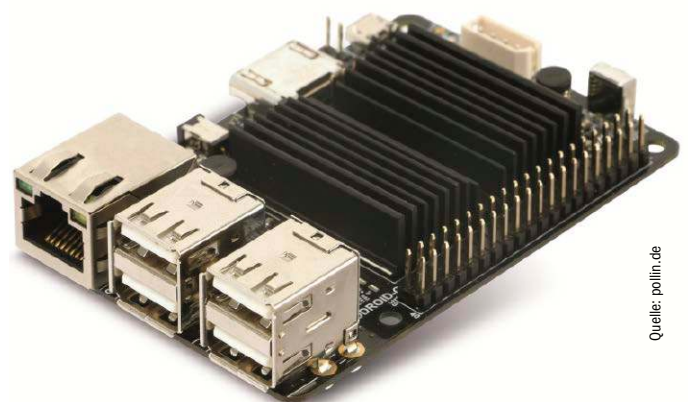
Die grundsoliden Platinen Odroid C1 und C2 waren 2015 mit Quadcore-CPU, einem oder zwei GB RAM sowie Gigabit-Ethernet als Raspberry-Konkurrenz konzipiert. Sie konnten aber schon neben dem Raspberry Pi 3 B+ (Anfang 2018) nur noch aufgrund der schnelleren Ethernet-Schnittstelle be-

stehen – und neben dem aktuellen Raspberry 4 wohl definitiv nicht mehr. Der Odroid C2 wird derzeit immer noch für knapp 55 Euro verkauft – allerdings bereits mit fallender Preistendenz. Die Raspberry-Variante mit zwei GB RAM kostet 50 Euro und schlägt den Odroid C2 (ebenfalls zwei GB RAM) in allen anderen Belangen. ■



HC1/2 („Home Cloud“) basieren auf dem XU4, haben aber einen SATA-Anschluss für eine Festplatte (HC1 nur 2,5 Zoll). Wo dies genügt, bietet die Hardware ein aufgeräumtes Mini-NAS.

Quelle: pollin.de



Quelle: pollin.de

Mini-PCs & Notebook-Upcycling

Klein, aber nicht zu lahm: Wenn es auf geringen Platzbedarf und geringe Leistungsaufnahme ankommt, können neben Raspberry & Co. Mini-PCs die richtige Wahl sein. Alternativ bieten sich ausgemusterte Notebooks an.

VON THORSTEN EGGELING

PCs gibt es in zahlreichen Bauformen und Leistungsklassen. Der klassische Desktop-PC kommt für viele Nutzer kaum noch infrage, sein Ausbaupotenzial lockt inzwischen wahrscheinlich nur noch Gamer. Wer heute einen Computer braucht, greift eher zum Notebook. Das benötigt nicht viel Platz, hat Monitor und Tastatur dabei und ist mobil. Dass es genügend Abnehmer für weitere Bauformen gibt, beweisen Platinen-PCs wie der Raspberry Pi. Das Angebot nehmen aber wahrscheinlich vorwiegend Linux-Enthusiasten und PC-Bastler wahr. Aufgrund des verbauten ARM-Prozessors lässt sich auf dem Gerät auch nicht jedes Betriebssystem installieren und die begrenzte Leistung schränkt die Einsatzmöglichkeiten ein.

Ein PC mit x86-Prozessor ist flexibler und verspricht mehr Leistung bei geringer Stromaufnahme, auch wenn er in einem sehr kleinen Gehäuse steckt. In der Regel müssen Sie dafür aber deutlich mehr Geld ausgeben als für einen Raspberry Pi. Für einige Aufgaben eignen sich ferner ausgemusterte Notebooks oder sogar der Kauf eines solchen.

Mini-PCs mit Intel-Prozessoren

Bei der Ausstattung eines Computers kommt es darauf an, wofür Sie ihn einsetzen wollen. Ein unterer Mittelklasse-PC für um die 400 Euro reicht für die täglichen Büroarbeiten aus. Preisgünstige Notebooks kosten in etwa dasselbe. Mehr Spaß machen natürlich Geräte um die 1000 Euro und mehr, die sich dann auch für an-



Kleine Computer: Die Leistung von Mini-PCs hängt von der verbauten CPU ab. Preisgünstige Modelle lassen sich unter Linux gut als Dateiserver oder Mediacenter nutzen.

spruchsvollere Software eignen. Kleine Datei- oder Webserver für das heimische Netzwerk benötigen nicht viel Leistung. Dauerläufer sollen auch die Stromrechnung nicht in die Höhe treiben, weshalb hier Platinenrechner wie der Raspberry Pi ausreichen (siehe ab Seite 54).

Wem es vor allem auf eine geringe Baugröße ankommt, kann zu einem kompakten Mini-PC greifen. Die gibt es inklusive CPU, RAM und Festplatte/SSD für 200 bis 1600 Euro. Barebones für eine eigene Zusammenstellung enthalten meist nur die aufgelötete CPU und kosten mit 110 bis 850 Euro entsprechend weniger.

Die große Preisdifferenz erklärt sich vor allem durch die eingesetzten Prozessoren und die zugehörigen Chipsätze. Intel Atom, Celeron und Pentium sind langsa-

mere CPUs, Intel Core i3, i5, und i7 sind schneller. Eine höhere Zahl in der Produktbezeichnung steht für bessere Leistungsmerkmale wie Cache oder Taktfrequenz. Das beim Celeron vorangestellte „N“ weist auf einen Prozessor für Mobilsysteme hin, bei Intel-Core-CPU's ist es ein „M“. „HQ“ steht für Hochleistungsgrafik, „U“ für einen geringen und „Y“ für eine extrem geringe Leistungsaufnahme. „G“-Modelle besitzen eine separate Grafikeinheit, beim Intel Core i7-8809G handelt es sich um die leistungsfähige Grafik AMD Radeon RX Vega M GH. Mit einer Leistungsaufnahme von bis zu 100 Watt erzeugt das Gespann einiges an Abwärme, was eine ausreichende Kühlung notwendig macht.

Das Leistungsspektrum der Mini-PCs legt auch deren Einsatzbereich fest. Die preis-

günstigen Modelle eignen sich als Dateiserver im Heimnetzwerk oder Mediacenter im Dauerbetrieb. Sie bieten fast durchweg mehr Leistung als Platinenrechner, wenn auch zu einem etwas höheren Preis. Die deutlich teureren Geräte sind dagegen eher ein Ersatz für Desktop-PCs im Towergehäuse oder leistungsstarke Notebooks.

Konfigurationsbeispiel I: Zotac Zbox CI327

Die Zotac Zbox CI327 kostet etwa 180 Euro und ist mit einer Intel Celeron N3450 Quad-core-CPU ausgestattet, die mit bis zu 2,2 GHz taktet. Das Gehäuse misst 12,8 x 12,7 x 5,7 Zentimeter. Der Prozessor ist passiv gekühlt, die Wärme wird über das Gehäuse abgeführt. RAM und Festplatte sind nicht im Kaufpreis enthalten. Acht GB RAM kosten etwa 40 Euro, vier GB (20 Euro) reichen aber aus, wenn das Gerät nur als Mediacenter mit Kodi oder als Dateiserver ohne grafische Oberfläche dienen soll. In das Gehäuse passt eine Festplatte oder SSD mit 2,5 Zoll. Eine kleine SSD mit 120 GB gibt es schon für 30 Euro, sodass sich die absolute Minimalausstattung insgesamt etwa auf 230 Euro beläuft.

Hochgeschwindigkeit können Sie von der Celeron-CPU nicht erwarten. Dank SSD ist das System nach dem Einschalten jedoch schnell betriebsbereit und für Kodi oder einfache Serveraufgaben die Leistung mehr als ausreichend. Für Kodi können Sie auf dem Gerät beispielsweise Libre Elec installieren (<https://libreelec.tv>). Oder Sie richten auf dem Gerät eine Linux-Distribution wie Ubuntu oder Linux Mint ein. Kodi lässt sich dann bei Bedarf über die Paketverwaltung installieren. Sie können die Zotac Zbox aber auch als Datei- oder Webserver einsetzen. Da das Gerät über zwei Gigabit-Ethernet-Schnittstellen verfügt, bietet sich auch eine Verwendung als Router an, so etwa mit der flexibel konfigurierbaren Pfense-Firewall auf Free-BSD-Basis (<https://www.pfsense.org/>).

Konfigurationsbeispiel II: Intel NUC-Kit 8i5BEK

Die Intel-NUCs (Next Unit of Computing, www.pcwelt.de/nucpc) gibt es in unterschiedlichen Bauformen und mit CPUs in fast jeder Leistungsklasse. In den preisgünstigen Modellen ist eine Celeron-CPU verbaut (ab 130 Euro), es gibt aber auch Geräte mit Core-i7-CPU (bis etwa

Zahlreiche Anschlüsse: USB 2.0, 3.0 und Buchsen für HDMI sowie Displayport gehören meist zum Standard. Zwei Gigabit-Ethernet-Buchsen erweitern die Einsatzmöglichkeiten.

Schneller Laufwerkspeicher: Eine M2-SSD spart Platz im Gehäuse und beschleunigt den Mini-PC. Im Vergleich zur Festplatte startet das System deutlich schneller.

1500 Euro). Die Gehäuse haben meist eine Abmessung von 11,7 x 11,2 x 5,1 Zentimetern. Je nach Ausführung lässt sich eine 2,5-Zoll-Festplatte oder SSD einbauen, teilweise zusätzlich eine M2-SSD. In die flacheren Gehäuse mit 11,7 x 11,2 x 3,6 Zentimetern passt hingegen nur eine M2-SSD.

Intel unterscheidet zwischen NUC-Mini-PCs, die inklusive RAM, Laufwerk und Windows 10 geliefert werden, und NUC-Kits für eine eigene Zusammenstellung. Wir haben das Intel NUC-Kit 8i5BEK (369 Euro) ausprobiert, was mit zusätzlich 16 GB RAM (78,50 Euro) und einer Ein-TB-M2-SSD (213 Euro) unser Budget mit insgesamt 660 Euro belastet hat. Dafür gibt es zwar einen Intel Core i5-8259U (4x 2,3G Hz), der Preis liegt aber in etwa gleichauf oder sogar höher als bei einem ausgewachsenen PC im Towergehäuse. Der i5 benötigt eine aktive Kühlung. Deshalb ist ein kleiner Lüfter ver-



baut. Beim Neugerät ist er fast unhörbar, die Zeit wird jedoch zeigen, ob das so bleibt. Wer sich daran stört, kann auch nur ein Intel NUC-Mainboard erwerben und dazu ein Gehäuse mit Passivkühlung, das man schnell per Suche im Internet findet. Aufgrund der Standard-Intel-Hardware gibt es bei der Installation von Ubuntu 18.04 oder Libre Elec 9.0.2 keine Überraschungen. Als reiner Mediacenter-PC am TV-Gerät ist dieser Intel-NUC jedoch völlig überdimensioniert. Das Modell mit Core i5-CPU eignet sich eher als Desktopersatz oder für anspruchsvollere Serverrollen.

Mini-PCs mit Android-System

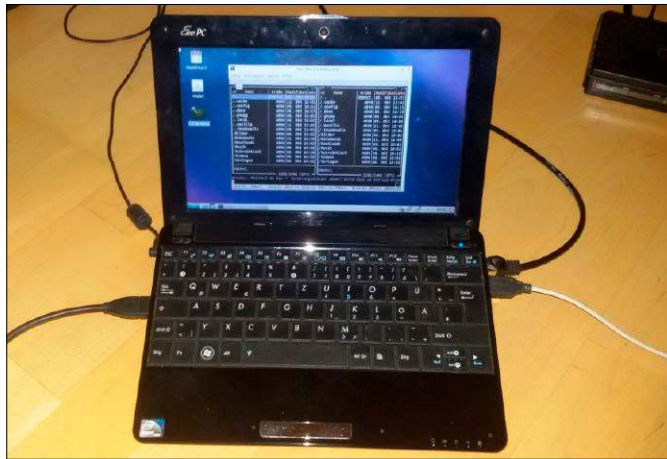
Im unteren Preissegment von 40 bis 100 Euro finden Sie etliche kleine Computer mit vorinstalliertem Android. Die Hardware arbeitet meist auf Basis eines ARM-Prozessors. Die Geräte sind eine optimale Ergän-

PCS AUF EINEM HDMI-STICK

Es geht noch eine Nummer kleiner. Die komplette PC-Hardware lässt sich auf einem HDMI-Stick unterbringen, den man mit einem Monitor oder TV-Gerät verbindet. Es gibt Modelle mit einer Intel Atom-, Celeron- oder Core-M-CPU ab etwa 145 bis 450 Euro. Die preisgünstigen Geräte dieser Klasse verfügen über zwei GB RAM und 32 GB Flashspeicher. Davon ist weniger Leistung zu erwarten als von einem Raspberry Pi 4 für 50 oder 60 Euro. Es ist jedoch möglich, jede Linux-Distribution und auch Windows 10 darauf zu installieren. Die leistungsfähigeren Stick-PCs sind aufgrund der hohen Preise kaum zu empfehlen, außer wenn man genau diese Bauform bevorzugt und sich mit den Einschränkungen abfindet.



HDMI-Stick: Im Fire-TV-Stick steckt ein vollwertiger PC. Durch das Android-System und den Mangel an Anschlüssen ist sein Einsatzgebiet jedoch stark auf Multimedia festgelegt.



Nicht vorschnell zum Elektronikschrott! Solche Netbooks erreichen locker die Leistung eines Raspberry 3 und arbeiten klaglos als Dateiserver oder wie hier als Desktop (Lubuntu).

zung für TV-Geräte, die keine oder ungenügende „Smart“-Funktionen besitzen. Netflix, Amazon Prime Video, die Mediatheken der TV-Sender sowie viele weitere Apps lassen sich damit komfortabel auf dem Fernseher, PC-Monitor oder Beamer nutzen. Der Amazon Fire TV Stick 4K ist besonders interessant, weil er für 59,99 Euro mehr bietet als manches teurere Gerät. Preislich liegt er damit im Bereich etwa des Raspber-

ry Pi, der sich zwar flexibler einsetzen lässt, bei Multimedia-Inhalten jedoch schnell an seine Grenzen gerät. Allerdings gibt es beim Amazon-Stick einige Einschränkungen: Apps lassen sich beispielsweise nur aus dem Amazon-Store installieren, das breitere Angebot des Google-Stores steht nicht zur Verfügung. Ausführliche Informationen dazu finden Sie unter www.pcwelt.de/2424592.

Betagte Notebooks neu beleben

Linux läuft auch auf Notebooks zufriedenstellend, die Sie inzwischen wegen zu geringer Leistung ausgemustert haben. Theoretisch lassen sich Notebooks in Betrieb nehmen, die 15 Jahre und älter sind. Niedrige Taktfrequenz, wenig RAM, USB 1.x und Fast Ethernet mit 100 MBit/s bereiten jedoch auch mit dafür angepassten Linux-Distributionen wenig Vergnügen. Sollte ein Notebook jedoch die Eckdaten ein GHz CPU, zwei bis vier GB RAM, USB 2.0 und Gigabit-Ethernet erfüllen, steht der Weiterverwendung nichts entgegen. Auch wenn ein genauer Vergleich schwierig ist, liegt ein derartiges Notebook etwa gleichauf mit einem Raspberry Pi 4.

Welches System wählen? Probieren Sie Ubuntu 18.04 oder Linux Mint 19 aus. Sollte die grafische Oberfläche zu zögerlich reagieren, greifen Sie zu Lubuntu oder Xubuntu. Beim alleinigen Einsatz als Dateiserver im Heimnetzwerk spielt das System kaum eine Rolle. Um RAM zu sparen, schalten Sie die grafische Oberfläche einfach ab. Nutzer von Ubuntu verwenden dafür diesen Befehl:

```
sudo systemctl set-default multi-user.target
```

Für die Anmeldung steht danach eine Textkonsole zur Verfügung, bei einem Server werden Sie aber den Fernzugriff über SSH bevorzugen. Alternativ greifen Sie zu einem Betriebssystem, das auf Serverdienste spezialisiert ist, so etwa das NAS-System Open Media Vault (www.pcwelt.de/OMV). Dienste wie Samba (Dateiserver auch für Windows-PCs), FTP und SSH sind standardmäßig dabei und lassen sich über eine Weboberfläche konfigurieren. ■

MINI-PCS MIT INTEL-CPU (AUSWAHL)

	Zotac Zbox CI327 Nano	Zotac Zbox MI549 Nano	Intel NUC-Kit NUC6CAYH	Intel NUC-Kit NUC8i5BEK
CPU	Celeron N3450	Intel Core i5-7300U	Intel Celeron J3455	Intel Core i5-8259U
GPU	HD Graphics 500	HD Graphics 620	HD Graphics 500	HD Graphics 655
RAM	bis zu 8 GB	bis zu 32 GB	bis zu 8 GB	bis zu 32 GB
Anschlüsse	SATA, HDMI 2.0, Displayport 1.2, VGA, 3x USB 3.0, 2x USB 2.0, 1x USB-C 3.0, Audioklinke	SATA, HDMI 2.0, Displayport über Thunderbolt 3 mit Adapter, 2x USB-C 3.1, 4x USB 3.0, Audioklinke	SATA, HDMI 2.0, VGA, 3x USB 3.0, 1x USB 2.0, Audioklinke, S/PDIF	M2 (SSD), HDMI 2.0, 1x Thunderbolt 3 (Display Port oder USB 3.1), 4x USB 3.1, Audioklinke
Netzteil	19 Volt, 40 Watt	19 Volt, 65 Watt	19 Volt, 65 Watt	19 Volt, 90 Watt
Netzwerk	2x Gigabit-Ethernet, WLAN (802.11ac), Bluetooth	2x Gigabit-Ethernet, WLAN (802.11ac), Bluetooth	Gigabit-Ethernet, WLAN (802.11ac), Bluetooth	Gigabit-Ethernet, WLAN (802.11ac), Bluetooth
Betriebssysteme	Linux, Windows	Linux, Windows	Linux, Windows	Linux, Windows
Hersteller	www.zotac.com	www.zotac.com	www.intel.com	www.intel.com
Preis (ohne RAM und Festplatte/SSD)	180	520	140	310

Zubehör für den Raspberry Pi

Für den Raspberry Pi gibt es viel interessantes Zubehör. Statten Sie das Gerät mit einer Kamera oder einem Minidisplay aus oder verwenden Sie Sensoren und Aktoren für Bastelprojekte.

VON THORSTEN EGGELING

Der Raspberry Pi gehört mit mehr als 20 Millionen verkauften Geräten zu den erfolgreichsten Ein-Platinen-PCs. Der ursprünglich als Lehr- und Lerncomputer entwickelte Raspberry Pi kann durch seinen günstigen Preis und die zahlreichen Einsatzmöglichkeiten überzeugen. Ein weiteres Argument ist, dass die Raspberry-Modelle hardwareseitig weitestgehend abwärtskompatibel sind. Das meiste Zubehör lässt sich weiterverwenden, auch wenn Sie auf ein neueres und schnelleres Modell umsteigen wie etwa aktuell auf den Raspberry Pi 4 (außer Gehäuse, Netzteil und HDMI-Kabel). Alles zusammen trägt dazu bei, dass ein breites Zubehörangebot verfügbar ist. Einiges ist für jeden Raspberry-Besitzer interessant, manches nur für Nutzer, die den Raspberry Pi als Experimentier- und Bastel-PC verwenden.

Gehäuse und Netzteil

Der Raspberry Pi wird als einzelne Platine verkauft oder als Starterkit inklusive Gehäuse, Netzteil und SD-Karte. Teilweise gibt es auch noch einen USB-Kartenleser für den PC, HDMI-Kabel und Kühlkörper dazu. Nur die Platine kostet zwischen etwa 35 Euro für den älteren Raspberry Pi 3 Modell B+, 40 Euro für den Raspberry 4 Mo-



Standardzubehör: Ein Netzteil benötigen Sie in jedem Fall. Es muss aber nicht das Original sein. Ein Gehäuse schützt das Gerät und per HDMI-Kabel erfolgt die Verbindung zum Monitor.

dell B mit einem GB RAM und etwa 60 Euro für das neueste Modell mit vier GB RAM. Starterkits mit unterschiedlicher Ausstattung kosten um die 75 Euro inklusive Raspberry Pi 3 oder 4.

Ob man das nötige Zubehör selbst auswählt oder ein Starterkit bestellt, ist Geschmackssache. Es ist auf jeden Fall flexibler, alle Teile einzeln zu bestellen. Beim Gehäuse beispielsweise haben Sie die Wahl zwischen Modellen aus Kunststoff oder aus Metall. Letztere ermöglichen eine bessere Wärmeableitung. Der Raspberry Pi 4 wird relativ heiß (siehe Artikel ab Seite 54), weshalb wenigstens Kühlkörper, vielleicht sogar Gehäuse mit Lüfter erforderlich sind. Für die passive Kühlung gibt es kleine Einzelkühlkörper, die man einfach auf die Chips klebt. Eine effektivere Wärmeableitung versprechen große Kühlkörper, die die gesamte Platine abdecken und gleichzeitig als einfaches Gehäuse dienen.

Beim Netzteil kann man zum original Raspberry-Pi-Netzteil greifen, für den Raspberry Pi 4 muss es bei fünf Volt mindestens drei Ampere liefern. Es kostet

knapp neun Euro und ist von angenehmer kleiner Bauform. Es funktioniert auch jedes andere Netzteil mit den gleichen oder besseren Leistungswerten.

Kameras für den Raspberry Pi

Es gibt mehrere Kameramodelle, die Sie an den Mini-PC anschließen können. Die erste Version war mit einem Fünf-Megapixel-Sensor ausgestattet (2952 x 1944 Pixel). Restbestände sind im Handel teilweise für unter 20 Euro zu bekommen. Das aktuelle Modell trägt Versionsnummer 2.1, besitzt einen Acht-Megapixel-Sensor (3280 x 2464 Pixel) und ist für etwa 25 Euro zu haben. Es ist in zwei Varianten mit und ohne Infrarotfilter erhältlich. Letztere ist an der dunklen Platine zu erkennen und für Aufnahmen in der Dämmerung und bei Nacht mit zusätzlicher Infrarotbeleuchtung gedacht. Es liegt ein kleiner IR-Filter aus Kunststoff bei, der Aufnahmen auch bei Tageslicht ermöglicht.

Der Anschluss der Kameras erfolgt über ein flaches Kabel an die 15-polige CSI-Schnittstelle (Camera Serial Interface) auf dem



Fotos und Videos: Das Kameramodul verwandelt den Raspberry Pi in einen Camcorder oder eine Webcam. Bei Bedarf verwenden Sie ein längeres Kabel zur Kamera.

Raspberry Pi. Der Pi sollte dann in einem Gehäuse untergebracht sein, das eine Durchführung für das Kabel besitzt. Es gibt auch Gehäuse mit einer Aussparung im Deckel, die ein aufklappbares Kameragehäuse aufnehmen können. Alternativ verwenden Sie ein eigenes Gehäuse für die Kamera. Sollte das Kabel zu kurz sein, gibt es im Handel längere Ersatzkabel.

Da sich an dem Anschluss seit der ersten Raspberry-Ausgabe nichts geändert hat, eignen sich die Kameras für die Modelle 1 bis 4. Damit das System die Kamera erkennt, gehen Sie im Menü auf „Einstellungen → Raspberry-Pi-Konfiguration“ und dann auf die Registerkarte „Schnittstellen“. Setzen Sie bei „Kamera“ die Option auf „Aktiviert“. Starten Sie Raspbian neu.

Im Terminalfenster nehmen Sie dann mit `raspistill -o bild.jpg` ein Bild auf oder mit `raspivid -t 10000 -o testvideo.mp4` ein Video mit einer Länge von zehn Sekunden. Wie Sie die Kamera für ein Überwachungssystem verwenden, lesen Sie unter

www.pcwelt.de/1925151, die Anleitung für eine einfache Webcam finden Sie unter www.pcwelt.de/2300255.

Displays für den Raspberry Pi

Der Raspberry Pi verfügt über eine HDMI-Buchse, an die Sie einen PC-Monitor oder ein TV-Gerät anschließen. Für spezielle Einsatzzwecke, etwa in Kraftfahrzeugen oder als öffentliches Infoterminal oder als Multimedia-Station, empfehlen sich kleinere Displays mit sieben bis zehn Zoll. Die gibt es auch als Touchscreen, was eine Bedienung ohne Maus und Tastatur erlaubt. Allerdings sollten Sie davon nicht allzu viel erwarten, weil sich die Raspbian-Oberfläche nicht besonders gut für die Fingerbedienung eignet. Ein Touchscreen kann jedoch sinnvoll sein, wenn Sie spezielle Anwendungen benutzen, die sich über große Bedienelemente bequem steuern lassen. Der offizielle Touchscreen der Raspberry Pi Foundation misst sieben Zoll und bietet eine Auflösung von 800 x 480 Pixeln (etwa 70 Euro). Im Lieferumfang ist eine Adapter-



Raspberry huckepack: Beim offiziellen Sieben-Zoll-Touchscreen der Raspberry Pi Foundation montieren Sie Adapterplatine und Raspberry Pi auf der Rückseite des Displays.

platine enthalten, die hinten auf das Display geschraubt wird. Der Raspberry Pi wird darüber angebracht und per Flachbandkabel verbunden (siehe Abbildung). Zur Stromversorgung dienen zwei Kabel, die zu den GPIO-Pins führen. Es genügt dann ein Netzteil für beide Geräte.

Wer einen größeren Touchscreen benötigt, findet im Handel Geräte mit HDMI-Anschluss (um die 100 Euro). Die Touchscreen-Signale gelangen über ein USB-Kabel zum PC. Der Vorteil: Diese Geräte sind nicht nur für den Raspberry Pi, sondern für beliebige PCs geeignet. In der Regel ist ein Treiber für die Steuerung erforderlich, den der Hersteller für Raspbian beziehungsweise Linux liefern muss. Informieren Sie sich vor dem Kauf, ob das gewünschte Gerät Linux unterstützt und welche Erfahrungen andere Benutzer damit gesammelt haben.

Spezialdisplays: Wenn der Raspberry Pi zur Steuerung von Geräten oder zur Erfassung von Messwerten eingesetzt wird, kann ein Minidisplay in Scheckkartengröße ausreichend sein. Die gibt es als LCD-, OLED- oder besonders stromsparende E-Paper-Module in Größen etwa zwischen 1,3 und 4,3 Zoll (Diagonale), LCDs wahlweise auch als Touchscreen. Die Platine bei Displays mit 2,7 bis vier Zoll entspricht in etwa der Größe der Raspberry-Pi-Platine. Die Module kosten je nach Größe und Ausstattung etwa zwischen 20 und 100 Euro.

Die Displaymodule sitzen meist auf einer HAT-Platine (Hardware Attached on Top), die auf die GPIO-Pins (General Purpose Input Output) gesteckt wird. In ein normales Gehäuse passt die Sandwich-Konstruktion in der Regel nicht. Sie benötigen ein Gehäuse mit einer Aussparung über den GPIO-Pins und Abstandsbolzen, auf denen sich das Display verschrauben lässt.



Stromsparende Anzeige: Ein E-Paper-Hat wird direkt auf die GPIO-Pins des Raspberry Pi gesteckt. Es eignet sich für die Anzeige von Benachrichtigungen oder Messwerten.

Für die kleinen Displays sind in der Regel spezielle Treiber erforderlich. Hersteller wie Waveshare (www.waveshare.com/wiki/) bieten in ihrem Wiki Links zum Treiberdownload sowie Raspbian-Images mit bereits integriertem Treiber. E-Paper-Displays lassen sich nur mit eigenen Programmen sinnvoll nutzen. Beispielcode in C++ und Python gibt es unter <https://github.com/waveshare/e-Paper>.

Mediacenter-PC fernbedienen

Die Mediacenter-Oberfläche Kodi (<https://libreelec.tv>) steuert man am bequemsten über eine Infrarot-Fernbedienung. Da die meisten TV-Geräte HDMI-CEC beherrschen, können Sie auch einfach die Fernbedienung des Fernsehers verwenden. Bei einigen Geräten müssen Sie die Funktion erst aktivieren. Weitere Infos dazu finden Sie im Handbuch des TV-Gerätes.

Sollte das nicht funktionieren oder wenn Sie den Raspberry Pi an einem PC-Monitor betreiben, können Sie die Infrarot-Fernbedienung Hama MCE Remote einsetzen (etwa 30 Euro). Der Infrarotempfänger wird per USB mit dem Raspberry Pi verbunden und die Fernbedienung ist sofort einsatzbereit.

Wer kein Geld ausgeben möchte, aber ein Smartphone besitzt, verwenden eine kostenlose App wie Kore (Official Remote for Kodi, www.pcwelt.de/M2BG6x) für das Android-Smartphone. Benutzer eines iPhones suchen im App Store nach „Official Kodi Remote“.

Baukästen, Sensoren und Aktoren

Der Raspberry kann Elektronikbauteile und den Einstieg in die Programmierung verbinden. Für circa 80 Euro gibt es Starterkits inklusive Raspberry Pi 3, die ein Steckbrett („Breadboard“), Verbindungskabel, Widerstände, Schalter und LEDs enthalten. Starterkits mit unterschiedlicher Ausstattung ohne Raspberry Pi kosten etwa zwischen 20 und 50 Euro. Teilweise sind bereits einige Sensoren enthalten, für die aber auch eigene Sensorkits in ähnlicher Preislage verfügbar sind.

Diese Sensoren messen Temperatur und Feuchtigkeit, es gibt aber auch Schallsensoren, Fotowiderstände, Hallsensoren, Flammensensoren und vieles mehr. Das Angebot wird mit Aktoren wie Berührungsschalter, Infrarotempfänger und -Sender, Potentiometer, Joystick und Display abgerundet.

Die Bauteile sitzen auf kleinen Platinen mit Steckkontakten und lassen sich über das Steckbrett mit dem Raspberry Pi verbinden. Wer nur ein spezielles Projekt verwirklichen möchte, kann alle genannten Bauteile auch einzeln erwerben. Meist kosten diese nur wenige Euro. Zum Ausprobieren muss man Sensoren auch nicht auf Platinen löten. Das Steckbrett reicht aus. Einen kleinen Überblick mit den 50 wichtigsten Sensoren und Modulen für den Raspberry Pi finden Sie über www.pcwelt.de/rpimod.

Es gibt direkte Links zu Shops, über die Sie die Bauteile beziehen können, Bilder vom Aufbau und Tutorials mit Programmierbeispielen. ■



Mediacenter: Mit einer Infrarotfernbedienung lässt sich Kodi komfortabel bedienen. Die Hama MCE Remote wird von Kodi automatisch erkannt und muss nicht konfiguriert werden.



Basteln mit dem Raspberry Pi: Starterkits bieten alle Bauteile für den Einstieg in die hardwarenahe Programmierung und Steuerung von Geräten. Sensorkits erweitern die Möglichkeiten.

RASPBERRY PI UND ZUBEHÖR ONLINE KAUFEN

Wer nach Raspberry-Zubehör sucht, wird am schnellsten im Internet fündig. Fast alle bekannten Onlinehändler haben die in diesem Beitrag genannten Geräte und Starterkits im Angebot.

Das breiteste Angebot findet man bei einem offiziellen „Raspberry Pi Approved Reseller“. Welche das sind, erfahren Sie auf www.raspberrypi.org/products nach der Produktauswahl („More info“) und Klick auf „Buy now“. Wählen Sie das gewünschte Modell und Land, um sich die Shops anzeigen zu lassen.

Der Raspberry Pi ist übrigens „Made in Wales“ und auch das Zubehör kommt teilweise aus Großbritannien. Im Moment ist noch nicht abzusehen, wie sich ein ungelegter Brexit auf die Preise auswirken wird. Wer direkt bei einem britischen Versender bestellt, muss dann mit Einfuhrsteuern rechnen. Durch Zoll, Steuer und längere Transportzeiten könnten sich die Produkte auch in deutschen Shops verteuern.



Videos konvertieren & bearbeiten

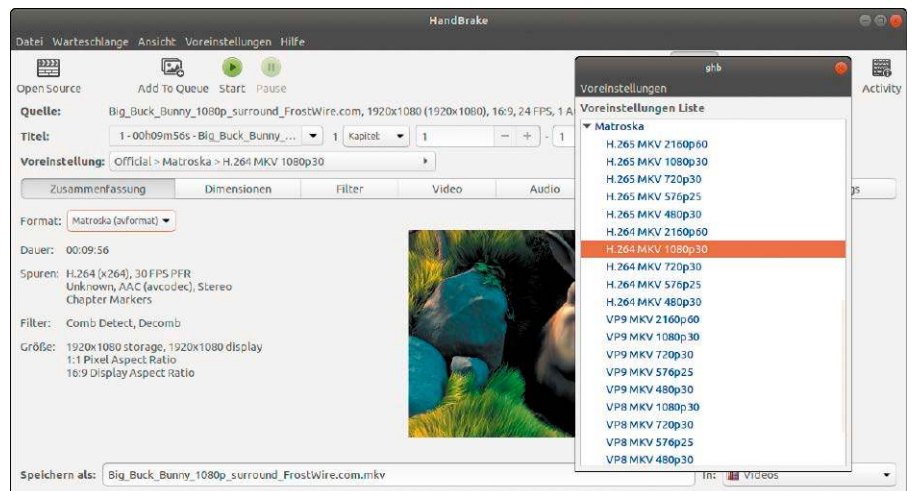
Videos sind oft zu groß für das Smartphone oder den USB-Stick. Geeignete Tools können die Größe reduzieren und den Inhalt bearbeiten. Eventuell werden nicht alle Tonspuren benötigt, andererseits fehlen vielleicht wichtige Untertitel.

VON THORSTEN EGGELING

Beim Umgang mit Videos stehen Sie häufig vor der Aufgabe, Tonspuren zu entfernen oder hinzuzufügen oder Untertitelspuren auszulesen und einzubauen. Für die endgültige Datei gilt es dann noch das richtige Format zu finden, wenn Sie diese über das Internet streamen oder einfach nur auf einem Datenträger weitergeben wollen. Zur Reduzierung der Größe lässt sich die Auflösung reduzieren und/oder die Komprimierung verbessern. Vor allem relativ große TV-Aufnahmen lassen sich effektiv verkleinern. Linux-Systeme lassen sich für alle genannten Aufgaben mit den passenden Tools ausstatten. Die gibt es mit grafischer Oberfläche, für die automatische Konvertierung aber auch für die Kommandozeile. **Service:** Eine ZIP-Datei mit allen Befehlszeilen und Scripts aus diesem Artikel laden Sie über www.pcwelt.de/vconv herunter.

1. Komprimierung von Video- und Audiostreams

Jede Komprimierungsmethode ist mit Qualitätsverlust verbunden. Die Entwickler der Algorithmen versuchen Bildinformationen wegzulassen, die das menschliche Auge ohnehin nicht sieht oder deren Fehlen nicht als störend empfindet. Der Trick besteht im Wesentlichen darin, nicht jedes Bild mit allen Informationen einzeln zu verwenden, sondern Referenzbilder in bestimmten Abständen zu verwenden und dazwischen nur die Unterschiede zu speichern. Werden dann noch die Auflösung und Bitrate reduziert, lässt sich ein Video stark verkleinern. Wie weit man dabei ge-



Platzsparende Umwandlung: Handbrake ist über die mitgelieferten Voreinstellungen schnell konfiguriert. Die Standardprofile lassen sich anpassen und unter anderen Namen speichern.

hen kann, hängt von den persönlichen Qualitätsansprüchen ab. Irgendwann ist der Punkt erreicht, an dem die Farben sehr kontrastarm erscheinen und das Bild verwaschen wirkt.

Bei Audiodateien lässt die Komprimierung Bereiche verschwinden, die das menschliche Ohr kaum wahrnimmt. Das sind beispielsweise besonders leise oder ähnliche Töne und hohe Frequenzen. Musik oder Filme enthalten in der Regel mindestens zwei (Stereo) oder sechs Audiokanäle (Surroundsound 5.1). Zwischen den Kanälen gibt es Überschneidungen und es spart Platz, nur die Differenzen zu speichern.

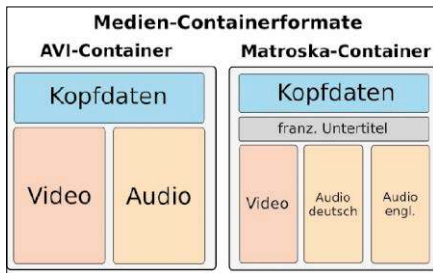
2. Video- und Audioformate

Bei Filmen begegnen Ihnen in der Regel die Containerformate MP4 und Matroska. Übliche Dateiendungen sind „.mp4“ oder „.m4v“, bei Matroska „.mkv“. MP4 ist ein

Industriestandard, was eine gewisse Sicherheit bei Geräten verspricht, die dieses Format offiziell unterstützen. Das Format ist aus Gründen der Kompatibilität auf bestimmte Video-, Audio- und Untertitelformate beschränkt.

Matroska ist deutlich flexibler und daher vorzuziehen. Es unterstützt die meisten Audio- und Videoformate. Die einst weit verbreiteten AVI-Container sind aufgrund der technischen Einschränkungen nur noch selten zu finden. AVI unterstützt beispielsweise keine Kapitelaufteilungen und nur Untertitel in Textform.

In einem Container werden die einzelnen Bestandteile des Films untergebracht, beispielsweise neben dem Video mehrere Tonspuren. Für die Videospur verwenden Sie in der Regel den H.264-Video codec (alias MPEG-4 AVC). Im Vergleich zu MPEG-2 (Video-DVD) arbeitet H.264 etwa dreimal effi-



Containerdateien: In AVI- oder MKV-Dateien stecken mehrere Streams mit unterschiedlicher Komprimierung. Die verwendeten Codecs sind entscheidend für die Dateigröße.

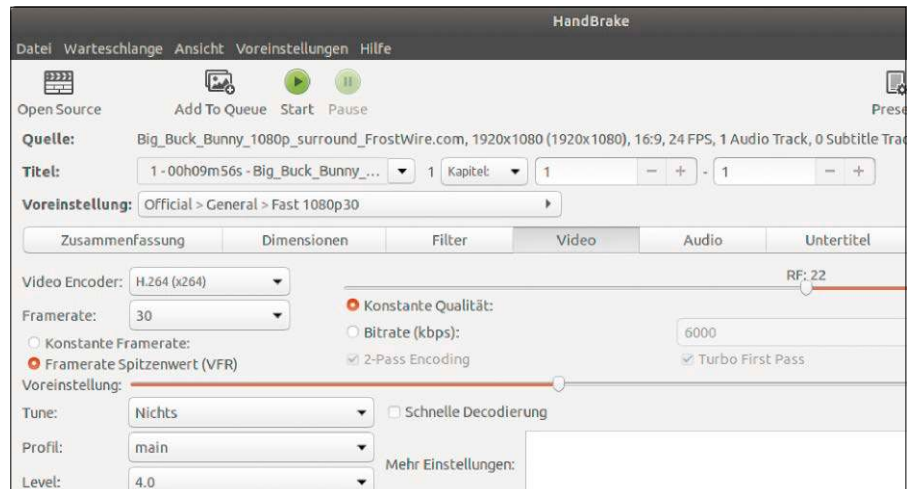
zienter. Bei gleicher Qualität schrumpft die resultierende Datei auf ein Drittel der MPEG-2-Größe. Allerdings ist der Rechenaufwand bei der Umwandlung größer. H.264 eignet sich auch für hochauflösende Videos; die meisten Grafikchips bieten dafür eine Hardwarebeschleunigung, um die Filme auch auf Geräten mit schwacher CPU ruckelfrei abzuspielen.

Alternativ verwenden Sie den Nachfolger H.265 (alias HEVC). Der ist noch effizienter als H.264, was die Dateigrößen um weitere 20 bis 25 Prozent verringern kann. Alle aktuellen Abspielprogramme unterstützen auch H.265, allerdings nicht jeder Grafikchip. Bei HD-Inhalten kann es daher zu Problemen bei der Wiedergabe kommen. Bei den Audiospuren ist MP3 (Lame-Encoder) erste Wahl, sofern Stereo ausreicht. Allerdings werden Sie die Spuren oft ohnehin nicht neu komprimieren, weil Sie die Multikanalformate AAC oder AC3 einfach direkt übernehmen können. Beide sind vor allem auf Video-DVDs zu finden.

TV-Aufnahmen (DVB) enthalten neben AC3 meist MPEG2-Stereospuren. Die Konvertierung in AAC oder MP3 ist hier sinnvoll, bewirkt aber keine besonders große Platzeinsparung.

3. Videos mit Handbrake konvertieren

Handbrake (<https://handbrake.fr>) unterstützt Videos in MP4- oder MKV-Containern. Als Videoencoder stehen beispielsweise H.264 und H.265 zur Verfügung, für Audio unter anderem AAC und MP3. Das Programm zeigt nach einem Klick auf „Presets“ eine Liste mit Voreinstellungen für unterschiedliche Qualitäten und Geräte. Experimentieren Sie mit verschiedenen Einstellungen, um das optimale Format für Ihr Gerät zu finden.



Videocodec wählen: In MP4- oder MKV-Containern verwenden Sie in der Regel den bewährten H.264-Codec. Sie können aber auch das neuere H.265 ausprobieren.

Sie können Handbrake (Paket: „handbrake“) aus dem Ubuntu-Standard-Repository installieren. Ubuntu 18.04 LTS bietet derzeit die Version 1.1.0 an. Über ein PPA lassen sich neuere Versionen installieren. Verwenden Sie zur Einrichtung die folgenden Terminalbefehle:

```
sudo add-apt-repository
  ppa:stebbins/handbrake-releases
sudo apt update
sudo apt install handbrake-gtk
  handbrake-cli
```

Für diesen Artikel haben wir Version 1.2.1 verwendet, die teilweise englischsprachige Beschriftungen zeigt.

Gehen Sie im Handbrake-Menü auf „Datei → Öffne Einzeldatei“ und wählen Sie die gewünschte Videodatei. Klicken Sie auf „Presets“ und stellen Sie im Fenster „Voreinstellungsliste“ das gewünschte Zielformat ein.

Über Schaltflächen wie „Dimensionen“, „Video“ oder „Audio“ erreichen Sie die detaillierten Einstellungen. Unter „Video“ können Sie beispielsweise den Videoencoder wechseln. Gehen Sie dann auf „Voreinstellungen → Speichern“, um die Änderungen der Voreinstellungen unter einem anderen Namen zu sichern. Sehen Sie bei „Audio“ nach, ob Handbrake alle gewünschten Tonspuren berücksichtigt hat. Andernfalls klicken Sie auf „Alle hinzufügen“. Entsprechend verfahren Sie unter „Untertitel“ mit den Untertitelspuren (siehe Punkt 5). Im unteren Bereich des Fensters tippen Sie den Dateinamen für die Zieldatei ein, hinter „In:“ wählen Sie den Ordner. Mit Klick auf „Start“ beginnt dann die Umwandlung. Handbrake kann auch Inhalte von Video-DVDs (ohne Kopierschutz) verarbeiten. Gehen Sie dazu auf das Menü „Datei → Öffne

VIDEODATEIEN ANALYSIEREN

Über die Art der Audio- und Videokomprimierung sagt der verwendete Container wie MP4 oder Matroska zunächst nichts aus. Auch eine Transportstreamdatei (meist „.ts“ oder „.m2t“), wie Sie bei TV-Aufnahmen entsteht, kann mehrere unterschiedlich komprimierte Spuren enthalten. Für eine schnelle Untersuchung des Inhalts eignen sich der VLC Mediaplayer oder der Smplayer.

Öffnen Sie in VLC die Datei, die Sie analysieren wollen, und gehen Sie auf „Werkzeuge → Codec-Informationen“. Sie erhalten eine Übersicht mit den enthaltenen Spuren, der Videoauflösung, der Bildwiederholrate und den verwendeten Codecs. In Smplayer rufen Sie die Daten über „Anzeigen → Informationen und Eigenschaften“ ab. Wer es noch genauer wissen will, installiert das Paket Mediainfo (in Synaptic: „mediainfo-gui“). Wenn Sie damit eine Videodatei öffnen und auf „View → Text“ gehen, gibt das Tool unter anderem auch Auskunft über die Art der enthaltenen Untertitelstreams sowie deren IDs und der Teletext-Seiten – sofern vorhanden (siehe Punkt 5).

Quelldateien“ und wählen Sie das Verzeichnis auf der Festplatte, in dem die für DVDs typischen Ordner „AUDIO_TS“ und „VIDEO_TS“ liegen. Entsprechend können Sie auch ein Verzeichnis angeben, in dem mehrere Videodateien liegen, etwa Mitschnitte einer TV-Serie. Klicken Sie auf „Start“, wenn Sie nur eine Datei oder eine DVD umwandeln wollen. Andernfalls gehen Sie im Menü auf „Warteschlange → Mehrere hinzufügen“, setzen ein Häkchen bei allen oder den gewünschten Titeln, bestätigen mit „OK“ und klicken dann auf „Start“.

4. Videos mit Handbrake CLI konvertieren

Handbrake bringt das Kommandozeilen-Tool Handbrake CLI mit, das Sie für einzelne Dateien oder zur automatischen Konvertierung eines ganzen Ordners mit Videodateien verwenden können. Für die Umwandlung mehrerer Dateien verwenden Sie ein Shell-Script. Sie finden es unter dem Namen „hb_convert.sh“ im Download zu diesem Artikel (www.pcwelt.de/vconv).

Kopieren Sie die Datei in Ihr Home-Verzeichnis. Dann öffnen Sie das Script in einem Editor und tragen hinter „PRESET=“ die gewünschte Voreinstellung ein. Ändern Sie die Angabe hinter „CONTAINER=“ auf „mp4“, wenn Sie MP4- statt MKV-Dateien bevorzugen.

Starten Sie dann das Script im Terminal:

```
~/hb_convert.sh [Pfad] [Ext]
```

Für den Platzhalter „[Pfad]“ setzen Sie den Pfad zum Ordner mit den Quelldateien ein. „[Ext]“ kann optional eine Dateinamenserweiterung (ohne Punkt) als Filter enthalten. Fehlt die Angabe, verarbeitet das Script alle gefundenen Dateien. Die konvertierten Dateien liegen danach im gleichen Ordner wie die Quelldateien und tragen ein „_1“ im Namen.

5. Untertitel auslesen und importieren

Handbrake bindet Untertitel nicht automatisch ein. Gehen Sie daher auf „Untertitel“ und klicken Sie auf „Hinzufügen“, um einzelne Untertitel zu laden, oder auf „Alle Hinzufügen“, um alle zu laden. Sollte Handbrake keine Untertitel finden, dann sind keine vorhanden oder das Format wird nicht unterstützt. Das Tool kann nur mit Untertiteln umgehen, wie sie bei DVD-Kopien (VOB-Dateien) oder MKV-Dateien zu finden sind. Mediainfo (siehe Kasten „Video-

```

Öffnen  *hb_convert.sh  Speichern
if [ -z "$1" ]; then
TRANSCODEDIR="." # aktuelles Verzeichnis verwenden
else
TRANSCODEDIR="$1" # Verzeichnis aus dem ersten Parameter
fi
if [ -z "$2" ]; then
EXTENSION="*" # oder EXTENSION="*.mp4" EXTENSION="*.mkv"
else
EXTENSION="$2" # Erweiterung aus dem zweiten Parameter
fi
# Dateien ermitteln und konvertieren
find "$TRANSCODEDIR"/* -type f -name "*, $EXTENSION" | while read line; do
echo "|usr/bin/HandBrakeCLI -i "$line" -o "${line%.*}_1.$CONTAINER" --
preset-import-gui --preset="$PRESET"
done
sh  Tabulatorbreite: 8  Z. 21, Sp. 37  EINF

```

Massenumwandlung: Handbrake CLI kann per Script (Ausschnitt) Videos automatisiert konvertieren. Laden Sie das Script über www.pcwelt.de/vconv herunter.

dateien analysieren“) meldet hier beispielsweise Formate wie „DVD-Video“ (Vobsub) oder „S_Text“. Mit „DVB Subtitle“ oder „Teletext“ kann Handbrake nichts anfangen. Mit Ccextractor (www.ccextractor.org) lassen sich Untertitelspuren aus Videodateien kopieren und dann für ein Video mit Handbrake wieder einbauen. Da die Untertitel etwa bei TV-Aufnahmen („DVB Subtitle“) nicht als Text sondern als Abfolge von Bildern vorliegen, muss der Text per OCR erkannt werden.

Zur Zeit gibt es kein PPA für Ccextractor, sodass Sie es selbst kompilieren müssen. Installieren Sie zuerst die nötigen Entwicklungstools (eine Zeile):

```

sudo apt install gcc git autoconf
pkg-config build-essential
tesseract-ocr libtesseract-dev
libleptonica-dev libcurl4-gnutls-dev
libglfw3 libglfw3-dev libglew-dev
libglew2.0 libxinerama-dev
libxcursor-dev libxi-dev
libavcodec-dev libavformat-dev
libswscale-dev

```

Installieren Sie ferner einige Trainingsdateien für die OCR-Software Tesseract (Deutsch, Französisch, Englisch):

```

sudo apt install tesseract-ocr-deu
tesseract-ocr-fra tesseract-ocr-eng

```

Schließlich erstellen Sie ein Arbeitsverzeichnis, laden den Quellcode herunter und kompilieren das Programm:

```

mkdir ~/src
cd ~/src
git clone https://github.com/CCExtractor/ccextractor.git
cd ccextractor/linux
./autogen.sh
./configure --enable-hardsubx
--enable-ocr --with-gui
make -j4
sudo make install

```

Mit der letzten Zeile installieren Sie Ccextractor in „/usr/local/bin“.

Das Tool lässt sich in den meisten Fällen einfach einsetzen. Der Auftrag `ccextractor [Video-Datei]` sucht nach allen verfügbaren Untertiteln und speichert diese mit der Endung „.srt“ im Ordner des Videos. Den Platzhalter „[Video-Datei]“ ersetzen Sie durch Pfad und Namen der gewünschten Datei. Die Umwandlung funktioniert nicht immer zuverlässig, was aber nicht die Schuld von Ccex-

Was steckt in der Datei? Mediainfo gibt Auskunft zu den Audio-, Video- und Untertitelspuren. Sie erfahren auch, um welche Art von Untertitelstreams es sich handelt.



tractor ist. Vor allem DVB-T/T2-Aufnahmen melden manchmal Teletext-Untertitelspuren, die aber keinen Inhalt haben.

Öffnen Sie die Videodatei im Player VLC und wählen Sie über „Untertitel → Untertiteldatei hinzufügen“ die gewünschte „srt“-Datei aus. Wenn alles passt, bauen Sie die Untertitel mit Handbrake in das Video ein. Dazu gehen Sie auf „Untertitel“ und klicken auf „Hinzufügen“. Stellen Sie die Sprache ein und öffnen Sie hinter „Datei“ die „srt“-Datei. Mit „OK“ und „Start“ beginnt die Konvertierung.

Tipp: Untertiteldateien im „srt“-Textformat finden Sie im Internet auf www.opensubtitles.org. Im Smplyer können Sie über „Untertitel → Untertitel auf opensubtitles.org suchen“ eine Datei für das gerade geladene Video herunterladen, sofern sich diese im Angebot befindet.

6. Videos mit Avidemux bearbeiten

Videoaufnahmen von einem TV-Receiver enthalten in der Regel den kompletten DVB-Transportstrom inklusive Videotext und mehreren Tonspuren. Die Größe der Dateien lässt sich reduzieren, indem Sie nur den Videostream und die gewünschte Tonspur extrahieren. Bei dieser Gelegenheit können Sie auch gleich Werbung oder Übergänge am Anfang und Ende der Aufnahme entfernen.

Mit Avidemux (www.avidemux.org) schneiden Sie Videodateien, speichern Audio- und Videostreams oder wandeln Dateien in andere Formate um. Anders als der Name vermuten lässt, kann das Tool auch mit MKV- oder MP4-Containern umgehen. Installieren Sie Avidemux über ein PPA (Personal Package Archive). Dazu verwenden Sie die folgenden drei Terminalbefehle:

```
sudo add-apt-repository
  ppa:ubuntuhandbook1/avidemux
sudo apt update
sudo apt install avidemux2.7-qt5
  avidemux2.7-qt5-data avidemux2.7-
  plugins-qt5 avidemux2.7-jobs-qt5
```

Danach starten Sie Avidemux, gehen auf „Datei → Öffnen“ und wählen die gewünschte Videodatei aus. Über die Bedienelemente am unteren Fensterrand spielen Sie das Video ab oder navigieren an eine bestimmte Position. Verwenden Sie die Pfeiltasten für eine framegenaue Positionierung. Per Klick auf die „A“-Schaltfläche setzen Sie eine Anfangsmarkierung und

```
te@Z77X: ~/Videos
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
Opening file: Tagesthemen.m2t
File seems to be a transport stream, enabling TS mode
Analyzing data in general mode
VBI/teletext stream ID 4116 (0x1014) for SID 769 (0x301)
- Programme Identification Data = ARD - Das Erste
- Universal Time Co-ordinated = Fri Aug 30 21:58:48 2019
Notice: Teletext page with possible subtitles detected: 150
- No teletext page specified, first received suitable page is 150, not guaranteed
Notice: Teletext page with possible subtitles detected: 775
Notice: Teletext page with possible subtitles detected: 799
100% | 01:36
Teletext decoder: 2406 packets processed

Number of NAL_type_7: 0
Number of VCL_HRD: 0
Number of NAL_HRD: 0
Number of jump-in-frames: 0
Number of num_unexpected_sei_length: 0
```

Untertitel auslesen: Teletext-Untertitel sind als Bildstreams enthalten. Ccextractor wandelt die Bilder per OCR in Text um, den Sie dann mit Handbrake als Untertitelstream einbauen.

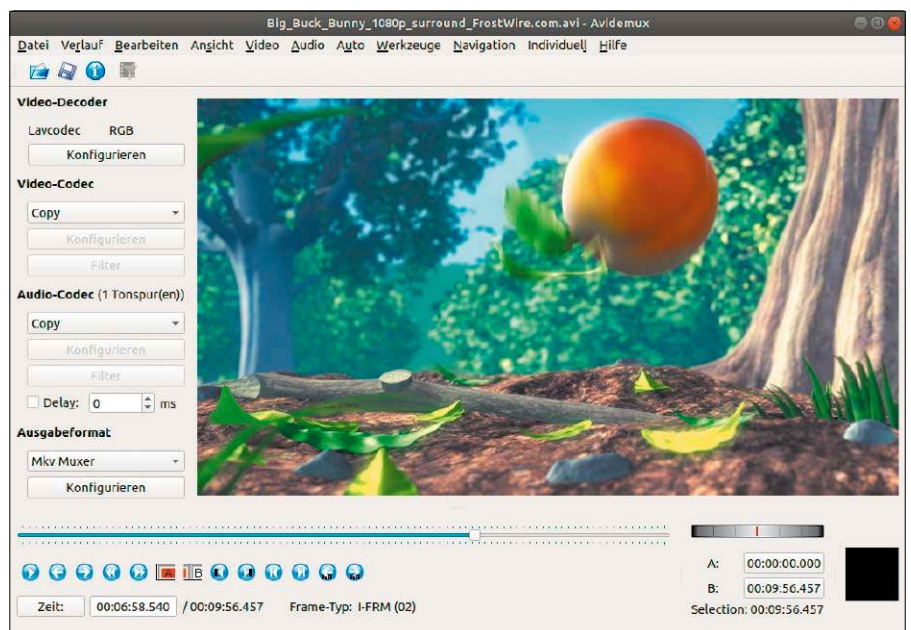
über „B“ eine Endmarkierung, beispielsweise bei einer Werbeunterbrechung. Gehen Sie im Menü auf „Bearbeiten → Löschen“, um den Bereich zwischen diesen Schnittmarken zu entfernen. Sollte sich unerwünschtes Material nur vor und hinter dem Film befinden, setzen Sie die Markierungen an Anfang und Ende des gewünschten Bereiches. Avidemux speichert nur den Bereich, der markiert ist.

Dann gehen Sie auf „Audio → Tonspuren wählen“ und entfernen die Häkchen vor den Tonspuren, die Sie nicht benötigen. Im linken Bereich des Fensters stellen Sie un-

ter „Audio-Codec“ und „Video-Codec“ jeweils „Copy“ ein. Unter „Ausgabeformat“ wählen Sie „MKV Muxer“.

Mit Klick auf die Schaltfläche „Video speichern“ erstellen Sie eine neue Videodatei ohne die überflüssigen Szenen. Avidemux arbeitet im Copymodus sehr schnell, weil das Tool die Streams nur in die Containerdatei kopieren muss.

Wenn Sie die Aufnahmen verkleinern wollen, ist eine Neucodierung erforderlich. Die können Sie mit Avidemux durchführen, indem Sie unter „Video- und Audio-Codec“ ein anderes Format wählen. ■



Video bearbeiten: Avidemux ist ein einfacher Videoschnitteditor, der sich auch für MP4- und Matroska-Container eignet. Ohne Neukomprimierung arbeitet das Tool sehr schnell.

CDs, DVDs und ISO-Dateien

ISO-Dateien spielen bei Linux-Livesystemen eine wichtige Rolle, aber auch bei Sicherungskopien von Video-DVDs. Mit den richtigen Linux-Werkzeugen lassen sich ISO-Dateien bearbeiten und DVDs kopieren.

VON THORSTEN EGGELING

CDs und DVDs spielen zwar eine zunehmend geringere Rolle, für ISO-Dateien gibt es aber nach wie vor wichtige Einsatzbereiche. Linux-Distributionen werden meist als ISO-Dateien ausgeliefert, die sich nicht nur für bootfähige DVDs eignen, sondern auch für den USB-Stick. Bei Bedarf können Sie eigene Dateien in ein ISO einbauen oder es mit individuellen Einstellungen neu zusammensetzen. ISO-Dateien lassen sich auch in den Grub-Bootloader einbinden und von der Festplatte starten. Ein Multiboot-Stick mit mehreren ISOs ist ebenfalls möglich.

Da nicht jeder Videos über das Internet streamt oder Musik als MP3 konsumiert, gibt es weiterhin klassische Aufgaben für CDs und DVDs. In vielen Haushalten ist immer noch ein DVD-Abspieler zu finden, der Audio-CDs und Video-DVDs wiedergeben oder Diashows zeigen kann. Mit geeigneten Tools lassen sich auch unter Linux dafür Medien erstellen.

Nicht zu vergessen sind auch die CDs und DVDs, die vielleicht schon seit einigen Jahren auf dem Dachboden liegen. Wenn sich darunter unwiederbringliche Schätze verbergen, sollten Sie an eine Sicherungskopie denken.



ISOs und DVD unter Linux: Das Brennprogramm Brasero kann CDs und DVDs kopieren. Das Ziel kann sowohl eine ISO-Datei sein als auch der typische DVD-Rohling.

Service: Eine ZIP-Datei mit allen Befehlszeilen und dem Script aus diesem Artikel laden Sie über www.pcwelt.de/ZdTwEa herunter.

1. ISO-Dateien analysieren

Was tatsächlich in einer ISO-Datei steckt, finden Sie mit

```
file [Dateiname.iso]
```

heraus. Den Platzhalter ersetzen Sie durch den Namen der zu untersuchenden Datei und gegebenenfalls zusätzlich mit dem kompletten Pfad. Beim ISO einer bootfähigen Linux-Distribution gibt das Tool beispielsweise folgendes aus:

```
DOS/MBR boot sector; partition 2 :
ID=0xef, start-CHS
(0x3ff, 254, 63), end-CHS
(0x3ff, 254, 63), startsector 652,
4672 sectors
```

Informationen zu den Partitionen holen Sie mit dieser Zeile ein:

```
fdisk -l [Dateiname.iso]
```

„DOS/MBR boot sector“ kommt zum Einsatz, wenn Sie den Inhalt der ISO-Datei mit dd auf einen USB-Stick kopieren. Fdisk meldet zwei Partitionen, die erste und größere mit dem Typ „Leer“. Das ist die Partition auf der DVD, die Sie im Dateimanager

sehen und die das Dateisystem ISO 9660 enthält, was Fdisk aber nicht anzeigen kann. Danach folgt eine kleine Partition für den Uefi-Bootloader.

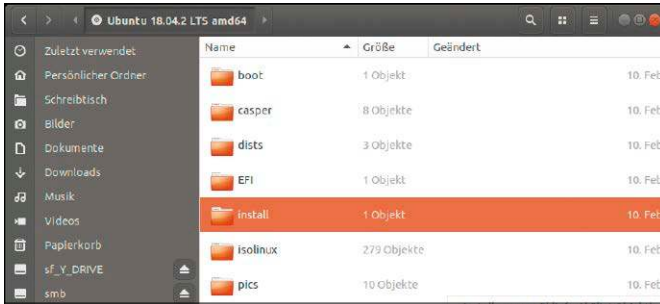
Beim Abbild einer Video-DVD meldet file in der Regel „UDF filesystem data“ (Universal Disk Format). UDF bietet im Vergleich zu ISO 9660 längere Dateinamen und tiefere Verzeichnisbäume. Aus Gründen der Kompatibilität ist auch bei UDF-DVD meist zusätzlich ein ISO-9660-Dateisystem enthalten.

2. ISO einer Linux Live-DVD anpassen

Der Inhalt einer ISO-Datei lässt sich im Dateimanager über das Kontextmenü entpacken („Hier entpacken“) oder in das Dateisystem einhängen („Öffnen mit → Einhängen von Laufwerksabbildern“). Im Terminal verwenden Sie beispielsweise

```
sudo mkdir /mnt/iso
sudo mount -o loop [ISO-Datei] /mnt/iso
```

„[ISO-Datei]“ ersetzen Sie durch den Namen beziehungsweise den kompletten Pfad zur ISO-Datei. Für unser Beispiel verwenden wir die Datei „ubuntu-18.04.2-desktop-amd64.iso“ von Ubuntu 18.04.



Kopieren Sie alle Ordner und Dateien von „/mnt/iso“ in ein Arbeitsverzeichnis, etwa nach „~/work“. Fügen Sie Dateien hinzu oder verändern Sie Konfigurationsdateien. Dazu ein Beispiel: Im Uefi-Modus startet Ubuntu mit einer englischsprachigen Oberfläche. Um das zu ändern, öffnen Sie die Grub-Konfigurationsdatei:

```
cd ~/work/boot/grub
```

```
sudo gedit grub.cfg
```

Bauen Sie in die Abschnitte „Try Ubuntu without installing“ und „Install Ubuntu“ jeweils vor „--“ abgetrennt durch ein Leerzeichen diese Zeichenfolge ein:

```
debian-installer/language=de
console-setup/layoutcode?=de
```

Danach speichern Sie die Datei.

ISO erstellen: Ein ISO-Datei inklusive El Torito, Isolinux und Grub erfordert eine komplexe Befehlszeile. Anhaltspunkte dafür, wie die originale ISO-Datei erstellt wurde, liefert das Tool Xorriso (Installation über das gleichnamige Paket). Die Befehlszeile

```
xorriso -report_about warning
-indev ~/Downloads/ubuntu-
```

18.04.2-desktop-amd64.iso

```
-report_system_area as mkisofs
```

liefert grundlegende Informationen. Passen Sie Pfad und Dateinamen an. Kopieren Sie dann die Ausgabe des Tools für ein Bash-Script in einen Texteditor. Es handelt sich um nur eine Befehlszeile. Wegen der besseren Lesbarkeit fügen Sie am Ende jeder Zeile ein „\“ an. Die Bash-Shell interpretiert dann alle Zeilen zusammenhängend. Ein paar Details sind noch zu ergänzen, etwa „xorriso -as mkisofs“ (der Aufruf des Tools) und „-joliet“ (Dateisystem für Windows-Systeme) am Anfang und „-o Ubuntu.iso work“ am Ende. Hinter „-o“ steht der Name der Zieldatei und „work“ ist unser Arbeitsverzeichnis. Das Ergebnis sieht dann in etwa so aus wie in der Abbildung rechts oben (das Script „remaster_iso.sh“ ist auch im Download zu diesem Artikel enthalten). Die Zeile „--interval“ enthält Verweise auf die ISO-Datei, aus der Xorriso die Informationen gewonnen hat. Darüber wird der MBR-Bootsektor aus der ISO-Datei eingebunden. Um davon unabhängig zu sein, installieren Sie das Paket „isolinux“. Die

ISO-Inhalt kopieren:

Den Inhalt der ISO-Datei kopieren Sie in einen beliebigen Ordner, in dem Sie Dateien bearbeiten. Aus dem Ordner erstellen Sie dann eine neue ISO-Datei.



Komplexe Befehlszeile: Für Linux-DVDs sind zahlreiche Optionen erforderlich, um aus einem Ordner mit Dateien ein bootfähiges ISO-Abbild zu erzeugen.

Zeile im Script lautet dann so:

```
-isohybrid-mbr /usr/lib/ISOLINUX/
isohdpxf.bin
```

Die Zeile „--interval [...]“ kann dann entfallen. Zur Prüfung starten Sie den Befehl `xorriso -indev [Boot-DVD.iso] -toc` und ersetzen dabei „[Boot-DVD.iso]“ durch die Datei der Original-DVD, und bei einem zweiten Aufruf verwenden Sie das selbst erstellte ISO. Die Ausgaben sollten in den meisten Punkten übereinstimmen.

3. ISOs für Daten-DVDs neu erstellen

Ein ISO-Abbild lässt sich unter jedem PC-Betriebssystem ohne zusätzliche Software öffnen beziehungsweise in das Dateisystem

ISO VON FESTPLATTE ODER USB-STICK BOOTEN

ISO-Dateien lassen sich in das Grub-Menü des installierten Systems einbauen. Das ist praktisch, wenn Sie etwa ein Livesystem regelmäßig als Surfsystem verwenden oder ein Rettungssystem benötigen. Installieren Sie unter Ubuntu 18.04 oder Linux Mint 19 das Paket „grml-rescueboot“. Danach erstellen Sie einen Ordner, der die ISO-Dateien aufnehmen soll:

```
sudo mkdir /boot/grml
```

Kopieren Sie die gewünschten ISO-Dateien in diesen Ordner und führen Sie danach

```
sudo update-grub
```

aus.

Wenn Sie ISO-Dateien von einem USB-Stick booten möchten, verwenden Sie das Tool Multisystem, für das Sie einen FAT32-formatierten USB-Stick benötigen. Zu Installation verwenden Sie diese vier Zeilen:

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

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

tem einhängen. Es eignet sich daher gut für ein Backup abgeschlossener Projekte, da sich das ISO-Abbild nicht ändern lässt. Mit einem Brennprogramm wie Brasero ist die Aufgabe ganz einfach. Installieren Sie das Tool über die Paketverwaltung von Ubuntu oder Linux Mint und starten Sie es. Dann klicken Sie auf „Daten-Projekt“ und ziehen den Ordner der Dateisammlung in das Brasero-Fenster. Nachdem Brasero die Projektgröße errechnet hat, klicken Sie rechts unten auf „Brennen“, vergeben den Namen für die ISO-Datei und klicken auf „Abbild erstellen“.

Wer solche Backups automatisieren möchte, kann auch die Kommandozeile benutzen. Die Befehlszeile

```
genisoimage -o ~/home.iso -R -J ~/
Dokumente
```

erstellt beispielsweise die Datei „home.iso“ im eigenen Home-Verzeichnis („~“).

4. Video-DVDs abspielen und kopieren

Bevor Sie Video-DVDs abspielen können, müssen Sie unter Ubuntu 18.04 oder Linux Mint 19 ein zusätzliches Paket installieren. Im Terminalfenster verwenden Sie den folgenden Befehl:

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

Die angezeigten Meldungen bestätigen Sie mit „OK“ beziehungsweise „Ja“. Nach der Installation und dem 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 (Paket: „vlc“).

Wenn die Wiedergabe funktioniert, lässt sich die DVD auch kopieren. Dazu installieren Sie zuerst das Tool Dvdbackup:

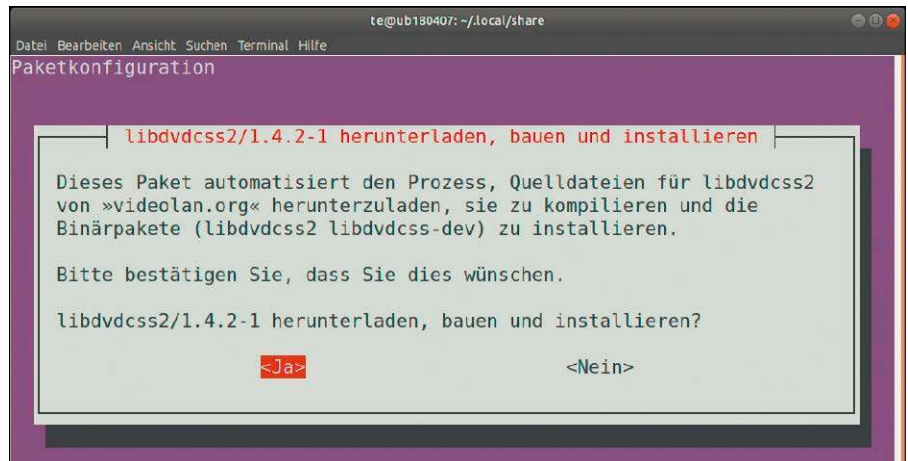
```
sudo apt install dvdbackup
```

Für ein vollständiges Backup des DVD-Inhalts verwenden Sie diese Befehlszeile:

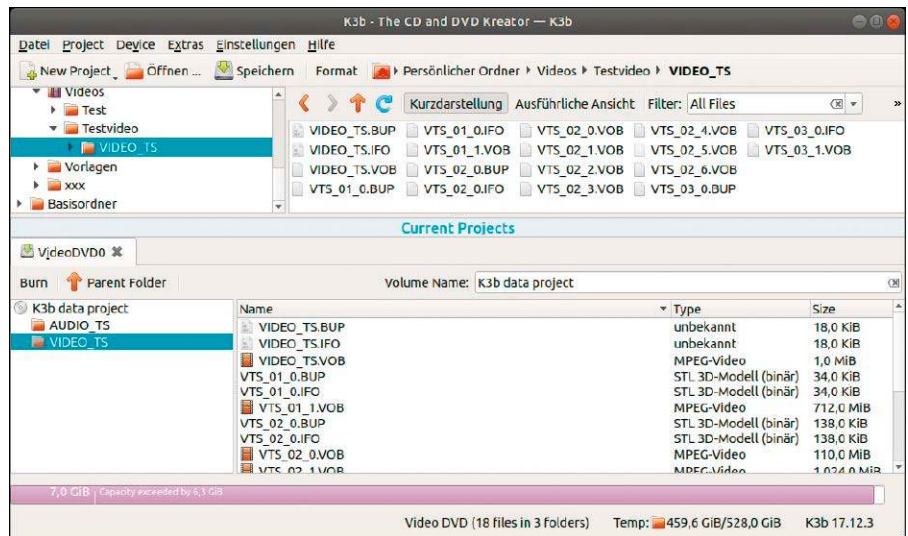
```
dvdbackup -i /dev/dvd -p -o
```

```
[Zielpfad] -M
```

Für den Platzhalter „[Zielpfad]“ setzen Sie einen Ordernamen ein, beispielsweise „~/Videos“. Der Standard-Gerätepfad „/dev/dvd“ sollte vorhanden sein und verweist auf das erste DVD-Laufwerk. Sie können aber auch „/dev/sr0“ oder „/dev/sr1“ für das erste beziehungsweise zweite DVD-Laufwerk verwenden. Sobald Dvdbackup seine Arbeit abgeschlossen hat, finden Sie



Ungewöhnliche Paketinstallation: Das Paket „libdvd-pkg“ lädt nur den Quellcode herunter. Die Binärdateien werden danach individuell auf Ihrem PC erstellt.



Brennen mit K3b: Das KDE-Programm bietet zahlreiche Funktionen und kann als Backup auch Video-DVDs aus einem „VIDEO-TS“-Ordner auf der Festplatte erstellen.

im Zielverzeichnis einen Ordner, der die Bezeichnung der DVD trägt. Darin liegt das Verzeichnis „VIDEO_TS“ mit den VOB-Dateien der Videos. Der Inhalt des Ordners lässt sich direkt abspielen, indem Sie ihn vom Dateimanager auf das geöffnete Fenster des VLC-Player ziehen.

Die Dateien können Sie mit Handbrake auch in ein anderes Format konvertieren, beispielsweise MP4 oder Matroska (siehe Artikel ab Seite 68). Um aus den kopierten Dateien wieder eine DVD zu erzeugen, genügt diese Befehlszeile:

```
mkisofs -dvd-video -udf -v "[Name]"
-o ~/[Name].iso [Video-Ordner]
```

Für den Platzhalter „[Name]“ setzen Sie die Bezeichnung der DVD ein. „[Video-Ordner]“ steht für den Pfad, in dem der Ordner „VIDEO_TS“ mit den VOB-Dateien liegt.

Grafische Oberfläche nutzen: Verwenden Sie dafür das meist vorinstallierte Brasero. Brasero ist primär ein Brennprogramm, kann aber auch CDs oder DVDs in Abbilddateien kopieren. Für Video-DVDs ist die Installation des Pakets „libdvd-pkg“ Voraussetzung, wie oben beschreiben. Legen Sie die Video-DVD ein und starten Sie Brasero. Klicken Sie auf „CD/DVD kopieren“. Unter „Wählen Sie die zu beschreibende CD/DVD aus“ verwenden Sie die Option „Abbilddatei“. Per Klick auf „Eigenschaften“ lassen sich Name und Pfad ändern. Klicken Sie dann auf „Abbild erstellen“. Die resultierende ISO-Datei ist ein Abbild der Original-DVD, allerdings keine ganz exakte Kopie. Die ISO-Datei lässt sich daher auch auf anderen PCs ohne installiertem „libdvd-pkg“ abspielen.

Ziehen Sie die Datei einfach auf das geöffnete VLC-Fenster. Eine neue DVD als Sicherungskopie lässt sich daraus ebenfalls erstellen. Verwenden Sie dafür in Brasero die Schaltfläche „Abbild brennen“.

Aus dem Ordner „VIDEO_TS“ lässt sich mit Brasero keine DVD brennen oder ISO-Datei erstellen. Dafür benötigen Sie k3b, das Sie über das gleichnamige Paket installieren.

5. Audio-CDs kopieren

Musik-CDs liegen in einem gänzlich anderen Format vor als Daten- oder Video-DVDs. In der ursprünglichen Form enthält eine Audio-CD nur unkomprimierte Audiodaten, die einzelnen Spuren sind durch eine kleine Pause voneinander getrennt. Auf der CD lassen sich auch Zusatzinformationen unterbringen, etwa Texte mit Infos zu Titel oder Interpret sowie die Namen der Musikstücke. Einige Player etwa in Autoradios können diese Infos anzeigen.

Es ist am einfachsten, die Audiodateien von der CD zu lesen und in ein anderes Format zu konvertieren. Dafür können Sie das Tool Ripperx einsetzen. Die Installation `sudo apt install ripperx flac lame` ergänzen Sie durch die Pakete „flac“ (verlustlose Konvertierung in Flac-Dateien) und „lame“ (Konvertierung in MP3-Dateien).

Nach dem Start des Tools klicken Sie zuerst auf „Config“. Auf der Registerkarte „Allgemein“ stellen Sie die Zielverzeichnisse für die WAV- und MP3-Dateien ein. Auf der Registerkarte „MP3“ stellen Sie „Lame MP3 encoder“ oder „FLAC encoder“ ein. Speichern Sie die Änderungen per Klick auf „OK“. Legen Sie eine Audio-CD ein und klicken Sie auf „CDDB“. Wenn die CD in der Datenbank enthalten ist, werden nach kurzer Zeit die Beschriftungen gefüllt. Klicken Sie zum Abschluss auf „Go!!!“.

6. 1:1-Kopien von Audio-CDs

Von Audio-CDs lassen sich auch originalgetreuen Kopien des kompletten Datenträgers erstellen. Dafür sind jedoch mehrere Tools und Umwege erforderlich. Eine Kopie lässt sich dann mit folgendem Befehl erstellen:

```
cdrdao read-cd --read-raw --device /dev/sr0 --driver generic-mmc:0x20000 --paranoia-mode 0 --datafile image.bin image.toc
```

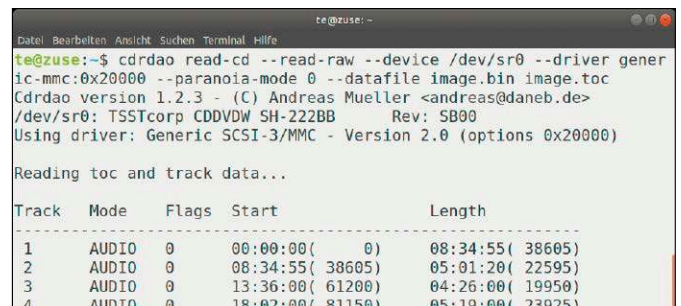
„image.bin“ enthält alle Tracks von der CD und „image.toc“ ein Inhaltsverzeichnis mit Zeitangaben, wo diese Tracks zu finden



Sicherheitskopie für Audio-CDs: Ripperx liest die Audio-CD ein und ermittelt per CDDB-Abfrage Informationen zu Interpret, Album und Musiktiteln. Die Titel lassen sich als MP3 speichern.

Kopie des Originals:

Cdrdao speichert den Inhalt einer Audio-CD in einer einzelnen Daten-datei. Daraus lässt sich eine neue Audio-CD mit den gleichen Eigenschaften erstellen.



sind. Mit der Zeile `toc2cue image.toc image.cue` erstellen Sie eine „cue“-Datei mit den gleichen Zeitangaben, nur in einem anderen Format. Die Tools cdrdao und toc2cue sollten bei Ubuntu standardmäßig installiert sein. Wenn nicht, rüsten Sie das Paket „cdrdao“ nach.

Ob die Datei „image.bin“ tatsächlich alle Daten der Audio-CD enthält, lässt sich nicht auf die Schnelle prüfen. Das Abbild lässt sich unter Linux von Haus aus nicht einbinden und die „bin“-Datei auch nicht in VLC abspielen. Sie benötigen zusätzlich das Tool cdmu, das sich über ein PPA installieren lässt (drei Zeilen):

```
sudo add-apt-repository ppa:cdemu/ppa
sudo apt-get update
sudo apt install cdmu-daemon cdmu-client gcdemu
```

Mit dieser Zeile erstellen Sie dann ein virtuelles CD-Laufwerk für die „cue“-Datei:

```
sudo cdmu load 0 image.cue
```

Mit

```
sudo cdmu device-mapping
```

ermitteln Sie, unter welchem Gerätepfad es erreichbar ist, beispielsweise „/dev/sr1“.

Das virtuelle Laufwerk taucht zwar im Dateimanager auf, zeigt aber nicht wie bei der originalen Audio-CD die Tracks an. Dass das Abbild dennoch vollständig ist, beweist folgender Befehl:

```
cdparanoia -d /dev/sr1 -vsQ
```

Sie sehen nun alle zuvor kopierten Audio-tracks. Die Tracks lassen sich außerdem mit `cdparanoia -d /dev/sr1 -B` als WAV-Dateien auslesen. Ripperx kann ebenfalls mit dem virtuellen CD-Laufwerk umgehen. Sie müssen nur über „Config“ auf der Registerkarte „Wav“ hinter „Zusatzoptionen“ den Parameter „-d“ und den Gerätepfad eintragen:

```
-d /dev/sr1
```

Die virtuelle CD lässt sich dann wie oben beschrieben rippen. Eine Sicherungskopie der Audio-CD brennen Sie bei Bedarf mit dieser Befehlszeile

```
sudo cdrdao write --device /dev/sr0 --driver generic-mmc --buffers 128 --speed 8 image.toc
```

auf einen Datenträger. ■

Spieleklassiker unter Linux

Wer einst geliebte Spieleklassiker unter Linux neu entdecken will, erreicht das mühelos mit guten Spezialangeboten. Nur bei aktuellen Spielertiteln muss man etwa den Streamingdienst Steam nutzen.

VON STEPHAN LAMPRECHT

Spätestens mit der Ankündigung von Google, mit Stadia in das Streaming von Spielen einsteigen zu wollen, ist klar, wohin die Reise beim Gaming gehen wird: Zocken ohne Konsole oder hochgezüchtete Spielerechner – die Cloud macht es möglich. Aber was ist mit Klassikern, die einem vor Jahren Spaß gemacht haben? Wir zeigen Ihnen, wie Sie legendäre Spiele unter Linux zum Leben erwecken.

GOG – „Good Old Games“

Die Spieleindustrie kennt legendäre Titel. Das Strategiespiel *Command & Conquer*, die Aufbausimulation *Civilization* und Shooter aus dem Hause Apogee gehören dazu. Sie fesselten den Spieler zu einer Zeit, als ein Pentium-Rechner mit acht MB (!) RAM den High-End-Standard bei Computern definierte. Wer wehmütig daran zurückdenkt, kann die alten Titel ganz einfach wieder für sich entdecken. Denn der Anbieter GOG (www.gog.com) bietet viele solche Spiele für Linux an.

Die Spiele bei GOG sind frei von DRM-Restriktionen. Bei den Klassikern greifen die Entwickler auf die letzten Versionsstände zurück und haben deren Installationsroutinen soweit überarbeitet, dass sie unter Linux installiert werden können. Dabei ist zu



beachten, dass Ubuntu für die Macher die Referenz bildet. Unterstützt werden von den meisten Titeln die Versionen 14.04, 16.04 und 18.04.

Es ist jederzeit den Versuch wert, die im Debian-Format angebotenen Spiele auch unter anderen Distributionen zum Laufen zu bekommen. Klappt das allerdings nicht, kann der Support kaum weiterhelfen. Dafür belasten Fehlkäufe aber den Geldbeutel nicht arg. Das Gros des Angebots ist für unter zehn Euro zu bekommen. GOG hat inzwischen auch einen eigenen Client entwickelt, der den Einkauf neuer Spiele, die Pflege einer Bibliothek und den Austausch mit Freunden unterstützt. Wenn das Spiel das unterstützt, können damit Spielstände in der Cloud gespeichert werden. Allerdings gibt es GOG Galaxy (noch) nicht in einer generischen Linux-Version.

Zum Ausprobieren aus dem riesigen Angebot von GOG haben wir dann auch gleich zwei Empfehlungen für Sie. An der Entwicklung von *The Dig* hat Steven Spielberg mitgearbeitet. Bei dem Science-Fiction-Abenteuer schlüpft der Spieler in die Rolle eines Raumschiffkommandanten, der einen Asteroiden untersuchen soll. Dieser hält auf die Erde zu, entpuppt sich indes als ein

fremdes Raumschiff. Dies muss erkundet und dabei einige Rätsel gelöst werden.

Spaß bereiten nach wie vor die Adventures rund um *Indiana Jones*. Wie bei *The Dig* entfalten, gemessen an heutigen Maßstäben, die einfachen Klötzchengrafiken ihren ganz eigenen Charme. Und da es immer mehr Quellen für Spiele unter Linux wie Steam, GOG und auch generische Titel gibt, sollten Sie sich einmal das Programm Lutris (<https://lutris.net/>) ansehen. Denn es schafft Ordnung in der Spielesammlung und importiert Titel aus den unterschiedlichen Quellen.

Wine, Scumm VM und DOS-Box

Die Installation eines Spiels aus dem Repertoire von GOG läuft in der Regel problemlos. Wenn Sie Spaß am Basteln haben, gibt es aber auch andere Wege, Ihre alten Originalspiele wiederzubeleben. Es gibt drei Umgebungen, mit denen es gelingen kann, Windows- und DOS-Spiele unter einem aktuellen Linux auszuführen. Welcher davon Erfolg verspricht, lässt sich über eine Internetrecherche herausfinden. Die Suche nach dem Stichwort „Spiele“ auf einschlägigen Hilfeseiten wie ubuntuusers.de hilft meist weiter.

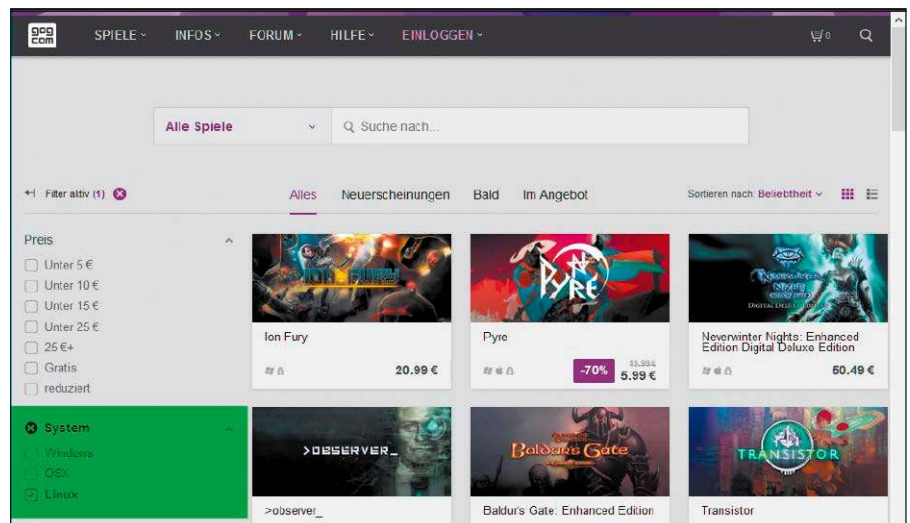
Klassischer Helfer ist Wine: Es stellt Windows-Bibliotheken bereit, die von Windows-Programmen und eben auch Spielen genutzt werden. Der wahrlich legendäre Klassiker Command & Conquer wird etwa von einer Schar Unentwegter im Internet unter der Adresse <https://cncnet.org/tiberian-sun> am Leben erhalten und setzt dabei auf die Wine-Umgebung.

Money Island, Indiana Jones oder Maniac Mansion stammen dagegen aus der Spieleschmiede Lucas Arts. Und deren Macher haben seinerzeit einen Weg gewählt, der das Spielen unter Linux Jahrzehnte später ermöglicht. Den Titeln gemeinsam ist der Einsatz des Frameworks „Script Creation Utility for Maniac Mansion Virtual Machine“ – kurz Scumm VM. Das Programm gehört zum festen Bestandteil der Paketmanager vieler Distributionen. Einmal installiert, kann der Spieler mit ein bisschen Unterstützung aus dem Internet versuchen, seine Lucas-Arts-Titel zu reanimieren. Dazu wird in einem versteckten Verzeichnis im Benutzerordner („~/Games/ScummVM“) ein Ordner für das Spiel angelegt und dorthin die notwendigen Programmdateien kopiert.

Über einen Start von Scumm VM und der Funktion, einen Spieleordner hinzuzufügen, wird der jeweilige Titel hinzugefügt. Schließlich gibt es dann noch die DOS-Box, die ebenfalls in den Paketquellen verfügbar sein sollte. Damit wird unter Linux eine DOS-Umgebung simuliert, die Grundlage für unzählige Spieletitel bildet. Wirklich beeindruckend ist die Liste der Spiele, die von diesem Emulator unterstützt werden (www.dosbox.com/comp_list.php). Über die Konfigurationsdateien von DOS-Box reservieren Sie einen Teil ihres Benutzerordners als „Festplatte“ für DOS. Auf diesen Datenträger können Sie dann von den Originaldatenträgern die Spiele installieren. Viele Titel sind von ihren Entwicklern längst zu Public Domain erklärt worden und lassen sich kostenfrei herunterladen. Damit löst sich auch das Problem elegant, wo man denn noch ein Laufwerk für 3,5 Zoll-Disketten herbekommt, um die alten Schätze überhaupt lesen zu können.

Holarse: Ein Spieleuniversum

Wenn es um Spielen unter Linux geht, führt kein Weg am Portal Holarse vorbei. Dabei spielt es keine Rolle, ob es um ältere oder neuere Titel geht. Auf der Seite www.holar-

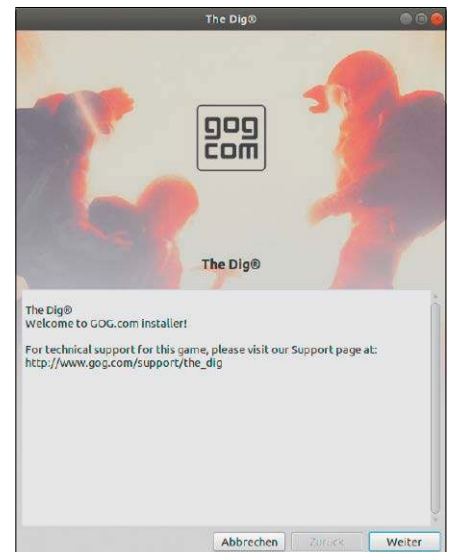


Bei www.gog.com gibt es ein großes Angebot an erschwinglichen Spieletiteln. Mit dem Systemfilter unter „Alle Spiele“ filtern Sie gezielt die Spiele, die unter Linux laufen.

se-linuxgaming.de können Sie sich einfach inspirieren lassen und sich über Spieletitel informieren. Zu jedem Eintrag gibt es eine kurze Beschreibung, Bilder sowie Bezugsquellen. Oder Sie suchen gezielt nach einem Klassiker und informieren sich darüber, über welchen der gezeigten Wege Sie das Spiel unter Linux zum Laufen bekommen. Es geht aber auch der umgekehrte Weg. Ein Blick in die Rubrik „ScummVM“ fördert die Spiele ans Licht, die sich unter der VM installieren lassen. Nützlich ist die Lektüre der Tipps und Tricks auch im Hinblick auf das fast unerlässliche Zubehör wie Joysticks oder Konsolencontroller, die sich oftmals auch unter Linux einbinden lassen.

Steam und Steamlink

Ob aktuell oder bereits etwas älter: Bei kommerziellen Spielen führt kaum ein Weg an der DRM-Plattform Steam vorbei. Alle führenden Publisher nutzen die Verkaufsplattform, die auch über die Rechte der Spieletitel wacht. Die Plattform selbst hatte einmal große Pläne, eine eigene Konsole zu veröffentlichen. Daraus wurde allerdings nichts. Mit Steamlink ist eine interessante Option übrig geblieben, die das Streaming von Spielen an andere Clients erlaubt. Das Spiel selbst läuft unter Steam auf Windows. Das Programm Steamlink, das in den Paketquellen von Raspbian enthalten ist, verwandelt einen Raspberry in einen Client, der dann das Spielen per Netzwerk an einem anderen Ort möglich macht. Nachteil ist natürlich, dass auch der Windows-Rechner laufen muss. ■



GOG (www.gog.com) gibt jedem Spiel einen Installer mit, der unter Ubuntu problemlos funktioniert.



Grafiken aus den 90er-Jahren haben heute ihren eigenen Charme. Am fesselnden Charakter eines Epos wie The Dig ändert das Alter nichts.

Samba im Terminal

Samba- und Windows-Freigaben nutzt man in der Regel im grafischen Dateimanager und der beherrscht das Protokoll SMB/CIFS. Anders sieht es aus, wenn ein Netzrechner Daten im Terminal oder per Bash-Script automatisch übertragen oder abholen soll.



VON HERMANN APFELBÖCK

Linux ist erstens im Netzwerk zu Hause, zweitens priorisiert Linux das Terminal. Zu diesen beiden Binsenweisheiten will gar nicht passen, dass das Terminal mit Samba-Freigaben nichts anfangen kann. Direktes Schreiben auf oder Lesen von Samba-Servern ist hier nicht vorgesehen, was zum umständlichen Mounten in das lokale Dateisystem nötig ist – und dies vielleicht nur, um eine kleine Datei abzulegen. In diese Lücke kann das Terminaltool Smbclient springen, das ursprünglich als Diagnose- und Notfalltool für den Zugriff auf Windows-Rechner konzipiert war.

Die Problemstellung

Das nachfolgend beschriebene und mit Smbclient zu lösende Problem ist natürlich ein Minderheitenthema. Am Linux-Desktop wird für den Zugriff oder die Synchronisierung von Samba-Freigaben kaum jemand das Terminal verwenden. Jedoch kann es erwünscht sein, Zustände oder Dateilisten von Netzwerkrechnern auf einem anderen Rechner zu hinterlegen oder zentral zu sammeln. Unter Windows schreibt ein Terminalbefehl wie

```
dir /s /b > \\192.168.172.10\Data\
  Transfer\liste.txt
```

umstandslos und ohne Angabe der Authentifizierungsdaten auf eine Samba-Freigabe, sofern die Anmeldedaten auf dem Windows-Rechner hinterlegt sind. Linux-Rechner untereinander erledigen solche Kommunikation genauso elegant über SSH. Einfaches Schreiben und Lesen auf Samba-Freigaben funktioniert im Terminal hingegen nicht – jedenfalls nicht ohne externe Hilfe.

Smbclient: Bestandteil von Samba

Die Installation von Smbclient ist selten erforderlich, weil das Tool als Bestandteil des Metapakets Samba in der Regel vorliegt. Bei Bedarf kann es aber auch einzeln mit `sudo apt install smbclient` nachinstalliert werden.

Das Programm hat nicht nur ein ausuferndes Optionsarsenal (`smbclient --help`), sondern als interaktive Samba-Shell einen Befehlsvorrat von über 80 Kommandos. Davon können Sie sich überzeugen, indem Sie nach (Beispiel)

```
smbclient -U ha //192.168.172.10/
  Data
```

das Kommando „help“ eingeben. Beim Aufruf sind folgende Besonderheiten zu beachten:

1. Als Ziel müssen Sie genau die Samba-Freigabe eingeben. Allein die Angabe des Rechnernamens oder seiner IP-Adresse („//192.168.0.8“) scheitert ebenso wie die Angabe eines Unterverzeichnisses („//192.168.0.8/Data/Transfer“).

2. Als User „-U“ müssen Sie ein gültiges Samba-Konto auf dem entfernten Rechner verwenden. Dessen Samba-Kennwort wird danach automatisch abgefragt. Für automatisierte Aktionen können Sie aber das Kennwort auch gleich im Aufruf mitliefern (Beispiel):

```
smbclient -U ha%GeHeIm
  //192.168.172.10/Data
```

Mit „quit“, „exit“ oder „q“ beenden Sie die Samba-Verbindung wieder.

Von den zahlreichen Kommandos, die das Tool anbietet, sollte man sich nicht abschrecken lassen. In der Praxis werden Sie kaum eine Handvoll benötigen.

Zu den Klassikern gehören auch sonst bekannte Standards wie „cd“, „ls“ (dir),

„mkdir“, „rm“ (del). Wer das FTP-Kommandotool kennt, findet sich auch beim Rest sofort zurecht, weil sich Smbclient an diesem Vorbild orientiert.

Dateien liefern oder abholen

Ein interaktiver Gebrauch von Smbclient ist kaum praxisrelevant. Aber mit einem zweizeiligen Script lässt sich jetzt mühelos die Ablage einer Information auf einer entfernten Samba-Freigabe erreichen:

```
find /home -iname "*.*)" > raspi.txt
smbclient -U ha%GeHeIm
  //192.168.172.10/Data -c 'cd
  Transfer/1_Temp;put raspi.txt'
```

Hier wird erst eine Dateiliste erstellt und danach auf die Freigabe kopiert. Das wichtigste Detail im obigen Smbclient-Kommando ist die Fähigkeit, mit Schalter „-c“ einen oder mehrere mit Semikolon getrennte Befehl(e) mitgeben zu können. In diesem Fall ist es der Wechsel mit „cd“ in das gewünschte Verzeichnis und dann der Befehl „put“, um die Dateiliste zu kopieren. Es muss sich um eigene, interne Befehle von Smbclient handeln.

Nach demselben Muster können Sie eine bestimmte Datei von der Freigabe auf den aktuellen Rechner holen:

```
smbclient -U ha%GeHeIm
  //192.168.172.10/home -c 'cd
  ha;get liste.txt'
```

Die mit „get“ kopierte Liste landet dabei im aktuellen Verzeichnis des lokalen Systems. Im Allgemeinen wird das automatisierte Ablegen oder Abholen einer einzigen Datei das Haupteinsatzgebiet von Smbclient sein.

Die Fähigkeiten des Tools gehen aber deutlich darüber hinaus:

```
smbclient -U ha%GeHeIm
//192.168.172.10/Data -c 'cd
Depot/Sonderhefte;prompt off;mget
*.pdf'
```

Die Befehle „mget“ und „mput“ können alle Dateien einer bestimmten Dateimaske oder auch sämtliche Dateien eines Verzeichnisses (mget *.*) erfassen. Die Bestätigung für jede Datei lässt sich mit „prompt off“ abschalten und damit ist der Ablauf automatisierbar. Es geht noch umfangreicher:

```
smbclient -U ha%GeHeIm
//192.168.172.10/Data -c 'cd
Depot/Sonderhefte;recurse
on;prompt off;mask *.pdf;mget *
```

Der aktivierte „recurse“-Befehl durchläuft vom angegebenen Startordner aus sämtliche Unterverzeichnisse, um dann die angeforderten Dateien zu kopieren. Das Ganze funktioniert nach unserer Kenntnis nur mit dem zusätzlichen „mask“-Befehl.

Achtung: Im lokalen Zielordner werden sämtliche Unterverzeichnisse gemäß der Samba-Quelle erstellt, auch wenn diese Verzeichnisse keine der angeforderten Dateien enthalten.

Noch ein Hinweis: Die Kopierbefehle „get“, „put“, „mget“, „mput“ nehmen keine Rücksicht auf bestehende Dateien gleichen Namens. Diese werden überschrieben.

Akademische Spezialitäten von Smbclient

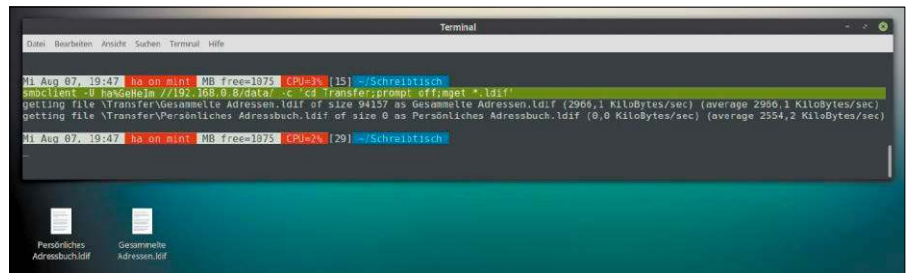
Startoption „-D“ oder „--directory“: Anstatt mit „cd“ in das gewünschte Verzeichnis zu wechseln, gibt es auch einen Startparameter für das Wunschziel:

```
smbclient -U ha%GeHeIm
//192.168.172.10/Data -D
Transfer/Backgrounds
```

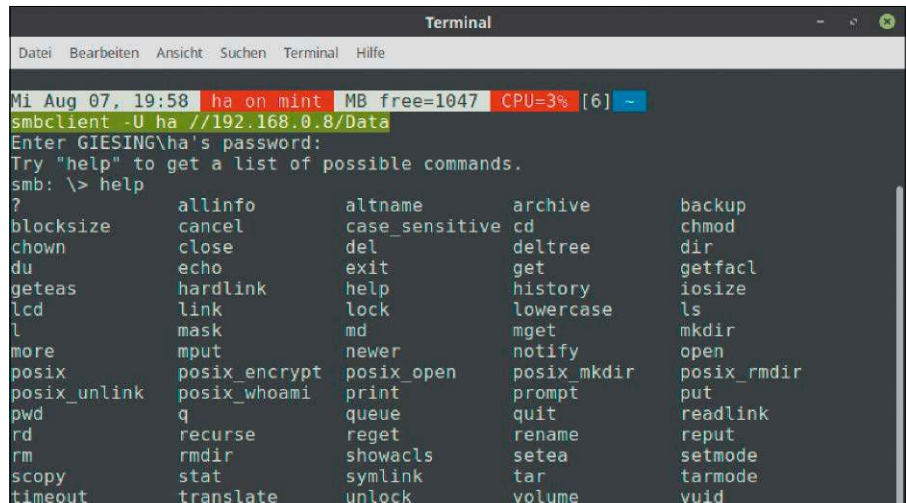
Der Serveraufruf selbst muss zwar direkt zur Freigabe führen, aber der gesuchte Unterordner kann dann gleich mit „-D“ angefordert werden.

Startoption „-A“ oder „--authentication-file“: Im Heimnetz sollte es kein Problem sein, das Samba-Kennwort im Klartext in einem Script abzulegen, zumal sich das Script durch Pfad und Dateirecht vor Fremdzugriff schützen lässt. Smbclient sieht dafür aber auch noch einen speziellen Startparameter vor, um solchen Schutz zu vereinfachen. Mit Schalter „-A“

```
smbclient -A /root/smbpass.txt
//192.168.0.8/Data [...]
```

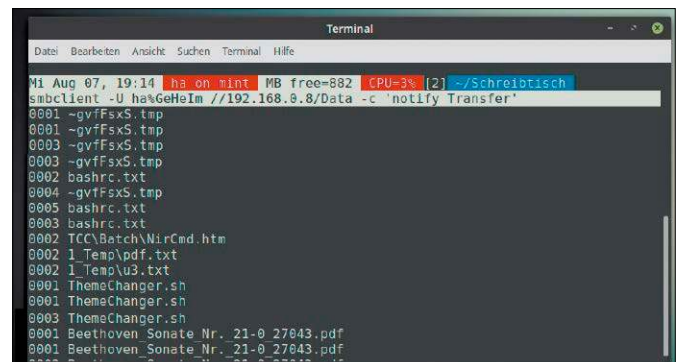


Typischer Kopierbefehl mit Smbclient: Ein einzeliges Kommando kann einzelne oder mehrere Dateien automatisch vom Samba-Server abholen oder dorthin hochladen.



Interaktiver Modus: Eine Übersicht mit „help“ kann nicht schaden, jedoch werden Sie die allermeisten der zahlreichen Kommandos nie benötigen.

Samba-Überwachung mit „notify“: Diese Möglichkeit von Smbclient ist kein Alltagsinstrument, gibt aber zuverlässig Auskunft über die Aktivitäten auf einer Freigabe.



kann eine Datei (im Beispiel „smbpass.txt“) angegeben werden, welche die Samba-Authentifizierungsdaten in folgender Form enthält (Beispiel):

```
username=ha
password=GeHeIm
domain=GIESING
```

Auch diese Datei ist natürlich im Klartext lesbar, kann aber – eventuell einfacher als ein Script oder Bash-Alias – durch Dateirechte geschützt werden.

Kommando „notify“: Der interne Befehl „notify“ bietet ein Überwachungsprotokoll.

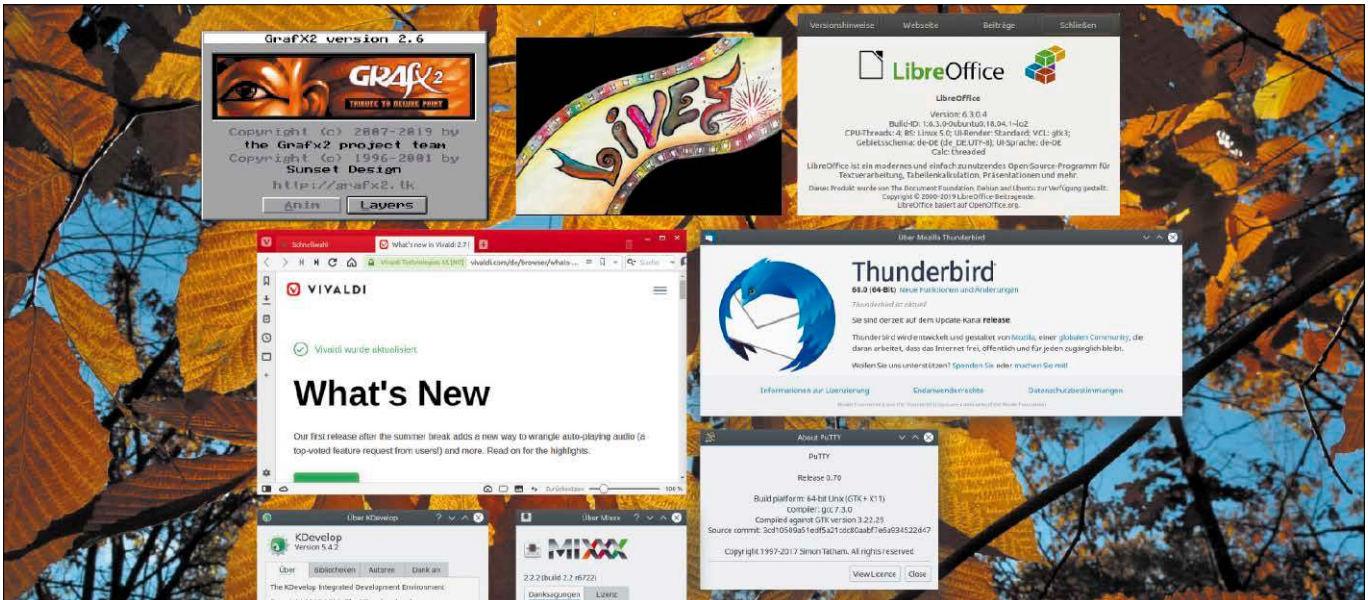
Der Befehl zeigt jede Dateiaktion innerhalb eines Ordners und aller Unterordner. Nach der Eingabe

```
smbclient -U ha%GeHeIm
//192.168.172.10/Data -c 'notify
Transfer'
```

können Sie in Echtzeit mitlesen, was in diesem Samba-Ordner erstellt, geändert oder gelöscht wird. Das Beispiel geht davon aus, dass sich das Verzeichnis „Transfer“ auf oberster Ebene der Freigabe „Data“ befindet. Der Notify-Befehl läuft endlos, bis Sie ihn mit Strg-C abbrechen. ■

Frische Software

Trotz Sommerpause machten wieder einige Open-Source-Schwergewichte mit neuen Versionen auf sich aufmerksam: Libre Office, Thunderbird und Putty sind den meisten Linux-Anwendern ein Begriff und liegen in aktuellen Ausgaben vor.



VON DAVID WOLSKI

Das Ende des Sommers bedeutet in der Open-Source-Szene auch, dass eine neue Runde von Googles „Summer of Code“ zum Abschluss kommt. Dieses Jahr wurde das Mentorenprogramm für Open-Source-Software zum fünfzehnten Mal in Folge abgehalten – dieses Jubiläum teilt sich der „Summer of Code“ mit der LinuxWelt. Es ist kein Zufall, dass sich beide Projekte das Jubiläum teilen, denn vor fünfzehn Jahren war die Zeit von Linux und Open Source mehr als reif, aus dem Serverraum hinaus in die allgemeinere IT zu treten. Heute sind Linux-Systeme und Open-Source-Programme fester Teil des täglichen Geschäfts mit Daten, aber eben auch auf so manchen Desktops zu Hause. Google hat mit der Unterstützung zahlreicher Projekte im jährlichen „Summer of Code“ keinen kleinen Verdienst an den Erfolgen von Linux und Open-Source-Software.

Googles Wette auf Open Source

Generell ist das Wohlwollen vieler Anwender gegenüber Google zurückgegangen. Zumindest ist das Loblied auf die Verdienste des IT-Konzerns beziehungsweise auf die heutige Holding Alphabet Inc deutlich leiser geworden. Die Firmennamen fallen heute meist im Zusammenhang mit Kritik an der Daten-Sammelwut des Konzerns, der gemessen an den Umsätzen aus seinen verschiedenen Sparten eben doch nur eine gigantische Online-Werbeagentur ist. Immerhin haben die Köpfe hinter Google noch nicht ganz vergessen, dass der Erfolg des Unternehmens beinahe von Anfang an auf Open Source gebaut war. Selbst das erste Firmenlogo hat Firmen-Mitgründer Sergey Brin noch eigenhändig in Gimp erstellt. Und auch wenn Googles eigene Unterstützung von Linux durch eigene Software eher mau ausfällt, so stehen über den „Google Summer of Code“ jedes Jahr stehen mehrere Millionen Euro für Studenten bereit, die Ideen und bezahlte Ar-

beitszeit in ausgewählte Open-Source-Projekte investieren.

Jährliche Talentsuche

Für Projekte ohne eigenes Finanzierungsmodell ist diese Hilfe zu einem wichtigen Motor geworden. Im Jahr 2019 waren unter anderem die 3D-Software Blender, das reife Displayprotokoll Wayland, die Fotoverwaltung Digikam und der Mediaplayer VLC im „Summer of Code“ vertreten. Über die Jahre hat das Programm über 14 000 Studierende aus insgesamt 109 Ländern geholfen, bezahlt an einem gut organisierten Open-Source-Projekt teilzunehmen. Mehr als 200 unterschiedliche Organisationen haben sich dabei bisher als Mentoren beteiligt. Dabei sind nicht immer nur die üblichen bekannten Großprojekte vertreten: Rund 20 Prozent der teilnehmenden Mentoren sind jedes Jahr Neuzugänge. Für Google ist das großzügige Programm natürlich auch eine Talentsuche, um früh die künftigen Codegenies ausfindig zu machen.

Blender 2.80

3D-Modeller und Renderprogramm

www.blender.org

Der kleine Versionssprung von 2.79 auf 2.80 täuscht. Die neue Blender-Version hat umfangreiche Umbauten erfahren. Äußerlich präsentiert sich die Oberfläche in einem neuen Gewand, das auf grafische Bedienelemente statt etlicher Tastenkombinationen setzt. Die Hotkeys funktionieren aber weiterhin. Die interne Renderengine Eevee ist komplett neu und kann Grafiken in Echtzeit berechnen, sofern leistungsfähige Hardware vorliegt. ■



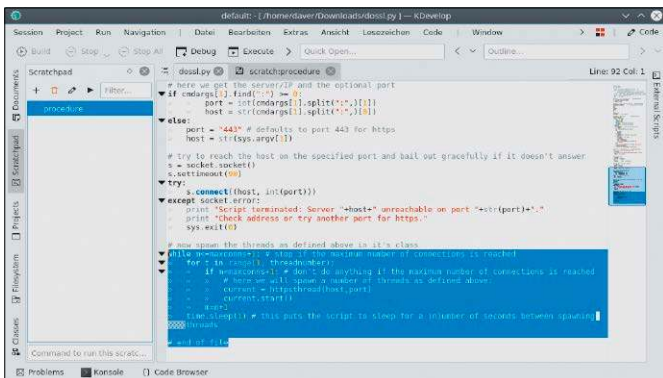
Blender 2.80 ist ein großes Update. Die Grafikkarte verlangt mindestens Open GL 3.3 und somit aktuellere Hardware der letzten fünf Jahre.

Kdevelop 5.4.2

Entwicklungsumgebung und Quelltexteditor

www.kdevelop.org

Kdevelop beweist, dass eine Entwicklungsumgebung nicht kompliziert sein muss. Die neue Version des Codeeditors bringt ein Plug-in zum Sammeln von Codeschnipseln mit und kann mit dem Build-System Meson umgehen. Gefehlt wurde auch an einer verbesserten Sprachunterstützung für PHP und Python. Fertige DEB-Pakete hat das PPA der Kubuntu-Backports (<https://launchpad.net/~kubuntu-ppa/+archive/backports>), aber es gibt auch ein Appimage. ■



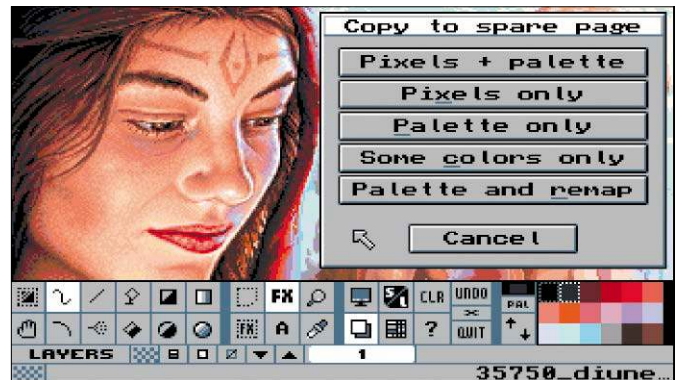
Codekünstler – nicht nur unter KDE: Kdevelop ist eine Entwicklungsumgebung mit Projektverwaltung für verbreitete Programmiersprachen.

Grafx 2.6

Pixelorientiertes Malprogramm

<http://grafx2.chez.com>

Grafx ist ideal für die Erstellung von pixelorientierten Grafiken für Websites, Spiele, Apps und Icons. Es ist in Aussehen und Funktionsumfang an das Amiga-Programm Deluxe Paint II und dessen DOS-Portierung angelehnt. Es gibt 256 Farben und nur eine geringe Auflösung, die auf modernen Bildschirmen hochskaliert wird. Dafür ist Grafx aber perfekt, wenn es um pixelgenaues Arbeiten geht. Als Ergänzung gibt es Ebenen und jüngere Dateiformate wie PNG. ■



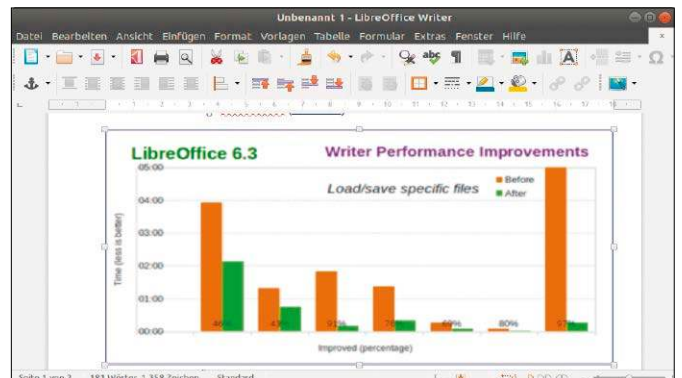
Spezialwerkzeug für Retrografiken, Spiele- und App-Entwicklung: Grafx 2.6 ist anachronistisch, aber bei Pixelgrafiken unschlagbar.

Libre Office 6.3

Umfassendes Büropaket in neuer Version

<http://de.libreoffice.org>

Libre Office legt ein halbes Jahr nach Version 6.2 eine neue Ausgabe vor, die auch in die nächsten Distributionen wie Ubuntu 19.10 einfließen wird. Neu ist eine Exportfunktion für das Archivformat PDF/A-2. Writer und Calc zeigen erhöhtes Tempo beim Öffnen und Speichern von Dokumenten. Für Ubuntu gibt es ein Snap-Paket, aber auch ein PPA (<https://launchpad.net/~libreoffice/+archive/ubuntu/ppa>) mit traditionellen DEB-Paketen des neuen Libre Office. ■



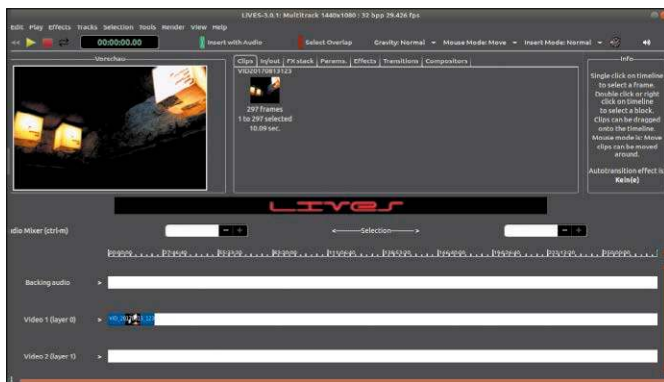
Schneller öffnen und speichern: Bei Fremdformaten von Microsoft Office glänzt Libre Office mit deutlich kürzeren Ladezeiten.

Lives 3.0.1

Videoschnitt mit flacher Lernkurve

<http://lives.sourceforge.net>

Dem Videoschnittprogramm gelingt eine gute Balance zwischen Funktionsvielfalt und Übersichtlichkeit. Für erste Ergebnisse ist es nicht nötig, Handbücher zu wälzen. Version 3.0.1 hat eine aktualisierte Oberfläche und gibt Videos ruckelfrei über Open GL aus, das über den Grafiktreiber Hardwarebeschleunigung nutzt. Fertige Pakete verlinkt die Projektseite, ferner gibt es mit <https://launchpad.net/~ubuntuhandbook1/+archive/ubuntu/lives> ein PPA für Ubuntu. ■



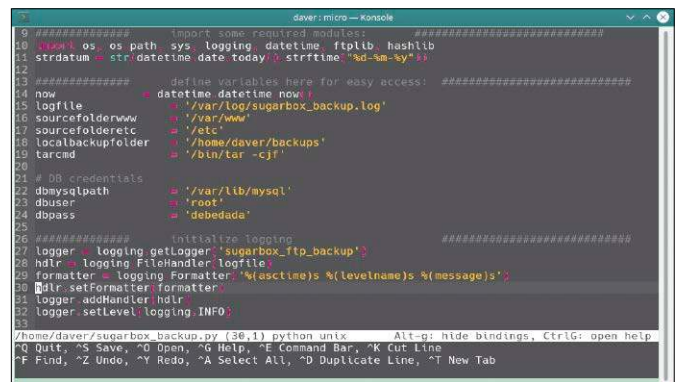
Videos schneiden mit wenig Vorbereitung: Das Linux Video Editing System, kurz „Lives“, zeichnet sich durch seine einfache Oberfläche aus.

Micro 1.4.1

Komfortabler Editor für die Shell

<https://micro-editor.github.io>

Gibt es nicht schon genügend Editoren für das Terminal? Micro will die Vorzüge einfacher Programme wie Nano mit den Fähigkeiten von Editoren wie Vim kombinieren. Dies gelingt mit einem aktivierten Mauscursor im Terminal und Standard-Hotkeys wie Strg-C und Strg-V zum Kopieren und Einfügen. Es gibt Syntaxhervorhebung für viele Programmiersprachen sowie eine LUA-Schnittstelle für Erweiterungen. Micro liegt auf der Projektseite als ausführbare Binary vor. ■



Micro ist für Einsteiger wie Fortgeschrittene geeignet: Alt-G blendet am Bildschirmrand eine Liste der Hotkeys ein.

Mixxx 2.2.2

MP3-Player mit Mixer und Crossfader

www.mixxx.org

Das plattformübergreifende Open-Source-Programm emuliert ein digitales DJ-Pult und kombiniert bis zu vier MP3-Player. Sampler, Equalizer und Effektgerät können ebenfalls aktiviert werden. Die Synchronisationsfunktion sorgt dafür, dass alle Tracks im Takt bleiben. Wichtigste Neuerung von Mixxx 2.2.2 ist der Wechsel von Qt 4 auf Qt 5 und damit die Unterstützung von Hi-DPI-Bildschirmen. Die Webseite liefert Installationsanleitungen für Ubuntu und Fedora. ■



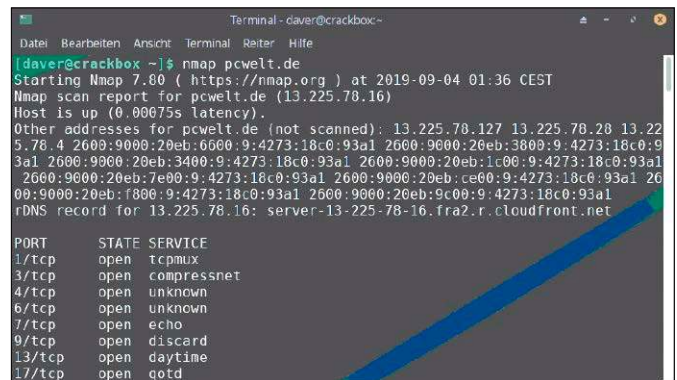
Gut gemixt: Mixxx ist einem DJ-Pult nachempfunden, um MP3-Dateien zu mischen. Es unterstützt Jack-Audio und externe Mixerhardware per USB.

Nmap 7.80

Mächtiger Portscanner

<https://nmap.org>

Auf der Jagd nach Sicherheitslücken ist der Portscanner Nmap unverzichtbar. Ein Jahr nach der letzten Version ist Nmap in neuer Version mit weiteren Scripts erschienen. Die Scripts dienen dazu, einen Server über Netzwerkpakete zu identifizieren, und umfassen Fingerabdrücke für Jenkins- und Windows-RDP-Server. Nmap steht auf der Projektseite als RPM für Fedora, Cent-OS und Open Suse zum Download bereit und ist im kommenden Ubuntu 19.10 enthalten. ■



Server abklopfen: Der Portscanner Nmap liefert in der neuen Version elf neue Scripts zur Identifikation von Serverdiensten mit.

Ocrmypdf 9.0.1

Textexport von PDF-Dateien

<https://github.com/jbarlow83/OCRmyPDF>

PDFs ohne Textebene sind in Archiven nicht durchsuchbar. Ocrmypdf schickt den Bildinhalt eines PDFs durch die OCR-Engine Tesseract und fügt das Ergebnis dem PDF als Textebene hinzu. Es handelt sich um ein Kommandozeilenprogramm, das installiertes Tesseract-OCR verlangt, das sich aber überall in den Standardpaketquellen findet. Version 9.0.1 ist derzeit nur in Debian Sid und Arch Linux verfügbar, andere Distributionen haben noch den Vorgänger. ■



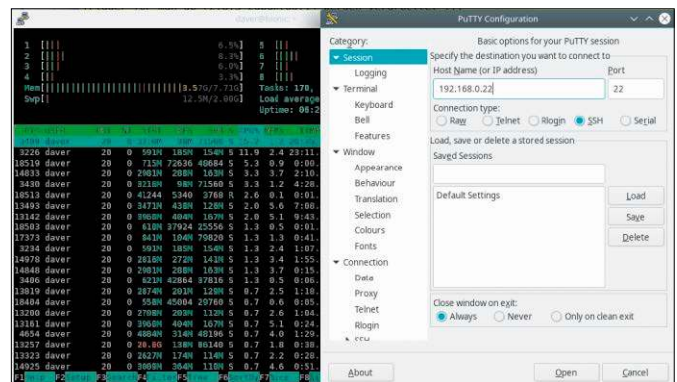
Pixel zu Buchstaben: Ocrmypdf nutzt die OCR-Software Tesseract, um PDF-Dateien um eine saubere Textebene zu ergänzen.

Putty 0.72

Plattformübergreifender SSH-Client

www.putty.org

Für Linux-Admins, die mit Windows arbeiten, ist der Terminalemulator und SSH-Client Putty eines der wichtigsten Werkzeuge, bis das neue Windows-Terminal aus der Betaphase herauskommt. Zudem unterstützt Putty in seinen unzähligen Optionen auch SSH-Tunnel unter Windows, um etwa eine verschlüsselte Socks-Proxy-Verbindung aufzubauen. In Putty 0.72 sind Fehlerbehebungen eingeflossen, die eine EU-finanzierte Bugsuche ans Licht brachte. ■



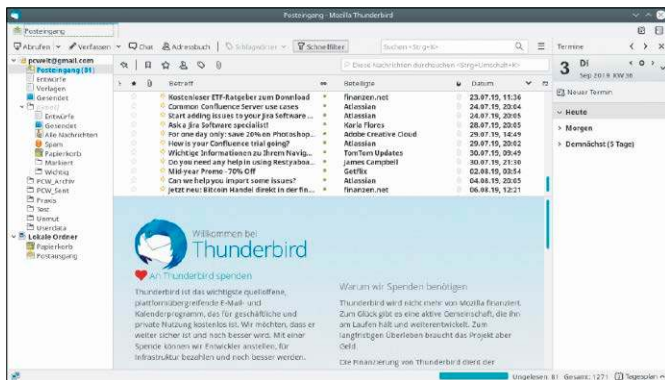
Putty gibt es auch für Linux: Unter Windows unverzichtbar dient Putty unter Linux hauptsächlich für serielle Verbindungen zum Debugging.

Thunderbird 68.0

Mailclient mit integriertem Kalender

www.mozilla.org/de/thunderbird

Thunderbird legt einen Versionssprung von 60 auf 68 hin. Nicht ohne Grund: In der neuen Version funktionieren alle Add-ons nicht mehr. Ab jetzt akzeptiert Thunderbird wie Firefox nur noch Webextensions. Es gibt ein neues dunkles Thema und wiederverwendbare Filelink-Anhänge. Aufgrund der vielen Änderungen wird Thunderbird 68 nicht als Update angeboten, sondern verlangt eine manuelle Neuinstallation. Fertige Binärpakete liefert die Webseite. ■



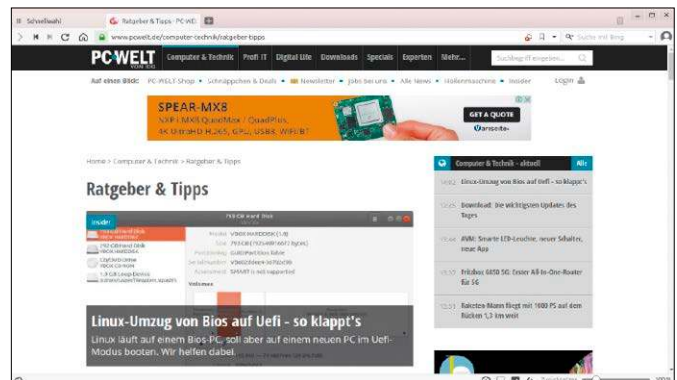
Neues Zeitalter für Thunderbird: So wie bei Firefox laufen jetzt nur noch neuere Webextensions. Die Oberfläche wurde modernisiert und um Funktionen ergänzt.

Vivaldi 2.7

Schneller Browser auf Chromium-Basis

<https://vivaldi.com>

Der Browser Vivaldi ist zwar nicht Open Source, sondern Freeware, taucht in der LinuxWelt aber häufiger auf. Denn die Entwicklung schreitet flott voran und jede Hauptversion bringt interessante Neuerungen. Vivaldi 2.7 stellt vorlaute Webseiten ruhig und erlaubt permanentes Stummschalten einer geöffneten Seite per Rechtsklick auf einen Tab. Die Audioausgabe lässt sich auch auf den aktiven Tab einschränken. Die Projektseite stellt DEB- und RPM-Pakete bereit. ■



Virtuoser Browser: Vivaldi ist eine gute Wahl für Anwender, die eine Alternative zu Firefox, Chrome und Chromium suchen.

3x LinuxWelt



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

Satte **33 %** gespart!

+ BestChoice Gutscheine* oder 10,-€ Geldprämie**



Jetzt testen:

3 x LinuxWelt als Heft frei Haus mit Gratis-DVD +
3 x LinuxWelt direkt aufs Smartphone & Tablet mit interaktivem Lesemodus +
10,- € BestChoice- oder BestChoice Entertainment-Gutschein* oder **10,- € Geldprämie****
= 17,- € (33 % gespart!)

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

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

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

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

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

ABONNIEREN	Vorname / Name			
	Straße / Nr.			
	PLZ / Ort			
	Telefon / Handy		Geburtstag	TT MM JJJJ
	E-Mail			

Ich bezahle bequem per Bankeinzug.
 Ich erwarte Ihre Rechnung.

BEZAHLEN	Geldinstitut
	IBAN
	BIC
	Datum / Unterschrift des neuen Lesers

LWPM062018

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

Ubuntu-Installationen

Dieser Beitrag erklärt alle Varianten der Ubuntu-Einrichtung und hat eine Reichweite, die weit über offizielles Ubuntu hinausgeht: Fast alle namhaften Desktopdistributionen verwenden beim Setup das Installationsprogramm von Ubuntu.

VON HERMANN APFELBÖCK

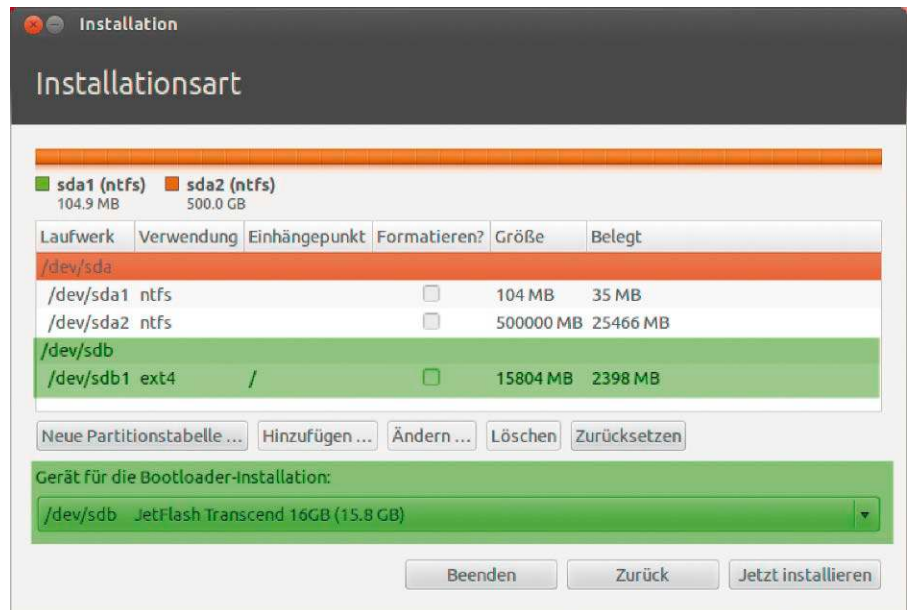
Installationen erfolgen über das (Ubuntu-) Livesystem, mit dem Sie Ihr Zielgerät booten und – im Normalfall – mit der Desktop-Verknüpfung „Ubuntu ... installieren“ die Einrichtung starten. Bis zur Version 18.04 LTS verwenden alle Ubuntus denselben grafischen Installer Ubiquity. Auf diesen beziehen sich die meisten der folgenden Infos. Wo nötig, benennen wir Unterschiede beim Installer Calamares, der inzwischen in den aktuellen Versionen von Kubuntu und Lubuntu 19.04 benutzt wird. Funktional bestehen zwischen Ubiquity und Calamares kaum Unterschiede.

Installation als alleiniges System

Zur Installation booten Sie den gewünschten Zielrechner mit dem System Ihrer Wahl. Dessen ISO-Abbild muss dazu vorher auf DVD oder auf USB-Stick geschrieben werden. Auf diese Aktion gehen wir hier nicht näher ein, zumal dies auf der Heft-DVD im PDF „LinuxWelt XXL“ erklärt wird („Der Umgang mit Systemimages“).

Standardmäßig sind PCs und Notebooks so eingestellt, dass sie automatisch von CD/DVD booten. Sollte dies anders konfiguriert sein, müssen Sie nach Einschalten das Bootmenü des Bios aufrufen. Dies erledigt in der Regel eine Funktionstaste, häufig F2, F8 oder F12, gelegentlich auch die Esc-Taste. Im Bootmenü wählen Sie dann das DVD-Laufwerk, das Sie an Kennzeichnungen wie „Internal CD/DVD“ oder „Atapi“ erkennen. Wenn Sie Ubuntu von USB booten, verwenden Sie ebenfalls das Bootmenü.

Beim gestarteten System handelt es um ein Livesystem, das den Installer mitbringt und auf dem Desktop als Verknüpfung anbietet. Für eine Ubuntu-Installation als alleiniges System sind keine weiteren Vorbereitungen nötig. Nach dem Start der Verknüpfung

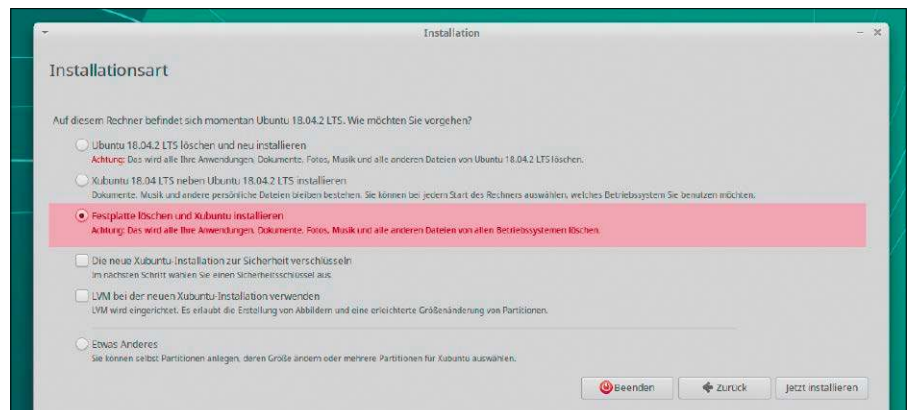


Installation auf externe USB-Medien: Hier müssen Sie das richtige Laufwerk manuell orten und partitionieren. Auch der Bootloader muss auf das USB-Laufwerk.

wählen Sie die Sprache, Tastatur und die „Installation von Drittanbieter-Software“. Nach diesen einfachen Abfragen erscheint eventuell die Frage „Aktive Partitionen aushängen?“. Um sich alle Möglichkeiten offen zuhalten, antworten Sie hier mit „Ja“, um

Zugriff auf alle Partitionen zu erhalten. Im nächsten Schritt erscheint der entscheidende Dialog „Installationsart“ mit zwei möglichen Szenarien:

1. Wenn die primäre Festplatte des Rechners kein System enthält, lautet die oberste



Einfachster Fall mit „tabula rasa“: Zum Einrichten als alleiniges System wählen Sie „Festplatte löschen ...“. Der Installer erledigt Partitionierung und Auslagerung automatisch.

und vormarkierte Option „Festplatte löschen und Ubuntu installieren“.

2. Hat der Installer auf der primären Festplatte ein System gefunden, dann erscheint als oberste und markierte Option „Ubuntu neben [...] installieren“ und erst als zweite Option „Festplatte löschen [...]“.

Für die Einrichtung von Ubuntu als alleiniges System verwenden Sie in beiden Situationen „Festplatte löschen [...]“. Die übrigen Optionen des Dialogs lassen Sie ungenutzt und beginnen mit „Jetzt installieren“ den Vorgang, der danach nur noch die Angaben für das erste Benutzerkonto verlangt. Die Festplatte wird formatiert, der Datenbestand (und ein eventuelles System) gelöscht und Ubuntu eingerichtet.

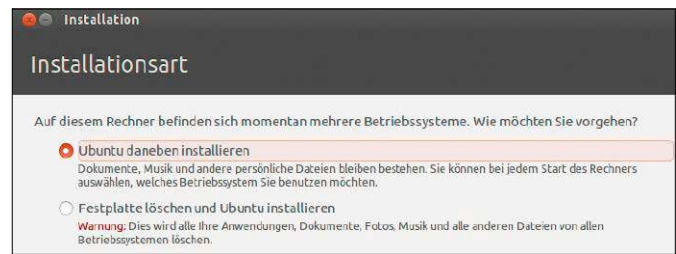
Installer Calamares: Falls Sie aktuelles Kubuntu oder Lubuntu 19.04 installieren, lautet der maßgebliche Schritt „Einrichtung der Festplatten“ oder „Partitionen“. Hier aktivieren Sie die Option „Geführt – vollständige Festplatte verwenden“, um das System als alleiniges Betriebssystem auf der primären Festplatte einzurichten.

Installation auf USB

Ubuntu lässt sich auch ganz regulär auf USB oder auf eine sekundäre interne Platte installieren. Da der Installer stets die erste interne Festplatte „/dev/sda“ als Ziel vorschlägt, müssen Sie bei der Einrichtung auf ein USB-Gerät manuell die richtige Zielpartition festlegen. Daher wählen Sie im Fenster „Installationsart“ die Option „Etwas Anderes“. Das Laufwerk muss neu partitioniert und formatiert werden, alle darauf befindliche Daten gehen verloren. Klicken Sie zunächst auf die „-“-Schaltfläche, um vorhandene Partitionen zu entfernen. Erstellen Sie dann auf dem „freien Speicherplatz“ mit der „+“-Schaltfläche eine neue primäre Partition mit dem kompletten Speicherplatz und dem Dateisystem Ext4. Hinter „Einbindungspunkt“ wählen Sie den Eintrag „/“ aus der Liste. Unter „Gerät für die Bootloader-Installation“ wählen Sie dasselbe USB-Laufwerk aus, auf dem Sie installieren – etwa „/dev/sdb“. Es ist wichtig, auch den Bootloader auf USB zu schreiben, andernfalls startet das System nur auf dem Rechner, mit dem Sie installiert haben. Bei Installation auf eine sekundäre interne Platte verwenden Sie hingegen „/dev/sda“ für den Bootloader.

Calamares: Bei diesem Installer (Kubuntu oder Lubuntu 19.04) lautet der maßgebliche

Hier wurden mehrere vorhandene Systeme erkannt. Wenn Sie „daneben“ installieren, entsteht durch Verkleinern einer bestehenden Partition eine neue für Ubuntu.



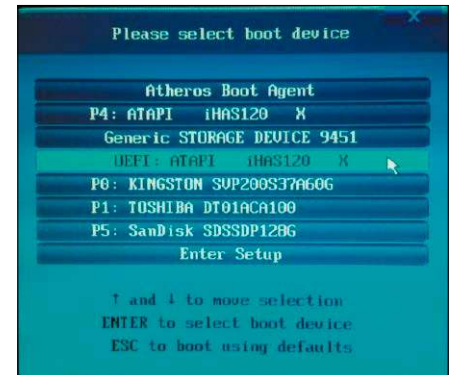
che Schritt „Einrichtung der Festplatten“ bzw. „Partitionen“. Hier benötigen Sie für USB-Installation den Unterpunkt „Manuell“. Nach „Weiter“ erhalten Sie eine Laufwerkliste, können dort ein USB-Medium wie „/dev/sdb1“ löschen und neu anlegen – mit den gleichen Einstellungen wie oben bei Ubiquity beschrieben.

Multiboot mit Ubuntu

Der Ubuntu-Installer erkennt und respektiert vorhandenes Windows oder Linux. Etwas knifflig ist jedoch die Unterscheidung zwischen Bios- und Uefi-Partitionschema. Bei der oben beschriebenen Soloinstallation spielt der Partitionsstil keine Rolle. Sobald aber zwei oder mehr Systeme parallel installiert werden sollen, dann wird der richtige Partitionsstil – Bios/MBR versus Uefi/GPT – entscheidend. Die Parallelinstallation kann nur gelingen, wenn das Livesystem in jenem Modus gestartet wird, in dem das bereits installierte System läuft. Andernfalls kann der Installer das vorhandene System nicht erkennen und wird dieses, sofern der Benutzer das Problem nicht bemerkt, bei der Ubuntu-Installation überschreiben.

Auf PCs mit Windows 8 oder 10 herrscht der moderne Uefi-Modus mit GPT-Partitionsstil. Weitere Systeme müssen auf die gleiche Weise eingerichtet werden. Da der Parallelbetrieb von Windows und Linux eines der verbreitetsten Multiboot-Szenarien ist, fokussieren wir uns nachfolgend auf die Parallelinstallation neben Windows im Uefi-Modus. Den aktuellen Partitionsstil des existierenden Systems können alle einschlägigen Tools ermitteln – unter Windows die „Datenträgerverwaltung“, unter Ubuntu Gparted, Gnome-Disks oder der KDE-Partitionsmanager. GPT erscheint hier als „gpt“, der MBR-Modus als „msdos“.

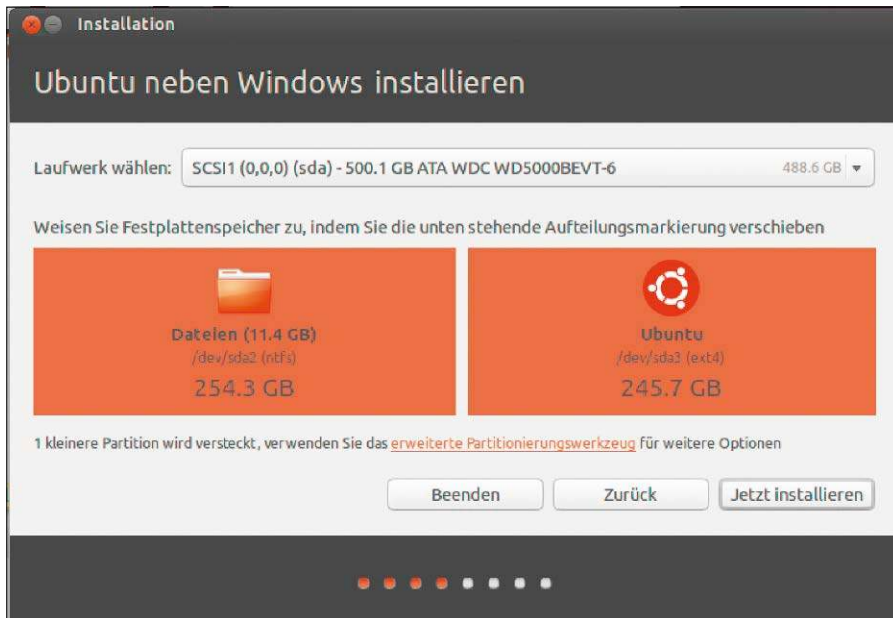
Uefi und GPT: Uefi/GPT ist bei Linux-Nutzern unbeliebt, weil es Komplikationen mit sich bringt. Allerdings ist GPT (GUID Partition Table) eine technisch notwendige Antwort auf die Tatsache, dass der alte MBR-



Uefi-Bootmenü: Die eingelegte DVD mit dem Livesystem erscheint zweimal – als „P4: ATAPI“ und als „Uefi: ATAPI“. Für eine Uefi-Installation muss diese zweite Bootoption gewählt werden.

Partitionsstil nur maximal zwei TB pro Partition adressiert – eine Grenze, die aktuelle Festplatten längst überschreiten. Für die Installation neben Windows 8/10 gelten folgende Regeln:

1. Nur 64-Bit-Linux beherrscht GPT. Auch 32-Bit-Systeme können natürlich im Multiboot-Betrieb arbeiten, jedoch nur im Bios-/MBR-Partitionsstil. Ein Multiboot mit Windows 8/10 ist damit nicht möglich.
2. Die Heft-DVD der LinuxWelt bootet nur im Bios-Modus und eignet sich nicht für eine Uefi/GPT-Parallelinstallation. Sie müssen das gewünschte ISO-Abbild auf ein eigenes Medium transferieren (DVD oder USB) und Ubuntu damit installieren. Die ISO-Abbilder der Heft-DVD (unter „Image-Dateien“) können Sie aber sehr wohl verwenden und sich den Download sparen.
3. Wenn das passende Installationsmedium vorliegt, müssen Sie damit den Zielrechner über das Bootmenü des Uefi-Bios starten. Das Bootmenü ist meistens durch frühzeitiges Drücken der Taste F2, F8, F12 oder Esc zu erreichen. Dort erscheinen dann die Laufwerke zwei Mal – einmal mit, einmal ohne den Vorsatz „UEFI“. Für Uefi-Parallelinstallation wählen Sie den „UEFI“-Eintrag. Einen eindeutigen Hinweis, dass Sie im richtigen Modus sind, liefert danach der Ubuntu-Installer, sofern er das vorhandene



Parallelinstallation: Der Installer verkleinert automatisch die bestehende Partition (links), um Platz für Ubuntu (rechts) zu schaffen. Mit der Maus verändern Sie die Kapazitäten nach Bedarf.

System anzeigt und die Option „Ubuntu neben [XXX] installieren“ anbietet oder auch allgemein „Ubuntu daneben installieren“, wenn mehrere Systeme vorliegen.

Hinweis „Secure Boot“: Uefi-Installationen haben einen weiteren Fallstrick. Die Uefi-Funktion „Secure Boot“ verhindert das Booten nicht signierter Systeme, was den Start von Schadsoftware verhindern soll. Im Unterschied zu Ubuntu-Derivaten besitzen aber offizielle Ubuntu-Editionen eine „Secure Boot“-Signatur. Nur wer selbst kompilierte Kernel oder Treiber einsetzen will, muss „Secure Boot“ im Uefi-Bios deaktivieren („Bios Features → Security“ oder ähnlich).

Starten Sie im Livesystem das Setup über das Desktopicon. Was das Fenster „Installationsart“ dann anbietet, hängt von der Situation ab. Wir gehen hier von einer Parallelinstallation neben Windows aus, jedoch gelten diese Infos auch für ein bereits bestehendes Linux-System im Uefi-Modus:

A. Gibt es nur eine Festplatte, die derzeit von Windows belegt ist, sehen Sie die Option „Ubuntu neben Windows Boot Manager installieren“. Nach einem Klick auf „Weiter“ schlägt der Assistent eine neue Aufteilung der Partitionen vor, indem er die Windows-Partition verkleinert und Platz für Ubuntu schafft. Die Partitionsgröße lässt sich ändern, indem Sie die Aufteilungsmarkierung mit der Maus verschieben.

B. Ist neben einem installierten Windows oder Linux eine freie Partition vorhanden,

erkennt der Installer das automatisch. Auch in diesem Fall wählen Sie die Option „Ubuntu neben Windows Boot Manager installieren“.

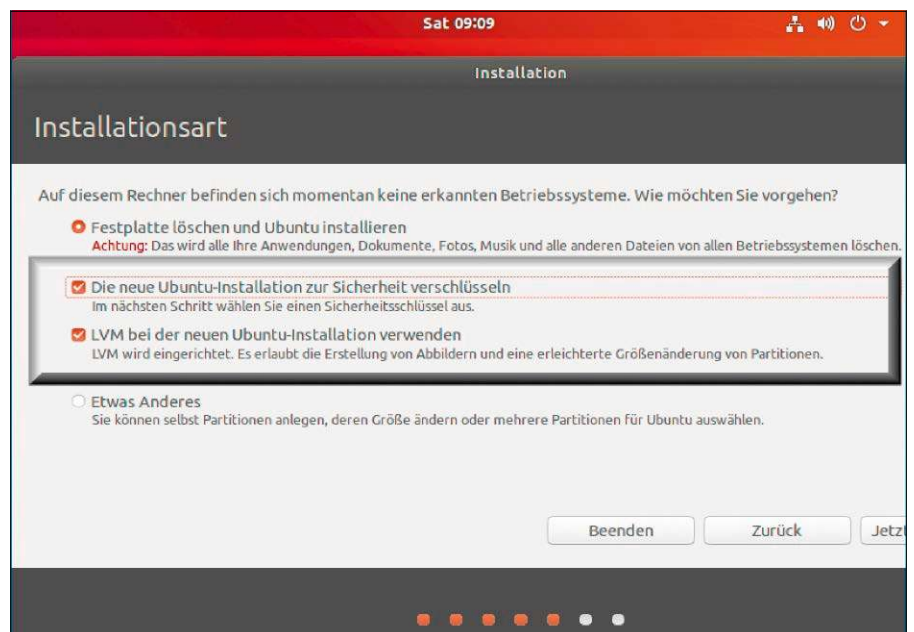
C. Sind zwei oder mehr Systeme vorhanden, dann führt das Angebot, „Ubuntu neben [XXX]“ zu installieren, zu einer weiteren Aufteilung und Partitionierung wie unter Variante A. Wenn Sie das neue System nicht zusätzlich installieren, sondern vielmehr eines der bestehenden Systeme durch das

neue ersetzen möchten, gehen Sie anders vor und wählen „Etwas Anderes“. Die weiteren Schritte sind so wie oben für die Installation auf USB beschrieben: Sie löschen in der Laufwerkliste mit der „-“-Schaltfläche die Partition des obsoleten Systems und erstellen dann im „Freien Speicherplatz“ mit der „+“-Schaltfläche eine neue Ext4-Partition mit dem Mountpunkt „/“.

Die verschlüsselte Systempartition

Luks-verschlüsselte Systempartitionen sind der beste Schutz für Notebooks. Der Datenträger lässt auch beim Booten durch Fremdsysteme keinen Einblick in die Daten zu. Luks-Verschlüsselung (des Systems) ist nur bei der Installation möglich – nicht nachträglich. Die Ubuntu-Installer Ubiquity und Calamares bieten diese Option per einfachen Klick an. Der entscheidende Dialog im Installationsprogramm lautet „Installationsart“ (oder „Partitionen“). Beachten Sie, dass Sie für die Verschlüsselung dem Installer die gesamte primäre Festplatte überlassen müssen. Die Festplatte sollte leer sein oder nur noch Daten enthalten, die Sie nicht mehr benötigen.

Für Luks-Verschlüsselung wählen Sie „Festplatte löschen und Ubuntu installieren“. Darunter aktivieren Sie „Die neue Ubuntu-Installation ... verschlüsseln“ (Calamares: „Verschlüssele System“). Sobald Sie dies tun, wird der Punkt „LVM [...] verwenden“



Luks-Datenträgerverschlüsselung: Diese Option ist in allen Ubuntu's einfach einzurichten, sofern das neue System die komplette primäre Festplatte übernehmen darf.

aktiv. Der Logical Volume Manager (LVM) ist notwendig, um neben der kleinen Bootpartition die Luks-formatierte Partition und die virtuelle LVM-Partition unterzubringen, die bei korrekter Kennworteingabe unverschlüsselt ins Dateisystem geladen wird. Wenn Sie dann auf „Weiter“ klicken, folgt die Abfrage des Sicherheitsschlüssels (Kennwort). Dieser sollte eine gewisse Mindestkomplexität haben, aber für tägliche Eingabe zumutbar sein, denn das System startet später nur noch nach Kennworteingabe. Der Rest der Installation verläuft wie gewohnt. Wenn Sie später das System booten, erscheint stets die Abfrage „Please unlock disk [...]“. Dort geben Sie das Kennwort ein, um den Systemstart fortzusetzen.

Hinweis: Neben der Luks-Verschlüsselung gibt es für Desktopbenutzer keinen Anlass, bei der Installation „LVM“ zu aktivieren. Der Logical Volume Manager ist eine Abstraktionsschicht für Serversysteme mit flexiblen Kapazitätsansprüchen, um Festplatten zusammenzufassen und dynamisch zu erweitern.

Ubuntu Server: Netinstaller mit Highlights

Wer Ubuntu auf PC oder Notebook einrichten will, wird den Ubuntu Server kaum auf der Rechnung haben. Der kann aber auch ein Desktopsystem installieren und bietet dabei interessante Vorteile. Vom Ubuntu Server gibt es zwei unterschiedliche Installer: ein großes Installationsmedium, das die meisten Pakete mitbringt, und einen winzigen Netinstaller, der alles aus dem Internet bezieht. Die angesprochenen Vorteile bringt nur der kleine Netinstaller (65 bis 75 MB), den Sie von <http://cdimage.ubuntu.com/netboot/> beziehen können. Empfohlene Version ist 18.04 LTS. Ethernet ist technische Voraussetzung für diese Installationsmethode, WLAN wird nicht unterstützt. Nun zu den Vorteilen:

1. Den Ubuntu Server gibt es bis hin zu den jüngsten Versionen auch noch in 32-Bit-Ausführung. 32-Bit-Systeme gehen sparsamer mit dem Arbeitsspeicher um und sind daher erste Wahl für ältere Hardware mit bis zu vier GB RAM, auch wenn eine 64-Bit-CPU vorliegt.

2. LTS-Versionen von Ubuntu Server erhalten wie die Ubuntu-Hauptversion (Gnome) volle fünf Jahre Updatesupport. Für alle anderen offiziellen Editionen (Kubuntu, Xubuntu, Mate etc.) gilt dies bekanntlich



Netinstaller für Ubuntu Server: Diese Setupmethode eignet sich auch für Desktopinstallationen und hat dabei zwei Vorteile (maximale Supportdauer und 32 Bit).

nicht: Sie erhalten nur drei Jahre Unterstützung. Da der Netinstaller am Ende eine Auswahl des Desktops vorsieht, können Sie sich ein Kubuntu (KDE), Xubuntu (XFCE) et cetera nach Belieben einrichten – mit fünf Jahren Support.

Das kleine Abbild (mini.iso) des Netinstallers bietet nur einen einfachen textbasierten Installer. Der Ablauf ist aber analog dem grafischen Ubiquity und unterstützt auch Verschlüsselung und Parallelinstallation. Für unseren Tipp entscheidend ist der abschließende Dialog „Softwareauswahl“, der nicht nur Serverpakete wie Samba, Open SSH oder Lamp anbietet, sondern auch sämtliche Oberflächen, die Sie von offiziellen Ubuntu-Editionen kennen.

Die Installationsvariante „OEM install“

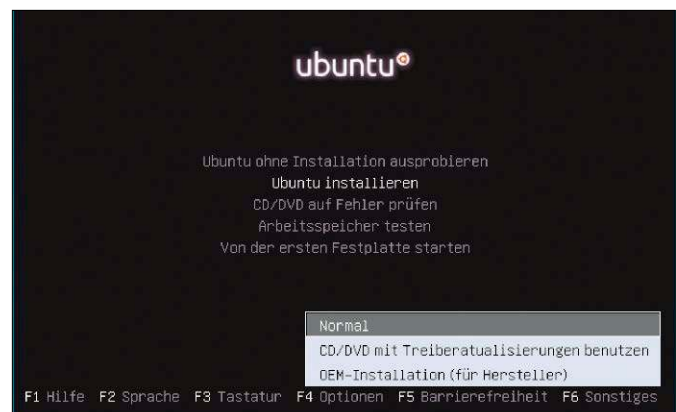
Wer Ubuntu für sich selbst installiert, hat mit der OEM-Variante keinerlei Vorteile. Aber die OEM-Installation bietet sich an für eine saubere Installation für Freunde oder Familienmitglieder. „Saubere“ deshalb, weil Sie das System mit einem temporären Konto „oem“ konfigurieren und der künftige

Besitzer später unabhängig über sein eigenes Konto entscheidet (Name, Kennwort). An den OEM-Installer kommen Sie nur, wenn Sie den Bootvorgang des Livesystems mit der Umschalt-Taste ausbremsen. Dann erscheint eine Auswahl mit fünf Optionen: Taste F4 blendet die „OEM Installation (für Hersteller)“ ein. Der Ablauf unterscheidet sich zunächst kaum von einer normalen Installation.

Ein wichtiger Unterschied ergibt sich beim Anlegen des Erstbenutzers („Wer sind Sie?). Dieser ist unveränderbar als „oem“ vorgegeben.

Der erste Start des so installierten Systems geht ohne Anmeldung zum Desktop. Nun können Sie im temporären Konto „oem“ das System optimieren. Nur systemweite Aktionen sind sinnvoll (Aktualisierung, Installationen, Netzwerk), benutzerspezifische Anpassungen nicht. Danach kann am Desktop der Link „Vorbereitung zur Auslieferung...“ geklickt und der Rechner dem Endbenutzer übergeben werden. Diesem wird dann der bekannte Dialog „Wer sind Sie?“ erneut angeboten, um nun den endgültigen Erstbenutzer anzulegen. ■

Nicht nur für Händler: Die OEM-Installation ermöglicht eine „saubere“ Systemeinstellung für Freunde und Bekannte.



Die 30 besten Systemtipps

Wenn Ubuntu oder Linux Mint auf halbwegs aktuelle Hardware trifft, sind diese Systeme bereits nach der Standardinstallation schnell und komfortabel. Mit den folgenden 30 Systemtipps gewinnen Sie aber Leistung, Kontrolle und Bedienkomfort hinzu.

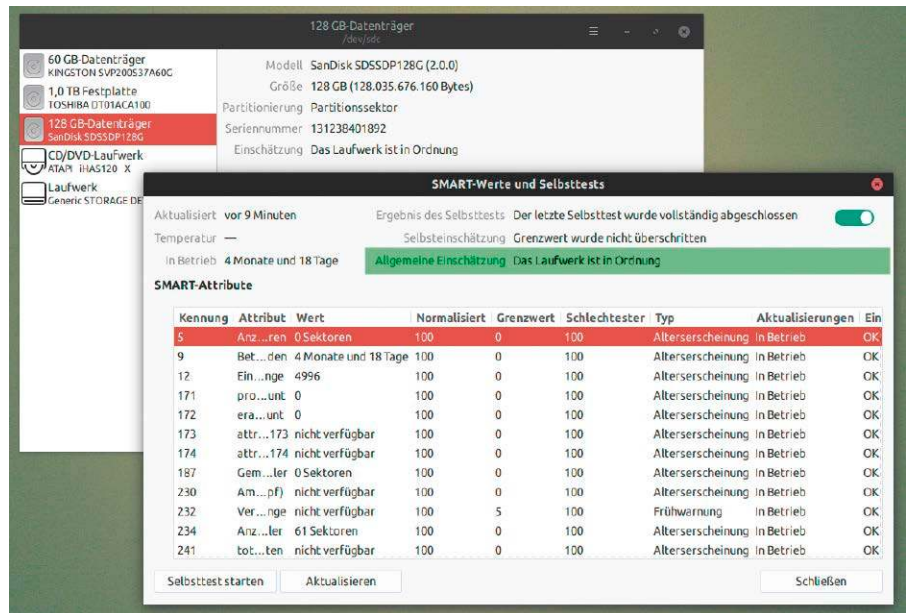
VON HERMANN APFELBÖCK

Die folgenden 30 Systemtipps beziehen sich auf Standards und Standardprogramme unter Debian-basierten Distributionen und insbesondere Ubuntu und Linux Mint. Sie dürften aber im Prinzip auch für andere Distributionen gelten, wobei aber die praktische Umsetzung und Programmbezeichnungen abweichen können.

1. Der Zustand von Festplatten (SMART)

Moderne Festplatten folgen dem SMART-Standard (Self Monitoring, Analysis and Reporting Technology) und können Auskunft über ihren Gesundheitszustand geben. Die einschlägigen grafischen Werkzeuge Gnome-Disks („Laufwerke“) und der KDE-Partitionmanager zeigen die SMART-Werte interner Festplatten an. Das KDE-Tool äußert sich unter „Gerät → Status“ recht knapp, jedoch ist eine positive „Gesamtbewertung: Healthy“ sowie die Angabe der fehlerhaften Sektoren im Prinzip ausreichend. Gnome-Disks sollte 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 umgehend ersetzen.

Per USB angeschlossene Festplatten berücksichtigt das KDE-Tool ebenfalls, Gnome-Disks allerdings nicht. Hier benötigen Sie das Paket „smartmontools“ (`sudo apt install smartmontools`) und dann folgenden



Diese SSD ist neuwertig und darf weitermachen: Gnome-Disks und die KDE-Partitionsverwaltung lesen die SMART-Werte von Datenträgern aus.

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. Messwerte wie Seek- und Read Errors sind kaum relevant.

2. Der Zustand des Notebookakkus

Der Akku ist Verschleißteil Nummer eins im Notebook. Wie es um die Komponente steht, können viele Linux-Desktops recht detailliert mit dem Tool „Energistatistiken“ ermitteln (gnome-power-statistics, mate-power-statistics etc.). Meist führt das unscheinbare Applet in der Systemleiste direkt zu diesem Tool. Neben irrelevanten Infos zeigt „Laptop-Akku → Details“ die Werte „Energie (Design/Entwurf)“ und „Energie wenn vollständig geladen“. Der erste ist ein idealer Referenzwert, der zweite zeigt die reale Akku-Ladekapazität. Ist die Differenz gravierend, sollten Sie den Nachkauf eines neuen Akkus erwägen.

Falls ein Desktop das grafische Statistiktool nicht mitbringt, lassen sich diese Werte auch auf der Kommandozeile mit `upower --monitor-detail` erfragen. Upower ist meistens Standard oder mit gleichnamigem Paketnamen schnell nachinstalliert.

3. Swapdatei komplett abschalten

Die Beobachtung der RAM-Auslastung im Taskmanager zeigt auf neuerer Hardware (und auch auf älterer Hardware mit einem dafür angemessenen Linux) praktisch immer, dass keine RAM-Auslagerung auf Festplatte stattfindet. Bei Rechnern mit acht oder 16 GB ist das Dauerzustand. Folglich können Sie dort die Swapdatei komplett abschalten. Das ist mit wenigen Handgriffen erledigt: Im laufenden System beenden diese beiden Terminalbefehle

```
sudo swapoff /swapfile
```

```
sudo rm /swapfile
```

die Auslagerung und löschen die Auslagerungsdatei. Zuletzt deaktivieren Sie in der Datei „`/etc/fstab`“ die Zeile

```
/swapfile ...
```

durch das Kommentarzeichen „`#`“.

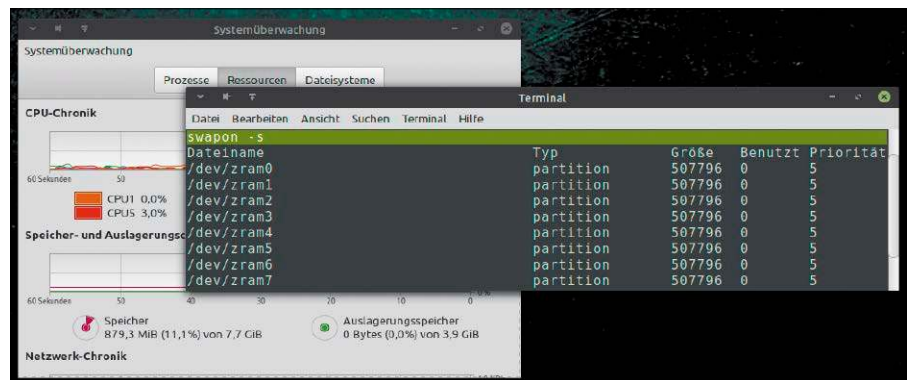
Beachten Sie, dass der Ruhezustand „Bereitschaft“ (Suspend to RAM) weiterhin funktioniert. „Hibernation“ (Suspend to Disk) ist derzeit in den aktuellen Ubuntu-Varianten ohnehin nicht mehr vorgesehen, seit Ubuntu von der Swappartition auf die Swapdatei umgestellt hat.

4. Komprimierte Auslagerung mit Zram

Zram ist eine interessante Alternative zur Auslagerung auf Festplatte. Das Kernel-



Zustand des Akkus ermitteln: Die Energistatistiken zeigen den Referenzwert „Energie (Design)“ oder „Energie (Entwurf)“, der von „vollständiger Ladung“ nicht zu weit abweichen sollte.



Zram reserviert je nach RAM und CPU erhebliche Speicheranteile. Wie Sie im Bild sehen (0 Bytes von 3,9 GB), wird aber kein RAM abgezweigt, solange dies nicht erforderlich ist.

Modul reserviert einen Teil des Arbeitsspeichers, um dort mehrere RAM-Disks anzulegen, die als komprimierter Auslagerungsspeicher bei Engpässen dienen. In den Standardeinstellungen reserviert Zram die Hälfte des verfügbaren Arbeitsspeichers, teilt diesen durch die Anzahl der verfügbaren CPU-Kerne und richtet pro Kern ein

Blockgerät ein. Bei einer CPU mit vier Kernen, entstehen vier Swapgeräte mit der Bezeichnung „`/dev/zram0`“, „`/dev/zram1`“ etc. Der Speicher wird aber dynamisch vergeben: Solange nichts auszulagern ist, nimmt Zram nichts in Anspruch. Erst wenn Auslagerung benötigt wird, geht RAM nach Bedarf vom physikalisch vorhandenen RAM

POWERTIPP 1: STANDBY-MODUS FÜR DATENLAUFWERKE

Bei Laufwerken, die nur Daten enthalten, können Sie Stromverbrauch und Lebensdauer durch Standby-Abschaltung deutlich verbessern. Für interne Datenfestplatten kann das Systemtool Gnome-Disks („Laufwerke“) über „Laufwerkseinstellungen → Bereitschaft“ den Timer für den Ruhezustand festlegen. Dort gibt es einen Schieberegler, ab welcher Frist der Inaktivität das Gerät in den Standby-Modus geschaltet werden soll.

Bei USB-Festplatten kommt man nur manuell mit dem Tool `hdparm` ans Ziel. Ermitteln Sie im Terminal zunächst mit `blkid`

die Laufwerke, Bezeichnungen und UUID-Kennungen. Ist die gewünschte Festplatte beispielsweise „`/dev/sdb`“, dann aktivieren Sie mit folgendem Befehl den Ruhezustand:

```
sudo hdparm -y /dev/sdb
```

Wenn das prinzipiell funktioniert, können Sie eine automatische Abschaltung festlegen:

```
sudo hdparm -S 180 /dev/sdb
```

Der Wert hinter „`-S`“ steht für „180 x 5 Sekunden“, also 15 Minuten. Diese Konfiguration wirkt allerdings nur bis zum nächsten Neustart des Systems. Für eine dauerhafte Änderung bearbeiten Sie die „`hdparm`“-Konfigurationsdatei:

```
sudo gedit /etc/hdparm.conf
```

Fügen Sie im Editor folgende Zeile am Ende der Datei an:

```
/dev/disk/by-uuid/[UUID] { spindown_time = 180 }
```

Den Platzhalter [UUID] ersetzen Sie – ohne die Klammern – durch die zuvor mit `blkid` ermittelte UUID.

ab. Zram befindet sich in den Paketquellen von Ubuntu und lässt sich mit minimalen Aufwand einrichten:

```
sudo apt install zram-config
```

Damit ist das Modul sofort aktiv, wie Sie mit `swapon -s` leicht kontrollieren können.

Wir empfehlen Zram als Ersatz für die Auslagerungsdatei auf Rechnern mit guter RAM-Ausstattung. Zram soll aber auch auf Rechnern mit geringem Speicher (Raspberry & Co.) Vorteile bringen, da die Auslagerung ins RAM wesentlich schneller ist und effiziente Komprimierung für minimalen Verbrauch sorgt. Zram lässt sich durch Deinstallieren von `zram-config` wieder abschalten.

5. Auslagerungsaktivität anpassen (Swappiness)

Wer die Auslagerung nicht abschalten möchte, kann über den „Swappiness“-Wert das Verhalten steuern. Der Wert darf zwischen zehn und 100 liegen. Je höher der Wert, desto aktiver schreibt der Kernel Speicherseiten aus dem RAM in die Swapdatei. Der voreingestellte Standard liegt bei 60. Ein niedriger Wert kann bei guter RAM-Ausstattung, aber langsamer mechanischer Platte vorteilhaft sein. Umgekehrt kann ein hoher Wert die Systemleistung bei wenig RAM verbessern, sofern die Swapdatei auf einer schnellen SSD liegt. Mit diesem Befehl `sudo sysctl vm.swappiness=90`

ändern Sie den Wert temporär. Um einen Wert dauerhaft festzulegen, müssen Sie folgende Konfigurationsdatei bearbeiten:

```
sudo nano /etc/sysctl.conf
```

Suchen Sie in der Datei nach „`vm.swappiness`“ und ändern Sie den Wert: `vm.swappiness=90`

Falls die betreffende Zeile fehlt, fügen Sie sie am Ende der Datei hinzu:

6. Einfacheres Systempasswort

Wer über sudo das System verwaltet, muss sein Systempasswort sehr häufig eingeben. Komplexe und lange Kennwörter sind eher lästig – und auf einem Desktopsystem auch nicht notwendig. Abgesehen vom Erstbenutzer, der bei der Installation eingerichtet wird, haben Ubuntu & Co. allerdings erhöhte Komplexitätsanforderungen an das Passwort für alle weiteren Konten. Das gilt auch

bei Passwortänderungen für das Erstbenutzerkonto.

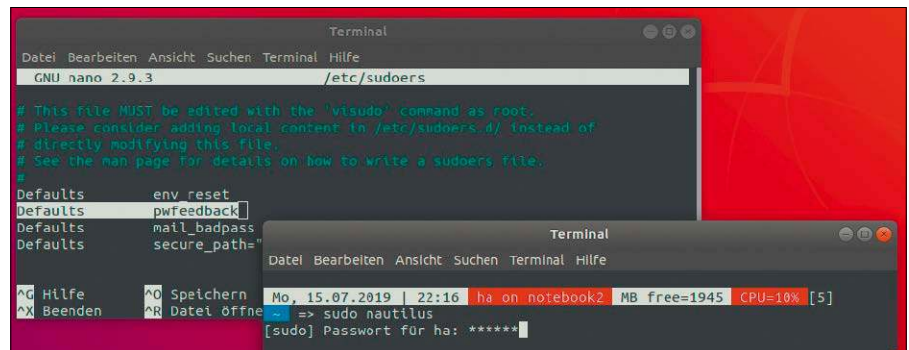
Wie immer unter Linux gibt es eine Stelle, um auch die Standards zu steuern: Öffnen Sie die folgende Datei

```
sudo nano /etc/pam.d/common-password
```

mit root-Recht, so finden Sie in der ersten „`password`“-Zeile die Anweisung „`obscure`“. Das erzwingt eine Mindestkomplexität des Passworts (Sonderzeichen) und kann einfach gelöscht werden. Durch die Ergänzung „`minlen=6`“ (Beispiel) am Ende derselben Zeile können Sie außerdem die Mindestlänge auf den gewünschten Wert herabsetzen.

7. Sudo-Passworteingabe mit Kontrolle

Standardmäßig schreibt man im Terminal das sudo-Kennwort ohne Rückmeldung im



Das Tool sudo nach der Konfigurationsänderung: Sternchen bei der Passworteingabe dienen als Rückmeldung der bereits getätigten Tastatureingaben.

POWERTIPP 2: RAMDISK ALS ZWISCHENDEPOT

16 GB RAM sind auf heutigen Notebooks keine Ausnahme

mehr. Für den typischen Einsatz mit Office und Mediaplayer ist solche Ausstattung purer Luxus, mit dem sich aber Sinnvolles anfangen lässt. Wenn Sie einen zentralen Ordner, über den Sie den ganzen Datenaustausch inklusive Downloads abwickeln, in eine schnelle Ramdisk verlegen, entstehen mehrere Vorteile: mehr Leistung, automatische Entsorgung beim Herunterfahren, Schonung von SSD/Festplatte, Nutzung der brachliegenden RAM-Ressourcen.

Eine Ramdisk ist über die Datei „`fstab`“ schnell erstellt:

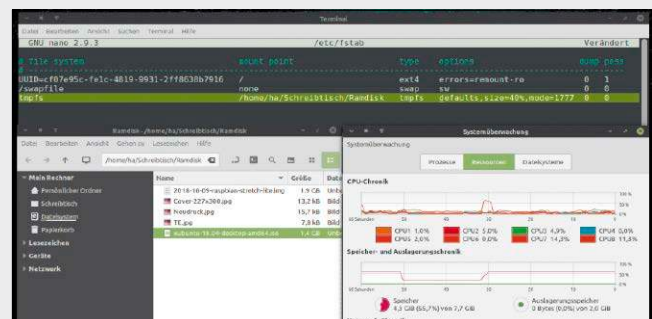
```
sudo nano /etc/fstab
```

Hier fügen Sie die weitere Zeile

```
tmpfs /home/ha/Schreibtisch/Ramdisk tmpfs
defaults,size=40%,mode=1777 0 0
```

hinzu (der Mountpfad des Beispiels muss angepasst werden). Nach dem Speichern starten Sie Linux neu. Die angegebene Kapazität (hier 40 Prozent des Speichers) wird nicht statisch abgezweigt. Bleibt der Mountpunkt ungenutzt, verbraucht die

Ramdisk auch keinen Speicher, wovon Sie sich mit einem Taskmanager wie etwa dem Gnome-System-Monitor leicht überzeugen können. Der Umgang mit Ramdisk-Daten erfordert etwas Disziplin und Gewöhnung, weil die Daten beim Shutdown gelöscht werden.



Ein Tipp für brachliegendes RAM: Die in der „`fstab`“ eingetragene Ramdisk dient hier als temporäres Datendepot in einem Desktopordner.



Multimonitor-Layout mit xrandr-Script: Den komplexen Befehl kann das grafische xrandr als Shell-Script ablegen, das dann als Autostart dauerhaft für das gewünschte Layout sorgt.

Blindflug – eine auf Desktopsystemen eher paranoide Sicherheitseinstellung, um die Länge des Passworts zu verbergen. Es ist aber kein Problem, sich die bereits getippten Buchstaben mit Stellvertreterzeichen „*“ anzeigen zu lassen. Der Aufruf

```
sudo visudo
```

öffnet die Datei „/etc/sudoers“ im voreingestellten Editor. Unter

```
Defaults env_reset
```

fügen Sie die zusätzliche Zeile

```
Defaults pwfeedback
```

ein. Nach dem Speichern (Strg-O) und Beenden des Editors (Strg-X) zeigt die sudo-Abfrage ein Sternchen pro eingegebenem Zeichen. Unter Linux Mint ist dies inzwischen bereits Standard.

8. Deutsche Systemanmeldung

Wer für sein Systempasswort keine Sonderzeichen benutzt, wird das Problem gar

nicht bemerken: Es gibt Fälle, wo zwar das komplette System auf Deutsch eingestellt ist, der Anmeldebildschirm jedoch englisches Tastaturlayout benutzt. Das führt dann bei Zeichen wie „z“, „y“, „ß“, „-“, „=“ zu Anmeldeproblemen. Lösung ist der Eingriff in die Datei „/etc/default/keyboard“. Die Datei enthält nur wenige Zeilen, die maßgebliche sollte

```
XKBLayout="de"
```

lauten.

9. Multimonitorbetrieb mit Xrandr-Autostart

Bei Multimonitorbetrieb lässt sich über die Systemeinstellungen die Konfiguration und Position der Bildschirme exakt festlegen. Es gibt aber Fälle, wo Systeme diese Einstellung nicht permanent speichern und die Einrichtung bei jedem Start erneut erfolgen müsste – und das wäre unzumutbar.

Unter der Haube nutzen die grafischen Werkzeuge das Tool xrandr, daher kann der passende xrandr-Befehl als Autostart das Problem lösen. Und noch besser: Die Syntax der komplexen xrandr-Kommandos müssen Sie nicht selbst ermitteln. Das kann Ihnen das grafische Tool arandr abnehmen (`sudo apt install arandr`). Damit arrangieren Sie die Bildschirme mit der Maus nach Wunsch und gehen dann auf „Layout → Speichern unter“. Das auf diesem Weg gespeicherte Shell-Script legen Sie dann als zusätzlichen Eintrag unter „Startprogramme“ ab.

10. Schriftgrößen optimieren (DPI)

Bei Standardeinstellungen ist die Bildschirmdarstellung je nach Monitorgröße und Auflösung nicht immer optimal. Viele Programme haben eigene Zoomfunktionen, aber es gibt auch systemweite Methoden. Die Auflösung herabzusetzen ist möglich, geht aber immer mit Qualitätsverlust einher. Bessere Ergebnisse erzielt eine Anpassung der Schriften.

- Der Gnome-Desktop kann über das Tool Gnome-Tweaks die Schriftgrößen stufenlos skalieren. Die Einstellung lautet dort „Schriften → Skalierungsfaktor“.
- Cinnamon unter Linux Mint zeigt in den normalen Systemeinstellungen unter „Schriften“ die allgemeine Option „Skalierungsfaktor der Schrift“. Sie können an gleicher Stelle aber auch die Schrittgrößen für einzelne Objekte im Detail anpassen.

POWERTIPP 3: RECHNER ABSCHALTEN UND AUFWECKEN

Wenn ein PC oder Server zwischen 22:00 Uhr abends und 8:00 Uhr morgens garantiert nicht gebraucht wird, liegt es nahe, ihn für diese zehn Stunden abzuschalten. Das spart Strom und verlängert die Lebenszeit der Hardwarekomponenten. Das Tool Rtcwake, Bestandteil des meist vorinstallierten Standardpakets „util-linux“, kann Rechner sowohl abschalten wie zeitgesteuert wieder einschalten. Im einfachsten Fall sieht ein Kommando so aus:

```
sudo rtcwake -m off -s 300
```

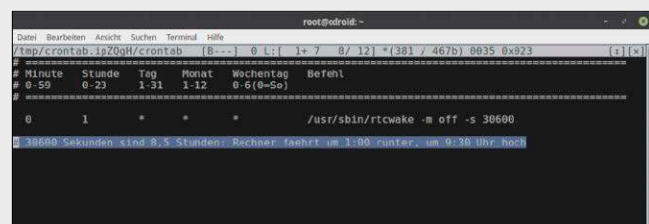
Der Befehl ist gut geeignet, um zu testen, ob die Hardware prinzipiell mitspielt. Der Schalter „-m“ bestimmt den Abschaltmodus „standby“, „mem“, „disk“, „off“ oder „no“. Das im Beispiel gewählte „off“ fährt das System komplett herunter und Parameter „-s“ gibt in Sekunden an, wann der Rechner wieder starten soll. Um rtcwake als Cronjob abzulegen, muss der Befehl in der Crontab von root untergebracht werden:

```
sudo crontab -e -u root
```

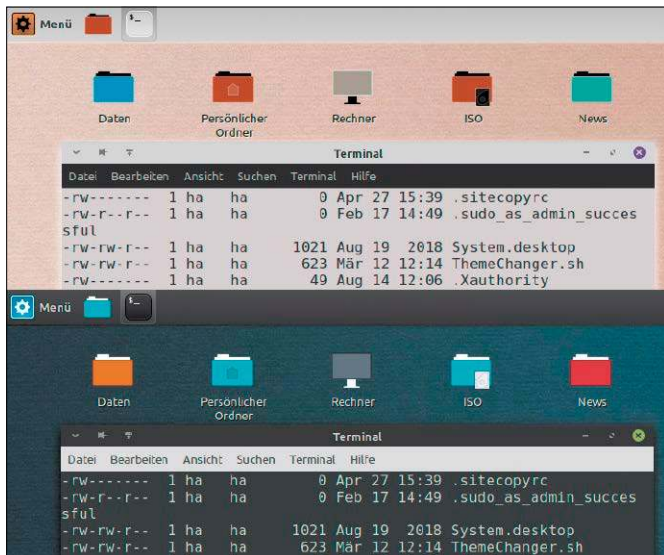
Folgender Cronjob

```
0 22 * * * /usr/sbin/rtcwake -m off -s 36000
```

schaltet den Rechner um 22:00 Uhr ab und startet ihn wieder nach 36 000 Sekunden um 8:00 Uhr.



Ein Cronjob für Rtcwake: Dieser Rechner wird um 1:00 Uhr beendet und hat ab 9:30 Uhr wieder Dienst.



Einfache Farbumstellung mit Xcalib: Das hilft bei ungünstigen Lichtverhältnissen und funktioniert auf jedem Linux.

Desktop invertieren kann, ist das Programm Xcalib. Xcalib ist unter Ubuntu und Mint mit

`sudo apt install xcalib` schnell nachinstalliert. Zum Invertieren der Bildschirmfarben genügt dann dieser Befehl („-i“ für „inverse“, „-a“ für „alter“):

`xcalib -i -a`
Mit demselben Befehl kehren Sie wieder auf die normale Einstellung zurück. Wirklich elegant wird dieses Tool, wenn Sie ihm unter „Einstellungen → Tastatur → Tastaturkürzel“ noch einen einprägsamen Hotkey spendieren.

Theoretisch lassen sich ähnliche Bildschirmoptimierungen durch einen Wechsel zu einem „HighContrast“-Theme erzielen. Xcalib hat aber den enormen Vorzug, auf jedem Desktop und ohne Recherche der verfügbaren Themen zu funktionieren.

12. Shutdown mit Zeitangabe

Nicht selten ergibt sich die Situation, dass man bei Arbeitsende das System beenden möchte, aber nicht beenden kann, weil ein Kopiervorgang oder ein Download noch einige Zeit läuft. Abzuwarten wäre lästig und auch unnötig, denn das Shutdown-Kommando beherrscht sowohl Uhrzeiten als auch Fristen:

```
sudo shutdown -P 23:00
sudo shutdown -P 60
```

Der erste Befehl beendet das System exakt um 23:00 Uhr, der zweite nach 60 Minuten. Das sudo-Kennwort wird sofort abgefragt, sodass Sie anschließend den Rechner verlassen können.

13. Maßnahme gegen Desktophänger

Die Reparaturmethoden der Linux-Desktops bei hängender Oberfläche sind nicht einheitlich.

Die Hotkeys Strg-Alt-Esc und Strg-Alt-Rücktaste sind relativ verbreitet, aber keineswegs überall gültig. Folgender Trick sollte auf den meisten Distributionen funktionieren, indem er den Display-Manager neu startet (sudo-Recht ist erforderlich). Der jeweils verwendete Display-Manager lässt sich wiederum vorher aus einer Konfigurationsdatei ermitteln:

```
dm=$(basename "$(cat /etc/X11/default-display-manager)")
sudo service $dm restart
```

Als knappes Alias „redesk“ ersparen Sie sich den Tippaufwand:

- KDE zeigt in den Systemeinstellungen unter „Schriftarten“ den Punkt „DPI für Schriften erzwingen“ und daneben das Eingabefeld für den gewünschten Wert.
- Der Budgie-Desktop skaliert in den „Budgie Desktop Einstellungen“ unter dem Punkt „Schriftarten“.
- LXQT zeigt den maßgeblichen Punkt unter „Erscheinungsbild → Schriften“.
- Bei Mate gehen Sie in den Systemeinstellungen auf „Erscheinungsbild → Schriften“ und auf „Details“. Ganz oben lässt sich der DPI-Wert exakt einstellen, sofern Sie vorher die automatische Erkennung abschalten.
- Unter XFCE finden Sie in den Systemeinstellungen den Punkt „Einstellungsbearbei-

tung“. Hier geht es ganz nach unten zur Kategorie „xsettings“. Im Wertefenster finden Sie dann erneut ganz unten den Eintrag „Xft“ mit dem Unterpunkt „DPI“. Den aktuellen Wert können Sie hier durch einen eigenen ersetzen.

11. Bildschirmfarben invertieren

Bei sehr ungünstigen (hellen) Lichtverhältnissen wird Text besser lesbar, wenn die typischen Farbverhältnisse (dunkel auf hell) umgekehrt werden. Ad hoc und auf Webseiten mit miserablen Kontrasten kann es genügen, mit Strg-A alles zu markieren und damit die Farbverhältnisse umzuschalten. Ein praktisches Tool, das den kompletten

POWERTIPP 4: GRAFISCHE OBERFLÄCHE AUS- UND EINSCHALTEN

Die Linux-Option, die grafische Oberfläche einfach aus- und (bei Bedarf) wieder einzuschalten, ist vor allem für Platinenrechner interessant. Besonders wichtig wird dieser Trick bei Mini-PCs mit geringer Systemauswahl – wenn beispielsweise nur ein Ubuntu Mate zur Verfügung steht, dessen Desktop aber praktisch nicht benötigt wird. Typisch ist aber auch, dass die Oberfläche zur Einrichtung willkommen ist, danach aber nicht mehr. Wenn Sie nur noch die Serverdienste brauchen (Samba, SSH, Apache), dann lässt sich auf allen Ubuntu-basierten Systemen die Oberfläche mit

```
sudo systemctl set-default multi-user.target
```

abschalten. Die Maßnahme gilt ab dem nächsten Neustart. Je nach verwendeter Oberfläche werden dadurch einige Hundert MB RAM sowie CPU-Ressourcen frei. Mittels des Kommandos

```
sudo systemctl set-default graphical.target
```

ist der Desktop bei Bedarf auch wieder dauerhaft einzuschalten. Die abgeschaltete Oberfläche können Sie auf der Konsole außerdem jederzeit manuell mit

```
startx
```

starten.


```
alias redesk='DM=$(basename "$(cat
/etc/X11/default-display-
manager)");sudo service $DM
restart'
```

Nach dieser Aktion erscheint der Anmeldebildschirm für eine neue Desktopsitzung. Die Methode funktioniert auch in einer virtuellen Konsole (Strg-Alt-F1), falls die grafische Oberfläche nicht mehr reagiert.

14. Fensterkiller Xkill optimal nutzen

Xkill ist praktisch überall vorinstalliert. Es beendet grafische Programme, deren Fenster nicht mehr reagieren, ohne dass Sie Programmname, Fenstername oder PID kennen müssen. Beim Aufruf von xkill verwandelt sich der Mauszeiger in ein Kreuz, mit dem Sie das Programm mit linker Maustaste anklicken und damit beenden. Die rechte Maustaste beendet xkill ohne Aktion.

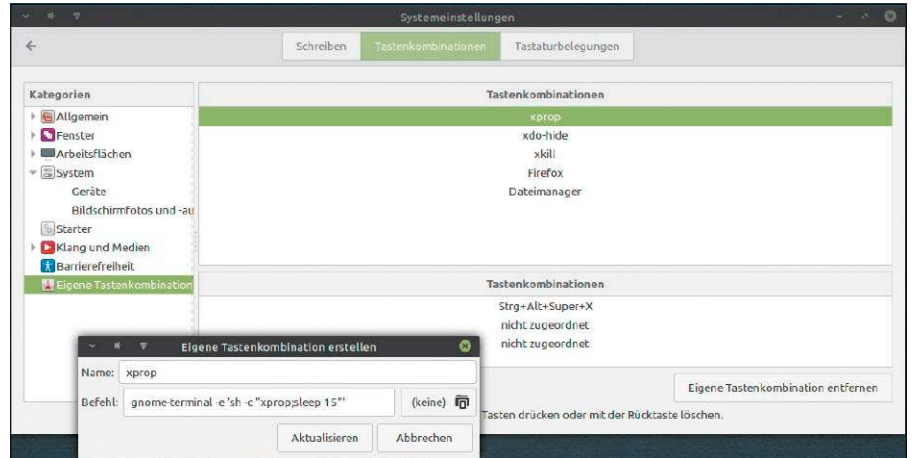
Mit dem lästigen manuellen Terminalaufruf `xkill` ist das Tool aber kaum die Hälfte wert. Einige Distributionen verwenden den Hotkey Strg-Alt-Esc, doch meistens ist kein globaler Hotkey eingestellt. Das sollten Sie unter „Systemeinstellungen → Tastatur → Tastaturkürzel“ ändern (oder ähnlich lautend), indem Sie xkill unter „Eigene Tastaturkürzel“ eintragen und dem Programm durch Drücken der Tastenkombination Strg-Alt-Esc, Strg-Alt-K oder wie gewünscht zuweisen.

15. Programminfo Xprop optimal nutzen

Für xprop gilt Ähnliches wie für xkill. Es ist überall Standard, benötigt aber einen manuellen Aufruf im Terminal. Das häufigste Motiv, xprop zu verwenden, ist die Frage nach dem Programmnamen eines Fensters. Also etwa die Frage: Wie lautet der Name des Dateimanagers, den ich gerade benutze? Nach dem Start von xprop verwandelt sich der Mauszeiger in ein Kreuz, mit dem Sie auf das gewünschte Fenster klicken. Im Terminal erscheint dann der zugehörige Programmname. Wer xprop oft benutzt, sollte sich einen Hotkey zurechtlegen.

Da für die Infoausgabe ein Terminal benötigt wird, ist der Befehl für den xprop-Hotkey schwieriger als bei xkill. Folgende Variante funktioniert auf Ubuntu und Linux Mint mit Gnome-Terminal:

```
gnome-terminal -e 'sh -c
"xprop;sleep 10"'
```



Cleverer Hotkey: Zum Abfragen von xprop-Infos genügt die eingestellte Tastenkombination. Das Terminal zur Ausgabe der xprop-Infos startet gleich mit.

Die Anzeigedauer der xprop-Information, hier zehn Sekunden, ist beliebig einstellbar.

16. Wartezeit des Grub-Bootloaders

In Dual- oder Multiboot-Umgebungen wartet der Grub-Bootloader standardmäßig zehn Sekunden auf eine Auswahl, bis er das erste, oberste Defaultsystem automatisch wählt. Vor allem dann, wenn man überwiegend dieses System nutzt, ist es sinnvoll, den Eintrag

```
GRUB_TIMEOUT=10
```

in der Datei „`/etc/default/grub`“ etwa auf „3“ (Sekunden) zu verkürzen und danach mit dem Kommando

```
sudo update-grub
```

die Bootumgebung neu zu initialisieren.

17. Der Programmturbo Preload

Das Tool Preload beschleunigt häufig oder über „Startprogramme“ immer gestartete Anwendungen. Der einfache Dienst proto-

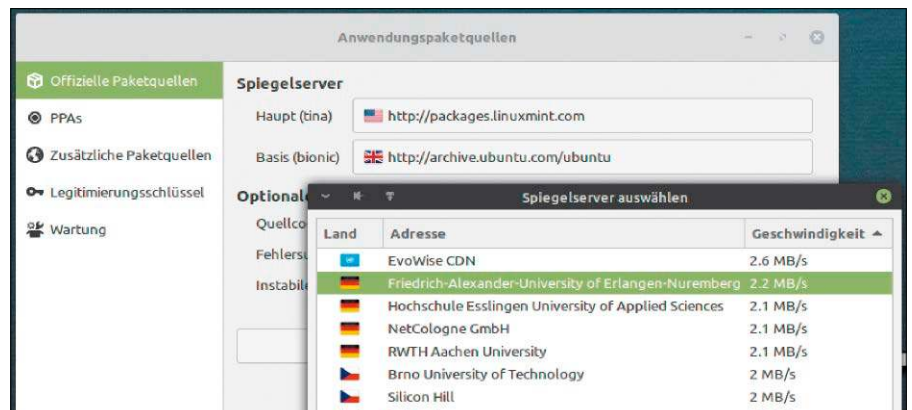
kolliert Ihre Programmvorlieben und lädt die Favoriten vorab in den Arbeitsspeicher. Der eigentliche Programmstart verläuft dadurch deutlich schneller. Preload ist in den Paketquellen verfügbar und in Ubuntu und Co. mit

```
sudo apt install preload
```

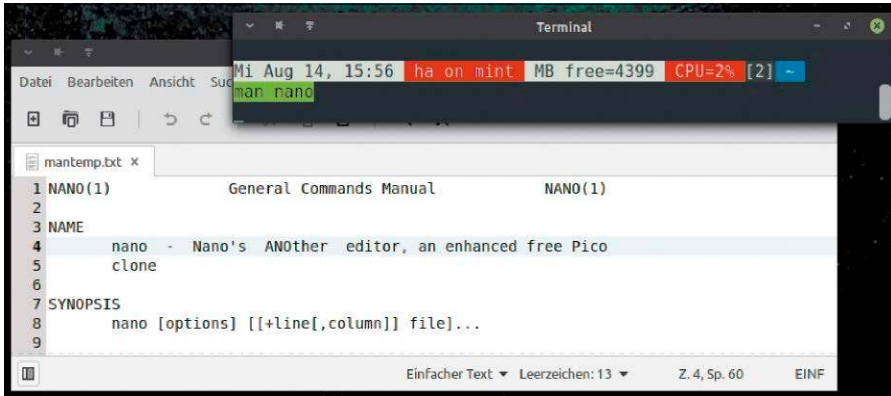
schnell nachinstalliert. Theoretisch können Sie in die Konfiguration des einfachen Tools manuell eingreifen („`/etc/preload.conf`“), dies ist jedoch weder erforderlich noch inhaltlich ergiebig.

18. Schnellen Spiegelserver einstellen

Für Installationen und Updates benötigen Sie einen Server, der die Paketquellen bereitstellt und möglichst schnell ausliefern soll. Je schneller Ihre Internetverbindung ist, desto mehr profitieren Sie von einem schnellen Spiegelserver. Ubuntu und Linux Mint können den geeignetsten deutschen Server selbst ermitteln: Dazu gehen Sie in



Lokaler und schneller Server für Updates und Installationen: Ubuntu und Linux Mint zeigen durch Schnelltests die geeignetsten Kandidaten für den Softwarebezug.



Man-Hilfeseiten in den grafischen Editor umleiten: Das vereinfacht Navigation und Suche in den unbeliebten, aber unvermeidlichen Manpages.

Ubuntu auf „Anwendungen & Aktualisierungen“, in Linux Mint zu den „Anwendungspaketquellen“. Dort finden Sie den aktuell eingestellten Spiegelserver. Diesen können Sie anklicken und erhalten unter Linux Mint direkt eine Liste der schnellsten Server, unter Ubuntu gehen Sie auf „Anderer“, wonach Sie im Unterfenster die Option „Besten Server auswählen“ antreffen. Auch Ubuntu macht dann einige Verbindungstests und schlägt dann einen Server vor. Für Deutschland immer eine gute Wahl ist *netcologne.de*, das Sie auch direkt manuell auswählen können.

19. Bash-History mit Schlüsselwörtern

Ein einfacher Trick, um interessante Terminalbefehle bei Bedarf schnell wiederzufinden, besteht in der Kommentierung der Kommandos durch Schlüsselwörter.

Ein Beispiel:

```
lsblk -o name,fstype,uuid,size,type,
mountpoint,label # Festplatte
Disk
```

Der so eingegebene Befehl funktioniert wie gewohnt; alles ab dem Kommentarzeichen „#“ wird ignoriert. Der Befehl landet aber inklusive Kommentar in der Datei „*~/.bash_history*“. Folglich können Sie später in der Historysuche (Strg-R) ein Schlüsselwort wie „Festplatte“ eingeben und die Suche wird Ihnen die Befehle mit diesem Kommentar anbieten.

20. Besser lesbare Manpages

Manpages sind eine doppelte Zumutung: erstens inhaltlich, weil sie niemals anschauliche Beispiele enthalten, zweitens technisch aufgrund des antiken Standardviewers. Immerhin dieser zweite Mangel lässt

sich ohne großen Aufwand beheben, indem Sie den Text an den Editor Ihrer Wahl schicken (hier gedit):

```
function man ()
{
/usr/bin/man $* > ~/mantemp.txt
if [ -s ~/mantemp.txt ]; then
gedit ~/mantemp.txt & disown
fi
}
```

Wenn Sie diese Funktion in die Datei „*~/.bashrc*“ eintragen, erhalten Sie angeforderte Hilfeseiten künftig im grafischen Editor angezeigt.

21. Reduzieren von Systemmüll

Die Paketverwaltung von Debian, Ubuntu, Mint speichert die heruntergeladenen Pakete bei Installation und Aktualisierung in einem Zwischenspeicher unter „*/var/cache/apt/archives*“. Diesen Cache, der über Monate und Jahre erheblich anwachsen kann, leeren Sie mit

```
sudo apt-get clean
```

am besten regelmäßig.

Eine weitere Halde von Systemdaten kann sich durch deinstallierte Software ergeben, deren abhängigen Pakete weiter auf dem System verbleiben. Der Befehl

```
sudo apt-get autoclean
```

kann solche Pakete ermitteln und löschen. Das Dateisystem Ext4 reserviert auf jeder Partition einen Speicherbereich für das Konto root. Das soll gewährleisten, dass sich root auch auf voller Systempartition noch anmelden kann. Aus historischen Gründen liegt der reservierte Platz bei fünf Prozent, das sind bei einer 240-GB-SSD immerhin 12 GB. Die Reserve können Sie mit dem Tool *tune2fs* gefahrlos verringern:

```
sudo tune2fs -m 3 /dev/sda1
```

Dies verringert die Anzahl der reservierten Blöcke auf „*/dev/sda1*“ auf drei Prozent.

22. Benutzerdateien komprimieren

Für effiziente Komprimierung ist Tar erste Wahl. Ein typischer tar-Befehl zum Einpacken beginnt mit einigen Optionen, nennt dann das Zielarchiv und zuletzt Ordnerpfad oder Dateimaske der zu sichernden Daten:

```
tar -czvf depot.tar.gz Depot
```

```
tar -czvf pdf.tar.gz *.pdf
```

Das Beispiel geht davon aus, dass sich tar im richtigen Verzeichnis befindet.

Die Nutzung gepackter „tar.gz“-Archive ist unter Ubuntu und Mint mit dem Archivmanager praktisch genauso komfortabel wie der Umgang mit unkomprimierten Daten im Dateimanager. Es ist also nicht nötig, die Daten für jede Nutzung auszupacken.

23. Samba versus SSH

Aufräumarbeiten beim Dateibestand von Linux-Servern lassen sich auf Netzfrequenzen über Samba erledigen. Der effiziente Weg ist das aber definitiv nicht, vor allem wenn diese Arbeiten viele Löschaktionen beinhalten.

Verschieben, Löschen, Aufräumen ist über das SSH-Terminal und damit direkt am Server weitaus schneller als mit der Vermittlung über Samba. Aufräumen sollten Sie daher immer mit dem SSH-Terminal – und hier am bequemsten mit dem Midnight Commander!

24. Hostname (Rechnername) ändern

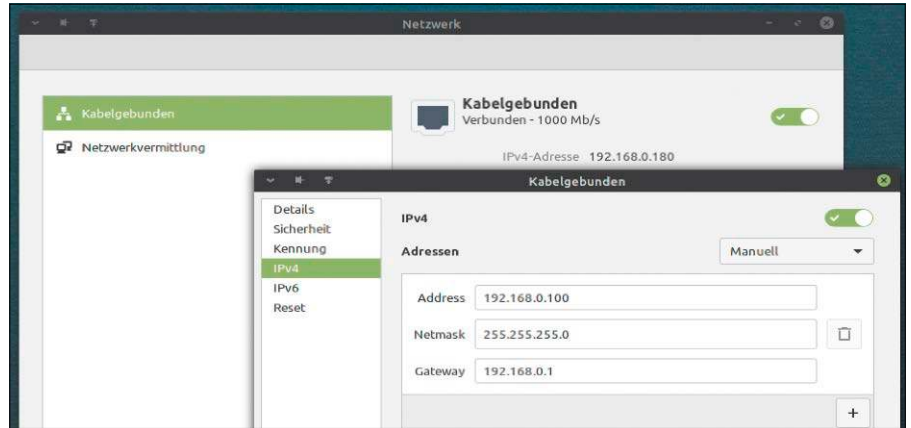
Bei der Installation eines Desktopsystems bestimmen Sie den Hostnamen des künftigen Systems selbst. Bei den komplett ausgelieferten Systemimages für Platinenrechner ist der Hostname hingegen vorgegeben und wenig aussagekräftig („*raspberrypi*“, „*odroid*“). Und auch bei der Installation von Desktopsystemen kann sich ein achtlos vergebener Hostname später als ungünstig herausstellen: Hostnamen erscheinen in der Routerübersicht und werden als Browseradressen und in Netzkommandos genutzt. Eine nachträgliche Änderung ist aber kein Problem. Sie öffnen mit root-Recht folgende Datei

```
sudo gedit /etc/hostname
```

und tragen statt des bisherigen Namens den neuen ein. Danach starten Sie den Rechner neu.

25. Feste IP für Linux-Geräte

Server sowieso, aber letztlich jeder Linux-Rechner, der in irgendeiner Weise etwa per SSH oder Samba erreichbar ist, benötigt eine feste IPv4-Adresse im lokalen Netz. Nur so ist der Rechner via SSH, Samba im Dateimanager oder Apache im Browser zuverlässig erreichbar. Die gewünschte IP können Sie über das Netzwerkkaplet in den Systemeinstellungen anfordern, indem Sie unter „IPv4“ die automatische DHCP-Vergabe abschalten und die Methode „Manuell“ einstellen. Darunter geben Sie die Wunsch-IP im lokalen Adressraum ein, darunter „255.255.255.0“ als Netzmaske und die Router-IP als „Gateway“. Nach dem nächsten Neustart gilt die neue IP-Adresse, sofern sie nicht anderweitig vergeben ist. Alternativ funktioniert das auch über die Konfigurationsoberfläche des Routers. In der Fritzbox (<http://fritz.box>) finden Sie unter „Heimnetz → Netzwerkverbindungen“ ganz unten die Schaltfläche „Gerät hinzu-



fügen“. Hier geben Sie „Name“ (Hostname) und „MAC-Adresse“ des Geräts ein (siehe unten), darunter die Wunsch-IP. Die Fritzbox wird nun melden, dass das Gerät bereits unter einer anderen IP bekannt ist, und Sie müssen mit „OK“ bestätigen, dass

Sie die bisherige Einstellung überschreiben wollen. Danach starten Sie das Gerät neu. Hostname und die physikalische MAC-Adresse eines Rechners erfahren Sie mit den Terminalbefehlen `hostname` und `ip adress` auf dem jeweiligen Gerät. ■

Sie die bisherige Einstellung überschreiben wollen. Danach starten Sie das Gerät neu. Hostname und die physikalische MAC-Adresse eines Rechners erfahren Sie mit den Terminalbefehlen `hostname` und `ip adress` auf dem jeweiligen Gerät. ■

POWERTIPP 5: PLATZSPARENDE STARTERICONS

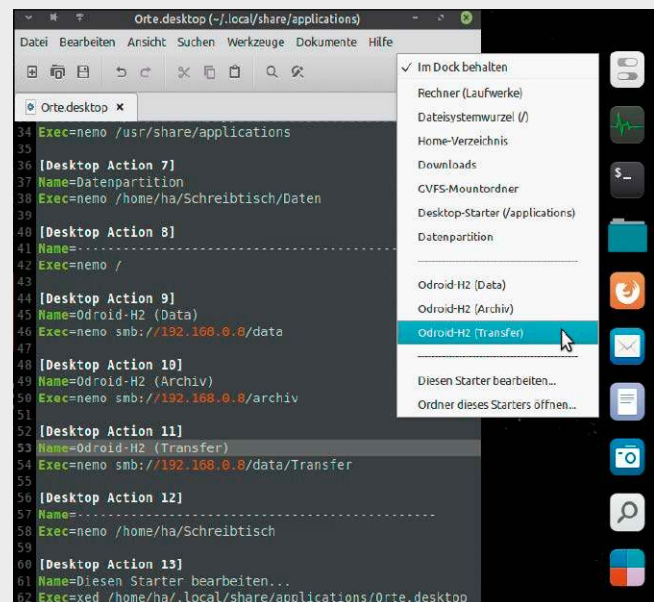
Starterverknüpfungen für Programme sind einfache Textdateien unter „/usr/share/applications“ mit der Endung „.desktop“ und einem Standardsatz von Direktiven wie „Name=...“, „Exec=[Programmaufruf]“ oder „Icon=[Icondatei]“. Das Format solcher Desktopdateien erlaubt aber nicht nur einen Programmaufruf, sondern eine beliebige Anzahl von Startern. Diese bietet das Startericon nach Rechtsklick im Kontextmenü an, sofern es in eine Starterleiste eingebaut ist. Ideal ist das Dock Plank (Paketname „plank“), aber auch das Starterdock von Ubuntu ist möglich.

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

Zum Einbau in den Starter von Ubuntu 18.xx/19.xx muss das Script nach „~/local/share/applications“ und dort ausführbar geschaltet werden. Nur an dieser Stelle berücksichtigt es die Gnome-Programmübersicht (das Symbol mit neun Punkten) und kann von dort per Rechtsklick und „Zu Favoriten hinzufügen“ in das Dock übernommen werden. Beachten Sie, dass im Ubuntu-Dock Script-Änderungen immer erst nach einer Neuanmeldung aktiv werden, während das Plank-Dock Änderungen im laufenden Betrieb einliest.

Die Script-Datei in der Abbildung zeigt das Prinzip: Unter „[Desktop Entry]“ ist die Hauptaktion für den Linksklick definiert. Der Eintrag „Actions=“ in der Hauptsektion meldet die nachfolgenden Zusatzaktionen an, die dann in den Untersektionen als „[Desktop Action <Name>]“ nur noch eine Bezeich-

nung und den Programmaufruf benötigen. Der Einfachheit halber nummerieren Sie dabei die „Actions“ einfach durch. Drei Beispiele auf <https://paste.ubuntu.com/p/2Tkrp8tH8b/> liefern Ihnen Vorlagen für solche Desktopdateien, um die einfache, aber doch lästige Tipparbeit auf ein Minimum zu reduzieren.



Das Dateimanager-Icon im Plank-Dock zeigt und lädt nach Rechtsklick eine ganze Reihe wichtiger Ordner. Die Abbildung zeigt auch einen Teil der dafür verantwortlichen Desktopdatei.

Tadelloser Linux-Desktop

Für Gnome zeigen die folgenden Deskoottipps eine Möglichkeit, beliebige Autostart-Einträge bequem mit einem grafischen Editor festzulegen. Zudem gibt es ein neues Panel für Gnome und einen Blick auf die Zukunft von KDE.

Ulauncher: Der bessere Ausführen-Dialog

Oft ist die Tastatur schneller als die Suche nach Programmen in Anwendungsmenüs. Unter KDE gibt es deshalb mit Krunner einen mächtigen Ausführen-Dialog, der Autovervollständigung von Programmnamen und viele Abkürzungen beherrscht. Gnome und seine nahen Verwandten wie Cinnamon haben demgegenüber nur einen simplen Befehlsstarter.

Der Ulauncher rüstet unter Ubuntu und seinen Derivaten einen Anwendungsstarter und Suchdialog nach, der Autovervollständigung, Zusatzfunktionen wie Rechenoperationen, Websuche und auch eine unscharfe Suche nach Dateien anbietet. Das in Python geschriebene Tool orientiert sich stark am beliebten Suchwerkzeug Alfred unter Mac-OS X und integriert eine wachsende Zahl an optionalen Plug-ins, die den Funktionsumfang weiter ausbauen können.

Obwohl sich der Ulauncher noch nicht in den Paketquellen Ubuntus findet, ist eine Installation nicht weiter schwer. Denn es gibt für fertige DEB-Pakete ein Repository der Entwickler, das Sie mit den beiden Terminalbefehlen

```
sudo apt-add-repository
  ppa:agornostal/
  ulauncher
sudo apt-get update
ins System aufnehmen. Das
Kommando
sudo apt install ulauncher
installiert dann das Tool in der
aktuellen Version 5.x in Ubuntu
und seinen Varianten.
```

Der erste Aufruf des Ulaunchers muss noch manuell über seinen Eintrag im Anwendungsmenü erfolgen. Später holt die Tastenkombination Strg-Leertaste den Dialog auf den Bildschirm, in Gnome alternativ auch der Klick auf das neue Symbol in der Systemleiste. Das schlichte Suchfeld durchforstet den Rechner bei Eingaben standardmäßig nach passenden Programmnamen und bietet eine passende Liste zur Autovervollständigung an. Für die Suche im Web mit Google ist das Präfix „g“ voreingestellt und „wiki“ schlägt einen Begriff in der Wikipedia nach. Diese Abkürzungen über Präfixe sind in den Einstellungen erweiterbar. Die Einstellungen, welche sich bei einem Klick auf das Zahnradsymbol rechts im Ulauncher-Fenster öffnen, bieten auch die Möglichkeit, Ulauncher automatisch beim Start des



Ulauncher in Aktion: Der mächtige Programmstarter mit Autovervollständigung ist für Ubuntu fertig paketiert und eine ideale Ergänzung für Gnome, da er nur einen minimalen Ausführen-Dialog besitzt.

Desktops auszuführen. Dort finden Sie die Option „Launch at login“ unter „Preferences“, welche Ulauncher als Autostart-Eintrag definiert.

Eine umfangreiche Liste unter https://ext.ulauncher.io/?api_version=2.0.0 präsentiert die Erweiterungen für Ulauncher

5.x. Um eine der Erweiterungen zu installieren, gehen Sie in den Einstellungen des Ulaunchers auf „Extensions → Add Extension“ und fügen ins angezeigte Feld die zuvor kopierte URL einer Erweiterung ein, die dann heruntergeladen und aktiviert wird. -dw

Gnome: Autostart-Einträge erstellen

Gnome legt Wert auf eine klare, vereinfachte Bedienung und macht es selbst fortgeschrittenen Anwendern nicht einfach, den Desktop an eigene Wünsche anzupassen.

Damit ist der Desktop einfach, aber vergleichsweise unflexibel. So gibt es beispielsweise keine komfortable Möglichkeit, über die Gnome-Einstellungen oder über Gnome-Tweak selbst

definierte Autostart-Einträge zu erzeugen.

Es gibt einen kleinen Umweg, Autostart-Verknüpfungen in Gnome zu beliebigen Programmen und Scripts mit etwas Komfort und mittels einer grafischen Anwendung zu erstellen. Möglich macht dies der Verknüpfungseditor Arronax, der dazu dient, „.desktop“-Dateien zu erstellen und zu bearbeiten. Arronax ist ein kompaktes Tool, das der Entwickler als fertiges DEB-Paket bereitstellt. Der primäre Einsatzzweck ist nicht die Erstellung von Autostarts, aber auch dazu ist es bestens geeignet. Denn Autostart-Einträge sind nichts weiter als „.desktop“-Dateien, die im Ordner „~/config/autostart“ im Home-Verzeichnis liegen.

Arronax liegt als DEB-Paket auf der Webseite des Entwicklers zum Download (www.florian-diesch.de/software/arronax/dist/arronax_0.7.1_all.deb). Es gibt zwar auch ein PPA als externes Repository, aber nachdem

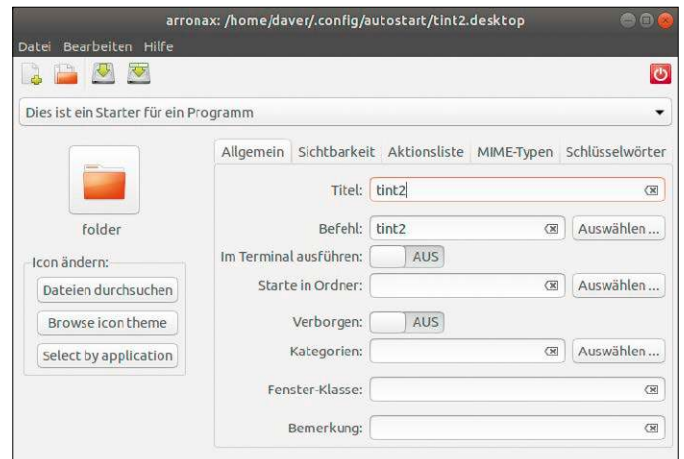
Arronax keine weiteren Pakete für Abhängigkeiten nachinstallieren muss, ist das PPA nicht nötig. Stattdessen installiert das Kommando

```
sudo dpkg -i
  arronax_0.7.1_all.deb
```

das Programm in Ubuntu und Debian.

Die Erstellung einer Autostart-Verknüpfung unterscheidet sich in Arronax zunächst nicht von einer gewöhnlichen Programmverknüpfung. In Arronax wählt man zunächst oben im Editor die Option „Dies ist ein Starter für ein Programm“ aus. Darunter erwarten das Feld „Titel“ einen Namen und das Feld „Befehl“ den Programmaufruf, der auch Parameter enthalten darf. Auch eine Script-Datei kann hier angegeben werden. Die anderen Felder sind optional.

Um die fertige Verknüpfung zu sichern, öffnet der Klick auf das Festplattensymbol in der Menüleiste den Speichern-Dialog. Damit aus der Verknüpfung ein Autostart wird, muss die



Programmverknüpfungen selbst gebaut: Das Programm Arronax ist ein fähiger Editor für „.desktop“-Dateien. Im richtigen Verzeichnis gespeichert werden diese dann zu Autostarts.

„.desktop“-Datei nur im richtigen (versteckten) Ordner, nämlich unter „~/config/autostart“ im Home-Verzeichnis abgelegt werden. Dazu ist es nötig, im Speichern-Dialog im Feld „Name“ den gesamten Pfad im Schema

```
~/config/autostart/
  [Name].desktop
```

anzugeben, denn der Datei-

browser zeigt keine versteckten Verzeichnisse an.

Autostart testen: Funktioniert der Starter wie gewünscht? In einem Terminalfenster kann das Kommando

```
gtk-launch .config/
  autostart/[Name].desktop
```

den Autostart-Eintrag ausführen und zeigt dabei eventuelle Fehlermeldungen an. **-dw**

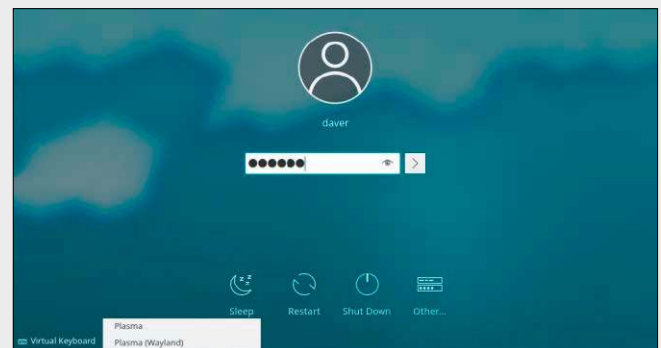
BLICK IN DIE ZUKUNFT: KDE UND WAYLAND

Wayland ist seit 2016 eine feste Größe unter dem Gnome-Desktop. In der Gnome-Ausgabe von Debian 10 ist Wayland inzwischen der Standard-Fenstermanager. Aber auch das KDE-Team schickt sich an, den Desktop fit für Wayland zu machen. Die Developer- und Testinedition von KDE Neon lädt zum Ausprobieren ein.

Noch ist das Fenstersystem X11 samt seinen Protokollen der übliche Unterbau der grafischen Oberflächen auf Linux-Systemen. Das neue Displayprotokoll Wayland schickt sich aber an, diesen Unterbau zu modernisieren, sicherer zu machen und die Fähigkeiten der heutigen Grafikkarten besser zu nutzen. Mit Gnome funktioniert das bereits passabel. Der nächste große Desktop mit optionalem Wayland-Unterbau wird KDE Plasma 5 sein. Diese Entwicklung begann 2015 an und verlief streckenweise zäh. Jetzt ist die Wayland-Unterstützung in KDE soweit, dass sich neugierige Anwender mit vertretbarem Aufwand schon mal ein Bild von den Fortschritten machen können: In der Developeredition der KDE-Vorzeigedistribution KDE Neon (Download unter <https://neon.kde.org/download>, 2 GB) ist eine optionale Wayland-Session enthalten, die ohne größere Probleme läuft. Das installierbare Livesystem läuft zunächst noch mit Xorg und dem X11-Windowssystem. Nach der Installation findet

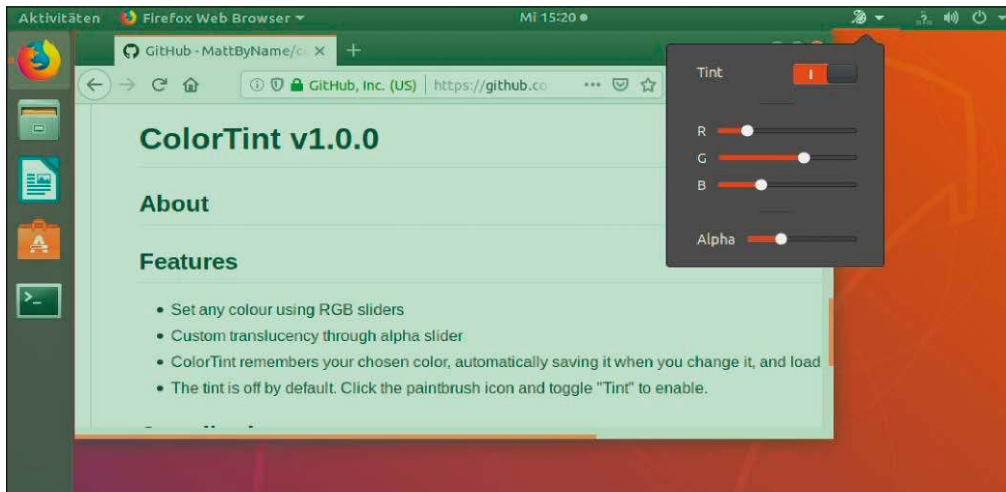
sich aber unten links auf dem Anmeldebildschirm die Option „Desktop Session / Desktop-Sitzung“, unter der sich die Einstellung „Plasma (Wayland)“ wählen lässt.

Tipp: Mit welcher Displayarchitektur ein System gerade läuft, Xorg oder Wayland, zeigt die Eingabe des Befehls „xrandr“ in einem Terminalfenster. Im Falle von Wayland steht dann in der zweiten Zeile der Ausgabe „XWAYLAND0 connected“.



KDE Plasma 5 mit Wayland: Die Vorzeigedistribution KDE Neon bietet in der Developer- und Testinedition bereits eine Option an, den Desktop mit Wayland auszuprobieren.

Gnome: Desktop komplett einfärben



Gnome-Desktop mit Farbstich: Die Erweiterung Colortint stattet das Panel mit RGB-Farbreglern aus, die den Desktop und alle Programmfenster in das gewünschte Licht tauchen.

Einige Bildschirme, insbesondere Displays auf Notebooks, sind in ihrer Farbbalance unangenehm. Eine Erweiterung für Gnome erlaubt die Farbpassung des gesamten Desktops samt der Programmfenster anhand eines RGB-Reglers. Der Farbregler Colortint kann nicht nur kleine Farbabweichungen ausgleichen und den Kontrast über einen Alphakanal justieren, sondern die gesamte Bildschirmausgabe unter Gnome abtönen und einfärben. Bei längeren Arbeiten am Bildschirm können Farbwechsel dafür sorgen, dass die Augen gerade abends weniger ermüden. Die Erweiterung ist unter <https://extensions.gnome.org/extension/1789/colortint> im offiziellen Gnome-Verzeichnis zu finden und im Quelltext zudem unter <https://git.io/fjhW1>. Sowohl Xorg als auch Wayland unter Gnome werden unterstützt. Und so gelingt die Einrichtung dieser und anderer Gnome-Erweiterungen (siehe Tipp zu Dash To Panel) über den vorinstallierten Browser Firefox:

1. Zuerst machen Sie den Browser Firefox generell fit für Gnome-Erweiterungen. Dazu installieren Sie die Firefox-Erweiterung von <https://extensions.gnome.org/>

me.org oder auch von <https://addons.mozilla.org/en-US/firefox/addon/gnome-shell-integration>.

2. Gnome braucht die neue Komponente „chrome-gnome-shell“, um Firefox einzubinden. Das gleichnamige Paket findet sich unter diesem Paketnamen in den Standard-Paketquellen aller Linux-Distributionen mit Gnome und ist in Debian/Ubuntu beispielsweise mittels `sudo apt install chrome-gnome-shell` installiert.
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> zu aktivieren. Nach der Installation der Gnome-Erweiterung Colortint zeigt sich in der Gnome-Systemleiste das neue Symbol einer Farbpalette; ein Klick darauf öffnet ein Menü mit Farbreglern, Alphakanal und einem Hauptschalter zum generellen Aktivieren der Erweiterung. Im Hintergrund arbeitet Colortint nicht mit dem Tool Xrandr, denn dies würde unter Wayland nicht funktionieren, sondern direkt mit der Gnome-Bibliothek Clutter, die den Desktop per Open GL auf den Bildschirm bringt. **-dw**

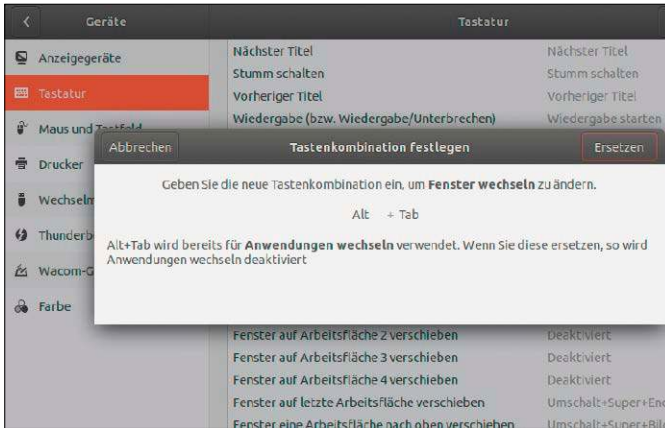
Gnome: Unterfenster einzeln umschalten



Ohne Gruppenzwang: Ab Gnome 3.28, das in Ubuntu 18.04 der Standarddesktop ist, gibt es einen Umschalter für die einzelnen Anwendungsfenster.

Auf eine klassische Taskleiste verzichtet Gnome und in Ubuntu übernimmt die vorinstallierte Erweiterung Dash To Dock diese Funktion. In Gnome selbst spielt die Tastenkombination Alt-Tab zum Wechsel von Programmfenstern die entscheidende Rolle. Umständlich ist hier aber die Navigation zu mehreren Unterfenstern einer Anwendung, denn diese sind in einer zweiten Ebene gruppiert. Wenn beispielsweise mehrere Browserfenster oder Libre-Office-Fenster geöffnet sind, so zeigt die weniger bekannte Tastenkombination Alt-^ einen

Umschalter für die Unterfenster der laufenden Anwendung. Dort dienen dann die Pfeiltasten dazu, das gewünschte Fenster auszuwählen. Das Caret-Zeichen „^“ befindet sich auf einer deutschen Tastatur genau über der Tab-Taste und ist somit bequem im Aktionsradius der linken Hand. Es gibt aber noch eine weitere Möglichkeit, im Fensterumschalter nur Einzelfenster und keine Fenstergruppen anzuzeigen. Dazu ist ab Gnome 3.28, das etwa in Ubuntu 18.04 den Desktop stellt, keine Erweiterung mehr nötig. Es genügt die Änderung eines der voreingestellten Tastaturkürzel:

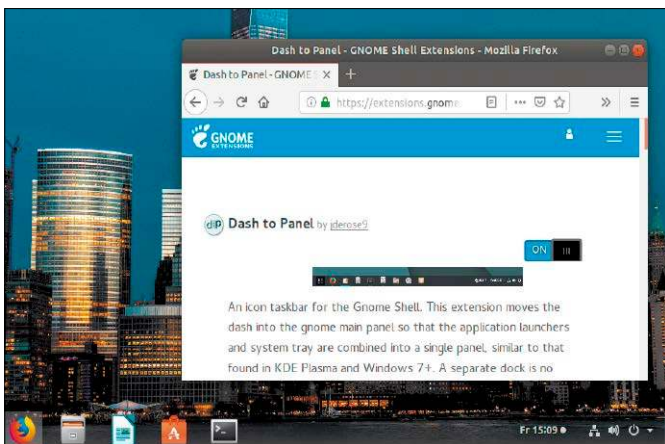


Fensterumschalter mit Tastenkombination: In den Gnome-Einstellungen muss nur die bereits vorhandene Aktion „Fenster wechseln“ mit dem Hotkey Alt-Tab ausgetauscht werden.

1. In den Gnome-Einstellungen öffnet das Untermenü „Geräte → Tastatur → Tastaturkürzel“ die konfigurierbare Liste aller Tastenkombinationen.
2. Unterhalb der Kategorie „Navigation“ befindet sich der Eintrag „Fenster wechseln“, für den standardmäßig keine eigen-

ne Tastenkombination festgelegt ist. Dies ändern Sie mit einem Klick auf den Eintrag, um danach durch einen Druck auf Alt-Tab die neue Kombination festzulegen. Ab jetzt blendet Alt-Tab die Liste von Einzelfenstern an, um zwischen diesen umzuschalten. -dw

Dash To Panel: Eine Taskleiste für Gnome



Unten statt vertikal: Die Gnome-Erweiterung Dash To Panel zeigt am unteren Bildschirmrand eine Leiste mit Favoriten und laufenden Tasks. Für Einsteiger ist dies das gewohntere Bild.

Ubuntu benutzt seit der Vorstellung des Gnome-Desktops als Standard-Arbeitsumgebung die Erweiterung Dash To Dock, die eine vertikale Leiste als Programmstarter und

Taskleiste einblendet. Die seitliche Platzierung ist auf Notebookbildschirmen ideal, allerdings für Umsteiger von Windows oder von anderen Desktops ungewohnt.

Wer eine Starterleiste lieber am unteren Bildschirmrand hat, bekommt in Gnome mit der Erweiterung Dash To Panel eine alternative Leiste. Diese Erweiterung kann in Ubuntu das seitliche Panel ersetzen. Voraussetzung ist dazu zunächst, in Ubuntu das herkömmliche Favoriten-dock mit dem Kommando `sudo apt remove gnome-shell-extension-ubuntu-dock`

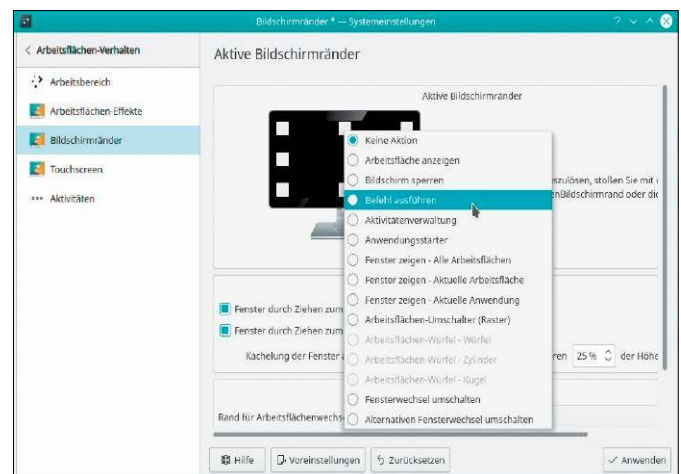
zu entfernen. Nach einer erneuten Anmeldung am System begrüßt der Standard-Gnome-Desktop. Das alternative Panel für den unteren Rand liegt zur Installation im Verzeichnis der Erweiterungen unter der Adresse <https://extensions.gnome.org/extension/1160/dash-to-panel>. Die Installation funktioniert, wie im Tipp auf der vorherigen Seite bereits gezeigt, über den Browser Firefox. -dw

KDE Plasma: Schnell zum Ausführen-Dialog

Eine nützliche Abkürzung in KDE Plasma 5 sind aktive Bildschirmränder, die bei der längeren Berührung mit dem Mauszeiger eine vordefinierte Aktion ausführen. In KDE kann beispielsweise der Dialog von Krunker einfach per Mausgestik in den Vordergrund geholt werden.

Die Funktion der aktiven Ränder haben sich die KDE-Entwickler bei Gnome 3 abgeschaut, wo beispielsweise der Mauszeiger in der linken oberen Ecke die Übersichtsseite aufruft. KDE Plasma 5 erlaubt die Konfiguration benutzerdefinierter Aktionen in Ecken und Rändern. Es

ist dabei wichtig, dem Desktop diese Funktion nur in kleiner Dosis zu verabreichen, sonst werden die aktiven Ränder und Ecken sehr schnell lästig und kollidieren mit anderen wichtigen Controls der Systemleiste oder der Programmfenster. Als nützlich kann sich aber der Ausführen-Dialog von Krunker als Aktion am oberen Bildschirmrand erwiesen. Um diese Aktion zu aktivieren, gehen Sie in den Systemeinstellungen von KDE auf „Arbeitsflächen-Verhalten → Bildschirmränder“, klicken auf den oberen Rand und wählen im angezeigten Dialog „Befehl ausführen“.



Ausführen-Dialog per Mausgestik: Die aktiven Bildschirmränder in KDE Plasma 5 sind bei richtiger Dosierung durchaus nützlich – so etwa, um Krunker einzublenden (Ausführen-Dialog).

Befehlsempfänger

Nützliches für den Linux-Alltag: Die Konsolentipps zeigen einen versteckten Batchmodus in Libre Office, graben Tunnelverbindungen über SSH, werfen unerwünschte Benutzer von einem Linux-System und räumen den Befehlsverlauf auf.

Libre Office: Dokumente in PDFs umwandeln

Sollen Dokumente zur Ansicht ausgetauscht werden, so ist es in vielen Fällen einfacher, mit PDF-Dateien zu arbeiten. Denn die meisten Anwender bringen es unabhängig vom Wissensstand und dem verwendeten Betriebssystem in jedem Fall zustande, eine PDF-Datei zu öffnen und auszudrucken.

Geht es um die Konvertierung vieler Office-Dokumente nach PDF, so ist Libre Office auch im Terminal eine Hilfe. Das Office-Programm kennt zur Stapelverarbeitung auch den Modus „headless“, der es ermöglicht, die Anwendung ohne GUI zum Konvertieren von Dateien nach PDF aufzurufen. Der folgende Befehl verwandelt alle Dateien vom Typ ODT im aktuellen Verzeichnis und allen Unterverzeichnissen in PDFs und behält

Stapelverarbeitung mit Libre Office: Für die Kommandozeile bietet das Office-Programm eine Funktion an, um Dokumentdateien automatisch nach PDF zu konvertieren.

dabei die Originaldateien:

```
find . -type f -iname "*.odt" -exec libreoffice --headless --convert-to pdf '{}' \;
```

Das Ganze funktioniert auch mit allen anderen Dateitypen, mit denen Libre Office umgehen kann. Um beispielsweise Calc-Dateien vom Typ ODS zu kon-

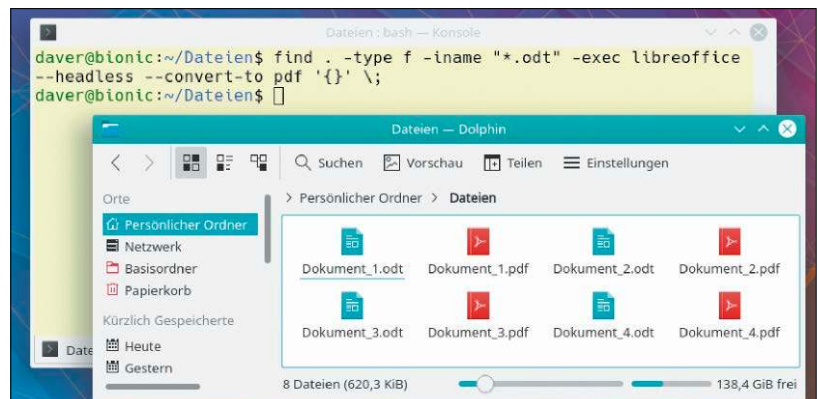
vertieren, dient folgendes Kommando

```
find . -type f -iname "*.ods" -exec libreoffice --headless --convert-to pdf '{}' \;
```

In neueren Ausgaben von Libre Office, die sich immer besser auf Microsoft-Dateien verstehen, ist dieser Weg auch gut ge-

eignet, um fremde Office-Formate nach PDF umzuwandeln.

Achtung – Bug: Die Kombination der Parameter funktioniert erst ab Libre Office 5.3 zuverlässig. In älteren Versionen bleibt das Office-Programm kommentarlos untätig, falls bereits eine Instanz von Libre Office auf dem Desktop geöffnet ist. **-dw**

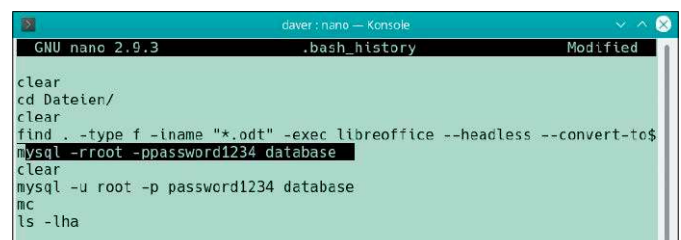


Bash: Zeilen aus dem Verlauf löschen

Wer mit öfters mit My SQL hantiert, schreibt möglicherweise Passwörter aus Bequemlichkeit direkt in die Kommandozeile und damit in den Befehlsverlauf der Kommandozeile. Passwörter sollten aber auf Mehrbenutzersystemen und Systemen ohne Vollverschlüsselung nie in die History kommen, da dies immer einen potenziellen Verlust vertraulicher Informationen darstellt.

Befehlsverlauf ausmisten: Gerade auf Mehrbenutzersystemen sollten Sie darauf achten, dass sich keine wichtigen Passwörter in die Datei „~/.bash_history“ verirren.

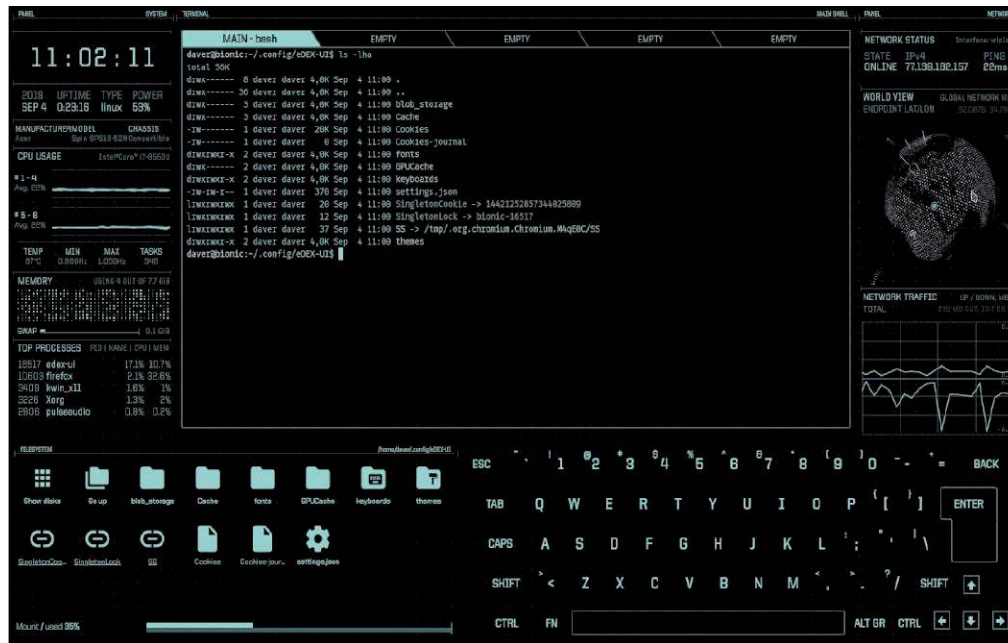
Es müssen aber nicht gleich Passwörter sein, die im Befehlsverlauf unerwünscht sind. Auch sonst sammeln sich über die Zeit etliche Kommandos in der History, die auf Dauer bei der Suche nach einem bestimmten, wieder benötigten Befehl stören. Hin



und wieder ist es also keine schlechte Idee, den Befehlsverlauf der Shell aufzuräumen und überflüssige Kommandos zu löschen. Dies ist nicht schwer,

denn in der Bourne Again Shell (Bash), die in den meisten Linux-Distributionen der Standard ist, liegt die Datei „~/.bash_history“ mit dem Befehlsverlauf als

Edex-UI: Futuristisches Terminal



Wenig Nutzwert, aber beeindruckend: Edex-UI ist ein Terminalemulator mit vielen Effekten und Extras. Das Programm beruht auf dem Electron-Framework und liegt als Appimage vor.

Düster und unattraktiv wirkt ein Terminalfenster auf die meisten Nutzer. Eine gelungene Showwinlage ist im Gegensatz zur üblichen Kommandozeile der Terminalemulator Edex-UI, der eine futuristische Shell anbietet. Dabei geht es aber nicht nur um Show, denn der Edex-UI zeigt auch Systeminfos wie CPU- und RAM-Auslastung an. Außerdem gibt es eine Bildschirmstastatur, die sogar für Touchscreens geeignet ist.

Unterm Strich steht bei diesem verspielten Programm nicht unbedingt der Nutzwert im Vordergrund. Edex-UI ist deshalb in den Paketquellen der Linux-Distributionen nicht vertreten, steht aber erfreulicherweise als universelles Appimage zur Verfügung und muss deshalb nicht kompiliert werden.

Die letzte Version des Programms findet sich stets auf der Github-Seite des Entwicklers unter <https://github.com/GitSquared/edex-ui/releases>. Das Appimage für Linux gibt es in 32 und 64 Bit.

Nach dem Download macht das Kommando

```
chmod +x [Datei].AppImage
./[Datei].AppImage
```

startet das Programm, das eifrig Gebrauch vom Electron-Framework macht und entsprechend speicherhungrig ist. Die erste Rückfrage „Would you like to integrate eDEX-UI.Linux.x86_64.AppImage with your system“ beantwortet man bei einem ersten Aufruf mit „No“, wenn man das Programm nicht gleich installieren möchte. Edex-UI braucht ein paar Momente, seine effektreiche GUI zu starten. In der Mitte befindet sich ein Terminalfenster, links unten gibt es anklickbare Verknüpfungen zu Ordnern, rechts unten eine Bildschirmstastatur. Die Tastenkombination Strg-D beendet das Programm.

Edex-UI 2.2.2: Verspieltes Terminalprogramm, auch für Touchscreens geeignet. Open Source (GPL 3), Download des Appimage unter <https://github.com/GitSquared/edex-ui/releases>. **-dw**

Und „Tschüss“: Benutzerkonten gründlich entfernen

Dies kommt auf allen Mehrbenutzersystemen vor: Ein Benutzerkonto auf einem Linux-Server wird nicht mehr benötigt. Nun gilt es, den Benutzeraccount auf dem Server zu sperren, eventuell vorhandene Daten zu finden, zu sichern oder zu löschen und auch ansonsten alle Wege zurück zu versperren. Mit dieser systematischen Anleitung ist das kein Problem.

Auf größeren Serversystemen mit etlichen Benutzern ist es nicht immer gleich klar, wer eigentlich noch am System angemeldet ist.

1. Benutzer abmelden: Der erste Schritt vor der Entfernung eines Benutzerkontos ist deshalb die Abmeldung des betreffenden Users und das Stoppen jeglicher Benutzerprozesse mit diesem Kommando:

```
sudo pkill -KILL -u [User]
```

2. Anmeldung verbieten: Im zweiten Schritt gilt es, eine künf-

tige Anmeldung des Benutzers kurzerhand mit `sudo passwd -l [User]` zu verhindern.

3. Dateien sammeln und sichern: Schließlich geht es darum, alle Dateien des Users zu finden und eventuell in einem zentralen Verzeichnis zu sichern, falls später eine Bestandsaufnahme nötig sein sollte. Das Kommando `sudo find / -user [User]` zeigt alle Dateien im gesamten Dateisystem an, die diesem User gehören.

4. Benutzeraccount und Home-Verzeichnis entfernen: Sind die Dateien gesichert, dann kann es nun daran gehen, das Konto und das Verzeichnis des Users mit diesem Befehl unwiderruflich zu löschen:

```
sudo userdel -r -f [User]
```

Danach sind der Account, das Home-Verzeichnis und das Mailverzeichnis des Benutzers Geschichte. **-dw**

Gezähmte Geräte

Die Hardwaretipps werfen diesmal einen Blick auf USB-Ports und die Möglichkeit, USB 3.1 der zweiten Generation nachzurüsten. Scrcpy bringt Android-Geräte buchstäblich auf den Linux-Desktop und Fwupd liefert Firmwareupdates unter Linux.

USB und Thunderbolt: Wo sind die Geräte?

Ein USB- oder Thunderbolt-Gerät ist angesteckt und blinkt vor sich hin, aber auf dem System rührt sich nichts. Das Gerät wird nicht erkannt und taucht im Fall von Laufwerken weder im Dateimanager und auch nicht unter den üblichen Einhängen im Verzeichnis „/media“ (Debian, Ubuntu) oder „/run/media“ (Fedora, Manjaro, Arch Linux) auf.

Wenn Linux mit angesteckten USB- oder Thunderbolt-Geräten nichts anzufangen weiß, muss nicht gleich das Gerät selbst kaputt sein. Kabel für USB-C und Thunderbolt können schon mal Probleme machen. Und im Fall von USB-Sticks sind ungültige und defekte Dateisysteme der Hauptgrund für ein hängendes USB-Laufwerk, das nirgends

```
daver@bionic:~$ sudo dmesg -wH
[Sep 5 01:23] usb 1-4: USB disconnect, device number 8
[ +2,242523] usb 1-4: new low-speed USB device number 9 using xhci_hcd
[ +0,198583] usb 1-4: New USB device found, idVendor=0e8f, idProduct=00a8, bcdDevice= 3.11
[ +0,000006] usb 1-4: New USB device strings: Mfr=1, Product=2, SerialNumber=0
[ +0,000004] usb 1-4: Product: 2.4G RX
[ +0,000002] usb 1-4: Manufacturer: DaKai
[ +0,005540] input: DaKai 2.4G RX as /devices/pci0000:00/0000:00:14.0/usb1/1-4/1-4:1.0/0003:0E8F:00A8.0008/input/input37
[ +0,060595] hid-generic 0003:0E8F:00A8.0008: input,hidraw0: USB HID v1.10 Keybo
```

Widerspenstige USB-Laufwerke: In diesem Fall kann Linux einen angeschlossenen USB-Datenträger nicht erkennen, da ein Fehler des Dateisystems vorliegt, wie das Kernel-Log über den Befehl dmesg berichtet.

auftaucht. Um herauszufinden, wo ein angestecktes Gerät abgeblieben ist, lohnt sich ein Ausflug auf die Befehlszeile. Hier kann das Kommandozeilentool lsusb alle angesteckten und erkannten USB- und Thunderbolt-Geräte anzeigen und damit Probleme mit Kabel oder USB-Port ausschließen. Mehr Details bei

funktionsuntüchtigen externen Geräten aller Art, nicht nur bei Laufwerken, weiß der Befehl dmesg. Dieser Befehl zeigt das Kernel-Log an, mit den neuesten Meldungen zuletzt. Und es gibt dazu einen Trick, nur die relevanten Meldungen anzuzeigen: Das Kommando

```
sudo dmesg -wH
```

öffnet das Kernel-Log im Beobachtungsmodus. Steckt man jetzt Geräte ab und ein, so zeigt der Kernel in Echtzeit die Meldungen bei der Erkennung der Geräte und Dateisysteme an. So sind nun auch eventuelle Fehlermeldungen sichtbar, die man auf dem Desktop nicht zu sehen bekommt. -dw

USB 3.1: Kompatible Karten nachrüsten

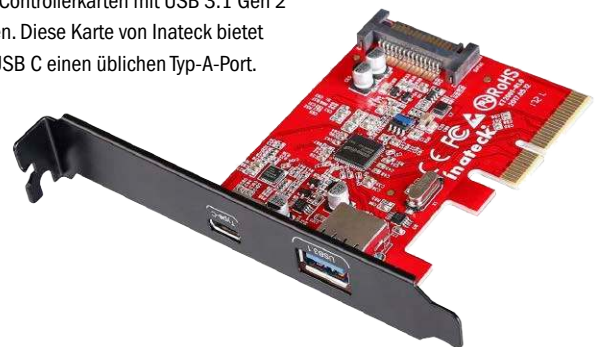
Moderne Notebooks und neue Hauptplatinen sind mit Ports für den USB-Standard 3.1 ausgestattet. Dieser Standard bietet nicht nur weit höhere Geschwindigkeiten als USB 3.0, sondern auch Anschlüsse vom Typ C. Auch ältere Desktop-PCs können mit einer PCI-Karte mit USB 3.1 ausgestattet werden. Linux-Anwender können aber nicht jede beliebige Karte einsetzen.

Die Unterstützung von USB 3.1 ist die Sache des Linux-Kernels,

der den Standard USB 3.1 Gen 2 mit bis zu zehn GBit Übertragungsgeschwindigkeit ab Version 4.6 kennt. Im Idealfall erkennt ein einigermaßen aktuelles Linux-System also nachgerüstete Controllerkarten automatisch, lädt das Treibermodul und bindet dann klaglos USB-3.1-Geräte mit optimaler Geschwindigkeit ein.

In der rauen Wirklichkeit halten sich einige Hersteller aber mit ihren Controllerchips nicht an die Spezifikationen und liefern

Günstige PCI-Express-Karte: Ältere PCs lassen sich mit PCI-Controllerkarten mit USB 3.1 Gen 2 aufrüsten. Diese Karte von Inateck bietet neben USB C einen üblichen Typ-A-Port.



Karten aus, die nur mit einem speziellen Treiber funktionie-

ren, den es natürlich nur für Windows gibt. →

Controllerkarten, die mit Linux dank einem Chipsatz von Asmedia problemlos arbeiten, sind die Karten von Inateck. Eine Karte mit USB 3.1 Gen 2 und einem USB-C- sowie Typ-A-Port des Herstellers kostet im Versandhandel rund 30 Euro (<https://amzn.to/2kOodu3>). Diese Karten verlangen mindestens nach einem Steckplatz nach PCIx4. Für die Stromversorgung angeschlossener USB-Geräte verfügt die PCI-Karte zudem über einen SATA-Stromanschluss, der mit dem Netzteil des Computers verbunden werden muss. Um zu überprüfen, ob eine Karte korrekt erkannt wurde, dient

```
daver@bionic:~$ lsusb -t
/: Bus 02.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/6p, 5000M
/: Bus 01.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/12p, 480M
|__ Port 1: Dev 26, If 0, Class=Mass Storage, Driver=usb-storage, 480M
|__ Port 4: Dev 24, If 1, Class=Human Interface Device, Driver=usbhid, 1.5M
|__ Port 4: Dev 24, If 0, Class=Human Interface Device, Driver=usbhid, 1.5M
|__ Port 5: Dev 3, If 1, Class=Wireless, Driver=btusb, 12M
|__ Port 5: Dev 3, If 0, Class=Wireless, Driver=btusb, 12M
|__ Port 6: Dev 4, If 0, Class=Human Interface Device, Driver=usbhid, 12M
|__ Port 7: Dev 5, If 0, Class=Video, Driver=uvcvideo, 480M
|__ Port 7: Dev 5, If 1, Class=Video, Driver=uvcvideo, 480M
|__ Port 8: Dev 6, If 0, Class=Vendor Specific Class, Driver=rtsx_usb, 480M
|__ Port 9: Dev 7, If 0, Class=Vendor Specific Class, Driver=, 12M
daver@bionic:~$
```

Das Kommandozeilentool `lsusb` zeigt die USB-Ports: Ports nach dem Standard USB 3.1 Gen 2 mit bis zu zehn GBit/s Übertragungsgeschwindigkeit sind mit der Angabe „10000M“ markiert.

nach der Inbetriebnahme der Befehl `lsusb -t` im Terminalfenster, der die neuen USB-Ports auflistet. Ports nach dem Stan-

dard USB 3.1 Gen 2 sind in der Ausgabe am Ende der Zeile mit der Bezeichnung „10000M“ markiert.

Dieser Befehl ist auch nützlich, um die verfügbaren USB-Ports von Notebooks und Hauptplatinen zu identifizieren. **-dw**

Fwupd: Firmware unter Linux aktualisieren

Nicht nur Hauptplatinen verlangen nach Firmwareupdates: Eine ganze Reihe an externer Hardware, die an PCs angeschlossen ist, fordert von Zeit zu Zeit neue Firmware. Unter Linux war der Aktualisierungsprozess häufig ein Problem, weil Hersteller üblicherweise Windows-Programme für Firmwareupdates ausliefern. Mittlerweile hat sich die Situation gebessert.

Die GNOME-Entwickler haben zusammen mit Dell das Updatetool `Fwupd` entwickelt, das Hardwareherstellern eine Standardschnittstelle für Firmwareupdates unter Linux bietet, um Aktualisierungen für Hardware aus einem Onlinerepository abzurufen. Die Resonanz auf das Projekt war erstaunlich gut und mittlerweile finden sich fast 10 000 Firmwareupdates verschiedener Hersteller im Repository. Unter GNOME läuft `Fwupd` automatisch im Hintergrund und das GNOME-Software-Center informiert über verfügbare Firmwareaktualisierungen. Dies funktioniert aber auch mit anderen Desktopum-

Firmwareupdate unter Linux. Das Projekt `Fwupd` begann als Initiative von Dell und der GNOME Foundation. Inzwischen steuern fast alle großen Hardwarehersteller aktualisierte Firmwaredateien bei.

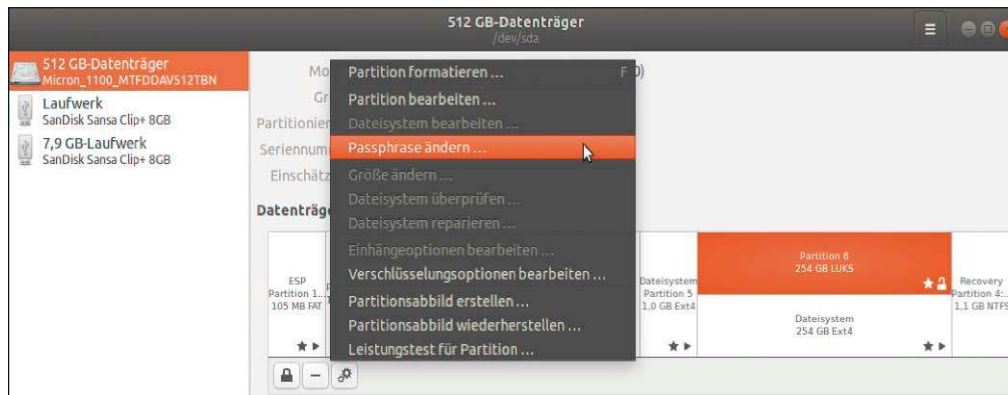
gebungen, denn `Fwupd` ist auch auf der Kommandozeile vertreten. Das dafür benötigte Paket „`fwupdate`“ liegt in den Standardrepositories vieler Linux-Distributionen und in Debian sowie Ubuntu ist es mit dem Befehl `sudo apt-get install fwupdate` schnell nachinstalliert. Anschließend zeigt das Kommando

The screenshot shows the `fwupd.org` website interface with a search bar and a list of vendors. A terminal window is overlaid on the right, showing the command `sudo fwupdmgr get-devices` and its output, which lists various hardware devices with their IDs, GUIDs, and supported firmware versions.

`sudo fwupdmgr get-devices` alle erkannten angeschlossenen Geräte an. Die Eingabe `sudo fwupdmgr refresh` bringt die Firmwaredatenbank auf den neuesten Stand und die beiden Befehle `sudo fwupdmgr get-updates` und `sudo fwupdmgr update` aktualisieren dann die erkannte Hardware, falls neuere Firmwareupdates vorliegen.

Hinweis: Die Firmwaredatenbank für Linux ist ein Projekt im Aufbau und noch nicht zu hundert Prozent komplett. Die großen Hardwarehersteller steuern inzwischen aber regelmäßig aktualisierte Firmwaredateien bei. Eine Suche in der Datenbank nach Hersteller und Gerätenamen ist auf der Webseite <https://fwupd.org> möglich. **-dw**

Cryptsetup/Luks: Passwörter einfach ändern



Ein neues Passwort für verschlüsselte Partitionen: Der Partitionierer Gnome-Disks kann mit Cryptsetup/Luks umgehen und recht einfach das Kennwort verschlüsselter Partitionen ändern.

Auch das Passwort für verschlüsselte Partitionen und vollverschlüsselte Linux-Systeme verlangt hin und wieder eine Änderung. Etwa, wenn das Passwort einfach schon zu lange in Gebrauch war oder wenn ein Rechner im Firmenumfeld die Hände wechselt.

Die einfachste Möglichkeit, Passwörter für Partitionen zu ändern, die mit Cryptsetup/Luks verschlüsselt sind, bietet das grafische Werkzeug Gnome-Disks („Laufwerke“). In den

Hauptausgaben von Debian und Ubuntu ist es bereits vorinstalliert, andernfalls ist es bei der Verwendung anderer Ausgaben mit dem Befehl

```
sudo apt install gnome-disk-utility
```

auch schnell nachgerüstet. In den Anwendungsmenüs der diversen Desktops taucht das Tool dann als „Gnome Disks“ auf. Wie alle Partitionierungswerkzeuge verlangt das Programm beim Aufruf root-Berechtigungen beziehungsweise das sudo-Pass-

wort. Gnome-Disks zeigt links eine Liste der physikalischen Laufwerke an und im Hauptfenster eine Übersicht der darauf eingerichteten Partitionen. Die mit Cryptsetup/Luks verschlüsselten Volumes sind mit einem Schloss gekennzeichnet. Per Klick auf eine dieser Partitionen markiert man diese und klickt dann links unten auf das Zahnrad-Symbol. In diesem Menü findet sich auch die Option „Passphrase ändern“ zum Ändern des Passworts.

Ohne grafische Oberfläche: Gibt es auf einem System keinen Desktop, so klappt der Passwortwechsel auf der Kommandozeile mit diesem Befehl:

```
sudo cryptsetup
luksChangeKey /dev/
sd [XX]
```

Den Stellvertreter „[XX]“ müssen Sie durch die tatsächliche Partitionsbezeichnung ersetzen. Wie diese auf dem System lautet, kann das Kommando `lsblk` ermitteln, das alle Partitionen im Terminal auflistet. **-dw**

Scrcpy: Android-Geräte auf dem Linux-Desktop

Auf dem Linux-Desktop gleichzeitig das Android-Smartphone oder Tablet im Auge behalten – dieses Kunststück bringt das Programm Scrcpy fertig, hinter dem die Entwickler des Android-Emulators Genymotion stehen. Das Open-Source-Programm bringt den Bildschirm eines angeschlossenen Android-Geräts auf den Linux-Desktop und erlaubt von dort aus dessen Fernsteuerung.

Nützlich ist dies nicht nur für Anwender, die eingehende Kurznachrichten auf dem Smartphone verfolgen wollen, sondern auch für App-Entwickler, die ein reales Gerät zum Debuggen einer App benötigen. Scrcpy zeigt den Android-Bild-

schirm in einem Programmfenster an und reagiert auf Maus- und Tastatureingaben. Damit Scrcpy auf einem Linux-System Kontakt zu Android aufnehmen kann, sind nur wenige Vorbereitungen nötig. Eine App ist nicht nötig, aber auf dem verwendeten Gerät muss USB-Debugging in den Entwickleroptionen eingeschaltet sein. Je nach Android-Version gibt es verschiedene Wege zu den Entwickleroptionen. Anleitungen für alle Android-Versionen gibt es online unter <http://www.pc-welt.de/1898618>.

Scrcpy liegt im Quellcode auf Github (<https://github.com/Genymobile/scrcpy>), muss aber zumindest in Ubuntu nicht selbst

kompiert werden. Hier gibt es bereits ein Snap-Paket zur einfachen Installation in den Ubuntu-Systemen. In einem Terminalfenster ist das Programm mittels

```
sudo snap install scrcpy
```

als Snap einzurichten. In den Anwendungsmenüs der Desktopumgebungen taucht das Snap zwar nicht auf, aber im Terminal können Sie Scrcpy mit dem einfachen Aufruf `scrcpy` starten.

Es erwartet ein angeschlossenes Android-Gerät mit aktivierten Entwickleroptionen an einem der USB-Ports.

Eine zusätzliche App ist nicht nötig. **-dw**



Fernsteuerung von Android auf dem Linux-Desktop: Scrcpy zeigt den Bildschirm eines angeschlossenen Android-Geräts an und erlaubt dessen Bedienung mit Tastatur und Maus.

Software-spezialitäten

Zur Zusammenstellung von PDF-Dokumenten aus Einzelseiten und gibt es unter Linux ein neues Tool. Außerdem gibt es Tipps zu Libre Office und Thunderbird sowie eine funktionierende Methode, APKs von Google Play herunterzuladen.

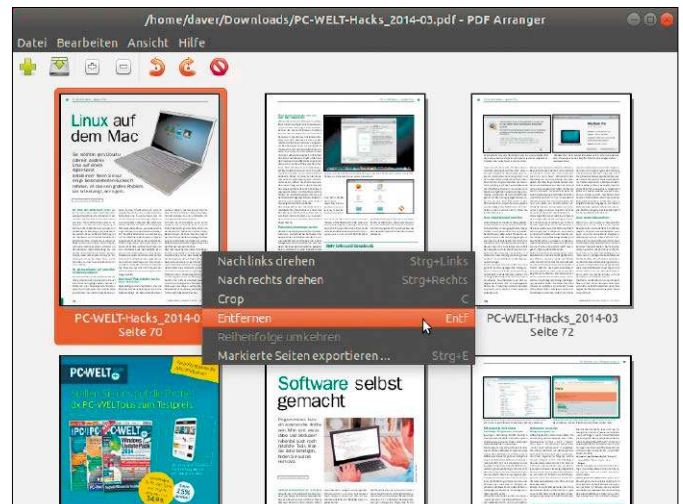
PDFs teilen, löschen, umsortieren

Ein nützliches Format zum unkomplizierten Austausch von Dokumenten sind PDFs. Ein PDF-Betrachter ist Bestandteil jeder Linux-Distribution, Libre Office kann PDF-Dateien erzeugen und über den Druckdialog der meisten Desktopumgebungen gibt es sogar die Möglichkeit, beliebige Inhalte als PDF auszugeben. Wenn es darum geht, ein vorhandenes PDF zu bearbeiten, Seiten hinzuzufügen oder zu entfernen, sind aber zusätzliche Tools nötig.

Eines der komfortabelsten Programme für den Linux-Desktop zur Bearbeitung von Seiten ist der PDF Arranger. Das grafische Tool zeigt die Seiten eines geöffneten PDFs nebeneinander an. Diverse Aktionen für eine Seite zeigt ein Rechtsklick auf selbige an: Der PDF Arranger kann dann Seiten drehen, zuschneiden, entfernen und exportieren. Ein Verschieben mit der gedrückten rechten Maustaste arrangiert das geladene PDF nach Wunsch um. Auf diese Weise funktioniert auch das Zusammenfügen mehrerer PDF-Dateien: Das Plus-Symbol in der Menüleiste fügt dem geöffneten PDF am Ende das ausgewählte Dokument hinzu und die zusätz-

lichen Seiten können neu gemischt oder entfernt werden. Das Ausgabeformat von PDF Arranger ist ebenfalls wieder ein PDF. Das Programm ist keine Neuentwicklung, sondern basiert auf dem älteren Tool PDF Shuffler, das aber schon lange kein Update mehr gesehen hatte. Als Abspaltung hat der PDF Arranger dem nützlichen Tool wieder Leben eingehaucht und es auch in die Standard-Paketquellen aktueller Linux-Distributionen gebracht: Ab Debian 10 und Ubuntu 19.04 steht der PDF Arranger in den Standard-Paketquellen bereit und ist mit dem Kommando

```
sudo apt install
pdfarranger
zu installieren. Auch Fedora 30
und Arch Linux bieten das Pro-
gramm in ihren Quellen an. Wer
ein Ubuntu 18.04 mit Langzeit-
support einsetzt, muss auf das
Tool auch nicht verzichten,
denn es gibt ein PPA (inoffiziel-
les Repository), das die beiden
Kommandos
sudo add-apt-repository
ppa:linuxuprising/apps
sudo apt update
ins System einbinden, bevor
dann der bereits genannte Be-
fehl apt install [...] zur Installati-
on schreitet. -dw
```



PDF-Dateien neu arrangieren und zusammenfügen: Der PDF Arranger ist ein grafischer Editor, der die Seitenreihenfolge in PDFs ändern kann und aus mehreren Dateien neue PDFs baut.

Google Play: Apps als APK sichern

Es kommt vor, dass Spiele und Apps aus dem Angebot von Google Play verschwinden. Beispielsweise, wenn ein Entwicklerbüro gekauft wird oder schlicht seine Pforten schließt. Besonders nützliche Apps und geliebte Spiele sollte man also besser auch als APK-Datei archivieren, die sich in Android zur Not dann auch noch manuell installieren lässt, wenn die App nicht mehr regulär verfügbar ist. Nützlich sind APK-Dateien natürlich auch, wenn auf einem

Gerät eine inoffizielle Android-Variante ohne Google Services läuft.

Helferanwendungen, die sich als Android-Gerät ausgeben, können die einzelnen APK-Dateien von Apps und Spielen von Google Play herunterladen. Allerdings gibt es das Problem, ein funktionierendes und seriöses Programm dieser Art zu finden. Programme für den Zugriff auf Google Play haben generell ein kurzes Verfallsdatum, da Google das Protokoll für den Download von Apps hin und



APKs herunterladen: Raccoon gibt sich als Android-Gerät aus und kann Apps von Google Play als APK-Datei zur späteren Installation speichern. Voraussetzung ist ein Google-Konto.

wieder ändert. Raccoon ist ein Java-basiertes Programm, das mit den Änderungen auf Google Play bisher sehr gut Schritt halten konnte und deshalb schon einmal in der LinuxWelt vorgestellt wurde. Raccoon ist Open Source, als Java-Programm auch für Windows sowie MacOS X verfügbar und erscheint schon seit über fünf Jahren mit

regelmäßigen Updates. Kürzlich ist Raccoon in der aktualisierten Version 4.8 erschienen. Damit das Tool Zugriff auf Google Play erhält, benötigt es zur Anmeldung ein gültiges Google-Konto. Die Entwickler von Raccoon empfehlen, dafür ein gesondertes Google-Konto anzulegen, damit Experimente zum Download von Apps nicht

im tatsächlichen Google-Konto auftauchen. Zum Aufruf von Raccoon ist es in den meisten Linux-Distributionen zunächst nötig, eine Java-Runtime zu installieren. In Debian, Ubuntu und seinen Varianten erledigt dies der Befehl

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

in der Kommandozeile. Nach dem Download von Raccoon 4.8 von dessen Projektwebseite startet der Befehl

```
java -jar raccoon-4.8.0.jar
```

das Programm. Nach der Eingabe der Kontodaten des Google-Accounts kann sich Raccoon entweder als ein neues Pseudogerät ausgeben oder per Hardwareprofil ein tatsächliches Android-Gerät imitieren. Nach der erfolgten Anmeldung durchsucht Raccoon das Angebot von Google Play anhand der angegebenen Schlüsselwörter im Suchfeld. Nach einem Klick auf die Beschreibung

und „Download“ lädt das Programm die zugrundeliegende APK-Datei herunter und speichert diese im Verzeichnis „~/Raccoon/content/apps“ im Home-Verzeichnis.

Ein Wermutstropfen: Früher war Raccoon mit seinem vollen Funktionsumfang kostenlos und spendenfinanziert. Nun bekommt man gegen eine Gebühr von zehn Euro vom Entwickler einen Lizenzschlüssel, der die fortgeschrittenen Funktionen freischaltet. Dann ist die direkte Installation von APKs auf angeschlossenen Android-Geräten per Android Debug Bridge (ADB) möglich und die Verwaltung mehrerer Geräteprofile.

Raccoon 4.8:

Download für APK-Dateien und Desktopclient für Google Play, englischsprachiges Open-Source-Programm (Apache-Lizenz), benötigt eine Java-Runtime. Download unter <http://raccoon.onyxbits.de/releases>. **-dw**

LINUX-DISTRIBUTIONEN: PASSENDE PAKETE FINDEN

Software selbst kompilieren – diese Möglichkeit ist eine Stärke von Open-Source-Betriebssystemen wie Linux, auf welchen die gesamte Toolchain zum Kompilieren von Quellcode schnell verfügbar ist.

Es bleibt aber die Schwierigkeit, die oft noch benötigten Entwicklerpakete als Abhängigkeit aus den Paketquellen zusammensuchen. Die Erfüllung aller Abhängigkeiten kann auch für erfahrene Anwender tückisch sein und auf älteren Linux-Distributionen auch mal kläglich scheitern.

Fertige Pakete: Es ist immer angenehmer, Programme und Bibliotheken über den Paketmanager der verwendeten Distribution zu installieren. Einen Blick in die Standard-Paketquellen aller verbreiteten Linux-Distributionen erlaubt die Onlinedatenbank von <https://pkgs.org>. Eine Suche listet die gefundenen Pakete mit Version und der Ausgabe der Linux-Distribution auf, in welcher diese verfügbar ist. Diese Seite ist auch wichtig, um schon vor dem Umstieg auf eine neuere Ausgabe der verwendeten Distribution in Erfahrung zu bringen, ob dort ein eventuell benötigtes Programm schon in einer aktuelleren Version verfügbar ist.

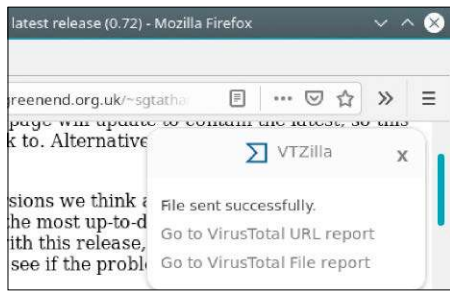
App-Container: Bequemer als Kompilieren ist die Installation einer Anwendung als Container. Mittlerweile kümmern sich zusehends mehr Entwickler darum, Linux-Programme in App-

Container-Formaten bereitzustellen. Die verbreiteten Formate der unterschiedlichen Linux-Distributionen umfassen momentan das universelle Appimage, Snaps von Ubuntu und Co. sowie Flatpaks für Fedora und Mint sowie andere Gnome-affinen Distributionen. Für Snaps gibt es <https://snapcraft.io>, für Flatpaks die Seite <https://flathub.org> und für Appimages eine Liste und Suche unter <https://appimage.github.io>.

Name	Description	Authors	Update Information
AKASHA	Network Akasha platform	AkashaProject	no valid OpenPGP data found
Utility	Utility	anastasluo MPL-2.0	no valid OpenPGP data found
ANT_Download	System Virtual Machine for Atari 32-bit applications	aramym GPL-2.0	Yes, can use AppImageUpdate no valid OpenPGP data

Verzeichnis für Appimages: Das universelle Containerformat ist nicht in den Linux-Paketmanagern integriert, unterhält aber auf <https://appimage.github.io> eine gepflegte Liste.

Browser: Downloads auf Malware testen



Firefox-Downloads mit Virustotal prüfen: Die Firefox-Erweiterung schickt die empfangene Datei zu <https://www.virustotal.com> und blendet dann diesen Link zum Ergebnis der Analyse an.

Linux ist in seinen Ausprägungen nicht anfällig für typische Malware, die sich in Form von Viren und Würmern in ausführbaren Dateien verbreitet. Allerdings kann es in gemischten Netzwerken bei einem regen Dateiaustausch mit Windows-Systemen zur Zwischenstation für infizierte Downloads werden.

Für einen Check einzelner Downloads auf Malware ist keine Antivirensoftware nötig. Solche ist unter Linux sowieso nicht für den typischen Desktopeinsatz verfügbar, sondern so wie Clam AV eher für

die Überwachung von Dateiservern gedacht.

Zur Überprüfung einzelner Dateien eignet sich der von Google betriebene Onlinedienst Virustotal (<https://www.virustotal.com>), der hochgeladene Dateien analysiert.

Eine geeignete Browsererweiterung kann eine Datei nach dem Download oder auch per Downloadlink an Virustotal übergeben und überprüfen lassen.

Firefox: Die offizielle Erweiterung von Virustotal steht unter <https://addons.mozilla.org/en-US/firefox/addon/vtzilla> zur Installation in Firefox bereit. Nach



Chrome-Downloads mit Virustotal prüfen: Die Erweiterung für Chrome/Chromium von Virustotal kann per Rechtsklick auf einen Downloadlink die betreffende Datei überprüfen.

einem Download sendet das Add-on die Datei automatisch an Virustotal und blendet in einem Fenster den Link zum Malwarebericht ein. Eher unkritische Dokumentdateien mit typischen Endungen wie DOC, DOCX, ODT, PDF können die Einstellung des Add-ons von einer Überprüfung ausnehmen, damit an Virustotal nicht verse-

hentlich vertrauliche Dokumente gesendet werden.

Chrome/Chromium: Für die Google-Browser gibt es ebenfalls eine offizielle Erweiterung, die jedoch etwas anders funktioniert. Nach der Installation über <https://bit.ly/2v1Gh7P> zeigt ein Klick auf einen Downloadlink den Punkt „Check with VirusTotal“ an. **-dw**

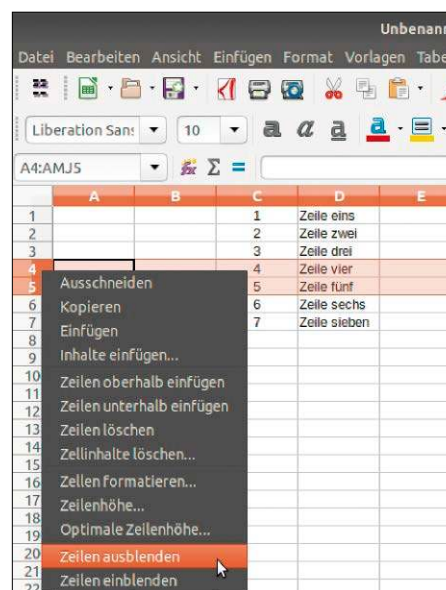
Libre Office Calc: Nur sichtbare Zellen kopieren

In umfangreichen Tabellen werden aus Gründen der Übersicht oft einzelne Zeilen und Spalten ausgeblendet – eine einfache Methode, das Unwesentliche wegzufiltern. Jetzt sollen nur die sichtbaren Zellen markiert und in eine andere Arbeitsmappe kopiert werden. Dabei kopiert Libre Office Calc aber immer sowohl die sichtbaren als auch die ausgeblendeten Zellen in die andere Arbeitsmappe ein. Auf den Hilfeseiten in Libre Office gehen die Macher der Office-Suite detaillierter auf dieses Verhalten ein: Zellen, die über die Funktion „Daten → Autofilter“ und „Daten → Weitere Filter“ unsichtbar sind, bleiben beim Kopieren und Einfügen

außen vor. Zeilen und Spalten, die per Rechtsklick und der Funktion „Ausblenden“ unsichtbar gemacht wurden, landen hingegen bei der Kopieraktion in der Zwischenablage.

Hier kann eine Libre-Office-Erweiterung helfen: Die Ergänzung „Copy only visible cells“ ignoriert beim Kopieren von Zellen die ausgeblendeten Inhalte. Nach der Installation der Erweiterung von <https://extensions.libreoffice.org/extensions/copy-only-visible-cells> über den „Extension Manager“ zeigt sich in Libre Office Calc ein neuer Menüpunkt „Bearbeiten → Kopieren sichtbarer Zellen“.

Copy only visible cells 2.0: Erweiterung für Libre Office ab Version



Unsichtbares nicht kopieren: Ausgeblendete Zellen machen Tabellen übersichtlicher. In Libre Office Calc ist eine Erweiterung nötig, damit diese Zellen beim Kopieren nicht berücksichtigt werden.

5.2. Deutsch, Open Source (Lieser GPL 3). Download unter <https://extensions.libreoffice.org/extensions/copy-only-visible-cells>.

-dw

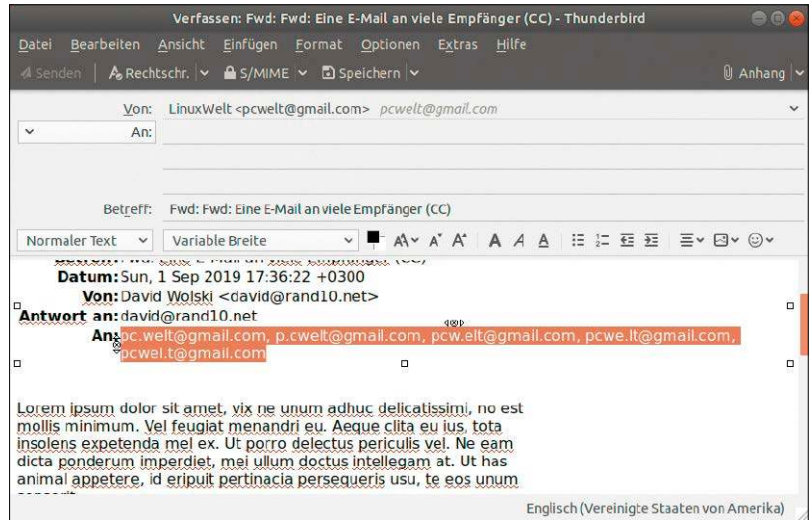
Thunderbird: Empfängerliste schnell kopieren

Die Arbeit in Teams bringt es mit sich, dass E-Mails zu einem Projekt oft an eine ganze Reihe von Empfängern gehen sollen. Bei der manuellen Eingabe von Adressen können aber schnell mal Fehler passieren. Das Mailprogramm Thunderbird kann im Adressbuch aber auch Empfängerlisten anlegen.

Thunderbird kann einzelne Adressen per Rechtsklick in den Kopfteil einer Nachricht in das Adressbuch übernehmen. Für mehrere Adressaten funktioniert dies aber an dieser Stelle im Fenster empfangener Nachrichten nicht. Stattdessen wählt man zur Übernahme einer ganzen Adressliste zunächst die Funktion „Weiterleiten“. In der Ansicht der neu generierten Nachricht, die man natürlich nicht weiterleitet, zeigen die Headerzeilen im Messagebody in der Spalte „An“ die

Eine List für Listen:

Thunderbird zeigt alle sichtbaren (CC) Empfänger im Header einer E-Mail an. Von dort aus lassen sich alle Adressen kopieren und als Adressbucheintrag speichern.



gesamte Liste der Empfänger, an welche die Nachricht ursprünglich als CC („Carbon Copy“) adressiert war.

Mit Kopieren und Einfügen ist diese Liste erst einmal auch schnell in eine neue E-Mail übertragen. Nach einem Druck auf Strg-V und der Tab-Taste

sind alle kopierten Adressen wieder säuberlich untereinander in einzelne Felder aufgeteilt. Und so klappt die Übernahme dieser Empfängerliste in das Thunderbird-Adressbuch: Nach einem Klick auf „Adressbuch → Neue Liste“ im Hauptfenster von Thunderbird und

einer Beschreibung für den neuen Eintrag kopieren Sie die Adressen als eine Zeile darunter in die Liste.

Das Mailprogramm speichert so alle kopierten Empfänger unter einem Eintrag, der sich dann ganz einfach abrufen lässt. **-dw**

Ubuntu: Alte Snap-Container entfernen

Das Snap-Containerformat in Ubuntu und seinen Varianten bekommt von den Machern der Distribution weiterhin viel Aufmerksamkeit und wird prominent als Lösung vieler Probleme beworben. Eine unangenehme Eigenschaft der Snaps ist aber deren hoher Platzbedarf, der auf eher kleinen SSD-Laufwerken schon mal zum Problem wird. Zudem halten die Ubuntu-Distributionen bis zu drei Versionen eines installierten Snaps auf dem System, um einen Schritt zurück zu einer älteren Version zu ermöglichen.

Jede Snap-Version verlangt aufgrund ihrer Bibliotheken ordentlich Platz auf dem Dateisystem. Laufen alle installierten Snaps unproblematisch, ist es

nicht nötig, die älteren Versionen auch noch zu behalten. Wie viele alte Snaps bereits installiert sind, verrät folgender Terminalbefehl:

```
sudo snap list --all
```

Archivierte, aber inaktive Snaps sind in der tabellarischen Übersicht in der letzten Spalte „Notes“ mit dem Hinweis „disabled“ beziehungsweise „deaktiviert“ gekennzeichnet. Eine Deinstallation eines dieser Snaps gelingt dann mit diesem Kommando:

```
sudo snap remove [Name]
--revision [Revision]
```

Den passenden Namen für den Platzhalter „[Name]“ entnehmen Sie der gleichnamigen Spalte „Name“ und den Wert von „[Revision]“ der Spalte „Rev“. Folgender Beispielbefehl entfernt das Snap „gnome-cal-

```
daver@bath:~$ snap list --all
```

Name	Version	Rev	Tracking	Publisher	Notes
core	16-2.39.3	7270	stable	canonical✓	core,disabled
core	16-2.40	7396	stable	canonical✓	core
core18	20190723	1074	stable	canonical✓	base
core18	20190709	1066	stable	canonical✓	base,disabled
gnome-3-26-1604	3.26.0	74	stable/...	canonical✓	disabled
gnome-3-26-1604	3.26.0-20190705	90	stable/...	canonical✓	-
gnome-3-28-1804	3.28.0-10-gaa70833.aa70833	71	stable	canonical✓	-
gnome-calculator	3.30.1	260	stable/...	canonical✓	disabled
gnome-calculator	3.32.1	406	stable/...	canonical✓	-
gnome-characters	v3.32.1-gitt2.3367201	296	stable/...	canonical✓	disabled
gnome-characters	v3.32.1-gitt2.3367201	317	stable/...	canonical✓	-
gnome-logs	3.32.0-4-ge8f3f3ca8	61	stable/...	canonical✓	-
gnome-logs	3.30.0	45	stable/...	canonical✓	disabled
gnome-system-monitor	3.30.0	57	stable/...	canonical✓	disabled
gnome-system-monitor	3.32.1-3-g0ea89b4922	100	stable/...	canonical✓	-
gtk-common-themes	0.1-4-g08bc1b2	818	stable/...	canonical✓	disabled
gtk-common-themes	0.1-22-gab0a26b	1313	stable/...	canonical✓	-

```
daver@bath:~$ sudo snap remove gnome-calculator --revision 3.30.1
```

Alte Snaps aussortieren: Ein länger genutztes Ubuntu-System bevorratet ältere Versionen von installierten Snap-Paketen. Die Deinstallation sorgt für Platz auf kleinen SSDs.

```
sudo snap remove gnome-calculator --revision 260
```

Viele Aktionen in der Befehlszeile sind mit verknüpften Kommandos automatisierbar – so auch diese: Die Zeile

```
sudo snap list --all | grep
"disabled\|deaktiviert"
| awk '{system("sudo snap
remove " $1 " --revision "
$3)}'
```

deinstalliert alle archivierten inaktiven Snaps in einem Aufwasch. **-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.

Programmfenster und virtuelle Desktops

Nach entsprechenden Deskooptipps der LinuxWelt habe ich mich inzwischen sehr an den Einsatz virtueller Arbeitsflächen gewöhnt, zwischen denen ich unter Linux Mint mit Strg-Alt-Rechts/Links wechsele. Allerdings gibt es immer wieder Situationen, wo ich den Dateimanager oder Browser permanent benötige. Dann muss ich sehr häufig zur passenden Arbeitsfläche zurückwechseln.

Harald T., per Mail

Die Fenstermanager unter Linux können ziemlich viel, wovon Linux Mint oder Ubuntu nur die wichtigsten Funktionen anzeigen. Die für diese Situation einschlägige Funktion ist aber auch hier zu finden: Wenn Sie die Titelleiste von Dateimanager oder Browser rechts anklicken (oder alternativ die Tastenkombination Strg-Leertaste drücken), dann erscheint das Fenstermenü mit der Option „Immer auf der sichtbaren Arbeitsfläche“. Ist diese Option aktiviert, erscheint dieses Fenster auf jeder Arbeitsfläche.

Die Einstellung gilt aber nicht dauerhaft für das jeweilige Programm, sondern nur für das aktuelle Fenster-Handle. Sobald das Fenster geschlossen wird, geht auch die Option wieder verloren.

Vereinfachte Dateiausgabe

Meine einfachen Bash-Skripts bestehen meistens nur darin, einige waktuelle Systeminformationen oder Dateilisten in eine Ausgabedatei zu schreiben. Dabei finde ich es reichlich umständlich, nach dem Muster

```
date > ~/out.txt
echo "----" >> ~/out.txt
```

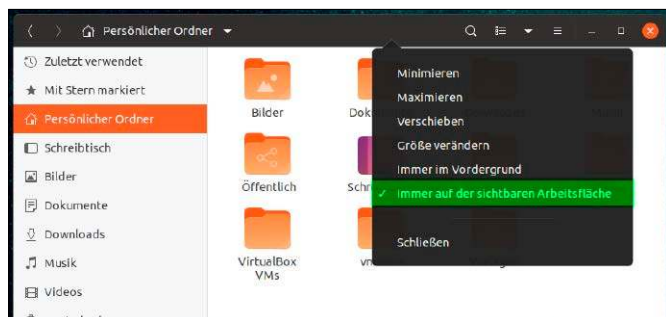
Zeile für Zeile die Ausgabedatei anzugeben.

Jens P., per Mail

Diese Schreibweise ist nicht nur lästig, sondern außerdem fehleranfällig, denn eine Umleitung mit „>“ (Datei wird neu angelegt) statt mit „>>“ (Anhängen) überschreibt bekanntlich den bisherigen Inhalt. Die Bash-Shell akzeptiert aber auch folgende, wesentlich elegantere Syntax:

```
{
date
echo "----"
lsblk -f
[...]
} > ~/out.txt
```

Alle Befehle innerhalb der Klammer schreiben dann ihre Infos in die zuletzt genannte Ausgabedatei. Die müssen Sie nur einmal und mit einfachem Umleitungszeichen eingeben. Statt den geschweiften Klammern können Sie auch runde Klammerzeichen verwenden.



Diese Einstellung sorgt dafür, dass ein Programmfenster auf allen virtuellen Arbeitsflächen und dort jeweils in gleicher Größe und Position angezeigt wird.

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:

idx-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
 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 Beteiligungsverhältnis: 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
Redaktionsassistentz: Manuela Kubon

Einsendungen: Für unverlangt eingesandte Beiträge sowie Hard- und Software übernehmen wir keine Haftung. Eine Rücksendegarantie geben wir nicht. Wir behalten uns das Recht vor, Beiträge auch auf anderen Medien, etwa auf DVD oder online, zu veröffentlichen.

Copyright: Das Urheberrecht für angenommene und veröffentlichte Manuskripte liegt bei der IT Media Publishing GmbH & Co. KG. Eine Verwertung der urheberrechtlich geschützten Beiträge und Abbildungen, insbesondere durch Vervielfältigung und/oder Verbreitung, ist ohne vorherige schriftliche Zustimmung des Verlags unzulässig und strafbar, soweit sich aus dem Urheberrechtsgesetz nichts anderes ergibt. Eine Einspeicherung und/oder Verarbeitung der auch in elektronischer Form vertriebenen Beiträge in Datensysteme ist ohne Zustimmung des Verlags unzulässig.
Haftung: Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Die Veröffentlichungen in der LinuxWelt erfolgen ohne Berücksichtigung eines eventuellen

Patentschutzes. Auch werden Warennamen ohne Gewährleistung einer freien Verwendung benutzt.
Bildnachweis: sofern nicht anders angegeben: Anbieter

Anzeigen
Anzeigenleiter:
 Sven Schrader
 Tel. 089/3398052-41
 E-Mail: schrader@it-media.de

Vertrieb
Vertrieb Handelsaufgabe:
 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 1/2020 erscheint am **29.11.2019**

Aus Aktualitätsgründen können sich Themen ändern.

Windows 7 geht! Ubuntu kommt!

Planen Sie rechtzeitig den Umstieg: Dieser Schwerpunkt diskutiert alle Varianten, das demnächst ablaufende Windows 7 durch Linux komplett oder teilweise (Multiboot, Virtualisierung) zu ersetzen, und vermittelt Ihnen das Know-how, die für Sie richtige Umstiegsvariante zu wählen. Ferner geht es um die geeigneten Distributionen, die sich für solchen Umstieg anbieten und allesamt aus dem Umfeld von Ubuntu stammen, aber nicht zwingend „Ubuntu“ heißen (Linux Mint, Elementary OS).



Sichere Daten im Netz & Web

Dateiverschlüsselung, Rechte, Tools und Tricks: Das Schwerpunktthema dreht sich um Datenschutz im Internet und Netzwerk. Die LinuxWelt bespricht alle wesentlichen Szenarien des Datenverkehrs und der Datenspeicherung im Web und im lokalen Netz: Welche Maßnahmen sind für welche Daten angemessen und komfortabel? Wo ist welche Verschlüsselung notwendig, wo ratsam? Welche Software, welcher Webdienst bietet die gewünschte Sicherheit?



Ubuntu 19.10



Vorstellung im Heft und Livesystem auf DVD: Version 19.10 („Eoan Ermine“) ist zwar nur ein Zwischenschritt, aber der kann wegweisend sein für die wichtige Langzeitversion LTS 20.04, die im Frühjahr nächsten Jahres ansteht. Traditionell fokussieren diese letzten Versionen vor einer LTS-Version vor allem auf Stabilität, weniger auf Innovation und Leistung. Überraschungen sind aber nie ausgeschlossen. Ob es mehr Neues gibt als einen aktualisierten Gnome-Desktop 3.34 und Nvidia-Treiber per Installation, erfahren Sie in der kommenden LinuxWelt.

Debian 10 „Buster“

Linux-Fels in Version 10: Schon für dieses Heft geplant, aber aus DVD-Kapazitätsgründen verschoben, holt die LinuxWelt die Vorstellung des Linux-Schwergewichts Debian 10 demnächst nach. Debian spielt seine tragende Rolle hinter den Kulissen: Fast alle prominenten Desktopsysteme wie Ubuntu oder Mint nutzen die Debian-Basis. Auch zahlreiche Spezialisten wie Raspbian, Open Media Vault, Bunsenlabs, Clonezilla, Tails, Steam-OS vertrauen auf das Debian-Fundament. Version 10 „Buster“ ist ein Meilenstein für Debian-Fans und für zahlreiche Derivate.





Sonderheft
für nur
12,90€

WLAN, DSL & Co.
ganz einfach
verbessern!

Jetzt bestellen unter
www.pcwelt.de/wlan 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 8/19 XXL Alles vernetzen! für nur 12,90€.

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

ABONNIEREN	Vorname / Name			
	Straße / Nr.			
	PLZ / Ort			
	Telefon / Handy		Geburts-tag TT MM JJJJ	
	E-Mail			

Ich bezahle bequem per Bankeinzug.
 Ich erwarte Ihre Rechnung.

BEZAHLEN	Geldinstitut
	IBAN
	BIC
	Datum / Unterschrift des neuen Lesers

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](https://www.tuxedocomputers.com)