JETZT NEU! Mit Extra-Download-DVD!

LINUX WELT

5/2022
August/September

Deutschland 8,99 €
Schweiz sfr 18,00 · Österreich + Benelux 10,50 €

Einsteiger-Tipps

So geht's ganz leicht: Cleverer Umgang mit Ordnern und Dateien

50 geniale Linux-Helfer

So verbessern Sie Ihr System!

NEU für Sie ausgewählt: Die besten Tools für

- System
- Hardware
- Datenschutz
- Desktop
- Terminal
- Netzwerk

Power-Tipps für das neue Ubuntu

Geniale Desktop-Tweaks für Komfort und Leistung

Retten mit Multiboot

Stick erstellen mit mehreren Systemen

Coole Platine für Ihr Linux

Raspberry-Konkurrent: Der neue Odroid M1

16 SEITEN SPECIAL

Linux sicher wie nie!

Schützen Sie Ihr System & Netzwerk: Viren bekämpfen, WLAN absichern, Daten verschlüsseln, VPN einrichten u.v.m.

DVD IM HEFT!

Multiboot
6 Top-Systeme

- Ubuntu Mate 22.04 LTS
- Peppermint-OS 5-22-2022
- Xubuntu LinuxWelt-Edition 22.04
- Open Suse Leap (Installer) 15.4
- Endeavour-OS „Artemis" 22.6
- Void Pup 22.02

LinuxWelt Digital XXL 5/22
Über 340 Seiten Linux-Know-how

EXTRA! DOWNLOAD-DVD!

Multiboot
Livesysteme & Tools

- Backbox 7
- 4M Linux 40
- Clonezilla 3.0
- Gparted Live 1.4

So geht's!
1. DVD runterladen
2. Auf Stick kopieren
3. Einfach loslegen

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

PC WELT

Windows unautorisiert!

Jetzt am Kiosk!

Sonderheft
für nur
9,90 €

Auf DVD: Profi-Paket zum Freischalten & Ausreizen

Bestellen unter
www.pcwelt.de/pcwelt-sonderheft 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 4/22 Windows für nur 9,90 €.

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

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PC-WELT aus dem Haus IDG Tech Media GmbH, Georg-Brauchle-Ring 23, 80992 München, Registergericht München, HRB 99110, Geschäftsführer: Jonas Triebel.
Die Kundenbetreuung erfolgt durch den PC-WELT Kundenservice, DataM-Services GmbH, Postfach 9161, 97091 Würzburg

Schatzsuche im Tool-Dschungel

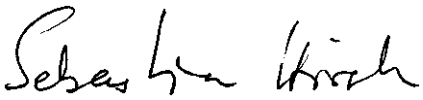
Schätze zu suchen (und nach Möglichkeit auch zu finden) gehört seit jeher zu den Tätigkeiten, die jeden faszinieren: Der Nervenkitzel bei der Suche oder der Adrenalinkick beim Finden lassen niemanden kalt. Allerdings gibt es Ausnahmen – das stundenlange Stöbern etwa auf schwer verständlichen Websites oder in Tool-Listings im Internet ist nicht unbedingt jedermanns Sache.

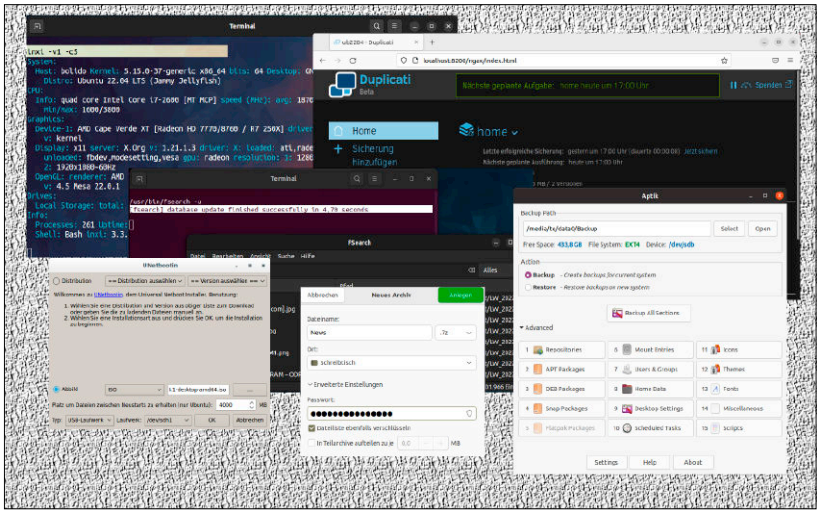
Ebensowenig wird das Laden, Installieren, Ausprobieren und Löschen der gefundenen Tools zu jedermanns Lieblingsbeschäftigung zählen – und so mancher mag die Zeiten zurücksehnen, wo es für jede Aufgabe mehr oder minder nur ein Werkzeug gab.

Um Ihnen nun die Sucharbeit nach den besten Tools für Ihre Aufgaben zu ersparen, haben wir 50 sehr gute Systemwerkzeuge zusammengetragen, die ihresgleichen suchen. Sei es für klassische Systemaufgaben, für die Dateiverwaltung, die Hardware-Pflege oder den Netzzugriff – unsere Tools gehen meist weit über das hinaus, was die integrierten Standardwerkzeuge können. Und das Beste: Sie können sich ohne langes Suchen gleich auf das Ausprobieren konzentrieren. Viel Spaß dabei!

Sebastian Hirsch
Chefredakteur
shirsch@it-media.de

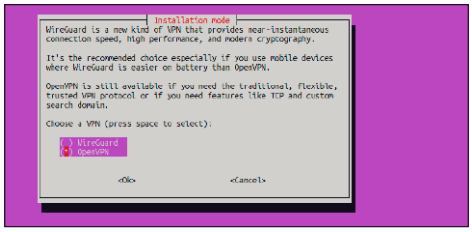
Herzlichst, Ihr





50 geniale Linux-Helfer

Das Heftspecial empfiehlt und erklärt die besten Ergänzungen für System, Backup, Netzwerk und Desktop. Es handelt sich ausnahmslos um Top-Werkzeuge, die auf keinem Linux fehlen sollten. S. 28



Sicher wie nie!

VPN, Datenschutz, Serverkontrolle: Das Special bringt Basics, Tools und Tricks für sichere Linux-Systeme. S. 44

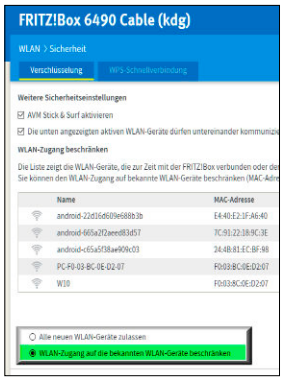
Neu: Odroid M1

Cooler Raspberry-Gegner mit SATA & NVMe: Die neue Hardkernel-Platine ist ungewöhnlich anschlussfreudig. S. 76

Grundlagen

Special I – Top-Tools für System, Desktop und Netzwerk

Special II – Sicherheit & Datenschutz



Standards

Die Highlights der DVD

Auf Heft-DVD: 5 Linux-Desktops und ein kleines Livesystem

Ubuntu Mate, Xubuntu, Endeavour und Peppermint sind mittelschwere Desktopdistributionen, die sich auch für nicht mehr taufrische Hardware eignen. Der Open-Suse-Installer installiert ein etwas anspruchsvolleres KDE-System. Das kleine Puppy-Livesystem Void Pup ergänzt die Sammlung.

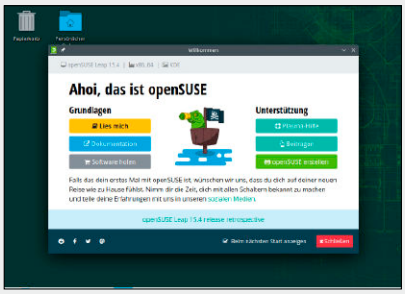
S. 10

Ubuntu Mate 22.04

Ein Allzwecksystem im besten Sinne: Diese Ubuntu-Variante mit Mate-Oberfläche ist genügsam, einsteigertauglich und anpassungsfähig.

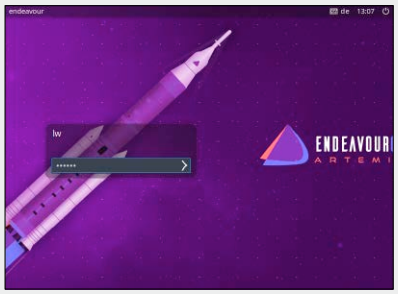
Open Suse Leap 15.4

Bewährter Desktop, bewährter Server: Open Suse „Leap" tendiert zunehmend zu Serveraufgaben, gefällt aber auch mit KDE in der Desktop-Rolle.

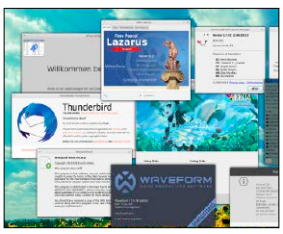


Endeavour-OS „Artemis"

(Noch) nichts für Einsteiger, aber immer komfortabler: Das schnelle Endeavour macht Arch-Linux mit Installer und Systemtools mehrheitsfähig.

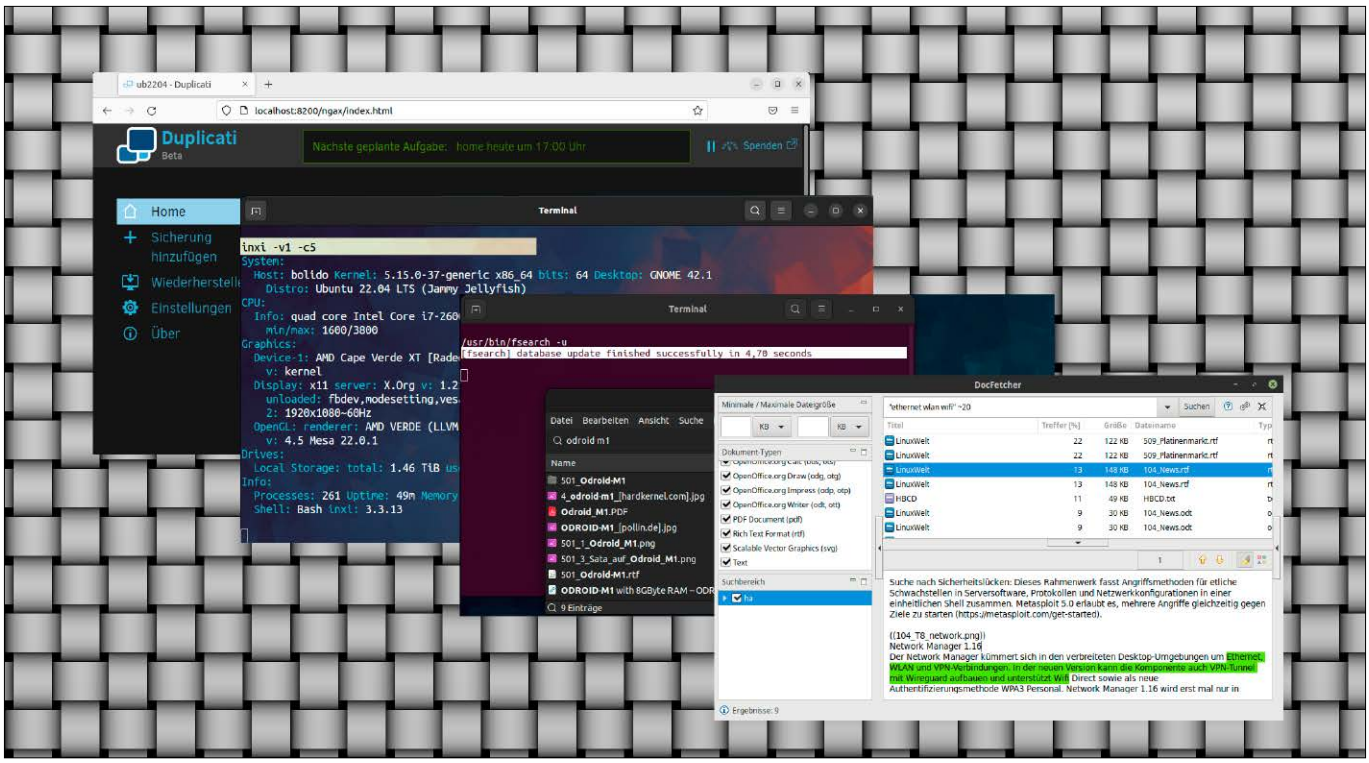


Software & Distributionen



Netzwerk & Server

Praxis



Jäger und Sammler

„Die besten Tools“ versprechen wir am Titel, und die bekommen Sie auch: Die in diesem Heft vorgestellten Werkzeuge sind sorgfältig ausgewählte Empfehlungen der LinuxWelt-Redaktion, die auf jedem Linux-System die Produktivität steigern.

VON HERMANN APFELBÖCK

Neben großer Softwareprominenz wie Libre Office, Browser, Gimp oder VLC gibt es eine Legion von kleinen, spezialisierten Hilfsprogrammen („Tools“). Da ist im Linux-Umfeld (und im Windows-Biotop mindestens genauso) manches redundant, anderes allzu eng spezialisiert, wieder anderes schlicht qualitativ fragwürdig. Alles einsammeln, nur weil es Open Source, Freeware und gratis ist, ist gewiss nicht die optimale Strategie.

Der verantwortungsvolle Jäger erlegt nicht alles, was sich bewegt: Nur die wirklich besten Kandidaten für den jeweiligen Job lohnen eine Installation.

Die qualitativ besten Tools von der Spreu zu trennen, ist ein Job, der viel Erfahrung – auch mit der Spreu – voraussetzt. Diesen Job nehmen wir Ihnen ab: Die ab Seite 28 vorgestellten Tools umfassen 45 Einzelvorstellungen plus eine Handvoll Verweise zu wichtigen Alternativen – insgesamt 50 Werkzeuge, die allesamt zur Spitzenklasse der Linux-Werkzeuge zählen. Noch besser: Diese „Premier League“ ist mit den hier genannten Tools auch ziemlich vollständig repräsentiert. Mehr brauchen Sie nicht, um für alle Aufgaben optimal ausgerüstet zu sein. Und da nicht jedes System alle Aufgaben erledigen muss, gilt auch hier der Ratschlag, gezielt auszuwählen. Dabei hilft die Kategorisierung der Sammlung in Systemtools, Infozentralen, Sicherungswerkzeuge, Netzwerktools und Desktopergänzungen.

Bei einer Sammlung von Top-Tools werden erfahrene Linux-Nutzer auf manchen Klassiker treffen, den sie längst kennen und nutzen. Das ist unvermeidlich, aber unsere Empfehlungen halten gewiss auch für Kenner Überraschungen bereit.

Egal ob Linux-Kenner oder Einsteiger – jede Toolvorstellung liefert ausreichend Informationen, um den sofortigen praktischen Einsatz zu ebnen und den Wert und das Alleinstellungsmerkmal der Software zu verdeutlichen.

Weitere Themen im Heft

Im zweiten Heftschwerpunkt ab Seite 44 geht es um **Systemschutz, Netzwerkabsicherung und Datenschutz.** Fünf Beiträge diskutieren engere Aspekte der Router- und NAS-Absicherung, der Einrichtungsvarianten für VPN, einer jüngeren Methode der Home-Verschlüsselung sowie der Dienste-Analyse und der Schädlingserkennung. Ein einleitender Beitrag ergänzt das Sicherheitsspecial um allgemeine Grundregeln zu Datensicherheit und Datenschutz.

Von den weiteren Einzelbeiträgen möchten wir zwei an dieser Stelle herausheben:
„**Multiboot mit ISO-Dateien**“ geht investigative Wege, um ISO-Images mit und ohne Persistenz oder im Multiboot-Ensemble von USB zu starten. Bestimmte Aspekte dieser Boot-Zaubereien eignen sich auch für angepasste Windows-Installationen (ab Seite 22).
Der neue **Raspberry-Konkurrent Odroid M1** hat mit SATA, NVMe, eMMC, SD, USB respektables Anschlusspotenzial. Die LinuxWelt-Redaktion hatte den Platinenrechner im Test und meldet sehr viel Licht und ganz wenig Schatten (ab Seite 76).

Exzellente Desktops: Mit zwei Ubuntus, Open Suse und den sehr ansehnlichen Distributionen Peppermint und Endeavour ist Debian-, Slackware- und Arch-Prominenz verteten. Das winzige Livesystem Void Pup ergänzt die Heft-DVD.

Die Heft-DVD

Die Heft-DVD liefert vier Livesysteme zum Ausprobieren und Installieren, den reinen Installer für Open Suse Leap 15.4 sowie das pure Livesystem Void Pup. Das enthaltene Xubuntu 22.04 ist ein **exklusiver Service für LinuxWelt-Leser**, weil es entgegen der Ubuntu-Politik einen klassischen Firefox-Browser mitbringt. Ein bislang seltener Gast auf der LinuxWelt-DVD ist **Endeavour-OS,** das auf dem besten Weg ist, Arch Linux am Endanwender-Desktop zu etablieren.
Die Heft-DVD kann aber mehr, als diese Linuxsysteme zu booten: Unter „Extras und Tools“ gibt es Nothelfer wie Super Grub Disk. Als DVD-Inhalte finden Sie Software wie Unetbootin, USB Imager und Putty, außerdem das stets aktualisierte PDF „LinuxWelt Digital XXL 5/22“.
Die Benutzung der DVD ist einfach: Inhalte wie das XXL-Handbuch oder die enthaltene Software erreichen Sie mit jedem System nach Einlegen der DVD im Dateimanager.
Um hingegen Livesysteme, Installer oder ein Boottool wie Super Grub zu starten, müssen Sie den Rechner mit der DVD neu booten. Standardmäßig geschieht dies bei eingelegter DVD automatisch. Falls nicht, rufen Sie beim Start per Tastendruck (leider nicht standardisiert: F2, F8, F10, Esc?) das Bios-Bootmenü auf und wählen hier manuell das DVD-Laufwerk.
Bei der Nutzung eines Livesystems bleiben Ihre Festplatte und das dort installierte System unberührt. Das ändert sich erst, wenn Sie aus einem Livesystem den dort enthaltenen Installer starten. Falls Sie eine Dualboot-Installation neben einem bereits bestehenden System planen, müssen Sie Klarheit haben, in welchem Modus (Bios/Uefi) jenes installiert ist, und dann im selben Modus installieren. Die Heft-DVD beherrscht Bios wie Uefi und zeigt den aktuellen Modus im Menü an.
Extra-DVD: Beachten Sie die zusätzliche Multiboot-DVD zum Download, die mit Backbox, 4M Linux, Clonezilla und Gparted Live vier leistungsfähige Reparatur- und Sicherheitssysteme bootet. Infos zum Download und den enthaltenen Spezialdistributionen finden Sie auf Seite 13. ■

AUF DVD

Distributionen

10 **Peppermint-OS 5-22-2022**
Webfokussiertes Desktopsystem auf Debian-Basis mit XFCE

11 **Ubuntu Mate 22.04 LTS**
Offizielle Ubuntu-Variante mit einsteigerfreundlichem Mate

12 **Xubuntu 22.04 LTS**
LinuxWelt-Edition mit schnellem Firefox als DEB-Installation

12 **Open Suse Leap 15.4**
Grafischer Netinstaller für das aktuelle Open Suse Leap

14 **Void Pup 22.02**
Reines Puppy-Livesystem mit minimalistischem konzept

60 **Endeavour-OS 22.6 „Artemis“**
Sehr schnelles Arch Linux mit Installer und Konfigurationstools

Extras und Tools
Supergrub, Memtest, Hardware Detection Tool, Plop-Bootmanager u. a. m.

Software für Linux und Windows:
7-Zip, USB Imager, Infrarecorder, Bittorrent-Client, Unetbootin, Putty/Kitty

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

Auf DVD: 6 Mal Linux

Neben zwei Ubuntus 22.04 in der einsteigerfreundlichen Mate-Edition und einem Xubuntu mit klassischen Firefox sind auch der Installer von Open Suse Leap 15.4 und das neue Endeavour-OS vertreten.

Ubuntu Mate 22.04 (64 Bit)
Für Einsteiger und jene Anwender, die einen bequemen Linux-Desktop suchen, ist Ubuntu Mate im Kreis der offiziellen Ubuntu-Versionen eine heiße Empfehlung. Die Softwareboutique macht die Installation der gewünschten Programme besonders einfach. Das System liegt auch als ISO-Datei vor.

Peppermint-OS 5-22-2022 (64 Bit)
Ciao Ubuntu, hallo Debian: Peppermint-OS wechselt seine Betriebssystembasis zu Debian 11. Der Desktop ist hier ein XFCE 4.16 mit vielen Anpassungen. Es bleibt aber ein komfortables, schlankes System mit Webfokus. Es ist auch als ISO-Datei auf DVD.

Xubuntu LinuxWelt-Edition 22.04 LTS (64 Bit)
Ein Ubuntu-System für Fortgeschrittene, die wissen, was sie brauchen; Diese Variante mit XFCE-Oberfläche liefert eine von der LinuxWelt angepasste Edition, in der Firefox dauerhaft als DEB vorinstalliert ist (aus den Mozilla-Paketquellen). Das System ist auch als ISO-Datei auf DVD.

Open Suse Leap 15.4 Installer (64 Bit)
Kein Livesystem, sondern ein bootfähiger grafischer Installer: Damit installieren Sie Open Suse Leap 15.4 mit KDE 5.24 oder anderen Desktops. In dieser Ausgabe aktualisiert Open Suse Leap seine Kernkomponenten unter anderem auf den Kernel 5.14. Der Installer ist auch als ISO-Datei auf DVD.

Endeavour-OS „Artemis“ 22.6 (64 Bit)
Dieses Arch-Linux hat ursprünglich das beliebte Antergos abgelöst und einen ähnlichen Anspruch – den einfacheren Einstieg zu Arch Linux. Endeavour-OS ist als Livesystem mit grafischem Installer auf DVD, der viele Desktops zur Auswahl bietet. Das System ist auch als ISO-Datei auf DVD.

Void Pup 22.02 (64 Bit)
Das kleine Livesystem nutzt Puppy Linux als Basis und ist für einen geringen Ressourcenverbrauch optimiert. Void Pup ist aus Void-Linux-Paketen gebaut und bringt eine sehr schlanke Arbeitsoberfläche mit. Ein Browser ist vorinstalliert. Void Pup bootet von DVD sowohl im Bios- als auch im Uefi-Modus.

Extras & Tools

Netboot.xyz 2.0.57 (64/32 Bit)
Dieses bootfähige Tool ist selbst keine Linux-Distribution, sondern ein Bootprogramm, das eine große Auswahl von Linux-Systemen per Menü anbietet, von Github in den Arbeitsspeicher herunterlädt und startet. Netboot.xyz basiert auf iPXE und arbeitet auf regulärer PC-Hardware mit Ethernet-Verbindung ins Internet.

Shred-OS 2021.08.2
Das winzige Livesystem startet ein Menü im Textmodus, um Daten auf magnetischen Datenträgern endgültig zu überschreiben. Auch Wiederherstellungstools können dann nichts mehr rekonstruieren. Auf Flashspeichern, SSDs und USB-Sticks ist das Tool wirkungslos, denn die Controllerbausteine dieser Datenträger erlauben kein sequenzielles vollständiges Überschreiben. Auf magnetischen Datenträgern ist Shred-OS sehr zuverlässig. Es startet im Uefi- sowie Bios-Modus.

Super Grub Disk 2.04
Im Uefi und Bios-Modus: Das startfähige Tool Super Grub Disk 2 liefert eine Boothilfe für Linux-Systeme, bei welchen der Bootloader vom Typ Grub 2 nicht mehr intakt ist oder von Windows überschrieben wurde. Im Multibootmenü der DVD wird das Tool unter „Extras und Tools“ bei einem Boot im Bios- und Uefi-Modus angezeigt und liegt als ISO-Datei im Ordner „Extras“.

Hardware Detection Tool 0.5.2
Nur im Bios-Modus: Das Hardware Detection Tool liefert einen Überblick zur kompletten Hardware eines Rechners, auch wenn dort noch kein Betriebssystem installiert ist. In einem englischsprachigen Menü zeigt HDT Kategorien wie PCI, RAM, Prozessor und Bios an und liefert dort dazu alle technischen Details.

Memtest 86+ 5.31b
Nur im Bios-Modus: Memtest 86+ zeigt sich im Multibootmenü beim Start der DVD im Bios-Modus. Die Speicheranalyse testet die RAM-Module auf Fehler und unterstützt dabei 32-Bit- als auch 64-Bit-CPUs sowie alle verbreiteten RAM-Typen. Das Tool beginnt sofort nach dem Start automatisch mit den Tests, die jederzeit unterbrochen werden können.

Plop Bootmanager 6
Nur im Bios-Modus: Der Plop Bootmanager ist ein Boothelfer mit einem eigenen Treiber für USB-Geräte und CD/DVD-ROM-Laufwerke. So kann dieser Bootmanager von diesen Laufwerken booten, obwohl dies das Bios des PCs nicht unterstützt.

Software auf DVD

laufwerke.sh
Das Bash-Script der LinuxWelt-Redaktion listet angeschlossene Laufwerke mit ihrer eigenen SATA-Geschwindigkeit und der Geschwindigkeit des SATA-Ports auf. Mehr Infos dazu liefern die Hardwaretipps im Praxisteil (Seite 101).

laufwerke.py
Das Python3-Script der LinuxWelt-Redaktion hilft ebenfalls mit der Auflistung der angeschlossenen Laufwerke, um mehrere SATA-Datenträger in einem Rechner optimal auf die verfügbaren SATA-Ports zu verteilen. Es zeigt mehr Details als das Bash-Script und nutzt dazu die Smartmontools.

Infrarecorder 0.53
Immer wieder nützlich: Ein Brennprogramm für ISO-Dateien unter einer Open-Source-Lizenz, welches Windows-Anwendern hilft, die mitgelieferten Imagedateien auf Heft-DVD auf einen DVD-Rohling zu brennen. Der bewährte Infrarecorder 0.53 für Windows (alle Versionen) liegt mit Installer und als portable Version vor.

USB Imager 1.0.8
Das Tool USB Imager dient zur bootfähigen Übertragung einer Imagedatei Image auf einen USB-Stick oder eine Speicherkarte. Das Open-Source-Tool für Linux, Windows und Mac-OS bietet eine deutschsprachige Oberfläche.

Tixati 2.89
Die Heft-DVD liegt als ISO-Datei zur Übertragung auf USB-Sticks oder zum Brennen auf Dual-Layer-DVDs jetzt auch als Bittorrent-Download vor. Die Torrent-Datei liegt unter *https://git.io/JykeH* auf Github. Tixati ist dazu ein Bittorrent-Client für Windows (Freeware ohne Adware), englischsprachig in 32- und 64-Bit-Version auf DVD.

Unetbootin 7.02
Das nützliche USB-Tool mit grafischer Oberfläche transferiert mit wenigen Klicks die ISO-Images von Ubuntu und seinen Abkömmlingen wie Linux Mint bequem auf USB-Stick oder Speicherkarten und macht diese mit einem eigenen Bootmenü startfähig. Hinzu kommt eine wichtige Option für persistenten Speicher. Auf DVD finden sich 32-Bit und 64-Bit-Ausgaben für Linux, Windows und Mac-OS.

Putty 0.77
Putty ist der klassische Terminalclient für den SSH-Zugriff auf Linux-Server unter Windows. Putty liegt als portables Tool vor, das unter allen Windows-Versionen ohne Installation läuft. Das Open-Source-Programm ist englischsprachig.

Kitty 0.76.0.8
Kitty ist eine Abspaltung von Putty und ebenfalls ein Terminalclient für SSH, allerdings mit einigen ergänzten Funktionen und bequemen Features wie direkte Kennwortübergabe. Genau wie Putty wird es einfach über seine EXE-Datei gestartet.

7-Zip 21.07
Neue Ausgabe des Open-Source-Programm 7-Zip: Das Tool 7-Zip für Windows ist eine leistungsfähige Alternative zu den Packern Winzip und Winrar. 7-Zip kommt nicht nur mit gängigen Formaten wie ZIP, CAB, RAR, ARJ zurecht, sondern auch mit typischen Linux-Formaten wie GZ. Außerdem ermöglicht es kennwortgeschützte Archive.

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

LinuxWelt XXL Digital: Das komplette Handbuch 5/22

Gezielt suchen – entspannt schmökern: Das aufgefrischte PDF liefert zeitlose Grundlagen und aktualisierte Rubriken zu Linux und Open Source. Das neue E-Book wirft einen Blick auf zehn Jahre Raspberry Pi sowie auf das neue Ubuntu 22.04 LTS. Ein gerade neu aufgenommenes Praxisthema zeigt die Konfiguration des Network-Managers per Scripts, die einen Standortwechsel automatisieren können. Ein neuer Praxisartikel zum Bootmanager Grub 2 erklärt den Systemstart mit und ohne Grub.

Weitere Infos

Die Vorstellung der sechs Systeme auf DVD und eines zusätzlichen DVD-Image (4,7 GB) zum Download per Bittorrent beginnt ab Seite 10. Endeavour-OS hat einen eigenen Artikel im Heft bekommen (Seite 60). Zusätzliche Anleitungen und Hinweise zu den Distributionen auf Heft-DVD liefert die dortige Übersicht, die Sie über die Datei „index.html“ in einem beliebigen Browser öffnen.

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

Sagen Sie uns Ihre Meinung – und gewinnen Sie!

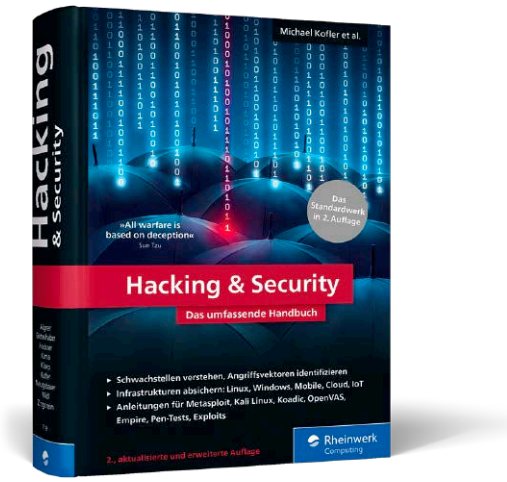
Wir möchten Linux-Hefte machen, die ganz Ihren Bedürfnissen und Interessen entsprechen. Dabei können Sie uns helfen! Füllen Sie einfach unseren Fragebogen im Internet aus. Das Beantworten der Fragen dauert nur rund zehn Minuten.

Unter allen Teilnehmern verlosen wir 3 Exemplare des Buches „Hacking & Security“ aus dem Rheinwerk Verlag.

Angriffe abwehren, Systeme absichern, Schwachstellen aufspüren

Hacking & Security

Das umfassende Handbuch



Autoren: Michael Kofler, André Zingsheim, Klaus Gebeshuber, Stefan Kania, Markus Widl, Peter Kloep, Roland Aigner, Thomas Hackner, Frank Neugebauer
Verlag: Rheinwerk Computing, 1134 Seiten, 2., aktualisierte und erweiterte Auflage 2020, gebunden, 49,90 Euro
ISBN: 978-3-8362-7191-2

Nur wenn Sie verstehen, wie ein Angreifer denkt, können Sie Ihre IT-Systeme auch wirklich absichern. Dieses umfassende Handbuch ist der Schlüssel dazu. Die Security-Profis rund um Bestseller-Autor 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!

- **Schwachstellen verstehen, Angriffsvektoren identifizieren**
- **Infrastrukturen absichern: Linux, Windows, Mobile, Cloud, IoT**
- **Anleitungen für Metasploit, Kali Linux, hydra, OpenVAS, Empire, Pwnagotchi, Pen-Tests, Exploits**

PLUS: Gratisheft für alle Teilnehmer

SO FUNKTIONIERT'S:

Auf *www.pcwelt.de/lin* gelangen Sie direkt zu unserer Leserbefragung und nehmen automatisch an der Verlosung teil. Von der Verlosung ausgenommen sind Mitarbeiter des Verlags und deren Angehörige. Der Rechtsweg ist ausgeschlossen. **Einsendeschluss für das Gewinnspiel in LinuxWelt 5/2022 ist der 26.09.2022.**

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

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

Jeder Teilnehmer bekommt als Dankeschön die LinuxWelt XXL 2/2022 „Linux statt Windows“ (ohne Datenträger).

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

Peppermint-OS 5-22-2022

Abschied von Ubuntu: Peppermint-OS tauscht den Unterbau mit Debian aus. Es bleibt dabei ein komfortables, webfokussiertes Desktopsystem mit XFCE 4.16 als Arbeitsfläche. Peppermint liegt als installierbares Livesystem auf Heft-DVD.

VON DAVID WOLSKI

Nicht nur an den Linux-Interna, sondern auch an der Oberfläche hat sich einiges getan: Peppermint-OS setzte einst auf eine sehr schlanke LXDE-Umgebung, zu der Teile von XFCE schrittweise über die Jahre hinzukamen. Jetzt ist Peppermint-OS bei einem beinahe puren XFCE 4.16 angekommen. Wie bisher ergänzt die Distribution aber weitere eigene, vornehmlich in Python 3 programmierte Tools zur Einrichtung sowie zur vereinfachten Konfiguration: Ein grafischer Updatemanager aktualisiert das System bei Bedarf oder auch zu einstellbaren Zeiten im Hintergrund. Auch für Einsteiger-Linux macht das System deshalb eine gute Figur, wobei einige der eigenen Tools und das Livesystem jedoch nur in Englisch vorliegen.

Erster Gruß: Zur Einrichtung präsentiert Peppermint-OS einen Willkommensbildschirm, der Schaltzentralen für den Desktop und ein Menü zur weiteren Softwareinstallation bietet.

Individuell: Pakete zur Installation wählen

Die Abkehr von Ubuntu bedeutet auch ein Abschied vom Ubuntu-Installer Ubiquity, der jetzt von Calamares abgelöst wurde, den beispielsweise auch Manjaro und Kubuntu verwenden. Bei der ersten Einrichtung aus dem Livesystem heraus zeigt sich Peppermint-OS mit dem neuen Installer aber gleich flexibler: Verschiedene Paketgruppen stehen zusätzlich in ausklappbaren Kategorien zur Auswahl. Nach erfolgter Installation begrüßt ein englischsprachiger Willkommensbildschirm für die ersten Schritte. Dort gibt es über „Open Pephub → Hardware & Software → Suggested Packages“ eine Liste, die weitere Anwendungen mit wenigen Klicks aus dem Debian-Stable-Zweig nachrüstet. Es gibt dort auch die Möglichkeit, das System fit für Flatpaks sowie Snap-Pakete zu machen und deren Runtimes einzurichten. Später steht als grafischer Paketmanager das bekannte Synaptic bereit.

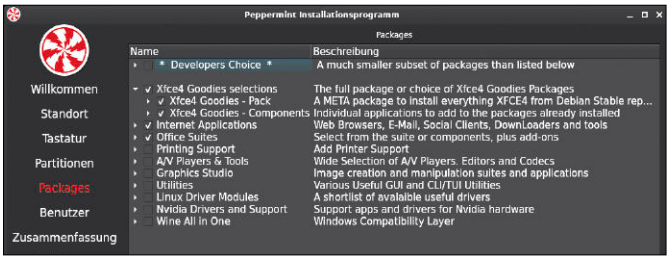
Web-Apps: Eigene Links erstellen

Traditionell setzt die Distribution einen Schwerpunkt auf Anwendungen, die im Webbrowser laufen.

Diese sollen sich hier, ähnlich wie Electron-Apps, möglichst nahtlos zwischen den regulären Anwendungen einfügen und Browserelemente ausblenden.

Während die ersten Ausgaben der Distribution dazu noch Mozilla Prism nutzten und noch vorgefertigte Links zu Google Docs, Pixlr und anderen Cloud-Apps mitlieferten, gibt Peppermint-OS nun keine dieser Webanwendungen vor. Es gibt über den Menüpunkt „Internet → Ice“ aber wieder einen Baukasten, der aus URLs von Web-Apps Programmverknüpfungen im Anwendungsmenü erstellt. Damit dies funktioniert, muss Google Chrome oder Chromium installiert sein. Im Baukasten kommt die gewünschte Bezeichnung in das Feld „Name...“ und darunter die komplette URL. Ganz unten gibt es eine Klickbox, welche die so eingerichtete Web-App in einer Browserinstanz isoliert, also nicht auf Cache und Cookiespeicher zugreifen kann. Dies ist wichtig, um verschiedene Log-ins und Identitäten bei Onlinediensten zu trennen.

Mehr Infos zu Peppermint-OS
Website: *http://peppermintos.com*
Dokumentation:
http://peppermintos.com/guide



Paketbote: Wer genau weiß, was benötigt wird, kann schon im Installer diese Paketgruppen auswählen.

Ubuntu Mate 22.04

VON DAVID WOLSKI

Aus dem offiziellen Ubuntu-Zoo ist dies die einsteigerfreundlichste und dabei sehr anpassungsfähige Ubuntu-Variante (in 64 Bit auf DVD). Die Aufmerksamkeiten beginnen schon nach der Installation, am Willkommensbildschirm zur weiteren Einrichtung. An dieser Stelle gibt es unter „Anwendungen" eine besonders bequeme Paketverwaltung, welche eine Reihe an populären Programmen mit wenigen Klicks einrichtet – auch Software, die sich nicht in den Standard-Paketquellen findet wie beispielsweise Spotify, Google Chrome und Microsoft Edge. Davon abgesehen liefert Ubuntu Mate eine Softwareausstattung, die für den Gnome-Desktop typisch ist, mit Firefox, Libre Office 7.3 und dem Player Celluloid 0.20. Viele ehemalige Gnome-Programme wie Texteditor, PDF-Betrachter und Dateimanager sind ebenfalls in ihrer Mate-Abspaltung vorhanden. Anders als die Ubuntu-Hauptedition unterstützt die Mate-Variante neben App-Containern im Snap-Format auch von Haus aus die Flatpaks der Gnome Foundation. Dieses Ausscheren vom offiziellen Kurs Canonicals kommt Anwendern zugute, die auch Programme von Flathub benötigen. Der Mate-Desktop (Version 1.26) hat in dieser Ausgabe wieder viel Liebe zum Detail gesehen und Fehlerbehebungen erhalten, die dafür sorgen, dass in Ubuntu Mate wieder das flotte Umschalten des Arbeitsflächen-layouts funktioniert. Unter anderem gibt es das Layout „Mutiny", das ein Dock im Stil von Unity anzeigt.

Mehr Infos zu Ubuntu Mate
Website: *https://ubuntu-mate.org*
Dokumentation:
https://ubuntu-mate.org/about

Xubuntu 22.04 LinuxWelt-Edition

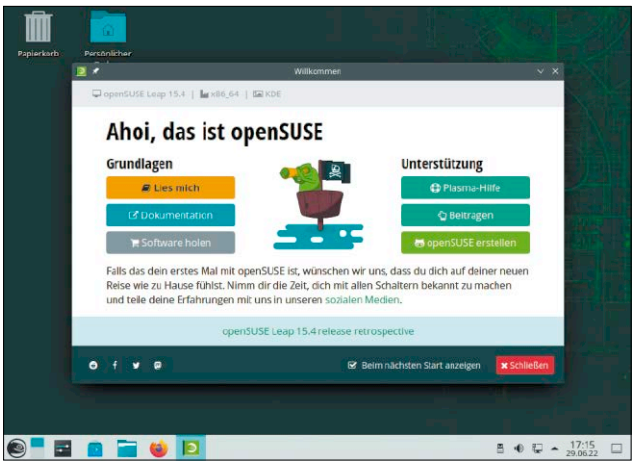
VON DAVID WOLSKI

Xubuntu 22.04 war schon bei der letzten LinuxWelt dabei, meldet sich hier aber in einer besonders fettarmen LinuxWelt-Edition zurück, in welcher Firefox als DEB-Paket vorinstalliert ist. Der Browser stammt aus dem externen Ubuntu-Repository *https://launchpad.net/~mozillateam/+archive/ubuntu/ppa* und diese Quelle wird hier bevorzugt und ist auch für automatische Aktualisierungen aktiviert. Bei Systemupdates wird also nicht die Snap-Version von Firefox über das DEB geschrieben, sondern stets selbiges aktualisiert. Davon abgesehen liefert die LinuxWelt-Edition nur das Nötigste und überlässt es den Anwendern, weitere Programme selbst über apt oder über die grafische Paketverwaltung von Synaptic zu installieren. Diese Xubuntu-Variante ist also eine Distribution für Anwender, die einen klassischen Firefox möchten und im Übrigen wissen, was sie sonst auf dem Desktop sehen wollen. Als Oberfläche dient das aktuelle XFCE 4.16 mit einem gewohnt aufgeräumten blau-grauen Erscheinungsbild mit dem Thema „Greybird". Es ist die bekannt funktionale, schlichte, aber ausbaufähige Arbeitsumgebung, die auch mit sehr hohen Auflösungen (Hi-DPI) zurechtkommt. Zwischen 100 und 200 Prozent Skalierung sind in den Einstellungen zur Anzeige auch Zwischenschritte möglich – ideal für Laptops mit ungewöhnlicher Pixeldichte oder kleinen Displayformaten zwischen 12 und 14 Zoll. Xubuntu auf Heft-DVD startet als Livesystem und enthält den gewohnten Ubuntu-Installer. Aufgrund der schmalen Grundausstattung verlangt das System zunächst nur sechs GB Platz auf dem Datenträger.

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

Open Suse Leap 15.4 (Installer)

VON DAVID WOLSKI

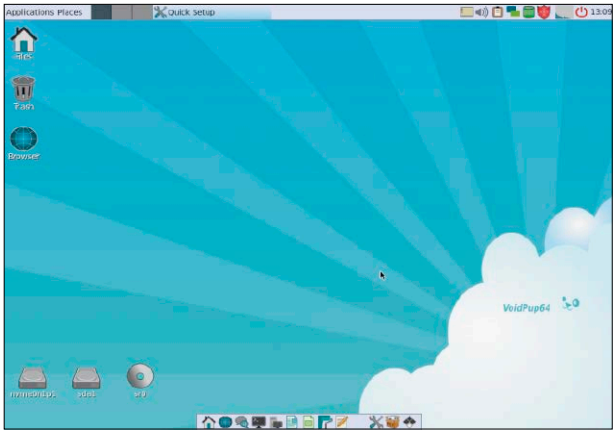


Für viele Linux-Anwender der älteren Semester war Suse das erste Linux auf dem eigenen PC. Inzwischen wandelt Open Suse aber in den Fußstapfen von Suse Linux Enterprise, von welchem es die wichtigen Pakete übernimmt. Genau genommen handelt es sich um eine freie Variante von Suse Linux Enterprise (SLE), die im jährlichen Rhythmus als neue Hauptversion vorliegt. Dies bringt mehr Stabilität und lange Unterstützungszeiträume bei etwas älteren Softwareversionen. So ist der Kernel noch in Version 5.14 enthalten, allerdings mit vielen Backports von aktuelleren Kernel-Versionen. In einer Sache ist sich Suse treu geblieben: Die traditionsreiche Linux-Distribution bleibt ein Aushängeschild für KDE und seine Anwendungen, denn diese Umgebung macht hier eine besonders gute Figur. In den Paketquellen enthalten ist KDE Plasma 5.24, das seitens der KDE-Entwickler wieder als Version mit Langzeitsupport markiert wurde. Zudem sind aber auch Gnome 41 und XFCE 4.16 verfügbar. Die Softwareauswahl umfasst Libre Office 7.2, den Browser Firefox, der bei einer KDE-Installation noch durch Konqueror ergänzt wird. Als Mediaplayer ist nur noch der VLC vorinstalliert. Weitere Player müssen manuell nachinstalliert werden und warten mit weiteren Codecs in externen Repositorys (*https://opensuse-community.org*). Auf Heft-DVD ist Open Suse Leap 15.4 nicht als Livesystem, sondern als grafischer Installer vertreten, der die ausgewählten Pakete über eine Internetverbindung bezieht. Diese muss über Ethernet bereitstehen, WLAN funktioniert nicht.

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

Void Pup 22.02

VON DAVID WOLSKI

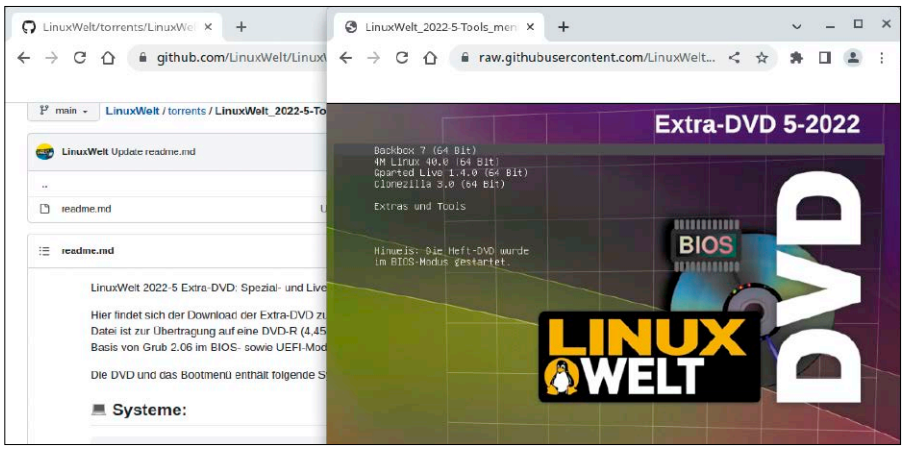


Ein neues Rezept für ein minimalistisches Livesystem aus der Familie von Puppy Linux: Bei Void Pup handelt es sich um ein besonders kleines Puppy-System, das als Basis Void Linux nutzt (*https://voidlinux.org*). Diese anspruchsvolle Entwicklung aus dem Umkreis von Net BSD zeichnet sich durch ihren sehr schlanken Aufbau aus, die vom üblichen Puppy-Desktop JWM und Konfigurationstools ergänzt wird. Entsprechend gering ist der Speicherbedarf des Livesystems: Nur 250 MB RAM sind nach dem Start belegt. Als Browser ist Light 48 vorinstalliert, der auf Firefox ESR basiert. Light verspricht aber, durch Verzicht auf einige Komponenten schneller und ressourcenschonender als Firefox ESR zu sein. Für WLAN-Verbindungen steht der Frisbee Network Manager bereit. Die von der Heft-DVD startende Version nutzt den Linux-Kernel 5.15. Bei der kompakten Größe des gesamten Systems von nur 390 MB bringt Void Pup nur wenige vorinstallierte Anwendungen mit, jedoch gibt es die Möglichkeit, weitere Programme temporär zur Laufzeit nachzuladen. Die Paketverwaltung von Puppy öffnet das Anwendungsmenü über „Setup → Puppy Package Manager“. Void Pup (in 64 Bit und mit Uefi-Unterstützung auf Heft-DVD) schöpft aus dem Paketangebot von Puppy Linux, allerdings mit kleinerer Auswahl. Das System spricht ausschließlich Englisch. Nach dem Start kann man aber im Willkommen-Fenster deutsche Tastaturbelegung und die gewünschte Bildschirmauflösung auswählen. Ein einfacher Installer im Anwendungsmenü unter „Setup → Puppy installer“ kann das Livesystem auf einem USB-Stick einrichten.

Mehr Infos zu Void Pup
Website:
https://sourceforge.net/projects/vpup
Dokumentation:
https://puppylinux-woof-ce.github.io

Extra-DVD für USB-Sticks

Es gibt wieder eine weitere Multiboot-DVD, die nicht dem Heft beiliegt, sondern als Bittorrent-Download angeboten wird (4,7 GB). Diese Extra-Scheibe versammelt Spezialsysteme und Linux-Distributionen für Fortgeschrittene.



Bootmenü der Extra-DVD: Diese kann auch von einem USB-Stick booten. Die Downloadlinks für Bittorrent auf Github bieten neben der Extra-DVD auch die reguläre Heft-DVD.

VON DAVID WOLSKI

Das Bild zeigt das Bootmenü der Extra-DVD, ferner unsere Github-Seite mit den Downloadlinks für Bittorrent. Die reguläre Heft-DVD ist dort auch vertreten. Seit Anfang des Jahres 2022 präsentieren wir diese Extra-DVD, die sich nach einer Umwandlung zurück in ein ISO-Image auch auf einen USB-Stick übertragen lässt. Möglich macht dies der Bootloader 2.06, der für unsere Multibootumgebung sorgt. Nützlich ist dies nicht nur bei PCs ohne optisches Laufwerk, denn von USB starten und laufen die Systeme auch bedeutend schneller. Solche Übertragung auf USB klappt sowohl mit der regulären Heft-DVD als auch mit der Extra-DVD.

Die Systeme im Extra-Image

Der Umfang der Extra-DVD ist mit 4,7 GB zu groß, um das Image als Download per HTTP anzubieten. Besser geeignet ist das Protokoll Bittorrent, das die Netzwerklast auf mehrere unserer Server verteilt. Die Torrent-Datei und einen Magnet-Link mit einer unkorrumpierbaren Checksumme hat die LinuxWelt-Redaktion auf der Github-Seite *https://github.com/LinuxWelt/LinuxWelt/blob/main/torrents/LinuxWelt_2022-5-Tools* hinterlegt. Folgende Systeme sind im Image per Multibootmenü untergebracht:

Backbox 7: Sicherheitsexperten greifen für die Jagd nach Netzwerkproblemen zu einer besonderen Klasse von Livesystemen: Backbox 7 ist ein Werkzeugkasten mit Tools für Netzwerkchecks und zum Aufspüren von Sicherheitslücken im LAN und auf Servern. Zwar werden die enthaltenen Tools auch von der Hackerszene mitentwickelt, die Zielgruppe sind aber Administratoren und Sicherheitsexperten. Der Einsatz der Werkzeuge auf dem eigenen PC, Server und Netzwerk ist legitim und nützlich. Sie finden damit Sicherheitslücken, bevor es jemand anderes tut. In diesem Kontext sind diese „Dual-Use"-Programme, die Gutes bewirken oder auch Schaden anrichten können, auch in Deutschland noch legal.

4M Linux 40: Dieses Livesystem gibt es schon einige Jahre, hat aber erst seit wenigen Versionen Unstimmigkeiten im Aufbau und der Bedienung ausgebügelt. Als Grundlage dient Tinycore Linux, das hier um etliche Anwendungen erweitert ist, um ein universelles Livesystem im Stil von Knoppix bereitzustellen. 4M Linux ist allerdings komplett in Englisch. Beim Start gibt es aber in einem automatisch gestarteten Terminalfenster die Möglichkeit, auf das deutsche Tastaturlayout zu wechseln.

Clonezilla 3.0: Das Backuptool für ganze Festplatten oder einzelne Partitionen liegt in einer neuen Hauptversion vor. Es sichert Abbilder in Imagedateien, die es entweder lokal auf einer anderen Festplatte, auf einem USB-Medium oder per SSH und Samba auf einem Server speichert. Die Backupimages kann Clonezilla platzsparend gepackt speichern. Auch eine direkte Klonoption von einem Datenträger zum anderen ist enthalten. Neu ist die Unterstützung für APFS (Apple File System) und Luks-Partitionen.

Gparted Live 1.4.0: Der Partitionierer Gparted darf auf keiner bootbaren Toolsammlung fehlen und ist auch in anderen Livesystemen enthalten. Version 1.4.0 ist die offizielle und besonders frische Ausgabe der Gparted-Entwickler in einem kompakten unabhängigen System, das Gparted automatisch startet. Die neue Version des Partitionierers kann Dateisystemlabels von Linux-Dateisystemen ändern, erkennt Bcache-Partionen und aktualisiert den Linux-Kernel auf 5.16. ■

Gnome macht mobil

Eine richtungsgebende Idee hinter Gnome 3 ist der konvergente Desktop für PCs sowie Tablets und Smartphones. Bislang gelang Gnome der Sprung auf das Smartphone-Display noch nicht, aber das soll sich jetzt ändern. Dahinter steht der „Prototype Fund" als Initiative des Bundesministeriums für Bildung und Forschung. Die deutlichsten Neuerungen werden laut Gnome-Entwicklern Gesten zur Navigation auf der Oberfläche sein, eine bessere Bildschirmtastatur und eine Statusleiste für Smartphones. Zielplattform sind Linux-Smartphones wie das Librem 5 sowie künftige Geräte mit Linux statt Android. ■

Apple: Rosetta für Linux

Mit der Kompatibilitätsschicht Rosetta ist es auf Macs mit Apples ARM-Prozessor M1 möglich, x86-Anwendungen auszuführen. Die Technik steht ab Mac-OS 13 „Ventura" auch für virtuelle Linux-Maschinen bereit. Dazu stellt der Host dem Gastsystem die Laufzeitumgebung von Rosetta bereit. Wichtig ist dies auch für Linux-Container, die auf Apple-Computern laufen sollen. Rosetta könnte auch auf anderen ARM-Systemen jenseits von Mac-OS für Linux nützlich werden – dazu müsste Apple die Technik aber unter einer Open-Source-Lizenz freigeben. ■

AMD: Mehrere GPUs unter Linux

Der Linux-Kernel soll mit Version 5.20 einen neuen Treiber von AMD erhalten, der mehrere Grafikkarten in einem System besser verbindet. Dabei sollen die GPUs über den PCI-Express-Bus direkt zusammenarbeiten, ohne dabei Inhalte über den Hauptspeicher zu kopieren. Dies verspricht deutlich bessere Leistung beim Einsatz mehrerer GPUs für Fließkommaoperationen. Bislang kümmerten sich die Computerbibliotheken von AMD um die Zusammenarbeit mehrerer GPUs, was nun effizienter dem Linux-Kernel überlassen wird. Voraussetzung ist ein Chipsatz, der den gesamten Speicher der AMD-Radeon-Karten per PCI Express adressieren kann. ■

Alle News von David Wolski

Vorschau auf Linux-Kernel 5.19

Die kommende, für Anfang August geplante Kernel-Version lag zum Redaktionsschluss zwar erst als Release Candidate vor, macht die Neuerungen aber bereits absehbar.

Mit Genugtuung hat Linux Torvalds zum Kernel 5.19 verkündet, dass die Multiplattform-Unterstützung für ARM nach 12 Jahren Arbeit endlich fertig sei. Damit kann der Quellcode eines Kernel-Zweigs ohne weitere Modifikationen mehrere ARM-Plattformen und Systems-on-Chip (SoCs) bedienen, ein ambitioniertes Ziel, das ab Kernel 3.7 in Angriff genommen wurde. Den Start machen die älteren Plattformen ARMv4T und ARMv5, aber dies wird jetzt leichter ausbaufähig.
Insgesamt fallen rund 60 Prozent der Neuerungen Hardwaretreibern zu, wobei die Unterstützung von AMD-Grafikchips wieder den größten Teil ausmacht (mit ersten Patches für die Serie Radeon RX 7000). Auch Intel hat für seine gerade ausgelieferten Grafikchips Arc Alchemist viele neue Zeilen Treiber beigesteuert. Ebenfalls von Intel stammt ein Selbstcheck für die kommende CPU Generation „Saphire Rapids", um Schaltkreise in Prozessoren zu überprüfen und Fehler in Halbleitern zu entdecken. Bei den Arbeiten an Dateisystemen sind Verbesserungen für ExFAT und BTRFS bemerkenswert: BTRFS macht beständig Fortschritte und geht das Thema Raid 5/6 nochmals an, welches bisher auf Eis lag. ■

Nvidia: Treiber etwas offener

Der proprietäre Treiber für Nvidia-Grafikkarten wird ab Version 515 einem anderen Aufbau folgen: Das eigentliche Kernel-Modul wird nun endlich Open Source. Jedoch werden die eigentlichen Treiberfunktionen weiterhin als Firmwareblob geladen – Nvidia lässt sich also weiterhin nicht in die Karten schauen. Immerhin macht das neue Kernel-Modul die Paketierung sowie die Installation der proprietären Nvidia-Treiber viel einfacher. Zuerst wird der Treiber für die GPUs der Turing- und Ampere-Serie Nvidias erscheinen. Zusammen mit IBM/Red Hat und Canonical möchte Nvidia das freie Treibermodul in den Kernel-Quellcode bringen. In der Zwischenzeit soll aber auch der freie Linux-Treiber Nouveau für Nvidia-GPUs über die proprietäre Firmware Zugang zu fortgeschrittenen Fähigkeiten wie Reclocking und Temperaturkontrolle erhalten. ■

Kernel: NTFS wieder mit Unterstützung

Nachdem die Weiterentwicklung des Moduls für das NTFS-Dateisystem eingeschlafen war, haben Kernel-Entwickler Alarm geschlagen. Denn auch auf Anfragen an den ursprünglichen Programmierer hatte sich lange niemand gemeldet. Jetzt gibt es Entwarnung und das NTFS-Modul, welches Paragon Software beigesteuert hat, bekommt wieder aktive Entwicklung: In den Kernel 5.19 flossen bereits einige überfällige Fehlerbehebungen für diesen Dateisystemtreiber ein. ■

Linux auf Apple-Mobilgeräten

Nach über einem Jahr an Experimenten ist es Entwicklern gelungen, den Linux-Kernel auf dem iPad Air 2 und dann auch auf dem iPhone 5s zu booten. Es handelt sich dabei um die Apple-Geräte mit älteren A7- und A8/A8X-ARM-Prozessoren, welche schon lange kein Betriebssystemupdate mehr bekommen. Sollte um die jetzt vorgestellten Arbeiten eine Linux-Distribution entstehen, so wären diese Altgeräte also wieder sinnvoll nutzbar. Damit ein Linux-Kernel überhaupt bootet, ist ein trickreiches Vorgehen gefragt: Die Entwickler nutzen eine Sicherheitslücke namens „Checkra1n“, die den Bootloader der Apple-Geräte überlistet, um unsignierte Systeme zu laden. Für diesen ersten Ausbruch aus den eng gesteckten Grenzen Apples ist derzeit noch ein Rechner mit Mac-OS nötig, wie die Anleitung zeigt. ■

Android: Thunderbird und K-9 kooperieren

Während das Team hinter Thunderbird Version 102 des freien Mailclients veröffentlicht hat, ist die eigentliche Überraschung die Ankündigung einer Android-Ausgabe. Die Android-App werden die Thunderbird-Entwickler aber nicht im Alleingang stemmen, sondern kooperieren dazu mit den Machern von K-9 Mail – ein populärer Mailclient für Android. Die Idee der engen Zusammenarbeit gibt es seit 2018, aber jetzt erst wechselte der Hauptentwickler von K-9 zu Thunderbird. Die kommende App wird Open Source sein, den Namen „Thunderbird Mobile“ erhalten und die wichtigsten Funktionen beider Mailclients vereinen. ■

SICHERHEITSNEWS

Hertzbleed: Neue CPU-Schwachstellen
Aktuelle CPUs passen ihre Taktfrequenz dynamisch den Aufgaben an. Sicherheitsforschern ist es gelungen, durch die Beobachtung von Frequenzwechseln von Prozessoren auf einem System detaillierte Rückschlüsse auf kryptografische Operationen zu ziehen und sogar geheime Schlüssel zu rekonstruieren, die in einem anderen Prozess laufen. Spezielle Hardware ist dazu nicht nötig – es genügt, auf dem gleichen System die Frequenzen der CPU-Kerne zu protokollieren. AMD und Intel sind gleichermaßen betroffen. Bislang hilft nur, eine dynamische Taktanpassung über die Firmware eines Rechners zu deaktivieren. Die sechs Entdecker der Lücke, die an mehreren US-Universitäten forschen, arbeiteten schon seit letztem Jahr an praktischen Angriffen durch dynamisches Taktverhalten und haben ihre Erkenntnisse unter *www.hertzbleed.com* veröffentlicht.

Virtualbox: Host gibt Infos preis
Der Entwickler von Wireguard hat zufällig entdeckt, dass sich per Interrupts und SIMD-Datensätzen in einem Gastsystem in Oracle Virtualbox das Hostsystem ausspionieren lässt. SIMD steht für „Single Instruction, Multiple Data“ und ist eine Befehlserweiterung von x86-Prozessoren, um gleichzeitig mehrere gleichartige Datensätze zu verarbeiten. In einem veröffentlichten harmlosen Codebeispiel (*https://t.co/TlXKGy0Czn*) für Linux hält dazu ein Hardwareinterrupt für ein Touchpad her, um Daten in einem Gast vom Host abzugreifen. Betroffen ist nur Linux als Host. Zum Redaktionsschluss stand ein Patch noch aus.

Neue Studie: Sicherheit und Open Source
Generell hat Open-Source-Software in Sachen Sicherheit einen guten Ruf, der auch empirisch belegbar ist. Offenen Code kann jeder einsehen, daher werden Bugs und Sicherheitslücken schneller entdeckt. Aber dies trifft leider keineswegs auf alle Projekte zu – so etwa bei kaum noch gepflegten Bibliotheken, die dennoch weitergenutzt werden. Die Linux Foundation und die Beratungsfirma Snyk haben deshalb eine Langzeitstudie erstellt, um die Risiken mit realen Zahlen zu verdeutlichen. So hat sich die Zeit, die zwischen der Entdeckung einer Sicherheitslücke und deren Behebung vergeht, von 2018 bis 2021 von durchschnittlich 49 auf 110 Tage mehr als verdoppelt. Typische Open-Source-Entwicklungsprojekte haben 80 direkte Abhängigkeiten zu eingebundenen Bibliotheken oder Komponenten und weisen im Mittel 49 Schwachstellen auf.

BSI: Warnung vor Kaspersky
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt in deutlichen Worten vor den Programmen des russischen Antivirus-Spezialisten Kaspersky. Warnung vor Spionagetätigkeiten durch dessen Antivirenprogramme gibt es schon, seit israelische Behörden das russische Softwarehaus 2017 „in flagranti“ erwischten. Nun spart BSI-Präsident Arne Schönbohm nicht an drastischen Worten: Wer in kritischer IT-Infrastruktur noch Software von Kaspersky einsetze, handele fahrlässig. Die mutmaßlichen Spionagetätigkeiten durch die Antivirenprogramme seien eine „Gefahr für die nationale Sicherheit“.

Drupal: Webseiten gefährdet
Eine Schwachstelle in einer Komponente des Content-Management-Systems Drupal erlaubt schlimmstenfalls die Übernahme von Drupal-Websites. Verantwortlich ist die PHP-Bibliothek Guzzle (*https://docs.guzzlephp.org*) in Drupal, die vor allem von externen Modulen genutzt wird. Die Lücke wurde sofort als hoch eingestuft und von den rasch veröffentlichten Drupal-Versionen 9.2.21, 9.3.16 sowie 9.4.0 geschlossen. Dieser Fall ist ein weiteres Beispiel dafür, wie Lücken in verwendeten Bilbliotheken auch gut geführten Open-Source-Projekten gefährlich werden können.

UPDATETELEGRAMM

Manjaro 21.3.0
Die populäre Arch-Variante aktualisiert ihren Installer auf Calamares 3.2. Außerdem sind alle Desktops aufgefrischt, nämlich auf Gnome 42, KDE Plasma 5.24 und auf eine neue Zwischenversion von XFCE 4.16. Als Linux-Kernel dient Version 5.15. Wie Arch Linux ist Manjaro als Rolling Release konzipiert und deshalb eher ein Linux-System für Fortgeschrittene (*http://manjaro.org*).

Systemd 251
Das Init-System liegt in neuer Version vor: Es folgt in seinem Quellcode dem C-Standard C11 des Linux-Kernels und hebt die Mindest-Kernel-Version auf 4.15 an. Lennart Pöttering verweist in einem langen Blog-Eintrag zum neuen Systemd auf die Komponente „Systemd-Sysupdate“, das von Linux-Distributionen für ein Systemupdate genutzt werden kann. Dieser Weg der Aktualisierung ist jenem von Smartphones nachempfunden, bei welchen ein unverändertes Systemabbild auf einer Partition erhalten bleibt. Interessant ist der Updatemechanismus für Immutable-Distributionen mit unveränderlichem Basissystem, also beispielsweise für Steam-OS 3.0 oder Fedora Silverblue.

Armbian 22.05
Neues Leben für alte Ein-Platinen-Computer: Armbian ist eine Linux-Distribution für ARM-Boards (Banana Pi, Cubietruck und weitere), welche unabhängig vom Hersteller regelmäßig neue Versionen mit Fehlerbehebungen und aktuellen Paketen liefert. Die aktuelle Ausgabe holt weitere Boards ins Boot, etwa den Radxa Rock 3A, Orange Pi R1 und den Odroid N2 (*www.armbian.com*).

Putty 0.77
Für Windows-Anwender ist der SSH-Client Putty weiterhin eine komfortable Alternative zum Windows-eigenen SSH-Programm im Terminal. Putty 0.77 (auf Heft-DVD) kann nun mit SSH-Proxyserver umgehen. Es kommt auch mit Tunnelverbindungen klar, die über einen anderen SSH-Server geleitet werden, um beispielsweise ein anderes System in einem Netzwerk über ein Gateway zu erreichen (*www.putty.org*).

Nix-OS: Neuer grafischer Installer

Die Linux-Distribution Nix-OS erhielt zuletzt viel Aufmerksamkeit, denn der programmierbare Paketmanager und die Konfiguration im Stil von Ansible sind ideal für Container und Cloudinstanzen. Nix-OS erlaubt mit seinem Aufbau einen hohen Grad an Automatisierung beim Aufsetzen neuer Systeme. Der Einstieg ist allerdings nicht einfach und die Dokumentation war bislang kaum für Einsteiger geeignet. Das aktuelle Nix-OS 2.8 senkt jetzt mit seinem neuen grafischen Installer die Einstiegshürden und will sich eine neue Anwenderschaft erschließen (*https://nixos.org*).

Supercomputer: AMD liegt vorne

Quelle: Oak Ridge National Laboratory

Auf der Liste der weltweit 500 schnellsten Supercomputer (*https://top500.org*) hat der AMD-Cluster Frontier den ARM-basierten Supercomputer Fugaku vom ersten Platz verdrängt. Dabei durchbricht Frontier (Tennessee, USA) auch zum ersten Mal die Exaflop-Grenze. Mit einem Wirkungsgrad von 62,68 Gigaflops pro Watt Leistungsaufnahme ist der Supercomputer auch in dieser Disziplin auf dem ersten Platz. Frontier nutzt AMD-EPYC-Prozessoren der Serie Milan in Kombination mit AMD-GPUs vom Typ Instinct MI250x für Fließkommaoperationen. Ein angepasstes Linux-System erlaubt die besonders effiziente Zusammenarbeit dieser beiden Prozessortypen. CPUs von AMD stecken nun in der Hälfte der zehn schnellsten Supercomputer, wobei Frontier noch in der Testphase ist.

Open Suse: Neuaufbau im Herbst

Open-Suse-Entwickler möchten diese Linux-Distribution wieder neu positionieren und neue Trends definieren. Ein Trend, dem bereits Ubuntu Core, Fedora Silverblue und Steam-OS 3.0 folgen, ist der Ansatz einer separat aktualisierten Betriebssystembasis, zu welcher Konfiguration und Programme nur modulare Ergänzungen sind. Der Betriebssystemkern bleibt davon unverändert. Das Konzept nennt sich „Immutable System“ und belässt ein von Anwendern unveränderliches Systemimage auf einer eigenen Partition. Damit ist Konsistenz gegeben, während Anwendungen im Stil von Apps als App-Container oder auch als Container-Server-Instanzen (Micro-Services) hinzuinstalliert werden. „Adaptable Linux Platform“ (ALP) nennt Open Suse diesen Ansatz, der die weitere Zukunft der Distribution weisen könnte.

Kernel: Rust rückt näher

Auf dem jährlich abgehaltenen Open-Source-Summit im Juni 2022, einer Konferenz der Linux Foundation mit tonangebenden Linux-Entwicklern, hat Linus Torvalds eine Einschätzung gegeben, wann Rust im Linux-Kernel bisherigen C-Code ersetzen könnte. Laut Torvalds sind die ersten in Rust neu programmierten Teile schon für den Kernel 5.20 oder 5.21 bereit. Rust hat den Vorteil eines abgesicherten Speichermanagements, das Bugs mit Pufferüberlauf signifikant reduziert. Die Initiative, Rust in den Linux-Kernel zu bringen, stammt ursprünglich von Google, wobei hinter Rust als Programmiersprache die Mozilla Foundation steht.

Copilot: Microsoft hilft programmieren

Der Dienst Github Copilot von Microsoft ist fertig. Das Plug-in für Visual Studio, Jetbrains und den Editor Neovim schlägt Programmierern per künstlicher Intelligenz ganze Codeblöcke vor. Nach der Testphase ist der Copilot jetzt zu einem Preis von zehn US-Dollar im Monat verfügbar. Für Schüler, Studenten und Entwickler von anerkannten Open-Source-Projekten ist der Dienst kostenlos buchbar (*https://github.com/pricing#faq-copilot*). Microsoft griff bei der Entwicklung, Analyse von Quellcode und Mustererkennung auf Open-Source-Projekte bei Github zurück. Die Open-Source-Szene befürchtet deshalb, dass freier Code ohne klare Lizenzierung zunehmend über Copilot in proprietäre Software gerät. ■

Flutter 3: Toolkit für alle

Das plattformübergreifende Toolkit Flutter, das die Anwendungsentwicklung unter Linux, Windows und Mac-OS abdeckt, wurde von Google in Version 3 veröffentlicht. Flutter ist Open Source und für die Erstellung grafischer Programme optimiert. Es basiert auf Googles eigener Programmiersprache Dart und der Grafikbibliothek Skia. Beteiligt an Entwicklung und Portierung auf Linux ist auch Canonical, denn die Firma will für Ubuntu ausgiebig von Flutter Gebrauch machen, um wieder mehr Desktopprogramme sowie einen neuen Installer auszuliefern. Eine Vorschauversion des kommenden Installers veröffentlicht Canonical bereits unter *https://github.com/canonical/ubuntu-desktop-installer* und auf alternativen ISO-Images von Ubuntu 22.04. ■

Docker Desktop für Linux

Eine grafische Oberfläche zur einfacheren Einrichtung von Containern für Serverdienste und Anwendungen in einer isolierten Umgebung ist jetzt mit Docker Desktop auch für Linux verfügbar. Für Windows und Mac-OS gab es dieses Programm, das sich an Einsteiger wendet, schon einige Jahre. Enthalten sind Docker Compose, Buildkit, ein Schwachstellenscanner, der nach veralteten Komponenten sucht, sowie eine Anbindung für Kubernetes. Pakete im Format DEB und RPM für die verbreiteten Linux-Distributionen stehen unter *https://docs.docker.com/desktop/linux/install* zum Download bereit. Docker Desktop steht unter einer kommerziellen Lizenz, ist aber für privaten Gebrauch und für Unternehmen bis 250 Mitarbeiter kostenlos. ■

Facebook/Meta: NVME als Arbeitsspeicher

In Rechenzentren wie jenen von Meta (früher Facebook) ist Arbeitsspeicher ein knappes Gut und DRAM für die Arbeitslasten laut der Technikleitung zu teuer geworden. Günstiger ist Flashspeicher auf NVMEs, der aber im Vergleich zu RAM deutlich langsamer ist (etwa um den Faktor 30 bis 50). Dennoch haben die Entwickler daran gearbeitet, weniger häufig benötigte Speicherbereiche auf NVMEs auszulagern – nicht etwa in den regulären Swapbereich, sondern in einen schnelleren Zwischenspeicher. Diese Ergänzung des Linux-Kernels, die noch nicht als offizieller Patch eingereicht wurde, nennt sich Transparent Memory Offloading (TMO) und ist bei Meta schon seit einem Jahr in Gebrauch – auf rund fünf Millionen Linux-Servern. TMO ist für bestimmte Prozesse wie Datenbanken maßgeschneidert. Eine Übernahme in den Linux-Kernel erfordert noch Arbeit, um generelle Anwendungsbereiche abdecken zu können. ■

UPDATETELEGRAMM

KDE Plasma 5.25
Weniger als ein halbes Jahr nach der letzten Version erschien das neue KDE Plasma 5.25. Die Version behebt 400 Einzelfehler, versteht zusätzliche Gesten auf Touchscreens, passt Akzentfarben von Anwendungen automatisch ans Hintergrundbild an und liefert viele Verbesserungen unter Wayland. KDE Plasma 5.25 wird im kommenden KDE Neon ausgeliefert und ist unter Arch Linux sowie Manjaro bereits jetzt verfügbar (*https://kde.org/plasma-desktop*).

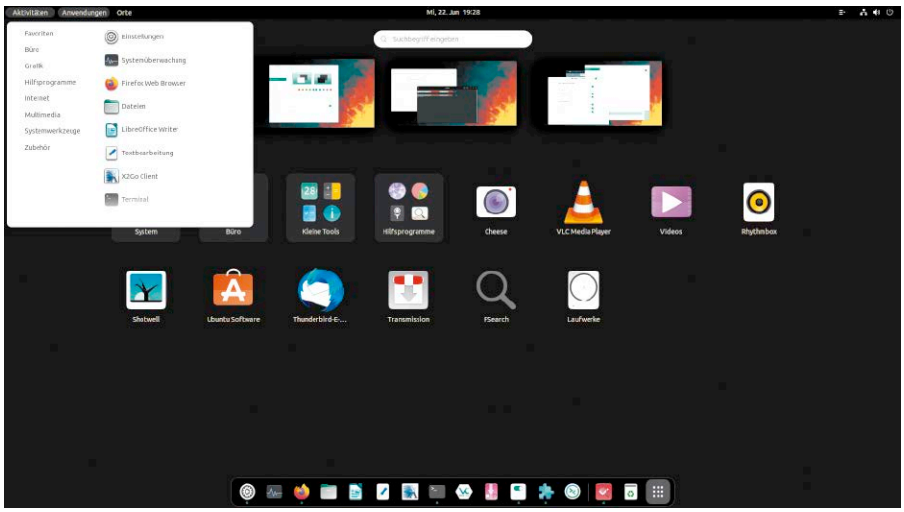
Free CAD 0.20
Freie CAD-Programme unter einer Open-Source-Lizenz sind rar und eine erfreuliche Ausnahme ist Free CAD, welches ein hohes Entwicklungstempo vorlegt. Die 3D-CAD-Software im Stil von Autocad ist für technische Konstruktionen und Architektur geschaffen. Das Programm kann aus Objekten auch 2D-Pläne erstellen und hat einen neuen Arbeitsbereich für technische Zeichnungen (*www.freecadweb.org*).

Digikam 7.7
Die Fotoverwaltung für Fortgeschrittene macht zusehends auch jenseits von KDE einen starken Eindruck, dank einem universellen Appimage, das jetzt auch die volle internationale Sprachunterstützung enthält. Neu ist die Unterstützung für das neue Bildformat JPG-XL, das sich wachsender Beliebtheit erfreut. Wie immer wurden weitere herstellerspezifische RAW-Formate hinzugefügt, etwa für die Olympus OM-1 (*www.freecadweb.org*).

Gnome 42.2
Eine Zwischenversion mit Fehlerbehebungen feilt weiter an den Kanten von Gnome 42.2: Der grafische Paketmanager „Gnome-Software“ arbeitet nun besser mit Flatpak-Apps zusammen und stellt komplexe Berechtigungen übersichtlich dar. Die „Einstellungen“ haben ein Untermenü für Snap-Apps in Ubuntu bekommen, um auch deren Berechtigungen nachträglich bearbeiten zu können. Gnome 42.2 wird im kommenden Ubuntu 22.10 (Oktober) enthalten sein (*www.gnome.org*).

Ubuntu 22.04 optimieren

Die letzte LinuxWelt hat das neue Ubuntu 22.04 inklusive aller offiziellen Varianten vorgestellt. Dieser Artikel fokussiert sich auf Optimierungsoptionen in Canonicals Hauptedition mit dem Gnome-Desktop.



VON HERMANN APFELBÖCK

Obwohl sich an Gnome und etlichen Sonderlichkeiten von Ubuntu 22.04 die Geister scheiden, ist Canonicals Hauptedition ohne Zweifel ein elegantes und schnelles System. Dieser Artikel geht von einem installierten und prinzipiell eingerichteten Ubuntu aus (Aktualisierung, Spiegelserver, Sprache, Anzeige, Netzwerk, Energieeinstellungen). Wir machen einen Rundgang, rüsten nach, was fehlt, und optimieren die Oberfläche. Denn es bleibt unverständlich, warum manches unentbehrliche Zubehör nicht mitgeliefert wird, das die Akzeptanz der Ubuntu-Hauptedition entscheidend fördern könnte.

1. Vorab: Empfohlene Ergänzungen

Die folgenden kleinen Helfer sind klassisch über *apt install [Name]* aus den Paketquellen zu beziehen. Die zuerst genannten Tools dürfen als unentbehrlich gelten, danach folgen optionale, aber empfehlenswerte Ergänzungen:

libfuse2 ist eine unscheinbare Bibliothek, die unter Ubuntu 22.04 schlicht vergessen wurde. Sie ist notwendig, um Software im Appimage-Format starten zu können.

gnome-tweaks erscheint auf deutschem System als „Optimierungen". Die Bedeutung des Tools ist gesunken, seit es keine Gnome-Erweiterungen mehr verwaltet. Die Angebote unter „Fenster" und „Schriften" sind aber weiterhin unentbehrlich.

gnome-shell-extension-manager ist auf deutschem Ubuntu als „Erweiterungs Manager" anzutreffen. Er ist alternativlos, um Gnome-Erweiterungen zu beziehen, zu (de-)aktivieren und zu konfigurieren, nachdem die frühere Möglichkeit über Firefox neuerdings ausfällt.

dconf-editor ist eine grafische Hilfe, um die Einstellungen von Gnome- und Gnome-Software zu steuern. Wer das standardmäßige gnome-control-center („Einstellungen") sowie das Tool gnome-tweaks genau analysiert, wird feststellen, dass dort die allermeisten relevanten Optionen bequemer zugänglich sind. Dennoch bleiben Ausnahmen, und hier kann der „dconf-Editor" aushelfen.

nautilus-admin ist eine winzige, aber nützliche Erweiterung für den Dateimanager, um per einfacher Kontextoption root-Zugriff zu erhalten.

p7zip-full, also der Packer 7-Zip, ist nicht nur für den Austausch von Packerarchiven sinnvoll, sondern vor allem wegen seiner Verschlüsselungsoption attraktiv. Dazu folgt ein Komfort-Tipp an späterer Stelle (Punkt 8).

Optionale Ergänzungen sind **preload** (Programmbeschleuniger), **plocate** (Suchindexer für das Terminal) und der **classicmenu-indicator**, der ein sehr einfaches klassisches Menü in der Systemleiste anbietet.

Dies alles sind kleine klassische Pakete. Gnome-Erweiterungen sind auf andere Weise zu beziehen, wie im späteren Punkt 6 (Gnome-Shell-Extension-Manager) näher erläutert wird.

2. Die Bedienungsgrundlagen

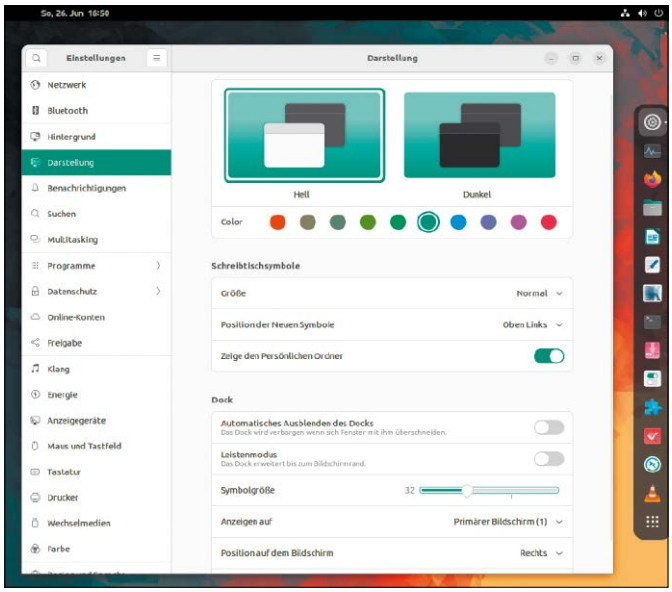
Als Umschalter und Programmstarter dient die Übersichtsseite „Aktivitäten", die über die Windows-Taste (Super) oder durch Klick auf „Aktivitäten" in der Systemleiste erreichbar ist.

Das Resultat ist multifunktional, denn es erscheint ganz oben das Suchfeld zur Programmsuche, darunter eine Übersicht der virtuellen Desktops und in der Bildschirmmitte eine Taskübersicht aller Fenster des aktuellen Desktops.

Der Hotkey Super-A startet eine alternative Gesamtübersicht, ebenfalls mit Suchfeld und Desktops, aber hier mit der Gesamtübersicht aller Programme (quasi das Startmenü von Gnome). Aufräumen dieser Übersicht durch Zusammenfassen passender Programme ist per Drag & Drop elegant zu erledigen. Die entstehenden Sammelordner lassen sich sprechend benennen.
Trotz der „Aktivitäten" gibt es Alternativen, die sich nicht von anderen Desktops unterscheiden: Hotkey Alt-Tab wechselt zwischen Programmen, Hotkey Strg-Alt-Rechts/Links wechselt zum nächsten virtuellen Desktop. Anders als originales Gnome liefert Ubuntu standardmäßig das Favoritendock mit. Dort enthaltene Starter können Sie nach Rechtsklick mit der Option „Aus Favoriten entfernen" beseitigen. Umgekehrt fügen Sie neue Programme am einfachsten über die Anwendungsübersicht hinzu (Super-A), indem Sie dort ein Programm nach Rechtsklick im Dock anheften („Zu Favoriten hinzufügen").

3. Das Gnome-Control-Center

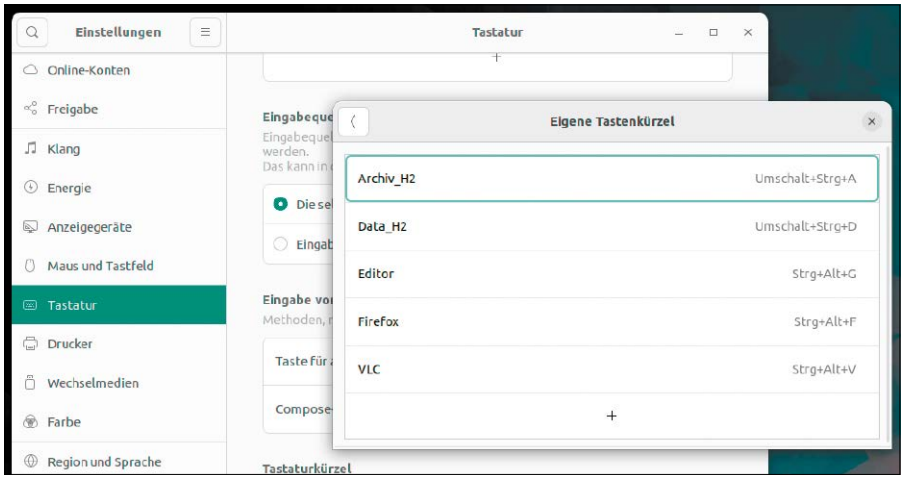
Die zentralen „Einstellungen" sind etwas chaotisch, aber ergiebig.
Die **wesentliche Optik** bestimmen die Punkte „Hintergrund" und „Darstellung". Letztere bietet neuerdings einen dunklen Modus sowie Akzentfarben, die sich auf Icons, Markierungen und Menüs auswirken. Das Favoritendock kann hinsichtlich Symbolgröße und Position (rechts, links …) angepasst werden.
Virtuelle Desktops: Eine oft unterschätzte Kategorie ist „Multitasking". Dass man mit der linken oberen Bildschirmecke die Aktivitäten-Ansicht auslösen kann („Funktionale Ecke"), ist eher marginal. Der Punkt „Arbeitsflächen" ist hingegen produktiv: Wer statt den dynamischen Desktops eine feste Anzahl bevorzugt (nach unserer Ansicht genügen zwei bis vier), kann das hier einstellen. Für den Desktopwechsel sind standardmäßig die Hotkeys Strg-Alt-Rechts/Links vorgesehen, nimmt man die Umschalt-Taste hinzu, wird das aktive Fenster mit transportiert.
Interessant für den Multimonitorbetrieb ist die zusätzliche Option, virtuelle Desktops nur auf dem primären Bildschirm zu wechseln: Damit erhält man sich auf dem zweiten Bildschirm ein konstantes Bild (Programm), während der Hauptbildschirm die Desktops wechseln kann.
Tastenkombinationen: Unter „Einstellungen → Tastatur → Tastaturkürzel" werden Sie viele aktivierte Standard-Hotkeys antreffen, die Sie nie nutzen. Hotkeys, die Sie definitiv nicht brauchen, können Sie abschalten. Um einen Standard-Hotkey zu deaktivieren, gehen Sie auf die Eingabetaste und nutzen im Folgedialog „Tastenkombination festlegen" die Rücktaste. Die Aktion ist dann noch mit „Festlegen" zu bestätigen. Auf die beschriebene Weise können Sie auch jeden Standard-Hotkey neu belegen, indem Sie statt der Rücktaste die gewünschte neue Tastenkombination drücken. An unterster Stelle des Fensters „Tastaturkürzel" finden Sie die Rubrik „Eigene Tastaturkürzel". Sie eröffnet die Möglichkeit, Programmen oder Dateiobjekten einen individuellen Hotkey zuzuweisen (die Rubrik „Starter" zeigt nur eine kleine Anzahl von Programmprominenz wie Terminal, „Einstellungen" oder Standardbrowser). Unter „Eigene Tastaturkürzel" ist jedes beliebige Programm erreichbar. Sie wählen „Tastenkombination hinzufügen", geben einen „Namen" ein (unwichtig) sowie den „Befehl" (wichtig). Der Befehl kann schlicht „vlc" lauten, aber auch komplexer „nautilus smb://192.168.178.8/archiv". Mit „Tastenkombination festlegen" drücken Sie dann den Hotkey Ihrer Wahl.



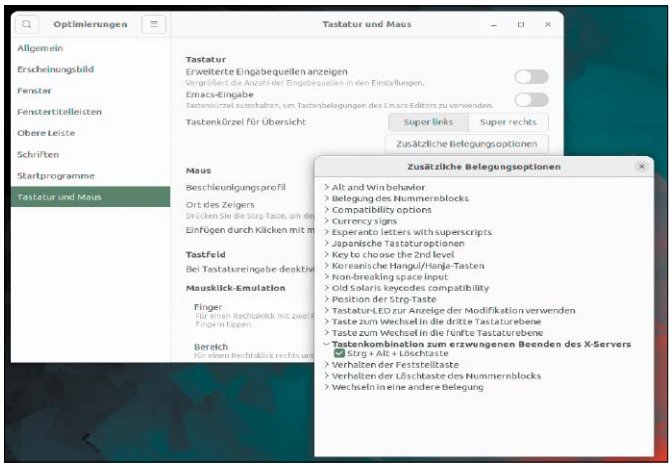
Der Dialog „Darstellung" im Gnome-Control-Center: Hier ist viel Optik komprimiert – Dunkel-Hell-Thema, Akzentfarben, Dockgröße, Dockposition und Schreibtischsymbole.

4. Die „Optimierungen" (gnome-tweaks)

Der Funktionsumfang von gnome-tweaks („Optimierungen") ist nicht groß, aber relevant:
Der Punkt „Schriften" erlaubt eine stufenlose exakte Schriftenskalierung. Die standardmäßigen „Einstellungen" bieten unter



Hotkeys anpassen und erstellen: Einfache Tastaturstarter sind unter „ Einstellungen –› Tastatur –› Tastaturkürzel" schnell erstellt und sorgen für Schnellstarts ohne Pixelsuche.



Gnome-Tweaks („Optimierungen“): Das Tool ist allein schon wegen der Schriftenskalierung eine Empfehlung. Die Optionen zur Tastenbelegung sind in einem Untermenü versteckt.

„Barrierefreiheit“ dagegen nur die, nicht genauer skalierbare Option „Große Schrift“.

Der Punkt „Fenster“ kann modale Unterdialoge vom Hauptfenster abkoppeln. Außerdem gibt es hier die Option, den „Fensterfokus“ bereits beim „Überfahren“ mit der Maus zu ändern (also ohne Klick). Ein oft nicht geläufiges Feature: Fenster lassen sich nicht nur mit der Titelleiste, sondern an jeder Position verschieben, wenn man die Super-Taste drückt. Diese „Fenster-Aktionstaste“ können Sie hier abschalten oder auf Alt-Taste verlegen.

Der Punkt „Erscheinungsbild“ kann die Fensteroptik, Titelleisten und Icons wesentlich verändern. Ergiebig ist das aber nur, wenn die schmale Auswahl der vorinstallierten Themes und Iconsets durch Gnome-Themen aus dem Web erweitert wird.

Unter **„Tastatur und Maus“** finden Sie Angebote, Tasten stillzulegen, neu zu belegen oder zu vertauschen. Die interessantesten Optionen verstecken sich im Unterpunkt „Zusätzliche Belegungsoptionen“. So ist etwa die „Tastenkombination zum erzwungenen Beenden des X-Servers“ inaktiv und kann hier scharf geschaltet werden. Allerdings ist „Strg+Alt+Löschtaste“ nicht etwa Strg-Alt-Entf, sondern Strg-Alt-Rücktaste.

5. Der Dconf-Editor

Was immer in den generellen „Einstellungen“, in den „Optimierungen“ oder in Programmeinstellungen zu finden ist, ist dort bequemer zu nutzen. Der relativ unübersichtliche Dconf-Editor hilft aus, wo die Reichweite der anderen Werkzeuge endet. Ein Beispiel ist etwa die Einstellung im Dateimanager Nautilus, statt des „Krümel“-Pfades immer den editierbaren Pfad in der Adresszeile anzuzeigen. Die findet sich beim Dconf-Editor unter „org → gnome → nautilus → preferences → always-use-location-entry“.

Ein zweites Beispiel: Beim Abmelden über das Sitzungsmenü erscheint noch einmal ein Rückfrage. Die lässt sich unter „org → gnome → gnome-session → logout-prompt“ deaktivieren. Noch ein Beispiel? Der klassische Taskwechsel mit Alt-Tab berücksichtigt standardmäßig nur die Fenster des aktuellen, virtuellen Desktops. Der Schalter unter „org → gnome → shell → window-switcher“ stellt dies um, sodass alle Programme aller Desktops erreichbar sind.

6. Der Gnome-Shell-Extension-Manager

Dieses Tool ist für Ubuntu-Nutzer mehr oder weniger Pflicht. Damit lassen sich die installierten Gnome-Erweiterungen („Installed“) ein- und ausschalten, komplexere über das Zahnradsymbol genauer konfigurieren. Ferner kann das Register „Browse“ weitere Gnome-Extensions nachinstallieren.

Das Tool erscheint als „Erweiterungs Manager“ in der Gnome-Übersicht. Bei der Websuche nach neuen Erweiterungen mit „Browse“ nutzen Sie am besten parallel einen Browser und die Adresse *https://extensions.gnome.org*. Hier ist nämlich Blättern und Stöbern möglich, während das lokale Tool nur einen kleinen Ausschnitt anzeigt. Interessante Erweiterungen können dann aber mit dem Tool im „Browse“-Fenster gesucht werden, wonach kompatible Extensions die Schaltfläche „Installieren“ anbieten. Installiertes landet in der Übersicht „Installed“ und kann dort aktiviert, deaktiviert und konfiguriert werden.

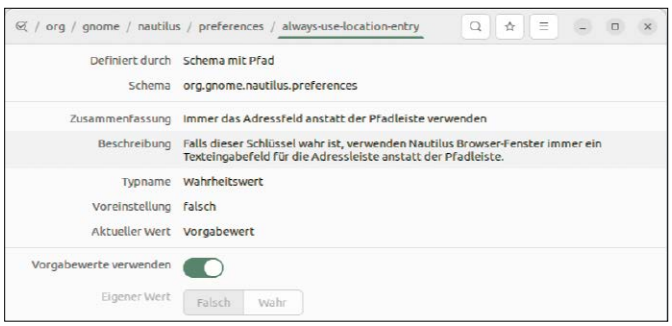
Eine Übersicht über die zahlreichen Extensionen ist hier nicht möglich, allenfalls die eine oder andere Empfehlung: **„Applications Menu“** bietet ein klassisches Kategorienmenü in der Systemleiste – das Menü ist schlicht, aber hübscher als der spartanische Classicmenu-Indicator.

„Places Status Indicator“ erscheint in der Systemleiste als „Orte“ und repräsentiert genau das, was der Nautilus-Dateimanager in der Navigationsleiste anbietet – die Standardverzeichnisse und die Lesezeichen.

„Floating Dock“ ist ein verspieltes, frei platzierbares Dock auf dem Desktop. Es zeigt sich nach der Installation als Icon mit drei weißen Punkten. Ein Klick blendet die Dock-Favoriten ein – standardmäßig identisch mit jenen, die das Ubuntu-Standarddock präsentiert. Mit anderen Worten: „Floating Dock“ ist als platzsparender, beweglicherer Ersatz für das Ubuntu-Dock gedacht, das man daher deaktivieren sollte. Das Dock bietet neben den Favoriten nach Rechtsklick auch noch Beenden-Optionen.

7. Icons auf dem Desktop

Gnome verbietet eigentlich Icons auf dem Desktop. Bei Ubuntu sorgt die vorinstallierte Gnome-Erweiterung „Desktop Icons NG“ (DING) für einige Desktopsymbole und Datenablage am Desktop. Das Wesentliche erreicht man über Rechtsklick am Desktop und „Arbeitsfläche-Einstellungen“ oder – identisch– mit dem Gang in die „Einstellungen“ und „Darstellung → Schreibtischsymbole“. Beides bleibt aber marginal – eine detaillierte Auswahl der Desktopsymbole bietet nur der Gnome-Shell-Extension-



Dconf-Editor: Die meisten Dconf-Einstellungen sind über reguläre Einstellungsmenüs erreichbar. Der Dconf-Editor geht aber, wie hier bei Nautilus, über offizielle Optionen hinaus.

Manager (Punkt 6). In der Zahnrad-Konfiguration der „Desktop Icons NG“ können Home-Ordner, Papierkorb, externe Laufwerke und Netzwerklaufwerke am Desktop aktiviert werden. Außerdem gibt es Positions- und Größeneinstellungen.

Eigene Desktopverknüpfungen? So wirklich dringend sind diese nicht, wenn das Dock für Programmfavoriten sorgt und die Erweiterung „Desktop Icons NG“ für wichtige Orte. Nichtsdestotrotz: Programmstarter erreichen Sie ganz einfach so (Beispiel):

```
cp /usr/share/applications/vlc.
  desktop ~/Schreibtisch/
```

Der so kopierte VLC-Starter muss dann am Desktop per Rechtsklick und „Start erlauben“ noch genehmigt werden. Desktopverknüpfungen zu Ordnern erstellen Sie hingegen am einfachsten per Softlink:

```
ln -s ~/Downloads/ ~/Schreibtisch/
```

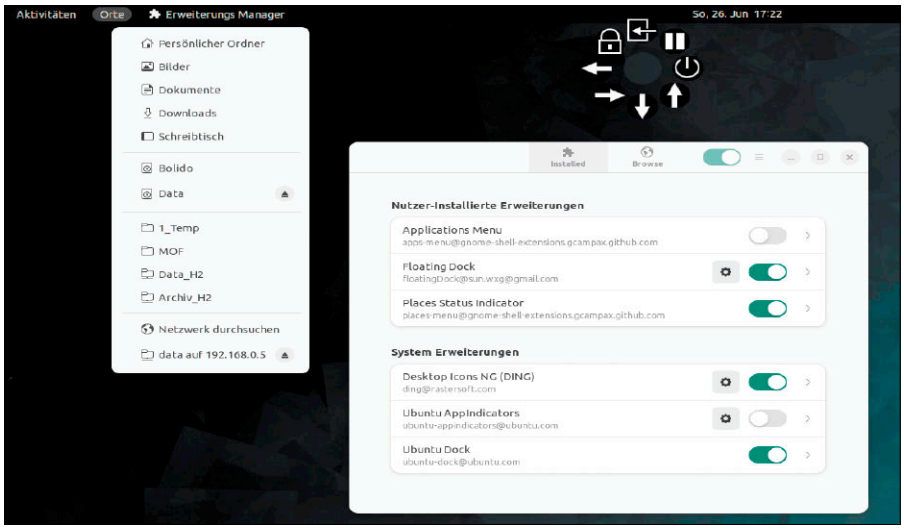
Das Ziel der Verknüpfung (hier „~/downloads“) muss dauerhaft verfügbar sein. Nicht gemountete Laufwerke oder Netzpfade führen zu Fehlern. Der Softlink ist also nicht geeignet, einen Automount auszulösen.

8. Nautilus-Erweiterungen

Der Dateimanager präsentiert sehr karge „Einstellungen“. Stets zu empfehlen ist die Option „Dauerhaft löschen“, die einen gleichnamigen Kontexteintrag aktiviert, um Dateiobjekte sofort zu löschen (ohne Papierkorb). Weitere Optionen sind zuschaltbar oder abstellbar, aber nur mit der Kenntnis der betreffenden Nautilus-Erweiterungen: So basieren etwa die Freigabeoption oder der Terminalstart im Nautilus-Kontext auf den Erweiterungen **nautilus-share** und **nautilus-extension-gnome-terminal**. Wer sie nicht braucht, kann sie per *sudo apt purge […]* vom System entfernen. Eine fehlende Erweiterung, die wir andererseits für wichtig erachten, nennt sich „nautilus-admin“. Ist diese installiert, zeigt der Dateimanager das zusätzliche Kontextmenü „Als Systemverwalter öffnen“. Geänderte Erweiterungen gelten immer erst nach der nächsten Anmeldung und eine Übersicht über alle Nautilus-Erweiterungen erhalten Sie so:

```
apt-cache search nautilus*
```

Noch individueller wird Nautilus durch selbst gebaute Erweiterungen. Da Ubuntu 22.04 das Tool nautilus-actions zum Ausbau des Nautilus-Menüs aktuell nicht mehr unterstützt, lassen wir diese Möglichkeit außen vor. Es gibt aber noch eine Option:



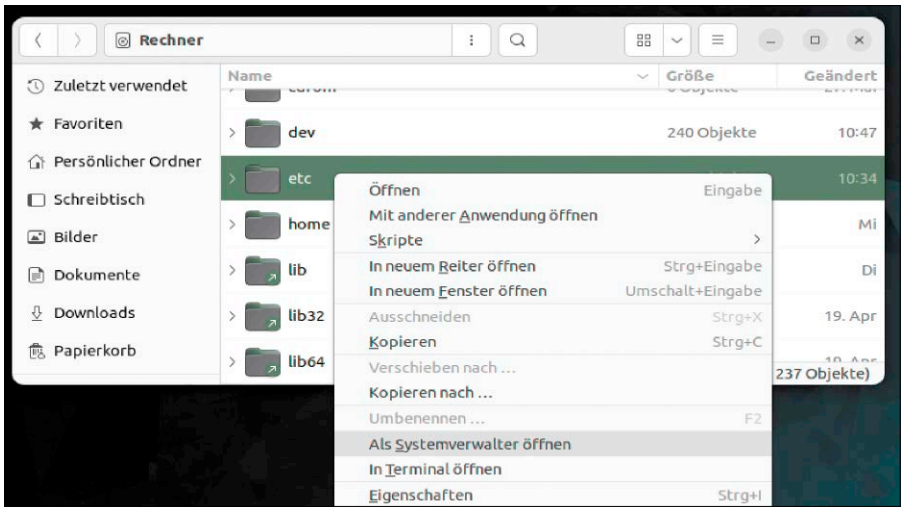
Gnome-Shell-Extension-Manager: Wer die Ubuntu-Oberfläche aufpeppen oder zähmen will, kommt an diesem Tool nicht vorbei (hier mit „Floating Dock“ und „ Places Status Indicator“).

Nautilus stellt unter „~/.local/share/nautilus/scripts“ ein spezielles Verzeichnis bereit: Hier enthaltene Shells-Scripts erscheinen im Kontextmenü unter „Skripte“, wenn mindestens ein Script vorliegt. Darunter zeigen sich die Scripts mit ihren Dateinamen (Endung „.sh“ ist nicht erforderlich). Ein nützliches Beispiel ist ein Script namens „Ver- und Entschlüsseln“ für schnelle Verschlüsselung von Ordnern und Dateien mit 7-Zip:

```
echo "$1" | grep ".7zEnc"
if [ $? -eq 0 ]
 then
 7z x -p"Das.G3heime.PASSW0RT" $1
 else
 7z a -p"Das.G3heime.PASSW0RT" -t7z
 -mhe=on $1.7zEnc $1
fi
```

Der entscheidende Vorteil gegenüber einer manuellen Nutzung mit dem Archivmanager dürfte klar sein: Das Passwort steht fest, wird beim Ein- und Auspacken per Script übergeben und muss nicht eingegeben werden. Da das Kennwort offen im Dateisystem liegt, eignet sich die Methode zwar nicht zum lokalen Datenschutz, aber sehr gut zum Versand von Daten in die Cloud.

Noch ein Hinweis: Verwenden Sie solche Scripts nur im Dateimanager, nicht am Desktop. Das Verhalten am Desktop ist – wie oft unter Gnome – nicht konsistent. In unserem Beispiel funktioniert das Verschlüsseln, aber nicht das Auspacken. Im Dateimanager unter „Schreibtisch“ gibt es kein Problem. ■



Nautilus-Erweiterungen: Viele Kontextoptionen basieren auf externen Tools, so auch der Wechsel zum root-Recht über die Erweiterung „nautilus-admin“.

Multiboot mit ISO-Dateien

Linux-Distributionen und Rettungssysteme lassen sich von einem USB-Stick booten, auf dem sich aber immer nur ein System unterbringen lässt. Wir stellen Tools vor, die den Start mehrerer Systeme von einem USB-Laufwerk ermöglichen.

VON THORSTEN EGGELING

Linux-Distributionen werden in der Regel als ISO-Dateien für CDs und DVDs ausgeliefert. Die Dateien sind aber so konstruiert, dass sich damit auch ein bootfähiger USB-Stick für die Linux-Installationen erstellen lässt. Allerdings kann man immer nur ein einzelnes System vom USB-Stick starten, da die Bootumgebungen der verbreiteten Linux-Distributionen weitestgehend identisch sind. Kopiert man ein zweites Installationssystem auf den Stick, werden die Dateien des vorherigen Systems überschrieben.

Wer mehrere Linux-Distributionen und vielleicht Windows vom USB-Stick installieren möchte, kann die ISO-Dateien auch direkt booten. Wir stellen Tools vor, die das ermöglichen. Das ist auch für Rettungs- und Reparatursysteme nützlich, die sich ebenfalls auf einem USB-Stick unterbringen lassen. Die Anzahl ist nur durch die Kapazität des Laufwerks begrenzt. Die Methode ist keinesfalls nur auf USB-Sticks anwendbar. ISO-Dateien lassen sich genauso gut von einer USB-Festplatte oder dem eingebauten SATA-Laufwerk booten.

Bootstick erstellen: Das Tool „Startmedienersteller“ belegt den USB-Stick komplett mit allen Partitionen aus der ISO-Datei. Das ist unpraktisch, wenn man unterschiedliche Systeme starten möchte.

Wie ein Linux-Livesystem bootet

Die ISO-Dateien vieler Linux-Installationsmedien enthalten zwei Bootmanager. Isolinux (*https://wiki.syslinux.org*) ist für den Start auf älteren PCs mit herkömmlichem Bios (Basic Input Output System) oder auf neueren Uefi-Geräten mit aktiviertem CSM (Compatibility Support Module) zuständig. Neben einem ISO-9660-Dateisystem enthält das ISO zusätzlich die Eltorito-Erweiterung, mit der eine CD/DVD erst bootfähig wird. Eltorito kann ein Festplatten- oder Floppy-Abbild mit einem Minisystem starten, über das dann das Linux-System geladen wird. Es ist aber flexibler, stattdessen den Programmcode von Isolinux in den Speicher zu laden und dann den Bootvorgang fortzusetzen. Isolinux bietet ein umfangreiches Menüsystem, über das man bereits vor der Installation beispielsweise die Sprache auswählen, eine Hilfe aufrufen oder zusätzlich Kernel-Parameter übergeben kann.

Der zweite Bootmanager heißt Grub2 (*www.gnu.org/software/grub*). Er kommt bei PCs mit Uefi-Firmware zum Einsatz. Neuere Distributionen wie Ubuntu 22.04 verwenden ihn auch für den Bios-Modus. Auf die Grub-Konfiguration verwenden die Distributoren bisher keine große Mühe. Obwohl auch dieser Bootloader sich ansprechend gestalten lässt, zeigt sich das Grub-Menü meist in schlichtem Schwarzweiß und bietet keine Vorauswahl der Sprache.

Booten vom USB-Stick: Im einfachsten Fall wird der Inhalt der ISO-Datei exakt auf den USB-Stick kopiert, beispielsweise mit

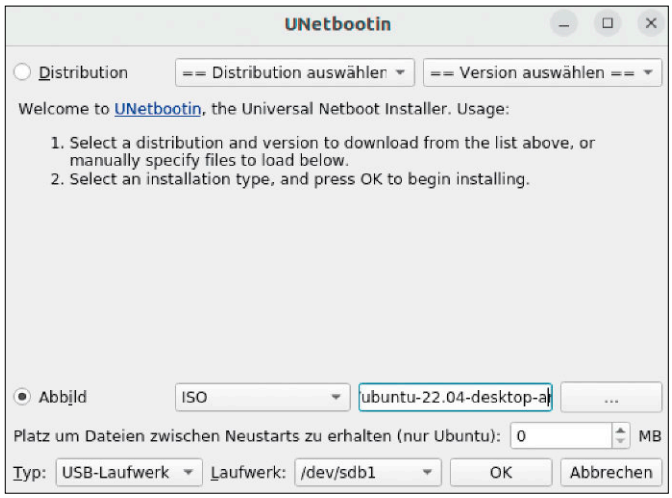
```
sudo dd if=[Boot-DVD.iso] of=/dev/
  sd[X]
```

„[X]“ steht für die Laufwerksbezeichnung. Dabei gehen alle vorhanden Daten verloren. Das gleiche Ergebnis erzielt man unter Ubuntu mit dem Tool „Startmedienersteller“ für die grafische Oberfläche. Nutzer von Linux Mint finden ein ähnliches Programm im Startmenü unter „Zubehör → USB-Abbilderstellung“.

Auf dem Stick befinden sich dann die gleichen Partitionen wie auf der DVD. Eine große schreibgeschützte ISO-9660-Partition enthält die Systemdateien und deren Inhalt ist im Dateimanager sichtbar. In den ersten

512 Bytes ist außerdem ein MBR (Master Boot Record) untergebracht, damit das System auch auf Bios-PCs booten kann. Dahinter folgt die ESP-Partition (Efi System Partition) für Uefi-PCs mit den Grub2-Bootloader-Dateien. Selbst wenn der USB-Stick mehr Speicherplatz bietet, als die ISO-Datei benötigt, ist der Rest nicht mehr nutzbar. Nach der Linux-Installation kann man den Stick neu formatieren, um ihn für andere Zwecke zu verwenden.

Tools wie Unetbootin (*https://unetbootin.github.io*) oder Rufus (nur für Windows, *https://rufus.ie*) funktionieren anders. Beide kopieren die Dateien aus dem ISO auf den USB-Stick, der für Linux mit dem Dateisystem FAT32 formatiert sein muss. Unetbootin installiert für Bios-PCs in jedem Fall den Bootloader Syslinux und erstellt automatisch eine passende Konfigurationsdatei. Rufus richtet Syslinux nur ein, wenn das System Isolinux verwendet. Andernfalls wird der Grub2-MBR auf Bios-PCs verwendet. Für Uefi-PCs sind bei beiden Tools keine besonderen Maßnahmen erforderlich, weil die PC-Firmware auf einer FAT32-Partition den Bootloader im Ordner „/EFI/boot/“ findet. Anders als bei dd steht der nicht belegte Platz auf dem USB-Stick weiter zur Verfügung. Die Installationsdateien eines weiteren Linux-Systems lassen sich jedoch nicht zusätzlich auf das Laufwerk kopieren.



Unetbootin: Auch dieses Tool kann nur ein einzelnes System auf den USB-Stick kopieren und verändert zudem das Bootmenü. Dafür bleibt aber Speicherplatz für andere Zwecke übrig.

Ventoy: Installationsabbilder direkt vom Stick starten

Der Bootloader Grub2 kann ISO-Abbilder einbinden und das enthaltene System starten. Dafür ist eine Konfigurationsdatei erforderlich, die den Pfad zu ISO-Datei, Kernel und Ramdisk-Datei („initrd“) enthält. Das Tool Ventoy (*www.ventoy.net*) automatisiert die Grub2-Konfiguration so gut wie möglich. Es findet ISO-Dateien auf dem USB-Stick und erstellt automatisch ein dazu passendes Menü, über das sich das gewünschte System booten lässt. Mit Ventoy kann man die meisten bekannten Linux-Distributionen und Windows verwenden. Eine Liste der getesteten ISO-Dateien ist unter *www.ventoy.net/en/isolist.html* einsehbar.

Schritt 1: Zur Installation laden Sie die „tar.gz“-Datei für Linux von *https://github.com/ventoy/Ventoy/releases* herunter. Entpacken Sie das Archiv und starten Sie dann Ventoy-GUI.x86_64. Sollte das Programm auf Ihrem PC nicht starten, lässt sich Ventoy im Webbrowser nutzen: Gehen Sie im Terminal in den Ordner, wo Sie das Tool entpackt haben. Dort starten Sie dieses Script:

```
sudo ./VentoyWeb.sh
```

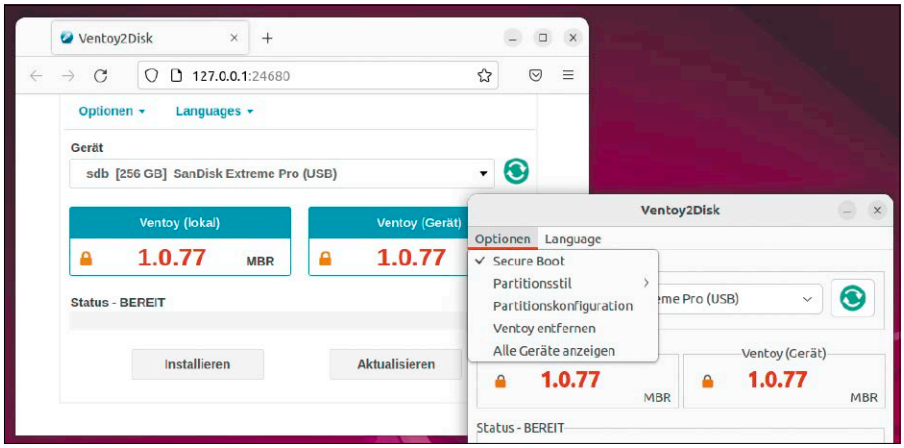
Es zeigt die URL an, über die sich die Weboberfläche im Browser erreichen lässt, standardmäßig *http://127.0.0.1:24680*.

Schritt 2: Stellen Sie über „Language“ als Sprache „German (Deutsch)“ ein. Unter „Optionen“ aktivieren Sie „Secure Boot“. Das ist nur für Windows 11 erforderlich, weil sich Windows 10 oder Linux auch bei deaktiviertem Secure Boot installieren lässt. Wählen Sie unter „Gerät“ den USB-Stick aus und klicken Sie auf „Installieren“. Der Stick wird neu formatiert, alle enthaltenen Daten gehen verloren. Wenn Sie „Optionen → Alle Geräte anzeigen“ wählen, bietet Ventoy auch Festplatten als Ziel an. Prüfen Sie daher die Einstellung genau, damit Sie nicht versehentlich das falsche Laufwerk formatieren.

Ventoy belegt eine kleine 32-MB-Partition, auf der Grub2, die Bootloader-Dateien für Uefi und einige Tools untergebracht sind. Ein Master Boot Record wird ebenfalls auf den USB-Stick geschrieben, damit auch Bios-PCs davon booten können.

Die zweite Partition wird mit dem Dateisystem ExFAT formatiert und steht auch als Datenspeicher weiter zur Verfügung. Die meisten Linux-Systeme kommen mit der ExFAT-Partition zurecht, aber nicht alle. Soll nur Linux installiert werden, formatiert man die „Ventoy“-Partition mit dem Dateisystem Ext4 neu. Das erhöht die Kompatibilität und verbessert die Leistung. Wer auch Windows installieren möchte, wählt das Dateisystem NTFS. Das eignet sich auch für Linux, weil der Kernel den dafür nötigen Treiber seit Langem enthält.

Schritt 3: Kopieren Sie die gewünschten ISO-Dateien auf den Stick und booten Sie den PC damit. Beim ersten Start und bei aktiviertem Secure Boot erscheint die Mel-



USB-Stick mit Ventoy: Das Tool lässt sich als Desktopanwendung oder im Browser starten. Für Uefi-PCs müssen Sie die Option „Secure Boot“ aktivieren, sofern diese im Bios aktiv ist.

Ventoy-Bootmenü: Alle für Ventoy bereitgestellten ISO-Dateien erscheinen automatisch im Menü. Die Funktionen der F-Tasten sind am unteren Bildschirmrand zu sehen.

dung „Access denied“, die Sie mit „OK“ übergehen. Danach drücken Sie eine beliebige Taste, gehen auf „Enroll key from disk“, wählen „VTOYEFI“ und danach „Enroll _This_Key_In_Mokmanager.cer“. Zum Abschluss gehen Sie auf „Continue“, „Yes“ und „Reboot“.

Ventoy zeigt ein Menü für die Systemauswahl. Darüber starten Sie das gewünschte Installationssystem und die Einrichtung läuft wie gewohnt ab. Über die Taste F2 („Browser“) haben Sie außerdem Zugriff auf die Festplatten im PC und können dort gespeicherte ISO-Dateien auswählen und booten.

Ventoy: Livesystem mit Persistenz

Livesysteme lassen sich auch als Rettungs- oder Zweitsystem nutzen. Die Konfiguration und zusätzlich installierte Software existieren jedoch nur im RAM und gehen bei einem Neustart verloren. Ubuntu und Linux Mint bieten aber mit „Persistenz“ eine Funktion, über die sich individuelle Anpassungen speichern lassen und dann auch beim nächsten Start wieder zur Verfügung stehen.

Schritt 1: Ventoy unterstützt eine Persistenzdatei, die Sie im Terminal mit

```
sudo ./CreatePersistentImg.sh
```

erstellen. Standardmäßig erzeugt das Script die Datei „persitence.dat“, die Platz für ein GB Daten bietet. Wer eine größere Datei benötigt, legt beispielsweise mit

```
sudo ./CreatePersistentImg.sh -s
  2048
```

eine Größe von zwei GB fest. Kopieren Sie die Datei in den Ordner „ventoy“ auf dem USB-Stick.

Schritt 2: Starten Sie das Script „Ventoy Plugson“ im Terminal:

```
sudo ./VentoyPlugson.sh /dev/sd[X]
```

Den Platzhalter „[X]“ ersetzen Sie durch den Buchstaben, über den der USB-Stick erreichbar ist. Das Script zeigt mit *http://127.0.0.1:24681* die URL für die Weboberfläche an, die Sie im Browser aufrufen.

Schritt 3: Gehen Sie auf „Persistence Plugin“ und klicken Sie auf „+ Add“. Hinter „File Path“ fügen Sie den kompletten Pfad zur ISO-Datei ein, die die Persistenzdatei verwenden soll (Beispiel):

```
media/[User]/Ventoy/ISO/ubuntu-
  22.04-desktop-amd64.iso
```

„[User]“ ersetzen Sie durch Ihren Benutzernamen.

Hinter „Dat File“ tragen Sie den Pfad zur zuvor kopierten Persistenzdatei ein (Beispiel):

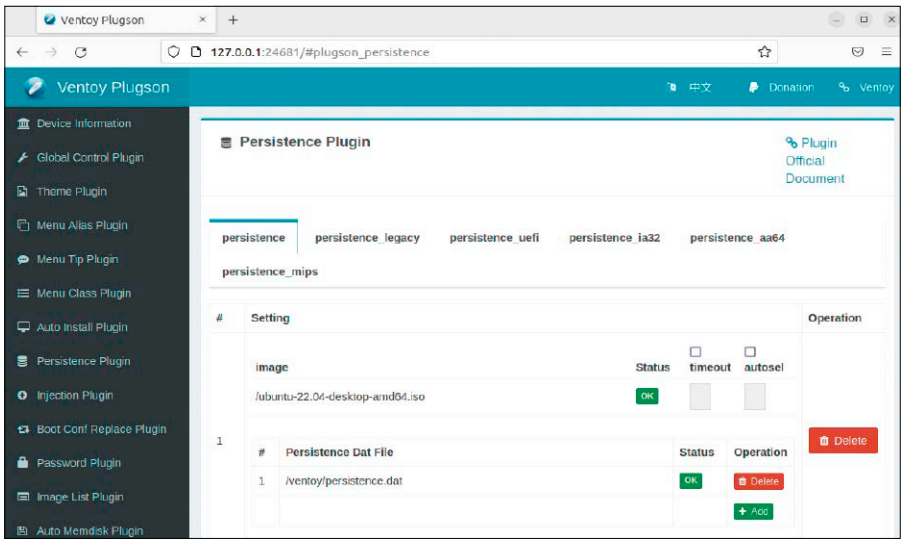
```
/media/[User]/Ventoy/ventoy/
  persistence.dat
```

Klicken Sie auf „OK“, um die Änderungen zu speichern. Das Tool erstellt die Konfigurationsdatei „ventoy.json“ im Ordner „ventoy“. Beim Start des Livesystems lässt Ventoy die Wahl zwischen „boot without persistence“ und „boot with /ventoy/persistence.dat“. Bei der Konfiguration von „Persistence Plugin“ können Sie ein Häkchen vor „timeout“ setzen und darunter die Zeit für einen Countdown eintragen. Nach Ablauf der Zeit startet das System automatisch mit Persistenz.

Ventoy: Optionen für die Windows-Installation

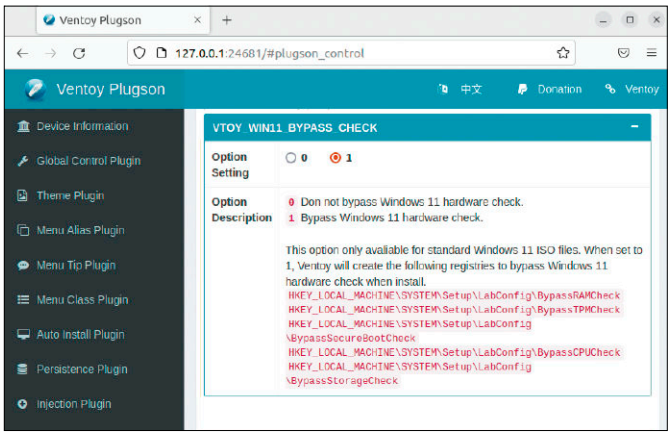
Über Ventoy lassen sich nicht nur ISO-, sondern auch WIM-Dateien booten (Windows-Images). Der Vorteil: Ein individuell angepasstes Installationsabbild („install.wim“) lässt sich direkt verwenden, ohne dass man eine neue ISO-Datei erstellen muss. Nützlich ist das beispielsweise, wenn man unter Windows mit Rufus (*https://rufus.ie*) einen Installationsstick erstellt, der die Hardwareanforderungen von Windows 11 umgeht (Option „Extended Windows 11 Installation (no TPM / no Secure Boot)“).

Damit das Verfahren funktioniert, muss die Ventoy-Partition auf dem Stick mit dem Dateisystem NTFS formatiert sein. Außerdem ist das Wimboot-Plug-in für Ventoy erforderlich. Laden Sie es über *https://m6u.de/WBOOT* herunter. Erstellen Sie auf dem Ventoy-Stick den Ordner „ventoy“ und kopieren Sie die Datei „ventoy_wimboot.img“ hinein. Danach kopieren Sie den gesamten Ordner „sources“ vom Rufus-Stick auf den Ventoy-Stick. Wenn Sie den PC davon booten, wählen Sie im Menü „boot.wim“, um das Installationssystem von Windows 11 zu starten.



Zusätzliche Konfiguration: Über die Webanwendung Plugson können Sie weitere Optionen festlegen. Einstellungen eines Ubuntu-Livesystems beispielsweise lassen sich in einer Persistenzdatei speichern.

Ventoy bietet auch für Original-ISO-Dateien von Microsoft eine Option, den Hardwarecheck bei der Windows-11-Installation zu umgehen. Starten Sie Ventoy Plugson wie vorher beschrieben. Unter „Global Control Plugin“ aktivieren Sie im Abschnitt „VTOY_WIN11_BYPASS_CHECK“ die Option „1“. Dadurch werden bei der Windows-Installation die unter der Option genannten Registry-Einträge hinzugefügt und Windows lässt sich dann auf Hardware installieren, die offiziell nicht unterstützt wird. Da es sich um eine inoffizielle Methode handelt, ist nicht garantiert, dass Windows stabil läuft und dass die Installation mit dem Registry-Patch auch in zukünftigen Windows-Versionen möglich ist.



Windows 11: Die Hardwareprüfung des Microsoft-Systems lässt sich über Registry-Einträge aushebeln, die Ventoy bei der Windows-Installation automatisch einbauen kann.

Grml-Rescueboot: ISO-Dateien von Festplatte starten

ISO-Dateien lassen sich in das Grub-Menü des installierten Systems einbauen. Das ist nützlich, wenn Sie beispielsweise ein Livesystem regelmäßig als sicheres Surfsystem verwenden oder Rescuezilla für Backups starten (siehe Beitrag ab Seite 34).

Schritt 1: Installieren Sie unter Ubuntu 20.04, 22.04 oder Linux Mint 20 das Paket „grml-rescueboot“:

```
sudo apt install grml-rescueboot
```

Schritt 2: Standardmäßig soll der Ordner „/boot/grml“ die ISO-Dateien aufnehmen, den Sie mit

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

erstellen. Wenn das Verzeichnis „/boot“ auf einer eigenen Partition liegt, die nicht genügend Platz bietet, können Sie den Pfad in der Datei „/etc/default/grml-rescueboot“ ändern. Beispielsweise mit dieser Zeile:

```
ISO_LOCATION="/grml"
```

Erstellen Sie das angegebene Verzeichnis.

Schritt 3: Passen Sie die Datei „/etc/default/grub“ an. Hier müssen die Zeilen

```
GRUB_TIMEOUT_STYLE=menu
GRUB_TIMEOUT=10
```

enthalten sein, damit das Grub-Menü angezeigt wird. Beim Wert hinter „GRUB_TIMEOUT=“ geben Sie die Anzahl der Sekunden an, nach denen der Standardeintrag automatisch gestartet wird.

Schritt 4: Kopieren Sie die gewünschten ISO-Dateien in den konfigurierten Ordnern und führen Sie danach

```
sudo update-grub
```

aus. Wenn Sie den Rechner neu starten, sehen Sie zusätzliche Einträge im Grub-Menü, über die sich die ISO-Dateien booten lassen.

Zusätzliche Anpassungen für grml-rescueboot: Das Grub-Menü wird mit *update-grub* über Scripts im Ordner „/etc/grub.d/“ erzeugt. Die Datei „42_grml“ sucht nach Dateien im ISO-Ordner und erstellt die dafür passenden Einträge. Das Script setzt darauf, dass im ISO die Datei „/boot/grub/loopback.cfg“ enthalten ist, die Optionen für das direkte Booten der ISO-Datei enthält. Bei gängigen Distributionen ist die Datei vorhanden, bei einigen anderen aber nicht. Das bekannte System Rescue (*www.system-rescue.org*) beispielsweise oder auch Gparted Live (*https://gparted.org*) lassen sich daher nicht booten. Das Script „42_grml“ lässt sich aber dafür anpassen. Die relevanten Zeilen für System Rescue sehen Sie in der Abbildung. Dazu gehört noch „/grml/sysresc_loop.cfg“, das als Ersatz für „/boot/grub/loopback.cfg“ dient. Die Beispieldateien können Sie über *https://m6u.de/mubo* herunterladen.

In unseren Konfigurationsdateien finden Sie außerdem Optionen für Gparted Live und das LinuxWelt-Rettungssystem sowie Anpassungen für Ubuntu 22.04, damit das System gleich mit deutschsprachiger Oberfläche startet. ■

Öffnen — 42_grml — /etc/grub.d — Speichern

```
115 if [ "$grml" = "systemrescue-9.02-amd64.iso" ];  then
116   cat << EOF
117 menuentry "${title}" {
118 ${grub_prep}
119         iso_path="${rel_dirname%/}/${grml}"
120         export iso_path
121         rmmod tpm
122         configfile /grml/sysresc_loop.cfg
123 }
124 EOF
125 else
126   cat << EOF
127 menuentry "${title}" {
128 ${grub_prep}
129         iso_path="${rel_dirname%/}/${grml}"
130         export iso_path
131         kernelopts=" $CUSTOM_BOOTOPTIONS $additional_param "
132         export kernelopts
133         # support booting recent GRUB versions on UEFI systems
134         rmmod tpm
135         loopback loop "${rel_dirname%/}/$grml"
136         set root=(loop)
137         configfile /boot/grub/loopback.cfg
138 }
139 EOF
140 fi
141 done
```

Öffnen — sysresc_loop.cfg — /grml — Speichern

```
1 menuentry " System Rescue 9.0.2 (64 Bit) - Normaler Start" {
2     probe -u $root --set=rootuuid
3     set imgdevpath="/dev/disk/by-uuid/$rootuuid"
4     loopback loop $iso_path
5     probe -l loop --set=isolabel
6     linux  (loop)/sysresccd/boot/x86_64/vmlinuz scandelay=1 archisolabel=$isolabel
  img_dev=$imgdevpath img_loop=$iso_path archisobasedir=sysresccd iomem=relaxed setkmap=de
7     initrd (loop)/sysresccd/boot/intel_ucode.img (loop)/sysresccd/boot/amd_ucode.img (loop)/
  sysresccd/boot/x86_64/sysresccd.img
8 }
```

Reiner Text — Tabulatorbreite: 8 — Z. 6, Sp. 112 — EINF

Individuelle Grub-Konfiguration: Für einige Distributionen sind Anpassungen im der Datei „42_grml“ nötig. System Rescue beispielsweise lässt sich ansonsten nicht aus einem ISO starten.

18 Jahre TUXEDO Computers
wie alles begann

Das Hardware-Unternehmen feiert Jubiläum und träumt von mindestens weiteren 18 Jahren. Die Geschichte von TUXEDO Computers beginnt wie alle guten Tech-Stories: Nicht in einer Garage, aber in einem Wohnzimmer am PC. Aber alles der Reihe nach.

Ein Blog mit der Dokumentation eines Umstiegs von Windows auf Linux war der schnöde Anfang. Und es sah zunächst nicht danach aus, als würde eine große Sache daraus werden. Davon abgesehen befand sich der zukünftige Geschäftsgründer noch in seiner Kaufmannsausbildung. 18 Jahre später sind wir klüger und die Welt um eine wichtige Anlaufstelle, wenn es um Notebooks und PCs mit dem freien Betriebssystem geht, reicher.

Von einer Person auf fast 50 Mitarbeiter

Das Unternehmen entwickelte sich von einem Ein-Mann-Betrieb zu einem florierenden Geschäft mit aktuell fast 50 Mitarbeitern, die in den Bereichen Backoffice, Support, Entwicklung, Produktmanagement, System- und Serveradministration, Vertrieb, Fertigung und Marketing tätig sind. Zunächst konnte man den Vorgänger von TUXEDO Computers in Bayreuth finden – ab 2013 ging es dann nach Königsbrunn bei Augsburg und mündete 2019 in den Umzug nach Augsburg direkt in die aktuellen Räumlichkeiten, die bis Ende des aktuellen Jahres noch erweitert werden. So viel sei verraten: Es wird ein Platz für eine Dauerpräsentation verschiedener TUXEDO-Notebooks eingerichtet, wie auch Räume, die für Schulungszwecke und Veranstaltungen zur Verfügung stehen.

"Mein Anspruch war es von Anfang an, der Community ein voll funktionsfähiges Produkt zu geben!"

Wie alles begann

Wie kommt ein junger Mann dazu, ein Unternehmen zu gründen? Das Interesse an Computerhardware und -software geht auf das Jahr 1995 zurück, als Herbert Feiler seinen ersten PC bekam: *„(...) einen soliden 100-MHz-Intel-i486 mit Windows 95“*, erinnert er sich. Nach vielen problembedingten Neuinstallationen wurde der Nachfolger Windows XP angekündigt. Und wie heute führt jede neue Windows-Version dazu, dass sich viele Nutzer nach Alternativen umsehen. Der spätere TUXEDO-Gründer war einer von ihnen. Er dachte sich, wenn er sich an ein neues Aussehen und die Bedienung von Windows anpassen muss, kann er auch gleich ein freies Betriebssystem nehmen, mit mehr Anpassungsfähigkeit und mit einer größeren Bandbreite an Variationen. Ab da war es um ihn geschehen und seine Linux-Reise begann.

Linux-Distribution über CDs und DVDs

Allerdings stellte sich dieses Abenteuer doch schwieriger heraus als gedacht. Bevor er zufrieden war, musste er zunächst ein paar bekannte wie auch weniger bekannte Distributionen testen. Vor knapp 20 Jahren gestaltete sich das noch etwas mühsamer, als heute: *„Damals, in den Zweitausendern, war die Internetverbindung noch ein bisschen langsamer als heute“*, schmunzelt er und überlegt. Die wichtigste Hauptinformationsquelle waren daher die Print-Magazine der Linux-New-Media-Gruppe (Linux Magazin und Linux User), über die Herbert Feiler einige Distributionen auf CDs / DVDs erstehen und ausprobieren konnte. Die Reise hat durchaus Spuren bei Herbert Feiler hinterlassen. Denn, aus der Erfahrung heraus und um anderen Leuten zu helfen, die Hürden zu umgehen, die er nehmen musste, richtete er damals die Website "linux-tests.de" mit Tipps und Tricks rund um Linux, quasi einen Vorläufer der heutigen Blogs, ein.

Frage im Forum als Initialzündung

Auf dieser Website hielt er seine Erfahrungen fest und gab Tipps und Tricks in Sachen Linux. Zusätzlich gab es ein Diskussionsforum, in dem sich Leser und Websitebesucher austauschen und gegenseitig helfen konnten. Und hier kommt die eigentliche Initialzündung! Wir erinnern uns zurück an die Frage, warum ein junger Mann ein Unternehmen gründen will. In diesem Forum tauchten immer wieder Fragen auf, wo was zum Thema Linux gekauft werden kann. Und dann war es soweit: Herbert Feiler beschloss ein eigenes Online-Geschäft zu eröffnen und gründete am 15.12.2003 den "Linux-Onlineshop". Hauptsächlich konnten Kunden zu Beginn Merchandise-Artikel, wie Tassen, T-Shirts, Aufkleber, Bücher und Softwareboxen mit Linux-Distributionen auf CD / DVD, kaufen – zur damaligen Zeit eine sehr populäre Variante.

Nicht nur Merchandise – auf Hardware erweitert

Im Laufe der Jahre wurde die Produktpalette ausgebaut, vor allem, weil auch im Forum immer wieder diskutiert wurde, welche PCs sich für Linux eignen. So entstand die Idee, das Geschäft um Computer zu erweitern: *„Die erste Hardware, die wir verkauften, war ein Micro-ATX-Desktop-Computer in Standardgröße, später Mini-PCs, Full-Size-ATX-Desktops und dann Note-books/ Laptops“*, erklärt Herbert Feiler. Doch war es sehr schwierig, kompatible Hardware zu finden, die einwandfrei mit Linux funktionierte. Es gab viele erfolglose Versuche und Tests im Keller des Elternhauses, bis Herbert Feiler zufrieden war: *„Mein Anspruch war es von Anfang an, der Community ein voll funktionsfähiges Produkt zu geben, nicht etwas, das fast perfekt funktioniert, es musste perfekt sein! Das war auch der Grund, warum ich mit Desktop Computern und nicht mit Notebooks angefangen habe. Desktops sind immer noch viel einfacher mit Linux zu betreiben. Notebooks haben viele spezielle Funktionen, die man oft erst zurückentwickeln muss.“*

Linux-Onlineshop Ade – Hallo TUXEDO Computers!

Inzwischen ist der Linux-Onlineshop dem Internetauftritt des Unternehmens TUXEDO Computers gewichen. TUXEDO ist in diesem Zusammenhang ein Wortspiel aus dem englischen Wort für Maßanzug und dem Linux-Maskottchen Tux. Interessierte finden hier eine breite Auswahl an linuxfähigen PCs und Notebooks, die individuell und an die jeweiligen Bedürfnisse angepasst werden können. Ob für den privaten Gebrauch, für Business oder Gaming, ob Workstation oder Ultrabook – TUXEDO hat für Linux-Interessierte immer ein passendes Angebot. Dabei setzt das Unternehmen mittlerweile auf eine eigene Distribution: *„Mit unserer eigenen Distribution, basierend auf Ubuntu mit dem KDE Plasma sind wir völlig frei, alles so anzupassen, dass sie perfekt mit unseren Geräten funktioniert“*, erklärt Herbert Feiler.

Eigene Entwicklung, Anpassungen, Treiber

Der Anspruch zu Beginn des Unternehmens hat sich auch nach 18 Jahren nicht geändert: Linux-Kompatibilität alleine reicht nicht - perfekt funktionierende Linux-Hardware will das Unternehmen bieten. Daher programmiert die Entwicklungsabteilung eigene Treiberpakete und Software-Lösungen, wie das TUXEDO Control Center oder TUXEDO Tomte für ein optimales Linux-Erlebnis. Warum ist das notwendig? *„Bei Laptops gibt es immer spezielle Tasten, die nicht sofort funktionieren, das Touchpad braucht eigen Treiber, die Lüftersteuerung läuft immer nur rudimentär, die Tastaturbeleuchtung ist nicht oder nicht vollständig steuerbar und vieles mehr“*. Aber etwas hat sich nach 18 Jahren doch verändert: *„Die ganze Linux-Gemeinschaft ist viel strukturierter und es gibt viele Unternehmen, die jetzt zusammenarbeiten, um Hürden gemeinsam zu meistern, weil sie ein gemeinsames Ziel haben“*, resümiert Herbert Feiler.

Stetig wachsende Bekanntheit

Vor allem im Businessbereich hat sich TUXEDO einen Namen gemacht. Wer auf Sicherheit und Datenschutz achtet, kommt an dem Augsburger Unternehmen kaum vorbei.

Auch aus der Community wird die Zusammenarbeit mit dem Hardware-Anbieter gesucht. So wurden Geräte gemeinsam mit dem Manjaro-Team auf deren Distribution hin optimiert, mit KDE tauscht man Programmierarbeiten aus und das Formula-Student-Team EcurieAix der RWTH Aachen wird sowohl fachlich als auch finanziell unterstützt.

Ausblick

Fragt man Herbert Feiler, wie er sich die Zukunft von TUXEDO Computers vorstellt, so schmunzelt er und antwortet: *„Natürlich ganz vorne dabei – mit tollen und weiterhin qualitativ hochwertigen Geräten!“*

Jetzt kommen zunächst einmal im Herbst weitere 500 qm Büroräume hinzu und bis Ende des Jahres feiert das Unternehmen seine Volljährigkeit. Dazu werden mehrere TUXEDO-Geburtstags-Fan-Pakete verlost und vielleicht gibt es noch den ein oder anderen Geburtstagskuchen für Kunden und Kundinnen sowie Fans.

Geschäftsführer: Herbert Feiler

TUXEDO Computers
Alter Postweg 101
86159 Augsburg

Mitarbeiter: 50
Gründung: 15.12.2003
Profession: Linux-Spezialist

www.tuxedocomputers.com

TUXEDO COMPUTERS

Produktive Systemtools

Das Heftspecial „Top-Tools“ bringt Empfehlungen der Redaktion in den fünf Kategorien System, Hardware, Backup, Netzwerk und Desktop. Es handelt sich durchgehend um Ergänzungen, die nicht (überall) standardmäßig vorliegen.

VON HERMANN APFELBÖCK

Mit dem Stichwort „Tool“ verbinden wir zweierlei Auswahlfilter, nämlich eine engere Spezialisierung sowie das Fehlen im Standardsystem. Große Anwendungen wie Browser, Office, Medienplayer oder Bildbearbeitung bleiben also ebenso draußen wie Standardzubehör, das jedes System mitbringt (etwa Dateimanager oder Editor). Den Start machen produktive und je nach Situation oft unentbehrliche Systemergänzungen.

7z: Packer mit Verschlüsselung

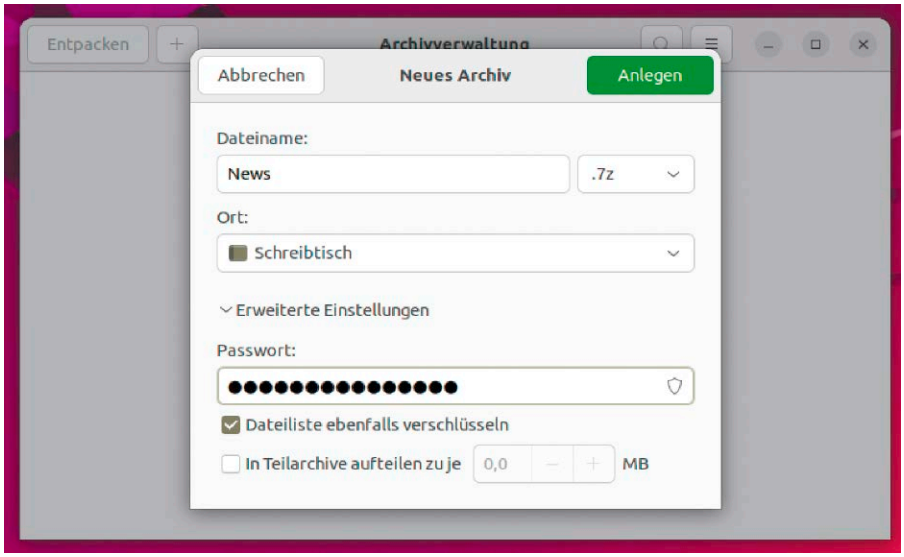
Archivmanager wie File-Roller und Ark integrieren eine Reihe von Packerformaten wie ZIP, TAR, TAR.GZ oder RAR. 7-Zip (7z) ist nicht standardmäßig an Bord, obwohl es für den Archivaustausch mit Windows eine wichtige Rolle spielt. Mit

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

rüsten Sie die Komponente schnell nach. Beachten Sie, dass 7-Zip unter Linux ohne eigene Oberfläche ankommt. Der Packer ist nach der Installation automatisch im jeweiligen Archivmanager integriert.

7-Zip hat den interessanten Nebenaspekt, dass es Packarchive mit Passwort verschlüsseln kann. Wenn Sie nach Rechtsklick auf einer Datei (oder einem Ordner) „Komprimieren“ und das Format „7z“ wählen, gibt es unter „Erweiterte Einstellungen“ die Passwortoption. Diese eignet sich für Verschlüsselung einzelner Dateien oder Ordner.

Hinweis: Alle Dateimanager erlauben den Einbau zusätzlicher Kontextmenüs. Wie Sie 7z-Verschlüsselung in den Ubuntu-Dateimanager Nautilus integrieren und sich damit die Passworteingabe sparen, zeigt der Beitrag ab Seite 18.



7z im Archivmanager: Das Packerformat 7-Zip ist fast Pflicht, zumal es eine Passwortoption bietet, die sensible Dateien sicher verschlüsselt.

Synaptic: Die beste alternative Paketverwaltung

Synaptic kombiniert auf Debian/Ubuntu-Systemen die Vorteile einer grafischen Paketverwaltung mit dem Umfang und der Reichweite von apt. Ubuntu-Nutzer erhalten das Tool mit diesem Befehl:

```
sudo apt install synaptic
```

Synaptic bietet wie apt – und im Unterschied zu „Ubuntu Software“, „Software-Center“, „Boutique“ oder wie immer – sämtliche Software aus den Paketquellen zur Installation an (also auch Tools für die Kommandozeile, Bibliotheken und Entwicklerpakete). Per Klick auf „Neu laden“ aktualisieren Sie die Paketdatenbank und über „Suche“ finden Sie die gewünschten Pakete. Sie können außerdem links im Fenster „Bereiche“ wie „Internet“ oder „Grafik- und Bildbearbeitung“ anklicken. Wenn Sie ein Paket installieren wollen, klicken Sie es mit der rechten Maustaste an und gehen auf „Zum installieren vormerken“. Das Fenster „Zusammenfassung“ zeigt die anstehenden Änderungen und mit „Anwenden“ beginnt die Installation.

Für Deinstallationen wählen Sie im Kontextmenü eines Pakets „Zum Entfernen vormerken“ und klicken danach auf „Anwenden“. Prüfen Sie im Fenster „Zusammenfassung“ die Angaben unter „Zu entfernen“. Ist die Liste sehr lang, besteht die Gefahr, dass wichtige Abhängigkeiten dabei sind. In diesem Fall sollten Sie die Deinstallation besser abbrechen. Bei systemrelevanten Pro-

grammen gibt Synaptic aber ohnehin eine Warnmeldung aus.

Locate: Schnelle Dateisuche

Schnelle Terminal-Dateisuche ist auf Servern unerlässlich, aber auch auf dem Desktop willkommen (Suchtools, die sich nur für den Desktop eignen, finden Sie im Beitrag ab Seite 40). Terminaltool der Wahl ist aufgrund seiner Geschwindigkeit locate, das auf Ubuntu-Systemen mit

```
sudo apt install plocate
```

schnell nachgerüstet ist. Das Paket „plocate" enthält neben dem Suchkommando locate auch das unentbehrliche Indexierungstool updatedb. Damit die Dateiliste aktuell bleibt, muss je nach Rechnernutzung täglich oder auch häufiger der Befehl

```
sudo updatedb
```

ausgeführt werden. Das ist ein Fall für einen Cronjob des root-Kontos (*crontab -e*):

```
0 10 * * * /usr/bin/updatedb
```

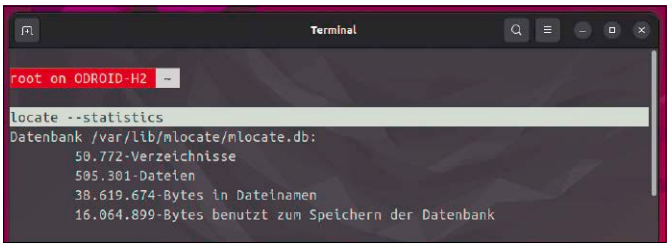
Ein Befehl wie

```
locate -A -i hendrix woodstock
```

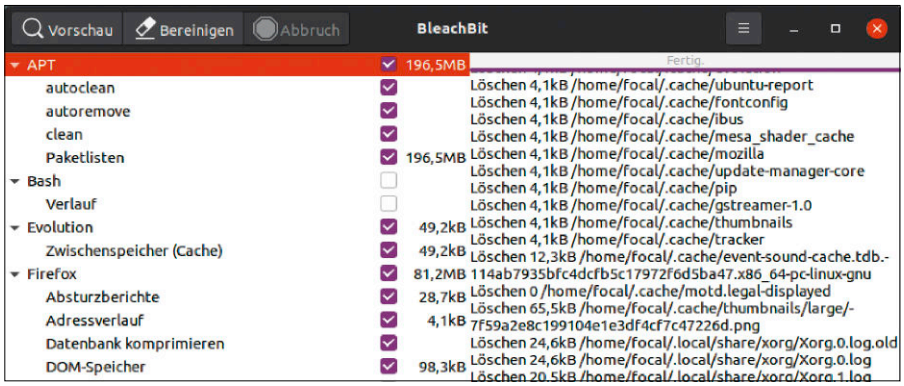
liefert sofort alle passenden Dateien mit komplettem Pfad – auch bei sehr großen Datenbeständen. Die Eingabe der fast immer notwendigen Parameter „-A" (alle Wörter müssen im Dateinamen vorkommen) und „-i" (Groß/Kleinschreibung ignorieren) können Sie sich mit einem Alias

```
alias loc='locate -A -i'
```

in der Datei „~/.bashrc" ersparen. Standardmäßig berücksichtigt locate keine USB-Laufwerke. Um dies bei Bedarf zu ändern, muss in der Konfigurationsdatei „/etc/updatedb.conf" nach „PRUNEFS=..." (ausgeschlossene Dateisysteme) der Eintrag „usbfs" gelöscht werden.



Locate-Statistik: Ein paar Hunderttausend Dateien sind für das indexbasierte Tool keine beschwerliche Aufgabe. Die Ergebnisse einer locate-Suche erscheinen sofort.



Bleachbit: Das Werkzeug leistet gute Dienste beim automatisierten Aufräumen von Browsercache, Updatecache, verwaisten Paketen und anderen Dateileichen.

Bleachbit: Der Lösch-Klassiker

Bleachbit hat manches thematisch ähnliche Tool durch seinen Funktionsumfang klar distanziert. Unter Ubuntu ist es mit Paketnamen „bleachbit" in den Standard-Paketquellen verfügbar. Das Programm erklärt die einzelnen Löschoptionen vorbildlich, zeigt den zu erwartenden Speichergewinn und warnt vor eventuell riskanten Optionen. Die meisten Löschaktionen finden im Home-Verzeichnis statt (Browser, Mail, Office), jedoch kann Bleachbit auch in der Paketverwaltung löschen, wenn es mit dem Menülink „BleachBit (as root)" oder mit *sudo bleachbit* im Terminal gestartet wird. Bleachbit macht auch manchen Gang ins Terminal überflüssig, um in der Paketverwaltung aufzuräumen (*apt autoremove, apt clean*). Das Entsorgen überflüssiger Sprachen beherrscht es unter „Bearbeiten → Einstellungen → Sprachauswahl".

Rtcwake automatisiert Systemstart

Systemstart und Shutdown können Sie komplett automatisieren: Das Tool rtcwake ist auf einigen Linux-Systemen bereits vorinstalliert, andernfalls mit gleichnamigem Paketnamen schnell nachgerüstet. Rtcwake kann einen Rechner ausschalten (oder in einen ACPI-Ruhezustand versetzen) und zur gewünschten Zeit wieder starten. Im einfachsten Fall sieht ein Kommando so aus:

```
sudo rtcwake -m off -s 60
```

Der Befehl ist gut geeignet, um zu testen, ob die Hardware mitspielt (x86-Hardware praktisch immer, ARM-Rechner nicht immer). Der Schalter „-m" bestimmt den ACPI-Modus. Mögliche Werte sind „standby", „mem", „disk" oder „off" (komplettes Ausschalten). Als zweiter Parameter ist hier „-s" („seconds") mit einer nachfolgenden Zeitangabe in Sekunden angegeben. Der obige Testbefehl wird also das System herunterfahren und nach einer Minute neu starten (60 Sekunden).

Obwohl mit Schalter „-t" („time) auch eine exakte Zeitangabe möglich ist, empfehlen wir, den geplanten Neustart immer mit Parameter „-s [...]" anzugeben, selbst wenn es sich um viele Stunden handelt. Es ist wenig Mühe, etwa zehn Stunden in Sekunden umzurechnen (10*3600=36 000).

Um Shutdown und Start zu automatisieren, kommt der Zeitplaner Cron ins Spiel: Nach dem Aufruf der Crontab-Editors mit

```
sudo crontab -e
```

schaltet folgender Crontab-Eintrag

```
0 22 * * *
 /usr/sbin/rtcwake -m off -s 36000
```

den Rechner täglich um 22:00 Uhr ab und startet ihn nach 36 000 Sekunden (zehn Stunden) wieder – somit exakt um 8:00 Uhr.

Unetbootin für Ubuntu live

Unetbootin transportiert ein Livesystem (ISO-Image) auf den Zieldatenträger Ihrer Wahl. Das Tool gibt es für Linux, Windows und Mac-OS X (auf Heft-DVD, Download unter *https://unetbootin.github.io/*). Um ein ISO-Image bootfähig auf USB-Stick zu befördern, wählen Sie im Dialog unten die Option „Abbild" und navigieren dann mit der Schaltfläche „..." zur gewünschten Datei. Nach Klick auf „Öffnen" erscheint der komplette Pfadname im Eingabefeld. Danach wählen Sie neben „Typ" die Option „USB-Laufwerk" und neben „Laufwerk" geben Sie die Kennung des USB-Sticks an. Kontrollieren Sie die Laufwerkskennung des USB-Sticks ganz genau, denn Unetbootin wird das Medium komplett überschreiben. Wer

Unetbootin mit Persistenzoption: Damit kann das Ubuntu-Livesystem Einstellungen speichern und zusätzliche Software dauerhaft nachinstallieren.

ein Ubuntu installieren will, kann ebenso gut ein Tool wie Etcher, Win 32 Disk Imager oder dd verwenden. Der entscheidende Vorteil von Unetbootin liegt im optionalen Persistenzspeicher, der aus eingefrorenen Livesystemen anpassungsfähige Zweitsysteme macht.

Wenn Sie eine beliebige Ubuntu-Variante (auch Linux Mint oder Elementary OS) auf USB kopieren, erscheint im Programmfenster die zusätzliche Option: Neben „Platz um Dateien zwischen Neustarts zu erhalten" können Sie eine Speichergröße festlegen, beispielsweise „4000 MB". Dies ermöglicht es, im späteren Livesystem weitere Programme zu installieren oder das System individuell einzurichten. Systemeinstellungen und nachinstallierte Programme bleiben dann erhalten.

Veracrypt: Daten verschlüsseln

Veracrypt ist das empfohlene Verschlüsselungsprogramm für Anwender, die Daten zwischen Linux und Windows transportieren. Downloads für alle Plattformen (auch Mac-OS X) gibt es unter *https://veracrypt.fr/en/Downloads.html*. Veracrypt eignet sich insbesondere für größere Datenmengen, während für kleinere Ad-hoc-Archive das bereits genannte 7z die einfachere Wahl sein dürfte.

Veracrypt-Container haben eine statische Größe, die Sie beim Anlegen definieren: Nach „Create Volume → Create [...] file container → Standard VeraCrypt volume" geben Sie Pfad und Namen einer bisher nicht existierenden Datei an. Das wird der Container für die verschlüsselten Daten. „Encryption Option" belassen Sie auf den Standards und geben danach die Containergröße an. Danach kommt die Passwortvergabe. Zur Schlüsselerstellung auf Basis des Passworts will Veracrypt Mausbewegungen im eigenen Fenster, was Sie nach beendeter Fortschrittsanzeige mit „Format" abschließen. Damit ist der Container einsatzbereit.

Mit „Select File" im Hauptdialog navigieren Sie zur Containerdatei. Mit „Mount" und Eingabe des Passworts wird diese geladen und im Dateimanager geöffnet. Auf diesem Datenträger lesen, arbeiten, kopieren Sie wie auf einem normalen Laufwerk. Mit „Dismount" im Hauptdialog entladen Sie den Container, der somit wieder geschützt ist. Beachten Sie, dass Sie beim Mounten von Containern nach dem sudo-Kennwort gefragt werden, das mit dem Containerpasswort nichts zu tun hat und vermutlich anders lautet. Die Nutzung in anderen Betriebssystemen ist identisch, jedoch muss Veracrypt überall vorliegen, wo Sie die Container verwenden wollen.

Preload: Startbeschleuniger

Das Tool Preload beschleunigt Programmstarts, die Sie häufig oder regelmäßig nach jeder Anmeldung verwenden oder sogar als Autostarts eingerichtet haben (unter „Startprogramme"). Der einfache Dienst protokolliert die Programmvorlieben und lädt dann die Favoriten vorab in den Arbeitsspeicher. Der eigentliche Programmstart verläuft dadurch schneller. Preload ist in den Paketquellen verfügbar und mit

```
sudo apt install preload
```

schnell nachinstalliert. Theoretisch können Sie in die Konfiguration des einfachen Tools manuell eingreifen („/etc/preload.conf"), dies ist jedoch nicht erforderlich.

Powertop: Der Energiemonitor

Powertop von Intel ist vor allem für Notebooks relevant, um die Akkulaufzeiten zu verbessern, kann aber auch auf PCs den Stromverbrauch reduzieren. Das Tool liegt in den Standard-Paketquellen aller wichtigen Linux-Distributionen und ist mit

```
sudo apt-get install powertop
```

schnell installiert. Nach dem Aufruf mit root-Recht

```
sudo powertop
```

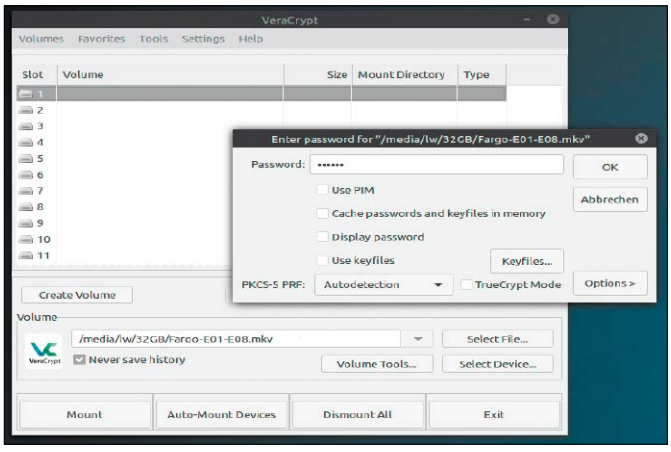
sammelt das Tool Daten und zeigt dann einen Statusbericht mit geschätztem Strombedarf, CPU-Modi und eine Liste aller Prozessnamen, die den Stromsparmodus durch Hardwareanfragen unterbrechen. So lassen sich auch Prozesse ausfindig machen, welche Stromsparfunktionen verhindern und auf Notebooks für laute Lüftergeräusche im Leerlauf sorgen.

Eine Reihe von Empfehlungen liefert Powertop unter „Einstellbarkeit" (Registerwechsel mit Tab-Taste). Temporär für die aktuelle Sitzung aktiviert die Eingabetaste die jeweilige Option. In der Regel wird man mit

```
sudo powertop --auto-tune
```

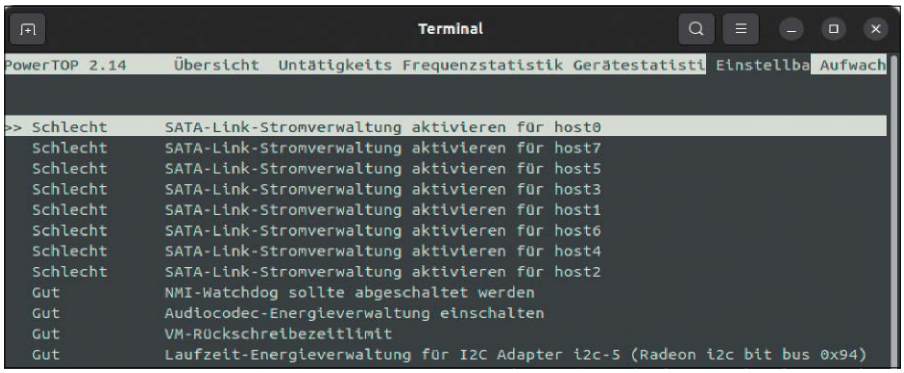
alle möglichen Stromsparoptionen aktivieren. Soll dies immer automatisch geschehen, hilft folgender Auftrag in der Crontab:

```
@reboot /usr/sbin/powertop --auto-tune
```



Veracrypt-Container: Das Programm ist eine exzellente Verschlüsselungsmethode für mittlere Datenmengen und den Austausch mit Windows-Systemen.

Dies muss mit *sudo crontab -e* in der Crontab von root erfolgen, da Powertop stets root-Recht benötigt.



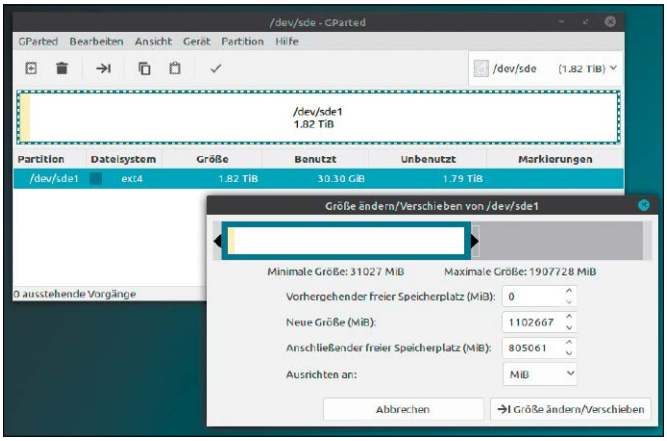
Powertop: Das Tool misst den aktuellen Energiebedarf und kann aktiv Optimierungsmaßnahmen schalten.

Gparted: Partitionsgrößen ändern

Das auf vielen Gnome-affinen Linux-Distributionen vorinstallierte Gnome-Disks hat einen deutlich breiteren Funktionsumfang als Gparted. Allerdings kann es keine Partitionsgrößen ändern (ohne Datenverlust), und wo immer dies notwendig wird, bleibt Gparted die Software der Wahl. Zum Teil ist es vorinstalliert, wo nicht, mit

```
sudo apt install gparted
```

schnell nachinstalliert. Gparted kann nicht nur nach Rechtsklick über „Größe ändern/verschieben" bestehende Partitionsgrößen ohne Datenverlust ändern, sondern ist generell das zuverlässigste Programm für Formatierung, Partitionierung, Label- und UUID-Anpassung. Beachten Sie, dass das Hauptfenster immer nur die Partition(en) des rechts oben gewählten Datenträgers anzeigt. Beachten Sie ferner, dass Gparted angeforderte Aktionen nicht sofort tätigt, sondern in einem Auftragsstapel sammelt, den Sie erst mit „Bearbeiten → Alle Vorgänge ausführen" auslösen.



Gparted verkleinert Partitionen ohne Datenverlust: Das können inzwischen auch andere Partitionsmanager, aber keiner so zuverlässig wie der Altmeister.

Genisoimage: Dateien zusammenlegen

Dieses Werkzeug packt Datensammlungen (Hörbücher, alte Fotosammlungen, alte Script-Projekte), die nicht oder nicht mehr bearbeitet werden müssen, in ISO-Images. Das Tool ist nicht Standard, aber mit gleichlautendem Paketnamen aus den Paketquellen zu beziehen. Folgendes typisches Beispiel

```
genisoimage -l -J -R -joliet-long -o
  Zauberberg.iso Zauberberg/
```

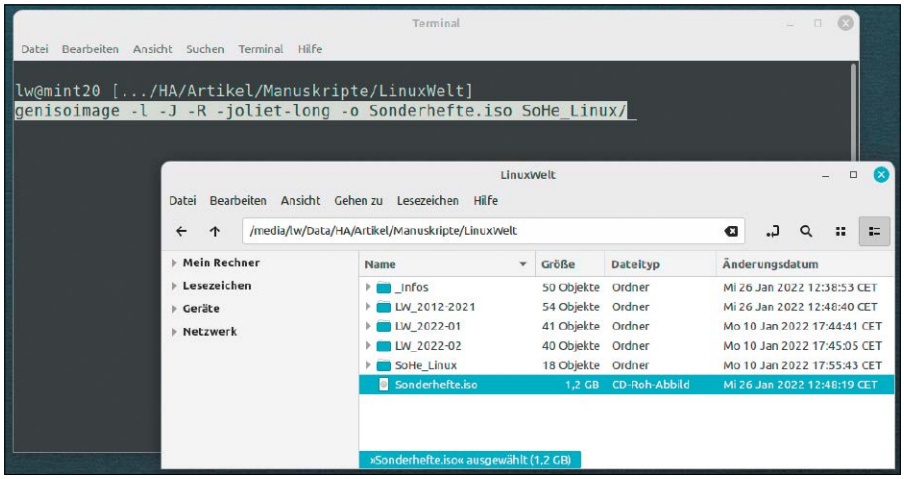
nutzt mehrere Parameter: Die ersten vier Schalter haben nur die eine Aufgabe, lange Dateinamen, Sonderzeichen und eventuell tief verschachtelte Unterverzeichnisse zu berücksichtigen. Nach Schalter „-o" muss dann der Name der zu erstellenden ISO-Datei folgen, und am Ende steht der Ordner, den Sie einpacken möchten. Im Beispiel wird angenommen, dass dies im aktuellen Ordner stattfindet.

Dconf-Editor: Desktop- und Softwarekonfiguration

Dconf nennt sich das Konfigurationssystem der Gnome-basierten Oberflächen Gnome, Cinnamon, Mate und XFCE. Viele Einstellungen dieser Desktops sind nicht mehr in einzelnen Textdateien verstreut, sondern in der Dconf-Zentrale „~/.config/dconf/user" versammelt. Diese ist binär, lässt sich aber mit dem Dconf-Editor bearbeiten. Das Tool rüsten Sie mit

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

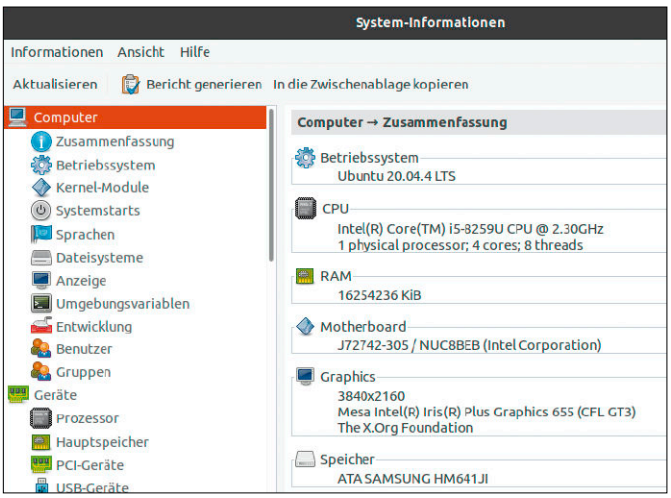
nach. Der hierarchische Dconf-Aufbau hat seinen umfangreichsten Zweig unter „org → gnome". Ein Beispiel für eine Einstellung, die nur auf diesem Weg erreichbar ist, ist das Zielverzeichnis für Bildschirmfotos. Das lässt sich in dconf unter „org → gnome → gnome-screenshot" und dem Wert für „autosave-directory" individuell anpassen. Ein weiterer Kandidat ist der Dateimanager Nemo (Linux Mint u. a.): Die zahlreichen Optionen unter „org → nemo → preferences" übertreffen das Angebot, das Nemo selbst unter „Bearbeiten → Einstellungen" anbietet. ■



ISO-Abbilder mit Genisoimage: Wenn das Schalterarrangement steht, ist das Werkzeug besonders effizient, um eine ganze Reihe von Daten-ISOs zu erstellen.

System- und Hardwareinfos

Mit geeigneten Tools lässt sich herausfinden, welche Prozesse auf dem PC gerade aktiv sind und welche Hardware verbaut ist. Teilweise reichen die Bordmittel, mit Zusatztools sind jedoch tiefere Einblicke möglich.



Welche Hardware steckt im PC? Der „System Profiler und Benchmark“ (Hardinfo) zeigt alle wichtigen Daten rund um CPU, Mainboard, RAM und Grafikchip an.

VON THORSTEN EGGELING

Linux-Distributionen bieten Werkzeuge, um das System zu untersuchen und zu überwachen. Über Informationen zur CPU- oder Speicherauslastung lässt sich beispielsweise die Ursache herausfinden, warum ein System nicht flüssig läuft. Zur Hardware liefert Linux von Haus aus nur wenige Daten, was sich aber mit zusätzlichen Tools verbessern lässt.

Hardinfo: Infotool für den Desktop

Infos zur Hardware sind bei Ubuntu und Linux Mint rar (siehe „Einstellungen → Info“ oder „Einstellungen → Systeminformationen“). Mehr als die Typenbezeichnungen von Prozessor und Grafikchip, verfügbarer Arbeitsspeicher und die Kapazität der Festplatte sind hier nicht zu ermitteln. Deutlich mehr Daten liefert das Tool Hardinfo („System Profiler und Benchmark“), das unter Ubuntu mit

```
sudo apt install hardinfo
```

nachinstalliert werden muss. Hardinfo ist übersichtlich, klickfreundlich und zeigt wesentliche Infos zu Prozessor, Hauptspeicher und USB-Geräten. Unter „Sensoren“ wird die CPU-Temperatur angezeigt, sofern die Hauptplatine die Daten dafür liefert. Auch zu System, Laufzeit, eingehängten Dateisystemen und Netzwerk erhalten Sie hier Basisinfos.

Tiefschürfend ist Hardinfo jedoch nicht: Wer etwa eine eindeutige Aussage über die Erweiterungsflags seiner CPU sucht, muss auf die einschlägigen ls-Kommandos im Terminal ausweichen (lscpu für die CPU, lsusb für USB-Komponenten, lspci für PCI, SATA, Audio, Ethernet).

Inxi: Infotool im Terminal

Das Kommandozeilentool inxi ist eine kompakte und schnelle Info-Perle mit dem Blick fürs Wesentliche. Inxi ist in allen Paketquellen verfügbar und mit

```
sudo apt install inxi
```

schnell nachinstalliert. Inxi wird auf jedem System das Wichtigste anzeigen, ist aber umso vollständiger, wenn alle von ihm genutzten Tools vorliegen. Der Befehl

```
inxi --recommends
```

kann über Fehlendes informieren. Die Terminaleingabe

```
inxi -v8
```

wirft alle wesentlichen Hardwareinfos aus. „-v8“ steht für maximale Gesprächigkeit. Selbstverständlich kann inxi auch gezielt Einzelinfos abrufen, etwa *inxi -S* zur Anzeige des Betriebssystems oder *inxi -s* zur Abfrage der Temperatursensoren. Die Verbose-Level v0 bis v8 decken nicht das ganze Spektrum von inxi ab. So ist etwa auch eine Analyse à la Taskmanager möglich:

```
inxi -tc5 -tm5
```

Dies liefert die fünfressourcenintensivsten Tasks für CPU (c) und Speicher (m).

Smartctl: Datenträgercheck im Terminal

Am Desktop genügt zur Datenträgerkontrolle in der Regel das Tool „Laufwerke“ (Gnome-Disk-Utility). Es zeigt bei Festplatten und SSDs hinter „Einschätzung“ Infos zum Zustand, beispielsweise „Das Laufwerk ist in Ordnung“. Die aktuelle Temperatur wird meist ebenfalls ausgegeben.

Wo kein grafisches Tool wie Gnome-Disks an Bord ist, so etwa auf SSH-administrierten Servern, können Sie den Zustand von Datenträgern im Terminal abrufen. Das einschlägige Werkzeug heißt Smartctl und hat zudem größere Reichweite als grafische Werkzeuge, da es auch mit NVMe-Laufwerken umgehen kann. Auf einigen Distributionen ist Smartctl Standard, wo nicht, kann es mit dem Befehl

```
sudo apt install smartmontools
```

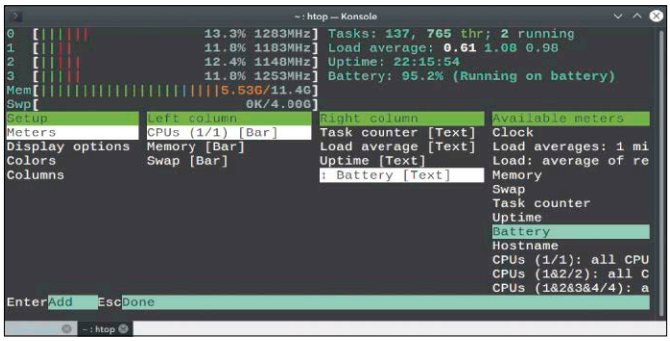
gegebenenfalls schnell nachinstalliert werden. Die typische Abfragesyntax

```
sudo smartctl -A /dev/sda
sudo smartctl -A /dev/nvme0
```

erfordert immer sudo-Recht und die Angabe einer Laufwerkskennung. Neben den Basisdaten werden in der Regel die Einschätzung des Laufwerkszustandes sowie die Temperatur angezeigt.

Noch ausführlicher ist Smartctl mit Parameter „-a“. Wichtige Werte sind „Reallocated_Sectors_Ct“, (defekte Sektoren) und „Spin_Retry_Count“ (gescheiterte Anlaufversuche bei mechanischen Platten), die im Optimalfall „0“ zeigen sollten. Eine simple summarische Antwort liefert Schalter „-H“ mit der Antwort „PASSED“, welche die allgemeine Einsatztauglichkeit eines Laufwerks bestätigt.

Basisinfos mit „Verbose-Level 1“: Was das Werkzeug inxi in einer Sekunde an Hardware-, System-, Netzwerk- und Laufwerksdaten ermitteln kann, ist unübertroffen.



Was läuft? Htop ist ein informativer und anpassungsfähiger Taskmanager für das Terminal und kann abgestürzte Prozesse beenden.

Nvidia/AMD/Intel: Kontrolle des Grafikchips

Wenn eine Nvidia-Grafikkarte im PC steckt, installieren Sie für eine bessere Leistung den proprietären Treiber über „Zusätzliche Treiber“ (Ubuntu) oder „Treiberverwaltung“ (Linux Mint). Damit erhalten Sie automatisch das Infotool „Nvidia X Server Settings“. Neben allgemeinen Informationen zeigt der Bereich „GPU 0“ die Speicherbelegung und die Auslastung des Grafikprozessors („GPU“). Hinter „Video Engine Utilization“ steigt der Wert, wenn mit einem Videokonverter ein Video unter Verwendung der Hardwarebeschleunigung umgewandelt wird. Unter „Thermal Settings“ lässt sich die aktuelle Temperatur der GPU ermitteln. Nutzer eines AMD-Grafikchips können Informationen mit dem Tool Radeon-Profile ermitteln. Eine Installationsanleitung gibt es unter *https://github.com/marazmista/radeon-profile*.

Kommt ein Intel-Grafikchip zum Einsatz, dann installieren Sie das Paket „intel-gpu-tools“. Mit dem Befehl

```
sudo intel_gpu_top
```

erhalten Sie Informationen zur GPU-Auslastung, Taktfrequenz und Leistungsaufnahme.

Htop: Prozesse und Systembelastung

Was auf dem System läuft, lässt sich auf grafischen Desktop mit der exzellenten „Systemüberwachung“ (gnome-system-monitor) herausfinden und unter „Prozesse“ per Klick auf den Spaltenkopf nach CPU-Auslastung oder Speicherbelegung sortieren. Über „Beenden“ oder „Abwürgen“ lassen sich nicht reagierende Prozesse zwangsweise beenden.

Fast noch besser– und im Falle der SSH-Fernwartung alternativlos – ist das Tool htop, das sich über das gleichnamige Paket nachinstallieren lässt. Htop darf als Pflichtinstallation auf jedem Linux-Server gelten. Es lohnt sich, das Tool über „F2 Setup“ sorgfältig einzurichten. „Meters“ betrifft den Kopfbereich mit den Basisinformationen in zwei Spalten. Hier sollten CPU-Auslastung, Speicher, Uptime und ähnlich grundlegende Angaben organisiert werden. Die verfügbaren Infos unter „Available meters“ können mit den angezeigten Funktionstasten in die rechte oder linke Spalte integriert werden. „Columns“ betrifft die eigentliche Taskanzeige. Hier sind annähernd 70 Detailinfos pro Prozess möglich, in der Regel sind „Percent_CPU“, „Percent_MEM“, „Command“) ausreichend und übersichtlich.

Im Alltag sind „F3 Search“ und „F4 Filter“ unentbehrlich, um die Anzeige auf bestimmte Prozesse einzugrenzen. „F9 Kill“ bietet sanfte und harte Kill-Varianten zum Abschuss hängender Tasks.

Ncdu: Datenträgerbelegung

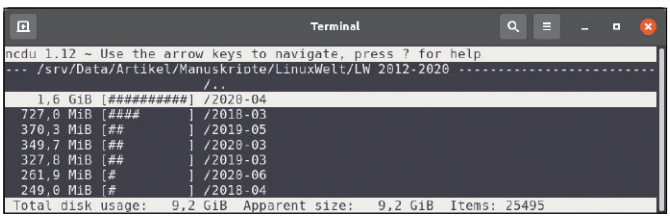
Ncdu sortiert die Verzeichnisse nach der enthaltenen Datenmenge und bietet eine komfortable Festplattenanalyse. Denn ncdu beherrscht wie ein Dateimanager die Navigation zwischen den Verzeichnissen und kann dort auch aktiv löschen. Das Tool ist mittel des Befehls

```
sudo apt install ncdu
```

schnell installiert. Die einzig wichtige Bedienregel ist die Auswahl des Startverzeichnisses. Ist ncdu nämlich einmal gestartet, wird es in keine höhere Verzeichnisebene wechseln. Wer das komplette Dateisystem durchforsten will, sollte ncdu mit

```
ncdu /
```

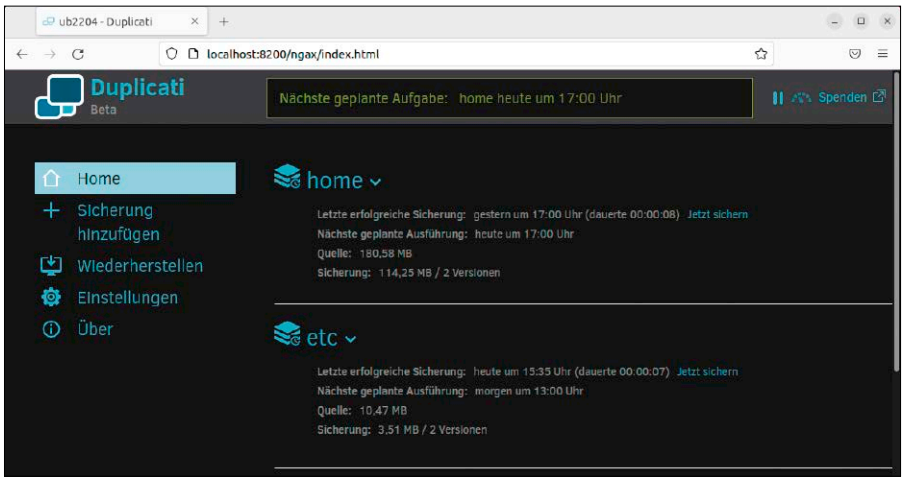
im Wurzelverzeichnis starten. Die Navigation erfolgt mit Cursortasten. Ncdu sortiert automatisch nach Ordnergrößen, kann aber mit Taste „n“ auch nach Namen sortieren, mit „s“ wieder nach Größe. „d“ ist der Löschbefehl mit nachfolgender Löschbestätigung. ■



Verzeichnisgrößen mit „NCurses Disk Usage“: Ncdu ist ein Muss auf SSH-verwalteten Systemen und selbst am Desktop eine Empfehlung.

Tools für Backups und Systemschutz

Datensicherung ist zwar eine eher lästige Aufgabe, aber trotzdem notwendig. Wir stellen Tools vor, mit denen sich Backups besonders komfortabel und sicher erledigen lassen.



Dateien mit Duplicati sichern: Konfiguration und Bedienung erfolgen im Webbrowser. Für Ordner außerhalb von „/home“ muss Duplicati als Dienst gestartet werden.

VON THORSTEN EGGELING

Was man sichern sollte, hängt von der Art der PC-Nutzung ab. In der Regel genügt ein regelmäßiges Backup der Home-Verzeichnisse. Das schützt vor Datenverlust, etwa wenn man eine wichtige Datei versehentlich löscht. Mit einem geeigneten Tool kann man den Vorgang automatisieren. Sind viele Programme und vielleicht noch Serverdienste installiert, empfiehlt sich ab und zu eine Komplettsicherung der Festplatte. Wir stellen Tools vor, mit denen sich ein Abbild des Laufwerks erstellen und bei Bedarf auch auf einer neuen Festplatte wiederherstellen lässt.

Duplicati: Datensicherung (auch im Netz)

Duplicati eignet sich für regelmäßige Backups der persönlichen Dateien. Das Tool unterstützt Sicherungen auf lokalen Laufwerken, über FTP und SFTP sowie Google Drive, Dropbox, Microsoft Onedrive und einige mehr. Fortlaufende Sicherungen erfolgen inkrementell. Duplicati speichert also nur die Änderungen gegenüber dem vorherigen Backup.

Unter *https://www.duplicati.com/download* finden Nutzer von Ubuntu oder Linux Mint ein DEB-Paket, das sich über den Paketmanager der Distribution installieren lässt. Im Terminal verwendet man im Downloadverzeichnis diese Befehlszeile:

```
sudo apt install ./
  duplicati_2.0.6.3-1_all.deb
```

Passen Sie den Dateinamen für neuere Versionen an.

Startet man Duplicati vom Desktop aus, läuft es mit den Rechten des Benutzers. Ein Backup nach Zeitplan wird nur durchgeführt, wenn Sie angemeldet sind und Duplicati gestartet haben. Der Zugriff auf die Weboberfläche erfolgt im Browser über *http://localhost:8200*.

Für Backups von Ordnern, auf die der Standardbenutzer nicht zugreifen darf, muss Duplicati als Systemdienst gestartet werden. Geplante Backups werden dann automatisch im Hintergrund ausgeführt. Den Dienst aktivieren und starten Sie im Terminal mit diesen beiden Befehlen (Ubuntu/Linux Mint):

```
sudo systemctl enable duplicati
sudo systemctl start duplicati
```

Backups konfigurieren: Den Webserver-Port vergibt Duplicati automatisch. Die erste Instanz, die Linux als Systemdienst gestartet hat, erhält den Port 8200. Wird Duplicati zusätzlich manuell gestartet, ist die Oberfläche über Port 8300 erreichbar. Ist der Systemdienst nicht konfiguriert, gilt auch hier die URL *http://localhost:8200*. Per Klick auf „Sicherung hinzufügen“ definieren Sie eine Backupaufgabe mit Hilfe eines Assistenten.

Backup zurücksichern: Nach einem Klick auf „Wiederherstellen“ wählen Sie das gewünschte Backup und danach die Elemente im Dateisystem. Die Dateien lassen sich am ursprünglichen Ort wiederherstellen oder in ein anderes Verzeichnis kopieren. Erfolgt die Wiederherstellung nach einer Linux-Neuinstallation, wählt man die Option „Direkte Wiederherstellung von Sicherungsdateien“.

Tipp: Für ein Backup des eigenen Home-Verzeichnisses etwa auf eine USB-Festplatte genügt folgende Befehlszeile:

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

„[Laufwerks-ID]“ ist die Bezeichnung einer Festplatte, die Linux unter „/media/$USER“ eingebunden hat. Ändern Sie den Pfad entsprechend Ihrer Systemkonfiguration.

Timeshift: Inkrementelles Systembackup

Timeshift (*https://teejeetech.com/timeshift*) erstellt Momentaufnahmen des Dateisystems. Beim Zurückspielen lässt sich der vorherige Zustand wiederherstellen. Als Ziellaufwerk sollte man eine zweite Festplatte verwenden, damit das Backup bei einem Ausfall der Systemfestplatte erhalten bleibt.

Timeshift ist bei Linux Mint bereits vorinstalliert, Ubuntu-Nutzer verwenden im Terminal diese drei Befehle:

```
sudo add-apt-repository -y
 ppa:teejee2008/ppa
sudo apt update
sudo apt install timeshift
```

Nach dem ersten Start wählen Sie als „Schnappschusstyp" die Option „rsync" und geben das Ziellaufwerk und einen Zeitplan an. Die Home-Verzeichnisse sind bei Timeshift standardmäßig ausgenommen, weil bei einer Wiederherstellung sonst die persönlichen Daten überschrieben werden. Die eigenen Dateien sollte man besser mit Duplicati sichern. Dateien und Ordner lassen sich aus dem Timeshift-Backup nach einem Klick auf „Durchsuchen" über den Dateimanager kopieren. „Wiederherstellen" setzt das System auf den gewählten Wiederherstellungspunkt zurück.

Aptik: Backup vor Neuinstallationen

Wer viel Software installiert hat, kann den Aufwand nach der Linux-Neuinstallation oder bei der Einrichtung eines Zweitrechners verringern. Mit einer Liste der installierten Pakete und einem Backup der verwendeten Repositorien lässt sich der vorherige Zustand schnell wiederherstellen. Dabei sollte man – wenn vorhanden – auch Snap- und Flatpak-Pakete nicht vergessen. Weitere Backupkandidaten sind Schriftarten, Desktopthemes, Icons und selbst erstellte Einträge in der Datei „/etc/fstab".

Mit Aptik (*https://teejeetech.com/product/aptik*) lässt sich alles Genannte und noch einiges mehr sichern. Es ist allerdings kostenpflichtig (22 Euro). Eine ältere kostenlose Version für die Kommandozeile lässt sich über *https://github.com/teejee2008/aptik* herunterladen. Es ist aber nicht garantiert, dass es unter aktuellen Distributionen einwandfrei funktioniert.

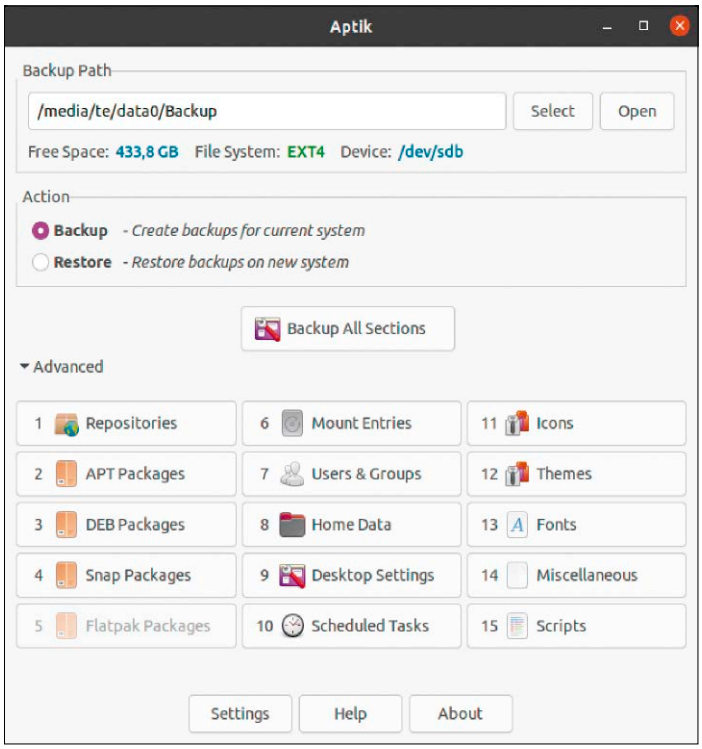
Tipp: Wenn eine Liste mit den manuell installierten Paketen genügt, kann man im Terminal diese Befehlszeile verwenden (Ubuntu/Linux Mint):

```
comm -23 <(apt-mark showmanual |
 sort -u) <(gzip -dc /var/log/
 installer/initial-status.gz | sed
 -n 's/^Package: //p' | sort -u) >
 pkglist.txt
```

Nach der Neuinstallation genügt dann dieser Befehl:

```
sudo apt-get install $(cat pkglist.
 txt)
```

Damit stellt man die Pakete aus der zuvor gesicherten Liste wieder her.



Einstellungen mit Aptik speichern: Das Tool speichert neben den persönlichen Dateien auch die apt-Konfiguration und eine Liste der selbst installierten Pakete.

Rescuezilla: Sicherungskopie der Festplatte

Eine 1:1-Kopie des Festplatteninhalts ist die sicherste Backupmethode. Der Vorgang ist jedoch bei gut gefüllten Laufwerken zeitaufwendig und zwischen den Backups anfallende Änderungen muss man extra sichern. Bei PCs, die als Dateiserver dienen und auf denen sich – außer durch Updates – wenig ändert, kann eine Abbildkopie der Festplatte jedoch sinnvoll sein.

Rescuezilla (*https://rescuezilla.com*) erstellt Imagebackups von Partitionen und ganzen Laufwerken. Die Sicherung lässt sich auf einer USB-Festplatte oder einem Netzwerklaufwerk speichern. Aus der heruntergeladenen ISO-Datei brennen Sie eine DVD oder Sie erstellen einen bootfähigen USB-Stick etwa mit Etcher (*https://etcher.io*) (siehe dazu auch den Artikel ab Seite 22). Nach einem Klick auf „Sichern" geben Sie Quelllaufwerk, Partitionen und Ziellaufwerk an. Hinter „Komprimierungsmethode" wählen Sie „Unkomprimiert". Sie können dann über den von Rescuezilla angebotenen Image Explorer einzelne Dateien oder Ordner aus dem Image extrahieren. Nach einem Klick auf „Wiederherstellen" lässt sich das gesicherte Image wieder auf eine Festplatte kopieren.

Rescuezilla verwendet im Hintergrund Clonezilla (*https://clonezilla.org*). Profis können Clonezilla direkt im Terminal starten und die zusätzlichen Optionen dieses Programms nutzen. ■

Komplettbackup mit Rescuezilla: Das Programm bietet eine übersichtliche deutschsprachige Oberfläche, die Partitionen mit wenigen Mausklicks als Image sichert.

Die besten Netzwerktools

Was man für Netzwerk und Web zwingend benötigt, ist bei allen Linux-Distributionen vorinstalliert. Die hier empfohlenen Werkzeuge erweitern aber die Möglichkeiten und den Bedienkomfort und bringen Windows besser ins Linux-Biotop.

VON HERMANN APFELBÖCK

Die nachfolgenden Tools konzentrieren sich auf die Interaktion zwischen Rechnern im Netzwerk, auf Router- und Gerätekontrolle sowie Download und Datenaustausch. Der Aspekt der Netzwerksicherheit bleibt hier unberücksichtigt – mit Verweis auf den weiteren Heftschwerpunkt „Sicherheit & Datenschutz".

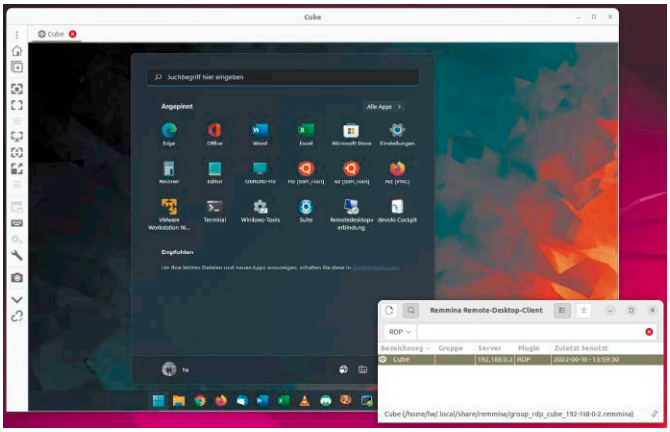
Remotedesktop-Lösungen

Remoteverbindungen mit einem entfernten Linux- oder Windows-Desktop sind sicher die komfortabelste Art, um dort – ohne den aktuellen Arbeitsplatz verlassen zu müssen – eine Software zu verwenden, einen Download zu absolvieren oder die Konfiguration zu kontrollieren. Je nach Zugriffsrichtung sind folgende Werkzeuge zu empfehlen:

Von Linux/Windows auf Windows: Die Serverkomponente des Remotedesktops fehlt in Windows Home und ist nur in der Pro-Version enthalten. Ist dies der Fall, kann sich jedes Windows (auch Home) mit der Clientkomponente „Remotedesktopverbindung" (mstsc.exe) verbinden, jedes Linux mit Remmina. Remmina („Betrachter entfernter Schreibtische") ist in vielen Distributionen vorinstalliert und ermöglicht den Zugriff auf das Windows-RDP-Protokoll. Falls Remmina fehlt, hilft diese Nachinstallation:

```
sudo apt install remmina remmina-
  plugin-rdp
```

In Remmina klicken Sie auf die „+"-Schaltfläche und tippen hinter „Bezeichnung" einen aussagekräftigen Namen für die Verbindung ein. Hinter „Protokoll" stellen Sie „RDP" ein.



Remotedesktop mit Remmina: Der bewährte Zugriffsclient verbindet sich zu Linux- und Windows-Rechnern mit Desktopfreigabe.

Bei „Server" tragen Sie die IP-Adresse des Windows-Rechners ein, bei „Benutzername" und „Benutzerpasswort" die Anmeldedaten für das Windows-System.

Von Linux/Windows auf Linux: Hier empfehlen wir das Tool X2go (*https://wiki.x2go.org*). Nähere Erläuterungen zu X2go finden Sie im Heftbeitrag ab Seite 92. Wenn auf einem Linux-Server X2go läuft, kommt allerdings nur der X2go-Client (für Linux, Windows, Mac-OS) in Betracht. Remmina ist nicht kompatibel.

SSH und Putty für Linux/Windows

Schlichtes SSH ist der Standard beim Fernzugriff auf Linux-Systeme und benötigt auf Serverseite nur die Installation des OpenSSH-Servers:

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

Die Clientkomponente („ssh") bringt jedes Linux-System standardmäßig mit.

Putty (siehe *www.putty.org* für die Windows-Variante sowie gleichnamiges Paket „putty" in allen Linux-Paketquellen) verdankt seine Popularität dem Umstand, dass es unter Windows jahrzehntelang keine Alternative gab, um sich mit SSH-Servern zu verbinden. Das Tool bietet nach etwas Gewöhnung eine komfortable Verwaltung mehrerer SSH-Server. Unter Linux liegt es im Ermessen des Benutzers, das standardmäßige ssh im Terminal oder Putty zu verwenden.

Die Basiskonfiguration ist einfach: Sie geben unter „Host Name" die IP-Adresse des Servers an. Mit „Connection type: SSH" und dem vorgegebenen Standardport 22 können Sie sich mit „Open" bereits verbinden. Für häufigeren Zugriff lohnt es sich, unter „Saved Sessions" eine aussagekräftige Bezeichnung zu verwenden und diesen Server mit „Save" dauerhaft zu speichern. Unter „Window → Translation → Remote character set" sollten Sie immer den Eintrag „UTF-8" wählen, mit „Window → Colors" (sowie „Fonts") bestimmen Sie Erscheinungsbild und Schriftgrößen.

Alternativlos ist Putty auch unter Windows nicht mehr: Das elegantere Smartty (*https://sysprogs.com/SmarTTY/*) hat eine einfache Serververwaltung, startet mehre-

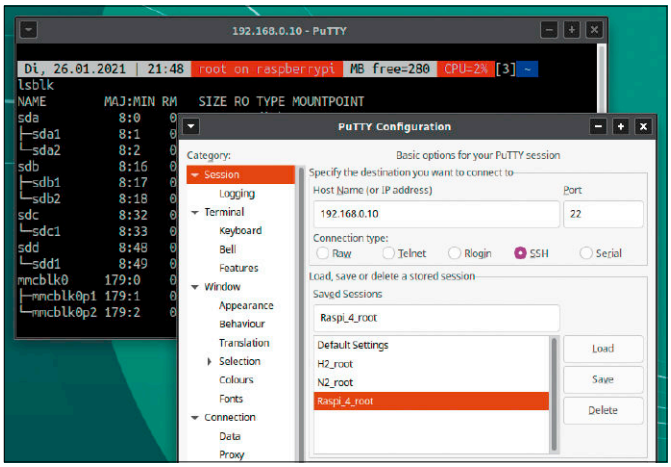
re SSH-Konsolen in Tabs und bringt einen komfortablen Texteditor, einen Keygenerator und Xming für grafische Programme mit. Neben dem normalen Terminal gibt es wahlweise das „Smart Terminal“, das das aktuelle Verzeichnis grafisch darstellt und den Ordnerwechsel per Mausklick erlaubt. Das „Smart Terminal“ beherrscht das Editieren von Textdateien per Doppelklick und bietet grafische Autocompletion für Befehls- und Dateinamen.

Termius: SSH-Client für Android und iOS

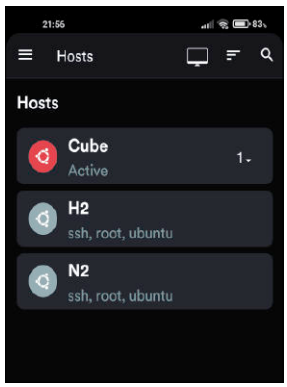
SSH-Terminals für Smartphones und Tablets gibt es etliche, die sich funktional nicht viel nehmen. Daher entscheiden Übersichtlichkeit und Anpassungsfähigkeit – und hier ist das englischsprachige Termius mit der beste Kandidat. Die App gibt es für Android und iOS. Unter „Host“ legen Sie mit dem Plus-Zeichen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

Midnight Commander: SSH-Datenaustausch

Natürlich hat der Midnight Commander (MC) einen Klassikerstatus als generelles Systemtool und ist auch am grafischen Desktop eine Empfehlung. Wir führen ihn hier dennoch als Netzwerktool, weil er bei der SSH-Fernwartung als quasi-grafischer Dateimanager unentbehrlich ist. Besonderes Netzwerk-Highlight ist der direkte SSH/SFTP-Datenaustausch. Der MC beherrscht SFTP über die Option „Shell-Verbindung“ in den Menüs „Links/Rechts“. Wie bei SSH auf der Kommandozeile geben Sie hier die IP-Adresse an, optional mit dem gewünschten User, also etwa „root@192. 168.0.10“, gegebenenfalls auch mit abweichender Portangabe „root@192. 168.0.10: 4444“. Nach Eingabe des Kennworts zeigt der Midnight Commander in einer Fensterhälfte das Dateisystem des Servers, in der anderen das des zugreifenden Clientsystems. **Tipp:** Auch Windows ist von dieser Option nicht mehr ausgeschlossen, sofern dort das WSL (Windows Subsystem for Linux) und dort wiederum der Midnight Commander installiert ist.



Putty für Windows und Linux: Unter Windows ist dieser SSH-Client der Klassiker, unter Linux eher optional. Putty ist nicht immer intuitiv, aber funktional unumstritten.



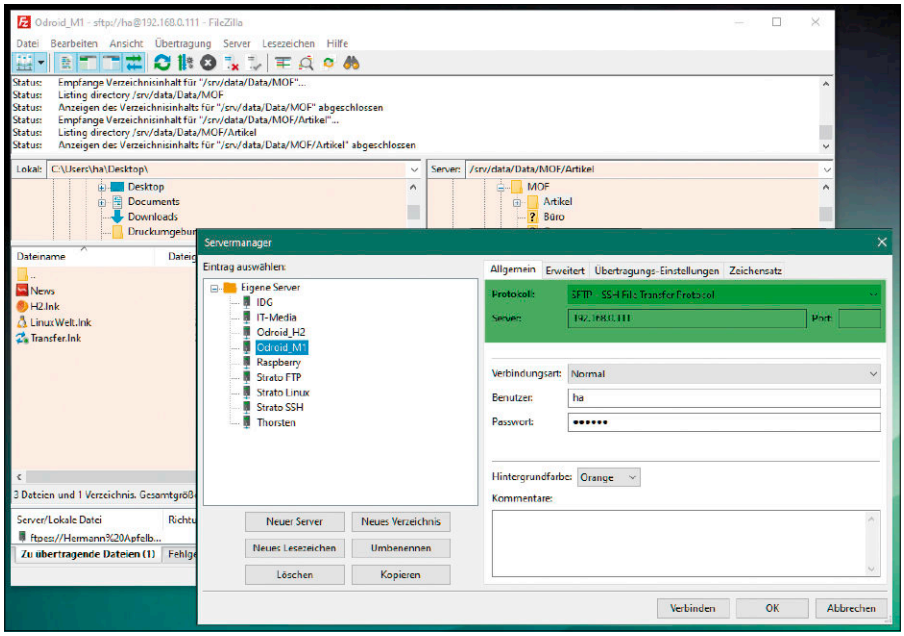
SSH-Client Termius für Android und iOS: Die englischsprachige App verwaltet beliebig viele Server übersichtlich und optisch ansprechend.

Filezilla: Für FTP und SSH (SFTP)

Linux-Dateimanager können über die Option „Mit Server verbinden“ oder auch per Direktadresse (etwa „sftp://192.168. 178.12“ für den SFTP-Zugriff per SSH) mit SSH- und FTP-Servern umgehen. Trotzdem ist auch unter Linux ein spezialisiertes FTP- und SFTP-Programm mit eigener Serververwaltung einfach komfortabler. Filezilla liegt bei allen Distributionen in den Paketquellen und ist mit

```
sudo apt install filezilla
```

schnell nachinstalliert.
Während Filezilla unter Linux nur ein Komforttool darstellt, ist es fast ein Muss auf



Ideale Ergänzung für Windows, das mit Linux kommuniziert: Filezilla beherrscht den Zugriff über SSH (SFTP).

Windows-Systemen, die mit FTP- und mit SSH-Servern arbeiten: Statt des mühsamen Dateiaustauschs über das Putty-SSH-Terminal ist ein SSH-Server in Filezilla mit IP-Adresse, Port (Standard 22) und SFTP-Protokoll und den Zugangsdaten schnell eingerichtet und ermöglich dann die direkte Datenübertragung zwischen Windows und dem Linux-Rechner.

Nmap: Netzübersicht & Kontrolle

Was früher allenfalls Firmen-Admins beschäftigt hat, wird auch in heutigen Heimnetzen zum Anliegen: Was läuft in meinem Netz gerade alles - und gehört das alles tatsächlich zu meinem Netz? Hier hilft entweder der Router oder das Tool nmap. Nmap ist in der Regel nicht vorinstalliert, aber mit dem Paketnamen „nmap“ in allen Repositorys erhältlich. Folgendes nmap-Kommando

```
nmap -sP 192.168.178.*
```

schickt Ping-Anfragen an alle 255 Adressen des Adressraums. Der schnelle Ping-Scan zeigt dann alle laufenden Netzgeräte mit Hostnamen und IP-Adresse.

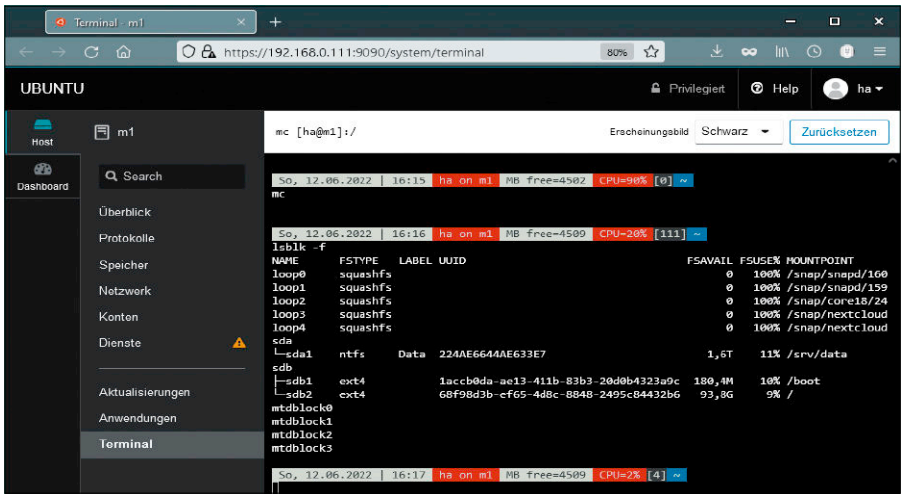
Ohne Ping-Parameter („-sP“) macht nmap sorgfältige und zeitaufwendige Portscans: Sie erhalten zu jedem Rechner Hostnamen, IP-Adresse, MAC-Adresse und die Liste aller offenen Ports. Ist der intensive Vorgang für den gesamten lokalen Adressraum zu langwierig, lässt sich auch ein einzelner PC befragen (*nmap 192.168.178.10*).

Cockpit: Server im Blick

Der Verfasser dieses Beitrags ist kein Fan von zusätzlichen Serverdiensten, die letztlich keinen Mehrwert gegenüber dem schlichten SSH-Netzzugriff einbringen. Per SSH verbinden und dann am Zielrechner Tools wie htop oder inxi starten, ist meist der sparsamere und flexiblere Weg für eine Serverkontrolle im Vergleich zu einem Webserver. Cockpit ist dennoch eine Empfehlung, weil es nicht nur hübsch ist, sondern mit seinem eingebauten Terminal einen SSH-Server weitgehend ersetzen kann (allerdings nicht dessen Dateiprotokoll SFTP). Cockpit ist überall verfügbar und unter Ubuntu mit

```
sudo apt install cockpit
```

bequem installiert. Der Webserver ist damit sofort aktiv und im Netz mit jedem Browser über die Adresse „[IP-Adresse]:9090“ zu erreichen. Melden Sie sich mit einem beliebigen, auf dem Serversystem vorhandenen



Kontrolle plus Systemwartung: Der Cockpit-Webserver hat eine gefällige Oberfläche und bringt sein eigenes Terminal mit.

Benutzerkonto an. Auf der Startseite hält Cockpit eine Reihe von Informationen parat. In der grafischen Auswertung sehen Sie die CPU- und Speicherauslastung, Schreib- und Lesevorgänge der Laufwerke und den aktuellen Netzverkehr. Außerdem stellt Cockpit die Daten zum verwendeten Betriebssystem, Rechnernamen und eventuell verfügbaren Updates zusammen. Zusätzlich bietet Cockpit ein Terminal, um wie bei SSH auf der Kommandozeile zu arbeiten.

Cockpit überwacht auch mehrere Systeme parallel. Voraussetzung dafür ist, dass dort ebenfalls Cockpit installiert ist.

Stimmen die Voraussetzungen, ist es einfach, einen weiteren Server aufzunehmen. Dazu wechseln Sie in das „Dashboard“. In der kleinen Liste am unteren Bereich genügt ein Klick auf das Pluszeichen, um danach die IP-Adresse des nächsten Systems einzutragen.

Fritzbox-Tools: Router per Kommandozeile

Die fb_tools (Fritzbox-Tools) sind eine umfangreiche Sammlung von PHP-Scripts zur Steuerung der Fritzbox über Terminalbefehle. Je nach Befehl kann man Infos aus der Fritzbox auslesen, Konfigurationsbackups anlegen und Einzelfunktionen von außen starten. Die Fritzbox-Tools können nicht mehr als das, was ein zutrittsberechtigter Fritzbox-Nutzer auch in der Konfigurationsoberfläche erledigen kann, aber damit lassen sich Informationen wie die öffentliche IP-Adresse oder der Onlinezähler in zwei Sekunden auslesen.

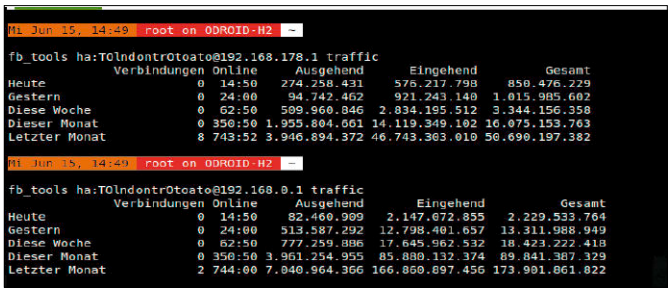
Da PHP unter Linux vorliegt, genügt für Debian/Ubuntu-basierte Distributionen der Download des DEB-Pakets „fb-tools.deb“ von *www.mengelke.de/Projekte/FritzBox-Tools* und die Installation im Terminal:

```
sudo dpkg -i fb-tools.deb
```

Es gibt einige einfache „Modes“, die ohne Benutzerauthentifizierung sofort Antworten liefern:

```
fb_tools boxinfo
fb_tools systemstatus
fb_tools getip
```

Damit erhalten Sie die Basisdaten über Modell, Hardwarerevision, Provider, Laufzeit, Neustarts und die öffentliche IP-Adresse. Alle wirklich interessanten Funktionen setzen aber eine Anmeldung voraus, die dem eigentlichen Befehl einfach mitgegeben wird:



Hübscher Fritzbox-Vergleich: Ein Rechner in mehreren Netzen erreicht mit den Fritzbox-Tools alle Fritzbox-Router und kann – wie hier – deren Traffic-Statistiken gegenüberstellen.

```
fb_tools sepp:Geh3im@fritz.box
  anrufliste
```

Mit dieser Syntax und somit korrekter Anmeldung sind aber auf jüngeren Fritzboxen immer noch nicht sämtliche Funktionen realisierbar. Die Lösung dafür liegt in der Fritzbox-Konfiguration unter „System → Fritz!Box-Benutzer → Zusätzliche Bestätigung → Ausführung bestimmter Einstellungen und Funktionen zusätzlich bestätigen". Die Option ist standardmäßig aktiviert und verhindert einige Kommandos der Fritzbox-Tools. Es ist Ermessensfrage, ob man dies dauerhaft abschalten will. Danach sind etwa folgende Aktionen möglich:

```
fb_tools […] traffic
```

Der Mode „traffic" gibt die Daten aus, die in der Konfigurationsoberfläche unter „Internet → Online-Monitor → Online-Zähler" zu finden ist.

```
fb_tools […] led off
fb_tools […] reconnect
```

Diese beiden Kommandos schalten die LED-Leuchten aus und machen eine Neuverbindung zum Provider.

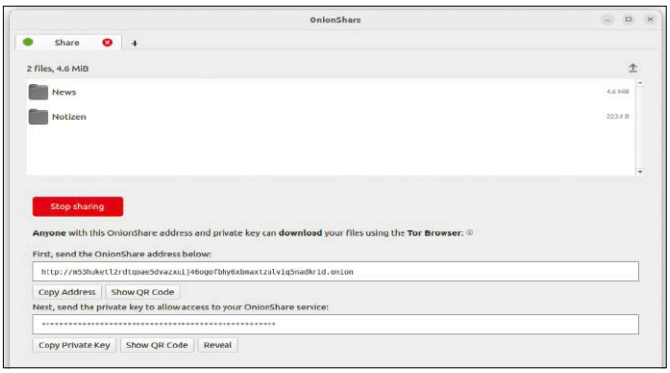
Onionshare: Abhörsicherer Datenaustausch

Der Datenaustausch via Internet erfolgt in der Regel über eine Zwischenstation (HTTP, FTP, SSH, Cloud). Die Kombination des Austauschtools Onionshare mit dem TOR-Browser (*www.torproject.org*) erlaubt hingegen eine verschlüsselte Direktverbindung zwischen Sender und Empfänger. Onionshare gibt es für Linux, Windows und Mac-OS auf der Projektseite *https://onionshare.org/*. Die empfohlene Installationsweise für Ubuntu und Derivate ist das Snap-Format:

```
sudo snap install onionshare
```

Ein klassisches DEB-Paket ist in den Paketquellen zwar ebenfalls verfügbar, aber mindestens unter Ubuntu 22.04 fehlerhaft.

Die Bedienung von Onionshare ist einfach: Sie fügen unter „Share Files" die Dateien ein, die Sie weitergeben wollen. Onionshare startet dann auf dem Sender-PC einen temporären Webserver mit einer temporären Darknet-URL „http://[...].onion/[...]". Diese URL teilen Sie per Mail oder Telefon dem Empfänger mit. Dieser muss den TOR-Browser benutzen (oder das Livesystem Tails, das diesen vorkonfiguriert enthält), um die Adresse zu erreichen. Mit Schließen von Onionshare auf dem Sender-PC wird die Verbindung getrennt und die temporäre Darknet-URL verfällt wieder. Ungeachtet des zweifelhaften Darknet-Umfelds darf Onionshare zu den abhörsichersten Transfermethoden zählen.



Datenaustausch mit Onionshare: Der Transfer läuft verschlüsselt und direkt über einen temporären Webserver mit temporärer Darknet-Adresse.

Qbittorrent: Zentraler Torrent-Client

Downloads über das Torrent-Protokoll entlastet HTTP-Server und ist auch beim Bezug von Linux-Distributionen oft die erwünschte, zum Teil die einzige Downloadoption. Wer mehrere Rechner hat (Linux, Windows, Tablet) sucht dann auf jedem System ein passendes Torrent-Tool – und davon gibt es viele. Einfacher ist ein zentraler Bittorrent-Client, den alle Netzgeräte im Browser nutzen. Das Tool Qbittorrent ist mit

```
sudo apt install qbittorrent-nox
```

sofort aus den Paketquellen geholt. Als Server genügt jeder kleine Platinenrechner. Nach dem Start des Tools (*qbittorrent-nox*) ist der Server über „[IP-Adresse]:8080" mit jedem Browser im Netz erreichbar.

Der Zugang erfolgt zunächst als Benutzer „admin" mit Passwort „adminadmin". Kennwort und Zugriffsport können Sie in der Oberfläche unter „Werkzeuge → Optionen" ändern.

Wichtig ist es unter „Geschwindigkeit", bei „Herunterladen" auf „0" zu setzen, um das maximale Downloadtempo zu erzielen. Jeder Teilnehmer im Netz, der IP-Adresse und Zugangspasswort kennt, kann in der Qbittorent-Oberfläche mit „Datei → Torrent-Datei hinzufügen" eine Torrent-Datei zum Server hochladen und somit den Download auslösen. Idealerweise ist das Downloadverzeichnis per Samba freigegeben und für alle erreichbar.

Alternativer Tipp: Das Terminaltool aria2 beherrscht neben HTTP und FTP auch Torrent-Downloads. Aria2 kann von verschiedenen URLs oder über mehrere Verbindungen herunterladen.

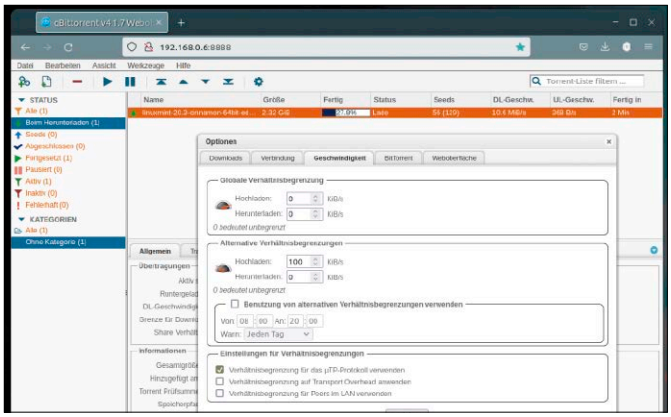
Interessant ist auch die Fähigkeit, Downloads jederzeit zu unterbrechen und später fortsetzen zu können. Das Werkzeug ist aus den Paketquellen mit

```
sudo apt install aria2
```

zu installieren. Als Kommandotool dient aria2c, das den Download nach

```
aria2c https://[seite.com]/
  [name..].torrent
aria2c name.torrent
```

sowohl von Torrents aus dem Web oder von lokal vorliegenden Torrent-Dateien startet. Im Prinzip genügt statt Qbittorrent auch dieses kleine Tool als zentraler Torrent-Downloader auf einem System mit SSH-Server. ■



Der Qbittorrent-Server ist im Netzwerk mit jedem Browser zu erreichen. Die Konfigurationsoptionen muss man nur einmal absolvieren.

Die besten Desktop-Tools

Die nachfolgende Toolsammlung ist eine sorgfältige Auswahl spezialisierter Software, die wir teils generell, teils für bestimmte Zielgruppen oder Desktops empfehlen. Nicht jedes Tool eignet sich für jeden, aber jedes ist eine produktive Perle.

VON HERMANN APFELBÖCK

Bei den hier vorgestellten Tools für den Desktop handelt es sich um Ergänzungen, die standardmäßig nicht installiert sind und eine kleine, spezielle Aufgabe vorbildlich erledigen. Wie in den voranstehenden Beiträgen bleiben auch hier große Anwendungen wie Browser oder Office außen vor. Um den Wert der Tools zu vermitteln, gehen wir so weit in die praktische Tiefe, dass das Potenzial deutlich wird und schnelle Benutzung sofort nach der Installation möglich ist.

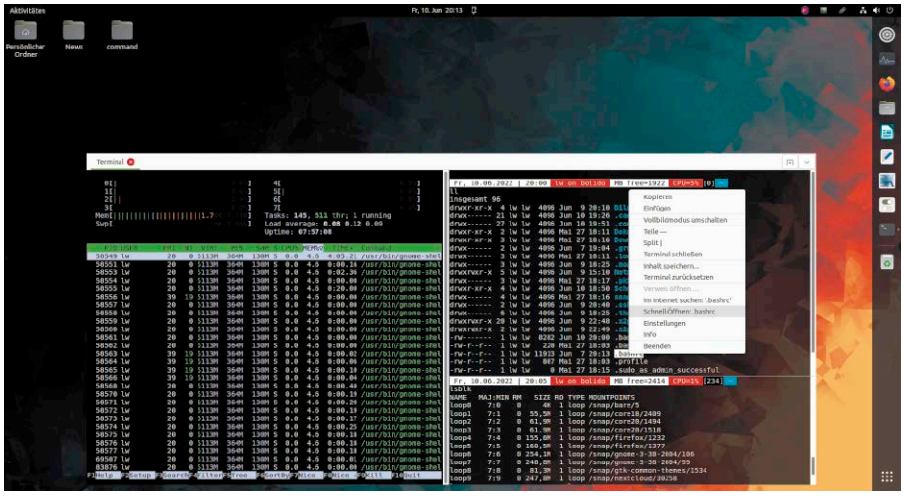
Guake: Terminal per Knopfdruck

Bei vielen Nutzern muss am Linux-Desktop immer ein Terminal zur Hand sein. Hier ist Guake eine nützliche Ergänzung (besser als das ähnliche Tilda). Das Drop-down-Terminal hat kein skalierbares Fenster, sondern blendet sich in fester, aber beliebig einstellbarer Größe nach Hotkey F12 ein und aus. Dieser und viele weitere Hotkeys sind individuell konfigurierbar. Automatisches Ausblenden kann auch bei Fokusverlust eingestellt werden, also durch beliebigem Klick außerhalb des Terminals. Diese Option sollte man aber erst aktivieren, wenn alle Guake-Einstellungen optimal sind.

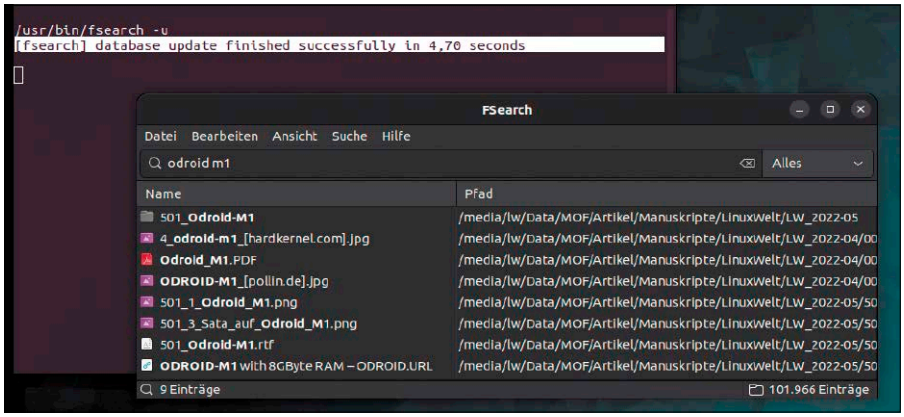
Die Guake-Einstellungen (Rechtsklick in Guake-Fenster und „Einstellungen“) bieten Transparenz, diverse Farbschemata, Shell-Tabs und vieles mehr. Für den automatischen Start bei der Anmeldung ist die Option „Allgemein → Guake bei der Anmeldung starten“ zuständig. Im Fenster läuft die Bash – alle Bash-Einstellungen werden also übernommen. Das Fenster bietet bei Rechtsklick vertikale und horizontale Fenstersplits, erlaubt jede Positionierung und jederzeit den Vollbildmodus per Hotkey. Guake ist über den gleichnamigen Paketnamen mit

```
sudo apt install guake
```

schnell installiert. Der zusätzliche guake-indicator für die Systemleiste ist optional.



Das Permanentterminal Guake bietet opulente Anpassung – und verschwindet, wenn man es nicht braucht.



Elegante Dateisuche mit Fsearch: Suche und Einstellungen sind mit der komfortablen Oberfläche zu erledigen. Die Aktualisierung der Dateiliste erfolgt am besten per Cronjob.

Fsearch: Schnelle Dateisuche

Fsearch ist ein Suchtool für Dateinamen (keine Dateiinhalte), das auf Basis einer Dateiliste wesentlich schneller arbeitet als eine Dateisuche im Dateimanager. Es liefert passende Ergebnisse ab dem ersten einge-

tippten Buchstaben und ein Klick auf eine Datei öffnet diese in der Standardanwendung. Standardmäßig gilt einfache Und-Syntax, wenn Sie mehrere Suchwörter eingeben. Die Einrichtung unter Ubuntu/Mint erfolgt über ein PPA:

```
sudo add-apt-repository
 ppa:christian-boxdoerfer/
 fsearch-daily
sudo apt update
sudo apt install fsearch
```

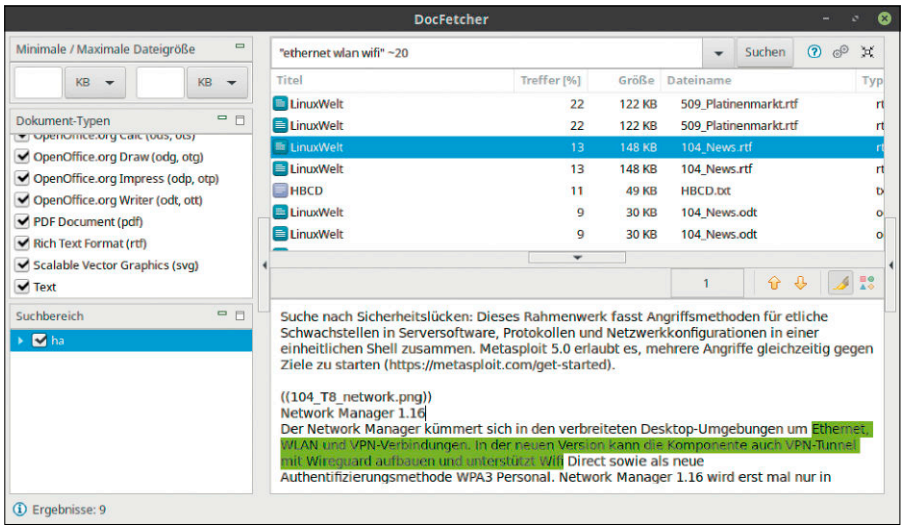
Im gestarteten Programm stellen Sie unter „Bearbeiten → Einstellungen → Datenbank“ die gewünschten Pfade ein, da zunächst nur das Home-Verzeichnis eingetragen ist. Damit die Suche stets aktuelle Ergebnisse liefert, sollte die Dateiliste regelmäßig aktualisiert werden. Dies können Sie jederzeit manuell erledigen („Datei → Datenbank aktualisieren“). Eleganter ist es, die Datenliste periodisch über den Befehl

```
fsearch -u
```

zu aktualisieren, am besten wie hier

```
0 */4 * * * /usr/bin/fsearch -u
```

in einer Cronjob-Zeile angefordert werden (hier alle vier Stunden).



Schnell, zuverlässig und unkompliziert: Für die Suche nach Textinformationen aller Art ist der plattformunabhängige Docfetcher erste Wahl.

Docfetcher: Suche nach Dateiinhalten

Dateimanager oder Tools wie Fsearch suchen nur nach Dateinamen. Wer viel mit Texten zu tun hat, braucht ein zusätzliches Werkzeug wie Docfetcher. Es leistet Volltextsuche für Office-, PDF-, Epub-, HTLM- und Textdateien. Docfetcher erfordert eine Java-Runtime (*sudo apt install default-jre*) und das Tool selbst erhalten Sie unter *http://docfetcher.sourceforge.net*. Entpacken Sie die ZIP-Datei in Ihr Home-Verzeichnis. Eine Installation ist nicht nötig: Sie starten Docfetcher einfach mit dem enthaltenen Script „Docfetcher-GTK3.sh“.

Um den Suchindex zu erstellen, klicken Sie mit der rechten Maustaste in das leere Feld unter „Suchbereich“ und gehen im Menü auf „Index erstellen aus → Ordner“. Wählen Sie den Ordner mit den Dateien aus, die Sie durchsuchen wollen. Ein Klick auf „OK“ startet dann die Indexierung. Im späteren Betrieb bemerkt der laufende Docfetcher geänderte oder neue Dateien automatisch und nimmt sie in den Index auf. Sie können die Aktualisierung aber auch manuell auslösen, indem Sie den oder einen Eintrag im Suchbereich markieren und nach Rechtsklick auf „Aktualisieren“ gehen.

Zur Suche tippen Sie oben im Suchfeld ein Wort ein und klicken auf „Suchen“. Mehrere durch Leerzeichen getrennte Begriffe verknüpft Docfetcher mit logischem „OR“. Sie können das durch ein explizites „AND“ ändern. Stehen die Begriffe wie hier

```
"Linus Torvalds"
```

in Anführungszeichen, wird nach dieser exakten Wortfolge gesucht. Mit der Nachbarschafts-Suche

```
"Ubuntu Nautilus" ~20
```

sucht Docfetcher Texte mit diesen Wörtern, die bis zu 20 Wörter voneinander entfernt vorkommen dürfen.

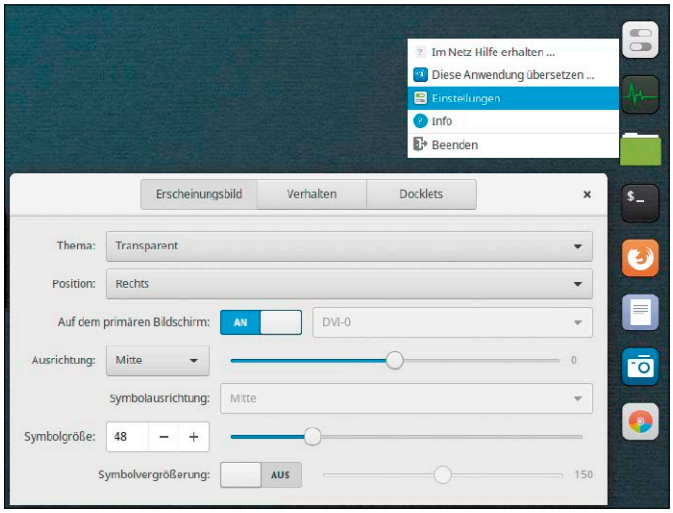
Plank: Das Favoritendock

Die Systemleisten vieler Linux-Desktops lassen sich zum Favoritenstarter ausbauen. Abgesehen vom Favoritendock in Ubuntu Gnome und vielleicht noch der „Gruppierten Fensterliste“ in Cinnamon ist aber fast überall das Plank-Dock einfacher und schicker. Plank ist im Terminal mit

```
sudo apt install plank
```

schnell installiert. Damit das Dock dauerhaft läuft, müssen Sie es unter „Systemeinstellungen → Startprogramme“ mit dem Befehl „plank“ als Autostart einrichten. Die Konfiguration des Docks (Position, Symbolgröße, Thema, Ausblendverhalten) erreichen Sie durch Drücken der Taste Strg und Rechtsklick auf ein beliebiges Dockicon: Im Kontextmenü erscheint der Eintrag „Einstellungen“ und das Dock kann dann unter „Erscheinungsbild“ positionell, optisch und größentechnisch angepasst werden.

Neue Favoriten legen Sie ganz einfach dadurch an, dass Sie das gewünschte Programm starten, auf dessen Symbol im Dock rechtsklicken und die Option „Im Dock behalten“ wählen. Einen nicht mehr



Attraktiv und einfach: Das Plank-Dock ist als Favoritenstarter den meisten Lösungen über die Systemleiste klar vorzuziehen.

benötigten Starter ziehen Sie einfach vom Dock auf den Desktop. Positionsverschiebungen sind per Drag & Drop ebenfalls intuitiv. Mit Strg-Taste und Linksklick starten Sie eine weitere Instanz eines bereits laufenden Programms – wichtig etwa für Terminal oder Dateimanager.

Zim: Notizblock und Mini-Wiki

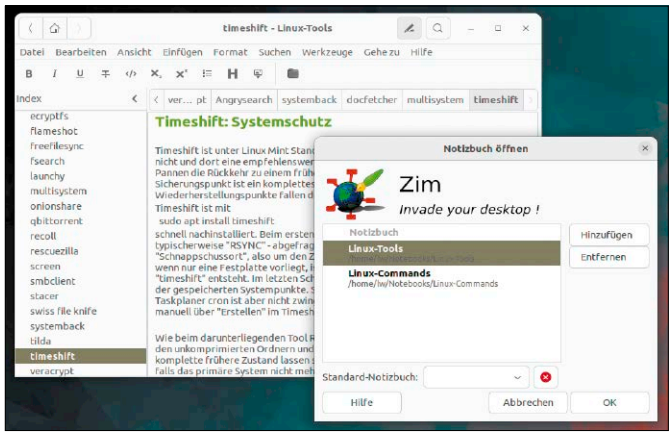
Zim (*https://zim-wiki.org*) ist ein interessanter Mittelweg zwischen einfachen lokalen Notizen wie Tomboy und aufwendigeren Wiki-Lösungen wie Dokuwiki oder Mediawiki auf Basis eines Apache/Nginx-Servers. Ein Wiki ist es nicht, weil neue Seiten nur auf dem lokalen Rechner und somit in der Praxis von einem Nutzer angelegt werden können. Jedoch kann der eingebaute Webserver die Notizen für den Lesezugriff im Netzwerk anbieten. Zim liegt in den meisten Standard-Paketquellen und ist mit

```
sudo apt install zim
```

schnell installiert. Das komplett deutschsprachige Tool beherrscht reichhaltige Formatierungs- und Darstellungsoptionen, Bilder, Tabellen und Weblinks, ist aber in der Basisbedienung kinderleicht. Zuerst erstellen Sie ein Notizbuch und in der Navigationsspalte dann die einzelnen Seiten oder Unterseiten. Sobald Sie bei einer vorhandenen „Seite“ eine „Neue Unterseite“ anfordern, wird diese zur Kategorie und intern von einer Datei zu einem Ordner umgewandelt. Diese Struktur wird im Dateisystem unter „~/Notebooks/[...]“ durch Ordner und Textdateien abgebildet. Mit „Suchen → Notizbuch durchsuchen“ gibt es eine schnelle, indexbasierte Suchfunktion für die komplette Sammlung.

Für eine Freigabe der Sammlung im lokalen Netz verwenden Sie „Werkzeuge → Webserver starten“. Die Sammlung ist dann mit jedem Browser über die IP-Adresse des Zim-Rechners und Standardport 8080 zu erreichen. Dabei muss die Option „Öffentlichen Zugriff erlauben“ aktiviert werden, obwohl es sich nur um die Freigabe im lokalen Netz handelt. Externe Dateiinhalte wie Bilder zeigt der Browser nur dann an, wenn diese am Zim-System im Notizbuch-Ordner unter „~/Notebooks/[Notizbuchname/[...]“ abgelegt sind.

Interessant für den Aufbau eines Mini-Wikis ist die Tatsache, dass sich pure Textdateien einfach nach „~/Notebooks/[Notizbuchname]“ kopieren lassen und dann zum Zim-Inhalt werden. Dazu braucht es nur



Desktop-Wiki Zim mit eingebautem Webserver: Zim ist eine funktionsreiche, aber einfach bedienbare Notizensammlung mit Server, die alle Inhalte im Netzwerk anbietet.

einen Standardheader, der sich von einer bereits vorhandenen Notizseite übernehmen lässt. Ein Massenimport ist nicht vorgesehen, aber mit einer Konstruktion wie hier angedeutet

```
for FILE in `ls -A *.txt`; do cat
  header $FILE > ~/Notebooks/
  [Kategorie]/$FILE;done
```

leicht zu erzielen (der „header“ muss als Datei vorliegen).

Autokey: Globale Textbausteine

Autokey ermöglicht systemweite Textbausteine für alle Programme. Das Tool liegt in den Standard-Paketquellen und lässt sich über die Anwendungsverwaltung oder auf der Kommandozeile

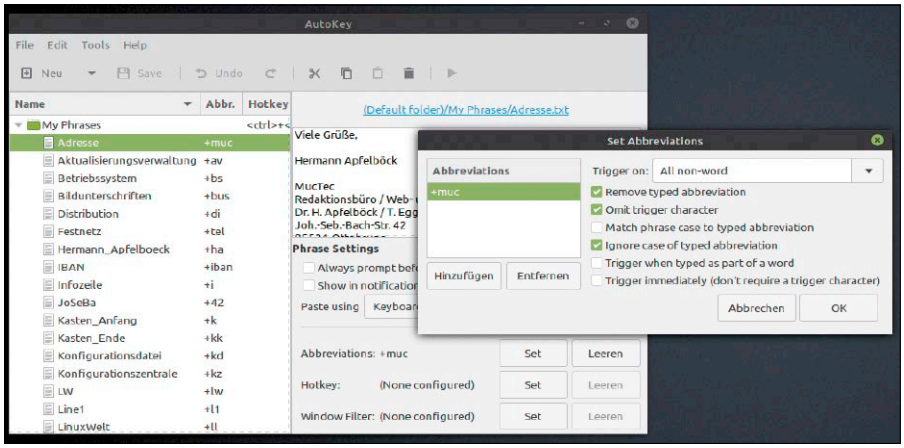
```
sudo apt install autokey-gtk
  autokey-common
```

nachrüsten (unter KDE und LXQT „autokey-qt“ statt „gtk“). Autokey funktioniert nur unter Xorg, nicht unter Wayland, was insbesondere jüngeres Ubuntu Gnome und Fedora ausschließt. Abhilfe bietet entweder die Rückkehr zu Xorg oder der Einsatz des ähnlichen Tools Espanso, das allerdings noch nicht die Reife von Autokey besitzt.

Für Autokey sorgen Sie zuerst unter „Systemeinstellungen → Startprogramme“ (oder ähnlich) für den automatischen Start des Programms autokey-gtk (oder autokey-qt). Dann wird es bei jeder Anmeldung geladen und erscheint in der Systemleiste.

In der Konfiguration finden Sie im linken Bereich unter „My Phrases“ einige Beispiele. Mit „Neu → Phrase“ legen Sie einen neuen Eintrag an. Dabei vergeben Sie einen Namen wie etwa „IBAN“ und bestätigen mit „OK“. Der Name hat nur organisatorische Funktion. Im Editorfenster rechts oben steht „Enter phrase contents“, was Sie nun durch den gewünschten Text ersetzen – etwa mit Adresse oder Ihrer IBAN-Nummer. Der Text kann ein Wort, ein Satz, ein komplette Adresse oder mehrere Textabsätze umfassen.

Die weitere Konfiguration eines Textbausteins findet im Bereich unter dem Editorfenster statt: Typischerweise soll eine knappe Eingabe den Textbaustein auslö-



Autokey-Textbaustein mit empfohlenen Einstellungen: Aus der Eingabe „+muc“ und einer Triggertaste (Tabulator, Leertaste) wird die volle Adresse – in jedem Editor, Mailprogramm oder Webdienst.

sen – etwa „+iban“ für die IBAN-Nummer. Dazu klicken Sie neben „Abbreviations“ auf „Set“. Im Unterdialog „Set Abbreviations“ wählen Sie „Hinzufügen“ und geben „+iban“ ein. Ein für alle Bausteine verwendetes zusätzliches Sonderzeichen wie „+“ stellt sicher, dass Sie die Kürzel nicht unabsichtlich auslösen.

Quittieren Sie das Kürzel mit der Eingabetaste. Rechts daneben definieren Sie den Auslöser („Trigger on:“). Mit „All non word“ löst jedes Sonderzeichen wie Leerzeichen, Eingabetaste, Tabulator, Punkt oder Bindestrich den Textbaustein aus. Weitere wichtige Optionen dieses Dialogs sind „Remove typed abbreviation“ und „Omit trigger character“. Beides sollten Sie immer aktivieren, damit Eingabekürzel und Auslöserzeichen (etwa Leerzeichen oder Tabulator) gelöscht werden. Ist alles definiert, klicken Sie auf „OK“ und im Hauptdialog auf „Save“. Neue Kürzel sind sofort aktiv.

Eine ansehnliche Liste von Bausteinen ist nicht in wenigen Minuten zu haben, aber diese Investition lohnt sich, zumal sich angelegte Bausteine auch auf andere Rechner übertragen lassen. Dazu kopieren Sie einfach den Ordner „~/.config/autokey/data“ an selber Stelle auf ein anderes System.

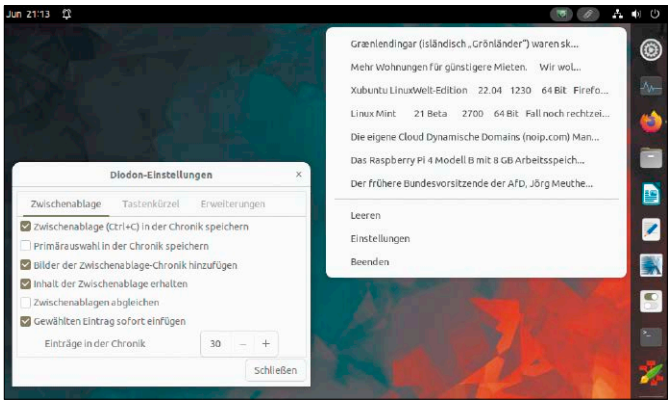
Diodon: Clipboardsammler

Das Tool Diodon ist gute Ergänzung für Anwender, die in einer Zwischenablage für Web- und Textrecherchen eine größere Menge von Text- und Bildmaterial ansammeln, um sie später in einer Textverarbeitung oder einem Webdienst einzutragen. Diodon ist in den Paketquellen der meisten Linux-Distributionen vertreten und mit

```
sudo apt install diodon
```

schnell installiert. Erfreulicherweise trägt es sich dabei gleich automatisch als globaler Autostart ein. Für den allerersten Start verwenden Sie den Befehl „diodon“. Ein Klick auf das neue Büroklammer-Symbol in der Systemleiste öffnet den bisherigen Verlauf der Zwischenablage und mit „Einstellungen“ die einfache Konfiguration. Ganz unten ist die maximale Anzahl der Einträge zu definieren, bei den oberen Optionen ist „Primärauswahl […] speichern“ gut zu überlegen, weil dann praktisch jeder markierte Text – ohne „Kopieren“ oder Strg-C – sofort im Diodon-Verlauf landet.

Wenn die Ablage die gewünschte Reihe von Textteilen und Bildern enthält, öffnen Sie das Programm, etwa eine Textverarbeitung, die diese Elemente empfangen soll: Danach klicken Sie in der Diodon-Chronik einfach auf den Eintrag, der kopiert werden soll. Wenn das Zielprogramm Bilder verarbeiten kann, funktionieren auch diese, andernfalls wird es diese einfach ignorieren.



Clipboardsammlung in Didion: Das Tool ist einfach, aber für Text- und Bildsammlungen aus dem Internet oder aus lokalen Quellen genau richtig.

Vielleicht das einzige Manko des ebenso einfachen wie praktischen Tools: Die Einträge lassen sich unseres Wissens nur insgesamt löschen („Leeren“), nicht einzeln.

Tipp für Ehrgeizige: Mit Copyq finden Sie in allen Standard-Paketquellen ein Tool mit unfassbarer Funktionsbreite, das neben der primären Clipboardsammlung auch als Textbausteinsammler und Programmstarter dienen kann. Das Tool individuell und alltagstauglich zu konfigurieren, bedeutet aber erst einmal einen anstrengenden Gang durch das übergroße Optionsangebot.

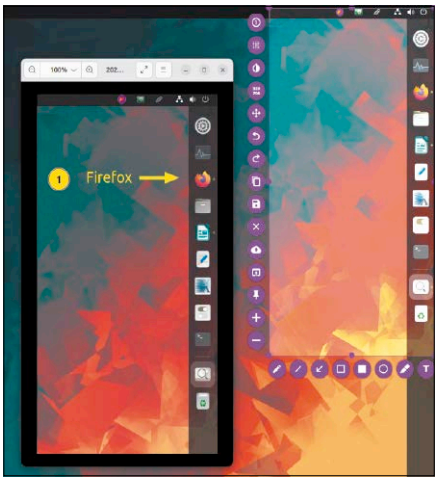
Flameshot: Aufbereitete Bildschirmfotos

Die mitgelieferten Screenshotwerkzeuge von Gnome, KDE & Co. sind allesamt ausreichend und mit vorkonfigurierten Hotkeys wie „Druck“ und „Alt-Druck“ auszulösen. Eventuelle Nachbearbeitungen wie Hinweispfeile, Farbmarkierungen oder Überpinseln persönlicher Daten erledigt man dann gewöhnlich in einer Bildbearbeitung. Wenn solche Nacharbeiten regelmäßig anfallen, kann das Tool Flameshot das ideale Werkzeug sein. Flameshot ist mit

```
sudo apt install flameshot
```

schnell nachinstalliert. Beim ersten Start bietet es automatisch seine Konfiguration an: Unter „Interface“ bestimmen Sie Farbe und Anzahl der Bearbeitungselemente, der „Opacity“-Faktor definiert die Verdunklung des Bildschirms und sollte eher unter 50 Prozent bleiben. Unter „Filename Editor“ geben Sie dynamische Dateinamen mit Zeitstempel beim Speichern der Screenshots vor.

Bei künftigen Starts ziehen Sie auf dem verdunkelten Bildschirm mit der Maus den zu fotografierenden Bereich. Feinjustierung ist mit den Anfassern des markierten Rechtecks möglich, exakter und pixelgenau mit den Cursortasten. Das Tool zeigt ferner Buttons zur sofortigen Bearbeitung – Pfeile, Linien, rechteckige und runde Rahmen, eine Blur-Funktion zum Verwischen. Die Farbe der Zeichenelemente kann nach Rechtsklick aus einer Farbpalette gewählt werden. Der Screenshot wird dann entweder für die Weiterbearbeitung in die Zwischenablage kopiert (Copy-Button) oder als Datei gesichert (Save-Button). Die Esc-Taste unterbricht den Vorgang macht den Desktop wieder zugänglich. Ob die Zeichenelemente für Ihre Zwecke ausreichen, kann nur der Versuch zeigen. Aber allein schon die exakte Justierung und die Blur-Funktion machen Flameshot zur Empfehlung. ■



Bildschirmfoto mit Flameshot: Das Tool bearbeitet das Foto schon bei der Herstellung. Hier wurde, wie das fertige Bild links zeigt, eine Beschriftung mit Pfeil eingetragen.

Sichere Daten: Die Grundregeln

Große IT oder Homeoffice: Die Grundregeln für Datensicherheit und Datenschutz sind identisch. Der Unterschied ist „nur“ quantitativ, aber natürlich erheblich – je mehr Nutzer, Geräte, Systeme und Daten, desto anspruchsvoller wird die Aufgabe.

VON HERMANN APFELBÖCK

© David Wolski

Dieser Heftschwerpunkt zeigt Maßnahmen, um Router, Desktop-PCs, Mobilgeräte und Serversysteme gegen Angriffe und Datenspionage abzuschirmen. Der einleitende Beitrag ergänzt diese Einzelmethoden durch einen Überblick über die Grundziele der IT-Sicherheit und über die dafür nötigen operativen Maßnahmen.

Prinzipien: Worum geht's?

Im Detail – hinsichtlich der Einzelmaßnahmen für Geräteschutz, Benutzer- und Zugangskontrolle, Softwarekonfiguration, Backup und Verschlüsselung – sind die Themen Datensicherheit und Datenschutz hochkomplex. Im Prinzip geht es aber nur um drei Problemfelder, und diese sind im überschaubaren Geräte- und Nutzerpark privater Endanwender durchaus beherrschbar:

1. Datenverlust durch interne Fehler: (Hardware-/Systemausfälle, Benutzerpannen): Dies ist das mit Abstand häufigste Szenario für massiven Datenverlust. Die wichtigsten Maßnahmen, hier vorzubeugen, wird dieser Beitrag in aller Kürze aufzeigen, zumal dieser Aspekt in den folgenden Artikeln nicht mehr auftritt.

2. Datenverlust durch externe Schadsoftware (Virenbefall und gehackte Server): Dieses Szenario wird oft paranoid überschätzt. Es ist nicht so, dass Killerviren über das Ethernet-Kabel in den Rechner kriechen oder durch das Funknetz einfliegen. Vielmehr etabliert der Heimrouter für alle angeschlossenen Geräte ein privates Netz, das vom öffentlichen Netz unabhängig ist und jeden Zugriff aus dem Internet ablehnt. Eine Sendung aus dem öffentlichen Netz an den Router wird nur in genau zwei Situationen erlaubt und „durchgelassen“:

A. Der Benutzer hat im Router explizit eine Portfreigabe geschaltet, um den Internetzugriff auf einen Serverdienst zu erlauben. Dabei kann es sich etwa um einen Datenserver, eine Nextcloud oder eine Smart-Home-Funktion handeln, die er von außerhalb nutzen möchte. Dieses Thema kommt in den nachfolgenden Beiträgen zur Sprache und wird nachfolgend nur noch kurz erwähnt. Der allgemeine Rat: Portfreigaben für Serverdienste sind nur etwas für erfahrene Anwender.

B. Damit ein Nutzer am öffentlichen Netz teilnehmen kann, müssen eintreffende Sendungen erlaubt sein, wenn er sie selbst angefordert hat. Das kann eine HTML-Seite, ein Download oder eine Mail sein. Technisch geschieht Folgendes: Eine lokale IP macht eine Anfrage (etwa Mausklick auf Link) auf einem Webserver. Der Router merkt sich die lokale IP, schickt die Anfrage an den Server im öffentlichen Netz. Die Sendung kommt zurück an die öffentliche IP des Heimrouters, der diese aufgrund aktiven Anfrage aus dem lokalen Netz akzeptiert und dann an jene lokale IP schickt, woher der Auftrag kam.

Somit ist klar: Es kommt nichts von außen, was nicht von innen angefordert wurde. Jedoch ist nicht zu verhindern, dass sich die Nutzer aktiv Sendungen ins lokale Netz holen, die sie besser nicht abrufen sollten – etwa ausführbare Downloads und Mails mit schädlichen Anhängen. Theoretisch ist schon der Klick in Webseiten oder HTML-Mails problematisch, wenn dadurch ausge-

löste Web-Scripts auf ungepflegte Browser mit Sicherheitslücken treffen. Die wichtigsten Maßnahmen, um die alltägliche Browser- und Mailnutzung abzuhärten, ist ebenfalls ein knappes Thema dieses Beitrags.

3. Datenpreisgabe an Unbekannte (verlorene Datenträger, offene Funknetze, Daten in der Cloud – auch Mail, Browsersynchronisierung): Dies scheint die objektiv harmloseste Bedrohung. Aber was eine versehentliche oder selbst verschuldete Preisgabe personenbezogener Daten anrichten kann, hängt von der Menge und der Qualität der Daten ab. Was US-Big-Data-Sammler aus Verlaufsprotokollen oder unverschlüsselten Clouddateien an persönlichen Interessensprofilen akkumulieren, ist lästig bis alarmierend. Regelrecht existenzgefährdend sind aber verlorene Datenträger, die sensible geschäftliche oder persönliche Informationen direkt enthalten oder die Zugangsdaten zu solchen Informationen wie Firmenserver, Bank, Bezahldienst et cetera. Dieses Datenschutzthema wird später nur mehr in einem speziellen Beitrag zur Home-Verschlüsselung (mit Gocryptfs) behandelt, daher gibt es hier einige wichtige Grundregeln.

Maßnahmen (1): Systemschutz & Backup

Wer seiner Hardware, seinem Betriebssystem und sich selbst ohne Rückversicherung vertraut, ist naiv, faul, fahrlässig. Die Katastrophe kann sich Zeit lassen, aber sie kommt (garantiert). Maßnahmen, die den Fortbestand aller Benutzerdaten oder des gesamten Systems sichern, gibt es in Menge. Dabei stellt sich nur die Frage des Umfangs und Aufwands.

Datenbackups mit Rsync: Unter Linux, wo Neuinstallationen und Softwarewiederherstellung geringen Aufwand bedeuten, stehen die Benutzerdateien eindeutig im Vordergrund. Und dafür sind Backups oder Synchronisierungen mit Rsync oder Tar eindeutig erste Wahl. Grafische Alternativen wie Freefilesync (*www.freefilesync.org*) scheinen auf den ersten Blick komfortabler, aber ein einmal geprüftes und als Alias abgelegtes Backupkommando ist schneller, effizienter und automatisierbar.

Tar hat den Vorteil, dass die Dateisysteme von Quelle und Ziel keine Rolle spielen, da alle Attribute intern gesichert werden, außerdem gibt es optionale Komprimierung. Die Daten landen in Archiven, die jeder Archivmanager auch ohne Auspacken nutzen kann. Das von uns bevorzugte Rsync hat den Vorteil, dass alle Daten auch auf dem Sicherungsziel uneingeschränkt zu benutzen sind. Es sichert auf interne und externe Laufwerke, Netzwerkfreigaben und jeden Rechner, auf dem ein SSH-Server läuft. Rsync hat reichlich Schalter, doch fasst die Option „-a“ oder „--archive“ häufig benötigte Funktionen zusammen.

Rescuezilla schreibt Systemimages: Diese Aktion ist eine Systemschutzmaßnahme. Für periodische Datensicherung ist der Einsatz des externen Livesystems zu aufwendig.

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

Das Beispiel geht davon aus, dass das Ziellaufwerk „/media/[...]“ eingehängt ist. Beachten Sie beim Quellordner immer den abschließenden Slash (/). Für periodische Sicherung ergänzen Sie den Schalter „--update“ oder „-u“, damit nur neue Daten kopiert werden:

```
rsync --archive --update /home/ha/
  /media/ha/usb/backup
```

Die Schalter „--verbose“ („-v“) und „--progress“ („-P“) sind immer zu empfehlen, um den Vorgang gesprächiger zu machen.

Eine 1:1-Spiegelung erzwingt der Schalter „--delete“:

```
rsync -auvP --delete /home/ha/ /
  media/ha/usb/backup
```

Was in der Quelle „/home/ha“ seit dem letzten Kopiervorgang gelöscht wurde, wird auch auf dem Ziel gelöscht. Mit falschen Pfadangaben wäre das fatal, daher ist vorher ein Testlauf mit „--dry-run“ anzuraten (*rsync -av --delete --dry-run* ...).

Rsync kann von jedem Netzwerkrechner Daten beziehen oder dorthin kopieren, wo ein SSH-Server läuft. Die Sicherung folgt diesem Schema

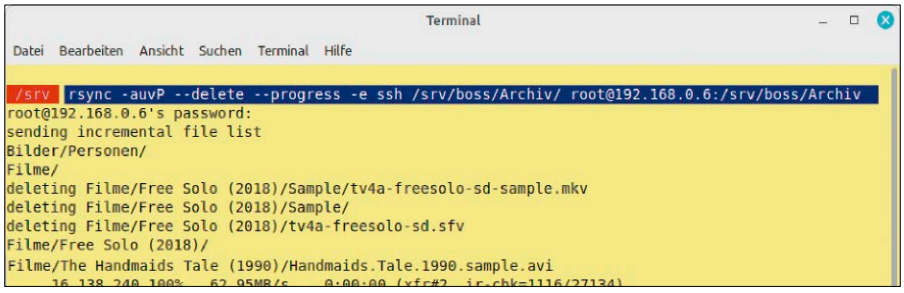
```
rsync -auvP -e ssh ha@192.168.0.20:
  /home/ha/ /home/ha
```

oder mit

```
rsync -auvP -e ssh /home/ha/
  ha@192.168.0.20:/home/ha
```

in die andere Richtung.

Laufwerkssicherung: Diese Rückversicherung ist kompromisslos und schließt Systemdaten wie Benutzerdateien ein. Zur bloßen Datensicherung sind solche Laufwerkimages aber zu aufwendig, weil sie periodisch wiederholt werden müssten, um den geänderten Datenbestand zu repräsentieren. Erforderliche Werkzeuge sind die Livesysteme Rescuezilla (*https://rescuezilla.com*) oder Clonezilla (*https://clonezilla.org*), weil das Kopieren im laufenden System technisch scheitern würde. Clonezilla



Rsync-Abgleich – lokal, im Netz und auch mit SSH: Solche 1:1-Kopien mit Delete-Schalter sorgen für exakt identischen Datenbestand auf Quelle und Ziel.

beherrscht einige Netzwerkfähigkeiten mehr (beim Sicherungsziel) sowie optionale Komprimierung und Verschlüsselung der Imagesicherung. Außerdem kann es einen Datenträger ohne Zwischenschritt einer Imagesicherung direkt auf einen zweiten „klonen" (Option „device-device"). Das grafische Rescuezilla ist andererseits wesentlich bedienfreundlicher.

Nichts gesichert? Livesystem zur Datenrettung! Streikt das System, aber nicht die Hardware, ist auch ohne Backup noch nichts verloren. Nach dem Rechnerboot mit einem beliebigen, möglichst vertrauten Linux-Livesystem haben Sie vollen Zugriff auf das Home-Verzeichnis und können alle oder ausgewählte Dateien auf ein externes (drittes) Laufwerk retten.

Maßnahmen (2): Sicher im Internet

Eingangstür vom öffentlichen Web ins lokale Netz ist der Router. Die Hackerindustrie klopft permanent und massenhaft beliebige öffentliche IP-Adressen ab – auch Ihren Router, wenn es der Zufall will. Wer Dienste nach außen öffnet, und sei es auch nur eine winzige Smarthome-Funktion, fährt etwas sicherer, wenn der Router im Stealth-Modus arbeitet (Fritzbox: „Internet → Filter → Listen → Firewall im Stealth Modus"). Er antwortet dann nicht auf Ping-Anfragen aus dem Internet. Hacker-Scripts schicken schnelle Pings oft einem Portscan voraus, um Zeit zu sparen.

Gegen direkte Portscans Ihrer öffentlichen Adresse ist kein Kraut gewachsen, aber auch hier gibt es höhere Hürden: Wenn Sie Ihrem Dienst statt des Standardports (nach außen) einen selbst gewählten fünfstelligen Port zuweisen, werden die meisten Scans nichts finden, weil sie aus Zeitgründen nur etliche Standardports abfragen.

Das Funknetz: Das WLAN muss natürlich verschlüsselt sein (Fritzbox: „WLAN → Sicherheit → Verschlüsselung"). WPA2 oder WPA3 und ein komplexes Kennwort halten die Nachbarn fern, die andernfalls nicht nur mitsurfen könnten, sondern auch Zugang zu den Daten im Heimnetz erhielten. Immerhin besteht hier aber eine weitere Zugangshürde, weil Netzfreigaben in der Regel ebenfalls eine Benutzeranmeldung erfordern.

MAC-Filterung ist eine weitere Abhärtungsmaßnahme, die nur noch definierte Hardware ins WLAN lässt (Fritzbox: „WLAN → Sicherheit"). Jedes später hinzukommende Gerät im Haushalt oder jedes Besuchergerät muss später explizit mit seiner MAC-Adresse erlaubt werden („WLAN-Gerät hinzufügen").

Das Betriebssystem: Mit Linux können Sie genau wie unter Windows unfreiwillig Schadsoftware in Downloads, Mails oder Web-Scripts herunterladen – dies aber praktisch ohne Folgen: Linux ist gegen Schadsoftware so gut wie immun, weil fast alle Viren und Würmer für Windows programmiert sind. Solange die Trägerdateien nicht im lokalen Netz auf Windows-Rechner kopiert werden, besteht keine Gefährdung.

Linux statt Windows: Malwareschutz im Internet ist tatsächlich so einfach zu erreichen, und dies unabhängig vom jeweiligen Browser, Mail-, Chat-, FTP-, Usenet- oder Torrent-Client.

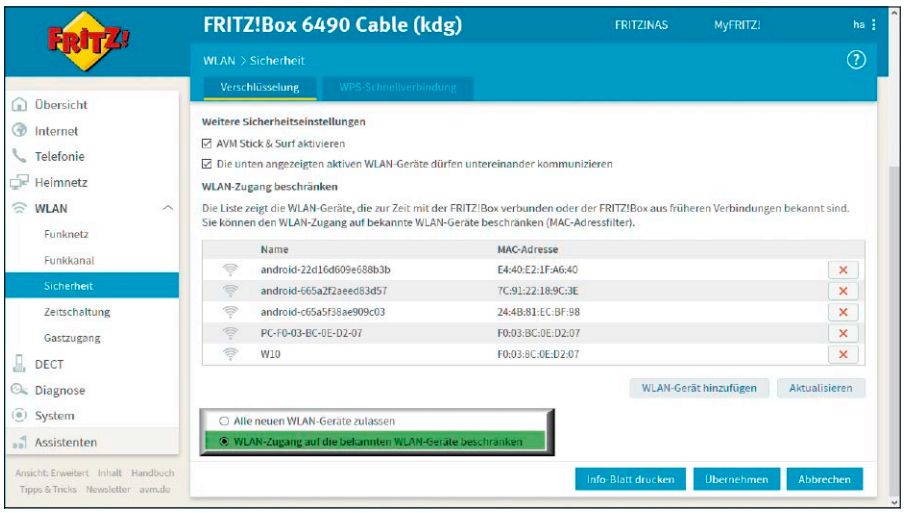
Für Windows-Nutzer ist es daher der beste Rat, mit einem schlanken Linux in einer virtuellen Maschine (VM) ins Internet zu gehen. Der Bedienkomfort einer VM (unter Virtualbox oder Vmware) ist deutlich höher als mit externen Linux-Surfsystemen, für die man sein Standardsystem verlassen und den Rechner neu booten muss. Wenn ein Desktoprechner mindestens vier bis acht GB RAM mitbringt und einen aktuellen Prozessor, läuft das Linux mit Browser in der VM praktisch genauso flüssig wie in einem nativen System.

Der Browser: Ungeachtet der Linux-Immunität gegenüber Viren bleibt die Gefahr von Java-, Javascript- und PHP-Script, die über Browser-Sicherheitslücken Code einschleusen (meistens Windows-Code, aber rechnen muss man mit allem). Auch Linux-Browser müssen daher ständig aktualisiert werden. Dies geschieht automatisch und zeitnah, aber nur, sofern die Paketquellen dies gewährleisten. So wird bei Debian derzeit ein Aktualisierungsstau kritisiert, der zu veralteten Browsern führt. Ubuntu delegiert seit Version 22.04 die Verantwortung für Firefox an Mozilla. Ein aktueller Firefox ist somit garantiert, allerdings im unbeliebten Snap-Container.

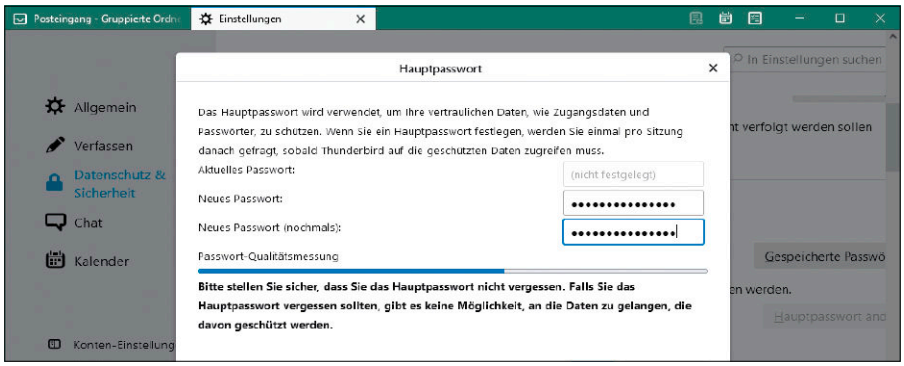
Theoretisch können Browser alle Script-Aktivitäten abschalten (Firefox, „about:config", „javascript.enabled" oder Chrome, „Einstellungen → Datenschutz und Sicherheit → Website-Einstellungen → JavaScript"). Das ist aber kaum praktikabel, da es dann Fehlermeldungen hagelt. Ein Kompromiss ist das Add-on Noscript für Chrome und Firefox. Es blockiert Javascript, Java und andere ausführbare Inhalte. Damit ist Noscript der Schädlingsstopp schlechthin, aber ebenfalls unbequem, weil fast jede Webseite Script-Code verwendet. Immerhin landen einmal erlaubte Sites in einer Whitelist und müssen später nicht mehr bestätigt werden, aber zunächst müssen Sie auf vielen interaktiven Seiten die Script-Ausführung manuell erlauben.

Das Mailprogramm: Mails an sich sind nicht gefährlich. Aber sie sollten Mails bleiben und nicht ins Web gehen. Und Mailanhänge von Unbekannten haben auf dem System nichts verloren. Beim unter Linux meistgenutzten Mailclient Thunderbird lohnen sich folgende Optionen:

Die Einstellung „Ansicht → Nachrichteninhalt → Reiner Text" verhindert die hübsche Anzeige von HTML-Format, damit aber auch trügerische Tarnoptik und Links. Ein Kompromiss ist „Vereinfachtes HTML". Unter „Extras → Einstellungen → Datenschutz &



WLAN-Kennwort genügt nicht: Diese Option lässt nur noch die per MAC-Adresse bekannten Geräte ins Funknetz.



Sinnvoll auf Notebooks: Das Thunderbird-Hauptpasswort verschlüsselt die Mailcontainer, sodass bei Fremdzugriff weder die Nachrichten noch die Zugangsdaten lesbar sind.

Sicherheit“ sollte „Externe Inhalte in Nachrichten erlauben“ abgeschaltet sein. Nützlich ist ferner weiter unten die interne Phishing-Heuristik: „Nachrichten auf Betrugsversuche (Phishing) untersuchen“.

Wenn Sie dann noch auf Notebooks Ihre Zugangsdaten schützen, sind Sie auch datenschutztechnisch auf der sicheren Seite. Thunderbird bietet dafür das „Hauptpasswort“ („Extras → Einstellungen → Datenschutz & Sicherheit → Hauptpasswort verwenden“. Dadurch werden die Zugangsdaten verschlüsselt, sodass ein Fremdzugriff auf Dateiebene erfolglos ist. Eine weitere Datenschutz-Bitte, der nicht alle Seiten folgen werden, ist die Option „Websites eine „Do Not Track“-Mitteilung senden“. Dies ist aber sowieso hinfällig, sofern sich man die Mails als Reintext zeigen lässt.

Maßnahmen (3): Datenschutz und Verschlüsselung

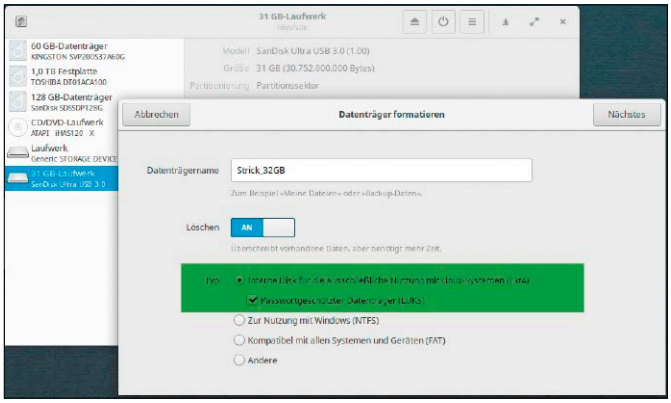
Notebooks, USB-Medien, Cloud: Alles, was das Haus und das lokale Netz verlässt, kann in fremde Hände gelangen oder ist in fremden Händen. Verschlüsselung sorgt dafür, dass die Daten nichts preisgeben.

1. Mobile Notebooks: Bei Notebooks, die viel unterwegs sind, sollte man mit kleineren Lösungen erst gar nicht anfangen: Hier empfiehlt sich eine Linux-Installation mit verschlüsselter Systempartition (Luks/Cryptsetup). Das verlorene oder unbeaufsichtigte Notebook lässt dann auch beim Booten durch ein Fremdsystem keinerlei Einblick in die Daten zu. Die meisten Linux-Installer (Ubuntu-Derivate, Debian-Derivate, Open Suse, Fedora, Manjaro und andere) bieten diese Option im Partitionierungsdialog direkt an. Voraussetzung ist dabei immer, dass Sie dem Löschen der primären Festplatte zustimmen und das neue System diese komplett übernehmen darf. Cryptsetup-verschlüsselte Systeme haben nur eine winzige unverschlüsselte Boot-Partition, alles andere wird erst aufgesperrt, wenn nach „Please unlock disk [...]“ das korrekte Passwort eingegeben wird.

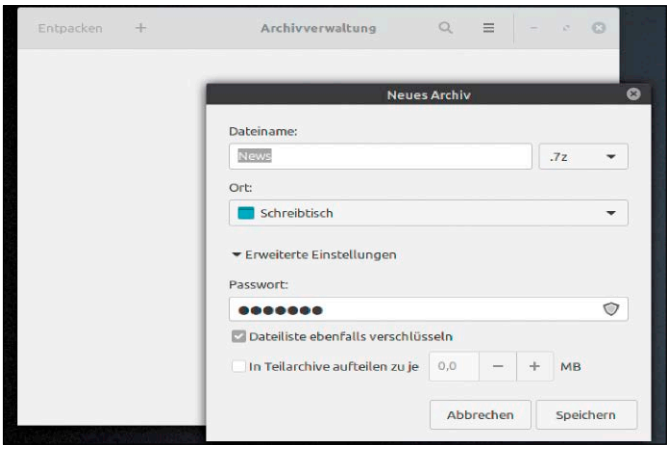
2. USB-Medien: USB-Datenträger lassen sich ebenfalls mit Luks/Cryptsetup verschlüsseln. Die Maßnahme ist aber gut zu überlegen, weil damit ein Austausch mit Windows- oder Mac-Systemen ausscheidet. Die Aktion ist mit Gnome-Disks oder dem KDE-Partitionmanager ganz einfach: Nach „Partition formatieren“ wählen Sie als „Typ“ den Eintrag „Verschlüsselt, kompatibel mit Linux-Systemen (LUKS + Ext4)“ und vergeben die „Passphrase“ – also das Kennwort.

3. Cloud, USB und sensible Dateien: Einfachster Schutz bei geringeren Datenmengen ist die Ad-hoc-Verschlüsselung von Einzeldateien oder eines Ordners. Ohne Einschränkung anwendbar ist der Packer 7Zip (Paket „p7zip-full“). Passwortgeschützte Archive eignen sich für Dateien in der Cloud, können aber auch für mobile Datenträger ausreichen. Da es 7-Zip für Linux, Windows und Mac-OS (7zX) gibt, ist der Austausch solcher Archive problemlos.

7-Zip erscheint unter Linux nicht als selbständiges Programm, sondern integriert sich in die „Archivverwaltung“. In Zusammenarbeit mit dieser Archivverwaltung oder dem 7z-Filemanager unter Windows ist Verschlüsseln und Entschlüsseln recht komfortabel: Sie ziehen Datei oder Ordner einfach mit der Maus in das Fenster („Archivverwaltung“ oder „7-Zip“), bestätigen unter Linux, dass damit ein neues Archiv angelegt werden soll, und geben dann das Format „7z“ an. Unter „Erweiterte Einstellungen“ vergeben Sie das Passwort. ■



Komplettverschlüsselung für USB-Medien: Mobile USB-Sicherheit ist ganz einfach über Gnome- und KDE-Laufwerktools erreichbar. Eine Nutzung unter Windows ist dann allerdings nicht möglich.



Packer 7-Zip als Datenschützer: In der Archivverwaltung muss das Format „.7z“ gewählt werden, damit die Verschlüsselungsoption angeboten wird.

Home: Individuell verschlüsselt

Private Daten auf Notebooks verlangen immer besonderen Schutz. Aber auch auf Mehrbenutzersystemen sollten Daten verschlüsselt sein. In Ubuntu/Debian sorgt Gocrypt FS für eine individuelle und komfortable Home-Chiffrierung.

VON DAVID WOLSKI

Die sicherere Verschlüsselung vertraulicher Daten ist im Unternehmensumfeld meist Pflicht, um Auflagen der IT-Compliance zu erfüllen. Aber auch die Vorstellung, dass wichtige Daten auf einem privat genutzten Laptop mit dem Verlust des Geräts in fremde Hände fallen, ist nicht angenehm. Die aktuellen Linux-Distributionen wie Ubuntu 22.04 bieten bei der Einrichtung über Cryptsetup/Luks eine Komplettverschlüsselung des Systems an.

Diese Methode gilt als sehr sicher, ist aber nicht ohne Einschränkungen und zusätzliche Komplexität: Auf Linux-Systemen, die auch Serverrollen erfüllen und unbeaufsichtigt booten sollen, ist die Luks-Systemverschlüsselung nicht praktikabel. Denn beim Systemstart muss jemand zugegen sein, um das Passwort zur Entschlüsselung der Partitionen einzugeben. Zudem ist dieses Passwort für alle Anwender auf dem System gleich. Für eine individuelle Verschlüsselung ist diese Methode also nicht geeignet.

Gocrypt FS und Fuse: Ein neuer Ansatz

Ein alternativer Weg, der jenem von Ecrypt FS ähnelt, der bis Ubuntu 18.04 für die Verschlüsselung von Home-Verzeichnissen sorgte, ist Gocrypt FS. Gocrypt FS ist ein ausgereiftes, in Go geschriebenes Tool zur Erstellung verschlüsselter Dateisysteme über das Kernel-Modul „File System In Userspace“ (Fuse). Die Einrichtung ist in Debian/Ubuntu mit wenig Aufwand erledigt, denn es finden sich bei diesen Distributionen alle Zutaten in den Standard-Paketquellen. Zudem gibt es schon ein Grundgerüst zur automatischen Entschlüsselung bei der Anmeldung über die Konfiguration von PAM (Pluggable Authentication Modules), die sich unter Linux um die Delegation von Log-in-Informationen an die verschiedenen Systemkomponenten kümmert.

Gegenüber Ecrypt FS, das Linux Mint 21 weiterhin verwendet, hat Gocrypt FS den Vorteil, in aktiver Entwicklung zu sein und weniger Bugs zu haben. Zwei leicht verschmerzbare Minuspunkte gibt es, die nicht verschwiegen werden sollen: So wie auch Ecrypt FS wird das verschlüsselte Home beim Abmelden eines Benutzers nicht ausgehängt, sondern nur bei einem Neustart. Zweitens ist Gocrypt FS im Vergleich zu Luks-Partitionen langsamer bei den Datenträgerzugriffen, weil es sich um ein Fuse-Dateisystem handelt.

Vorbereitung und Installation

In wenigen Handgriffen ist ein verschlüsseltes Home in Debian/Ubuntu eingerichtet. Aus den Paketquellen installiert zunächst das Kommando

```
sudo apt install gocryptfs libpam-
  mount
```

die benötigten Pakete. Gocrypt FS übergibt die Anlage eines verschlüsselten Home zunächst dem Administrator. Das Paket „libpam-mount“ ist dabei das Bindeglied zwischen dem Log-in als Benutzer und der Entschlüsselung des Home-Verzeichnisses per Mountbefehl, Fuse und Gocrypt FS.

Nach der Installation dieser Pakete geht es auch schon an die Erstellung des verschlüsselten Ordners für einen neu angelegten User, welcher hier im Beispiel „benutzer“ heißen soll. Es ist nicht möglich, von einem Benutzerkonto den eigenen Ordner zu verschlüsseln, dafür ist immer ein zweiter User

mit sudo-Privilegien oder root nötig. Zuerst wird das vorhandene Home-Verzeichnis des abgemeldeten Benutzers mit allen seinen Dateien im Terminal in einen temporären Ordner verschoben

```
sudo mv /home/benutzer /home/
 benutzer.tmp
```

und ein neues, später verschlüsseltes Verzeichnis angelegt:

```
sudo mkdir /home/benutzer.enc
```

Dieser Ordner wird nun verschlüsselt und später nach der Anmeldung nach „/home/benutzer“ unverschlüsselt eingehängt. Um den Ordner vorzubereiten, dient folgender Befehl:

```
sudo gocryptfs -init /home/
 benutzer.enc
```

Gocrypt FS fragt nun das gewünschte Passwort ab, das identisch mit dem Systemkennwort von „benutzer“ sein muss. Gocrypt FS legt eine JSON-Datei mit dem Password-Hash im Ordner ab und zeigt zur späteren Entschlüsselung im Falle eines vergessenen Kennworts auch einmalig einen Generalschlüssel an, den man unbedingt sicher verwahren sollte. Nun erstellen die folgenden beiden Kommandos

```
sudo mkdir /home/benutzer
sudo gocryptfs /home/benutzer.enc /
 home/benutzer
```

das neue, leere Verzeichnis „/home/benutzer“ als Einhängepunkt und hängen dort den entsperrten Gocrypt-FS-Ordner ein. Aus dem zuvor erstellten temporären Home-Verzeichnis kopiert dann

```
sudo cp -rT /home/benutzer.tmp /
 home/benutzer
```

alle Dateien rekursiv zurück ins neue Home, wobei Gocrypt FS alles chiffriert speichert. Damit alles wieder dem „benutzer“ gehört, ist die Rechteanpassung mit

```
sudo chown -R benutzer:benutzer /
 home/benutzer /home/benutzer.enc
```

nötig und ein Aushängen des neuen Home-Verzeichnisses, das anschließend auch zusammen mit dem temporären Ordner gelöscht wird:

```
sudo fusermount -u /home/benutzer
sudo rm -r /home/benutzer
```

Keine Sorge: Bei einer Anmeldung wird es aus dem verschlüsselten Ordner auf dem Datenträger von Gocrypt FS neu erzeugt.

PAM: Ein Regelwerk für Gocrypt FS

Nun ist nochmal Aufmerksamkeit verlangt. Denn das Home von „benutzer“ ist vorbereitet und soll künftig nach der Anmeldung des Users gleich entschlüsselt an Ort und Stelle sein. Das verlangt zwei Anpassungen in Konfigurationsdateien. Einmal in der Datei „/etc/fuse.conf“, in welcher das Kommentarzeichen (#) vor der letzten Zeile

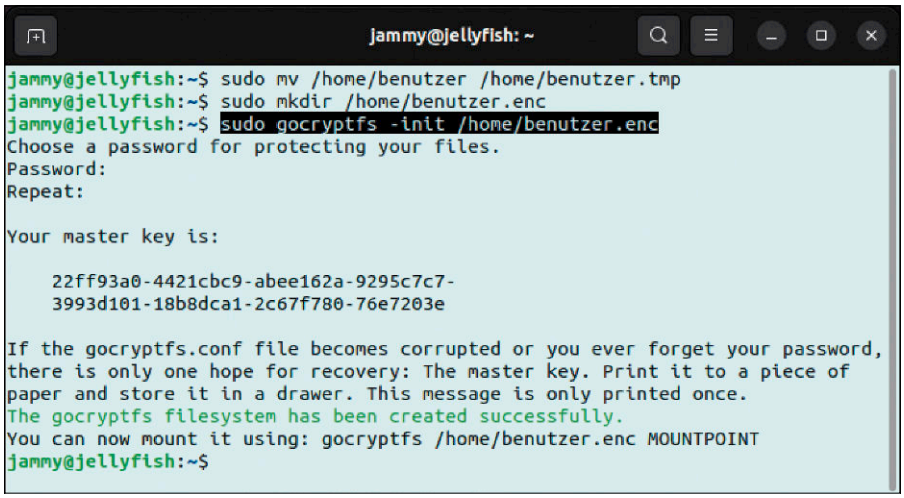
```
user_allow_other
```

entfernt wird und danach nicht nur root den Zugriff auf das neue Home erlaubt. Die zweite Änderung betrifft das anfangs installierte Modul „libpam-mount“ von PAM, das seine Einstellungen aus der Datei „/etc/security/pam_mount.conf.xml“ bezieht. In diese Datei, die mit root-Rechten oder vorangestellten „sudo“ in einem Texteditor geöffnet wird, kommt nun, genau vor dem abschließenden Tag „</pam_mount>“ diese Definition in eine durchgehende Zeile:

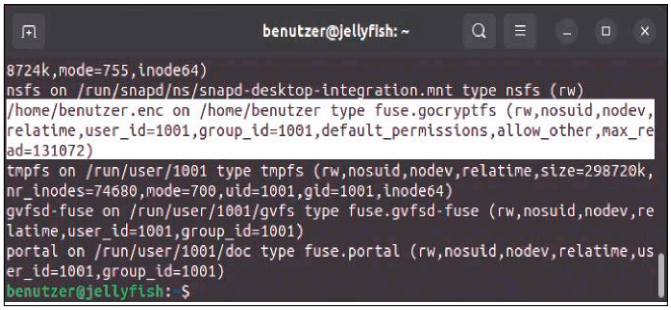
```
<volume user="benutzer"
 fstype="fuse" options="nodev,nos
 uid,quiet,nonempty,allow_other"
 path="/usr/bin/gocryptfs#/
 home/%(USER).enc" mountpoint="/
 home/%(USER)"/>
```

Ab jetzt funktioniert die Anmeldung des Benutzers „benutzer“ über die Konsole oder den grafischen Displaymanager und hängt über das gegebene Anmeldepasswort das Home-Verzeichnis unverschlüsselt ein.

Soll auf dem System ein weiterer Benutzer ein verschlüsseltes Home bekommen, dann sind alle Schritte mit dem anderen Usernamen nochmal auszuführen. Für jeden Benutzer ist auch wieder eine Zeile in der Datei „/etc/security/pam_mount.conf.xml“ hinter „user=“ erforderlich. ■



Den neuen Ordner vorbereiten: Dafür ist ein separates Benutzerkonto mit sudo-Berechtigungen nötig. Gocrypt FS zeigt einmalig einen Wiederherstellungsschlüssel für Notfälle an.



Eingehängt und entschlüsselt: Die Ausgabe des Befehls „mount“ zeigt, dass PAM den Ordner „/home/benutzer.enc“ automatisch nach dem Log-in verfügbar gemacht hat.

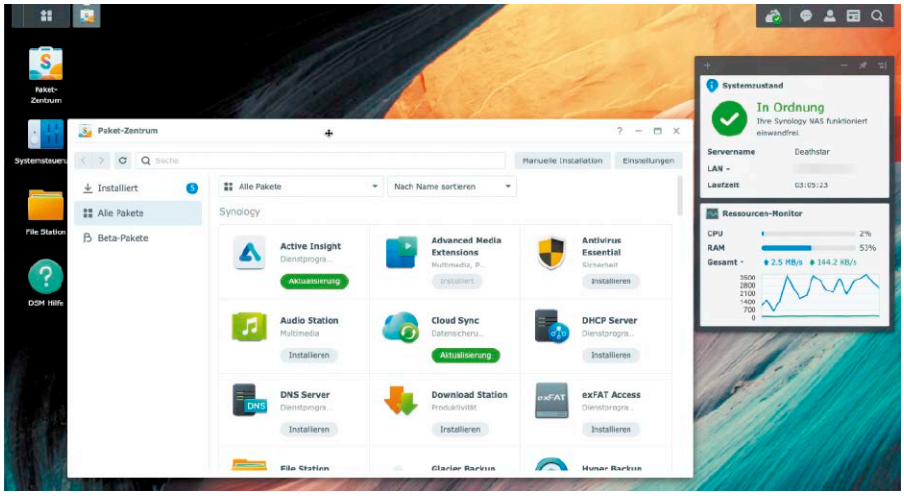
PRO & CONTRA

+ automatische Entschlüsselung bei der Anmeldung
+ verwendet kein systemweites Passwort
+ wenig Aufwand in Debian/Ubuntu
+ Weniger Bugs als das eingestellte Ecrypt FS
– manuelle Einrichtung zu Beginn erforderlich
– Gocrypt FS ist langsamer als Cryptsetup/Luks
– Gocrypt-FS-Ordner wird nicht automatisch ausgehängt

So wird Ihr NAS sicherer

Aus Sorge um Datenschutz und Datensicherheit bevorzugen viele Anwender den Einsatz eines eigenen Netzwerkspeichers gegenüber der Cloud. Aber ganz so einfach ist das nicht. Auch NAS-Geräte müssen abgesichert werden.

VON STEPHAN LAMPRECHT



Die ideale Welt sieht in Hinblick auf die Datensicherheit so aus: Das NAS liegt isoliert im heimischen Netzwerk, das von Bedrohungen von außen durch eine Firewall geschützt ist. Ein Datenverkehr zwischen dem offenen Netz des Internets und den heimischen Geräten wäre damit unmöglich. Allerdings existiert dieses ideale Szenario spätestens dann nicht mehr, wenn im Haushalt auch Elemente für das Smart Home installiert sind. Denn zu deren Komfort gehört der Fernzugriff über das Internet. Ein Hub oder ein smartes Thermostat könnte Angreifern also als Sprungbrett für Attacken dienen. Das ließe sich dadurch lösen, dass das NAS in einem separaten Netz liegt. Aber wer macht sich schon die Mühe? Deswegen lohnt es sich, die Sicherheit des Netzwerkspeichers gezielt zu verbessern.

Den Admin-Zugang sichern

Die meisten Geräte werden mit dem Standardnutzer „admin“ ausgeliefert, dem dann auch noch das triviale Passwort „admin“ zugeordnet ist. Das versuchen die Hersteller dadurch zu heilen, dass sie die Nutzer schon während der ersten Einrichtung dazu auffordern, dieses allzu einfache Passwort zu ändern. Noch besser ist es, auf das Standardbenutzerkonto „admin“ ganz zu verzichten. Schließlich haben Bots für Brute-Force-Attacken mit diesem Benutzernamen bereits 50 Prozent der benötigten Informationen. Legen Sie also einen neuen Nutzer an, dem Sie ein starkes Passwort mitgeben. Diesen ordnen Sie dann die Rechte eines Administrators zu. Nachdem Sie sich davon überzeugt haben, dass das funktioniert hat, loggen Sie sich mit diesem Konto ein und deaktivieren (oder löschen) das vorherige Admin-Konto. Auf einem aktuellen Synology-NAS wechseln Sie in die Systemsteuerung und wählen „Benutzer & Gruppen“. Mittels „Bearbeiten“ finden Sie auf der nachfolgenden Bildschirmseite dann die Option zum Deaktivieren. Ebenso kann die Einrichtung einer Zwei-Faktor-Authentifizierung sehr sinnvoll sein. Im Betriebssystem der Synology ist das unter „Sicherheit, Konto“ bereits eingebaut. Der zweite Faktor wird dann in den persönlichen Einstellungen der Benutzer aktiviert.

Unnötige Dienste abschalten

Besonders in heterogenen Umgebungen neigen Einsteiger dazu, zu viele Dienste zu aktivieren. In einem Haushalt, in dem neben Linux auch Windows- und Mac-Systeme zum Einsatz kommen, scheint es nur konsequent, wenn auch die passenden Freigabeprotokolle eingeschaltet werden. Neben dem eigentlichen Datenprotokoll lassen sich dann auch gleich noch Dienste aktivieren, die den Zugriff auf das NAS vereinfachen. Das sieht trivial aus, ist es aber nicht. Denn es gibt auch (wenn auch wenige) Konstellationen, in denen es zu Filelock-Problemen kommen kann, wenn Clients über unterschiedliche Protokolle parallel auf die gleiche Freigabe zugreifen.

Sie werden etwa häufig lesen, dass Sie im Falle von Apple am besten AFP nutzen. Das sei performanter und ideal. Tatsächlich schwenkt Apple aber immer zusehends auf SMB um. SMB-Freigaben versteht jedes Linux, Windows und Mac-OS. NFS wiederum, einstmals von Sun entwickelt, ist perfekt für Linux-Umgebungen.

Schauen Sie kritisch unter „Systemsteuerung → Dateidienste“ nach (Synology, ähnlich bei anderen NAS-Systemen), was dort

alles aktiviert ist. Über das SMB-Protokoll können Sie unter Windows eine Freigabe als Netzlaufwerk auch direkt via IP-Adresse anlegen. Die Netzwerkerkennung von Windows ist komfortabel, aber eben nur optional. Gleiches gilt auch für das Apple-Pendant Bonjour. Besonders vorsichtig sollten Sie mit Portfreigaben sein. Denn mit jedem Port, den Sie öffnen oder weiterleiten, schaffen Sie einen zusätzlichen Kanal von außen in das lokale Netz.

Cloudservices? Mit Risiken!

Fast jeder NAS-Hersteller bietet einen optionalen Zugang via Cloud auf das NAS an. Damit soll dann der Zugriff von unterwegs auf Fotos, Musik, Dateien und Verwaltungsfunktionen besonders einfach werden. Ein passendes Benutzerkonto ist schnell eingerichtet und via App auf dem Smartphone gelangen Sie dann tatsächlich von überall auf alle Daten und Verwaltungsfunktionen des heimischen NAS-Geräts. Technisch handelt es sich hier einfach um einen Dienst für dynamische DNS-Einträge.

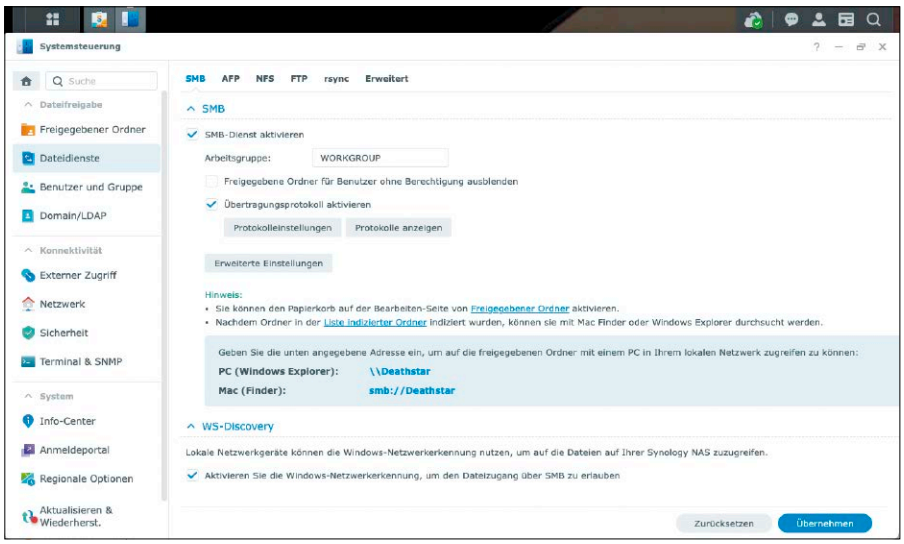
Wie schon bei den oben genannten Diensten sollten Sie sorgfältig abwägen, ob Sie solchen Fernzugriff tatsächlich benötigen. Sie begeben sich damit in die Abhängigkeit vom Hersteller, der sich um die Sicherheit dieser Dienste und seiner Anmeldeportale kümmern muss. Tritt dort eine Sicherheitslücke auf, sind Sie zwar nicht der einzige Betroffene, das hilft Ihnen dann aber auch nicht weiter.

Falls Sie diese Dienste abschalten: Wie präsentieren Sie dann etwa unterwegs Ihre Fotos? Eine denkbare Alternative wäre ein zusätzlicher Raspberry Pi als Server. Es gibt unzählige Anwendungen, die Galerien für Fotos anbieten. Und mittels eines Programms wie Rsync können Sie auf dem NAS gespeicherte Bilder mit dem Raspberry abgleichen. Sie kommen also zum gleichen Ergebnis, ohne den Zugang zum zentralen Datenspeicher freizugeben.

Ein NAS bleibt besser ein NAS

Was gibt es nicht alles an Softwarepaketen für die NAS-Modelle der führenden kommerziellen Hersteller? Der Zugriff auf diese Wundertüte ist verführerisch, schließlich handelt es sich ja um einen kleinen Computer in einem kompakten Gehäuse, der rund um die Uhr läuft. Der Ansatz, ein NAS durch allerlei Zusatzfunktionen aufzubohren, stammt noch aus der Zeit, als kompakte und stromsparende Computer noch ziemlich teuer waren. Spätestens mit dem Raspberry Pi wurde das anders. Dessen Ausstattung überholt inzwischen ältere NAS-Systeme in der Leistung deutlich.

Eine der wichtigsten Sicherheitsmaßnahmen für jedes NAS-System besteht darin, den bereits vorhandenen User „admin“ zu deaktivieren oder zu löschen.



Alles abschalten, was nicht benötigt wird oder redundant ist: Apple kommt gut mit SMB zurecht. Kontrollieren Sie, welche sonstigen Dienste noch aktiv sind – E-Mail vielleicht?

Sie sollten sich also genau überlegen, ob Sie sich einen Gefallen tun, wenn Sie ein Serversystem wie Wordpress auf dem gleichen System laufen lassen, das alle wichtigen Dokumente und Erinnerungen speichert. Besser für Wartung und Sicherheit ist es, das NAS auf seine Kernfunktion zu beschränken. Wenn es Bedarf an weiteren Serverfunktionen gibt, sollte für einen Raspberry noch Platz sein. Diese Investition sollten Ihnen die Daten wert sein.

Nicht nur Synology hat in den vergangenen Jahren viel unternommen, die Sicherheit der Geräte zu verbessern. Mit wachsender Verbreitung wurden diese aber auch verstärkt Ziel von Attacken. Es lohnt sich, den Bereich „Sicherheit“ in der Systemsteuerung genauer anzuschauen. Hier finden Sie Optionen, um Passwörter regelmäßig erneuern zu lassen, können deren Stärke vorgeben und auch zu häufige Anmeldeversuche blockieren.

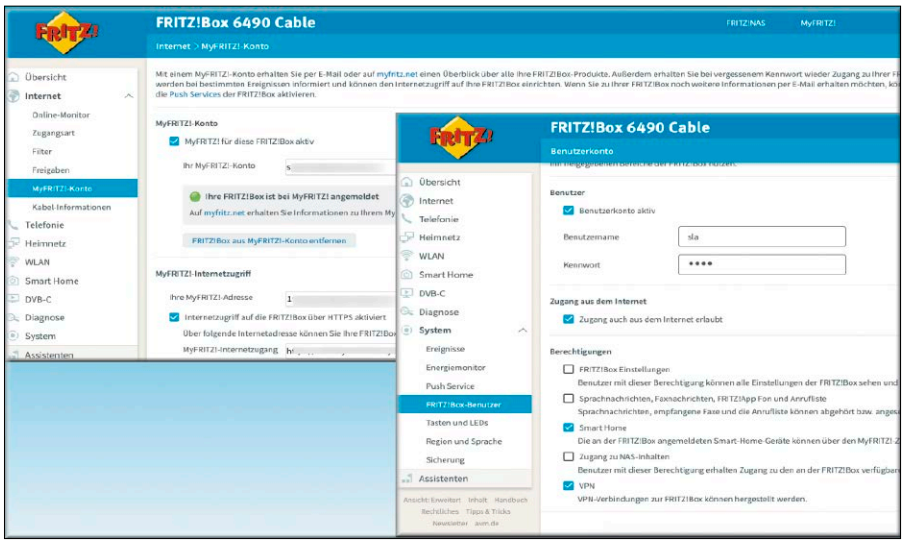
Ob nun ein NAS eines kommerziellen Herstellers oder Raspberry-Server im Eigenbau: Sie sollten das System stets aktuell halten. Wird eine Aktualisierung des Betriebssystems angeboten, installieren Sie diese möglich zügig. Bei einem kommerziellen NAS wird es zudem auch gelegentlich neue Firmware geben, die Sie ebenfalls einspielen sollten.

Alle Maßnahmen nützen nichts, falls das Gerät gestohlen oder irreparabel geschädigt ist. Deswegen benötigt ein NAS mit wertvollen Daten streng genommen ein weiteres Datenbackup, das an einem anderen Ort liegt. ■

Mit VPN sicher und anonym

Mit einem VPN bleiben vertrauliche Daten auch in einem fremden Netzwerk sicher. Aber nicht alle VPN-Lösungen sind gleich. Wir erklären, wie Sie VPN einsetzen und eigene Server aufsetzen.

VON STEPHAN LAMPRECHT



Fritzbox als VPN-Server: Dazu muss „MyFritz“ aktiviert und einem Nutzer der Zugang per VPN erlaubt werden.

Der Grundgedanke hinter einem „Virtual Private Network“ besteht darin, eine sichere Verbindung zwischen zwei verschiedenen Netzen herzustellen. Dabei wird die Infrastruktur einer potenziell feindlichen Umgebung verwendet. Da die Signale zwischen beiden Netzen verschlüsselt werden, läuft die Kommunikation sicher in einer Art Tunnel ab. Deswegen werden VPN-Verbindungen oft als „Tunnel“ bezeichnet. Via VPN können sich die Mitarbeitenden mit dem Unternehmensnetzwerk verbinden, genauso, als säßen sie am Schreibtisch im Büro. Das weltweite Internet schrumpft somit auf die Funktion eines ziemlich langen LAN-Kabels. Wenn Sie über diese VPN-Verbindung mit Ihrem Browser einen Server aufrufen, nutzen Sie die IP-Adresse des VPN-Netzwerks, also nicht die vom DSL- oder Kabelprovider zugewiesene Adresse. Genau damit werben kommerzielle Anbieter.

Was leistet ein VPN?

Ziemlich marktschreierisch, wie es sich für Werbung gehört, bieten im abendlichen TV-Programm eine Reihe von Unternehmen die Nutzung ihrer VPN-Verbindungen an: Nur damit könne man heute sicher und anonym im Internet surfen. Wie bei Werbung üblich, ist das nicht völlig falsch, hat aber einen Haken. Kommerzielle VPN-Anbieter können die Grundlagen des Internets nicht aushebeln. Damit Datenpakete zwischen zwei Punkten ausgetauscht werden können, benötigt ein Client eine IP-Adresse. Sie bekommen also auch bei Nutzung des Angebots eine IP-Adresse zugewiesen. Nur ist die nicht mit der tatsächlichen IP-Adresse Ihres Anschlusses identisch. Insofern surfen Sie „anonym“. Dazu gleich noch einmal mehr. Erst einmal zum Nutzen eines VPN selbst.

Sie benötigen Server und Client: Um ein VPN einzusetzen, benötigen Sie einen VPN-Server. Der kümmert sich um den Verbindungsaufbau und sichert im Hintergrund den Datenverkehr. Und Sie müssen auf dem Client, also Ihrem Computer, Tablet oder Smartphone, eine VPN-Verbindung einrichten, die dann die Daten des Servers nutzt.

Was kann das eigene VPN und was kann es nicht? Für Firmen ist die Nutzung eines VPN schon allein deshalb interessant, weil über die Verbindung zum Computer auch Informationen rauschen, die besser vertraulich bleiben. Aber auch für Privatanwender gibt es gute Gründe: Wenn Sie unterwegs ein fremdes WLAN nutzen, können Sie nicht sicher sein, dass dieses nicht kompromittiert wurde und Informationen mitgeschnitten werden, zum Beispiel Kreditkarteninformationen. Mit einem VPN bleiben diese Informationen verschlüsselt und uneinsehbar. Ein gewichtiges Argument der kommerziellen Anbieter liegt aber nicht in der Vertraulichkeit der Verbindungen, sondern in der Umgehung des Geoblockings: Einfach die Software des Anbieters nutzen, eine IP-Adresse des gewünschten Landes auswählen und schon können Sie sich auch Videos oder Sportübertragungen ansehen, die aus Deutschland nicht abrufbar sind. Oder umgekehrt, wenn Sie sich gerade im Ausland befinden.

Anonym sind Sie damit indes nicht, denn die Adressräume wurden von den Anbietern reserviert. Wenn Sie auf Anonymität angewiesen sind, müssen Sie darauf vertrauen, dass der Anbieter Ihre tatsächliche IP-Adresse und Ihre Daten für sich behält. Einen Anbieter, mit dem wir gute Erfahrun-

gen gemacht haben, nennen wir am Ende des Artikels. Um wirklich anonym zu bleiben, müssten Sie sich aber eher mit einer Lösung wie dem TOR-Browser anfreunden. Wenn es aber in erster Linie darum geht, sichere Verbindungen in einer fremden Netzumgebung aufzubauen, ist ein VPN perfekt. Wie Sie dies erreichen, zeigen wir anhand von Beispielen mit sehr unterschiedlichem technischen Aufwand.

Der schnelle Weg zum VPN: Die Fritzbox

Ein einfacher Weg zum VPN besteht darin, die eigene Fritzbox als VPN-Server zu nutzen. Befinden Sie sich also im fremden WLAN eines Cafés oder Hotels, stellen Sie eine Verbindung mit Ihrer heimischen Fritzbox her. Rufen Sie anschließend eine Internet-URL auf, wird diese von Ihrer Fritzbox ausgeliefert. Das funktioniert problemlos, wenn Ihr Anschluss via IPv4 erreicht werden kann. Die Nutzer eines Kabelanschlusses benötigen einen regulären Dual-Stack. Zeigt die Fritzbox, dass sie DS-Lite verwendet, kommt diese VPN-Methode nicht infrage.

Die Einrichtung des VPN-Zugangs verläuft bei allen anderen Anschlüssen so: Als Basis dient der von AVM angebotene Cloud-Dienst „MyFritz!“. Melden Sie sich an Ihrer Fritzbox an und gehen Sie auf „Internet → MyFritz!-Konto“. Sofern Sie noch kein solches Konto besitzen, geben Sie eine gültige E-Mail-Adresse ein und folgen den Schritten für die Registrierung. Im Verlauf müssen Sie die E-Mail-Adresse bestätigen, werden auf die AVM-Seite weitergeleitet und legen ein (starkes!) Passwort an.

Sobald Sie ein solches Konto besitzen, zeigt Ihnen der Besuch des Menüs, dass die Fritzbox mit dem Dienst verbunden ist, ferner auch die öffentliche Internetadresse der Fritzbox. Unter dem Feld mit der URL befindet sich der Schalter für die Einrichtung eines Nutzers, der auf die Fritzbox extern zugreifen darf. Klicken Sie auf „FritzBox-Benutzer einrichten“. Nun vergeben Sie einen Benutzernamen und ein Passwort. Nach „Übernehmen“ muss die Eingabe mit einer Tastenkombination eines angeschlossenen Telefons bestätigt werden oder mit der Fritz-Taste auf dem Router. Um jetzt den Zugang zu testen, benötigen Sie eine externe Verbindung etwa über das Smartphone mit mobilen Daten und bei ausgeschaltetem WLAN. Sie nutzen dabei die erwähnte URL und verwenden den Benutzernamen und das Passwort des gerade angelegten Benutzers. Jetzt wechseln Sie über „System → Fritzbox-Benutzer“ und klicken auf das Stiftsymbol neben dem Benutzer. Hier aktivieren Sie dann die Option „VPN“. Nach „Übernehmen“ ist der Zugang realisiert.

Im nachfolgenden Dialog sehen Sie eine Zusammenfassung der Zugangsdaten. Drucken Sie sich diese am besten aus. Mit diesen Informationen können Sie jetzt auf anderen Geräten eine VPN-Verbindung herstellen (siehe Kasten „VPN-Zugang nutzen“).

```
root@sla-Inspiron-15-5518: /etc/wireguard
sla@sla-Inspiron-15-5518:~$ sudo -i
[sudo] Passwort für sla:
root@sla-Inspiron-15-5518:~# cd /etc/wireguard
root@sla-Inspiron-15-5518:/etc/wireguard# umask 077
root@sla-Inspiron-15-5518:/etc/wireguard# wg genkey | sudo tee privatekey | wg pubkey | sudo tee pubkey
AxdTy8fs1cwvPii8TyKFUynits2zhlyQe/aUZ+ti0QI=
root@sla-Inspiron-15-5518:/etc/wireguard# ls
privatekey  pubkey
```

Um Wireguard einzusetzen, müssen auf dem Server und dem Client Schlüsselpaare erzeugt werden, die dann wechselseitig hinterlegt werden.

```
root@sla-Inspiron-15-5518: /etc/wireguard
root@sla-Inspiron-15-5518: /etc/wireguard
 GNU nano 5.6.1                          /etc/wireguard/wg0.conf
[Interface]
PrivateKey =
Adress = 192.168.207.1/24
ListenPort = 51820
SaveConfig = true


PostUp = ufw route allow in on wg0 out on eth0
PostUp = iptables -t nat -I POSTROUTING -o eth0 -j MASQUERADE
PostUp = ip6tables -t nat -I POSTROUTING -o eth0 -j MASQUERADE
PreDown = ufw route delete allow in on wg0 out on eth0
PreDown = iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
PreDown = ip6tables -t nat -D POSTROUTING -o eth0 -j MASQUERADE
```

Die Verbindungen und erlaubten Clients werden in Wireguard in einer Konfigurationsdatei hinterlegt.

Wireguard: Eigener VPN-Server unter Ubuntu

Mehr Möglichkeiten haben Sie, wenn Sie einen eigenen VPN-Server einrichten. Mit Wireguard gibt es eine relativ einfach zu installierende Lösung. Um Wireguard benutzen zu können, benötigen Sie einen Rechner, auf dem Linux läuft und der über das Internet zu erreichen ist. Das darf auch eine virtuelle Maschine im Internet sein. Das ist vor allem dann eine gute Lösung, wenn Sie den VPN-Zugang nur verwenden wollen, wenn Sie unterwegs sind.

VPN-PROTOKOLLE

Für die sichere Kommunikation via VPN müssen sich Client und Server verständigen. Grundlage ist dabei ein gemeinsames Datenprotokoll. Die drei wichtigsten sind folgende:

- **Open VPN** ist quelloffen und recht verbreitet, beim Aufbau eines Servers allerdings nicht einfach zu durchschauen. Software wie Pi VPN räumt aber viele Hürden aus dem Weg. Auf Open VPN basieren auch häufig die Ansätze kommerzieller Anbieter.
- **Wireguard** ist eine freie VPN-Software, die ein eigenes Protokoll nutzt und für die meisten Betriebssysteme zur Verfügung steht.
- **L2TP/IPSec** sind streng genommen zwei Protokolle, die stets in Kombination genutzt werden. Es wird häufig im professionellen Umfeld genutzt, wenn Administratoren Homeoffice-Arbeitsplätze oder externe Standorte mit dem Unternehmensnetzwerk verbinden wollen. Die Fritzbox nutzt ein Derivat dieses Protokolls für ihr VPN.

Daheim starten Sie einfach die Instanz beim Hoster und nach Ihrer Rückkehr wird sie wieder beendet.

Zur Installation von Wireguard genügt bei vielen Distributionen ein Befehl:

```
sudo apt install wireguard
```

Nutzen Sie eine LTS-Version von Ubuntu, wie das bei virtuellen Maschinen oft der Fall ist, werden Sie die Paketquellen erst ergänzen müssen. Dies folgt dem bekannten Muster:

```
sudo add-apt-repository
  ppa:wireguard/wireguard
sudo apt update
sudo apt install wireguard
```

Im nächsten Schritt sorgen Sie dafür, dass alle Pakete, die an der Wireguard-Schnittstelle ankommen, weitergeleitet werden. Dazu öffnen Sie die Datei „/etc/sysctl.conf“. Hier tragen Sie zwei Zeilen ein:

```
net.ipv4.ip_forward=1
net.ipv6.conf.all.forwarding=1
```

Eventuell sind die Zeilen vorhanden und es genügt, das Kommentarzeichen „#“ zu entfernen. Speichern Sie die Datei und aktualisieren Sie die Konfiguration mit diesem Befehl:

```
sysctl -p
```

Die Kommunikation bei Wireguard wird mittels öffentlicher und privater Schlüssel auf dem Server und dem Client abgesichert. Deswegen muss das Schlüsselpaar zunächst auf dem Server angelegt werden. Das geht – mit root-Recht – so:

```
cd /etc/wireguard
umask 077
wg genkey | sudo tee privatekey | wg
  pubkey | sudo tee pubkey
```

Anschließend liegen im Verzeichnis „/etc/wireguard“ zwei Dateien, die unschwer als privater und öffentlicher Schlüssel zu erkennen sind. Jetzt kommt die einzige Hürde. Wireguard arbeitet als Router in seinem VPN-Netz. In der Konfiguration müssen Sie daher eine virtuelle Netzwerkschnittstelle schaffen, die hier mit „wg0“ bezeichnet werden soll. Der Router muss einen Adressraum verwalten, der sich mit den IP-Adressen Ihres eigentlichen Netzwerks nicht in die Quere kommt. Mit einem Editor legen Sie die Datei „/etc/wireguard/wg0.conf“ an und tragen dort folgende Zeilen ein:

```
[Interface]
PrivateKey = [privaten Key hier
  eintragen]
Address = 192.168.207.1/24,
  fd0d:86fa:c3bc::1/64
ListenPort = 51820
SaveConfig = true
```

Ein Wort zu den Adressen. Der erste Wert definiert den IPv4-Bereich 192.168.207.1 bis 192.168.207.254, der im Netzwerk des Autors nicht verwendet wird. Wenn Sie IPv6-Adressen nutzen wollen, ist die Schaffung einer sogenannten „Unique Local Address“ nicht so einfach, weil es nahezu unendliche Möglichkeiten gibt. Unter *https://simpledns.plus/private-ipv6* können Sie sich einen zufällig generierten Adressraum erstellen lassen. Das erleichtert die Sache. Speichern Sie die Datei.

Jetzt geht es an das Forwarding der Pakete. Dazu finden Sie zunächst die Netzwerkschnittstelle des Servers heraus, die öffentlich erreichbar ist. Führen Sie in einem Terminal das Kommando

```
ip route list default
```

aus. Bei den ausgegebenen Strings suchen Sie nach dem Eintrag mit dem Zusatz „dev“. Dahinter steht dann der Name der Schnittstelle, etwa „eth0“. Jetzt öffnen Sie erneut die Datei „/etc/wireguard/wg0.conf“ und fügen am Ende der Datei diesen Codeblock ein.

```
PostUp = ufw route allow in on wg0
  out on eth0
PostUp = iptables -t nat -I
  POSTROUTING -o eth0 -j MASQUERADE
PostUp = ip6tables -t nat -I
  POSTROUTING -o eth0 -j MASQUERADE
PreDown = ufw route delete allow in
  on wg0 out on eth0
PreDown = iptables -t nat -D
  POSTROUTING -o eth0 -j MASQUERADE
PreDown = ip6tables -t nat -D
  POSTROUTING -o eth0 -j MASQUERADE
```

Nach dem Speichern der Datei müssen Sie noch der Firewall gestatten, Datenverkehr zum Port von Wireguard durchzulassen:

```
sudo ufw allow 51820/udp
sudo ufw allow OpenSSH
```

Mit root-Recht stoppen Sie einmal die Firewall (*sudo ufw disable*) und starten Sie erneut (*sudo ufw enable*), damit die Änderungen aktiv werden. Wenn Wireguard beim Start des Systems aktiviert werden soll, konfigurieren Sie noch den Dienst:

```
sudo systemctl enable wg-quick@wg0.
  service
sudo systemctl start wg-quick@wg0.
  service
```

Dies gilt für alle Ubuntu & Co. mit Systemd.

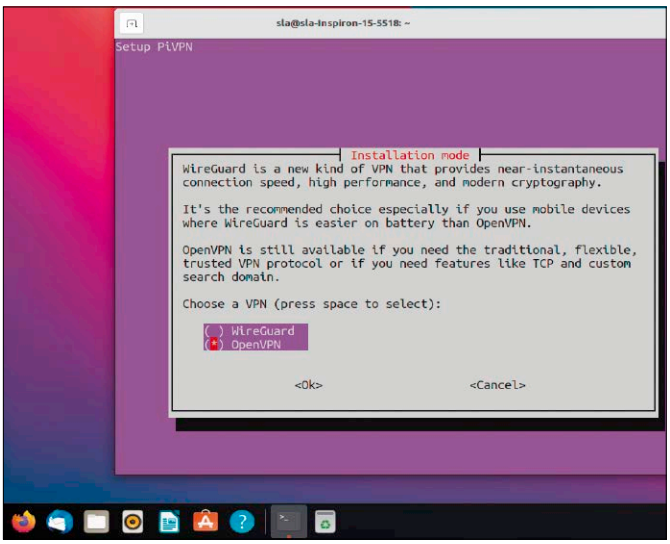
Wireguard: Clientgeräte einrichten

Für mobile Clients mit Android und iOS gibt es in den App Stores die passende Software zur Einrichtung. Soll ein Linux-Client eingerichtet werden, installieren Sie darauf Wireguard. Anschließend müssen Sie dort – wie gezeigt – ein Schlüsselpaar erzeugen. Mit einem Editor wie Nano

```
sudo nano /etc/wireguard/wg0-
  client.conf
```

legen Sie auf dem Client eine eigene Konfigurationsdatei an. Bei der Wahl des Namens sind Sie völlig frei, die Ähnlichkeit mit der Serverdatei ist hier beabsichtigt, um die Unterschiede deutlich zu machen. Die Datei erhält zunächst einmal folgenden Inhalt:

```
[Interface]
PrivateKey = [privaten Key hier
  eintragen]
# Wir zählen einfach die IP-Adresse
  um "1" hoch
```



Pi VPN wurde eigentlich für den Raspberry Pi entwickelt. Es funktioniert aber auch unter Ubuntu und anderen Distributionen und vereinfacht die Einrichtung von Open VPN erheblich.

```
Address = 192.168.207.2/24
Address = fd0d:86fa:c3bc::2/64
[Peer]
PublicKey = [öffentlicher Key des
 Servers]
AllowedIPs = 192.168.207.1/24
Endpoint = [Server-IP oder Domain-
 Name]:51820
```

Das ist die grundlegende Konfiguration. Wenn Sie vorhaben, jeglichen IP-Verkehr durch den Tunnel zu schicken, müssen noch ein paar Ergänzungen vorgenommen werden. Diese lesen Sie am besten in der offiziellen Dokumentation des Projekts nach. Sie müssen dem Server anschließend noch mitteilen, dass sich der Client verbinden darf. Das geht mit einem einfachen Kommando im Terminal:

```
wg set wg0 peer [öffentlicher
 Schlüssel des Clients] allowed-ips
 192.168.207.2/24
```

Läuft der Server, starten Sie eine Verbindung auf dem Client im Terminal:

```
sudo wg-quick up wg0
```

Damit sollte die Verbindung stehen.

VPN mit Raspberry Pi und Open VPN

Eine Alternative zu Wireguard ist Open VPN. Damit und mit einem Raspberry Pi können Sie einen VPN-Server verblüffend einfach umsetzen. Möglich macht dies das Projekt Pi VPN (*https://www.pivpn.io/*). Ursprünglich ausschließlich für Open-VPN-Verbindung gestartet, kann es heute auch das Wireguard-Protokoll verwenden. Die Installation und Einrichtung sind inzwischen auch nicht mehr ausschließlich auf den Raspberry beschränkt.

Mit dem Kommando

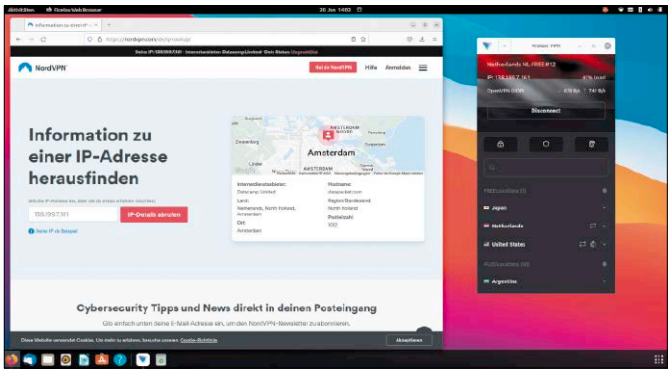
```
curl -L https://install.pivpn.io |
 bash
```

starten Sie die Einrichtung und Konfiguration, die problemlos bei IPv4-Adressen funktioniert. Hier gelten also die gleichen Einschränkungen am Kabelanschluss, wie sie bereits erwähnt wurden.

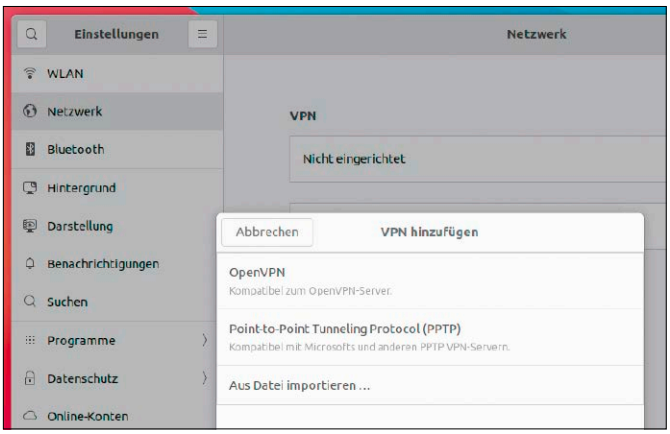
Das Programm begleitet Sie durch alle Schritte inklusive der optionalen Auswahl eines alternativen DNS-Servers. Auch auf die Portweiterleitung am Router werden Sie hingewiesen. Hier kann tatsächlich nichts schiefgehen. Einmal abgeschlossen, legen Sie mittels

```
pivpn add
```

einen Client an, der dann auch die Zugangsdatei erzeugt.



Der kommerzielle Anbieter Proton aus der Schweiz hat einen untadeligen Ruf. Die Installation und Nutzung gehen leicht von der Hand.



Open VPN erzeugt für Clients eine Zugangsdatei. Deren Informationen lassen sich etwa im Network-Manager von Ubuntu einfach importieren.

Kommerzieller Anbieter: Proton VPN

Kommerzielle Angebote reduzieren den technischen Aufwand auf ein Minimum. Ob der VPN-Anbieter allerdings Ihre Daten speichert oder ob Sie tatsächlich anonym surfen, ist eine Frage des Vertrauens. Einen untadeligen Ruf genießt das Schweizer Unternehmen Proton, das auch einen kostenfreien VPN-Zugang anbietet. Dieser finanziert sich aus den Gebühren der Nutzer, die sich für das kostenpflichtige Abo entschieden haben, das mehr Geschwindigkeit und mehr Konfigurationsoptionen bietet (für fünf bis zehn Euro pro Monat). Die Einrichtung unter Ubuntu ist extrem einfach. Sie holen sich von der Website *https://protonvpn.com* das Installationspaket und installieren es per Doppelklick.

Damit werden zunächst nur die Paketquellen hinzugefügt. Nach dem Update der Quellen installieren Sie mit

```
sudo apt update
sudo apt install protonvpn
```

die Software.

Das war dann auch schon alles: Programm starten, die Zugangsdaten zum Proton-Account eintragen – das genügt und Sie können die gewünschte geografische Verbindung auswählen und nutzen. ■

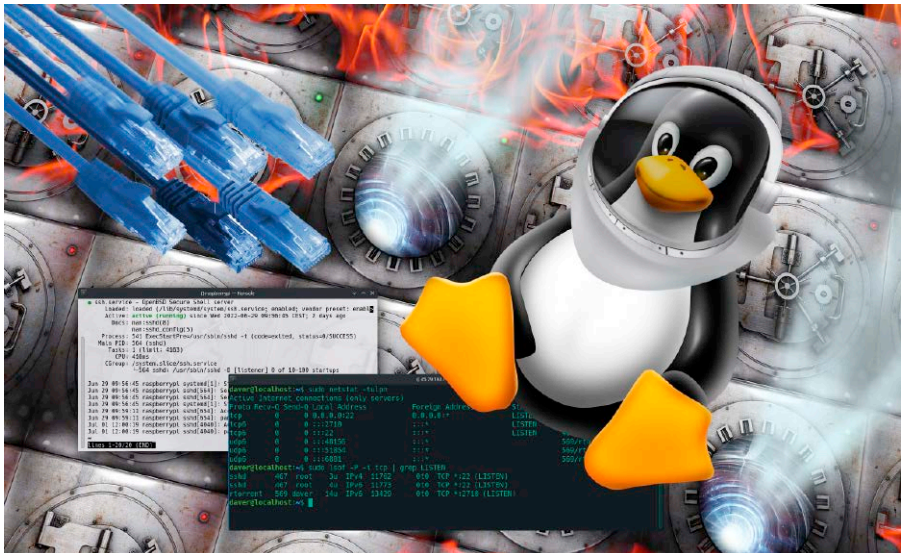
VPN-ZUGANG NUTZEN

Wie nutzen Sie eine VPN-Verbindung auf den Clients? Kommerzielle Anbieter stellen entweder eine eigene Software für die Einwahl zur Verfügung oder zumindest die passende Konfigurationsdatei. Unter Ubuntu können Sie unter den Einstellungen im Bereich „Netzwerk“ und „VPN“ eine neue Verbindung mit einem Klick auf das Pluszeichen hinzufügen. Sie haben anschließend die Auswahl, die Details aus einer Datei zu importieren. Solche Dateien erzeugt auf Wunsch auch Open VPN. Bei Wireguard nutzen Sie entweder die passende App für mobile Geräte oder müssen, wie im Haupttext beschrieben, die Software installieren und die Konfiguration anpassen.

Schotten dicht: Ports und Dienste

Was läuft hier? Auf Linux-Systemen, die schon lange in Betrieb sind, einige Experimente mitgemacht haben oder von anderen Personen eingerichtet wurden, ist eine Überprüfung der laufenden Dienste und geöffneten Ports empfehlenswert.

VON DAVID WOLSKI



Die großen, gut gepflegten Linux-Distributionen Debian, Ubuntu, Fedora und Open Suse sind auch für den Einsatz auf Servern geschaffen. Sie müssen im Grundzustand, also nach einer Installation, in einer sicheren Konfiguration vorliegen und dürfen nicht ungefragt Serverdienste starten, die Ports ins Netzwerk öffnen. Wer schon mal kleine Server von der Sorte Raspberry Pi eingerichtet hat, weiß, dass dieser geschlossene Ansatz auf Kosten von Komfort und Bequemlichkeit geht. Er verhindert aber, dass ein Linux-System schon in seiner Standardkonfiguration angreifbar ist oder mit unzureichenden Standardpasswörtern Zugriff auf laufende Serverdienste eröffnet.

Übersicht: Server und geöffnete Ports

Auf einem Server verschaffen Tools in der Kommandozeile per Innenansicht den Überblick, welche laufenden Prozesse auf einem Netzwerkport geöffnet haben. Diese bieten einen unverstellten Blick auf die Zuordnung von Ports und Diensten über den Kernel, ohne dabei einen vorgeschalteten Portfilter zu beachten.

Netstat: Der traditionelle Weg, geöffnete Ports anzuzeigen, führt über das Tool netstat. In aktuellen Linux-Distributionen ist es nicht mehr vorinstalliert, liegt aber im Paket „net-tools“ in den verbreiteten Linux-Distributionen bereit und ist in Debian/Ubuntu mit dem Befehl

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

zu installieren. Anschließend liefert

```
sudo netstat -tulp
```

eine tabellarische Übersicht zu Protokollart (TCP oder UDP), verwendeten Netzwerkadressen und verbundenen Adresse bei aktiven Verbindungen. In den letzten beiden Spalten namens „PID/Program name“ und „State“ zeigt das Tool Status und Prozessnamen der Dienste. Steht beim Status „LISTEN“, dann wartet der Prozess auf eingehende Verbindungen. Die Portzuordnung erfolgt in der Spalte „Local Address“ hinter einem Doppelpunkt. Steht hier also beispielsweise „0.0.0.0:22“, bedeutet das, dass ein Dienst auf allen verfügbaren Netzwerkadressen („0.0.0.0“) auf dem Port 22 lauscht. Dies ist üblicherweise der SSH-Server und am Ende der Zeile werden hier eine Prozessnummer und der Prozessname angegeben sein – „sshd“ in diesem Beispiel.

Lsof: In neueren Linux-Distributionen wird zunehmend statt dem älteren, nicht stetig weiterentwickelten netstat das Tool lsof empfohlen. Die Eingabe

```
sudo lsof -P -i tcp | grep LISTEN
```

erstellt eine ähnliche, etwas übersichtlichere Tabelle lauschender Prozesse mit Namen und Portnummer. Die Dienst- und Prozessnamen stehen hier gleich am Anfang jeder Zeile.

Zuordnung von Prozess und Dienst: Zum grundsätzlichen Verständnis offener Ports gehört die Tatsache, dass sich ein Netzwerkport nicht wie eine Tür schließen lässt. Vielmehr muss der verantwortliche Task oder Dienst beendet sein, um damit auch den Port zu schließen. Noch wichtiger ist die Tatsache, dass offene Ports im lokalen Heimnetz kein Risiko bedeuten, solange diese nicht per Portfreigabe im Router für das Internet geöffnet werden. Die von lsof oder netstat angezeigten Namen verweisen

entweder auf ein Programm oder auf einen Dienst. Die meisten Linux-Distributionen nutzen heute Systemd zur Diensteverwaltung und ein Befehl wie dieser

```
sudo systemctl status sshd
```

zeigt dann Informationen zum befragten Dienst an. In diesem Beispiel handelt es sich um den Open-SSH-Server. Alle diese Schritte dienen zur Identifizierung, was auf einem Linux-System unter der Haube läuft. Wenn es klar ist, dass ein Dienst überflüssig ist, so hilft ein Trick dabei, diesen testweise abzuschalten: Das Kommando

```
sudo shutdown -r 10
```

setzt einen automatischen Neustart des Systems in zehn Minuten an und

```
sudo systemctl stop sshd
```

stoppt den angegebenen Dienst, hier den Open-SSH-Server. Nun hat man zehn Minuten Zeit zu testen, ob der Linux-Server weiterhin wie gewünscht funktioniert. Klar, ausgerechnet den SSH-Dienst abzuschalten, dürfte in den meisten Fällen kontraproduktiv sein, denn nun ist keine neue Anmeldung mehr über das Netzwerk per SSH möglich. Dies ist aber nicht weiter schlimm, denn nach zehn Minuten startet der Server neu und reaktiviert den Dienst wieder. Erst das Kommando

```
sudo systemctl disable --now sshd
```

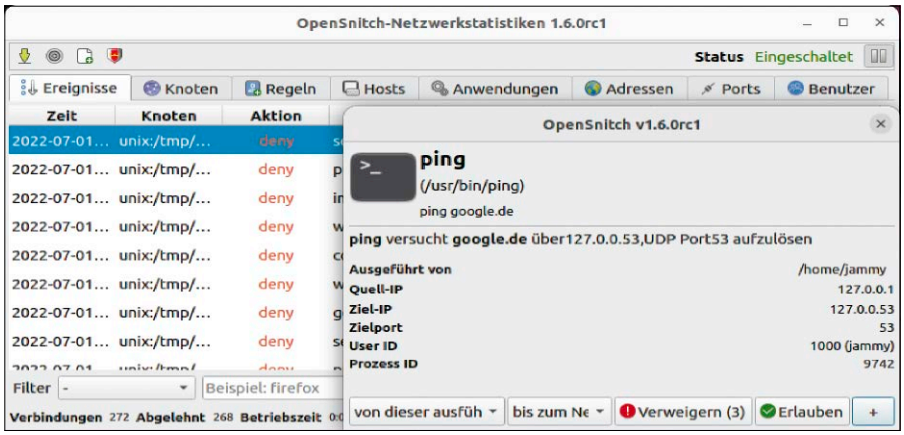
würde den angegebenen Dienst dauerhaft abschalten.

Opensnitch: Check für Desktopsysteme

Von Mac-OS X ist das Tool Little Snitch bekannt, das die angeforderten Netzwerkverbindungen von Programmen überwacht. Das grafische Python-Tool Opensnitch überträgt das Konzept auf den Linux-Desktop und erlaubt einen Blick darauf, was Anwendungen ins Netzwerk senden und von dort empfangen. Das englischsprachige Tool für Fortgeschrittene liegt unter *https://github.com/evilsocket/opensnitch/releases* auf der Github-Webseite des Entwicklers. Die Installation unter Ubuntu und Abkömmlingen wie Linux Mint erfolgt über die angebotenen DEB-Dateien „opensnitch_[Version]_amd64.deb“ und „python3-opensnitch-ui_[Version].deb“, die man in ein leeres Verzeichnis herunterlädt und dort dann mit dem Befehl

```
sudo dpkg -i *.deb
sudo apt -f install
```

installiert. Der zweite Befehl löst die weiteren Abhängigkeiten auf und Opensnitch wird dann noch einige Python-Pakete automatisch nachinstallieren.



Eingehende und ausgehende Verbindungen aufzeigen: Opensnitch ist eine Desktopfirewall (Anwendungsfirewall) für Linux, die Programmen den Netzwerkzugriff auch verweigern kann.

Ubuntu ab Version 22.04: Bevor die Oberfläche von Opensnitch funktioniert, ist noch die Installation einer zusätzlichen Bibliothek mittels

```
sudo apt install python3-pip
pip3 install --ignore-installed
  grpcio
```

nötig. Auf dem Linux-System startet Opensnitch einen Systemd-Dienst und legt ein Symbol im Infobereich der Systemleiste ab, das in einem Fenster die Netzwerkverbindungen nach Prozessen aufschlüsselt. Außerdem schlägt Opensnitch immer Alarm und zeigt die Verbindungsdetails an, sobald eine Anwendung zum ersten Mal eine Netzwerkverbindung herstellt. Die Verbindung kann der Button „Allow connection“ erlauben oder mit „Block connection“ verbieten. Wer das Tool später nicht mehr benötigt, kann es mit dem Befehl

```
sudo apt remove --purge opensnitch
```

wieder vom System entfernen (und damit auch den zugehörigen Wächterdienst).

Paketfilter: UFW-Regeln erstellen

Paketfilter sind sinnvoll, wenn Serverports für das Internet freigegeben sind und somit Dienste öffentlich nach außen anbieten. Auf üblichen Desktopsystemen ist dies standardmäßig nicht der Fall und Linux-Distributionen installieren deshalb auch keine Firewallregeln. Ubuntu macht es aber heute mit dem Tool ufw (Uncomplicated Firewall) vergleichsweise einfach, Regeln für das nicht ganz triviale Kernel-Paketfilter zu erstellen.

Mit dem Kommando

```
sudo apt install ufw
```

ist das Tool bei Bedarf installiert. Die Syntax ist einfach gehalten und erstellt im Hintergrund die komplexeren nftables-Regeln. Um beispielsweise nur den Port 22 (SSH) zu erlauben, genügt dieser Befehl:

```
sudo ufw allow 22
```

Anschließend wird die Firewall mit

```
sudo ufw enable
```

gestartet und mit

```
sudo ufw status
```

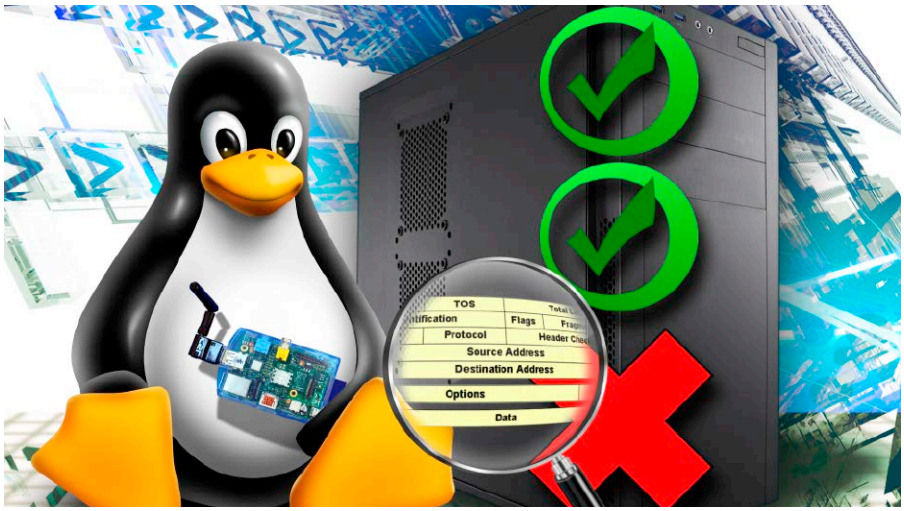
überprüft. ■

„WELL KNOWN PORTS“: BEKANNTE HAUSNUMMERN

Die Portnummern zwischen 1 und 1023 sind reservierte Ports für häufig verwendete Serverdienste, auf die Clients einen typischen Dienst erwarten dürfen. So nutzen beispielsweise Webserver für HTTP den Port 80 und für HTTPS den Port 443. Diese „Well Known Ports“ ermöglichen den Clients die Verbindung zu Servern, ohne dass eine explizite Konfiguration notwendig wäre. Um die Organisation dieser Portnummern kümmert sich die Internet Assigned Numbers Authority (IANA) und stellt die aktuelle Liste mit weiteren Dokumenten unter *www.iana.org/assignments/port-numbers* bereit. Eine deutschsprachige Übersicht hat die Wikipedia (Liste_der_standardisierten_Ports).

Einbrüche erkennen

Wer will auf meinen Linux-Server? Gibt es eventuell doch eine übersehene oder ungepatchte Schwachstelle, die ungebetene Gäste anlockt? Aktive Überwachungsmethoden informieren über verdächtige Aktivitäten auf Linux-Servern.



VON DAVID WOLSKI

Erschwingliche Ein-Platinen-Computer und günstige Cloudinstanzen haben den Aufwand erheblich gesenkt, einen Linux-Server zu betreiben. Bei jedem von außen erreichbaren Server sind aber rigorose Sicherheitsvorkehrungen Pflicht, die das System sicher halten und einen Einbruch unwahrscheinlich machen. Das betrifft auch heimische Miniserver, die nur an einer DSL-Leitung hängen und lediglich über eine dynamische Hostadresse erreichbar sind. Auch dort werden ungebetene Besucher anklopfen und Einlass begehren. Dieser Beitrag zeigt erst zwei einfache Methoden, das System per Logauswertung im Auge zu behalten, und geht dann auf das Intrusion Detection System (IDS) Tripwire ein.

Vor Einbrüchen: Das System checken

Ein Linux kann nur so nur sicher sein, wie es seine Konfiguration zulässt. Automatisierte Checks helfen, potenziell unsichere Einstellungen, manipulierte Dateien und typische Konfigurationsfehler aufzuspüren. Je nachdem, welche Serverdienste auf einem System aktiv sind, wählt Lynis die passenden Tests aus seiner Datenbank und liefert eine englischsprachige Auswertung in seiner eigenen Logdatei. Die stets aktuelle Version von Lynis ist auf der Entwickler-Seite bei Github verfügbar und mit einigen Befehlen schnell eingerichtet: Zuerst holt

```
git clone https://github.com/
  CISOfy/lynis
```

die Dateien von Github. Dann geht es mit

```
cd lynis
```

in das Verzeichnis, wo der Befehl

```
sudo chown -R 0:0 *
```

den Scripts die benötigten Berechtigungen gibt. Der Befehl

```
sudo ./lynis audit system
```

führt das Tool mit sudo-Recht aus. Lynis zeigt den Fortschritt und Warnungen im Terminalfenster. Nach dem Abschluss des Testlaufs präsentiert Lynis Empfehlungen zur Absicherung des Systems sowie URLs mit Hintergrundinformationen. Die Warnung zu „systemd-analyze security“ kann man dabei ignorieren, denn dabei geht es nur um optionale Sandbox-Funktionen von Systemd, welche Linux-Distributionen in ihrer Standardkonfiguration nicht nutzen.

Logwatch: Über Angriffe informiert

Eine schnell eingerichtete automatische Auswertung von Logdateien, die Angriffsmuster über das Netzwerk zeigt, liefert das Programm Logwatch. Es erstellt täglich einen Bericht über ungewöhnliche Vorkommnisse auf dem System. Auf Servern mit einem Mailserver wie Postfix/Sendmail/Exim2 kann es den Bericht auch per Mail an einen User auf dem lokalen System senden, die dieser per „mutt“ abruft – also mit dem Mailprogramm in der Shell. Soll ein Benutzer wie root auf dem System die Zusammenfassung im lokalen Postfach erhalten, so genügt dazu auch ein lokaler Mailserver ohne Verbindung zu einem anderen SMTP-Server im Internet.

Debian, Raspbian, Ubuntu, Fedora, Open Suse und Arch bieten alle das Paket „logwatch“ in ihren Paketquellen. In Debian & Co. wird es mit

```
sudo apt install logwatch
```

installiert. Das Kommando

```
sudo logwatch
```

präsentiert im Terminal eine Übersicht zu Ereignissen. Erkannte Scans gegen einen Webserver wie Apache und Nginx sowie SSH-Angriffe sind ganz oben aufgelistet.

Tripwire: Einen Stolperdraht spannen

Auf wichtigen oder exponierten Linux-Servern kann ein IDS (Intrusion Detection System) helfen, unautorisierte Manipulationen an vordefinierten Dateien sofort zu erkennen. Prominente Konfigurationsdateien von Webservern bieten sich dafür an. Das wäre für einen Server der größte anzunehmende Unfall und das System wird danach als Ganzes nicht zu retten sein. Die Gewissheit darüber ist aber enorm wichtig, denn

unentdeckte Einbrüche, übernommene Server unter fremder Kontrolle sind ein wahrer Alptraum.

Ein lange bewährtes IDS auf Dateisystemebene ist Tripwire („Stolperdraht"). Es kontrolliert Dateien nach vorher erstellten Checksummen, welche in einer geschützten signierten Datenbank hinterlegt sind. Auf Änderungen hin schlägt Tripwire Alarm – nach einem manuellen Check, automatisch per E-Mail oder auch in einer eigenen Logdatei. Zu beachten ist, dass Tripwire auch bei unbeaufsichtigten Updates anschlägt und die Berichte dann sehr umfangreich werden. Es verlangt daher etwas Übung, die Berichte zu lesen. Tripwire ist dennoch einfach genug, um beispielsweise das Verzeichnis eines Webservers und bestimmte Konfigurationsdateien im Auge zu behalten. Die Installation gelingt in den tonangebenden Distributionen über die Standard-Paketquellen, in Debian/Ubuntu über dieses Kommando:

```
sudo apt install tripwire
```

Die Installation sorgt auch gleich für die erste Initialisierung des Wächters mit einigen Abfragen.

1. Mailversand: Soll der Administrator Mails von Tripwire erhalten, so kann hier Postfix konfiguriert werden. „Nur lokal" ist die richtige Option für den Mailempfang nur auf dem gleichen System.

2. Passwörter: Die Abfrage nach der Erzeugung der Site-Passphrase für Tripwire und des lokalen Schlüssels beantwortet man mit „Ja". Ebenso die Frage, ob die Tripwire-Konfigurationsdatei und Richtliniendatei neu erzeugt werden sollen. Gut merken muss man sich die dann vergebenen neuen Passwörter für die Tripwire-Administration, denn sie werden später immer wieder verlangt.

3. Neue Regel definieren: In diesem Beispiel soll Tripwire das Apache-Konfigurationsverzeichnis „/etc/apache2/sites-available" mitüberwachen. Dazu öffnet man die Datei „/etc/tripwire/twpol.txt" mit root-Recht oder vorangestelltem „sudo" in einem Texteditor. Ans Ende der Datei kommen folgende Zeilen:

```
(
rulename = "Apache2",
severity= $(SIG_HI)
)
{
/etc/apache2/sites-available ->
 $(SEC_CRIT);
}
```

Lynis in Aktion: Der Scanner präsentiert gefundene Sicherheitslücken, potenzielle Probleme und Empfehlungen, um die Sicherheit eines Linux-Systems systematisch zu verbessern.

Tripwire schlägt an: In unserem hinzugefügten überwachten Verzeichnis „/etc/apache2/sites-available" gab es Änderungen an Dateien, wie Tripwire in seinem Bericht auflistet.

Anschließend erzeugt das Kommando

```
sudo twadmin -m P /etc/tripwire/
 twpol.txt
```

die Regel-Datei neu und fragt dazu die zuvor vergebene Site-Passphrase ab.

4. Datenbank erstellen: Nun soll Tripwire die Checksummen der überwachten Dateien erstellen, was der Befehl

```
sudo tripwire --init
```

nach der Eingabe des Tripwire-Passworts („local passphrase") erledigt. Dieser Schritt ist immer nach Änderungen am System und Aktualisierungen notwendig, um neue Checksummen zu erzeugen.

5. Check ausführen: Eine manuelle Überprüfung führt nun der Befehl

```
sudo tripwire --check
```

aus. Wurde die Apache-Konfiguration zwischenzeitlich geändert, so moniert die Ausgabe von Tripwire dies im Abschnitt „Rule Name: Apache2" und listet dort die betroffenen Dateien auf. ■

VIRENSCANNER: FÜR DATEISERVER WICHTIG

Für ein stets aktualisiertes Linux-System ist Malware kaum ein Risiko, zumal die Zahl von wirksamen Linux-Viren verschwindend gering ist. Eine reale Gefahr ist aber die versehentliche Verbreitung von Windows-Viren und Würmern in Netzwerken über einen Linux-Dateiserver, dem zwar die Malware nichts ausmacht, der diese aber im Netzwerk verteilt. Linux-Anwender sollten daher verdächtige Downloads, insbesondere ausführbare Windows-Dateien, zum Check auf den von Google betriebenen Onlinedienst Virustotal (*www.virustotal.com*) hochladen und analysieren lassen.

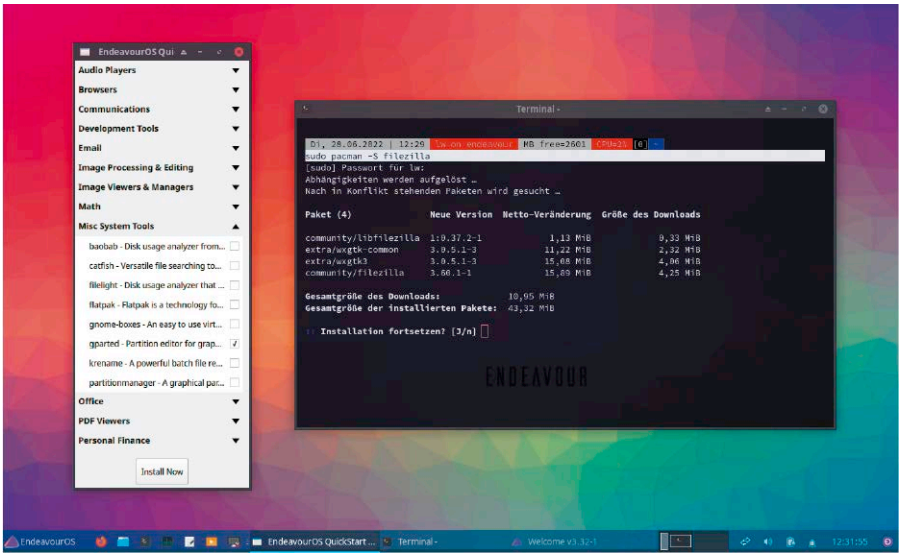
Für automatisierte Scans per Kommandozeile gibt es für Linux den Virenscanner Clam AV. Die Erkennungsraten für Malware liegen bei Tests bei 76 Prozent, damit ist Clam AV im Mittelfeld. Verweise auf Paketquellen für verbreitete Linux-Distributionen liefert die Projektwebseite. Für Nextcloud als Dateiserver gibt es Clam AV übrigens auch als Plug-in.

Endeavour-OS: Flottes Arch

Wie alle Linux-Fans macht die LinuxWelt-Redaktion periodisch den Klick nach distrowatch.com zum Distributionsranking. Dass derzeit (Anfang Juli) Endeavour-OS ganz vorne liegt, trifft sich gut: Das System ist soeben in neuer Version erschienen.

VON HERMANN APLELBÖCK

Das jüngste Endeavour-OS 22.6 (ab hier kurz „EOS“) hat vor allem die ARM-Unterstützung für Raspberry- und Odroid-Platinen ausgebaut. EOS ist Nachfolger des eingestellten Antergos und hat denselben Anspruch wie das bekanntere Manjaro, nämlich mit einem grafischen Installer den Zugang zu Arch Linux zu vereinfachen. Laut Distrowatch hat EOS Manjaro inzwischen den Rang abgelaufen und liegt aktuell auf Platz 2 vor Mint, Manjaro, Ubuntu, Debian & Co. Generell scheinen Arch-Derivate und deren Rolling-Release-Modell derzeit hoch im Kurs: Sie gelten als besonders schnell und stets aktuell. Nachteile sind gelegentliche Paketkonflikte, eine Fokussierung auf das Terminal und eventuell nicht vollständig deutsch lokalisierte Komponenten. Die Frage dieses Artikels ist daher, ob sich EOS als das derzeit wohl beste Arch als Alltags-Desktop eignet?



Schnelles Arch: Das reaktionsfreudige Endeavour-OS (hier mit XFCE) ist komfortabel zu installieren, fordert aber früher oder später Terminalkompetenz.

Bezug und Installation

Das Installations-ISO und Livesystem erhalten Sie auf *https://endeavouros.com/latest-release* (1,8 GB) und als LinuxWelt-Leser sofort bootfähig auf der Heft-DVD. Dieser Live-Installer bringt standardmäßig den XFCE-Desktop mit, jedoch sind Sie nicht zwingend auf diese Oberfläche festgelegt. Der „Welcome“-Dialog des Livesystems zeigt mehrere Optionen, und im Normalfall wird die Installation mit „Start the Installer“ ausgelöst. Alle anderen Optionen können Sie ignorieren, allenfalls die Option „Endeavour community editions“ ist für Nutzer interessant, die sich für exotische bis experimentelle Oberflächen interessieren (Sway, Qtile, Openbox sowie die Endeavour-Eigenentwicklung Worm).

Die primäre Option „Start the Installer“ eröffnet dann wiederum die zwei Möglichkeiten „Offline“ und „Online“. Wer den mitgelieferten XFCE möchte, kann „Offline“ rein vom Installationsmedium installieren. Dies ist der schnellste und einfachste Weg. „Online“ bezieht Teile des Systems aus dem Web und erlaubt die Auswahl zwischen neun prominenten Oberflächen (Gnome, KDE, Cinnamon etc.).

Verantwortlich für das Setup ist der Calamares-Installer, den auch Manjaro und einige Ubuntu-Varianten nutzen. Die typischen Fragen betreffen Sprache, Zeitzone, Tastatur, Partitionierung (mit optionaler Systemverschlüsselung) und Erstbenutzer. Setzt man hier, wie vorgeschlagen, das Benutzerpasswort mit dem des Administrators identisch, erzielt man ein sudo-Verhalten genau wie bei Ubuntu & Co.

EOS: Ein erster Rundgang

Das System präsentiert sich am XFCE-Desktop und allen installierten Programmen komplett deutschsprachig mit ganz wenigen Ausnahmen bei EOS-eigenen Tools. Thema der neuen „Artemis“-Version ist die Apollo-Mission und Standardhintergrund am Anmeldebildschirm und am Desktop dazu passend eine steil startende Rakete: Hier wird der Mythos vom schnellen Arch gepflegt, der sich dann tatsächlich bestätigt: Das System bootet auf einem älteren Rechner (allerdings auf SSD) in zehn Sekunden. Da kann ein Ubuntu 22.04 nicht

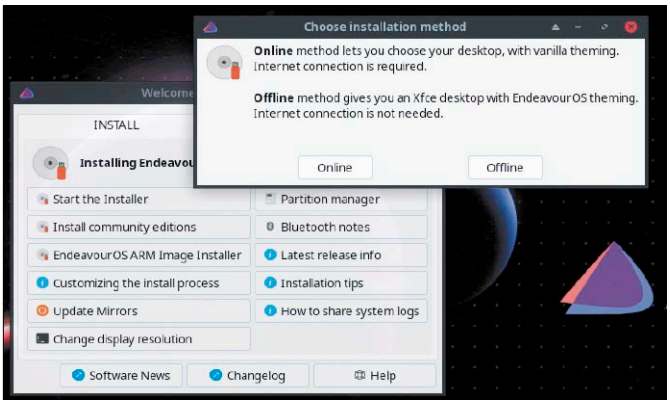
mithalten (13 Sekunden). Wie flink ein klassisch installierter Firefox agieren kann, wird Snap-geschädigte Ubuntu-Nutzer ebenfalls positiv überraschen. Auch der Start von Software-Schwergewichten wie Gimp ist praktisch per Mausklick geschehen. Wir kennen mit Bodhi Linux nur ein einziges Debian/Ubuntu mit vergleichbaren Reaktionszeiten.

Ressourcentechnisch fordert EOS mit dem Standarddesktop XFCE nicht mehr, aber auch nicht weniger als ein Debian/Ubuntu, nämlich etwa 650 MB ab Anmeldung. Auf der Festplatte bleibt es nach der Installation deutlich unter fünf GB, sollte aber für den Dauerbetrieb wie jedes Linux wenigstens 50 bis 100 GB auf der Systempartition vorfinden (Benutzerdaten nicht eingerechnet). Hardwaretechnisch gibt es mit den von uns genutzten Standardkomponenten keinerlei Einschränkungen. EOS verwendet Kernel 5.18 und arbeitet problemlos im Multimonitorbetrieb, erkennt alle Medien, akzeptiert Linux-bewährte WLAN-Adapter, beherrscht ACPI-Ruhezustände und erkennt Funktions-Sondertasten auf Notebooks.

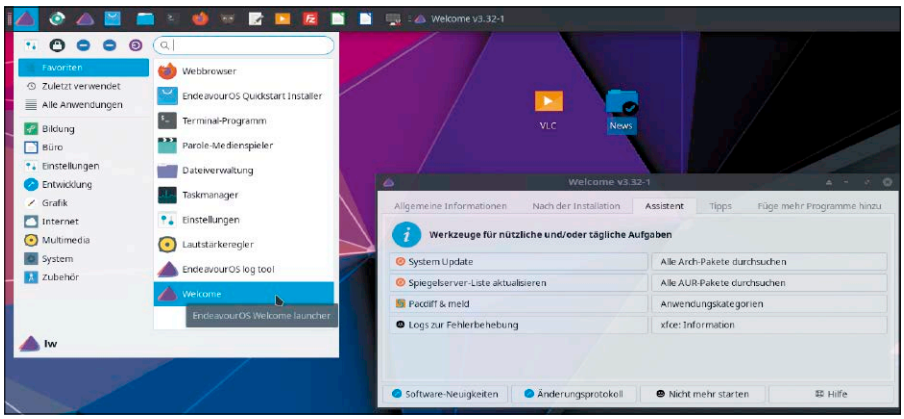
Nach der Anmeldung meldet sich der komplett deutsch lokalisierte „Welcome“-Dialog (eos-welcome). Die Angebote „Spiegelserver“ und „System-Update“ sollte man nach der Installation umgehend aufgreifen. EOS ist terminaldominiert, aber viele Aktionen wie eben auch die Systemaktualisierung kann man sich mit „Welcome“ vereinfachen. Es handelt sich um eine umfangreiche Kommando- und Script-Sammlung, die man als Autostart zwar abschalten („Nicht mehr starten“), aber als Favorit im Menü oder in der Systemleiste bereithalten sollte. EOS arbeitet wie die allermeisten neueren Distributionen mit dem Init-Dienst systemd. Komponenten und Kommandos von systemctl, journalctl funktionieren daher wie gewohnt.

Paketmanager und Installationen

EOS nutzt die Arch-Paketquellen, bietet für den Softwarebezug aber nur ein sehr einfaches grafisches Programm. eos-quickstart („EndeavourOS Quickstart Installer“) zeigt eine kategorisierte Auswahl prominenter Software, die nach Markierung und „Install Now“ umstandslos installiert wird. Schwergewichte wie Chromium, Gimp, Libre Office, Thunderbird, VLC sind hier in jedem Fall anzutreffen. Im Dauerbetrieb und für die Installation speziellerer Tools wird



„Welcome“ im EOS-Livesystem: „Start the Installer“ startet das Setup mit Calamares wahlweise „Offline“ oder „Online“ mit Desktopwahl.



„Welcome“ im installierten System: Diese nützliche Sammlung von URLs und Verwaltungskommandos erspart einige Terminalausflüge.

das aber nicht ausreichen: Schon die Suche nach einem SSH-Server oder einem Werkzeug wie Filezilla bleibt hier vergeblich. Basiskommandos des Terminal-Paketmanagers pacman sind daher unerlässlich. Dieser bezieht die Software aus den offiziellen Arch-Quellen. Ein zweiter Paketmanager yay kann zusätzlich die inoffiziellen AUR-Quellen nutzen. Wir empfehlen Arch-Einsteigern, zunächst bei den Arch-Quellen und bei pacman zu bleiben. Fürs Erste genügt (Beispiel)

```
pacman -Ss filezilla
```

zur Suche nach Software, ferner

```
sudo pacman -S filezilla
```

zur Installation und

```
sudo pacman -R filezilla
```

zur Deinstallation. Das komplette Systemupdate mit

```
sudo pacman -Syu
```

kann man alternativ auch mit dem Terminallink im Hauptmenü „System → UpdateIn-Terminal“ erledigen oder mit dem freundlichen „Welcome“. Letzteres weist unter „Assistent → Alle Arch-Pakete durchsuchen“ außerdem auf das Inventar unter *https://archlinux.org/packages*, das eine bequeme Onlinesuche erlaubt. Passendes kann dann mit *pacman -S […]* installiert werden.

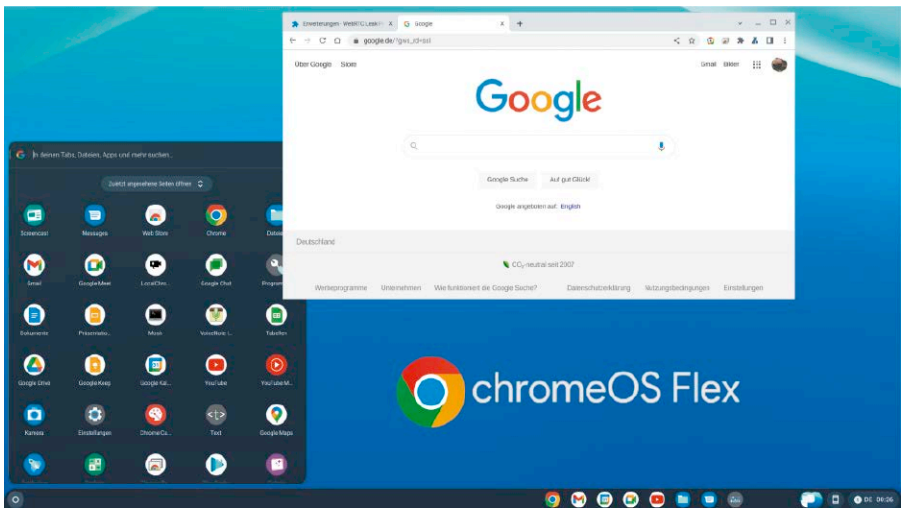
Systemverwaltung und Desktop

Neben den genannten grafischen EOS-Werkzeugen eos-quickstart (limitierter Software-Installer) und eos-welcome (wichtige klickfreundliche Script-Sammlung) bleibt es Arch-typisch spartanisch. Nahezu alles, was unter „/usr/bin/eos-*“ an Systemprogrammen zu finden ist, sind terminalnahe Helfer.

An grafischen EOS-Tools, die auch im Menü auftauchen, ist neben den bereits genannten nur noch der eos-update-notifier zu erwähnen, der die Frequenz der Systemaktualisierung einstellen kann. Im Übrigen überlässt EOS die grafische Systemverwaltung dem jeweils benutzten Desktop. Wer Terminaldefizite hat, ist daher mit Desktops wie Gnome, KDE oder Cinnamon am besten beraten, die eine große Reichweite auch in Richtung Systemverwaltung besitzen. Nutzern ohne Terminalaffinität wird man diese beeindruckend schnelle Distribution dennoch nicht empfehlen können. ■

Linux-Variante Chrome-OS Flex

Chrome-OS Flex benötigt wenige Systemressourcen und eignet sich daher auch für ältere Rechner. Primäre Zielgruppe sind Nutzer, die wenig Software benötigen oder sogar nur mit dem Webbrowser auskommen.



Chrome-OS Flex: Das Betriebssystem ist für die Nutzung des Webbrowsers und von Diensten wie Google Drive und Google Doc ausgelegt. Man kann aber auch offline arbeiten.

VON THORSTEN EGGELING

Chrome-OS erhält man nur vorinstalliert auf Notebooks („Chromebooks“) und das System ist für die jeweilige Hardware passgenau konfiguriert und optimiert. Unter der Bezeichnung Chrome-OS Flex bietet Google das Betriebssystem jetzt auch kostenlos zum Download an. Für die Nutzung aller Funktionen ist ein Google-Konto Voraussetzung. Das System lässt sich auf beliebigen Notebooks oder PCs installieren, wenn die Hardware unterstützt wird. Es eignet sich gut für ältere Hardware mit einem Baujahr ab etwa 2010, auf der es flüssiges Arbeiten verspricht.

Zurzeit befindet sich Chrome-OS Flex noch in der Entwicklung und es ist nicht garantiert, dass das System auf jedem Gerät stabil läuft. Man kann es jedoch ohne Risiko von einem USB-Stick booten und ausprobieren.

Chromium-OS, Chrome-OS & Chrome-OS Flex

Chrome-OS ist ein kommerzielles Betriebssystem mit einem Linux-Kernel, das von Google auf Basis des quelloffenen Chromium-OS (*www.chromium.org*) entwickelt wird. Ähnlich wie bei Android, baut Google eigene Apps wie Google Docs, Youtube oder Gmail in Chrome-OS ein.

Unter dem Namen „Cloudready Home Edition“ ist eine Variante des Google-Systems bereits seit einiger Zeit kostenlos von Neverware erhältlich (*www.neverware.com*). Das Unternehmen bietet ebenfalls kostenpflichtige Editionen inklusive Support für Firmen und Schulen an. Ende 2020 hat Google Neverware übernommen, weshalb die Firma jetzt Cloudready zu Chrome-OS Flex weiterentwickelt und auch Google-Programme einbaut.

Allen genannten Systemen ist gemeinsam, dass der Browser Chrome im Mittelpunkt steht. Über Webapplikationen kann man Texte verfassen, Tabellen erstellen, Fotos verwalten und E-Mails versenden. Standardmäßig bieten sich dafür Google-Applikationen wie Google Drive und Gmail an. Man muss aber nicht permanent online sein und kann Dokumente auch ohne Internetverbindung bearbeiten.

Hardware und Software für Chrome-OS Flex

Chrome-OS Flex unterstützt nicht jede Hardware. CD/DVD-Laufwerke, Fingerabdruckleser und Thunderbolt beispielsweise funktionieren nach Angaben von Google nicht oder nur eingeschränkt. Die minimalen Anforderungen an die Hardware sind:

- 64-Bit-CPU von Intel oder AMD
- vier GB RAM
- Installationslaufwerk ab 16 GB Kapazität
- Gerät mit Bios- oder Uefi-Firmware
- USB-Stick mit acht GB oder mehr

Google führt außerdem einige Grafikchips an, die den Leistungsanforderungen nicht genügen: Intel GMA 500, 600, 900, 950, 3600 und 3650. Nvidia-Grafikchips werden generell nicht empfohlen. Über *https://m6u.de/cosf* lässt sich eine Liste mit Geräten abrufen, für die Google eine Zertifizierung plant.

Software: Einige wenige Apps sind vorinstalliert, beispielsweise Dateimanager, Texteditor und Rechner. Mit der Gallery-App kann man Bilder bearbeiten, PDF-Formulare ausfüllen, Videos ansehen und Audioinhalte abspielen. Zusätzliche Programme lassen sich über den Google Web Store als Chrome-Erweiterungen installieren. In einer virtuellen Linux-Umgebung

kann man auch Linux-Programme starten (siehe Kasten).

Chrome-OS Flex installieren

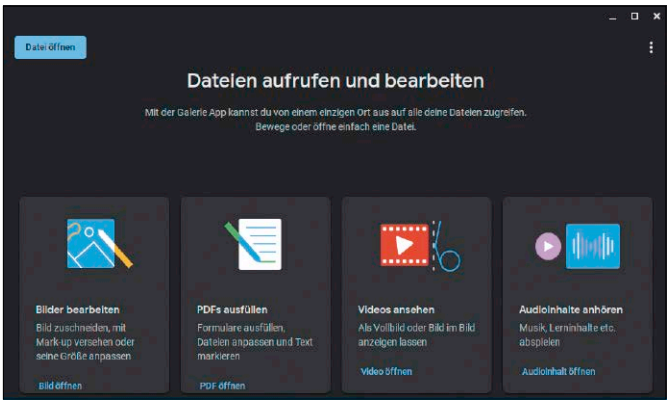
Bei der vereinfachten Installation lässt sich keine Zielfestplatte angeben und das System verwendet einfach das erste gefundene Laufwerk (SATA/NVMe/USB-Laufwerk). Daher wichtig: Vor der Installation darf außer dem Installationsstick nur das Ziellaufwerk angeschlossen sein. Danach können Sie andere Laufwerke wieder anschließen und über das Bootmenü der Firmware das gewünschte System wählen.

Der offizielle Weg zu Chrome-OS Flex führt über die Chrome-Erweiterung „Programm zur Chromebook-Wiederherstellung“ aus dem Google Web Store (*https://chrome.google.com/webstore*). Die Erweiterung funktioniert nur unter Chrome-OS, Windows und Mac-OS, weshalb Linux-Nutzer das Installationsabbild direkt herunterladen müssen.

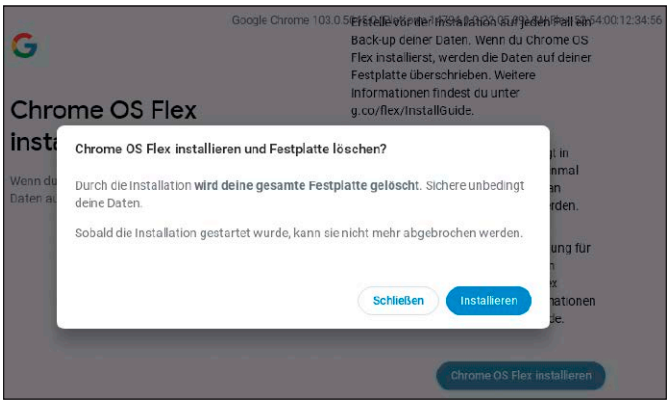
Schritt 1: Gehen Sie im Browser auf *https://chromiumdash.appspot.com/serving-builds*. Wählen Sie hinter „Servicing Build“ den Eintrag „Chrome OS Flex“ und klicken Sie unter „Recovery Images“ auf die höchste Versionsnummer. Entpacken Sie die heruntergeladene ZIP-Datei und ändern Sie die Dateiendung von „.bin“ auf „.img“.

Schritt 2: Stecken Sie einen USB-Stick am PC an. Starten Sie unter Ubuntu oder Linux Mint das Tool „Laufwerke“ (gnome-disk-utility) und klicken Sie auf der linken Seite den USB-Stick an. Rufen Sie über die Taste F10 das Menü auf und gehen Sie auf „Laufwerksabbild wiederherstellen“. Wählen Sie hinter „Abbild zur Wiederherstellung“ die IMG-Datei (siehe Schritt 1) und klicken Sie auf „Wiederherstellung starten“. Kontrollieren Sie genau, dass das richtige Ziellaufwerk angegeben ist, und klicken Sie auf „Wiederherstellen“. Danach müssen Sie das Administratorpasswort eingeben.

Schritt 3: Booten Sie die Hardware, auf der Sie installieren möchten, mit dem USB-Stick. Stellen Sie Sprache und Tastaturbelegung ein. Danach wählen Sie „Erst einmal nur ausprobieren“. Sie können sich mit Ihrem Google-Konto anmelden oder Sie klicken links unten auf „Als Gast nutzen“. Testen Sie, ob die Hardware funktioniert. Das System unterscheidet sich nicht von einem auf Festplatte installierten, läuft aber abhängig von der USB-Hardware in der Regel etwas langsamer.



Google-Apps: Gallery ist eines der wenigen bei Chrome-OS Flex vorinstallierten Programme. Es dient als Bildbearbeitung, PDF-Editor, Video- und Audioplayer.



Das Setup verwendet einfach die erste Festplatte und bietet keine Auswahl. Nur die Zielfestplatte darf angeschlossen sein, damit nicht das falsche Laufwerk überschrieben wird.

Schritt 4: Um das System zu installieren, klicken Sie rechts unten auf die Uhr und dann auf „Gastsitzung beenden“. Klicken Sie auf „Weiter“ und am unteren Bildschirmrand auf „Chrome OS Flex installieren“. Wenn Sie sich mit einem Google-Konto angemeldet haben, klicken Sie auf „Abmelden“ und dann auf „Chrome OS Flex installieren“. Folgen Sie den Anweisungen auf dem Bildschirm.

Schritt 5: Booten Sie den PC vom Installationslaufwerk. Melden Sie sich über ein Google-Konto an oder nutzen Sie „Als Gast anmelden“. ■

LINUX-ANWENDUNGEN IN CHROME-OS NUTZEN

Wem Chrome-Erweiterungen und vorinstallierte Apps nicht genügen, der kann auch Linux-Anwendungen unter Chrome-OS Flex starten. Die Funktion steht allerdings nicht auf jeder Hardware zur Verfügung, weil dafür einige Sicherheits- und Virtualisierungsfunktionen des Prozessors erforderlich sind. Die Installation ist in den „Einstellungen“ unter „Erweitert → Entwickler“ nach einem Klick auf „Aktivieren“ schnell geschehen. Danach steht ein Linux-Terminal mit einem Debian-System zur Verfügung. Mit

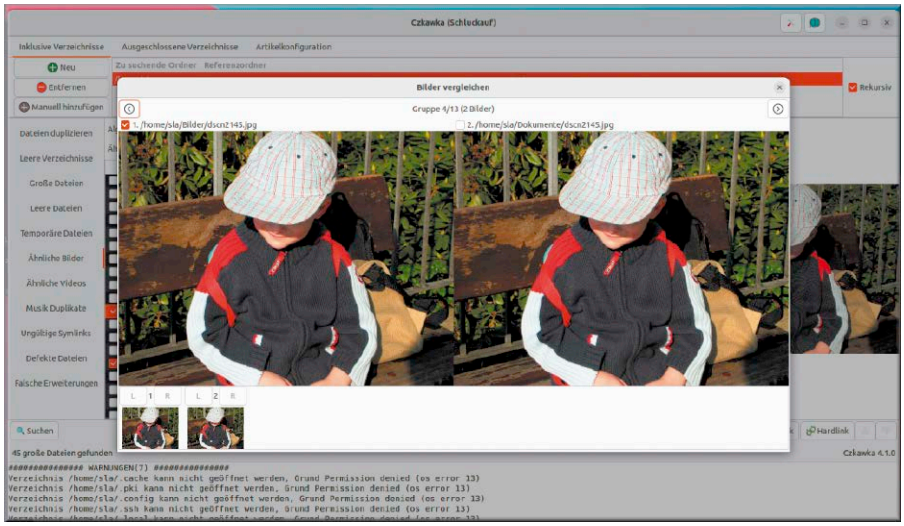
```
sudo apt update
sudo apt install vlc
```

lässt sich beispielsweise der VLC Media Player installieren. Sie starten ihn über das Startmenü des Desktops („Launcher“) unter „Linux-Apps“. Im Dateimanager ist er bei Multimediadateien im Kontextmenüpunkt „Öffnen mit“ zu finden. Entsprechend lassen sich auch Libre Office oder Gimp installieren und wie unter Linux nutzen. Standardanwendungen aus der Linux-Umgebung laufen angenehm schnell, von der Virtualisierung ist kaum etwas zu bemerken. Anders kann es aussehen, wenn der Rechner nicht genug Leistung bereitstellt oder man Programme benötigt, die CPU und Grafikchip besonders beanspruchen.

Dublettensuche mit Czkawka

Je länger mit einem System gearbeitet wird, umso mehr Speicherplatz wird verschwendet. Dateidubletten zählen zu den größten Ärgernissen. Czkawka ist ein jüngeres Werkzeug, das beim Aufräumen hilft.

VON STEPHAN LAMPRECHT



Einmal vorschnell auf „Kopieren" statt „Verschieben" geklickt, und schon gibt es doppelte Dateien auf dem System. Wenn es sich um Dokumente handelt, die einen „sprechenden" Dateinamen verwenden, lassen die sich auch manuell finden. Bei Bilddateien oder Musikstücken wird es hingegen schwierig – gerade, wenn sie aus unterschiedlichen Quellen stammen. Das Tool Czkawka, was so viel wie „Schluckauf" bedeutet (Tschechien und Kafka stecken aber wohl auch noch drin), kümmert sich um redundante Dateien auf dem System.

Installation im Containerformat

Die App lässt sich mit etwas Bastelarbeit auch unter Windows oder sogar auf dem Mac nutzen. Unter Linux ist das deutlich einfacher. Hier steht die Anwendung auf der Projektseite (*https://github.com/qarmin/czkawka*) bereit oder kann wahlweise als Snap, Flatpak oder Appimage installiert werden. Entscheiden Sie sich unter Ubuntu etwa für Snap, genügt dieser Terminalbefehl:

```
sudo snap install czkawka
```

Wenn Sie auch Videodateien untersuchen wollen, wird zusätzlich die Bibliothek „ffmpeg" benötigt. Diese finden Sie in allen Distributionen in den offiziellen Paketquellen.

Dubletten – Ähnlichkeiten – Ungültiges

Das Werkzeug Czkawka ist nicht auf die Suche von doppelten Dateien beschränkt. Sie können damit auch motivähnliche Bilder, Varianten von Audiodateien oder Videos finden, zudem auch ungültige symbolische Verknüpfungen oder leere Verzeichnisse und Dateien. Die verschiedenen Suchoptionen erreichen Sie über die linke Seitenleiste im Programmfenster. Die einzelnen Bereiche sind ausführlich beschrieben, lediglich bei der Dublettensuche gab es einen Fehler bei der Übersetzung: „Dateien duplizieren" verdoppelt natürlich nicht die Dateien, sondern sucht doppelte Dateien.

Suche starten: Nach dem Programmstart ist standardmäßig das Home-Verzeichnis als Ziel der Suche ausgewählt. Möchten Sie einen anderen Ordner durchsuchen, klicken Sie auf „Neu" und wählen diesen Ordner aus. Czkawka kann auch Netzlaufwerke oder externe Datenträger durchsuchen.

Exkurs: Wenn Sie Czkawka mit Benutzerrecht starten, ist das Programm auf die Verzeichnisse und Dateien beschränkt, auf die Sie selbst Zugriffsrechte haben. Um auch in anderen Ordnern nach doppelten Dateien oder leeren Ordnern zu suchen, müssen Sie die Anwendung mit root-Rechten aufrufen.

Über den Abschnitt „Ausgeschlossene Verzeichnisse" legen Sie danach optional Ordner fest, die Czkawka nicht durchsuchen soll. Das ist spätestens dann nützlich, wenn Sie Dubletten vorsichtshalber in einen eigenen Ordner verschoben haben. Mit dem Ausschluss vermeiden Sie, dass Ihnen dieselben Dateien erneut als Dubletten präsentiert werden.

Im nächsten Schritt entscheiden Sie sich für die gewünschte Suche, also etwa für „Dateien duplizieren". Bei der Suche nach Duplikaten gehen alle Anwendungen ähnlich vor. Sie untersuchen Dateinamen, Dateigröße und arbeiten mit Hash-Werten. Letztere Option dauert zwar am längsten, bietet aber die genauesten Ergebnisse – und dies unabhängig vom Dateinamen. Zwischen

den Prüfmethoden entscheiden Sie sich über das Listenfeld unterhalb der Verzeichnisliste. In dieser Optionsleiste werden im Falle einer anderen Suchfunktion, etwa nach ähnlichen Bildern, andere Einstellungen sichtbar. Im Falle der komplexen Ähnlichkeitssuche würde es den Rahmen sprengen, die unterschiedlichen Varianten im Detail vorzustellen. Mit einem Klick auf „Suchen“ starten Sie dann den Suchlauf.

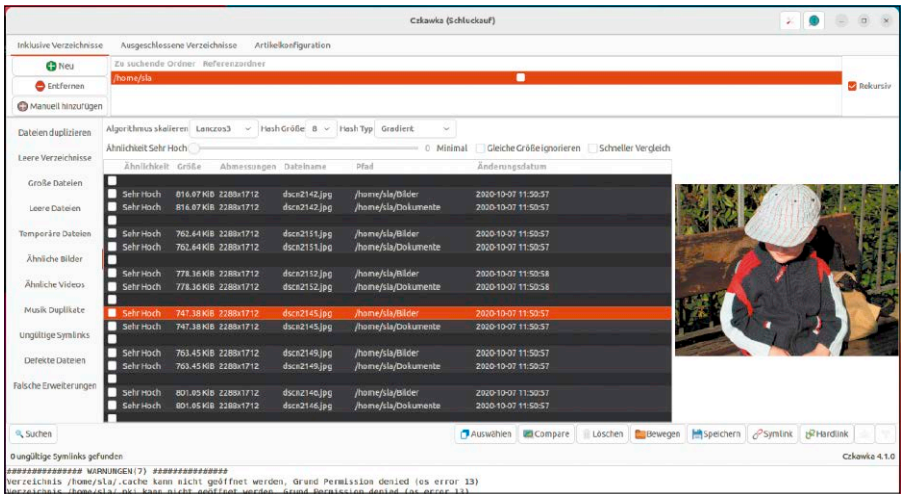
Entscheidungshilfe bei Dubletten

Am Ende des Suchlaufs präsentiert das Programm die Ergebnisse in der Bildschirmmitte – im Falle der Suche nach Platzverschwendern geordnet nach der Dateigröße der Dokumente. In der rechten unteren Ecke finden Sie in der Werkzeugleiste bei jedem Suchlauf den Eintrag „Speichern“. Damit halten Sie das Ergebnis in Form einer Textdatei fest, um diese später manuell abzuarbeiten. Haben Sie nach ähnlichen Bildern oder Videos gesucht, liefert die Anwendung eine visuelle Entscheidungshilfe mit.

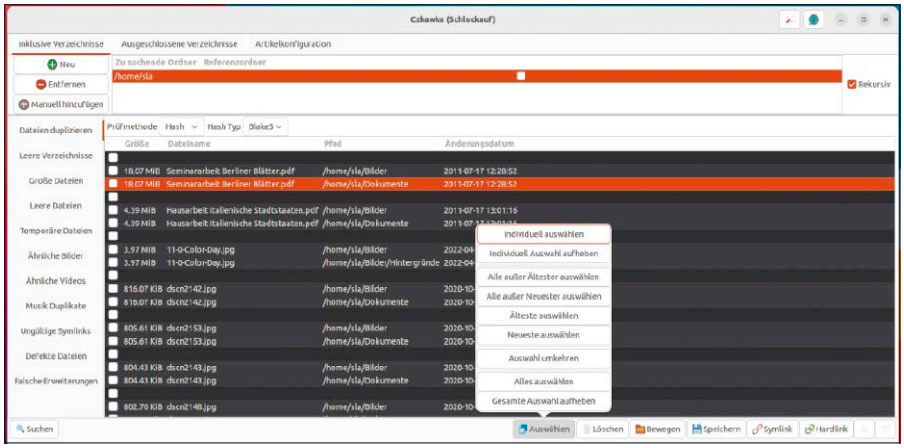
Mit einem Klick auf den Eintrag zeigt Czkawka dann den Inhalt der Datei an. So können Sie sich davon überzeugen, tatsächlich nur eine Dublette erwischt zu haben. Klicken Sie auf „Compare“, dann werden beide Bilder direkt nebeneinandergestellt. Mit einem einfachen Mausklick in das Optionsfeld neben dem Dateinamen setzen Sie eine Markierung auf die Datei. Diese bleibt erhalten, wenn Sie die Vorschau schließen. Anschließend können Sie über die Schalter in der Werkzeugleiste in der Mitte entscheiden, ob Sie die Auswahl verschieben oder löschen wollen.

Über den Schalter „Auswählen“ kehren Sie bei Bedarf die Selektion auch wieder um oder nutzen die Möglichkeit, nur die neueren Dateien auszuwählen, bevor Sie sich an die Bearbeitung weiterer Objekte machen.

Bei der Suche nach doppelten Musiktiteln kann das Tool Vorschläge aufgrund von Titeln, Bitraten oder Ähnlichkeitssuche liefern. Ein direkter Vergleich wie bei Fotos funktioniert hier verständlicherweise nicht. Es bleibt Ihnen also nichts anderes übrig, als jeweils kurz in den Titel hineinzuhören. Das ist auch bei Videos der Fall. Hier gab es bei Redaktionsschluss leider ein Problem mit den Versionen, die als Snap installiert wurden und sich nicht mit ffmpeg verbinden ließen. Bei Flatpak- und Appimage-Installationen trat das Problem nicht auf.



Die Czkawka-Oberfläche ist gut strukturiert und macht den Umgang einfach. Bei der Ähnlichkeitssuche haben Sie die Wahl zwischen verschiedenen Ansätzen.



Nach der Sichtung der Ergebnisse markieren Sie Ihre Auswahl, um dann Dubletten auf einen Rutsch zu verschieben oder auch komplett zu löschen.

Die Alternativen fslint und rdfind

Czkawka ist nur eine Möglichkeit, um Ballast im Dateisystem abzuwerfen. Ähnlich arbeitet das Programm fslint, das sogar eine grafische Oberfläche mitbringt, wenn es im Terminal mit *fslint-gui* ausgeführt wird. Auf diese Weise gestartet, erkennen Sie auch unschwer die Inspirationsquelle des Entwicklers von Czkawka.

Nutzer aktueller Ubuntu-Versionen werden fslint allerdings in den Paketquellen vergeblich suchen. Da das Tool ältere Python-Bibliotheken verwendet, wurde ihm kurzerhand die offizielle Unterstützung entzogen. Wer sich die Mühe ersparen will, hier erst durch die Installation zusätzlicher alternativer Bibliotheken Abhilfe zu verschaffen, findet als Snap eine nicht offizielle Version, die mit

```
sudo snap install fslint-unofficial
```

installiert werden kann. Funktional unterscheiden sich fslint und Czkawka kaum voneinander. Bei der Kontrolle von doppelten Fotomotiven ist Czkawka aber dank der visuellen Unterstützung die bessere Wahl. Zudem dürfte das Tool beim initialen Scannen umfangreicher Verzeichnisse etwas schneller sein, da es einen völlig anderen Unterbau nutzt.

Rdfind gehört ebenfalls zu den Klassikern auf der Suche nach doppelten Dateien und läuft als Tool für die Kommandozeile. Es ist als Paket „rdfind“ in allen Repositorys zu finden. Wie fslint kann es mit Scripts genutzt und automatisiert werden. Rdfind vermag viel, erfordert aber ein intensiveres Studium der Manpages, um auch die verschiedenen Schalter und Optionen korrekt einzusetzen. Für die schnelle Suche zwischendurch sind Czkawka und fslint mit grafischer Oberfläche die bequemste Möglichkeit, um Ballast abzuwerfen. ■

Das ist neu in Inkscape 1.2

Nach gut einem Jahr folgt auf Inkscape 1.1 die neue Version 1.2. Der äußerlich unscheinbare Versionsschritt täuscht: Die Entwickler haben einige spannende neue Funktionen eingebaut und außerdem die Bedienung verbessert.

VON THORSTEN EGGELING

Inkscape ist in etwa mit Adobe Illustrator vergleichbar. Das Vektorgrafikprogramm eignet sich für künstlerische und technische Illustrationen, beispielsweise für Comics, Cliparts, Logos, Flyer, Broschüren und Diagramme. Die Vektorgrafiken ermöglichen eine scharfe und verlustfreie Skalierung der Elemente für den Bildschirm und Druck unabhängig von der Auflösung. Als Dateiformat kommt bei Inkscape SVG zum Einsatz (Scalable Vector Graphics). Wir stellen Ihnen die wichtigsten Neuerungen bei Inkscape 1.2 vor, das im Mai 2022 erschienen ist.

Inkscape installieren oder aktualisieren

Im Downloadbereich von *https://inkscape.org* wird für Linux eine Datei im Appimage-Format angeboten. Über den Dateimanager machen Sie die heruntergeladene Datei über das Kontextmenü „Eigenschaften“ ausführbar, indem Sie unter „Zugriffsrechte“ ein Häkchen vor „Datei als Programm ausführen“ setzen (Linux Mint: „Der Datei erlauben, sie als Programm auszuführen“). Außerdem gibt es Inkscape 1.2 auch als Snap-Paket für Ubuntu und als Flatpak für Linux Mint. Die Installation dieser Formate ist über Ubuntu-Software und bei Linux Mint über die Anwendungsverwaltung möglich. Nicht zuletzt stellt Inkscape über ein PPA ein klassisches DEB-Paket bereit, mit dem sich die ältere Version auch aktualisieren lässt. Eine Anleitung finden Sie über *https://m6u.de/NKPPA*.

Mit mehreren Seiten arbeiten

Das Seitenwerkzeug ist eine der interessantesten Neuerungen in Inkscape 1.2. Das Programm kann jetzt mehrere Seiten in einer Datei anlegen, bisher waren nur einseitige Dokumente möglich. Das neue Werkzeug erscheint ganz unten in der Werkzeugleiste. Nach einem Klick darauf blendet Inkscape eine Befehlsleiste ein. Über die erste Schaltfläche erstellt man weitere Seiten. Die Abmessungen der schon vorhandenen Seiten werden übernommen oder Sie geben hinter der Schaltfläche eine andere Größe und Seitenausrichtung an. Die Reihenfolge der Seiten lässt sich über die Befehlsleiste ändern. Den größten Vorteil mehrseitiger Dokumente sieht man beim PDF-Export, der über „Datei → Kopie speichern“ erfolgt. Hinter „Dateityp:“ muss „Portable Document Format (*.pdf)“ eingestellt sein, womit sich ein mehrseitiges PDF erzeugen lässt.

PDF-Dateien bearbeiten

PDFs sind für die Anzeige am Bildschirm und für den Druck konzipiert, nachträgliche Änderungen sind offiziell nicht vorgesehen. Mit Inkscape geht es trotzdem. Sie können PDF-Dokumente öffnen und den Inhalt anpassen. Wie gut das funktioniert, hängt von der Komplexität des PDFs ab. Außerdem müssen die enthaltenen Schriftarten installiert sein, andernfalls kommt es zu Fehlern bei der Formatierung.

Bisher war nur der Import einzelnen Seiten möglich. Wenn Sie in Version 1.2 ein PDF öffnen, ist im Fenster „PDF-Importeinstellungen“ ein Häkchen vor „Alles“ gesetzt, womit alle Seiten importiert werden. Ist das Häkchen nicht gesetzt, können Sie dahinter angeben, welche Einzelseite Sie importieren wollen. Über „Datei → Kopie speichern“ lässt sich das geänderte PDF wieder speichern.

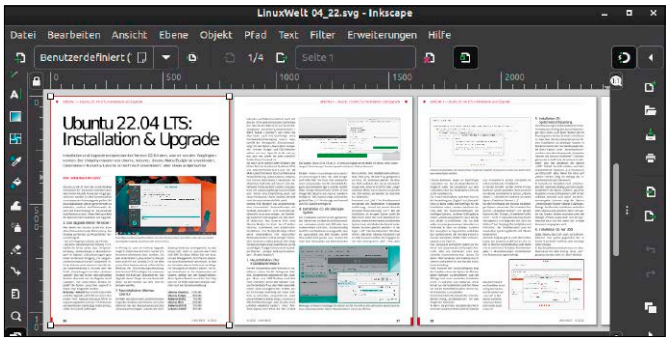
Neuerungen bei der Bedienung

Für die Inkscape-Entwickler stellt sich die Herausforderung, die Bedienung bei neuen Versionen nicht zu stark zu verändern, aber trotzdem sinnvolle Verbesserungen einzubauen. Die komplette Übersicht der Änderungen inklusive Tipps finden Sie über *https://m6u.de/RN12*.

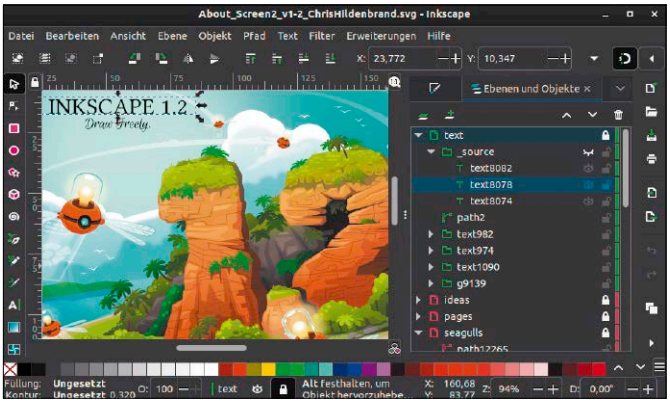
Dialoge komfortabler nutzen: Im Inkscape-Sprachgebrauch sind Dialoge Fenster, über die sich Optionen einstellen lassen. Die Dialoge sind meist an das Hauptfenster angedockt, lassen sich aber auch in einem unabhängigen Fenster darstellen. Bisher war nicht immer klar, ob ein Menüpunkt einen Dialog einblendet oder ob sich dahinter eine andere Funktion verbirgt. Deswegen gibt es jetzt ganz rechts im Dialogbereich ein Minimenü. Nach einem Klick auf den kleinen Pfeil kann man den gewünschten Dialog auswählen, der dann in einem eigenen Reiter dargestellt wird. Über „Ansicht → Dialoge ein-/ausblenden“ im Hauptmenü oder die Taste F12 lässt sich der Dialogbereich aktivieren, wenn Inkscape ihn nicht anzeigt. Über das Minimenü können Sie außerdem den aktuellen Reiter schließen oder in ein neues Fenster verschieben. Die Dialoge „Ebenen“ und „Objekte“ wurden in Inkscape 1.2 in „Ebenen und Objekte“ zusammengeführt, die Elemente werden dabei farblich hervorgehoben. Die Optionen „Unschärfe“ und „Deckkraft“ fehlen im neuen Dialog. Dafür muss man jetzt den Dialog „Füllung und Kontur“ verwenden.

Einrasten und ausrichten: Die „Einrasten-Kontrollleiste“ wurde durch eine Schaltfläche und ein Menü ersetzt, die beide rechts oben im Fenster sichtbar sind. Die Schaltfläche mit dem Magnetsymbol schaltet „Einrasten“ ein und aus. Der Pfeil daneben öffnet ein Menü, über das sich die Einrasten-Funktion für die Bereiche „Objektrahmen“, „Knoten“ und „Ausrichtung“ abschalten lässt. Nach einem Klick auf „Fortgeschritten“ erscheinen Optionen, die detaillierte Einstellungen ermöglichen. Die Beschriftungen helfen dabei, die gewünschte Option zu finden.

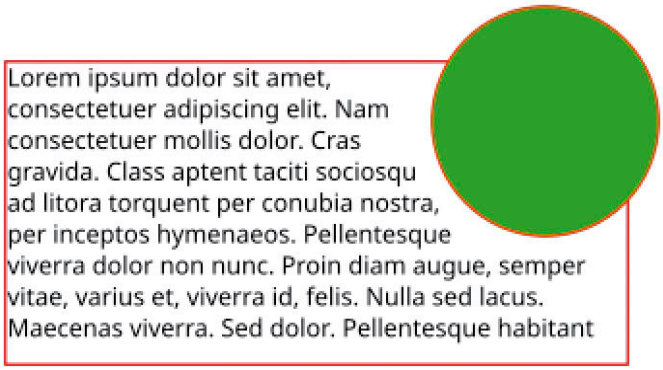
Farbpalette: Die schnelle Auswahl einer Farbe erfolgt wie bisher über die Farbpalette am unteren Bildschirmrand. Nach einem Klick auf die Menüschaltfläche am rechten Rand blendet Inkscape jetzt nicht nur die Bezeichnungen ein, sondern liefert auch eine Vorschau. Über „Einstellungen“ lässt sich die Anzahl der Farbreihen angeben und hinter „Rand:“ der Abstand der Farbfelder. Mit dem Wert hinter „Kachelgröße“ kann man die Größe der Farbfelder jetzt feiner einstellen als zuvor.



Neues Seitenwerkzeug: Ein Dokument kann jetzt mehr als eine Einzelseite enthalten. Das ist etwa beim PDF-Import nützlich, weil sich dann alle Seiten wieder in einer Datei speichern lassen.



Vereinfachter Dialog: Die Elemente aus „Ebenen“ und „Objekte“ sind jetzt zusammen in einem Dialog untergebracht und farblich abgehoben. Das erleichtert die Orientierung.



Objekt mit Text umgeben: Über „Text → Rahmen umfließen“ lässt sich ein Textobjekt mit einer geometrischen Form verknüpfen, sodass der Text die Form umfließt.

Erweiterungen: Clipart-Grafiken für Illustrationen findet man kostenlos im Internet. Für den bequemen Download ist bei Inkscape 1.2 die Erweiterung „Import Clipart“ vorinstalliert („Datei → Bilder aus dem Internet importieren“). Wählen Sie eine Quelle wie „Inkscape Community“ oder „Open Clipart Library“, tippen Sie einen Suchbegriff ein und bestätigen Sie mit der Enter-Taste. Per Klick auf „Import“ bauen Sie die ausgewählte Grafik in Ihr Dokument ein.

Objekte mit Text umgeben: Für diese neue Funktion benötigen Sie ein Textobjekt und eine Form, etwa ein Rechteck. Über „Text → Umbruch an Form anpassen“ lässt sich der Text dann in die Form einpassen. Bauen Sie eine weitere Form ein, etwa einen Kreis. Wählen Sie nur das Textobjekt sowie den Kreis und gehen Sie auf „Text → Rahmen umfließen“. Der Text richtet sich dadurch am Kreis aus.

Bei unseren Tests im Juni 2022 funktionierte die Erweiterung jedoch unabhängig von der Installationsart (Appimage, Snap, Flatpak, PPA) mit keiner Programmversion. Ursache dafür ist ein fehlendes Python3-Paket, was Sie bei einer PPA-Installation mit

```
sudo apt install python3-
  cachecontrol
```

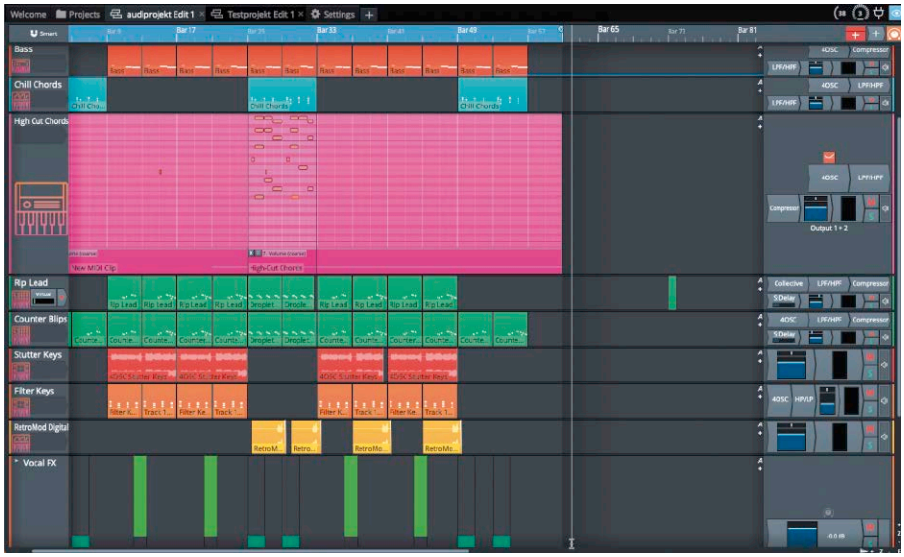
korrigieren können. Bei den Containerformaten Snap & Co. müssen Sie allerdings auf ein Update warten. ■

Mächtige DAW: Tracktion Waveform

Linux eignet sich hervorragend für die Musikproduktion. Ambitionierte Amateure und Profis, die noch auf der Suche nach der passenden Software sind, sollten sich die Digital Audio Workstation (DAW) Tracktion Waveform 12 ansehen.

VON STEPHAN LAMPRECHT

Tracktion Waveform ist eine kommerzielle DAW, die zum Listenpreis von 149 Dollar angeboten wird. Dazu gibt es noch eine ganze Reihe von Bundles mit Plug-ins. Das Komplettpaket schlägt mit 599 Dollar zu Buche. Schon die Basisversion ist also kein Schnäppchen, aber im direkten Vergleich nicht zu teuer. Auf jeden Fall aber zu viel Geld, um es unbesehen zu investieren. Glücklicherweise gibt es eine kostenlose Version, die sich lediglich in wenigen (!) und eher von Profis verwendeten Funktionen unterscheidet. Somit können auch Hobbymusiker das Programm unter Linux, Windows und Mac-OS einsetzen.



Die Gratisversion der DAW lässt nur wenige, eher von Profis verwendete Funktionen vermissen. Für Hobbymusiker bleiben schon hier kaum Wünsche offen.

Benutzerkonto für die Installation

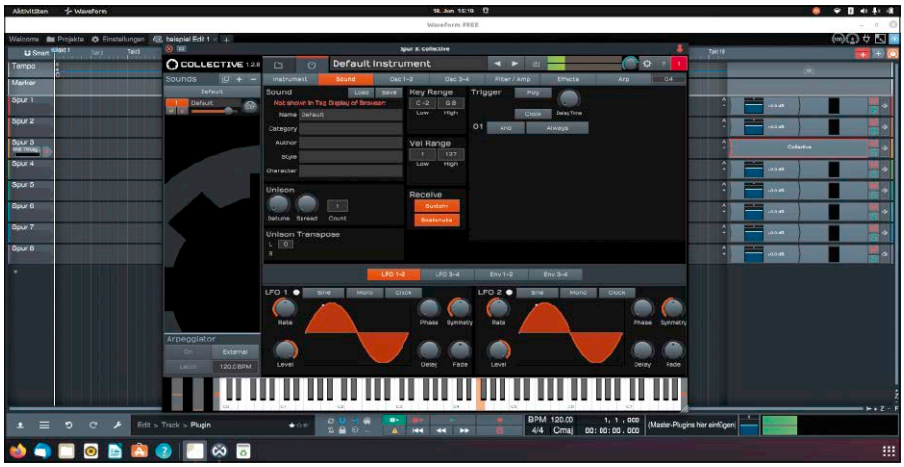
Für den Einsatz unter Linux empfiehlt der Hersteller die Distribution Ubuntu. An diese Empfehlung haben wir uns gehalten. Die eigentliche Installation sollte keine Probleme bereiten, da Waveform nicht auf Bibliotheken des Desktops zurückgreift, sondern auf einem eigenen Framework basiert, was auch die Audioausgabe umfasst. Als Basis für die Installation haben wir uns für ein System entschieden, auf dem Ubuntu Studio seinen Dienst verrichtet. Waveform war darauf noch nicht installiert, wohl aber andere DAW-Lösungen mitsamt Erweiterungen.

Um an den Download zu gelangen, müssen Sie auf der Website ein Benutzerkonto eröffnen (*https://marketplace.tracktion.com/*). Auch die kostenlose Version wird also „erworben", wenn auch, ohne Geld zu verlangen. Über den Bereich „My Downloads" können Sie in Ihrem Benutzerkonto das Paket jederzeit erneut installieren. Empfehlenswert ist der Download und die Installation des „Download Managers", der als DEB-Paket zur Verfügung steht. Nach der Eingabe der Daten des Benutzerkontos stellt dieser die zur Verfügung stehenden „Käufe" übersichtlich bereit. Alternativ laden Sie sich das DEB-Paket von Waveform herunter und installieren es manuell.

Nach dem ersten Start fragt Waveform, ob Sie das neue Soundsystem verwenden wollen. Gegen die Aktivierung spricht nichts, zumindest gab es auf dem Testsystem keinerlei Probleme damit. Im Gegensatz zu manch anderer Software lässt sich Waveform auch nicht unter Volllast aus dem Tritt bringen. Eine Einführung zeigt nach dem Start die ersten Schritte. Damit laden Sie sich dann optional Demosongs herunter, werden zu Anleitungen geleitet und können das System auf bereits vorhandene Plug-ins durchsuchen. Die Software nutzt das aktuelle Konzept vieler DAWs und bindet Erweiterungen im VST-, VST3- und LADSPA-Format ein. Voraussetzung ist, dass sich diese an den unter Linux üblichen Standardpfaden befinden. Ansonsten passen Sie die Pfade über „Settings" an. Der Besuch dieser Sektion ist ohnehin zu empfehlen, weil Sie unter „Appearance" weitere Sprachen installieren können, um die Oberfläche in Deutsch zu sehen. Falls Ihnen der dunkle Modus nicht gefällt, ändern Sie dort auch das gewählte Farbschema.

Nach einer Änderung der Pfade müssen Sie einen weiteren Suchlauf nach Plug-ins beginnen, um dann auf Erweiterungen wie Softwaresynthesizer zugreifen zu können.

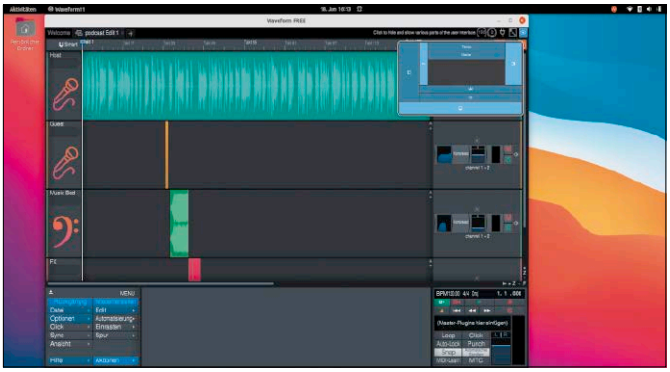
Der Wechsel von einem Plug-in zum anderen auf einer bereits existierenden Spur könnte allerdings etwas deutlicher gekennzeichnet sein. Falls Sie ein externes MIDI-Keyboard nutzen, sollte dieses problemlos erkannt werden. Das Feintuning wie Kanäle oder die Zuweisungen von Instrumenten auf bestimmte Bänke nehmen Sie ebenfalls in diesen Optionen vor.



Mehr Spaß macht es mit einer richtigen Klaviatur, aber dank virtuellem Keyboard bedienen Sie auch als Plug-in vorhandene Synthesizer.

Erste Schritte auf Basis einer Vorlage

Um die ersten Schritte im Umgang mit Waveform zu üben, nutzen Sie bei der Anlage eines neuen Projekts eine der angebotenen Vorlagen. Die zeigen, dass sich Waveform als Tool für alle Musikproduktionen versteht. Anders als andere Lösungen setzt es nicht den Schwerpunkt auf Loops, Nachvertonung oder klassische Studioarbeit, sondern will den Nutzer bei allen Aufgaben unterstützen. Die Wahl der Vorlage hat unmittelbaren Einfluss auf die Zahl der Spuren oder Kompressionen. Da die zahlreichen Optionen und Paletten selbst auf größeren Bildschirm stark ablenken können, machen Sie sich mit dem Augensymbol am oberen Rand des Programmfensters vertraut. Darüber können Sie einzelne Bereiche ausblenden und genauso schnell wieder auf den Bildschirm holen.



Die Projekttemplates richten Waveform für die unterschiedlichen Aufgaben ein. In diesem Beispiel geht es um die Produktion eines Podcasts.

Ein Vorteil der Nutzung eines eigenen Frameworks fällt bei der täglichen Arbeit sofort auf. Wer mehrere Fenster nebeneinander stellen will oder auch noch etwas von seinem Desktop sehen möchte, wird begeistert sein, wie gut sich die Oberfläche selbst an kleinere Notebookbildschirme anpasst. Hier wurde responsives Design nahezu perfekt umgesetzt. Es spricht also auch nichts gegen die Nutzung im Livebetrieb auf der Bühne.

Apropos Livebetrieb: Sie sollten vorher prüfen, ob alle nicht von Tracktion stammenden Plug-ins wie gewohnt arbeiten. Audio- und MIDI-Spuren lassen sich mit Waveform live aufnehmen, mixen und abspielen. Um aber produktiv arbeiten zu können, ist es ratsam, sich das eine oder andere Youtube-Tutorial anzusehen. Ihre Softwaresynthesizer und Klangquellen können Sie in der Software auch zu Racks arrangieren. MIDI-Clips werden auf Wunsch einfach mit einem Rechtsklick zu Step-Clips. Damit können Sie dann so arbeiten, wie Sie es von Step-Sequenzern gewohnt sind. Moderne Audioproduktionen sind dank der Softwareunterstützung heute recht komplex und entsprechend schnell unübersichtlich. Eine bemerkenswerte Funktion von Waveform sind die Folderspuren. Damit kombinieren Sie verschiedene Spuren wie in einem Dateiordner zu einer gemeinsamen Einheit, die dann visuell wie eine Spur erscheint und damit wieder mehr Platz im Programmfenster schafft.

Videos vertonen

Es würde den Rahmen dieses Beitrags sprengen, die vielen nützlichen Funktionen und Möglichkeiten von Waveform im Detail vorzustellen. Der Blick in die hervorragende Onlinedokumentation ist ohnehin hilfreich, um mit allen Details vertraut zu werden. Eine etwas überraschend erscheinende Funktion verdient es indes, noch erwähnt zu werden. Denn Waveform unterstützt mittels der Synchronisation von Xjadeo, das praktischerweise gleich mitinstalliert wird, bei der Nachvertonung von Videoclips. Allerdings wird das erst mit einem zweiten Bildschirm richtig komfortabel. Der Videoplayer folgt hier den Bewegungen des Mauszeigers auf der Zeitleiste des Audioclips und benötigt für die Darstellung Platz auf dem Bildschirm. Einzige Einschränkung: Xjadeo unterstützt lediglich AVI-Dateien. Liegt das Filmmaterial also in einem anderen Format vor, müssen Sie dies erst mit einer der vielen Anwendungen für Linux konvertieren.

Das mag auf den ersten Blick hemdsärmelig wirken, ist aber konsequent: Schließlich geht es um Audioproduktion und nicht um beste Bildqualität.

Fazit

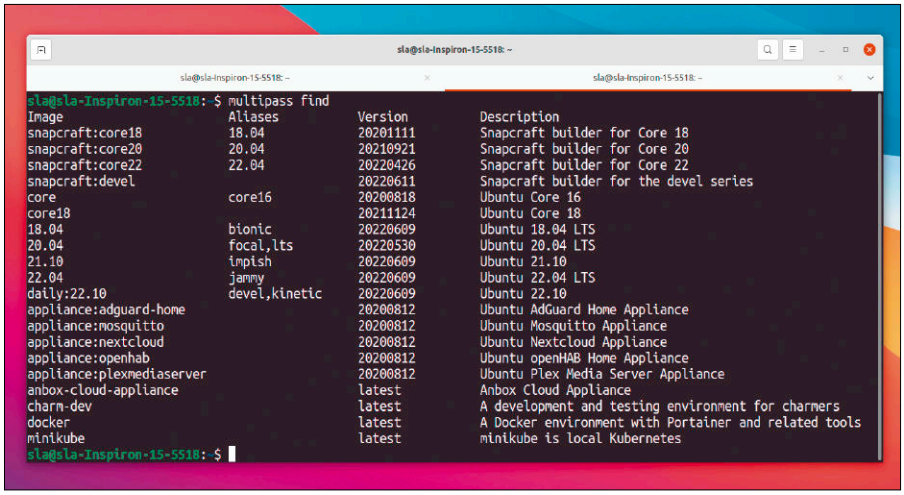
Waveform kann im Heimstudio wie auf der Bühne überzeugen. Die vollständig ausgestattete DAW bleibt trotz ihres Funktionsumfangs bedienbar. Für Einsteiger dürfte die Lernkurve dennoch steil sein. Wer sich indes schon mit Klangerzeugung und dem Abmischen von Audiotracks beschäftigt hat, wird auf bekannte Techniken stoßen. Schon die kostenfreie Version lässt kaum Wünsche offen und lässt sich mit den kostenpflichtigen Plug-ins des gleichen Herstellers ergänzen. ■

Multipass: Virtuelle Maschinen ganz einfach

Die Nutzung virtueller Maschinen hat in den vergangenen Jahren die IT-Welt nachhaltig verändert. Mit einem Knopfdruck lassen sich ganze Infrastrukturen aufbauen und ausprobieren. Mit Multipass können das nun auch Endanwender.

VON STEPHAN LAMPRECHT

Mit Multipass vereinfacht Canonical, die Firma hinter der Entwicklung von Ubuntu, den Einsatz von virtuellen Systemen signifikant. Schneller und einfacher haben Sie unter Linux noch keine VM aufsetzen können. Die Herkunft der Software hat allerdings direkten Einfluss auf den Einsatz und das Angebot: Multipass wird ausschließlich als Snap angeboten, also im von Canonical entwickelten Containerformat. Ebenfalls wenig überraschend ist die Tatsache, dass bei der Auswahl der virtuellen Maschinen eindeutig die Distribution Ubuntu im Fokus steht.



Diverse Ubuntu-Versionen und einige speziellere Appliances: Multipass bietet eine inzwischen ordentliche Auswahl virtueller Maschinen und Server-Appliances.

Angebot und erste Installationen

Unter Ubuntu ist die Installation von Multipass rasch abgeschlossen. Es genügt ein Befehl im Terminal:

```
sudo snap install multipass
```

Seit der ersten Vorstellung von Multipass hat Canonical das Angebot virtueller Instanzen sukzessive ausgebaut. Der Befehl

```
multipass find
```

sorgt für den ersten Überblick. Neben Daily-Builds für die kommende Ubuntu-Version können Sie die drei letzten LTS-Varianten nutzen, eine Docker-Umgebung installieren oder spezialisiertere Appliances von Canonical, die den Betrieb von Nextcloud, Open HAB oder Plex vereinfachen.

Die Übersicht des Angebots ist insofern wichtig, als Sie die genaue Imagebezeichnung für die Installation einer virtuellen Maschine benötigen. Um also etwa ein Ubuntu 21.10 mit dem Namen „testsystem" zu installieren, führen Sie im Terminal folgendes Kommando aus:

```
multipass launch --name testsystem
  21.10
```

Die erstmalige Einrichtung des Systems beansprucht etwas mehr Zeit, weil die notwendige Imagedatei erst heruntergeladen werden muss. Das Terminal informiert Sie über den Fortschritt. Am Ende erhalten Sie einen Hinweis „Launched", sofern alles funktioniert hat. Mit dem Kommando

```
multipass list
```

verschaffen Sie sich jederzeit einen Überblick über die laufenden Instanzen. Da zum Angebot auch eine VM mit Docker gehört, können Sie sich die ersten Schritte mit Containern gefahrlos in einer solchen virtuellen Instanz erarbeiten. Ein wichtiges Kommando im Zusammenspiel mit einer VM ist „exec". Damit führen Sie Befehle direkt in der VM aus, ohne sich dort erst via Shell anzumelden. Haben Sie das System „LinuxWelt" auf Basis des Images „Docker" eingerichtet, können Sie Docker dann auch ferngesteuert starten:

```
multipass exec LinuxWelt docker
```

Das war es auch schon. Docker läuft.

Wenn Sie einen individuellen Namen vergeben haben, ist es sehr einfach, sich mit der virtuellen Maschine zu verbinden. Dazu nutzen Sie das Kommando „shell":

```
multipass shell testsystem
```

Das virtuelle System begrüßt Sie jetzt, als hätten Sie sich via SSH oder direkt in einem Terminal angemeldet. Multipass installiert auch einen Eintrag im Systemabschnitt der Kontrollleiste. Darüber starten Sie bei Bedarf Instanzen oder öffnen ein Terminal. Dort können Sie nun die gewohnten Kommandos nutzen, etwa um weitere Software oder Serverdienste zu installieren, die Sie benötigen. Die Shell verlassen Sie einfach mit dem Kommando „exit" wieder. Die virtuelle Maschine läuft weiter.

Daten zwischen Host und VM teilen

Wenn Sie dies wünschen, können Sie Dateien zwischen dem Host und der virtuellen Maschine austauschen. Das funktioniert über das Mounten eines lokalen Verzeichnisses. Sie können das gesamte Home-Verzeichnis einfach in die VM integrieren, aber auch jeden anderen Pfad, sofern Sie dort die Dateirechte besitzen. Das geht sowohl nachträglich als auch beim Start einer virtuellen Maschine. Um das Home-Verzeichnis mit der VM zu verbinden, nutzen Sie dieses Kommando (Beispiel):

```
multipass mount $HOME LinuxWelt
```

Achten Sie beim Experimentieren mit virtuellen Maschinen und solchen Freigaben darauf, dass Sie in der VM auch Dateien löschen und ändern können, die auf dem Hostsystem liegen. Mittels

```
multipass umount LinuxWelt
```

heben Sie die Verbindung wieder auf. Sie können auch ein Zielverzeichnis auf der VM vorgeben, unter der das Hostverzeichnis gemountet werden soll (Beispiel):

```
multipass mount $HOME LinuxWelt:/
  test/
```

Wenn die Verbindung bereits beim Starten aktiviert werden soll, ergänzen Sie das Kommando „launch“ um den Schalter „- mount“ mit den gewünschten Pfadangaben.

Desktop nachinstallieren

Sie würden gern eine grafische Oberfläche nutzen? Auch das funktioniert. Dazu wird ein Desktop in der virtuellen Maschine installiert und via RDP angesprochen. Melden Sie sich zunächst in der virtuellen Maschine an. Dort installieren Sie mit

```
sudo apt install ubuntu-desktop
sudo apt install xrdp
```

die grafische Oberfläche und den Server für den Remotedesktop, alternativ auch das Paket „freerdp“. Um sich anmelden zu können, müssen Sie dem Nutzer „ubuntu“, der sich sonst einfach mit dem Multipass-Kommando direkt mit der Maschine verbindet, ein Passwort zuweisen. Das erledigen Sie mit

```
sudo passwd ubuntu
```

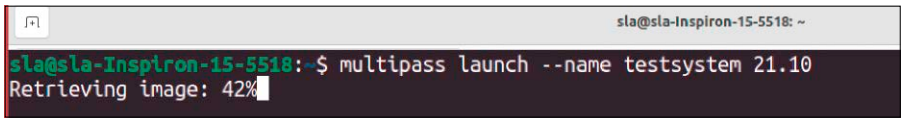
und nachfolgender Passworteingabe. Sind Installation und Einrichtung des Benutzers abgeschlossen, ist die Serverseite fertig. Sie benötigen jetzt auf dem Hostsystem noch eine Software, die das RDP-Protokoll unterstützt. Immer eine gute Wahl ist Remmina, zumal es auf Ubuntu-Systemen in der Regel vorinstalliert ist. Falls nicht, holen Sie das mittels des Kommandos

```
sudo apt install remmina remmina-
  plugin-rdp
```

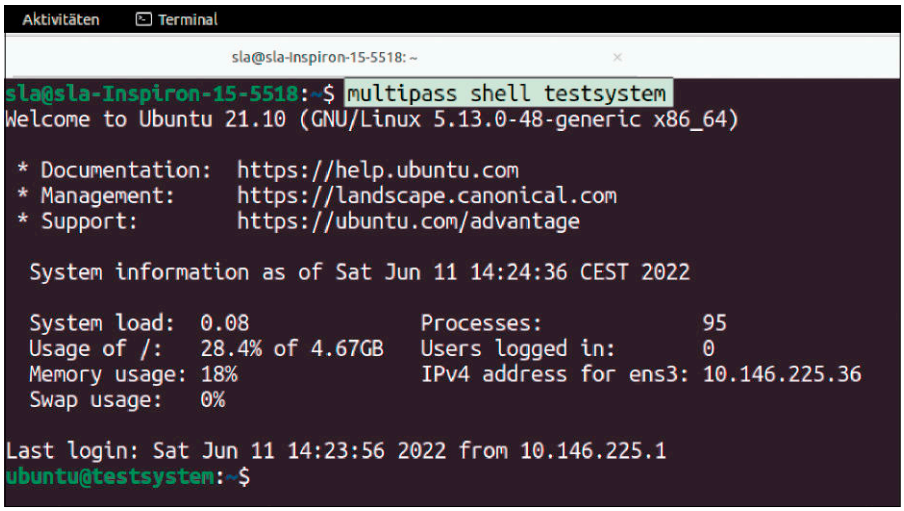
nach. Über „multipass list“ fragen Sie dann die aktuelle IP-Adresse der virtuellen Maschine ab und verbinden sich mit

```
remmina -c rdp://[IP-ADRESSE]
```

und dem gerade vergebenen Passwort mit dem Desktop der VM.

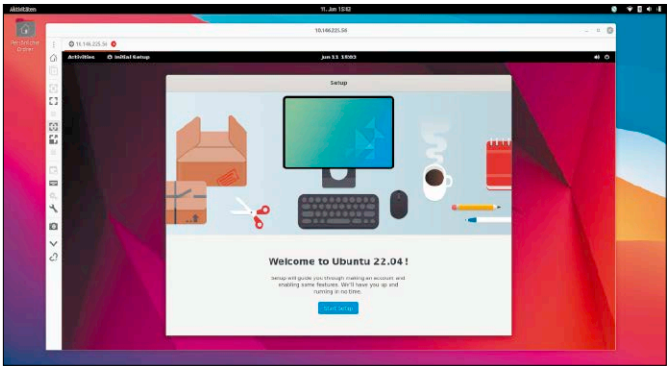


Installation einer VM-Instanz: Die Imagebezeichnung – hier „21.10“ – entnehmen Sie der Spalte „Image“ des Befehls „multipass list“.



Mit dem Kommando „shell“ melden Sie sich beim virtuellen System an.

Multipass-Instanzen können auch mit einem Desktop ausgestattet werden, auf den Sie dann via Remotedesktop zugreifen.



Hardware und Instanzen

Bereits beim Start einer VM können Sie die Zahl der verwendeten CPU-Kerne und die Größe des Arbeitsspeichers verändern. Dazu werden die Parameter „-c“ und „-m“ benötigt. Soll also die neue Instanz zwei CPU-Kerne und vier GB Arbeitsspeicher nutzen, so lautet der Aufruf so:

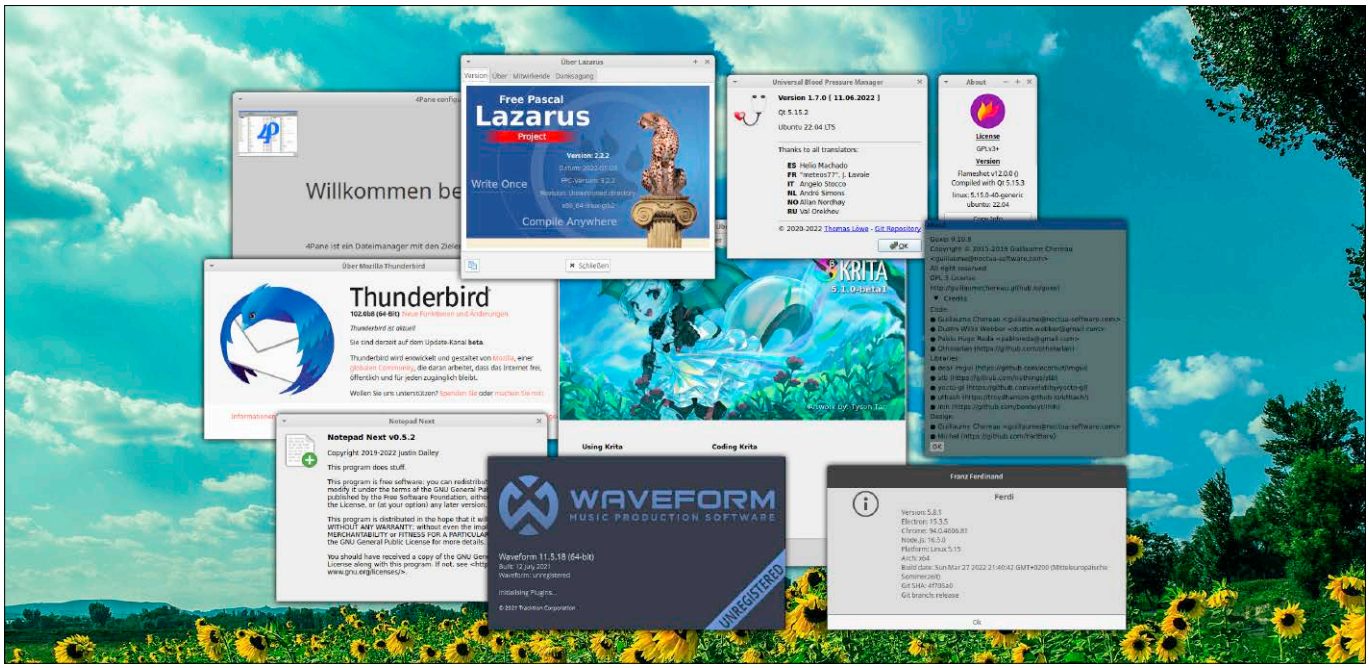
```
multipass launch -c 2 -m 4G – name
  LinuxWelt
```

Der weitere Schalter „-d“ (für „disk“) steht für die Größe des Massenspeichers der VM. Auch hier können Sie nach Belieben die Werte verändern. Sie sollten bei allen Optionen nur bedenken, dass Sie die Ressourcen dem Hostsystem abziehen.

Wenn Sie eine virtuelle Maschine stoppen wollen, erledigen Sie dies mittels

```
multipass stop [Name]
```

und der Schalter „delete“ verschiebt die Instanz in einen separaten Papierkorb. Wenn Sie sich die Liste Ihrer Instanzen ansehen, werden Sie danach immer noch die gelöschte Maschine finden, die sich mit „recover“ wiederherstellen ließe. Möchten Sie die VM komplett löschen, verwenden Sie das Kommando „multipass purge [Name]“. ■



Neue Software

In der Open-Source-Szene gibt es keine lange Sommerpause: Als Schwergewicht macht Thunderbird mit einer neuen Hauptversion auf sich aufmerksam. Außerdem gibt es wieder viele kleine, clevere Produktivitätstools in den folgenden Vorstellungen.

VON DAVID WOLSKI

Mit zunehmender Bedeutung von Open Source sind auch besonders unangenehme Zeitgenossen und deren Anwälte auf Projekte aufmerksam geworden: Patent-Trolle kaufen ein breites Portfolio an Patenten an allen möglichen Softwareentwicklungen auf, um diese dann für puren Profit durch Rechtsstreitigkeiten und Unterlassungsklagen gegen andere Entwickler zu verwenden. In der allgemeinen Softwareentwicklung und im Cloudbusiness ist eine regelrechte Schattenwirtschaft entstanden, wo diese Patent-Trolle agieren, im juristischen Englisch „Patent Assertion Entities".

Sie analysieren andere Unternehmen in Bezug auf etwaige Rechtsverletzungen und greifen sie juristisch an, verlangen Lizenzkosten oder eine Beteiligung an den Erlösen. Ein Fall, der gleich in die Öffentlichkeit kam, war eine Unterlassungsklage gegen die Gnome Foundation wegen der Fotoverwaltung Shotwell im Jahr 2019.

Jetzt, nach mehreren Jahren Rechtsstreit, fand der Fall für die Gnome Foundation ein gutes Ende: Zunächst kam durch Spenden eine Summe von 150 000 US-Dollar für eine außergerichtliche Einigung zusammen. Ein Open-Source-Enthusiast und Anwalt der Kanzlei „Lex Pan Law" blies zudem zum Gegenangriff und erreichte dazu im Nachhinein noch eine Löschung der abgemahnten Patente – diesen Trollen ist damit der Zahn gezogen.

Trolle aus den eigenen Reihen

Dieses Geschäftsmodell der Patentklagen ist unerfreulich für die Betroffenen. Es funktioniert aber auch in die andere Richtung: Der einstige Hauptentwickler der Netzwerkkomponente „Netfilter" des Linux-Kernels verklagte noch Jahre nach seiner Mitarbeit am Kernel etliche Firmen wegen Lizenzverletzungen, wenn diese den Paketfilter ohne korrekte Lizenzierung und Auszeichnung nach der GPL in ihren Produkten nutzten. Im Embedded-Bereich sind dies nicht wenige Firmen und es sind etwa fünfzig solcher Fälle bekannt geworden. Der Kernel-Entwicklergemeinde fielen die Aktionen, gedacht nur zur Bereicherung eines einzelnen, sehr unangenehm auf. Die Linux Foundation und Linus Torvalds selbst raten stets vom Rechtsweg bei Lizenzverletzungen ab, da dies der weiteren Akzeptanz von Linux in der Industrie abträglich ist. Eine gütliche außergerichtliche Einigung hat nach der Philosophie der Kernel-Gemeinde immer den Vorzug gegenüber dem Rechtsweg.

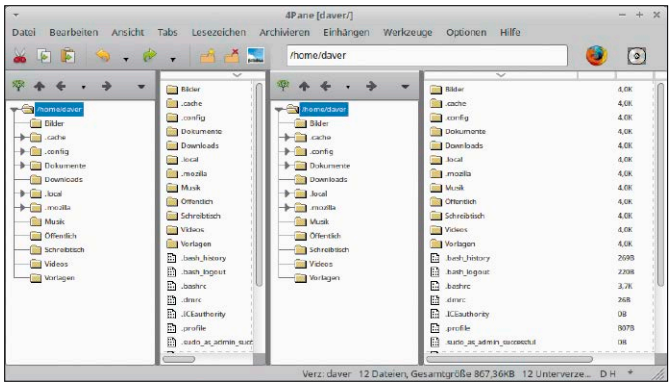
Einen Patent-Troll aus den eigenen Reihen musste das Kernel-Team deshalb selbst einfangen und vor Gericht zerren. Dort wurde mit einem ehemaligen Mitglied ein gerichtlicher Vergleich abgeschlossen, um Alleingänge bei lizenzrechtlichen Klagen zu unterbinden.

Der Vergleich wurde mit dem ehemaligen Netfilter-Entwickler am Landgericht Mannheim geschlossen: Heute bedarf es vor juristischen Schritten wegen Lizenzverstößen immer einer Abstimmung mit Mehrheit im aktiven Netfilter-Team.

4Pane 7.0

Mehr-Fenster-Dateimanager für Fortgeschrittene
https://4pane.co.uk

Zeitlos ist das Konzept zweier Fenster für Dateioperationen. Denn es geht ja meist darum, etwas von A nach B zu kopieren oder zu verschieben. Entwickler und Admins haben es aber oft mit mehreren Ordnern zu tun. Für diesen Zweck ist 4Pane gemacht, das in zwei Spalten eine Baumansicht und Ordneransicht anzeigt. Es gibt Undo-Schritte, Archivmanagement und ein eingebautes Terminal. Version 7.0 liegt ab Ubuntu 22.04 in den Standard-Paketquellen. ■

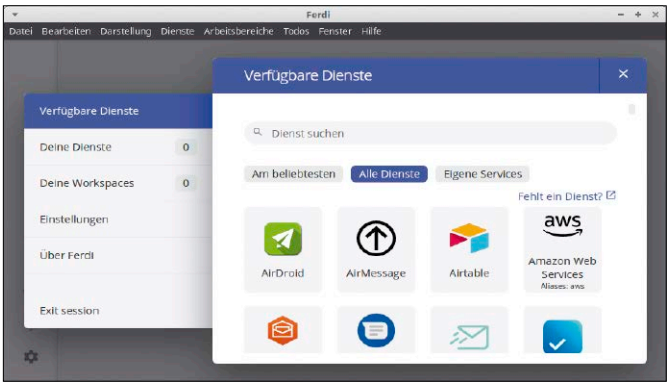


Dateimanager 4Pane: Das gut konfigurierbare Werkzeug bietet über Hilfsprogramme auch Netzwerkfunktionen für SSH, NFS und Samba an.

Ferdi 5.8.1

Freier Multimessenger
https://github.com/getferdi/ferdi

Fast jeder größere Onlinedienst hat heute seine eigenen Kurznachrichtendienste, um Teams die Kommunikation zu erleichtern. Hinzu kommen die üblichen Messenger Slack, Matrix, Whatsapp und Telegram. Ferdi bringt Dutzende Dienste unter einen Hut. Zudem gibt es eine Aufgabenplanung für Microsoft Todo, Franz Todo, Todoist und Any.do. Fertige DEB-Pakete für Debian/Ubuntu und einen Appimage-Container liefert die Projekt-Webseite. ■

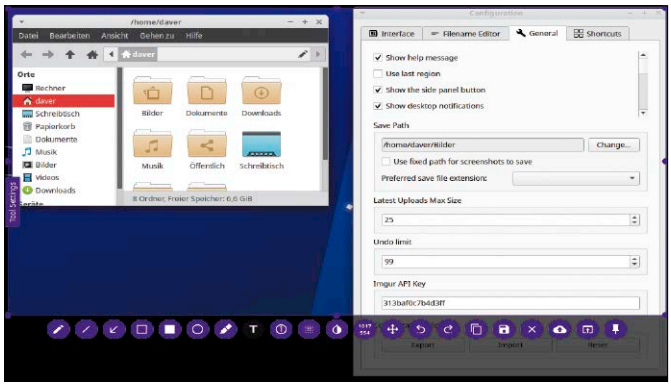


Kommunikationsfreudig: Ferdi ist eine Abspaltung des Programms Franz und vereint wie dieses Dutzende Messenger in einer Oberfläche.

Flameshot 12.0

Bildschirmfotos aufnehmen und bearbeiten
https://flameshot.org

Flameshot kann den Bildschirm eines Linux-Desktops sowie von Windows und Mac-OS aufnehmen. Auch Programmfenster oder ein manuell ausgewählter Bereich sind möglich. Anders als die typischen Screenshottools liefert es gleich einen Werkzeugkasten mit und macht damit den Gang in eine Grafikbearbeitung oft unnötig. Flameshot funktioniert außerdem auch schon unter Wayland. Fertige Binarys und ein Appimage liefert die Webseite. ■



Bitte recht freundlich: Flameshot ist ein plattformübergreifendes Screenshottool, das gleich typische Funktionen der Bildnachbearbeitung mitliefert.

Goxel 0.10.8

Erstellt 3D-Modelle aus Bausteinen
https://goxel.xyz

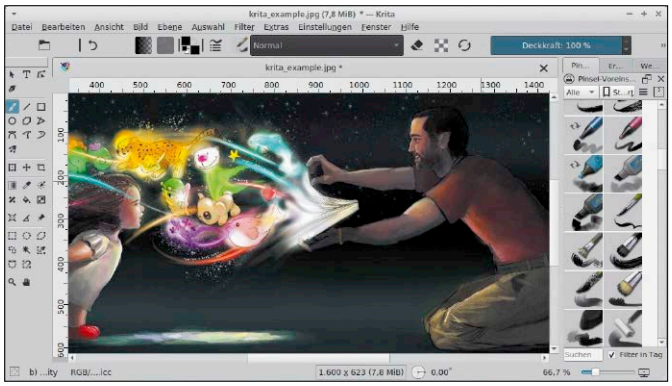
Illustrationssoftware wie Inkscape oder Modeller wie Blender verlangen viel Einarbeitungszeit. Für stilisierte Grafiken in Präsentationen und auf Webseiten ist Goxel einfacher. Es dient der Erstellung von Polygongrafiken und 3D-Modellen, die wie in Minecraft aus quadratischen Elementen zusammengesetzt werden. Für die Blöcke stehen Farben und Materialien zur Auswahl, für erstellte Szenerien Beleuchtungseffekte und schließlich Exportfunktionen. ■

3D-Modelle aus Blöcken: Goxel ist ein Editor, der den Minecraft-Stil imitiert. Eine Online-App steht unter *https://goxel.xyz/live* bereit.

Krita 5.1

Anspruchsvolle Grafikbearbeitung
https://krita.org

Während Gimp 3.0 auf sich warten lässt, kommt das Grafikprogramm Krita flott voran. Version 5.1 verbessert die Unterstützung von Webp-Grafiken, kann mit PSD-Dateien (Photoshop) umgehen und führt das Format JPG XL ein, das im Web zusehends wichtiger wird. Auf einem Touchscreen können Eingaben individuell angepasst werden und die Android-Version wurde durch Vektorrechnung (SIMD) beschleunigt. Die Webseite liefert ein Appimage für Linux. ■

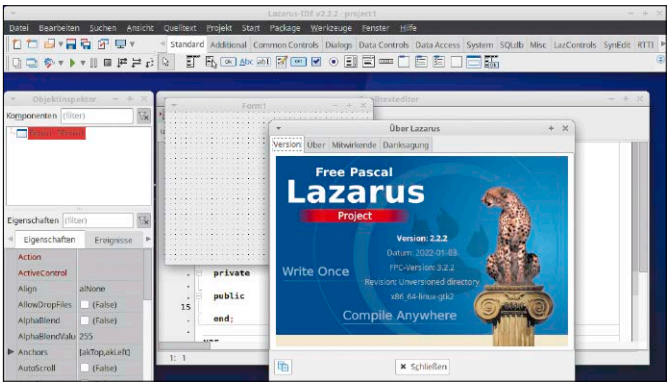


Ideal für Zeichnungen: Krita hat Gimp im künstlerischen Bereich den Rang abgelaufen. Es liegt auch in einer Android-Ausgabe vor.

Lazarus 2.2.2

Entwicklungsumgebung im Stil von Delphi
www.lazarus-ide.org

Unter Windows hatte die Entwicklungsumgebung Delphi eine treue Gemeinde. Lazarus hat vor zwanzig Jahren dessen Nachfolge angetreten, nachdem Borland Delphi einstellte. Die Lazarus-Bibliothek ist auch für kommerzielle Software geeignet. Grafische Programme können mit Qt, GTK2, unter Mac-OS mit Cocoa oder Carbon und in Windows mit der Win API erstellt werden. Die Installation gelingt mit DEB- oder RPM-Paketen von der Webseite. ■

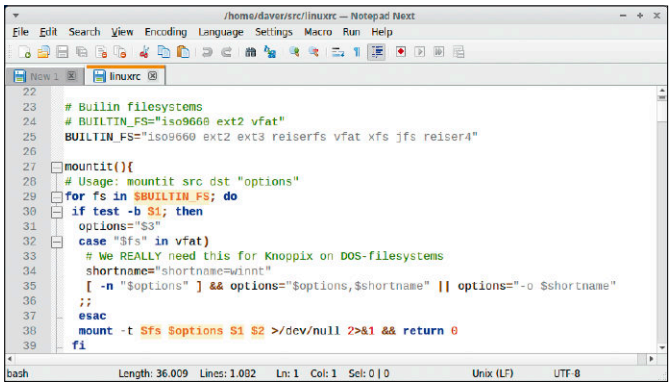


Grafische Programme entwickeln: Lazarus ist die freie Fortführung von Borland Delphi und zu einem gewissen Grad sogar plattformunabhängig.

Notepad Next 0.5.2

Klon des Texteditors Notepad++
https://github.com/dail8859/NotepadNext

Windows-Umsteiger oder Anwender, die beide Systeme nutzen, suchen unter Linux oft eine Entsprechung für gewohnte Tools. Dieser Editor ist ein Nachbau des Windows-Tools Notepad++. Notepad Next ist in Qt5 erstellt und liefert ähnlichen Funktionsumfang, Aufbau und Hotkeys wie das Windows-Vorbild. Es gibt eine Mehrfensteransicht, Syntaxhervorhebung und Codefolding (Ausblenden von Abschnitten). Für Linux liegen ein Appimage und ein Flatpak vor. ■

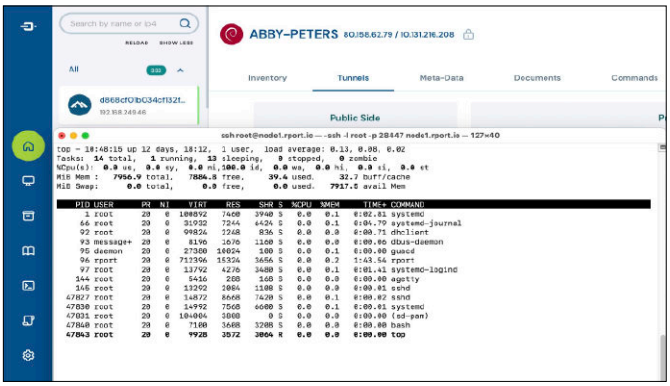


Eingängiger Editor für kleine und größere Aufgaben: Notepad Next ist ein Klon von Notepad++ und bildet dessen Funktionalität und Aussehen nach.

Rport 0.7.2

Fernwartung durch Reverse Tunneling
https://oss.rport.io

Das plattformunabhämgige Rport ist eine Server-Client-Lösung, um auf Systeme zu kommen, die hinter einer Firewall oder einem Router mit NAT stehen. Dazu baut jeder Client eine verschlüsselte SSH-Verbindung zum Rport-Server auf, der selbst gehostet werden kann. Die neue Version 0.7.2 erlaubt sichere Dateiübertragung zu Clients (Windows, Mac-OS, Linux) und verfügt über einen zentralen Aufgabenplaner. Fertige Pakete stellt die Webseite bereit. ■

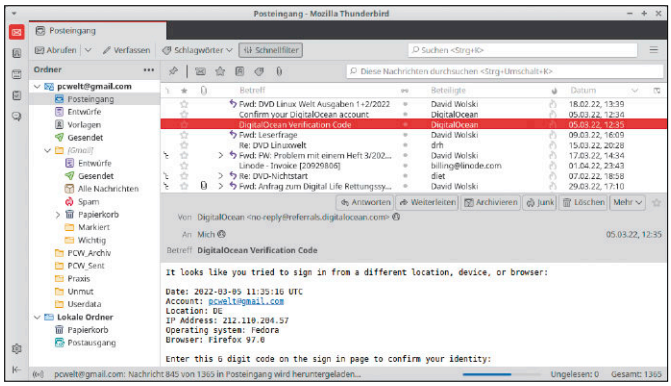


Alles durch den Tunnel: Rport erstellt SSH-Verbindungen über HTTP Connect vom Client zum Server, um dann beliebige TCP-Protokolle zu tunneln.

Thunderbird 102

Neue Version des Mailclients
www.thunderbird.net/de

Etwas mehr als ein Jahr nach der letzten Hauptversion macht Thunderbird den Sprung auf Version 102. Hier gibt es ein neues Adressbuch mit Kontaktübersicht und Unterstützung für das Chatprotokoll Matrix. Der Editor hat eine Vorschau für eingefügte URLs und die Import/Export-Funktion erlaubt den einfacheren Mailumzug auf andere Systeme. Fertige Pakete liefert die Webseite, für Ubuntu auch das PPA *https://launchpad.net/~mozillateam/+archive/ubuntu/ppa*.

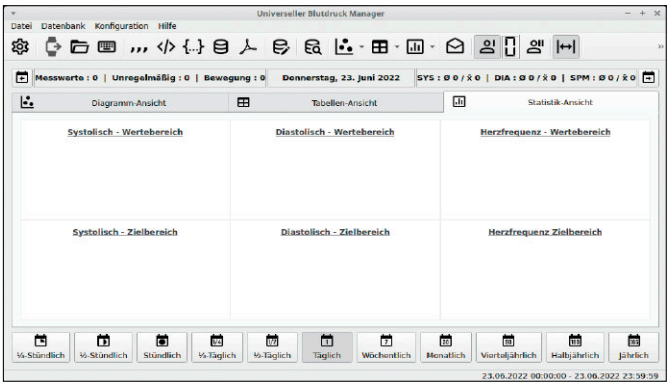


Mail, Matrix und mehr: Mit Thunderbird 102 wird das überarbeitete Programm auch zum Chatclient für das verschlüsselte Protokoll von Matrix.

Univ. Blood Pressure Manager 1.7

Verwaltung und Analyse von Blutdruckmesswerten
https://codeberg.org/LazyT/ubpm

Wer auf den Blutdruck achten muss, bekommt mit dem Universal Blood Pressure Manager ein Tool zur Aufzeichnung und Auswertung von Messdaten über längere Zeiträume. Die Software ist mehrsprachig, kann die Datenformate CSV, XML, JSON, SQL einlesen oder direkt von Messgeräten der Hersteller Beurer, Hartmann und Omron. Das Programm arbeitet offline, ohne Daten zu Herstellern zu übertragen, und liegt für Linux als Appimage vor.

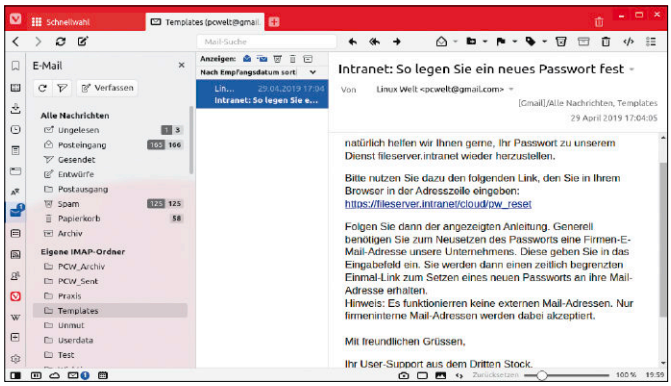


Blutdruck im Blick: Der freie Universal Blood Pressure Manager wertet manuell eingegebene oder eingelesene Blutdruckmesswerte aus.

Vivaldi Mail 1.0

Integrierter Mailclient im Browser Vivaldi
https://vivaldi.com

Hier handelt es sich nicht um ein eigenständiges Programm, sondern um eine neue Komponente des Browsers Vivaldi, der das Konzept der einst beliebten Mozilla Suite wieder aufleben lässt. Das Mailprogramm arbeitet mit POP- und IMAP-Servern, unterhält einen Offlinespeicher, erkennt Mailthreads und Mailinglisten, um diese in Ordnern zusammenzufassen. Integriert ist auch ein RSS-Feed-Reader. Zur Installation gibt es DEB- und RPM-Pakete.

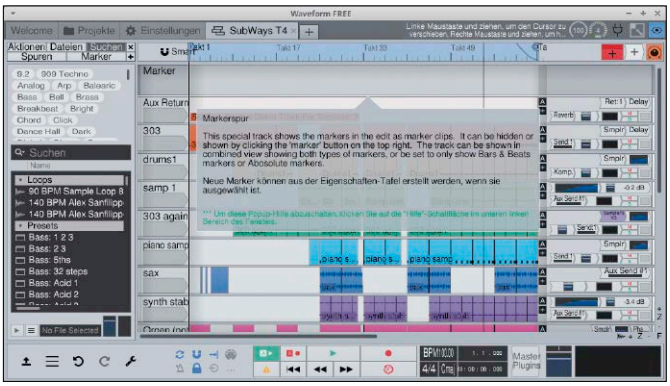


Verbindet Browser, Mail und Produktivitätstools: Vivaldi Mail 1.0 ist ein Neuzugang im gleichnamigen Browser, muss aber erst aktiviert werden.

Waveform Free 11

Kostenlose Variante des Audiotools
www.tracktion.com/products/waveform-free

Das mächtige Waveform Pro für professionelle Ton- und Musikproduktion ist kein Open-Source-Programm. In unregelmäßigen Abständen bietet der Hersteller aber eine ältere Version als Freeware an. Waveform Free 11 gibt es auch wieder in einer Linux-Ausgabe, die nach der Eingabe einer gültigen Mailadresse freigeschaltet wird. Die Unterschiede zur Pro-Version betreffen einige Effekte und reduzierte Methoden zur Klangerzeugung.



Kostenlose Version für Linux: Waveform Free ist ein semiprofessionelles Studio-Produktionstool zum Schneiden und Arrangieren beliebig vieler Tracks.

Odroid M1: Neue Raspi-Konkurrenz

Seit Erscheinen des Raspberry-Modells 4 ist es für andere Platinenhersteller eine echte Herausforderung, zu einem angemessenen Preis ein überzeugendes Konkurrenzprodukt anzubieten. Der neue Odroid M1 will mit SATA-3-Port und NVMe-Slot punkten.

VON HERMANN APFELBÖCK

Die Platinenfamilie Odroid des koreanischen Herstellers Hardkernel (*www.hardkernel.com*) gehört seit Jahren zu den größten Raspberry-Konkurrenten. Die Odroid-Hardware ist robust und in der Regel ausgewogen konzipiert. Das einfache Grundkonzept war schon immer, für etwas mehr Geld mehr Leistung als der gerade aktuelle Raspberry zu liefern oder andere Anschlussmöglichkeiten als dieser. Die bisherige Palette mit Odroid XU4, Odroid HC4, Odroid N2 und Odroid H2 (nicht mehr verfügbar) wird neuerdings ergänzt durch die Platine Odroid M1. Wir hatten den Platinenrechner im Test und zeigen, was ihn auszeichnet und ob er sich einen Platz neben dem dominierenden Raspberry 4 verdient.

Odroid M1: Schnell ausverkauft

Vorneweg: Mit 150 Euro muss man mindestens rechnen, sofern man neben der eigentlichen Platine (etwa 100 Euro oder 120 Euro mit vier oder acht GB RAM) das unentbehrliche Netzteil (etwa 7 Euro), ein Gehäuse (etwa 13 Euro) und ein Kabel- und Montageset für SATA (etwa 13 Euro) benötigt. Und Achtung: Dies waren die Preise einschlägiger Elektronik-Versandhändler wie Pollin oder Reichelt im April und Mai. Seit der Odroid M1 in erster Marge schnell vergriffen war, stiegen umgehend die Preise. Es ist nicht auszuschließen, dass das genannte Bundle bis Erscheinen dieses Artikels bei 180 oder 200 Euro liegt. Preisdynamik, Lieferengpässe und eventuelle Wartezeiten zeigen, dass der Odroid M1 seine Nische sofort gefunden hat.

Die nachfolgenden Eckdaten versprechen in der Tat ein besonders flott laufendes Betriebssystem dank Installation auf NVMe, SATA oder eMMC sowie einen rasanten Serverbetrieb dank SATA-Laufwerk. Ein Sorglospaket für Einsteiger ist die Platine im Unterschied zum universellen Raspberry 4 indes nicht: WLAN- und Bluetooth-Chip fehlen, beim Einsatz eines SATA-Laufwerks gibt es Bedingungen, die man vorab kennen sollte, und auch bei USB ist nicht jede beliebige Anschlussoption möglich. Nicht zuletzt gibt es vorläufig nur ein schmales Angebot bei der Systemsoftware, sodass der Käufer bei der Auswahl des Betriebssystems eventuell Kompromisse eingehen muss. Aber das lohnt die Hardware allemal.

Anschlussfreudiger Odroid M1: Die Standardports oben bieten Gigabit-Ethernet, HDMI, je zweimal USB 2.0 und USB 3.0. Darunter gibt es den Slot für eine NVMe-SSD, rechts unten SATA-Datenport und SATA-Stromversorgung, unten Mitte den eMMC-Anschluss. GPIO-Pins und Audio-Klinkenbuchse sind ebenfalls vertreten.

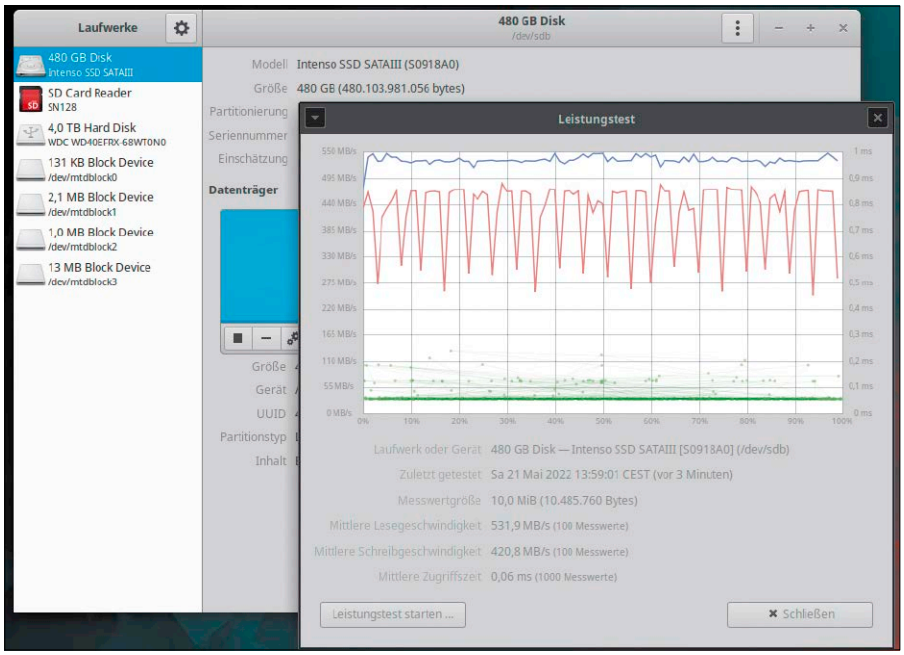
Odroid M1: Die technischen Eckdaten

Die ARM-Hardware läuft mit einem leicht angepassten Rockchip-Prozessor (RK3568B2) mit vier Cortex-A55-Kernen und einer Taktfrequenz von knapp zwei GHz. Diese CPU bringt die Platine in die Liga des Raspberry 4, erreicht dessen Leistung aber nicht ganz (siehe Kasten „Mini-Benchmark“ auf dieser Seite). Für den fest verbauten LPDDR4-Arbeitsspeicher gibt es zwei Varianten der Platine mit vier oder acht GB RAM. Der Preisunterschied beträgt gut 20 Euro. Nach unserer Marktbeobachtung wurde die Acht-GB-Variante am schnellsten ausverkauft und fordert derzeit auch die längeren Wartezeiten auf die nächsten Margen. Im Prinzip sollten für typische Serverrollen im Heimnetz aber auch vier GB RAM völlig ausreichen.

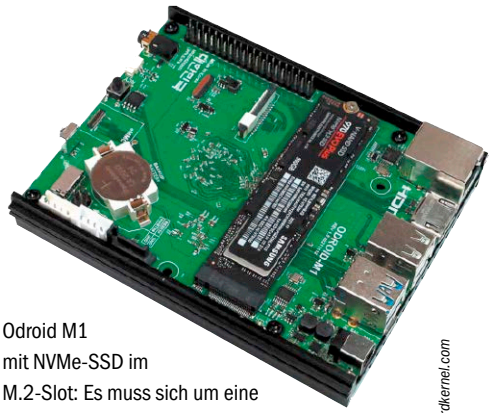
Für den Netzwerkanschluss ist ein Gigabit-Ethernet-Port vorhanden und zur Monitorausgabe ein HDMI-Anschluss. Für die sehr ordentliche bis gute Soundausgabe kann neben HDMI auch ein 3,5-Millimeter-Klinkenstecker dienen. Für Bastler und Industrieeinsatz kommt ferner noch ein DSI-Anschluss für einen kleinen LCD-Bildschirm hinzu. Ebenfalls für Bastlerprojekte kann eine Kamera über CSI angeschlossen werden. Auch die vom Raspberry bekannte 40-Pin-GPIO-Leiste ist verbaut.

Interessant für den Servereinsatz wird es bei den Anschlüssen für Datenträger: USB darf nicht fehlen und ist im Prinzip fünfmal vertreten – zweimal USB 3.0, zweimal USB 2.0 sowie ein Micro-USB-Anschluss (OTG). Der untere der beiden USB-3.0-Ports wird allerdings deaktiviert, falls der kleine OTG-Anschluss genutzt wird. Das ist kein großes Limit, aber man sollte dieses Detail nicht vergessen. Für an USB 3.0 angeschlossene Laufwerke gilt wie bei allen ähnlichen Platinen die Empfehlung, besser Datenträger mit eigener Stromversorgung anzuschließen. Zwei 2,5-Zoll-Laufwerke an USB und eventuell noch ein zusätzliches SATA-Laufwerk kann das Netzteil der Platine nicht stabil versorgen.

Das optionale SATA-Laufwerk versorgen die zwei Standardanschlüsse für das Daten- und das Stromkabel. Letzterer ist ein Fünf-Volt-Anschluss für 2,5-Zoll-HDDs oder SSDs. Eine große 3,5-Platte mit 12-Volt-Anschluss kann die Platine folglich nicht versorgen,



Leistungstest mit Gnome-Disks: Die (ältere) SATA-SSD liefert im Odroid M1 den erwarteten Datendurchsatz.



Odroid M1 mit NVMe-SSD im M.2-Slot: Es muss sich um eine PCIe-SSD handeln (Stichwort „M-Key“ oder „Key M“). Ebenfalls im M.2-Faktor erhältliche SATA-Laufwerke funktionieren nicht.

Quelle: www.hardkernel.com

MINI-BENCHMARK MIT RASPBERRY UND ODROID

Ein kleiner Vergleich mit der simplen arithmetischen Iteration

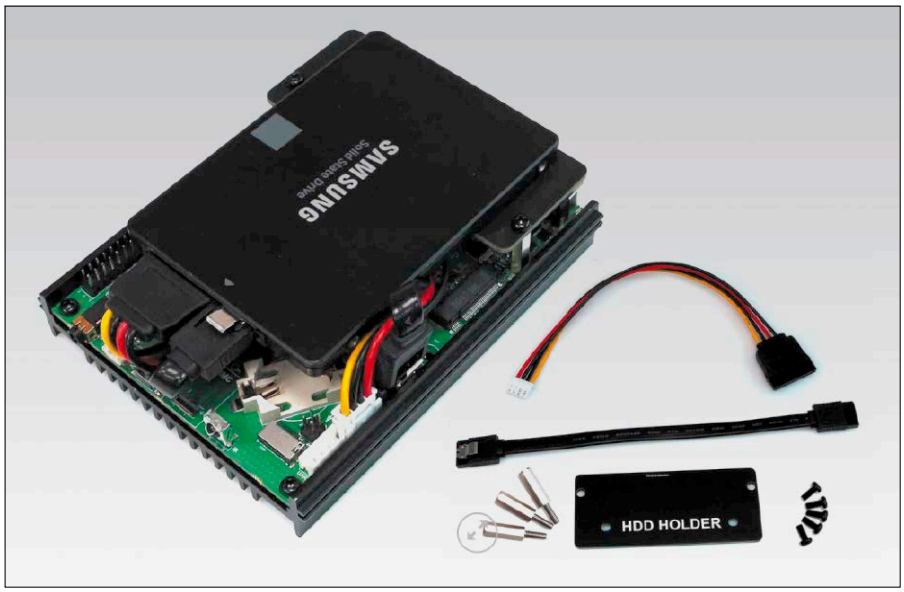
`time $(i=0; while (( i < 9999999 )); do (( i ++ )); done)`

auf etlichen Geräten ordnet die CPU-Leistung des neuen Odroid M1 ganz gut ein. Diese primitive Methode haben wir gewählt, weil auf den diversen Geräten mit diversen Betriebssystemen eine andere einheitliche Methode zu viel Aufwand erfordert hätte. Über die Aussagekraft des simplen Benchmarks lässt sich streiten, aber die Rangfolge deckt sich mit unserer praktischen Alltagserfahrung mit diesen Geräten. Der Raspberry Pi 4 liegt vor der neuen Odroid-Platine, deutlicher noch der Odroid N2 und der nicht mehr erhältliche Odroid H2. Der Fokus des neuen Raspberry-Konkurrenten Odroid M1 liegt eindeutig beim Angebot der Datenträgeranschlüsse, nicht bei der CPU-Leistung.

CPU-MINI-BENCHMARK

Gerät	Prozessor	Architektur	Zeit*
PC-System	Intel i7 (3,2 GHz)	x86	23,61
Odroid H2	Intel Celeron J4105 (2,5 GHz)	x86	45,45
Altes Notebook	AMD Phenom Dual (3,0 GHz)	x86	55,94
Odroid N2	Amlogic (1,8 GHz) / A53 (1,9 GHz)	ARM	67,99
Raspberry Pi 4	Cortex A53 (1,4 GHz)	ARM	113,11
Odroid M1	Rockchip RK3568B2 (2 GHz)	ARM	129,55
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

*kleiner ist schneller (Angabe in Sekunden)



Odroid M1 mit montierter SSD: Das Montageset für etwa 13 Euro ist unter Umständen entbehrlich, wenn SATA-Standardkabel vorrätig sind. Das Standardgehäuse ist bei einem SATA-Einbau in jedem Fall überflüssig, weil es dafür keinen Platz bietet.

diese müsste dann also mit externem Netzteil betrieben werden. Das von Hardkernel angebotene SATA-Montage-Set für circa 13 Euro umfasst nur die beiden Standardkabel und einen Hartplastik-„HDD-Holder“, um die SATA-Platte mit der Platine zu verschrauben. Das Zubehör ist verzichtbar, sofern Standardkabel vorliegen und der Datenträger nicht befestigt werden muss.

Für das Betriebssystem (oder Daten) gibt es neben dem üblichen Slot für eine Micro-SD-Karte und dem SATA-Laufwerk noch weitere Optionen: Es ist ein eMMC-Slot vorhanden (Embedded Multimedia Card) sowie ein Anschluss für ein SSD-Laufwerk vom Typ NVMe M.2. Letzteres muss eine PCIe-NVMe sein, eine NVMe mit SATA-Controller funktioniert dort nicht.

Wichtige Infos zur Systeminstallation

Auf *https://wiki.odroid.com/odroid-m1/odroid-m1* gibt es bislang nur einige wenige Systemimages zum Download (siehe dort „os_images“), die dann mit einschlägigen Tools wie Etcher oder Gnome-Disks auf SD-Karte zu übertragen sind. Zum Redaktionsschluss war die Auswahl verfügbarer Systeme noch sehr bescheiden und überdies unglücklich gewählt: Wer – naheliegend – die Hardware für Serveraufgaben nutzen will, wird nicht unbedingt zu Android 11 greifen. Ansonsten gibt es ein Ubuntu 20.04 ausgerechnet mit der anspruchsvollen Gnome-Oberfläche, die für die Hardware nicht angemessen erscheint. Zum Zeitpunkt des Produkttests erschien uns daher als einzig passende Wahl ein purer Ubuntu Server 20.04, auf den wir anschließend ein sparsames XFCE nachinstallierten. Die Zugangsdaten für fertige Odroid-Images lauten seit jeher „odroid“ mit Kennwort „odroid“.

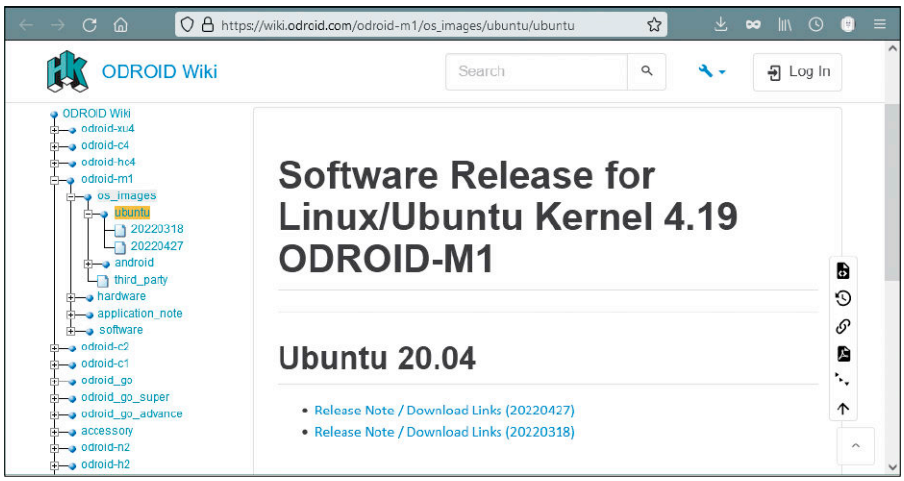
Diese traditionelle Systembestückung für Platinenrechner ist aber auf SD-Karten (eventuell noch eMMC) beschränkt. Wer das System auf SATA oder NVMe installieren will, muss einen anderen Weg einschlagen. Und dieser Weg erweist sich insgesamt als der klügere, weil er ein sauberes System ohne „odroid“-Konto, eine größere Systemauswahl, eine individuelle Desktopauswahl und vor allem die freie Wahl des Systemdatenträgers eröffnet.

Beim Start der Platine (mit oder ohne installiertes Betriebssystem) meldet sich das integrierte Minimalsystem Petitboot, das einige wesentliche Systeminfos anzeigt und ferner eine Multiboot-Auswahl des Betriebssystems erlaubt (falls etwa auf SD, SATA und NVMe verschiedene Systeme bereitstehen). Entscheidender ist aber die Fähigkeit von Petitboot, Betriebssysteme über das Internet zu laden und zu installieren. Diese Fähigkeit wird bei Hardkernel- oder Vertreiber-Dokumentationen lapidar vorausgesetzt, ist aber bislang nirgendwo prominent dokumentiert.

Um die im Netz verfügbaren Systeme aufzulisten, müssen Sie in Petitboot zunächst die unterste Option „Exit to shell“ wählen und dann die folgenden zwei Befehle eingeben:

```
udhcpc
netboot_default
```

Der erste stellt die Verbindung zum Netzwerk sicher, der zweite setzt die Bootpriorität auf die Netzwerkinstallation. Nach „exit“ und Verlassen der Mini-Shell zeigt das Petitboot-Menü oben die verfügbaren Betriebssysteme. Dies sind mehr, als die Downloadseite als traditionelle Images anbietet, allerdings ist von Kandidaten mit dem Hinweis „Work in Progress“ oder „Experimental“ eher abzuraten, da dies in unserem Fall prompt in einem fatalen Boothänger nach dem ersten Systemstart endete. Zum Zeitpunkt dieser Recherche waren nur Ubuntu 20.04 und Debian 10 als stabi-

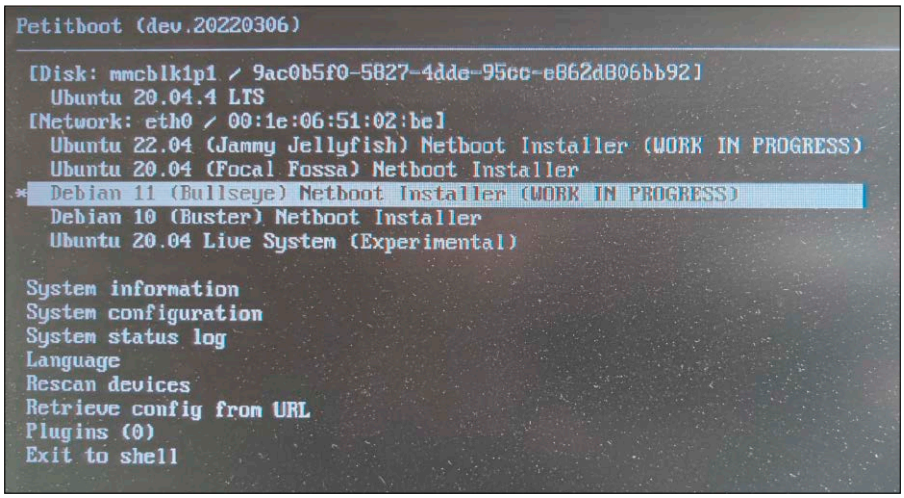


Klassische Images auf *https://wiki.odroid.com*: Dieser Weg eignet sich nur für den Transport auf SD-Karte. Eine Installation auf SATA oder NVMe muss über das Minisystem Petitboot erfolgen.

le Kandidaten erreichbar. Mindestens Ubuntu 22.04 und Debian 11 werden umgehend folgen.

Die weiteren Vorteile dieser Installationsweise sind offensichtlich: In den bekannten textbasierten Installern von Ubuntu und Debian sorgen Sie vorab für eine saubere Lokalisierung des Systems, für ein individuelles Systemkonto und entscheiden gegen Ende der Installation im Tasksel-Dialog über Desktop und gewünschte Serverdienste (SSH, Apache).

Für den Systemdatenträger gibt es beim Partitionierungsdialog kein Verbot – SD-Karte, NVMe-, SATA-, eMMC- oder auch USB-Laufwerke sind möglich.



Besser und flexibler als ein Imagedownload: Im integrierten Odroid-Minimalsystem können Sie die Netboot-Option freischalten und dann das gewünschte System aus dem Internet beziehen.

Odroid M1: Praxis, Tipps und Einordnung

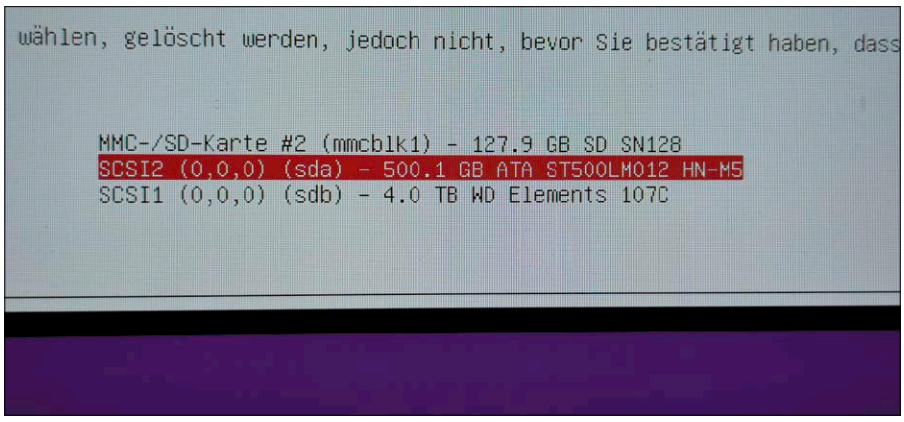
Die Platine arbeitet lüfterlos und somit absolut lautlos. Ähnlich dem Odroid N2 sitzt die gesamte Hardware auf einem großen passiven Kühlkörper und nach Ausweis des Sensortools des von uns genutzten XFCE-Desktops erreicht die Platine selbst bei Last kaum 40 Grad. Dies bestätigen auch eine haptische Kontrolle sowie der sehr niedrige Stromverbrauch: Wir messen etwa zwei Watt im Leerlauf und bringen den Odroid M1 selbst unter hoher Last nicht über 3,5 Watt Leistungsaufnahme – eventuelle mechanische Laufwerke oder Displays sind hier natürlich nicht eingerechnet.

Tipp zur Desktopwahl: Sofern man dem allzu anspruchsvollen Desktop Gnome aus dem Weg geht, arbeitet der Minirechner mit einem XFCE, LXDE oder LXQT jederzeit auch mit grafischer Oberfläche flüssig. Selbst für einen Odroid M1 in reiner Serverrolle empfehlen wir die Installation eines Desktops, der dann per HDMI oder VNC neben der SSH-Fernwartung auch eine bequeme Oberfläche anbietet. Bei vier oder sogar acht GB RAM fällt der meist ungenutzte Desktop kaum ins Gewicht.

Tipp für Datenfreigaben: Mechanische SATA-HDDs, auch wenn sie ausschließlich als Datenfreigabe dienen, sollten unbedingt mit dem Standard-Dateisystem Ext4 formatiert werden. Das von Hardkernel früh angebotene Ubuntu 20.04 hat einen relativ betagten Kernel mit mäßiger NTFS-Unterstützung. Der Datendurchsatz kommt damit kaum über 30 bis 40 MB/s und liegt damit sogar unter den etwa 80 MB/s, die per USB angeschlossene Datenträger erreichen. Es wäre daher kontraproduktiv, die M1-Platine wegen der SATA-Schnittstelle zu erwerben und dann mit NTFS auszubremsen. SSDs am SATA-Port sind hingegen mit jedem beliebigen Dateisystem schnell genug, um im Gigabit-Netzwerk die Daten mit den maximalen 110 bis 120 MB/s auszuliefern.

Tipp zum Zubehör: Für den Odroid M1 gibt es ein hübsches blaues Aluminiumgehäuse, das als Staubschutz prinzipiell zu empfehlen wäre. Es wird einfach auf die passende Rille des großen Kühlkörpers aufgeschoben und dann auf beiden Seiten mit Endabdeckungen verschraubt. Ganz zu Ende gedacht ist das nicht, weil sich das Gehäuse mit dem interessantesten Hardwareangebot der Platine nicht verträgt: Ein SATA-Laufwerk bringen Sie nämlich nicht unter, wenn Sie das Gehäuse nutzen. Es ist nicht einmal möglich, die SATA-Kabel nach außen zu legen und das Laufwerk außerhalb zu nutzen, denn allein schon die eingesteckten SATA-Kabel machen es unmöglich, das Gehäuse auf die Platine zu schieben. Kurz: Wer vorhat, am Odroid M1 ein SATA-Laufwerk anzuschließen, kann sich den Kauf des Gehäuses von vornherein sparen.

Einordnung: Im Umfeld des Raspberry Pi 4 und den weiteren aktuellen Odroid-Platinen wird das Modell Odroid M1 aufgrund seiner Flexibilität mühelos seinen Platz finden. Daran lässt sich praktisch alles anschließen und einbauen, was man in der Schublade liegen hat. Da wird dann die kleine SSD, die für den Desktoprechner längst unterdimensioniert war, zum idealen Systemdatenträger. Als Datenserver garantiert die Platine jederzeit volle Gigabit-Leistung (120 MB/s), wenn die Daten auf einem SATA-Laufwerk liegen. Laufwerke an USB 3.0 liefern die Daten nicht schneller, aber auch nicht langsamer aus als beim Raspberry Pi 4 – also je nach Datengrößen etwa mit 40 bis 80 MB/s. ■

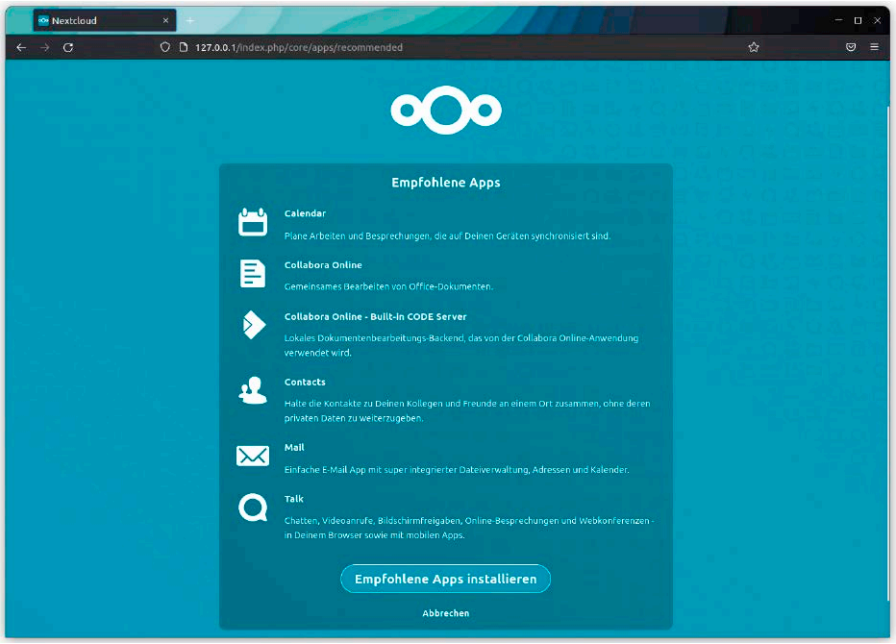


Mit Petitboot gestarteter Netinstaller (hier Debian): Damit bringen Sie das Betriebssystem auf jedes beliebige Laufwerk, das an der Odroid-Platine angeschlossen ist.

Nextcloud im Heimnetz

Dateien lassen sich über diverse Methoden im eigenen Netzwerk bereitstellen. Eine individuell eingerichtete Nextcloud ist sicher nicht die einfachste Servervariante, bietet aber breite Funktionalität und hohen Komfort.

VON HERMANN APFELBÖCK



LinuxWelt-Leser wissen es: Dies ist nicht der erste Beitrag zur Nextcloud (oder Owncloud). Allerdings setzen wir hier einen inhaltlichen Fokus auf die vielseitigen Anwendungsmöglichkeiten dieser Cloudsoftware. Wir behandeln die Nextcloud als Intranetserver im lokalen Netz, gehen dafür aber genauer auf die Apps und Optionen ein, die ein Nextcloud-Server hier sinnvollerweise anbieten kann. Daher vereinfachen wir auch das Thema der Installation und verzichten komplett auf den Aspekt der Öffnung für den Internetzugriff.

Einfache Installation als Snap

Für eine Nextcloud im Homeoffice oder im Kleinbetrieb mit einer Handvoll Mitarbeiter genügt ein Ein-Platinen-Rechner wie der Raspberry 4. Je nach Menge aktuell angemeldeter Nutzer und aktivierter Apps hat die Hardware aber durchaus zu arbeiten: Vier GB RAM sollten vorliegen, ferner für längerfristigen Einsatz ein größerer und schneller Systemdatenträger (schnelle SD-Karte oder Sata-SSD/HDD mit 128 GB aufwärts), idealerweise ergänzt durch ein größeres USB-Laufwerk, das später in die Nextcloud eingebunden wird.

Nextcloud erfordert einen kompletten LAMP-Server und eine nicht ganz einfache Apache- und Datenbankkonfiguration. Ungeachtet gewisser Nachteile (etwas mehr Ressourcenbedarf, theoretische Apache-Konflikte und lokale Pfadumleitungen) ist für eine Nextcloud im Intranet-Homeoffice die Einrichtung als Snap die mit Abstand einfachste Installationsvariante.

Es genügt nämlich dieser Befehl:

```
sudo snap install nextcloud
```

Danach ist der Webserver am lokalen Rechner bereits im Browser mit der Adresse *http://localhost* erreichbar. Vergeben Sie einen Kontonamen und das zugehörige Kennwort. Dies wird der primäre Administrator der Nextcloud-Instanz. Dann klicken Sie auf „Installieren“. Anschließend erhalten Sie das Angebot „Empfohlene Apps“, um damit schon mal eine Grundausstattung einzurichten. Nicht alle diese Module sind für den Einsatz im lokalen Netz einschlägig, aber doch einige. Überflüssige lassen sich später leicht wieder entfernen. Auf anderen Rechnern im Netz erreichen Sie die Instanz mit der IP-Adresse des Server-Rechners in dieser Form (Beispiel):

```
192.168.178.20/index.php
```

Für häufigen Einsatz empfiehlt sich ein Browserlesezeichen.

Tipp 1: Wir haben das Nextcloud-Snap auf mehreren Systemen getestet, und in der Regel funktioniert der Browser-Zugriff mit „[IP-Adresse]/index.php“ auf Anhieb. Der Browser wird zwar die unverschlüsselte HTTP-Adresse als „nicht sicher“ melden, aber das muss Sie im lokalen Netzwerk nicht kümmern. Falls die Seite wider Erwarten nicht erreichbar ist, kontrollieren Sie in der Konfigurationsdatei „config.php“

```
sudo nano /var/snap/nextcloud/
  [Version]/nextcloud/config/
  config.php
```

den Abschnitt „trusted_domains“. Dieser sollte einen Eintrag mit der IP-Adresse des Servergeräts enthalten. Steht hingegen nur

```
0 => 'localhost',
```

so ergänzen Sie darunter diese weitere Zeile (IP anpassen!)

```
1 => '192.168.178.20',
```

und starten das System neu.

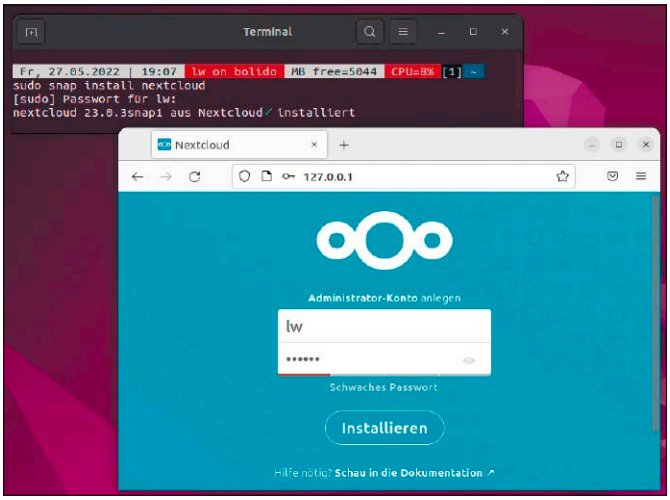
Tipp 2: Eine Snap-Installation ist ungünstig, wenn auf dem System bereits ein Apache-Webserver läuft. Das führt nicht nur zu Ressourcenverschwendung, sondern auch zu Portkonflikten. Der Apache-Server im Nextcloud-Snap nutzt standardmäßig die Ports 80 (HTTP) und 443 (HTTPS). Dies lässt sich im Prinzip umstellen (*sudo snap set nextcloud ports.http=81*), jedoch empfehlen wir im Hinblick auf einfache Verhältnisse das Nextcloud-Snap nur für Rechner ohne Apache.

Erste Schritte in Nextcloud

Alle administrativen Aufgaben erreichen Sie über das Benutzermenü (Kontosymbol ganz rechts oben). Administratorkonten sehen hier mit „Apps“ und „Benutzer“ zusätzliche Menüeinträge, außerdem bietet das Menü „Einstellungen“ für Administratoren einen zusätzlichen globalen Bereich „Verwaltung“ (während normale Benutzer hier nur das Angebot „Persönlich“ vorfinden). Eine erste Aktion, die sowohl für den Admin wie für spätere Benutzer anfällt, ist der Gang zu „Persönlich → Persönliche Informationen“, um hier Sprache und Gebietsschema auf „Deutsch“ zu setzen. Alle weiteren Angaben sind optional.

Als nächsten Schritt des Erstbenutzers und Admins lohnt sich ein Blick unter „Verwaltung“ und dort „Sicherheit“ sowie „Teilen“. Für eine lokale Nextcloud-Instanz (aber nur hier!) sind einige Standards übertrieben. So können etwa die Komplexitätsanforderungen an die Zugangskennwörter deutlich reduziert werden. Es ist zweckmäßig, dies bereits vor dem Anlegen zusätzlicher Teilnehmer festzulegen.

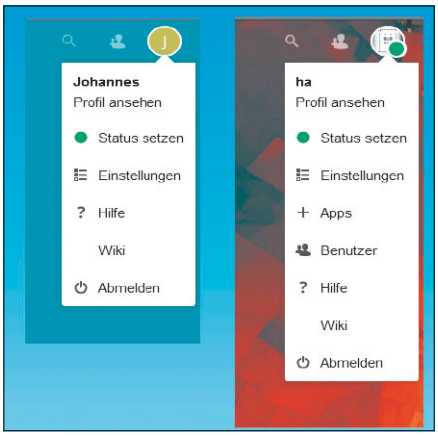
Eine weitere wichtige Anlaufstelle unter der nur für Admins zugänglichen „Verwaltung“ ist der Punkt „System“. Der bietet einen grafischen Systemmonitor und zeigt unter „Festplatte“ die gemounteten Laufwerke. Das ist besonders bei einer Snap-Installation relevant, weil hier die Mountpunkte intern umgeleitet werden. Die Pfade sind später für die Einbindung externer Datenträger wichtig und können an dieser Stelle einfach kopiert werden. Die benötigten



Einfacher geht's nicht: Mit einem Kommando ist der Nextcloud-Server samt Apache, Datenbank und PHP startbereit.

Manchmal erforderlich, meistens nicht: Wenn Browser die Nextcloud-Anmeldung verweigern, dann hilft es, die IP-Adresse des Nextcloud-Servers manuell als „trusted_domain“ nachzutragen.

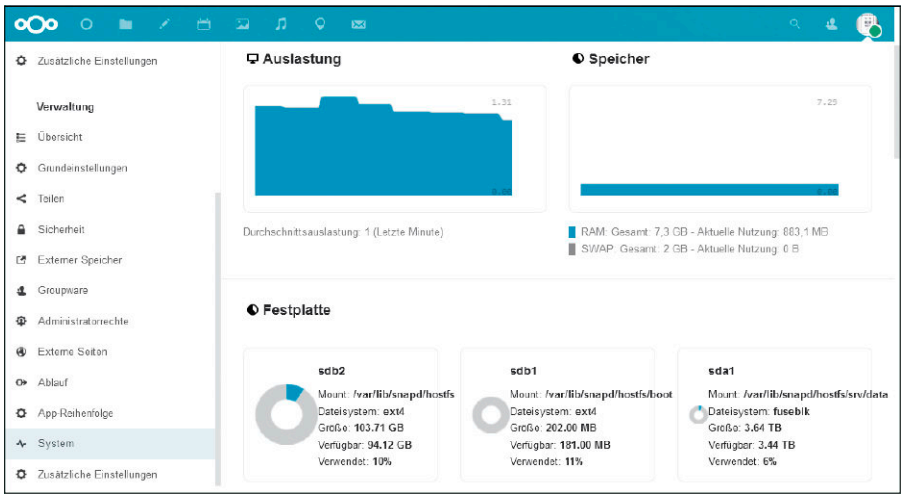
Konten legen Sie dann über das Benutzermenü mit dem Eintrag „Benutzer“ und dann „Neuer Benutzer“ an. Mindestens erforderlich sind der Kontoname und das Passwort. In der Spalte „Gruppen“ können Sie das neue Konto als „admin“ deklarieren, sofern der neue Benutzer administrative Rechte erhalten soll. Dieser Nextcloud-Dialog bietet auch die Einrichtung weiterer Gruppen („+ Gruppe hinzufügen“), jedoch sollte die einfache Standardunterscheidung zwischen Admin-Konten und normalen Benutzerkonten ausreichen. Die neuen Benutzer können später über „Einstellungen → Persönlich“ selbst für deutsche Lokalisierung, für sonstige Konteneigenschaften sorgen und auch ein neues Passwort einrichten. Theoretisch können Sie als Admin die Lokalisierung und Kontoinfos auch vorab (durch Anmeldung in den neuen Konten) eintragen, um den Teilnehmern eine Eingangshürde zu nehmen.



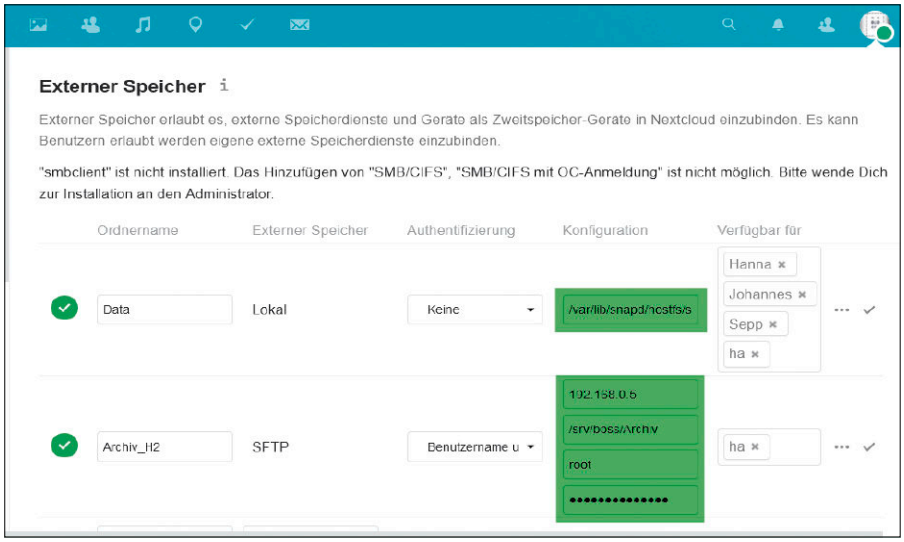
Das Benutzermenü von Admin versus Benutzer: Admins dürfen Apps und Benutzer installieren und ändern. Auch der Umfang der „Einstellungen“ ist beim Benutzer nur „Persönlich“.

Auswahl der gewünschten Apps

Die Nextcloud ist ein modularer Kosmos mit sehr vielen optionalen Plug-ins („Apps“). Es wäre eine Illusion zu glauben, eine neu installierte Nextcloud nach einer Stunde produktiv nutzen zu können. Den Grundstein legt der Administrator über die Auswahl der aktiven Apps. Wird nach Klick auf das Benutzermenü links oben das Menü „+Apps“ gewählt, erscheint ein umfangreiches und relativ unübersichtliches Angebot: „Deine Apps“ listet alle installierten



Nextcloud-Systemmonitor: Diese Infos unter „Einstellungen –› Verwaltung –› System“ sind nur für den Admin zugänglich. Wichtig sind – gerade beim Nextcloud-Snap – die angezeigten Mountpfade.



Wichtige App für andere Apps: „External storage support“ integriert lokale Laufwerke und Netzressourcen und ist damit die Voraussetzung für Multimedia- und Daten-Apps.

– aktive wie inaktive – Module alphabetisch auf, während „Aktive Apps“ und „Deaktivierte Apps“ die installierten Module der Gesamtliste entsprechend filtern. Der Punkt „App-Pakete“ zeigt einige vorgeschlagene App-Bundles, die als Gruppe installiert, aktiviert oder deaktiviert werden können. Die Bundles „Hub-Paket“ und „Groupware-Paket“ sind meistens unentbehrlich, aber auch größtenteils schon vorhanden, wenn Sie bei der Installation das Angebot „Empfohlene Apps“ angenommen haben.

Ein weiterer App-Filter ist der nächste Navigationspunkt „Vorgestellte Apps“. Hier handelt es sich um bewährte Module der Nextcloud-Entwickler, die in technischer Hinsicht allesamt als Empfehlungen gelten können, was aber natürlich noch nichts über ihre inhaltliche Relevanz für eine lokale Intranetlösung aussagt. Was in der Navigation dann darunter folgt, also ab „Anpassung“ abwärts, sind rein inhaltliche Sammlungen: Hier steht dann in einer Kategorie wie „Dateien“ oder „Organisation“ Unentbehrliches neben Wichtigem bis Marginalem oder sehr Speziellem. Technisch ungetestete Apps werden aber ausdrücklich als solche angezeigt und ihre Installation bleibt im Ermessen des Nutzers.

Diverse Versions-, Kommentar- oder Kollaborationsmodule sind im privaten Kontext verzichtbar. Im Zweifel erhalten Sie in der App-Übersicht nach Klick auf den App-Eintrag eine englischsprachige, meistens sehr knappe Beschreibung. Da die Nextcloud die Apps im laufenden Betrieb ein- und ausschalten kann, bedeutet es aber wenig Aufwand, sich von der Notwendigkeit einer Komponente durch einfaches Ausprobieren zu überzeugen. Fast überall zu empfehlen sind in der Regel folgende Module:

- **„Calendar“** (Kalender-App)
- **„Dashboard“** (nicht notwendige, aber hübsche Startseite)
- **„External storage support“** (externe Datenträger und Freigaben)
- **„File Sharing“** (Datenaustausch unter Nextcloud-Benutzern)
- **„Mails“** (kompletter Mailclient)
- **„Music“** (Player und Musikverwaltung)
- **„Notes“** (einfache Notizen)
- **„PDF Viewer“** (PDF-Anzeige)
- **„Photos“** (Bildviewer mit Diashow)
- **„Text“** (einfacher Texteditor)
- **„Video player“** (Medienwiedergabe)

Je mehr von den größeren, serverrelevanten Apps Sie aktivieren (und gegebenenfalls vorher herunterladen), desto mehr füllt sich die Symbolleiste oben neben dem Nextcloud-Logo. Die einzelnen Apps sind dann per Klick auf ihr Symbol erreichbar. Alle Optionen, die sich im linken Navigationsbereich zeigen, beziehen sich immer ausschließlich auf die aktuell gewählte App.

Nextcloud-Apps: Spreu und Weizen

Nach dieser summarischen Auflistung wichtiger Apps stellt sich die Frage, welche Module für eine heimische Cloud sinnvoll und produktiv sind. Im Prinzip genügen schon zwei, drei oder eine Handvoll ausgewählter Apps, um einen Nextcloud-Server zu rechtfertigen. Typische Kollaborationsapps wie „Contacts“ (Kontakte), „Tasks“ (Aufgaben und Termine) und „Talk“ (Textchats und Videochats) sind für eine Intranetcloud weniger relevant. Auch Office-Kollaboration steht hier kaum an vorderster Stelle: „Collabora Online“ bietet zwar Kompatibilität mit Microsoft-Formaten, benötigt aber die Anbindung zu einem externen Server und ist relativ langsam.

Unverzichtbare App „Dateien“: „Dateien“ ist eine nicht mehr abwählbare Standard-App. Über das „+“-Zeichen legen Sie hier neue Ordner an oder laden einzelne oder mehrere Dateien vom lokalen System in die Nextcloud. Auch Drag & Drop vom lokalen Dateimanager in das Dateien-Fenster funktioniert. Selbst wenn die App „Dateien“ nur als Datenhalde für die Teilnehmer dient, ist dies eine bequeme Zentrale, da man sich

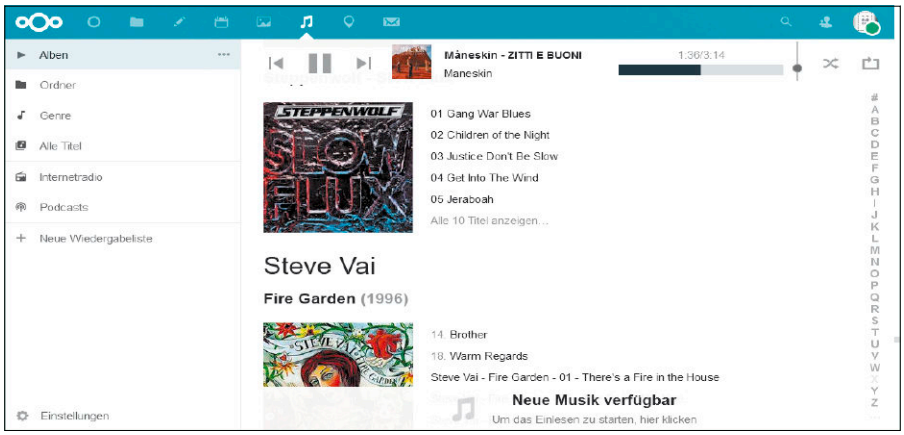
im Unterschied zu einem Samba-Server um die Benutzerrechte nicht kümmern muss. Falls andere Nextcloud-Nutzer Ihre Dateien verwenden oder herunterladen sollen, klicken Sie auf das Teilen-Symbol neben einer Datei oder einem Ordner und tippen dann im Feld unter „Teilen“ den Benutzernamen ein.

„External storage support“: Diese App – deutsch „Externer Speicher“ – erweitert die persönliche Nextcloud-Dateiablage für die Benutzer um einen allgemein zugänglichen Dateibestand. Damit wird die Nextcloud zu einem universellen Datenserver im Netz. Bei dieser App wird gerne die Einbindung von SFTP-Server (SSH), FTP-Server, Amazon, Webdav, SMB/CIFS betont. Weit wichtiger als diese Optionen, die meist schlicht zu langsam sind, ist die Einbindung von Datenträgern, die direkt am Nextcloud-Rechner angeschlossen sind. Auch dies erfordert den „External storage support“.

Die aktivierte Funktion erreichen Sie als Administrator mit „Einstellungen → Verwaltung → Externer Speicher“. Vergeben Sie einen sprechenden Ordnernamen, der später bei allen Benutzern auf oberster Ebene in der „Dateien“-App erscheinen wird. In der Auswahl „Speicher hinzufügen“ wählen Sie „Lokal“ für einen direkt am Nextcloud-Rechner angeschlossenen Datenträger. Als „Ort“ tragen Sie den Mountpunkt des Mediums ein. Bei einer Snap-Nextcloud ist dies allerdings nicht reale Mountordner, sondern ein umgeleiteter unter „/var/lib/snapd/hostfs/...“. Den richtigen Pfad finden Sie am einfachsten unter „Verwaltung → System → Festplatte“.

Die App „Externer Speicher“ eignet sich auch hervorragend zum Zusammenführen von verteilten Netzressourcen. So sind etwa Linux-Rechner mit SSH-Server schnell im Dateien-Bereich der Nextcloud eingetragen. Statt „Lokal“ wählen Sie hier „SFTP“, als „Authentifizierung“ die Option „Benutzername und Passwort“ und als „Konfiguration“ tragen Sie die IP-Adresse ein (gegebenenfalls mit Portangabe – etwa 192.168.0.178.20:2222), darunter den Mountpunkt der benötigten Ressource, ferner SSH-Benutzer (!) und dessen Kennwort. Welche Nextcloud-Benutzer auf einen externen Speicher zugreifen dürfen, lässt sich exakt einstellen. Eventuell ist es sinnvoll, die Freigabe generell schreibgeschützt zu setzen.

„Music“ – ein vollständiger Audioserver: Als Audiowiedergabe konkurrieren mehrere Nextcloud-Apps. Die App „Music“ bietet neben der Wiedergabe eine Medienverwaltung und berücksichtigt auch die Metadaten. „Music“ darf den Rang eines zwar schlichten, aber kompletten Medienservers beanspruchen. Neu eingebundene Nextcloud-Ressourcen („Externer Speicher“) können erfasst werden, sobald sie in der App unter „Ordner“ auftauchen: Dann erscheint im Hauptfenster unten „Neue Musik verfügbar“ und ein Klick darauf startet den Medienscan. Dieser kann durch einen App-Wechsel jederzeit unterbrochen und später fortgesetzt werden. Dies ist vorbildlich, weil somit die Nextcloud nicht durch langwierige Scans dauerhaft ausgebremst wird. Einmal eingelesene Songs sind über „Alben“, „Genre“ oder „Titel“ erreichbar.



„Musik“ als Beispiel einer Nextcloud-App: Der Navigationsbereich links sowie die dortigen „Einstellungen“ beziehen sich immer ausschließlich auf die aktuell gewählte App.

Die „Mail“-App: Allein der Nextcloud-Mailclient kann ein ausreichender Grund für eine Nextcloud sein. Statt nämlich auf diversen Rechnern je einen Mailclient à la Thunderbird oder Outlook zu verwenden, können alle Nextcloud-Nutzer ihre Mails im Browser via Nextcloud abfragen. Das Nextcloud-Modul ist ansehnlich und verwaltet für jeden Nutzer mehrere Mailkonten (im Navigationsbereich „Einstellungen → E-Mail-Konto hinzufügen“). In der Regel genügen zum Einrichten die Mailadresse und das Zugangskennwort. Mobile Geräte sollten aber weiterhin ihr eigenes Mailprogramm behalten, um auch außerhalb des lokalen Netzes Nachrichten zu empfangen.

„Photos“ und „Notes“: „Notes“ bietet einfache Notizen mit inhaltlichen Kategorien. Letztere sind über das unscheinbare „...“-Menü (rechts oben) über „Details“ zu vergeben. Die App speichert die Notizen einfach im Klartext ab und sortiert sie dabei in Ordner mit den Namen der Kategorien. Die Foto-App ist ebenfalls einfach, erkennt bei angeklickten Ordnern enthaltene Bilddateien und zeigt diese als Thumbnail-Vorschau. Beim Klick erscheint das Einzelbild und erlaubt Blättern oder automatische Diaschau. Eine Bearbeitung ist nicht möglich.

Hübsche optionale Ergänzungen: „Maps“ („Karten“) integriert Openstreetmap-Karten in die Nextcloud und ermöglicht dort individuelle Einträge mit Ortsfavoriten, Fotos und Strecken.

Der „EPUB/CBZ/PDF ebook reader“ ergänzt den auf PDFs beschränkten „PDF-Viewer“ um weitere Formate.

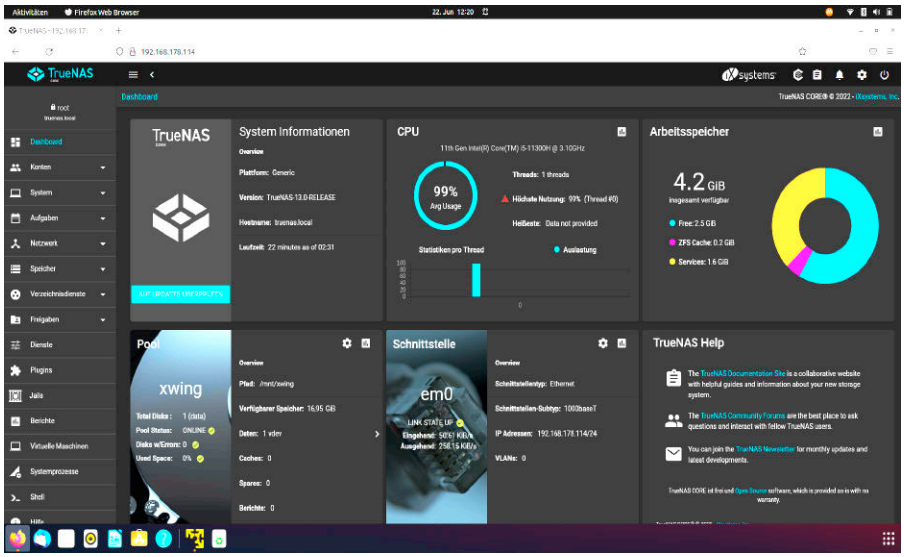
„External Sites“ – nicht zu verwechseln mit „External storage“ – ist eine unscheinbare Funktion, um URLs aus dem Intranet oder dem Internet in Nextcloud zu integrieren. Das ist ein netter Service für unbedarfte Nextcloud-Nutzer, die ihrem Browser keine Lesezeichen beibringen können. Die über „Einstellungen → Verwaltung → Externe Seiten“ erreichbare Funktion kann beliebige Adressen in das Benutzermenü aufnehmen (Position „Einstellungsmenü“). Als Symbol im „Kopfbereich“ (also quasi als App) ist nur für eine einzige externe Seite sinnvoll, weil das Symbol nicht beschriftet ist.

Zahlreiche winzige Apps bringen keine Serverfunktionen, erhöhen aber den Bedienkomfort. „Right Click“ ist selbsterklärend und vorinstallierter Standard. Das optionale „AppOrder“ kann die Reihenfolge der angezeigten Apps in der Symbolleiste oben nach Wunsch anpassen. Auch solche kleine Apps sind über „Einstellungen → Verwaltung“ (oder „Einstellungen → Persönlich“) zu konfigurieren. ■

Modernisiertes True NAS 13

Wer sich seinen Netzwerkspeicher selbst zusammenbaut, benötigt dafür ein Betriebssystem. Mit Open Media Vault und True NAS gibt es zwei ausgereifte Lösungen. Wir haben uns das neueste Release True NAS 13 genauer angesehen.

VON STEPHAN LAMPRECHT



Das ehemalige Free NAS wird von einem kommerziellen Unternehmen weiterentwickelt, das neben der kostenlosen Variante auch lizenzpflichtige Versionen vertreibt. Die aktuelle Version erhalten Sie als „True NAS Core“ auf der Website des Herstellers (*www.truenas.com/truenas-core/*). Dort wird die neueste Version 13 als ISO-Datei angeboten, mit der Sie den Rechner starten, der als NAS dienen soll.

Das Fazit vorab: True NAS 13 bringt keine revolutionären Neuerungen. Punktuelle Verbesserungen und Bootperformance machen die Version dennoch interessant – und die Vorgängerversion kann ein direktes Upgrade durchführen. Wer aber im Homeoffice lediglich seine Daten und Medien zentral speichern will, findet in Open Media Vault die zugänglichere und anspruchslosere Alternative.

Neuer Unterbau

Wer sich für den Aufbau eines eigenen NAS-Systems entscheidet, muss bedenken, dass er die Hardware wahrscheinlich schneller zusammenbaut, als das System zu konfigurieren. True NAS bietet sehr viele Möglichkeiten: Technisches Grundverständnis über Dateisysteme und Netzwerktechnik ist notwendig, um das System so einzurichten, damit es später genau das tut, was es soll.

Eine der wesentlichen Neuerungen bei True NAS 13 bleibt für die Nutzer weitgehend unsichtbar. Mit diesem Release wechselt das System auf Free BSD 13 als Unterbau. Dabei nutzen die Entwickler eine besonders kompakte Version, die eigentlich für sogenannte Embedded-Systeme gedacht ist. Der neue Motor soll insbesondere die Gesamtleistung von True NAS verbessern – und das tut er auch bereits beim Systemstart. Das können nur Nutzer beurteilen, die schon mit dem Vorgänger gearbeitet haben, aber das System startet in der Tat deutlich schneller.

Voraussetzungen und Installation

Das ISO-Image wird auf einen Datenträger kopiert und der Zielrechner damit gestartet. True NAS unterstützt Bios- wie Uefi-Rechner. Grundsätzlich läuft die Software aber ausschließlich mit 64-Bit-CPUs, was aber heute keine Einschränkung mehr darstellen sollte. Der Speicherbedarf ist im Unterschied zu Open Media Vault enorm, wofür in erster Linie das Dateisystem ZFS verantwortlich ist: Als Minimalvoraussetzung werden acht GB RAM genannt. Wenn mehrere Clients auf das System zugreifen, sollte besser mehr RAM zur Verfügung stehen. Und wie jedes NAS sollte Free NAS eine Ethernet-Schnittstelle mit Gigabit-Tempo vorfinden. Was Sie auf jeden Fall benötigen, sind zwei physische Datenträger – einen kleinen für das System, einen großen für die eigentlichen Daten.

Nach dem Systemstart vom Installationsmedium führt Sie die Software durch wenige Schritte, darunter die Auswahl des Zielmediums und die Vergabe des root-Passworts. Nach einem Neustart befinden Sie sich in einem Terminalfenster, das die IP-Adresse der Admin-Oberfläche anzeigt. Die weitere Konfiguration und Wartung von True NAS erfolgt über das Netzwerk im Browser.

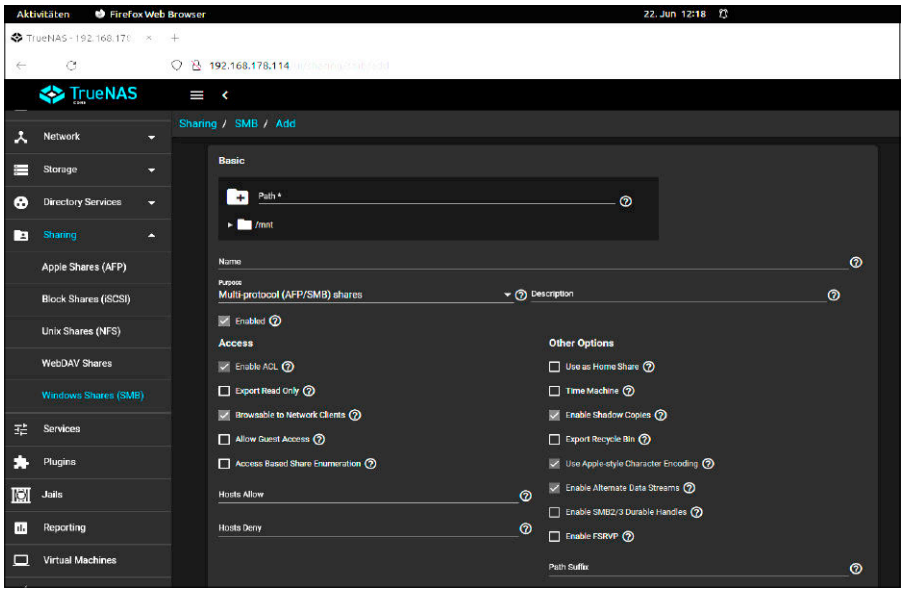
Dashboard, ZFS und Dienste

Falls Sie True NAS bereits kennen, müssen Sie schon recht genau hinsehen, um zu entdecken, was sich an der Oberfläche verändert hat. Zu den kleineren Verbesserungen zählt die farbige Darstellung der CPU-Temperatur. Generell wirkt alles etwa moderner und logischer. Neu ist ein Widget mit einer Hilfssektion, die via Links auf Dokumentation und Nutzerforen verweist. Nach einer Umstellung der Systemsprache auf Deutsch in den Einstellungen fällt die Arbeit umso leichter.

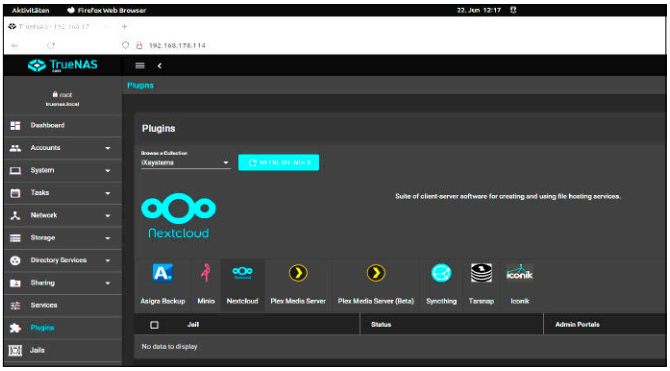
ZFS und Storage Pools: Intern arbeitet True NAS beim Aufbau und Verwaltung der Datenpools mit dem Dateisystem ZFS. Wer bereits ein NAS besitzt, muss etwas umdenken, denn ZFS nutzt „Storage Pools" für die Verwaltung des physikalischen Speicherplatzes. Der von anderen NAS-Systemen gewohnte Volumemanager entfällt, weil er hier nicht notwendig ist. ZFS wird als Filesystem für das Rechenzentrum bezeichnet, was den professionellen Anspruch von True NAS unterstützt. Trotzdem lässt True NAS auch Einsteiger nicht allein. Wer etwa versucht, eine Freigabe mittels AFP einzurichten, bekommt den Hinweis, dass Apple bereit seit einiger Zeit auch SMB unterstützt und favorisiert. Die Unterstützung der jungen Samba-Version 4.15 gehört ebenfalls zu den Neuerungen dieser Version.

Jails, Plug-ins und Dienste: Ein NAS übernimmt im Heimbüro und kleineren Unternehmen oft weitere Aufgaben, als nur Dateien zentral zur Verfügung zu stellen. Auch True NAS bietet diverse weitergehende Möglichkeiten. Datenaustausch und Integration von Cloudspeichern kann mittels Diensten und hinterlegten Anmeldeinformationen realisiert werden. Bei den unterstützten Services ist eigentlich alles dabei, was aktuell ist: Amazon S3, Backblaze, Google Cloud oder auch Microsoft Azure Blobs. Auch Google Drive, Dropbox oder Onedrive sind zugänglich.

Nach der Installation sind zunächst nur unbedingt notwendige Dienste aktiviert. Um Zugriff per FTP, Webdav oder SSH zu erhalten, sind die betreffenden Dienste erst zu starten. Um eine True NAS-Instanz etwa mit einem anderen Standort zu verbinden, steht Open VPN als Server wie als Client zur Verfügung. Mittels Rsync synchronisieren Sie Dateien mit anderen Geräten. Auch hier gibt es in der aktuellen Version eine Verbesserung. Denn Rsync kann auf Wunsch jetzt auch nur eine einzelne Datei auf Veränderungen überprüfen.



Nach der Zusammenstellung eines Speicherpools können Sie die Freigaben einrichten. Die Optionen sind zahlreich, aber gut erklärt.



True NAS kann mit einer Reihe von Plug-ins erweitert werden: Nextcloud, Syncthing und Plex dürften die interessantesten Kandidaten sein.

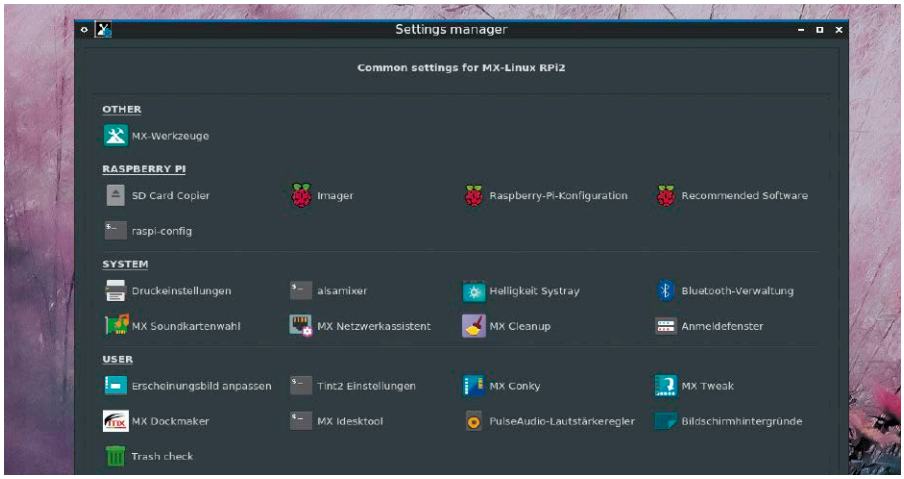
Zur Ausstattung gehört auch eine Reihe ausgewählter Plug-ins. Für Privatanwender dürften der Plex Media Server und Syncthing am interessanten sein. Auch eine Nextcloud lässt sich unkompliziert installieren. Installierte Plug-ins werden später in der Rubrik „Jails" geführt. Dabei handelt es sich um eine virtuelle Umgebung. Die Trennung der zusätzlichen Anwendungen von der Hardware trägt zur Stabilität des Systems bei, wie auch die Erfahrungen während des Tests zeigten: Während die Admin-Oberfläche von Nextcloud nicht mehr antwortete, zeigte sich das True NAS-System insgesamt völlig unbeeindruckt.

Virtualisierung: True NAS bietet zusätzlich die Option, eigene virtuelle Maschinen einzurichten. Eine großzügige Speicherausstattung und ein schneller Prozessor vorausgesetzt, installieren Sie sich so zusätzlich auf dem NAS etwa noch Ubuntu Server. Die Einrichtung der Virtualisierung ist leicht verständlich und folgt den von anderen Virtualisierern bekannten Schritten.

Konfiguration von Aufgaben: Eine Stärke von True NAS ist der vielseitige Bereich für wiederkehrende Aufgaben. Ob SMART-Test oder Synchronisation per Rsync – alles lässt sich über gut strukturierte Menüs einrichten und anpassen. Da bei der Synchronisation mit Cloudanbietern oder auch via Rsync schnell Daten überschrieben werden, sind die Erläuterungen zur Sync-Einrichtung umfangreich und deutlich formuliert. Die Einrichtung einer Synchronisation mit der Cloud könnte noch einfacher ausfallen, da im Aufgabenbereich kein direktes Anlegen der Zugangsdaten vorgesehen ist. Zunächst müssen also alle Zugangsdaten hinterlegt sein, bevor die Dialoge für die Arbeit an den Dateien ausgefüllt werden können. ■

Pfeilschnelles MX Linux für Raspberry Pi

Fluxbox ist ein Fenstermanager, der besonders sparsam mit Ressourcen umgeht. Mit MX Linux landet Fluxbox nun auch auf dem Raspberry Pi. Wir haben uns das Projekt „Ragout“ einmal genauer angesehen.



VON STEPHAN LAMPRECHT

Das Ziel des Fenstermanagers Fluxbox besteht darin, einen ansehnlichen Desktop mit vielen Einstellmöglichkeiten zu bieten, dabei aber extrem sparsam beim Ressourcenverbrauch zu sein. Und die sind bei Platinenrechnern wie dem Raspberry Pi bekanntlich immer knapp. Wie gut das funktioniert, haben wir auf den Raspberry-Modellen 3 und 4 ausprobiert.

Problemlose Installation

Die Installation läuft nach dem bewährten Muster: Auf der Projektseite (*https://mxlinux.org/blog/mx-linux_raspberry-pi-respin-ragout2-released/*) finden Sie den Link zum Download der Imagedatei: Herunterladen – Entpacken – auf eine SD-Karte kopieren, schließlich den Raspberry damit starten. Das System lief auf beiden Modellen ohne Probleme durch. Wenige Augenblicke nach dem Systemstart begrüßt Sie bereits der Desktop. Der hatte auf dem Raspberry Pi 3 zumindest nach dem ersten Start etwas Schluckauf und der erste Klick auf ein Desktopicon holte uns direkt wieder in eine Konsole. Nach einigen Fehlermeldungen kehrte der Raspberry 3 aber wieder zum grafischen Desktop zurück und zeigte danach keine weiteren Auffälligkeiten mehr.

Nach dem Start existiert auf dem System lediglich der Benutzer „pi“ mit dem gleichlautenden Passwort und das System nutzt das englischsprachige Tastaturlayout. Dies sind die zwei typischen Aufgaben, die gleich im ersten Schritt korrigiert werden sollten. Glücklicherweise ist der Schalter, der zu den Einstellungen führt, im Dock nicht zu übersehen. Der nachfolgende Dialog bietet sowohl Zugriff auf die Optionen von MX Linux als auch auf das bekannte raspi-config. Darüber können Sie schnell die Tastaturbelegung und die Sprache anpassen.

Für die Benutzerverwaltung gibt es mit den MX Tools ein sehr bequemes Programm, das die Einrichtung weiterer Benutzerkonten sehr sinnvoll strukturiert. Sehen Sie sich in den Einstellungen etwas genauer um.

Das Infotool Conky ist eine Bereicherung für einen Desktop und schreibt eine Reihe von Statistiken zur Auslastung von Ressourcen und andere Benachrichtigungen direkt auf die Arbeitsfläche. Der Desktop selbst sieht zwar etwas anders als gewohnt aus, aber Sie werden in Hinblick auf die Bedienung kaum Unterschiede zu anderen Projekten bemerken. Der Umstieg ist also keine Hürde und das System arbeitet auf dem Raspberry erstaunlich flott.

Solide Softwareausstattung

MX Linux für den Raspberry basiert auf Debian 10 (Buster), das an vielen Stellen an die Besonderheiten des Platinenrechners angepasst wurde. Das umfasst insbesondere die Nutzung eines offiziellen Raspberry-Displays. So können unter MX Linux Kontextmenüs durch längeres Drücken aufgerufen oder virtuelle Tastaturen verwendet werden.

Wie alle Distributionen setzt auch „Ragout“ auf eine Auswahl von Standardanwendungen. Als Browser wird in diesem Release Chromium verwendet, womit der Abschied von Firefox verbunden war. Voreingestellter Editor ist Featherpad, als Dateimanager nutzt das System Thunar und als Terminalemulator das XFCE4-Terminal. Außerdem sind zur Medienwiedergabe der VLC und für die Büroarbeit Libre Office an Bord. Lediglich ein E-Mail-Programm suchen Sie vergeblich. Softwaredefizite beheben Sie entweder im Terminal mit apt oder mit der grafischen Alternative Synaptic, die bereits vorinstalliert ist.

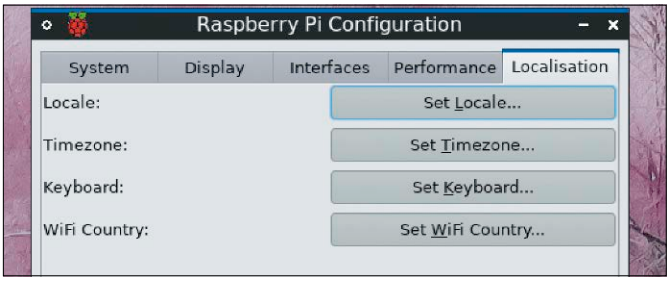
Tägliche Arbeit: Anders, aber nicht schlechter

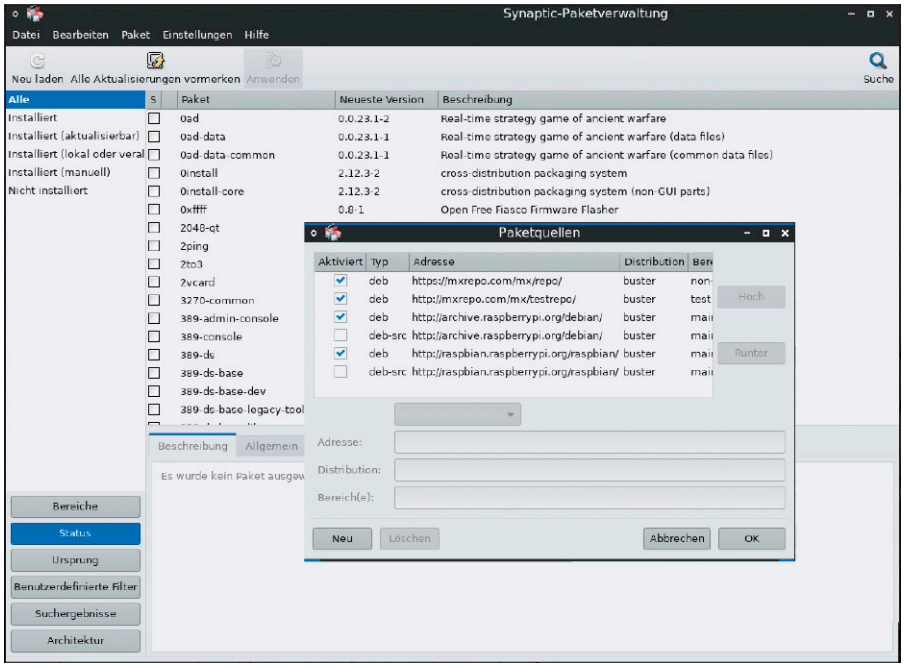
Wer bisher nur mit dem Desktop von Pi-OS gearbeitet hat, muss sich an manchen Stellen umgewöhnen, was Menüstrukturen betrifft. Das Arbeiten mit dem System fühlt sich etwas anders an, bedarf aber keiner völligen Umgewöhnung. Der Desktop reagiert stets flott auf die Eingaben.

Eine besondere Erwähnung verdienen auf jeden Fall die „MX-Tools“, die verschiedene Aufgaben rund um die Systemverwaltung kombinieren und ein echter Gewinn für das System sind. So kümmert sich „MX Cleanup“ um Dateireste und hilft beim Aufräumen der Festplatte. Ein Codec-Installer versorgt die Distribution mit den erforderlichen Umwandlern, um Medienformate wiederzugeben, obwohl mit VLC bereits ein Medienallrounder dabei ist. Den bereits erwähnten Benutzermanager würde man sich auch für manch andere Distribution wünschen, schließlich kümmert sich das Tool nicht nur um die Einrichtung und das Löschen von Benutzerkonten, sondern auf Wunsch auch um den Umzug von Home-Verzeichnissen. Das ist praktisch und zeitsparend.

Mit einem kleinen Zusatzprogramm hinterlegen Sie auf Wunsch eigene Tastenkürzel für die Nutzung der Arbeitsfläche oder passen die schon eingerichteten Hotkeys an eigene Wünsche an.

Nach dem ersten Start müssen Sie ein paar Dinge anpassen. Dazu gehören die Tastaturbelegung und die Änderung des Passworts für den Standardnutzer „pi“.





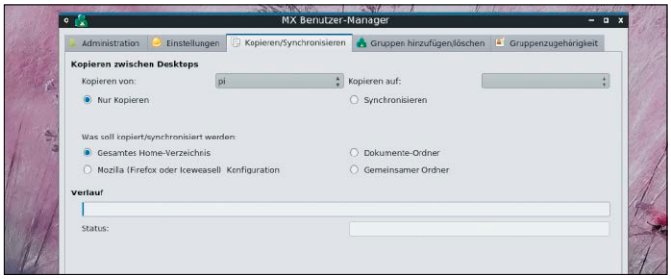
Die Grundausstattung an Software genügt typischen Ansprüchen an Office-Arbeiten und Medienwiedergabe. Mit Apt oder Synaptic ergänzen Sie den Umfang nach Wunsch.

Externe Geräte funktionieren problemlos

Desktop hin oder her: In der Praxis hat der Raspberry ja in aller Regel andere Aufgaben, als Office-Dokumente zu bearbeiten oder im Internet zu surfen. Deswegen musste sich das System auch einen Test mit aktuellen Erweiterungsboards gefallen lassen. Wir haben eine Reihe von HAT-Boards (Hardware attached on top) ausprobiert. Hier gab es keine weiteren Auffälligkeiten, lediglich bei einem etwas älteren Board des Herstellers Pimoroni musste einmal direkt durch Zugriff via raspi-config nachgeholfen werden. Was das offizielle Zubehör für den Raspberry betrifft, lässt sich festhalten, dass alles, was unter Pi-OS läuft, auch unter MX Linux funktionieren sollte.

Das trifft genauso auf den Anschluss externer Geräte zu. Externe Festplatten, zwei Drucker und ein Scanner ließen sich problemlos in Betrieb nehmen. Die verwendeten Modelle der Hersteller Brother und HP wurden allerdings auch mit Bedacht angeschafft, weil sie ein umfassendes Treiberangebot bieten, um unter Linux und Mac-OS zu funktionieren.

Zu den Systemtools gehört auch eine ordentliche Benutzerverwaltung. Die kann deutlich mehr als nur Passwörter zu verändern.



Eine für solche OS-Aufsätze typische Schwachstelle kann auch Ragout nicht vollständig lösen. Da die systemnahe Konfiguration in das Aufgabenfeld von raspi-config fällt, decken die Verwaltungstools der Arbeitsfläche nicht alle Aufgaben ab. Für Anwender mit geringer Erfahrung beginnt damit ein kleines Verwirrspiel, wo sich denn nun eine Eigenschaft des Systems verändern lässt. Aber hier sind den Entwicklern einfach die Hände gebunden.

Das Fazit

Der schnelle Fenstermanager Fluxbox gepaart mit einem aktuellen Debian-Unterbau machen auf dem Raspberry eine gute Figur. Das System läuft flott, bietet reichhaltige Softwareausstattung und zeigt sich kompatibel mit Erweiterungen und dem offiziellen Zubehör des Raspberry. Damit erhalten Sie eine funktionale und attraktive Alternative zum klassischen Pi-OS. ■

Umbrel: Server-Baukasten

Mit Umbrel ist zum Aufbau von Bitcoin-Nodes ein Serversystem gereift, das Dienste in Docker-Container kapselt, die in einem App Store bereitstehen. Der Bitcoin-Part ist inzwischen in den Hintergrund getreten und der Server-Baukasten universeller.

VON DAVID WOLSKI

Die Zutaten, die einen typischen Webserver ausmachen, sind überschaubar: Linux, Webserver, Datenbank, PHP oder eine andere Scripting-Schnittstelle wie Python, Node.js, Java, oder Go. Diese Rezeptur hat Linux als Server-Betriebssystem etabliert, zumal Linux-Server alle Komponenten unter einem Dach unterbringen und viele Rollen gleichzeitig erfüllen können. Aber die Aufgabe wird anspruchsvoll in der Administration, wenn ein einziger Server viele unterschiedliche Dienste anbieten soll, die eigene Komponenten und bestimmte PHP-Versionen und Datenbanken verlangen. Denn diese dürfen sich nicht in die Quere kommen, nicht die gleichen Ports belegen und nicht auf gleiche Konfigurationsdateien zugreifen. Mit der strikten Trennung von Einzeldiensten wie PHP und Datenbanken steigt der Aufwand der Serverpflege. Die Virtualisierung von Betriebssystemen unter einem Hypervisor wie Vmware hat dieses Problem entschärft: Virtuelle Maschinen sind wie physische Systeme voneinander getrennt. Eine ebenso effiziente Lösung im Linux-Umfeld ist die Container-Runtime Docker, die auch im hier vorgestellten Umbrel (*https://umbrel.com*) arbeitet und die Einstiegshürden signifikant senkt.

Docker-Container: Einstieg mit Umbrel

Docker sperrt Serverumgebungen ohne Systemvirtualisierung in Container ein, die auf jedem modernen Linux-System unter der Docker-Runtime laufen. Statt einem kompletten Betriebssystem virtualisiert Docker nur Teile davon und ein aufwendiger Hypervisor entfällt. Der Clou ist, dass Docker geschickt die Fähigkeiten des Kernels verwendet, um isolierte Container für Programme bereitzustellen: Control Groups (cgroups) limitieren Speicher, CPU-Zyklen, I/O-Leistung für einen Prozess und Kernel-Namespaces isolieren Prozesse strikt voneinander. Die Arbeit mit Docker verlangt aber Lust am Experimentieren und etwas Geduld, sich in Containertechniken einzuarbeiten.

Umbrel nutzt die Docker-Technik, macht es aber einfacher, viele Dienste ohne Konflikte auf einem einzigen Linux-System auszuführen. Dabei versteckt Umbrel die Docker-Runtime und ihre Tools hinter Menüs im Webbrowser, um populäre Dienste wie Nextcloud, Pi-Hole und Bitcoin-Tools im Stil eines App Stores anzubieten. Umbrel steht unter einer Open-Source-Lizenz und die angebotenen Docker-Container liefern ebenfalls bekannte Open-Source-Lösungen für Server. Nextcloud, Matrix, Pi-Hole, Crypto-Wallets, Bitcoin- und Lightning-Nodes sind im Nu installiert und einsatzbereit. Der Preis dafür ist ein geringeres Maß an Anpassungsfähigkeit: Während beispielsweise ein selbst aufgesetzter Nextcloud-Server enormes Optimierungspotenzial hat, um die Leistung mittels Datenbankeinstellungen, Caching und PHP-Feintuning zu verbessern, ist eine Nextcloud in Umbrel eher eine Instantpackung.

Eigene Zutaten und Modifikationen am Programmcode sind hier nicht vorgesehen. Dafür gibt es Updates für die Serverbausteine aus dem App Store der Umbrel-Entwickler. Dieser Service erinnert an die per Klick hinzubuchbaren Servermodule auf Cloudplattformen wie AWS, Azure, Digital Ocean und Linode. Umbrel ist dabei aber frei, quelloffen und kostenlos – die Firma

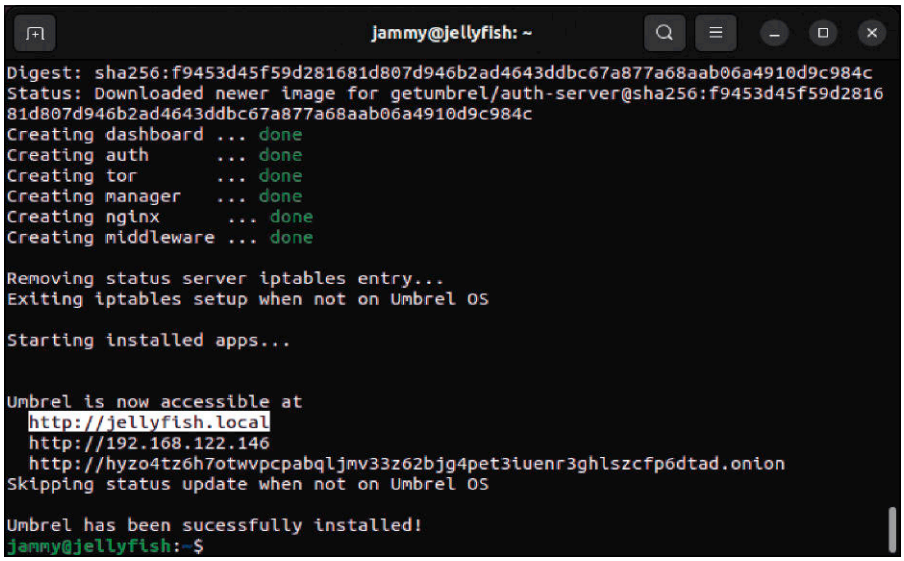
dahinter finanziert sich über Dienstleistungen für Bitcoin-Schwergewichte und deren Nodes sowie über Venturekapital. Allerdings gibt es mit der Version 0.5 eine neue Lizenz (Polyform Noncommercial 1.0), die im Stil der Creative Commons einen Weiterverkauf eines vorinstallierten Umbrel-Servers oder die Vermietung auf Cloudplattformen ausschließt. Zielgruppe von Umbrel sind Anwender sowie Linux-Admins, die den Schnelleinsteig in eine neue Materie suchen und die Dienste auf einem Server zu Hause hosten wollen.

Voraussetzungen und Installation

Umbrel liegt mit Version 0.5 in zwei Formen vor: Es gibt ein Image für den Raspberry Pi 4, das zur ersten Einrichtung auf eine Micro-SD-Karte kommt und nach dem ersten Boot die weitere Einrichtung übernimmt. Die zweite, jüngere Variante ist ein Aufsatz für ein bereits vorhandenes Debian- oder Ubuntu-System auf herkömmlicher PC-Hardware. Um diese Einrichtung kümmert sich dann ein Installations-Script, das alle weiteren Teile wie Docker-Runtime, Docker-Compose und eine GUI für die Verwaltung im Webbrowser aus den Umbrel-Quellen herunterlädt. Dieser Weg ist auch in einer virtuellen Maschine praktikabel, in welcher schon ein aktuelles Debian/Ubuntu läuft.

In jedem Fall ist es wichtig, die Hardware- und dabei speziell die Datenträgervoraussetzungen von Umbrel im Auge zu behalten. Docker-Container verlangen deutlich mehr Platz als traditionelle Serverdienste – aufgrund der abgekapselten eigenen Bibliotheken und Komponenten in Docker-Images. Dazu kommt noch eine erhebliche Datenmenge, falls Umbrel einen Lightning-Node und Bitcoin-Tools aufsetzen soll. Denn diese verlangen eine lokale Kopie der Bitcoin-Blockchain mit rund 700 GB. Und auch ohne diese Dienste fordern Dateiserver wie Nextcloud oder die Fotoverwaltung Photoprism Platz für ihre Daten.

Platzbedarf: Auf einem vorhandenen Debian/Ubuntu ohne Bitcoin-Tools sind 50 GB ein Minimum an verfügbarem Platz für Umbrel und Docker-Dienste, ohne dabei die im Betrieb gespeicherten Dateien in Betracht zu ziehen. Auf einem Raspberry Pi 4 verlangt Umbrel deshalb ein anderes Setup, um nicht alles auf einer Micro-SD-Karte speichern zu müssen: Für das Basissystem genügt eine SD-Karte mit 16 GB aufwärts. Zusätzlich verlangt Umbrel nach einer entsprechend großen SSD oder schnellen HDD mit eigener Stromversorgung am USB-3-Port der Platine. Wer ernsthaft einen Lightning-Node für Bitcoin-Transaktionen betreiben will, kommt an einer SSD mit einem TB Speicherplatz nicht vorbei, für alle anderen Umbrel-Serverdienste tut es auch ein kleinerer Datenträger.



Abschluss des Installations-Scripts auf einem Ubuntu-System: Umbrel ist nicht mehr nur für einen Raspberry Pi 4 geeignet, sondern per Script auch in Debian/Ubuntu zu installieren.

RAM: Egal ob auf einem Raspberry Pi, in einer VM oder einem vorhandenen Debian/Ubuntu, sind vier GB Arbeitsspeicher das Minimum für Umbrel plus einige laufende Serverdienste.

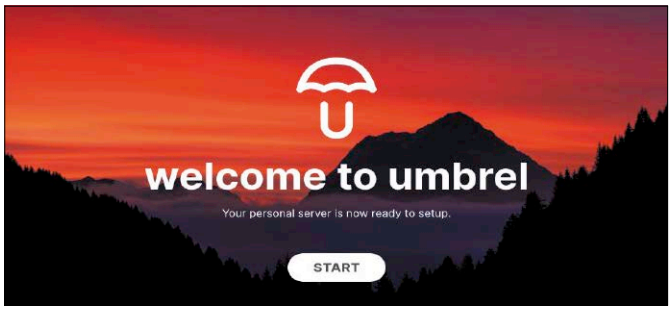
CPU: Einige Serverdienste und Bitcoin-Tools erzeugen eine anhaltend hohe Prozessorlast, auf dem Raspberry Pi 4 auch mal über Stunden. Wichtig ist also bei dieser Platine eine gute aktive Kühlung. Auf einem Raspberry Pi 4 ohne Lüfter besteht die Gefahr von Instabilität im Betrieb.

Die Installation auf einem Raspberry Pi beginnt mit dem Download der gezippten

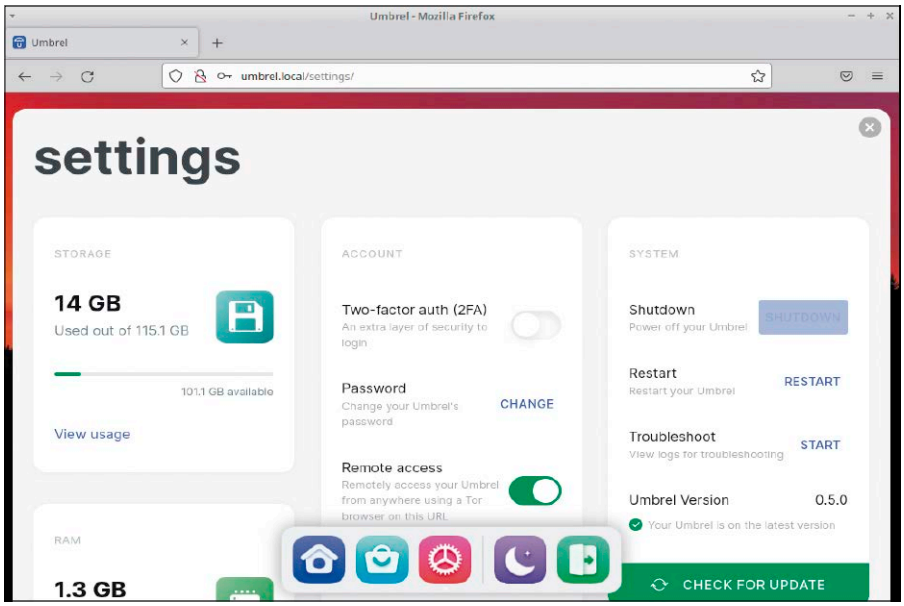
UMBREL: DER WEG ZUM UNIVERSELLEN SERVER

Die Idee zu Umbrel entstand 2019, um mit ein paar Docker-Rezepten einen Lightning-Node für schnelle Bitcoin-Transaktionen auf einem Raspberry Pi aufzusetzen. Seine Herkunft als Server für selbst gehostete Cryptotools kann Umbrel nicht verheimlichen, denn im hauseigenen App Store sind weiterhin viele dieser Dienste vertreten. Auch der Erfolg und die finanzielle Unterstützung dieses Open-Source-Projekts sind maßgeblich in der Cryptoszene verankert, selbst wenn die Lobeshymen zu Cryptowährungen aktuell wieder leiser werden.

Mit der aktuellen Version 0.5 ist Umbrel rechtzeitig der Schritt zum universellen Server für ausgewählte Docker-Dienste gelungen. Die Cryptotools und die umfangreichen Blockchain-Daten von rund 700 GB sind nicht mehr Teil des vorinstallierten Pakets, sondern liegen jetzt optional im App Store. Der Raspberry Pi ist auch nicht mehr die alleinige Zielplattform von Umbrel, zumal die Platine auch nicht die Leistung hat, mehrere anspruchsvolle Serverdienste gleichzeitig auszuführen. Die Installation ist nun per Script auch auf einem Debian und Ubuntu möglich (x86-Hardware und ARM). Für eine Installation auf Cloudinstanzen oder einem Server im Internet ist Umbrel aber nicht gemacht. Die Entwickler weisen darauf hin, dass Umbrel hinsichtlich seiner Systemsicherheit noch in der Betaphase ist, und haben die noch offenen Punkte transparent unter *https://github.com/getumbrel/umbrel/blob/master/SECURITY.md* aufgelistet. Als Einsatzbereich bleibt es also vorerst beim LAN hinter einem Router und damit in einer vertrauenswürdigen Umgebung.



Administration per Webbrowser: Die Besonderheit von Umbrel ist die Server- und Docker-Abstraktionsschicht über eine Weboberfläche. Hier geht es zur Einrichtung des Admin-Kontos.



Blick in die Einstellungen: Umbrel tritt mit dem Anspruch an, allein über die Weboberfläche administrierbar zu sein.

Imagedatei von *https://umbrel.com/#start* (980 MB). Nach dem Entpacken der ZIP-Datei liegt die IMG-Datei „umbrel-os-v0.5.0.img“ vor, die mit Balena Etcher (Download unter *www.balena.io/etcher* für Linux, Windows, Mac-OS, 91 MB) oder dem Raspberry Pi Imager (*www.raspberrypi.com/news/raspberry-pi-imager-imaging-utility*) auf die Micro-SD-Karte übertragen wird. Die weitere Installation von Umbrel verlangt noch vor dem Einschalten die Verbindung mit dem externen Laufwerk per USB-Port. Achtung, dieser Datenträger wird von Umbrel komplett überschrieben, denn die Installation startet nach dem Boot der Platine automatisch. Nach zehn Minuten ist die Weboberfläche von Umbrel dann in einem Browser im LAN erreichbar – über die Adresse *http://umbrel.local* oder über die IP-Adresse des Raspberry Pi. Wie bei jedem Server sollte die Hardware für Umbrel mit einer gleichbleibenden IP-Adresse arbeiten, um Dienste und die Weboberfläche zuverlässig aufrufen zu können. Die feste IP kann im Router festgelegt werden.

Anders verläuft eine Installation unter Debian/Ubuntu ab, denn diese erledigt ein vorbereitetes Bash-Script der Entwickler, welches im Terminal mittels

```
curl -L https://umbrel.sh | bash
```

heruntergeladen und ausgeführt wird. Das Downloadtool curl muss vorhanden sein, alles Weitere erledigt das Script automatisch. Der Vorgang dauert bei flotter DSL-Verbindung etwa fünf Minuten. Abschließend zeigt das Script im Terminal die Adressen an, um den neuen Server zu erreichen – mit Hostname oder IP-Adresse im LAN sowie einer Onion-Adresse über das TOR-Netzwerk, für das ein Client automatisch mitinstalliert wird. Bei einem Aufruf einer dieser Adressen im Browser erfolgt dann die Einrichtung des Benutzerkontos, das in Zukunft das Admin-Konto für Umbrel wird.

Dienste: Apps auswählen und installieren

Anfangs bringt Umbrel außer dem Webserver für die englischsprachige Administrationsoberfläche und einen Client zur Teilnahme am TOR-Netzwerk keine Serverdienste mit. Die Weboberfläche im Stil eines Smartphones präsentiert eine noch leere Übersicht der installierten Dienste und bietet ein Dock mit einem Link in den App Store an, über welchen derzeit 55 Dienste installierbar sind (Stand Juli 2022). Die Dienste sind auf Github (*https://github.com/getumbrel/umbrel-apps*) hinterlegt und im App Store in Rubriken aufgeteilt, wobei die Themenbereiche um Bitcoin und das Lightning-Netzwerk weiterhin dominieren. Eine Installation erfolgt per Klick auf einen Eintrag, der zu einer Unterseite mit einer Vorstellung, Links zur Projektwebseite und zur Dokumentation führt. Die Schaltfläche „Install“ richtet den Dienst ein und der Button „Open“ öffnet direkt in der gleichen Browserinstanz die Weboberfläche des Serverprozesses zur weiteren Konfiguration. Über den App Store ist ein Dienst auch flott wieder deinstalliert.

Einige der verfügbaren Docker-Container für Lightning bauen aufeinander auf und tauschen untereinander Daten aus, beispielsweise zur Analyse der Bitcoin-Blockchain. Der App Store warnt, falls ein noch von anderen Containern benötigter Dienst zur Deinstallation markiert wird, damit das System in keinen inkonsistenten Zustand gerät. Am unteren Rand gibt es im Dock noch eine Seite mit Einstellungen über das Zahnrad-Symbol. Hier findet sich eine Übersicht, wie viel Platz auf dem Datenträger für Umbrel noch verfügbar und wie viel RAM aktuell frei ist. Es finden sich Schaltflächen zum Herunterfahren und zum Neustart des Systems sowie der Punkt „Troubleshoot“, der Logdateien von Umbrel und des Linux-Kernels anzeigt. Zur Verwaltung des Admin-Zugangs gibt es einen Punkt zur Passwortänderung und zur Einrichtung einer Zwei-Faktor-Authentifizierung. Außerdem zeigt das Feld „Remote Access“ die Onlineadresse für das TOR-Netzwerk zum Fernzugriff über einen TOR-Browser an. Diese Zugangsart eignet sich zur Fernwartung, ist aber wegen der eingeschränkten Geschwindigkeit des TOR-Netzwerks kaum für Dateiübertragungen zu gebrauchen.

Im LAN: Dateiserver und Werbefilter

Wer nichts mit Cryptowährung und Bitcoin am Hut hat, bekommt im App Store einige Serverdienste für das LAN geboten, die hier besonders flott installiert sind. Als Dateiab-

lage ist die Nextcloud in Version 22 verfügbar. Umbrel stellt die Nextcloud samt PHP und Datenbank über Docker bereit. Speziell für das Teilen und Organisieren von Fotos ist die Serveranwendung Photoprism gemacht (siehe *https://photoprism.app*), die ebenfalls mit wenigen Klicks in Umbrel installiert ist. Die Besonderheit sind Hilfen wie eine Gesichtserkennung über KI, eine automatische Kategorisierung per Motiverkennung und eine Weboberfläche, die auch auf Smartphones gut aussieht.

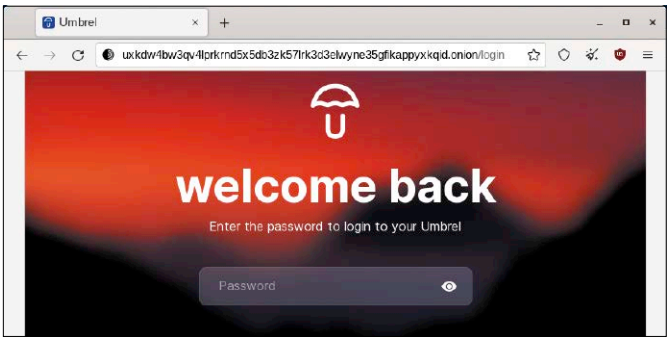
Ein Werbefilter für das lokale Netzwerk ist die Serverkomponente Pi-Hole, die Internetadressen von Werbe- und Trackingservern über einen eigenen DNS-Server blockiert. Die Listen dieser Adressen werden regelmäßig aktualisiert. Über die IP-Adresse des Umbrel-Servers kann Pi-Hole als vorgeschalteter DNS-Server zentral im Router festgelegt werden. Es ist dann nicht nötig, die neue DNS-Adresse allen Clients im Netzwerk bekannt zu machen. Die Fritzbox bietet diese Konfiguration unter „Internet → Zugangsdaten → DNS-Server".

Crypto: Bitcoin- und Lightning-Nodes

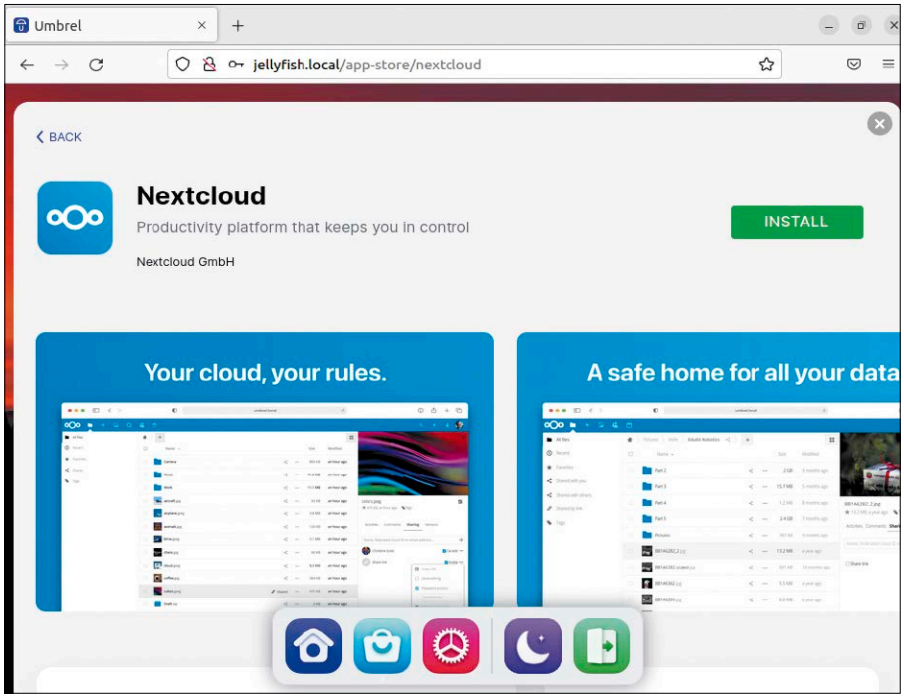
Dieser Beitrag betrachtet Umbrel als universellen Homeserver im LAN. Die speziellen Dienste zur Teilnahme am Lightning-Netzwerk und für die Verwendung von Bitcoin-Werkzeugen sollen aber nicht unter den Tisch fallen, denn dies ist die ursprüngliche Paraderolle von Umbrel.

Lightning-Netzwerk: Dies ist ein alternativer Zahlungskanal, der auf dem Bitcoin-Netzwerk aufbaut, aber nicht jede Transaktion in der Blockchain speichern muss. Dies beschleunigt Zahlungsvorgänge, spart Zeit und schließlich auch Energie, denn zwei Nodes im Lightning-Netzwerk können sich Bitcoin-Zahlungen senden oder diese sogar für andere Parteien weiterleiten. Erst wenn ein Zahlungskanal geschlossen wird, muss der Saldo als letzte Transaktion zurück in die Blockchain übertragen werden. Lightning ist besonders für kleinere Zahlungen populär und entlastet das Bitcoin-Netzwerk. Über Umbrel sind ein selbst gehosteter Lightning-Node und weitere darauf aufbauende Tools wie ein Chat und Analysewerkzeuge ohne hohen Aufwand einzurichten.

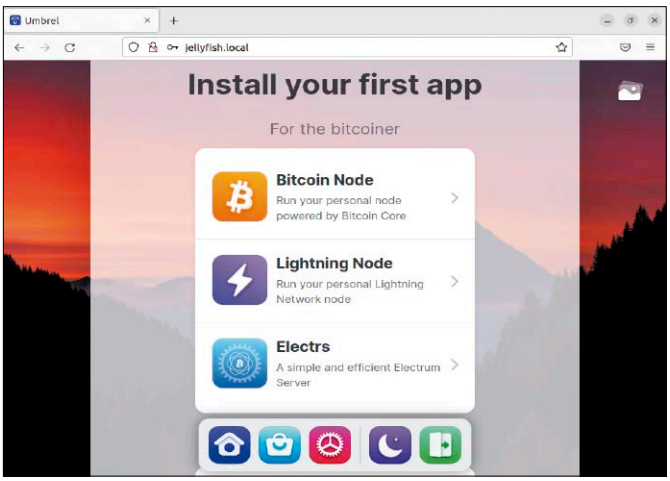
Bitcoin-Nodes: Umbrel entstand ursprünglich, weil sich der Hauptentwickler mit einem eigenen Node von Bitcoin-Dienstleistern unabhängig machen wollte. Im App Store sind weiterhin diverse Bitcoin-Wallets verfügbar, die sich direkt mit einem eigenen Bitcoin-Node verbinden lassen. Ein Terabyte an Festplattenplatz sollte dann aber für Umbrel verfügbar sein, da eine lokale Kopie der gesamten Blockchain vorliegen muss. ■



Zugriff von außen: Umbrel richtet automatisch einen TOR-Client ein, um über eine Onlineadresse aus der Ferne erreichbar zu sein. Dies gelingt über einen TOR-Browser wie hier in Tails.



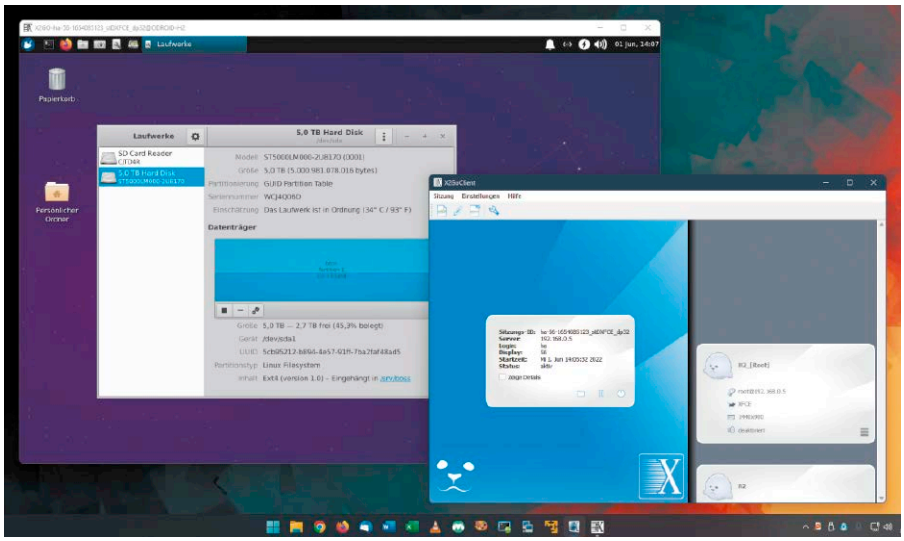
Schneller Start mit Nextcloud: Über Docker richtet Umbrel mit wenigen Klicks einen Webserver, PHP, Datenbank und Nextcloud als Container ein. Dies ist einer der Vorzüge dieses Systems.



Wurzeln des Projekts: Anfangs fokussierte sich Umbrel auf Bitcoin- und Lightning-Netzwerke. Diese Komponenten sind heute im App Store optionale Angebote neben anderen.

Remotedesktop mit X2go

Dieser Beitrag ist in erster Linie eine Empfehlung, weniger ein technischer Ratgeber. Die Benutzung des hier empfohlenen Remote-Tools X2go ist nämlich auch für Einsteiger keine Herausforderung.



Ein Windows, ein Remoteserver und dazwischen X2go: Dieses Remotedesktop-Tool ist wackeligen und hakeligen VNC-Lösungen eindeutig vorzuziehen.

VON HERMANN APFELBÖCK

Fernwartung im SSH-Terminal ist zuverlässig, schnell, sicher. Wer nicht alle Belange etwa der Datenträger- oder Benutzerverwaltung im Terminal souverän beherrscht, wird dennoch Remotedesktop-Tools begrüßen, die einen freundlicheren Zugang zum entfernten Rechner im Netzwerk ermöglichen. Der Fernzugriff mit dem bekannten VNC-Protokoll (Virtual Network Computing) auf den grafischen Linux-Desktop ist jedoch von der Solidität der SSH-Fernwartung weit entfernt.

Einschlägige VNC-Server gibt es eine ganze Reihe wie Vino-Server, x11vnc, Tight VNC, Kfrb, Real VNC. Die Erfahrungen damit sind aber durchwachsen. Zum Teil erfordert die Serverkonfiguration das Studium von 50 Aufrufparametern, im andern Fall funktioniert die Verbindung bei einem Linux-System bestens und mit dem zweiten nie, im nächsten Fall läuft der Arbeitsspeicher voll bis zur Systemgrätsche, sobald der VNC-Remoteserver gestartet ist. Ein ganz aktueller Problemfall des offenbar dauerhaft fragilen Remotedesktops ist Ubuntu 22.04 mit Gnome, das explizit für Windows-Clients neuerdings das Windows-Protokoll RDP verwendet, aber derzeit keinen Zugriff von Windows-Rechnern zulässt.

Nun kann man sich auf den Standpunkt stellen, dass Windows-Clients auf Linux-Systemen eh nichts verloren haben. In der Tat: Bliebe Linux unter sich, wäre manches Problem hinfällig. Aber solche Linux-Monokultur entspricht nicht der Realität.

Es sind ja vorwiegend Windows-Systeme und Windows-Nutzer, die einen soliden Zugriff auf den grafischen Linux-Desktop wünschen. Für Linux-Systeme unter sich ist SSH mit schnellem X11-Forwarding einzelner grafischer Programme meistens völlig ausreichend.

Desktopzugriff mit X2go

Die Open-Source-Software X2go (*https://wiki.x2go.org*) ermöglicht den Fernzugriff auf den Desktop eines anderen Linux-Systems. Die Serverkomponente lässt sich nur unter Linux installieren, Zugriffsclients gibt es hingegen außer für Linux auch für Windows und Mac-OS.

Nehmen wir es vorweg: X2go ist nicht mit jedem Linux-Desktop kompatibel. Außerdem ist das Remotetool verglichen mit VNC-Lösungen oder gar SSH ein eher schwerer Brocken sowohl bei der Server- wie bei der Clientkomponente. Der Aufbau der entfernten grafischen Oberfläche ist immer etwas zäh, wie später noch technisch begründet wird. Alle diese Einschränkungen nimmt man aber bereitwillig in Kauf: Denn X2go funktioniert einfach – mit doppelter Betonung auf „funktioniert“ und auf „einfach“:

- Da X2go intern auf SSH aufbaut, muss man sich keine zusätzliche Zugangsverwaltung aneignen. Zugriff haben wie bei SSH alle Systemkonten. Auf dem „Server“ muss neben X2go nur der Open-SSH-Server laufen, so wie es sich für Linux-Server sowieso gehört.
- Sobald X2go die entfernte Oberfläche angeboten hat, erfolgt die Bedienung jederzeit mit alltagstauglicher Geschwindigkeit.
- Der Remotedesktop ist ungeachtet der in der X2go-Konfiguration angegebenen Auflösung später beliebig skalierbar.
- X2go kümmert sich um Maus, Tastatur und Soundausgabe auf dem Client, erlaubt Druckaufträge und bietet einen Weg zum direkten Datenaustausch mit dem lokalen System.

Kompatible Desktops und Installation

Obwohl die X2go-Clientkomponente so gut wie alle Linux-Desktops in seiner Konfiguration anbietet, gelten derzeit nur XFCE, LXDE, Mate und Openbox als vollständig

kompatibel. Hardwarebeschleunigte Oberflächen wie Gnome, Cinnamon, Budgie sind ungeeignet, auch aktuelles KDE und LXQT sind aufgrund ihrer Qt5-Grafikbibliotheken inkompatibel. Bevorzugter Remotedesktop für X2go ist XFCE. Wer ganz sicher gehen will, kann dort den Effektkompositor deaktivieren („Einstellungen → Feineinstellungen der Fensterverwaltung → Anzeigenkomposit", ähnlich auch unter Mate) – dies ein Rat der Entwickler, der aber nach unserer Erfahrung meistens unnötig ist.

Die Einschränkung auf die genannten Linux-Desktops und das bevorzuge XFCE klingt limitierend, ist im Hinblick auf die zu verwaltenden Systeme aber tolerabel. In erster Linie geht es ja um Headless-Server und Ein-Platinen-Rechner, die überwiegend per SSH und gelegentlich per X2go besucht werden. Für solche Systeme sind XFCE oder LXDE genau die geeigneten Oberflächen. Liegt ein anderer Desktop vor, kann XFCE natürlich nachgerüstet werden:

```
sudo apt install xubuntu-desktop
```

Natürlich ist es eine Ermessensfrage, ob der Einsatz von X2go diese Maßnahme rechtfertigt. Beachten Sie aber die technische Eigenheit von X2go, nicht etwa den laufenden Desktop des Servers abzugreifen, sondern eine eigene Sitzung zu erstellen. Dies erklärt den relativ zähen Start der Remotesitzung, hat aber den Vorteil, dass diese Desktopumgebung auf dem Server nur vorhanden sein, aber nicht unbedingt als Standardoberfläche laufen muss.

Die X2go-Serverkomponente muss auf dem „Server"-System installiert werden. Sie ist mittlerweile in den meisten Repositorys direkt erhältlich, daher genügt zur Installation folgender Befehl:

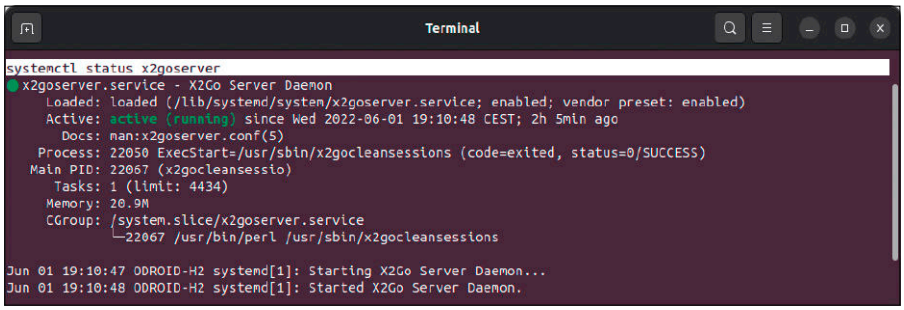
```
sudo apt install x2goserver
  x2goserver-xsession
```

Wer unter Ubuntu & Co. die neueste Version nutzen will, kann das Servertool auch aus seinem PPA beziehen:

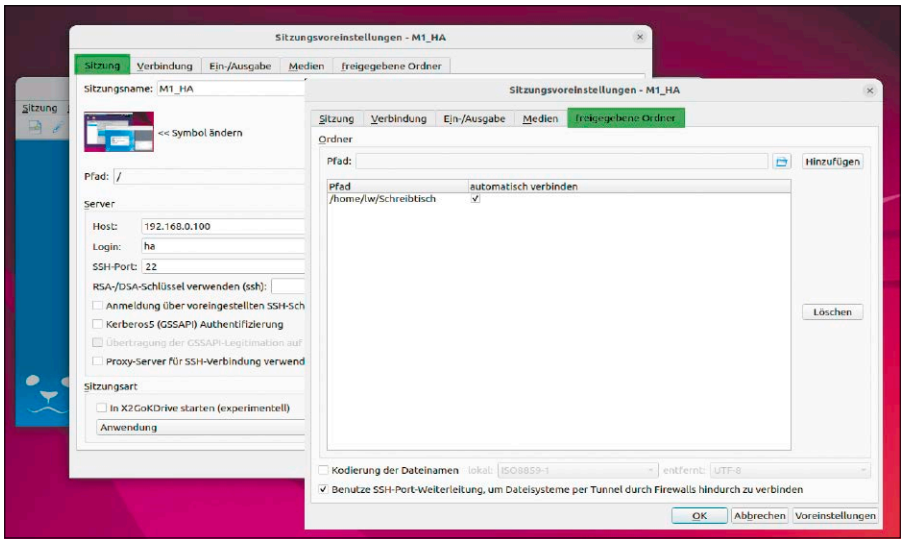
```
sudo add-apt-repository ppa:x2go/
  stable
sudo apt update
sudo apt install x2goserver
  x2goserver-xsession
```

Der Server wird dabei automatisch und dauerhaft als Systemdienst „x2goserver" eingerichtet.

Die X2go-Clientkomponente installieren Sie dann auf allen Systemen, die auf den Server zugreifen sollen. Unter Debian/Ubuntu kann dies mit



Dienst am Serversystem: Die Installation der X2go-Serverkomponente etabliert automatisch einen permanent laufenden Systemdienst.



X2go-Konfiguration im Client: Diese Aufgabe ist keine Herausforderung, da nur unter „Sitzung" eine IP-Adresse und ein Systemkonto notwendig sind. Alle anderen Registerkarten sind freundliches Beiwerk.

```
sudo apt install x2goclient
```

aus den Standardquellen erfolgen. Clientsoftware für Windows- und Mac-Systeme gibt es auf *https://wiki.x2go.org* unter „Download" (mswin, OS X).

Verbindungen herstellen

Ähnlich bekannten SSH- oder VNC-Tools speichert der X2go-Client die einmal eingestellte Konfiguration eines Servers, sodass später der Doppelklick auf den Eintrag genügt. Natürlich sind mehrere Servereinträge möglich, aktiv genutzt werden kann aber nur jeweils einer.

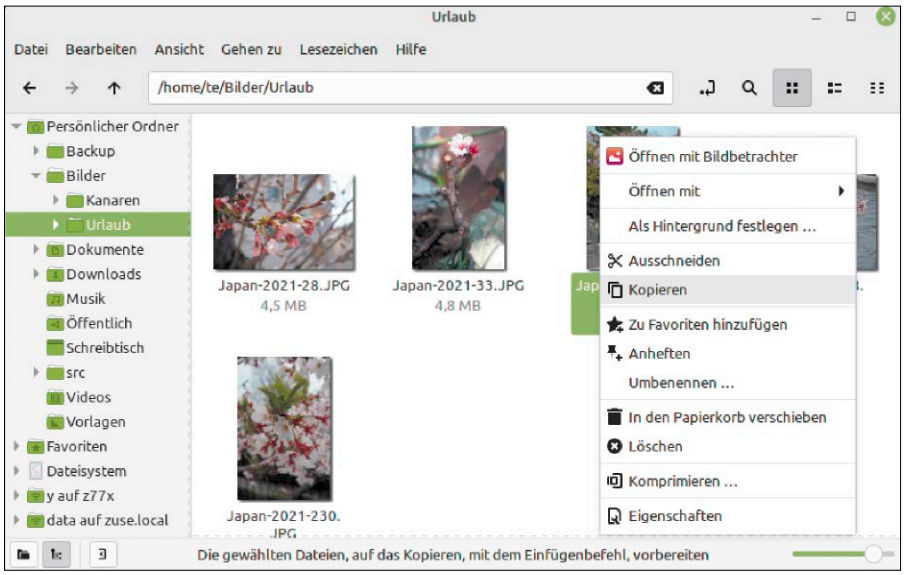
Starten Sie den Client. Mit „Sitzung → Neue Sitzung" legen Sie den ersten Server an. Vergeben Sie hinter „Sitzungsname" eine Bezeichnung, die den Rechner klar identifiziert – etwa „Raspberry4". Neben „Host:" tragen Sie die IP-Adresse des Servers ein. Wie immer in solchen Fällen sollte die IP-Adresse statisch feststehen (was Sie bei Bedarf im Heimrouter festlegen). Hinter „Login" geben Sie das Systemkonto am Serversystem ein und neben „SSH-Port" die Portnummer, falls sie vom Standard „22" abweicht. Unter „Sitzungsart" wählen Sie idealerweise „XFCE" – sofern zutreffend. Alle weiteren Optionen sind nicht zwingend, können aber als nützliche Vorgaben für Auflösung, Soundausgabe und passwortlose Anmeldung den Komfort erhöhen. Unter „Freigegebene Ordner" lassen sich Verzeichnisse des Clientrechners eintragen, die dann gleich am Desktop des Remotesystems erscheinen, wenn die Option „automatisch verbinden" gewählt wird. Am Ende klicken Sie auf „OK", um die Einstellungen zu speichern.

Der Server ist nun rechts eingetragen und nach Klick auf den Eintrag müssen Sie nur noch das Systemkennwort eingeben und sich mit „OK" verbinden. Die sauberste Methode, eine Remotesitzung wieder zu beenden, ist nicht der „Beenden"-Knopf im X2go-Client, sondern eine Abmeldung im Remotefenster – also über dessen Hauptmenü oder das Sitzungsmenü. ■

Dateien und Ordner organisieren

Der Umgang mit Dateien und Ordnern gehört zum PC-Alltag. Die Linux-Dateimanager sind den meisten Aufgaben gewachsen, mit ein paar Tricks und zusätzlichen Werkzeugen lässt sich jedoch einiges optimieren.

VON THORSTEN EGGELING



Für die meisten Benutzer ausreichend: Ein Dateimanager wie Nemo (Linux Mint) ist das komfortabelste Tool, wenn es darum geht, Dateien zu kopieren oder umzubenennen.

Für Backups müssen Dateien oder Ordner kopiert, für eine Neuorganisation verschoben oder je nach Inhalt sinnvoll umbenannt werden. Im Dateimanager lässt sich das komfortabel erledigen, entweder über Menüpunkte oder Tastenkombinationen. Wer gerne mit der Maus arbeitet, kann auch Drag & Drop verwenden. Man spart einiges an Mühe und findet Dateien schneller wieder, wenn man sich ein sinnvolles Ablagesystem überlegt. Wie stellen Tools vor, die Sie dabei unterstützen. Das Meiste kann man jedoch mit Bordmitteln bewältigen, entweder im Dateimanager oder im Terminal.

Elemente im Dateisystem

Das Dateisystem orientiert sich an Arbeitsweisen, die schon vor Einführung des Computers galten. In jedem gut organisierten Haushalt oder Büro stehen Aktenhefter, in denen man Dokumente ablegt. Dem entsprechen auf dem PC Ordner und Dateien. Die deutschsprachigen Bezeichnungen „Datei“ und „Verzeichnis“ beschreiben den Gegenstand nur ungenau, weil diese ursprünglich eher für eine Sammlung zusammengehöriger Daten beziehungsweise Inventarlisten verwendet wurden.

Deswegen ist es passender, zunächst nur von Elementen im Dateisystem zu sprechen, von denen es zwei gibt. Das eine heißt „Verzeichnis“ (Synonym: „Ordner“) und kann mehrere Elemente enthalten (Verzeichnisse und Dateien).

Das andere wird als „Datei“ bezeichnet und es enthält Daten wie Text, Tabellen oder Videoinhalte. Für Basisoperationen wie Kopieren, Verschieben oder Umbenennen spielt es jedoch keine Rolle, ob es sich bei einem Element um eine Datei oder einen Ordner handelt.

Unter Linux gibt es die Besonderheit, dass auch Geräte Elemente im Dateisystem sind. Eine Festplatte lässt sich beispielsweise über „/dev/sda“ ansprechen („device file“). Diese Dateien dienen Programmen als Schnittstelle zum Gerät, der Benutzer sollte sie nicht direkt verwenden.

Unterhalb von „/sys“ und „/proc“ erstellt der Kernel automatisch Ordner und Dateien in einem virtuellen Dateisystem. Darüber lassen sich Informationen zur Hardware auslesen. Im Terminal liefert beispielsweise

```
cat /proc/cpuinfo
```

jederzeit aktuelle Daten zum Prozessor. Einige Dateien sind auch beschreibbar, um Optionen für Kernel oder Treiber temporär zu setzen. Von diesen speziellen Fällen abgesehen, sollte man in diesen Ordnern nichts ändern oder löschen.

Effektiv mit dem Dateimanager arbeiten

In fast allen Linux-Dateimanagern gelten dieselben Tastenkombinationen und auch die Kontextmenüs von Dateien und Ordner schauen ähnlich aus. Mit Strg-C kopieren Sie ein Element des Dateisystems und mit Strg-V fügen Sie es ein. Nach einem rechten Mausklick sind die entsprechenden Menüpunkte „Kopieren“ und „Einfügen“ zu sehen. Strg-C wirkt sich auf das zuvor angeklickte Element aus, mit Mausklicks bei gedrückter Strg-Taste lassen sich mehrere Dateien oder Ordner markieren. Strg-A

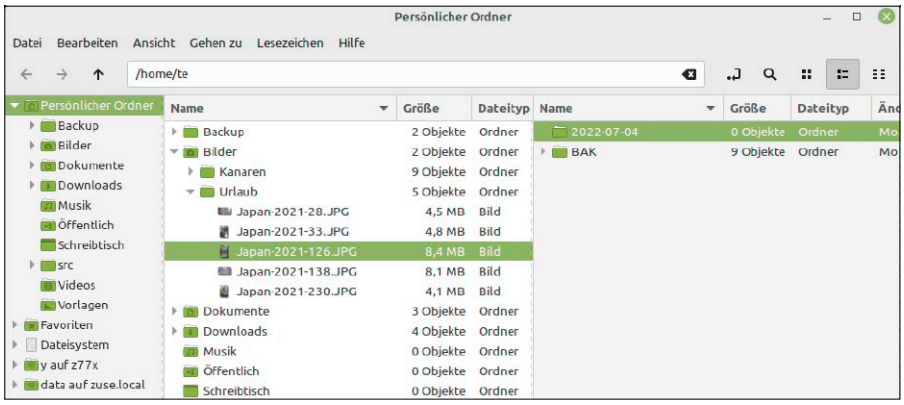
markiert alle Elemente. Verwenden Sie Strg-X statt Strg-C, wenn Sie Elemente verschieben wollen. Danach wechselt man in den Zielordner, in den man alles mit Strg-V einfügt.

Für den Datenaustausch dient bei Strg-C/Strg-V die Zwischenablage. Die Operationen finden nur im Hauptspeicher statt, wobei nicht die tatsächlichen Dateien, sondern nur Verweise kopiert werden. Sonst wäre der Speicher bei großen Dateien schnell voll. In der Zwischenablage landet im Wesentlichen nur Text. Wenn Sie im Dateimanager eine Datei mit Strg-C kopieren und dann in einem Texteditor Strg-V drücken, wird daher der Dateiname inklusive Pfad eingefügt. Wurden mehrere Elemente kopiert, speichert die Zwischenablage eine Liste der Pfade und Dateinamen. Eine Ausnahme sind Bilder, die Sie mit Strg-C in einem Bildbearbeitungsprogramm kopieren. Die Zwischenablage enthält dann das Bild, nicht nur den Verweis.

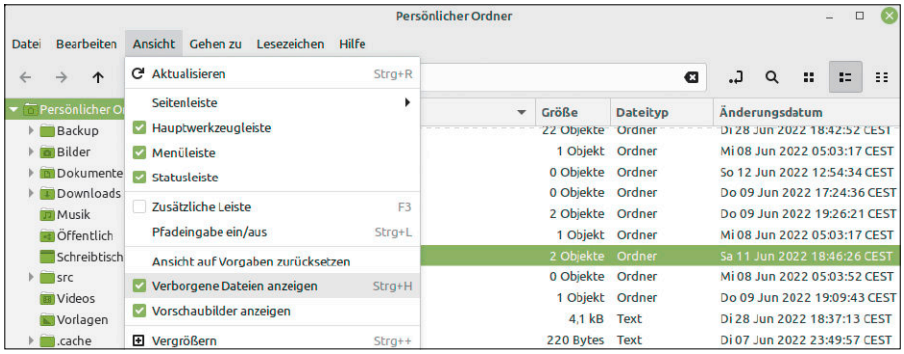
Mehrere Fenster nutzen: Kopieraktionen lassen sich bequemer durchführen, wenn Sie zwei Fenster des Dateimanagers öffnen. Nutzer von Ubuntu und Linux Mint verwenden dafür die Tastenkombination Strg-N. In einem Fenster wechseln Sie zum Quellverzeichnis und im anderen zum Zielverzeichnis. Sie müssen dann nicht umständlich zwischen den Ordnern navigieren. Außerdem lassen sich Elemente einfach mit der Maus in das andere Fenster verschieben. Wenn Sie dabei die Strg-Taste gedrückt halten, werden die Dateien kopiert. Liegt das Zielverzeichnis auf einem anderen Laufwerk, wird die Datei per Drag & Drop kopiert. Im Ubuntu-Dateimanager (Nautilus) halten Sie dabei die Strg- und Shift-Taste gedrückt, wenn Sie eine Datei verschieben wollen. Beim Dateimanager von Linux Mint (Nemo) genügt die Shift-Taste.

Als Alternative kann man in fast allen Linux-Dateimanagern mit Strg-T Tabs öffnen, in denen Sie sich unterschiedliche Ordner anzeigen lassen. Per Drag & Drop auf die Titelleiste eines Tabs verschieben Sie Ordner oder Dateien. Halten Sie dabei die Strg-Taste gedrückt, wenn Sie die Elemente kopieren wollen. Beim Linux-Mint-Dateimanager öffnet die F3-Taste eine geteilte Ansicht, was zielgenaues Drag & Drop auch in ein Unterverzeichnis ermöglicht.

Hinweis: Ordner und Dateien im Home-Verzeichnis, deren Namen mit einem Punkt beginnen, enthalten Konfigurationsdaten.



Zwei-Panel-Ansicht: Der Dateimanager von Linux Mint bietet eine geteilte Ansicht. Man muss dann nicht umständlich in den Zielordner wechseln und Drag & Drop wird vereinfacht.



Alles sehen im Dateimanager: Wenn Sie versteckte Konfigurationsdateien und Ordner kopieren wollen, müssen Sie sich die verborgenen Dateien anzeigen lassen.

Diese zeigt der Dateimanager standardmäßig nicht an. Um das zu ändern, hilft ad hoc der Hotkey Strg-H, dauerhaft die Einstellung „Verborgene Dateien anzeigen".

Umbenennen nach Muster

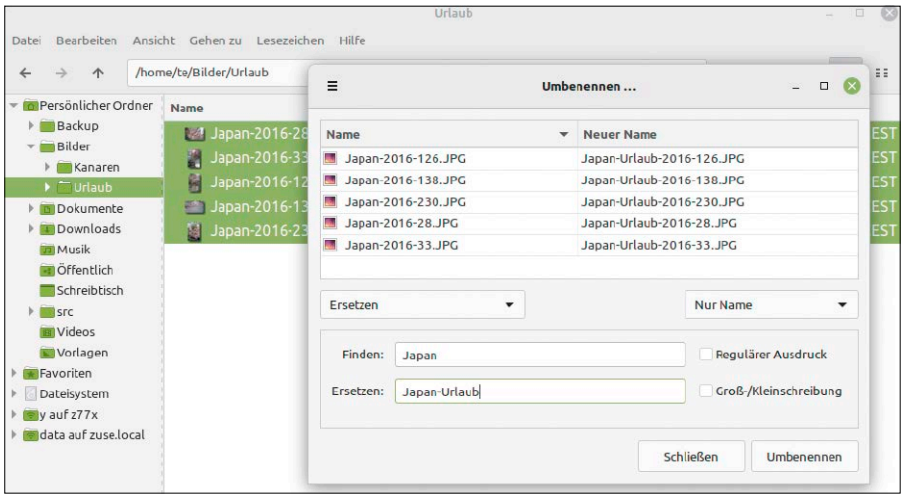
Im Dateimanager lässt sich der Name von Dateien und Ordnern über die Taste F2 oder den Kontextmenüpunkt „Umbenennen" ändern. Sind mehrere Elemente ausgewählt, zeigen die Dateimanager von Ubuntu und Linux Mint einen Dialog für die Mehrfachumbenennung. Sie können beispielsweise Teile der Dateinamen ersetzen oder Text hinzufügen. Es erscheint eine Vorschau mit dem Ergebnis, ein Klick auf „Umbenennen" führt die Änderungen durch. Wem dieser Funktionsumfang nicht ausreicht, der installiert mit

```
sudo apt install gprename
```

ein zusätzliches Tool. Gprename zeigt in der linken Spalte einen Ordner-Browser und rechts davon die Dateiliste. Die Funktionen zum Umbenennen befinden sich im unteren Bereich. Neben Schaltern wie „Alles klein" gibt es unter „Ersetzen/Löschen" eine Ersetzungsfunktion, die reguläre Ausdrücke versteht.

DATEIEN PER FILTER AUSWÄHLEN UND KOPIEREN

Die Suchfunktion (Strg-F) der Dateimanager von Ubuntu und Linux Mint arbeitet wie ein Filter. Sie können damit die Sicht auf einen Zweig des Dateisystems gemäß bestimmter Kriterien einschränken. Die Suchmaske kann eine Dateinamenserweiterung wie „jpg" oder „pdf" sein oder ein Teil des Dateinamens. Wenn Sie die Bezeichnungen mit Datum und Stichwörtern ergänzt haben, lassen sich beispielsweise Elemente mit einem bestimmten Stichwort einfach finden. Die Dateiliste im Suchergebnis können Sie mit Strg-A auswählen und die Dateien dann wie gewohnt kopieren, verschieben oder löschen.



Dateien umbenennen: Sind mehrere Dateien markiert, öffnet sich bei „Umbenennen“ ein Fenster, über das sich Dateinamen oder Namensteile suchen und ersetzen lassen.

Der KDE-Dateimanager Dolphin bietet nur die Umbenennung mit einem neuen Namen und die automatische Nummerierung. Für KDE ist daher das Tool Krename empfehlenswert, das sich mit

```
sudo apt install krename
```

installieren lässt. Über „Hinzufügen“ wählen Sie die Elemente aus, die Sie umbenennen möchten. Auf der Registerkarte „4. Dateiname“, stellen Sie unter „Einfacher Dateiname“ Präfix und Suffix ein. Über die Schaltfläche mit dem „i“ in einem Kreis wählen Sie jeweils die passende Funktion, beispielsweise „[date]“ für das aktuelle Datum. Auf der Registerkarte „Fortgeschrittenen-Modus für Dateinamen“ sehen Sie die Variablen hinter „Vorlage:“. Die Zeile lässt sich bei Bedarf anpassen. Eine Vorschau zeigt das zu erwartende Ergebnis, erst der Klick auf „Fertigstellen“ führt die Änderungen durch.

Dateien und Ordner strukturiert ablegen

Wenn viele persönliche Dateien auf der Festplatte liegen, sollte man über ein strukturiertes Ablagesystem nachdenken. Die Linux-Standardinstallation liefert dafür mit Ordnern für unterschiedliche Dateitypen wie „Dokumente“, „Bilder“ und „Videos“ bereits eine Vorlage. Wie man weiter vorgeht, hängt von den eigenen Vorlieben ab. Aussagekräftige Bezeichnungen für Ordner und Dateien können ein Baustein sein.

Karl Voit hat sich in seinem Blog (*https://karl-voit.at*) einige Gedanken zur effektiven Dateiablage gemacht. Seine einfache Methode: Man bringt Datum und Stichwörter („tags“) in Datei- und/oder Ordnernamen unter, was man manuell durch Umbenennen erledigen kann. Ein gewünschtes Element lässt sich dann über die Navigation im Dateimanager, aber auch über die Suchfunktion schneller finden. Zur Vermeidung von Fehlern und zur Vereinfachung sollte man das Python-Script „date2name“ (*https://github.com/novoid/date2name*) verwenden. Zur Vorbereitung installieren Sie im Terminal

```
sudo apt install python3-pip
```

Das Tool lässt sich dann mit

```
pip3 install date2name
```

im Home-Verzeichnis im Verzeichnis „.local/bin“ installieren, das Sie mit

```
source ~/.profile
```

in den Suchpfad aufnehmen. Mit der Zeile

```
date2name [Dateiname]
```

baut das Script das Änderungsdatum am Anfang des Dateinamens ein. Ersetzen Sie den Platzhalter durch den Namen der Datei. Ein weiteres Tool (*https://github.com/novoid/filetags*) installiert dieser Befehl

```
pip3 install filetags
```

und der Aufruf erfolgt so:

```
filetags [Dateiname]
```

Danach tippen Sie das gewünschte Stichwort ein und bestätigen mit der Eingabetaste. Mehrere Stichwörter lassen sich mit Leerzeichen getrennt vergeben. Der resultierende Dateiname kann dann beispielsweise so aussehen:

```
2022-07-04 Artikel_Dateien –
  entwurf.odt
```

Scripts in den Dateimanager einbauen: Für mehr Komfort startet man solche Tools über den Dateimanager. Erstellen Sie eine Textdatei mit dem Namen „date.sh“ und diesem Inhalt (zwei Zeilen):

```
#! /bin/bash -e
$HOME/.local/bin/date2name "$@"
```

Machen Sie die Datei mit

```
chmod +x date.sh
```

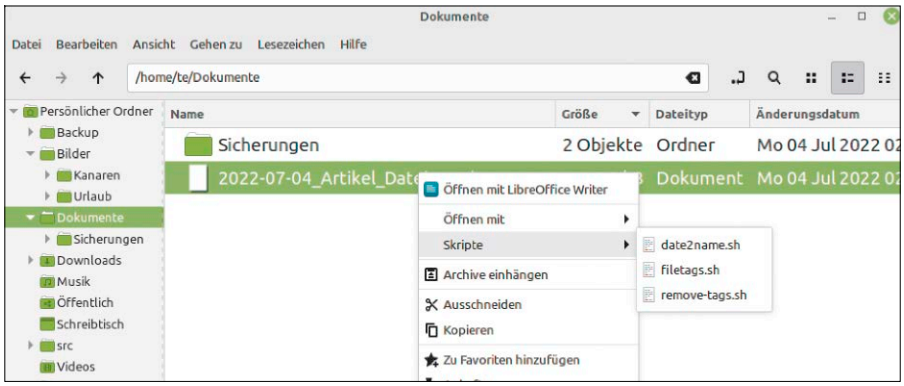
ausführbar. Eine zweite Textdatei erhält den Namen „filetags.sh“ mit diesem Inhalt (zwei Zeilen):

```
#! /bin/bash -e
gnome-terminal -- python3 $HOME/.
  local/bin/filetags "$@"
```

In einer dritten Datei „remove-tags.sh“ ändern Sie die zweite Zeile in

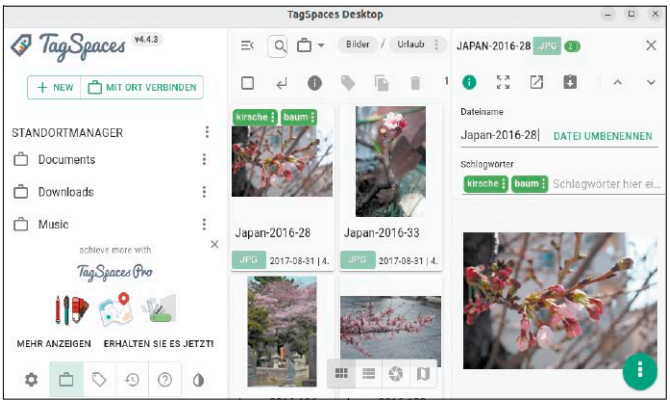
```
gnome-terminal -- python3 $HOME/.
  local/bin/filetags --remove "$@"
```

Machen Sie auch diese Dateien ausführbar und verschieben Sie alle Dateien in den Ordner „.local/share/nautilus/scripts“ (Linux Mint: „.local/share/nemo/scripts“). Klicken Sie eine Datei im Dateimanager mit der rechten Maustaste an und wählen Sie im Kontextmenü „Scripte → date2name.sh“, um das Datum in den Namen einzubauen. Nach dem Klick auf „Scripte → filetags.sh“ öffnet sich ein Terminal, über das Sie Stichwörter vergeben. Mit „Scripte → remove-tags.sh“ entfernen Sie Stichwörter.



Dateien einheitlich kennzeichnen: Die Tools date2name und filetags kann man über ein Script in den Dateimanager einbauen und dann Datum und/oder Stichwörter in die Namen einsetzen.

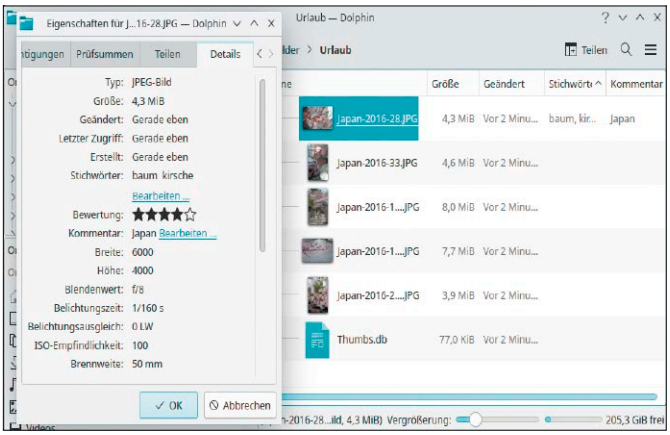
Tipp: Der Dateimanager Tagspaces (*www.tagspaces.org*) arbeitet nach einem ähnlichen Prinzip. Auch er baut die Begriffe einfach in den Dateinamen ein und zeigt Vorschaubilder inklusive der vergebenen Schlagwörter. Über die Suchfunktion lassen sich Dateien mit bestimmten Schlagwörtern schnell finden.



Alternativer Dateimanager: Tagspaces kann Stichwörter in Dateinamen einbauen und auch wieder entfernen. Die Stichwörter lassen sich für die Suche nutzen.

Dateimanager mit Stichwortfunktion

Im KDE-Dateimanager Dolphin lassen sich Elemente im Dateisystem mit Metadaten verknüpfen. Zur Verfügung stehen Stichwörter, Kommentare und Bewertungen. Die Metadaten kann man jedoch erst verwenden, wenn die Inhalte in den Suchindex aufgenommen werden. Dazu rufen Sie die „Systemeinstellungen“ auf, gehen auf „Suchen → Dateisuche“, setzen Häkchen vor „Dateisuche aktivieren“ und „Auch Dateiinhalt indizieren“. Danach klicken Sie auf „Anwenden“. Nur Dateien in Ihrem Home-Verzeichnis werden indiziert. Über „Ordnereinstellung hinzufügen“ lassen sich weitere Ordner angeben.



KDE-Dateimanager Dolphin: In den Eigenschaften einer Datei können Sie Stichwörter unterbringen, die der Dateimanager anzeigt und nach denen Sie bei der Suche filtern können.

Im Dateimanager klicken Sie einen Ordner oder eine Datei mit der rechten Maustaste an und gehen auf die Registerkarte „Details“. Hier können Sie jeweils nach einem Klick auf „Hinzufügen“ Stichwörter und Kommentare festlegen. Hinter „Bewertung:“ klicken Sie auf eines der Sternchen. Die Metadaten sind im Dateimanager in der Detailansicht (Strg-3) zu sehen. Nach einem rechten Mausklick auf den Spaltenkopf können Sie angeben, welche Spalten Sie sehen wollen.

Mit Strg-F blenden Sie die Suchleiste ein. Ist die Registerkarte „Dateiname“ aktiv, sucht Dolphin nach Dateien und Ordnern, deren Name den Suchbegriff enthält. Aktivieren Sie die Registerkarte „Inhalt“, wenn Sie auch den Dateiinhalt durchsuchen möchten. Nach einem Klick auf „Beliebige Bewertung“ fügen Sie Bewertungen als Suchkriterium hinzu. Unter „Stichwörter hinzufügen“ setzen Sie Häkchen vor die Stichwörter, auf die Sie die Suche einschränken wollen.

Mit Dateien im Terminal arbeiten

Im Terminal versprechen Tools wie cp (kopieren) oder mv (verschieben) nicht besonders viel Komfort. Mit den richtigen Optionen sind es zwar mächtige Werkzeuge, für Gelegenheitsnutzer aber nur eingeschränkt zu empfehlen. Der Zugang zum Terminal-Dateimanager Midnight Commander erschließt sich dagegen schneller. Installieren Sie den Klassiker mit

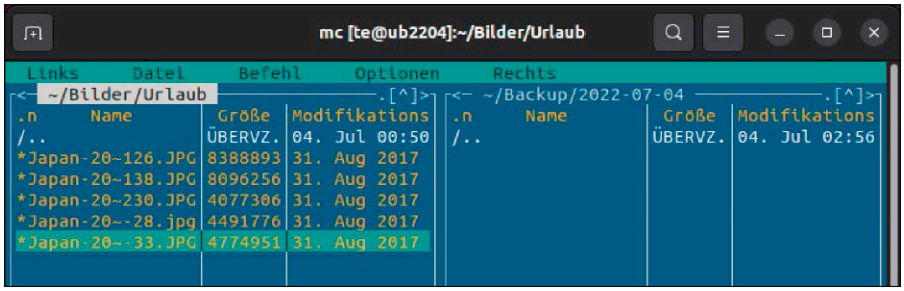
```
sudo apt install mc
```

und starten Sie ihn mit diesem Befehl:

```
mc
```

Das Programm zeigt zwei Panels, in denen sich zwei unterschiedliche Ordner darstellen lassen. Mit der Tab-Taste wechseln Sie zwischen den Panels und navigieren mit den Cursortasten und der Eingabetaste. Mit F5 kopieren Sie das markierte Element in den Ordner, den das andere Panel anzeigt. Drücken Sie mehrfach die Taste Einfg, wenn Sie mehrere Elemente markieren möchten. Die F6-Taste dient zum Verschieben, F8 zum Löschen und mit F7 erstellt man neue Ordner. Alle F-Tasten-Befehle sind am unteren Rand zu sehen und lassen sich auch mit der Maus klicken.

Den Umgang mit dem Terminal erleichtert der Midnight Commander ebenfalls. Mit Alt-Enter fügen Sie den Namen der markierten Datei in die Eingabezeile ein. Strg-O blendet den Midnight Commander aus und zeigt das Terminal. Sie können die Befehlszeile bearbeiten und beispielsweise den Namen eines Tools voranstellen, mit dem Sie die Datei öffnen möchten. Mit Strg-O kehren Sie zum Midnight Commander zurück. ■



Im Terminal arbeiten: Midnight Commander eignet sich für die schnelle Navigation im Dateisystem. In der Zwei-Panel-Ansicht lassen sich Dateien bequem in andere Ordner kopieren.

Clevere Konsole

Die Tipps für Arbeiten in der Shell drehen sich diesmal um die Navigation im Dateisystem und um die Einbindung von externen Medien. Zudem gibt es wieder einige findige Tools für die Kommandozeile wie den Systemmonitor Btop++.

Schöner Systemmonitor: Btop++

Einer der ersten ansehnlichen System- und Prozessmonitore für das Terminal war htop, das heute in vielen Linux-Distributionen neben dem einfacheren top ebenfalls vorinstalliert ist. In den letzten Jahren kamen, dank höherer Bildschirmauflösungen, einige clevere, aufwendige und besonders informative Programme in diesem Stil hinzu. Eines der neuesten Tools ist das Programm Btop++.

Jede Menge Infos zu System und Ressourcen: Der Systemmonitor Btop++ tritt die Nachfolge der ähnlich gestalteten Tools Bashtop und Bpytop an und ist in C++ geschrieben.

Dieser neue Prozess- und Ressourcenmonitor fasst mehrere Leistungsdaten in einem (möglichst großen) Terminalfenster zusammen. Zu sehen gibt es oben die CPU-Auslastung, die auch per Kerne aufgeschlüsselt ist und die Temperaturen anzeigt. Darunter gibt es in der zweiten Spalte die Speicherauslastung, Laufwerksbelegung und eine ausführliche Prozessliste. Links unten zeigt ein Feld den Netzwerkdurchsatz mit eingehenden und ausgehenden Daten an.

Das Besondere an Btop++ (*https://github.com/aristocratos/btop*) ist nicht allein die ansehnliche Aufmachung: Es ist nicht mehr in Script-Sprache geschrieben wie die Vorgängerprogramme des gleichen Programmierers, sondern in C++. Das Programm ist damit effizienter, braucht selbst weniger Ressourcen und läuft nun auch auf einem älteren Raspberry Pi passabel. In Ubuntu 22.04 und dem neuen Open Suse Leap 15.4 ist Btop++ schon aus den Standard-Paketquellen installierbar, in Ubuntu mittels

```
sudo apt install btop
```

und in Open Suse in der Befehlszeile mit dem Paketmanager Zypper:

```
sudo zypper in btop
```

Für andere Linux-Distributionen für die x86-Architektur sowie ARM steht Btop++ als kompilierte Binary mit statisch verlinken Bibliotheken unter *https://github.com/aristocratos/btop/releases* zum Download bereit. Für Raspberry-Pi-OS für ARM 32 Bit ist beispielsweise das angebotene Archiv „btop-arm-linux-musleabi.tbz“ die passende Version. Es handelt sich bei allen angebotenen Dateien um „tar.bz2“-Archive, die nach dem Download mit

```
tar xjvf [Datei].tbz
```

entpackt werden. Im ausgepackten Unterverzeichnis „/bin“ findet sich die ausführbare Datei „btop“ und es gibt auch ein automatisiertes Installations-Script, welches mittels

```
./install.sh
```

ausgeführt wird und dann nach dem sudo-Passwort fragt, um das Tool systemweit verfügbar zu machen.

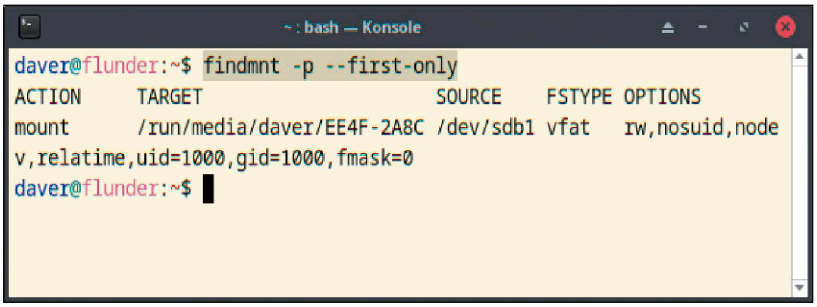
Nach dem Aufruf *btop* präsentiert die Esc-Taste ein Menü für Optionen und eine Hilfeseite. Es gibt zahlreiche Abkürzungen, um einen bestimmten Teil der anzeigten Metriken zu vergrößern oder auszublenden. Verschiedene „Themes“ können das Farbschema der angezeigten Elemente anpassen, je nachdem, ob das Terminal einen hellen oder dunklen Hintergrund hat. Zum Beenden dient die Taste Q. **-dw**

Findmnt: Eingebundene Laufwerke finden

Wo ist welcher Datenträger eingehängt und welches Dateisystem hat dieser? In der Befehlszeile eignet sich der übliche Befehl mount, der alle Einhängepunkte mit Dateisystem und Optionen anzeigt, nicht mehr gut. Denn moderne Linux-Distributionen zeigen hier auch alle virtuellen Laufwerke an und Ubuntu listet obendrein alle Snaps auf, die als Loopback-Dateisystem eingebunden sind.

Eine bessere, geordnete Übersicht liefern die Befehle lsblk sowie findmnt, welche jeweils alle einhängten Dateisysteme und Laufwerke in einer Baumansicht anzeigen.

Die Ausgaben sind ähnlich, allerdings kann findmnt auf der Suche nach einem bestimmten Laufwerk mit Filtern und Suchfunktionen dienen. Dazu einige praktische Beispiele.



Neu angelegten Mountpunkt ermitteln: Nach diesem Aufruf wartet findmnt darauf, dass ein neues Laufwerk angeschlossen und von Automount eingehängt wird.

Mountpunkt finden: Ist das Verzeichnis bekannt, das als Einhängepunkt für ein Dateisystem oder Laufwerk dient, etwa „/mnt/raid“, so zeigt

```
findmnt /mnt/raid
```

alle Infos zu diesem Mountpunkt an – mit Laufwerks-ID, Dateisystem und Mountoptionen.

Laufwerk finden: Wo ist ein Datenträger eingehängt? Umgekehrt kann die Eingabe von

```
findmnt /dev/sda1
```

anhand der ID zeigen, in welchem Verzeichnis ein Dateisystem steckt.

Dateisysteme filtern: Sind nur die Einhängepunkte mit bestimmten Dateisystemen interessant, so zeigt das Kommando

```
findmnt -t vfat,ext4,btrfs
```

nur Mountpunkte mit den Dateisystemen FAT32 (VFAT), Ext4 und BTRFS an.

Interaktiver Modus: Wenn automatisches Einhängen von externen Datenträgern auf einem Desktop aktiviert ist, so kann findmnt darauf warten, bis das Laufwerk eingesteckt wird.

```
findmnt -p --first-only
```

Sobald das externe Medium eingehängt ist, zeigt dieser Befehl den neuen Mountpunkt im Terminal mit seinem Pfad sowie Laufwerks-ID an und beendet sich dann selbständig. **-dw**

Externe Medien: Einhängepunkt per Symlink

In vielen Distributionen erscheinen eingehängte Laufwerke, etwa USB-Sticks, nicht unterhalb von „/media/[user]“ wie in Debian/Ubuntu, sondern im Unterverzeichnis „/run/media/[user]“. Bei Arbeiten in der Befehlszeile ist der lange Pfad unbequem, wenn man ihn stets eingeben muss, um zum gewünschten externen Laufwerk zu kommen.

Abhilfe schafft ein Symlink (symbolischer Link) zum Verzeichnis der eingehängten Wechseldatenträger im eigenen Home-Verzeichnis. Dies verkürzt die Wege in Distributionen wie Fedora, Manjaro, Arch Linux und anderen beim Ordnerwechsel erheblich. Der Befehl

```
ls -s /run/
  media/$(whoami) ~/medien
```

erstellt einen Symlink namens „medien“ im Home-Verzeichnis. Es ist wichtig, diesen Symlink anzulegen, wenn ein USB-Laufwerk schon angesteckt ist, denn ansonsten existiert der Pfad nicht. Anschließend kann man mit

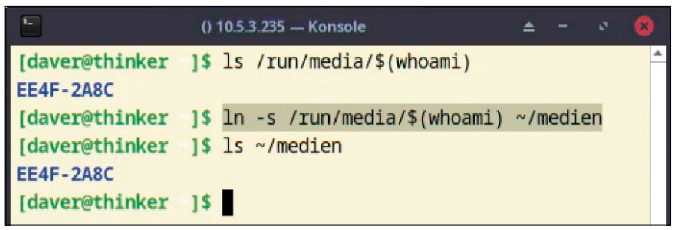
```
cd ~/medien
```

immer in den Ordner wechseln, der in seinen Unterverzeichnissen alle automatisch eingehängten Wechselmedien enthält. Steckt gerade keines am Computer, so zeigt der Symlink ins Leere (verwaister Symlink) und ist bei einer Auflistung mit ls im Home-Verzeichnis rot markiert.

Debian/Ubuntu: Auch wenn der Pfad hier deutlich kürzer ausfällt, so kann der Ordner für Automount mittels

```
ls -s /media/$(whoami) ~/
  medien
```

auch hier als Symlink im Home abgelegt werden. **-dw**

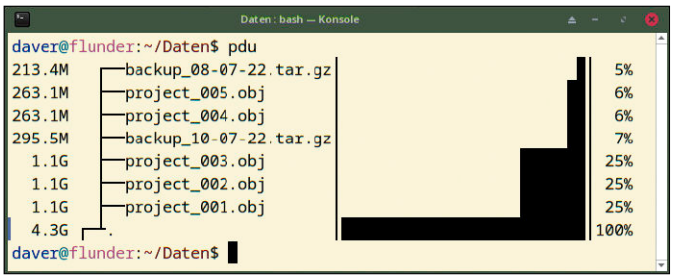


Kurze Wege dank Symlink: Dieser Tipp ist besonders nützlich für Systeme wie Fedora, Open Suse, Manjaro und Arch, die USB-Medien unterhalb von „/run/media/[user]“ einhängen.

Datenträgerbelegung: Flott visualisieren

Schnelle NVMEs sind weiterhin bedeutend kleiner als übliche Festplatten. Wer das Dateisystem auf überfüllten NVMEs flott in der Shell analysieren will, bekommt mit dem Kommandozeilentool pdu ein Werkzeug zur Visualisierung von Datenträgern oder einzelnen Ordnern. Parallele Threads machen es um etliches schneller als die traditionellen Tools.

Ein verwandtes und allbekanntes Programm ist ncdu. Bei einem vollen Dateisystem arbeitet es schon eine Weile, bis die Statistik und eine schlichte Darstellung der Ergebnisse in einer Baumstruktur stehen. Das al-



Was braucht wie viel Platz? Das Kommandozeilentool pdu listet Dateien und Unterordner ausgehend von aktuellen Verzeichnis mit Größenangaben und einem Größenvergleich auf.

ternative pdu erledigt dies deutlich schneller, auf SSDs und NVMEs sowieso, da diese Laufwerkstypen von Haus aus Parallelität für mehrere Programmthreads bieten. Diese Fähigkeit nutzt pdu, das in Go programmiert ist.

Die Installation gelingt dank vorkompilierter Binarys auf der Github-Seite des Entwicklers ohne Probleme: Unter *https://github.com/KSXGitHub/parallel-disk-usage/releases* liegen ausführbare Programmdateien. Für ein Linux-System (64 Bit, x86-Architektur) ist der Download der Datei „pdu-x86_64-unknown-linux-gnu" einschlägig, die dann mit

```
chmod +x pdu-x86_64-
  unknown-linux-gnu
```

noch ausführbar geschaltet werden muss. Der Aufruf

```
./pdu-x86_64-unknown-
  linux-gnu
```

stellt den Inhalt ab dem aktuellen Verzeichnis dar. Die linke Spalte zeigt dabei den jeweiligen Dateinamen und rechts zeigt ein Balken und eine Prozentangabe die relative Dateigröße. Um pdu von einem beliebigen Pfad aus aufrufen zu können, kopiert man die Programmdatei am besten ins Verzeichnis „~/.local/bin", das für diese Zwecke vorgesehen ist und sich in den meisten Linux-Distributionen schon in der Pfad-Umgebungsvariable „$PATH" befindet.

Das Kommando

```
mkdir -p ~/.local/bin
```

erstellt das Verzeichnis, falls noch nicht vorhanden, und

```
cp pdu-x86_64-unknown-
  linux-gnu ~/.local/bin/
  pdu
```

kopiert die Programmdatei als „pdu" dorthin. **-dw**

Ordner: Beliebige Sprungmarken setzen

Der vorherige Tipp zeigt, wie ein häufig benötigter Systemordner im Home-Verzeichnis bequem per Symlink erreichbar sein kann. Dieses Konzept ist ausbaufähig, um Lesezeichen zu beliebigen Ordnern zu setzen und wieder zu entfernen.

Möglich machen das ein kleines Lesezeichen-System, die Fähigkeiten der Standard-Shell Bash und die optionale Umgebungsvariable „CDPATH", welche eine Liste von Verzeichnissen aufnimmt. Ein versteckter Ordner namens „.lesezeichen" im Home-Verzeichnis nimmt als Speicherort Sprungmarken als Symlinks auf, die auf diese Weise immer für den Befehl „cd" bereitstehen und so bequem abrufbar sind. Diese Sprungmarken bekommen als Präfix das Zeichen „@", um sie von tatsächlichen Ordnern zu unterscheiden. So gelingt dieser Aufbau in wenigen Schritten:

1. Den versteckten Lesezeichenorder erstellt folgender Befehl.

```
mkdir ~/.lesezeichen
```

2. Nun öffnet man die Konfigurationsdatei „.bashrc" im Home-Verzeichnis. Ganz ans Ende der Datei kommen die sieben Zeilen aus dem hier abgedruckten Kasten „Bash: Lesezeichen-Funktion definieren". Danach ist ein Schließen des Terminals und erneutes Öffnen notwendig, damit die Konfigurationsdatei neu eingelesen wird. Diese Zeilen legen die neue Bash-Funktion „merke" fest sowie die Auflösung von Symlinks über den Befehl „cd".

3. Jetzt sind die Lesezeichen einsatzbereit. Das neue Kommando

```
merke @lesezeichen
```

legt für jeweils das aktuelle Verzeichnis eine Sprungmarke mit dem Namen „@lesezeichen" oder einem anderen, beliebigen Namen mit dem Präfix „@" an. Später wechselt dann

```
cd @lesezeichen
```

wieder zurück in dieses Verzeichnis. Benötigt man die Sprungmarke „@lesezeichen" nicht mehr, so löscht diese das Kommando

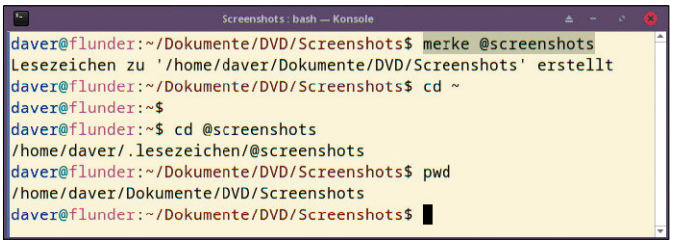
```
rm ~/.lesezeichen/@
  lesezeichen
```

wieder aus dem Lesezeichenordner.

Das vorangestellte „@" erfüllt zwei Zwecke: Erstens kommt dabei kein tatsächlich vorhandener Ordnernamen in die Quere. Zweitens ist so einfacher, die Autovervollständigung der Bash zu nutzen, denn nach der Eingabe des Teilnamens „cd @lese" gefolgt von einem Druck auf die Tab-Taste wird der Name der Sprungmarke automatisch vervollständigt. Eine Übersicht und Erinnerung, welche Sprungmarken schon angelegt sind, zeigt der Befehl

```
ls ~/.lesezeichen
```

an. Auf diese Weise lassen sich beliebig viele Lesezeichen mit beliebigen Namen anlegen und bequem abrufen. **-dw**



Lesezeichen: Diese selbst gebaute Bash-Funktion „merke" legt den jeweils aktuellen Ordner als Sprungmarke ab. Das Präfix „@" grenzt die Lesezeichen gegenüber echten Verzeichnissen ab.

BASH: LESEZEICHEN-FUNKTION DEFINIEREN

```
export CDPATH=.:~/.lesezeichen/
function merke {
ln -sr "$(pwd)" ~/.lesezeichen/"$1"
echo "Lesezeichen zu '$(pwd)' erstellt"
}
# Symlinks per cd auflösen:
alias cd="cd -P"
```

Hardware ahoi!

KDE Connect hat den Sprung auf das iPhone geschafft. Bluetooth gibt es bei alten Geräten in besserer Soundqualität und bei mehreren SATA-Laufwerken an der Hauptplatine helfen zwei Scripts zur idealen Portbelegung.

Bluetooth: SBC-XQ klingt besser

Audiosignale per Bluetooth an Kopfhörer, Headset und Verstärker müssen keine Radioqualität haben. Sowohl Pulseaudio als auch Pipewire unterstützen heute bessere Codecs. Headsets – auch ältere – machen dabei meist mit und klingen dann um Klassen besser.

Eine Bluetooth-Verbindung zu Audiogeräten arbeitet unter Linux bei Hi-Fi-Qualität zunächst nur mit 328 Kbps Übertragungsrate (SBC). Bei vielen Bluetooth-Geräten ginge aber noch mehr über den Standard „SBC-XQ", der je nach Audiohardware bis zu 730 Kbps unterstützt (Kilobits pro Sekunde). Auch die Fehlerkorrektur und der Overhead sind optimiert, was bessere Reichweite bei gleicher Soundqualität bringt. Nachsehen und ausprobieren lohnt sich in jedem Fall.

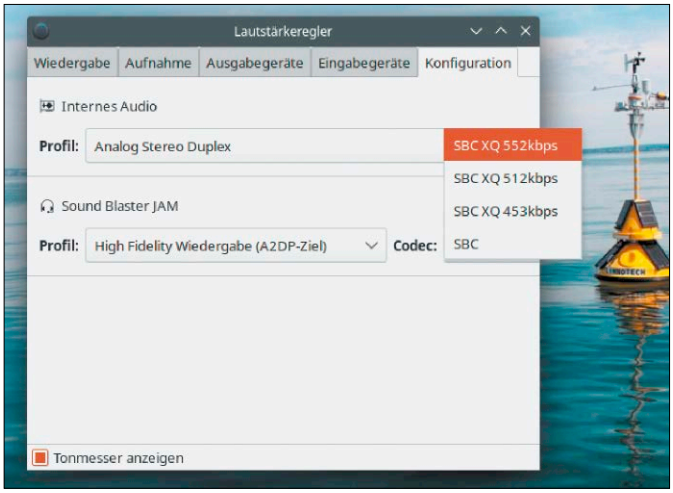
1. Egal, ob als Soundserver Pulseaudio oder das neue Pipewire dient, kommt zum Einstellen der Bluetooth-Codecs das Programm Pavucontrol zum Einsatz. In Debian, Ubuntu und Co. installiert das Kommando

```
sudo apt install
  pavucontrol
```

das grafische Tool.

2. Dann ist eine Verbindung der Bluetooth-Geräte mit dem Linux-Rechner nötig. Steht diese, so ruft man *pavucontrol* auf.

3. In Pavucontrol geht es auf das Register „Konfiguration" und unten auf den Eintrag des Bluetooth-Geräts, das hier mit Namen aufgelistet ist. Als Profil sollte immer „A2DP" ausgewählt sein (Hi-Fi-Qualität). Daneben stehen die unterstützten Audiocodecs des Geräts zur Auswahl, neben dem standardmäßig ausgewählten „SBC" auch das bessere „SBC XQ" mit höheren Bitraten. Mit neueren Headsets steht häufig auch der Codec „APTX" zur Auswahl, der für bidirektionale Kommunikation gemacht ist.



Codec für Bluetooth-Audiogeräte auswählen: Auch ältere Modelle, hier ein bereits mehrere Jahre alter Bluetooth-Kopfhörer, unterstützen SBC XQ mit höheren Bitraten.

Dieser Codec wird aber erst ab Pulseaudio 15 unterstützt, das nur in aktuelleren Distributionen verfügbar ist – etwa ab Ubuntu 21.10, Fedora 35 und Open Suse Leap 15.4. **-dw**

SATA-Ports: Ideale Belegung ermitteln

Seit Markteinführung von SATA vor zehn Jahren wurde dieser serielle Bus für Datenträger zweimal aktualisiert. SATA liegt daher in drei Revisionen vor: Während SATA-III von 2009 Geschwindigkeiten bis zu sechs Gbps bietet, sind die älteren Standards SATA-II und SATA-I für maximal drei Gbps beziehungsweise 1,5 Gbps ausgelegt. Auf Hauptplatinen sind meist SATA-III- und SATA-II Ports vorhanden und wer mehrere Laufwerke in Betrieb hat, will natürlich schnelle SSDs an den schnellen SATA-Ports haben.

Bei vielen Hauptplatinen sind schnelle und langsame SATA-Ports farblich abgesetzt und SATA-III-Anschlüsse sind blau oder rot. Sind alle Farben gleich, hilft oft nur Ausprobieren, um die schnellen Ports zu ermitteln. Aber auch Laufwerke sind nicht alle gleich: Es gibt SSDs aus den Anfangsjahren dieser Speichertechnologie, die nur SATA-I oder SATA-II unterstützen. Als Hilfestellung bei der Identifizierung der angeschlossenen SATA-Laufwerke, der maximalen SATA-Geschwindigkeit und der verwendeten Ports finden sich zwei Scripts der Linux-Welt-Redaktion auf Heft-DVD:

laufwerke.sh: Dieses Bash-Script wird mit

```
bash laufwerke.sh
```

gestartet, analysiert dann die Geräteliste des Linux-Kernels und schlüsselt die SATA-Laufwerke in drei Spalten anhand der Modellbezeichnung, der Nummer des SATA-Ports und dessen maximaler Geschwindigkeit auf. Dies hilft, um Laufwerke und Ports zuzuordnen.

laufwerke.py: Viele Infos mehr zeigt dieses Python-Script, das die Ausgabe von smartctl analy-

```
Konsole
daver@raider:~ $ sh laufwerke.sh

Modell                          SATA-Link                       SATA-Speed
-------------------------------------------------------------------------------
X41100RLSanDisk Ultra II 240    /sys/class/ata_link/link1       6.0 Gbit/s
M0MA020Micron_1100_MTFDDAV51    /sys/class/ata_link/link2       6.0 Gbit/s
80.00A80WDC WD20EZRZ-00Z5HB0    /sys/class/ata_link/link3       6.0 Gbit/s
8MX4OABB0TOSHIBA DT01ACA200     /sys/class/ata_link/link4       3.0 Gbit/s
SC60 ST2000VN004-2E4164         /sys/class/ata_link/link5       3.0 Gbit/s
```

Das schlichte Script laufwerke.sh: Sind auf einem System keine sudo-Privilegien verfügbar, so ermittelt das Script SATA-Laufwerke und Portgeschwindigkeiten.

```
Konsole
daver@raider:~ $ sudo python3 laufwerke.py

SATA-
Laufwerk     Grösse   Modell                 SATA        Speed      Port
                                             Version     Laufwerk   Speed
-------------------------------------------------------------------------------
/dev/sdd     1.8T     TOSHIBA DT01ACA2[3]    SATA 3.0    6.0Gb/s    6.0Gb/s
/dev/sdb     1.8T     ST2000VN004-2E41       SATA 3.1    6.0Gb/s    6.0Gb/s
/dev/sde     476.9G   Micron_1100_MTFD       SATA 3.2    6.0Gb/s    6.0Gb/s
/dev/sdc     1.8T     WDC WD20EZRZ-00Z       SATA 3.0    6.0Gb/s    3.0Gb/s
/dev/sda     223.6G   SanDisk Ultra II       SATA 3.2    6.0Gb/s    3.0Gb/s
```

Das Python-Script laufwerke.py: Laufwerks-ID, Größe, Modell, SATA-Version, SATA-Geschwindigkeit und tatsächliche Portgeschwindigkeit werden tabellarisch aufgelistet.

siert und die maximal unterstützte SATA-Geschwindigkeit von Laufwerken sowie die reale Anbindungsgeschwindigkeit am SATA-Port meldet.

Dieses Script hat deshalb ein paar Voraussetzungen mehr. Es verlangt nach dem Paket „smartmontools“ und weist beim Start darauf hin, falls dieses nicht installiert ist. Zudem ist zur Ausgabe aller Infos root-Recht erforderlich:

```
sudo python3 laufwerke.py
```

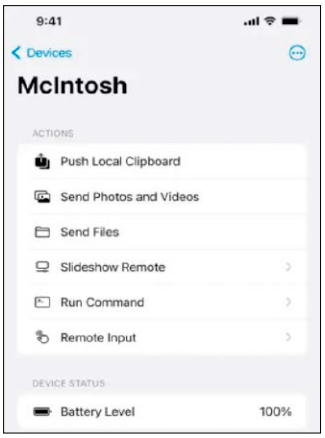
Als Benutzerkontext aufgerufen kann laufwerke.py die Geschwindigkeit von Laufwerk sowie SATA-Port nicht ermitteln und zeigt dann nur eingeschränkte Infos und einen Hinweis an.

laufwerke.sh und laufwerke.py: Terminal-Scripts zur Auflistung der SATA-Laufwerke und deren Anbindungsgeschwindigkeit, auf Heft-DVD und Download unter *https://github.com/LinuxWelt/Scripts*. **-dw**

KDE Connect: App für iOS

Einer der großen Vorzüge bei der Arbeit mit Android-Geräten ist unter anderem die KDE-Komponente KDE Connect, die auch in anderen Desktopumgebungen wie Cinnamon installierbar ist. KDE Connect ist nach monatelanger Betaphase nun auch für Apple iOS erschienen.

Das KDE-Team arbeitet seit November 2021 an einer KDE-Connect-App für iPhones und iPads. Bislang war es nötig, die App für iOS über ein Testflight-Konto zu installieren, über welches Apple Apps in Betaversionen verteilt. Das ist nicht mehr nötig, denn KDE Connect steht nun über *https://apps.apple.com/de/app/kde-connect/id1580245991* zur Installation auf iOS 14 oder höher bereit.



KDE Connect für iOS: Die Versionsnummer ist niedrig, aber die App für iOS (ab Version 14) ist der Betaphase entwachsen. Der Funktionsumfang entspricht der Android-Variante.

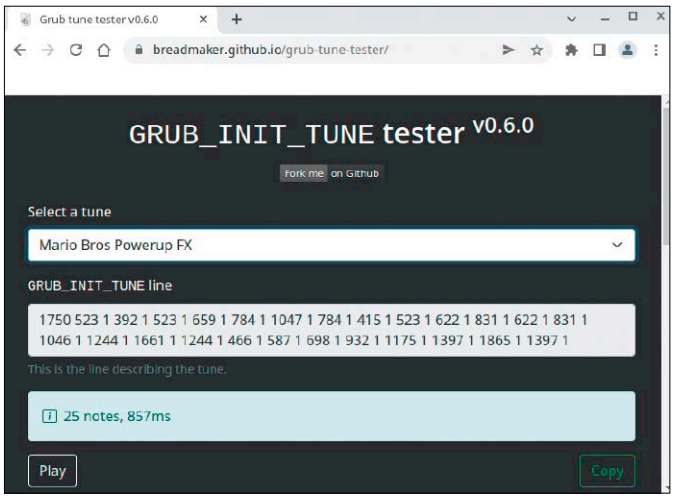
Der Funktionsumfang ist nun gleichauf mit der Version für Android und umfasst Dateiübertragung in beide Richtungen, Teilen der Zwischenablage, Eingaben auf dem iOS-Gerät für den Linux-Rechner und sogar definierbare Remotebefehle, um auf dem Linux-System Scripts oder Programme zu starten. KDE Connect für iOS ist Open Source und der Quellcode ist auf *https://invent.kde.org/network/kdeconnect-ios* öffentlich. **-dw**

Grub: Tonabfolgen beim Booten

Es kann ein Gag sein oder auch ein nützlicher akustischer Hinweis auf Linux-Systemen ohne Monitor: Grub 2 kann beim Start und der Auswahl eines Systems eine Tonabfolge über den PC-Lautsprecher abspielen. Hilfreich ist dies beispielsweise, wenn ein Rechner signalisieren soll, dass ein bestimmtes installiertes System gebootet wird.

Die Heft-DVD zu dieser Ausgabe demonstriert die Funktion in Grub 2. Bei der Auswahl des Menüs „Extras und Tools“ spielt der Bootloader die Tonfolge eines Power-ups aus dem Spielklassiker „Super Mario Bros“ ab. Die Tonabfolge haben wir nicht selbst nachgebaut, denn unter *https://breadmaker.github.io/grub-tune-tester* gibt es eine kleine Bibliothek an Grub-2-Tonabfolgen mit einer Abspielmöglichkeit im Webbrowser.

Verantwortlich für die Ansteuerung des PC-Lautsprechers ist das Statement „play“, welches als weitere Parameter eine Takt-



Soundbibliothek für Grub 2: Auf dieser Webseite stehen einige Tonsequenzen zum Einbau in den Bootloader per Kopieren und Einfügen bereit. Sie lassen sich dort auch vorab anhören.

rate erwartet (1/60 einer Sekunde), gefolgt von der Dauer eines einzelnen Tons und dessen Tonhöhe in Hertz. Dazu ein Beispiel: Die Anweisung

```
play 60 600 1
```

lässt Grub 2 einen Ton mit 600 Hertz für eine Sekunde abspielen. Um diesen Ton in eine Grub-2-Konfiguration zu übernehmen, muss eine Anweisung in die Konfigurationsdatei „/etc/default/grub“. Diese Datei öffnet man mit root-Recht (sudo) in einem Editor und trägt dort die Zeile

```
GRUB_INIT_TUNE="60 600 1"
```

in einer beliebigen neuen Zeile ein. Damit die Änderung wirksam wird, erwartet die Grub-Konfiguration eine Aktualisierung des Bootloaders:

```
sudo update-grub2
```

Bei Fedora, Open Suse und Arch Linux ist dieses Kommando erforderlich:

```
sudo grub2-mkconfig -o /
  boot/grub2/grub.cfg
```

Nun ist ein kleiner einfacher Dauerton natürlich zu langweilig für einen gut konfigurierten Linux-Rechner. Die erwähnte Github-Webseite liefert etliche Beispiele für Grub 2, die zum Kopieren und Einfügen bereitstehen. **-dw**

Blitzschlag: Gut gerüstet im Homeoffice

Sommerzeit bedeutet bei hohen Temperaturen auch immer Gewitterzeit. Ein Haus muss nicht direkt vom Blitz getroffen werden, damit die eigenen Geräte im Haus gefährlicher Überspannung ausgesetzt sind. Leidtragende wissen, dass auch Einschläge einige Häuser weiter Schäden an elektronischen Geräten, Netzteilen, Computerhardware und Netzwerktechnik verursachen können. So erging es auch dem Autor dieser Zeilen.

Die erste naheliegende Schutzmaßnahme gegen Überspannungen im Haushalt und im Büro betrifft den Stromanschluss von Geräten. Es gibt etliche Ausführungen von Zwischensteckern für etwa zehn Euro und Steckdosenleisten mit Überspannungsschutz, die zumindest dann helfen, wenn ein Blitz nicht direkt ins Gebäude oder dessen Elektroinstallation und Erdung einschlägt. Dieser Schutz hält aber nicht ewig, denn Ein-Aus-Zyklen und unbemerkte Überspannungen lassen diese Geräte im Haushalt durch elektrochemische Reaktionen am verwendeten Metalloxid-Varistor altern. Ein Steckdosenschutz, als Typ 3 „Feinschutz“ klassifiziert, gilt nach zwei bis drei Jahren Betriebszeit als nicht mehr zuverlässig.

Bei Altbauten ist darauf zu achten, dass Feinschutz ohne Grob- und Mittelschutz sowieso überfordert wäre. Auch ist ein Netzteil, extern für Drucker oder Laptop, sowie ein PC-Netzteil für den Feinschutz auch schon wirksam – schlimmstenfalls ist das Netzteil kaputt, aber nicht das damit angeschlossene Gerät. Bei integrierten Netzteilen, etwa bei Monitoren und TV-Geräten, ist ein zwischengeschalteter Feinschutz an der Steckdose empfehlenswert, denn interne Netzteile sind schwerer austauschbar.

Selbstverständlich ist es der beste Schutz bei naher Blitzentladung, die Geräte komplett vom Stromnetz zu trennen, bis das Unwetter nachlässt. Aber selbst dann ist die Elektronik, von Computern zu Smart-TV, über Router und Switch nicht sicher: Bei starken Überspannungen im Netzwerk frittiert es die Bausteine auf Hauptplatinen, in Routern, Kabelmodems und allen anderen Geräten mit Ethernet-Anschluss. Auch LANs mit Ethernet sollten also auf einen Überspannungsschutz als Feinschutz verfügen. Als weiterführende Literatur gibt es von VDE e.V. ein Papier zum Überspannungsschutz im Ethernet (*www.vde.com/de/blitzschutz/faq/ueberspannungsschutzimlan*).

Feinschutz im LAN und für DSL: Auch für Ethernet und DSL gibt es Netzwerkkabel-Kopplungen zum Überspannungsschutz, die eine galvanische Trennung herbeiführen. Diese Kopplungen sind mit jeweils zwei RJ45-Anschlüssen auf jeder Seite versehen und können auch als Verlängerungsadapter eingesetzt werden. Es gibt Überschutz-Adapter für Ethernet im Preisbereich von mehreren Hundert Euro mit hohem Überspannungsschutz für ganze Büroetagen bis hin zu kleinen Ausführungen für rund zehn Euro für den Homeoffice-Bereich von Delock (*https://tinyurl.com/46m2wme8*). Wichtig ist, die Erdung am Gehäuse dieser Adapter an einen Erdleiter anzuschließen, um Ableitstrom abzuführen. Als Erdung kann ein Kabel mit einer Lüsterklemme und ein Heizungsrohr dienen, keinesfalls aber das Gehäuse von Computern oder anderer Netzwerkhardware wie einem Switch. Nach unseren Tests mit Iperf3 verursacht der Überspannungsschutz von Delock keine Geschwindigkeitseinbußen und funktioniert auch zwischen DSL/VDSL-Anschluss und Router beziehungsweise Modem. **-dw**

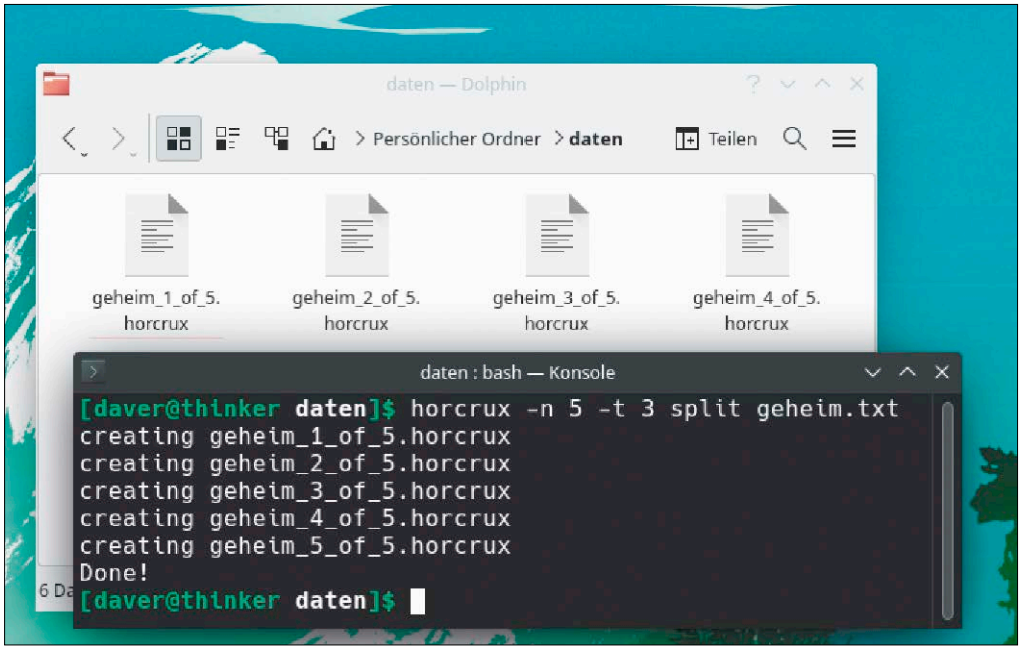
Blick ins Innere: Der Überspannungsschutz von Delock für RJ54-Verbindungen (Ethernet, DSL) ist eine galvanische Trennung. Die Lasche muss zusätzlich mit Masse verbunden werden.

Spannende Software

Die Softwaretipps sind diesmal auch ein Fundus von cleveren Tools, Programmen und Tipps, welche nach der Shell verlangen. Wie gewohnt, kommen weitverbreitete Programme wie Libre Office, Firefox und Thunderbird zum Zug.

Horcrux: Dateien teilen und zusammenfügen

In Teams kann es nötig sein, zur Wiederherstellung von Servern und Diensten eine Passwortdatenbank zu hinterlegen. Das clevere Tool Horcrux, benannt nach magischen Objekten aus der Harry-Potter-Buchserie, zerteilt dazu eine Datei in mehrere verschlüsselte Stücke. Nur wenn diese Teile mindestens teilweise wieder zusammengesetzt werden, entsteht wieder die Originaldatei. In der realen Welt arbeitete Wikileaks mit einer ähnlichen Technik, um Informationen zu teilen und nur per Mehrheit verfügbar zu machen. Das Programm ist also dafür verwendbar, eine Mindestanzahl von Teamkollegen vorzugeben, um vertrauliche Informationen wie Passwörter und Zugangsdaten abzurufen.



Zerschneiden, verschlüsseln und aus beliebigen Teilen rekonstruieren: Horcrux ist ein Tool, das Dateien in Stücke aufteilt, von welchen später nur eine Mindestanzahl benötigt wird.

Die Anzahl der mindestens notwendigen Teile ist bei Horcrux frei definierbar. Zudem enthalten die einzelnen Stücke keine verwertbaren Informationen im Klartext, sind also für sich genommen wertlos. Horcrux ist auch dazu geeignet, eine vertrauliche Datei in Teilen für den Notfall in verschiedenen Clouddiensten zu speichern. Ein Vorteil von Horcrux ist dabei, dass es plattformübergreifend für Linux, Windows und Mac-OS zur Verfügung steht.

Es handelt sich um ein Kommandozeilentool. Unter Linux muss es für x86-Hardware (32 und 64 Bit) sowie ARM nicht extra kompiliert werden, denn auf der Webseite des Entwicklers stehen fertige Binarys zum Download bereit (*https://github.com/jesseduffield/horcrux/releases*). Nach dem Herunterladen entpackt der Befehl

```
tar xzvf horcrux_0.2_
  Linux_x86_64.tar.gz
```

das Archiv und die enthaltene Binary, die anschließend mit den beiden Kommandos

```
mkdir -p ~/.local/bin/
mv horcrux ~/.local/bin/
```

in das benutzerspezifische Verzeichnis für ausführbare Programme in der Shell verschoben wird. Nun ist das Tool in jedem beliebigen Ordner aufrufbar. Um eine Datei wie „geheim.txt“ aufzuteilen, genügt der Aufruf

```
horcrux -n 5 -t 3 split
  geheim.txt
```

um fünf Teile zu erzeugen, von welchen mindestens drei notwendig sind, um die Datei wiederherzustellen. Diese Mindestzahl ist optional und kann auch identisch mit der Menge der Einzelteile gleichgesetzt werden. Horcrux erstellt nun die Dateistücke als „[name]_1_of_5.horcrux“. Um später die Originaldatei aus den Teilen zu restaurieren, kopiert man diese wieder in einen Ordner und führt dort

```
horcrux bind .
```

aus, wobei sich das Tool die einzelnen Stücke selbst zusammensucht und das Ergebnis in das gleiche Verzeichnis schreibt. Statt dem Punkt, der für das aktuelle Verzeichnis steht, kann auch ein anderer Pfad angegeben werden.

Horcrux 0.2: Kryptografisches Tool zum Aufteilen und Zusammenfügen von Dateien, Open Source, Download von Binarys unter *https://github.com/jesseduffield/horcrux* (900 KB). **-dw**

Exifcleaner: Metadaten entfernen

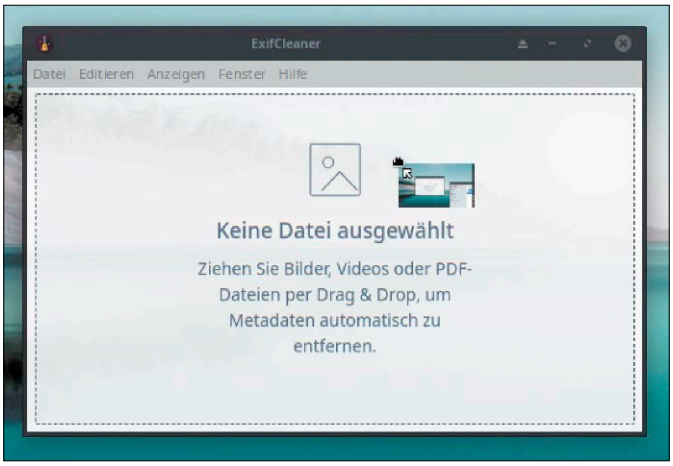
Versteckte Header- und Metadaten in Bilddateien und Dokumenten können dabei helfen, Ordnung zu schaffen und große Datenmengen nach Filtern zu sortieren oder zu durchsuchen. Gleichzeitig verraten Metadaten etwa bei Bildern auch eine Menge über Autor, Ort und Zeit einer Fotoaufnahme.

Das grafische Tool Exifcleaner (*https://exifcleaner.com*) entfernt Metadaten und Exif-Header von Bilddateien, von Videos und von PDF-Dateien. Es kann nicht nur einzelne Dateien säubern, sondern erlaubt auch die Auswahl mehrerer Dateien oder ganzer Ordner. Die Installation unter Linux ist nicht schwer, denn es gibt den Exifcleaner als universelles Appimage auf der Entwickler-Webseite *https://github.com/szTheory/exifcleaner/releases* zum Download, außerdem als RPM- und DEB-Paket. Neben Linux werden auch Windows und Mac-OS unterstützt. Es handelt sich um eine Electron-Anwendung, die eine Portierung sehr einfach macht, aber auch sehr groß ist.

Nach dem Download unter Installation des Pakets, das in Ubuntu und Debian beispielsweise mittels

```
sudo apt install ./
  [paket].deb
```

flott installiert ist, kann der Exifcleaner über das Anwendungsmenü oder die Gnome-Übersichtsseite gestartet werden. Das Programmfenster nimmt als Ziel per Drag & Drop Dateien oder Ordner auf. Ein Entfernen von Metadaten erfolgt umgehend, ohne weitere Bestätigung, und es wird lediglich die Zahl der bearbeiteten Dateien angezeigt.



Bilddateien, Videos und PDFs säubern: Der Exifcleaner entfernt Metadaten und Exif-Header von Bilddateien, damit diese Dateien nichts mehr über Herkunft, Ort, Zeit verraten.

Exifcleaner 3.6: Grafisches Open-Source-Programm zum Entfernen von Metadaten aus Bilddateien, Videos und PDFs, Download für Linux, Windows und Mac-OS unter *https://github.com/szTheory/exifcleaner* (70 MB bis 100 MB). **-dw**

Firefox: Lesezeichen prüfen

Wenn Firefox die Synchronisationsfunktion nutzt, kommen über die Jahre unüberschaubar viele Lesezeichen zusammen. Viele funktionieren nach längerer Zeit nicht mehr oder sind uninteressant geworden. Die Erweiterung „Keep or Delete Bookmarks" kann Firefox-Lesezeichen automatisch überprüfen. Es ist eine Hilfe, zwischendurch und in Arbeitspausen Lesezeichen zu sichten und auszusortieren.

Die nun vorliegende Version 2 des Add-ons legt Anwendern alle bemängelten Lesezeichen zum Gegencheck vor und macht das systematische Durchgehen durch eine bessere Tastatursteuerung deutlich flotter. Zudem gibt es eine Funktion, bereits übersprungene Lesezeichen nochmals anzuzeigen.

Wie die meisten Add-ons gibt es „Keep or Delete Bookmarks" über die offizielle Erweiterungs-Webseite (*https://addons.mozilla.org/de/firefox/addon/keep-or-delete-bookmarks*) zur Installation in Firefox.

Oben rechts zeigt sich dann ein neues Symbol, das die Lesezeichendurchsicht im Browserfenster in einem neuen Tab startet. Die Erweiterung zeigt immer ein zufälliges Lesezeichen an, überprüft, ob es auf eine noch existierende Webseite zeigt, und bietet drei Aktionen an:

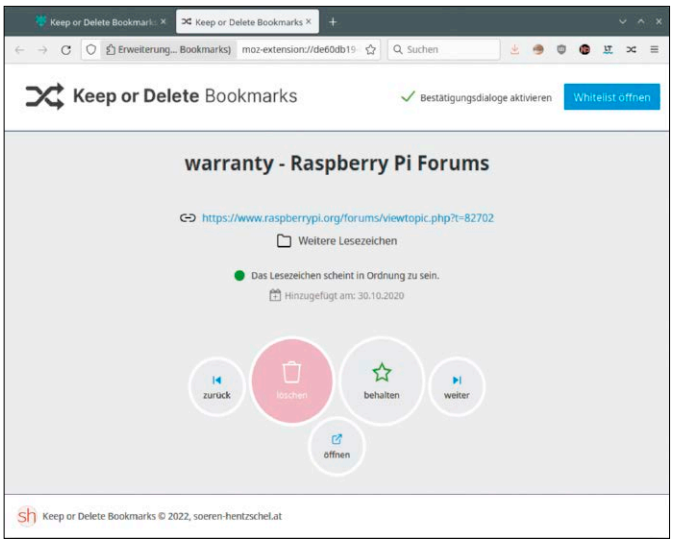
1. Lesezeichen löschen – dies löscht den Eintrag augenblicklich aus dem Bookmarks-Ordner, was sich nicht rückgängig machen lässt.

2. Lesezeichen explizit behalten – es wird zu einer Whitelist hinzufügt und die Erweiterung wird für dieses Lesezeichen nicht mehr nachfragen, ob man es behalten oder löschen will.

3. Weiterspringen – den Status des Lesezeichens ohne Änderung beibehalten und zum nächsten springen.

Keep or Delete Bookmarks 2.0: Systematischer, semi-automatischer Check für Lesezeichen in Firefox.

Installation unter *https://addons.mozilla.org/de/firefox/addon/keep-or-delete-bookmarks*. **-dw**



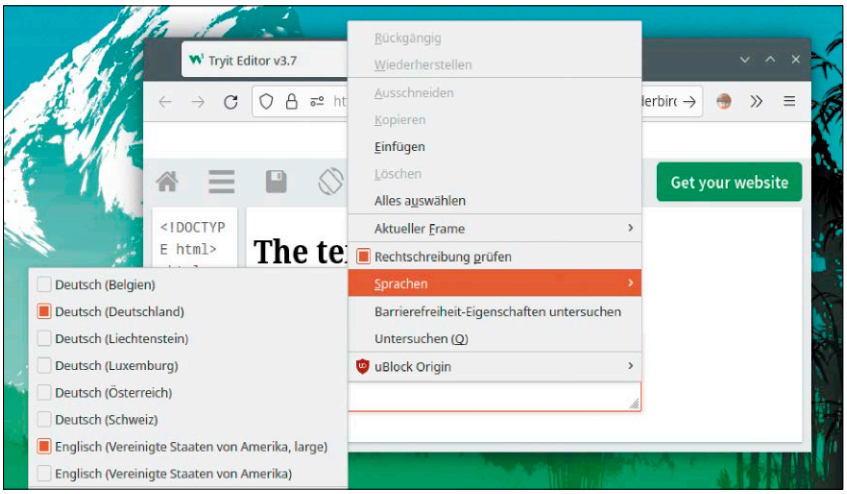
Lesezeichen-Check: Diese Erweiterung prüft die Firefox-Lesezeichen durch automatische Verbindungstests.

Firefox: Mehrere Spellchecker verwenden

Viele Anwender schreiben im Web in mehreren Sprachen. Eine lange angefragte Komfortfunktion für Firefox war deshalb die Möglichkeit, mehrere Sprachen für die eingebaute Rechtschreibprüfung gleichzeitig zu nutzen.

Ab Firefox-Version 100 funktioniert es endlich, mehrere der installierten Sprachen gleichzeitig in der Rechtschreibprüfung zu aktivieren. Generell ist dann eine multilinguale, gleichzeitige Prüfung auch in gemischten Texten möglich. Klar, dabei kann es bei Groß- und Kleinschreibung zu Konflikten kommen, aber zumindest grobe Fehler sind gut sichtbar. Und so macht man Firefox zum Sprachtalent:

1. In einem beliebigen Eingabefeld auf einer Webseite klickt man mit der rechten Maustaste auf den zu prüfenden Text und aktiviert dann im Kontextmenü die Option „Rechtschreibung prüfen".



Multilinguales Sprachtalent: Firefox 100 liefert nach vier Jahren Diskussion die angefragte Rechtschreibprüfung in mehreren Sprachen.

2. Beim erneuten Aufruf dieses Kontextmenüs zeigt sich ein neues ausklappendes Untermenü namens „Sprachen". Dort erscheinen alle installierten Wörterbücher in einer Liste, die per Checkbox aktivierbar sind (siehe Abbildung oben).

3. Die ausgewählten Sprachen bleiben aktiviert, aber nur auf der gleichen Webseite und im jeweiligen Eingabefeld. Werden weitere Sprachen benötigt, so gibt es nach einem Rechtsklick im Kontextmenü über „Sprachen → Wörterbücher hinzufügen" eine Abkürzung zur Installation weiterer Sprachen.

Übrigens: Auch das beliebte „Languagetool" (*https://addons.mozilla.org/de/firefox/addon/languagetool*) gibt es als Browsererweiterung. Es unterstützt ebenfalls mehrere Sprachen und hat sogar eine Option „Muttersprache", welche vor häufigen Verwechslungen ähnlicher Wörter zwischen Sprachen warnt. Diese kostenlose Rechtschreibprüfung geht dabei allerdings über den Server des Anbieters – die Language-Tooler GmbH aus Potsdam. **-dw**

Ubuntu: Übereifriger Programmkiller

Eine nicht gut gelungene Neuerung in Ubuntu 22.04 & Co. ist die Behandlung von Situationen mit knappem Arbeitsspeicher. Sind RAM und Swap ausgereizt, bleibt ein Linux-System gnadenlos stehen – im Falle von Servern gilt es das unbedingt zu vermeiden. In diesen Situationen schickt Ubuntu 22.04 den Programmkiller Systemd-Oomd los, der Benutzerprogramme rigoros abschießt.

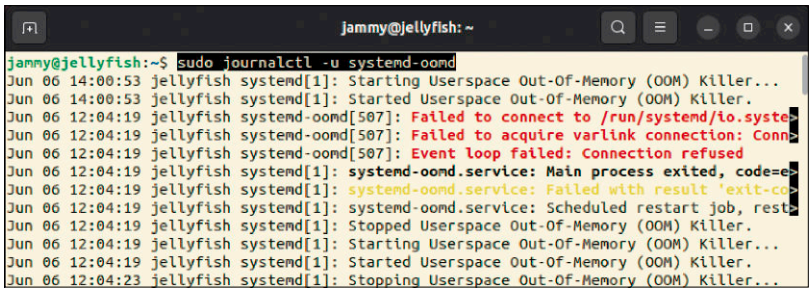
In Ubuntu 22.04 sind die Voreinstellungen von Systemd-Oomd zu aggressiv. Auf Rechnern mit weniger als acht GB RAM passiert es deshalb zu häufig, dass Programme wie Firefox und Libre Office unvermittelt beendet werden, obwohl sogar noch Arbeitsspeicher und Swap verfügbar wären.

Dieses Verhalten Ubuntus wird auf dem Bugtracker der Distribution gerade eifrig diskutiert (*https://bugs.launchpad.net/ubuntu/+source/systemd/+bug/1972159*). Um das Verhalten nach dem unvermittelten Ende von Anwendungen zurückzuverfolgen, dient folgender Befehl im Terminal:

```
sudo journalctl -u
  systemd-oomd
```

Es listet die letzten Aktionen des Programmkillers auf.

Eine Lösung durch ein verteiltes Update steht noch aus. Die Lösung wird sein, die Voreinstellungen von Systemd-Oomd so weit zu lockern, dass Anwender nicht zu früh ihre Programme am Desktop verlieren – und schlimmstenfalls ungesicherte Arbeiten dazu. Bis diese Fehlerbehebung erscheint, kann man aber auch sofort Abhilfe schaffen. Ein gangbarer Weg, knappe Speichersituationen zu entschärfen, ist die Vergrößerung des Auslagerungsbereichs, der auf den meisten Installationen auf lediglich ein GB dimensioniert ist. Eine großzügigere Swapdatei bedeutet nicht, dass Ubuntu dann häufiger ausla-



Systemd-Oomd und seine Killerkommandos: Der Blick in die Aufzeichnungen von Journald zeigen, ob das System Programme aufgrund von (vermeintlich) knappem Speicher beendet hat.

gert. Sie nimmt aber den Druck von den Systemressourcen, Systemd-Oomd anzustoßen. Eine zweite Lösung, geeignet für Rechner mit wenig RAM, aber flotter CPU, ist die Aktivierung von Zram, das einen Teil des Arbeitsspeichers als komprimierte Auslagerungsdatei bereitstellt und damit ebenfalls Situationen mit knappem Speicher entschärft.

Mehr Swap: Um die Auslagerungsdatei auf vier GB zu vergrößern, genügen vier Befehle im Terminal. Zuerst deaktiviert

```
sudo swapoff /swapfile
```

die aktuelle Swapdatei und

```
sudo fallocate -l 4G /
  swapfile
```

erstellt an der gleichen Stelle eine größere. Nun legen diese beiden Kommandos

```
sudo mkswap /swapfile
```

```
sudo chmod 600 /swapfile
```

das Dateiformat und die korrekten Zugriffsrechte fest. Abschließend aktiviert

```
sudo swapon /swapfile
```

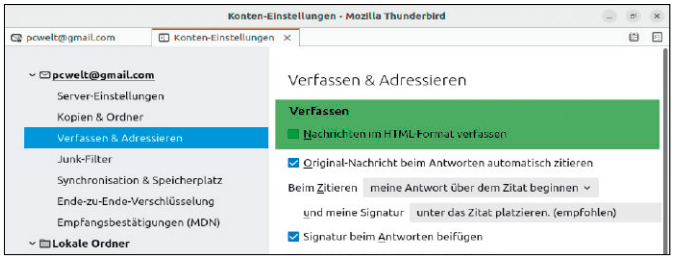
die neue Auslagerungsdatei ohne Neustart.

Komprimiertes Swap: In Ubuntu ist es vergleichsweise einfach, den gepackten Auslagerungsbereich im RAM über Zram zu aktivieren. Denn ein Paket in den Standard-Paketquellen installiert alle Komponenten, liefert eine sinnvolle Konfiguration mit und aktiviert auch gleich den benötigten Systemd-Dienst für Zram. Alles das ist mit dem Befehl

```
sudo apt-get install zram-
  config
```

erledigt. Der Preis dieser maßnahme ist eine leicht erhöhte CPU-Auslastung. **-dw**

Thunderbird: Keine HTML-Mails verfassen



HTML gilt nicht nur auf Mailinglisten als schlechtes Benehmen: HTML-Mails sorgen durch Inkompatibilität mit anderen Mailprogrammen oft für Ärger.

Mails mit Formatierungen bedienen sich HTML-Tags, um dann in anderen Mailprogrammen und Webdiensten mit HTML-Renderer wieder fast wie im Originalformat zu erscheinen. Auf Mailinglisten ist dies jedoch verpönt, da HTML-Tags zu viele Probleme verursachen. Auch bei der Weiterverarbeitung von Mails, etwa beim Weiterleiten und Zitieren, macht HTML mehr Ärger, als es die HTML-Optik wert ist. Generell gilt es als guter Stil, Mails nur im puren Textformat zu versenden, denn dies funktioniert überall.

Auf vielen Mailinglisten ist das sogar Pflicht: HTML-Mails ziehen Beschwerden aus der Gruppe oder sogar einen Ausschluss nach sich. In Thunderbird ist die Option, HTML-Mails zu versenden, pro Konto einstellbar: Nach Alt-Taste zum Einblenden des Hauptmenüs und „Extras → Konteneinstellungen“ ist die oberste Option „Nachrichten im HTML-Format verfassen“ per Klickbox zu deaktivieren. **-dw**

Libre Office: Hängende Fenster und Cursor

Welches grafische Toolkit ist aktiv? Hier zeigt Libre Office an, welche „Visual Component Library“ (VLC) für Menüelemente verwendet werden. Ausgereift sind derzeit nur GTK2 und GTK3.

Die freie Office-Suite hat mittlerweile mehrere Schnittstellen für verschiedene Oberflächen, um in Gnome sowie in KDE Plasma passende grafische Elemente anzuzeigen. Die Qt-Schnittstelle für KDE ist aber noch nicht mit GTK3 für Gnome gleichauf. Im Alltag macht Libre Office mit Qt noch Probleme.

Ärgerliche Szenarien mit Libre Office unter KDE sind nicht mehr reagierende Editorfenster und hängende Eingabecursor. Erst mehrere Klicks auf andere Programme und der Gang zurück in ein Libre-Office-Fenster haucht diesem wieder Leben ein. Auf diese Weise kann man nicht ungestört arbeiten. Es empfiehlt sich daher, auch unter KDE die GTK3-Oberfläche von Libre Office zu nutzen, bis die aktuellen Probleme behoben sind. Zunächst muss dazu das Paket „libreoffice-kf5“ deinstalliert werden, was in Ubuntu und Co. mittels

```
sudo apt remove
  libreoffice-kf5
```

im Terminal gelingt. Dann installiert der Befehl

```
sudo libreoffice-gtk3
```

das Toolkit GTK3 für Libre Office. Dieses Paket ist mit dem gleichen Namen in den Standard-Paketquellen der anderen Linux-Distributionen. Beim nächsten Start wählt Libre Office automatisch dieses Toolkit. In Arch Linux und Manjaro kommt es vor, dass Libre Office stattdessen das generisch X11-Toolkit wählt, das sehr unansehnlich und altmodisch ist. In diesem Fall ist es nötig, Libre Office mit einer Umgebungsvariablen auszustatten, welche die verwendete Oberfläche erzwingt. Dazu erstellt man mit

```
sudo nano /etc/profile.d/
  libreoffice.sh
```

eine neue Script-Datei mit einem Texteditor wie Nano und gibt dieser folgenden Inhalt:

```
export SAL_USE_
  VCLPLUGIN=gtk3
```

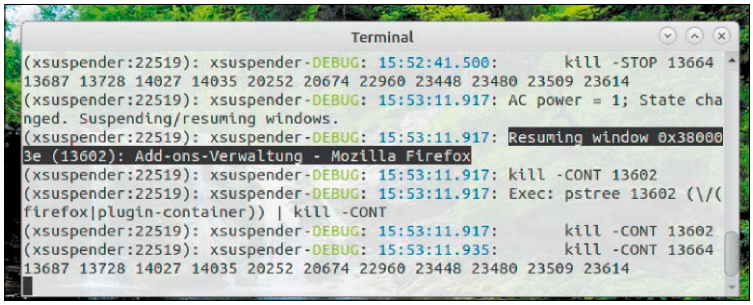
Es ist nicht notwendig, die Datei ausführbar zu machen. Ab der nächsten Anmeldung nutzt Libre Office stets GTK3 als Toolkit, auch unter KDE Plasma. Die Info „Hilfe → Über LibreOffice“ im Menü des Büroprogramms zeigt in der Zeile „Benutzeroberfläche“ das verwendete Toolkit an. **-dw**

Idealer Desktop

Eine Notizanwendung für Linux Mint leistet auch in anderen aktuellen Ubuntu-Systemen gute Dienste. Und auf Systemen mit schmaler Hardwareausstattung kann der Wächter Xsuspender im Hintergrund die gerade nicht benötigten Anwendungen anhalten.

Xsuspender: Anwendungen pausieren

Laufende Programme belegen Systemressourcen, auch wenn sie auf der grafischen Arbeitsfläche aktuell nicht im Vordergrund stehen. Auf Desktop-PCs fällt dies kaum ins Gewicht, aber auf Laptops machen sich die dabei genutzten CPU-Zyklen durch reduzierte Akkulaufzeit bemerkbar. Das Tool Xsuspender entzieht Programmen ohne Fokus diese Ressourcen und hält einen Prozess damit effektiv an.



Stoppen und bei Bedarf wieder in Gang setzen: Xsuspender nutzt Signale des Linux-Kernels, um grafische Anwendungen im Hintergrund anzuhalten, wenn diese aktuell nicht gebraucht werden.

Xsuspender funktioniert bislang nur unter Xorg. Wayland, unter Gnome und bei einigen Linux-Distributionen schon Standard, erlaubt das Anhalten von grafischen Anwendungen per „SIGSTOP"-Signal nicht. Die hier vorgestellte Lösung von Xsuspender (*https://kernc.github.io/xsuspender*) eignet sich also nur bei Desktops, die mit dem herkömmlichen Xorg laufen. Dies ist auch bei Ubuntu 22.04 noch eine Option, die auf der Anmeldeseite zur Verfügung steht. Zur Installation von Xsuspender gibt es auf der Github-Webseite des Projekts fertige Pakete für Debian, Ubuntu, Raspberry-Pi-OS und Arch Linux.

Das angebotene DEB-Paket für Ubuntu ist laut Entwickler für die Version 21.10 gemacht, funktioniert aber auch im neuesten Ubuntu 22.04. Es ist nach dem Download mittels

```
sudo apt install ./xsuspender_1.3-1_amd64.deb
```

installierbar. Die Konfiguration erfolgt über eine Textdatei, deren Syntax unter „Manual" auf der Projektwebseite unter *https://kernc.github.io/xsuspender/xsuspender.1.html* erklärt ist. Dazu gibt es auch eine mitgelieferte Beispielkonfiguration mit vielen vordefinierten Programmen, die nach einer kleinen Anpassung einsatzbereit ist.

1. In der Konfigurationsdatei steht, welche Anwendungen Xsuspender nach wie vielen Sekunden anhalten soll, wenn sie im Hintergrund sind. Eine übliche Zeit dafür sind zehn Sekunden. Die Identifizierung einer Anwendung erfolgt über deren Fensterklassen-Titel und nicht über den Programmnamen. So kann Xsuspender auch wirklich nur jene Programme pausieren, deren Fenster alle im Hintergrund sind.

Die Beispielkonfiguration wird mit dem Kommando

```
cp /usr/share/doc/xsuspender/examples/xsuspender.conf ~/.config/
```

durch Umkopieren in den Ordner „.config" im Home-Verzeichnis aktiv geschaltet.

2. Mit Chromium ist Xsuspender jetzt schon einsatzbereit. Damit auch Firefox angehalten wird, ist eine kleine Korrektur der Konfiguration in der Datei „~/.config/xsuspender.conf" notwendig: Unterhalb des Eintrags „[Firefox]" muss die Zeile

```
match_wm_class_group_contains = Firefox
```

auf

```
match_wm_class_group_contains = firefox
```

geändert werden, da hier die Großschreibung der Fensterklasse nicht korrekt ist.

3. Die Konfigurationsdatei enthält weitere Einträge für Chromium, Virtualbox und Clementine. Mit diesen Informationen können Sie auch Programme auf eigene Faust hinzufügen.

4. Einen ersten Test, ob die Konfiguration korrekt funktioniert, zeigt dann dieser Befehl:

```
G_MESSAGES_DEBUG=xsuspender xsuspender
```

Jetzt berichtet Xsuspender detailliert über die eigenen Aktionen. Ist nun beispielsweise Firefox oder Chromium länger als zehn Sekunden im Hintergrund oder minimiert, so wird Xsuspender die Meldung „kill -STOP" und deren Prozess-ID als Aktion melden und bei einer Reaktivierung des Fensters ein „kill -CONT", um die Anwendung wieder in Gang zu setzen.

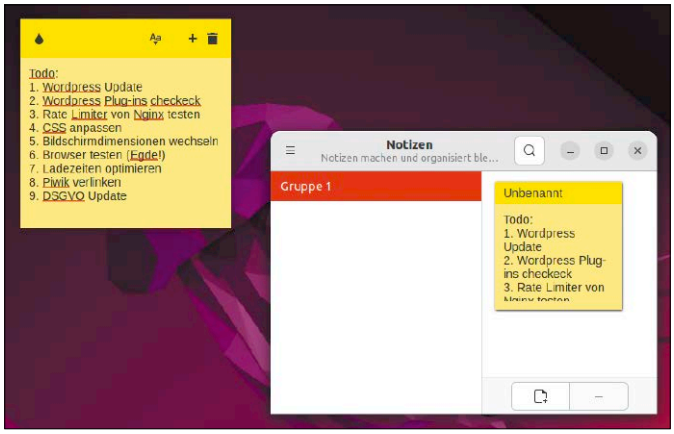
5. Funktioniert alles, so ist Xsuspender auch als automatisch gestartetes Programm schnell eingerichtet.

Es gibt dafür eine Vorlage, die das Kommando

```
cp /etc/xdg/autostart/xsuspender.desktop ~/.config/autostart/
```

in den richtigen Ordner kopiert. Nun muss die Datei „~/.config/autostart/xsuspender.desktop" noch mit einem Texteditor geöffnet werden, um die Zeile „Hidden=true" auf „Hidden=false" zu ändern. Damit wird Xsuspender ab der nächsten Anmeldung im Hintergrund gestartet. **-dw**

Sticky: Klebezettel für alle Desktops



Zettel auf den Desktop kleben: Die Anwendung Sticky von Linux Mint ist mit wenig Aufwand auch in Ubuntu und Varianten installierbar. In Gnome funktioniert sie auch unter Wayland.

Als permanente Zwischenablage für Textnotizen, die auch einen Neustart übersteht, legen viele Anwender Textdateien auf dem Desktop an, die bei der nächsten Anmeldung gleich ins Auge fallen. Andere Desktopumgebungen wie KDE Plasma und Gnome (mit Erweiterung) bieten eigene Post-it-Notizen direkt für den Desktophintergrund. Von Linux Mint stammt eine Anwendung, die auch in Ubuntu und seinen Varianten auf jedem Desktop gut funktioniert.

Das Tool von Linux Mint ist einfach aus einem PPA (externes Repository) zu installieren und läuft in Gnome auch schon unter Wayland ohne Probleme. Zur ersten Installation nimmt in einem Terminalfenster die Eingabe von

```
sudo add-apt-repository
 ppa:kelebek333/mint-
 tools
```

die Quelle auf. Ignorieren kann man dabei noch einmal die Warnung in Ubuntu 22.04, dass die Methode zur Aufnahme des Signaturschlüssel nicht mehr zeitgemäß sei. Die Befehle

```
sudo apt update
sudo apt install sticky
```

installieren die Anwendung dann aus dem PPA.

Über das Anwendungsmenü startet Sticky das Notizprogramm mit dessen Hauptfenster zum Anlegen neuer Notizen und zu deren Organisation in Gruppen. Rechts oben im Menü hinter dem Symbol mit drei horizontalen Strichen gibt es mit „Einstellungen → Automatischer Start“ auch gleich eine Möglichkeit, das Programm beim Log-in auszuführen und damit alle Notizen wieder anzuzeigen.

Unter „Notizen“ sind noch die Standardgröße und die vorgegebene Farbe der Haftzettel einstellbar. **-dw**

Gnome: Hintergrund der Anmeldung

Zusammen mit Gnome 3 erschien auch GDM3 („Gnome Display Manager“) in einer komplett neuen Version. Displaymanager sind bekanntlich die Anmeldefenster für den grafischen Desktop. GDM3 hat Funktionalität entfernt und präsentiert sich eher schlicht. Wie für Gnome typisch, gibt es über die Desktopumgebung auch keine Möglichkeit mehr, das Aussehen von GDM3 anzupassen. Der Displaymanager hat ein Gewand bekommen, das in Konfigurationsdateien festgelegt ist und zum restlichen Gnome-Desktop einer Linux-Distribution passen soll.

GDM3 bezieht sein vordefiniertes Aussehen aus Dateien unter „/etc/gdm3“ sowie „/var/lib/gdm3/.config“. Deren manuelle Anpassung ist wenig angenehm. Leichter geht es mit dem Konfigurations-Script von *https://github.com/realmazharhussain/gdm-tools*, welches zumindest den Hintergrund der Anmeldung auf ein gewünschtes Bild festlegen kann. Das Script verlangt ein paar Kommandozeilentools, die in Debian/Ubuntu im Terminal mit

```
sudo apt install wget
 libglib2.0-dev dconf-cli
```

schnell nachgerüstet sind. Anschließend holt das Kommando

```
wget https://github.com/
 realmazharhussain/gdm-
 tools/archive/refs/
 heads/main.zip
```

das Archiv ab, welches dann der folgende Befehl

```
unzip main.zip
```

entpackt. Weiter geht es dann mit dem Wechsel in das neu angelegte Verzeichnis

```
cd gdm-tools-main
```

und dem Aufruf des Installations-Scripts:

```
./install.sh
```

Das Script fordert sudo-Recht, um alles nach „/usr/local“ zu kopieren. Nun kann der Aufruf

```
set-gdm-theme -s default
 ~/beispiel.jpg
```

das Bild „beispiel.jpg“ im eigenen Home-Verzeichnis als Hintergrundbild für GDM3 einrichten. Statt eines Hintergrundbildes ist auch die Vergabe einer durchgehenden Hintergrundfarbe als hexadezimaler RGB-Wert möglich:

```
set-gdm-theme -s
 --background '#3e5164'
```

Eine Rückkehr zum Standard ist ebenfalls einfach und mit dem Aufruf

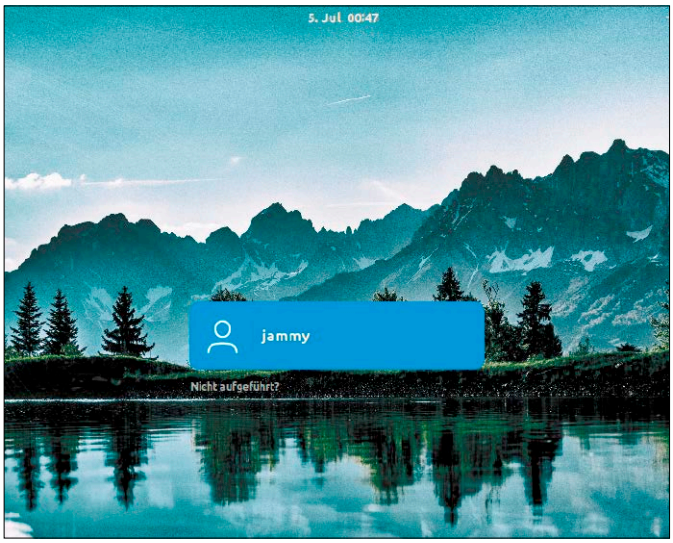
```
set-gdm-theme -r
```

erledigt.

Soll das Script gar nicht mehr auf dem System sein, so entfernt es der Aufruf der Deinstallationsroutine mit

```
./uninstall.sh
```

wieder. Das Uninstall-Script liegt im Ordner der zuvor entpackten Dateien. **-dw**



Andere Ansichten: Die Anmeldeseite von GDM3 ist mit Hilfe eines Scripts leichter anpassbar. Ein selbst gewähltes Bild oder eine durchgehende Farbe ist damit schnell auf den Hintergrund tapeziert.

Gnome: Ein winziges Dock

Das Dock in Gnome unter Ubuntu macht ein Umschalten zwischen laufenden Anwendungen und den Start von Favoriten viel einfacher. Eine platzsparende Alternative, die alles im oberen Panel unterbringt, ist nun als Gnome-Erweiterung verfügbar.

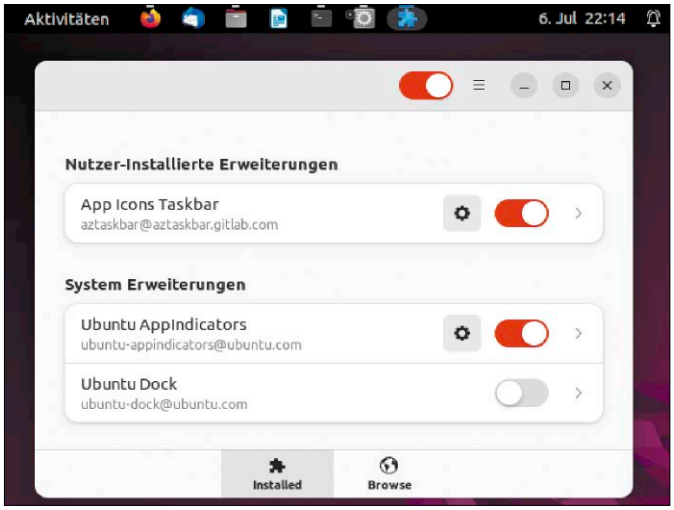
Die Erweiterung App Icons Taskbar greift die Idee des Docks auf, zeigt Favoriten und laufende Programme als Symbol – dies alles in der Systemleiste von Gnome.

Die Einrichtung erfolgt in Linux-Distributionen wie Fedora, Manjaro, Arch Linux und anderen über die Webseite der Gnome-Erweiterungen (*https://extensions.gnome.org/extension/4944/app-icons-taskbar*) über Firefox mit einem Klick auf den angezeigten Schalter. In Ubuntu funktioniert das im Snap-Paket von Firefox nicht mehr, da der Browser keinen Zugriff auf das Verzeichnis der lokalen Gnome-Erweiterungen hat. Hier hilft der neue Gnome Extension Manager, der mit

```
sudo apt install gnome-
  shell-extension-manager
```

zu installieren ist. Unter „Browse“ ist das Verzeichnis der Erweiterungen durchsuchbar und der gesuchte Kandidat „App Icons Taskbar“ mit wenigen Klicks installiert.

Im Menü „Installed“ aktiviert oben der Kippschalter die Verwaltung der Shell-Extension, kann dann die neue Erweiterung einschalten und ferner das vorhandene „Ubuntu Dock“ deaktivieren. **-dw**

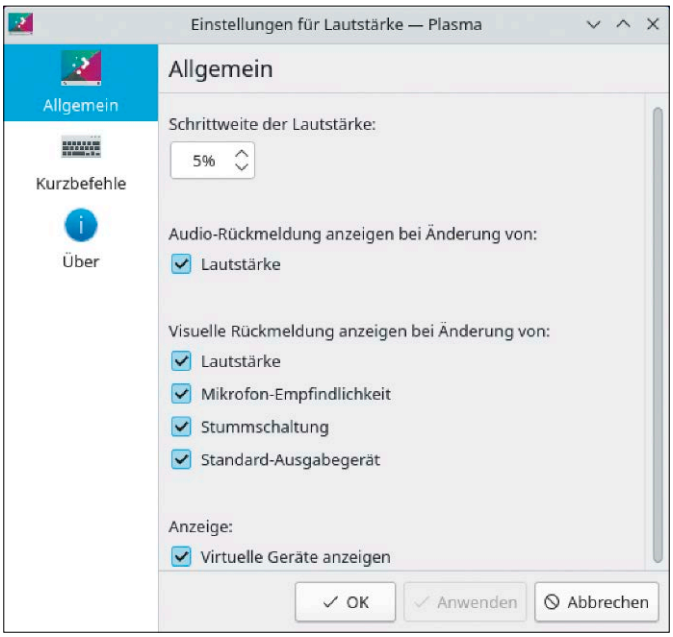


Kleine Symbole statt großes Dock: Die Gnome-Erweiterung App Icons Taskbar ist dem Ubuntu-Dock ähnlich, braucht aber nur wenig Platz und arbeitet auch mit dem Arc Menu zusammen.

KDE Plasma: Alle Audioausgänge anzeigen

Pulse Audio und Pipewire unterstützen als Soundserver die gleichzeitige Ausgabe über mehrere Geräte, ferner virtuelle Audioports, um beispielsweise Streams vom lokalen Rechner mitzuschneiden. Diese virtuellen Ein- und Ausgänge sind nicht nur über das Extratool Pavucontrol sichtbar, sondern auch im Mixer von KDE Plasma.

Die erweiterte Ansicht muss aber zunächst aktiviert werden: Ein Rechtsklick auf das Lautsprechersymbol im KDE-Panel öffnet den Dialog „Lautstärke einrichten“. Unter „Allgemein“ gibt es dann ab KDE Plasma 5.24 die zusätzliche Option „Anzeige: Virtuelle Geräte anzeigen“, welche alle Regler von Pulse Audio und Pipewire einblendet. **-dw**



Wo sind alle Ein- und Ausgabeports? In den neueren Ausgaben von KDE Plasma kann die Lautstärkeregelung virtuelle Geräte von Pulse Audio und Pipewire anzeigen.

XFCE: Clipboard per Klick

Auf Linux-Desktops sind Clipboardmanager wichtig, denn unter Linux ist der Inhalt der Zwischenablage ein vergängliches Gut. Wird ein Programm geschlossen, ist auch der kopierte Inhalt in der Zwischenablage weg. Zwar funktionieren auch die Programm Clipit und Copy Q unter XFCE, für diesen Desktop gibt es aber mit Clipman auch eine maßgeschneiderte und gut konfigurierbare Lösung.

Clipman läuft nur unter XFCE und unterhält eine Liste der letzten Clipboardinhalte, die nicht nur über einen Eintrag in der XFCE-Leiste abrufbar sind. Die Liste ist auch per Mausklick abrufbar, was die Bedienung des Clipboardmanagers sehr flott gestaltet. So klappt die Einrichtung: Das Paket ist in allen Linux-Distributionen zur Installation verfügbar, die XFCE im Angebot haben, und in Debian/Xubuntu mit

```
sudo apt install xfce4-
  clipman-plugin
```

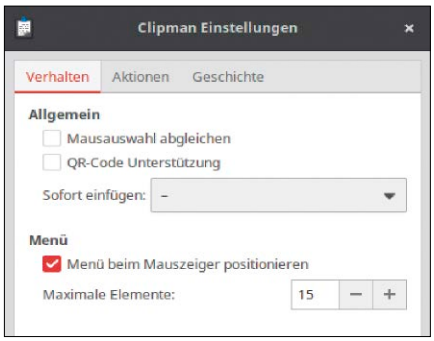
schnell eingerichtet. Clipman muss zunächst manuell gestartet werden. Im Menü ist es unter dem Namen „Zwischenablageverwaltung“ vertreten und zeigt sich nach einem Aufruf in der XFCE-Leiste. Dort geht es nach einem Rechtsklick auf dessen Symbol in das Untermenü „Eigenschaften → Verhalten“ und dort auf die Option „Menü beim Mauszeiger positionieren“.

Nun fehlt noch eine griffige Tastenkombination, um das ausklappende Menü von Clipman bei Bedarf einfach aufzurufen.

Die Vergabe von Tasten erfolgt über das Menü „Einstellungen → Tastatur → Tastenkürzel für Anwendungen“. Ganz unten fügt die Option „Hinzufügen“ einen neuen Eintrag hinzu, der im Feld „Befehl“ diesen Aufruf erhält:

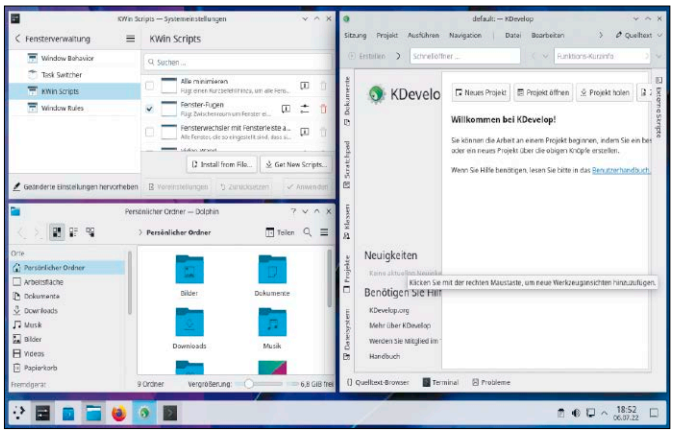
```
xfce4-popup-clipman
```

Im nächsten Dialog „Tastenkürzel für Befehl“ wird dann die gewünschte Tastenkombination gedrückt, beispielsweise die Windows-Taste (Super-Taste) und C. Nach einem Klick auf „Schließen“ ist die Abkürzung aktiv und der festgelegte Hotkey zeigt neben dem Mauszeiger das Auswahlmenü von Clipman mit allen Inhalten an, um sie in der aktuellen Anwendung einzufügen. **-dw**



Verlauf der Zwischenablage per Tastendruck: Der Clipman von XFCE ist auch per Tastenkombination aufrufbar. Diese Option platziert den Dialog direkt am Mauszeiger.

KDE Plasma: Fenster durch Abstände hervorheben



Elegante Zwischenräume: Für hohe Auflösungen ist diese Modifikation des KDE-Compositors Kwin vorteilhaft, die zwischen Fenstern automatisch Abstände setzt.

Entwickler, Linux-Admins, aber auch Grafiker haben meist eine Menge Fenster gleichzeitig auf dem Bildschirm. Bei großen Bildschirmen und hohen Auflösungen bietet die KDE-Erweiterung Window Gaps eine optische Trennung durch einen vordefinierten Abstand zwischen Programmfenstern.

Diese Erweiterung arbeitet perfekt mit dem neuen, eleganten schwebenden Panel von KDE Plasma 5.25 zusammen, das im Juni 2022 erschienen und schon in der KDE Neon User Edition verfügbar ist (*https://neon.kde.org/download*). Auch für Arch Linux und Manjaro liegt schon ein Update vor. Die Einrichtung der KDE-Erweiterung, die als Script für den Compositor Kwin umgesetzt ist, ist über die Github-Webseite des Entwicklers schnell erledigt. Erst holt

```
git clone https://github.com/nclarius/tile-gaps.git
```

die benötigten Dateien und die beiden Kommandos

```
cd tile-gaps
./install.sh
```

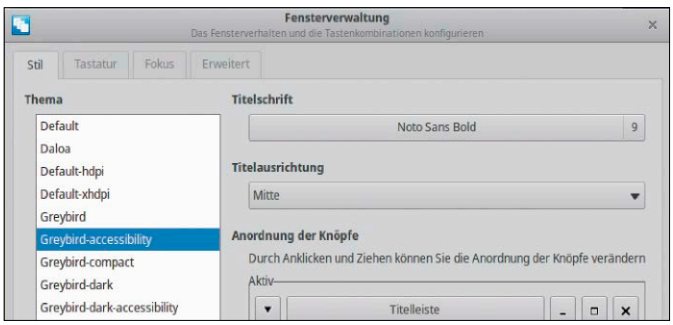
installieren dann die Erweiterung. Anschließend gibt es in den Systemeinstellungen unter „KWin Script“ den neuen Eintrag „Fenster-Fugen“ mit einem eigenen Einstellungssystem. Ein Klick darauf erlaubt die Anpassung des Abstands zwischen den Fenstern, der standardmäßig auf acht Pixel festgelegt ist. Ist die Erweiterung per Checkbox aktiviert, so arrangiert sie alle Programmfenster bei der Kachelung automatisch. Die Kachelung funktioniert in KDE, indem man ein Fenster an einen der Bildschirmränder zieht und es dann loslässt. Die dazu passende Einstellung für das Panel von KDE Plasma 5.25 findet sich nach einem Rechtsklick auf die Leiste und „Bearbeitungsmodus starten → Weitere Einstellungen → Floating Dock“. Generell funktioniert die Erweiterung aber auch mit älteren Versionen von KDE. **-dw**

Xubuntu: Zu schmale Fensterränder

Zu dünn ausgefallen: In Xubuntu 22.04 (auf Heft-DVD) bringt das voreingestellte Aussehen das Problem sehr schmaler Fensterränder zurück. Mit der Maus muss man hier genau zielen und mit Touchpads ist eine präzise Größenänderung nervig und nahezu ausgeschlossen.

Schnelle Abhilfe bringt eine Tastenkombination: Nach dem Halten der Alt-Taste und einem Rechtsklick auf eine beliebige Stelle im Programmfenster ist dessen Größe durch Ziehen des Mauscursors ebenfalls anpassbar. Ein genaues Zielen auf den Rahmen ist dann nicht nötig. Ein zweiter Weg, der das Aussehen des XFCE-Gewands „Greybird“ von Xubuntu leicht verändert, führt im Anwendungsmenü über die „Fensterverwaltung → Stil“.

Der dortige Eintrag „Greybird-accessibility“ beziehungsweise „Greybird-dark-accessibility“ verbreitert Fenstertitel sowie Ränder und ist damit gut für Notebooks mit kleinem Display geeignet. Für richtig hohe Auflösungen gibt es auch noch das Aussehen „Default-hidpi“, das die Fensterränder massiv verbreitert. **-dw**



Bequemere Bedienung: Alternative Themes in Xubuntu machen den Rand von Fenstern einige Pixel breiter und erleichtern damit die Größenänderung per Maus.

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.

Laufwerke ausblenden

Neben meinem Ubuntu-System ist noch ein zweites Betriebssystem installiert. Dessen Partition wird zwar unter Ubuntu nicht gemountet, aber im Dateimanager unter „Andere Orte" angezeigt. Dadurch ist es ein Leichtes, das Dateisystem versehentlich zu laden. Ich möchte diese Partition schützen, zumal noch eine weitere Person das Ubuntu-System benutzt.

Karsten N., per Mail

Gegen versehentliches Mounten im Dateimanager lassen sich Laufwerke und Partitionen von Fremdsystemen gut schützen, indem sie dort einfach nicht mehr auftauchen. Solches Ausblenden gilt aber nur für den Dateimanager – gegen destruktiv gesinnte Aktionen im Terminal und mit root-Recht schützt es nicht. Unter Ubuntu-Distributionen, die das Gnome-Disk-Utility („Laufwerke") verwenden, markieren Sie dort das Laufwerk und die betreffende Partition und klicken dann auf das Zahnradsymbol unter der Partitionsdarstellung. Mit dem Dialog „Einhängeoptionen bearbeiten" deaktivieren Sie erst die „Vorgaben der Benutzersitzung" und lassen alle Optionen abgeschaltet. Entscheidend ist, dass die Partition beim Systemstart nicht gemountet wird (erste Option) und – das bewirkt das Ausblenden – in der Benutzerschnittstelle nicht angezeigt wird (zweite Option).

Unter der Hand wird, um eine Partition **nicht zu zeigen,** ein Extra-Eintrag in der Datei „/etc/fstab" angelegt, was natürlich auch manuell geschehen kann. Im Prinzip genügt:

```
UUID=[…] none auto nofail,noauto 0 0
```

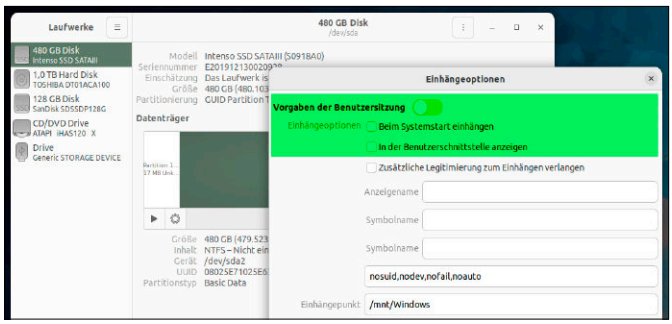
Da hier kein Mountpunkt angegeben ist („none"), wird die Partition auch dann nicht eingehängt, falls dies im Terminal und mit root-Recht versucht würde.

XFCE und Cinnamon

Bei den Linux-Mint-Vorstellungen der LinuxWelt ärgere ich mich regelmäßig, dass Cinnamon so gelobt wird, während die XFCE-Edition unter den Tisch fällt. Ich finde XFCE insgesamt benutzerfreundlicher und nicht zuletzt die farbliche Anpassungsfähigkeit der XFCE-Leisten ästhetisch perfekt.

Gerard B., per Mail

XFCE ist ein exzellenter Desktop und Xubuntu und andere XFCE-Distributionen sind bei uns immer erste Empfehlungen für ältere Hardware. Im Falle von Linux Mint sehen wir aber bei Cinnamon das entscheidende Motiv, diese Distribution zu wählen. Der Desktop ist funktionsreicher und schicker. Sie haben aber recht: Farbliche Anpassung der Leisten bietet er bislang nicht, jedoch sollte die kleine Cinnamon-Erweiterung „Transparent Panels" auch Ästheten zufriedenstellen. ■



Gnome-Disks („Laufwerke"): Passende, sprich: fehlende Einhängeoptionen unterbinden, dass der Dateimanager einen Datenträger anzeigt.

SERVICE

Linux-News online
Aktuelle News rund um das Thema Linux lesen Sie unter *www.pcwelt.de/computer-technik/betriebssystem-software/linux*.

Kontakt zur Redaktion
Wir freuen uns über jede Mail! Bei Fragen zum Heft LinuxWelt wenden Sie sich am besten an *linux@it-media.de*. Bitte beachten Sie, dass wir keinen Support für spezielle Hardware oder die Linux-Systeme auf der Heft-DVD leisten können.

LinuxWelt-Kundenservice für Einzelheft-Käufer
Haben Sie eine Ausgabe von LinuxWelt verpasst? Hier können Sie einzelne Hefte nachbestellen:
DataM-Services GmbH
Postfach 916, 97091 Würzburg
Tel.: 0931/4170-177
Fax: 0931/4170-497
(Mo bis Fr, 8 bis 17 Uhr)
E-Mail:
idg-techmedia@datam-services.de

LinuxWelt-Kundenservice für Abonnenten: Fragen zum bestehenden Abonnement / Premium-Abonnement, zum Umtausch defekter Datenträger, zur Änderung persönlicher Daten (Anschrift, E-Mail-Adresse, Zahlungsweise, Bankverbindung) bitte an
Zenit Pressevertrieb GmbH
LinuxWelt-Kundenservice
Postfach 810580, 70522 Stuttgart
Tel: 0711/7252-233
(Mo bis Fr, 8 bis 18 Uhr)
Fax: 0711/7252-333
E-Mail: *linuxwelt@zenit-presse.de*

Digitalabo in der App
https://www.idgshop.de/linuxwelt/linuxwelt-magazin-abo/linuxwelt-in-pcwelt-plus-digital

Verlag

IT MEDIA PUBLISHING GMBH & CO KG

IT Media Publishing GmbH & Co. KG
Gotthardstr. 42, 80686 München
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

Inhaber- und Beteiligungsverhältnisse: Alleinige Gesellschafterin der IT Media Publishing GmbH & Co. KG ist die IT Media Publishing Verwaltungs GmbH, München, Geschäftsführer Sebastian Hirsch.

WEITERE INFORMATIONEN

Redaktion

Gotthardstr. 42, 80686 München
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 Stahl

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.

Haftung: Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Die Veröffentlichungen in der LinuxWelt erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Auch werden Warennamen ohne Gewährleistung einer freien Verwendung benutzt.

Bildnachweis
123rf – cluckv, AdobeStok – M.a.u; sofern nicht anders angegeben: Anbieter

Anzeigen

Anzeigenleitung:
Brigitta Reinhart
RMS GmbH
Tel. 089/464729
E-Mail: *breinhart@it-media.de*

Vertrieb

Vertrieb Handelsauflage:
MZV GmbH & Co. KG, Ohmstraße 1
85716 Unterschleißheim
Tel. 089/31906-0
Fax 089/31906-113
E-Mail: *info@mzv.de*
Internet: *www.mzv.de*
Druck: Mayr Miesbach GmbH
Am Windfeld 15, 83714 Miesbach
Tel. 08025/294-267

Verlag

IT Media Publishing GmbH & Co. KG
Gotthardstr. 42, 80686 München
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:
53,50 € (D), 59,50 € (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 6/2022 erscheint am 30. September 2022

Aus Aktualitätsgründen können sich Themen ändern.

Hardwarerecycling mit Linux

Distributionen und Rollen für alte Hardware: Dieses Special wurde angekündigt, geschoben und postwendend von erstaunlich vielen Lesern nachgefragt. Die nächste LinuxWelt holt das nach – garantiert. Denn in der Tat: Allzu viele PCs, Netbooks, Notebooks ohne ernsthafte technische Mängel verstauben im Keller, weil sie aktuellen Ansprüchen nicht mehr genügen. Wenn alte Hardware für Windows nicht mehr taugt, leistet sie oft noch gute Dienste mit anspruchslosen Linux-Distributionen und als Linux-Server sowieso. Die nächste LinuxWelt zeigt Chancen und Grenzen beim Recycling alter Geräte.

Linux Mint 21

Vorstellung der neuen Mint-Version 21 (und auf Heft-DVD): Mindestens in Deutschland ist Linux Mint der Favorit am Linux-Desktop. Die auf LTS-Ubuntu basierte Distribution stellt im Sommer ihren Unterbau auf Ubuntu 22.04 um und geht zur Version 21 („Vanessa“). Im Fokus steht der Mint-eigene Desktop Cinnamon in Version 5.4 mit vielen Neuerungen und verbesserten Applets, aber auch ein grafisches Upgradetool ist angekündigt. Politisch interessant wird auch die Frage, wie sich das Mint-Team beim Standardbrowser entscheidet, nachdem die Ubuntu-Basis Firefox nur noch als Snap-Container ausliefert.

Hardware- und Netzwerkzubehör

Kreative Gadgets für Homeoffice und Netzwerk: Kleines Zubehör für die heimische IT kann die Leistung steigern, für Ordnung sorgen oder die Ergonomie verbessern. Für den IT-Arbeitsplatz, die Medienwiedergabe und das Netzwerk gibt es ständig neue Ideen in Form nutzwertiger Hardwarelösungen. Solches Zubehör behebt meistens für wenig Geld bisherige Problemfelder oder Komfortdefizite. Die LinuxWelt empfiehlt kleine Gadgets, die sich in der Praxis bewährt haben.

Der Kosmos Systemd

Eine lohnende Know-how-Investition: Systemd ist inzwischen auf den allermeisten Linux-Systemen der primäre Systemdienst (Init-Daemon) und damit Herrscher über alle nachrangigen Dienste. Mit den zugehörigen Kommandozeilentools wie systemctl, networkctl oder journalctl kann der Systembenutzer seinerseits Systemd kontrollieren und in die Konfiguration eingreifen. Anlässe dies zu tun, gibt es genug – etwa um Serverdienste nach einer Konfigurationsänderung neu zu starten. Die LinuxWelt liefert einen Praxisratgeber mit einem systematischem Überblick und vielen Beispielen, wie man sich die zweifellos anstrengende Syntax aneignet und vereinfacht.

LINUX WELT

Mini-Angebot!

Satte **33 %** gespart!

3x LinuxWelt inkl. Prämie*

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

Jetzt testen:

3 x LinuxWelt als Heft frei Haus mit Gratis-DVD +
3 x LinuxWelt direkt aufs Smartphone & Tablet mit interaktivem Lesemodus +
10,- € Geldprämie*

=18,- € (anstatt 25,50 EUR)

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 18,- € und erhalte 3 Ausgaben inkl. 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. 53,50 EUR. Danach ist eine Kündigung zur übernächsten Ausgabe jederzeit möglich.

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

BEZAHLEN

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

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

LWPM062018

* wird mit Abo-Preis verrechnet

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

Leis(e)tungsstark!

TUXEDO Pulse 15 - Gen2

AMD Ryzen 7 5700U-35W
8 Kerne | 16 Threads

WQHD-Display
2560 x 1440 | 165 Hz

Bis zu 18 h Laufzeit
91 Wh Lithium-Ionen

Leichtes Magnesiumgehäuse
1,7 cm dünn | 1,5 kg leicht

100% Linux

5 Jahre Garantie

Lifetime Support

Gefertigt in Deutschland

Deutscher Datenschutz

Support vor Ort

TUXEDO COMPUTERS 18 JAHRE JUBILÄUM

tuxedocomputers.com

jetzt bewerben!

Neuer Job gesucht?
tuxedocomputers.com/jobs