JETZT NEU! Mit Extra-Download-DVD!

4 196691 608994 02

2/2023
Februar – März

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

LINUX WELT

Einsteiger-Tipps

- Paketmanager streikt? Das ist die Lösung!
- Durchblick im Kernel-Chaos

Alle Systeme parallel nutzen

So starten Sie jedes System in einer virtuellen Maschine

- Alle Linux-Systeme gefahrlos ausprobieren
- Server für alle Zwecke einrichten
- Virtuelle PCs zum Testen aufsetzen u.v.m.

Profi-Workshop: So installieren Sie Windows vollautomatisch

NEU: Virtualbox 7 auf DVD!

Troubleshooting

So umgehen Sie die schlimmsten Ubuntu-Bugs

Linux auf dem USB-Stick

Die schnellsten & besten Systeme für den Stick

Nie wieder Werbung

Fertig konfiguriert! Raspi als Ad-Blocker nutzen

Linux im Netzwerk

Schneller, stabiler, sicherer: Hardware installieren · Datenaustausch optimieren
Alle Geräte einbinden: Drucker, Scanner, Smart-TV …

NEU: Mint 21.1

Überarbeiteter Desktop, weniger Kennwortabfragen, verbesserte X-Apps u.v.m.

DVD IM HEFT!

Multiboot
4 Top-Systeme

1. Linux Mint 21.1
2. Ubuntu 22.04.1 mit Virtualbox
3. LinuxWelt-Rettungssystem 9.2
4. Bodhi Linux 7.0

LinuxWelt Digital XXL 2/23
Über 330 Seiten Linux-Know-how

EXTRA! DOWNLOAD-DVD!

Multiboot
Livesysteme & Tools

1. MX 21.2.1 Workbench
2. Gparted Live 1.4.0-6
3. Puppex Bookworm 220714
4. Wifiway32 1.1

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

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

LINUX WELT

Linux Tipps-Handbuch

Jetzt am Kiosk!

Sonderheft
für nur
12,90 €

Mit Multiboot-DVD und Extra-Download-DVD

Bestellen unter
www.pcwelt.de/linuxwelt-xxl 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 LinuxWelt SH XXL 1/23 Linux Tipps-Handbuch 2023 für nur 12,90 €.

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

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

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 den PC-WELT Kundenservice, DataM-Services GmbH, Postfach 9161, 97091 Würzburg

ChatGPT: Die KI ist gelandet

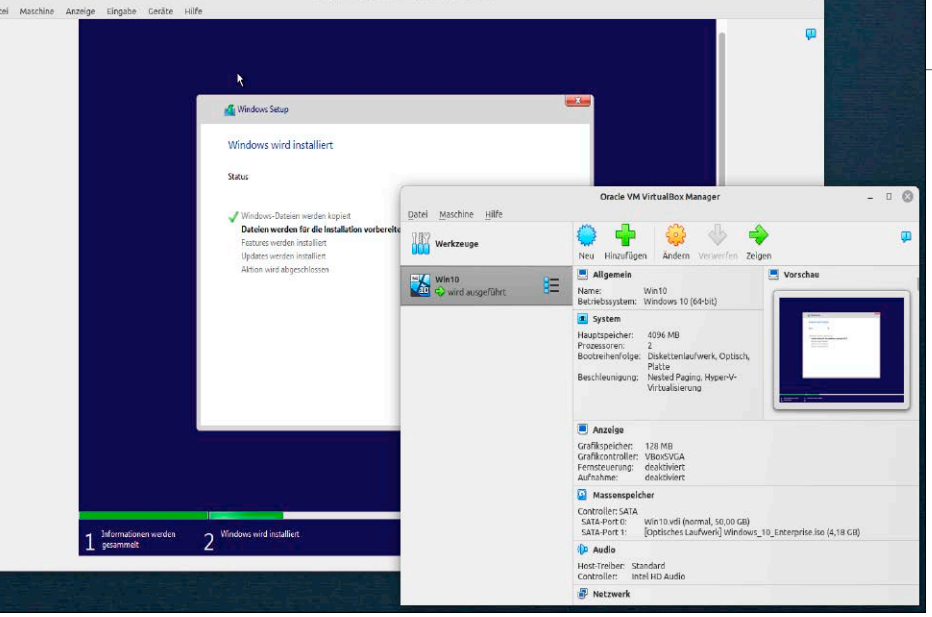
Es fegt ein Begeisterungssturm durch die sozialen Netze: Technikaffine Anwender nutzen den mit künstlicher Intelligenz betriebenen Chatbot ChatGPT (*https://openai.com/blog/chatgpt*) und sind durchweg fasziniert. Er antwortet auf alle Fragen meist eloquent und kenntnisreich. Programmierer lassen sich beim Coden helfen, Marketing-Menschen entlocken der Maschine PR-Kampagnen, Hobby-Köche holen sich Rezeptideen, und viele Nutzer bekommen Antworten auf ganz normale Fragen, etwa „Was hilft gegen Husten?".

Arne Arnold
Redakteur
aarnold@it-media.de

Die KI ist nicht perfekt, zum Beispiel erzählt ChatGPT immer wieder Unsinn – als hätte der Umstand, dass Irren menschlich ist, einen Weg in diese KI gefunden. Außerdem wurde das Tool mit Daten trainiert, die nur bis 2021 reichen. Neues fehlt entsprechend. Und manchmal klingen die Antworten von ChatGPT mehr nach Geplapper als nach Informationen. Vor allem technikferne Anwender scheinen das so zu empfinden.

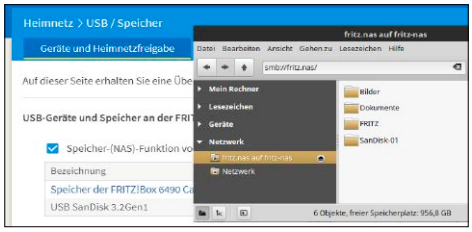
Dennoch: Es überwiegt der Eindruck, dass diese KI eine Qualität erreicht hat, die etwas verändern wird. Das werden alle zu spüren bekommen, die mit der Vermittlung von Wissen arbeiten. Für manche wird dadurch das Leben einfacher, andere müssen sich warm anziehen.

Herzlichst, Ihr



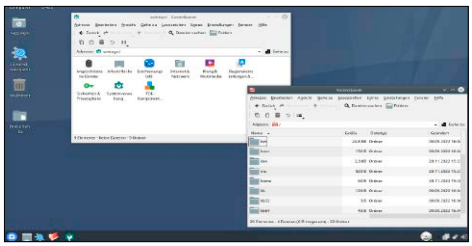
Alle Systeme parallel nutzen

Windows unter Linux? Linux unter Windows? Server ohne Extrahardware? Der Heftschwerpunkt zeigt, welche Chancen Virtualisierung eröffnet und dabei Kosten und Aufwand spart. **S. 32**



Linux im Netz

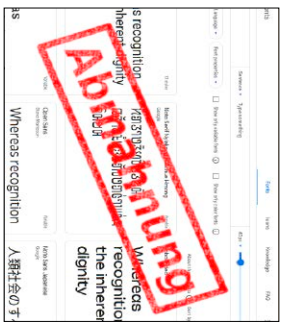
Hardware, Server, Desktop: Das Special bringt Grundlagen und Optimierungen für Heimnetze mit Linux. **S. 48**



Linux auf USB

Schnell, klein und trotzdem komfortabel: Diese Distributionen empfehlen sich für den Einsatz auf USB. **S. 64**

Grundlagen



Special I – Virtualisierung

Special II – Netzwerken unter Linux

Standards

Die Highlights der DVD

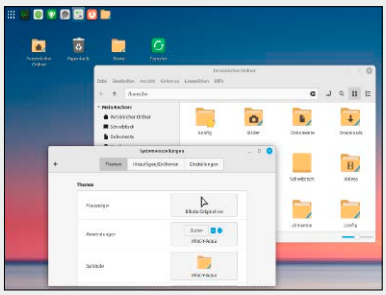
Auf Heft-DVD: Drei Desktops und das LinuxWelt-Rettungssystem 9.2

Live und gut: Das unten nicht aufgeführte LinuxWelt-Rettungssystem ist in neuer Version 9.2 ein opulent ausgestattetes Livesystem mit allen Werkzeugen, um Linux-Probleme oder Löschpannen zu beheben. Für die Webnutzung stehen gleich drei Browser zur Auswahl – Firefox, Chromium und Opera.

S. 10

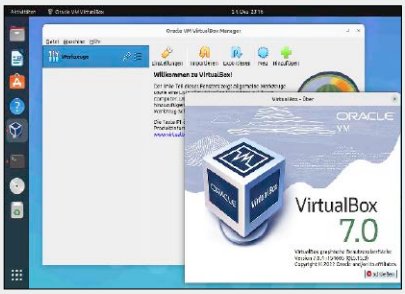
Linux Mint 21.1 (Cinnamon)

Frische „Vera“: Auf der Basis von Ubuntu 22.04.1 gibt es freundliche Themenoptik und Verbesserungen bei Flatpak- und Systemverwaltung.



Ubuntu 22.04.1 (Gnome)

Das aktuelle Ubuntu-Point-Release ist als Spezialedition auf der Heft-DVD – mit Firefox als klassisches DEB-Paket und mit vorinstalliertem Virtualbox 7.



Bodhi Linux 7

Mit exotischem Desktop und fehlenden Systemzentralen ist Bodhi nichts für Anfänger, aber stets ein Tipp für Speedfans oder schwache Hardware.

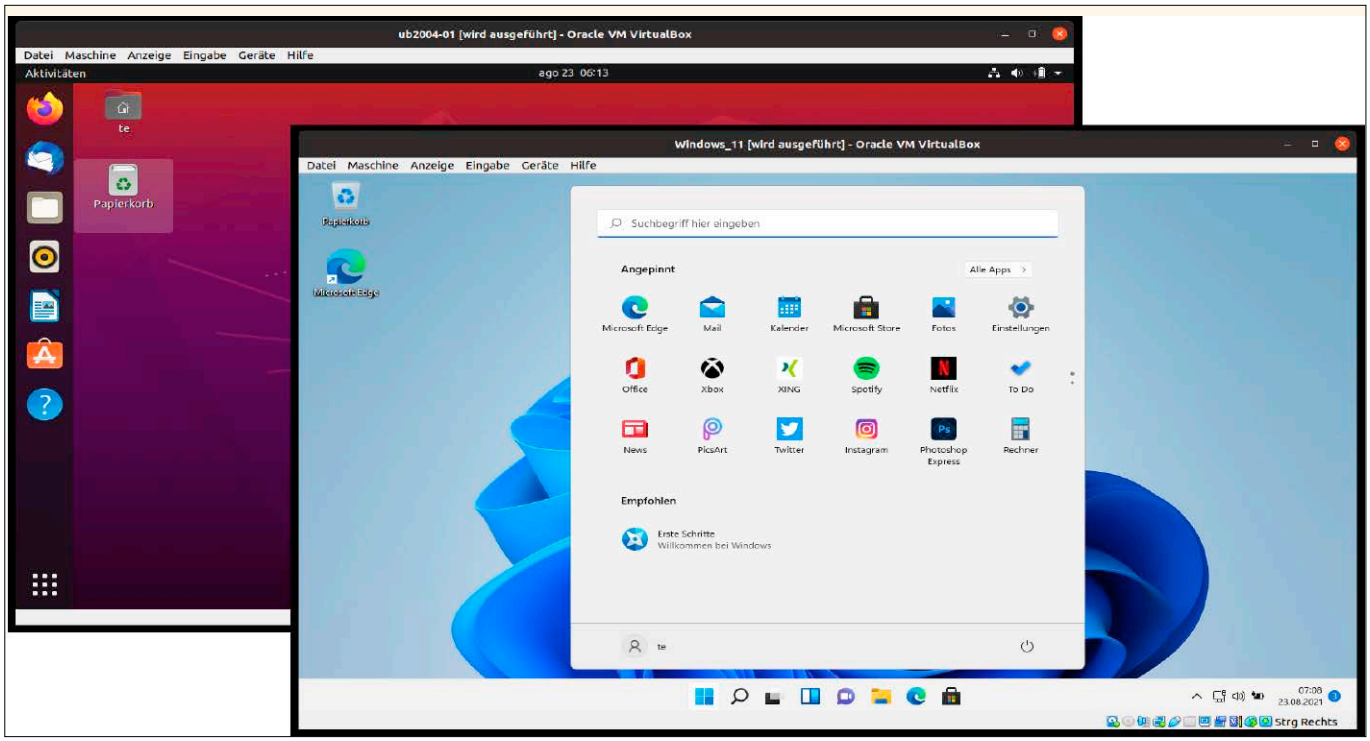
Distributionen & Software

Raspberry & Server

Praxis

Desktops & Server in virtueller Maschine

Virtualisierung wird immer schneller und komfortabler und hat längst ihren Platz beim normalen Endanwender gefunden. Das große Heftspecial ab Seite 32 konzentriert sich auf das – gegenüber Vmware Player – deutlich funktionsreichere Oracle Virtualbox.



VON HERMANN APFELBÖCK

Altgediente IT-Profis und Fachredakteure fragen sich zuweilen: Wie haben wir das eigentlich früher gemacht? Ganz früher nämlich, als es noch keine Virtualisierer gab: Das Ausprobieren eines Linux-Desktops erforderte dedizierte Testhardware oder kompliziertes Umpartitionieren. Der Einsatz von Software anderer Betriebssysteme nötigte zum Umbooten oder zum Rechnerwechsel. Und zum Einsatz oder Test von Serverdiensten war eine passende Hardware freizuräumen. Ja – man brauchte viel Hardware, Geduld bei Installationsproblemen angesichts unflexibler Hardwarekonstallationen und außerdem die pragmatische Wegwerfmentalität, dass das eben installierte System trotz aktuellem Konfigurationsaufwand vielleicht schon in einer Woche dem nächsten weichen muss. Virtualisierung beseitigt alle diese Sorgen: Ein guter Rechner mit viel Speicherplatz kann Dutzende von Systemen dauerhaft aufbewahren und ein, zwei, vielleicht drei dieser virtuellen Maschinen gleichzeitig starten. Ausstattungs- oder Treiberprobleme gibt es nicht, weil virtuelle Komponenten wie SATA-Controller oder Netzadapter standardisiert sind. Auch ein eventueller Umzug auf eine andere Hardware ist eine Lappalie, da im Prinzip nur eine einzige Datei – die virtuelle Festplatte – kopiert werden muss.

Virtualisierer wie Virtualbox und Vmware sind ein Segen, weil sie Hardwareinvestitionen, Administrationsaufwand und Energiebedarf drastisch verringern. In der großen Cloud-IT ist Virtualisierung daher eine Selbstverständlichkeit, die preisgünstige Webserver erst ermöglicht. Für Endanwender und Heim-Admins gilt im kleineren Maß-

stab genau dasselbe: Ein gelegentlich genutztes Windows oder Linux braucht keinen eigenen PC und ein kleiner Webserverdienst keinen Platinenrechner. Und für den Blick in eine interessante Linux-Distribution muss man gewiss keine Partition freiräumen.

Weitere Themen im Heft

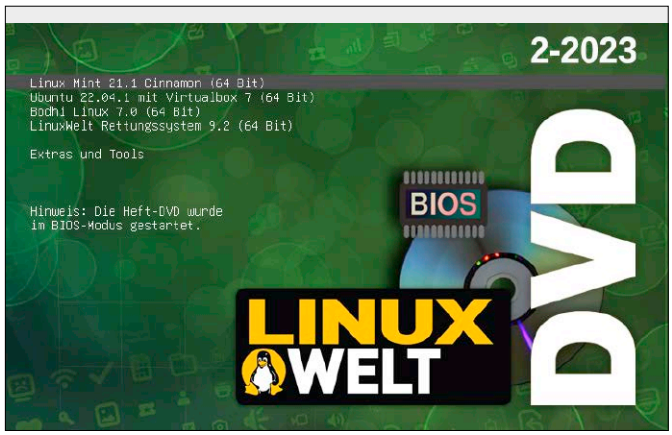
Der zweite Heftschwerpunkt (ab Seite 48) liefert Grundlagen und Optimierungstipps für das lokale Heimnetz. Hier geht es sowohl um die Hardwarevoraussetzungen als auch um Serverdienste und Datentransfer. Linux Mint 21.1 und Ubuntu 22.04.1 sind auf der DVD vertreten und erhalten im Heft ausführliche Artikel: Der Beitrag zu Linux Mint ab Seite 18 berichtet über alle Neuheiten und über die Mint-Versionspolitik. Ab Seite 22 gibt es Problemlöser für das aktuelle Ubuntu.

Die Heft-DVD: Mit delikaten LinuxWelt-Pralinen

Die Heft-DVD bietet die Desktopsysteme Linux Mint 21.1, Ubuntu 22.04.1 und Bodhi Linux 7. Während Linux Mint im Original vertreten ist, sind die beiden anderen Distributionen speziell modifiziert: Beide bieten einen Firefox-Browser im klassischen DEB-Format. Bei Ubuntu kommt ferner ein vorinstalliertes Virtualbox 7 dazu, das in dieser neuen Version in den Ubuntu-Paketquellen noch nicht bereitsteht. Als Livesystem ist die neue Version 9.2 des LinuxWelt-Rettungssystems an Bord – eine Beigabe, für die sich längeres Aufbewahren der DVD lohnt.

Die DVD kann aber mehr, als diese Systeme zu booten: Unter „Extras und Tools“ gibt es Nothelfer wie Super Grub Disk. Als DVD-Inhalte finden sich außerdem das aktualisierte PDF „LinuxWelt Digital XXL 2/23“ und unentbehrliche System- und Imagingtools für Linux und Windows.

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, F12, 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 den Bios- wie Uefi-Modus.



Drei Ubuntu-Varianten verschiedener Prägung: Mint, Ubuntu und Bodhi haben alle dieselbe Systembasis. Das originale Ubuntu (mit Gnome) ist eine LinuxWelt-Spezialedition mit vorinstalliertem Virtualbox 7.

Heft-DVD und Extra-DVD zum Download: Die Heft-DVD und die Extra-DVD stehen unter *https://github.com/LinuxWelt/Linux-Welt* als Download bereit – als Bittorrent- und als HTTP-Download. Die Extra-DVD enthält die Spezialsysteme MX Workbench, Wifiway, Puppex Bookworm und Gparted Live. Wie Sie den ISO-Download auf USB-Stick kopieren, erfahren Sie auf der Heft-DVD und auf der Github-Seite. ■

AUF DVD

Distributionen

10 **Ubuntu 22.04.1** (64 Bit)
Ubuntu-Point-Release in LinuxWelt-Spezialedition: mit Virtualbox 7 und Firefox-Browser

11 **Bodhi Linux 7** (64 Bit)
Aktualisiertes Speed-Ubuntu mit ungewöhnlichen Moksha/Enlightenment-Desktop

12 **LW-Rettungssystem 9.2** (64 Bit)
Erweiterter Werkzeugkasten der LinuxWelt-Redaktion für alle Linux-Pannen und Notfälle

18 **Linux Mint 21.1 „Vera“** (64 Bit)
Neues Mint mit vielen Detailverbesserungen auf aktualisierter Basis von Ubuntu 22.04

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

Software und Shell-Scripts
Imagingtools zur ISO-Bearbeitung und Scripts für klassische DEB-Browser

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

Viermal Linux

Mit dem Geschmack frischer Minze: Linux Mint 21.1 ist als installierbares Livesystem mit von der Partie. Extra-Aufwand haben wir mit einer modifizierten Variante von Ubuntu 22.04.1 betrieben, das ein bereits vorinstalliertes Virtualbox 7 mitbringt.

Linux Mint 21.1 Cinnamon (64 Bit)
Linux Mint 21.1 fast alle bisherigen Updates und Patches zusammen und bringt eine neue Cinnamon-Ausgabe auf den Desktop, die optischen Feinschliff erhalten hat. Das System erhält Updates bis Frühjahr 2027. Das Livesystem startet von DVD entweder im Bios- oder Uefi-Modus und liegt auch als originalgetreue ISO-Datei vor.

Ubuntu 22.04.1 mit Virtualbox 7 (64 Bit)
Passend zum Heftspecial „Virtualisierung" gibt es das neue Point Release von Ubuntu mit einem vorinstallierten Virtualbox 7. Der Virtualisierer ist anhand der Paketquellen von Oracle eingebunden und nach der Installation sofort einsatzbereit. Virtualbox wird auch zusammen mit dem System aktualisiert. Außerdem ist Firefox als klassisches DEB-Paket aus dem PPA der Mozilla Foundation vorinstalliert. Das System ist auch als ISO-Datei vertreten.

Bodhi Linux 7.0 (64 Bit)
Das ungewöhnliche inoffizielle Ubuntu-System mit dem exotischen Moksha/Enlightenment-Desktop meldet sich mit einer neuen Ausgabe zurück, die nun auch auf Ubuntu 22.04.1 LTS aufbaut. Die grafische Oberfläche ist deutlich gereift und liefert nun deutsche Sprachpakete mit. Bodhi Linux 7.0 liegt auch als originalgetreue ISO-Datei auf der DVD.

LinuxWelt-Rettungssystem 9.2 (64 Bit)
Dieses Livesystem aus der LinuxWelt-Redaktion ist eine Neuentwicklung auf der Basis von Porteus 5.0 und Slackware. Es gibt neue Wiederherstellungstools und drei Browser zur Auswahl. Mehr dazu lesen Sie in der Distributionsvorstellung auf Seite 12. Anhand der mitgelieferten ISO-Datei ist das System auch einfach auf USB-Stick übertragbar.

Extras & Tools

Netboot.xyz 2.0.65 (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 für den Bios-Modus: Einen Überblick zur kompletten Hardware eines Systems bietet das startfähige Hardware Detection Tool, auch wenn noch kein Betriebssystem installiert ist. In einem englischsprachigen Menü zeigt HDT Kategorien wie PCI, RAM, Prozessor und Bios an.

Neu: Memtest 86+ 6.0
Das Testprogramm für den Arbeitsspeicher hat nach vielen Jahren ein Update auf Version 6.0 bekommen, unterstützt aktuelle Typen von RAM und bootet nun sowohl im Bios-Modus als auch unter Uefi. Es beginnt sofort nach dem Start mit den Tests, die jederzeit zur Auswahl weiterer Optionen 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

Infrarecorder 0.53
Das bewährte Brennprogramm für ISO-Dateien steht unter einer Open-Source-Lizenz und hilft Windows-Anwendern, Linux-Imagedateien der Heft-DVD oder aus dem Internet auf einen DVD-Rohling zu brennen. Der Infrarecorder 0.53 für Windows (alle Versionen) liegt mit Installer und alternativ als portable Version vor.

USB Imager 1.0.8
Das Tool USB Imager dient zur bootfähigen Übertragung von Imagedateien auf einen USB-Stick oder eine Speicherkarte. Das Open-Source-Tool für Linux, Windows und Mac-OS bietet eine deutschsprachige Oberfläche und ersetzt in unserer Toolsammlung den früheren Win 32 Disk Imager.

Tixati 3.12
Die Heft-DVD liegt als ISO-Datei für die Übertragung auf USB-Sticks oder zum Brennen auf Dual-Layer-DVDs jetzt auch als Download vor. Die Links dazu und Bittorrent-Downloads sind auf *https://github.com/LinuxWelt* auf Github untergebracht. Tixati ist ein Bittorrent-Client für Windows – englischsprachige Freeware ohne Adware.

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 0.78
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 0.76.0.13
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 22.01
Kann einpacken: Das Open-Source-Programm 7-Zip ist eine leistungsfähige Alternative zu den Packern Winzip und Winrar, kommt aber auch mit gängigen Formaten wie TAR, GZIP, XZ, ZIP, CAB, RAR, ARJ und anderen zurecht. Es liegt für Windows in 64 Bit und 32 Bit auf DVD.

navidrome.service
Die Unit-Datei für Systemd gehört zum Artikel über den Streamingserver Navidrome (ab Seite 88). In der Datei müssen für den Autostart von Navidrome nur noch zwei Zeilen angepasst werden. Die Kommentierung der Datei zeigt, um welche Anpassungen es geht.

deb-firefox.sh
Das Shell-Script für die Kommandozeile (Bash) dient dazu, auf einem Ubuntu 22.04 LTS/Ubuntu 22.10/Ubuntu 23.04 den als Snap vorinstallierten Browser Firefox zu entfernen und stattdessen das DEB-Paket aus dem PPA der Mozilla Foundation nachzurüsten.

deb-chromium.sh
Der Chromium-Browser liegt für Ubuntu 22.04 LTS noch als herkömmliches DEB-Paket vor und kann aus einem PPA installiert werden. Das Shell-Script richtet diese Paketquelle ein und entfernt einen installierten Chromium-Browser. Es funktioniert nur unter Ubuntu 22.04 und dessen offizielle Varianten.

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

Weitere Infos

Die Vorstellung der fünf Systeme auf DVD und dem zusätzlichen DVD-Image (4,7 GB) zum Download beginnt ab Seite 10. Zusätzliche Anleitungen und Hinweise zu den Distributionen auf Heft-DVD liefert die dortige Übersicht, die Sie über die Datei „index.html" in einem beliebigen Browser öffnen.

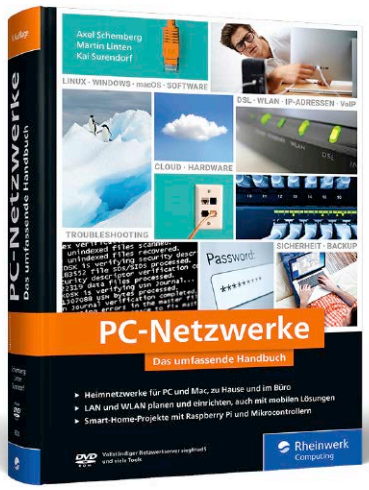
Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

- 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 „PC-Netzwerke – Das umfassende Handbuch“ aus dem Rheinwerk Verlag.



Randvoll mit Grundlagenwissen und Praxisprojekten

PC-Netzwerke

Autoren: Martin Linten, Axel Schemberg, Kai Surendorf
Verlag: Rheinwerk Computing, 831 Seiten, 9., aktualisierte und erweiterte Auflage 2023, gebunden, 29,90 Euro
ISBN: ISBN 978-3-8362-8528-5

Bewährt, praxisnah und randvoll mit wertvollen Informationen – Sie erhalten nicht nur umfassende Grundlagen zur Einrichtung Ihres Netzwerks, sondern finden auch Praxis-Anleitungen, mit denen Sie Ihre Computer, Fernseher, Tablets und Smartphones zu Hause oder im Büro professionell vernetzen. Mit vielen Beispiel-Projekten (z. B. UMTS-Router, Radiowecker und Media Player – LibreELEC (Kodi) – mit Rasperry Pi) für eigene Netzwerk- und Hausautomationsideen.

- **PCs vernetzen, zu Hause und im Büro**
- **LAN und WLAN planen und einrichten, inkl. mobile Lösungen**
- **Hausautomation mit Tasmota und ESP8266 & NAS-Projekt mit Raspberry Pi**

PLUS: Gratisheft für alle Teilnehmer

SO FUNKTIONIERT'S:

Auf *https://bit.ly/lin0223* 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 2/2023 ist der 28.3.2023.**

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 Extra 03/2022: „Handbuch der Linux-Befehle“ (ohne Datenträger).

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

Ubuntu 22.04.1 mit Virtualbox 7

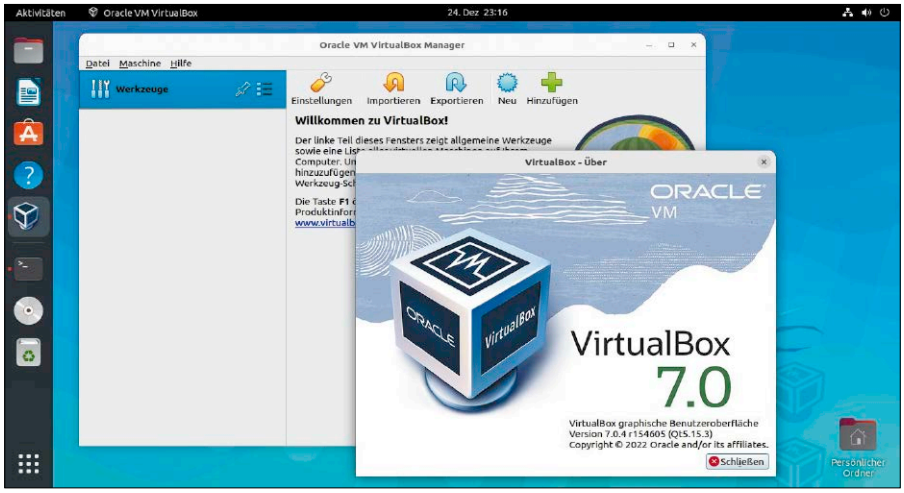
Passend zum Virtualisierungsspecial liefern wir Point Release 22.04.1 der Ubuntu-Version (64 Bit) mit dem vorinstallierten Virtualisierer Virtualbox 7.0.4 aus. Dieser ist anhand der offiziellen Paketquellen von Oracle eingerichtet.

VON DAVID WOLSKI

Diese Version ist ein Point Release, das in neuen Installationsmedien alle bisher erschienenen Aktualisierungen bereitstellt. Die fallen hier gar nicht mal unspektakulär aus; unter anderem liefert diese aufgefrischte Hauptausgabe von Ubuntu 22.04 neue Kernel-Treiber für Grafikchips und Gnome 42.2. Das ist für eine LTS-Version kein kleiner Schritt und es sind viele Bugfixes für den Desktop enthalten. Der Dateimanager Nautilus hat dabei die meisten Fehlerbehebungen erhalten. Auf dem Desktop gab es in den Einstellungen gab schon zuvor unter „Erscheinungsbild“ eine Auswahl der Farbgebung für hervorgehobene Fensterelemente bei Gnome-Programmen, um der Oberfläche eine persönliche Note zu verleihen. Es muss also kein anderes Theme mehr installiert und über Gnome Tweaks aktiviert werden, um das Erscheinungsbild mit Farbakzenten anzupassen. Ebenfalls ist eine einfache Umschaltung von einem hellen zu einem übergreifenden dunklen Gewand enthalten. Dies funktioniert mit Gnome-Programmen bereits, obwohl noch gar nicht alle Anwendungen dieser Ubuntu-Ausgabe in der GTK4-Version vorliegen.

Hallo GTK4 – Ciao Themes!

Mit dem schrittweisen Wechsel der Gnome-Oberfläche zum Toolkit GTK4 sind Themes gar nicht mehr vorgesehen, was viele Anwender zunächst als Einschränkung wahrgenommen haben. Aber mit seinen eigenen Erweiterungen und Anpassungen in Ubuntu 22.04 LTS fällt das in der Praxis nicht schwer ins Gewicht fällt. Wayland funktioniert nun auch endlich mit den proprietären, nachinstallierbaren Nvidia-Grafiktreibern. Es muss dann aber weiterhin für Nvidia auf der Anmeldeoberfläche aktiviert werden.



Modifizierte Version von Ubuntu 22.04.1: Virtualbox 7 ist hier aus der offiziellen Paketquelle von Oracle bereits eingerichtet. Außerdem ist Firefox als DEB vorinstalliert.

Der Kernel bleibt hier noch bei Version 5.15 mit zurückportierten Sicherheitspatches. In den Paketquellen kann aber schon Kernel 5.17 über das Paket „linux-image-5.17.0-1025-oem“ manuell nachinstalliert werden. Insgesamt fünf Jahre, also bis April 2027, erhält Ubuntu 22.04 Updates, mit einer Anmeldung am Service „Ubuntu Pro“ (*https://ubuntu.com/pro*) sogar zehn Jahre. Dieser Dienst ist mittlerweile für bis zu fünf Ubuntu-Systeme kostenlos und macht diese Linux-Distribution auch für Anwender und Hobby-Admins zum Dauerläufer.

VM-Host mit Virtualbox 7

Schon nach dem Booten zeigt die abgewandelte Farbgebung, dass es sich um ein angepasstes Ubuntu 22.04.1 aus der Linux-Welt-Redaktion handelt. Denn hier ist Oracle Virtualbox 7 schon vorinstalliert und nach der Installation des Systems sofort einsatzbereit. Eine Programmverknüpfung findet sich in der Anwendungsübersicht unter „Aktivitäten“. Auch die Virtualbox-Erweiterungen für USB 3.0 in Gastsystemen und RDP-Verbindungen zu VMs sind schon vorhanden. In den Standard-Paketquellen Ubuntus befindet sich derzeit noch die ältere Version Virtualbox 6.x. Daher haben wir das neue Virtualbox 7 über die externen Paketquellen von Oracle eingebunden, wie unter *www.virtualbox.org/wiki/Linux_Downloads* für Debian dokumentiert. Der Vorteil dieser Einbindung über eine externe Paketquelle: Liegt ein neueres Virtualbox der 7er-Versionsreihe vor, so holt die Aktualisierungsverwaltung beziehungsweise ein „apt upgrade“ in der Kommandozeile automatisch die aktualisierte Version. Auch werden bei einem Kernel-Update die passenden Kernel-Module für Virtualbox gleich mit eingerichtet. Sollte dies nach vielen Modifikationen am System einmal nicht funktionieren, beispielsweise nach der Installation eines anderen Kernels ohne passende Kernel-Headerdateien, so gibt das Kommando

```
sudo /sbin/vboxconfig
```

in der Kommandozeile Auskunft darüber, was zum automatischen Bau neuer Module noch fehlt.

Mehr Infos zu Ubuntu 22.04.1
Website: *https://ubuntu.com/#download*
Dokumentation: *https://wiki.ubuntu.com*

Bodhi Linux 7.0

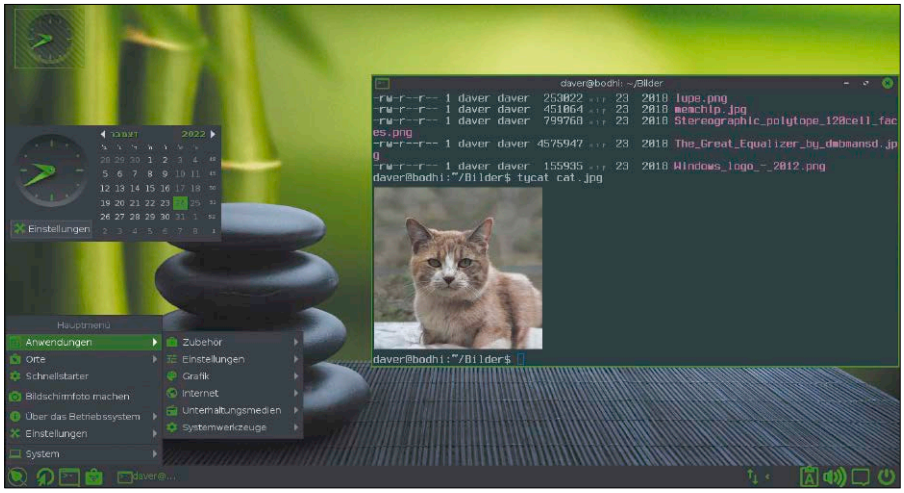
Eine Weile war es still um diese inoffizielle Ubuntu-Variante mit ihrem ungewöhnlichen bis gewöhnungsbedürftigen Enlightenment-Desktop: 2022 erschien keine neue Version. Nun aktualisiert Bodhi Linux 7.0 seine Basis auf Ubuntu 22.04.1.

VON DAVID WOLSKI

Unter den eigenständigen Desktopumgebungen ist Enlightenment ein Unikum. Denn es kommt auf dieser Arbeitsfläche weder Qt noch GTK als Toolkit zum Einsatz, sondern eine eigene Sammlung an Bibliotheken, die auf geringen Ressourcenbedarf optimiert ist. Die Sparsamkeit in Sachen Arbeitsspeicher und der teils eigenwillige C-Quellcode mit Anleihen von C++ zeigen, woher Enlightenment stammt: aus einer Frühzeit der Linux-Desktops. 1997 erschien die erste farbenfrohe Version und ließ andere Oberflächen alt aussehen. Tatsächlich gehört Enlightenment, auf das Bodhi Linux mit eigenen Desktop Moksha aufbaut, zu einer der ältesten grafischen Umgebungen für Linux. Viele Ideen des maßgeblichen Entwicklers haben das Motiv, clevere, ungewöhnliche Lösungen zu finden, um auch unter bescheidenen Hardwareausstattungen einen effektvollen und besonders schnellen Desktop zu präsentierten. Und so wurde auch Samsung auf Enlightenment aufmerksam, adaptierte es zwischen 2010 und 2019 für das hauseigene Betriebssystem Tizen als Oberfläche für Smart-TVs, die nur über begrenzten Arbeitsspeicher und Prozessorpower verfügen. Die vergleichsweise umständlichen Entwicklungswege von Enlightenment wollten aber eine jüngere Generation von Programmierern nicht begeistern. So ist der Desktop ein Exot geblieben, dank dem unerschöpflichen Eifer seines Erfinders aber weiterhin lebendig.

Einfacher zur passenden Sprache

Bodhi Linux trimmt Enlightenment in einer eigenen Abspaltung auf Stabilität und Benutzbarkeit, hat einige der besonders grellen Gewänder des Desktop aus der Garderobe genommen und kleidet die Oberfläche in gedeckte Farben. Nach der Installation, die wie in anderen Ubuntu-Derivaten



Verspieltes und Nützliches: Das Terminal von Bodhi/Moksha ist eine Besonderheit. Spezielle Befehle wie „tyls“ können Vorschaubilder und Grafiken direkt in der Shell anzeigen.

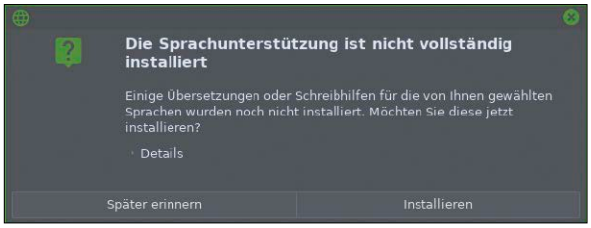
mit dem Installer Ubiquity erfolgt, fallen die Reaktionsfreudigkeit und der geringe Speicherbedarf auf: Mit 400 MB ist das Basissystem zufrieden, das nun auf Ubuntu 22.04.1 aufbaut. Besser klappt in Bodhi Linux 7.0 nun endlich die Sprachunterstützung ab der Installation: Es sind keine Basteleien mehr nötig, um deutsche Sprachdateien nachzurüsten. Was noch fehlt, wird einfach über „Anwendungen → Language Support“ nachinstalliert.

Ubuntu-System ohne Snaps

Viel ist an Software jedoch nicht vorhanden. Bodhi ist als Minimalsystem für alte Hardware konzipiert und größere Pakete wie Libre Office, Firefox, Chromium und Gimp sind nicht vorinstalliert. Mit Synaptic gibt es aber den grafischen Paketmanager von Debian und die meisten Programme aus dem Fundus von Ubuntu 22.04 sind damit schnell eingerichtet. Aber nicht alle: Snaps sind unter Bodhi Linux gründlich deaktiviert: Wie in Linux Mint ist die Snapd-Runtime auch nicht nachinstallierbar.

In dieser speziell angepassten Bodhi-Version haben wir deshalb Firefox als aus dem PPA *https://launchpad.net/~mozillateam/+archive/ubuntu/ppa* vorinstalliert. Trotzdem bleibt Bodhi Linux ein System für Anwender, die ihren Desktop selbst mit Software ausstatten und wissen, welche Programme sie brauchen.

Mehr Infos zu Bodhi Linux
Website: *www.bodhilinux.com*
Dokumentation:
www.bodhilinux.com/w/wiki

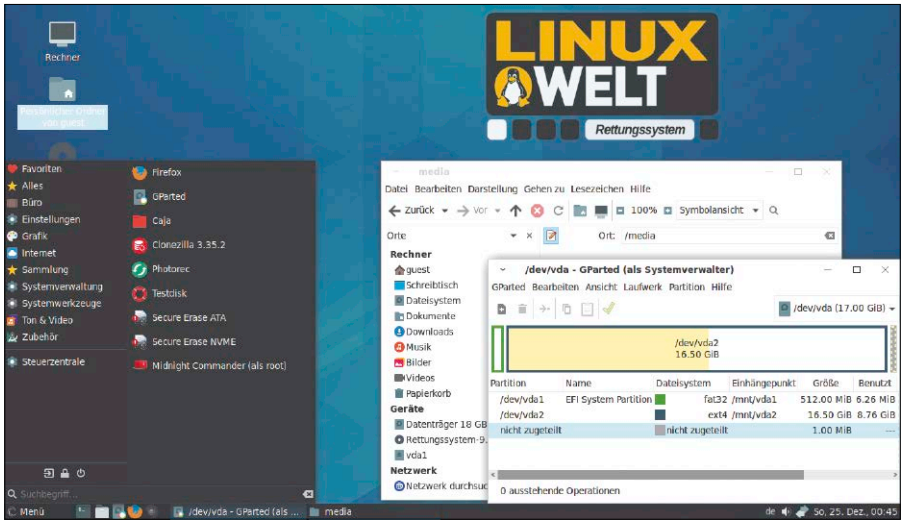


Nicht mehr sprachlos: Bodhi Linux 7.0 liefert jetzt deutsche Sprachunterstützung mit. Weitere Sprachpakete sind über diesen Dialog schnell nachgerüstet.

LinuxWelt-Rettungssystem 9.2

Die aktualisierte und ergänzte Ausgabe des LinuxWelt-Rettungssystems (in 64 Bit auf DVD) ist auf bestem Wege, eine freie Alternative zu Parted Magic zu werden. Neu hinzugekommen sind das Notfalltool ddrescue und frische Browser.

VON DAVID WOLSKI



Großer Werkzeugkasten: Das Rettungstool ddrescue ergänzt das neue System, das auch neue Browserversionen liefert. Die allerwichtigsten Tools befinden sich unter „Favoriten“.

Ursprünglich entstand dieses System aus der LinuxWelt-Redaktion aus einem erweiterten Porteus 4.0, da sich dieses Slackware-System mit eigenen Paketen sowie mit Arch-Linux-Software gut ausbauen und flott aktualisieren ließ. Mittlerweile hat das Rettungssystem in Version 9.x nicht mehr viel mit Porteus zu tun. Lediglich die Basispakete stammen von der Version 5.0 des kompakten Livesystems. Weitere Software für systemnahe Arbeiten und zur Datenrettung, auch auf Windows-Maschinen mit Bitlocker-Verschlüsselung und NTFS-Dateisystem, haben wir selbst ergänzt. Ziel ist es, im Funktionsumfang mit Parted Magic gleichzuziehen, das seit 2013 nicht mehr kostenlos vorliegt.

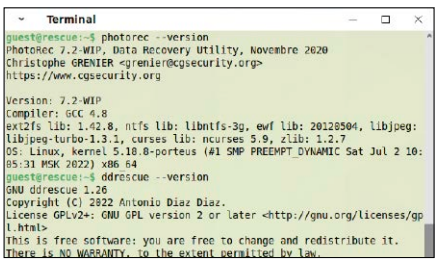
Neuerungen und Ergänzungen

In dieser Ausgabe liegen Gparted 1.4 sowie die Kommandozeilentools Testdisk und Photorec in der neuesten Version 7.2 vor – mit verbesserter Mustererkennung von gelöschten Dateien. Weil heute viele Windows-Systeme mit Bitlocker verschlüsselt sind, steht in der Shell das Werkzeug Dislocker bereit, der mit Hilfe eines Wiederherstellungsschlüssels Bitlocker-NTFS-Dateisysteme unverschlüsselt einhängen kann. Für Linux-Systeme gibt es Ext4magic zur Wiederherstellung gelöschter Dateien auf Ext4-Datenträgern. Der Verschlüsseler Veracrypt, welcher auch mit alten Truecrypt-Images und Partitionen umgehen kann, ist auf 1.25.9 aktualisiert.

Ganz neu hinzugekommen ist das Rettungstool ddrescue in der Shell, das defekte Datenträger durch hartnäckige Wiederholungen der Leseoperationen meist doch noch in ein Image auslesen kann. Als Browser liegen Firefox 102 ESR, Chromium 108 und Opera 92 mit VPN-Funktion vor. Es gibt ferner zwei Eigenentwicklungen der LinuxWelt-Redaktion: Unter „Anwendungen → Systemwerkzeuge“ gibt es ein Tool zum sicheren Löschen von SSDs („SATA Secure Erase“) sowie ein weiteres für NVMEs („NVME Secure Erase“).

Einfacher Transfer auf USB-Sticks

Auch wenn sich Tools und Kommandozeilenprogramme wie testdisk, photorec, ext4magic und dislocker an fortgeschrittene Anwender richten, so ist die Oberfläche des Livesystems einladend und einfach. Nach dem Start des Mate-Desktops wartet der übliche Network-Manager rechts oben darauf, eine WLAN-Verbindung aufzubauen. Zu den grafischen Programmen finden sich in der oberen Leiste des Mate-Desktops Verknüpfungen für den bequemen Zugriff auf die wichtigsten Programme. Es sind NTFS-Treiber mit an Bord und der Dateimanager kann Windows-Partitionen damit direkt öffnen. Das Rettungssystem kann dank Mate-Desktop genügsam mit Ressourcen haushalten. Es läuft auf einer 64-Bit-CPU der letzten 15 Jahre und mit einem GB RAM. Ab mehr als vier GB Arbeitsspeicher, also auf halbwegs aktuellen Rechnern, kann das Livesystem über das Multibootmenü komplett in den Speicher geladen werden und läuft dann extrem flott. Es handelt sich um ein reines Livesystem ohne Installationsmöglichkeiten. Im Verzeichnis „Image-Dateien“ auf Heft-DVD liegt die ISO-Datei des Systems, die mit Tools wie dd (Linux) oder dem USB Imager 1.08 (Download unter *https://bztsrc.gitlab.io/usbimager*, auch auf Heft-DVD) auf einen USB-Stick geschrieben werden kann, um einen Rechner davon zu booten.

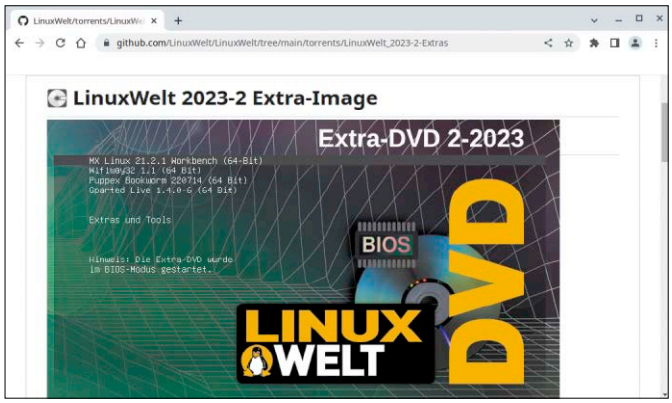


Neue Rettungstools: Das Wiederherstellungsprogramm Photorec hat ein Update auf Version 7.2 erhalten, die das Format gelöschter Dateien präziser erkennt.

Die Extra-DVD: Inhalt

Es gibt immer eine Menge interessanter Livesysteme, die einfach nicht mehr auf unsere Heft-DVD passen. Die Extra-DVD ist ein Image für USB-Sticks und DVDs (4,7 GB), welches zum Download bereitsteht und vier weitere Systeme als Werkzeugkasten liefert.

VON DAVID WOLSKI



Separates Downloadimage: Vier Livesysteme liegen als Werkzeugkasten für USB-Stick oder DVD im Downloadimage vor. Es handelt sich um Spezialsysteme für Fortgeschrittene.

Das Thema des zusätzlichen ISO-Images sind diesmal Spezialsysteme für Fortgeschrittene. Vier weitere Linux-Systeme finden sich im Multibootmenü des Images, das im Bios- und im Uefi-Modus starten kann. Die ISO-Datei steht über unsere Github-Webseite *https://github.com/LinuxWelt* zum Download bereit und liegt damit auf eigenen Servern der Redaktion. Auf Github finden Sie eine kurze Dokumentation und Downloadanleitung. Bislang standen die DVDs und Extra-Imagedateien per Bittorrent zum Download, aber Bittorrent ist mittlerweile optional. Wer über eine flotten Weg ins Internet verfügt, kann die ISO-Dateien über den Browser direkt per HTTP herunterladen. Dabei helfen insgesamt drei Server, um die Downloads im Wechsel zu bedienen.

MX Workbench 21.2: Dieses Livesystem ist universeller Werkzeugkasten mit übersichtlicher Präsentation aller Tools gleich nach dem Start. Unter anderem finden sich hier Festplattentools wie Photorec und Testdisk. Auch der einfach aktualisierbare freie Virenscanner Clam TK ist mit von der Partie und eine gute Option, sich unabhängig von einem installierten Betriebssystem eine zweite Meinung einzuholen, falls der Verdacht auf Virenbefall besteht. Mit kommerziellen Antivirenprogrammen kann das freie Clam TK nicht konkurrieren, denn es fehlen heuristische Erkennungsmethoden. Bekannte Malware und Viren findet aber auch dieser Scanner.

Wifiway32 1.1: Das englischsprachige Livesystem aus Spanien stattet ein Slackware-System mit Tools zur Netzwerkanalyse in Drahtlosnetzwerken aus. Auf dem XFCE-Desktop finden sich diverse Scanner und Sicherheitstools im Menü „Wifiway“. Hier warten beispielsweise unter „Hardware“ allgemeine Analysetools wie Lin SSID, um Signalstärken von Access Points und Routern aufzuzeichnen. In den Untermenüs „Wireless, „Pentesting“, „Wpa“ und „Wpa wps“ sind Analysewerkzeuge zur WLAN-Sicherheit untergebracht, um Lücken in der Verschlüsselung von WLANs und schwache Anmeldepasswörter zu entlarven.

Puppex Bookworm 220714: Hierbei handelt es sich um ein Livesystem aus der Familie von Puppy Linux, das auf dem brandneuen Debian 12 Bookworm basiert. Puppex ist deutlich aufgeräumter als die regulären Puppy-Ausgaben, liefert einen (englischsprachigen) Mate-Desktop und den Browser Firefox. In der Kommandozeile kann temporär zur Laufzeit der Paketmanager apt beliebige Programme aus den Quellen von Debian 12 installieren – solange das RAM reicht. Es handelt sich also um ein universell verwendbares Debian-Livesystem. Nach dem Booten ist zunächst ein US-Tastaturlayout aktiv, aber ein Klick rechts oben auf die Statusanzeige „en“ kann zu einem deutschen Layout wechseln.

Gparted Live 1.4.0-6: Das Livesystem ist immer nützlich, denn hier startet der mächtige Partitionierer Gparted in der neuesten Version gleich nach dem Booten. Gparted eignet sich bestens zur Neupartitionierung, Partitionsänderung und Formatierung von Festplatten. Es unterstützt dabei eine grandiose Anzahl von Dateisystemen und auch viele Arten von Partitionstabellen aus dem Umfeld von Linux, Unix und Windows. Diese Version von Gparted Live ist ein kleines Update, das jetzt auf Debian 11 basiert. ■

IMAGE AUF USB-STICK SCHREIBEN

Zum Kopieren des heruntergeladenen ISO-Images auf einen USB-Stick mit ausreichend Platz eignet sich der plattformunabhängige USB Imager unter Linux, Windows und Mac-OS. Das Open-Source-Programm (auf Heft-DVD, Download unter *https://bztsrc.gitlab.io/usbimager*) ist darauf spezialisiert, IMG- und ISO-Images von Livesystemen und Multibootimages bootfähig auf USB-Sticks oder Speicherkarten zu transferieren. Es zeigt eine sehr einfache, deutschsprachige Oberfläche zur Auswahl von Quelldatei und Ziellaufwerk.

Valve: Linux-Gaming wächst

Die Spieleschmiede Valve Software hat Einblicke in seine Linux-Strategie gegeben: So seien mittlerweile über hundert hauptberufliche Entwickler im Hardware-, Software- und Treiberbereich mit Linux-Gaming beschäftigt. Und nicht nur direkt mit dem Steam Deck – Valve investiert auch in die allgemeine 3D-Renderbibliothek Mesa, die Grundlage vieler Linux-Desktops ist. Ein zweiter wichtiger Betätigungsbereich ist Vulkan als performanter Ersatz für Direct X sowie Open GL. Das dritte Feld ist Proton als Kompatibilitätsschicht, die von Wine abstammt. ■

Linux Foundation Europe am Start

Die vor drei Monaten gegründete Linux Foundation Europe hat mit einem ersten Projekt die Arbeit aufgenommen: Unter dem Namen Sylva erarbeitet der europäische Zweig der Linux Foundation zusammen mit Telekom, Ericsson, Nokia, Orange, Telecom Italia, Telefonica und Vodafon ein freies Cloud-Rahmenwerk für Telekommunikationsdienstleister. Das Projekt wird den Anforderungen an Datenschutz in Europa gerecht und soll Insellösungen in der Cloud durch einen einheitlichen Softwarestack ersetzen. ■

PHP 8.2 mit neuen Typen

Beinahe im jährlichen Turnus erscheint die PHP-Runtime mit Fortschritten hinsichtlich Performance und Funktionalität. Auch PHP 8.2 präsentiert neue Features für die Programmierung von Webdiensten. Es gibt eine API zur Erzeugung von Zufallszahlen – gerade bei Cookies und für kryptografische Funktionen ein Plus. Drei neue Typen gibt es zur Definition von Variablen: TRUE, FALSE und NULL. Weniger umständliche IF-Konstrukte versprechen neu eingeführte Verknüpfungen von UND/ODER-Operationen. Eine Weiterführung von Nur-Lesen-Eigenschaften in PHP 8.1 ist eine jetzt ergänzte Klasse, die nur im Quellcode, nicht zur Laufzeit geändert werden darf. ■

Alle News von David Wolski

Vorschau auf Kernel 6.2

Obwohl Version 6.1 mit Verzögerung erschien, ist die Entwicklung von Kernel 6.2 bereits in vollem Gange, verläuft laut Linus Torvalds aber zunächst „höllisch“.

Der kommende Kernel 6.2 soll pünktlich zum anvisierten Termin Mitte Februar erscheinen. Entsprechend knapp fiel diesmal das „Merge Window“ aus, also jener kurze Zeitraum direkt nach der Veröffentlichung eines Kernels, in welchem die Neuerungen für die nächste Version in den Quellcode aufgenommen werden. Die haben es dieses Mal in sich: Torvalds rechnet mit 13 500 einzelnen Änderungen von insgesamt 1800 Entwicklern. Mit „Accel“ bekommt Linux ein Subsystem, das Aufgaben aus dem Bereich der künstlichen Intelligenz beschleunigt und eng verwandt mit dem Grafik-Subsystem ist. Nach vielen Jahren bekommt das Dateisystem BTRFS Feinschliff für seine Raid-5/6-Fähigkeiten, die bisher als experimentell galten. Für PCI-Hardware gibt es ein überarbeitetes Interruptsystem, das den Linux-Kernel fit für kommende PCI-Geräte und deren Treiber für die x86-Prozessorarchtiektur macht. Die derzeit unbefriedigende PCI-Anbindung unter ARM soll in späteren Kernel-Versionen ebenfalls dieses Interruptsystem nutzen. Auch eine Kuriosität findet sich unter den Neuerungen: Der Floppytreiber ist ab Kernel 6.2 wieder in einem guten Zustand, nachdem die Diskettenunterstützung seit 2016 zunächst wegen mangelndem Testequipment unter die Räder gekommen war. ■

XFCE 4.18: Wayland rückt näher

Zwei Jahre nach der letzten Hauptausgabe liegt der Desktop XFCE in Version 4.18 vor. Sie kommt rechtzeitig für die Aufnahme in Xubuntu 23.04, das im April erscheinen wird. XFCE beginnt ab jetzt damit, Komponenten und Programm fit für den Displayserver Wayland zu machen, aber davon ist für Anwender noch wenig zu sehen. Sichtbarer sind die ergänzten Features, besonders im überarbeiteten Dateimanager Thunar. Dort gibt es eine teilbare Ordneransicht, benutzerdefinierte Tastenkürzel sowie farbliche Markierung für Ordner und Dateien. Ein nettes Detail ist der überarbeitete Compositor, der für dezente Effekte wie Transparenz sorgt und störende „Tearing“-Effekte beim Verschieben von Fenstern vermeidet. Manjaro 22 und die Vorschauversion von Xubuntu 23.04 (*https://cdimage.ubuntu.com/xubuntu/daily-live/current*) zeigen das neue XFCE in einem Livesystem. ■

Canonical: Tuning für Snaps

Nicht nur zähe Startzeiten von Programmen im Snap-Format von Canonical haben harsche Kritik auf sich gezogen: Nachdem ausgerechnet Firefox ab Ubuntu 21.10 nur noch als Snap in dieser Distribution vorliegt, wurden die Grenzen des Paketformats deutlich: Einige Firefox-Erweiterungen und die Gnome-Shell-Integration wollten damit nicht funktionieren. Im November 2022 hat Canonical nachgebessert, leider einige Monate nach der LTS-Version von Ubuntu 22.04. Snaps haben einen neuen Kanal namens „Native Messaging“ erhalten, der in Firefox Interprozesskommunikation ermöglicht und damit wieder alle Erweiterungen erlaubt. Das Firefox-Snap startet auch schneller, weil es nun mit LZO-Algorithmus komprimiert ist. Weitere Tricks wie vorausschauendes Caching sollen die Startzeit demnächst weiter verbessern. ■

Distributionen: Neue Installer kommen

Das Jahr 2023 wird gleich für drei populäre Linux-Distributionen neue Installationsprogramme bringen, die auf einer Weboberfläche basieren: Open Suse ist mit seinem D-Installer vergleichsweise weit, denn dieser hat schon LVM2-Datenträgermanagement und Vollverschlüsselung an Bord. Der neue Ubuntu-Installer, welcher auf dem von Google entwickelten Toolkit Flutter aufbaut, soll zur Version 23.04 im April vorzeigbar sein. Noch nicht so lange in Arbeit ist für Fedora die neue Anaconda-Version mit webbasierter Oberfläche. Erst seit Fedora 37 gibt es eine Vorschau, die aber noch keine manuelle Partitionierung und Verschlüsselung erlaubt. Alle drei Installer haben gemein, dass sie auch im Browser laufen und somit eine Linux-Installation aus der Ferne ausführen können. ■

SICHERHEITSNEWS

Vmware: Ausbrüche möglich

Eigentlich sollen Virtualisierer ihre Gastsysteme sicher abschotten. Eine Sicherheitslücke, die den Ausbruch von Malware aus einer Gast-VM erlaubt, betrifft Vmware über die Analysefunktion „Vrealize Network Insight“. Die Lücke wird als kritisch eingestuft. Gastsysteme könnten auf dem Hostsystem ohne Authentifizierung eigene Befehle ausführen. Die Lücke hat aufgrund der Verbreitung von Vmware den eigenen Identifizierungscode CVE-2022-31702 erhalten und verlangt ein Update des Vrealize-Networks (sofern dies zum Einsatz kommt). Es handelt sich dabei ausgerechnet um einen Dienst, der virtuelle Maschinen nach Analysen von offenen Ports und Netzwerkaktivitäten bei einer Sicherung helfen soll. Das Update steht aber bereit.

Kernel: Samba strauchelt

Seit Version 5.15 hat der Linux-Kernel einen eigenen Samba-Server namens Ksmbd, den Samsung beigesteuert hatte. Im SMB2-Protokoll dieses Servers wurde schon im August eine kritische Lücke gefunden, wie die Zero-Day-Initiative von Trend Micro nun bekanntgab. Ksmbd kontrollierte die Existenz eines Dateiobjekts auf dem Server vor Operationen nicht und somit war ein Einschmuggeln von Code über das Netzwerk möglich, der dann im Kernel-Kontext ausgeführt wird. Voraussetzung dafür ist, dass Ksmbd manuell aktiviert ist. Alle Kernel-Versionen erhielten bereits einen Patch für die Schwachstelle.

Lastpass: Streuwerte gestohlen

Die LinuxWelt wird nie müde, das eigene Hosting von Diensten zu empfehlen, gerade wenn es um vertrauliche Daten geht. Wie richtig dieser Ansatz ist, zeigt ein aktueller Einbruch bei Lastpass, einem cloudbasierten Passwortdienst. Offenbar war ein Zugriff auf vertrauliche Daten gelungen. Um welche Art Daten es sich handelte, gab Lastpass kürzlich bekannt: Die Einbrecher nahmen eine Kopie der verschlüsselten Kundensafes mit, haben also schlimmstenfalls Zugriff auf die alle Kundenpasswörter, sofern ihnen der Crack des Hauptpassworts gelingt. Lastpass beschwichtigt, dass dies bei einem komplexen Hauptpasswort beinahe ausgeschlossen scheint. Wer aber ein einfaches Lastpass-Hauptpasswort verwendet, sollte alle dort gespeicherte Zugangsdaten schleunigst ändern (*https://blog.lastpass.com/2022/12/notice-of-recent-security-incident*).

Ciao, Windows 8.1

Seit 10. Januar 2023 erhält Windows 8.1 keine Updates, Fehlerbehebungen oder Sicherheitspatches mehr. Ein weiterer Einsatz ist damit mit erheblichen Risiken behaftet, gerade im Netzwerk. Auch um Office 365 und 2019 will sich Microsoft unter dem alten Windows nicht mehr kümmern. Theoretisch besteht die Möglichkeit, mit etwas Experimentierfreude kostenlos ein Upgrade auf Windows 10 zu machen. In der Praxis dürfte aber zu alte Hardware im Wege stehen. Die LinuxWelt-Redaktion rät zur Installation eines einsteigerfreundlichen Linux-Systems wie Xubuntu oder Ubuntu Mate auf gealterten Windows-Rechnern.

Android 14: Neue Wurzelzertifikate

Ab dem kommenden Android geht Google ein Problem an, das ältere Android-Versionen ab einen bestimmten Alter komplett obsolet machte: Der Zertifikatsspeicher des Betriebssystem soll ab Android 14 über die Google-Play-Services aktualisierbar sein – und nicht mehr statisch. Hier liegen die Wurzelzertifikate zur Überprüfung von TSL-Zertifikaten für HTTPS und andere Netzwerkprotokolle. Bislang konnte Android bei Austausch oder Ablauf eines Wurzelzertifikats durch eine Signaturbehörde das neue Zertifikat nicht verifizieren.

Typo 3 führt fremden Code aus

Mitte Dezember fand sich im Content-Management-System Typo 3 eine üble Lücke im Formulardesigner: Angreifer konnten über Formulare auf einer Webseite PHP-Code einschleusen, den Typo 3 dann auf dem Server ausführte. Behoben ist das Malheur ab Version 12.1.2 beziehungsweise ab den LTS-Ausgaben 11.5.20 LTS und 10.4.33 von Typo 3.

OSV-Scanner: Bibliotheken im Check

Google hat Ende letzten Jahres den länger entwickelten Open Source Vulnerability Scanner (*https://github.com/google/osv-scanner*) auf den Weg gebracht. Das Werkzeug kann Quellcode auf verlinkte, unsichere Bibliotheken überprüfen. Die Datenbank von freien, oft genutzten, aber verwundbaren Softwarekomponenten und Bibliotheken hat Google schon im Jahr davor der Allgemeinheit vorgestellt. Das Tool von Google ist in Go geschrieben und steht für Linux, Windows und Mac-OS bereit.

UPDATETELEGRAMM

LXQT 1.2
Der schlanke Desktop hat die Nachfolge von LXDE angetreten und nutzt wie KDE das Toolkit Qt 5 und 6 für seine grafischen Elemente. Die Oberfläche wirkt wie die kleine Schwester von KDE, aber bisher auch wie das hässliche Entlein. Ausgabe 1.2 verschönert Systemleisten, Terminalemulator, Dateimanager sowie Bildbetrachter. Ein neuer Powermanager macht LXQT attraktiver für Laptops. Für Lubuntu gibt es ein PPA mit frischen Paketen (*https://lxqt-project.org*).

Kali Linux 2022.04
Das Spezialsystem für Sicherheitsexperten und sicherheitsbewusste Anwender aktualisierte in seiner letzten Ausgabe im Jahr 2022 den Kernel auf Version 6.0 und erweiterte sein Arsenal um frische Tools. Mit Nethunter Pro gibt es für das Pinephone eine neue Kali-Linux-Ausgabe, welche diese Smartphones in mobile Hackinggeräte verwandelt (*www.kali.org*).

Clam AV 1.0
Nach 20 Jahren erhält der Open-Source-Virenscanner Clam AV die Versionsnummer 1.0. Die Entwicklung war gemächlich, weil Viren und Würmer unter Linux bis heute kein ernstes Problem darstellen. Für Dateiserver, die im Netzwerk auch Windows bedienen, sind Virenscanner wie Clam AV aber ein Grundschutz und ihr Einsatz deshalb auch auf Linux-Systemen zu empfehlen (*www.clamav.net*).

Tenacity 1.3
Seit dem Wechsel zur Muse-Group hat der Audioeditor Audacity wegen seiner Datenerhebung ab Version 3.0 Kritik auf sich gezogen.
Mitentwickler haben mit Tenacity und Saucedacity zwei Forks gegründet, die nun zu Tenacity verschmelzen, um Synergien zu schaffen. Tenacity macht deshalb gleich mit Versionsnummer 1.3 weiter und ist als Flatpak und Arch-Linux-Paket (AUR) verfügbar (*https://codeberg.org/tenacityteam*).

CERN setzt auf Alma Linux

Seit der Einstellung von Cent-OS als Klon von Red Hat Enterprise Linux buhlen zwei Nachfolger um die Gunst der Anwender und Admins: Rocky Linux und Alma Linux werden wie vorher Cent-OS aus den Quellcodepaketen von Red Hat gebaut. Das Forschungszentrum CERN verwendet für die eigene IT bislang Cent-OS 7, das zwar noch Fehlerbehebungen bis 2024 erhält, aber in Sachen Aktualität langsam hinterherhinkt. Nach dem Ende des Supports werden das Europäische CERN und das US-amerikanische Fermilab auf Alma Linux umsteigen, denn dieser Klon hat sich laut den Kernforschungszentren bei eigenen Tests unter realen Anforderungen am besten bewährt. Mit diesen Größen im Hintergrund dürfte die Zukunft von Alma Linux (*www.almalinux.org*) auf längere Zeit gesichert sein. ■

Entwickler: Linux vor Mac-OS

Dass Windows auf dem Desktop Marktführer ist und noch einige Weile bleiben wird, steht außer Frage. Tatsächlich ist es aber gar nicht so einfach, die Verbreitung von Linux zu quantifizieren. Nach einer Erhebung der Frage-Antwort-Website Stackoverflow unter der eigenen Anwenderschaft (zumeist Softwareentwickler) gibt es nun belastbares Zahlenmaterial: Während 49 Prozent der Entwickler Windows für die Arbeit verwenden, nutzen 40 Prozent Linux und 33 Prozent Mac-OS als Betriebssystem. Diese Angaben ergeben in Summe mehr als hundert Prozent, weil viele IT-Profis mehr als nur ein Betriebssystem nutzen. ■

20 Jahre Arch Linux

Arch Linux hat sich in den letzten 20 Jahren aus einer kleinen Variante von „Linux from Scratch“ plus Paketmanager zu einer illustren Linux-Distribution entwickelt, die vor allem Linux-Enthusiasten schätzen. Generell gilt Arch Linux als Rolling Release, das seine Pakete vergleichsweise schnell aus Upstream-Quellcode aktualisiert. Vor allem ist Arch ein Linux, das Anwender als Administratoren des eigenen Systems versteht. Den Ansatz verfolgen auch Gentoo und Void sowie Alpine. Zur Langlebigkeit von Arch Linux und dem Erfolg von Abspaltungen wie Manjaro und Steam-OS 3 trug aber vor allem ein Faktor bei: das informative Wiki *https://wiki.archlinux.org*, das unter *https://wiki.archlinux.de* auch viele Artikel in Deutsch pflegt. Eine weitere Professionalisierung durch Valve Software ist absehbar, nachdem deren hauseigenes Linux-System für das Steam Deck auf Arch Linux aufbaut. ■

Serpent-OS in erster Version

Von Ikey Doherty, dem Kopf hinter dem Budgie-Desktop und der Linux-Distribution Solus, gibt es ein neues Linux-System mit vielen neuen Ideen: Serpent-OS verfügt über einen Paketmanager, der Programme und deren Konfiguration im Stil von Nix-OS verwaltet. Das Wurzeldateisystem kann nur gelesen werden und wird im Stil von Fedora Silverblue oder Android als komplettes Image aktualisiert. Systemd erlaubt dabei die Auswahl eines früheren Systemzustands beim Booten. Die größeren Softwarepakete und der Kernel erhalten wie in Intels Clear Linux für die dominierenden Prozessortypen spezielle Compilerflags, um mehr Leistung aus der CPU herauszuholen. Ein potenzielles Problem hinter dem ambitionierten Ansatz ist die offensichtliche kurze Aufmerksamkeitsspanne des Hauptentwicklers Doherty: Nachdem er 2018 das Team von Solus unvermittelt verließ, gibt es jetzt schon wieder Zweifel an seinem Engagement für Serpent-OS. Aber jetzt gibt es nach zwei Jahren Entwicklungszeit immerhin erste ISO-Images der Distribution (*https://serpentos.com/download*). ■

Offene Karten: Overture Foundation

Um Google Maps vom Thron zu stoßen, haben sich die Tech-Riesen Microsoft, Amazon, Meta sowie das niederländische Unternehmen Tomtom unter dem Dach der Linux Foundation zusammengetan, um das eigene Kartenmaterial zu verbessern. Die Unternehmen wollen die eigenen Daten zusammenführen, aber auch freie Datensätze von Gemeinden sowie das Material von Openstreetmap nutzen und alles in ein standardisiertes Format überführen. Die neuen Karten sollen 2023 erscheinen und unter dem Community Data License Agreement stehen, das eine freie Nutzung erlaubt. ■

Wiedergeburt: Owncloud Infinity Scale

Als sich Nextcloud vor sechs Jahren von Owncloud abspaltete, wollten die verbliebenen Entwickler nicht aufgeben. Owncloud Inc. hatte seitdem mit größeren Partnern wie dem CERN eine komplette Neuprogrammierung dieser Cloudlösung in Angriff genommen. Nach vier Jahren Arbeit ist Owncloud Infinity Scale jetzt fertig, startet gleich mit Version 2.0 und verbannt PHP aus dem Back-End. Tatsächlich erscheint die PHP-Basis in Nextcloud bis heute vielen Administratoren und Anwendern in der Praxis als Hemmschuh, denn PHP war ursprünglich nicht für die Verarbeitung großer Datenmengen gemacht. Anstatt alles für PHP 8.x umzuschreiben, setzte Owncloud gleich auf das C-ähnliche und performante Go. Der Einsatz zahlt sich nun offensichtlich aus, denn Owncloud Infinity Scale sitzt durch seine Partner fest im Sattel. Die Community-Edition (*https://owncloud.com/download-server*) für eigene Server ist unter der Lizenz AGPL-3.0 weiterhin frei. ■

UPDATETELEGRAMM

Intel IWD 2.0
Im Herbst beklagten Kernel-Entwickler auf der Konferenz „Linux Plumbers Conference“ den verbesserungswürdigen Zustand der WLAN-Treiber unter Linux. Lindern soll die Probleme nun der von Intel entwickelte „Inet Wireless Dämon“, der sich als Ersatz für den alternden „WPA-Supplicant“ anbietet. IWD gilt seit 2019 als stabil, wurde aber von Ubuntu 22.10 und anderen Distributionen noch nicht als Standard übernommen (*https://iwd.wiki.kernel.org*).

OBS Studio 29
Das Open-Source-Programm zur semiprofessionellen Produktion von Streams und Videopräsentationen bekommt als neuen Codec AV1 unter AMD-Radeon-Chips und Intel Arc mit Hardwarebeschleunigung. Dies war bislang Nvidia-Grafikkarten vorbehalten. Außerdem gibt es als Audiofilter einen Drei-Band-Equalizer und etliche Fehlerbehebungen bei den schon bekannten Funktionen (*https://obsproject.com*).

KI: Freies Training mit Milliarden Bildern

Die gemeinnützige Stiftung LAION (Large-Scale Artificial Intelligence Open Network) hat eine freie Datenbank mit 5,85 Millionen Bildern und deren Beschreibungen zum Training von künstlicher Intelligenz veröffentlicht. Die Datenbank steht unter einer Creative-Commons-Lizenz und enthält die Bilder nicht selbst, jedoch die Beschreibungen und die Links zu den öffentlich abrufbaren Bildmaterialien im Web. Rund 2,3 Milliarden der Beschreibungen sind in Englisch und 2,2 Milliarden in anderen Sprachen. Um die Datenbank lokal für das KI-Training zu speichern, sind mehrere hundert TB Speicherplatz nötig (*https://laion.ai/blog/laion-5b*). ■

Meson: Aufstrebendes Buildsystem

Das freie Buildsystem Meson zum automatisierten Kompilieren größerer Softwareprojekte ist inzwischen eines der tonangebenden Rahmenwerke für den Bau freier Software. Unter anderem nutzen Systemd, Mesa und Gnome Gstreamer dieses Rahmenwerk. Jetzt hat Meson die Versionsnummer 1.0 erreicht und kann nach zehn Jahren mit Anpassungen und Erweiterungen für viele Programmiersprachen als ausgereift gelten. Fedora Linux kann den Siegeszug Mesons durch eine Auswertung seiner Pakete quantifizieren: Von 2017 bis 2022 wuchs der Anteil an Programmen mit diesem Buildsystem in den Fedora-Paketquellen von vier auf stolze 34 Prozent. ■

Neue Baustellen: Rust im Kernel

Die Basis einer Infrastruktur für die Programmiersprache Rust hat der Linux-Kernel 6.1 mit der Testumgebung Kernel CI schon ausgerollt. In absehbarer Zeit können kleinere Kernel-Subsysteme in Rust-Quellcode entwickelt werden, was hinsichtlich von Speicherzugriffen ein höheres Maß an Fehlerfreiheit und damit Sicherheit verspricht als C. Nun zeigen sich ganz praktische Probleme: Um einen Kernel kompilieren zu können, müssen Linux-Distributionen eine komplette Toolchain ausliefern, also alle Werkzeuge vom Linker bis zum Compiler. Und die Rust-Entwicklergemeinde nutzt dafür eine eigene Toolsammlung namens Rustup. Ausgerechnet die steht in einigen Linux-Distributionen wie Debian aber nicht in neuen Versionen zur Verfügung, denn es müssen erst noch Rust-Entwickler in den Distributionen gefunden werden, die sich um diese Pakete kümmern. ■

Neu: Linux Mint 21.1 „Vera“

Linux Mint rechnet anders als seine Systembasis Ubuntu: Die halbjährlichen Point Releases mit aktualisierten Installationsmedien und optionalen Software- und Kernel-Updates gelten quasi als neue Version. Mit Linux Mint 21.1 vom Dezember 2022 ist es wieder so weit.

VON HERMANN APFELBÖCK

Die Entwicklung von Linux Mint folgt stets, aber mit einigem zeitlichen Abstand, seiner Ubuntu-Basis (Ubuntu LTS mit Langzeitunterstützung). Dabei macht es auch jedes Point Release mit. Version 21.1 hat jüngst seine Systembasis auf den Stand von Ubuntu 22.04.1 gebracht – also auf das erste Point Release der Ubuntu-Langzeitversion 22.04 LTS (vom August 2022). Linux Mint bietet wie Ubuntu LTS einen Supportzeitraum von fünf Jahren (Sicherheitsupdates, Kernel-Updates, Funktionsupdates). Im Falle von Version 21.1 bedeuten dies noch verbleibende gut vier Jahre bis April 2027, da ab dem Ersterscheinen von Ubuntu 22.04 zu zählen ist (April 2022). Die Supportdauer bis 2027 gilt für alle drei Mint-Editionen.

Aufgrund seiner Produktionsweise als später Ubuntu-Epigone ist Linux Mint kein technischer Trendsetter, zumal schon Ubuntu bei seinen Langzeitversionen relativ konservativ angelegt ist. Prominentes Beispiel: Der Linux-Kernel, den Mint und Ubuntu Anfang 2023 verwenden, trägt noch die Versionsnummer 5.15 und stammt vom Ende des Jahres 2021. Das ist zweifellos konservativ und durchaus so gewollt: Linux Mint zielt auf Nutzer, die ein solides, produktives Arbeitssystem ohne Experimente wollen. Dafür wird aber in jeder Version an Mint-Systemkomponenten, Mint-Themen, Iconsets, Mausoptik fleißig gefeilt und insbesondere der Mint-eigene Desktop Cinnamon stets verbessert. Das gilt auch für das aktuelle Mint 21.1 – dazu unten mehr.

Release-Politik von Linux Mint

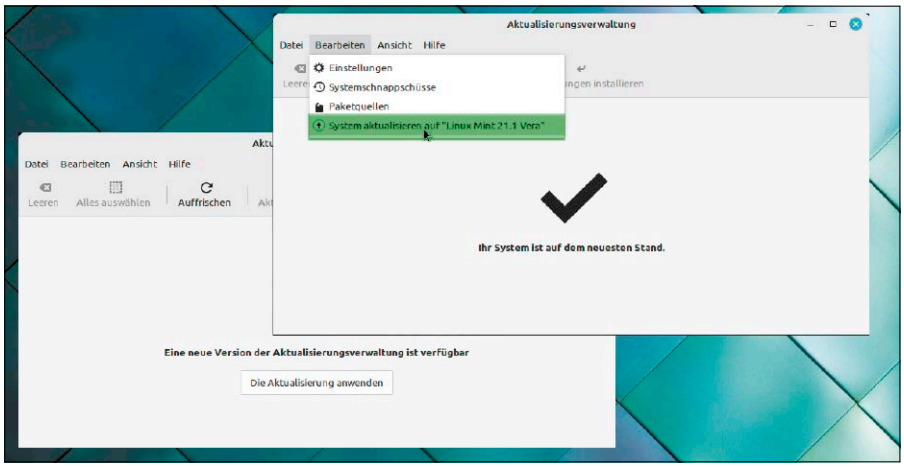
Ist Ubuntu bereits konservativ, dann Linux Mint aufgrund seiner ungefähr viermonatigen Nachzugsfrist erst recht. Und Linux Mint geht sogar noch einen Schritt weiter: Anders als Ubuntu versteht Linux Mint Point Releases mehr oder weniger als neue Versionen, die dann auch ihren eigenen Namen erhalten (Version 21.1: „Vera“). Dabei geht es um mehr als nur Etikettierung und Namenskosmetik, dann anders als bei Ubuntu ist hier eine explizite Upgradeentscheidung des Benutzers erforderlich, um den Status des nächsten Point Releases zu erreichen. Wer das nicht macht, verharrt bei der einmal installierten Version. Während sich Ubuntu-Langzeitversionen automatisch zum Stand des aktuellen Point Release aktualisieren, können Sie also beispielsweise ein Linux Mint 21 jahrelang auf diesem originalen Status erhalten. Die Aktualisierungsverwaltung liefert dann zwar die Sicherheitsupdates, jegliche Änderungen an Software, Desktop oder Kernel unterbleiben jedoch.

Ist das empfehlenswert? Aus Stabilitätsgründen kann dieser Weg gewählt werden. Man muss sich dann aber darüber im Klaren sein, dass die Mint-Upgrades immer alle Zwischenschritte gehen müssen. Solange nicht Version 21.1 vorliegt, können Sie später nicht auf Version 21.2 oder 21.3 aktualisieren, falls diese interessante Neuheiten bieten sollten. Vor allem aber können Sie 2024 nicht auf die nächste Mint-Hauptversion 22 upgraden, solange Sie nicht alle Zwischenschritte 22.1 (jetzt), 22.2. (Sommer 2023), 22.3 (Winter 2023) vollzogen

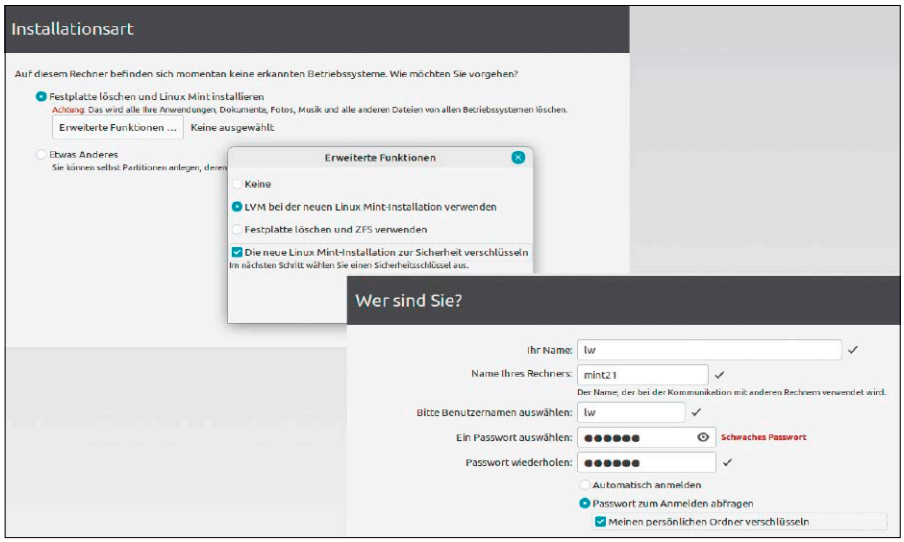
haben. In der Regel fahren normale Desktopnutzer daher am besten, wenn sie die Point Releases, also alle Unterversionen mitmachen. Wie Sie Mint 21 („Vanessa“) auf das aktuelle Mint 21.1 „Vera“ hieven, ist im folgenden Abschnitt erklärt.

Das Upgrade von Version 21

Ein laufendes Linux Mint 21 „Vanessa“ bringen Sie mit wenig Mühe auf den aktuellen Stand von Version 21.1 „Vera“. Es ist das für Linux Mint mittlerweile gewohnte Prozedere: Wenn Sie die Aktualisierungsverwaltung starten, wird der Hinweis erscheinen, dass eine „neue Version der Aktualisierungsverwaltung“ vorliegt – also des Tools, das Sie gerade nutzen. Diese Version installieren Sie über die Schaltfläche „Die Aktualisierung anwenden“. Das Werkzeug startet sich nach dem Download automatisch neu, um die neue Version der Software zu laden. Falls nicht schon geschehen, bringen Sie zunächst Mint 21 mit „Auffrischen“ und „Aktualisierungen installieren“ auf den neuesten Stand. Das eigentliche Upgrade starten Sie danach mit dem Menüpunkt „Bearbeiten → System aktualisieren auf Linux Mint 21.1 Vera“. Der Vorgang sollte nur wenige Minuten dauern, weil die Differenzpakete zwischen der Originalversion und dem ersten Point Release nicht umfangreich sind. Auch den Linux-Kernel ändert das erste Ubuntu-Point-Release generell nie: Der wird erst im nächsten Release erneuert (Februar 2023, nachfolgend Mint 21.2 circa Juni 2023).



Upgrade zur Version 21.1: Da es sich im Grunde nur um eine Aktualisierung zum Point Release handelt, ist die Aktion in wenigen Minuten erledigt.



Installation mit nach wie vor zwei Verschlüsselungsangeboten: Die Komplettverschlüsselung (oben) ist die bessere, falls Linux Mint den ganzen Datenträger übernehmen darf.

Neuinstallationen von Mint 21.1

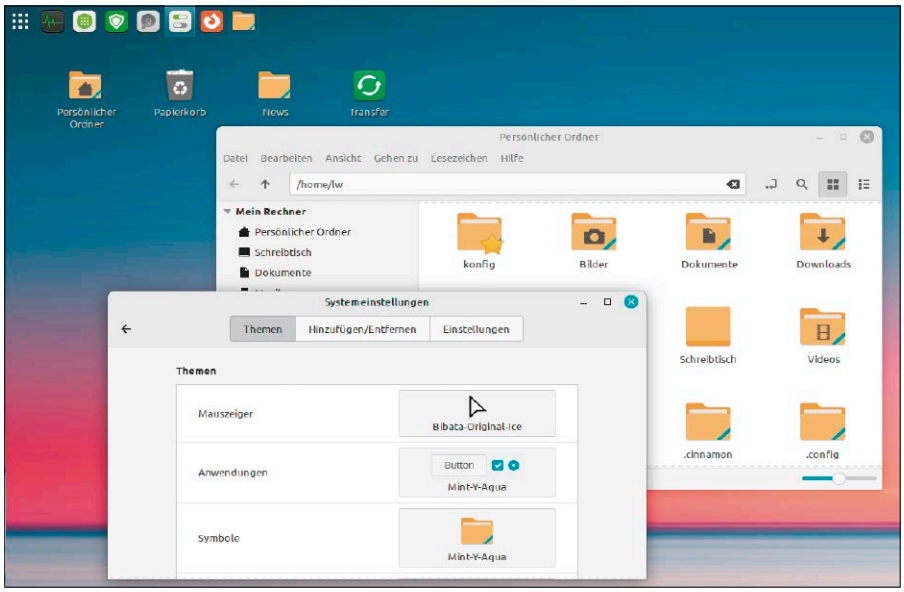
Wer Linux Mint neu installieren will, sollte immer das Installationsmedium mit der jeweils aktuellsten Version nutzen, im Moment also das neue 21.1 „Vera“. Es enthält alle Sicherheitsupdates seit der Hauptversion 21 und erspart damit viele Downloads via Aktualisierungsverwaltung. Linux Mint 21.1 ist wie gewohnt über die Projektseite *https://linuxmint.com/download.php* zu beziehen, die dann zu den eigentlichen Spiegelservern weiterverlinkt („Download mirrors“). Die Auswahl des Downloadservers spielt keine Rolle für die spätere Sprachlokalisierung. Nach wie vor bietet Linux Mint drei verschiedene Editionen mit den Desktops Cinnamon, Mate und XFCE an, wobei die Edition mit der Mint-eigenen Cinnamon-Oberfläche der eindeutige Favorit sein dürfte.

LinuxWelt-Leser, die sich für die Cinnamon-Edition interessieren, können diese als Livesystem von der beiliegenden Heft-DVD starten und installieren. Das Livesystem liegt auch als originales ISO-Image auf der Heft-DVD (unter „Image-Dateien“) und kann auf USB kopiert werden.

Der Download der beiden anderen Editionen (Mate, XFCE) beträgt jeweils 2,5 GB. Das heruntergeladene ISO-Image muss mit den üblichen Mitteln (Etcher, Win 32 Disk Imager, USB Imager, Gnome-Disks, dd) auf USB kopiert werden, um es danach am Zielrechner zu booten und zu installieren.

Egal ob Heft-DVD oder ISO-Download – es handelt sich in jedem Fall um ein Livesystem, das ein Ausprobieren der jeweiligen Edition sowie die Installation über den einzigen Desktoplink „Install Linux Mint“ ermöglicht. Zum Setup verwenden alle drei Mint-Editionen das identische Installationsprogramm, den Ubuntu-Installer Ubiquity. Die Unterschiede zum originalen Ubiquity werden zunehmend geringer, nachdem das Mint-Team seit Version 21 unter „Installationsart“ das fortgeschrittene Dateisystem ZFS unter „Erweiterte Funktionen“ anbietet. ZFS halten wir für ein Desktopsystem für überdimensioniert. Linux Mint war einige Versionen derselben Meinung, übernimmt diese Option aber mittlerweile vom originalen Ubuntu-Installer.

Als einzige nennenswerte Abweichung bleibt die Home-Verschlüsselung bei der Einrichtung des ersten Kontos („Wer sind Sie?“). Hier erscheint weiterhin die Option „Meinen persönlichen Ordner verschlüsseln“. Wenn Sie diese aktivieren, wird das



Aufgefrischte Optik für alle Mint-Editionen: Mit neuen Farben, Symbolen und Mausthemen verabschiedet sich Mint von der mintgrünen Prägung. Konservative können aber jederzeit zur früheren Optik zurückkehren.

Home-Verzeichnis dieses Erstkontos mit allen Benutzerdateien und Konfigurationsdateien verschlüsselt (mit Ecrypt FS). Die geschützten Daten werden bei der Systemanmeldung automatisch entschlüsselt, durch Abmeldung oder Herunterfahren automatisch verschlüsselt. Unterm Strich ist aber die Vollverschlüsselung (Luks/Cryptsetup) an früherer Stelle des Setups sicherer und schneller („Installationsart → Erweiterte Funktionen → LVM…verwenden → Die […]-Installation […] verschlüsseln“.

Linux Mint 21.1: Allgemeine Neuerungen

Linux Mint 21.1 gibt es weiterhin in Editionen mit Cinnamon-, Mate- und XFCE-Desktop. Während von den Desktops Mate mit Version 1.26 und XFCE mit Version 4.16 keine Neuerungen kommen, erhält der Mint-eigene Cinnamon 5.6 etliche Neuigkeiten (siehe unten). Alle drei Editionen stellen keine hohen Hardwareansprüche. Als Minimalanforderungen nennt das Mint-Team für alle drei Ausgaben dasselbe – nämlich zwei GB RAM sowie 20 GB Festplattenplatz, was allenfalls für die XFCE-Edition ausreichen könnte. Vier GB RAM und 100 GB auf Platte sowie mindestens eine Dualcore-CPU mit zwei GHz sollte man der Cinnamon-Edition unbedingt anbieten.

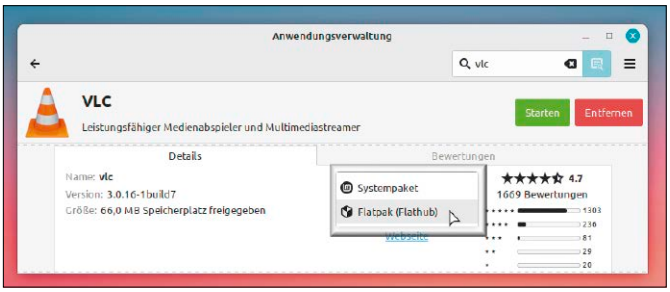
Themen und Farben: Das Erscheinungsbild aller Editionen wurde durchgehend modernisiert: Version 21.1 verabschiedet sich vom standardmäßigen Mint-Grün und nutzt in der aktuellen Version standardmäßig ein blaues Thema („Mint-Y-Aqua“). Die Ordnersymbole sind bei diesem Thema in Gelb mit einer kleinen blauen diagonalen Linie. Ganz Mint-typisch sind diese Standards aber nur ein Vorschlag: Unter „Systemeinstellungen → Themen → Symbole/Anwendungen“ gibt es reichlich Varianten, um zu älteren Themen zu wechseln („Mint-Y-Legacy“), zum Teil auch zur Ubuntu-Optik („Yaru“-Themen).

Mausthemen: Mehr als optische Marginalie sind die neuen „Bibata“-Themen für den Mauszeiger. Der bunte, sich drehende Aktivitätscursor bei ressourcenintensiven Aktionen ist noch eher optisches Gimmick. Der dezent bunt wechselnde Mauszeiger bei Größenänderungen an Fenstern hilft hingegen aktiv bei der Fensterskalierung. Man erkennt schneller, wann der richtige Pixelbereich für Größenänderungen getroffen ist. Voraussetzung für die hübschen und funktionalen Mauszeiger ist, dass unter „Systemeinstellungen → Themen → Mauszeiger“ ein „Bibata“-Cursor ausgewählt wird. Unter XFCE („Maus und Touchpad“) und Mate („Erscheinungsbildeinstellungen → Anpassen“) sind die Zeigerthemen anders verortet, aber natürlich ebenfalls konfigurierbar.

Desktopsymbole: Der Mint-Desktop zeigt standardmäßig keine Symbole mehr (abgesehen von der Installer-Verknüpfung im Live- und Installationsmedium). Jedoch behält die Arbeitsoberfläche uneingeschränkt alle bekannten Fähigkeiten als Datei-, Ordner-, Starter- und (nur in Cinnamon) als Deskletablage. Wer die gewohnten Standardicons wie Papierkorb oder „Persönlicher Ordner“ aktivieren will, kann das in allen Editionen unter „Systemeinstellungen → Schreibtisch“ jederzeit erledigen.

Reduzierte sudo-Abfragen: Die Notwendigkeit von Passworteingaben wurde systemweit hinterfragt und – wo möglich – die Eingabepflicht reduziert. So startet die „Treiberverwaltung“ (mintdrivers) jetzt im Benutzermodus und der Nachweis des sudo-Rechts ist erst nötig, wenn tatsächlich Treiber installiert werden. Synaptic und die Aktualisierungsverwaltung registrieren ein einmal eingegebenes Kennwort und fordern es nicht mehrfach für mehrere Aktionen. Auch bei der Deinstallation von im Benutzerkonto installierter Flatpaks fragt Linux Mint nicht mehr nach dem Kennwort.

Flatpak: Die Unterstützung für Flatpak-Software ist generell vertieft: In der grafischen „Anwendungsverwaltung“ erhält die Übersicht über installierte Anwendungen jetzt den Hinweis „Flathub“ (oder eine andere Flatpak-Quelle), wenn es sich um einen Flatpak-Container handelt. Bei der Auswahl neuer Software gibt es für jedes Programm, das als klassisches Paket wie als Flatpak bereitsteht, das Drop-down-Feld mit den Einträgen „Systempaket“ und „Flatpak“. Dies erlaubt den schnellen Vergleich von Softwareversionen und Downloadgrößen. Die „Aktualisierungsverwaltung“ wiederum erledigt Updates für Flatpaks genauso wie für klassische Debian-Pakete. Übri-



Verbesserte Flatpak-Integration: Die Anwendungsverwaltung erlaubt für eine gesuchte Software den schnellen Vergleich zwischen dem klassischen Paket und dem Flatpak.

gens: In der Ablehnung des konkurrierenden Snap-Formats bleibt sich Linux Mint treu: Das System hat Snap-Verbot, solange die Datei „/etc/apt/preferences.d/nosnap.pref“ existiert.

X-Apps: Diese Zubehörprogramme sorgen seit Jahren für Homogenität in allen Editionen. Wichtige X-Apps sind der Texteditor Xed („Textbearbeitung“), der Player Xreader („Dokumentenbetrachter“) oder der Bildbetrachter Xviewer. Für das aktuelle Mint 21.1 verbessert wurde das Peer-to-Peer-Werkzeug Warpinator zum Datenaustausch im lokalen Netz, das sich aus jetzt Sicherheitsgründen nach einer Stunde automatisch beendet. Das Tool Webapps (webapp-manager) erhält weitere Optionen, unter anderem, um die gewünschte Webseite im privaten Modus abzurufen. Webapps ist ein praktisches Werkzeug, um Internetseiten wie lokale Software (ohne Browsernavigation) in das System und das Hauptmenü zu integrieren.

Linux Mint 21.1: Cinnamon-Edition

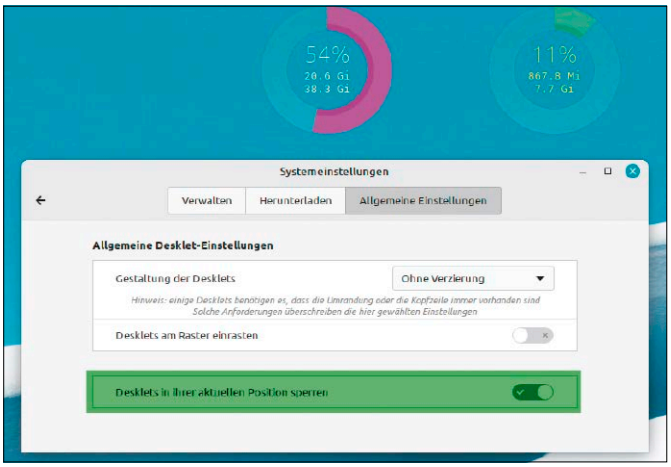
Cinnamon 5.6 und zugehörige Komponenten wie der Dateimanager Nemo oder die Systemeinstellungen haben für die Zwischenversion 21.1 kleine, aber feine Neuerungen erhalten.

Systemmeldungen: In den Systemeinstellungen können Sie unter „Meldungen“ die Dauer der eingeblendeten Systembenachrichtigungen steuern. Der Standard steht auf vier Sekunden. Wer nichts verpassen will, kann diesen Wert höher setzen.

Desklets sperren: Desklets, also die optionalen grafischen Info-Widgets am Cinnamon-Desktop, lassen sich nun positionell sperren. Die neue Option finden Sie unter „Systemeinstellungen → Desklets → Allgemeine Einstellungen“.

Monitoreinstellungen: Die grundlegenden Anzeigeeinstellungen für Auflösung, Skalierung, Frequenz unter „Systemeinstellungen → Bildschirm“ sind nun direkt am Desktop mit Rechtsklick erreichbar. Dieser Link ist derzeit noch nicht Deutsch übersetzt und lautet „Display Settings“.

Leisten-Applet „Eckleiste“ (cornerbar): Zu den Cinnamon-Neuerungen gehört ein Applet in Form eines unscheinbaren Balkens in der Systemleiste, das beim Mausklick die offenen Fenster ausblendet, um einen Blick auf den Desktop zu gewähren. Beim Rechtsklick zeigt das Applet weitere Funktionen wie Arbeitsflächenübersicht und Fensterübersicht. Welche Funktion man beim Mausklick oder Mittelklick priorisiert, lässt sich in den Applet-Einstellungen definieren.

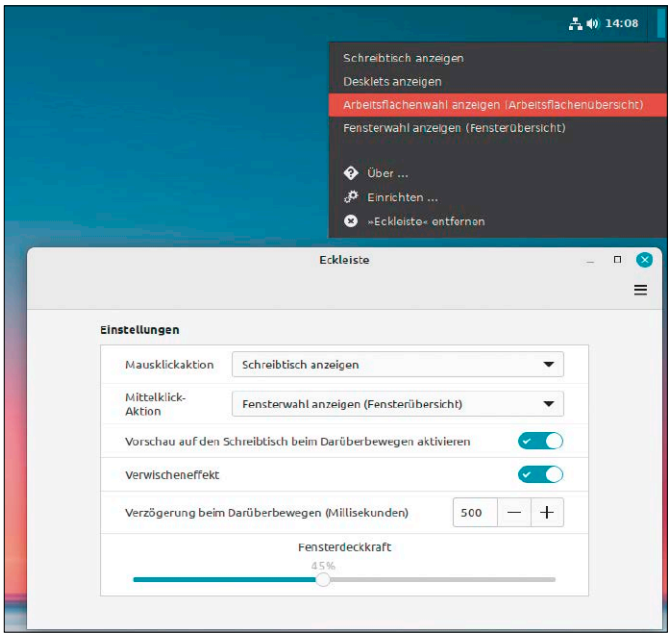


Fester Ort für Cinnamon-Desklets: Eine zusätzliche Option in den Systemeinstellungen verhindert versehentliches Verschieben von Desklets.

Nach Rechtsklick auf die Systemleiste und „Applets“ ist die „Eckleiste“ mit dem Plussymbol zu aktivieren und mit dem Zahnradsymbol näher zu konfigurieren. Wenn es nicht automatisch ganz links eingeordnet wird, muss man dies über den „Leistenbearbeitungsmodus“ per Drag & Drop korrigieren. Das relativ kleine Control ist nur in der ganz linken oder rechten Bildschirmecke ohne Zielmanöver gut zu erreichen.

Das Applet ist eindeutig funktionsreicher als der altbekannte Vorgänger „Schreibtisch anzeigen“ (show-desktop). Mit einer „Aktiven Ecke“ (siehe Systemeinstellungen) ist aber Vergleichbares zu erreichen. Die beiden Funktionen können sich aber durchaus ergänzen, dann allerdings auf keinen Fall in derselben Bildschirmecke.

Dateimanager: In der Nemo-Adresszeile war bislang Strg-L zum Umschalten zwischen Textpfad und Breadcrumb-Anzeige notwendig. Dies vereinfacht Nemo jetzt, indem ein schlichter Mausklick auf den Breadcrumb-Pfad zur ausgeschriebenen Anzeige wechselt und die Taste Esc wieder zurück. Nemo verzichtet außerdem standardmäßig auf eine Menüanzeige. Diese kann interaktiv mit Alt-Taste oder dauerhaft mit „Ansicht → Menüleiste“ aktiviert werden. Als winzige neue Funktionserweiterung bietet Nemo für ISO-Dateien die neue Kontextoption „Verify“ (bislang noch nicht Deutsch übersetzt). Diese kann die Prüfsumme und somit die Echtheit von ISO-Dateien verifizieren. ■



Leistenapplet „Eckleiste“: Das winzige Balken-Control ganz rechts oben kann die bisherigen Funktionen „Aktive Ecken“ und „Schreibtisch anzeigen“ ersetzen.

Problemlösungen für Ubuntu 22.04

Auch LTS-Versionen Ubuntus sind nicht frei von Versäumnissen der Entwickler oder von eigenwilligen, unpraktischen Standardeinstellungen. Die folgende Sammlung präsentiert häufige Probleme und deren Lösungen in Ubuntu 22.04 LTS und Varianten.

VON DAVID WOLSKI

Kaum eine andere Distribution bekommt bei jeder Ausgabe so viel Aufmerksamkeit wie Ubuntu. Die Entwicklung von Ubuntu und die einzelnen Softwarepakete sind weiterhin eng mit Debian GNU/Linux verbunden, da dies die Basis für Ubuntu stellt. Auch im Entwicklerteam gibt es einige personelle Überschneidungen. Die Größe der Ubuntu-Community erlaubt eine Veröffentlichung alle sechs Monate und eine Ausgabe mit Langzeitsupport von fünf Jahren im Zweijahresrhythmus. Die praktische Erfahrung seit April hat gezeigt, dass Ubuntu 22.04 nicht weniger Probleme macht als noch die LTS-Version 22.04. Einige Schwierigkeiten mit Firefox als Snap-Paket und mit dem aggressiven Out-of-Memory-Killer von Systemd verlangen Nacharbeiten, die eine LTS-Version Ubuntus eigentlich vermeiden sollte. Einige dieser Probleme und Lösungen sind keine Fehler, sondern einfach auf einem Desktopsystem unpraktische Standardeinstellungen. Canonical hat mit seiner Linux-Distribution heute eher Server- und Cloud-instanzen als den Endanwender-Desktop im Fokus.

Die folgenden Themen behandeln Stolperfallen und Ungereimtheiten, die uns in der Redaktion selbst in Ubuntu 22.04 begegnet sind oder für welche auf der Frage-Antwort-Webseite *https://askubuntu.com* besonders häufig nach Lösungen gesucht wird. Einige der präsentierten Lösungen sind auch für Ubuntu 22.10 beziehungsweise im kommenden 23.04 relevant, denn auch dort werden wieder Snap-Pakete zu bändigen sein.

OOMD: Aggressiver Programmkiller

Server sollen auch in Situationen mit wenig freiem Arbeitsspeicher weiterlaufen und dürfen im Falle eines Speichermangels nicht einfach stehenbleiben. Systemd hat deshalb den Out-of-Memory-Dämon (OOMD) für Server eingeführt, der besonders speicherhungrige Prozesse bei knappem Arbeitsspeicher radikal beendet. Ab Ubuntu 22.04 ist dieser Programmkiller auch auf Desktopinstallation aktiviert und verursachte vielen Anwendern Probleme, weil vor allem Browserinstanzen auf Rechnern mit weniger als vier GB RAM oft abgeschossen wurden.

```
jammy@jellyfish: ~
            0 htop
[ 4498.074931] oom-kill:constraint=CONSTRAINT_NONE,nodemask=(null),cpuset=/,mems_allowed=0,global_oom,task_memcg=/user.slice/user-1000.slice/user@1000.service/app.slice/app-gnome-libreoffice\x2dwriter-2859.scope,task=soffice.bin,pid=2943,uid=1000
[ 4498.074977] Out of memory: Killed process 2943 (soffice.bin) total-vm:2232568kB, anon-rss:766672kB, file-rss:0kB, shmem-rss:0kB, UID:1000 pgtables:2996kB oom_score_adj:0
[ 4503.384477] audit: type=1400 audit(1672730570.606:258): apparmor="ALLOWED" operation="connect" profile="libreoffice-soffice" name="/run/user/1000/at-spi/bus" pid=8472 comm="soffice.bin" requested_mask="wr" denied_mask="wr" fsuid=1000 ouid=1000
[ 4503.429405] audit: type=1400 audit(1672730570.650:259): apparmor="ALLOWED" operation="file_perm" profile="libreoffice-soffice" name="/run/user/1000/at-spi/bus" pid=8472 comm="soffice.bin" requested_mask="r" denied
```

Übereifriger Programmkiller: OOMD ist in Ubuntu 22.04, 22.10 und 23.04 unterwegs. Auf Desktopsystemen mit weniger als vier GB RAM hilft ein Abschalten des Dienstes.

In Ubuntu 22.04.1 LTS und 22.10 gab es deshalb außerplanmäßige Updates für OOMD: Der Out-of-Memory-Dämon hat in der Konfigurationsdatei „/usr/lib/systemd/system/-.slice.d/10-oomd-root-slice-defaults.conf“ die Ergänzung „ManagedOOM Swap=auto“ erhalten und ignoriert deshalb zumindest Auslagerungsaktivitäten. Auf Systemen mit wenig Arbeitsspeicher wird OOMD auf Desktops aber weiterhin Programme beenden, die plötzlich sehr viel RAM beanspruchen. Um das Verhalten zurückverfolgen, dient folgendes Kommando, das die letzten Aktionen des automatischen Programmkillers in den Kernel-Meldungen mit den Zeilen „Out of memory“ zeigt:

```
sudo dmesg
```

Um OOMD in Ubuntu dauerhaft zu deaktivieren, dient dieser Befehl:

```
systemctl disable --now systemd-oomd
```

Nach unserer Einschätzung ist OOMD auf Desktopsystemen nicht hilfreich und nicht notwendig.

Snaps: Updates anhalten

Über ein gewöhnliches Systemupdate mittels apt wird Snap-Software nicht aktualisiert. Stattdessen verfügen Snaps über eine separate Updatefunktion, die alle installierten Pakete dieser Art täglich automatisch viermal aktualisieren will. Im Terminal zeigt das Kommando

```
snap refresh --time
```

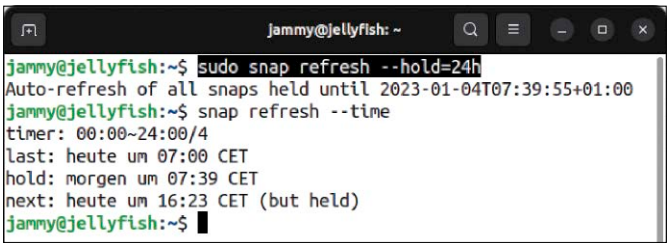
an, wann der nächste Check erfolgen soll. Diese kurze Frequenz hat einen Haken: Läuft eine Snap-Anwendung, so kann das Paket nicht aktualisiert werden und wird seit Ubuntu 22.04 auf den nächsten Updatecheck verschoben. Um neue Versionen installierter Snaps manuell zu installieren, kann dann der eingegebene Befehl

```
sudo snap refresh
```

manuell eine Aktualisierung ausführen. Unterwegs mit einem Notebook, wenn eine Internetverbindung deutlich langsamer ist, sorgt das automatische Update von Snaps wegen der knappen Bandbreite für Ungemach und wird eventuell gar nicht fertig. Für diesen Fall gibt es die neue Möglichkeit, Updates auszusetzen. Dafür ist eine aktuelle Version des Snapd-Rahmenwerks nötig, welche der Befehl

```
sudo snap refresh snapd --channel=latest/edge
```

installiert. Anschließend kann die Eingabe des Kommandos



Einen Tag lang anhalten: Damit Snap-Aktualisierungen im Hintergrund nicht Bandbreite verschwenden, können diese Updates mit diesem Befehl aufgeschoben werden.

Wo bleibt der Sound? Die Mixeranwendung Pavucontrol kann die Audioeinstellungen, Geräte und Ausgänge überprüfen. In diesem Beispiel fehlt in Ubuntu 22.04 eine Konfigurationsdatei.

```
sudo snap refresh --hold=24h
```

die automatische Installation von neuen Snap-Versionen für 24 Stunden anhalten.

Pipewire und Pulseaudio

Bei der Wahl der Soundserver setzt Ubuntu 22.04 auf einen Mix aus dem herkömmlichen Pulseaudio und dem modernen Pipewire. Letzteres ist im System für Screensharing und Web RTC in Browsern unter Wayland zuständig. Die sonstigen Aufgaben bei der Soundausgabe erledigt weiterhin Pulseaudio.

Es passiert vor allem bei Upgrades von älteren Ubuntu-Systemen auf 22.04, dass Pulseaudio in diesem Gespann zunächst nicht funktioniert. Die Mixeranwendung Pavucontrol ist zur Überprüfung nötig, ob die Ausgabe überhaupt unter „Konfiguration“ eingeschaltet ist. Sie muss aber zunächst mit

```
sudo apt install pavucontrol
```

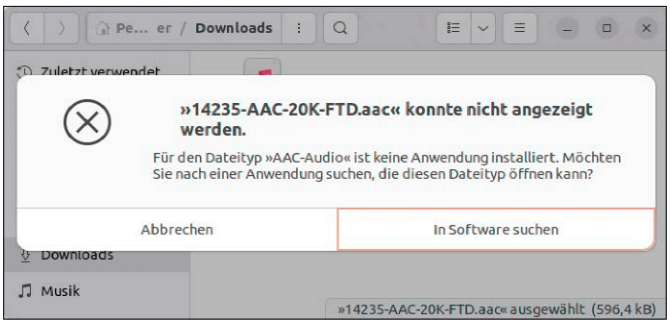
installiert werden. Gibt es keine Ausgänge für Pulseaudio beziehungsweise nur ein Ausgabegerät namens „dummy“, so ist meist die Konfiguration nach einem Upgrade nicht komplett. Die beiden Befehle

```
sudo touch /usr/share/pipewire/media-session.d/with-pulseaudio
systemctl --user restart pipewire-session-manager
```

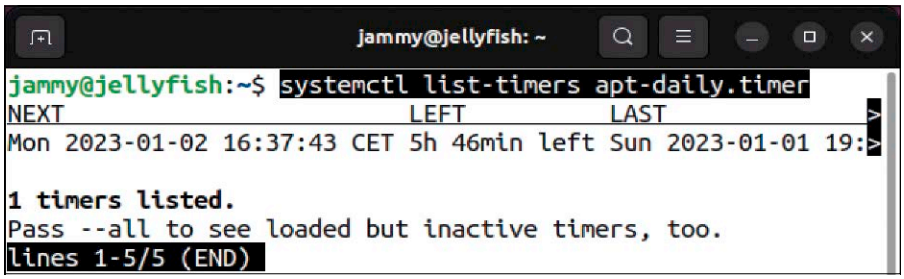
korrigieren das Problem.

Nachrüsten: Codecs und Extras

Ubuntu liefert in seinen Paketquellen nicht nur Open-Source-Programme aus, sondern auch Linux-Software, die einer kommerziellen oder auch unklaren Lizenz unterlie-



Diese Suche läuft oft ins Leere: Gnome versucht, ein passendes Programm für eine Mediendatei zu finden, und kann auch nach Codecs suchen, aber dies gelingt meistens nicht.



Wann ist die nächste Systemaktualisierung? Die von Haus aus aktivierten „Unattended Upgrades" blockieren den Paketmanager bei umfangreichen Updates eine ganze Weile.

gen. Dazu zählen einige Audio- und Videocodecs und Truetype-Fonts von Microsoft, die für die Darstellung einiger Webseiten und Dokumente vorteilhaft sind. Die von einigen Gnome-Programmen angebotene Suche nach Codecs in den Paketquellen ist nicht immer erfolgreich. Zuverlässiger ist es, gleich nach der Ubuntu-Installation alle häufig benötigten Codecs und Extras in einem Terminalfenster mit diesem Befehl

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

nachzurüsten.

Blockiertes apt: Unattended Upgrades

Eher für Server interessant, aber auch in der Desktopausgabe von Ubuntu 22.04/22.10 aktiviert, ist die automatische Installation von Sicherheitsupdates im Hintergrund über den Dienst „Unattended Upgrades". Damit die Server der Paketquellen dabei nicht überlastet werden, lösen Ubuntu-Systeme den Download an zufälligen Zeiten aus. Wann das eigene System wieder ein Hintergrundupdate startet, zeigt das Kommando

```
systemctl list-timers apt-daily.
 timer
```

in der Kommandozeile an.

Bei langsamen Internetverbindungen oder im WLAN führt dies nach dem Start des Systems immer wieder dazu, dass der Paketmanager apt längere Zeit nicht für andere Aktionen verfügbar ist, weil im Hintergrund Updates installiert werden. Der Hinweis von apt in der Kommandozeile lautet dann „E: Could not get lock /var/lib/dpkg/lock - open (11: Ressource unavailable)".

Wenn dies ein immer wieder auftretendes Problem ist, dann empfiehlt es sich, die Aktualisierungen besser regelmäßig manuell mit *sudo apt upgrade* einzuspielen und die automatischen Sicherheitsupdates abzuschalten. Auf Desktopsystemen ist dies völlig legitim. Um den Dienst zu konfigurieren, dient der Aufruf dessen Konfigurations-Scripts:

```
sudo dpkg-reconfigure -plow
 unattended-upgrades
```

In einem angezeigten textbasierten Menü schaltet dann die Auswahl „Nein" die automatischen Updates aus.

Paketmanager: Werbung abschalten

Wer in Ubuntu 22.04 mit apt in der Kommandozeile Updates und das Paketmanagement vornimmt, erhält beim Aufruf im Terminal hin und wieder Werbung für Ubuntu Pro. Dies ist ein Extraservice Canonicals, welcher nach einer Registrierung insgesamt zehn Jahre Updates für Ubuntu LTS verspricht. Nach Kritik an den zusätzlichen Nachrichten hat Canonical verraten, dass sich diese Werbeeinblendungen mit dem Kommando

```
sudo pro config set apt_news=false
```

sehr einfach abschalten lassen.

Server: Einfachere Netzwerkkonfiguration

Während Debian-Server ihre Netzwerkeinstellungen im alten Stil über die Datei „/etc/network/interfaces" erledigen, nutzt der Ubuntu Server schon seit Ausgabe 18.04 LTS seine eigene Konfigurationsmethode über Netplan.io. Es handelt sich dabei um einen Parser für das YAML-Format, um auch komplexe Netzwerkkonfigurationen abzubilden. Netplan.io ist aber speziell für die Ubuntu-Server-Ausgabe gemacht und in keiner anderen Linux-Distributionen per Standard eingerichtet. Von Canonical gibt es auf der Webseite *https://netplan.io* eine Vorstellung mit englischsprachigen Beispielen zum Einstieg.

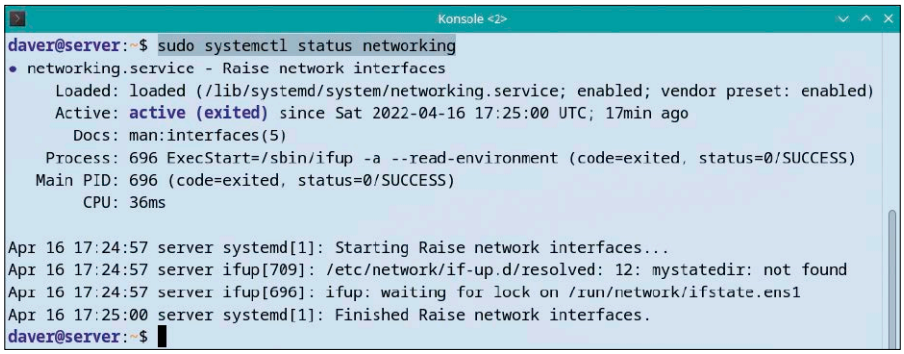
Netplan.io ist nur eine Abstraktionsschicht mit eigener Syntax. Wer diese nicht verwenden will, kann wieder die herkömmliche Netzwerkkonfiguration im Debian-Stil auf einem Ubuntu-Server nutzen, der dabei aber vorübergehend offline geht. Das ist beim Wechsel zu bedenken. Zuerst gilt es, den Hardwarenamen der Netzwerkschnittstelle zu ermitteln, die der Befehl

```
ip a
```

im Abschnitt „2:" für Ethernet anzeigt und die beispielsweise „enp3s0" lautet. Diese Angabe muss man sich notieren, denn sie ist für die herkömmliche Konfigurationsdatei wichtig.

ALTERNATIVE NETZWERK-KONFIGURATION

```
#loopback
#Datei /etc/network/interfaces
auto lo
iface lo inet loopback
#Ethernet, "enp3s0" bitte anpassen
auto enp3s0
allow-hotplug enp3s0
iface enp3s0 inet dhcp
```



Herkömmliche Netzwerkkonfiguration in Ubuntu 22.04 nutzen: Die Ausgabe von systemctl zum traditionellen Netzwerkdienst zeigt, ob der Umstieg geklappt hat, und hilft bei der Fehlersuche.

Den herkömmlichen Debian-Netzwerkdienst installiert dann dieses Kommando:

```
sudo apt install ifupdown
```

Wie bei Debian erwartet dieser Dienst eine klassische Konfigurationsdatei namens „/etc/network/interfaces“, die mit root-Recht erstellt wird:

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

Diese Datei erhält den Inhalt, wie er im Kasten „Alternative Netzwerkkonfiguration“ hier abgebildet ist. Die Angabe „enp3s0“, also der vorher ermittelte Hardwarename der Schnittstelle, muss unbedingt angepasst werden. Damit die Netzwerkschnittstelle automatisch über DHCP ihre IPv4- und IPv6-Adressen bezieht, verlangt auch noch die Datei „/etc/dhcp/dhclient.conf“ eine Ergänzung: Ganz unten fügt man hier diese Zeile ein:

```
send dhcp-client-identifier =
  hardware;
```

Nun kann vor dem Neustart des Serversystems der Systemd-Dienst für Netplan.io mit folgendem Kommando deaktiviert werden:

```
sudo systemctl mask networkd-
  dispatcher systemd-networkd-wait-
  online systemd-networkd.socket
  systemd-networkd
```

Danach steht der Neustart des Ubuntu-Systems mit *sudo reboot* an und dort zeigt dann die Eingabe von

```
sudo systemctl status networking
```

an, ob alles geklappt hat. Schlägt die Initialisierung des Netzwerks fehl, so liegt dies meist an einer ungültigen Hardwareadresse der Ethernet-Schnittstelle und es lohnt sich hier eine erneute Kontrolle auf die Ausgabe von „ip a“.

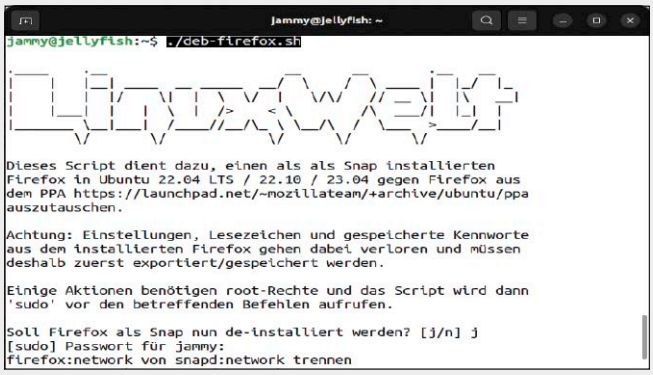
Ubuntu-Server bei Internetprovidern: Ist ein Ubuntu-Server nur per SSH erreichbar, dann ist diese Operation durchaus riskant, denn schlimmstenfalls ist die Maschine erst mal nicht erreichbar. Es empfiehlt sich deshalb zuvor als Nothaken, die Möglichkeiten einer Verbindung zum Server per KVM oder webbasierter Konsole zu aktivieren oder auch gleich alle Schritte über eine Notfallkonsole auszuführen. Die meisten Serveranbieter und Clouddienste bieten diese an. ■

FIREFOX UND CHROMIUM ALS DEB-PAKET

Als Canonical ausgerechnet Chromium und dann auch noch den Standardbrowser Firefox als Snap-Paket in Ubuntu auslieferte, war die Skepsis bei vielen Anwendern zu Recht groß. Denn die Browser starten als Snap zu langsam und einige Add-ons wollten auch nicht mehr funktionieren, weil Berechtigungen fehlen. Mittlerweile hat Canonical bei der Einbindung von Firefox nachgebessert – der Start ist deutlich flotter und viele Erweiterungen wie etwa die Gnome-Browsererweiterung zur Einbindung von Gnome-Shell-Extensions von *https://extensions.gnome.org* funktionieren wieder. Dennoch bleibt der Start auf Systemen mit schwächeren CPUs zunächst bei beiden Browsern schleppend, denn Snaps liefern ein gepacktes Dateisystem mit, das erst mal dekomprimiert werden will.

Firefox und Chromium gibt es in den aktuellen Ubuntus nicht mehr in den offiziellen Paketquellen. Allerdings liefern weiterhin PPAs, also externe Paketquellen, die Webbrowser stets aktuell in der üblichen Form als DEB-Paket aus: Für Firefox gibt es von der Mozilla Foundation das PPA *https://launchpad.net/~mozillateam/+archive/ubuntu/ppa* und für Chromium bietet sich *https://launchpad.net/~phd/+archive/ubuntu/chromium-browser* an. Eine Schwierigkeit ist es aber, Firefox oder Chromium als Snap erst einmal loszuwerden. Denn bei dem vorhandenen DEB-Paket in den Standard-Paketquellen handelt es sich um einen Platzhalter, der immer wieder das Snap installiert. Auch ein Systemupdate würde den als DEB installierten Firefox wieder gegen das Snap-Paket austauschen.

Es ist also mehr zu beachten: Per apt-Pinning muss das nachträglich installierte DEB eine höhere Priorität bekommen als das Snap-Paket aus den regulären Quellen. Gut ist es außerdem, falls die unbeaufsichtigten Updates aktiviert sind, diese auf Firefox beziehungsweise Chromium automatisch auf den neusten Stand bringen. Insgesamt kommen hier eine Menge kleine Handgriffe im Terminal zusammen, die in der Wiederholung auf mehreren Ubuntu-Systemen lästig werden. Wir haben deshalb für die Installation von Firefox und Chromium über die



Firefox als DEB-Paket: Das Script von Heft-DVD deinstalliert das Snap-Paket in Ubuntu 22.04 und holt den Browser vom offiziellen PPA der Mozilla Foundation.

genannten PPAs jeweils ein Shell-Script erstellt, dass diese Handgriffe übernimmt und dabei gut nachvollziehbar ist. Für Firefox ist das Script „deb-firefox.sh“ im Unterverzeichnis „Software“ auf der Heft-DVD und für Chromium erledigt „deb-chromium.sh“ die Installation. Zuvor werden die Browser als Snap erst deinstalliert, falls vorhanden. Diese Aktionen verlangen nach dem sudo-Passwort und fragen dies im Terminal zuvor ab. Um eines der Scripts zu starten, kopiert man es in einen beliebigen Ordner, macht es mit

```
chmod +x deb-firefox.sh
```

ausführbar und ruft es dann mit

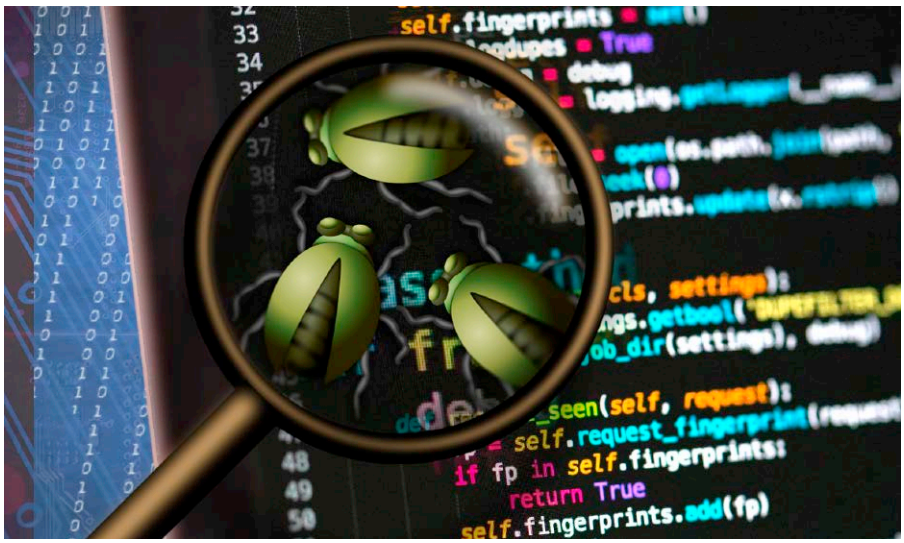
```
./deb-firefox.sh
```

auf. Das Script „deb-chromium.sh“ verlangt die gleiche Behandlung. Die weiteren Schritte sind in der Ausgabe des jeweiligen Scripts erläutert und es gibt auch eine kurze Anleitung, wieder das Snap zu installieren, falls gewünscht.

Hinweis: Eine Deinstallation des Snap-Pakets löscht alle vorhandenen Profildaten, Lesezeichen und eventuell gespeicherten Passwörter. Diese Daten sollte man deshalb zuvor exportieren und danach im klassischen DEB-Browser wieder importieren.

Kleine Geschichte großer Bugs

Die Geschichte von Hardware und Software ist geplagt von Fehlern – allgemein als „Bugs“ bezeichnet. Wir werfen einen historischen, unterhaltsamen Blick auf jene Fehler, welche uns die IT immer wieder vermiesen.



VON DAVID WOLSKI

Wo programmiert wird, schleichen sich Fehler ein – aus Unkenntnis, Versehen, durch äußere Einflüsse oder kurzsichtige Planung. Die perfekte Rechenmaschine, den perfekten Computer mit mehreren Subsystemen wird es nicht geben. Diese Erkenntnis lehrt schon eines der ersten Computerprogramme überhaupt, geschrieben 1842 von Ada Lovelace für die geplante und nie gebaute analytische Rechenmaschine von Charles Babbage.
Bei diesem Bug handelt es sich um eine Verwechslung von Variablen: Wo „v5 / v4“ gedruckt ist, hätte „v4 / v5“ stehen müssen. Zur Entschuldigung von Ada Lovelace: Es kann sich dabei auch schlicht um einen Setzerfehler handeln.

Frühe Käferkunde: Edisons Fehlersuche

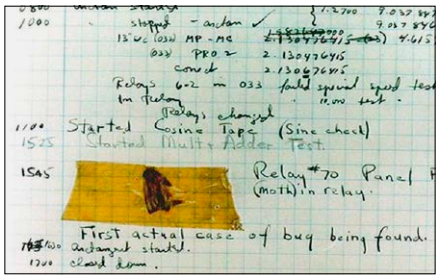
Der Begriff „Bug“ für Fehler in der Entwicklung oder Ausführung kommt definitiv aus dem Ingenieurswesen und war schon Ende des 19. Jahrhunderts verbreitet. Das verraten die Aufzeichnungen von Thomas Alva Edison, der für Fehlfunktionen eines Telegrafiegeräts 1870 häufig das Wort „Bug“ in Briefen an Kollegen verwendete – auch schon mit einer Portion Humor. So beginnt Edison schon mit einer fiktiven Klassifizierung der Bugs in Latein, wie es zur Beschreibung von Flora und Fauna üblich ist, und nennt einen späteren Bug „Callbellum“, der laut seinen Ausführungen in allen Apparaturen eines Telefons gute Lebensbedingungen fand.

Harvard Mark II: Eingeklemmte Insekten

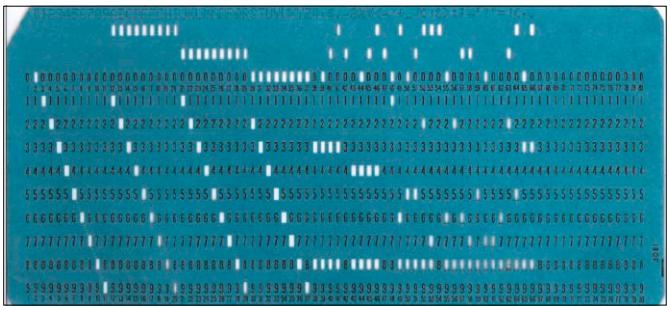
Echte Insekten hatten es auf die Relais des Computers Harvard Mark II abgesehen, der 1947 unter der Ägide von Howard Aiken an der Harvard-Universität in Betrieb ging. Unter anderem arbeitete auch die Informatikpionierin Grace Hopper an der Programmierung des Mark II, welcher mit elektromagnetischen Hochgeschwindigkeitsrelais arbeitete. Einer der Ingenieure fand in einem der Relais eine eingeklemmte Motte, die Kontakte blockierte. Im handschriftlichen Log zum Betrieb des Mark II gibt es dazu einen eigenen Eintrag, der scherzhaft mit „erster echter Bug gefunden“ betitelt ist und die hinter Folie eingeklebte Motte enthält. Grace Hopper verwendete schon routinemäßig den Begriff „Debugging“ für die Fehlersuche in den frühen Großcomputern.

Kommafehler und falsche Einheiten

Die NASA fand nach dem katastrophalen Scheitern von Raumfahrtmissionen immer wieder vermeintlich banale Fehler in programmierten Abläufen als Ursache. 1962 musste der Satellit Mariner I kurz nach dem Start in einer herbeigeführten Explosion zerstört werden, nachdem die Trägerrakete vom Kurs abkam. Der Grund war eine fehlende Punktierung im Programmcode einer Steuereinheit, die die Mission scheitern ließ, welche damals rund 80 Millionen US-Dollar kostete (heute 630 Millionen). Nicht minder schmerzhaft war 1999 der Verlust des Mars-Orbiters, nachdem die Ingenieure zur Berechnung der Flugdaten britische Maßeinheiten nutzten, die NASA diese aber metrisch interpretierte. Die Sonde kam dem Mars deshalb hundert Kilometer zu nah – oder waren es Meilen?



Auszug aus dem handschriftlichen Log des Mark II: Die diensthabenden Ingenieure machten sich einen Spaß daraus, die gefundene Motte in einem Relais für die Nachwelt aufzukleben.



Daten auf einer IBM-Lochkarte: Jedes Bit ist hier wertvoll und dies veranlasste eine unterdimensionierte Notation von Datumsangaben, die später zum Y2K-Bug führte.

Datumsfehler: Jahr 2000 und Jahr 2038

Einer der berühmtesten Bugs, der überall große Aufmerksamkeit fand, war der Jahr-2000-Fehler (Y2K-Bug). Das Problem entstand schlicht aus einer verkürzten zweistelligen Schreibweise für Datumsfelder, nach der „00" als das Jahr 1900 interpretiert wurde und nicht als 2000. Der Bug geht auf die Verwendung von Lochkarten zurück, auf welchen jedes Bit eine wertvolle Ressource war. Es kam ab 1998 Panik auf, dass es einen weltweiten Zusammenbruch von IT-Systemen geben könnte. Dieser blieb weitgehend aus – jedoch nicht, weil der Bug harmlos war. Stattdessen setzten Regierungen groß angelegte Debugging-Aktionen an, die sich über Monate erstreckten. Im Jahr 2038 wird der zur Zeitrechnung verwendete 32-Bit-Integerwert auf Unix-Systemen überlaufen und in den negativen Bereich springen. Zur Vermeidung größerer Probleme in EDV-Systemen weltweit verlangt der Datumsbug auch wieder jetzt schon lang angelegte Lösungen. Der Linux-Kernel wurde zwischen Version 4.18 (2018) und 5.6 (2020) analysiert, um den 2038-Fehler in allen seinen Subsystemen zu beseitigen.

Meltdown und Spectre

Wohin übermäßige Ambitionen in der Entwicklung möglichst performanter Prozessoren führen, zeigen die weiterhin aktuellen Lücken Meltdown und Spectre. Diese setzten bei der Abarbeitung von Programmcode auf spekulative, vorausschauende Ausführung. Ein unerwünschter Nebeneffekt: Laufende Prozesse können damit Adressräume des Speichers lesen, auf die sie keinen Zugriff haben dürften. Die Entdecker der Lücken informierten Mitte 2017 die Hersteller betroffener CPUs. Anfang 2018 wurden diese CPU-Bugs öffentlich gemacht, die bis heute Fehlerbehebungen in Betriebssystemen und im nachladbaren Microcode von Prozessoren verlangen.

Das CVE-System: Kennung für Bugs

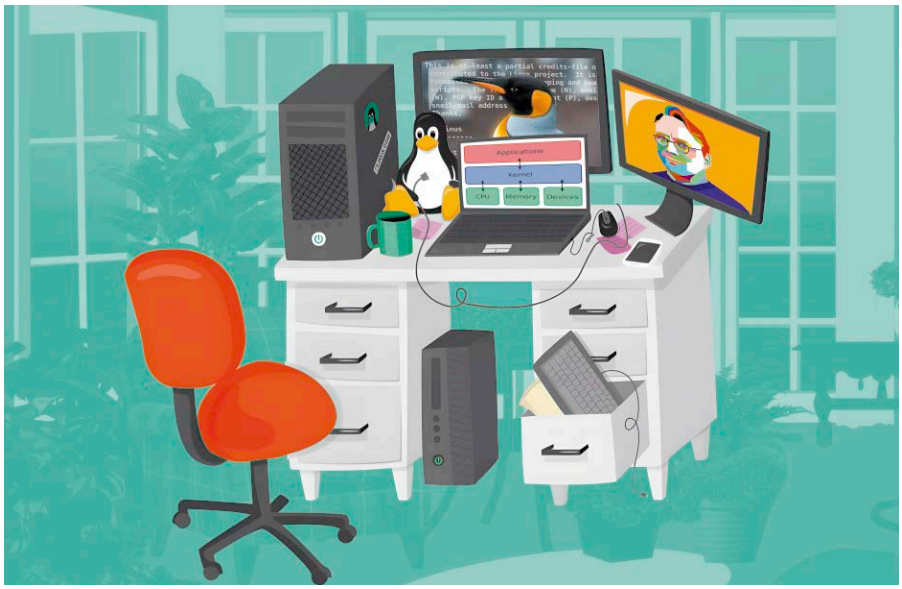
Die Menge an sicherheitskritischen Bugs über Betriebssysteme hinweg verlangt eine eindeutige Identifizierung. 1999 hat die US-Behörde NCF das Klassifikationssystem CVE (Common Vulnerabilities and Exposures) zur weltweiten Nomenklatur von Sicherheitslücken in Betrieb genommen. Dazu gehört auch die Einstufung von Schwere und Risiko. Sicherheitskritische Bugs in verbreiteter Software erhalten deshalb eine CVE-Nummer, wenn die Entdecker oder die Verantwortlichen einer Software diese beantragen. Der Bug „Heartbleed" hat beispielsweise die ID CVE-2014-0160. Die CVE-Datenbank ist im Web unter *https://www.cve.org* öffentlich einsehbar. ■

DIE SCHLIMMSTEN LINUX-BUGS

Die Entwicklungsweise des Linux-Kernels als Kooperation von bis zu 2000 Einzelentwicklern unter den wachsamen Augen von Linus Torvalds soll vor allem Bugs ausschließen.
Der Entwickler Eric Raymond formulierte dazu 1999 den Satz „Bei genügend Augenpaaren werden alle Bugs offensichtlich" („Given enough eyeballs, all bugs are shallow"), der auch als das Linus-Gesetz bekannt wurde.
Fehlerfrei ist der Kernel nicht, denn diverse Subsysteme sind komplex und teilweise unterbesetzt. Dies führt immer wieder zu schweren Bugs in Linux-Systemen und im Kernel selbst. Die schlimmsten erhalten neben einer CVE-Klassifizierung griffige Namen und sogar Logos.
Heartbleed: Diese Sicherheitslücke, die Millionen Linux-Server betraf und viele Embedded-Systeme immer noch betrifft, hat 2014 ein unterbesetztes Open-Source-Projekt – Open SSL – ins Licht der Öffentlichkeit gerückt. Ein Programmierfehler plauderte Speicherinhalte eines Servers über eine SSL-Verbindung und die Heartbeat-Erweiterung von Open SSL aus. Heartbleed markierte den Start von großen Sicherheits- und Finanzierungsinitiativen für wichtige Open-Source-Projekte.
Shellshock: Die Lücken von 2015 in der Shell Bash erlauben es, an Umgebungsvariablen Funktionsdefinition mit Shell-Code anzuhängen. Brisant wurde die Lücken, weil sie sich unter bestimmten Umständen auf Webservern mit CGI-Scripts ausnutzen lassen, wenn diese die Bash aufrufen.
Dirty COW: 2017 wurde eine Sicherheitslücke im Kernel bekannt, die auf das Jahr 2007 zurückgeht. Diese Lücke betrifft eine Methode, über welche der Kernel Copy-on-Write-Aktionen (kurz „COW") auf Dateien im Speicher durchführt. Schlimmstenfalls war ein root-Zugriff möglich.
Dirty Pipe: Anfang 2022 sorgte eine falsche Behandlung von Prozess-Pipes im Kernel ab Version 5.8 für Aufregung, die es gewöhnlichen Usern erlaubte, in fremde Dateien zu schreiben. Zusätzliche Brisanz hatte die Lücke, weil auch Android betroffen ist und viele ältere Android-Smartphones keine Systemupdates vom Hersteller mehr erhalten.

Durchblick im Kernel-Chaos

Um den Linux-Kernel muss man sich spätestens dann kümmern, wenn Hardware unter Linux nicht funktioniert. Es ist allerdings nicht ganz einfach herauszufinden, welche Kernel-Version man benötigt.



VON THORSTEN EGGELING

Der Kernel ist ein zentraler Bestandteil des Betriebssystems. Er sorgt für die Einbindung der Hardware, stellt Softwareschnittstellen dafür bereit und er verwaltet den Speicher sowie die Prozesse. Neuere Kernel verbessern die Hardwareunterstützung. Falls das für neue Geräte erforderlich ist, muss man einen aktuelleren Kernel verwenden. Ubuntu und Linux Mint bietet unterschiedliche Methoden für die Installation.

Wann ein neuer Kernel erforderlich ist

Im optimalen Fall läuft nach der Linux-Installation alles rund, die Hardware im PC arbeitet anstandslos und ohne Fehler. In diesem Fall unterstützt der Kernel die verwendeten PC-Komponenten und es gibt keinen Handlungsbedarf.

Anders sieht es aus, wenn einzelne Geräte nach der Installation nicht funktionieren oder neue Hardware hinzugekommen ist, die von der genutzten Linux-Distribution nicht unterstützt wird. Zuerst sollte man ermitteln, ob es einen Kernel gibt, der die betroffene Hardware unterstützt.

Eine Analyse der Hardware lässt sich besonders einfach über *https://linux-hardware.org* durchführen. Nutzer von Ubuntu oder Linux Mint installieren das nötige Tool im Terminal mit

```
sudo apt install hw-probe
```

und starten es danach so:

```
sudo -E hw-probe -all -upload
```

Sie erhalten dabei eine URL, die Sie im Browser aufrufen. Auf der Seite sehen Sie unter „Host“, welchen Kernel Ihr System aktuell verwendet. Unter „Devices“ sind alle internen und externen Geräte mit Namen und IDs aufgelistet. Steht in der Spalte „Status“ der Eintrag „works“ oder „detected“, sollte das Gerät funktionieren. Beim Status „failed“ wurde kein Treiber gefunden, geladen oder konfiguriert. Wenn vorhanden, verweist ein Kasten rechts daneben auf eine mögliche Lösung.

Klicken Sie „failed“ an, um weitere Infos zum Gerät zu erhalten. Bei einer Meldung wie „We have not found a driver for the device in any Linux kernel versions up to 6.1“ gibt es bisher keinen Kernel, der die Hardware unterstützt. Oft befindet sich ein Treiber aber bereits in der Entwicklung. Sie finden dann Links zu Informationen über einen passenden Treiber, den Sie in der Regel selbst kompilieren müssen. Die Situation ist günstiger, wenn ein Treiber in einer aktuelleren als der auf Ihrem PC installierten Kernel-Version zu finden ist. Welche Möglichkeiten Sie dann haben, erklären die nachfolgenden Abschnitte.

Neue und neuere Kernel

Der Linux-Kernel wird fortlaufend weiterentwickelt und mit neuen Modulen (Treibern) für aktuelle Hardware ausgestattet. Einige Linux-Distributionen setzen auf besonders hohe Stabilität und aktualisieren die Hauptversion des Kernels während des Supportzeitraums nicht automatisch oder nur selten. Auskunft über die Kernel-Versionen gibt *www.kernel.org*. Die Langzeitunterstützung (LTS) geht zur Zeit (Stand Dezember 2022) zurück bis Kernel 4.9. Aktuelle LTS-Distributionen verwenden meist Kernel 5.4 bis 5.19.

Wer einen deutlich jüngeren Kernel benötigt, steigt am einfachsten auf eine Distribution um, die fortlaufend aktualisiert wird

(„Rolling Release“). Beispiele dafür sind Manjaro (*https://manjaro.org*) oder Open Suse Tumbleweed (*https://software.opensuse.org/distributions/tumbleweed*). Die Aktualität betrifft jedoch alle Pakete und nicht nur den Kernel. Die Pakete sind weniger ausgiebig getestet, weshalb man mit Inkompatibilitäten rechnen muss, die sich nur durch manuelle Eingriffe beheben lassen.

Langsame Entwicklung bei Ubuntu & Co.

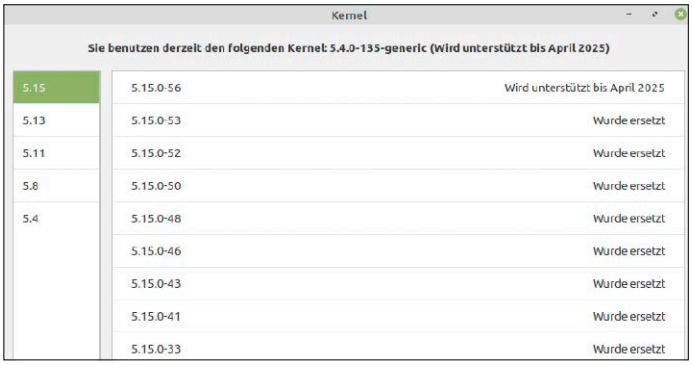
Für Ubuntu erscheinen etwa halbjährig Point Releases (22.04.1, 22.04.2, und so weiter). Enthalten sind jeweils alle bisherigen Updates und ab Point Release xx.xx.2 nach knapp einem Jahr auch ein neuer Kernel (also ab Frühjahr 2013). Wer Ubuntu neu installiert, verwendet möglichst die aktuellste ISO-Datei von *https://ubuntu.com/download/desktop* und erspart sich damit umfangreiche Updatedownloads. Ein installiertes Ubuntu wird automatisch auf ein Point Release aktualisiert. Ubuntu 20.04 beispielsweise erhält den Kernel 5.15 (20.04.5), der auch in Ubuntu 22.04/ 22.04.1 enthalten ist.

Wer den neueren Kernel schon jetzt benötigt, wechselt von Ubuntu 22.04 auf 22.10. Die STS-Version (Short Term Support) bietet auch neuere Programme, arbeitet aber möglicherweise nicht so zuverlässig wie ein LTS-Ubuntu. Ein Wechsel zur nächsten LTS-Version ist erst im April 2024 möglich (Ubuntu 24.04). Für die Umstellung starten Sie „Anwendungen & Aktualisierungen“ und gehen auf „Aktualisierungen“. Wählen Sie hinter „Über neue Ubuntu-Versionen benachrichtigen“ den Eintrag „Für jede Version“. Rufen Sie „Aktualisierungsverwaltung“ auf. Die neue Version wird Ihnen angeboten und lässt sich per Klick auf „Aktualisieren“ einrichten.

Linux Mint verfolgt eine konservativere Updatestrategie als Ubuntu. Ohne Eingriff des Benutzers bleibt es bei der ursprünglichen Kernel-Version. Linux Mint 20 basiert auf Ubuntu 20.04 und bringt daher den Kernel in der Version 5.4 mit. Point Releases gibt es ebenfalls, der Kernel bleibt aber standardmäßig bei Version 5.4.

Wer einen neueren Kernel benötigt, geht in der Aktualisierungsverwaltung auf „Ansicht → Linux Kernel“, wählt den aktuellsten Kernel (zur Zeit 5.15) und klickt auf „Installieren“. Danach ist das System auf dem gleichen Stand wie Ubuntu 20.04.5.

Hardware prüfen: Der Bericht auf *https://linux-hardware.org* zeigt an, für welches Gerät Treiber fehlen. Man muss den Treiber selbst kompilieren oder zu einem neueren Kernel wechseln.



Neue Kernel für Linux Mint: Die Distribution installiert neue Kernel nicht automatisch. Über die Aktualisierungsverwaltung lassen sich Upgrades auswählen – sofern verfügbar.

Ein Upgrade auf Linux Mint 21 (basiert auf Ubuntu 22.04) ist ebenfalls möglich. Dazu führt man im Terminal diese beiden Befehlszeilen aus:

```
sudo apt install mintupgrade
sudo mintupgrade
```

Folgen Sie den Anweisungen des Assistenten. Das aktualisierte System verwendet Kernel 5.15, was Stand Dezember 2022 die höchste verfügbare Version für Ubuntu 20.04/22.04 sowie Linux Mint 20/21 ist.

Individuellen Kernel verwenden

Ubuntu und Linux Mint lassen sich auch mit einem deutlich neueren Kernel ausstatten, als die Distributionen bieten. Die DEB-Pakete für die Installation sind unter *https://kernel.ubuntu.com/~kernel-ppa/mainline* zu finden. Die neuesten Versionen lassen sich allerdings nicht in den LTS-Ausgaben installieren, weil einige Bibliotheken zu alt sind. Man kann den Kernel selbst erstellen, was mit einem gewissen Zeitaufwand verbunden ist.

Eine ausführliche Anleitung können Sie über *https://m6u.de/BMKE* abrufen. Derzeit lassen sich die Kernel-Versionen 5.16 bis 6.0 unter Ubuntu 20.04/22.04 sowie Linux Mint 20/21 kompilieren.

Ungenutzte Kernel entfernen

Ubuntu und Linux Mint entfernen ältere Kernel nicht automatisch, was der Sicherheit dient. Halten Sie beim Start des PCs die Umschalt-Taste gedrückt. Im Grub-Menü lässt sich dann über „Advanced options for Ubuntu“ ein älterer Kernel starten. Bei einem bereits länger genutzten System sammeln sich zahlreiche Kernel-Versionen an. Problematisch können Installationen mit einer eigenen Bootpartition sein. Ist diese nicht ausreichend bemessen, schlägt die Installation einen neuen Kernels fehl. Im schlimmsten Fall führt das zu einem undefinierten Zustand und Linux startet nicht mehr. Sie sollten daher die Befehlszeile

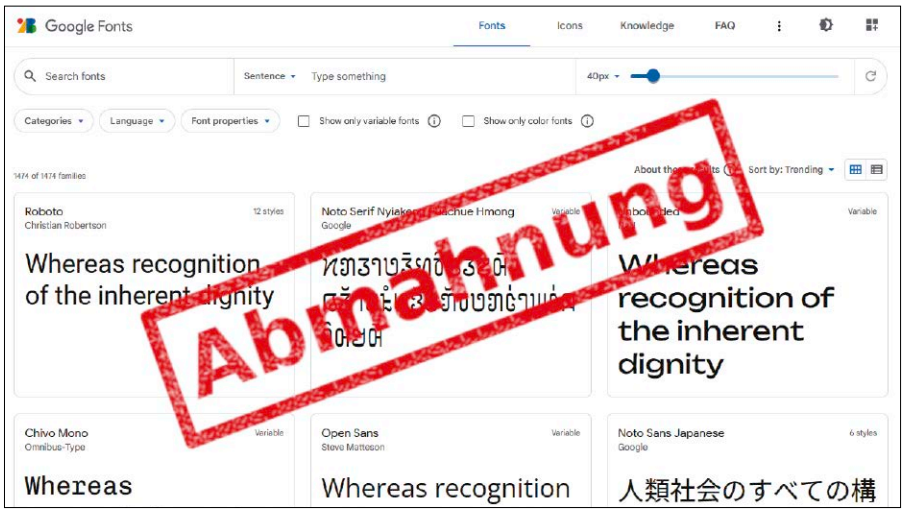
```
sudo apt autoremove
```

regelmäßig ausführen. Damit entfernen Sie nicht mehr verwendete Pakete inklusive alter Kernel-Versionen. Nebenbei geht dann auch die Installation neuer Kernel schneller, weil der Paketmanager die Ramdisk-Dateien und Treiber für weniger Kernel-Instanzen erzeugen muss. ■

Abmahnungen wegen Google-Fonts

Man sollte die eigene Website prüfen, bevor ein Schreiben vom Anwalt im Postkasten liegt. Zur Zeit werden vermehrt Abmahnungen verschickt, die den Download von Google-Fonts bemängeln.

VON THORSTEN EGGELING



Google bietet kostenlose Schriftarten für Websites an. Wenn diese ohne Zustimmung des Besuchers von Google-Servern geladen werden, kann das rechtliche Folgen haben.

Verstößt der Betreiber einer Website gegen geltendes Recht, kann das juristische Konsequenzen haben. Seit einiger Zeit mehren sich Meldungen über Abmahnungen, die neben der Unterlassung auch Schadenersatz fordern. Dabei wird die Einbindung von Google-Fonts abgemahnt, welche die IP-Adresse eines Besuchers an das US-Unternehmen übermitteln. Um solchen Ärger zu vermeiden, sollten Sie Google-Fonts rechtssicher in Ihre Website einbauen.

Was sind Google-Fonts?

Mit geeigneten Schriftarten lässt sich die Darstellung von Text auf Webseiten deutlich verbessern. Der Browser lädt die Fonts aus dem Internet und verwendet sie statt der auf dem Rechner installierten Schriftarten. Google stellt für diesen Zweck zahlreiche Schriftarten unter einer Open-Source-Lizenz kostenlos bereit (*https://fonts.google.com*). Die Einbindung in eine Website erfolgt dann über eine CSS-Datei etwa so:

```
<link rel='stylesheet' id='google-
  web-fonts-css' href='//fonts.
  googleapis.com/css?family=Open+S
  ans%3Aregular%7COpen+Sans%3A700&
  #038;ver=1.1.6' type='text/css'
  media='all' />
```

In der CSS-Datei sind Download-URLs für die Fonts enthalten (Beispiel):

```
src: url(http://fonts.gstatic.com
  /s/opensans/v34/memvYaGs126MiZpBA
  UvWbX2vVnXBbObj2OVTS-muw.woff2)
  format('woff2');
```

Die Downloads erfordern zusätzliche Bandbreite, wodurch sich der Aufbau von Webseiten verlangsamt. CSS-Dateien und Fonts lädt der Browser allerdings in seinen Cache. Ein erneuter Download ist später in der Regel nicht erforderlich. In älteren Browsern (vor 2020) wurden identische Google-Fonts auch beim Besuch anderer Websites aus dem Cache geladen. Aus Sicherheitsgründen wird das nicht mehr unterstützt. Der Vorteil einer zentralen Bevorratung in einem CDN (Content Delivery Network) entfällt und man kann die Fonts daher auch vom eigenen Server ausliefern.

Eigene Webseiten prüfen: Ob in Ihrer Internetpräsenz Google-Fonts zum Einsatz kommen, finden Sie im Browser heraus. Nach einem rechten Mausklick in die Seite wählen Sie in Firefox „Seitenquelltext anzeigen“. Suchen Sie (mit Strg-F) im Quelltext nach „google“ und „gstatic“. Wenn CSS-Dateien oder Fonts von Google geladen werden, finden Sie im Quellcode entsprechende Verweise. Etwas genauer geht es mit den Entwicklerwerkzeugen, die sich über den Kontextmenüpunkt „Untersuchen“ einblenden lassen. Gehen Sie auf „Netzwerkanalyse“, setzen Sie ein Häkchen vor „Cache deaktivieren“ und laden Sie die Webseite über Strg-R neu. Klicken Sie auf „Schriften“. In der Spalte „Host“ sehen Sie, woher die eingebundenen Schriftarten stammen. Sollte es sich nicht um Ihre eigene Domain handeln, sollten Sie Maßnahmen ergreifen. Prüfen Sie nicht nur die Startseite, sondern auch Unterseiten.

Über *https://www.e-recht24.de/google-fonts-scanner* können Sie Ihre Website zusätzlich prüfen und erhalten dabei weiterführende Informationen zur Rechtslage.

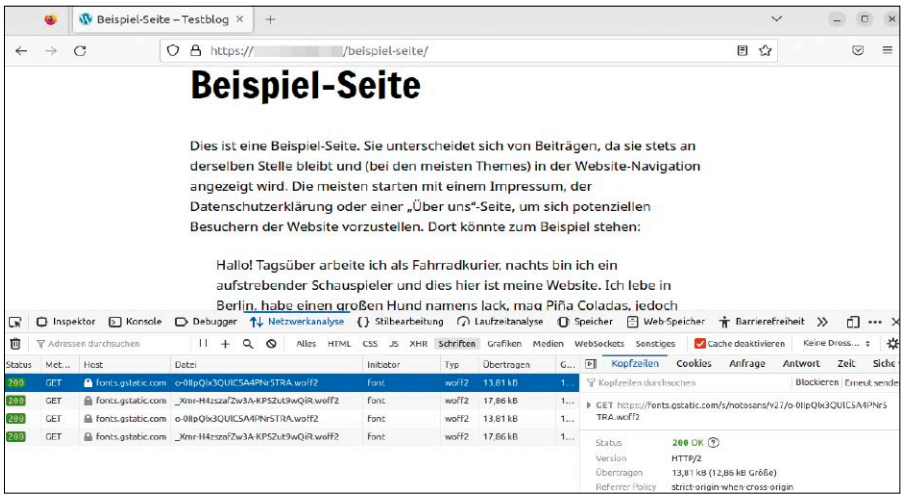
Rechtliche Probleme mit fremden Inhalten

Bei jedem Aufruf einer Webseite oder beim Download erfährt der Webserver die IP-Adresse des Besuchers. Dabei handelt es

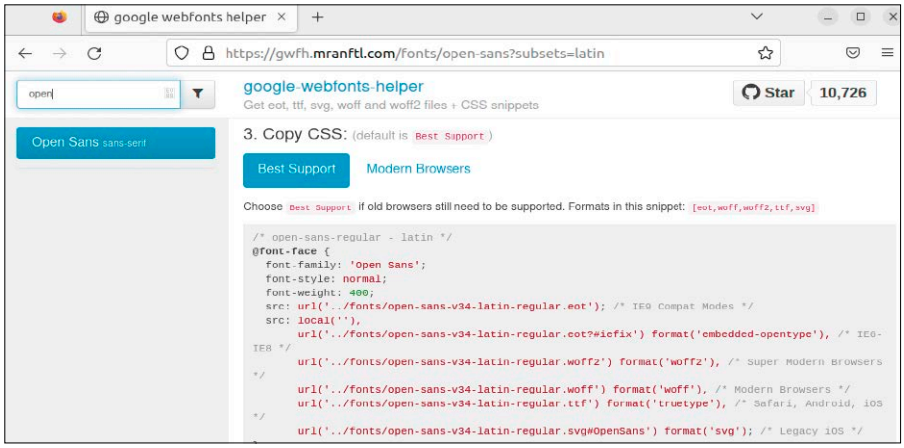
sich laut DSGVO (*https://dsgvo-gesetz.de*) um personenbezogene Daten, weil sich mit der IP-Adresse die Identität des Besuchers ermitteln lässt. Ein Webserver darf diese Daten nur so lange sammeln, wie es technisch notwendig ist. In den Logdateien beispielsweise müssen die IP-Adressen pseudonymisiert werden, damit keine Rückschlüsse auf die Identität des Besuchers möglich sind. Wenn Sie den Webserver nicht selbst betreiben, also keinen vollen Zugriff auf dessen Konfiguration haben, muss der Webhoster nach Artikel 28 DSGVO für die Einhaltung der rechtlichen Bestimmungen sorgen. Der Hoster bietet Ihnen dafür eine Vereinbarung zur Auftragsverarbeitung an.
Sobald Sie fremde Dienste in Ihre Webseiten einbinden, werden die Inhalte von anderen Webservern abgerufen, die ebenfalls die IP-Adresse des Besuchers erfahren. Das gilt für Google-Fonts, Google-Adsense, Youtube, Twitter, Facebook und viele andere. Es gilt als rechtssicher, wenn Sie bei jedem externen Inhalt nach der Einwilligung des Besuchers Ihrer Webseiten fragen („Opt-in"). Teilweise kann auch eine Information in der Datenschutzerklärung reichen sowie die Möglichkeit, externe Inhalte generell abzuwählen („Opt-out"). Wirkungsvoll ist außerdem ein Fenster, das vor Aufruf der Website erscheint, in dem Sie die Zustimmung zu Cookies sowie zur Datenschutzerklärung und allen darin genannten Funktionen einholen.
Auch für externe Dienste ist eine Vereinbarung zur Auftragsverarbeitung beim jeweiligen Anbieter erforderlich. Für Werbeeinblendungen über Adsense stellt Google die nötigen Erklärungen und DSGVO-Mitteilungen bereit, für Google-Fonts bisher aber nicht. Unter *https://developers.google.com/fonts/faq/privacy* heißt es lediglich, dass Google IP-Adressen nicht speichert und nicht analysiert.

Abmahnungen wegen Google-Fonts vermeiden

In den bisher bekannt gewordenen Abmahnungen geht es um eine Forderung auf Unterlassung, die eher als unstrittig gelten kann. Dazu wird ein Schadenersatz in Höhe von 140 bis 170 Euro gefordert, teilweise zuzüglich Anwaltsgebühren, was dann mehr als 200 Euro ergibt.
Die Abmahner könnten Ihre Forderungen mit dem Urteil des LG München vom 20.01.2022 (Aktenzeichen: 3 O 17493/20, *https://m6u.de/LGMU*) begründen. Darin wurde der Beklagte zu einem Schadenersatz von 100 Euro verurteilt. Im Urteil heißt es zum Abruf der Google-Fonts: „Die Übermittlung der IP-Adresse, erfolgte damit nicht nur einmalig. Der damit verbundene Eingriff in das allgemeine Persönlichkeitsrecht ist im Hinblick auf den Kontrollverlust des Klägers über ein personenbezogenes Datum an Google, ein Unternehmen, das bekanntermaßen Daten über seine Nutzer sammelt und das damit vom Kläger empfundene individuelle Unwohlsein so erheblich, dass ein Schadensersatzanspruch gerechtfertigt ist.".
Wer eine Abmahnung erhält, kann die Forderung entweder begleichen oder sich (bevorzugt) anwaltlichen Rat suchen. Zur Zeit ist noch nicht ausreichend geklärt, ob Massenabmahnungen sich tatsächlich auf „individuelles Unwohlsein" berufen können.



Webseiten prüfen: Ob Fonts von Google eingebunden sind, lässt sich im Browser mit den Entwicklertools herausfinden. Unter „Host" erscheint dann „fonts.gstatic.com" oder ähnlich.

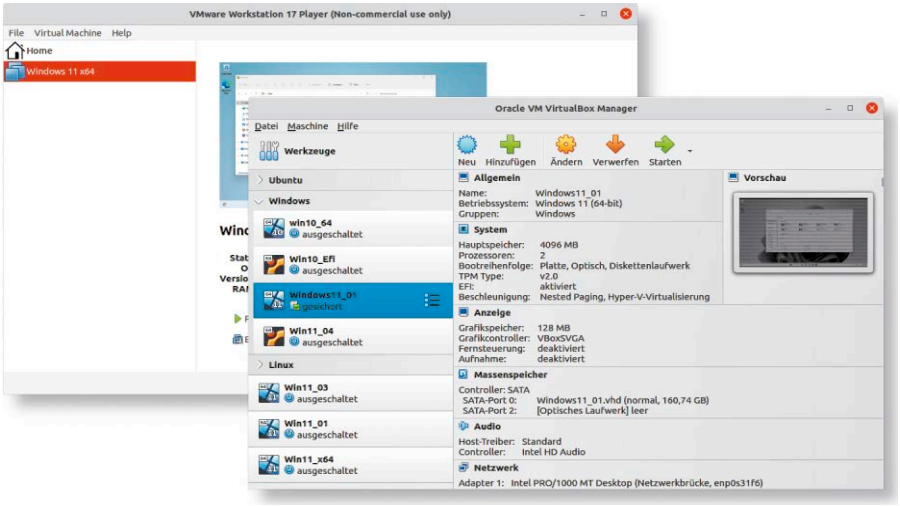


Fonts lokal hosten: Google-Webfonts-Helper liefert den CSS-Code für die Einbindung von Schriftarten und bietet Fontdateien in passenden Formaten zum Download an.

Fonts lokal bereitstellen: In jedem Fall sollte man Google-Fonts über den eigenen Webserver ausliefern. Dabei bietet der Google-Webfonts-Helper (*https://gwfh.mranftl.com*) Unterstützung. Nach Auswahl der gewünschten Schriftart erhält man den nötigen CSS-Code und einen Downloadlink für die Fontdateien. Beides kopiert man auf den Webserver und bindet den CSS-Code in die Seiten ein.
Nutzer von Wordpress installieren das Plug-in OMGF (*https://daan.dev/wordpress/omgf*), das sich über „Einstellungen → Optimize Google Fonts" konfigurieren lässt. Nach einem Klick auf „Speichern & Optimieren" baut es eine zusätzliche CSS-Datei mit den Fontdefinitionen ein. Die zugehörigen Fontdateien werden im Ordner „/wp-content/uploads/omgf" gespeichert und dann von Ihrem eigenen Webserver ausgeliefert. ■

Virtualbox gegen Vmware Player

Für Linux-Nutzer stehen mehrere Virtualisierungslösungen zur Verfügung. Wir vergleichen die Funktionen von Virtualbox und Vmware Workstation Player und geben eine Einschätzung der Leistungsfähigkeit.



Virtualbox und Vmware Player im Vergleich: Beide Virtualisierer lassen sich ähnlich bedienen und konfigurieren, Virtualbox bietet jedoch deutlich mehr Funktionen.

VON THORSTEN EGGELING

Virtualbox (*www.virtualbox.org*) steht unter einer Open-Source-Lizenz und ist damit kostenlos verfügbar. Vmware Workstation Player (*www.vmware.com*) ist nur bei privater Nutzung kostenlos. Beim Einsatz im Unternehmen sind circa 150 Euro fällig, außerdem gibt es eine funktionsreduzierte Version von Vmware Workstation Pro ab etwa 200 Euro. Mit beiden Produkten lassen sich virtuelle Maschinen (VMs) unter Linux erstellen und darin Windows- oder Linux-Systeme installieren und starten. Vmware Workstation Player bietet jedoch im Vergleich mit Virtualbox nur die wichtigsten Basisfunktionen.

Installation und erste Schritte

Download, Installation und Ersteinrichtung von Virtualbox beschreiben wir ab Seite 36. Für die Installation von Vmware Workstation Player gehen Sie auf *www.vmware.com/go/downloadplayer-de*, wählen die aktuelle Version 17.0 und klicken auf „Zu den Downloads“. Hinter „VMware Workstation 17.0.0 Player for Linux 64-bit“ klicken Sie auf „Jetzt herunterladen“. Starten Sie ein Terminal, wechseln Sie in das Downloadverzeichnis und starten Sie die heruntergeladene Datei beispielsweise mit

```
sudo sh Vmware-Player-Full-17.0.0
  -20800274.x86_64.bundle
```

Folgen Sie den Anweisungen des Installationsassistenten.

Neue VM erstellen: Beim Vmware Workstation Player sind nur wenige Eingaben erforderlich. Nach Klick auf „Create a New Virtual Machine“ fragt ein Assistent die nötigen Informationen ab. Man gibt eine ISO-Datei für die Linux- oder Windows-Installation an; der Player erkennt das System dann meist automatisch und setzt die passenden Optionen. Bei Windows 11 fordert der Assistent ein Passwort für die Verschlüsselung an, was für die TPM-Unterstützung erforderlich ist.

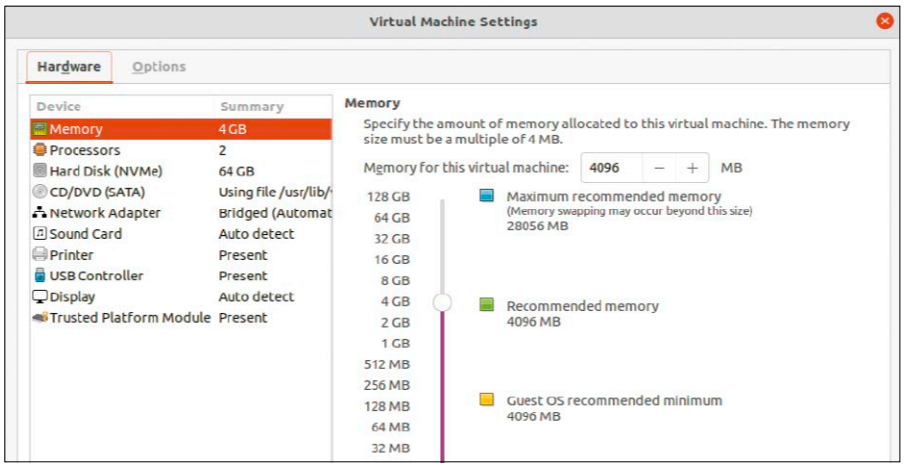
Bei Virtualbox ist der Ablauf ähnlich, der Assistent fragt jedoch mehr Einstellungen ab. Beim Erstellen einer neuen virtuellen Maschine können Sie beispielsweise auch die Größe des Hauptspeichers für das Gastsystem festlegen. Außerdem kann man den Typ der virtuellen Festplatte wählen und die unbeaufsichtigte Installation aktivieren (siehe Artikel ab Seite 34). Beides fehlt beim Player, weil er nur einen Typ virtueller Festplatten bietet und standardmäßig keine unbeaufsichtigte Installation unterstützt.

Leistung verbessern: Wie Virtualbox bietet auch Vmware Tools und Treiber für die Optimierung des Gastsystems an. Die Vmware-Tools verbessern die Grafikleistung und sind für den Datenaustausch über die Zwischenablage sowie für den direkten Zugriff auf Ordner des Hostsystems („Shared Folders“) erforderlich. Bei Gastsystemen wie Ubuntu oder Linux Mint ist keine zusätzliche Installation erforderlich, weil die Pakete „open-vm-tools“ und „open-vm-tools-desktop“ bereits vorinstalliert sind. Andernfalls hängt man das Medium mit den Vmware-Tools über „Virtual Machine → Install VMware Tools“ ein und führt die Installation durch.

Konfiguration von VMs

Bei Bedarf kann man bei Vmware Workstation Player die Einstellungen über „Virtual Machine → Virtual Machine Settings“ anpassen. Es sind ähnliche Grundeinstellungen wie bei Virtualbox verfügbar, beispielsweise für den im Gastsystem verfügbare Haupt-

speicher und die Anzahl der Prozessoren. Es fällt auf, das sich bei Vmware deutlich höhere Werte einstellen lassen: Für den Hauptspeicher bis zu 128 GB und bis zu 32 Prozessoren. Bei 128 GB Hauptspeicher für den Gast und realen 32 GB im Host-PC würde Vmware ständig Speicher auf die Festplatte auslagern müssen, was eine starke Verlangsamung bewirkt. Bei den Prozessorkernen kann man ohnehin nur so viele einstellen, wie das Hostsystem bietet. Mehr als zwei CPUs sind für Standardsoftware nicht erforderlich und bewirken auch keine Beschleunigung. Ein Vorteil gegenüber Virtualbox ergibt sich daher nicht.



VM im Player konfigurieren: Die Software bietet in den Einstellungen alle nötigen Optionen – aber auch nicht mehr. Die Vorgaben für das Gastsystem kann man in der Regel übernehmen.

Probleme bei der Konfiguration des Players

Die beim Player im Vergleich zu Vmware Workstation Pro reduzierten Optionen führen manchmal zu irreführenden Informationen. Ein Beispiel: Bei einem Host-PC mit 32 GB RAM und einer Auslagerungsdatei von nur zwei GB erscheint eine Fehlmeldung. Man soll die Auslagerungsdatei vergrößern oder in den „Preferences“ die Einstellung für den reservierten Speicher ändern. Die genannte Einstellung gibt es jedoch beim Player nicht. Das Problem lässt sich beheben, indem man in die Datei „/etc/vmware/config“ die Zeile

```
prefvmx.minVmMemPct = "100"
```

einträgt. Diese Lösung findet man erst nach intensiver Internetrecherche.

Ähnlich verhält es sich mit anderen fehlenden Einstellungen, obwohl der Player die Funktionen unterstützt, beispielsweise für Secure Boot oder Uefi-Firmware. Auch wenn nicht jeder Nutzer diese Einstellungen benötigt, ist der Weg über die Konfigurationsdateien umständlich – und das nur, weil Vmware den Player künstlich beschränkt hat. Bei Virtualbox sind alle relevanten Einstellungen über die grafische Oberfläche erreichbar.

Leistungsvergleich und Fazit

Die Ausführungsgeschwindigkeit ist in beiden Virtualisierern vergleichbar. Vmware Workstation Player liefert in einigen Bereichen etwas mehr Grafikleistung, etwa bei der 3D-Unterstützung. Die spielt nur bei Anwendungen eine Rolle, die Hardwarebeschleunigung über den Grafikchip nutzen, etwa bei Spielen. Dabei hilft auch, dass sich der virtuelle Grafikadapter mit acht GB RAM konfigurieren lässt. Der verfügbare Gastspeicher muss dafür 16 GB oder größer sein. Anspruchsvollere Spiele laufen aber auch mit diesen Einstellungen eher schlecht.

Als Vorteil von Vmware Workstation Player kann man die übersichtliche Konfiguration anführen – was aber für anspruchsvollere Nutzer zugleich der Nachteil ist. Sicherungspunkte, Klonen und Export von VMs oder der gleichzeitige Start mehrerer virtueller Maschinen fehlen (siehe Tabelle).

Es gibt wenig Grund, den Player statt Virtualbox zu verwenden. Einen weiteren Aspekt wollen wir nicht verschweigen: Vmware liefert hochpreisige Software für Unternehmen und hat einen hohen Qualitätsanspruch. Davon profitiert auch der Player. Bei Virtualbox arbeitet wahrscheinlich ein eher kleines Team an der Weiterentwicklung der Software. Mit häufigen Updates werden kleinere und größere Probleme zwar beseitigt, Nutzer müssen aber immer wieder mit ärgerlichen Fehlern rechnen. Allerdings sind in der Vergangenheit keine Probleme aufgetreten, die die Nutzung von Virtualbox verhindert oder ein Gastsystem zerstört hätten. ■

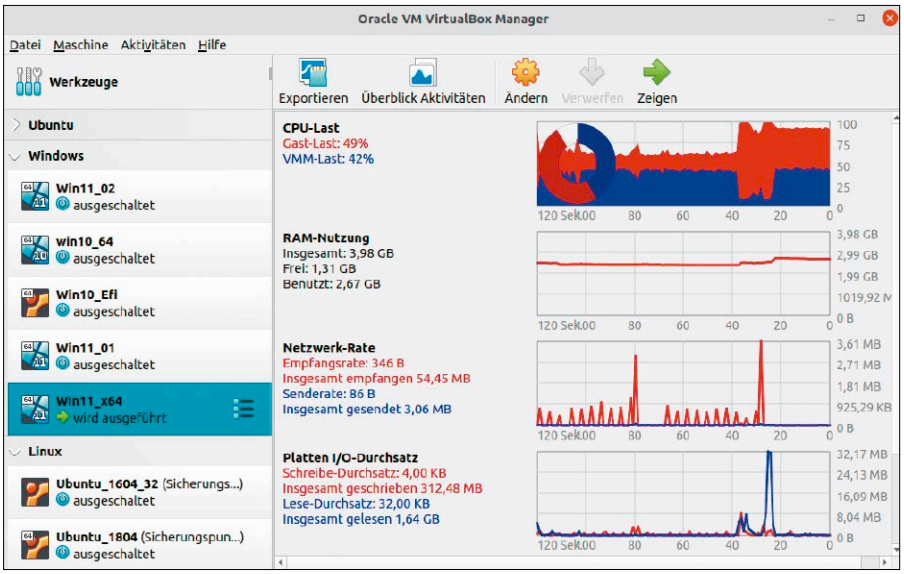
VIRTUALBOX VS. VMWARE PLAYER

	Oracle Virtualbox 7	Vmware Workstation Player 17
Hersteller-Website	*www.virtualbox.com*	*www.vmware.com*
Preis	kostenlos, größtenteils Open Source	ab 150 Euro, private Nutzung kostenlos
Funktionen	**Oracle Virtualbox 7**	**Vmware Workstation Player 17**
Anzahl der CPUs (maximal)	8	32
Drag & Drop (Host/Gast)	ja (teilweise)	ja
Fernzugriff (VNC)	ja	ja
Gemeinsame Ordner	ja	ja
Gemeinsame Zwischenablage	ja	ja
Maximaler Grafikspeicher	128 MB	8 GB
Maximaler Hauptspeicher	wie Host	128 GB
Mehrere Monitore	ja	ja
Mehrere VMs parallel	ja	nein
Open GL/DirectX	ja/ja	ja/ja
TPM/Secure Boot	ja/ja	ja/nein
USB 2.0/3.0 im Gastsystem	ja/ja	ja/ja
VM importieren/exportieren	ja/ja	ja/nein
VM-Klonfunktion	ja	nein
VM-Schnappschüsse	ja	nein
Vollbild/nahtloser Modus	ja/ja	ja/nein

Neu: Virtualbox 7

Gut drei Jahre nach dem letzten größeren Upgrade gibt Oracle eine neue Version von Virtualbox heraus. Einige der neuen Funktionen dienen vor allem der Unterstützung von Windows 11.

VON THORSTEN EGGELING



Auslastung überwachen: Das neue Tool „VM-Aktivitäten“ zeigt, wie intensiv eine virtuelle Maschine die CPU sowie RAM und Netzwerk beansprucht.

Eine Komplettrenovierung der Programmoberfläche hat Oracle nicht durchgeführt. Virtualbox 7 sieht auf den ersten Blick nicht anders aus als der Vorgänger 6.1 und die Bedienung erfolgt weitestgehend wie gewohnt. Neue Funktionen gibt es vor allem für Windows-Gastsysteme. Die Hardwareanforderungen von Windows 11 (siehe *https://bit.ly/Win11SP*) erfordern neben einem unterstützten Prozessor auch ein Trusted Platform Module (TPM) sowie Secure Boot. Beides hat Oracle nun in Virtualbox 7 eingebaut. Weitere Änderungen betreffen den Assistenten für die Einrichtung neuer virtueller Maschinen (VM), der jetzt mehr Optionen bietet und die Konfiguration erleichtert.

Was beim Upgrade zu beachten ist

Zwei Versionen von Virtualbox lassen sich nicht gleichzeitig installieren. Sollte auf Ihrem System bereits Virtualbox 6.1 oder älter installiert sein, beenden Sie zuerst alle gesicherten virtuellen Maschinen. Nach einem Upgrade lassen sich gesicherte VMs oft nicht mehr starten. Sie müssen dann auf „Verwerfen“ klicken und die ungespeicherten Daten gehen dann verloren.

Deinstallieren Sie Virtualbox im Terminal:

```
sudo apt purge virtualbox-6.1
```

Mit dem Befehl

```
apt search virtualbox
```

prüfen Sie, ob noch andere Pakete installiert sind, beispielsweise „virtualbox“ oder „virtualbox-dkms“. Gegebenenfalls entfernen Sie auch diese. Prüfen Sie, ob im Verzeichnis „/usr/src“ Unterordner mit Treiber-Quellcode liegen. Diese tragen im Namen „virtualbox“ oder „vboxhost“. Löschen Sie auch diese Ordner gegebenenfalls. Eine Beschreibung der Virtualbox-Neuinstallation finden Sie im Artikel ab Seite 36.

Der Assistent für neue VMs

In Virtualbox 7 hat Oracle den Assistenten für die Installation neuer virtueller Maschinen überarbeitet. Der „Experten-Modus“ zeigt jetzt alle Einstellungen gesammelt in einem Fenster. Die vier Bereiche „Name und Betriebssystem“, „Unbeaufsichtigte Installation“, „Hardware“ und „Festplatte“ kann man auf- und zuklappen. Der „Geführte Modus“ bietet fast die gleichen Optionen, zeigt die unterschiedlichen Bereiche aber jeweils nach einem Klick auf „Vorwärts“.

Schritt 1: Nach Auswahl der ISO-Datei unter „Name und Betriebssystem“, beispielsweise von Windows 11, bietet Virtualbox 7 eine Auswahl hinter „Edition:“. Dahinter gibt man die gewünschte Variante an, etwa „Windows 11 Home“ oder „Windows 11 Pro“. Die Auswahl ist wichtig, wenn man die unbeaufsichtigte Installation verwenden möchte, die standardmäßig aktiviert ist. Über ein Häkchen vor „Unbeaufsichtigte Installation überspringen“ lässt sich die Funktion deaktivieren.

Schritt 2: Bleibt die unbeaufsichtigte Installation aktiviert, trägt man im zugehörigen Bereich Benutzernamen und Passwort für die lokale Windows-Anmeldung ein. Ein Microsoft-Konto (und die Onlineanmeldung) werden dann nicht verwendet. Unter „Zusätzliche Optionen“ kann man einen Produktschlüssel für die Windows-Aktivierung eingeben. Ohne gültigen Schlüssel wird Windows nicht aktiviert, aber man kann das System einige Zeit ausprobieren. Ein Ablaufdatum, nach dem man Windows nicht mehr nutzen kann, hat Microsoft bisher nicht festgelegt.

Hinter „Hostname:“ tragen Sie den gewünschten Namen des Rechners ein. Eine Angabe hinter „Domain Name:“ ist im heimischen Netzwerk eigentlich nicht erforderlich. Virtualbox verlangt aber eine Eingabe wie „[Rechnername].local“ oder „[Rechnername].fritz.box“ bei einer Fritzbox als Router.

Setzen Sie ein Häkchen vor „Gasterweiterungen“, damit auch diese automatisch installiert werden. Darunter geben Sie den

Pfad zur ISO-Datei mit den Gasterweiterungen an. Unter Linux lauter der Pfad standardmäßig „/usr/share/virtualbox/VboxGuestAdditions.iso“.

Die unbeaufsichtigte Installation funktioniert auch mit vielen Linux-Distributionen, beispielsweise Debian, Ubuntu, Linux Mint, Fedora und Red Hat. Wenn eine Distribution oder Version nicht unterstützt wird, ist die unbeaufsichtigte Installation deaktiviert.

Tipp: Ab Seite 44 beschreiben wir, wie sich eine Windows-VM mit automatischer Installation per Script erstellen lässt. Mit individuellen Anpassungen kann man die Installation zielgerichtet steuern. Das lohnt sich vor allem, wenn man Windows häufiger oder auf mehreren Rechnern neu installiert.

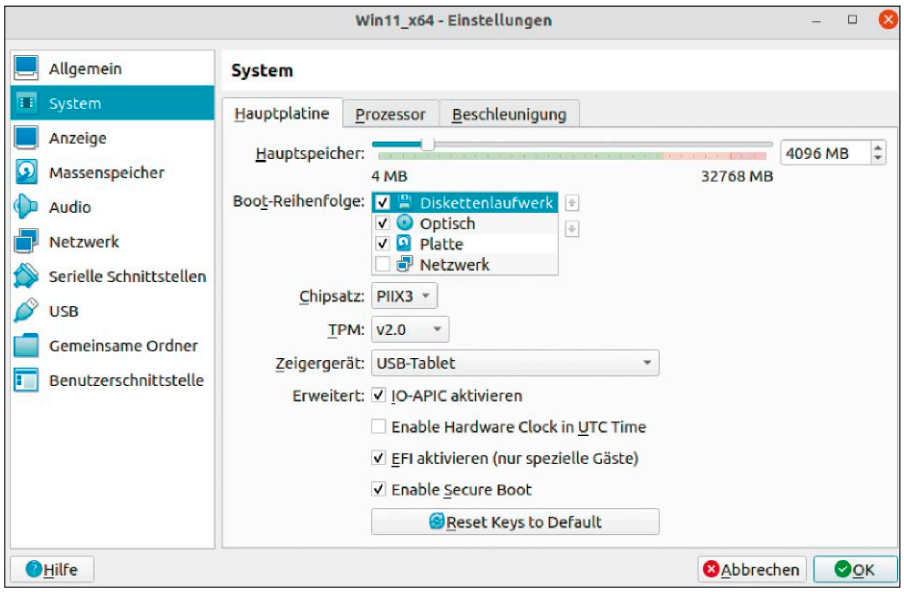
Schritt 3: Die Bereiche „Hardware“ und „Festplatte“ sind abhängig von der Betriebssystemauswahl vorkonfiguriert. Bei Windows ist ein Häkchen bei „EFI aktivieren“ gesetzt und das Gastsystem wird mit vier GB RAM, zwei Prozessorkernen und einer 80-GB-Festplatte konfiguriert. Die Größe der Festplatte ist vielleicht etwas knapp bemessen und Sie sollten mehr Platz einplanen. Da die virtuelle Festplatte standardmäßig „dynamisch“ erstellt wird, wächst ihre tatsächliche Größe erst bei zunehmender Belegung im Gastsystem.

Konfiguration einer VM anpassen

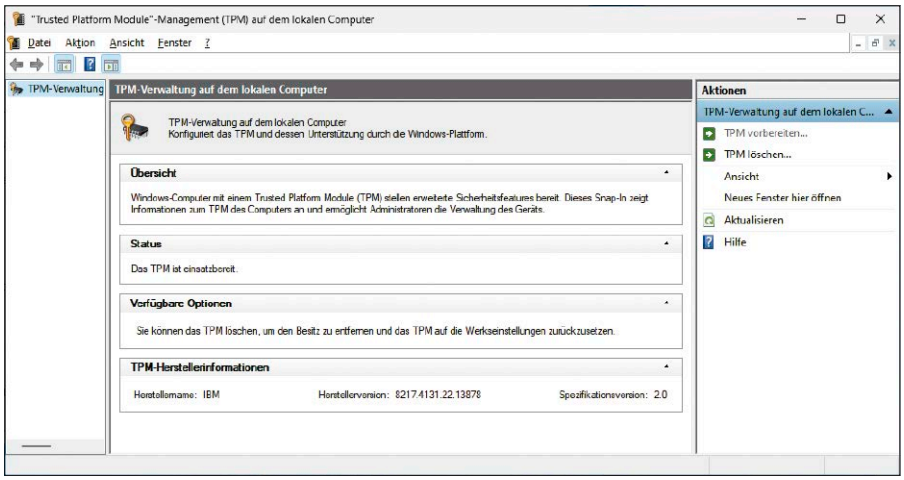
Wenn Sie die unbeaufsichtigte Installation aktiviert haben, startet die Installation sofort nach einem Klick auf „Fertigstellen“ im Assistenten. Will man vorher eigene Anpassungen vornehmen, lässt sich die Installation abbrechen, indem man das Fenster der virtuellen Maschine schließt und die Option „die virtuelle Machine ausschalten“ wählt. Nach einem Klick auf „Anpassen“ kann man dann Änderungen vornehmen.

Bei Ubuntu oder Linux Mint als Gastsystem sollte man auch bei Virtualbox 7 unter „Anzeige“ den Grafikspeicher auf 128 MB erhöhen. Damit lassen sich Darstellungsprobleme vermeiden.

Unter „Netzwerk“ stellt man „Netzwerkbrücke“ ein, wenn der Zugriff auf das lokale Netzwerk möglich sein soll. Bei Linux-Gästen ist unter „USB“ die Option „USB 2.0 (OHCI + EHCI)-Kontroller“ aktiviert. Geräte, die mit dem USB-3.0-Port des Host-PCs verbunden sind, lassen sich dann aber nicht einhängen. In der Regel wählen Sie daher „USB-3.0-Controller (xHCI)“. Bei Windows-Gastsystemen ist USB 3.0 bereits aktiviert.



Neue Optionen: Speziell für Windows 11 hat Oracle in Virtualbox 7 eine TPM-Emulation eingebaut. Außerdem lässt sich beim EFI-Modus jetzt auch Secure Boot aktivieren.



Windows-Installation prüfen: Mit TPM (Trusted Platform Module) kann Windows 11 erweiterte Sicherheitsfunktionen nutzen. Ob TPM arbeitet, kann das Tool „tpm.msc“ feststellen.

Bei Windows-Gastsystemen sind unter „System“ die neuen Funktionen TPM 2.0 und Secure Boot aktiviert. Bei der unbeaufsichtigten Installation sind diese jedoch nicht zwingend erforderlich, weil Oracle per Registry-Patch den Check der Hardwarevoraussetzungen abschaltet. Deshalb lässt sich Windows 11 auch dann in einer VM installieren, wenn die CPU nicht unterstützt wird. Allerdings ist nicht garantiert, dass das auch bei zukünftigen Windows-Versionen funktioniert.

Weitere Funktionen und Änderungen

In Virtualbox 7 lassen sich jetzt virtuelle Maschinen aus der OCI-Cloud (Oracle Cloud Infrastructure) hinzufügen und wie lokale VMs steuern.

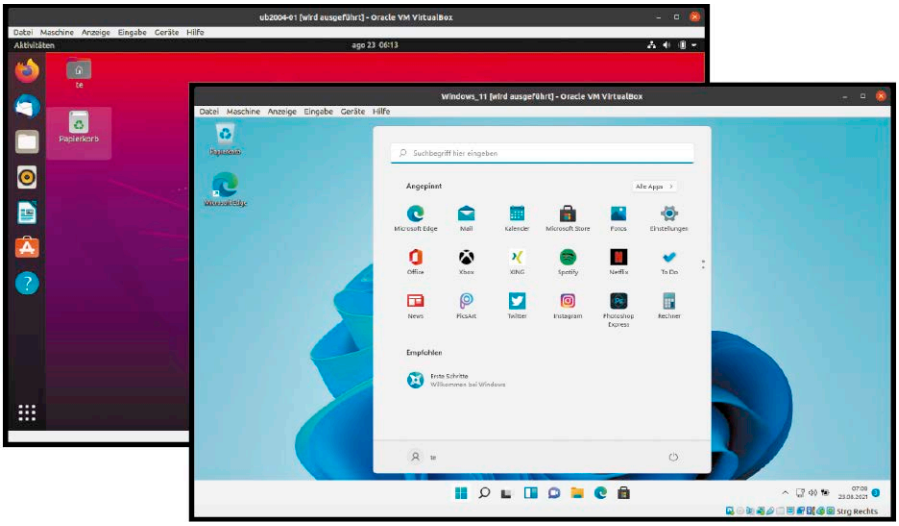
Cloudnetzwerke kann man über das Tool „Netzwerk-Manager“ konfigurieren. Für private Nutzer ist das wahrscheinlich weniger wichtig. Wer sich für OCI interessiert, findet Informationen dazu unter *https://www.oracle.com/de/cloud*.

Zusatzpakete werden jetzt über „Datei → Werkzeuge → Erweiterungspakete-Manager“ installiert und verwaltet. Neu ist außerdem die Übersicht unter „Datei → Werkzeuge → Überblick VM-Aktivitäten“. Damit lässt man sich die Auslastung etwa von Prozessor, RAM und Netzwerk anzeigen, entweder tabellarisch für alle VMs oder als Diagramm für eine VM. ■

Virtualisierung mit Virtualbox

Die vorausgehenden Seiten sollten zeigen, dass Virtualbox aus guten Gründen der beliebteste und funktionsreichste Virtualisierer unter Linux wie Windows ist. Wie Sie die Software praktisch nutzen, erklärt dieser Grundlagenbeitrag.

VON HERMANN APFELBÖCK



Oracle Virtualbox kann alles – und viel mehr, als dieser knappe Beitrag zeigen kann. Hier geht es nur um die Grundlagen – die Installation der Software, die Einrichtungsschritte für virtuelle Maschinen (VMs) und die allerwichtigsten Optimierungsmöglichkeiten.

1. Installation: Vollständig mit Erweiterungspaket

Die aktuelle Version (7.0.4) von Virtualbox erhalten Sie für alle Betriebssysteme unter *www.virtualbox.org/wiki/Downloads*. Zu den Varianten für die unterschiedlichen Linux-Distributionen führt dort der Link „Linux distributions“. Den Download installieren Sie dann nach Rechtsklick mit dem Paketmanager der Distribution, unter Windows durch Doppelklick des EXE-Programms. Anders als die Linux-Varianten bietet der Windows-Installer eine Selektion von Komponenten, wobei aber außer der Python-Unterstützung alle Optionen zu empfehlen sind.

Exkurs: Virtualbox ist selbstverständlich auch in den Paketquellen der Distributionen erhältlich. Dies aber in älteren Versionen 6.x, sodass der Vorteil einer automatischen Aktualisierung in diesem Fall keiner ist: Die Updates erstrecken sich nämlich nur auf die veraltete Hauptversionsnummer „6“. Eine weitere Installationsoption unter Linux wäre es noch, die Oracle-Paketquelle einzubinden und auf diesem Weg Updates für Version 7 zu erhalten. Dies führen wir hier nicht näher aus (siehe *www.virtualbox.org/wiki/Linux_Downloads*), da die Heft-DVD dafür eine Komplettlösung anbietet. Das dort vertretene Ubuntu 22.04.1 hat ein vorinstalliertes Virtualbox 7, das sich via Systemaktualisierung aktuell hält.

Erweiterungspaket: Auf der allgemeinen Downloadseite erscheint auch das „Oracle VM VirtualBox Extension Pack“. Dieses darf aus lizenzrechtlichen Gründen nicht mit dem freien Virtualbox ausgeliefert werden, ist aber für private Nutzung frei und kostenlos. Nach dem Download dieses Erweiterungspakets starten Sie Virtualbox und gehen im Virtualbox Manager auf „Werkzeuge“. Im mittleren Hauptfenster klicken Sie dann auf die Schaltfläche „Installieren“ und navigieren zum Download. Da der Dialog nur Dateien mit der Extension „.vbox-extpack“ anzeigt, ist die Auswahl einfach und eindeutig. Nach einem Warnhinweis startet die Installation. Das Erweiterungspaket ist zwar optional, aber für häufige Virtualbox-Nutzung uneingeschränkt zu empfehlen. Das frühere Hauptmotiv der USB-Unterstützung entfällt zwar, nachdem diese bereits im Basisprogramm vorliegt, aber das Erweiterungspaket bietet mit RDP-Fernsteuerung für Windows-VMs, Netboot und AES-Festplattenverschlüsselung nach wie vor nützliche Ergänzungen.

Gruppenzuweisung: Eine letzte Aktion vervollständigt die Installation unter Linux (unter Windows unnötig): Fügen Sie die Systembenutzer, die Virtualbox verwenden sollen, zur Gruppe „vboxusers“ hinzu:

```
sudo adduser [User] vboxusers
```

„[User]“ ersetzen Sie durch den Kontonamen des Benutzers. Wiederholen Sie den Befehl für alle gewünschten Konten. Melden Sie sich dann bei Linux ab und wieder an oder starten Sie das System neu. Diese vollständige Installation mit Erweiterung und Gruppenzuweisung ist für eine spora-

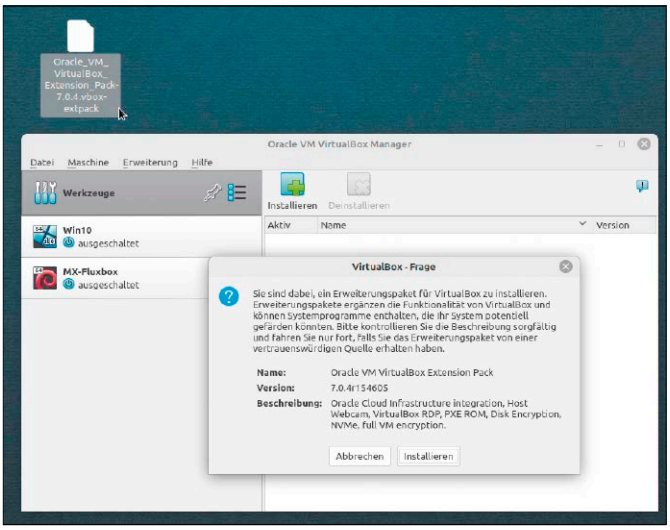
dische Nutzung von Virtualbox nicht zwingend, erspart aber eventuelle spätere Irritationen – insbesondere beim Versuch, USB-Geräte in einer VM zu nutzen.

2. Allgemeine Einstellungen

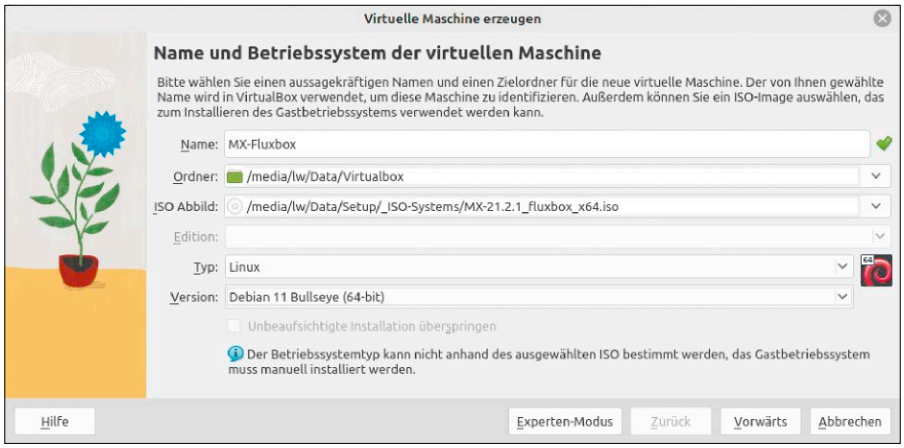
Der Start von Virtualbox am Desktop öffnet den „Oracle VM VirtualBox Manager" – zunächst nur mit dem Eintrag „Werkzeuge". Über eine grundsätzliche Einstellung können Sie vorab entscheiden, dies aber bei Bedarf auch später umstellen: Unter „Datei → Einstellungen → Allgemein" ist der Pfad vorgegeben, wo Virtualbox seine Dateien ablegen wird. Da dies viel Kapazität fordern wird, ist hier eventuell von vornherein ein Ort jenseits von „/home" besser geeignet.
Unter „Datei → Einstellungen → Eingabe → Virtuelle Maschine" lohnt sich in jedem Fall eine Durchsicht der Standard-Hotkeys. Den „Host"-Key mit Kombinationen wie Host-C, Host-L, Host-F, Host-Pos1 werden Sie ständig benötigen, um die VM-Darstellung (Vollbild; Skaliert, Fenster) zu ändern oder das VM-Fenstermenü zu aktivieren (Host-Pos1). Voreingestellter Host-Key ist die rechte Strg-Taste. Alle Hotkeys sind individuell einstellbar, auch der Host-Key.

3. Eine virtuelle Maschine einrichten

Mit der Schaltfläche „Neu" oder „Maschine → Neu" erstellen Sie eine VM. Den „Namen" vergeben Sie beliebig. Als „Ordner" ist voreingestellt, was unter „Datei → Einstellungen → Allgemein" als Standard gilt. Wichtig ist das „ISO Abbild", mit dem die Installation des neuen Systems erfolgt. Navigieren Sie hier über „Ändern" zum Installationsmedium des Systems. Dabei handelt es sich über die typischen Live- und Installer-Downloads für Linux-Distributionen oder um das Installations-ISO einer Windows-Version. Sobald dieses Medium eingetragen ist, erkennt Virtualbox automatisch „Typ" und „Version" dieses Systems. Falls nicht, wählen Sie „Typ" und „Version" manuell. Für Linux sind viele, aber nicht alle Distributionen aufgeführt. Nehmen Sie den Eintrag, der dem System am nächsten kommt, etwa „Ubuntu (64-bit)" für ein Linux Mint oder „Arch Linux (64 Bit)" für ein Endeavour-OS.
Wenngleich der Assistent die Hardwareeinstellungen von dieser Auswahl abhängig macht, ist diese Aktion – sofern überhaupt nötig – nicht kritisch, denn alle Voreinstellungen lassen sich durch manuelle Änderungen anpassen. Sie sollten aber für beste Kontrolle stets die Option „Unbeaufsichtigte Installation überspringen" anklicken.
Mit „Vorwärts" geht es zur RAM-Ausstattung und CPU-Vergabe für die VM. Vier GB und zwei CPU-Kerne sind für die meisten VMs ausreichend. Zum Teil genügt weniger. Die Einstellung hängt nicht zuletzt von der Hardware des Hostsystems ab und von der Frage, ob Virtualbox eventuell künftig sogar mehr als eine VM gleichzeitig mit Ressourcen versorgen soll. Kritisch sind auch diese Vorgaben nicht, da sie sich später – bei ausgeschalteter VM – jederzeit anpassen lassen.
Nach „Vorwärts" kommt der Punkt „Virtuelle Festplatte" mit drei Optionen. Im einfachsten Fall brauchen Sie überhaupt keine Festplatte („Keine Festplatte hinzufügen"), dann nämlich, wenn die VM nur ein Linux-Livesystem starten soll. Dann genügt das bereits vorher eingestellte ISO-Image. Soll das System hingegen ordentlich installiert werden, wählen Sie die oberste Option „Jetzt eine virtuelle Festplatte erstellen". Die Kapazität wählen Sie umso großzügiger, je länger die VM voraussichtlich laufen soll (Updates, Installationen). 30 bis 50 GB sind für Linux-Systeme realistisch, 50 bis 100 GB für Windows.
Wer sich hier nicht sicher ist, sollte die Option „Volle Größe erzeugen" immer inaktiv belassen (Standard) und damit eine dynamische virtuelle Festplatte erzeugen. Das hat zwei Vorteile – und einen Nachteil:
• Eine dynamische virtuelle Festplatte (VDI-Datei) fordert nur den aktuell nötigen Platz und wächst bis zum angegebenen Maximum. Sie belegt also eventuell nur 10 GB, obwohl 50 GB eingestellt sind.
• Eine dynamische VDI lässt sich später ohne Aufwand erweitern. Unter „Werkzeuge → Medien → Festplatten" gibt es einen Schieberegler wie bei der Ersteinrichtung.



Erweiterungspaket für Virtualbox: Das Zusatzpaket ist optional, bietet aber unter anderem den Zugriff auf USB 2.0/3.0. Am besten integrieren Sie es sofort nach der Virtualbox-Installation.



Anlegen einer neuen VM: Das „ISO-Abbild" mit dem Installationsmedium des gewünschten Systems ist in Virtualbox 7 eine erste und wichtigste Entscheidung.

Anlegen der Festplatte: Dynamische Festplatten belegen anfänglich wenig Platz, lassen sich später leicht vergrößern, sind aber langsamer als Laufwerke mit statischer Größe („Volle Größe“).

• Eine statische VDI („Volle Größe erzeugen“) ist im späteren Betrieb schneller.

Nach Abschluss des Schrittes „Virtuelle Festplatte“ und „Vorwärts“ ist die Definition der VM beendet und der grafische Assistent zeigt die Zusammenfassung.

Hinweis: Auf die dritte Option „vorhandene virtuelle Festplatte“ gehen wir später ein (Punkt 9).

4. Anpassungen der virtuellen Maschine

Die VM-Einrichtung via Virtualbox-Assistent führt in aller Regel zu einer sofort lauffähigen VM, lässt aber interessante Optionen außen vor. Es lohnt sich praktisch immer, vor dem ersten Start auf das Angebot „Ändern“ zu klicken und alle Optionen durchzugehen. Die Mehrzahl dieser Optionen setzt entweder das allgemeine Erweiterungspaket (Punkt 1) oder die Gasterweiterungen (Punkt 6) voraus:

Nicht optional, sondern unentbehrlich ist im Punkt „Anzeige“ ein hoher Wert für „Grafikspeicher“, am besten immer „128 MB“. Bei manchen Linux-Gastsystemen wählt Virtualbox den Wert so unterdimensioniert, dass die grafische Oberfläche nicht startet. Aktivieren Sie an dieser Stelle außerdem die Option „3D-Beschleunigung aktivieren“.

Unter „Allgemein → Erweitert“ können Sie durch die „Gemeinsame Zwischenablage“ und „bidirektional“ Inhalte zwischen Host- und Gastsystem über die Zwischenablage austauschen. Dies lohnt sich ebenfalls für „Drag’n’Drop“, um Dateien vom Dateimanager des Hostsystems in den Dateimanager des Gastsystems zu ziehen. Unter „USB“ sollte nicht nur der USB-Controller aktiviert sein, sondern auch die richtige USB-Version. Diese Angabe orientiert sich am Hostsystem und am USB-Port, wo Sie eventuelle USB-Datenträger voraussichtlich nutzen wollen.

5. Installation des virtuellen Systems

Nach dem Start der VM bootet diese über das virtuelle DVD-Laufwerk das Installationsmedium. Eventuell erwarten Sie von dieser VM gar nicht mehr als den Start eines typischen Linux-Livesystems und eine Installation entfällt somit. Wo dies zutrifft, sollte eine solche VM ausdrücklich „Live“ im Namen tragen (etwa „Knoppix-Live“), um es in der Virtualbox-Liste von installierten VMs zu unterscheiden.

In der Regel wird die VM aber eine virtuelle Festplatte enthalten, auf welche Sie nun das System ordentlich installieren. Der Vorgang unterscheidet sich in keiner Weise von einer normalen physischen Installation. Er ist allenfalls einfacher, weil nur eine (virtuelle) Festplatte vorhanden ist. Nach Abschluss der Installation und Herunterfahren der VM sollten Sie – wie nach jeder Installation – das Installations-ISO aus der VM-Konfiguration nehmen. Dies erledigen Sie über „Ändern“ im Virtualbox Manager. Entfernen Sie unter „Massenspeicher“ aber nicht das komplette DVD-Laufwerk, sondern nur das eingehängte ISO-Image. Das geht mit der Klickbox ganz rechts neben „Optisches Laufwerk“ und der Option „Entfernt das virtuelle Medium...“.

Das virtuelle DVD-Laufwerk selbst kann später noch anderweitig nützlich sein, insbesondere aber für die Installation der Gasterweiterungen.

6. Gasterweiterungen in die VM installieren

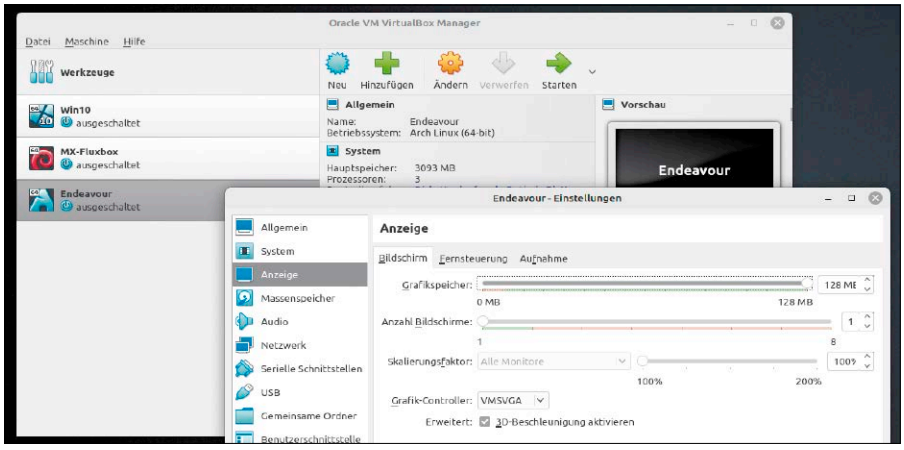
Im Unterschied zum allgemeinen Virtualbox-Erweiterungspaket werden die Gasterweiterungen in die jeweilige VM installiert. Gasterweiterungen sind optional, aber mindestens für häufiger genutzte VMs zu empfehlen. Sie enthalten Treiber für die Maus und den virtuellen Grafikadapter, verbessern damit Bildschirmauflösung, Skalierung, Mausverhalten und erlauben direkte Ordnerfreigaben zwischen Hostsystem und Gast-VM.

Die Gasterweiterungen lädt Virtualbox in das virtuelle DVD-Laufwerk einer laufenden VM, wenn Sie auf das VM-Fenstermenü „Geräte → Gasterweiterungen einlegen“ klicken. Falls die Menüleiste im Vollbild oder im skalierten Anzeigemodus nicht zugänglich ist, verwenden Sie den Hotkey Host-Pos1 (also standardmäßig Strg-Rechts-Pos1).

Das Installationspaket erscheint dann im DVD-Laufwerk der VM und in einer Windows-VM genügt dann der Doppelklick auf „VBoxWindowsAdditions.exe“. Unter Linux müssen Sie eventuell mit dem Terminal zum Pfad des DVD-Ordners navigieren und dann mit

```
sudo ./VboxLinuxAdditions.run
```

die Installation starten.



„Ändern“ der VM nach absolviertem Assistenten: Mindestens der Punkt „Anzeige“ verdient fast immer eine Korrektur beim „Grafikspeicher“.

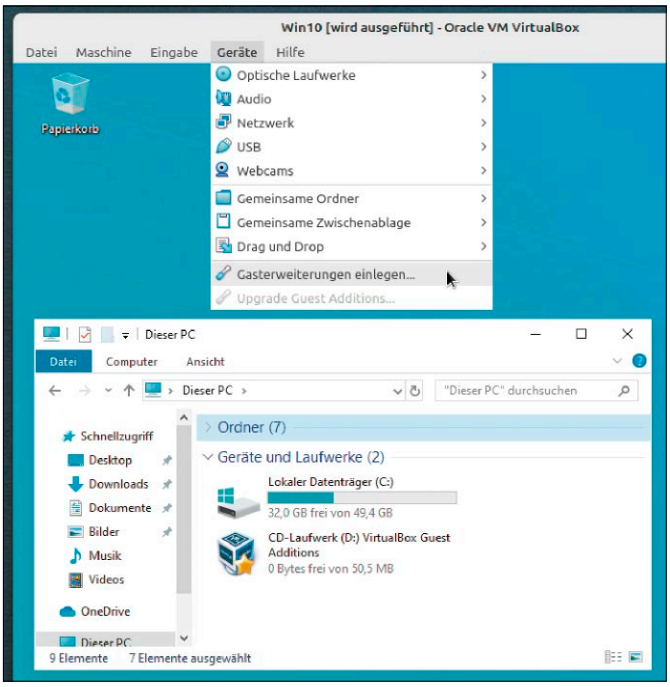
7. VM im Netzwerk: Netzwerkbrücke statt NAT

Standardmäßig gilt für VMs wie bei allen Virtualisierern der „NAT“-Modus im Netzwerk: Dabei dient Virtualbox selbst als virtueller Router und weist der VM eine zufällige IP-Adresse zu. Damit kommt die VM ins Internet, bleibt aber im lokalen Heimnetz isoliert. Es ist der VM zwar möglich, sich über die IP-Adressen des Heimnetzes mit Samba- oder SSH-Server zu verbinden, umgekehrt ist aber keine Verbindung zur VM möglich (SSH, Samba, VNC, RDP, Apache …). Wenn eine VM einen Dienst im Heimnetz anbieten soll, ist eine andere Einstellung erforderlich. Möglichkeiten gibt es mehrere, aber die einfachste erfordert nur einen einzigen Klick und sollte in den meisten Fällen genügen. Gehen Sie bei einer eingerichteten VM nach „Ändern“ auf das „Netzwerk“. Hier finden Sie unter „Netzwerk → Angeschlossen an“ eine Reihe weiterer Optionen. Mit „Netzwerkbrücke“ verbindet sich eine VM direkt mit dem Heimnetz. Die VM erhält also vom Heimrouter via DHCP eine lokale IP-Adresse genau wie ein physischer Rechner. Das macht die VM zum gleichberechtigten Mitglied des lokalen Netzes und sie kann dann von jedem anderen Gerät erreicht werden. Die Umstellung von „NAT“ zu „Netzwerkbrücke“ kann im Virtualbox Manager jederzeit und auch für eine aktuell laufende VM erfolgen.

8. Virtuelle Maschinen umziehen

Bei längerer Benutzung von Virtualbox summieren sich schnell einige VMs, die mit großen virtuellen Festplatten die Kapazität der Systempartition überfordern. Wenn alternative Datenträger zur Verfügung stehen, dann ist der Umzug von VMs kein Problem: Sie klicken einfach im Virtualbox Manager mit rechter Maustaste auf die betreffende VM und wählen dann „Verschieben“. Die Option ist nur aktiv, wenn die VM aktuell ausgeschaltet ist. Danach müssen Sie nur noch zum gewünschten neuen Zielordner navigieren. Virtualbox verschiebt dabei den Ordner mit dem Namen der VM inklusive Konfigurationsdatei (.vbox) und virtueller Festplatte (.vdi).

Wenn Sie ab einem bestimmten Zeitpunkt aus Platzgründen alle neu hinzukommenden VMs an einer anderen Stelle ablegen wollen, dann ändern Sie im Virtualbox Manager mit „Datei → Einstellungen → Allgemein“ den voreingestellten Standardpfad für die VMs. Die VMs aus dem bisherigen Standardpfad funktionieren weiterhin.



Optionale Gasterweiterungen (hier für Windows-VM): Über das Menü „Geräte“ lädt Virtualbox das Paket in das virtuelle DVD-Laufwerk. Von hier wird es dann in die VM installiert.

9. Virtuelle Festplatten von Vmware

Virtualbox kann die virtuellen Festplatten des Vmware Player (*.vmdk) direkt und ohne Konvertierung nutzen. Beim Erstellen einer VM wählen Sie beim Punkt „Virtuelle Festplatte“ die Option „Eine vorhandene virtuelle Festplatte verwenden“ und navigieren dann zur VMDK-Datei. Klicken Sie auf die erste, unbezifferte und kleinste dieser Dateien. Das ist der Verwaltungszeiger auf eventuell zahlreiche Inhaltsdateien einer dynamischen Festplatte. Die restliche Einrichtung der VM verläuft unverändert.

10. Virtualbox via Terminal

Virtualbox ist lückenlos – ohne grafischen Virtualbox Manager – über Terminalbefehle zu bedienen. Ein Motiv dafür werden Desktopnutzer angesichts der komfortablen Oberfläche zunächst nicht sehen. Im Netzwerk und mit SSH-Verbindung zum Hostsystem kann diese Option aber nützlich werden.

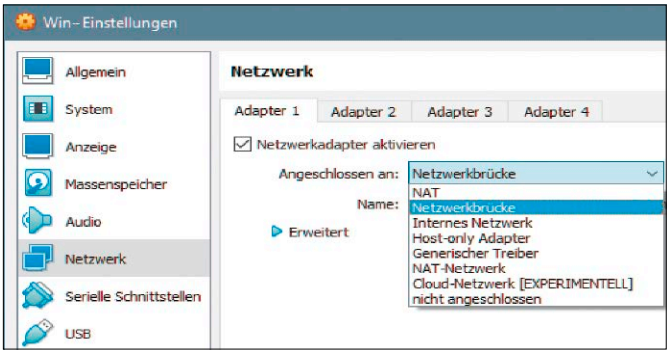
Dann ist nämlich nach SSH-Anmeldung am Hostsystem eine VM etwa mit

```
vboxmanage startvm "Cent-OS"
```

übers Netzwerk zu starten. Die auf dem Host vorhandenen VMs und deren genaue Namen kann der Befehl *vboxmanage list vms* ermitteln. Mit

```
vboxmanage controlvm "Cent-OS"
  poweroff
```

ist eine VM per SSH-Befehl auch wieder zu beenden. Für grafische VM-Desktops ist solche Fernbedienung kaum relevant, wohl aber für VMs, die im Netzwerk eine Serverfunktion erfüllen. Und auf dem lokalen Hostsystem kann die Terminalmethode nützlich sein, um eine VM per Autostart automatisch zu laden. ■

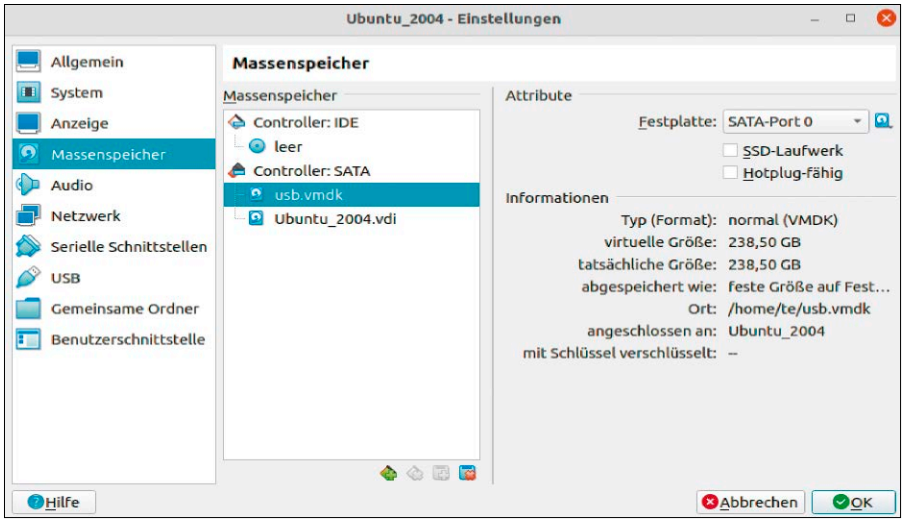


Wichtige Netzwerkeinstellung: Wenn die VM wie ein gleichberechtigter Rechner im lokalen Netz arbeiten soll (etwa als Server), hilft die Umstellung von „NAT“ auf „Netzwerkbrücke“.

Profitipps für Virtualbox

Ein Zweit-PC in Virtualbox funktioniert fast wie ein „echter“ Computer. Aber eben nur fast. Unsere Tipps helfen dabei, einige der Einschränkungen zu umgehen.

VON THORSTEN EGGELING



USB-Stick im Bios-Modus booten: Der Start des Systems gelingt über eine VMDK-Datei am „SATA-Port 0“. Deren Inhalt verweist direkt auf den USB-Stick am Host-PC.

Virtuelle Maschinen (VMs) arbeiten mit virtueller Hardware – und die hat nichts mit dem zu tun, was tatsächlich in Ihrem PC steckt. Eine Ausnahme sind einige USB-Geräte, beispielsweise USB-Laufwerke, von denen man mit den richtigen Einstellungen sogar booten kann. Auch im Netzwerk verhält sich eine VM mit Standardkonfiguration nicht wie andere PCs, was sich aber ebenfalls ändern lässt. Für den direkten Datenaustausch zwischen Host und Gast bietet Virtualbox alternativ spezielle Funktionen an.

System vom USB-Stick booten

In VMs mit aktiviertem Uefi binden Sie ein USB-Gerät über die Einstellungen ein. Gehen Sie dort auf „USB“ und wählen Sie den USB-Stick über die Schaltfläche mit dem grünen Plussymbol aus. Die Option „USB-3.0-Controller (xHCI)“ muss aktiviert sein, wenn der Stick mit einem USB-3.0-Port verbunden ist. Starten Sie die VM und setzen Sie den USB-Stick in der Bootreihenfolge an die erste Stelle, entsprechend der Beschreibung im nächsten Tipp. Danach lässt sich das System vom USB-Stick im Uefi-Modus booten.

Bios-Modus: Der USB-Stick muss als physisches Laufwerk in die VM eingebunden werden. Dafür sind erhöhte Zugriffsrechte erforderlich, die Sie als Mitglied der Gruppe „disk“ erhalten:

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

Den Platzhalter „[User]“ ersetzen Sie durch Ihren Benutzernamen. Melden Sie sich bei Linux ab und wieder an. Ermitteln Sie den Gerätepfad des Sticks im Terminal:

```
lsblk -p
```

Wenn in der Ausgabe beispielsweise „/dev/sdf“ für den USB-Stick auftaucht, hängen Sie das Gerät mit

```
sudo umount /dev/sdf?
```

aus. Danach verwenden Sie diesen Befehl (eine Zeile):

```
vboxmanage createmedium disk
  --filename ~/usb.vmdk
  --format=VMDK --variant RawDisk
  --property RawDrive=/dev/sdf
```

In den Einstellungen einer virtuellen Maschine gehen Sie auf „Massenspeicher“, klicken auf „Controller SATA“ und dann auf das Icon ganz rechts daneben („Festplatte hinzufügen“). Wählen Sie „usb.vmdk“ und klicken Sie auf „Auswählen“. Legen Sie die Reihenfolge hinter „Festplatte“ fest. „usb.vmdk“ muss mit „SATA-Port 0“ verbunden sein, die Systemfestplatte mit dem nächsten freien Port. Wenn Sie den virtuellen PC starten, bootet er vom USB-Laufwerk. Wird der Stick vom PC entfernt, müssen Sie „usb.vmdk“ wieder aus der Konfiguration löschen. Das System startet sonst nicht.

Bios/Uefi-Firmwaresetup aufrufen

Eine neu erstellte VM bootet von der ISO-Installationsdatei und das System lässt sich dann auf der bisher leeren virtuellen Festplatte installieren. Da im Uefi-Modus die nun bootfähige Festplatte in der Bootreihenfolge an erste Stelle steht, ist es nicht mehr möglich, ein System aus der ISO-Datei zu booten, etwa für eine Windows-Reparatur.

Die Bootreihenfolge lässt sich aber in der Uefi-Firmware der VM ändern. Dazu klickt man beim Start der VM möglichst schnell in das Fenster und drückt mehrfach die Esc-Taste. Der richtige Zeitpunkt ist allerdings schwer abzupassen – einfacher geht der Start in die Uefi-Firmware im Windows-Gastsystem mit

```
shutdown -r -fw -t 0
```

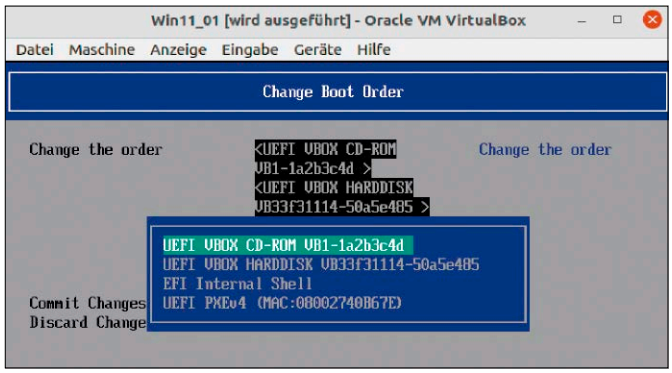
in einer Eingabeaufforderung mit Administratorrecht. Bei Linux-Systemen kommt

```
sudo systemctl reboot --firmware-
  setup
```

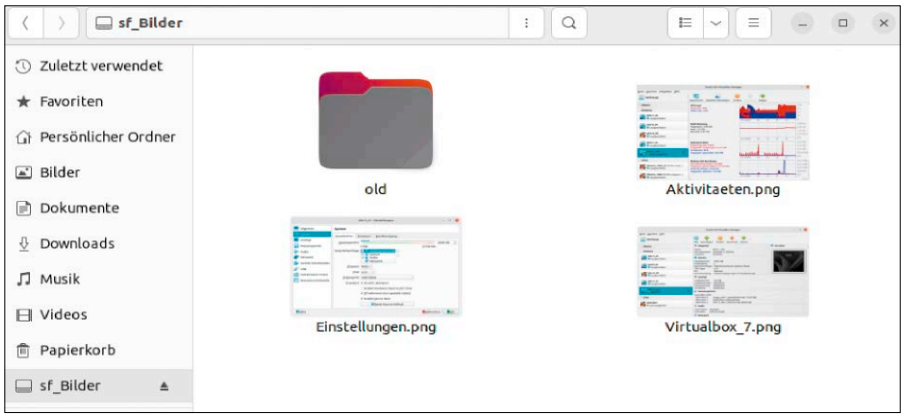
zum Einsatz.

Im Firmwaresetup navigiert man über „Boot Maintenance Manager“ zu „Boot Options → Change Boot Order“ und drückt die Eingabetaste. Mit den Tasten „+“ und „-“ lässt sich die Reihenfolge ändern und „UEFI VBOX CD-ROM“ an die erste Position schieben. Will man auch vom USB-Stick booten, setzt man diesen an die zweite Stelle. Bestätigen Sie mit der Eingabetaste und danach mit „Commit Changes and Exit“. Mit zweimal Esc gelangen Sie zurück ins Hauptmenü, in dem Sie „Continue“ wählen. Die VM bootet jetzt von der konfigurierten ISO-Datei.

Bios-Modus: Die Bootreihenfolge lässt sich in den Einstellungen einer VM unter „System“ festlegen. Standardmäßig befindet sich das virtuelle CD/DVD-Laufwerk in der Reihenfolge vor der Festplatte, was sich auch nicht automatisch ändert. USB-Laufwerke werden in den Einstellungen nicht berücksichtigt (siehe vorheriger Tipp). Beim Start einer VM kann man das Bootgerät über die Taste F12 temporär wählen.



Uefi-Bootreihenfolge: Von welchem Laufwerk eine VM bootet, stellen Sie im Firmwaresetup ein. Es lässt sich mit der Esc-Taste beim Start der virtuellen Maschine aufrufen.



Zugriff auf den Host-PC: „Gemeinsame Ordner“ sind eine Alternative zu Netzwerkfreigaben. Unter Linux – im Beispiel „sf_Bilder“ – ist der Ordner direkt im Dateimanager zu sehen.

Datenaustausch zwischen VM und Host

Standardmäßig konfiguriert Virtualbox den Netzwerkadapter für „NAT“. Die VM kann mit dieser Einstellung die Internetverbindung nutzen, erhält aber keinen Zugriff auf das lokale Netzwerk. Das lässt sich ändern, indem man den Netzwerkadapter als „Netzwerkbrücke“ konfiguriert. Schadsoftware in der VM kann dann allerdings ungeschützte Dateifreigaben infizieren. Die Verwendung der Alternative „Gemeinsamer Ordner“ gilt als sicherer, weil nur genau dieser Ordner betroffen sein kann. Voraussetzung dafür sind die installierten Gasterweiterungen (siehe Artikel ab Seite 36).

Gehen Sie im Fenster der laufenden VM auf „Geräte → Gemeinsame Ordner → Gemeinsame Ordner“. Über die „+“-Schaltfläche bestimmen Sie einen Ordner auf dem Host-PC für den Datenaustausch. Setzen Sie ein Häkchen vor „Automatisch einbinden“. Damit ein Nutzer auf den gemeinsamen Ordner zugreifen darf, fügen Sie ihn im Gastsystem zur Gruppe „vboxsf“ hinzu:

```
sudo usermod -aG vboxsf [User]
```

„[User]“ ersetzen Sie durch den gewünschten Benutzernamen. Starten Sie das Gastsystem neu. Den gemeinsamen Ordner finden Sie unter Linux im Navigationsbereich des Dateimanagers mit dem Präfix „sf_“. Unter Windows erreichen Sie den Ordner im Windows-Explorer über „Netzwerk“ und „Vboxsrv“.

Virtualbox bietet über „Maschine → Dateimanager“ im Fenster einer VM eine weitere Methode für den Datenaustausch. Geben Sie rechts unten Benutzernamen und Passwort für die Anmeldung im Gastsystem ein und klicken Sie auf „Sitzung öffnen“. Die Dateisysteme von Host- und Gast-PC werden nebeneinander angezeigt. Über die Schaltflächen in der Mitte lassen sich markierte Elemente übertragen.

Virtuelle Maschinen automatisch starten

Der Autostart ist bei VMs wünschenswert, in denen Serverdienste laufen. Die Dienste stehen dann im Netzwerk zur Verfügung, ohne dass der Benutzer eingreifen oder sich anmelden muss. Einen Systemd-Dienst mit dem Namen „vboxautostart-service“ richtet Virtualbox bei der Installation ein. Zur Konfiguration tragen Sie in die Datei „/etc/default/virtualbox“ diese zwei Zeilen ein:

```
VBOXAUTOSTART_DB=/etc/vbox
VBOXAUTOSTART_CONFIG=/etc/vbox/
  vboxauto.conf
```

Erstellen Sie die Datei „/etc/vbox/vboxauto.conf“ mit diesem Inhalt (zwei Zeilen):

```
default_policy = deny
[User] = {allow = true}
```

Den Platzhalter „[User]“ ersetzen Sie durch Ihren Benutzernamen. Danach führen Sie die folgenden vier Befehle aus:

```
sudo chgrp vboxusers /etc/vbox
sudo chmod 1775 /etc/vbox
VBoxManage setproperty
  autostartdbpath /etc/vbox
VBoxManage modifyvm "[VM]"
  --autostart-enabled on
  --autostop-type savestate
```

Für den Platzhalter „[VM]“ setzen Sie den Namen der virtuellen Maschine ein, die automatisch starten soll. Der Netzwerkadapter der VM muss als „Netzwerkbrücke“ konfiguriert sein, damit Serverdienste im lokalen Netzwerk erreichbar sind. Starten Sie Linux neu. Die virtuelle Maschine startet dann automatisch und deren Serverdienste sind im Netz verfügbar. ■

Fertige virtuelle VMs

Virtuelle Maschinen muss man nicht zwingend in Virtualbox konfigurieren, danach manuell installieren und mit Software und Diensten ausstatten. Windows, zahlreiche Linux-Desktops und viele Linux-Server gibt es komplett vorkonfiguriert zum Download.

VON HERMANN APFELBÖCK

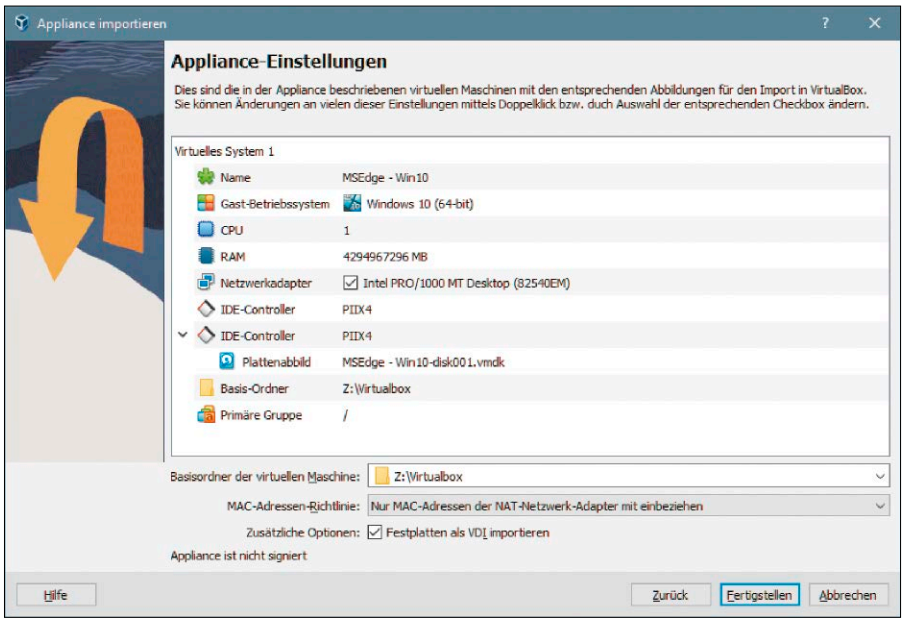
Für komplett ausgestattete VMs (Appliances) gibt es etliche und ergiebige Anlaufstellen im Internet. Im Prinzip ersparen Sie sich damit die Hardwareeinrichtung in Virtualbox, die anschließende Installation des Systems und eventuell die Konfiguration eines komplexen Serverdienstes. Ob und wo sich das wirklich lohnt, hängt vom Verwendungszweck und vom Nutzer-Know-how ab.

OVA-Format: Eingepackte PCs

Die standardisierte Hardware virtueller Maschinen macht es möglich, komplette Systeme einzupacken (Appliance) und diese auf jedem anderen Rechner via Virtualisierer zu starten. Als Virtualbox-Nutzer werden Sie theoretisch selbst mühelos zum Appliance-Entwickler, indem Sie eine sorgfältig konfigurierte VM mit dem Menü „Datei → Appliance exportieren“ als Appliance sichern und weitergeben können. Das Resultat der Aktion ist eine OVA-Datei (Open Virtual Appliance), im Prinzip ein gepacktes TAR-Archiv.

Vmware kennt die Methode analog und verwendet dabei das Format OVF (Open Virtualization Format). Dieses kann Virtualbox ebenso wie sein natives OVA-Format mit „Datei → Appliance importieren“ importieren.

Virtuelle Appliances werden aber nicht immer im OVA-Format angeboten: Die Seite *www.osboxes.org* liefert zum Beispiel grundsätzlich nur die virtuelle Festplatte aus, also VDI-Dateien für Virtualbox. Was ist der Unterschied zu OVA? Virtuelle Maschinen für Virtualbox bestehen im Wesentlichen nur aus dem VDI-Festplattenabbild und einer kleinen XML-Konfigurationsdatei mit der Endung „.vbox“. Folglich genügt eigentlich die virtuelle Festplatte, denn die Konfiguration für ein System ist mit dem Virtualbox Manager in drei Minuten erstellt. Das OVA-Paket hat daher gegenüber einem puren VDI-Abbild nur den kleinen Vorteil, die Konfiguration mitzuliefern, und als zweiten Vorteil eine reduzierte Downloadgröße dank Komprimierung.



Einfacher Import: Eine komplette VM im OVA-Format enthält das Festplattenabbild plus Konfiguration des virtuellen PCs. Letztere können Sie bei Bedarf anpassen.

Schlüsselfertige Desktop-VMs

Die schon genannte Site *www.osboxes.org* bietet nur die Festplattenabbilder. Klicken Sie dort auf „VM Images“ und wählen Sie das benötigte Format – VDI für das hier bevorzugte Virtualbox. Die zahlreichen virtuellen Festplatten sind standardmäßig 7z-gepackt. Unter Windows muss daher der Packer 7-Zip vorliegen (*www.7-zip.de*), unter Linux ist 7z-Unterstützung in der Regel Standard und im Bedarfsfall mit

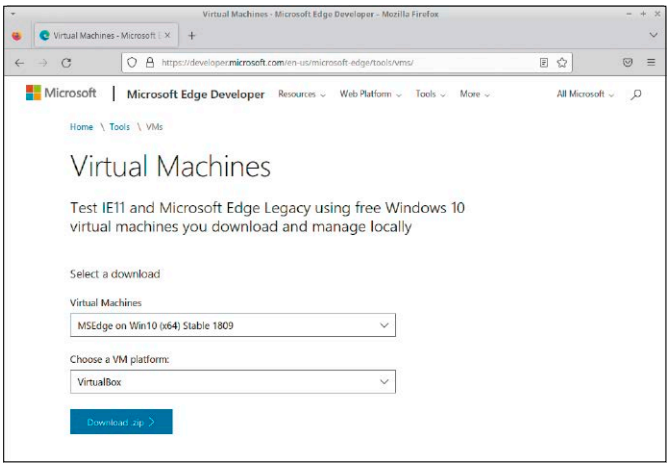
```
sudo apt install p7zip p7zip-full
```

schnell nachgerüstet. Die VDI-Images lassen sich dann einbinden, indem Sie in Virtualbox eine neue virtuelle Maschine erstellen und bei der Festplattenkonfiguration „Eine vorhandene virtuelle Festplattendatei verwenden“. Dazu klicken Sie auf das Ordnersymbol und navigieren zur heruntergeladenen VDI-Datei (der Pfad ist im Prinzip beliebig, aber für bessere Übersicht empfiehlt sich ein Sammelordner für solche VDIs). Nach Auswahl und „Hinzufügen“ ist die VM schon startklar.

Bei den Osboxes-Images handelt es sich überwiegend um Linux-Desktops (von „Android x86“ bis „Zorin OS“), die Sie anschließend beliebig anpassen können. Ganz ohne Pflegeaufwand sind sie dennoch nicht: Wenn Ihnen das voreingestelle Standardkonto – meist „osboxes“ mit Kennwort „osboxes.org“ – nicht zusagt, müssen Sie ein neues Konto einrichten. Oberfläche, Tasta-

tur, Zeitzone sind grundsätzlich US-amerikanisch, was in den Regions- und Spracheinstellungen des jeweiligen Systems geändert werden muss.

Weitere Eigenheiten einer Appliance sind nie auszuschließen. Der Download einer fertigen Desktop-Appliance garantiert zwar den besonders schnellen Einsatz, bleibt aber eher eine Empfehlung für die unkomplizierte Wegwerf-VM. Zudem bietet *www.osboxes.org* nicht durchgehend aktuelle Versionen, sondern zum Teil auch ältere Systeme. Wer eine Desktop-VM für den nachhaltigen Dauerbetrieb einrichten will, nimmt vielleicht doch besser die Mühe der Installation mit dem Originalsystem in Kauf.



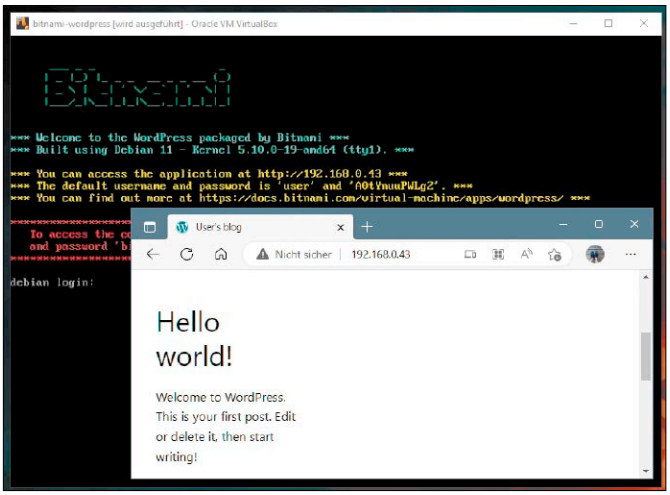
Die kostenlosen Windows-VMs von Microsoft sind primär für Webentwickler gedacht, enthalten aber ein vollständiges Windows für jeden Einsatzzweck.

Windows-Appliance von Microsoft

Microsoft bietet virtuelle Windows-Maschinen unter *https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/* kostenlos zum Download an. Das Angebot richtet sich an Entwickler, die Webseiten mit Edge testen wollen. Es handelt sich aber um komplette Windows-Systeme, die 90 Tage ohne Einschränkung laufen. Das verfügbare Windows 10 („MsEdge on Win10 (x64) Stable 1809“) hat eine Downloadgröße von 6,7 GB. Unter „Select platform“ stellen Sie „Virtualbox“ ein. Den gezippten Download entpacken Sie, öffnen die OVA-Datei per Doppelklick in Virtualbox oder wählen dort „Datei → Importieren“.

Microsoft gibt auf der Website den Tipp, vor dem ersten Start einen Schnappschuss der VM zu erstellen. Stellen Sie diesen vor Ablauf der 90 Tage wieder her, dann lässt sich die Windows-Appliance weitere 90 Tage nutzen. Dieser Hinweis und weitere Tipps zum Verlängern der Laufzeit erscheinen auch beim ersten Start der VM unübersehbar als Wallpaper. Für Linux-Anwender, die Windows vorübergehend für spezielle Software benötigen, ist die Appliance die eindeutig einfachere Alternative gegenüber der Installation des Windows-10-Enterprise-ISOs.

Ohne Nachbearbeitung geht es aber nicht: Das Wallpaper mit den Tipps wird früher oder später lästig. Eventuell wollen Sie auch das Standardkonto „IEUser“ mit Passwort „Passw0rd!“ ändern. Und auch die englischsprachige Oberfläche sowie die Zeitzone müssen über die „Einstellungen“ (Win-I) und „Time & Language → Region“ erst auf Deutsch und europäische Zeitzone gesetzt werden.



Typische Server-Appliance: Diese Wordpress-Instanz auf Debian-Basis von *www.bitnami.com* erspart die Webserver-Konfiguration und ist sofort im lokalen Netzwerk einsatzbereit.

Server-Appliances von Bitnami, Turnkey & Co.

Auf Serversysteme spezialisiert sind die Sites *www.bitnami.com* und *www.turnkeylinux.org*. Hier erhalten Sie – überwiegend in OVA-Format – CMS-Systeme wie Drupal, Typo3, Joomla und Wordpress sowie eine Vielzahl von Shop- und Entwicklungssystemen. Die VMs sind mit allem ausgestattet, was zum Betrieb notwendig ist, und ersparen Installation und Konfiguration von Apache/Nginx, My SQL und PHP. Das ist für alle, erst recht für unerfahrene Nutzer ein unschätzbarer Gewinn. Natürlich sind auch die Netzwerkeinstellungen der VM gleich so gesetzt („Netzwerkbrücke“), dass Serveranwendungen sofort funktionieren.

Eher an Entwickler und Firmen richtet sich das Appliance-Angebot von Vmware (*https://marketplace.vmware.com/vsx*). Das Portal bietet vorkonfigurierte Spezialsysteme. Nicht alle virtuelle PCs sind hier frei verfügbar, einige erfordern eine Registrierung oder eine Gebühr. Eine einmal optimierte VM als OVA-Paket oder als VDI-Image weiterzugeben, ist denkbar einfach. Daher lohnt sich die Suche nach einem solchen Angebot auch bei vielen Einzelprojekten, wie folgende, eher zufällig gewählte Beispiele abschließend zeigen sollen:

Only Office: Im Downloadbereich *www.onlyoffice.com/de/download-docs.aspx* lässt sich nach einem Klick auf „Community“ die „Univention-Anwendung“ wahlweise mit Nextcloud oder Owncloud als VM herunterladen und in Virtualbox importieren.

Whonix: Das anonymisierende Surfsystem ist in der Zielsetzung mit dem Livesystem Tails vergleichbar, hat aber als Virtualbox-Appliance einen anderen Ansatz mit zwei parallelen VMs. Die OVA-Appliance mit circa 2,2 GB gibt es unter *www.whonix.org/wiki/VirtualBox/XFCE*. Nach dem Import in Virtualbox erscheinen zwei neue VMs, wovon Sie immer erst das Gateway, danach die Workstation starten. Das Konstrukt erscheint aufwendig, läuft aber auf jedem durchschnittlichen Rechner mühelos. ■

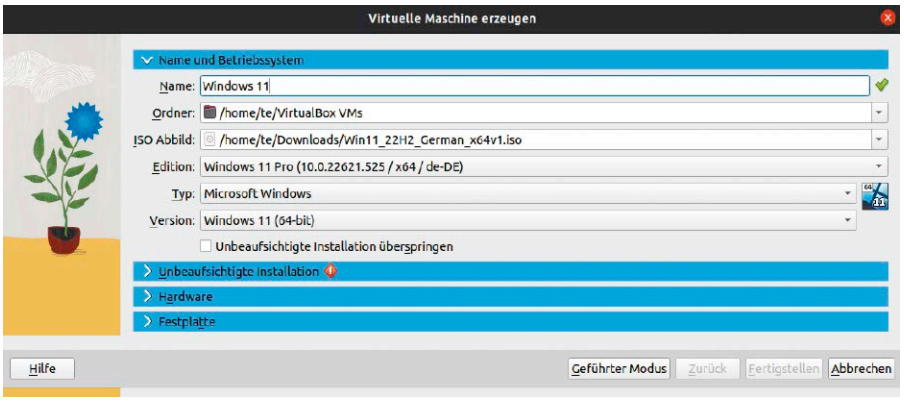
Linux hilft Windows

Nützliche Tools können unter Linux beim Umgang mit Windows-Installationen helfen. Man kann Windows vollautomatisch in einer virtuellen Maschine installieren oder ein vorhandenes Windows virtuell weiterverwenden.

VON THORSTEN EGGELING

Eine alternative Methode kann die Windows-Installation in Virtualbox beschleunigen. Das Setup kann unter Linux komplett automatisch und ohne Benutzereingaben erfolgen. Außerdem lässt sich ein bereits installiertes Windows auf eine virtuelle Festplatte übertragen und dann in Virtualbox weiterverwenden. Die Beschreibungen beziehen sich auf Ubuntu 20.04, 22.04, Linux Mint 20.x und 21. Bei anderen Distributionen weichen die Bezeichnungen der nötigen Zusatzpakete meist ab.

Service: Befehlszeilen und Beispieldateien für diesen Artikel können Sie über *https://m6u.de/depwin* abrufen. Darüber hinaus empfehlen wir die vorherige Lektüre der vorangehenden Virtualbox-Beiträge.



Windows in Virtualbox: Über den Assistenten ist die Windows-Installation schnell gelungen. Noch schneller und vollautomatisch lässt sich die Aufgabe per Script erledigen.

1. Virtuelle Festplatten und WIM-Dateien

Virtualisierungssoftware verwendet für die Installation von Systemen virtuelle Festplatten. Dabei handelt es sich um Dateien, die ein Festplattenabbild enthalten und sich wie eine physikalisch vorhandene Festplatte oder SSD nutzen lassen. Virtualbox verwendet standardmäßig VDI-Dateien (Oracle Virtual Disk Image), kann aber auch Microsofts VHD-Abbilder nutzen (Microsoft Virtual Hard Disk Format).

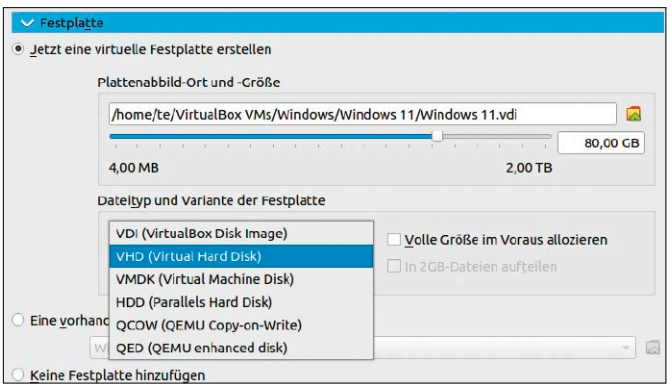
VHD und die Weiterentwicklung VHDX sind die Standardformate bei Microsofts Virtualisierungssoftware Hyper-V. Außerdem kann man seit Windows 7 aus einer VHD-Datei booten (Native Boot). Laut Microsoft soll man jüngeres VHDX bei Windows 10 und höher für Native Boot verwenden, bisher konnten wir aber bei Windows 10 und 11 keine Probleme mit dem VHD-Format feststellen. Virtualbox unterstützt das VHDX-Format zurzeit nicht, weshalb man beim Vorgänger bleiben muss, wenn man den PC auch direkt von der virtuellen Festplatte booten möchte. Wie sich eine VHD-Datei in den Windows-Bootmanager integrieren lässt, können Sie unter *https://m6u.de/depwin* nachlesen.

WIM (Windows Imaging Format) ist ein weiteres Abbildformat von Microsoft. WIM-Dateien sind komprimierte Archive eines Dateisystems, ähnlich wie ZIP-Dateien. Es können mehrere Dateisysteme enthalten sein, die sehr effizient gespeichert werden. Identische Dateien sind nur einmal enthalten. WIM-Dateien lassen sich für Windows-Backups nutzen, kommen aber vor allem bei der Windows-Installation zum Einsatz („install.wim“).

Das Windows-Setupprogramm bereitet die Partitionen sowie die Bootumgebung vor und extrahiert den Inhalt der Datei „install.wim“ auf das Ziellaufwerk. Auf das Windows-Setupprogramm ist man dabei nicht angewiesen. Eine WIM-Datei lässt sich auch unter Linux auf eine virtuelle oder physikalische Festplatte entpacken.

Für Windows 11 ergibt sich nebenbei der Vorteil, dass dann keine Hardwareprüfung erfolgt und sich das System also auch auf offiziell nicht unterstützter Hardware einrichten lässt.

Die Hardwarevoraussetzungen (siehe *https://bit.ly/Win11SP*) gelten ansonsten auch für virtuelle Maschinen.



Virtuelle Festplatte: Standardmäßig verwendet Virtualbox VDI-Dateien. VHD-Dateien lassen sich aber ohne Nachteile ebenfalls nutzen und eignen sich auch für Native Boot.

2. Linux-Tool für die Nutzung von WIM-Dateien

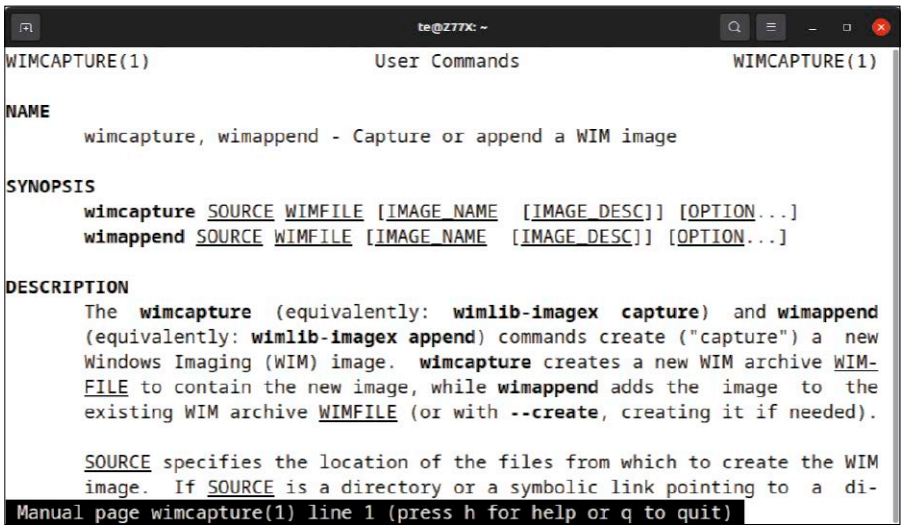
Unter Windows dient das Tool Dism zur Verwaltung von WIM-Dateien. Das Linux-Gegenstück dazu heißt wimlib-imagex (*https://wimlib.net*). Zu Installation verwenden Sie im Terminal die Zeile

```
sudo apt install wimtools
```

wimlib-imagex enthält Kommandos wie „apply" (entpacken), „capture" (archivieren) und „mount", womit sich eine WIM-Datei in das Dateisystem einhängen lässt. Um die Benutzung zu vereinfachen, gibt es einige Hardlinks auf wimlib-imagex, etwa wimapply, wimcapture und wimmount, über die sich die Kommandos direkt ausführen lassen. Der Aufruf ohne weitere Optionen liefert eine Kurzübersicht der möglichen Parameter. Mit beispielsweise

```
man wimcapture
```

erhalten Sie ausführliche Informationen mit Beispielen zur Verwendung.



Weitere Informationen: In den Manpages der einzelnen Wimlib-Tools finden Sie eine Übersicht der erforderlichen Parameter und Optionen sowie Beispiele zur Anwendung.

3. Windows in einer VHD-Datei installieren

Das Tool wimapply reicht aus, um Windows in eine VHD-Datei für eine virtuelle Maschine zu installieren. Die virtuelle Festplatte muss allerdings erstellt, partitioniert und formatiert werden. Danach lassen sich das Windows-System und die Windows-Bootumgebung einrichten. Wir gehen außerdem davon aus, dass Virtualbox bereits installiert ist. Das Virtualbox-Tool Vboxmanage für die Kommandozeile ermöglicht es, virtuelle Festplatten und virtuellen Maschinen automatisch zu erstellen.

Wir haben alle nötigen Befehlszeilen im Script „create_vhd_64.sh" für Windows 10 oder 11 (64 Bit) zusammengefasst (*https://m6u.de/depwin*). Wer Windows 10 in 32 Bit installieren möchte, verwendet „create_vhd_32.sh". Beide Scripts sind weitgehend identisch. Laden Sie das Paket unter „Releases" herunter und entpacken Sie es in Ihr Home-Verzeichnis, beispielsweise nach „deploy-windows".

Vorbereitungen: Bevor Sie die Scripts nutzen können, müssen Sie einige Zusatzpakete einrichten:

```
sudo apt install wimtools build-
  essential git libparted-dev
  python3-pip genisoimage libwin-
  hivex-perl qemu-utils pkg-config
  p7zip-full gettext
```

Sie benötigen das Tool ms-sys (*https://ms-sys.sourceforge.net*), mit dem sich ein Bootrecord für Windows erstellen lässt. Laden Sie die tar.gz-Datei herunter, entpacken Sie diese und führen Sie im Zielverzeichnis die Kommandos

```
make
sudo make install
```

aus. Die Hauptarbeit erledigt dann das Python-Script „setup_win10.py", das von *https://codeberg.org/regnarg/deploy-win10-from-linux* stammt. Es benötigt zusätzliche Python-Module, die Sie mit

```
pip3 install clize construct
  pyparted --user
```

installieren.

Nutzer der älteren Versionen Ubuntu 20.04 oder Linux Mint 20.x lassen pyparted weg und installieren diese Version:

```
pip3 install pyparted==3.11.7
  --user
```

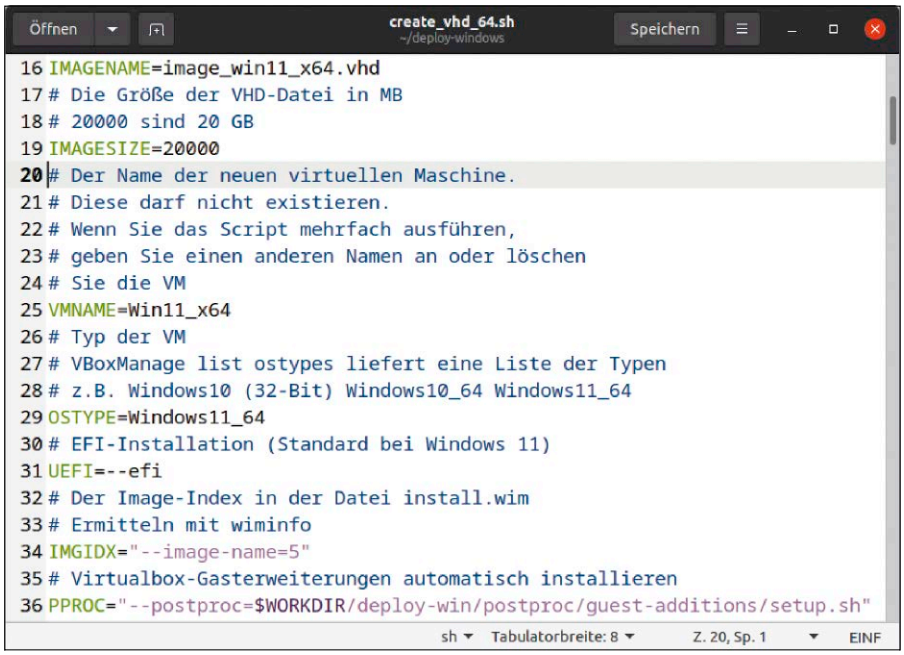
Laden Sie die ISO-Datei des Windows-Installationsmediums über *https://bit.ly/w10is* (Windows 10) oder *https://bit.ly/w11is* (Windows 11) herunter. Kopieren Sie die ISO-Datei in den Ordner „deploy-windows".

Script konfigurieren: Öffnen Sie „create_vhd_64.sh" oder „create_vhd_32.sh" in einem Texteditor und bearbeiten Sie den Abschnitt unter „Konfiguration". Hinter „ISOPATH=" tragen Sie die Bezeichnung der heruntergeladenen ISO-Datei ein. „IMAGESIZE=" legt die Größe der VHD-Datei fest. Hinter „NICDEVICE=" tragen Sie den Namen des Netzwerkadapters ein, den Sie im Terminal mit *ip a* ermitteln. Die Variable „PPROC" enthält den Pfad zu einem Script für die automatische Einrichtung der Virtualbox-Gasterweiterungen. Hinter „UNATT=" steht der Pfad zu einer XML-Datei für die

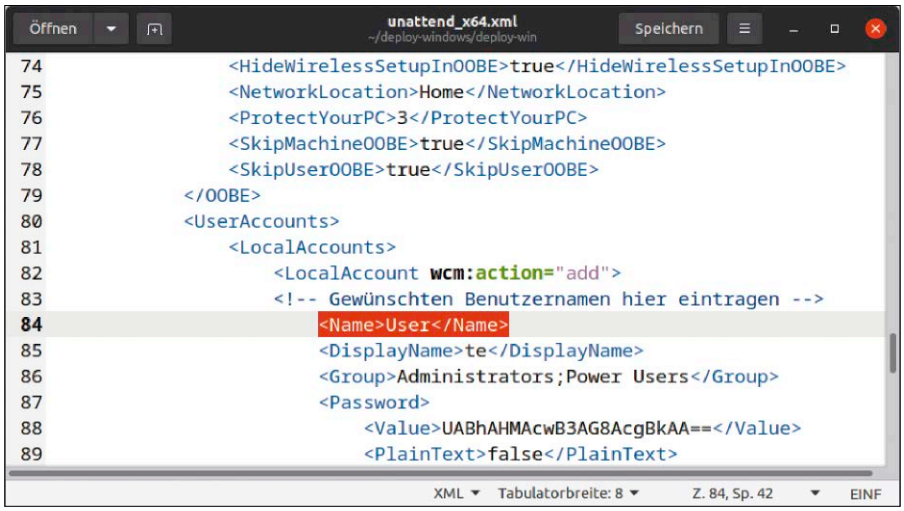
DIE KONFIGURATION DES WINDOWS-BOOTMANAGERS

Die Datei „BCD" enthält eine Datenbank mit Konfigurationsdaten für den Windows-Start. Es sind beispielsweise Informationen über das Startlaufwerk und der Pfad zum Startladeprogramm enthalten. Die Datei liegt auf der EFI-Partition im Order „EFI/Microsoft/Boot". Linux kann die BCD-Datenbank bislang nicht neu erstellen. Man kann aber die Datei vom Installationsdatenträger verwenden und bearbeiten. BCD verwendet das gleiche Speicherformat wie die Windows-Registry, weshalb die Datei sich mit Registrytools für Linux anpassen lässt. Eine Dokumentation der Optionen können Sie unter *https://m6u.de/WBCD* finden.

Über *https://m6u.de/depwin* können Sie ein Script und eine Reg-Datei aus dem Ordner „BCDs" herunterladen, die demonstrieren, wie sich eine universelle BCD-Datei für die Windows-Installation erstellen lässt. Für die Tipps dieses Artikel benötigen Sie das nicht, weil eine bereits vorbereitete BCD-Datei im Ordner „deploy-win" liegt.



Script anpassen: Das Script enthält einen Konfigurationsabschnitt, in dem Sie unter anderem die Größe der VHD-Datei und den Namen der virtuelle Maschine festlegen.



Automatische Windows-Installation: Die Datei „unattend_x64.xml“ dient der Windows-Konfiguration. Tragen Sie den gewünschten Benutzernamen für das lokale Konto ein.

automatische Windows-Installation ohne Benutzereingaben. Passen Sie die Datei für Ihre Installation an, die Kommentare geben dabei Hilfestellung.

Script starten: Führen Sie das Script im Terminal im Verzeichnis „deploy-windows“ etwa mittels

```
./create_vhd_64.sh
```

und Standardrechten aus. Das Script fordert das Passwort für höhere Rechte an. Anschließend können Sie die neue VM in Virtualbox starten. Wenn Sie das Script für eine weitere Installation verwenden wollen, müssen Sie in der Konfiguration andere Namen für die VHD-Datei und die virtuelle Maschine eintragen.

Bitte beachten Sie: Wenn Sie die VHD-Datei auch für Native Boot (siehe Punkt 1) verwenden möchten, sind Sicherungspunkte außerhalb der VM wirkungslos. Für eine Sicherung kopieren Sie einfach die VHD-Datei.

4. Weitere Anwendungen für wimlib-imagex

Die Wimlib-Installation enthält das Script „mkwinpeimg“, mit dem sich ein angepasstes Windows-PE erstellen lässt. Dabei handelt es sich um ein Mini-Windows für Wartungs- und Reparaturarbeiten, das auf der Datei „boot.wim“ basiert. Standardmäßig bietet Windows-PE keinen Netzwerkzugriff und nur wenige Programme. Mit unserem Beispiel-Script „mk-pe.sh“ aus dem Ordner „winpe“ (*https://m6u.de/depwin*) lässt sich das ändern. Es enthält einen Programmstarter, über den Sie Dateimanager und ein Tool für die Netzwerkkonfiguration starten können. Der Starter lässt sich mit portablen Apps erweitern. Beachten Sie, das sich in einem 64-Bit-PE ausschließlich 64-Bit-Programme ausführen lassen. Das Script erstellt eine ISO-Datei für DVDs, für einen USB-Stick kopieren Sie einfach den Inhalt des Ordners „winpe“ auf ein FAT32-Laufwerk.

„Install.wim“ anpassen: Ein weiteres Beispiel-Script liegt im Ordner „Win11-Bypass“. Es zeigt, wie sich die Windows-ISO-Datei mit 7z entpacken und die enthaltene „Install.wim“ mit wimmountrw in das Dateisystem einhängen lässt. Anschließend wird der Inhalt der Datei „bypass.reg“ mit hivexregedit (Paket „libwin-hivex-perl“) in die Registry importiert, die Einbindung mit wimunmount gelöst und die neue ISO-Datei „Windows_11_bypass.iso“ mit genisoimage erstellt. Die jetzt enthaltenen Registry-Werte ermöglichen die Neuinstallation von Windows 11 auch auf offiziell nicht unterstützter Hardware.

Festplatte statt VHD: Für die Windows-Installation auf einer zweiten Festplatte im PC, einem USB-Stick oder einem USB-Laufwerk ist nur eine Befehlszeile nötig. Starten Sie im Ordner „deploy-windows/deploy-win“

```
sudo -E ./setup_win10.py --efi
 --iso=[Windows-11-ISO] --disk=/
 dev/sd[X] --image-name=5
```

Setzen Sie für den Platzhalter den Pfad und Namen der ISO-Datei ein und hinter „--disk=“ den Gerätepfad zum Ziellaufwerk. Es muss neu partitioniert werden, alle enthalten Dateien gehen verloren.

5. Windows-Backup mit wimcapture

Wer Windows auf dem gleichen PC installiert hat, kann mit wimcapture ein Backup erstellen.

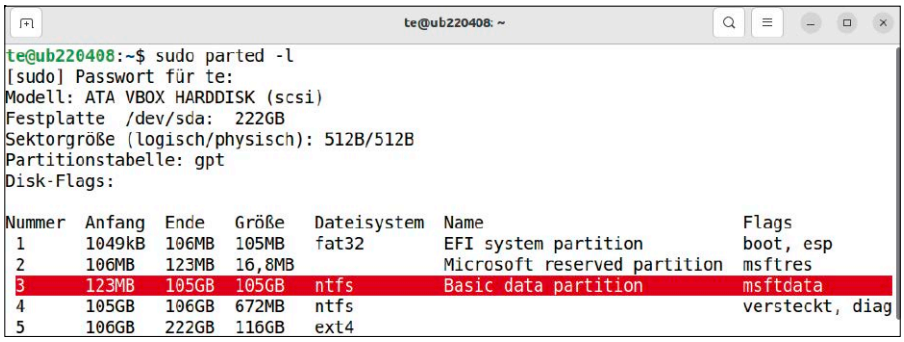
Vorbereitungen: Damit das Backup fehlerfrei gelingt, muss sich das Windows-Dateisystem in einem konsistenten Zustand befinden. Dazu muss Windows ordnungsgemäß beendet worden sein und darf sich

nicht im Ruhezustand befinden. Bei Windows 10/11 verwenden Sie dazu immer „Neu starten“ (nie „Herunterfahren“), bevor Sie ein Linux-System starten.

Im Terminal verschaffen Sie sich mit

```
sudo parted -l
```

einen Überblick über Festplatten und Partitionen. Windows 10 oder 11 sind standardmäßig im Uefi-Modus auf einer GPT-Partition installiert. Parted zeigt hinter „Festplatte“ die Laufwerksbezeichnung an, darunter steht die nummerierte Liste der Partitionen. Die Windows-Partition identifizieren Sie anhand der Größe und der Bezeichnung „Basic data partition“. Das ergibt dann beispielsweise „/dev/sda3“.



Partitionen ermitteln: Der Befehl „sudo parted -l“ zeigt die Partitionen auf der Festplatte an. Nummer „3“ auf „/dev/sda“ ergibt hier den Partitionspfad „/dev/sda3“.

Backup erstellen: Für das Backup verwenden Sie den Befehl wimcapture. Sollte die Windows-Partition gemountet sein, lösen Sie die Laufwerkseinbindung. Im Terminal führen Sie folgenden Befehl aus:

```
sudo wimcapture /dev/sda3 /Backup/
  Win.wim "" "2023-01-01"
```

Ersetzen Sie die Pfadangaben durch die für Ihr System erforderlichen Werte. „/dev/sda3“ ist bei unserem Beispiel die Windows-Partition und „/Backup/Win.wim“ ist das Backupziel. Danach folgen zwei Anführungszeichen für eine leere Bezeichnung sowie ein Datum als Beschreibung, anhand dessen Sie später unterschiedliche Backups auseinanderhalten können.

Inkrementelle WIM-Backups sind besonders platzsparend, weil nur die Änderungen zur ersten Sicherung in der Datei landen. Dafür verwenden Sie die Befehlszeile

```
sudo wimappend /dev/sda3 /Backup/
  Win.wim "" "2023-02-01"
```

Quelle und Ziel sind die gleichen wie bei wimcapture. Das Tool wimappend legt bei jedem Aufruf ein neues Image in der WIM-Datei an, das eine vollständige Wiederherstellung ermöglicht.

Die EFI-Partition ist mit dem Dateisystem FAT32 formatiert. Bei einer Standardinstallation von Linux und Windows auf einer Festplatte gibt es nur eine EFI-Partition, die beide Systeme gemeinsam nutzen. Folgender Befehl

```
sudo tar cvjf efi.tar.bz2 /boot/efi
```

sichert die EFI-Partition.

6. Restore mit wimapply durchführen

Zum Zurücksichern eines Backups verwenden Sie wimapply. Das Tool erwartet als Ziel eine leere Partition. Persönliche Dateien, die sich seit dem letzten Backup geändert haben, müssen Sie vor der Wiederherstellung extra sichern. Oder Sie erstellen zur Sicherheit mit wimcapture ein neues, vollständiges Backup. Sollte die Windows-Partition gemountet sein, lösen Sie die Laufwerkseinbindung. Formatieren Sie zunächst die Windows-Partition (Beispiel):

```
sudo mkfs.ntfs -f /dev/sda3
```

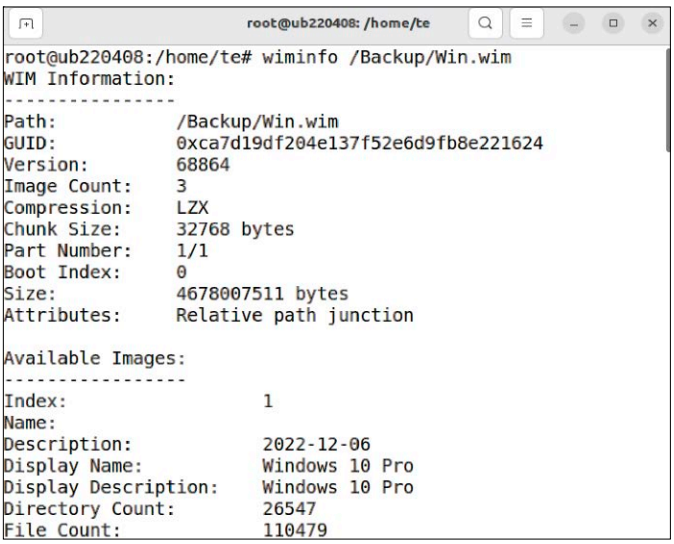
Prüfen Sie die Partitionsangabe genau, damit Sie nicht versehentlich die falsche Partition formatieren. Danach führen Sie folgenden Befehl aus:

```
sudo wimapply /Backup/Win.wim 1 /
  dev/sda3
```

Ersetzen Sie den Pfad zur WIM-Datei und die Gerätebezeichnung durch die für Ihr System gültigen Werte. Die „1“ steht für eine Indexnummer. Sind mehrere Abbilder enthalten, geben Sie die höchste Nummer für das aktuellste Backup an. Die Indexnummern und Beschreibungen lassen sich mittels des Befehls

```
wiminfo /Backup/Win.wim
```

ermitteln.



Index ermitteln: Der Befehl wiminfo liefert die Eigenschaften einer WIM-Datei. Sie erfahren dabei, wie viele Abbilder in der Datei stecken („Image Count“).

Restore auf neue Hardware: Nach Austausch der Festplatte oder für den Umzug auf einen neuen PC verwenden Sie ebenfalls wimapply. Auf einer leeren Festplatte fehlen jedoch die Bootpartition und die Konfiguration. Installieren Sie daher Windows zuerst wie in Punkt 4 beschrieben auf der neuen Festplatte, formatieren Sie die Systempartition neu und entpacken Sie die Sicherung mit wimapply.

Auf der EFI-Partition überschreiben Sie die Dateien mit jenen aus dem Backup (siehe Punkt 5).

Restore in einer VM: Das WIM-Backup lässt sich auch als VHD-Datei wiederherstellen und damit in einer VM nutzen. Als Basis verwenden Sie eine Installation wie in Punkt 3 beschrieben. Das Script „create_vhd_from_Backup.sh“ (*https://m6u.de/depwin*) hängt die Windows-Partition in der VHD-Datei in das Dateisystem ein, formatiert die Partition neu und entpackt das Backup mit wimapply. Passen Sie die Dateinamen und Pfade im Script an, bevor Sie es einsetzen. ■

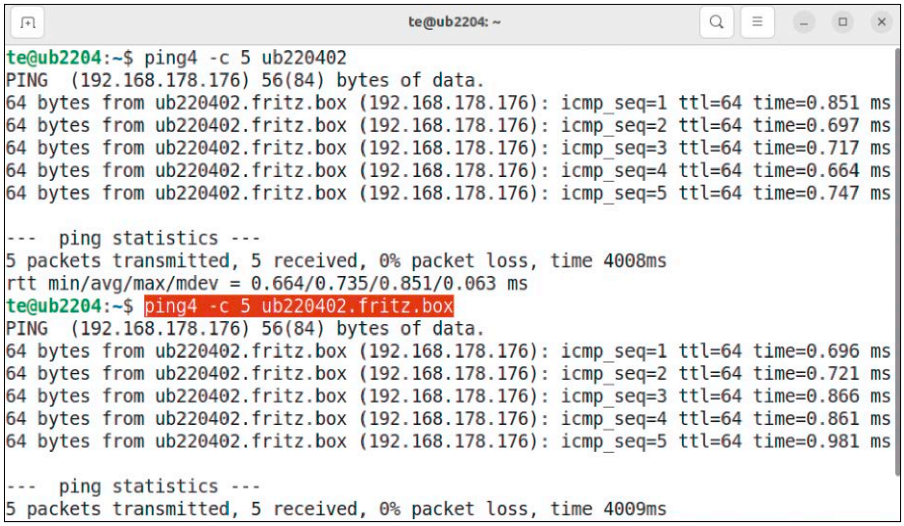
Orientierung im Heimnetzwerk

Linux-Systeme zeigen etwa im Dateimanager standardmäßig kaum oder keine Informationen zu Geräten im Netzwerk. Wer IP-Adressen und Ports beispielsweise für eine Weboberfläche sucht, ist auf andere Tools angewiesen.

VON THORSTEN EGGELING

Auch in kleinen Heimnetzwerk laufen heutzutage zahlreiche Geräte: Router, PCs, Notebooks, TV-Geräte, Smartphones, Tablets und einiges mehr sind miteinander verbunden. Im Vordergrund steht dabei, allen Geräten den Internetzugang zu ermöglichen. Nebenbei können die Geräte auch miteinander kommunizieren oder sie stellen Dienste bereit, etwa für den Austausch von Dateien oder das Multimedia-Streaming.

Falls es Probleme im Netzwerk gibt, sind diese nicht einfach zu untersuchen. Nicht immer ist sofort ersichtlich, welche Geräte Dienste anbieten und wie diese zu erreichen sind. Es ist daher hilfreich herauszufinden, was im Netzwerk läuft und wie die Geräte konfiguriert sind.



Namen im Netzwerk: Mit ping4 lässt sich prüfen, ob ein Rechner über seinen Namen und auch über einen lokalen Domainnamen wie „.fritz.box“ oder „.local“ erreichbar ist.

IP-Adressen, Ports und Protokolle

Jedes Gerät im Netzwerk besitzt eine eindeutige IP-Adresse (siehe Artikel ab Seite 60). Rechner A fordert beispielsweise im lokalen Netz über den Browser eine Webseite von Rechner B an. Der Webserver schickt das Ergebnis an Rechner A beziehungsweise an die IP-Adresse, von der die Anfrage stammt. Bei Internetzugriffen läuft es ähnlich ab. Allerdings sorgt der IP-Filter in der Firewall des Internet/DSL-Routers dafür, dass die IP-Adresse von Rechner A nicht direkt erreichbar ist. Der Router ersetzt per NAT (Network Address Translation) die IP von Rechner A durch die öffentliche IP des Routers, die der Internetanbieter zuweist. Er merkt sich die Herkunft der Anfrage und liefert die Antwort des Webservers an Rechner A im lokalen Netzwerk aus.

Da man sich IP-Adressen eher schlecht merken kann, kommt im lokalen Netzwerk und Internet die Namensauflösung zum Einsatz. Jedes Gerät besitzt einen Namen, den es bei einer DHCP-Abfrage an den Router übermittelt. Es erhält per DHCP seine eigene IP-Adresse und der Router merkt sich den Namen des Gerätes. Statt der IP-Adresse kann man daher den Gerätenamen verwenden und – abhängig vom Modell des Routers – beispielsweise auch „MeinPC.local“ oder „MeinPC.fritz.box“ (Fritzbox). Im Internet erledigen DNS-Server die Namensauflösung. Die Server wissen, dass etwa zu google.de die IP-Adresse 216.58.212.163 gehört, und intern kommunizieren Router, Browser und Webserver über diese IP-Adresse. Im Terminal lässt sich mit `ping4 -c 5 [Gerätename oder Domain]` herausfinden, ob die Namensauflösung funktioniert.

Der Vollständigkeit halber sei erwähnt, dass jedes Gerät in der Regel zwei IP-Adressen erhält – nach den Standards IPv4 und IPv6. IPv6 ist in lokalen Netzwerken jedoch kaum relevant, weshalb wir hier nicht weiter darauf eingehen.

Ports und Protokolle: Ein Gerät kann mit nur einer IP-Adresse mehrere unterschiedliche Serverdienste anbieten. Der jeweilige Server „lauscht“ an einem bestimmten Netzwerkport und nimmt auf diesem Anfragen entgegen. Eine Auswahl gängiger Ports finden Sie in der Tabelle „Wichtige Ports und Protokolle“. Unter Linux findet man die Portdefinitionen mit Kurznamen und teilweise auch mit näherer Beschreibung in der Datei „/etc/services“.

Die Ports bis einschließlich 1023 kann man unter Linux nur mit root-Rechten konfigurieren und man sollte sich an die Standards halten, um Fehlfunktionen zu vermeiden. Port 80 beispielsweise nutzen Webserver (HTTP), Port 22 SSH-Server. Die Ports von 1024 bis 49151 dürfen Benutzer in der Regel auch ohne besondere Rechte verwenden. 49152 bis 65535 sind als dynamische Ports zur freien Verwendung durch Anwendungen gedacht (zu den Standards siehe *https://www.rfc-editor.org/rfc/rfc6335*).

Neben den Ports spielen zwei Protokolle bei der Datenübertragung eine wichtige Rolle: TCP (Transmission Control Protocol) und UDP (User Datagram Protocol). Diese Protokolle legen fest, wie gültige Datenpakete beim Transport strukturiert sein müssen. TCP verwenden beispielsweise Webserver, E-Mail-Programme und SSH-Server. UDP dient in der Regel zur Übertragung kleiner Datenpakete für DHCP, DNS oder ähnliche Dienste. Die Unterscheidung der beiden Protokolle kann für die Konfiguration von Portfreigaben beziehungsweise einer Firewall wichtig sein.

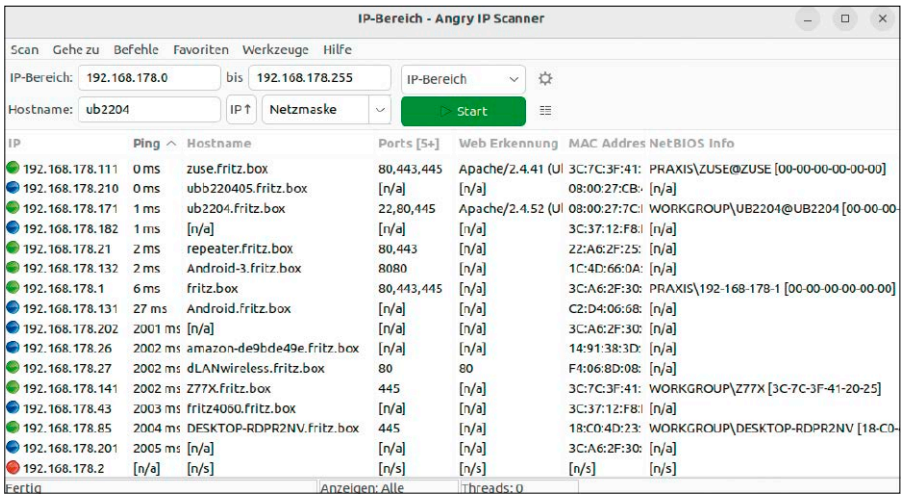
IP-Adressen und Ports

Zuerst ermitteln Sie im Terminal mit

```
ip a
```

den IP-Bereich, den Ihr Netzwerk verwendet (siehe Artikel ab Seite 52). Rufen Sie die Konfigurationsoberfläche des Routers im Browser auf – beispielsweise mit „http://192. 168.178.1“ oder „http://192. 168.0.1“. Bei einer Fritzbox funktioniert auch der Hostname „http://fritz.box“. Router bieten in der Regel eine Funktion, über die sich die aktiven Verbindungen anzeigen lassen. Bei einer Fritzbox gehen Sie auf „Heimnetz → Netzwerk“. Hier sehen Sie allerdings nur die Gerätenamen und IP-Adressen, nicht aber die offenen Ports.

Im Terminal lassen sich die geöffneten Ports mit nmap ermitteln (siehe Artikel ab Seite 60). Wer eine grafische Oberfläche bevorzugt, verwendet Angry IP Scanner (*https://angryip.org*). Im Downloadbereich finden Sie unter „Linux“ DEB-Pakete für Ubuntu und Linux Mint. Im gestarteten Programm geben Sie den IP-Bereich an und gehen auf „Werkzeuge → Einstellungen“. Auf der Registerkarte „Ports“ legen Sie fest, welche Ports das Tool untersuchen soll, beispielsweise „22,80,443,445,8000-8100“. Speichern Sie die Konfiguration per Klick auf „OK“, danach klicken Sie auf „Start“. Klicken Sie auf „Ping“ und dann auf „Sortiere nach Ping“. Die Tabelle zeigt jetzt die aktiven Geräte zuerst an.



IP-Bereich prüfen: Angry IP Scanner ermittelt, welche Geräte im Netzwerk aktiv und welche Ports geöffnet sind. Welche Ports das Tool prüfen soll, lässt sich einstellen.

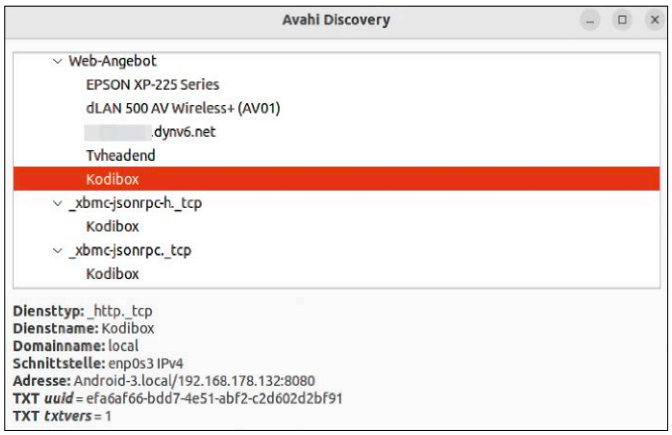
Dienstankündigungen im Netzwerk untersuchen

Nach einigen Diensten muss man im Netz nicht suchen, sie machen sich selbst bekannt. Linux nutzt dafür Avahi, das bei den meisten Distributionen standardmäßig installiert ist. Avahi ist kompatibel mit Bonjour (Mac-OS) und auch unter dem Namen Zeroconf bekannt. Über diese Technik senden Netzwerkdienste und auch viele Geräte wie Drucker, Multimedia-Abspieler, Router und Powerline-Adapter Informationen zur Konfiguration in das Netzwerk.

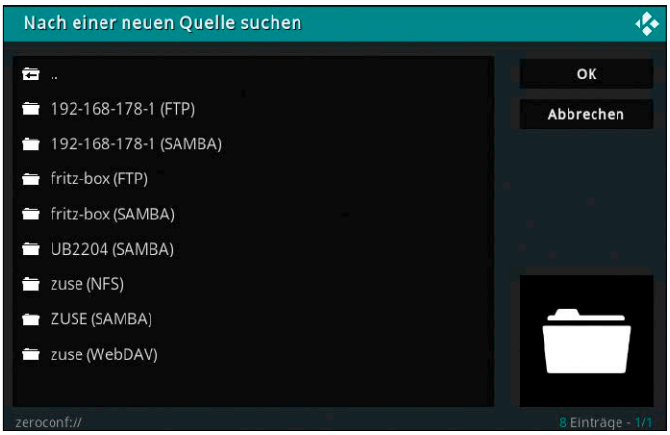
Standardmäßig nutzt Linux Avahi nur rudimentär. Der Ubuntu-Dateimanager beispielsweise zeigt unter „Andere Orte“ Samba-Freigaben anderer Linux-Rechner an. Heimnetzfreigaben (SMB und FTP) einer Fritzbox tauchen ebenfalls auf. Avahi wird außerdem bei der automatischen Erkennung und Konfiguration von Netzwerkdruckern genutzt.

WICHTIGE PORTS UND PROTOKOLLE (AUSWAHL)

Port	TCP	UDP	Beschreibung
7	TCP	UDP	Echo, für Ping-Abfragen
20	TCP	UDP	FTP, Dateitransfer
22	TCP	UDP	SSH, Fernzugriff
23	TCP	–	Telnet, Fernzugriff
25	TCP	–	SMTP, E-Mail senden
80	–	–	HTTP, Webserver
110	TCP	–	POP3, E-Mail empfangen
115	TCP	–	SFTP, Dateitransfer
137–139	TCP	UDP	Microsoft Netbios (für SMB)
143	TCP	UDP	IMAP, E-Mail empfangen
443	TCP	–	HTTPS, Webserver SSL
445	TCP	–	SMB, Dateitransfer
587	TCP	–	SMTP, E-Mail senden
993	TCP	–	IMAPS, E-Mail empfangen SSL
995	TCP	–	POP3S, E-Mail empfangen SSL
5353	–	UDP	Multicast DNS (mDNS, Zeroconf, Bonjour)
8000–8999	TCP	UDP	Alternative HTTP-Ports
49152–65535	TCP (teilweise)	UDP	Dynamische Portbereiche



Einige, aber nicht alle Dienste melden sich hier: Avahi Discover zeigt Server an, die ihr Angebot im Netzwerk bekannt geben. Die Information enthält Name, IP-Adresse und Port des Dienstes.



Medienquellen in Kodi finden: Der „Zeroconf-Browser“ zeigt beispielsweise Samba-, NFS- und FTP-Freigaben an. Für die direkte Einbindung muss aber ein Zugang ohne Anmeldung möglich sein.

Avahi kommt auch bei einigen Anwendungen zum Einsatz. In der Oberfläche des Mediencenters Kodi (Konfiguration siehe *https://www.pcwelt.de/article/1152089*) kann man beim Hinzufügen von Medienquellen auf die Option „Zeroconf-Browser“ gehen und dann den Server wählen. Dabei gibt es jedoch eine Einschränkung. Solcher Zugriff kann nur funktionieren, wenn der betreffende Server keine Anmeldung benötigt. Deshalb ist beispielsweise NFS (Network File System) besonders gut geeignet. Einen Artikel zur Konfiguration eines NFS-Servers finden Sie unter *https://www.pcwelt.de/article/1153455*. Eine FTP-Freigabe etwa von einer Fritzbox gibt man alternativ über „Netzwerkfreigaben hinzufügen“ an. Dabei kann man Benutzernamen und Passwort eintragen.

Avahi-Ankündigungen finden: Eine Übersicht der Server, die sich bei Avahi melden, liefert das nützliche Tool avahi-discover, das Sie über das gleichnamige Paket installieren. Die Baumansicht zeigt die angebotenen Diensttypen und Dienstnamen. Samba-Freigaben sind unter „Microsoft Windows Network“ zu finden und Drucker unter „UNIX Printer“.

Im Abschnitt „Web-Angebot“ sind die Geräte enthalten, die eine Weboberfläche anbieten. Ein Klick auf den Dienstnamen zeigt die Details. Hinter „Adresse“ stehen die IP-Nummer und der Port.

Diese Informationen sind hilfreich, etwa wenn Dienste nicht für den Standard-HTTP-Port 80 konfiguriert sind. Vollständig ist die Liste jedoch nicht. Eine Fritzbox beispielsweise gibt ihre Konfigurationsoberfläche nicht über Avahi bekannt.

Avahi für weitere Dienste nutzen

Avahi wird automatisch für Samba-Freigaben verwendet, wenn der Samba-Server installiert ist (siehe Artikel ab Seite 56). Eine zusätzliche Konfiguration ist nicht erforderlich. Für die Netzwerkprotokolle NFS, Webdav oder SFTP kann man Konfigurationsdateien im Ordner „/etc/avahi/services“ ablegen. Eine Beispieldatei „sftp-ssh.service“ für SFTP/SSH finden Sie im Ordner „/usr/share/doc/avahi-daemon/examples“ und eine Konfigurationsdatei für NFS können Sie über *https://m6u.de/AVAS* abrufen. Sobald Sie die Datei speichern, taucht auf anderen Linux-PCs im Dateimanager unter „Andere Orte“ (Ubuntu) oder „Netzwerk“ (Linux Mint) ein neuer Eintrag auf, beispielsweise „[Rechnername] (SSH/SFTP)“.

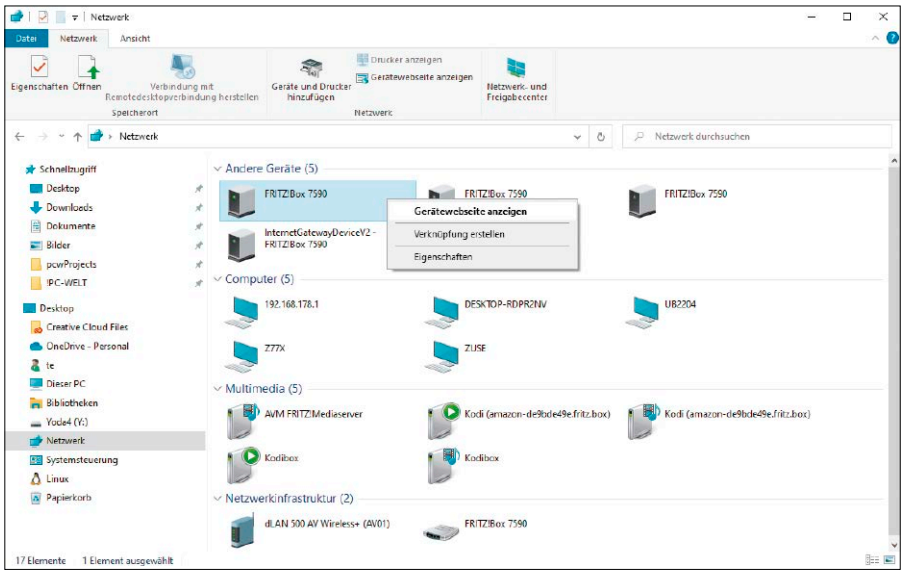
Die Sichtbarkeit von Samba-Freigaben

Windows verwendet für die Suche nach Netzwerkressourcen WS-Discovery (Web Services Dynamic Discovery) statt Avahi. Der Windows-Explorer zeigt unter „Netzwerk“ Dateifreigaben, Drucker, Geräte mit Weboberflächen oder Multimedia-Geräte an. Samba-Freigaben fehlen, weil Linux WS-Discovery bisher standardmäßig nicht unterstützt. Durch manuelle Eingaben gelingt der Zugriff unter beiden Systemen trotzdem (siehe Artikel ab Seite 56).

Komfortabler ist es jedoch, WS-Discovery in Linux nachzurüsten. Ab Ubuntu 22.04 oder Linux Mint 21 lässt sich der Dienst mit

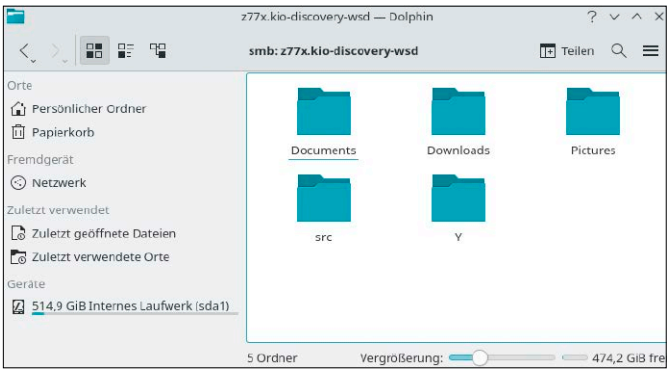
```
sudo apt install wsdd
```

installieren. Nutzer älterer Systeme instal-



Gesprächigeres Windows: Der Windows-Explorer zeigt fast den gesamten Gerätepark im Netzwerk an. Über das Kontextmenü gelangt man – wenn vorhanden – zur Gerätewebseite.

lieren wsdd manuell (*https://github.com/christgau/wsdd*). Der Dienst wird automatisch gestartet und dann tauchen Linux-Freigaben sofort im Windows-Explorer auf.
Hinweis: Es gibt einen ähnlichen Dienst mit dem Namen wsdd2, der sich aber nur für das smb3-Server-Modul eignet, das seit Kernel 5.15 verfügbar ist. Mehr Infos dazu finden Sie über *https://m6u.de/BMKE*.
Windows-Freigaben unter Linux sehen: Es gibt erste Ansätze, zumindest die KDE-Oberfläche mit WS-Discovery bekannt zu machen. Die nötige Erweiterung für den KDE-Dateimanager Dolphin ist in Kubuntu 22.04 und 22.10 enthalten, funktioniert jedoch sehr unzuverlässig. Besser sieht es bei KDE Neon aus (*https://neon.kde.org*), das zwar auf Ubuntu 22.04 basiert, aber eine neuere KDE-Version mitbringt. In Dolphin klickt man auf „Freigegebene Ordner (SMB)“ und sieht alle Windows- und Linux-Rechner mit SMB-Freigaben. Beim Klick auf eine Windows-Freigabe verwendet der Dateimanager den Pfad „smb://[Server].kio-discovery-wsd/“ und die freigegebenen Ordner erscheinen. Es ist bisher nicht bekannt, wann diese Funktion in die Dateimanager von Gnome oder Cinnamon eingebaut wird.
Tipp: Damit Dolphin auch Netzwerkressourcen wie FTP-, SFTP- oder NFS-Server anzeigt, installieren Sie das Paket „kde-zeroconf“. Sie erreichen die Dienste dann im Dateimanager per Klick auf „Netzwerkdienste“.

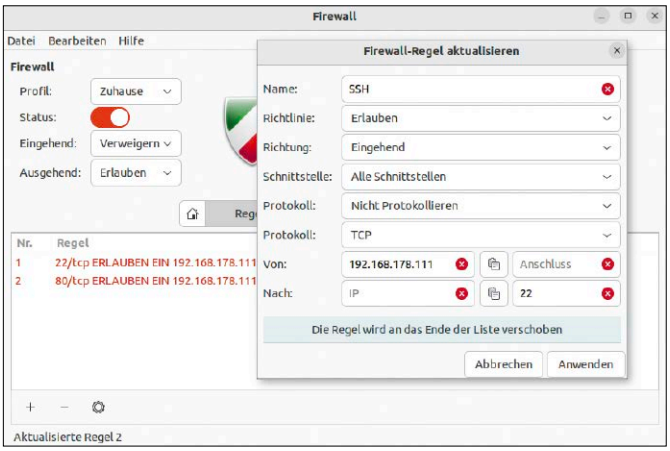


Windows-Freigaben in Dolphin: Die neueste Version des KDE-Dateimanagers beherrscht WS-Discovery und kann daher Windows-Server und deren Freigaben anzeigen.

Schutz durch die Firewall konfigurieren

Bei Ubuntu und Linux Mint ist die Firewallsoftware ufw standardmäßig installiert, allerdings nicht aktiv. Im privaten Netzwerk ist eine Firewall in der Tat überflüssig, weil der Internetrouter die Geräte im Netzwerk bereits vor Zugriffen aus dem Internet schützt. Ein Motiv, die Firewall trotzdem zu aktivieren, ist die potenzielle Gefährdung durch andere Rechner im Netzwerk – insbesondere, wenn diese unter Windows laufen. Auf einem Notebook, das man auch in fremden Netzen verwendet, sollte man die Firewall daher aktivieren. Das gilt jedoch nur, wenn Serverdienste auf dem Rechner laufen. Andernfalls sind keine Ports geöffnet und ein Angriff ist unmöglich. Eine Firewall bietet jedoch keinen Schutz vor böswilligen Websites oder virenverseuchten Downloads. Davon sind Linux-Systeme aber weit weniger betroffen als Windows.

Firewall mit Profilen: Eine aktivierte Firewall birgt immer die Gefahr, dass der Zugriff auf Dienste ungewollt verhindert wird. Die ufw-Konfiguration ist jedoch recht übersichtlich und bei Problemen kann man die Firewall jederzeit wieder ausschalten. Für die komfortable Konfiguration installieren Sie das Tool gufw („Firewall-Konfiguration“) über das gleichnamige Paket. Es bietet die drei Profile „Büro“, „Öffentlich“ und „Zuhause“, zwischen denen Sie je nach Aufenthaltsort umschalten. Wenn Sie „Büro“ oder „Öffentlich“ wählen, wird die Firewall aktiviert, was an der Stellung des Schalters hinter „Status“ zu erkennen ist. Die Einstellung bleibt auch nach einem Neustart erhalten. Bei aktivierter Firewall werden die Zugriffe auf alle Ports blockiert. Der Unterschied zwischen diesen beiden Profilen ist die Einstellung hinter „Eingehend“. „Ablehnen“ bei „Öffentlich“ verweigert den Zugriff ohne Rückmeldung an das aufrufende Programm. Es scheint dann so, als ob beispielsweise kein Webserver läuft, und die Verbindung wird sofort abgebrochen. „Verweigern“ hat eine ähnliche Wirkung, informiert den Client aber darüber, dass keine Verbindung möglich ist. In der Praxis führt das dazu, dass etwa ein Webbrowser länger benötigt, bis er Verbindungsversuche wegen Zeitüberschreitung abbricht.
Spezialkonfiguration für das Heimnetz: Im heimischen Netzwerk setzen Sie das Profil auf „Zuhause“. Die Firewall wird deaktiviert und Netzwerkgeräte können auf alle Serverdienste zugreifen. Wer eine erhöhte Sicherheit benötigt, kann die Firewall auch im Heimnetz aktivieren und beispielsweise den Zugriff auf den SSH-Server auf bestimmte IP-Adressen beschränken. Klicken Sie auf die „+“-Schaltfläche und gehen Sie auf „Erweitert“. Tragen Sie einen Namen ein, beispielsweise „SSH“. Hinter „Protokoll:“ wählen Sie „TCP“ und hinter „Von:“ geben Sie die IP-Adresse des berechtigten Rechners ein. Die Portnummer dahinter lassen Sie leer. In die Zeile „Nach:“ tragen Sie keine IP-Adresse, aber den Port „22“ ein und per Klick auf „Anwenden“ fügen Sie die Regel hinzu.
Entsprechend definieren Sie weitere Portregeln für diese oder andere IP-Adressen. Bitte beachten Sie, dass die Firewall erst einmal alle eingehenden Anfragen blockiert. Sie müssen daher für jeden Port eine Regel erstellen, den der PC im Netzwerk anbieten soll. ■



Extremschutz: In der Firewall lässt sich für das lokale Netzwerk konfigurieren, dass beispielsweise nur einer einzigen IP-Adresse der Zugang zu einem SSH-Server erlaubt ist.

Netzwerkhardware: Ausbau & Optimierung

Für Heimnetze genügt es oft, die Fähigkeiten des Routers konsequent zu nutzen und die Endgeräte an optimaler Stelle zu betreiben – verkabelt oder via Funknetz. Letzteres geht nicht? Auch kein Problem: Ethernet und WLAN lassen sich verlängern.

VON HERMANN APFELBÖCK

Dieser Beitrag zeigt den Umgang mit der wichtigsten Netzwerkhardware und Optionen des Netzwerkausbaus. Dabei geht es ausschließlich um das lokale Netz in den eigenen vier Wänden mit seinen typischen Geräten. Ein Großteil dieser Infos gilt betriebssystemunabhängig: Für Router, Switch, Access Point, Repeater, Powerline spielt das System der Endgeräts keine Rolle.

Der Heimrouter

Moderne Router vereinen eine Reihe von Hardwarefunktionen – Switch für (meist) vier Ethernet-Anschlüsse, Funknetz, DECT-Telefonie, NAS, Verbindung zum öffentlichen WAN. Alle Funktionen lassen sich in der Konfigurationsoberfläche über jeden Browser steuern. Hardwaretechnisch unerlässlich ist

- das Aktivieren und Einrichten des Funknetzes (Fritzbox: „WLAN → Funknetz“, Passwort unter „WLAN → Sicherheit“)
- das Festlegen der Ethernet-Leistung (Fritzbox: „Heimnetz → Heimnetzübersicht → Netzwerkeinstellungen“).

Router wie die Fritzbox sind im Browser über Standard-Hostnamen wie „fritz.box“ erreichbar, in jedem Fall aber mit der lokalen IP-Adresse. Die IP lautet oft „192.168.178.1“ oder „192.168.0.1“. Die Router-IP ermitteln Sie bei Bedarf mit

```
ip a
```

und ersetzen im letzten Block der IPv4-Adresse die angezeigte Ziffer (die IP des aktuellen Geräts) durch die „1“.

Um im allerersten Schritt an die Konfigurationsoberfläche heranzukommen, muss ein Gerät im Netz angemeldet sein. Dazu genügt ein mit Ethernet-Kabel verbundener PC mit einem beliebigen Betriebssystem.

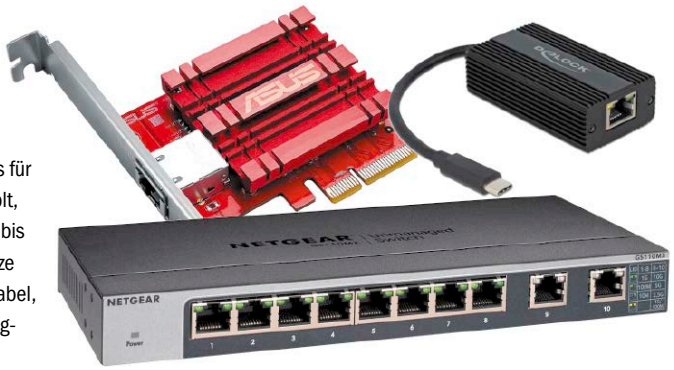
Aufgrund der zentralen Rolle wäre es optimal, wenn der Router auch einen zentralen Standort einnimmt. Je mehr Geräte Sie an den vier Ethernet-Ports in unmittelbarer Nähe nutzen können, desto besser. Das gilt ganz besonders für Geräte, die viel Datentransfer zu leisten haben, etwa Highspeed-Downloads oder Backups. Geräte mit Serverfunktion sind ebenfalls für schnelle Kabelverbindung prädestiniert, NAS bieten in der Regel gar kein Funknetz. Die oft unbefriedigende Netztauglichkeit von TV-Geräten lässt durch HDMI-Anschluss eines PCs oder eines Raspberry Pi vollständig kompensieren, der wiederum per Ethernet am Router hängt.

Für die optimale Reichweite des Funknetzes wäre eine zentrale Lage ebenfalls wünschenswert. Tatsache ist aber, dass Router oft ungünstig stehen, erzwungen durch die Nähe zum DSL- oder Kabelanschluss.

Ethernet: Das Kabelnetzwerk

Kabelgebundene Ethernet-Verbindungen sind schnell und unbeeinflusst von äußeren Störungen. PCs, Notebooks und Smart-TVs sind standardmäßig mit einer RJ-45-Buchse für Ethernet-Kabel ausgerüstet – in der Regel ein Gigabit-Ethernet-Adapter. Über Gigabit-Ethernet (1000 MBit/s) lassen sich theoretisch 125 MB/s übertragen. Nach Abzug der Verwaltungsdaten sollten rund 100 MB/s bleiben. Wenn das Tempo nicht erreicht wird, muss das aber nicht am Netzwerk liegen: Mechanische Festplatten,

Viele Ethernet-Ports für volles Tempo: Alle Endgeräte am Switch unterhalten sich unabhängig von der sonstigen Netzleistung mit Gigabit-Tempo.



10-GB-Netzadapter gibt es für PCIe-Ports oder Thunderbolt, 10-GB-Switches mit Ports bis zu 10 GBit/s. Für Heimnetze ist das noch kaum praktikabel, weil die Datenträger zu langsam sind.

insbesondere an USB, können das Netztempo ausbremsen, vor allem wenn viele kleine Dateien zu übertragen sind.

Fast Ethernet (100 MBit/s) ist obsolet, zumal es heutzutage sogar die WAN-Bandbreite aus dem Internet unterschreiten kann. Router und Switches mit Fast Ethernet sollten ersetzt werden. Ältere Rechner ohne Serveraufgaben können mit dem langsamen 100-MBit-Adapter aber natürlich weiterhin mitspielen.

Kabelausbau: Ein Ausbau der Ethernet-Verkabelung über den zentralen Router hinaus ist kostengünstig, aber aufwendig. Für Gigabit-Ethernet sind Cat-5e-Kabel zu empfehlen, die aber oft irreführend als „Cat 5" bezeichnet werden. Wer zukunftssichere Kabel verlegen möchten, greift zu Cat-6- oder Cat-7-Kabeln. Um Kabel in weitere Räume zu bringen, genügen 8-mm-Bohrer. Den weiteren Aufwand beim Abisolieren der Kabel und Crimpen der RJ-45-Stecker kann man sich dadurch ersparen, dass man Stecker wie Telegärtner J00026A2001 (*http://amzn.to/2pRA2jo*, circa 13 Euro) verwendet, die sich werkzeuglos an das Cat-Kabel anschließen lassen. Ohne Bastelei geht es aber auch hier nicht. Außerdem sind die Stecker etwas größer und finden in einem Switch nicht direkt nebeneinander Platz.

Ein für Privathaushalte relevantes Längenlimit für Ethernetkabel gibt es nicht: Bis zu 100 Meter bleiben verlustfrei, für noch längere Strecken müsste dann ein zwischengeschalteter Switch das Signal auffrischen.

Switch: Ethernet-Switches sind intelligenter Verteiler, die Datenpakete nur an das Gerät leiten, für das sie bestimmt sind. Externe Gigabit-Switches etwa von Netgear ermöglichen daher Gigabit-Tempo zwischen den direkt angeschlossenen Geräten. Dabei spielt es keine Rolle, mit welchem Tempo die Daten vom Router zum Switch gelangen. In einem Raum mit eventuell mäßiger WLAN- oder Powerline-Abdeckung kommunizieren dann immerhin alle Endgeräte hinter dem Switch mit Gigabit-Tempo. Kleinere Switches haben meistens fünf oder acht Ports und kosten etwa 25 bis 40 Euro. An welchen Port Sie welches Gerät anschließen, spielt keine Rolle.

10-GBit-Netzwerk: Gigabit-Ethernet dürfte im Heimnetz noch viele Jahre Standard bleiben, wenngleich längst 10 GBit/s verfügbar ist. Das liegt nicht nur daran, dass eine PCIe-Karte wie Asus 10Gbase-T XG-C100C aktuell knapp 100 Euro kostet. Entscheidender sind die notwendigen Aufrüstmaßnahmen mit erheblichen Folgekosten. Mit Festplatten und SSDs an SATA-Ports, USB 3.0/3.1 ist nämlich keine Verbesserung zu erzielen. Alle beteiligten Endgeräte müssten PCIe-SSDs, USB 3.2 oder Thunderbolt 3 verwenden, um vom 10-GBit-Netzwerk zu profitieren.

BREITBANDHARDWARE INS WAN

Auf die Hardware, die Ihr Internetprovider bereitstellt, haben Sie nur insofern Einfluss, als Sie im besten Fall zwischen verfügbaren Techniken und Breitbandverträgen das Geeignete auswählen. Ob tatsächlich eine offene Auswahl besteht zwischen einem DSL mit sechs bis 16 MBit/s, VDSL mit 100 bis 250 MBit/s, Kabel mit 100 bis 1000 MBit/s oder Glasfaser mit derzeit 300 bis 1000 MBit/s, ist regional höchst unterschiedlich. Während Telekom & Co. derzeit in Großstadtregionen (wo Kunden mit VDSL oder Kabel und 100- bis 500-MBit-Verbindungen null Leidensdruck haben) mit Glasfaserangeboten hausieren, bleiben die Kunden am Land auf Sechs-MBit-DSL sitzen.

Wie viel MBit/s braucht man wofür? Die Breitbandwährung MBit/s ist eine unhandliche Größe, die Sie am besten grob durch zehn teilen, um den MB-Durchsatz zu schätzen: Mit sechs MBit/s, also weniger als ein MB pro Sekunde, funktionieren Mail, soziale Netzwerke und HTML-Surfen in leidlicher Geschwindigkeit. 16 MBit/s ermöglichen Surfen, Softwaredownloads und Videostreaming mit erheblichen Qualitätsabstrichen. Ab 50 MBit/s sind auch größere Downloads wie Linux-ISO-Images keine Geduldsprobe und Streamen hoher Qualität wird störungsfrei. 100 MBit/s, also 10 bis 12 MB pro Sekunde, sollten auch Intensivnutzern und Downloadjunkies genügen, wobei dies mit den Personen im Haushalt oder Betrieb zu multiplizieren ist: Für mehrere Intensivnutzer in einem Haushalt sind 250- oder 500-MBit-Verträge nicht mehr abwegig.

Diese Anmerkungen zur Breitbandverbindung ins öffentliche WAN (Wide Area Network) sind auch für das lokale LAN (Local Area Network) und dessen Ausbau relevant. Je größer die Bandbreite aus dem Internet, desto wichtiger wird ein schnelles lokales Netz: Nichts ist ärgerlicher als eine 500-MBit-Verbindung ins Internet, von der am Endgerät nur ein Bruchteil ankommt, weil das lokale Netz schwächelt. Gründe für ein schnelles Heimnetz gibt es aber natürlich in Menge auch bei dünner DSL-Verbindung nach draußen: Das Backup vom PC zum NAS oder Platinenserver soll möglichst schnell durchlaufen, das Tablet soll Filme vom lokalen Server störungslos wiedergeben und die Remotedesktop-Verbindung ist am angenehmsten mit 32-Bit-Farben.

Powerline-Adapter: Diese Methode der Netzerweiterung ist solide, aber selten der versprochene Ferrari. Die „Pass-Thru"-Steckdose sorgt dafür, dass kein Stromanschluss verloren geht.

Powerline: Die Ethernet-Brücke

Wo direkte Verkabelung zu mühsam erscheint, ist eine Brücke über das Stromnetz eine echte Alternative. Powerline (auch Power LAN oder DLAN) ist eine Kabelvernetzung, die für die Hauptdistanz die Stromleitung nutzt, die kurzen Restwege übernehmen dann wieder Ethernet-Kabel. Für die angeschlossenen Endgeräte – egal ob Linux, Windows oder Mac-OS – handelt es sich um eine Ethernet-Verbindung. Die Adapter haben mindestens einen und bis zu drei Ethernet-Anschlüsse (es gibt auch Modelle mit zusätzlichem WLAN).

Im Handel finden Sie Adapter von AVM, Devolo oder Netgear. Abgesehen von der jüngeren Magic-Generation bei Devolo entsprechen die Adapter dem Homeplug-Standard: Sie funktionieren also auch mit älteren Homeplug-Adaptern. Geräte mit unterschiedlicher Übertragungsleistung lassen sich kombinieren, erreichen dann aber natürlich nur die Bandbreite des schwächsten Glieds.

Powerline benötigt mindestens zwei Adapter. Starterkits mit zwei Geräten kosten je nach Leistung etwa 100 bis 200 Euro. Ein Adapter kommt in eine Steckdose in der Nähe des Routers und wird per Ethernet-Kabel mit diesem verbunden. Den zweiten (dritten …) Adapter bringen Sie in der Nähe des Endgerätes unter und verbinden ihn über ein Ethernet-Kabel mit PC oder Notebook.

Vor der Erstbenutzung verbinden sich die zwei Adapter durch Drücken des Verschlüsselungsknopfes am Gehäuse, ein späterer Ausbau ist beim Hersteller Devolo auch durch die Cockpit-Software und manuelle Eingabe der Geräte-ID möglich.

Software für Devolo-Powerline: Das Tool ist ganz nützlich, da es Adapter ein- und ausschalten kann. Außerdem führt es zur Konfigurationsoberfläche des Geräts – falls eine existiert.

Powerline: Optimierungen

Powerline-Verbindungen sind sicher und relativ schnell – in der Regel jedem WLAN-Ausbau überlegen. Sie erreichen aber nicht annähernd den theoretischen Durchsatz von 500, 1200 oder gar 2400 MBit/s (Devolo Magic). Im Bestfall und bei kürzeren Distanzen erreichen die Adapter 40 Prozent der theoretischen Bruttoleistung, in ungünstigen Fällen aber auch nur 20 Prozent. Die von Herstellern angegebene Maximaldistanz von 300 Metern ist pure Theorie: Brauchbare Leistungen sind nur bei kurzen Strecken zu erwarten (10 bis 50 Meter).

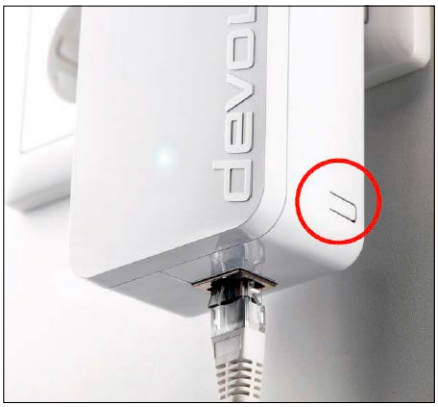
Neben der Distanz der Adapter und der Qualität der Stromleitung können andere Stromverbraucher im Haushalt den Durchsatz beeinträchtigen. Auch die Wahl der Steckdose ist kritisch: Im gleichen Raum können unterschiedliche Steckdosen Unterschiede bis zu 300 Prozent erzielen!

Die Adapter sollten immer direkt in die Wandsteckdose und niemals in Steckerleiste. Immer zu empfehlen sind daher die etwas teureren Adapter mit integrierter Steckdose („Pass-Thru"): Die Steckdose kann dann für andere Stromverbraucher oder für eine Steckerleiste genutzt werden. Ganz sorgenfrei ist das dennoch nicht, denn damit erschweren Sie sich die ganz einfache Troubleshooting-Maßnahme, einen DLAN-Adapter ein- und wieder auszustecken, falls dieser mal rot blinkt und die Arbeit verweigert.

Mit der Software Devolo Cockpit (*www.devolo.de/service/downloads*, auch für Linux) lassen sich Devolo-Adapter konfigurieren und ein- und ausschalten, was in Problemfällen die Störung fast immer behebt. Für den eigentlichen Betrieb der Adapter ist die Software nicht erforderlich.

WLAN: Das Funknetzwerk

Wireless LAN ist eine bequeme und kostengünstige Vernetzungstechnik – keine Kabel, geringer Arbeitsaufwand und alle Netzwerkgeräte bleiben mobil. Ein WLAN-Access-Point ist bereits im Router enthalten. Das Funknetz muss also nur aktiviert und mit Kennwort versehen werden. Notebooks, Tablets und Smartphones besitzen standardmäßig einen WLAN-Chip, PCs können am USB-Port nachgerüstet werden.



Powerline-Adapter einrichten: Durch zeitnahes Drücken der Verschlüsselungstaste am Gehäuse zweier Devolo-Adapter verbinden sich die Geräte.

WLAN-Geräte werden mit hohen Transferraten beworben. Beim derzeit noch meistverbreiteten Standard 802.11ac (Wi-Fi 5) gelten 1300 MBit/s als theoretisches Maximum, bei 802.11ax (Wi-Fi 6) sogar 9600 MBit/s. Reichweite und Geschwindigkeit einen WLANs hängen aber erheblich von Distanz, baulichen Gegebenheiten und weiteren Störeinflüssen ab. Bei Stahlbetonwänden und Ziegelmauern mit Feuchtigkeit reicht das Signal eventuell kaum in den nächsten Raum. Viele Funknetze der Nachbarschaft und andere elektrische Geräte verschlechtern die Signalqualität zusätzlich. Wenn das Funksignal für wichtige Räume nicht ausreicht, sind die typischen Optimierungstipps selten zielführend: Optimale Frequenz- und Kanalwahl erledigen moderne Router mit automatischen Einstellungen und ein Ortwechsel des Router scheitert in der Regel an den Gegebenheiten. Ohne zusätzliche Hardware sind

Repeater holen das Funknetz ein Stück näher an den Arbeitsplatz. Erwartungsgemäß reibungslos verstehen sich Fritz-Repeater mit Fritzbox-Routern.

Powerline-Wi-Fi-Adapter liefern das WLAN an jede Steckdose und jeden Ort (Basisadapter am Router vorausgesetzt). Klassische Access Points sind meistens noch leistungsstärker.

Access Point und seine Konfigurationsoberfläche: Ethernet-Kabel in die Buchse und in der Konfiguration ein neues WLAN anlegen – schon funkt das Gerät an gewünschter Stelle.

WLAN-Reichweitenprobleme nicht nachhaltig zu beheben (siehe unten). Im Zweifel über WLAN-Signalstärken gibt es diverse objektive Testmöglichkeiten. Fritzbox-Besitzer greifen am besten zur Android- und iOS-App „Fritz!App WLAN“.

WLAN-Optimierungen

WLAN-Repeater sind Signalverstärker der WLAN-Basisstation. Sie sollten in eine Wandsteckdose angesteckt werden, wo das Signal der Basisstation noch einigermaßen zu empfangen ist. Die Mitte zwischen Basisstation und Endgerät ist ein oft genannter Pauschaltipp, ein Platz nahe am Endgerät kann aber durchaus bessere Resultate liefern. Die Ersteinrichtung erfolgt entweder über die WPS-Taste an Router und Repeater oder manuell über die Repeater-IP-Adresse (die im Router zu ermitteln ist).

Ein Repeater kann den Datendurchsatz durchaus verdoppeln. Die unterschiedlichen Preise zwischen 30 und 120 Euro rechtfertigen sich durch theoretische Sendeleistungen von 300 bis 1700 MBit/s, durch Dualband-Fähigkeit (2,4 und fünf GHz) und Funktionen wie zusätzliche Ethernet-Anschlüsse. Da Repeater aber eher eine Notlösung bleiben, sind hochpreisige Repeater aber selten sinnvoll.

Powerline-Wi-Fi-Adapter: Powerline-Adapter können auch das Funknetz ausbauen, indem der entfernte Adapter (bei den Endgeräten) per Wi-Fi weiterfunkt. Devolo, AVM und andere bieten Powerline-Starterkits mit Basisadapter und Wi-Fi-Adapter ab etwa 90 Euro. Wenn bereits eine Powerline-Basis vorliegt, gibt es Wi-Fi-Erweiterungsadapter auch solo für etwa 50 Euro. Im Prinzip sind solche Lösungen nichts anderes als Access Points mit vergleichbaren Funktionen (Gastnetz, Kindersicherung, Zeitschaltung), die sich über eine Konfigurationsoberfläche steuern lassen.

Access Point: Wenn das Funknetz einen wichtigen Raum nicht abdeckt, dort aber Ethernet-Kabel oder Powerline vorliegt, kann ein Access Point die Mobilgeräte an dieser Stelle versorgen. Das Gerät muss im Prinzip nur mit einem Ethernet-Kabel verbunden werden. Detaillierte Einstellungen erlaubt eine Konfigurationsoberfläche für den Browser, notwendig sind nur Funknetzname (SSID) und Kennwort. Access Points sind in der Regel die schnelleren Geräte gegenüber Repeater und Powerline-Wi-Fi. Die deutlichen Preisunterschiede von 25 bis 150 Euro rechtfertigen sich durch die Wi-Fi-Version, wobei aber günstige Geräte mit Wi-Fi 5 (802.11ac) für einen Raum ausreichen können.

Oft genügt auch ein alter Router für diese Rolle, nachdem dort die Rolle als DHCP-Server (Verteilung von IP-Adressen) deaktiviert ist und auch sonst am besten alles außer WLAN. Im Übrigen verfahren Sie wie bei einem Access Point, definieren also SSID und Zugangskennwort.

Netzwerkadapter am Endgerät

Smartphone, Tablets und Notebooks besitzen standardmäßig einen WLAN-Chip, bei PCs und NAS-Geräten ist ein Gigabit-Ethernet-Port Standard. Wenn ein Netzadapter fehlt (eventuell auch ein zweiter für ein zweites Netzwerk), ist PCs, Notebooks, NAS- und Platinenrechnern leicht abzuhelfen. Fehlendes Ethernet können Ethernet-Adapter am USB-Port ergänzen. Das Zubehör sollte wie der Delock USB-Ethernet-Adapter (Delock 62121, ab 30 Euro, *https://tinyurl.com/25mzrwtu*) USB 3.x und Gigabit-Ethernet leisten. Billigere USB-Adapter bieten oft nur Fast Ethernet und/oder USB 2.0.

Ein fehlender WLAN-Chip bei PCs ist ebenfalls über USB zu kompensieren. Preisgünstige WLAN-Sticks für 10 bis 20 Euro gibt es zuhauf, sie sind aber nicht alle Linux-kompatibel. Daher sollte vor einem Kauf die Übersicht auf *https://wiki.ubuntuusers.de/WLAN/Karten* befragt werden. Die Infos zeigen, dass Linux die allermeisten Adapter der Anbieter Asus, AVM, D-Link, TP-Link unterstützt. ■

Ethernet via USB: Für unzureichend ausgestattete Notebooks ist dies eine nützliche Ergänzung (Delock 62121, circa 30 Euro für USB 3.x und Gigabit-Ethernet).

WLAN-Stick für USB-Port: PCs ohne Funkchip bekommen Sie für 20 bis 40 Euro mit einem USB-WLAN-Stick ins Funknetz.

Serverdienste für den Datenaustausch

Das Netzwerk hat zwei Aufgaben: Zum einen soll es jedes Endgerät ins Internet bringen, zum anderen die Endgeräte untereinander verbinden. Nur um den zweiten Aspekt wird es hier gehen, und dieser Aspekt ist der kompliziertere und kreativere.

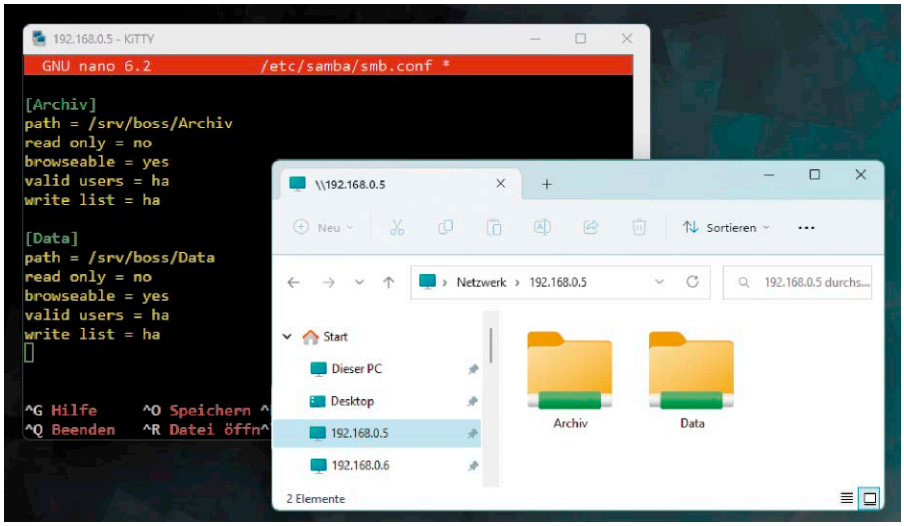
VON HERMANN APFELBÖCK

Verantwortlich für einen schnellen Internetzugang sind der Breitbandvertrag und die Hardware (siehe dazu ab Seite 52). Softwaretechnisch ist da wenig Spielraum. Im lokalen LAN sieht das ganz anders aus: Die Endgeräte können auf verschiedenen Wegen miteinander sprechen, um Daten, Medien, Software auszutauschen und verschiedene Rollen zu übernehmen. Voraussetzung ist in jedem, auch im einfachsten Fall, ein Serverdienst, der auf die Netzwerkanfragen anderer Endgeräte wartet. Dieser Beitrag erklärt die wichtigsten Serverdienste für ein typisches heterogenes Heimnetz mit Linux, Windows, Android, iOS, TV-Gerät als beteiligte Clients am Endgerät, mit Linux und Windows als potenzielle Server.

Serverdienste erfordern im Prinzip keine Investitionen in Extrahardware. Jeder Linux- oder Windows-Rechner, der ständig läuft, kann solche Dienste nebenbei übernehmen. Auch ein Router wie die Fritzbox kann für geringere Ansprüche genügen. Wer eine von sonstigen Aufgaben unabhängige Hardware im Dauerbetrieb bevorzugt, ist mit einem Raspberry Pi 4 oder einem ausgemusterten Notebook kostengünstig und gut beraten.

Windows- und Samba-Freigaben

Windows- und Samba-Freigaben sind die gebräuchlichste Methode für Datenzentralen im Netzwerk, da sie für jedes Gerät mit jedem Betriebssystem zu erreichen sind. Als Datenserver kommen PCs und Barebones mit Windows, PCs und Platinenrechner mit Linux (auch Router wie die Fritzbox) in Frage.



Linux-Samba dient in erster Linie Windows. Alle anderen Betriebssysteme, auch iOS und Android, sind mit SSH/SFTP-Diensten einfacher und funktionsreicher versorgt.

Server (1) Windows: Unter Windows ist die Serverkomponente Standard, die Freigabe für einen im Explorer markierten Ordner daher ohne Vorbereitung möglich. Aufmerksamkeit erfordert lediglich die Tatsache, dass das vereinfachende Windows-Konzept der „Heimnetzgruppe" nicht Linux/Android/Apple-kompatibel ist. Für Freigaben im gemischten Netzwerk muss daher im Explorer unter „Optionen → Ansicht" der „Freigabe-Assistent" abgeschaltet werden. Danach erfolgen Freigaben mit der Explorer-Kontextoption „Zugriff gewähren auf → Erweiterte Freigabe → Diesen Ordner freigeben". Danach kann über „Berechtigungen" im großzügigsten Fall „Jeder" den „Vollzugriff" erhalten. „Jeder" heißt nicht wirklich „Jeder", sondern nur „Jeder", der auf dem Windows-System ein Konto besitzt. Zugreifende Clients müssen sich folglich mit einem Systemkonto (des Windows-Servers) und Kennwort ausweisen. Zugriffsprobleme sind – genau wie bei Linux-Samba-Freigaben – selten netzwerkbedingt, sondern meistens auf mangelnde Dateirechte zurückzuführen. Das Windows-Konto, das über das Netzwerk zugreifen will, muss die nötigen lokalen Dateirechte besitzen. Diese können am Windows-System bei Bedarf über „Eigenschaften → Sicherheit" für den freigegebenen Ordner korrigiert werden.

Server (2) Linux: Auf Linux-Desktopsystemen ist die Samba-Serverkomponente selten vorinstalliert. Das ist mit aber

```
sudo apt install samba
```

schnell nachzuholen. Die Einrichtung des Samba-Servers kann dann einfach oder komplex ausfallen, je nach Benutzermenge und Freigabeort. Einfache und gut kombinierbare Varianten sind die Freigaben

• aller Home-Verzeichnisse
• eines bestimmten Datenordners für ein bestimmtes Konto.

Für den ersten Fall genügt das Freischalten der Zeile

```
;[homes]
```

und der nachfolgenden fünf Zeilen in der Konfigurationsdatei „/etc/samba/smb.conf“, indem jeweils das Semikolon entfernt wird. Dies ermöglicht allen Nutzern einen persönlichen und gegeneinander abgeschirmten Datenbereich auf dem Server. Beachten Sie dabei, dass die Home-Verzeichnisse in der Regel auf der Systempartition liegen, die für solche Freigabe ausreichend Platz bieten muss.

Für die Freigabe einer allgemeinen Daten- und Mediensammlung ist es rechtetechnisch am einfachsten, den betreffenden Pfad für ein einziges Pseudokonto freizugeben, das dann alle verwenden. Für diesen Fall müsste nur folgender Beispieleintrag ans Ende der Datei „smb.conf“:

```
[Archiv]
path = /srv/Archiv
writeable = no
valid users = archiv
write list = archiv
```

Das erlaubte Zugriffskonto (hier nur mit Leserecht) lautet hier also „Archiv“. Zugriffskonten müssen immer doppelt existieren – als Systemkonto und als Samba-Konto. Für das „Archiv“-Beispiel muss also mit

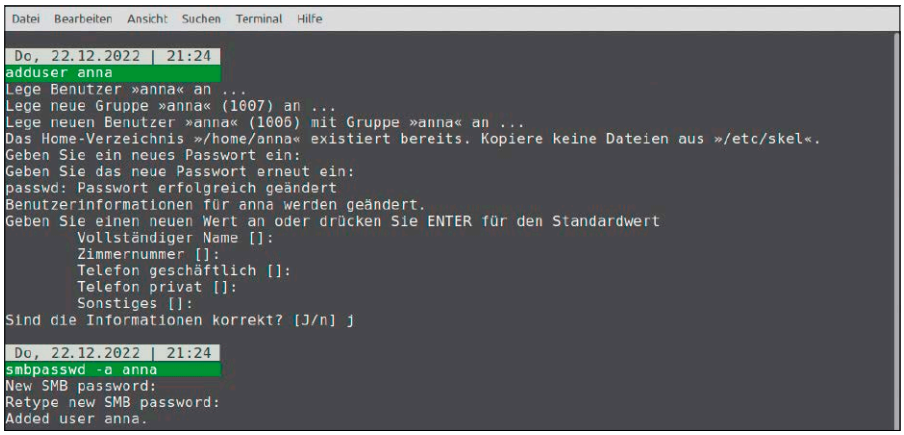
```
adduser archiv
smbpasswd -a archiv
```

ein Systemkonto und ein Samba-Konto angelegt werden – der Einfachheit halber beides mit demselben Kennwort. Für die oben angesprochene Freigabe von Home-Verzeichnissen gilt das analog: Wenn eine Person „Anna“ auf dem Server eine Home-Freigabe erhalten soll, ist dies mit

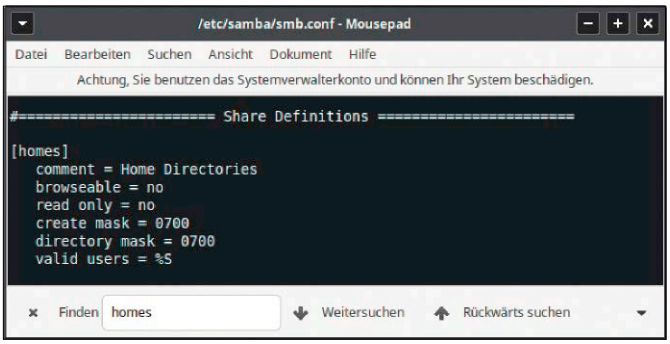
```
adduser anna
smbpasswd -a anna
```

vorzubereiten.

Server (3) Router (Fritzbox): Alle Router bieten eine NAS-Funktionalität, also Linux-Samba-Freigaben. In der Fritzbox-Konfigurationsoberfläche (*http://fritz.box* im Browser) aktivieren Sie dazu unter „Heimnetz → USB / Speicher → Geräte und Heimnetzfreigabe“ die Option „Speicher (NAS) [...] aktiv“, weiter unten unter „Heimnetzfreigabe“ ferner die Option „Zugriff über ein Netzlaufwerk (SMB) aktiv“. Damit ist der Samba-Server eingeschaltet. Die Fritzbox verlangt für den Zutritt außerdem ein Konto unter „System → Fritz!Box-Benutzer“. Das entspricht der Einrichtung von Systemkonto und Samba-Konto unter Linux wie oben beschrieben. In der Fritzbox-Konfiguration ist das mit „Benutzer hinzufügen“ und der Option „Zugang zu NAS-Inhalten“ zu erledigen. Künftig sind an die Fritzbox angeschlossene USB-Geräte (Ext2/3/4, NTFS, FAT, FAT32) per Samba freigegeben.



Systemkonto plus Samba-Konto: Dies sind die Grundvoraussetzungen für jeden Samba-Netzwerkzugriff. Das Kennwort kann identisch gewählt werden.



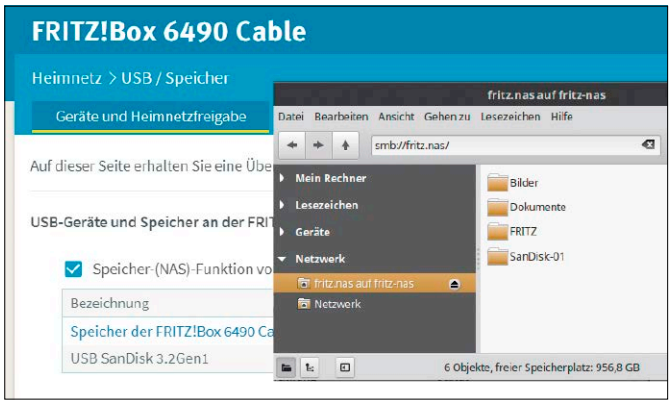
Samba mit Home-Freigaben: Das ist der einfachste Weg, für mehrere User eine Netzwerkheimat zu schaffen.

Clients (1) Windows: Linux- wie Windows-Freigaben erscheinen nicht automatisch unter „Netzwerk“ im Windows-Explorer. Es ist also mindestens einmal nötig, im Explorer manuell eine Samba-Adresse wie „\\192.168.178.1“ oder „\\fritz.nas“ einzugeben – also nach doppelten Backslash entweder die lokale IP-Adresse oder der Rechnername. Der Server (hier die Fritzbox) lässt sich dann im Windows-Schnellzugriff dauerhaft anheften und künftig mit einem Klick erreichen, sofern man sich die Zugangsdaten speichern lässt.

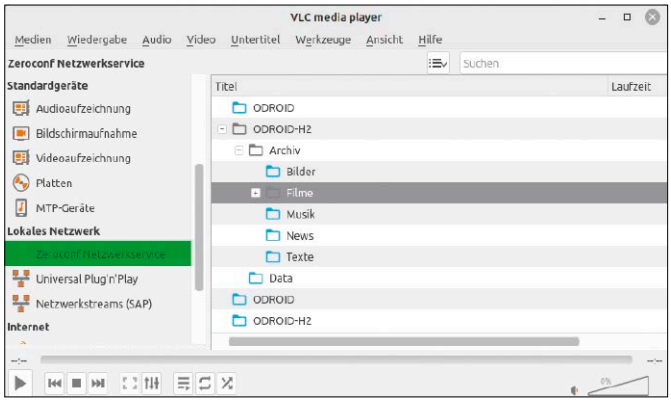
Clients (2) Linux: Auch in Linux-Dateimanagern erscheinen Freigaben nicht automatisch. Hier helfen Adressangaben wie „smb://192.168.178.1“ oder „smb://fritz.nas“. Und auch hier empfiehlt es sich, die lästige Adressangabe durch ein Lesezeichen in der Navigationsspalte des Dateimanagers zu ersetzen („Lesezeichen → Lesezeichen hinzufügen“ oder Drag & Drop der Netzressource).

Clients (3) Android/iOS: Als typische Abspielgeräte sollten Tablets und Smartphones Windows- und Samba-Freigaben nativ unterstützen, tun es aber nicht. Eine Extra-App muss her und der FE File Explorer ist dafür die beste Empfehlung: Neben Samba- und Windows-Freigaben kann er auch FTP, SFTP, Webdav und Clouddienste erreichen. Die kostenlose Version erlaubt allerdings nur eine einzige eingerichtete Serverquelle und nur wenige Audio- und Videoformate. Die Bezahlversion ist mit knapp fünf Euro die Investition wert. Bei Windows- und Samba-Freigaben ist nach Auswahl des Servertyps „Windows“ die lokale IP-Adresse anzugeben, das Speichern von „User“ und „Password“ vereinfacht den Zugriff.

Clients (4) VLC: Für Video- und Audiowiedergabe aller Art sollte man immer den VLC-Player priorisieren. Der zeigt Linux-Samba-Freigaben (aber keine Windows-Freigaben) automatisch und spielt von dort alle Medien. Das funktioniert auf allen Plattformen, aber nicht ganz identisch: Der



Fritz-NAS in der Konfiguration und im Linux-Dateimanager: Samba-Freigaben von USB-Geräten an der Fritzbox kosten wenig Aufwand.



Der VLC-Player findet Samba-Server. Das ist die praktischste Methode für die Medienwiedergabe auf Linux-, Windows-, Android- oder iOS-Clients.

Weg auf PCs führt über „Ansicht → Wiedergabeliste“ auf den Punkt „mDNS Netzwerk Diensterkennung“ (in älteren Versionen auf „Zeroconf Netzwerkservice“). In der Android-Variante zeigen sich Samba-Server unter „Dateien → Lokales Netzwerk“, in der iOS-Variante unter „Netzwerk → Dateiserver“.

SSH/SFTP mit Windows-Hürden

Die ausführliche Beschreibung für die Windows/Samba-Dienste hatte nur den einen Grund, dass kaum ein Heimnetz ohne Windows auskommt. Ohne Windows-Clients ist SSH mit seinem Dateiprotokoll SFTP völlig ausreichend und obendrein funktionsreicher.

Linux-Server: Die SSH-Serverkomponente ist auf Linux-Desktops meistens nicht vorinstalliert, aber mit dem Befehl

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

schnell nachgerüstet und damit auch sofort einsatzbereit. SSH erledigt drei Aufgaben gleichzeitig: Erstens erreicht man übers Netz das Terminal des Servers inklusive aller Terminalprogramme. Zweitens eröffnet das integrierte Protokoll SFTP Datenaustausch und Medienwiedergabe für jeden Linux- und Mac-OS-Dateimanager, aber auch für Android/iOS mit geeigneten Apps. Drittens können via X11-Forwarding grafische Programme des Servers genutzt werden.

Alle Einstellungen des Serverdienstes sind in der Datei „/etc/ssh/sshd_config“ zu steuern. Eine mögliche Anweisung, die einen Eingriff verdient, ist

```
X11Forwarding yes
```

statt auskommentierten „#X11Forwarding no“ (Standard). Weitere Änderungen sind in einem unkritischen Heimnetz selten nötig: Zwar hat standardmäßig jedes Systemkonto des Linux-Servers die Erlaubnis zum SSH-Fernzugriff, aber nur sudo-berechtigte Konten dürfen überall lesen und schreiben. Bei Bedarf kann die zusätzliche Zeile (egal wo)

```
AllowUsers sepp […]
```

den SSH-Zugriff auf bestimmte Konten beschränken.

Clients (1) Linux und Mac-OS: In das Terminal des Servers führt etwa folgendes Kommando (Beispiel)

```
ssh sepp@192.168.178.20
```

und ein Aufruf wie

```
ssh -X sepp@192.168.178.20
  thunderbird
```

kann auch grafische Programme des Servers auf dem lokalen System nutzen. Im Heimnetz noch wichtiger ist die Tatsache, dass Linux-Dateimanager das SSH-Dateiprotokoll beherrschen und mit einer Adresse (Beispiel)

```
sftp://sepp@192.168.178.20/srv/
  archiv/
```

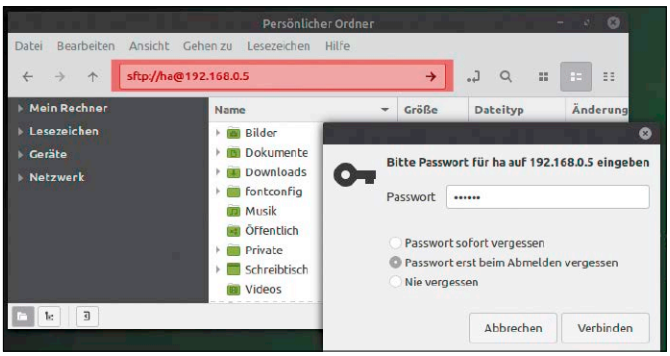
Samba-like und performanter an die Serverdateien kommen. Die Adresseingabe ist lästig, lässt sich aber durch ein Lesezeichen auf einen Mausklick abkürzen.

Clients (2) Android und iOS: Mobilgeräte können standardmäßig mit SFTP ebenso wenig umgehen wie mit Samba. Die schon für Samba empfohlene App FE File Explorer schließt diese Lücke vorbildlich. Für die SSH-Terminalnutzung gibt es ebenfalls Apps wie das kostenlose Termius.

Clients (3) Windows: Windows hat neuerdings einen nativen SSH-Client (neben dem verbreiteten Extratool Putty), aber X11-Forwarding und Dateiaustausch bleiben eingeschränkt. Im Prinzip geht mit Zusatztools (Vcxsrv für X11, *https://sourceforge.net/projects/vcxsrv*, ferner Filezilla für SFTP, *www.filezilla-project.org*) einiges mehr, aber für richtig komfortable Daten- und Mediennutzung müsste der Windows-Explorer SFTP-tauglich werden.

UPnP-Medienserver

UPnP-Server haben ihre Vorteile gegenüber der trockenen Dateiebene mit Samba oder SFTP: Sie bringen Video und Audio auch an Geräte wie Smart-TVs, die mit



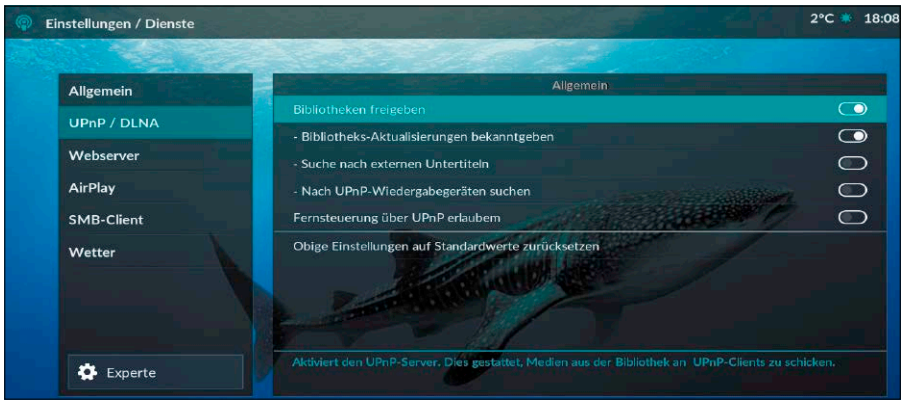
Datenzugriff und Mediennutzung per SFTP: Linux-Dateimanager sprechen SFTP und verbinden sich mit einem SSH-Server. Mac-OS, Android und iOS spielen ebenfalls mit.

Samba und SFTP nichts anfangen können. Außerdem sorgt die Auswertung der Medientags für schicke Präsentation und bessere Suchoptionen, die aus großen Sammlungen vergrabene Schätze holen können. Wirklich wertig wird UPnP im Vergleich zum einfacheren Samba- oder SFTP-Streaming aber nur, wenn das Video- und Musikmaterial sprechende Titel und zuverlässige Medientags besitzt.

Windows benötigt als UPnP-Server im Prinzip keine Extrasoftware, denn dies kann der Windows Media Player über „Streamen → Medienstreaming aktivieren" erledigen. Was der Player liefern soll, kann über „Organisieren → Bibliotheken verwalten" bestimmt werden. Die Medien erscheinen dann auf UPnP-kompatiblen Geräten wie etwa Smart-TVs oder auch im VLC- oder Banshee-Player unter „Universal Plug'n'Play".

Linux/Windows mit Kodi: An Streamingservern unter Linux besteht kein Mangel (Readymedia, Gerbera, Kodi, Plex, Emby), wobei aber Minimalisten wie Readymedia oder Gerbera den Geschmack dieser Zielgruppe eher verfehlen dürften. Erster Kandidat ist und bleibt das plattformunabhängige Kodi. Downloads für Windows oder Mac-OS sowie Installationsanleitungen für Linux gibt es unter *https://kodi.tv/download*. Damit das Medienangebot unter Kodi von UPnP-fähigen Playern wie VLC, Windows Media Player oder auch einem Smart-TV im Netzwerk gefunden wird, müssen Sie unter „System → Einstellungen → Dienste" den Dienst „UPnP/DLNA" aktivieren und dann die Option „Bibliotheken freigeben". Damit wird Kodi zum Streaming-Server.

Übers Netzwerk zu finden sind aber nur Medien, die Kodi in seine Bibliotheken eingelesen hat. Dies muss für alle Medientypen explizit erfolgen. Gehen Sie in Kodi auf „Videos → Dateien", wählen Sie „Videos hinzufügen" und klicken Sie auf „Durchsuchen". Nach Auswahl der Quelle lässt sich bei Videos der Inhalt festlegen. Zur Wahl stehen „Filme", „Serien" und „Musikvideos". Abhängig von der Auswahl lädt Kodi Coverbilder und Beschreibungen herunter. Nach einem Klick auf „Einstellungen" sollten Sie hinter „Bevorzugte Sprache" den Wert auf „de" festlegen, damit diese Informationen in deutscher Sprache erscheinen. Für Musik und Bilder läuft die Konfiguration entsprechend ab.



Kodi-Mediencenter als UPnP-Server: Mit diesen Einstellungen kann Kodi die Medien für andere Clients über das Netzwerk bereitstellen und auf andere Geräte streamen.

Remotedesktops

Remotedesktops bieten den Fernzugriff auf den kompletten grafischen Desktop. Dieser Netzwerkdienst eignet sich optimal zur Nutzung von Software, die nur auf dem Serversystem vorliegt, aber auch etwa für direkte Downloads auf dem dafür vorgesehenen Zielrechner.

Linux-Server: Als Remoteserver für Linux empfehlen wir X2go. Die Serverkomponente wird nach

```
sudo apt install x2goserver
```

als Systemdienst eingerichtet. Für optimale Darstellung empfiehlt sich am Server zusätzlich der Desktop XFCE:

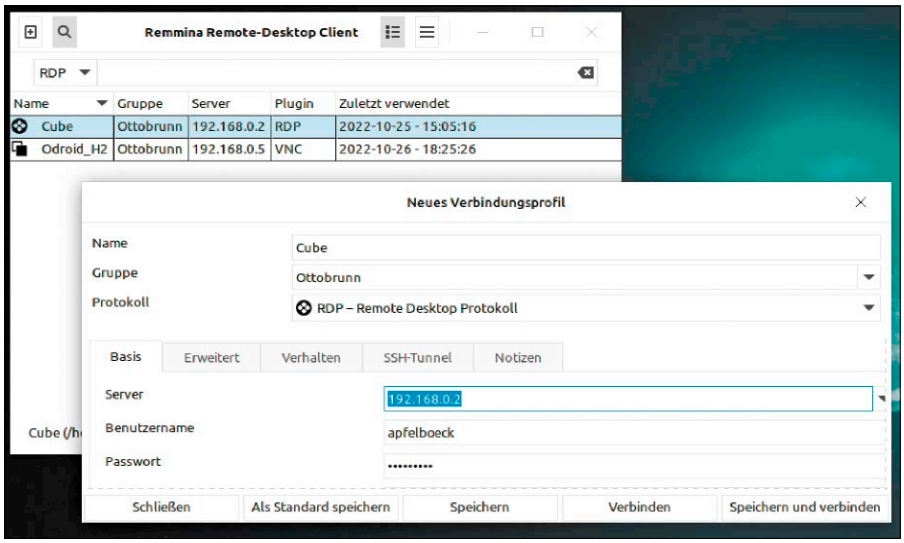
```
sudo apt install xubuntu-desktop
```

Zugriffsclients gibt es für Linux, Windows und Mac-OS unter *https://wiki.x2go.org*, für Debian/Ubuntu auch in den Standardquellen (*sudo apt install x2goclient*). Im X2go-Client definieren Sie mit „Sitzung → Neue Sitzung" den Server, was danach im Wesentlichen nur die Angaben der korrekten LAN-IP-Adresse und des bevorzugten Desktops erfordert (XFCE).

Windows-Server: Den Remotedesktop-Server (RDP) gibt es nur in Windows Pro. Liegt diese vor, kann der Serverdienst unter „Einstellungen → System → Remotedesktop" aktiviert werden. Windows-Clients verbinden sich mit der standardmäßig installierten Software „Remotedesktopverbindung" und Angabe der IP-Adresse des Servers. Linux-Rechner verwenden am besten Remmina, das nach

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

inklusive RDP-Plug-in nachzuinstallieren ist. Für den Zugriff muss in Remmina als Protokoll „RDP" und die IP-Adresse des Windows-Rechners eingegeben werden, alles Weitere ist optional. ■

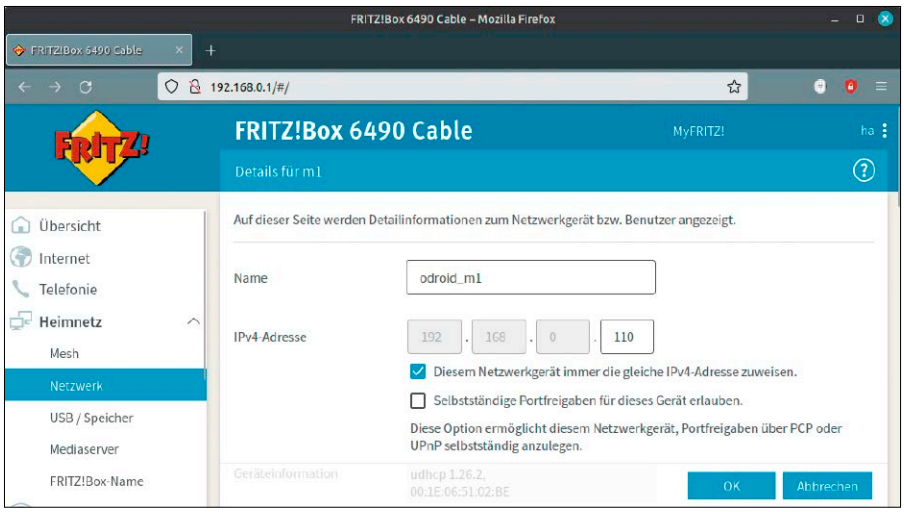


Remoteclient Remmina: Die lokale IP-Adresse und das RDP-Protokoll genügen, um in Linux einen Windows-Desktop zu nutzen.

Tipps & Tools für das Netzwerk

Die folgenden Tipps, Infos und Tools beziehen sich allesamt auf das lokale Heimnetz. Dabei geht in erster Linie darum, den Zugriff auf Netzgeräte zu vereinfachen und den Datenaustausch zu optimieren.

VON HERMANN APFELBÖCK



Feste IPv4-Adresse für Server aller Art: Jeder Rechner kann eine feste IP über seine Netzwerkeinstellungen anfordern. Einfacher ist die Vergabe in der Routerkonfiguration.

Tipps, IP-Konfiguration und Netzwerktools können keinen defekten Adapter und kein mangelhaftes Funknetz kompensieren – dazu ist Hardware erforderlich. Aber Sie erreichen Geräte schneller und kommunizieren umweglos, wenn Sie die IP-Konfiguration in die Hand nehmen und die passenden Werkzeuge zum Datenaustausch verwenden.

Feste IP-Adresse für Server

Alle Geräte mit Serverfunktion (Samba, SSH, Apache-Webserver, UPnP, Remotedesktop, Torrent) benötigen eine feste IP-Adresse – im lokalen Netz dringend, für Portfreigaben ins Internet zwingend. Nur dann funktionieren SSH-Verbindungen, Samba-Freigaben mit IP-Adresse oder IP-Lesezeichen im Browser zuverlässig. Heimrouter vergeben (als DHCP-Server) die lokalen IP-Adressen für die einzelnen Geräte keineswegs willkürlich. Es kann sein, dass ein Rechner oder ein Smartphone monatelang stets die identische IP-Adresse erhält, ohne dass dies explizit verlangt worden wäre. Das Bestreben, konstante Adressen zu vergeben, ist also schon Router-Standardverhalten. Die Garantie, dass ein NAS-Server beispielsweise die „10“ im vierten und letzten Byte der Adresse erhält, haben Sie aber nur, wenn dies ausdrücklich gefordert wird.

Jedes Netzgerät hat eine Systemeinstellung, um statt zufälligem IP-Bezug („DHCP“ oder „Automatisch“) eine feste IP anzufordern. Die nennt sich dann „Manuell“ (Linux, Mac) oder „Statisch“ (Android). Die empfohlene Methode ist aber der Weg zum Router. Der hat alle Geräte und Adressen im Blick, warnt vor Fehlern und erledigt die Aufgabe in der Konfigurationsoberfläche mit bequemen Eingabefeldern (während auf Linux-Servern eventuell Terminal und Konfigurationsdateien notwendig wären). Wenn Sie in der Fritzbox unter „Heimnetz → Netzübersicht“ in der Zeile des gewünschten Geräts das Stiftsymbol für die Bearbeitung anklicken, sehen Sie dort die Option „Diesem Netzwerkgerät immer die gleiche IPv4-Adresse zuweisen“.

Nach Klick auf „Ändern“ können Sie an vierter Stelle der Adresse die Wunschnummer eingeben. Der Router wird dann noch einen Hinweis bringen, dass diese IP erst nach dem nächsten Neustart des Geräts gelten wird.

Browserlesezeichen für Server

Wichtige Geräte im lokalen Netz bieten ihre Konfigurationsoberfläche über einen Webserver an, den Sie im Browser erreichen: Dazu gehört in jedem Fall die Oberfläche des Heimrouters, häufig weitere Netzgeräte mit integriertem Webserver wie Access Points, Repeater, NAS-Geräte, Medienserver, Netzwerkdrucker, eventuell auch eigene Serverdienste. Es lohnt sich also, im Browser Ihrer Wahl Lesezeichen für diese lokalen Adressen anzulegen. Dies funktioniert bei allen Browsern durch einfaches Drag & Drop aus der Adresszeile in Lesezeichenleiste. Danach ist noch über „Lesezeichen bearbeiten“ (oder ähnlich) ein sprechender Name zu empfehlen. Damit erreichen Sie künftig die Konfiguration all dieser Geräte mit einem Klick, ohne über IP oder Hostnamen nachdenken zu müssen. Voraussetzung ist, dass alle diese Geräte eine konstante IP-Adresse besitzen.

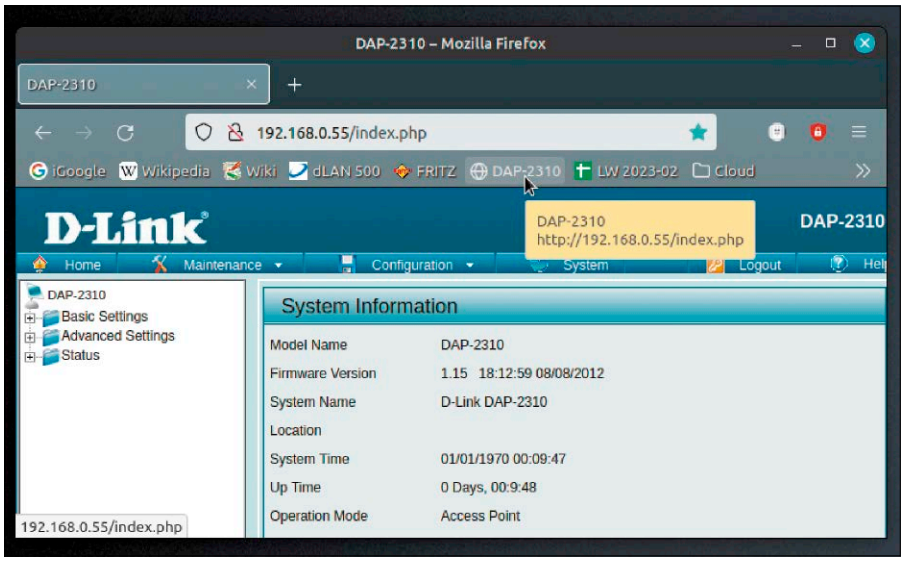
Die Subnetzmaske

Spätestens dann, wenn Sie bei einem Linux-oder Windows-Rechner eine benutzer-

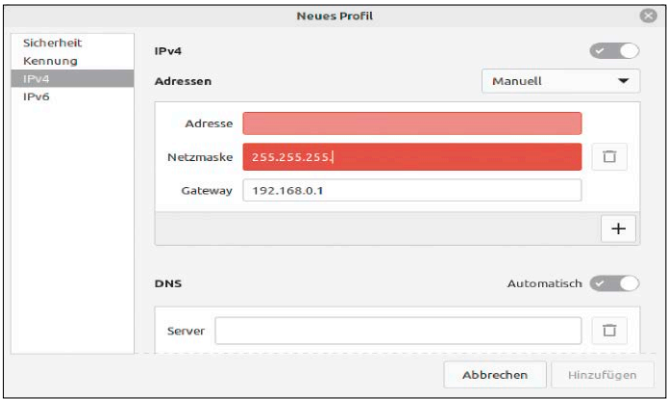
definierte IPv4-Adresse beziehen wollen (und das nicht am Router tätigen, sondern am Endgerät), kommt die Netzmaske ins Spiel. Diese wird neben der gewünschten IP und dem Standardgateway (Router-IP) abgefragt. Wer jahrelang mit Heimnetz-IPs zu tun hatte, der tippt automatisch „255.255.255.0“ ein. Das ist in allen Heimnetzen korrekt, aber warum eigentlich?

Die Bitmaske mit vier Bytes besagt, dass die ersten drei Bytes (also 24 Bits) belegt sind und daher nicht für Geräte vergeben werden können. Lediglich das vierte und letzte Byte bleibt frei zur Verfügung. Dies führt zu der typischen Situation im Heimnetz, dass die ersten drei Byte durch die Gatewayadresse (Router) vorgegeben sind (etwa 192.168.178) und nur die letzte Stelle (das vierte Byte) von „2“ bis „254“ für Geräte-IP genutzt werden kann. Die „1“ reserviert sich der Router, desgleichen reserviert ist „255“ als Rundrufadresse (Broadcast).

Anders als ein Netzclient fragt der Router bei einer festen IP-Vergabe nicht nach der Subnetzmaske – aus dem einfachen Grund, weil er sie kennt und selbst verwaltet. Theoretisch kann ein Router wie die Fritzbox durch die Subnetzmaske die Anzahl der möglichen Geräte sowohl verringern als auch erweitern („Heimnetz → Netzwerk → Netzwerkeinstellungen → IPv4-Einstellungen“). Die kleinste mögliche Subnetzmaske wäre „255.255.255.252“, die neben dem Router nur noch genau ein Netzgerät zuließe, während eine Netzmaske „255.255.254.0“ maximal 510 Geräte erlaubt, die Netzmaske „255.255.252.0“ mehr als tausend. Ein Ändern der Netzmaske in einem funktionierenden Netz mit diversen Clients wäre allerdings fatal und wird daher von einigen Providern generell gesperrt. Wo es erlaubt ist, wäre es nur bei der Ersteinrichtung des Netzes eine Überlegung wert, den Standard „255.255.255.0“ zu verlassen.



Browserlesezeichen für lokale Geräte: Sorgen Sie dafür, dass Sie die Routeroberfläche und andere Netzgeräte mit Webserver mit einem Klick erreichen.



Netzmaske oder Subnetzmaske: Die lautet in Heimnetzen immer „255.255.255.0“, weil die ersten drei Bytes vergeben sind und nur das letzte Byte für Netzgeräte frei bleibt.

Isolierte(r) Rechner oder Rechnergruppe

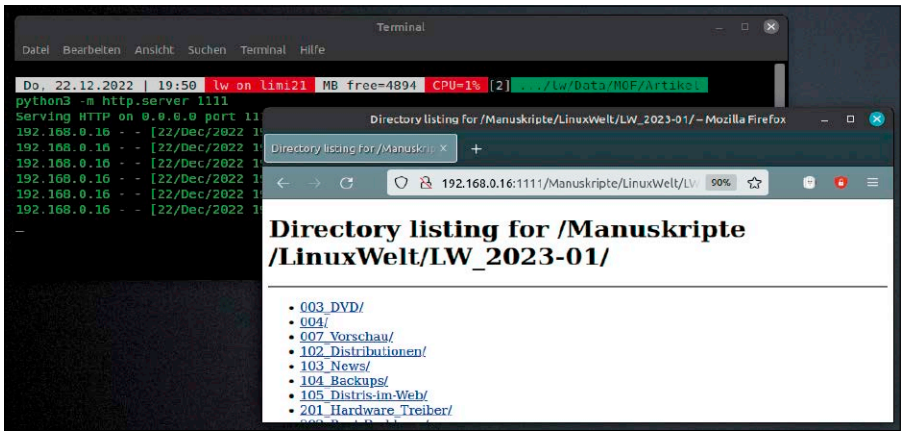
Wie praktisch alle Heimrouter bietet die Fritzbox zwei Netzwerke mit je eigenem Adressraum. Davon machen die allermeisten Nutzer nur Gebrauch, wenn sie ein WLAN-Gastnetz für Besucher anbieten wollen (Fritzbox: „WLAN → Gastzugang“). Das hat den doppelten Vorteil, dass das primäre Zugangskennwort geheim bleibt und dass alle Geräte im Gastnetz aufgrund des eigenen Adressraum isoliert bleiben („Client Isolation“): Die Geräte können zwar ins Internet, sehen aber weder Netzfreigaben noch generell Geräte im lokalen Netz, folglich auch keine lokalen Serverdienste wie etwa die Konfigurationsoberflächen des Routers oder eines NAS-Systems.

Router wie die Fritzbox können aber auch Ethernet-verbundene Geräte in das Gastnetz verlegen. Beim AVM-Router ist dafür der Ethernet-Port „LAN 4“ vorgesehen. Der lässt sich unter „Heimnetz → Netzwerk → Netzwerkeinstellungen“ mit einem Mausklick in das Gastnetz befördern: „Gastzugang für LAN 4 aktiv“. Weitere Einstellungen gibt es hier nicht: Für alle Geräte, die direkt oder indirekt (Switch, Powerline) am LAN-Port 4 angeschlossen sind, gilt dann der gesonderte Adressraum und „Client Isolation“ vom sonstigen Heimnetz. Auf diese Weise können Sie zwei getrennte Netze etwa für Homeoffice und Familie etablieren, ohne über Zugangsrechte und Kennwörter grübeln zu müssen. Standardadressraum bei der Fritzbox für das Zweitnetz ist 192.168.179.xxx. Der lässt sich aber – wie der primäre Adressraum – unter „Heimnetz → Netzwerk → Netzwerkeinstellungen → IP-Adressen“ auch ändern (nur bei Ersteinrichtung des Netzwerks zu empfehlen!).

Python: Einfache HTTP-Freigabe

Nahezu jedes Linux-System, übrigens auch das Linux-Subsystem unter Windows (falls installiert), kennt eine sehr einfache Option, einen Ordnerinhalt inklusive aller Unterordner ganz einfach anderen Teilnehmern im Netzwerk per Browser zugänglich zu machen.

Der Script-Interpreter Python, der in den meisten Linux-Distributionen vorinstalliert ist, enthält einen kleinen Webserver, der mit einem einzigen Befehl im Terminal aus dem gewünschten Verzeichnis heraus in Gang gesetzt wird:



HTTP-Server mit Python: Mit einem Terminalbefehl ist ein Webserver für das aktuelle Verzeichnis inklusive aller Unterordner eingerichtet.

`python3 -m http.server 4444`

Älteres Python benötigt diesen Aufruf:

`python -m SimpleHTTP-Server 4444`

Der Port (hier „4444“) ist jenseits von Standardports frei wählbar. Jeder Browser im lokalen Netz kann dann auf die Dateien in diesem Verzeichnis inklusive aller Unterverzeichnisse zugreifen. Soll der Miniserver immer im gleichen Verzeichnis starten, wäre ein Alias (Beispiel)

```
alias http='cd /srv/data/; python3
 -m http.server 4444'
```

eine schnelle Abkürzung unter Linux oder ein Link wie

```
wsl --cd /mnt/d/data/ --exec python
 -m SimpleHTTPServer 4444
```

ein Schnellstarter unter Windows (mit Linux-Subsystem).

Hat der „Server“-PC beispielsweise die IP-Adresse 192.168.0.2, so kommt man auf jedem Rechner mit dem Browser und der Adresse

`192.168.0.2:4444`

zur Freigabe. Hier geht dann alles, was heutige Browser beherrschen – Lesen, Abspielen, Anzeigen diverser Text-, Bild-, Audio- und Videoformate. Bei Formaten, die der Browser nicht beherrscht, ist der Download die Standardaktion. Wenn der Mini-Webserver in einem Verzeichnis auf eine Datei „index.html“ trifft, zeigt er erwartungsgemäß deren Inhalt. Strg-C im Terminal beendet den Mini-Webserver auf dem Server-System wieder.

Datenserver: Mehr als nur Datenhalde

Platinenserver- und NAS-Geräte werden meistens als reine Daten- und Backuphalde genutzt. Diese Rolle ist zwar wertvoll, aber ein solcher Server kann mehr, wie folgende Beispiele andeuten sollen:

Identische Programme auf mehreren PCs können Konfiguration, Vorlagen oder Sicherungskopien auf dem Server ablegen – mit dem Ergebnis, dass Sie auf allen Rechnern dieselbe Umgebung vorfinden. So akzeptiert der Firefox-Browser nach dem Startschalter „firefox -profile [...]“ jeden Pfad als Quelle für sein Benutzerprofil. Unter Libre Office lassen sich Backup- und Arbeitsverzeichnisse unter „Extras → Optionen → LibreOffice → Pfade“ auch auf Netzfreigaben verlegen.

Wenn es die Netzwerkleistung erlaubt, können portable Windows-Programme wie Filezilla auch komplett vom Netzlaufwerk laufen. Unter Linux kommen Tools im Appimage-Format in Betracht. Besonders flexibel sind Kommandointerpreter wie Bash, Powershell oder Cmd. Hier genügt es schon, das Netzlaufwerk in den Systempfad aufzunehmen und somit Scripts nur noch an einer Stelle pflegen zu müssen.

Es ist aber offensichtlich, dass solche Maßnahmen statt Komfort Ärger und Verzögerungen verursachen, wenn die Netzfreigabe nicht konstant verfügbar ist. Der Server muss also erstens zuverlässig laufen und zweitens immer eingebunden sein (siehe folgenden Tipp).

Mounten von Netzwerklaufwerken

Für stets erforderliche Netzressourcen reichen Lesezeichen im Dateimanager (und das damit manuell ausgelöste Mounten in das lokale Linux-Dateisystem) nicht aus. Die Freigabe sollte besser schon beim Systemstart zur Verfügung stehen und dafür in der Datei „/etc/fstab“ eingehängt werden. Das dafür nötige Paket „cifs-utils“ ist in der Regel bereits vorinstalliert. Eine Mountanweisung für eine Samba/Windows-Freigabe sieht im Prinzip so aus:

```
//[Server-IP]/[Freigabename] /
 [Mountverzeichnis] cifs
 [Optionen] 0 0
```

Die Optionen sind in diesem Fall aber nicht einfach, weil die Samba-Erlaubnis und Dateirechte berücksichtigt werden müssen. Ein konkretes Beispiel könnte dann folgendermaßen aussehen:

```
//192.168.178.10/Daten /mnt/Daten
 cifs rw,_netdev,auto,nofail,user
 name=sepp,password=geheim,uid=10
 00,gid=1000,file_mode=0644,dir_
 mode=0755 0 0
```

Der Mountpfad (hier unter „/mnt“) muss existieren. Das Beispiel geht davon aus, dass der lokale Benutzer und das Samba-Konto gleichlautend sind („sepp“). UID und GID des (lokalen) Linux-Benutzerkontos ermitteln Sie mit

```
id -u [Konto]
id -g [Konto]
```

Diese Anweisungen und die Rechtemasken sind nötig, damit der Benutzer auf die Freigabe Schreibzugriff erhält. Weitere Optionen wie „nofail“ und „_netdev“ machen den Vorgang fehlertoleranter. Verwenden Sie den Befehl *sudo mount -a*, um sich über Erfolg oder Misserfolg des fstab-Eintrags ohne Neustart zu informieren.

Netzwerktempo: Messungen

Für Tempomessungen im lokalen Netz gibt es Dutzende von Apps und Tools. Wer wissen will, wie viel Durchsatz in seinem Gigabit-Netz durch Powerline- und Funknetzbremsen noch übrigbleibt, kopiert am

Freigaben automatisch mounten: Mit einer Anweisung in der Datei „/etc/fstab“ lässt sich eine Samba/Windows-Freigabe ab Systemstart in das Dateisystem einhängen.

besten einfach eine große Datei von einer Netzfreigabe zum lokalen Rechner. Egal ob unter Linux oder Windows, wird der Dateimanager dabei auf jeden Fall eine Angabe in „MB/s“ anzeigen.

Spezielle Tools sind nur dann sinnvoll oder notwendig, wenn mit einem mobilen Android- oder iOS-Gerät an unterschiedlichen Orten gemessen werden soll. Fritzbox-Besitzer greifen am besten zur Android- und iOS-App „Fritz!App WLAN“. Über „Verbinden“ können Sie das Funknetz wechseln, falls das Heimnetz mehrere Sender hat, und unter „Mein WLAN“ gibt es die Option „WLAN messen“. Je nachdem, wie gut oder schlecht die Qualität der WLAN-Verbindung ist, schlägt der Pegel nach oben oder unten aus. Auf diese Weise können Sie ganz einfach ausmessen, in welchen Bereichen das Funksignal schwach ist. Mit „Stop“ beenden Sie die Echtzeitmessung und erhalten einen Bericht.

Nmap: Netzwerkübersicht

Was läuft in meinem Netz – und gehört das alles tatsächlich zu meinem Netz? Bei solchen Fragen hilft der Gang zur Routeroberfläche oder das Tool nmap. Nmap ist mit dem Paketnamen „nmap“ in allen Distributionen erhältlich.

Folgende nmap-Kommandos

```
nmap -sP 192.168.178.*
nmap -sP 192.168.178.* | grep
  "report"
```

schicken eine einfache Ping-Anfrage an alle 255 Adressen des Adressraums. Der Ping-Scan zeigt 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*).

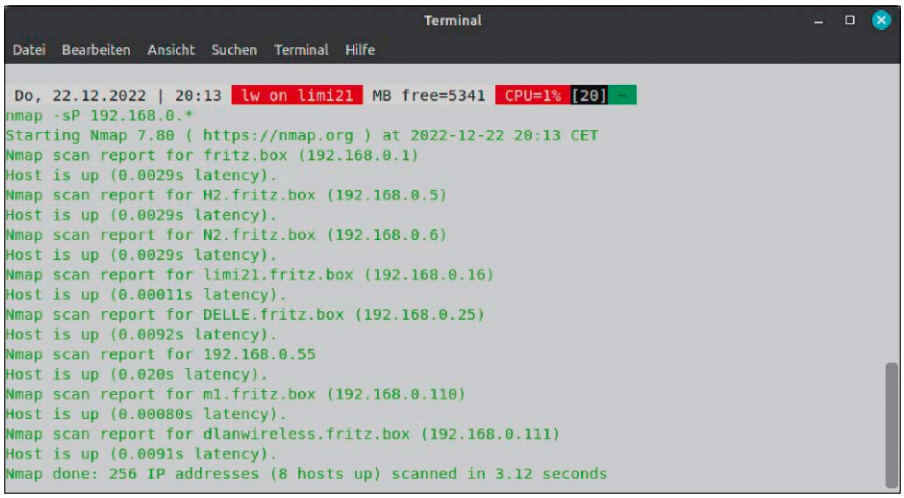
Risiken für ein Heimnetz entstehen durch offene Ports, die den Zutritt über das Internet in das lokale Netz erlauben. Kontrolle über eventuell vergessene Portfreigaben erhalten Sie im Router (Fritzbox: „Internet → Freigaben → Portfreigaben“). Mit nmap können Sie einen Test realisieren, der auch innere Feinde in Form von laufender Schadsoftware entlarvt. Dazu brauchen Sie Ihre öffentliche IP-Adresse. Die kennt Ihr Router („Übersicht“ in der Fritzbox), sie kann aber auch mit einem Tool wie inxi ermittelt werden (*inxi -i*). Die öffentliche WAN-IP, beispielweise 178.23.136.15, prüfen Sie dann mit diesem Kommando:

```
sudo nmap -Pn 178.23.136.15
```

Dabei untersucht nmap die Standardports von 1 bis 1000. Als Ergebnis sollten Sie, sofern Ihr Netz für das Internet komplett geschlossen sein soll, die Antwort erhalten „All scanned ports are filtered“. Ist das nicht der Fall, gehen Sie mit der angezeigten Portnummer der Sache auf den Grund:

```
sudo nmap -sV -Pn -p[Nummer]
  178.23.136.15
```

Mit Schalter „-sV“ zeigt nmap an, welches Programm oder welcher Dienst diesen Port benutzt. Ist dieser Prozess unerwünscht, beenden und deinstallieren Sie den Verursacher.



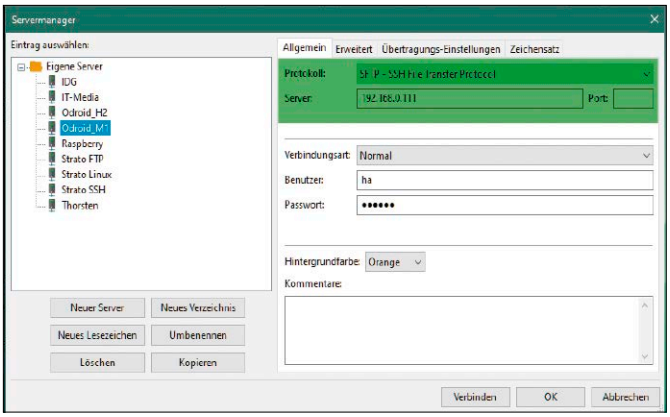
Überblick mit nmap: Der Portscanner nmap taugt auch für einfache Ping-Abfragen im lokalen Adressraum und löst dabei die Hostnamen auf.

MC und Filezilla für SSH

Der Midnight Commander (MC) sollte schon deshalb auf keinem System fehlen, weil er den direkten Datenaustausch mit SSH/SFTP-Servern über die Option „Shell-Verbindung“ beherrscht (in den Menüs „Links/Rechts“).

Wie bei SSH auf der Kommandozeile geben Sie hier die IP-Adresse an, optional gleich 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 Systems.

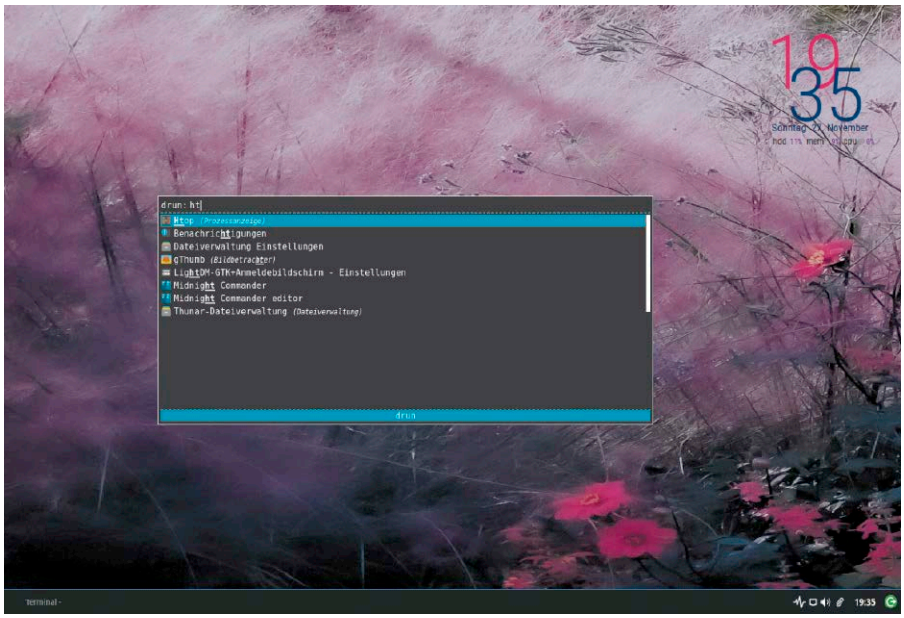
Auch Windows-Systeme dürfen mitmachen, sofern dort ein Windows Subsystem for Linux installiert ist und dort wiederum der Midnight Commander. Wer sich mit Windows ohne Subsystem mit SFTP-Servern verbinden will, greift am besten zum bewährten Filezilla (*www.filezilla-project.org*). SSH-Server sind in dessen Servermanager („Datei → Servermanager“) mit IP-Adresse, Port (Standard 22), SFTP-Protokoll und den Zugangsdaten schnell eingerichtet. ■



Wichtiger SSH/SFTP-Client unter Windows: Das Open-Source-Tool Filezilla muss auf jedes Windows-System, das mit SSH-Servern arbeiten will.

Schnelles Linux auf USB

Zweitsysteme auf USB eignen sich als mobile Allzwecksysteme, als sichere Surfsysteme oder als Reparatur- oder Backup-Dienstleister. Für die erstgenannten Einsatzgebiete ist Geschwindigkeit Pflicht, aber auch generell darf es gerne schnell gehen.



VON HERMANN APFELBÖCK

Gesucht wird das schnellste und beste Linux auf USB als Allzweck-Zweitsystem. Was wir in diesem Beitrag empfehlen werden, sind dann allerdings nicht die typischen Minimalisten oder Live-Spezialisten, die sich als Kandidaten scheinbar aufdrängen. Denn das Ergebnis sollte mehrheitstauglich und halbwegs komfortabel ausfallen – und das wirft diverse typische Mobil-Spezialisten aus dem Rennen.

Zur Info: Alle aufgeführten USB-Bootzeiten wurden mit einem 64-GB-Stick Sandisk Ultra 3.20 gemessen, allerdings auf einem älteren PC mit USB 3.0 (Gen1). Die Leistung kann auf ganz moderner Hardware besser ausfallen als hier gemessen, schlechter nur mit USB 2.0.

Aussortiert: Spezialsysteme für Bastler

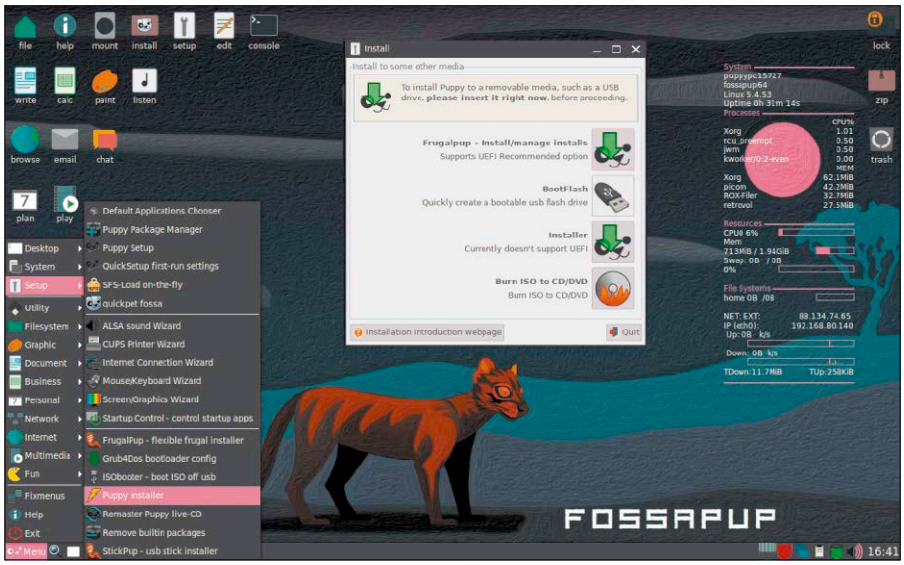
Es gibt einige bekannte Minimalisten, die sich auf den Livebetrieb als Zweit- oder Servicesystem spezialisiert haben. Ursprüngliche Zielsetzung von Live-Pionieren wie Knoppix und Puppy war allerdings eine Lösung für eine extreme Mangelsituation, die eigentlich aus der Zeit gefallen ist: Das System sollte mit CD-Kapazität zurechtkommen, die Nur-Lesbarkeit dieses Mediums muss mit virtuellen Dateisystemen im RAM kompensiert werden und dabei noch mit wenig RAM auf alter Hardware auskommen. Das sind Mangelbedingungen, die auf moderner Hardware und auf heutigen USB-Sticks eigentlich hinfällig sind. Minimalisten wie Porteus, Slax, Slitaz, Sparky, Tiny Core, Trisquel Mini oder Watt-OS setzen diese Techniken dennoch im Sinne einer Spezialisierung fort.

Aus diesem Grund sortieren wir außer Knoppix alle oben genannten Kandidaten aus, obwohl ein Slax ein USB-Schnellbooter ist (10 bis 12 Sekunden) und ein Puppy Linux wieselflink im Alltagsbetrieb arbeitet. Es gibt aber noch weitere Gründe: Slitaz (*www.slitaz.org/de*) und Tiny Core (*http://tinycorelinux.net*) sind Reduktionsrekorde ohne echte Alltagsrelevanz. Slax (*www.slax.org*), Puppy Linux (*http://distro.ibiblio.org/puppylinux*) und Porteus (*http://porteus.org*) sind allenfalls für Bastler relevant: Allein schon, deren nicht-hybride ISO-Images (nur auf CD/DVD-bootfähig) auf USB zu befördern, nötigt zu manuellen Schritten (Slax) oder zum Umweg über eine CD oder eine virtuelle Maschine (Puppy, Porteus). Weiterführende Anpassungen des Livesystems sind entweder kompliziert (Slax, Porteus) oder inhaltlich unbefriedigend: Die Puppy-Systeme bieten für ihr eigenes Paketformat wenig Software und diese praktisch nur englischsprachig.

Bei etlichen weiteren Minimalisten wie Sparky (*https://sparkylinux.org*), Trisquel (*https://trisquel.info*) oder Watt-OS (*http://planetwatt.com*) ergeben sich keine offensichtlichen Vorteile gegenüber einem Debian oder Derivaten wie MX Linux und Q4-OS.

Livesysteme: Ubuntu oder Knoppix?

Ein pures, unveränderliches Livesystem taugt nicht als Zweitsystem. Erst eine Persistenzoption für eigene Dateien, Anpassun-



Klein, schnell und eingebaute Persistenz: Puppy-Livesysteme können technisch überzeugen, sind aber nicht pflegeleicht und lassen (deutschsprachige) Software vermissen.

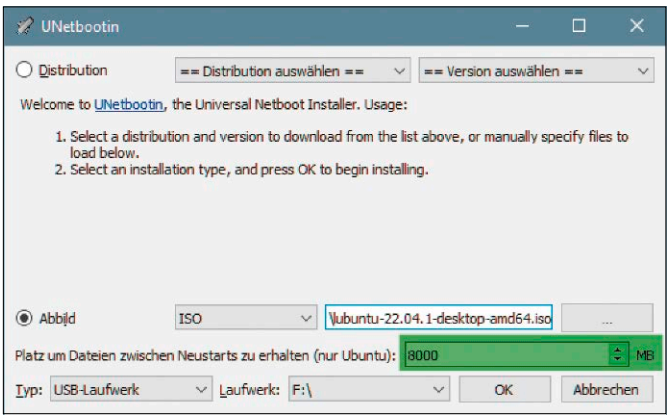
gen und Nachinstallationen macht das Zweitsystem attraktiv. Die Auswahl solcher anpassungsfähiger Livesysteme wäre trotz der oben aussortierten Live-Spezialisten enorm, weil jedes Ubuntu-basierte ISO-Installationsmedium über das Tool Unetbootin (auf Heft-DVD) mit Persistenz auf USB geschrieben werden kann. Sie müssen dazu im Unetbootin-Fenster neben der Option „Platz um Dateien zwischen Neustart zu erhalten" nur eine MB-Angabe eintragen. 2000 bis 8000 MB sind je nach Kapazität des USB-Sticks sinnvolle bis großzügige Werte. Unetbootin meldet dann beim Aktionsschritt 3 („Installiere Startverwalter") zusätzlich die Aktion „Erstellen der Persistenz".

Optimal sind Live-Ubuntus allerdings nicht, weil sie aufgrund eines standardisierten Checks des Livemediums nicht sonderlich schnell booten. 40 Sekunden sind auch bei kleinem Lubuntu oder Xubuntu für jeden Start einzurechnen. Aus Leistungsgründen sind Ubuntu-Distributionen daher eher ein Fall für ordentliche Installation auf USB. Noch ein zweiter Grund spricht gegen Live-Ubuntu auf USB: Es gibt dabei keine Möglichkeit, das USB-Medium durch Verschlüsselung zu schützen.

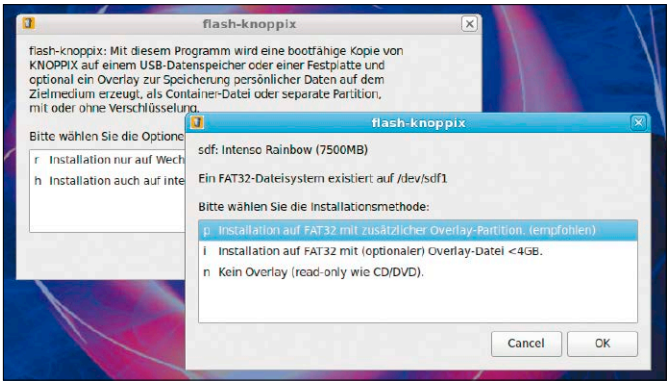
Das Debian-basierte Knoppix ist der Live-Klassiker schlechthin und ein „No-Brainer". Wem der relativ einfache LXDE-Desktop nicht zu schlicht ist, kann mit Knoppix definitiv nichts falsch machen. Deutschsprachig, mit exzellenter Hardwareerkennung, opulenter Softwareausstattung und anspruchslosem LXDE-Desktop ist Knoppix erste Wahl für ein Zweit- oder Surfsystem. Mit USB-Bootzeiten von 20 Sekunden zum eingabebereiten Desktop gehört Knoppix zu den schnellen Livestartern, wenngleich er mit Spezialisten wie Slax oder Porteus nicht ganz mithalten kann. Im laufenden Betrieb und beim Start von Programmen ist die Knoppix-Leistung durchschnittlich, aber jederzeit agil. Knoppix hat aber zusätzlich den unschätzbaren Vorteil, dass weder der LXDE-Desktop viel Eingewöhnung fordert noch Software nachinstalliert werden muss. Knoppix hat wirklich alles an Software und Tools am Start.

Der Download von einem der Mirrorserver unter *www.knopper.net/knoppix-mirrors* beträgt für die aktuellste Version 9.1 circa 4,4 GB. Achten Sie in der Liste der ISO-Dateien auf „-DE" im Dateinamen („Knoppix_V9.1DVD-2021-01-25-DE.iso"). Das hybride ISO-Abbild kann mit den üblichen Tools auf USB-Stick kopiert werden.

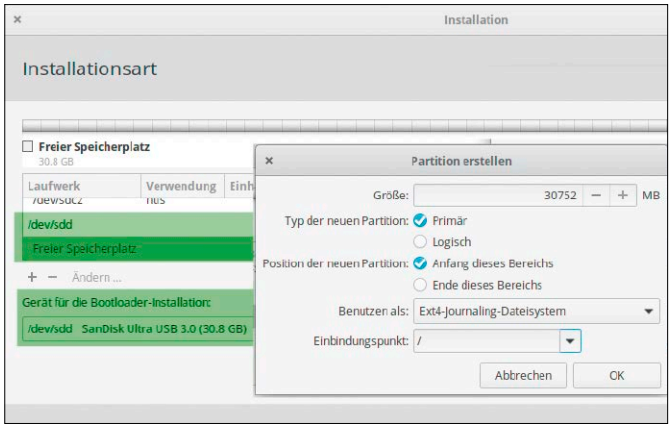
Für häufige Nutzung ist die Persistenzoption unentbehrlich, die bei Knoppix „Overlay-Partition" heißt. Dazu müssen Sie aber aus einem bereits laufenden Knoppix ein zweites erstellen. Das maßgebliche Tool „Flash Knoppix" finden Sie unter „Knoppix → Knoppix auf Flash kopieren". Nach Auswahl des Zieldatenträgers folgt die „Installation auf FAT32 mit zusätzlicher Overlay-Partition". Die Abfrage zur Größe der Overlaypartition können Sie auf einem USB-Stick einfach mit „OK" übernehmen. Dann erhält die Overlaypartition auf dem Stick die komplette Restkapazität, die das eigentliche Knoppix-System übriglässt. Eine letzte Frage betrifft den optionalen Verschlüsselungsschutz der Overlaypartiti-



Unetbootin und Ubuntu live mit Persistenz: Das ist besser als ein pures Livesystem, aber kaum optimal. Kleine Ubuntus sind regulär auf USB-Stick installiert schneller und flexibler.



Live-Klassiker Knoppix mit Persistenz: Die Overlay-Partition ermöglicht dem Livesystem Desktop-Anpassungen, Installationen und Deinstallationen.



USB-Installationen: Systempartition und Bootloader müssen als Ziel den USB-Stick erhalten. Mehr ist bei der Partitionierung nicht nötig, wenn die Installation im Bios-Modus erfolgt.

on. Es handelt sich um die einzige Möglichkeit, einen USB-Stick mit Knoppix systemweit zu schützen, weil Knoppix als Livesystem keine Benutzerverwaltung hat. Die Verschlüsselung schützt neben dem Knoppix-System auch die persönlichen Daten auf dem USB-Stick.

Mit Overlaypersistenz erlaubt Knoppix Anpassungen aller Art, auch Nachinstallationen und Entfernen überflüssiger Pakete. (De-)Installationen sind wahlweise über apt im Terminal zu realisieren oder auch über Synaptic.

USB-Installation: Schnelle Kandidaten

Jedes Linux lässt sich regulär auf USB-Stick installieren. Ein installiertes mobiles Linux auf USB oder SD-Karte ist genauso updatefähig, ausbau- und anpassungsfähig wie auf Festplatte. Anders als beim Livesystem (mit oder ohne Persistenz) ist hier ein USB-Stick mit mindestens 32 GB Kapazität zu empfehlen, besser größer.

Die Installation geschieht typischerweise im Livesystem, dessen ISO-Image Sie zunächst herunterladen, kopieren und dann im Bios-Modus starten. Bei der Partitionierung während der Installation müssen Sie dann den USB-Datenträger als Zielpartition für das System angeben, zweitens unbedingt auch als Zielort für den Bootloader. Die Vorgehensweise ist für die empfohlenen Systeme anschließend noch genauer beschrieben.

Bei der Wahl der Distribution gibt es keine prinzipiellen Beschränkungen. Aber im Sinne eines möglichst schnellen Bootvorgangs und einer agilen Systemnutzung gibt es besser und schlechter geeignete Distributionen.

Kleine Ubuntus: Im Gegensatz zum Livebetrieb booten auf USB installierte Ubuntus recht flott zum Desktop. Schnellster Starter ist das Ubuntu-basierte Bodhi Linux (*www.bodhilinux.com*), das in 13 Sekunden zum Desktop lädt. Bodhi ist auch im Betrieb und bei Programmstarts überragend schnell, lässt aber bequeme Konfigurationszentralen vermissen und hat einen gewöhnungsbedürftigen Moksha-Desktop. Unsere Ubuntu-Empfehlung ist daher das unkomplizierte Lubuntu, das – installiert auf USB 3.x – nach 21 Sekunden am Log-in ist.

Für die Lubuntu-Installation benötigen Sie das ISO-Image von *https://lubuntu.me/downloads/* (2,5 GB). Das hybride ISO-Abbild kann mit den üblichen Tools (Etcher, Gnome-Disks, USB-Imager et cetera) auf einen USB-Stick kopiert werden. Damit booten Sie einen Rechner, laden das Bios-Bootmenü (Esc, F8, F9, seltener F10, F11, F12) und dort den Stick im Bios-Modus (ohne „Uefi"). Das Livesystem bietet dann die Installation mit dem Tool Calamares an, die Sie auf einen zweiten und eigentlichen USB-Stick absolvieren. Der beim Setup wesentliche Punkt „Partitionen" muss also oben bei „Speichermedium" auf den USB-Stick verweisen. Über „Manuelle Partitionierung" löschen Sie dann eventuell vorhandene Partitionen des Sticks und erstellen auf dem nun „freien Platz" eine primäre Ext4-Partition mit Einhängepunkt „/". Die unscheinbare Option „Verschlüsseln" sorgt bei Bedarf für Vollverschlüsselung des Sticks. Zurück im Hauptdialog muss ganz unten die Option „Installiere Bootloader auf" unbedingt ebenfalls auf das USB-Laufwerk gesetzt werden, damit das USB-System später an jedem Rechner starten kann.

Hinweis: Andere Ubuntus wie Xubuntu oder Bodhi Linux verwenden einen anderen Installer (Ubiquity). Die Vorgehensweise unterscheidet sich dort deutlich, die prinzipielle Vorgehensweise ist aber entsprechend. Die Abbildung auf dieser Seite zeigt den einschlägigen Installer-Dialog.

Q4-OS ist mit Debian-Unterbau und Trinity-Desktop schnell und anspruchslos (Download unter *http://q4os.org*, auf Trinity-Variante achten!). Für einen reinen Livebetrieb ist es nicht ideal, weil es nach der Auswahl der deutschen Lokalisierung die nötigen Pakete stets erst aus dem Internet nachlädt und damit kaum unter einer Minute zu starten ist. Es ist aber ein idealer Kandidat für die reguläre Installation auf USB. Dazu muss das hybride Download-ISO erst auf einen USB-Stick kopiert und im Livesystem Q4-OS, das im Bios-Modus gestartet werden muss, auf einen zweiten und endgültigen USB-Stick installiert werden.

Die Installation erledigt hier ein eigener, aber Calamares-ähnlicher Installer, wobei unter „Software" am besten „Q4OS-Desktop" mit vollständiger Programmausstattung zu wählen ist. Unter „Partitionen" muss ganz oben unbedingt das richtige Speichermedium aktiviert werden, wobei Sie dann alles Vorhandene „Löschen" und mit „Erstellen" die Systempartition mit Einhängepunkt „/" anlegen. Eine Partitionsverschlüsselung mit Luks ist hier ebenfalls vorgesehen. Nach „OK" muss noch der Bootloader im Dialog ganz unten auf das USB-Laufwerk gesetzt werden.

Nach der Installation holen Sie die deutsche Lokalisierung nach, was das System selbst anbietet. Danach startet der „Desktop-Profiler", um die Softwareausstattung zu komplettieren.

Das installierte System startet auf USB-3.0-Stick in 15 Sekunden und belegt nach der Anmeldung für System und Desktop knapp 400 MB RAM. Der Desktop Trinity basiert auf dem eingestellten KDE 3 und wirkte lange Zeit reichlich retro. In den jüngsten Versionen (aktuell 4.10) hat sich die Oberfläche optisch gründlich modernisiert, und eingängig, übersichtlich sowie anpassungsfähig war sie schon immer. Die Arbeitsfläche ist eine klassische Dateiablage, das Menü ähnelt dem Stil älterer Windows-Versionen und die Systemleiste („Kontrollleiste") enthält mit Schnellstarter, Fensterliste und Indikatoren die typischen Elemente.

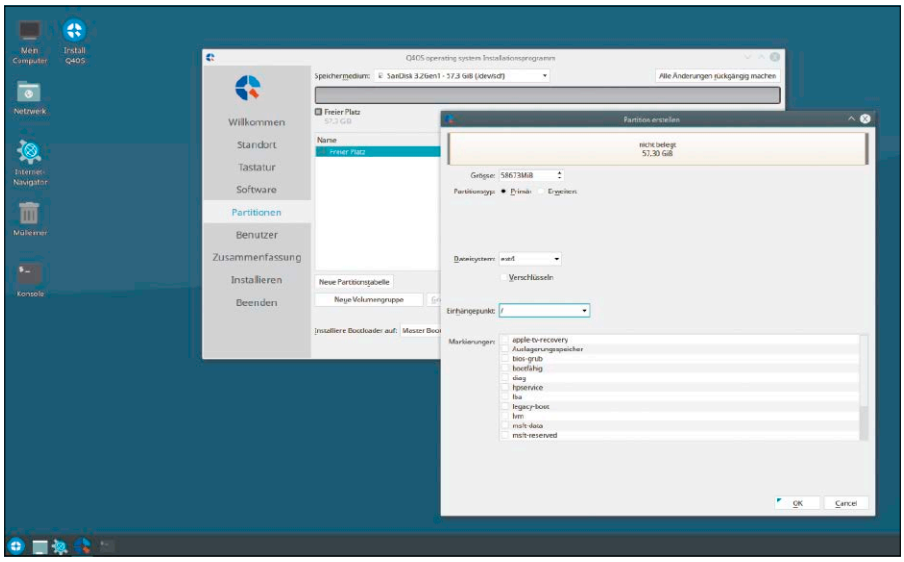
MX Linux: Diese Distribution (Download unter *https://mxlinux.org*) nutzt auf Debian-Basis entweder den klassischen XFCE-Desktop (1,7-GB-ISO) oder den besonders schlanken Fenstermanager Fluxbox (1,4-

GB-ISO), der sich lediglich einige XFCE-Anleihen wie den Xfce4-Appfinder leistet (als Menüersatz). Die Fluxbox-Variante ist für ein mobiles Zweitsystem eine schlanke Wahl, XFCE die komfortablere. Die eine oder andere englischsprachige Beschreibung oder Menübezeichnung muss man bei MX Linux aber in beiden Desktops in Kauf nehmen.

Auch für MX Linux muss zunächst das hybride Download-ISO auf einen USB-Stick kopiert werden. Mit dem Livesystem von MX Linux, das im Bios-Modus gestartet werden muss, wird es dann auf den zweiten und endgültigen USB-Stick installiert.

Das Setup verläuft einfach und linear, wenngleich ein paar Fragen mehr gestellt werden: Im Bootmenü des Livesystems wählen Sie zunächst mit F2 die Sprache „Deutsch“ und mit F3 die Zeitzone „Berlin“. Dann starten Sie den obersten Eintrag „MX-21.2“. Eventuelle Fragen nach der Grafikkarte quittieren Sie ohne Auswahl mit Eingabetaste, starten zum Desktop des Livesystems und klicken auf den Installer-Link am Desktop. Als „Art der Installation“ verwenden Sie „Normale Installation“ und wählen dann im Drop-down-Feld darunter sorgfältig den USB-Stick, der das Installationsziel ist. Beachten Sie darunter die Option „Verschlüsseln“, die System und Stick durch Luks-Datenträgerverschlüsselung schützt. Während der Installer dann bereits kopiert, werden die Daten für den Erstbenutzer, die Sprache und die Zeitzone, ein root-Kennwort, ein Computername sowie die Samba-Arbeitsgruppe abgefragt. Der Vorgang ist etwas umständlicher als bei Ubuntu & Co., aber letztlich einfacher, als diese Einstellungen später im laufenden System zu suchen.

Nach ordentlicher Installation auf USB 3.0 beträgt die Startzeit zur Desktopanmeldung etwa 18 Sekunden. Der RAM-Bedarf liegt unter 500 MB. Alle Programme, auch größere Brocken wie Browser oder LibreOffice-Komponenten, sind frappierend reaktionsschnell. Die Fluxbox-Variante von MX Linux ist tempomäßig mit Bodhi Linux vergleichbar, dabei aber deutlich pflegeleichter.



Q4-OS bei der USB-Installation: Die Distribution mit klassischem Trinity-Desktop hat sich optisch modernisiert und ist schneller und schlanker als jedes Ubuntu.

Systemoptimierung: Ausmisten und erweitern

Für ein ordentlich auf USB installiertes Linux-System gibt es nur eine nennenswerte Einschränkung: Installieren Sie besser keine proprietären Treiber, wenn das System auf unterschiedlicher Hardware funktionieren soll. Ansonsten haben Sie alle Möglichkeiten, Software zu installieren, Software zu entfernen sowie das System zu optimieren.

Software installieren und beseitigen: Alle hier empfohlenen Kandidaten verwenden das Debian-Paketformat und lassen sich über den apt-Paketmanager erweitern und entschlacken. Folglich können Sie in allen genannten Systemen in der üblichen Manier etwa mit

```
sudo apt install filezilla
```

Software ergänzen und Unnötiges mit *sudo apt remove […]* entsorgen.

Autostarts und Dienste: Um den Desktopstart und den Speicherbedarf zu optimieren, suchen Sie die „Startprogramme“ auf. Wenn eine solche Zentrale fehlt, hilft auch direkte Dateibearbeitung unter „/etc/xdg/autostart“ und „~/.config/autostart“. Komponenten, die Sie auf einem Mobilsystem nicht benötigen (Datensicherung, Blueman, Orca, Welcome …) deaktivieren Sie per Mausklick in der Zentrale oder durch Umbenennen auf Dateiebene.

Wer noch einen Schritt weiter gehen will, kann die gestarteten Dienste durchforsten:

```
sudo service --status-all
```

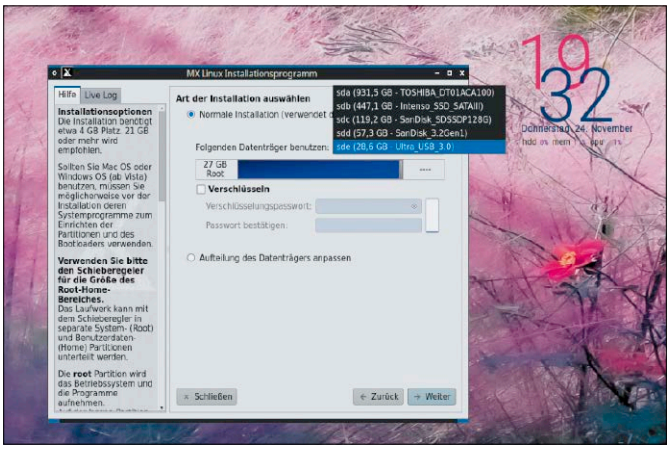
Dieser Befehl (statt systemctl) funktioniert sowohl unter systemd als auch ohne systemd – so etwa unter MX Linux. So sind die Dienste Cups (Drucken), Whoopsie (Fehlerreport), Apport (Fehlerprotokoll) oder Apparmor (Sicherheitserweiterung) auf einem Mobilsystem vermutlich entbehrlich. Einen Dienst stoppen Sie mit

```
sudo service whoopsie stop
```

und entfernen ihn später mit

```
sudo rm /etc/init.d/whoopsie
```

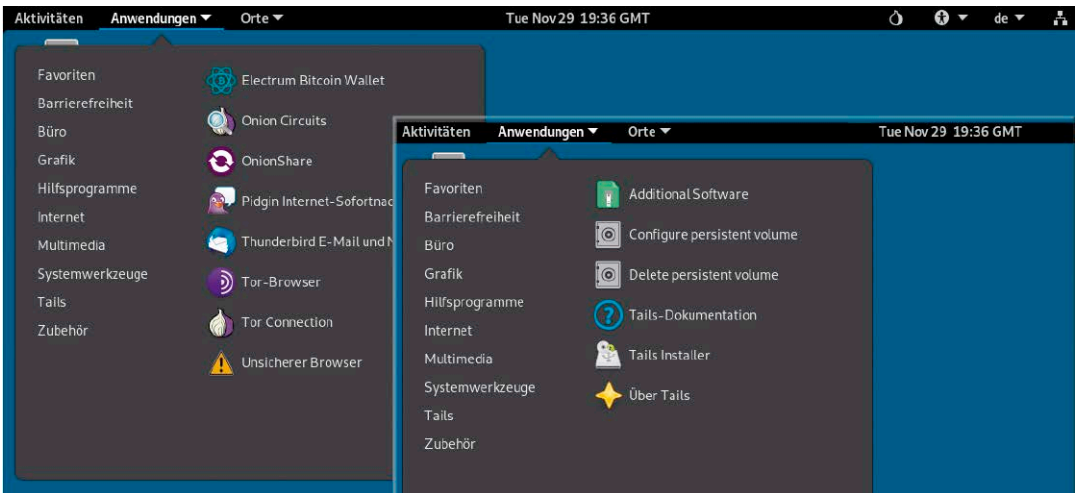
komplett, sofern er sich dauerhaft als überflüssig erweist. ■



Unser Favorit bei der Installation auf USB: MX Linux mit Fluxbox garantiert einen überaus agilen Programmalltag auf USB-Stick.

Surfsystem Tails 5.7

Das auf Datenschutz und Anonymisierung spezialisierte Tails hat jüngst Version 5.7 erreicht. Das Livesystem wird häufig aktualisiert, nicht zuletzt um neuere Versionen von TOR-Browser und Mailclient anzubieten. Eine Neuerung ist der Metadaten-Cleaner.



Die Tails-Menüs mit den wichtigsten Tools: Das Livesystem liefert eine komplette Ausstattung für einen anonymisierten Internetzugang.

VON HERMANN APFELBÖCK

Wir nehmen das jüngste Update des Debian-basierten Tails („The Amnesic Incognito Live System") zum Anlass, das prominente Surfsystem, seine Nutzung und seine Relevanz genauer vorzustellen. Die neueste Version 5.7 selbst bietet dazu wenig Anlass, denn der neue „Metadata-Cleaner" ist eine unscheinbare Ergänzung: Er löscht lediglich aus ausgewählten Foto-, Office- und Mediendateien die typischen internen Infos.

Restriktives Tails: Ein Fall für Sonderfälle

Geht es „nur" um sicheres Surfen, ist Tails gewiss nicht die adäquate Lösung. Dafür genügt schon Linux. Wenn Sie es noch sicherer haben wollen, verwenden Sie in Firefox die Add-ons Noscript und uBlock Origin (genau wie unter Tails). Für Datenschutz und Abwehr von Tracking sorgt in Firefox der „Private Modus".

Und wer selbst das noch steigern will, nutzt den Browser in einer virtuellen Maschine mit einem kleinen Linux. Bequemer als Tails ist selbst die letzte Variante allemal.

Tails zeigt, dass kompromissloser Datenschutz umgekehrt proportional zu komfortabler Systembenutzung ist.

Tails ist ein Komplettpaket, das lokal auf der benutzten Hardware überhaupt keine Spuren hinterlässt und im Internet keinerlei persönliche Spuren, nicht einmal die IP-Adresse. Damit ist das Debian-System ohne Zweifel eine effektive Anonymisierungswaffe: Der Firefox-basierte TOR-Browser schickt Webanfragen verschlüsselt durch drei zufällige Stationen des TOR-Netzwerks (Entry-, Zwischen- und Exit-Node) zum öffentlichen Zielserver.

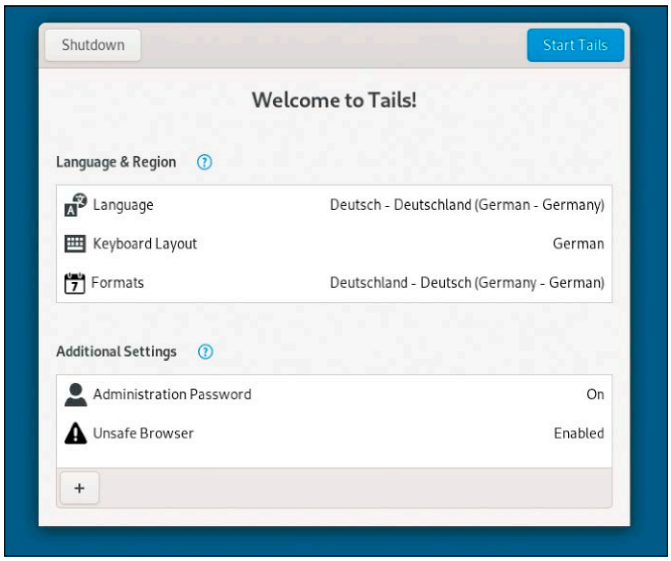
Der Zielserver erfährt folglich nur die IP-Adresse des Exit-Nodes, nicht diejenige des Rechners, von dem die Anfrage ursprünglich stammt. Innerhalb der TOR-Knoten kennt der Entry-Node zwar die IP-Adresse des Absenders, aber nicht den Inhalt der Anfrage (verschlüsselt), der Zwischen-Node weder die IP noch den Inhalt, der Exit-Node den Inhalt, der von dort unverschlüsselt zum Zielserver geht. Für den Rückweg gilt dasselbe. Die Nachverfolgung einer konkreten Internetaktion via TOR-Netz und TOR-Browser zu einer individuellen Person ist praktisch ausgeschlossen, es sei denn, es wären zufällig mehrere von Polizei und Geheimdiensten kontrollierte Nodes beteiligt. Der TOR-Browser funktioniert im gesamten öffentlichen Internet. Für das Darknet und dessen „Onion"-Sites ist das TOR-Netzwerk Bedingung.

Wer anonymes Surfen tatsächlich benötigt (in erster Linie Aktivisten, Regimegegner, Journalisten, Whistleblower, Hacker und Kriminelle), muss allerdings diverse Nachteile in Kauf nehmen, die aber allesamt berechtigt und in Tails technisch sauber umgesetzt sind:

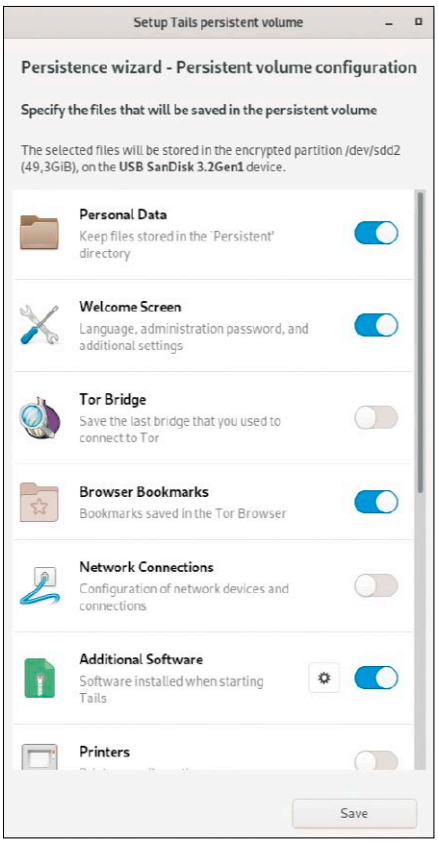
1. Das Livesystem schreibt sein komplettes Dateisystem in den Arbeitsspeicher und ist kaum unter 40, 50 Sekunden am „Welcome"-Dialog.

2. „Welcome" ist immer zu absolvieren, um deutsche Tastatur/Region einzustellen, optional den verschlüsselten Persistenzspeicher aufzuschließen (Kennwort) und eventuell Extra-Optionen (root-Passwort, „Unsicherer Browser") zu setzen. Erst danach kann mit „Start Tails" der Gnome-Desktop starten.

3. Ein gemischtsprachiges System (englisch-deutsch) ist trotz deutscher Lokalisierung zu akzeptieren.



„Welcome“ muss sein: Deutsche Lokalisierung und eventuelle Sonderwünsche sind bei jedem Systemstart zu absolvieren. Persistenz kann hier aber manchen Klick einsparen.



Amnesie-Ausnahmen: Einige Einstellungen, zusätzliche Software und Benutzerdateien kann das Tails im Persistenzspeicher ablegen. Das macht die Nutzung ein Stück komfortabler.

4. Tails ist ein restriktives Livesystem, das auch lokal keine Spuren hinterlassen will und dem Liveuser „Amnesia“ standardmäßig keinen Zugriff auf lokale Festplatten, USB-Laufwerke oder Netzfreigaben erlaubt. Wem das zu weit geht, muss am „Welcome“ unter „Additional Settings“ das root-Passwort freischalten. Dies ist auch Voraussetzung für die Nachinstallation zusätzlicher Software (mit Persistenz als zweite Voraussetzung).

5. Lokale Netzadressen etwa des Heimrouters oder eines Apache-Servers sind im TOR-Browser unzugänglich, da hier alle Adressen über externe TOR-Knoten gehen. Für einen Zugriff auf lokale Adressen muss im „Welcome“-Dialog der „Unsichere Browser“ freigeschaltet werden.

6. Der Weg ins Internet via TOR-Browser benötigt immer zwei Aktionen – erst den Zugang zum TOR-Netz via „Tor Connection“ (Zwiebelsymbol in den Gnome-Favoriten), danach den Start des TOR-Browsers.

7. Das TOR-Netz ist langsamer als direkte Internetverbindungen. Statt zweier Sendungen (Anfrage und Antwort) handelt es sich hier um insgesamt acht Stationen. Noch entscheidender ist aber, dass ein einziger langsamer Node den gesamten Durchsatz bremst. Unterm Strich ist das TOR-Netz die letzten Jahre aber deutlich schneller geworden. Das liegt schlicht daran, dass die Bandbreiten ständig wachsen und sich kaum mehr ein TOR-Node unter 30 MBit/s findet (siehe dazu das Tails-Tool „Onion Circuits“).

8. Unter Tails sind personalisierte Aktionen zu meiden. Ein Beispiel wäre etwa die Anmeldung am Google- oder Microsoft-Konto. Da die Anmeldung vom Exit-Node des TOR-Netzwerks kommt, müssen Google und Microsoft einen Fremdzugriff vermuten (unbekanntes Gerät, ungewöhnliche Region) und sperren eventuell das Konto.

Installation und Persistenz

Tails wird unter *https://tails.boum.org/install* im ISO- und im IMG-Format angeboten. Das eher irritierende „Windows – Mac-OS – Linux“-Angebot dient dort nur dazu, den Benutzer gleich zu den passenden Imagetools zu führen. Das ISO verwenden Sie für DVDs oder für virtuelle Maschinen, das IMG-Format für USB-Sticks. Letzteres schreiben Sie unter Linux etwa mit Gnome-Disks oder dem KDE-Partitionmanager auf den USB-Stick, unter Windows mit dem Win 32 Disk Imager.

Im ausgelieferten Zustand macht Tails seinem Namen alle Ehre. Wenn Sie unter „Welcome“ nur auf „Deutsch“ setzen, auf „Additional Settings“ verzichten und keine Persistenz einrichten, wird das Livesystem sein Amnesie-Versprechen am lokalen System hundertprozentig einhalten. Die Webanonymisierung via TOR wurde bereits besprochen.

Wer es etwas bequemer haben will, sollte das Tresorsymbol im Gnome-Favoritendock nutzen. Dieses Tool tails-persistence-setup etabliert auf dem Tails-USB-Stick eine Luks-verschlüsselte Extrapartition. Dabei wird die verbleibende Restkapazität neben der Systempartition verwendet. Die Luks-Partition kann später beim Systemstart im „Welcome“-Fenster durch Kennworteingabe entsperrt werden. Das ist optional und kann auch entfallen, wenn die Dienste der Persistenz aktuell nicht benötigt werden.

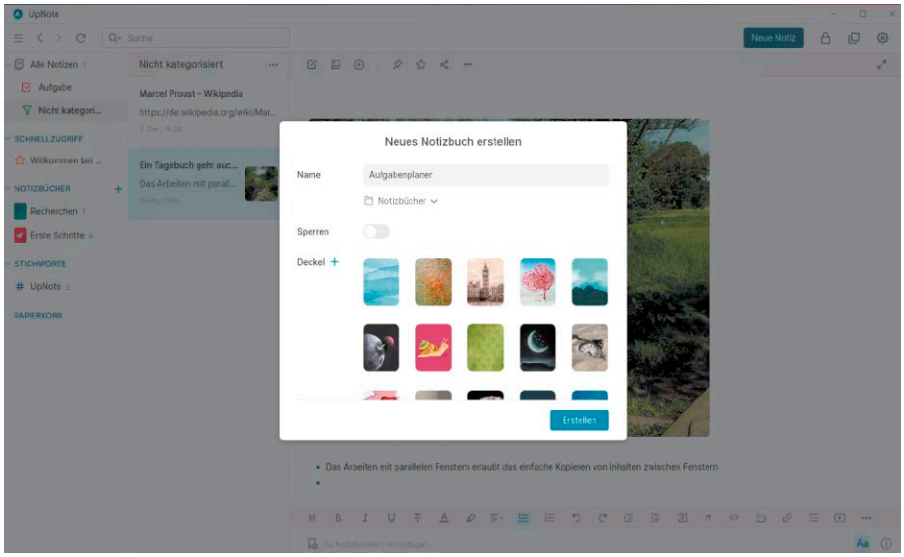
Was die verschlüsselte Partition speichern soll, kann der Nutzer in einem hübschen Optionsdialog detailliert auswählen: Die wichtigsten Optionen sind „Personal Data“ (Benutzerdateien, später unter „Orte → Persistent“ erreichbar), „Additional Software“ (Nachinstallationen), „Browser Bookmarks“ (Lesezeichen im TOR-Browser) und „Welcome Screen“. Letztere Option ist nützlich, weil dann das Aufschließen der Persistenz alle Welcome-Optionen automatisch erledigt.

Um zusätzliche Software in den Persistenzspeicher zu installieren, muss unter „Welcome“ das root-Konto freigeschaltet werden. Außerdem erscheint nach jeder Installation eine Abfrage, die mit „Install Every Time“ zu beantworten ist. Trotzdem kann nachinstallierte Software später natürlich nur dann genutzt werden, wenn beim Start der Persistenzspeicher geöffnet wurde. ■

Upnote: Software für Notizen

Wer viel am Computer arbeitet, benötigt eine Software für schnelle Gedankenblitze oder umfangreichere Notizen. Upnote will ein solcher Begleiter für den Alltag sein. Wir stellen die Lösung und ihre Besonderheiten vor.

VON STEPHAN LAMPRECHT



Das Angebot an Notizprogrammen unter Linux ist in den vergangenen Jahren gewachsen. Es reicht von Boliden wie Obsidian mit steiler Lernkurve bis zu den kleinen digitalen Post-its unter Gnome. Das kommerzielle Upnote liegt in etwa in der Mitte.

Plattformübergreifend, aber Closed Source

Wer ausschließlich freie Software einsetzen will, muss sich nach Alternativen umsehen. Denn Upnote ist eine Closed-Source-Anwendung, die auf dem Electron-Framework basiert. Daher gibt es zwar Varianten für Linux, Windows, Mac-OS, Android und iOS, aber es handelt sich um eine kommerzielle Software: Die Funktionen der Gratisversion sind eingeschränkt. So können Sie damit lediglich maximal 50 Notizen anlegen. Um die Beschränkung zu umgehen, ist der Abschluss eines Premium-Abos notwendig, das es für einen Dollar pro Monat oder gegen eine Einmalzahlung von 25 Dollar gibt. Die Installation des Programms starten Sie direkt über die Projektseite (*https://getupnote.com/#get-upnote*). Für Linux haben Sie die Wahl zwischen einem Paket im Snap-Format oder einem Appimage. Entscheiden Sie sich für das Appimage, müssen Sie die heruntergeladene Datei mit Chmod oder im Dateimanager ausführbar schalten.

Die ersten Schritte

Nach dem ersten Programmstart erscheint Upnote mit einem leeren Fenster. Klicken Sie dort auf „Erste Schritte“, öffnet dies eine gleichnamige Notiz, die anhand einer Beispielseite den Umgang mit den Textformaten vorstellt. Upnote organisiert die Einträge in Form von „Notizbüchern“, die Sie über die linke Seitenleiste organisieren. Im mittleren Teil des Fensters werden die zu einem Notizbuch gehörenden Einträge in Form einer Liste inklusive Vorschau dargestellt. Der Hauptteil ist die kombinierte Lese- und Bearbeitungsansicht. Zusätzlich können Sie mit „Tags“, also mit Stichwörtern arbeiten, um die Einträge zu organisieren.

Wenn Sie mit einem Klick auf „Neue Notiz“ ein neues Dokument anlegen, sehen Sie am unteren Rand des Eingabebereichs eine Leiste mit Schaltflächen für verschiedene Formatierungen. Die Leiste blenden Sie mit einem Klick auf das Symbol mit dem „A“ aus. Wenn Sie die Auszeichnungssprache Markdown beherrschen, dann können Sie Basisformatierungen auch direkt in den Text schreiben. Die entsprechenden Kommandos werden sofort ausgewertet und dargestellt. Dabei zeigt Upnote aber eine kleine Schwäche. Denn anders als in anderen Editoren gibt es keine Quellcodeansicht. Zudem ist die Markdown-Syntax nicht vollständig implementiert. So ist es nicht möglich, mit Fußnoten zu arbeiten, was im akademischen Umfeld ein Minuspunkt ist. Bei den Tastenkürzeln halten sich die Entwickler an bekannte Standards. So fügen Sie mittels Strg-K einen Hyperlink ein. Eher selten genutzte Formate verbergen sich hinter dem mit drei Punkten markierten Bereich in der Werkzeugleiste. Damit erreichen Sie etwa die Funktion zur Einbindung eines Videos. Schön für alle, die auch umfangreichere Texte in Markdown verfassen wollen, ist der Fokusmodus für die Notizen. Die Ansicht auf das ablenkungs-

freie Schreiben öffnet sich mit einem Klick auf den Doppelpfeil in der oberen Navigation. Wenn Sie mit Upnote Aufgabenlisten verwalten wollen, klicken Sie dazu einfach auf das Symbol für eine Checkliste am oberen Rand des Fensters. Hier finden Sie auch das Symbol, um ein Bild in den Text einzufügen. Danach öffnet sich der Dateidialog Ihres Systems.

Eine Möglichkeit zur Skalierung des Bildes blendet Upnote nach einem Klick auf das Objekt ein. Und es wird auch der Verweis auf ein Kontextmenü eingeblendet, über das Sie eine eingefügte Grafik wieder als einzelne Datei speichern können.

Freemium-Modell: Die Grenzen von „Kostenlos“

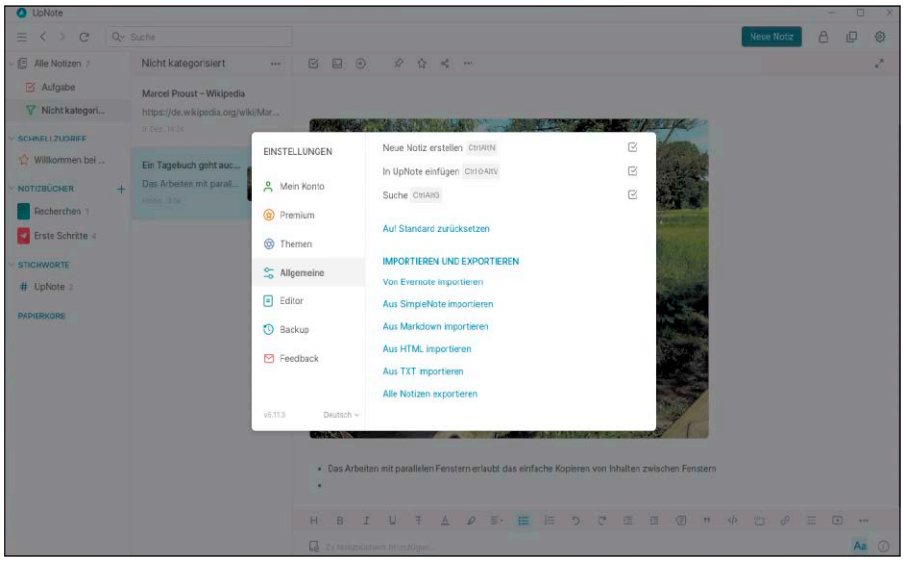
Es liegt nahe, dass ein kommerzieller Anbieter bei der Gratisvariante seiner Software Grenzen einbaut. Diese wirken in der aktuellen Upnote-Version allerdings etwas willkürlich. Ein Premium-Konto benötigen Sie etwa dann, wenn Sie Tabellen oder eine Datei in den Text einfügen wollen. Das ist auch der Fall, wenn Sie Notizen als PDF oder in Markdown exportieren möchten. Kostenlos ist lediglich der Export als HTML und reiner Text möglich.

Der Export verbirgt sich in den Einstellungen, die Sie über einen Klick auf das Zahnrad erreichen. Unter „Allgemein“ finden Sie im unteren Bereich die entsprechende Funktion. In den Einstellungen finden Sie auch unter „Mein Konto“ die Option, sich mit Benutzernamen und Passwort anzumelden. Ein solches Konto ist auch für die Synchronisation der Notizen auf verschiedenen Endgeräten die Voraussetzung.

Das Premium-Abo können Sie derzeit unter Linux nicht abschließen. Die einfachste Möglichkeit, um an Premium zu kommen, besteht darin, sich die mobile Variante auf das Smartphone (Android oder iOS) zu installieren, um im jeweiligen Store das Abo zu bezahlen. Anschließend eröffnen Sie dann ein Benutzerkonto. Wenn Sie sich dann unter Linux mit diesem Konto anmelden, stehen die Premium-Funktionen auch dort zur Verfügung.

Daten aus anderen Quellen

Kostenlos ist der Einsatz einer „Webclipper“ genannten Erweiterung für Chrome, Safari und Firefox. Einmal aktiv, übernehmen Sie dann den Inhalt der gerade im Browser angezeigten Seite als neue Notiz. Bisher ist es

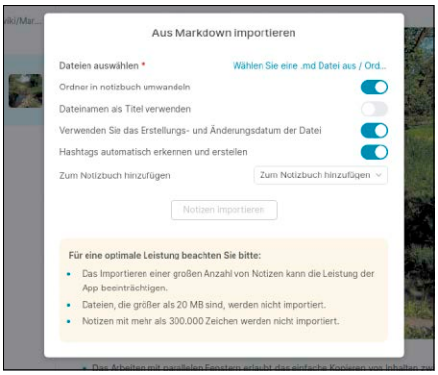


Der Import aus vielen externen Programmen ist eine Funktion, die der Premium-Version vorbehalten ist. Dazu zählt auch der Einsatz von Tabellen und Dateien in Notizen.

nicht möglich, nur einen Ausschnitt aus einem Dokument zu importieren oder eine bereits vorhandene Notiz als Ziel auszuwählen. Wenn Sie bereits mit einem anderen Programm zur Notizverwaltung gearbeitet haben und etwa den Vorzug der Synchronisation aller Notizen via Upnote nutzen wollen, können Sie mit der Premium-Funktion des Imports Daten aus anderen Quellen übernehmen. Zur Wahl stehen die Formate Markdown, TXT, HTML, Simple Note und Evernote. Im Falle der beiden letztgenannten Formate müssen Sie die Notizen erst aus der Quellanwendung exportieren – bei Simple Note in Form einer „json“-Datei, bei Evernote im herstellereigenen Enex-Format. Liegen die exportierten Dateien erst einmal vor, dann wählen Sie diese anschließend über den Importfilter aus. Den erreichen Sie über „Einstellungen, Allgemein“.

Notizen organisieren

Um Ihre Notizen zu organisieren und Inhalte schneller zu finden, gibt es eine Reihe von Optionen. Im oberen Teil des Programmfensters sehen Sie eine Suchfunktion. Je nach Auswahl auf der linken Seite durchsuchen Sie dann das gewünschte Notizbuch. Hotkey Strg-G durchsucht immer alle Einträge, unabhängig vom Ablageort. Bei der Suche haben Sie stets die Wahl zwischen Titel und Inhalt der Notizen. Am schnellsten organisieren Sie die Einträge, indem Sie ein Notizbuch aus der linken Navigation wählen. Sobald Sie einen neuen



Die Importfunktionen funktionieren fehlerlos. Im Falle von Simple Note und Evernote müssen die Daten aber erst dort exportiert werden.

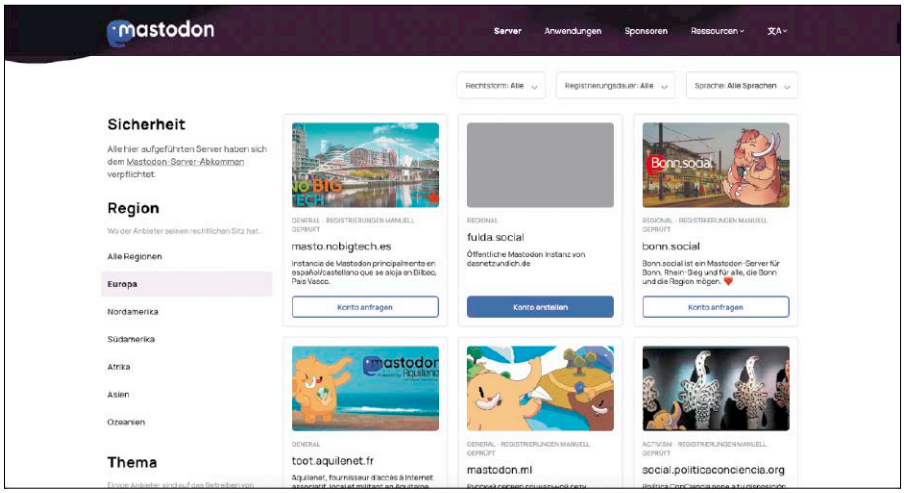
Eintrag anlegen, landet dieser im gewählten Notizbuch. Notizbücher können auch weitere Notizbücher enthalten. In diesem Fall zeigen Sie auf den Eintrag eines Notizbuchs und klicken auf die drei Punkte, um ein „verschachteltes Notizbuch“ zu erstellen. Über das Kontextmenü eines oder mehrere Einträge verschieben Sie diese in einen neuen Zielort.

Insgesamt ist Upnote ein praktischer Verwalter für Notizen – mit kleinen Schwächen. Dank der Cloudsynchronisation ist es einfach, eigene Einträge mit anderen zu teilen, ohne viel Aufwand zu betreiben. Die Abogebühren sind für die gebotenen Funktionen durchaus moderat, dürften aber angesichts zahlreicher lokaler oder webbasierter Alternativen (Tomboy, Evernote, Google Notizen, Notion, Obsidian, Mediawiki, Dokuwiki) trotzdem eine Hürde darstellen. ■

Mastodon statt Twitter

Seit der Übernahme von Twitter durch Elon Musk erlebt die Plattform Mastodon einen regen Zulauf. In diesem Artikel verraten wir Ihnen, was Sie für einen Umstieg von Twitter wissen müssen.

VON STEPHAN LAMPRECHT



Weil Mastodon dezentral organisiert ist, müssen Sie zunächst eine Instanz finden, auf der Sie sich anmelden und Mitglied werden können. Verzeichnisse erleichtern die Suche.

Mastodon gehört zum sogenannten Fediverse, womit ein dezentraler Verbund von verschiedenen Plattformen gemeint ist, die alle gemeinsam Daten austauschen. Das ist der wesentliche Unterschied zu Twitter. Sie werden Mitglied auf einer lokalen Instanz und ihre veröffentlichten Beiträge werden dann über das Netzwerk verbreitet. Solche Instanzen können ein paar Dutzend oder auch Tausende von Mitglieder umfassen. Dahinter stehen aber keine kommerziellen Unternehmen. Die meisten Instanzen werden von Privatpersonen oder Organisationen unterhalten. Wer jetzt skeptisch wird: Ja, es kann passieren, dass eine Instanz wieder schließen muss. Allerdings ist in Mastodon eine Option enthalten, um mit seinen Daten einfach umzuziehen. Und der Blick in die Computerhistorie zeigt, dass ein solcher Ansatz funktionieren kann. Mit dem Fidonet gab es bereits vor dem Internet ein den Globus umspannendes Netzwerk, über das die Nutzer Nachrichten austauschten.

So finden Sie eine Mastodon-Instanz

Die dezentrale Struktur von Mastodon erschwert den Einstieg. Es gibt eben kein zentrales Portal, wo Sie sich anmelden können. Zu den Instanzen müssen Sie wissen, dass diese unterschiedliche Schwerpunkte besitzen können. Sie beziehen sich dann auf eine Region oder auf ein bestimmtes Thema. So gibt es Instanzen, auf denen es vornehmlich um Technologie oder um politische Themen geht. Unter *https://joinmastodon.org/de/servers* finden Sie eine erste Anlaufstelle, um Instanzen zu finden, die Mitglieder aufnehmen.

Bevor Sie sich entscheiden, sehen Sie sich in der Beschreibung an, wie lange es den Server schon gibt und wie viele Menschen ihn nutzen – je länger und je mehr, umso besser. Von den thematischen Schwerpunkten merken Sie nur dann etwas, wenn Sie sich die „lokale Timeline" ansehen, die Beiträge der gleichen Instanz versammelt. Haben Sie einen Server gefunden, der Ihnen zusagt, besuchen Sie die Homepage und werden Mitglied.

Die Einrichtung von Clients

Genauso wie Twitter können Sie Mastodon auch direkt im Browser nutzen. Viele Mitglieder tun dies, weil sie die Oberfläche ausgefeilter empfinden. Wenn Sie einen Extraclient verwenden wollen, ist der Ablauf mehr oder weniger analog. Nach Programmstart werden Sie aufgefordert, wenigstens die Adresse Ihrer Instanz einzutragen, zum Beispiel „norden.social". Anschließend müssen Sie den Zugriff des Programms autorisieren. Dies geschieht durch die Anmeldung am Server via Browser. Der liefert einen Autorisierungscode zurück, der im Client eingetragen werden muss. Danach können Sie mit der Software Nachrichten lesen und verfassen. Den Zugriff einer App beenden Sie wieder über die Webansicht auf Ihrer Instanz. Unter „Einstellungen, Konto" finden Sie einen entsprechenden Abschnitt.

Für Linux gibt es eine Reihe von Clients, mit denen Sie Mastodon nutzen können. Einer der bekanntesten ist **Tootle,** der für den Gnome-Desktop entwickelt wurde und in den Quellen Ihrer Distribution als Paket „tootle" enthalten sein sollte. Entsprechend schnell haben Sie das Programm auch installiert. Die Anwendung ist einfach: Sie haben Zugriff auf die lokale und föderierte Timeline (alles, was gerade auf Mastodon passiert) und können nach Inhalten suchen. Zudem können Sie auch einfach zwischen verschiedenen Benutzerkonten wechseln.

Eine Alternative ist **Whalebird** (*https://github.com/h3poteto/whalebird-desktop/releases*), das es für Linux, Windows und Mac-OS gibt. Bei Linux haben Sie die Wahl zwischen DEB-Paket, Appimage oder Snap. Die Software erinnert in der optischen Aufteilung an Slack. Über die linke Navigation erreichen Sie die persönliche, lokale und föderierte Zeitleiste. Sie können nach Beiträgen suchen, nach Hashtags recherchieren und Listen anlegen. Auch Whalebird unterstützt mehrere Benutzerkonten, zwi-

schen denen Sie einfach mit einem Klick wechseln. Genau wie Tootle nutzt Whalebird Desktopbenachrichtigungen, damit Sie nichts verpassen.

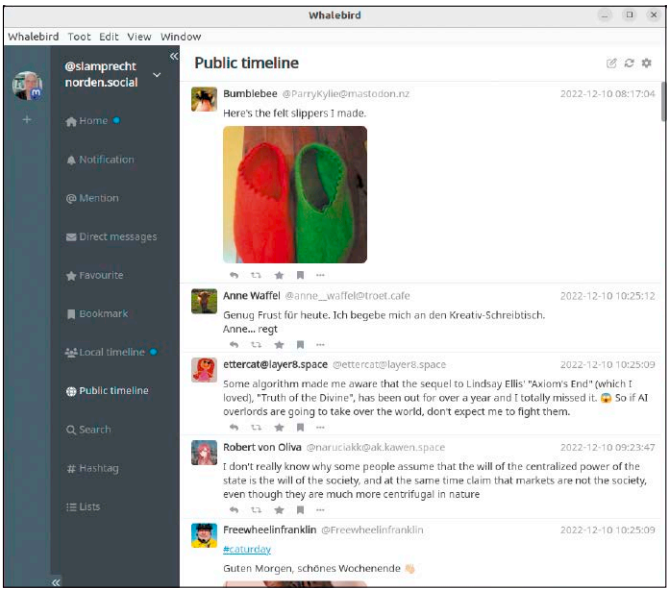
Wenn Sie auf der Suche nach einer Software sind, die auf dem KDE-Framework basiert, schauen Sie sich am besten **Tokodon** an, das unter *https://apps.kde.org/de/tokodon* als Flatpak zur Verfügung steht.

Sengi (*https://github.com/NicolasConstant/sengi/releases*) ist noch recht jung und verspricht eine zügige Weiterentwicklung. Der Entwickler bietet DEB-, Appimage- und Snap-Pakete, außerdem gibt es das Programm auch für Windows und Mac. Wenn Sie für Twitter bisher den Client Tweetdeck genutzt haben, werden Sie sich mit Sengi sofort heimisch fühlen. Denn mit dem Programm arrangieren Sie verschiedene Zeitleisten direkt nebeneinander.

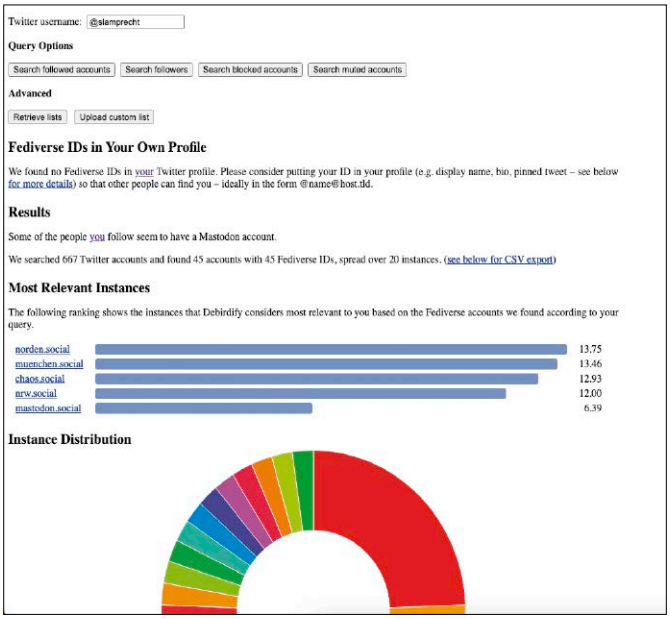
„The Desk" (*https://github.com/cutls/The Desk/releases*) ist eher ein Client für Experimentierfreudige. Er orientiert sich ebenfalls an Tweetdeck, arbeitet aber nicht immer stabil und ist außerdem keine eigene Software, sondern nur ein Wrapper für die Webansicht.

Unsere Empfehlung: Für die ersten Schritte machen Sie mit Tootle nichts falsch. Wenn Sie mehr Ansichten und Möglichkeiten wünschen, dann dürfte Whalebird der Favorit sein.

Für Linux gibt es eine ganze Reihe von Anwendungen, um Mastodon ohne Browser zu nutzen. Whalebird ist einer dieser Clients und bietet viele Funktionen.



Umzugshelfer: Um Follower von Twitter auf Mastodon zu erkennen und so schneller zu folgen, gibt es mittlerweile eine Reihe von Portalen.



Nehmen Sie Ihre Twitter-Follower mit!

Die vom neuen Eigentümer Elon Musk angestoßenen Veränderungen auf Twitter gefallen nicht allen Nutzern. Daher ist die Chance inzwischen größer, dass Sie einen ansehnlichen Anteil Ihrer Follower von Twitter auch auf Mastodon finden. Um sich Arbeit zu sparen, können Sie auf spezialisierte Dienste zurückgreifen. Dazu gehören Fedifinder (*https://fedifinder.glitch.me*), Twitodon (*https://twitodon.com*) oder auch Debirdify (*https://debirdify.pruvisto.org*). Die Vorgehensweise ist hier stets ganz ähnlich: Sie tragen den Twitter-Namen ein und autorisieren die Anwendung via Anmeldung auf Twitter. Danach gleichen die Hilfsanwendungen die beiden Netzwerke ab. Debirdify zeigt Ihnen sogar als nette Spielerei eine Grafik an, auf welche Instanzen sich die vermutlichen Twitter-Nutzer verteilen. Am Ende können Sie sich dann Dateien im CSV-Format herunterladen. In den Einstellungen von Mastodon, die Sie über die Webansicht erreichen, finden Sie den Abschnitt „Import". Dort wählen Sie aus, dass Sie eine „Folgeliste" importieren wollen. Nach dem Upload dieser Followerliste (CSV-Datei) wird diese an das System übertragen. Je nach Instanz und Ausstattung kann es eine Weile dauern, bis die Daten verarbeitet werden.

Mastodon ist anders als Twitter

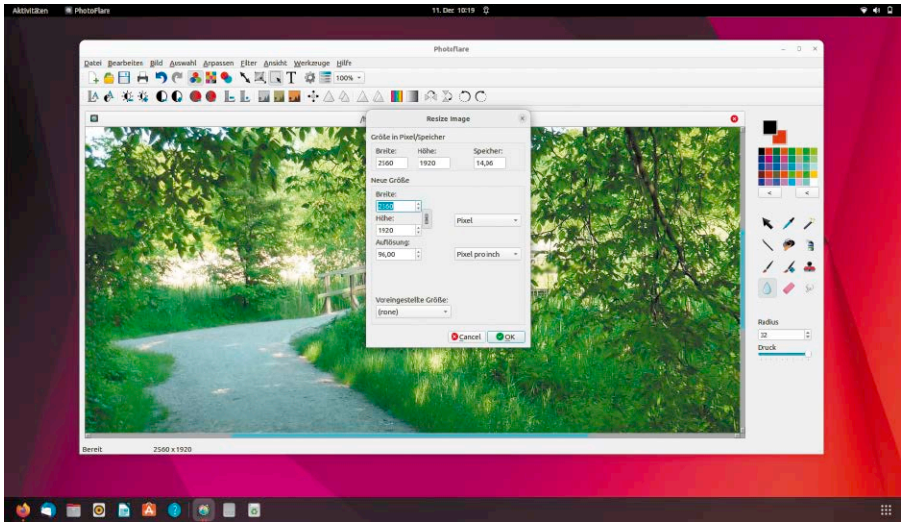
Das Beispiel des Datenimports deutet es bereits an: Mastodon ist eben nicht Twitter. Hier geht teilweise alles etwas langsamer zu. Prinzipiell kann tatsächlich jeder eine Mastodon-Instanz eröffnen – von der High-End-Maschine bis zum kleinen Tarifpaket bei einem Internethoster. Daher müssen Sie manchmal etwas Geduld aufbringen. Und wenn der Administrator an Ihrer Instanz schrauben muss, dann ist diese auch einmal für ein paar Stunden nicht erreichbar.

Andererseits macht dieser Ansatz auch viel vom Charme von Mastodon aus. Der Umgang untereinander ist freundlicher und angenehm. Und weil das Fediverse verglichen mit Twitter oder Facebook noch deutlich kleiner ist, werden Sie mehr Beiträge aufnehmen und lesen können. Wer dagegen nur auf der Suche nach Reichweite und Aufmerksamkeit ist, für den ist Mastodon keine Alternative zu Twitter. ■

Photoflare: Fotoeditor für jeden

Mit Photoflare gesellt sich ein weiteres Programm in die nicht gerade kleine Auswahl der Linux-Fotobearbeitungen. Oberfläche und Funktionen sind so konzipiert, dass sich ohne nennenswerte Einarbeitung sofort schnelle Ergebnisse erzielen lassen.

VON STEPHAN LAMPRECHT



Ambitionierte Fotografen und Experten, die am liebsten am Rohformat der Kameraaufnahmen arbeiten und sich mit der Restauration alter Aufnahmen beschäftigen, gehören nicht zur Zielgruppe von Photoflare (*https://photoflare.io*). Der Entwickler der Software hat Anwender im Blick, die gelegentlich ihre Fotos aufhübschen, ohne sich auf Boliden wie Gimp einlassen zu wollen. Vorbild ist das bisher nur für Windows erhältliche Photofiltre. Aktuell ist Photoflare kostenlos als Community-Edition verfügbar. Die Entwickler arbeiten aber auch an einer kommerziellen Edition.

Aktuelle Version besorgen

Einige Distributionen haben eine veraltete Version von Photoflare in ihren Paketquellen. Um mit dem aktuellen Release zu arbeiten, fügen Sie am besten das Repository des Entwicklers den Paketquellen hinzu. Unter Ubuntu erledigen Sie das folgendermaßen in einem Terminal:

```
sudo add-apt-repository
  ppa:photoflare/photoflare-stable
sudo apt update
```

Danach können Sie die Software mit

```
sudo apt install photoflare
```

installieren. Falls Sie mit Synaptic installieren, finden Sie unter „Einstellungen“ den Eintrag „Paketquellen“. Im Register „Andere Programme“ fügen Sie die Quelle mit „deb https://ppa.launchpadcontent.net/photoflare/photoflare-stable/ubuntu <Codename> main“ hinzu. Für Ubuntu 22.04 wäre dies also „jammy“, für die Version 22.10 „kinetic“.

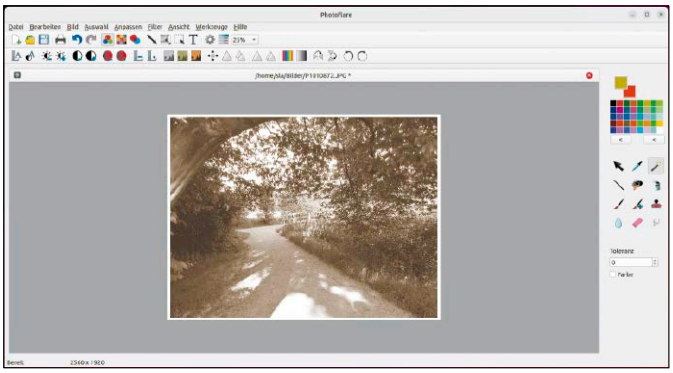
Ist die Installation abgeschlossen, starten Sie die App über den von Ihnen bevorzugten Weg. Nach dem ersten Start erscheint die noch leere Oberfläche in englischer Sprache. Unter „Tools“ rufen Sie „Preferences“ auf, wechseln in das Register „Startup“ und wählen dort „German“ als Sprache aus dem Listenfeld. Mittels „Restart“ rufen Sie die Anwendung erneut auf, um die Änderung zu übernehmen.

Das erste Bild bearbeiten

Über „Datei → Öffnen“ laden Sie jetzt das erste Bild, das Sie bearbeiten wollen. Photoflare unterstützt die gängigen Formate PNG, JPG, GIF, TIFF, BMP, ICO, PBM, PGM und PPM. Beim Öffnen passt Photoflare die Abmessungen des Fotos an das Programmfenster an. Über das kleine Listenfeld in der Werkzeugleiste ändern Sie bei Bedarf den Zoomfaktor.

Photoflare organisiert die Werkzeuge in Form verschiedener Symbolleisten. Die Werkzeuge korrespondieren mit den Menüeinträgen. Auf der rechten Seite des Programmfensters sind die Freihandwerkzeuge untergebracht, die zur Auswahl von einzelnen Bildbereichen, dem Löschen von Bildbereichen und dem Verwischen („Blur“-Effekt) genutzt werden. Haben Sie etwa ein Bildschirmfoto aufgenommen, wollen aber sensible Informationen unkenntlich machen, klicken Sie auf das kleine Tropfen-Symbol, definieren den Radius in Pixeln und verwischen dann mittels Klicken und Ziehen den Bereich. Ebenso einfach geht das Skalieren eines Bildes von der Hand. Klicken Sie dazu entweder in der Symbolleiste auf das Werkzeug mit dem „Doppelpfeil“ oder nutzen Sie das Menü „Bild → Bildgröße“. Im nachfolgenden Dialog zeigt Ihnen Photoflare im oberen Teil die aktuel-

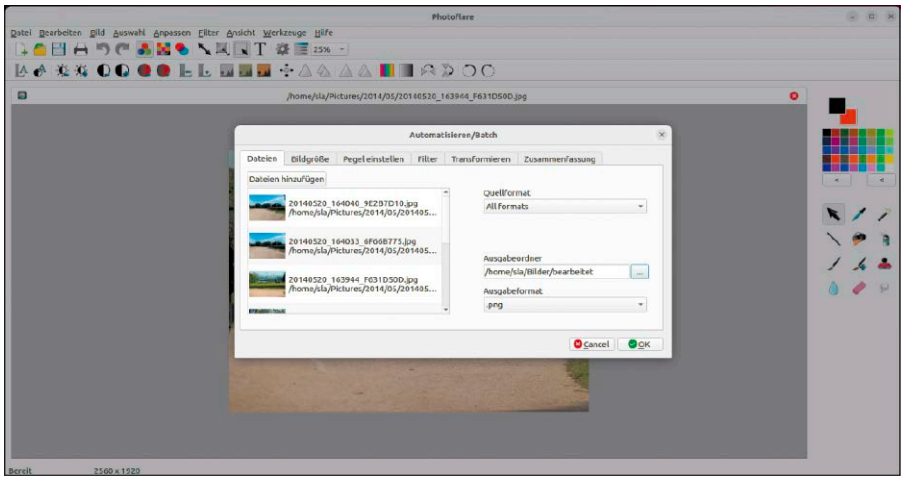
len Abmessungen. Diese verändern Sie jetzt mittels der Eingabefelder.
Zudem lässt sich auch die Auflösung verändern. Wenn die neuen Maße nicht die Proportionen des Ausgangsfotos berücksichtigen sollen, lösen Sie die Verbindung zwischen Breite und Höhe mit einem Klick auf das kleine Symbol zwischen den beiden Feldern. Optional dürfen Sie auch andere Maßeinheiten als die voreingestellten Pixel nutzen.



Die Oberfläche von Photoflare ist übersichtlich und aufgeräumt. Das Programm bringt aber alle wichtigen Funktionen und eine Reihe von interessanten Filtern und Effekten mit.

Fotobearbeitung mit typischen Filtern

Durch die Kombination von Werkzeugen und Effekten verleihen Sie Ihren Aufnahmen individuelle Optik. Um ein Foto mit einem „Rahmen“ zu versehen, wählen Sie aus dem Menü „Bild“ die Funktion „Leinwandgröße“ aus. Im nachfolgenden Dialog tragen Sie einen Pixelwert für die Höhe und Breite ein, die zusätzlich um das Foto gelegt werden soll. Diesen Teil könnten Sie, wenn Sie wollen, anschließend mit den Werkzeugen auf der rechten Seite noch einfärben. Über „Filter → Farbe → Sepia“ weisen Sie dem Bild den bekannten Alterungseffekt zu. Sie finden in dem Menü „Filter“ eine ganze Reihe weiterer Effekte. Für einen ausgefeilteren Rahmen nutzen Sie etwa die dafür integrierten Filter.



Die eingebaute Stapelverarbeitung ist ein beachtliches Feature für ein so schlankes Programm. Hauptregister vereinfachen die Auswahl der gewünschten Aktionen.

Transparenz schaffen: Bei Bildformaten, die dies unterstützen (PNG, GIF), können Sie auch mit Transparenz arbeiten. Dies ist ja gerade bei Kopfgrafiken von Blogs oder Onlineartikeln beliebt. Am zuverlässigsten funktioniert dies bei einfachen Grafiken und Fotos, die einen deutlich erkennbaren, im Idealfall einfarbigen Hintergrund verwenden. Dies ist bei Logo-Dateien meistens der Fall. Klicken Sie auf „Bild → Transparente Farbe“. Der Mauszeiger verändert sich zur Pipette. Mit dieser bewegen Sie sich in den Teil des Bildes, der später transparent sein soll. Mit einem Klick wählen Sie die Farbe aus. Im nachfolgenden Dialog nutzen Sie am besten die Funktion „Vorschau“, um sich vom späteren Ergebnis zu überzeugen.
Schärfe und Farbeffekte: Zur Ausstattung von Photoflare gehören auch Funktionen, mit denen Sie die Kontraste oder Farbsättigungen verändern können. Hier bietet das Programm allerdings nur einen Basisumfang an Funktionen. Anwender, die auf dieser Ebene die Bilder bearbeiten wollen und somit offenbar die notwendigen Kenntnisse besitzen, werden vermutlich zu einer Software greifen, die in dieser Hinsicht mehr bietet.

Stapelverarbeitung nutzen

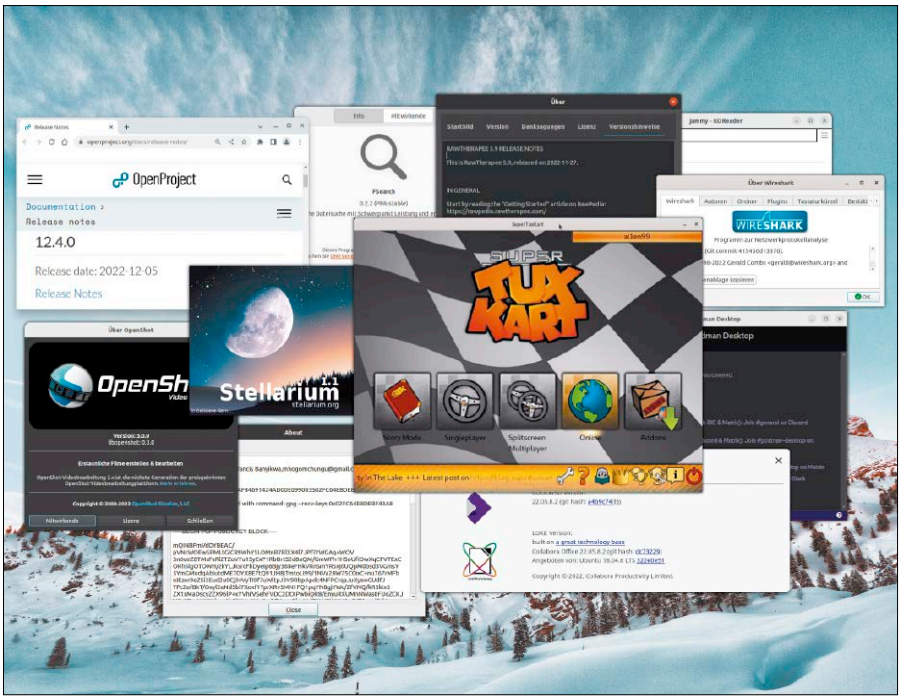
Für ein so schlankes Programm überraschend ist die Unterstützung einer Stapelverarbeitung. Die ist für alle Nutzer interessant, die an einer größeren Zahl von Bildern eine oder mehrere Bearbeitungsschritte ausführen müssen. Eine typische Aufgabe, die alle Blogautoren kennen, ist die Skalierung des Bildmaterials passend zur Blogvorlage.
Über „Werkzeuge → Automatisieren“ rufen Sie den Assistenten für die Stapelverarbeitung auf. Innerhalb des ersten Registers legen Sie zunächst die Dateien fest, die verarbeitet werden sollen. Außerdem können Sie optional ein Zielverzeichnis angeben, wo die bearbeiteten Dateien abgelegt werden. Zudem definieren Sie das Zielformat. Die weiteren Register stellen Ihnen die benutzbaren Werkzeuge zur Verfügung. Sie können alle oder eine Teilmenge benutzen. Um die Bildgröße zu verändern, wechseln Sie in das gleichnamige Register und aktivieren das Optionsfeld. Anschließend definieren Sie die Zielgröße. Damit die Proportionen der Fotos gleich bleiben, aktivieren Sie zusätzlich die Option „Seitenverhältnis beibehalten“.
Drehungen und Spiegelungen finden Sie im Register „Transformieren“ und natürlich können Sie auch Filter auf das Ausgangsmaterial anwenden. Nach der Definition der Arbeiten sehen Sie unter „Zusammenfassung“ noch einmal alle Aktionen, die Sie definiert haben. Mit „OK“ starten Sie den Vorgang. Sie können den Fortschritt mitverfolgen. Photoflare öffnet die Dateien in seinem Editor.

Schnelles Programm für wichtige Arbeiten

Die Community-Version von Photoflare kann voll überzeugen. Sie bietet alle wesentlichen Werkzeuge, um die grundlegenden Arbeiten am Bildmaterial umzusetzen. Die Software eignet sich für alle Einsteiger und Personen, die Fotos schnell und unkompliziert zur weiteren Verwendung in anderen Projekten bearbeiten müssen. ■

Neue Software

Die Softwarevorstellungen sind in dieser Ausgabe breit gefächert, enthalten aber nur Open-Source-Programme. Neben Schwergewichten wie der Collabora Online Developer Edition sind eine Menge nützliche Utilitys für den Linux-Alltag vertreten.



VON DAVID WOLSKI

Open-Source-Software ist heute eine feste Größe in der IT-Kultur von Unternehmen und Behörden und ein wichtiger Baustein im reibungslosen Funktionieren von kritischen IT-Infrastrukturen. Open Source, und damit ist bei weitem nicht nur der Linux-Kernel gemeint, ist aus der Bastel- und Hobbyecke längst herausgetreten. Sorgt das allein für eine höhere Entwicklungsgeschwindigkeit, für mehr Transparenz und für höhere Sicherheitsstandards? Leider nein.

Suche nach dem schwächsten Glied

Open-Source-Projekte haben den Ruf, besonders sicher zu sein, da der Quellcode für jedermann einsehbar ist. Trotzdem kann man nicht bei jeder offenen Software davon ausgehen, dass den Quellcode wirklich so viele Augen kontrollieren, wie es etwa beim Linux-Kernel der Fall ist. Die enorme Verbreitung von Open-Source-Komponenten zeugt von einem hohen Kostendruck bei der Entwicklung anderer Software und von manchmal blindem Vertrauen in gewachsene Strukturen. Für welche Strukturen sollen individuelle Programmierer einstehen, die manchmal mit einfachsten Mitteln und unter abenteuerlichen Umständen arbeiten – ohne regelmäßige Geldquelle? Genialität am Bildschirm und im Quellcode wird auch mal von trivialen Faktoren des täglichen Lebens überschattet und die Konsequenzen sind übersehene Bugs und schlimmstenfalls Sicherheitslücken. Auch fällt es zunächst nicht weiter auf, wenn Langstreckenläufer in ihrer oft selbst gewählten Einsamkeit mal straucheln, dann nicht mehr liefern und die Liste der unbearbeiteten Bugs immer länger wird.

Die Probleme erben dann größere, darauf aufbauende Softwareprojekte und reißen manchmal, wie im Fall der Schwachstelle „Log4Shell“, eklatante Sicherheitslücken quer durch die Bank – buchstäblich! Davor waren auch schon mal Open SSL, Gnupg und der Zeitgeber NTP bedrohte Bibliotheken mit schwächelnden Entwicklern, die dennoch im weltweiten IT-Alltag kritische Rollen einnehmen.

Census-Report der Linux Foundation

Offener Quellcode und eine transparente Entwicklung garantieren keine Sicherheit, das zeigen inzwischen viele Beispiele. Um Projekte zu identifizieren, die wenig Entwicklerpower hinter sich haben, aber in allen Ecken der verbreiteten IT im Einsatz sind, kümmert sich mittlerweile die Linux Foundation.

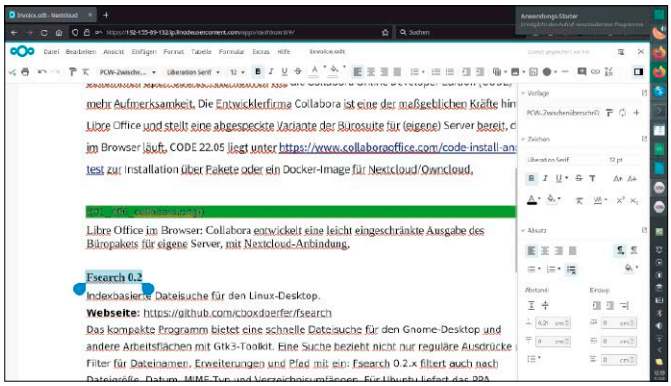
Jedes Jahr veröffentlicht das gemeinnützige Industriekonsortium eine Liste jener Software und Komponenten, die mehr Unterstützung gebrauchen könnten: Der „Census“-Report macht auf Probleme und wenig tragfähige Strukturen hinter wichtigen Open-Source-Projekten aufmerksam und ist gerade in seiner dritten Fassung in Arbeit. Die bisherigen Reports sind unter *https://www.linuxfoundation.org/research* einsehbar.

Die Ergebnisse erstaunen: Laut der Analyse der Top 500 der freien Softwarepakete haben mehr als 20 Prozent der Projekte nur eine(n) einzige(n) maßgebliche(n) Entwickler oder Entwicklerin. Es gilt deshalb, durch Initiativen und bezahlte Kräfte diesen Missstand zu beheben, bevor die Köpfe hinter wichtigen Open-Source-Komponenten die Lust verlieren oder in Rente gehen und übersehene Bugs kompletten IT-Infrastrukturen gefährlich werden.

Collabora CODE 22.05

Libre Office als Webapplikation für den eigenen Server
www.collaboraoffice.com/code

Nachdem MS Office 365 von Datenschützern scharf kritisiert wird, bekommen Open-Source-Alternativen wie die Collabora Online Developer Edition (CODE) mehr Aufmerksamkeit. Die Firma Collabora steht hinter Libre Office und bietet eine Variante der Büro-Suite für (eigene) Server, die im Browser läuft. CODE 22.05 liegt unter *www.collaboraoffice.com/code-install-and-test* zur Installation bereit – über Binärpakete oder ein Docker-Image für Nextcloud/Owncloud. ■

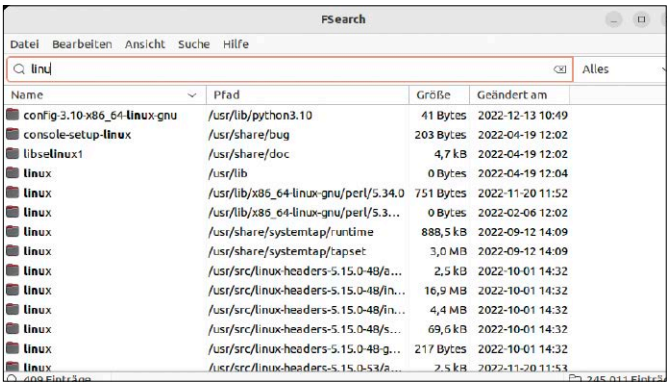


Libre Office im Browser: Collabora entwickelt eine leicht eingeschränkte Ausgabe des Büropakets für eigene Server (mit optionaler Nextcloud-Anbindung).

Fsearch 0.2

Indexbasierte Dateisuche für den Linux-Desktop
https://github.com/cboxdoerfer/fsearch

Fsearch ist bietet eine schnelle Dateisuche für den Gnome-Desktop und andere Arbeitsflächen mit Gtk3. Die Suche beherrscht Dateinamen, Extensionen, Pfade, reguläre Ausdrücke und nun auch Dateigrößen, Datum, MIME-Typ und Verzeichnisumfänge. Für Ubuntu liefert das PPA *https://launchpad.net/~christian-boxdoerfer/+archive/ubuntu/fsearch-stable* neue Pakete. Die Versionsnummer sollte nicht täuschen: Das Tool wird seit fünf Jahren gepflegt. ■

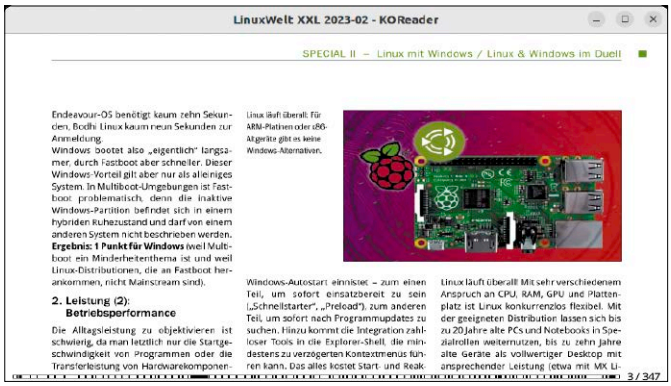


Nadel im Heuhaufen: Die Dateisuche Fsearch präsentiert Suchergebnisse dank dem zuvor erstellen Index augenblicklich.

Koreader 2022.10

Dokumentbetrachter für E-Books
https://koreader.rocks

Der Reader für E-Books ermöglicht komfortables Lesen von Dokumenten in den Formaten EPUB, PDF, HTML, DOCX, TXT. Die Oberfläche ist einfach und in hohen Kontrasten für E-Ink-Displays gehalten. Die Bedienelemente sind für Touchscreens geeignet und es gibt neben der Dokumentdarstellung einen Dateibrowser. Das Programm liegt für Linux, Android, Chrome-OS und Amazon Kindle vor. Für Ubuntu gibt es DEB-Pakete auf der Projektseite. ■

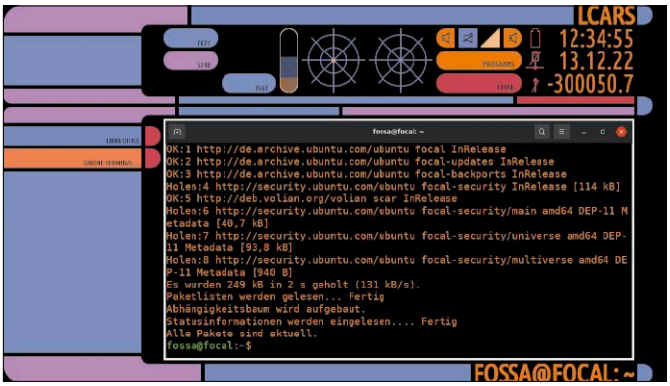


Lässiges Lesen: Koreader ist ein Dokumentbetrachter mit schlichtem Dateimanager für Linux und für Mobilgeräte mit Touch- und E-Ink-Display.

Lcars Desktop 22.1

Verspielte Desktopoberfläche für Star-Trek-Fans
https://lcarsde.github.io

Diese Desktopoberfläche will nicht mit Gnome, KDE und anderen Desktops konkurrieren, sondern die fiktive Oberfläche „Lcars" aus der Science-Fiction-Serie Star Trek abbilden. Mit Window-Manager, Anwendungsmenü und Statusleiste ist Lcars aber durchaus benutzbar und ein Hingucker etwa auf offenen Kiosk-Systemen. Für Arch Linux und Ubuntu gibt es fertige inoffizielle Pakete. Ein Anmeldemanager wie GDM (Gnome) oder SDDM (KDE) wird vorausgesetzt. ■

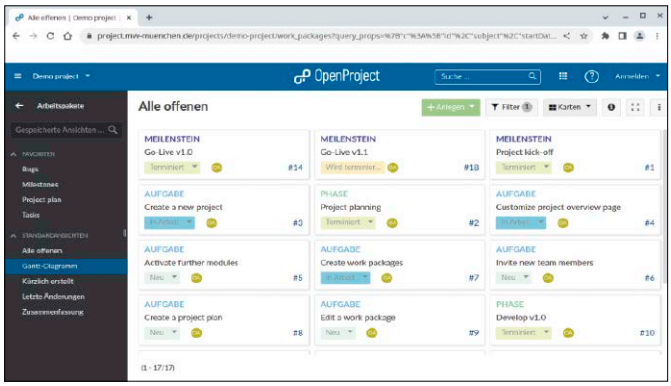


Faszinierend für Star-Trek-Fans: Lcars Desktop ist ein Nachbau der Oberfläche des Schiffscomputers der USS Enterprise.

Openproject 12.4

Servergestützte Projektverwaltung im Stil von Atlassian Jira
www.openproject.org

Das Open-Source-Programm bietet im Browser alle Tools zur Organisation von Softwareprojekten. Openproject steht in einer Community-Edition für das Hosting auf dem eigenen Server bereit. Version 12.4 hat eine Zwei-Faktor-Authentifizierung erhalten und für das Dateimanagement kann Nextcloud dienen. Eine Demo der Enterprise-Edition gibt es auf der Webseite. Pakete der freien Community-Edition liegen unter *www.openproject.org/download-and-installation*.

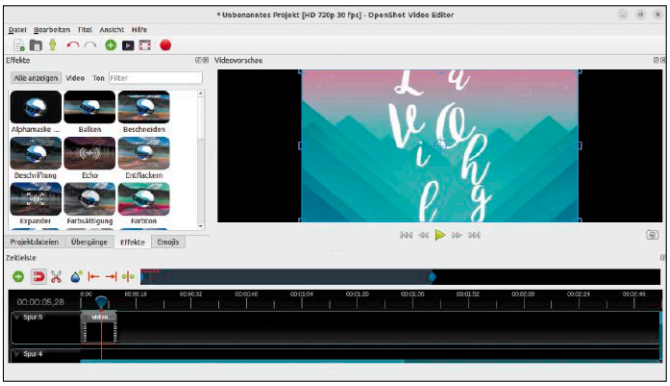


Openproject ausprobiert: Die kostenpflichtige Enterprise-Edition kann 14 Tage lang getestet werden. Die Community-Ausgabe ist kostenlos.

Openshot 3.0

Videoeditor mit intuitiven Bedienelementen
www.openshot.org

Unter den Videoeditoren für Linux hält Openshot einsteigerfreundliche Balance zwischen Funktionsumfang und Bedienkomfort – kein Profitool, aber gut genug für Videos aus mehreren Ausgangsclips, die an einer Zeitachse ausgerichtet und über Keyframes und Effekte überblendet werden. Version 3.0 wandert in die Paketquellen der kommenden Distributionen und steht auf *https://github.com/OpenShot/openshot-qt/releases* schon als Appimage bereit.

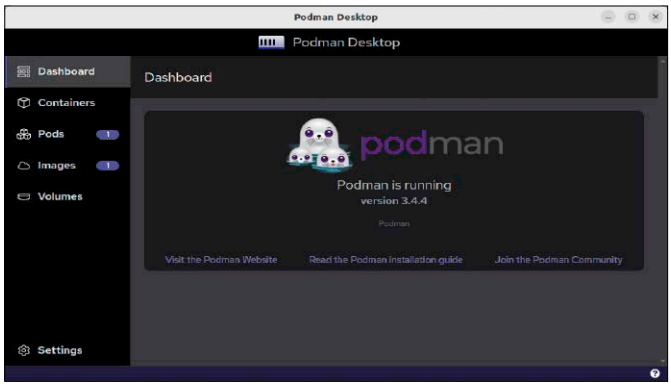


Schneiden ohne Leiden: Openshot ist ein guter Einstieg in den nicht-linearen Videoschnitt, verlangt aber leistungsfähige Hardware.

Podman Desktop 0.10

Grafische Verwaltungsoberfläche für Podman-Container
https://podman-desktop.io

Podman packt Linux-Anwendungen in abgeschottete Container und gilt als designierter Nachfolger der Docker-Runtime. Mit Podman Desktop gibt es nun auch für diese Containertechnik unter Linux ein grafisches Werkzeug für Anwender, die Container nicht in der Kommandozeile verwalten wollen. Podman Desktop ist noch kaum ein Jahr alt, doch die Entwicklungsgeschwindigkeit ist hoch. Es gibt bereits ein Flatpak-Paket für alle Linux-Distributionen.

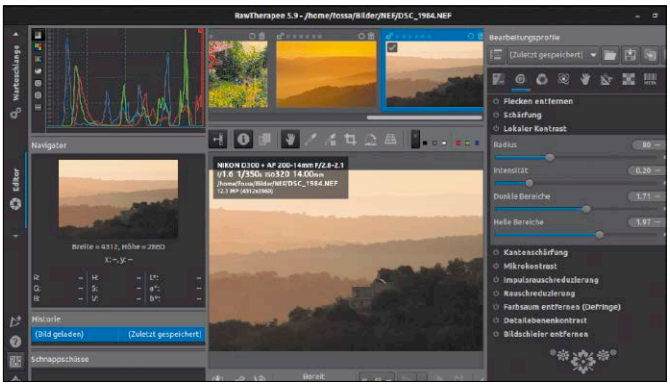


Container konstruieren: Podman Desktop liefert eine Administrationsoberfläche für laufende Podman-Container mit einer Ressourcenverwaltung.

Rawtherapee 5.9

Leuchttisch zur Umwandlung von RAW-Fotos
https://www.rawtherapee.com

Der RAW-Konverter ging zunächst als kommerzielles Programm an den Start, ist seit Version 3 aber Open Source. Im Funktionsumfang vergleichbar mit Darktable, macht Rawtherapee Einsteigern die ersten Schritte der RAW-Bearbeitung einfacher. Als neue Funktion gibt es unscharfe Auswahlbereiche, um Änderungen nur auf bestimmte Bildteile anzuwenden. Rawtherapee 5.9 ist schon in Fedora 37 verfügbar und kommt in die Paketquellen des nächsten Ubuntu.

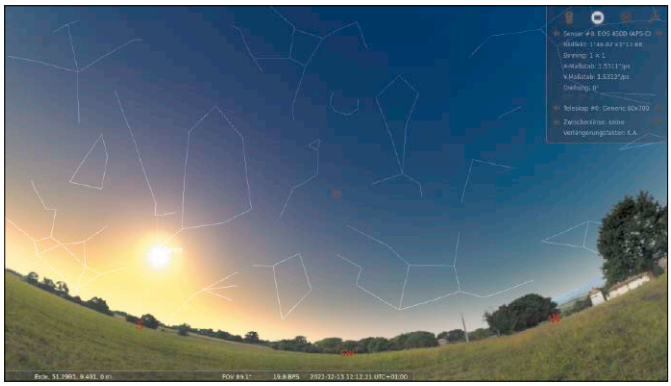


Lichtblick in der Dunkelkammer: Zu Bearbeitungsschritten kann Rawtherapee Sprungmarken als Undo-Funktion speichern.

Stellarium 1.1

Astronomieprogramm und digitales Planetarium
www.stellarium.org

Nach 20 Jahren Entwicklung hat Stellarium Ende 2022 die Versionsnummer 1.0 erreicht. Das Astronomieprogramm zur Bestimmung und Darstellung von Gestirnen hat einen spielerischen Ansatz: Wie ein Planetarium zeigt das freie Programm eine Darstellung des Himmels zu einer bestimmten Uhrzeit. Die Bibliothek umfasst neben Planeten 600 000 Sterne. Weitere 177 Millionen Objekte sind nachladbar. Stellarium liegt für Linux als Appimage vor. ■



Astronomisch: Stellarium zeigt mit Open GL eine Ansicht des Tages- und Nachthimmels von einem beliebigen Ort aus und mit einblendbaren Infos.

Super Tux Kart 1.4

Rennspiel mit Open-Source-Maskottchen
https://supertuxkart.net

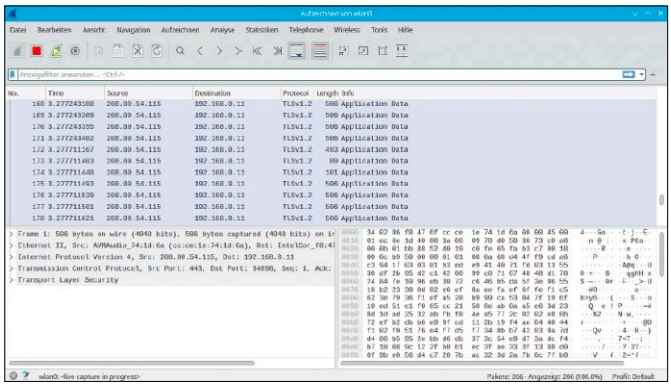
Das kurzweilige Rennen im Stil von Super Mario Kart mit Mehrspieler- und Onlinemodus legt im jährlichen Turnus frische Versionen vor. Super Tux Kart 1.4 hat Hi-DPI-Unterstützung für hohe Auflösungen. Eine optionale Vulkan-Schnittstelle liefert potenziell höhere Leistung als Open GL, um die Framerate auch auf schwächeren GPUs zu erhöhen. Die Webseite liefert fertige Binarys, das PPA *https://launchpad.net/~stk/+archive/ubuntu/dev* Pakete für Ubuntu. ■

Ohne Verkehrskontrolle: Super Tux Kart schickt Open-Source-Maskottchen wie Tux, Kiki und Konqi im Stil von Super Mario Cart ins Rennen.

Wireshark 4.0.4

Netzwerksniffer zur Paketanalyse
www.wireshark.org

Was sendet und empfängt ein Programm im LAN, im Internet, zu welchen Servern? Für die Analyse des eigenen Netzverkehrs und jenem anderer Geräte ist Wireshark seit Ende der 90er-Jahre das wichtigste Tool. Version 4 macht die Auswahl von Netzwerkschnittstellen einfacher und strukturiert die Ansicht- und Filteroptionen klarer. Für Linux gibt es Wireshark mit Oberflächen für GTK und Qt. In Fedora 27 liegt Version 4.0 bereits in den Standardquellen. ■

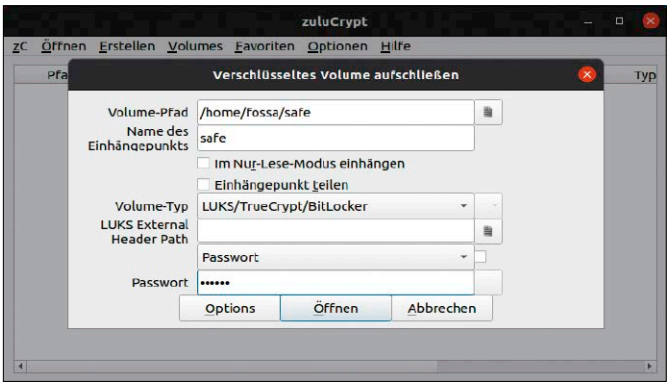


Verkehrskontrolle: Über einen manuell installierten, privaten Schlüssel kann Wireshark verschlüsselte Pakete anderer Rechner analysieren.

Zulucrypt 6.2

Erstellt und öffnet verschlüsselte Dateicontainer
http://mhogomchungu.github.io/zuluCrypt

Zulucrypt unterstützt als grafisches Front-End die Verschlüsselung einzelner Dateien, Dateicontainer und Partitionen. Auch mit der Linux-Verschlüsselung Luks2 (Linux Unified Key Setup) kann Zulucrypt 6.2 umgehen und vereinfacht über Menüs den Umgang mit Datenträgern und Containern. Zudem ist Zulucrypt kompatibel zu den Formaten von Veracrypt 1.2x und dem alten Truecrypt. Die Webseite bietet Binarys für Ubuntu, Debian, Fedora, Open Suse. ■



Vereinfachte Verschlüsselung: Zulucrypt versteht sich auf viele Formate und Verschlüsselungstechniken für Partitionen und Dateicontainer.

Troubleshooting für Raspberry Pi

Platinencomputer haben sich eine Fangemeinde erobert. Sie sind energieeffizient, vielseitig – aber nicht fehlerfrei. Dieser Artikel nennt die wichtigsten Troubleshooting-Maßnahmen für den Raspberry Pi, die aber analog auch für Odroid, Arduino oder Beagleboard gelten.

VON STEPHAN LAMPRECHT

Kompaktheit schützt vor Fehlern nicht: Natürlich können Ein-Platinen-Computer mal streiken und Probleme bereiten. Ein großer Vorteil gegenüber dem klassischen Desktop-PC oder Notebook ist zweifellos das Fehlen von mechanischen Bauteilen. Und gleich zwei Hauptprobleme lassen sich sehr einfach beheben. Was das Troubleshooting etwas erschwert, ist beim Raspberry Pi inzwischen die Modellvielfalt. Wir fokussieren uns hier auf die aktuelleren Modelle 3 und 4.

Ab ins Gehäuse damit!

Eine der besten Investitionen für Platinenrechner ist die Anschaffung eines soliden Gehäuses. Hier sparen Sie besser nicht am falschen Ende, sondern suchen nach einem Modell, das auch zum Einsatzzweck passt. Wenn der kleine Computer als Streaming-Maschine oder Dateiserver arbeiten muss, hat er ordentlich zu tun. Deswegen ist ein Gehäuse mit einem Kühlkörper für passive Kühlung oder einem aktiven Lüfter zu empfehlen. Letzterer kostet zwar etwas mehr Strom, verlängert aber das Leben. Das Gehäuse schützt zudem gegen Staub, der die Kühlung beeinträchtigt, und verhindert Kurzschlüsse, wenn Sie beim laufenden Rechner daran herumbasteln oder aus Versehen mit einem Leiter einen Kontakt berühren.

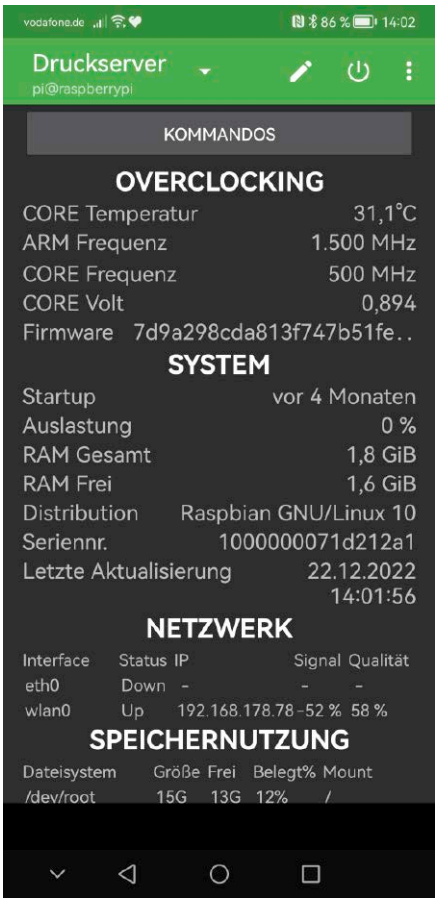
Sorgen Sie für solide Stromversorgung

Stürzt der Rechner während des Betriebs regelmäßig ab oder zeigen sich Artefakte oder bunte Streifen auf einem angeschlossenen Bildschirm, fällt der Verdacht schnell auf die eingesetzte Software. Nach unseren Erfahrungen resultieren die meisten Probleme aber schlicht aus einem unpassenden Netzadapter. Sie müssen nicht das offizielle Netzteil kaufen, sollten aber auf einen Netzadapter eines Markenherstellers zurückgreifen und auch ein hochwertiges USB-Kabel verwenden.

Probleme mit der Stromversorgung signalisiert der Computer auch bereits beim Start. Während dieser Prozedur benötigt er besonders viel Strom. Kommt es zu Engpässen, ist ein kleines buntes Quadrat auf dem angeschlossenen Bildschirm zu sehen. Erlischt die rote LED oder blinkt diese, dann ist die Spannungsversorgung nicht stabil. Haben Sie gerade kein besseres Netzteil zur Hand, dann versorgen Sie zumindest externe Verbraucher anderweitig mit Strom, um das Problem zu lösen.

Die Platine startet nicht?

Wenn der Minicomputer erstmals in Betrieb geht und nicht starten will, haben Sie vermutlich beim Aufspielen des Betriebssystems einen Fehler gemacht. Wenn Sie ein Programm wie den Pi Imager oder Etcher nutzen, sollten Sie stets die Funktion einsetzen, die nach dem Schreiben die Dateien noch einmal prüft. Lesen Sie die Speicherkarte in einen Leser auf einem anderen System ein und kontrollieren Sie, ob es darauf einen Ordner „boot“ gibt. Darin müssen sich unbedingt die Dateien „start.elf“ und „kernel.img“ befinden. Fehlen diese, spielen Sie das Betriebssystem erneut auf. Gibt es keine Auffälligkeiten, versuchen Sie es mit einer anderen Speicherkarte.



Behalten Sie das System im Blick: Wenn der Rasperry ohne Ein- und Ausgabegeräte „headless“ läuft, leistet die Android-App „Raspi Check“ gute Dienste.

Lief das System mit der SD-Karte bislang, wurde eventuell das Dateisystem oder eine der Startdateien beschädigt. Die einfachste Lösung: Übertragen Sie das System erneut und beginnen Sie mit einer frischen Installation. Um sich die Mühe der Neueinrichtung künftig zu ersparen, legen Sie nach

einer erfolgreichen Installation und einem Testlauf eine Kopie der Karte an:

```
sudo dd if=/dev/sdd
  of=~/raspberry-pi.img
```

Passen Sie den Gerätenamen an (hier „sdd“). Mit dem Kommando in umgekehrter Richtung spielen Sie die Sicherung später einfach wieder zurück.

Die Platine stürzt einfach ab?

Bei plötzlichen Abstürzen liegt der Verdacht nahe, dass die Software streikt. Gibt es in den Logdateien aber keine Auffälligkeiten und sind auch Probleme mit der Stromversorgung auszuschließen, können thermische Probleme oder eine Überlastung am USB-Anschluss eine Rolle spielen. Thermische Probleme ergeben sich immer dann, wenn Platinen in einem zu engen Gehäuse stecken, das zu wenig kühlt. Auch das Übertakten produziert viel Wärme. Vielleicht haben Sie Overclocking irgendwann aktiviert und vergessen, es wieder abzuschalten? Um den Raspberry Pi wieder mit der CPU-Frequenz bei Auslieferung zu betreiben, kontrollieren Sie beim Modell 3 oder 4, ob in der Datei „config.txt“ der Eintrag „arm_freq“ auskommentiert ist.

Ein anderer Grund für solche Probleme könnte mangelnder Arbeitsspeicher sein. So verbraucht etwa der USB-Treiber eine Menge RAM. Steht diese Schnittstelle unter hoher Last, kann dies dazu führen, dass dem System an anderer Stelle das RAM fehlt. In der Datei „/etc/sysctl.conf“ können Sie versuchen, den Wert unter „vm.min_free_kbytes“ höher anzusetzen.

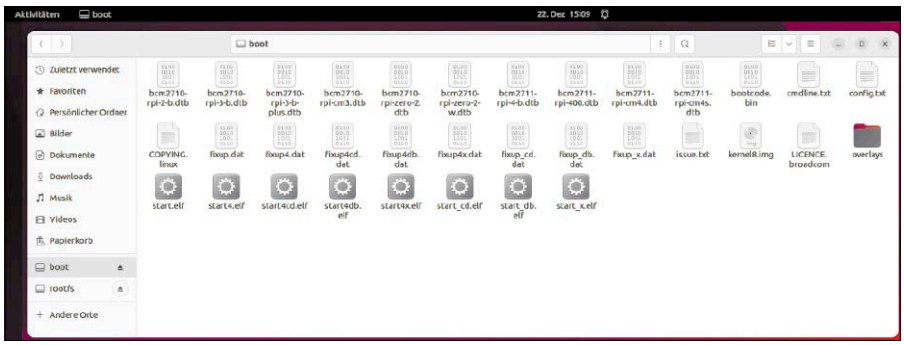
Falls das Problem weiter auftritt, könnte eine Änderung der Zeile

```
smsc95xx.turbo_mode=N
```

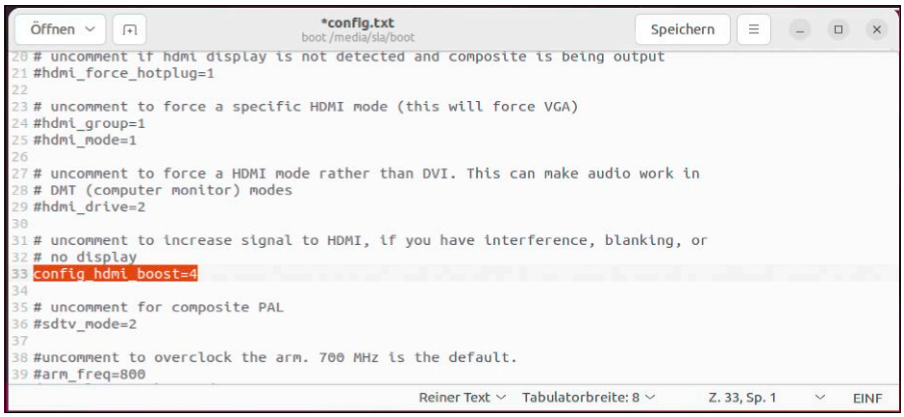
in der Datei „/boot/cmdline.txt“ zum Erfolg führen. Allerdings wird mit der Einstellung der Netzwerkdurchsatz heruntergeregelt. Sie erkaufen sich also höhere Stabilität mit geringer Netzwerkleistung.

Wenn der Bildschirm dunkel bleibt

Bleibt ein angeschlossener Monitor dunkel, während der Raspberry normal zu booten scheint, kontrollieren Sie die mechanische Kabelverbindung. Gerade bei den kleinen Micro-HDMI-Buchsen der jüngsten Raspberry-Generation kommt es manchmal zu so großem Zug, dass die Verbindung verloren geht. Außerdem könnten Sie versuchen, die zweite Buchse zu verwenden. Bringt das



Startet das System nicht mehr, dann kontrollieren Sie die SD-Karte auf die Existenz der wichtigen Startdateien.



Ein Texteditor genügt: Wie im Falle der Signalverstärkung am HDMI-Anschluss können Sie viel Feintuning in den Konfigurationsdateien erledigen.

nichts, ist etwas Handarbeit gefragt. Da der Pi ja kein Bios im üblichen Sinn besitzt, können Sie die Änderungen an den Einstellungsdateien vornehmen, an die Sie mit einem beliebigen Editor auf einem anderen System herankommen. Öffnen Sie die Datei „config.txt“ auf der Karte mit einem Texteditor Ihrer Wahl. Fügen Sie die Zeile

```
hdmi_safe=1
```

hinzu. Speichern Sie die Datei und legen Sie die Karte wieder ein. Versuchen Sie, das System mit dieser Einstellung zu starten.

Artefakte oder bunte Streifen auf dem Display?

Wenn sich auf dem Monitor in der rechten oberen Ecke bunte Pixel zeigen, ist das ein Signal für unzureichende Stromversorgung. Tauchen dagegen Schleier oder deutlich sichtbare Pixel auf, liegt das vermutlich an einem zu langen HDMI-Kabel. Denn was am Desktop-PC oder Notebook funktionieren mag, erzeugt beim Raspberry Pi zu viel Widerstand. Wenn Sie kein kürzeres HDMI-Kabel zur Hand haben, verstärken Sie das Signal mit den Einstellungen der „Systemsteuerung“. Öffnen Sie wieder die bereits erwähnte Datei „config.txt“ und ändern Sie den Wert von „config_hdmi_boost“. Erlaubt sind hier Werte zwischen 1 und 7. Probieren Sie zunächst einen mittleren Wert wie „4“. In den meisten Fällen bringt das schon Abhilfe.

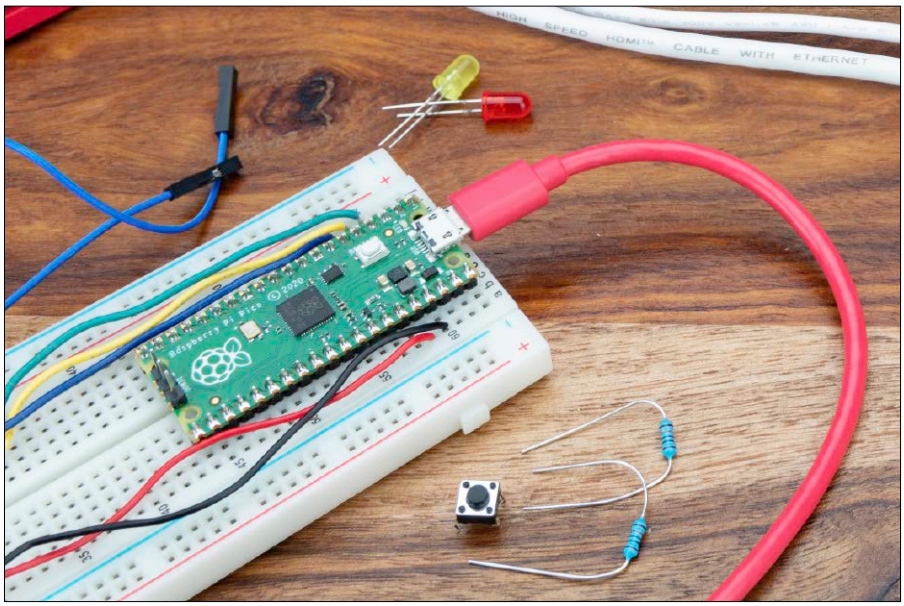
Anlaufstellen im Netz

Verständlicherweise mussten wir uns für diesen Artikel auf die häufigsten Fehlerquellen beschränken. Wenn Ihr Problem nicht aufgeführt war oder keine Lösung funktioniert hat, suchen Sie sich weitere Hilfe im Netz.

Rund um alle Raspberry-Modelle bietet die offizielle Dokumentation unter *www.raspberrypi.com/documentation* umfangreiches Material. Dort finden Sie beispielsweise auch eine Tabelle, welche die Bedeutung der verschiedenen Arten des Blinkens der LED erklärt. Außerdem finden Sie eine vollständige Referenz aller Kommandos in den Konfigurationsdateien. Noch mehr Hintergrundmaterial und insbesondere die Auflistung von Problemen anderer Nutzer (in englischer Sprache) bietet das Wiki von elinux.org (*https://elinux.org/Main_Page*). Dort finden auch Nutzer anderer Platinen Hilfestellungen und Tipps. ■

Alle Modelle des Raspberry Pi

Vor zehn Jahren kam nach mehreren Jahren Entwicklungsarbeit das erste Modell des Raspberry Pi heraus. Und der hat seitdem eine Erfolgsgeschichte hingelegt. Wir schauen auf Entwicklung zurück.



VON STEPHAN LAMPRECHT

Zufällig zum Redaktionsschluss dieser Ausgabe hat die Raspberry Pi Foundation die Frage beantwortet, wann der nächste Raspberry Pi kommen soll. Ambitionierte Bastler müssen tapfer sein: Die fünfte Version wird es wohl erst 2024 geben. Die Nachfrage ist ungebrochen, dabei war der frühe Raspberry Pi längst nicht der erste Platinencomputer. Während aber über den Arduino allenfalls Maker-Magazine berichteten, gab der Raspberry Pi der gesamten Kategorie einen regelrechten Schub. Das ist das große Verdienst, denn plötzlich waren die Platinen „schick". Das dürfte auch am Gesamtkonzept aus Marketing (Logo, Dokumentation) und der frühen Unterstützung durch ein gutes Betriebssystem gelegen haben.

Die Baureihen des Raspberry Pi

Bei einem vollständigen Rückblick darf die Unterscheidung der verschiedenen Baureihen nicht fehlen. Es wäre überraschend, wenn die Entwicklungsgeschichte völlig linear verlaufen wäre. Auch die Raspberry Pi Foundation hat den einen oder anderen Haken geschlagen. Dazu gehören die Modelle „Zero" und „Pico", die nur in industriellen Anwendungen und ausgesprochenen Bastlerkreisen eine Rolle spielen. Der Zero besitzt als Formfaktor die Abmessungen des Arduino und kommt in der aktuellen Version „Zero 2 W" mit einem Quadcore 64 Bit ARM Cortex-A53 Prozessor, der mit einem GHz getaktet ist und immerhin 512 MB SD-RAM mitbringt. Erstmals kam ein Zero im November 2015 auf den Markt – zum Kampfpreis von fünf Dollar. Ebenfalls winzig ist die Pico-Serie, die für den Einbau in Geräten gedacht ist und damit auf Anschlussmöglichkeiten wie die GPIO-Pins verzichten muss. Aktuell ist ein Modell (RP2040) mit einem Dualcore Arm Cortex-M0+ Prozessor und mit nur 264 KB RAM.

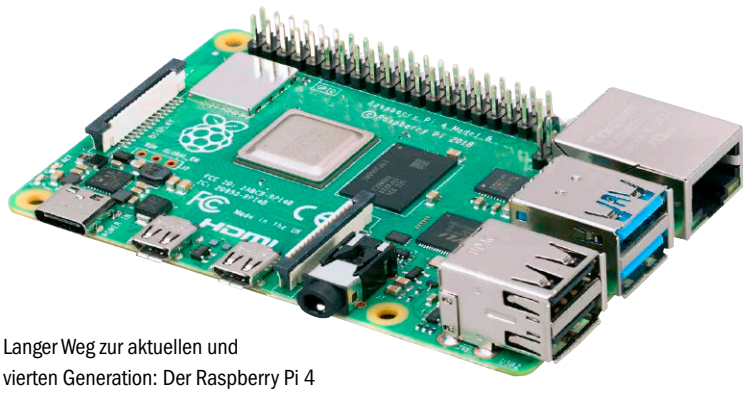
Modell B und B+

Die Baureihe, mit der die meisten Nutzerinnen und Nutzer erste Erfahrungen gesammelt haben werden, dürften die B-Modelle sein. Zwischenzeitlich tauchten auch immer mal wieder Raspberry-Modelle A ohne Netzadapter auf, die als Budgetvariante der korrespondierenden Geräte „Modell B" positioniert wurden. Unsere Empfehlung lautete stets, doch gleich zu „B" zu greifen. Der Raspberry Pi 1 Model B war auch das erste Modell, das 2012 im Handel erhältlich war. Zunächst mit 256 MB RAM, später dann mit 512 MB. Es bot bereits die GPIO-Leiste, Fast Ethernet, zwei USB-Buchsen, HDMI sowie eine 3,5-mm-Audio-Klinke. Ein ARM11-Chip (ARMv6) mit 700 MHz bildet das Herz der Maschine. Ihm folgte das Modell B+, das als zukünftige Referenz dienen sollte. 40 Pins bei der GPIO-Leiste, vier USB-Anschlüsse und der Wechsel auf Micro-SD-Karten prägten die Gerätegeneration.

Immer schneller, immer weiter …

Mit dem Raspberry Pi 2 Modell B wurde die Platine erwachsen. Denn die ARMv7-Architektur erweiterte die Einsatzmöglichkeiten des kleinen Computers deutlich. Damit konnten für ARM optimierte Versionen von Ubuntu und sogar Windows auf dem kleinen Rechner eingesetzt werden. Der Arbeitsspeicher hatte sich verdoppelt und das Herzstück wurde durch den

Den Raspberry Pi gibt es in diversen Ausprägungen. Besonders kompakt ist die Zero-Variante, die für industrielle Anwendungen konzipiert wurde.



Langer Weg zur aktuellen und vierten Generation: Der Raspberry Pi 4 liefert genügend Rechenpower und schnelle Schnittstellen für Serveranwendungen.

Broadcom BCM2836 mit 900MHz Quadcore Cortex-A7 gebildet.

Anfang 2016 kam dann der Pi 3 Model B. Damit unterstrichen die Entwickler erstmals den Anspruch, die Basis für einen Desktopersatz zu bauen. Denn die Platine machte Dongles für Bluetooth und WLAN überflüssig. Bluetooth 4.1 und WLAN 802.11n hielten Einzug. Das brachte aber auch einen Nachteil mit sich. So manches Gehäuse aus Metall kühlte zwar die Platine ordentlich, schirmte indes aber auch die Funksignale zu stark ab.

Prozessor war der Quadcore 1,2 GHz Broadcom BCM2837. Die via Micro-USB realisierte Stromversorgung wurde auf 2,5 A hochgeschraubt. Und dann fanden noch zwei weitere Schnittstellen auf der Platine Platz – der CSI-Port zum Anschluss an die offizielle Kamera und ein DSI-Anschluss, um die ersten Touchscreens zu verbinden. Nörgler warfen der Platine die immer noch recht lahme Ethernet-Schnittstelle vor. Der unmittelbare Nachfolger 2018, der Pi 3 Model B+, versuchte das auszugleichen: Die Ethernet-Schnittstelle konnte jetzt zwar theoretisch ein Gigabit, wurde aber über USB 2.0 auf 300 Mbps ausgebremst. Verwendet wurde nun ein Broadcom BCM2837B0, Cortex-A53 (ARMv8) mit 1,4 GHz. Der WLAN-Chip sprach indes 2,4 und fünf GHz. Zudem brachte die Platine auch die Möglichkeit für Power-over-Ethernet, was aber ein Extra-HAT-Board erforderte.

Pi 4 Model B – neuester Stand der Technik

Anfang 2019 erscheint mit dem Pi 4 der immer noch aktuelle Vertreter des Modells B. Die Platine erhielt ein neues Layout. Somit sind Gehäuse für die vorherigen Generationen gar nicht oder nur mit Umbauten kompatibel. Beim Arbeitsspeicher wurde auf LPDDR2-RAM gewechselt und erstmals hatten die Nutzer die Wahl zwischen einem, zwei oder vier GB RAM (seit 2020 sogar acht GB). Es gibt vier USB-Anschlüsse, davon zwei nach dem schnelleren Übertragungsstandard USB 3.0. Die Stromversorgung erfolgt über einen USB-C-Anschluss. Um die Tauglichkeit auf dem Desktop zu unterstreichen, unterstützen die beiden Micro-HDMI-Ports zwei 4K-Displays. Der Prozessor kann bei der Nutzung eines Anschlusses 4K-Inhalte mit 60 Bildern pro Sekunde liefern. Bei der Nutzung beider Ports halbiert sich die Framerate allerdings.

Die Ethernet-Schnittstelle liefert jetzt tatsächlich Gigabit-Durchsatz. Die CPU ist ein Broadcom BCM2711, Quadcore Cortex-A72 (ARM v8), der mit 1,5 GHz getaktet ist. Weiterhin dabei sind die Anschlussleisten für Touchdisplay und die offizielle Kamera. Vom Vorgänger behalten wurde der Micro-SD-Slot, der ohne Mechanik auskommt. Die Karten werden einfach eingeschoben. Bluetooth wurde auf den Standard 5 gehoben und für stabiles Arbeiten sollte ein Netzteil jetzt 3 A bei 5 V liefern.

Mehr Leistung produziert aber auch mehr Wärme. Wenn diese Platine überhaupt eine „Schwäche" hat, dann die deutlich wahrnehmbare Wärmeentwicklung unter Last. Wer den Computer gegen äußere Einflüsse schützen will, kommt um größere Kühlkörper oder aktive Luftkühlung nicht herum.

Mit dem Modell 4 besitzt der Pi so viel Rechenpower, dass damit sowohl die ARM-Version von Windows 10 oder eine kleine Arbeitsgruppe via Nextcloud versorgt werden kann.

Raspberry Pi 400: Return of the „Brotkasten"

Wer seine Kindheit in den 80er-Jahren verbracht hat, dürfte mit hoher Wahrscheinlichkeit seine ersten Schritte auf einem Commodore C64 unternommen haben – wegen seines kantigen Designs oft „Brotkasten" genannt. Seit rund zwei Jahren erlebt diese Idee mit dem Raspberry Pi 400 ein Revival. In einem kompakten Gehäuse vereint er die Platine und eine Tastatur. In Form eines Kits liegen dann auch noch Maus, Netzteil und HDMI-Kabel dabei. Lediglich ein Monitor ist noch nötig.

Für rund 100 Euro stecken in dem knapp 400 Gramm schweren Rechner ein Broadcom BCM2711 Cortex-A72 (ARM v8, mit vier Kernen, 64 Bit) mit 1,8 GHz und vier GB LP-DDR4-RAM. Ein Gigabit-LAN-Anschluss, WLAN-AC und Bluetooth 5.0 stellen die Verbindung zur Außenwelt her und dank zweier Anschlüsse nach USB 3.0 lassen sich auch externe Geräte gut verbinden. Clever, dass auch auf die GPIO-Pins nicht verzichtet werden muss. Wie unser Selbstversuch gezeigt hatte, macht das Konzept nicht nur Spaß, sondern eignet sich als Desktopersatz. ■

Das Konzept ist seit den 80er-Jahren bekannt – einfach einen Monitor anschließen und loslegen. Das geht mit dem Raspberry 400 Kit.

Werbefrei dank Adguard & Raspberry

Wer einen Werbeblocker benutzt, ist überrascht, wie schnell sich die Seiten im Browser ohne Werbebanner aufbauen. Mit der Software Adguard und einem Raspberry Pi sparen Sie sich die Mühe, Werbeblocker auf einzelnen Systemen zu installieren.

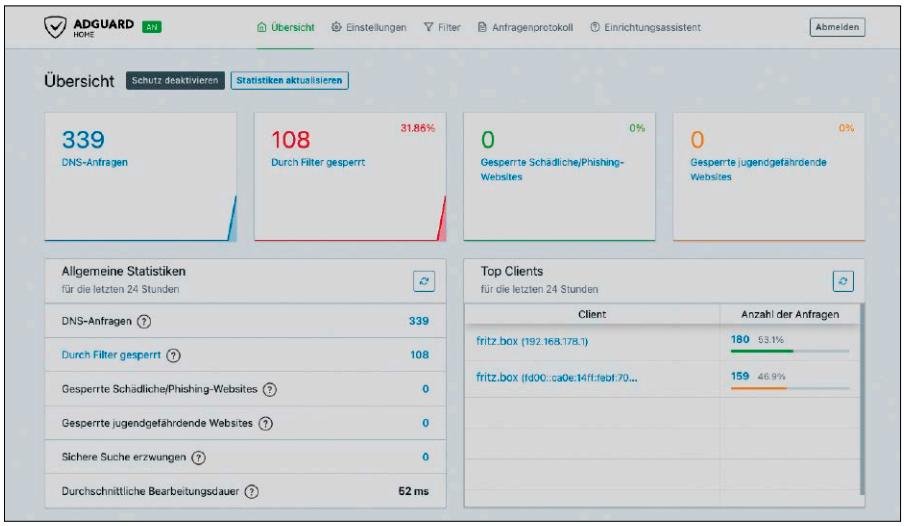
VON STEPHAN LAMPRECHT

Das Angebot an Werbeblockern als Erweiterung für den Browser ist riesig. Der Nachteil lokal installierter Programme wie Adblocker liegt auf der Hand. Sie müssen diese auf jedem Rechner installieren. Mit einer zentralen Lösung im Heimnetz sparen Sie sich diese Mühe. Dann müssen die Einstellungen nur an einer Stelle vornehmen und surfen mit allen Geräten viel schneller. Genau das erreichen Sie mit Adguard, das Sie ressourcenschonend auf einem Raspberry Pi installieren.

Der Raspberry vorbereiten

Wenn noch kein Betriebssystem auf dem Raspberry läuft, erledigen Sie dies am besten mit dem offiziellen Pi Imager (*www.raspberrypi.com/software*). Der bietet den Charme, dass Sie gleich ein anderes Passwort für den Nutzer „pi“ vergeben, den SSH-Zugang installieren und praktischerweise auch einen (Host-)Namen zuweisen können, was alle weiteren Schritte erleichtert. Da sich der kleine Computer nur um den Netzwerkverkehr kümmern soll, kann auch die Lite-Variante genutzt werden. Entscheiden Sie sich also bei „OS wählen“ für den Eintrag „Raspberry Pi OS (other)“ und „Pi OS Lite“.

Nach einem Klick auf das Zahnrad gibt es die erweiterten Optionen. Hier aktivieren Sie den SSH-Zugang, vergeben den Hostnamen und ein Passwort für den Nutzer „pi“. Verbindet sich der Pi via WLAN, können Sie auch gleich das Netzwerk einrichten. Deaktivieren Sie den Punkt „Telemetry“, sofern dieser angeschaltet ist.



Nun schreiben Sie das Betriebssystem auf die SD-Karte und starten den Raspberry damit. Für den nächsten Arbeitsschritt benötigen Sie die IP-Adresse des Raspi. Die finden Sie im Heimrouter heraus – bei einer Fritzbox unter „Heimnetz → Netzwerk“. Dank des bereits vergebenen Hostnamens ist das Gerät leicht zu identifizieren.

Adguard installieren und aufrufen

Öffnen Sie auf einem anderen Rechner im Heimnetz ein Terminal und geben Sie dort

```
ssh pi@[IP-Adresse]
```

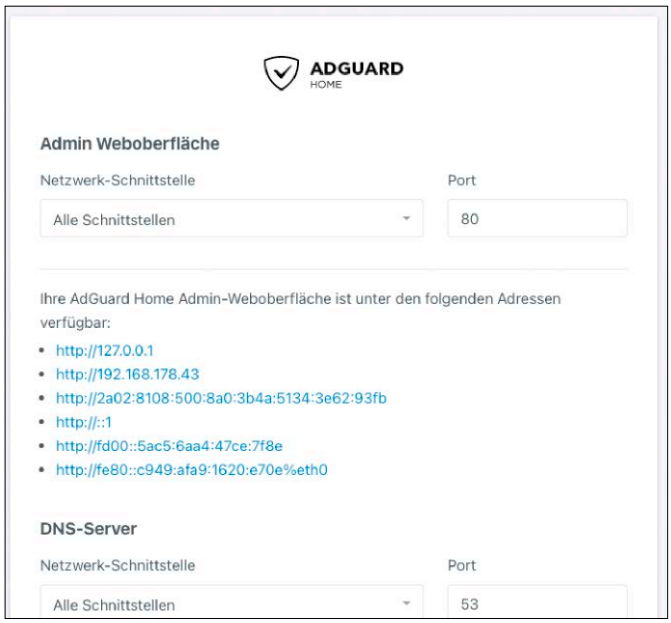
ein. Sie müssen jetzt den öffentlichen Schlüssel des Systems akzeptieren und mit „yes“ fortfahren. Außerdem werden Sie zur Eingabe des Passworts für den Benutzer „pi“ aufgefordert. Danach laden Sie das aktuelle Release von Adguard per Terminalbefehl herunter (eine Zeile):

```
wget https://github.com/
  AdguardTeam/AdGuardHome/
  releases/download/v0.107.21/
  AdGuardHome_linux_armv7.tar.gz
```

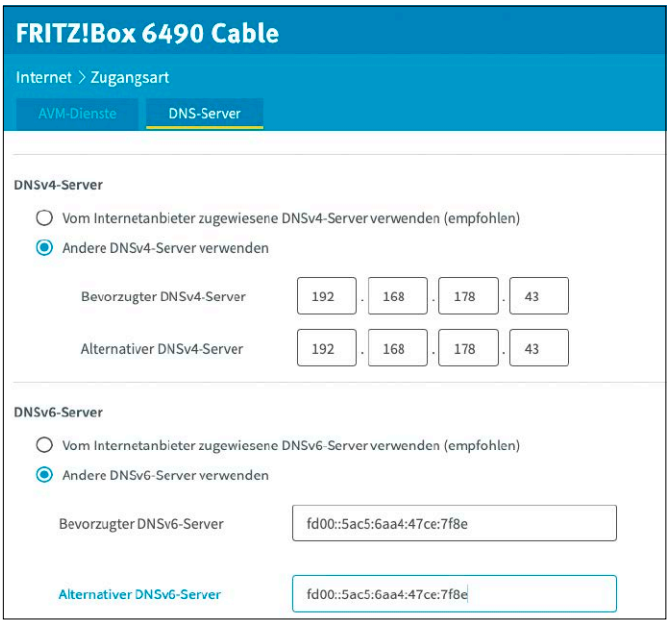
Besuchen Sie die Adresse zur Sicherheit vorher mit dem Browser, um festzustellen, ob es inzwischen eine neuere Version gab. Die eigentliche Installation erfolgt in drei kurzen Schritten. Sie entpacken das Archiv, wechseln in dessen Verzeichnis und starten die Installation:

```
sudo tar xvf AdGuardHome_linux_
  armv7.tar.gz
cd AdGuardHome
sudo ./AdGuardHome -s install
```

Meldet das System, dass der Dienst erfolgreich gestartet wurde, können Sie die SSH-Verbindung verlassen und die weitere Einrichtung im Browser erledigen. Dazu verwenden Sie die Adresse „http://[IP-Adresse]:3000“. Im ersten Dialog sollten Sie unter „Netzwerk-Schnittstelle“ aus Sicherheits-



Adguard ist einfach zu installieren. Sie müssen nur festlegen, welche Netzwerkschnittstelle überwacht werden soll. Alle weiteren Informationen blendet das System ein.



Einstellung im Heimrouter (hier Fritzbox): Damit die Clients im Netzwerk den zentralen Filter nutzen, muss Adguard als DNS-Server eingetragen werden.

gründen nur die dem Raspberry Pi zugewiesene IP-Adresse selektieren. Unter „DNS-Server" gilt das ebenso, es sei denn, es gibt auch noch eingerichtete Gastnetze. Im nächsten Schritt richten Sie den Benutzer für die Administration ein. Danach blendet Adguard die wichtige Information zur Konfiguration des Heimrouters ein. Diese Information finden Sie aber auch jederzeit später, indem Sie den „Einrichtungsassistent" ausführen.

Heimrouter konfigurieren

Sofern Sie selbst keinen Änderungen vorgenommen haben, ist das Heimnetz vermutlich so konfiguriert, dass der Router als DHCP-Server automatisch für die Vergabe von IP-Adressen an die Endgeräte sorgt. Dabei teilt er den Geräten auch mit, welcher Server sich um die Namensauflösung (DNS) kümmern soll. Hier setzt Adguard an, denn statt des DNS-Servers des Providers nutzen Sie fortan Adguard mit seinen Filtern auf dem Raspberry Pi.

Bei einer Fritzbox schalten Sie die „Erweiterte Ansicht" an und finden unter „Internet, Zugangsart" den Eintrag „DNS-Server". Dort tragen Sie die von Adguard angezeigten Werte unter „Andere DNSv4-Server" sowie „Andere DNSv6-Server" ein. Bei anderen Routern ist die Vorgehensweise ähnlich. Besonderheit bei der Fritzbox ist die Bestätigung der Änderung direkt am Gerät oder angeschlossenen Telefon.

Sobald Sie den DNS-Server im Heimrouter geändert haben, sollten Sie bereits werbefrei surfen. Adguard verlässt sich hier auf eine zentral von den Entwicklern gepflegte Liste, die in regelmäßigen Abständen aktualisiert wird. Wie viele DNS-Abfragen zu Werbe- und Trackingservern bereits unterbunden sind, zeigt das Dashboard des Systems an. Sie können übrigens über „Einstellungen → Client Einstellungen" auch einzelne Clients im Netzwerk von der Filterung ausnehmen. Generell lohnt es sich, sich mit Hilfe des Wikis (*https://github.com/AdguardTeam/AdGuardHome/wiki*) eingehender mit dem System zu beschäftigen. Dort wird auch erklärt, wie Sie eigene Filterregeln definieren.

Da in diesem Beispiel alle Anfragen aller Clients via Fritzbox Adguard erreichen, müssen Sie noch eine Bremse lösen. Unter „Einstellungen → DNS-Einstellungen" finden Sie im unteren Teil einen „Begrenzungswert" für die Anfragen pro Sekunde. Bei der Vorgabe „20" kann es für ein gut ausgestattetes Heimnetz schon einmal eng werden. Setzen Sie den Wert auf „0".

Adguard ist schnell installiert und arbeitet zuverlässig. Das trifft auch für den Fall zu, dass Sie doch einmal beim Surfen auf Werbung stoßen. Kein Filter arbeitet perfekt. Bevor Sie sich die Arbeit machen, den Filter manuell anzupassen, nehmen Sie die Ausnahme besser hin und freuen sich über täglich wachsende Zahlen geblockter Abfragen.

Adguard als Kindersicherung

Adguard kann weitere Aufgaben übernehmen: In den „Allgemeinen Einstellungen" kann der Webservice für die Kindersicherung aktiviert werden. Für die Abfrage der aufgerufenen Seiten wird der gleiche Mechanismus wie für Werbung verwendet. Ebenfalls elegant ist das Sperren von Diensten und Anwendungen. Wenn Sie etwa verhindern wollen, dass der Nachwuchs zu viel Zeit mit Spotify, Deezer, Tiktok oder Discord verbringt, ist auch das möglich. Dazu verwenden Sie das Menü „Filter" und anschließend „Gesperrte Dienste".

Insgesamt 43 Elemente stehen zur Wahl, deren Sperrung Sie mit einem Mausklick einrichten.

Troubleshooting für IPv6

Die Welt von IPv6 ist leider etwas komplizierter als das alte Protokoll. Denn die IPv6-Adresse von Adguard, die Sie in der Fritzbox als DNS eingetragen haben, kann sich verändern. Wird dieses „Präfix" vom Provider verändert, erhält der Raspberry Pi eine andere IPv6-Adresse. Das lässt sich in der Fritzbox verhindern, jedoch sind die Optionen etwas versteckt. Im Fenster „Heimnetz → Netzwerk → Netzwerkeinstellungen" klicken Sie auf „IPv6-Einstellungen". Hier aktivieren Sie die Option „Unique Local Addresses (ULA) immer zuweisen" und bestätigen die Einstellung. Damit ist auch dieses Problem gelöst. ■

E-Book-Server Calibre

Wer jenseits von Shop- und Verlagsgrenzen Ordnung in seine E-Books bringen will, kommt um Calibre nicht herum. Eher wenig bekannt ist, dass die Software einen Servermodus besitzt, um Sammlungen zentral im Netzwerk anzubieten.

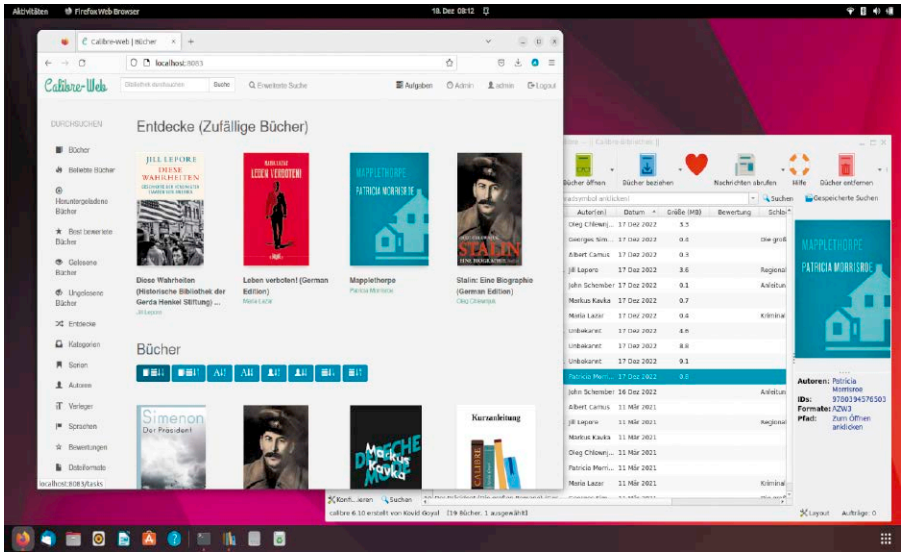
VON STEPHAN LAMPRECHT

Calibre gilt als eines der besten Werkzeuge rund um das Thema E-Books. Überwiegend wird Calibre als lokale Software genutzt, es enthält aber auch eine Serverfunktion. Mit etwas Bastelarbeit ist es sogar möglich, den zähen Kopierschutz von Amazon-E-Books so zu verändern, dass die Inhalte auch auf Nicht-Kindle-Geräten gelesen werden können. Darum soll es hier aber nicht gehen.

Calibre besitzt eine Netzfreigabe

Über die Calibre-Oberfläche können Sie eine Serverfunktion starten, die den Zugriff auf die gesamte Bibliothek über das heimische Netzwerk anbietet. Die verbundenen Geräte können anschließend Titel herunterladen oder auch direkt im Browser lesen. Um diesen eingebauten Server zu starten, rufen Sie die Einstellungen von Calibre auf. Sie finden unter „Versand“ den Eintrag „Netzwerkserver“. Im Hauptregister starten Sie den Server manuell und legen optional fest, dass dieser stets automatisch mit Calibre startet.

Sobald Sie den Server gestartet haben, zeigt das Programm im unteren Teil des Fensters an, über welche IP-Adresse und Port es die Inhalte zur Verfügung stellt. Der Aufruf erfolgt von jedem beliebigen System im heimischen Netz im Browser über die Adresse „http://[IP-Adresse]:8080“. „8080“ ist der Standardport, sofern Sie keine abweichende Portnummer festlegen. Grundsätzlich ist es wie bei allen Anwendungen im heimischen Netz ein Vorteil, wenn Sie dem Calibre-Server eine statische IP-Adresse in der Konfigurationsoberfläche des Routers zuweisen. Dann können Sie sich ein Lesezeichen für den schnelleren Zugriff einrichten. Um den Zugriff zu beschränken, kann auch eine Authentifizierung via Benutzernamen und Passwort gefordert werden. Die entsprechende Option finden Sie ebenfalls in diesem Register. Dann dürfen Sie allerdings nicht vergessen, im Register „Benutzerkonten“ mindestens ein solches Konto zu hinterlegen.



Der Calibre-Server präsentiert Ihre Buchsammlung übersichtlich und attraktiv im Browser. Die E-Books lassen sich herunterladen oder direkt im Browser lesen.

Bedienung im Headlessmodus

Die grundlegenden Arbeiten an der Bibliothek wie die Titelrecherche und die Einrichtung des Programms erledigen Sie am besten mittels der grafischen Benutzeroberfläche von Calibre. Die Serverkomponente kennt aber eine ganze Reihe von Kommandos für das Terminal, die eine vollständige Verwaltung des Bücherservers per SSH ermöglichen. Dabei lassen sich auch neue Inhalte in der Bibliothek hinterlegen. Um den Server von der Kommandozeile aus zu starten, genügt dieses Kommando:

```
calibre-server [PFAD-DER-
  DATENBANK]
```

Liegt die Calibre-Datenbank standardmäßig im Home-Verzeichnis des Benutzers, führt also das Kommando (Beispiel)

```
calibre-server /home/sla/Calibre-
  Bibliothek
```

zum Erfolg. Das Kommando entspricht somit dem Start des Servers in den Einstellungen der Software selbst. Nach dem Kommando zeigt die App dann auch gleich die IP-Adresse und den Port an, über den Sie von einem externen Rechner auf die Bibliothek zugreifen dürfen. Führen Sie den Aufruf des Servers mit dem Schalter „-- help“ aus, überrascht Sie Calibre damit, dass Sie prinzipiell alle Optionen, die die Oberfläche in den Einstellungen sammelt, auch direkt via Terminal erledigen könnten – inklusive des Benutzermanagements.

Während das Unterprogramm calibre-server die Optionen der Serverkomponente steuert, ist für die Pflege der Bibliothek und der Datenbank ein anderes Programm mit dem Namen calibredb zuständig. Über Schalter und Optionen steht ein umfangreiches Funktionsset zur Verfügung, mit dem sich alle grundlegenden Arbeiten an der Datenbank erledigen lassen. „calibredb

--help" zeigt alle Kommandos, Hilfe zu einzelnen Kommandos rufen Sie mit „calibredb [Befehl] --help" auf. Möchten Sie etwa die in einem Verzeichnis liegenden E-Books der Calibre-Datenbank hinzufügen, funktioniert das über diesen Befehl:

```
calibredb add --r [PFAD]
```

Mit Schalter „--r" oder „--recurse" berücksichtigt Calibre alle Unterverzeichnisse im angegebenen Pfad. Es ist dabei sogar möglich, die Auswahl auf bestimmte Dateimuster zu beschränken. Das ist etwa praktisch, wenn im Importordner die PDF-Dateien verschiedener Zeitschriften liegen, Sie aber nur die Ausgaben eines Titels in Calibre importieren wollen.

Calibre-Web als Alternative

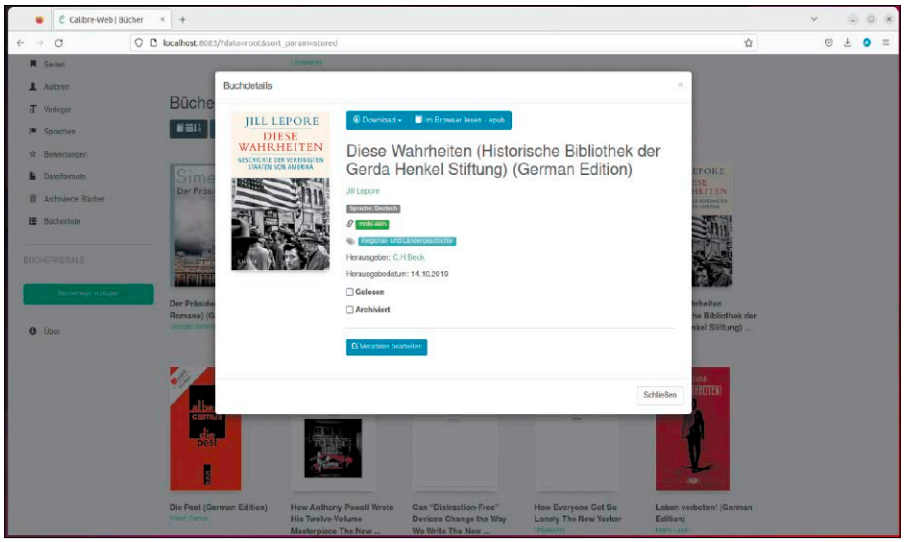
Mit Calibre-Web (*https://github.com/janeczku/calibre-web*) gibt es recht eine ansehnliche und funktionsreiche Alternative zur offiziellen Serverfreigabe des Hauptprogramms. Letztlich ist es aber eine Frage des Geschmacks, ob Sie dem Originalserver oder Calibre-Web den Vorzug geben. Die Installation von Calibre-Web verläuft über den Paketmanager von Python. Mittels

```
pip install calibreweb
```

beginnen Sie die Installation und Einrichtung. Quittiert das System den Programmaufruf mit einem Fehler, müssen Sie vermutlich erst Pip installieren (*sudo apt install python3-pip*). Das Script lädt alle Programmbestandteile und Abhängigkeiten für den Webserver herunter. Am einfachsten ist der Funktionsaufruf, wenn Sie nach der Installation in das Verzeichnis „.local/bin" in Ihrem Home-Verzeichnis wechseln und dort das Script „cps" aufrufen. Das Script macht keinerlei direkte Rückmeldung, aber binnen weniger Augenblicke können Sie mit einem Browser am System mittels „localhost" an einem anderen Rechner über die IP-Adresse die Oberfläche erreichen. Standardport ist „8083", also insgesamt etwa „http://192.168.178.113:8083".

Sie müssen sich als „admin" und Kennwort „admin123" anmelden. Damit die Bücher auch abgerufen werden können, teilen Sie direkt auf der Startseite der Software erst einmal den Speicherort der Calibre-Bibliothek mit. Das ist das Verzeichnis, in dem sich die Datei „metadata.db" befindet. Sobald Calibre-Web den Ort der Datenbank kennt, präsentiert es Ihnen die Bücher in übersichtlicher Form. Klicken Sie dann am besten auf den Nutzernamen „admin" in der oberen Navigation, um das voreingestellte Passwort zu verändern.

In den Einstellungen von Calibre finden Sie die Option, um den integrierten Server zu starten. Hier erfahren Sie anschließend auch die Zugriffsadresse.



Über die Detailansicht eines Titels in Calibre-Web organisieren Sie Ihre Lieblingstitel etwa in Form von „Regalen".

Nach dem Klick auf einen Titel stehen Ihnen die gleichen Optionen zur Verfügung, die auch Calibre selbst bietet. Sie laden sich das Buch lokal herunter oder lesen es direkt im Browser. Eine nette Idee ist die Organisation von Titeln in Form von „Regalen". Diese erreichen Sie über die linke Navigation. Das Hinzufügen eines Titels zu einem Regal erledigen Sie in der Detailansicht des Titels selbst. ■

„MORGENZEITUNG" IM BROWSER

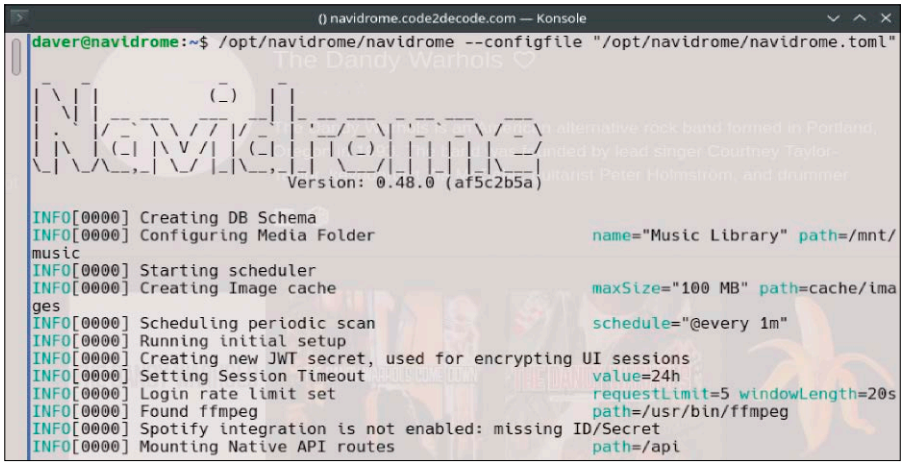
Neben der Freigabe der E-Books im lokalen Netzwerk bietet die Serverfunktion weitere interessante Optionen. Vielleicht haben Sie die Funktion „Nachrichten abrufen" bereits genutzt. Damit kann Calibre Nachrichten in Form eines oder mehrerer RSS-Feeds herunterladen und in die Bibliothek aufnehmen. Sie sind dabei nicht auf die (spärlichen) nationalen Quellen beschränkt. Durch benutzerdefinierte Quellen ist es im Prinzip möglich, jedes Blog oder jede Site einzubinden, die einen RSS-Feed anbietet. Läuft Calibre oder der Server permanent im Hintergrund, etwa auf einem Raspberry Pi, können Sie somit beim Frühstück via Browser auf dem Tablet ihre individuell zusammengestellte „Morgenzeitung" lesen.

Streaming mit Navidrome

Ein eigenes Spotify: Der Streamingserver Navidrome für Linux-Systeme präsentiert die lokal gespeicherte Musiksammlung zum Abspielen nicht nur im Browser. Auch Player und Apps mit der komfortablen Subsonic-API finden Unterstützung.

VON DAVID WOLSKI

Kaum jemand will die eigene, gern gehörte Musiksammlung nur mehr auf einem physischen Speicher wie einer Festplatte haben. Musik wird heute vorzugsweise per Streaming angehört, auf Smartphones oder Playern mit Internetverbindung. Streamingdienste wie Spotify haben das Konzept perfektioniert, Musik ganz nach Geschmack werbefinanziert oder im Abonnement überall verfügbar zu machen, wo es eine Internetverbindung gibt. Dies geht mit Linux auch auf eigene Faust: Die Open-Source-Software Navidrome bringt die Musiksammlung auf dem eigenen Server ins LAN oder ins Internet.



Erster Start und Kontrolle auf Fehler: Navidrome zeigt beim Aufruf in der Kommandozeile einen Statusreport mit Fehlermeldungen, falls mit Konfiguration oder Pfad etwas nicht stimmt.

Unterstützung für Subsonic-Clients

Navidrome hat mehr zu bieten als eine Browseroberfläche: Der Server ist kompatibel mit Subsonic, einem kommerziellen HTTP-Streamingdienst, der eine API für Player und spezialisierte Audiogeräte etabliert hat. Navidrome verlangt aber nur etwa ein Zehntel des Arbeitsspeichers von anderen Subsonic-Klonen wie Airsonic und ist damit auch für Ein-Platinen-Computer oder schmale Cloudinstanzen geeignet. Auch ein Transcodieren in Echtzeit ist möglich, um einzelne Clients mit datensparenden Streams zu versorgen.

Navidrome ist in Go programmiert, nutzt nur eine dateibasierte Sqlite-Datenbank und liefert außer Ffmpeg viele seiner Bibliotheken und einen internen Webserver selbst mit, was die Installation stark vereinfacht: Neben der eigentlichen Binary verlangt Navidrome nur noch nach einer Konfigurationsdatei und einer Servicedatei für Systemd, um den Streamingserver automatisch zu starten. Um Navidrome testweise spielen zu lassen, ist eine Installation zunächst gar nicht nötig, denn der Entwickler bietet unter *https://demo.navidrome.org* eine öffentliche Demo an, die auch als Subsonic-Server für Clients agiert. Benutzername und Passwort zur Anmeldung lauten schlicht „demo“.

Installation und Einrichtung als Dienst

Fertige Installationspakete von Navidrome gibt es bislang nur für Arch Linux und Fedora. Die Installation ist aber generell nicht anspruchsvoll und verlangt auf allen Linux-Distributionen nur ein paar Handgriffe. Eine (englischsprachige) Installationsanleitung liegt auch unter *https://www.navidrome.org/docs/installation* vor. Der folgende Weg unter Linux ist aber geradliniger als dort beschrieben.

1. Verzeichnisse erstellen: Traditionell kommen vom Paketmanager separat installierte Programme in das Verzeichnis „/opt“ und „/var“, also erstellt zunächst der Befehl

```
sudo mkdir -p /opt/navidrome /var/lib/navidrome
```

die nötigen Zielordner.

2. Programmdateien holen: Unter *https://github.com/navidrome/navidrome/releases* liegen die stets aktuellen Versionen als „tar.gz“-Archiv für verschiedene Prozessorarchitekturen. Für ein 64-Bit-Linux auf PC-Hardware ist die Version „x86_64“ die richtige, für den Raspberry Pi 4 mit 64-Bit-System das Archiv mit der Angabe „arm64“. Für einen älteren Raspberry Pi ab Modell 2 ist die Version „armv7“ geeignet. Nach dem Herunterladen entpackt dieser Befehl das Archiv ins Zielverzeichnis und passt dabei

gleich die Zugriffsrechte an:

```
sudo tar xvzf navidrome_0.48.0_
 Linux_x86_64.tar.gz -C /opt/
 navidrome/ --no-same-owner
```

Als einzige Abhängigkeit verlangt Navidrome das Paket „ffmpeg“ zum Recodieren von Audiodateien. In Ubuntu und Linux Mint ist es mittels

```
sudo apt install ffmpeg
```

aus den Standard-Paketquellen nachzurüsten, falls noch nicht vorhanden.

3. Konfiguration erstellen: Für den ersten Start verlangt Navidrome noch nach einer knappen Konfigurationsdatei, die mit dem Kommando

```
sudo touch /var/lib/navidrome/
 navidrome.toml
```

erstellt ist. In diese Datei kommen die folgenden drei Zeilen:

```
MusicFolder = "/home/[Konto]/
 Musik"
DataFolder = "/home/[Konto]/.
 navidrome"
DefaultLanguage = "de"
```

Das Verzeichnis „MusicFolder“ muss dem tatsächlichen Pfad zur Musiksammlung entsprechen, deren Ordner und Dateien zumindest lesbar sein müssen. Die Zeile „DataFolder“ gibt an, wo die Musikdatenbank gespeichert werden soll, hier im versteckten Ordner „.navidrome“ im Home-Verzeichnis.

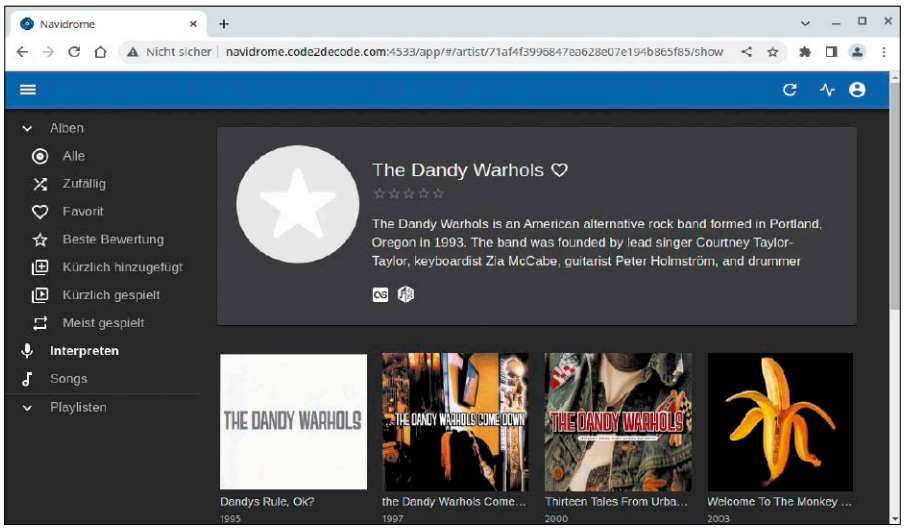
4. Navidrome starten: Der erste Aufruf in der Kommandozeile erfolgt dann mit diesem Kommando:

```
/opt/navidrome/navidrome
 --configfile "/var/lib/navidrome/
 navidrome.toml"
```

Dies prüft die Konfiguration und gibt Statusmeldungen auf die Konsole aus, die bei der Suche nach Fehlern helfen. Läuft alles korrekt, dann ist der Webserver von Navidrome per HTTP (unverschlüsselt) mit der IP-Adresse beziehungsweise dem Hostnamen des Rechners und auf Port 4533 verfügbar. Die komplette Adresse für den Browser lautet dann etwa *http://192.168.178.10:4533*. Der erste Schritt auf der Weboberfläche ist die Einrichtung eines Benutzers, der dann auch gleich Administrator der Navidrome-Instanz ist.

Weiterführende Konfiguration

Die Oberfläche zeigt sich dank der Konfigurationsdatei in Deutsch und links ein Menü. Die Musikstücke werden automatisch nach Album und Interpret kategorisiert. Der Punkt „Playlisten“ erstellt über einen Klick auf das Zahnradsymbol neue Listen. Dann können die drei Punkte hinter einem Song und „zur Playlist hinzufügen“ den Titel einer Liste zuordnen. Navidrome kann für jeden verbundenen Player und Browser eine passende Bitrate definieren. Diese Einstellung findet sich rechts oben im Admin-Menü unter „Players“, wo sich eine Liste der bislang genutzten Player zeigt. Ein Klick auf einen Eintrag kann mit „Max. Bitrate“ den Datenfluss auf Kosten der Qualität reduzieren, um auf Smartphones Bandbreite zu sparen. Die Benutzerverwaltung, die das Anlegen weiterer Konten erlaubt, ist rechts oben über „Nutzer“ aufrufbar.



Weboberfläche von Navidrome: Das Design passt sich je nach Bildschirmgröße an und ist in Deutsch übersetzt. Navidrome unterstützt Browser als Player sowie Apps per Subsonic-API.

Ein Punkt verlangt optionale Nacharbeiten: Navidrome bietet selbst nur unverschlüsseltes HTTP an, was für das lokale LAN in Ordnung geht, aber im Internet tabu ist. Um HTTPS mit einem TLS-Zertifikat auf einem Webserver zu nutzen, muss deshalb vor Navidrome ein Server wie Nginx geschaltet werden, der als Reverse Proxy arbeitet und den Webtraffic von außen an den Serverprozess durchreicht. Eine Beispielkonfiguration ist unter *https://tinyurl.com/navinginx* dokumentiert. ■

SYSTEMD: NAVIDROME ALS DIENST EINRICHTEN

Wer an Navidrome Gefallen findet und automatisch beim Systemstart ausführen will, richtet am besten einen Systemd-Dienst dafür ein. Auf Heft-DVD liegt dafür vorbereitet die Unit-Datei „navidrome.service“, welche dem Konfigurationsbeispiel unter *https://www.navidrome.org/docs/installation/linux/* folgt, aber um ausführliche (deutschsprachige) Kommentarzeilen erweitert ist. Die Zeilen

```
User=<benutzer>
```

sowie

```
Group=<gruppe>
```

sind in jedem Fall noch anzupassen. Hier müssen jeweils der Benutzername und die üblicherweise gleichlautende Benutzergruppe des Anwenderkontos eingetragen werden, unter dem Navidrome laufen soll. Folgendes Kommando kopiert dann die angepasste Datei in ihr Zielverzeichnis:

```
sudo install -o root -g root navidrome.service /etc/systemd/system/
```

Danach setzen die beiden Befehle

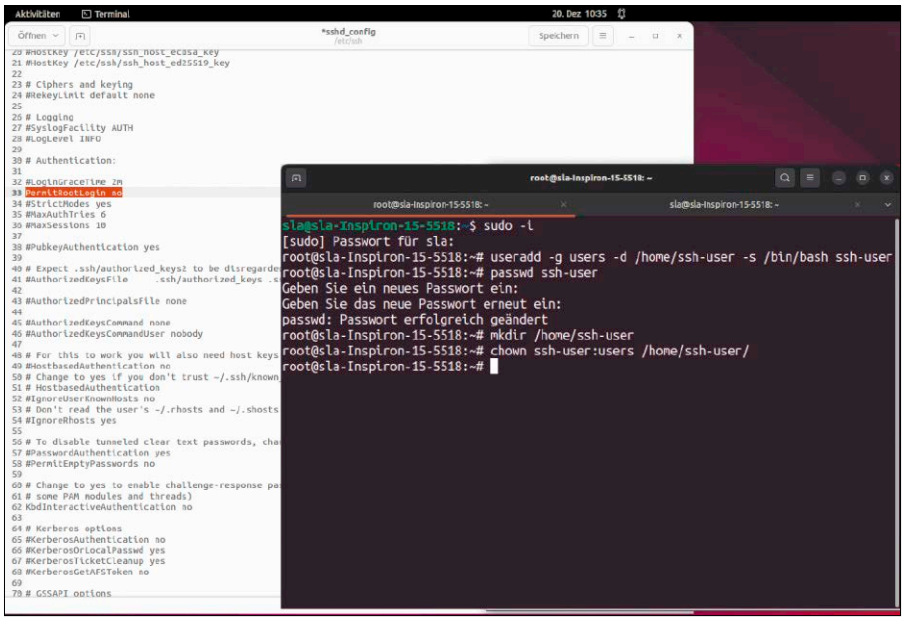
```
sudo systemctl daemon-reload
sudo systemctl enable --now navidrome.service
```

den Dienst in Gang, und der Befehl *sudo system status navidrome.service* zeigt, ob alles geklappt hat.

So härten Sie den SSH-Zugang

Mit dem SSH-Zugang arbeitet jeder Systembenutzer auf einem entfernten Rechner, als säße er direkt davor. Je nach Situation und Benutzerkreis ist es ratsam, sich Gedanken darüber zu machen, wie sich der Zugang absichern lässt.

VON STEPHAN LAMPRECHT



Soll ein Platinenserver wie der Raspberry Pi ohne angeschlossene Tastatur und Bildschirm bedient werden, dann bietet das SSH-Protokoll einen Weg dazu. Via SSH können Sie sich auch auf den meisten Cloudservern anmelden. Nach erfolgreicher Anmeldung stehen dann auch alle systemweiten Kommandos zur Verfügung. Nun arbeitet SSH ja als Tunnel durch das Web, ist also schon einmal besser geschützt als eine unverschlüsselte Verbindung zu einem System. Aber dennoch gibt es Optionen, den Zugang noch sicherer zu gestalten.

Die hier vorgestellten Maßnahmen können einzeln oder auch allesamt umgesetzt werden. Wie sicher der Zugang sein muss, bestimmt vor allem die Situation des Serversystems: Ist es über das Internet erreichbar, ist maximale Sicherheit angesagt, im lokalen Netz mag ein root-Verbot oder eine „AllowedUsers"-Anweisung genügen.

Keine Anmeldung für Root

Ein probates Mittel, um Angreifern weniger Möglichkeiten einzuräumen, besteht darin, keine Zugriffe von root via SSH zu erlauben. Diesen Weg gehen häufig auch kommerzielle Anbieter von Cloudservern. Hier ist allerdings genaues Arbeiten gefragt, damit Sie sich nicht selbst vom System aussperren. Diese zusätzliche Absicherung erfolgt in zwei Schritten – zunächst durch das Anlegen eines zusätzlichen Nutzers, der sich dann immer erst root-Recht verschaffen muss, im zweiten Schritt durch Deaktivierung des root-Zugangs via SSH. Wenn Sie direkt vor dem betreffenden Rechner sitzen, können Sie die Arbeiten auch in der grafischen Oberfläche der Benutzerverwaltung durchführen. Schneller geht es aber in der Konsole. Sie legen zunächst den neuen Nutzer an:

```
useradd -g users -d /home/sepp -s /
  bin/bash sepp
```

Jetzt weisen Sie dem Nutzer ein starkes Passwort zu. Das geht mit dem Kommando

```
passwd sepp
```

und anschließend legen Sie für diesen Nutzer noch sein Home-Verzeichnis an und geben ihm die Rechte daran:

```
mkdir /home/sepp
chown sepp:users /home/sepp/
```

Anschließend müssen Sie prüfen, ob Sie sich mit diesem Konto via SSH anmelden können. Hat das funktioniert und Sie befinden sich in dem leeren Home-Verzeichnis, versuchen Sie, ein beliebiges Kommando mit dem Zusatz „su" aufzurufen. Hat das funktioniert, schalten Sie den root-Zugriff für SSH ab. Das erledigen Sie in der Datei „/etc/ssh/sshd_config". Darin finden Sie die Zeile „PermitRootLogin". Das verändern Sie zu „no". Um die Änderungen zu übernehmen, starten Sie den SSH-Dienst mit

```
sudo systemctl restart sshd
```

neu. Um später mit root-Recht zu arbeiten, verwenden Sie nach dem Log-in auf dem System das Kommando *su -l*.

Verändern Sie den Standardport

Malware-Scripts und Angreifer lieben Standardeinstellungen. Daher empfehlen wir auch stets, nach der Installation eines

Dienstes die voreingestellten Passwörter zu ändern. Ähnlich verhält es sich mit Standardzugangswegen.

Um etwa öffentlich erreichbare Raspberry-Server auf Schwachstellen abzuklopfen, werden Angreifer die SSH-Standards nutzen und sich versuchsweise auf Standardport 22 mit dem Nutzer „pi“ und Kennwort „raspberry“ anmelden. Ungleich schwerer wird es für Angreifer mit geändertem Konto und Kennwort, noch schwerer wird es, wenn Sie den Standardport verändern. Dazu müssen Sie die Konfiguration für SSH ändern. Das können Sie wieder in der bereits genannten Konfigurationsdatei:

```
sudo nano /etc/ssh/sshd_config
```

Suchen Sie darin die Zeile „#Port“, entfernen Sie das Kommentarzeichen und tragen Sie statt „22“ einen Port Ihrer Wahl ein, zum Beispiel 479. Speichern Sie die Datei und starten Sie den Service mit *sudo systemctl restart sshd* neu. Wer jetzt versucht, das System von einem anderen Rechner durch die gewohnte Eingabe von „ssh [Konto]@[IP-Adresse]“ zu erreichen, wird abgelehnt werden.

Um sich auf dem geänderten Port zu verbinden, muss der Befehl mit

```
ssh -p 479 [Konto]@[IP-Adresse]
```

die exakte Portangabe mitliefern.

Anmeldung auf das Heimnetz beschränken

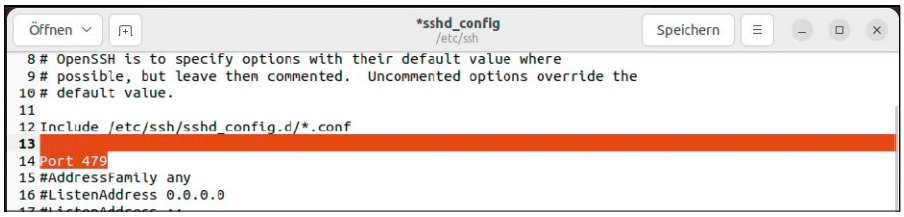
Die bisherigen Schritte machen es Angreifern und schädlichen Scripts deutlich schwerer. Sie nutzen nicht mehr den Standardzugang und eine Anmeldung von Root ist nicht möglich. Noch sicherer wird die Verbindung natürlich, wenn der Zugriff nur noch über bestimmte IP-Adressen erfolgen darf. Wenn diese Option in Betracht kommt, weil Sie stets nur von einem System aus einem festen IP-Bereich Anmeldungen durchführen, ist das eine vielversprechende Möglichkeit. Öffnen Sie die schon bekannte Konfigurationsdatei „sshd_config“. Um eine Anmeldung nur von einer einzigen IP-Adresse zu erlauben (hier aber für jedes Konto), fügen Sie die Zeile

```
AllowUsers *@192.168.178.10
```

ein. Das können Sie auch auf einen Adressbereich ausdehnen. Die Anweisung

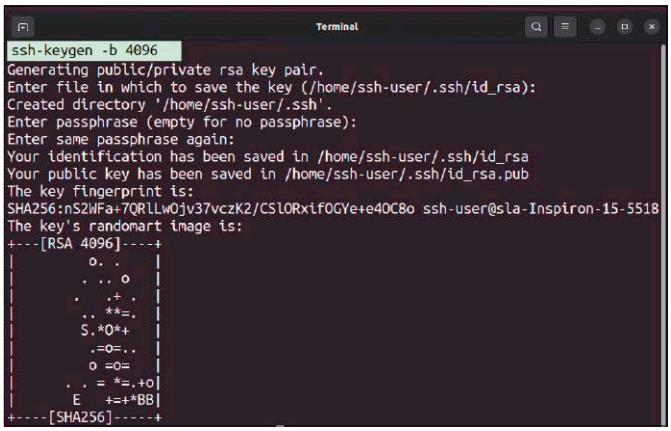
```
AllowUsers *@192.168.178.0/24
```

würde den für die Fritzbox typischen Adressraum von 192.168.178.0 bis 192.168.178.255 für die SSH-Anmeldung erlauben.



Eine einfache Maßnahme, es Angreifern deutlich schwerer zu machen, besteht darin, den Standardport (22) für SSH zu verändern.

Noch sicherer wird der Zugriff, wenn die Anmeldung ausschließlich via Schlüsseldateien erfolgt. Sie sollten den Schlüssel aber mit einem Kennwort („Passphrase“) schützen.



Anmeldung nur via Schlüsselpaar erlauben

Bei der Verwendung von Passwörtern besteht immer das Problem, dass diese erraten, ausprobiert oder entwendet werden können. Das ist bei der Verwendung von Schlüsselpaaren anders. Hier müssten öffentliche und private Schlüssel gestohlen worden und die Passphrase für den Zugriff bekannt sein. Um sich via Schlüssel anmelden zu können, legen Sie zunächst auf ihrem Stammsystem ein Schlüsselpaar an mittels des Befehls

```
ssh-keygen -b 4096
```

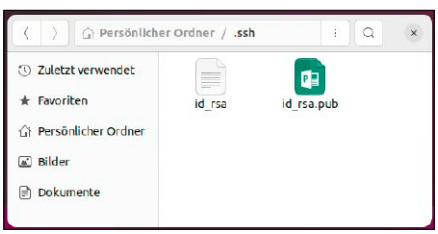
Beim Speicherort, der abgefragt wird, belassen Sie es bei den Voreinstellungen. Sie können jetzt eine „Passphrase“ (Kennwort) zum Schutz des Schlüssels nutzen. Das ist für hohen Sicherheitsanspruch empfehlenswert, denn ohne diese Hürde genügt ein entwendeter Schlüssel zur Anmeldung. Sie erhalten eine Rückmeldung wie „Your public key has been saved in /home/[nutzername]/.ssh/id_dsa.pub“. Diesen Schlüssel müssen Sie auf den Server übertragen. Der Einfachheit halber gehen wir davon aus, dass sich auf dem Zielserver im Home-Verzeichnis des aktuellen Nutzers bereits das versteckte Verzeichnis „./ssh/“ befindet. Um den öffentlichen Schlüssel zum Server zu kopieren, nutzen Sie dieses Kommando (Beispiel):

```
scp ~/.ssh/id_dsa.pub
  sepp@192.168.178.10
```

Bevor Sie jetzt die Anmeldung via Passwort abschalten, sollten Sie den Zugriff via Schlüssel unbedingt testen.

In der Konfigurationsdatei „sshd_config“ (am Server) ändern Sie dazu den Wert „No“ von „PubkeyAuthentication no“ in „yes“ und lesen die Konfiguration neu ein (*sudo systemctl restart sshd*). Danach testen Sie die Verbindung. Sie werden bei der Anmeldung nach der Passphrase für den Schlüssel gefragt (nicht nach dem Systemkennwort des Benutzers).

Wenn Sie sich auf diesem Weg erfolgreich anmelden konnten, schalten Sie in der Konfigurationsdatei „/etc/ssh/sshd_config“ (am Server) die Anmeldung mit Konto und Passwort aus. Suchen Sie dort nach der Zeile „PasswordAuthentication“ und ändern Sie den Wert von „yes“ auf „no“. ■

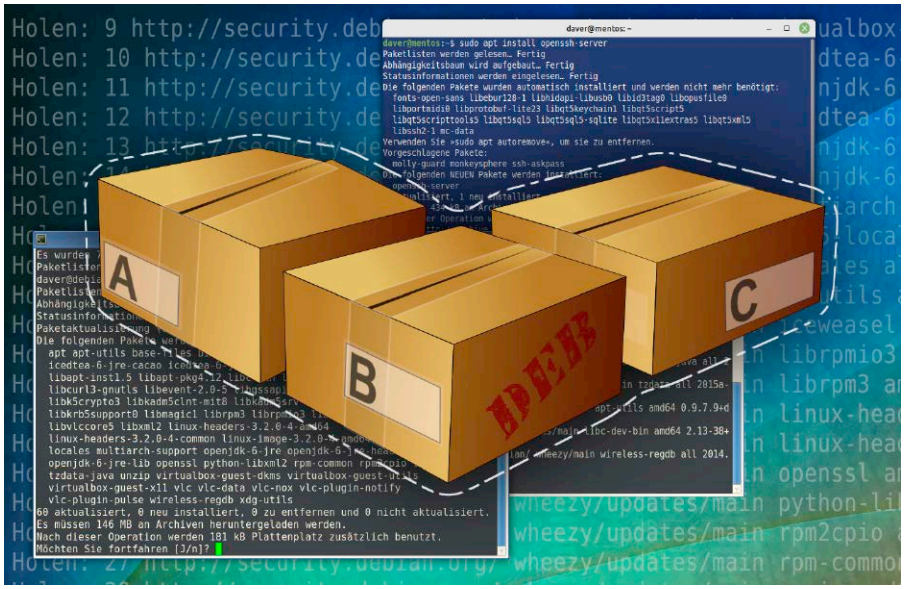


Es werden zwei Schlüsseldateien angelegt. Die öffentliche Datei des Nutzers, der auf den Server zugreifen soll, muss zum Server kopiert werden.

Paketmanager: Tipps und Fehlersuche

Installationen, Updates und Systemupgrades bereiten bei Linux nur selten Probleme. Wenn jedoch Fehler auftreten, ist die Reparatur oft nicht einfach. Wir geben Tipps zur Nutzung der Paketverwaltung und Ratschläge zur Behebung von Fehlern.

VON THORSTEN EGGELING



Die technische Basis der Paket-Infrastruktur ist bei Debian, Ubuntu sowie Linux Mint identisch und seit vielen Jahren bewährt. Trotzdem kann es zu Fehlern kommen: Systemupdates beispielsweise schlagen fehl oder es lassen sich keine neuen Programme installieren. Viele Probleme lasen sich einfach lösen, bei schweren Fehlern in der Systeminstallation kann die Fehlersuche jedoch aufwendig werden.

Das Ubuntu/Debian-Paketformat

Das Paketmanagement bei Debian, Ubuntu und verwandten Systemen ist zwar komplex, aber trotzdem transparent und nachvollziehbar. System und Software werden mit Hilfe von Softwarepaketen installiert, die in DEB-Dateien vorliegen. Dabei handelt es sich um gepackte Archive, die ausführbare Dateien, Bibliotheken und Konfigurationsdateien enthalten. Ebenfalls enthalten sind meistens einige Scripts, die beim Setup beispielsweise Konfigurationsdateien anpassen oder Systembenutzer erstellen. Eine DEB-Datei enthält aber selten alle Dateien, die zum Start des jeweiligen Programms erforderlich sind. Fast alle Tools und Anwendungen benötigen zusätzliche Programmbibliotheken, die oft Funktionen für mehrere Programme bereitstellen. Im DEB-Paket ist daher eine Textdatei mit Informationen über die Abhängigkeiten von anderen Paketen sowie optionalen Empfehlungen für zusätzliche Pakete enthalten. Der Distributor muss dafür sorgen, dass alle Pakete für ein System zusammenpassen und alle Abhängigkeiten erfüllbar sind. Die Pakete stammen jedoch nicht aus einer Hand. Es sind weltweit zahlreiche Entwickler („Maintainer“) an der Erstellung der Pakete beteiligt. Vor allem bei selten genutzten Programmen kommen daher Installationsfehler vor, die vielleicht bisher vom Anbieter nicht entdeckt wurden. Eine Suche nach der Fehlermeldung im Internet kann weiterhelfen. Eine Quelle für Informationen ist *https://bugs.launchpad.net/ubuntu*. Hier kann man nach Paketen suchen und sich die gemeldeten Fehler anzeigen lassen.

DEB-Dateien sind digital signiert und es gibt Prüfsummen für die enthaltenen Dateien. Der Paketmanager verweigert die Installation, wenn Signaturen oder Prüfsummen ungültig sind. Manchmal ist auch ein falsch gesetztes Systemdatum die Ursache. Liegt es zu weit in der Vergangenheit oder Zukunft, wird der Schlüssel als ungültig angesehen.

Tipp: Wer sich den Inhalt einer DEB-Datei genauer ansehen möchte, kann die Dateien extrahieren. Installieren Sie dazu das Archivprogramm ar mit

```
sudo apt install binutils
```

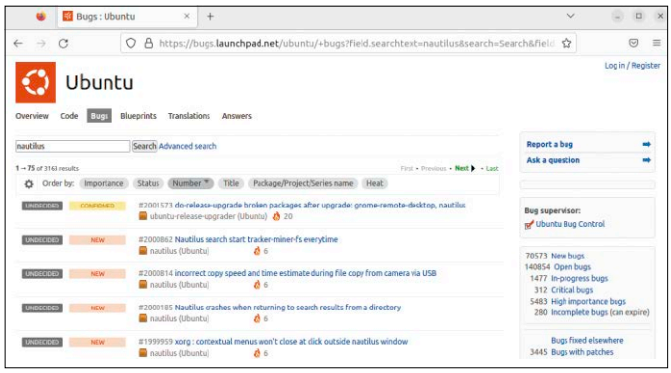
und entpacken Sie dann eine DEB-Datei mit

```
ar xv [Name der Datei]
```

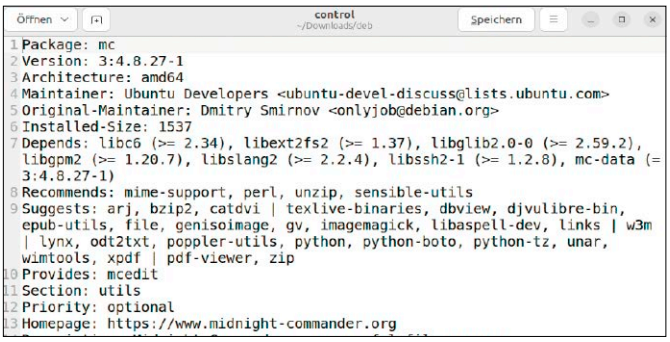
Das Ergebnis sind die Dateien „control.tar.zst“ und „data.tar.zst“ (oder .gz), die Sie mit

```
tar xvf [tar.zst-Datei]
```

entpacken. Dabei entstehen Order, in denen die ausführbaren Dateien und Konfigurationsdateien zu finden sind. „control“ enthält eine Beschreibung des Pakets und Informationen zu Abhängigkeiten, „md5sums“ die Prüfsummen der Dateien.



Fehlerberichte: Bei *https://bugs.launchpad.net/ubuntu* finden Sie eingesandte Fehlerberichte zu einzelnen Ubuntu-Paketen und oft auch Problemlösungen.

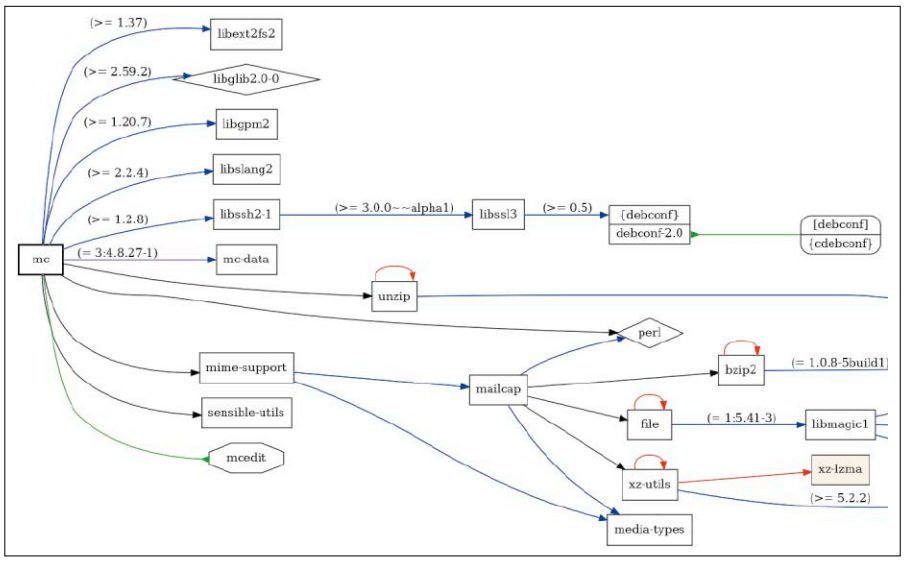


Paket-Internat: Die Datei „control“ in einem DEB-Paket enthält alle Informationen. Hinter „Depends:“ beispielsweise stehen die Paketabhängigkeiten inklusive Versionsnummern.

Pakete und Abhängigkeiten

In der Paketdatenbank sind die Informationen zu allen installierten Paketen gespeichert. Wird ein neues Programm installiert, lässt sich darüber prüfen, ob zusätzlich erforderliche Tools und Bibliotheken bereits vorhanden sind. Wenn nicht, werden diese automatisch mitinstalliert. Bei der Deinstallation eines Pakets werden gemeinsam genutzte und automatisch installierte Komponenten nicht entfernt. Anders sieht es aus, wenn man etwas deinstalliert, das von anderen Paketen benötigt wird. Es erscheint ein Hinweis, welche Pakete außerdem entfernt werden. Diese Meldung sollte man immer sehr ernst nehmen und genau prüfen. Wenn man die Situation nicht sicher einschätzen kann, sollte man auf die Deinstallation verzichten.

Die Abhängigkeiten von anderen Paketen müssen exakt erfüllt sein. Anwendungen benötigen die gleiche oder eine höhere Nebenversion von Programmbibliotheken, mit denen sie erstellt wurden. Bei Linux ist es Standard, dass bei der Hauptversion einer Programmbibliothek zwar neue Funktionen hinzukommen können, alte aber nicht wegfallen. Beim Upgrade, etwa von einer Version 6.x auf 7.x, ist das nicht immer der Fall. Im optimalen Fall verwenden alle Programme einer Distribution die gleichen Versionen der Programmbibliotheken. Das ist allerdings nicht immer möglich. Linux löst das Problem mit Versionsnummern in den Dateien. Unterhalb von „/usr/lib“ können beispielsweise die Dateien „libx.so.1“ und „libx.so.2“ liegen und jedes Programm findet dann die jeweils benötigte Version. Nach einem Update kann die Datei dann „libx.so.2.1.1“ heißen. In diesem Fall verweist der symbolische Link mit der Nummer der Hauptversion „libx.so.2“ auf „libx.so.2.1.1“ und für die Programme hat sich nichts geändert.



Nötige Pakete: Das Tool debtree bereitet den meist komplexen Abhängigkeitsbaum grafisch auf. Selbst ein einfaches Tool wie Midnight Commander benötigt mehrere Pakete.

Bei komplexeren Programmen ergibt sich ein sehr weit verzweigter Baum von Abhängigkeiten („dependency tree“) und die Paketverwaltung installiert zahlreiche Pakete. Wer es genauer wissen möchte, kann mit der Befehlszeile

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

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

Paketverwaltung im Terminal

Das zentrale Programm zur Paketverwaltung heißt unter Ubuntu und verwandten Systemen dpkg. Es wird im Hintergrund von allen Tools zur Paketverwaltung genutzt. Das Tool lädt jedoch keine Paketdateien herunter und prüft keine Abhängigkeiten. Deshalb werden Sie es nur selten direkt nutzen. Eine heruntergelade DEB-Datei lässt sich bei Bedarf im Terminal mit

```
sudo dpkg -i [DEB-Datei]
```

installieren. Bei mehreren Dateien verwenden Sie im Downloadordner

```
sudo dpkg -i *.deb
```

Sollten die Paketabhängigkeiten nicht bereits erfüllt sein, verwenden Sie danach diesen Befehl:

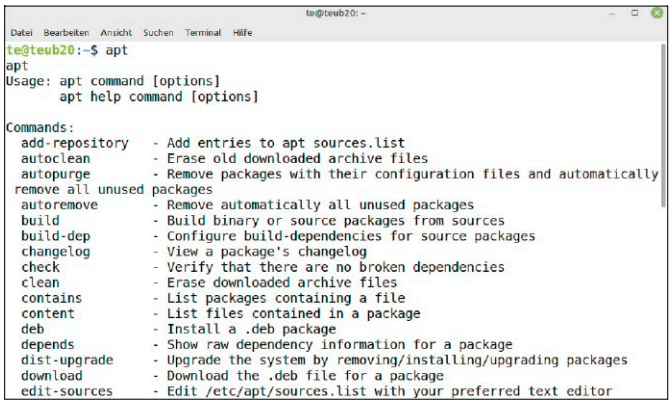
```
sudo apt -f install
```

Das Tool apt prüft die Abhängigkeiten und installiert alle fehlenden Pakete.

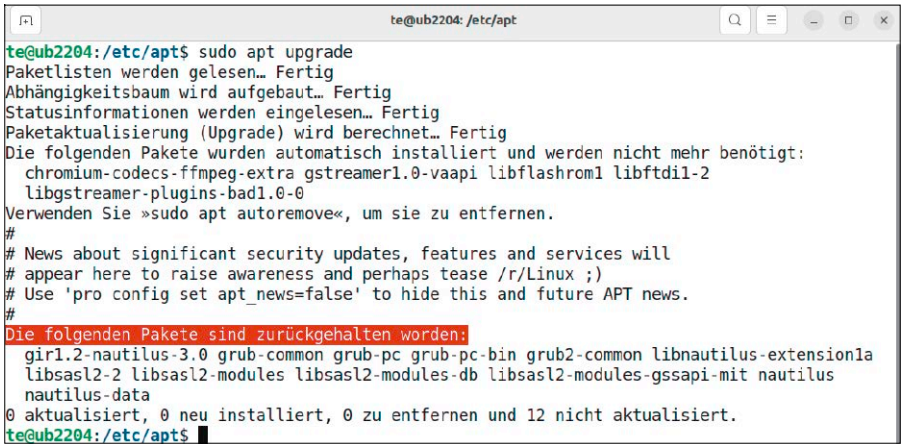
Seit Version 1.1 (ab Ubuntu 16.04) kann man DEB-Dateien auch direkt über apt installieren, wobei die Abhängigkeiten automatisch aufgelöst werden:

```
sudo apt install ./[DEB-Datei]
```

„install“ erwartet als Parameter den vollständigen Pfad zur Datei oder im Down-



Mint-Spezialität: Der Start von apt zeigt zahlreiche Optionen. Tatsächlich handelt es sich um ein Wrapper-Script, das je nach Option unterschiedliche Tools startet.



Auf später verschoben: Bei dieser Meldung sind Updates für die genannten Pakete verfügbar. Die Installation erfolgt jedoch erst, wenn mögliche Fehler beseitigt wurden.

load-Verzeichnis ein vorangestelltes „./“. Mehrere Pakete lassen sich mit

```
sudo apt install ./*.deb
```

einrichten.

Reguläre Nutzung von apt: Standardmäßig greift apt auf die in „/etc/apt/sources.list“ und unter „/etc/apt/sources.list-d“ konfigurierten Repositorien zurück. Die typische Anwendung für das Update von Paketen erfolgt mit den zwei Zeilen

```
sudo apt update
sudo apt upgrade
```

„update“ aktualisiert die Paketdatenbank, „upgrade“ lädt die Dateien herunter und beginnt mit der Installation. Fehler können auftreten, wenn ein Server gerade nicht erreichbar ist. Probieren Sie es später noch einmal oder kontrollieren Sie die URLs in den Paketquellen. Manchmal ist auch die Paketdatenbank blockiert, wenn im Hintergrund ein automatisches Update läuft (siehe Artikel ab Seite 22).

Eine fehlende IPv6-Unterstützung kann ebenfalls zu Problemen führen. In der Fehlermeldung wird dann bemängelt, dass beispielsweise der Server „2001:67c:1562::15“ (security.ubuntu.com) nicht erreichbar ist. Da alle Server auch über IPv4-Adressen verfügen, lässt sich das Problem über die apt-Konfiguration beben. Erstellen Sie mit

```
sudoedit /etc/apt/apt.conf.d/
  99force-ipv4
```

eine zusätzliche Konfigurationsdatei mit dem Inhalt

```
Acquire::ForceIPv4 "true";
```

Das Tool apt und die Paketmanager für die grafische Oberfläche verwenden jetzt nur noch IPv4-Adressen.

Unterschiede zwischen apt oder apt-get: apt ist bei Ubuntu eine vereinfachte Version von apt-get. Das Tool bietet die gebräuchlichsten Funktionen, beispielsweise

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

zur Installation neuer Pakete. Mehrere Pakete lassen durch Leerzeichen getrennt angeben, beispielsweise

```
sudo apt install apache2
  libapache2-mod-php php php-mysql
  mysql-server
```

für die Installation des Webservers Apache, PHP und der Datenbank My SQL. Für die Deinstallation eines Pakets verwenden Sie

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

Das Tool apt-get bietet fast die gleichen Optionen, aber noch einige zusätzliche. Es verhält sich aber teilweise anders. „upgrade“ bei apt-get aktualisiert nur die installierten Pakete, entfernt aber keine Pakete und fügt auch keinen neuen hinzu. Der Linux-Kernel beispielsweise wird damit nicht aktualisiert, weil es sich um ein neues Paket handelt. „apt upgrade“ installiert – wenn nötig – auch neue Pakete, entfernt aber ebenfalls keine Pakete.

Besonderheiten bei Linux Mint: Die Distribution verwendet beim Aufruf von apt ein Script aus dem Ordner „/usr/local/bin“. Abhängig von der verwendeten Option ruft es /usr/bin/apt, apt-get oder andere Tools auf. Bei „update“ und „upgrade“ beispielsweise kommt /usr/bin/apt zum Einsatz, bei „clean“ (heruntergeladene Pakete löschen) oder „check“ (unerfüllte Abhängigkeiten finden) wird apt-get verwendet.

Ungewöhnliche Meldungen von apt: Manchmal gibt „apt upgrade“ eine Info zu automatisch installierten Paketen aus, die nicht mehr benötigt werden. Sie können dann bedenkenlos

```
sudo apt autoremove
```

verwenden, um die Pakete zu entfernen.

Eine auffällige Meldung ist: „Die folgenden Pakete sind zurückgehalten worden:“. Darunter steht eine Liste mit den betroffenen Paketen. Dahinter verbergen sich Updates, deren problemlose Funktion noch nicht sichergestellt ist.

Die Pakete werden nach und nach an die Benutzer ausgeliefert, und die Entwickler beobachten dann die eingesandten Fehlerberichte. Bei Ubuntu heißt das Verfahren „Phasing“.

```
apt list --upgradable
```

gibt die Paketnamen der Updates inklusive der neuen Versionsnummern aus. Mit

```
apt show [Paketname] = [Neue
  Versionnummer]
```

lässt sich der Status eines Pakets ermitteln. Der Wert hinter „Phased-Update-Percentage:“ startet bei zehn Prozent und wird alle sechs Stunden um zehn Prozent erhöht, wenn keine Fehler gemeldet werden. Sie müssen daher nur bis zu maximal 54 Stunden auf die Installation warten, weitere Aktionen sind nicht erforderlich. Auskunft über die jeweils betroffenen Pakete liefert *https://people.canonical.com/~ubuntu-archive/phased-updates.html*.

Probleme beim Ubuntu-Upgrade beheben

Besondere Aufgabe erfüllen „apt full-upgrade“ und „apt-get dist-upgrade“. Beide arbeiten identisch und führen Updates auch dann durch, wenn sich Paketabhängigkeiten geändert haben, neue Pakete erforderlich sind oder installierte entfernt werden müssen. Zum Einsatz kommt eines der beiden Kommandos, wenn Sie ein Upgrade auf die nächste Ubuntu-Version im Terminal anstoßen wollen. Denn die Voraussetzung dafür ist ein möglichst vollständig aktualisiertes System. Verwenden Sie die folgenden vier Befehle:

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

In der Regel arbeitet „apt-get dist-upgrade“ unproblematisch. Man sollte es dennoch nicht als standardmäßigen Ersatz für „apt upgrade“ verwenden, weil bei Fehlern unter Umständen wichtige Pakete entfernt werden. In jedem Fall sollten Sie die Ausgaben des Befehls beachten und das Verhalten prüfen, wenn Deinstallationen durchgeführt werden sollen.

Die Ausführung von do-release-upgrade scheitert, wenn Systemaktualisierungen nicht für alle installierten Pakete möglich sind. Dieser Zustand kann nur eintreten, wenn aktuellere Software aus PPA-Repositorien installiert wurde, worauf apt auch hinweist. Man sollte zuerst versuchen, die PPA-Fremdsoftware zu deinstallieren. Vorher ist ein Backup des Systems oder wenigstens der persönlichen Dateien ratsam, weil das erfolgreiche Upgrade nicht mehr garantiert werden kann.

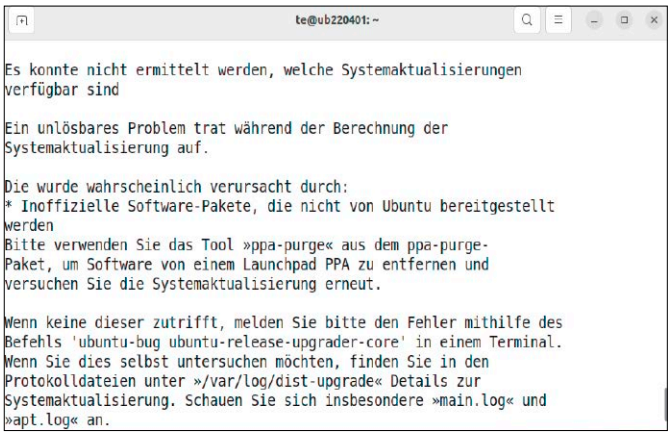
do-release-upgrade deaktiviert zuerst fremde Repositorien in den Listen unter „/etc/apt/sources.list.d“, was man später wieder rückgängig machen muss. Danach kann man ppa-purge verwenden, um die Fremdsoftware zu entfernen. Installieren Sie dieses Tool mit

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

und verwenden Sie es dann so:

```
sudo ppa-purge -o [Besitzer des PPA]
  -p [Name des PPA]
```

Die Werte für die beiden Platzhalter ermitteln Sie aus der URL in der zugehörigen Datei des PPAs unter „/etc/apt/sources.list.d“. Lautet diese beispielsweise „*https://ppa.launchpadcontent.net/SeppHuber/daily-builds*“, verwenden Sie die Befehlszeile



Massive Probleme: Fremdpakete können das Ubuntu-Upgrade verhindern. Bevor es gelingt, müssen alle Pakete durch die meist älteren Originale der Distribution ersetzt werden.

```
sudo ppa-purge -o SeppHuber-p
  daily-builds
```

Das Tool versucht, die Pakete aus dem PPA zu entfernen und – wenn vorhanden – die Pakete durch die gleichnamigen aus den Standard-Repositorien zu ersetzen. Um defekte Abhängigkeiten danach zu reparieren, führen Sie

```
sudo apt -f install
```

aus. Anschließend starten Sie erneut

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

Sollte das Upgrade erneut fehlschlagen, prüfen Sie die Logdatei „/var/log/dist-upgrade/main.log“. Am Ende der Datei weisen Angaben hinter „Error“ auf defekte Pakete hin, die das Upgrade verhindern. Entfernen Sie diese Pakete mit „apt remove [Paketname]“, auch wenn es sich um wichtige Systempakete handelt. Notieren Sie sich die Paketnamen für die spätere Neuinstallation. Danach sollte do-release-upgrade keine Probleme mehr melden.

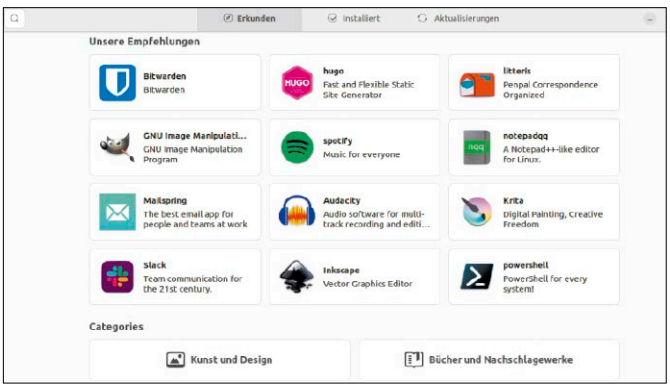
Paketverwaltung über die grafische Oberfläche

Im Terminal ist apt besonders nützlich, wenn man mehrere Pakete gleichzeitig installieren will. Außerdem gibt das Tool meist weiterführende Fehlermeldungen aus, die bei der Suche nach Problemen helfen. Man muss allerdings die Namen der Pakete kennen, die man installieren will.

Mehr Komfort bietet die grafische Zentrale „Ubuntu Software“ oder die „Anwendungsverwaltung“ von Linux Mint. Man kann sich die Empfehlungen oder in den Kategorien Programme und Beschreibungen ansehen und neue Programme einrichten. Ubuntu Software zeigt hauptsächlich Desktopanwendungen. Die Installation von Tools für das Terminal oder von Diensten ist daher hier nicht möglich.

Das Werkzeug Synaptic vereint die Vorteile einer grafischen Oberfläche mit denen von apt. Das Tool ist bei Linux Mint bereits vorinstalliert. Ubuntu-Nutzer können es über Ubuntu Software nachinstallieren. Synaptic bietet eine Suchfunktion und mehrere Filter, über die sich die Ansicht auf die gewünschte Software einschränken lässt. Das Tool im Vergleich zu Ubuntu Software etwas unübersichtlicher, dafür liefert die Suche schnellere Ergebnisse.

Anders als mit Ubuntu Software oder seinem Mint-Pendant lassen sich mit Synaptic alle verfügbaren Programme installieren, also auch Tools für die Kommandozeile, Bibliotheken und Entwicklerpakete. ■



Anwendungen für jeden Geschmack: Ubuntu Software zeigt, welche Programme verfügbar sind. Beschreibungen, Screenshots und Bewertungen helfen bei der Auswahl.

Konsolentipps

Diesmal gibt es in den Konsolentipps Trickreiches zur Umwandlung von Tabs und Leerzeichen zur Einrückung von Quellcode. Zwei Tools helfen bei Dateiübertragung von und zu Smartphones sowie beim Säubern des Befehlsverlaufs.

VON DAVID WOLSKI

Shellclear: Im Befehlsverlauf aufräumen

Die „History", also der Verlauf zuvor eingetippter Befehle, spart in der Bash und anderen Shells viel Tipparbeit über den Aufruf vergangener Kommandos. Die Cursor-oben/unten-Tasten gehen chronologisch durch die Befehle. Strg-R bietet eine Suchfunktion. Es kommt aber im Eifer der Systemkonfiguration vor, dass vertrauliche Daten wie Passwörter in diesem unverschlüsselten Verlauf landen – ein nicht seltener Fauxpas: Log-ins sollten nirgendwo im Klartext zu finden sein.

Neben Passwörtern verlangen auch API-Schlüssel, Datenbank-Log-ins und Github-Tokens besonderen Schutz. Hin und wieder ist es also eine gute Idee, den Befehlsverlauf der Shell aufzuräumen und verräterische Kommandos zu löschen. In der Bash, die in den meisten Linux-Distributionen der Standard ist, liegt die Datei „.bash_history" mit dem Befehlsverlauf als schlichte Textdatei in Home-Verzeichnis. Bei der ebenfalls vereinzelt verwendeten Shell ZSH lautet der Dateiname „.zhistory". Jede Zeile entspricht dort jeweils einem Befehl. Um aufzuräumen, öffnet man einfach diese Dateien in einem beliebigen Texteditor, löscht die unerwünschten Zeilen und speichert die Datei wieder.

Auf einem vollverschlüsselten System mit Luks2-Partition sind vertrauliche Daten im Befehlsverlauf weniger tragisch, aber auch unerwünscht. Schlimmer ist es, wenn auf einem Server oder einer Cloudinstanz Log-ins im Verlauf landen und dort vor der Schließung des Serverzugangs nicht sicher gelöscht werden. Für solche Fälle ist das clevere Tool Shellclear gemacht: Es überprüft nicht nur nach einem manuellen Aufruf den Verlauf von Bash, Zsh und Fish, sondern kann auch als Wächter konfiguriert werden. Bei dieser Konfiguration wird es bei jeder Anmeldung oder beim Öffnen eines Terminalfensters automatisch ausgeführt und überprüft die gespeicherten Kommandos auf etliche Muster: Abgedeckt sind Log-ins mit Curl, Wget, API-Schlüssel von Github, Gitlab, AWS, Facebook, Twitter, Slack, Sendgrid, Cloudflare und anderen Onlinediensten. Weil die Überprüfung nach Mustern per Script zu langsam wäre, ist Shellclear in Rust programmiert und liegt als vorkompilierte Binary für Linux (64 Bit, X86-Architektur) vor. Ein Installations-Script hilft bei der Einrichtung auf beliebigen Linux-Distributionen und ist mit dem Kommando

```
wget https://raw.
  githubusercontent.com/
  rusty-ferris-club/
  shellclear/main/
  install/install.sh
```

in das aktuelle Verzeichnis heruntergeladen. Die Eingabe

```
sudo sh install.sh
```

installiert die Binary in den Zielordner „/usr/local/bin/shellclear". Um den Verlauf auf verdächtige Muster zu überprüfen, dient dieser Aufruf:

```
shellclear find
```

Dies listet die gefundenen Stellen auf, entfernt sie aber noch nicht, um dem Benutzer die Kontrolle zu überlassen. Falls keine unerwünschten Löschaktionen zu erkennen sind, kann der Befehl

```
shellclear clear
```

die gezeigten Zeilen aus dem Verlauf löschen. Dabei kann Shellclear aber immer nur die gespeicherten Befehle der letzten Sitzung überprüfen, denn nur diese sind in der Verlaufsdatei gespeichert, neuere befinden sich erst nur im Arbeitsspeicher.

Um beim Start der Shell automatisch einen Check vorzunehmen, ergänzt man diese Zeile

```
eval $(shellclear --init-
  shell)
```

am Ende der Konfigurationsdatei „~/.bashrc". **-dw**

Shellclear überprüft den Befehlsverlauf nach typischen Mustern auf vertrauliche Daten und entfernt diese auf Wunsch aus dem Verlauf der Bash-, ZSH- und Fish-Shell.

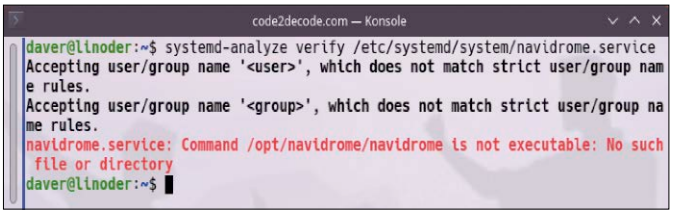
Systemd: Servicedateien prüfen

Bei der Arbeit auf dem eigenen Linux-System ist es schon mal nötig, zum Start von Diensten oder Servern eigene Servicedateien zu hinterlegen. Bevor es dann an den Start der eigenen Servicedatei geht, sollte man deren Syntax überprüfen.

Einen Check hat Systemd für Servicedefinitionen eingebaut, sodass kein weiteres Tool zum Überprüfen nötig ist. Die Eingabe des Befehls

```
systemd-analyze verify
  [Service-Datei]
```

geht die Syntax der angegebenen Datei durch und überprüft, ob aufgerufene Scripts und Programme in der Zeile „ExecStart=" vorhanden und ausführbar sind. Statt dem Platzhalter muss der exakte Pfad zu einer Servicedatei angegeben sein, also beispielweise „/etc/systemd/system/[Dienst].service" für einen systemweiten Dienst oder „~/.config/systemd/user/[Dienst].service" für einen selbst angelegten Service, der im Benutzerkontext laufen sollen. Kritische Fehler sind in der Ausgabe in roter Schrift hervorgehoben, Hinweise sind fett geschrieben. Diese Hinweise sind englischsprachig. **-dw**



Systemd-Kontrolleur: Für selbst geschriebene Serverdateien (Unit-Files) bietet Systemd einen Check, der Syntax und Pfad der ausführbaren Dateien überprüft.

Umwandeln: Tabulatoren und Leerzeichen

Zum Einrücken von Quellcode unterstützten die meisten Editoren entweder Leerzeichen oder Tabulatoren. Auch der Python-Interpreter kommt mit beidem klar, wenn diese Formatierungszeichen konsistent angewendet werden. Da kann es aber Konflikte geben, wenn Quellcodedateien aus anderen Quellen kommen, etwa von Github.

Einige Editoren wie Kate, Kdevelop und Geany können Tabulatoren zu Leerzeichen machen und umgekehrt. Der Aufwand dafür ist bei einer einzigen Datei vertretbar. Aber schon bei mehreren Quellcodedateien wird die Aufgabe lästig und ist schneller in der Shell erledigt. Die Konvertierung von Tabulatoren nach Leerzeichen und umgekehrt ist ein so häufig angefragtes Thema, dass ein Werkzeugpaar dazu schon vor Jahren in die GNU Coreutils aufgenommen wurde.

Die Befehle „expand" und „unexpand" sind deshalb auch in schmalen Linux-Systemen vorinstalliert und einsatzbereit. Die Besonderheit dieser Kommandos ist, dass sie beim Umwandeln von Leerzeichen in Tabulatoren nur die führenden Leerzeichen einer Zeile beachtet und umgekehrt Tabulatoren mit einer gewünschten Anzahl von Leerzeichen ersetzen kann.

Tabulatoren zu Leerzeichen: Dieser einfachere Fall ist auch der häufiger benötigte. In der Shell wandelt der Befehl

```
expand -t 3 datei.py >
  datei_neu.py
```

die Tabulatoren der Python-Datei „datei.py" in jeweils drei Leerzeichen um und schreibt den Inhalt in die neue Datei „datei_neu.py".

Mit einer Verknüpfung der weiteren Kommandozeilentools find und sponge kann man diese Umwandlung auf alle Dateien eines bestimmten Typs im aktuellen Verzeichnisbaum anwenden. Das erwähnte Programm sponge ist meist noch nicht installiert, aber in allen Linux-Distributionen über den Paketmanager über das Paket „moreutils" nachgerüstet, in Debian, Ubuntu und Linux Mint wie folgt:

```
sudo apt install moreutils
```

Der Befehl zur Umwandlung von Tabulatoren zu drei Leerzeichen in allen Dateien mit der Endung „.py" passt dann in eine einzige Zeile:

```
find . -iname '*.py' -type
  f -exec bash -c 'expand -t
  3 "$0" | sponge "$0"' {}
  \;
```

Die Dateien werden dabei rekursiv in allen Unterverzeichnissen überschrieben und es empfiehlt sich, vorher Sicherheitskopien anzulegen.

Leerzeichen zu Tabs: Seltener gefragt ist die Umwandlung von Leerzeichen in Tabs, welche das Tool unexpand auf intelligente Weise erledigt und nur führende Spaces beachtet. Der Aufruf zur Umwandlung von jeweils drei Leerzeichen in einen Tabulator lautet so

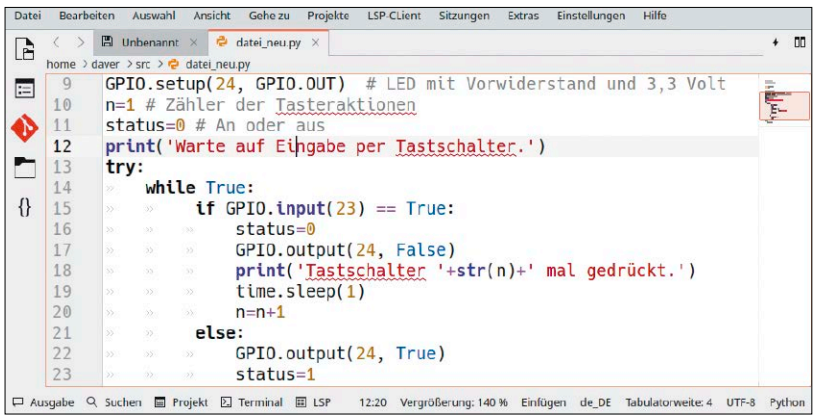
```
unexpand -t 3 datei.py >
  datei_neu.py
```

und erzeugt wieder eine neue Datei.

Auch diese Aktion ist mit dem Aufruf

```
find . -iname '*.py' -type
  f -exec bash -c 'unexpand
  -t 3 "$0" | sponge "$0" {}
  \;
```

auf alle Dateien einer bestimmten Endung in einem Verzeichnisbaum anwendbar. **-dw**



Tabulatoren oder Leerzeichen? Viele Programmiersprachen wie Python akzeptieren beide Formen der Einrückung. Die Befehle „expand" und „unexpand" können beides konvertieren.

QRCP: Dateitransfer für Smartphones

Die einfachste Methode zum Dateitransfer zwischen Linux-Desktops und Smartphones ist KDE Connect, das nicht nur mit KDE Plasma funktioniert. Was aber, wenn das Ziel- oder Quellsystem keine grafische Oberfläche hat?

Das Tool QRCP (*https://github.com/claudiodangelis/qrcp*) arbeitet mit einem eigenen kleinen Webserver, der Dateien über die Netzwerkschnittstelle senden und empfangen kann und sich danach selbst wieder beendet. Beim Start von QRCP im Terminal des Ziel- oder Quellsystems öffnet es einen zufälligen Port (der darf also nicht durch eine Firewall blockiert sein) und generiert dazu einen QR-Code mit der kompletten URL des Webservers. Es ist es also nicht notwendig, lange Adressen umständlich einzutippen. Auf dem Smartphone genügt zum Empfangen oder Senden einer Datei ein Webbrowser wie Chrome, Firefox oder Safari.

Zur Einrichtung steht das in Go programmierte QRCP als kompilierte Binary unter *https://github.com/claudiodangelis/qrcp/releases* für Linux und andere Systeme bereit, sowohl für x86-Architektur als auch für ARM. Die Installation in Linux-Systemen wie Debian, Ubuntu, Linux Mint, Fedora und Open Suse machen fertige DEB- sowie RPM-Pakete einfach.

In Ubuntu installiert beispielsweise nach dem Download des passenden Pakets der Befehl

```
sudo dpkg -i qrcp_0.9.1_
  linux_x86_64.deb
```

und in Fedora das Kommando

```
sudo rpm -ivh qrcp_0.9.1_
  linux_x86_64.rpm
```

das Programm.

Um nun eine Datei damit zu senden, genügt dieser Aufruf:

```
qrcp [Dateiname]
```

Der angezeigte QR-Code im Terminal muss auf dem Smartphone nur mit einer geeigneten App eingescannt werden, um die komplette URL parat zu haben, die man dann dort Browser aufruft. Sind mehrere Dateien angegeben, so erzeugt QRCP automatisch ein Zip-Archiv. Zum Empfangen dient dann folgender Aufruf:

```
qrcp receive
```

Auch hier entsteht wieder ein QR-Code. In diesem Fall führt die URL-Adresse auf eine Seite des Webservers mit Dateibrowser, um eine lokale Datei auszuwählen und dann mit der Schaltfläche „Transfer“ abzusenden. Die Datei landet im Pfad, aus dem QRCP heraus aufgerufen wurde. **-dw**

Senden und Empfangen aus der Shell: Das Tool QRCP nutzt einen eigenen Webserver, um Dateien von Smartphones per Browser zu empfangen oder Dateien zu übertragen.

Sudo: Aufzeichnen und Abspielen

Ein vorangestelltes „sudo“ ersetzt in der Linux-Kommandozeile nicht nur die Arbeit auf dem root-Account, sondern führt auch eine Kontrollinstanz ein. Denn sudo-Aktionen werden, anders als root, genau in den Logs protokolliert. Das dient nicht nur der Überwachung, sondern stellt auf Linux-Systemen auch eine Gedächtnisstütze dar.

Was habe ich gestern Nacht noch am Linux-System verändert? Diese Frage hat vor allem dann Brisanz, wenn nach vermeintlich kleinen Administrationsarbeiten an Konfiguration oder Dateien ein Dienst nicht mehr funktionieren will. Um im Notfall die eigenen Schritte zu rekonstruieren, hilft ein Blick in die Logdateien. „sudo“ hat eine Aufzeichnungsfunktion, welche ein abspielbares Protokoll der Shell sichert. In den Standardeinstellungen ist diese Protokollierung allerdings nicht aktiviert, sondern muss erst manuell eingeschaltet werden. Dazu öffnet das Kommando

```
sudo visudo
```

zunächst die Konfigurationsdatei von sudo im üblichen Editor der Shell. Dort kommen in den oberen Bereich der „Defaults“ folgende drei Zeilen als Ergänzung hinzu

```
Defaults log_output
Defaults! /usr/bin/
  sudoreplay !log_output
Defaults! /sbin/reboot
  !log_output
```

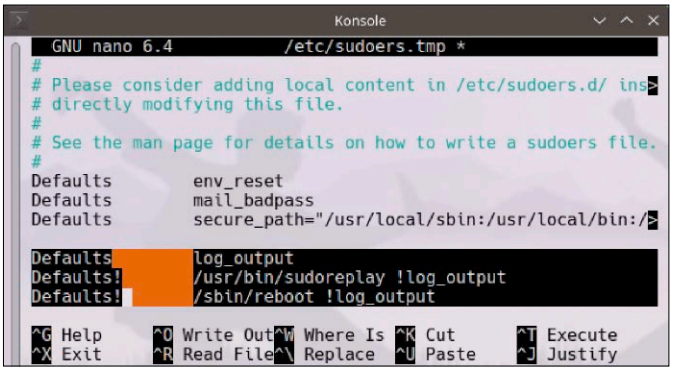
Nach dem Speichern der Datei zeichnet sudo dann jeden damit abgesetzten Befehl und dessen Ausgabe auf, in Form einer abspielbaren Animation im Textmodus. Die Eingabe von

```
sudo sudoreplay -l
```

zeigt alle Aufzeichnungen mit einer sechsstelligen ID hinter dem Part „TSID=“ an. Anhand dieser ID kann sudo dann die Aufnahme im Terminal mit

```
sudo sudoreplay <ID>
```

abspielen. Die Befehle werden dabei nur angezeigt und dies in der Geschwindigkeit, in der sie eingegeben wurden. Die Aufnahmefunktion geht dabei ziemlich weit und spielt sogar die Texteingaben in aufgerufenen Editoren ab. **-dw**



Sudo-Replay: Diese drei markieren Zeilen schalten einen internen Recorder des Sudo-Werkzeugs ein, das die Shell-Eingaben hinter „sudo“ zum späteren Abspielen aufzeichnet.

LINUX WELT

Mini-Angebot!

Satte **34,6 %** gespart!

3 x LinuxWelt + Geldprämie*

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 (Plus: Vorab erhalten Sie eine Ausgabe gratis) +
3 x LinuxWelt direkt aufs Smartphone & Tablet mit interaktivem Lesemodus +
10,- € Geldprämie (Wird mit dem Abopreis verrechnet)

=17,50 € (anstatt 26,75 Euro)

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

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

Ja, ich bestelle das LinuxWelt Mini-Angebot für 17,50 € und erhalte 3 Ausgaben + Geldprämie

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. Das Angebot ist innerhalb Deutschlands gültig.

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

LWPM062018

* 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

Tipps zur Hardware

Auf den nächsten drei Seiten wird Hardware gebändigt, verbunden und genauer angesehen: Von Netzwerkkabel über Webcams zu Logitech-Geräten geht es in den einzelnen Tipps um alltägliche Komponenten, die geschickt angeschlossen werden wollen.

VON DAVID WOLSKI

Ethernet: Anbindung und Geschwindigkeit

Im kabelgebundenen Netzwerk ist heute GBit-Geschwindigkeit üblich und damit Durchsatzraten von wenigstens 60 bis 80 MB pro Sekunde. Bleibt die tatsächliche Geschwindigkeit weit darunter, so hilft nur eine systematische Suche nach dem Flaschenhals im Netzwerk.

Ob eine Gigabit-Verbindung tatsächlich zustande kommt, ist von der Gegenstelle, dem Switch oder Router und seltener von den verlegten Kabeln abhängig. Der erste Schritt auf der Suche nach bremsenden Faktoren sollte dabei mit einem Blick auf das Linux-System beginnen: Ist die Schnittstelle dort überhaupt auf 1000 MBit (1 GBit) ausgelegt? Klappt in dieser Geschwindigkeit die Verbindung vom Rechner zum nächsten Ethernet-Port, etwa zum Switch?

1. Lokales System: In der Kommandozeile zeigt das Programm ethtool Details zu einer Ethernet-Schnittstelle an. Es ist in allen Linux-Distributionen verfügbar, muss aber meist noch installiert werden. In Debian/Ubuntu gelingt das mit diesem Terminalbefehl:

```
sudo apt install ethtool
```

Anschließend ermittelt zur Abfrage das Kommando

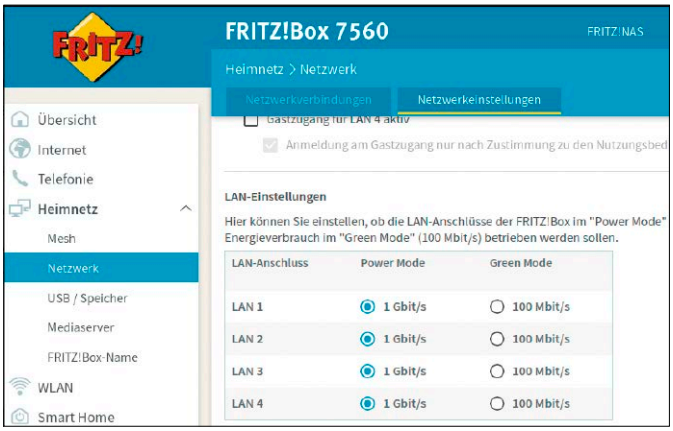
```
ip a
```

die Geräte-ID (Namen) der Ethernet-Schnittstelle, beispielsweise „enp3s0“. Die aktuellen Verbindungsinformationen kann nun der Befehl

```
ethtool enp3s0
```

abfragen. Die Zeile „Supported link modes“ gibt die unterstützten Geschwindigkeiten an, wobei „1000baseT/Full“ für Gigabit-Ethernet steht. In der Zeile „Advertised link modes“ ist angegeben, welche Ethernet-Modi die Schnittstelle über das verwendete Kabel anbietet, und „Link partner advertised link modes“ verrät, welche Geschwindigkeit die direkte Gegenstelle akzeptiert. Beide müssen ebenfalls mindestens“ 1000baseT/Full“ als besten Standard anzeigen, damit Gigabit-Ethernet funktioniert.

2. Switch und Router: Ein weiterer Blick auf den Switch und/oder den Heimrouter zeigt, ob dessen Ports Gigabit-LAN unterstützen. Spezielle Aufmerksamkeit verlangt die Fritzbox von AVM. Viermal Gigabit-Ethernet bieten nur die besseren Geräte. In der Administrationsoberfläche lohnt sich außerdem ein Blick in die Stromsparfunktionen unter „Heimnetz → Netzwerk → Netzwerkeinstellungen“. Hier ist nämlich für jeden Netzwerkport einstellbar, ob dieser mit 1 GBit („Power Mode“) oder stromsparend mit 100 MBit („Green Mode“) laufen soll.



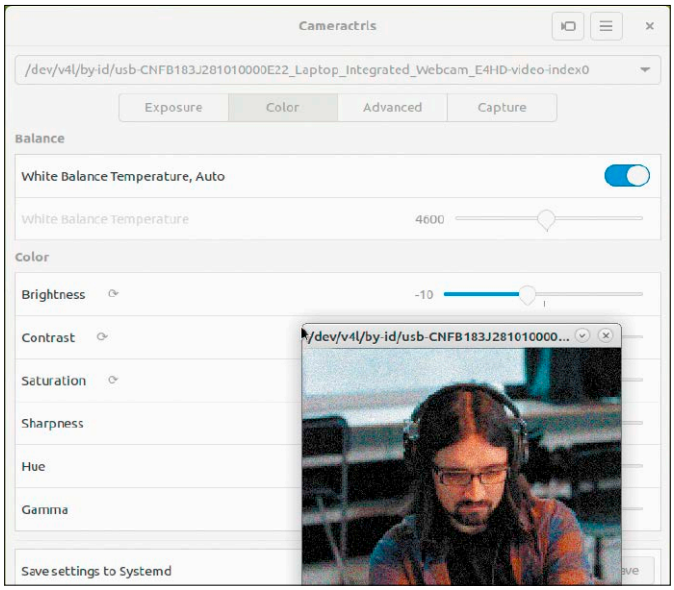
Volle Kraft: Damit Gigabit-Ethernet klappt, müssen alle Netzwerkgeräte diesen Standard anbieten. Auf einer Fritzbox lohnt sich ein Blick auf diese Porteinstellungen.

3. Kabel: Seltener, aber nicht ganz auszuschließen sind unpassende Ethernet-Kabel für Gigabit-LAN. Wer handelsübliche Cat-5e-Kabel verwendet, hat mit dem schnellen Gigabit-Netzwerkstandard kein Problem. Bei Cat-5-Kabeln, wie sie noch vor dem Jahr 1999 verlegt wurden, ist bei 100 MBit Schluss (Fast Ethernet). Keinen Einfluss auf die ausgehandelte Geschwindigkeit hat eine Abschirmung, die auf den Kabeln mit „STP“ (Shielded Twisted Pair) angegeben ist. **-dw**

Cameractrls: Feineinstellungen für Webcams

In wichtigen Videokonferenzen sollte das Bild der Webcam optimal passen. Die Bildqualität von integrierten Webcams in Notebooks ist aber oft nicht berauschend. Das grafische Tool Cameractrls kann dann Helligkeit und Kontrast der Kamera regeln.

Cameractrls ist noch kaum ein Jahr alt und der Weg in die Standard-Paketquellen von Linux-Distributionen ist noch weit (sofern es solide weitergepflegt wird). Es gibt aber schon ein universelles Flatpak (*https://flathub.org/apps/details/hu.irl.cameractrls*) sowie für Ubuntu ein



Ist das schön genug? Das Tool Cameractrls kann auf herkömmlichen Webcams Kontrast und Farben nachjustieren. Die Feinabstimmungen werden als Systemd-Script gespeichert.

Snap-Paket, das mit den beiden Befehlen

```
sudo snap install
  cameractrls
snap connect
  cameractrls:camera
```

einzurichten ist. Das zweite Kommando ist nötig, um dem Snap den Zugriff auf die Standard-Webcam zu gewähren. Für spezielle Kameraeinstellungen von Logitech und Kiyo Pro ist zur Einrichtung auch noch der Befehl

```
snap connect
  cameractrls:raw-usb
```

nützlich, um Ausschnitt und Tiefenschärfe steuern zu können. Das Programm selbst findet sich dann im Anwendungsmenü als „cameractrls“ und zeigt nach dem Start eine englischsprachige Benutzeroberfläche mit den Untermenüs „Exposure“ (Belichtung), „Color“, „Advanced“ und „Capture“.

Ein Klick auf das Kamerasymbol in der Titelleiste zeigt ein Livebild der Webcam. Wenn die passenden Feinabstimmungen getroffen sind, dann sichert ganz unten die Schaltfläche „Save“ alle Abstimmungen als benutzerdefiniertes Systemd-Script, das die gewünschten Einstellungen bei der Systemanmeldung automatisch anwendet. **-dw**

Videokonferenzen: Szenenbild mit OBS Studio

Für Livepräsentationen in Videokonferenzen genügt die Aufnahme per Webcam und Screensharing oft nicht. Wenn ein anspruchsvolleres Szenenbild gefragt ist, beispielsweise die Einblendung von Programmfenstern, Porträt und Firmenlogo, so erledigt die Software OBS Studio das Bühnenbild.

Die Verwendung von OBS Studio zum Bau von Szenenbildern für Videokonferenzen hat zudem den Vorteil, dass es Szenerien als Vorlage speichern und später wieder aufrufen kann. Auch ist es mit OBS Studio einfacher, weitere Videoquellen, etwa die Bildschirmausgabe eines zweiten Computers mit einem anderen Betriebssystem, in die Livepräsentation zu holen.

Die Software findet sich zwar in den Quellen der gut gepflegten Linux-Distributionen, ist in Ubuntu 22.04/22.10 aber nur als Snap-Paket vorhanden, dem etliche Plug-ins fehlen. Dies ist also keine vollwertige Ausgabe von OBS Studio. Besser ist es in Ubuntu, die neueste Version aus dem PPA der Entwickler als zu installieren. Dazu nehmen die Kommandos

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

die neue Paketquelle auf und

```
sudo apt install obs-
  studio
```

holt die aktuelle, stabile OBS-Studio-Version des Programms.

Webcam einbinden: Das ist der wichtigste Schritt, denn OBS Studio verlangt nach dem Kernel-Treiber „v4l2loopback“, um eine interne Webcam verfügbar zu machen.

Es ist aber nicht notwendig, dieses Kernel-Modul selbst zu kompilieren, denn die meisten Linux-Distributionen verfügen über ein Build-Script dafür, das über DKMS automatisch bei Kernel-Updates ausgeführt wird. In Ubuntu ist es mit den Kommandos

```
sudo apt install linux-
  generic
sudo apt install
  v4l2loopback-dkms
```

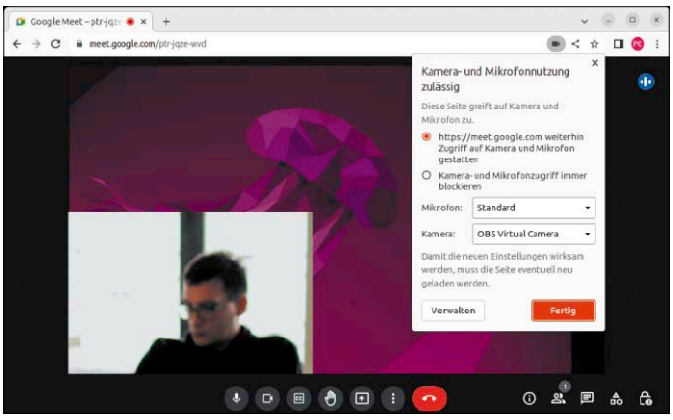
zu installieren und der Befehl

```
sudo modprobe
  v4l2loopback
```

lädt das Modul dann auch gleich (ohne Neustart).

Szenenbild bauen: In OBS Studio zeigt unten links der Abschnitt „Szenen“ die aktuelle Szenerie an, wie sie das Vorschaufenster oben ausgibt. Im Feld „Quellen“ daneben fügt ein Klick auf das Plus-Symbol weitere Audio- und Videoquellen von angeschlossenen Geräten hinzu. Die Internet-Webcam steht nun über „Videoaufnahmegerät (V4L2)“ bereit. Beispielsweise bindet „Bild“ eine bereits vorhandene Grafikdatei in die Szenerie ein, die im Vorschaubild oben die Maus wie gewünscht anordnen und auf Größe ziehen kann. Sieht die Szenerie gut aus, so streamt diese ein Klick auf „Virtuelle Kamera starten“ (rechts unten) für Videokonferenzprogramme und Webbrowser. Auf der Konfigurationsoberfläche des jeweiligen Konferenztools ist die virtuelle Kamera mit dem Livestream dann als „OBS Virtual Camera“ verfügbar.

Audio wird weiterhin über die verfügbaren Mikrofone aufgenommen, es handelt sich um einen puren Videostream. **-dw**



Szenenbild: OBS Studio kann ab Version 26 Webcams unter Linux einbinden und eine Szene als „Virtuelle Kamera“ wie hier in Google Meet streamen.

Solaar: Logitech-Geräte anbinden

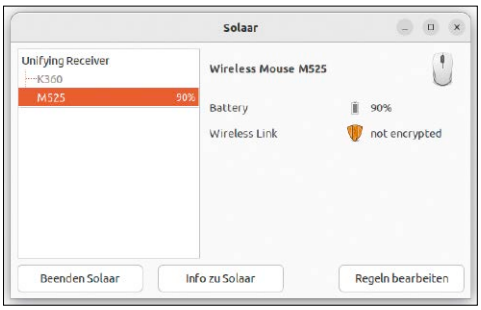
Drahtlose Logitech-Eingabegeräte arbeiten mit einem Empfänger am USB-Port, dem „Logitech Unified Receiver", der mehrere Geräte des Herstellers anbindet. Die Unterstützung unter Linux für diesen Receiver hat sich in den letzten Jahren deutlich verbessert. Das notwendige Konfigurationstool findet sich in den Standard-Paketquellen der tonangebenden Linux-Distributionen.

Ein Unified Receiver, leicht zu erkennen an dem orangen Sonnen-Logo, kann bis zu sechs Eingabegeräte von Logitech koppeln. Unter Linux funktioniert dies aber zunächst nur mit dem ersten Gerät zuverlässig. Kommen weitere hinzu, so schlägt die Verbindungsaufnahme (Pairing) meist fehl. Das Tool Solaar (*https://github.com/pwr-Solaar/Solaar*) ist dann auf dem Linux-System gefragt, um den Empfänger erneut in einen Pairingmodus zu versetzen. Es handelt sich um ein Programm, das in der Kommandozeile einsetzbar ist, aber auch eine grafische Oberfläche mitliefert. Die Installation ist einfach, denn das Paket „solaar" liegt in den Standardquellen der meisten Linux-Distributionen und ist in Debian/Ubuntu mit

```
sudo apt install solaar
```

eingerichtet.

Im Terminal versetzt das Kommando



Paarungsverhalten von Logitech-Mäusen und anderen Geräten: Solaar verbindet Eingabegeräte mit einem Unified Receiver, denn dieser nutzt sein eigenes USB-Protokoll.

```
solaar pair
```

den Unified Receiver in den Koppelungsmodus. Daraufhin muss das weitere Logitech-Gerät, das verbunden werden soll, kurz aus- und eingeschaltet werden, damit es Kontakt zum Receiver aufnimmt. Die Eingabe

```
solaar show
```

zeigt anschließend die verbunden Geräte an. Wird das Programm auf dem grafischen Desktop über dessen Anwendungsmenü gestartet, so sind diese Aktionen auch auf einer Oberfläche möglich. Links zeigt eine Liste den Receiver und die verbundenen Eingabegeräte an, rechts präsentiert Solaar Menüelemente zur Steuerung der jeweiligen Logitech-Geräte. Hier kann man nicht nur den Pairingmodus starten und den Batteriestatus prüfen, sondern beispielsweise bei Mäusen die Tastenbelegung ändern. **-dw**

Nvtop: Grafikkartenauslastung im Blick

Es ist einleuchtend, dass Spiele und Simulationen mit anspruchsvoller Grafik der GPU viel zu tun geben. Aber wie verhält es sich bei Desktops mit effektreicher Darstellung oder bei Open-CL- und CUDA-Anwendungen? Der Hardwaremonitor Nvtop für Grafikkarten gibt darüber Auskunft.

Der Name des Tools legt nahe, dass Nvtop nur für Nvidia-Grafikchips gemacht sei. Tatsächlich aber überwacht der Monitor für die Kommandozeile auch AMD- und Intel-Grafikchips beziehungsweise von integrierten Grafikeinheiten von CPUs. Bezüglich Intel und AMD gibt es aber noch Details zu Kernel und Version zu beachten: Leistungsdaten von MD-Grafikchips kann das Tool erst ab Linux-Kernel 5.14 auslesen, jene von Intel erst ab Version 5.19. Auch muss Nvtop zur Überwachung neuerer Grafikchip in einer frischen Version vorliegen, denn der Entwickler muss die Unterstützung immer wieder erweitern.

Daher funktioniert Nvtop aktuell nur in den neuesten Ausgaben von Linux-Distributionen optimal, also in Ubuntu 22.10, Fedora 36/37 und in Arch Linux. Dort findet sich das Paket „nvtop" zur Installation mit dem jeweiligen Paketmanager in den Standardquellen. In Ubuntu 22.10 ist das Paket allerdings schon wieder zu alt und es empfiehlt sich die Aufnahme eines PPAs über diese beiden Befehle im Terminal:

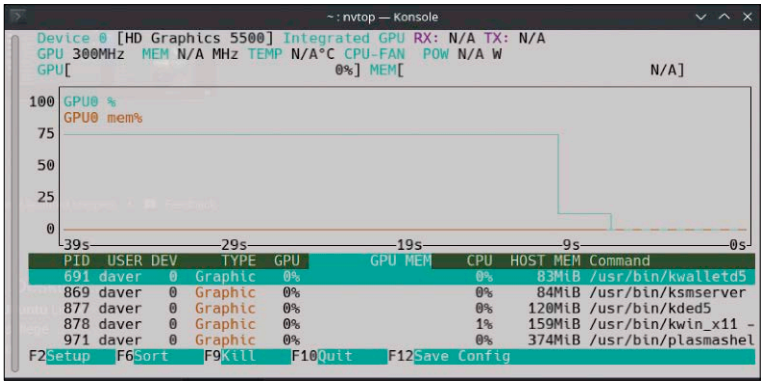
```
sudo add-apt-repository
  ppa:flexiondotorg/nvtop
sudo apt update
```

Mit dem Befehl

```
sudo apt install nvtop
```

ist das Hardwaretool dann eingerichtet und die Eingabe *nvtop* ruft es auf. Auf Intel-GPUs zeigt es zunächst noch den (englischsprachigen) Hinweis, dass einige Leistungsdaten wie Speicherauslastung, Temperatur und Ventilatorgeschwindigkeit nicht angezeigt werden. Das Programm zeigt dann im Terminal oben ein Diagramm der Auslastung von GPU und des GPU-Speichers und darunter eine Liste jener laufenden Prozesse, welche den Grafikchip beanspruchen. Zum Sortieren dient ein Druck auf F6, um eine Kategorie wie GPU- und CPU-Auslastung auszuwählen, die links angezeigt wird. Die Taste F10 beendet Nvtop.

Übrigens: Beim Aufruf mit normalen Benutzerrechten listet der Hardwaremonitor nur die eigenen Prozesse auf. Daher empfiehlt sich stets ein Start mit *sudo nvtop*. **-dw**



Gierige Grafik: Wie stark der Grafikprozessor von Nvidia, AMD oder Intel ausgelastet ist, zeigt das neue Tool Nvtop, das neuere Kernel-Versionen voraussetzt.

PC-WELT PLUS

GRATIS! Eine Ausgabe gedruckt & digital

Jetzt kostenlos die gedruckte & digitale Ausgabe bestellen!

Jetzt bestellen unter
www.pcwelt.de/gratis 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 die PC-WELT gratis.

Möchten Sie die PC-WELT Plus anschließend weiter lesen, brauchen Sie nichts zu tun. Sie erhalten die PC-WELT Plus für weitere 12 Ausgaben zum aktuellen Jahresabopreis von z.Zt. 87,60 EUR. Danach ist eine Kündigung zur übernächsten Ausgabe jederzeit möglich.

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PWPNA14140

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

Softwaretipps

Die Softwaretipps fokussieren sich auf Libre Office und auf Google-Dienste. Im Falle von Google steht der übliche Metatipp im Raum, dass die überragenden Google-Webdienste kaum verzichtbar sind, aber kritische Dosierung benötigen.

VON HERMANN APFELBÖCK

Google Tabellen: Teamwork und Freigaben

Wer Tabellen und Texte für ein Team anbieten will oder muss, ist mit den exzellenten Angeboten von Google Drive oder Microsoft Onedrive ungleich schneller produktiv als mit eigenen Lösungen auf der eigenen Homepage. Der nachfolgende Tipp löst ein etwas anspruchsvolleres, aber keineswegs seltenes Freigabeproblem für Google-Tabellen.

Bei der Freigabe von Google-Dokumenten gibt es zwei prinzipielle Optionen:

1. die Freigabe für definierte Personen, die dann ein Google-Konto zum Zugriff benötigen. Der erlaubte Zugriff lässt sich dann noch für jedes einzelne Konto genauer regeln („Mitarbeiter" mit Schreibzugriff, „Betrachter" mit Nur-Lesezugriff, ferner „Kommentator" mit Nur-Lesezugriff, aber zusätzlicher Kommentaroption).

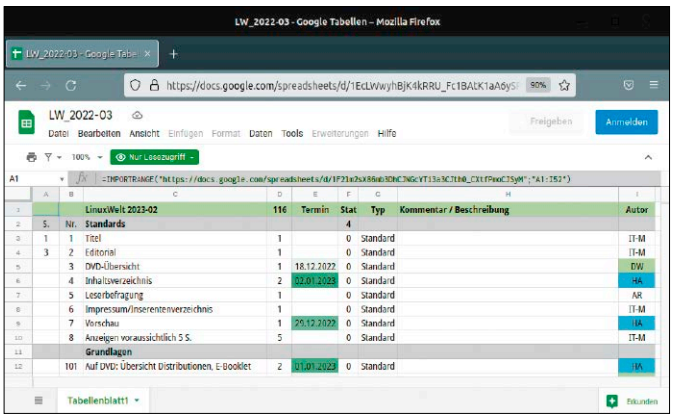
2. die pauschale Freigabe („Jeder, der über den Link verfügt"). Auch hier kann zwischen den Zugriffsrechten „Mitarbeiter", „Betrachter" und „Kommentator" unterschieden werden, dies aber dann natürlich pauschal und nicht personenbezogen.

Wenn nun eine Arbeitstruppe eine gemeinsame Tabelle nutzen soll, ergeben sich oft zwei sehr unterschiedliche Probleme:

1. Google-Verweigerer im Team lehnen es konsequent ab, ein Google-Konto zu nutzen.

2. Bestimmte Mitarbeiter sollen nur einen Teil der Tabelle einsehen.

Eine elegante Lösung für beide Probleme ist eine zweite, leere Tabelle mit folgender Funktion in der ersten Zelle A1:



Tabellenauszug oder Extra-Freigabe als Link: Die Funktion „Importrange" ermöglicht die dynamische Kopie eines Tabellenbereichs in einer zweiten Tabelle.

```
=IMPORTRANGE("[URL der
  Quelltabelle]";
  "[Bereich]")
```

Ein konkretes Beispiel wird dann etwa so aussehen:

```
=IMPORTRANGE("https://
  docs.google.com/
  spreadsheets/
  d/1F21m2sX8NGcYT_CJSyM/
  edit#gid=0";"A1:I52")
```

Beachten Sie, dass dieser Bezug nur die Daten übernimmt und je nach Datenmaterial eine manuelle Nachformatierung notwendig ist. Das ist aber nur einmal erforderlich.

Die zweite Tabelle liefert dann dynamisch alles aus, was gerade Stand in der Primärtabelle ist. Für die Sekundärtabelle verwenden Sie eine pauschale Linkfreigabe mit Nur-Leserecht („Betrachter"). Dies ist vor allem dann zwingend, wenn die Sekundärtabelle nur einen Ausschnitt der Quelltabelle anzeigen soll.

Mit Schreibrecht wäre es dem Mitarbeiter nämlich möglich, den Tabellenbereich (im Beispiel „A1:I52") einfach beliebig größer zu definieren. **-ha**

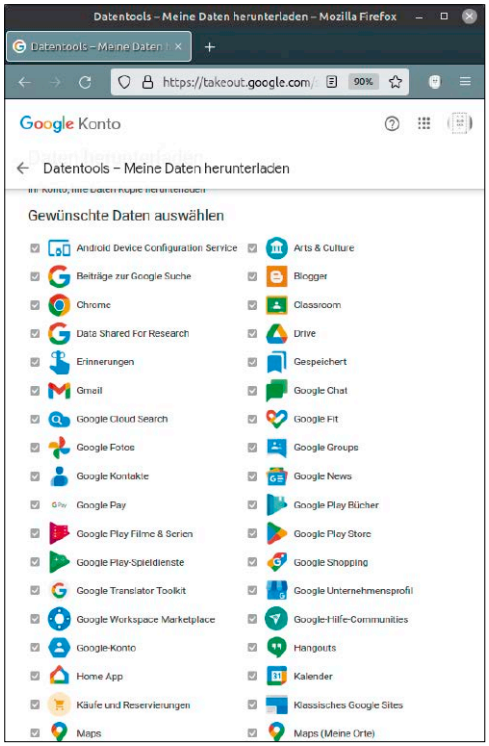
Google: Der ultimative Google-Check

Wenn Sie einige Jahre mit einem Google-Konto, mit mehreren Geräten und mit GPS-Chip im Smartphone unterwegs waren, weiß Google jede Menge über Sie: welche Kontakte Sie haben, was Sie in Google, Youtube, Maps, Google Shopping und im Play Store suchen, was Sie im Kalender vermerken und auf Google Drive speichern. Hinzu kommen die Bewegungsdaten des Smartphones. Haben Sie noch den Überblick, was Sie alles an Google-Diensten nutzen?

Eine Übersicht über vielleicht längst vergessene Aktivitäten, Infos und Uploads bieten folgende Adressen:

https://myaccount.google.com/
https://myaccount.google.com/profile
https://myaccount.google.com/dashboard
https://myactivity.google.com/myactivity
https://drive.google.com/drive/my-drive
https://photos.google.com

Wenn Sie hier alle Informationen und Dienste durchgehen und dabei Altlasten finden, die Sie heute Google nicht mehr anvertrauen möchten, dann entfernen Sie diese Inhalte oder



Google bietet ein „Take-out“ sämtlicher bei Google gespeicherten Daten. Die Durchsicht dieser Daten kann zum Abschalten etlicher Google-Dienste motivieren.

beenden die Dienste (im „Dashboard“). Bei den meisten aufgeführten Diensten gibt es nach dem Aufklappen ein Menü mit der Option „Daten herunterladen“. Dies kann sowohl dem besseren Überblick dienen als auch der lokalen Sicherung, bevor Sie einen Google-Dienst entfernen.

Eine umfassende Methode, alles einzusammeln, was Google an Daten besitzt, ist der Download aller Daten aus allen Diensten („Take-out“). Dafür gibt es diese beiden Adressen:

https://www.google.com/settings/takeout

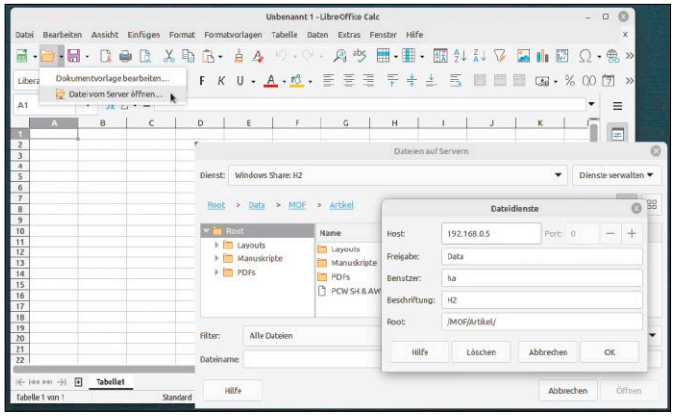
https://takeout.google.com/settings/takeout/light

Beide erlauben per Mausklick die Auswahl aller oder einiger Google-Dienste. Die zweite Adresse ist einfacher, die erste bietet aber mehr Downloadoptionen. Der vollständige Download aller bei Google gespeicherten Daten inklusive Google Mail, Google Drive, Google Fotos kann erheblichen Umfang haben. Daher ist es sinnvoll, alle Dienste, die man durch tägliche Nutzung im Griff hat, vom „Take-out“ auszunehmen. Interessant ist ja, was Google ohne aktive Mitwirkung des Nutzers ansammelt. Sie erhalten nach dem Auspacken des Take-outs eine sauber organisierte Verzeichnisstruktur. Im Ordner „Meine Aktivitäten“ finden Sie aufschlussreiche Protokolle und unter „Anzeigen“, „Bildersuche“, „Google-Suche“, „Maps_ Timeline“, „Shopping“ sammelt Google über Jahre, an welchen Inhalten, Orten und Produkten Sie interessiert sind. **-ha**

Libre Office: Server einrichten

Libre Office bietet eine eigene Verwaltung für lokale Samba- und SSH-Server. Einmal dort eingerichtet, sind die Dateimenüs „Vom Server öffnen“ und „Auf Server speichern“ produktiv zu nutzen. Damit entfällt vorheriges Mounten im Dateimanager.

Das Anlegen eines Datenservers muss nur in einer Office-Komponente erfolgen und gilt dann für alle. Wenn Sie erstmals das Menü „Datei → Vom Server öffnen“ verwenden, erscheint das Fenster „Dateien auf Servern“ mit leeren Unterfenstern. Über „Dienste verwalten → Dienst hinzufügen“ binden Sie einen Dateiserver ein. Die vielversprechende Liste zeigt unter anderem auch „Google Drive“, „Onedrive“ (in aktuellen Versionen), „Sharepoint“ und etliche weitere Serverdienste. Nach unserer Erfahrung funktionieren aber nur lokale Serverdienste zuverlässig – also in erster Linie „SSH“ und „Windows Freigabe“.



Libre Office kann Serverdienste selbst verwalten. In der Abbildung wurde ein Samba-Server hinterlegt, der dann ohne System- oder Dateimanager-Hilfe genutzt werden kann.

Bei einer Windows/Samba-Freigabe geben Sie den Hostnamen oder die IP-Adresse des Servers und den Freigabenamen ein sowie das Samba-Konto und dessen Kennwort. Im Feld „Root“ verwenden Sie „/“, falls Sie die komplette Freigabe ab oberster Ebene in Libre Office benötigen. Andernfalls ist als „Root“ auch ein Unterordner wie „/Texte/2023/“ möglich. Mit „OK“ wird der Server angelegt, wobei bei erster Nutzung dieser Funktion ein Masterpasswort für Libre Office abgefragt wird. Dieses Masterpasswort schützt und verschlüsselt Ihre Servereinträge.

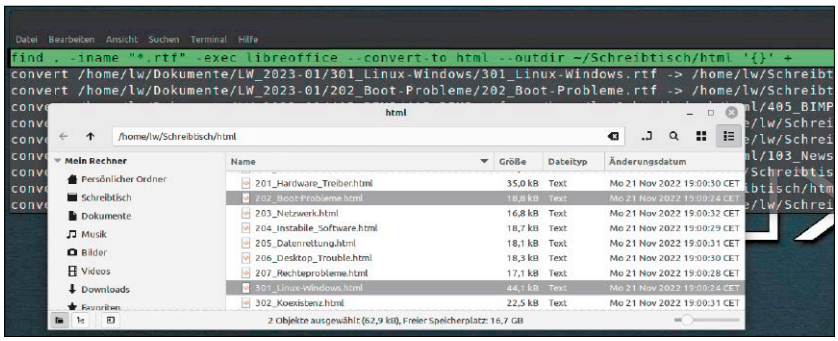
Für SSH-Server ist das Vorgehen weitgehend analog. Hier empfiehlt sich aber als „Root“-Vorgabe für Libre Office immer ein genauerer Pfad, um sich das Abwärtsnavigieren etwa nach „/home/user/Dokumente“ zu ersparen.

Einmal angelegt, öffnen und speichern Sie über die Serveroptionen im Dateimenü. Sind mehrere Server eingetragen, wählen Sie über das Dropdown-Feld „Dienst“ den aktuell gewünschten. **-ha**

Libre Office: Massenkonvertierung

Textverarbeitungen unterstützen neben ihrem nativen Speicherformat immer auch diverse Fremdformate, die sie öffnen oder mit „Speichern unter“ beziehungweise „Exportieren“ speichern können. Libre Office geht hier mit seinem Konvertierungsschalter ein ganzes Stück weiter und kann ganze Dokumentsammlungen umwandeln.

Die interessantesten Exportformate für Textdokumente sind purer Text („txt“), HTML („html“) und PDF („pdf“). Purer Text ist



Massenkonvertierung mit Libre Office: Die Suite bietet eine frappierend einfache Funktion, um diverse Formate in Text, PDF oder HTML umzuwandeln.

hilfreich, um Office-Binärformate in andere Medien einzubauen oder einfacher durchsuchbar zu machen, PDF bietet eine neutrale und überall identische Darstellun, und HTML erlaubt den Einbau in Webservern.

Folgende Befehle

```
libreoffice --convert-to
  pdf *.odt
libreoffice --convert-to
  txt *.docx
libreoffice --convert-to
  html *.docx
```

verarbeiten Writer- und Word-Dokumente im aktuellen Verzeichnis. Die Ausgabedateien übernehmen die Originalnamen und erhalten eine neue Extension. Soll die Ausgabe in ein anderes Verzeichnis erfolgen, hilft der zusätzliche Schalter „--outdir [...]“:

```
libreoffice --convert-to
  pdf *.odt --outdir ~/
  Schreibtisch
```

Mit der externen Hilfe von find ist sogar rekursive Massenkonvertierung in allen Unterordnern möglich (hier ausgehend vom aktuellen Verzeichnis):

```
find . -iname "*.docx"
  -exec libreoffice
  --convert-to txt '{}' +
```

Das Ganze funktioniert auch mit vielen anderen Dateiformaten, mit denen Libre Office umgehen kann. Die komplette Liste der zahlreichen Ein- und Ausgabeformate finden Sie unter *https://help.libreoffice.org/latest/de/text/shared/guide/convertfilters.html*. Diese beschränken sich keineswegs auf Textformate, sondern umfassen auch Tabellenkalkulation, Präsentation und Bildformate. **-ha**

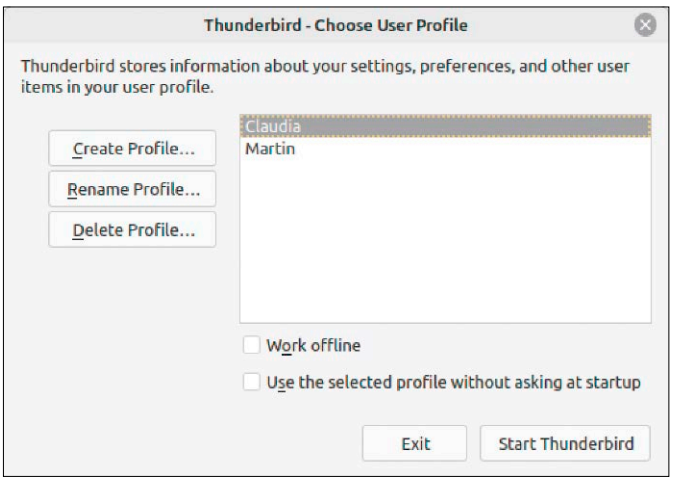
Thunderbird: Mails am Wohnzimmer-PC

Nicht auf jedem Mehrbenutzer-PC herrschen strenge Regeln: Ein Familien-PC, der in erster Linie den Fernseher füttert und Websuche leistet, benötigt nicht unbedingt getrennte Benutzerkonten. Wenn hier auch Mails abgeholt werden, kann das im selben Benutzerkonto und trotzdem mit sauber getrennten Mailbereichen für verschiedene Personen erfolgen. Dazu verhilft Thunderbird mit seiner Profilverwaltung.

So funktioniert's: Sie starten Thunderbird zunächst im Terminal mit diesem Kommando:

```
thunderbird
  --ProfileManager
```

Unter Linux ist der danach angezeigte Profildialog englischsprachig: Mit „Create Profile“ erstellen Sie das erste Profil und vergeben dafür den Namen des Nutzers. Danach wiederholen Sie den Vorgang für weitere Benutzer. Deaktivieren Sie dann unten unbedingt die Option „Use the selected profile without asking...“. Thunderbird soll nämlich künftig beim Start immer die Profilauswahl, also die angelegten Benutzer, zeigen und nachfragen, welches Profil gestartet werden soll. Danach starten Sie nacheinander die angelegten Profile und richten dort die zugehörigen Mailkonten ein (oder überlassen dies den Benutzern). Der explizite Parameter *thunderbird --ProfileManager* ist künftig nicht mehr nötig, da kein Default-Profil angegeben wurde. Das Mailprogramm zeigt also beim Start in jedem Fall die Profilauswahl und lädt dann das ausgewählte Profil. **-ha**



Ein Benutzerkonto, aber getrennte Mailprofile: Thunderbird ermöglicht am Familien-PC ohne Benutzerwechsel eine saubere Mailkonfiguration.

Libre Office Writer: Wortergänzungen nutzen

Der Writer indiziert jeden geladenen Text, sammelt die enthaltenen Wörter und schlägt sie beim Tippen vor. Dann genügt die Eingabe weniger Buchstaben, bis ein passender Wortvorschlag erfolgt, den Sie mit Eingabetaste übernehmen.

Je umfangreicher und komplexer der aktuelle Text bereits ist, desto umfangreicher fällt die Wörterliste aus. Die praktische Funktion lässt sich auch für neue Texte nutzen. Die Wortergänzung ist eine dynamische Funktion, die sich auf alle aktuell geöffneten Dokumente bezieht. Feineinstellungen über Umfang und Verhalten können Sie unter „Extras → AutoKorrektur → AutoKorrektur-Optionen“ auf der Registerkarte „Wortergänzung“ vornehmen. Die Mindestwortlänge sollte eher hochgesetzt werden, damit sich die Wortergänzungen auf komplexe und lange Wörter beschränken. Beim Anlegen neuer Texte genügt es, vorher eine thematisch ähnliche und möglichst umfangreiche Datei zu laden. De-

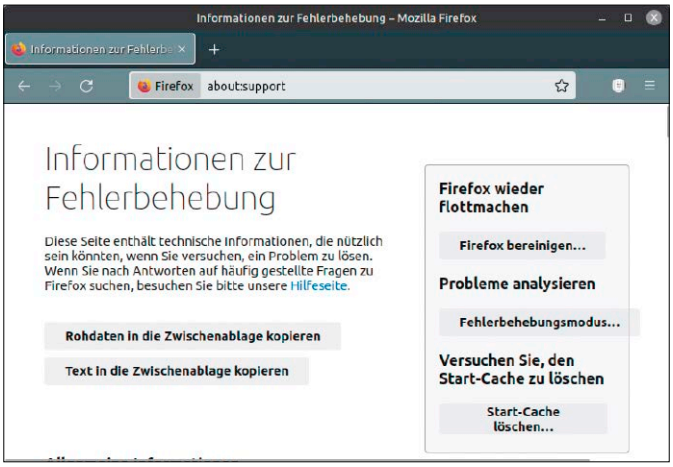
ren dynamisch generierte Wörterliste gilt dann auch für die neue Datei.
Wer die Funktion weiter optimieren will, verwendet am besten eine speziell angelegte Wörterliste mit allen notwendigen Fachbegriffen, Firmennamen, Webadressen sowie mit typischen Wörtern, wo man erfahrungsgemäß zu Tippfehlern tendiert. **-ha**

Firefox: Bewährte Aufräummethoden

Firefox ist wie jeder Browser ein anspruchsvolles Programm, das nicht nur CPU und RAM, sondern auch den Datenträger fordert. Periodische Säuberung schafft Platz und im Notfall helfen drastischere Maßnahmen.
Die lokal gespeicherten Daten kann Firefox über „Chronik → Neueste Chronik löschen“ entsorgen. Hier stehen zeitlich unter anderem „Alles“ oder „Die heutige Chronik“ zur Auswahl, inhaltlich sind alle Angebote außer „Cookies“ zu empfehlen (Cookies sind klein und unterm Strich eine Komfortfunktion auf häufig genutzten Sites).
Eine Säuberung, die eher für lahmende Feuerfüchse taugt, ist die Option „Firefox bereinigen“ auf der internen Seite „about:support“.
Hier geht es zurück zu Standardeinstellungen, wobei aber immerhin Lesezeichen und gespeicherte Kennwörter erhalten bleiben.
Noch weitreichender ist die Einrichtung eines neuen Profils nach diesem Firefox-Start:

```
firefox --profilemanager
```

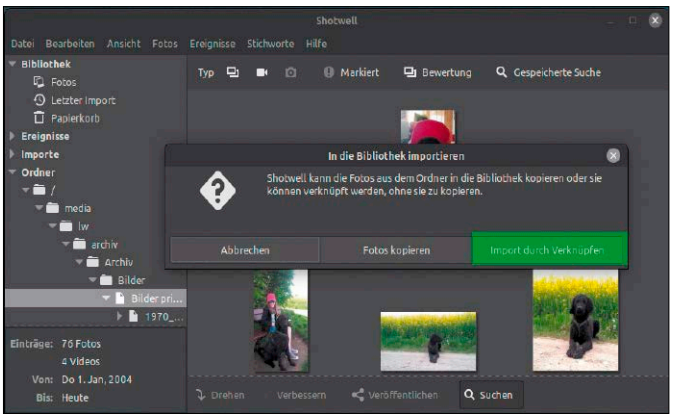
Diese Maßnahme ist radikal, bedeutet aber auch für einen sorgfältig eingerichteten Firefox keinen großen Aufwand, sofern alle Einstellungen über die Synchronisierung wieder zu restaurieren sind. **-ha**



Firefox-Bereinigung: Die interne Supportseite bietet einige nicht-destruktive Aufräumoptionen.

Shotwell: Schlagwörter für Fotos

Eine schnelle Personen-, Orts- oder Motivsuche ist in Fotosammlungen auf der Basis von Kamera-Dateinamen wie „CIMG2810.JPG“ und „20201022_152150.jpg“ ist schlicht unmöglich. Immerhin schreiben Kameras Metadaten in den Exif-Block der Bilddateien, also Aufnahmedatum und Ortsinfos (Geotags). Zur besseren Organisation der Fotos lässt sich der Exif-Block mit den Metadaten durch eigene Infos erweitern. Je nach Bildviewer nennen sich solche Infos „Markierung“, „Schlagwort“ oder „Stichwort“.
Systematische Personen-, Orte- und Aktionen-Tags sind unschlagbar, um Bilder schnell zu filtern. Das kostet zunächst Zeit, ist aber nachhaltig, weil diese Tags dauerhaft in den Bilddateien gespeichert werden. Sie gelten also unabhängig von der Software und vom Betriebssystem. Die meisten Linux-Bildviewer können solche Infos lesen und schreiben. Wenn es Ihnen nur um eine einfache Bildverwaltung geht, brauchen Sie kein Flaggschiff wie Digikam, dafür genügen die folgenden kleinen Pragmatiker:
In **Shotwell** gehen Sie auf „Datei → Aus Ordner importieren“. Wählen Sie dann die Option „Nur Verweise importieren“, denn andernfalls werden alle Dateien physisch kopiert. Bereits vorhandene Infotags werden beim Import automatisch eingelesen und auch sofort in der Navigationsspalte angezeigt. Ein Klick auf einen Tag filtert sofort die passenden Dateien. Neue Infos sind nach Rechtsklick und „Stichworte hinzufügen“ sowie „Stichworte ändern“ für einzelne wie mehrere markierte Bilder jederzeit möglich. Außerdem gibt es Bewertungen, gespeicherte Suchfilter und eine chronologische Ereignissortierung.
Gthumb (ähnlich Pix in Linux Mint) kopiert mit der Option „Datei → Importieren von → Ordner“ alle dort enthaltenen Bilder physisch unter „~/Bilder“ in das Home-Verzeichnis, was bei großen externen Bildersammlungen kaum erwünscht ist. Wählen Sie daher über die Navigationsspalte den ursprünglichen Quellordner mit den Bilddateien. Danach erscheint rechts oben über dem Anzeigefenster das unscheinbare, aber wichtige „Ordnen“. Wenn Sie hier „Schlagwort eingebettet“ wählen, werden alle Tags eingelesen. Diese zeigen sich danach in der Navigationsleiste unter „Kataloge → Schlagwörter“. Änderungen oder Neudefinitionen von Tags erfolgen für die markierten Bilder nach Rechtsklick und der Option „Schlagwörter“. **-ha**



Shotwell-Import: Der Import muss sein, damit Shotwell sämtliche Bilder analysiert. Das physische Kopieren der Bilder in Home-Verzeichnis ist aber nicht erforderlich.

Desktoptipps

Neben Tipps zum neuen Gnome 43 und Ubuntu 22.10 stehen diesmal auch die kleineren Desktops XFCE und LXQT im Fokus. Diese sind nämlich wandelbarer und attraktiver, als die meisten Anwender von Gnome, KDE und Co. es vermuten.

VON HERMANN APFELBÖCK

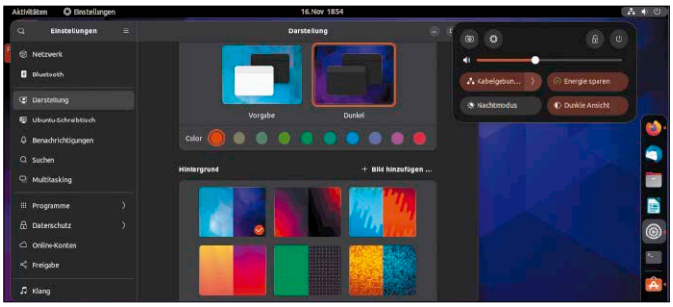
Gnome 43: Hell-Dunkel-Hintergründe

Der jüngste Gnome 43 hat ein neues optisches Feature, das garantiert vielen Nutzern gefallen wird. Praktischen Nutzwert hat das Ganze zwar kaum, aber es sorgt für einen perfekten Gesamteindruck beim Umschalten vom hellen auf den dunklen Modus und umgekehrt. Ubuntu übernimmt Gnome bekanntlich nicht in der originalen Ausführung und daher muss man beim aktuellen Ubuntu 22.10 etwas nachhelfen.

Gnome 43 hat den Systray-Bereich in der Systemleiste überzeugend überarbeitet. Neben funktional bedeutenderen Funktionen wie Netzwerk und Abschaltoptionen gibt es hier auch die Umschaltoption „Dunkle Ansicht“ (zur hellen Ansicht geht bei aktuellem Dunkelmodus es mit demselben Klick). Um solches Umschalten optisch zu perfektionieren, gibt es komplementäre Hell-Dunkel-Hintergrundbilder.

Es handelt sich dabei um abstrakte Themen gleichen Stils, die sich aber in Farbgebung und Helligkeit klar unterscheiden. Beim Umschalten des optischen Modus wechselt Gnome dann auch zum passenden Hintergrundbild.

Der von Canonical angepasste Gnome 43 unter Ubuntu 22.10 kann hier erst mitspielen, wenn



Neuer Gnome-Service: Komplementäre Hintergrundbilder wechseln automatisch mit, wenn der Darstellungsmodus geändert wird.

Sie die speziellen Hintergründe manuell nachladen. Nach

```
sudo apt install gnome-backgrounds
```

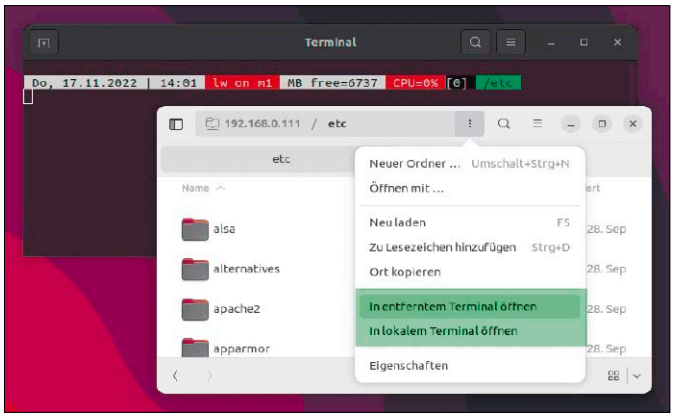
erscheinen die Hintergrund-Doppel unter „Einstellungen → Darstellung“ und können hier gewählt werden. Geht man dann auf den Systray-Bereich der Systemleiste und schaltet mit Klick auf „Dunkle Ansicht“ auf die andere Ansicht, wirkt sich das nun sofort auch auf das Hintergrundbild aus. **-ha**

Gnome 43: Nautilus und Terminal

Der Weg vom grafischen Dateimanager zum Terminal hat bei Gnome bislang eine externe Gnome-Erweiterung erfordert. Ab Gnome 43 ist das anders: Sowohl in der Nautilus-Adresszeile als auch im Kontextmenü aller Ordner erscheint mindestens eine neue Standardoption. Eine zweite gibt es für SSH/SFTP-Verbindungen und diese lohnt eine Optimierung.

Die Kontextoption „In Terminal öffnen“ ist als neuer Gnome/Nautilus-Standard in jedem Fall zu begrüßen. Noch bemerkenswerter ist diese Option für im Dateimanager gemountete Netzressourcen. Bei Samba-Freigaben geht das Terminal mit diesem Befehl ohne Umstand in den Gnome-Mountordner unter „/run/user/[xxxx]/gvfs/...“.

Handelt es sich um eine SSH/SFTP-Verbindung, wird es noch besser: Jetzt bietet Nautilus zwei Optionen: „In lokalem Terminal öffnen“ startet das Terminal im lokalen Mountordner mit dem übergebenen Pfad. Es gibt aber auch noch „In entferntem



Nautilus unter Gnome 43: Diese neuen Kontextoptionen sind nützlich und werden noch besser, wenn man etwas nachoptimiert.

Terminal öffnen“, was sofort eine SSH-Terminalverbindung startet. Dabei geht Gnome allerdings davon aus, dass sich der

aktuelle Systembenutzer verbinden will. Dann genügt die Eingabe des Systempassworts, das dieser Benutzer auf dem entfernten Rechner besitzt. Sinnvoll ist die Option „In entferntem Terminal öffnen“ also nur, wenn der lokale Benutzer ein gleichnamiges Konto auf dem entfernten Rechner besitzt. Richtig komfortabel wird die Option, wenn mit (Beispiel)

```
ssh-keygen
ssh-copy-id -i ~/.ssh/id_
  rsa.pub
  sepp@192.168.178.20
```

eine Schlüsselanmeldung eingerichtet wird.

Dann besteht der Weg vom Nautilus-Ordner zum SSH-Terminal an diesem Pfad nur noch aus zwei Klicks. **-ha**

KDE: Plasma Vaults

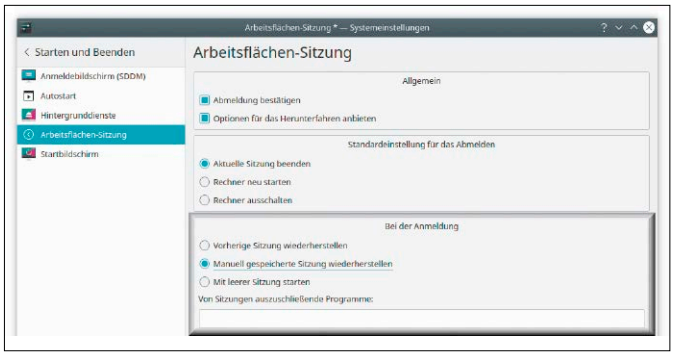
Plasma-Vaults sind ein spezielles Angebot von KDE, die durch ein Vorhängeschloss in der Kontrollleiste repräsentiert werden. Es handelt sich um eine einfache Dateiverschlüsselung, die durch die Desktopintegration besonders komfortabel ausfällt.

Ein Klick auf das Symbol klappt ein Fenster aus, wo Sie ein „Neues Vault erstellen“. Nach der Namensvergabe fragt Plasma Vault das gewünschte Passwort ab und danach die beiden Speicherorte des Containers. Den ersten – den verschlüsselten – Ort sollten Sie nicht ändern, wenn Sie mit den darunterliegenden Verschlüsselungsmethoden nicht näher vertraut sind. Der Ordner hingegen, wo Sie mit den entschlüsselten Daten arbeiten, kann an jeder bequemeren Stelle (etwa am Desktop) eingerichtet werden. Ist das Plasma Vault nach Kennworteingabe geöffnet, stehen die Daten in diesem Ordner uneingeschränkt zur Verfügung. Sobald der Container über das Vorhängeschloss ausgehängt wird, ist dieser Mountordner hingegen leer.

Die verschlüsselten Daten (mit verschlüsselten Dateinamen) befinden sich unter „~/.local/share/plasma-vault“. **-ha**

KDE: Sessionverwaltung im Griff

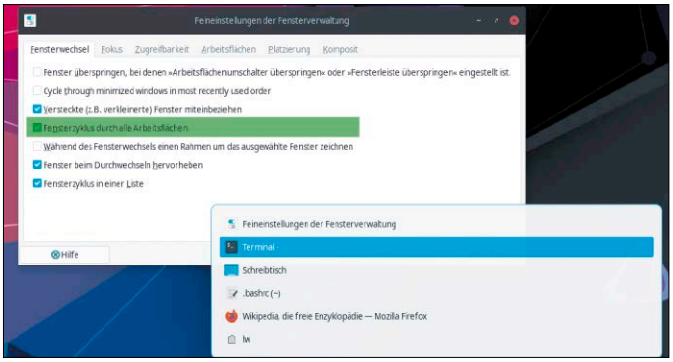
KDE hat die Angewohnheit, sich beim Abmelden oder Herunterfahren des PCs alle laufenden Anwendungen zu merken. Bei der nächsten Anmeldung springen dann die gleichen Programme automatisch an. Diese Funktion soll die Wiederaufnahme der Arbeit beschleunigen, ist aber meistens nur störend und kontraproduktiv.



Wiederherstellen der Sitzung: Diese KDE-Funktion lässt sich komplett abschalten oder – wie hier – bedarfsweise aktivieren. Als Standard ist sie eher lästig.

Dieses irritierende Verhalten ist auf vielen KDE-Distributionen als Standard voreingestellt. Die Erinnerungsfunktion an die Programme der letzten Sitzung findet sich unter „Systemeinstellungen → Arbeitsflächen-Sitzung“. Damit sich KDE keine Anwendungen beim Abmelden und Abschalten mehr merkt, aktivieren Sie hier die Option „Mit leerer Sitzung starten“. Weniger störend ist die Option „Manuell gespeicherte Sitzung wiederherstellen“: Ist dieser Punkt aktiviert, zeigt das Anwendungsmenü den zusätzlichen Menüpunkt „Sitzung speichern“. Dieser kann alle momentan laufenden Programme als Zusammenstellung sichern und beim nächsten Start automatisch starten, falls Sie dies explizit wünschen. **-ha**

XFCE: Taskwechsel mit allen Tasks



Alle Tasks von allen Arbeitsflächen: Der Alt-Tab-Taskwechsler in XFCE ist standardmäßig so eingestellt, dass er nur die Fenster der aktuellen Arbeitsfläche anbietet.

XFCE ist standardmäßig so konfiguriert, dass der Taskswitcher (Hotkey Alt-Tab) nur die Fenster der aktiven Arbeitsfläche anbietet. Für Systembenutzer, die ausgiebig virtuelle Arbeitsflächen verwenden, ist das unpraktisch.

Wenn Alt-Tab die aktuell geöffneten Fenster aller Desktops berücksichtigen soll, starten Sie die „Einstellungen“ (xfce4-settings-manager) und gehen zum Punkt „Feineinstellungen der Fensterverwaltung“. Dort finden Sie im Register „Fensterwechsel“ die einschlägige Option „Fensterzyklus durch alle Arbeitsflächen“.

Wer auf mehreren virtuellen Arbeitsflächen stets diverse Programme laufen hat, sollte dort eine weitere Option aktivieren: „Fensterzyklus in einer Liste“ verkleinert die Anzeige des Taskswitchers auf eine reduzierte und schmucklose Liste, die aber mit Icon und Beschreibung für den gezielten Taskwechsel völlig ausreicht. **-ha**

LXQT: Optimierte Systemleiste

Der kleine LXQT-Desktop ist erstaunlich anpassungsfähig. Die Konfiguration der Systemleiste ist zwar etwas umständlicher als beim vergleichbaren XFCE, aber funktional ebenbürtig. Damit bauen Sie sich das, was unter Windows 11

oder Gnome überhaupt nicht funktioniert und was selbst unter KDE oder Cinnamon vergleichsweise schwerfällt: eine attraktive, vertikale Systemleiste, die zu breiten modernen 16:10-Displays passt.

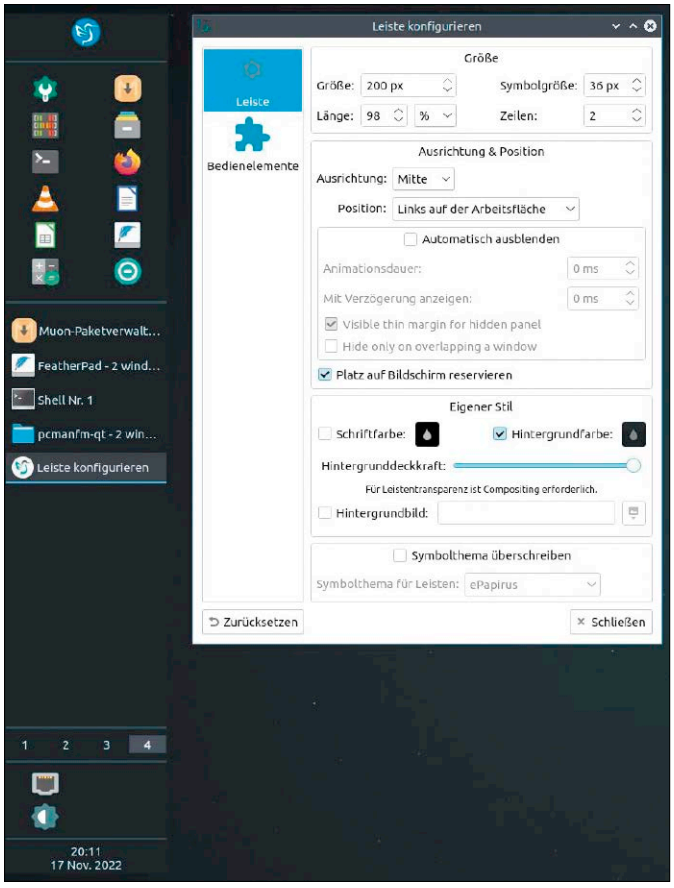
Die Verlagerung der standardmäßig horizontalen Leiste als vertikale an den linken oder rechten Rand gelingt nach Rechtsklick auf die Leiste über „Leiste konfigurieren → Leiste → Position". In der Regel ist die vertikale Leiste samt enthaltenen Icons jetzt zu schmal und die Symbole zu klein.

Das korrigieren Sie im gleichen Dialog über die Felder „Größe" und „Symbolgröße". Die maximale „Größe" (also jetzt die Breite) liegt bei „200 px".

Wie breit die Leiste werden soll, ist nicht zuletzt durch den Wert „Zeilen" zu bestimmen. Für nur eine Zeile sollten 100 Pixel genügen, für zwei Zeilen müssen Sie 140 Pixel und mehr rechnen.

Die wichtigsten Leistenapplets sind in der Regel das „Anwendungsmenü", der „Schnellstarter" für Favoritenprogramme und der „Anwendungsverwalter" (Taskliste). Diese lassen sich unter „Leiste konfigurieren → Bedienelemente" weiter anpassen. Bei einer schmalen Leiste ist für den „Anwendungsverwalter" die normale Anzeige mit „Symbol und Text" eher ungünstig und besser durch „Nur Symbol" zu ersetzen.

Das Applet „Schnellstarter" lässt sich per Drag & Drop aus dem Hauptmenü mit den wichtigsten Programmen belegen. Positionsänderungen funktionieren im Schnellstarter allerdings nicht mit der Maus, sondern nur mit den Kontextoptionen „Verschieben". Den letzten Optikschliff erhält die Leiste im Hauptdialog „Leiste konfigurieren" über eine Hintergrundfarbe, die Sie am besten vom Desktophintergrund beziehen („Farbe vom Bildschirm wählen") und mit der Option „Hintergrunddeckkraft" nach Wunsch transparent schalten. Falls jetzt die standardmäßige Zeitanzeige („Weltzeituhr") noch auf dem Kopf steht: Diese kann nach einem Rechtsklick über „Weltzeituhr konfigurieren" im Register „Allgemein" waagrecht gedreht werden. **-ha**



Lubuntu mit LXQT: Eine optisch und funktional perfekte Systemleiste kostet unter LXQT etwas Bastelei, ist aber besser machbar als bei manchen großen Desktops.

XFCE: Mit Windows-Taste ins Menü

Es bleibt unverständlich, warum das Standardmenü unter XFCE (Whisker-Menü) nicht dem üblichen Druck auf die Windows-Taste („Super"-Taste) gehorcht. Ein Befehl dafür ist nämlich vorgesehen, dieser wird aber in den XFCE-Distributionen nicht standardmäßig mit der Windows-Taste verknüpft.

Für die Verbindung zwischen XFCE-Desktop und dem Menü-Applet sorgt dieser Befehl:

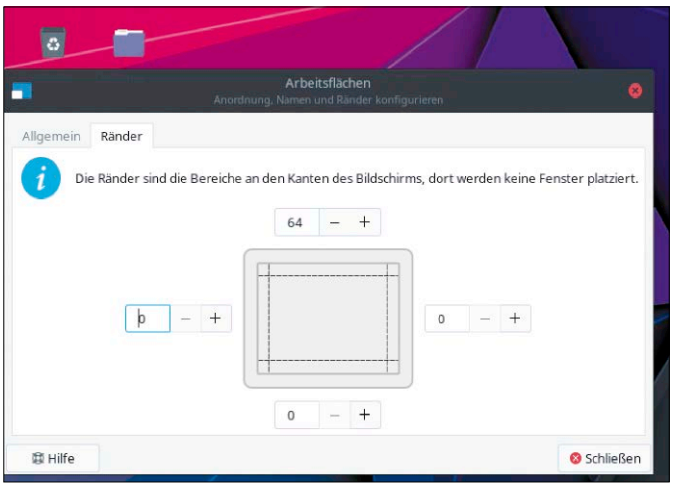
```
xfce4-popup-whiskermenu
```

Der Befehl muss also nur auf die Windows-Taste gelegt werden. Dies erfolgt unter „Einstellungen → Tastatur" auf der Registerkarte „Tastenkürzel für Anwendungen". Mit „+ Hinzufügen" entsteht ein neuer Eintrag, der als „Befehl" das Kommando „xfce4-popup-whiskermenu" erhält. Danach erfolgt die Eingabe der gewünschten Tastenkombination, also der Druck auf die Windows/Super-Taste. **-ha**

XFCE/LXQT: Arbeitsfläche mit „Rändern"

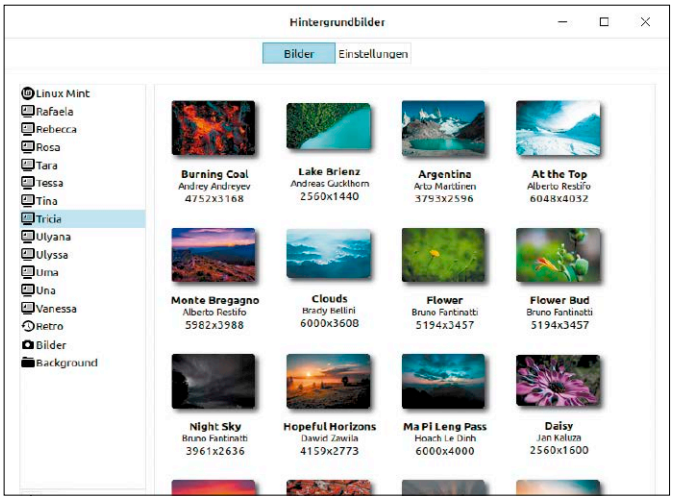
XFCE bietet wie LXQT eine Option namens „Ränder" für die Arbeitsfläche. Wie diese Option sinnvoll eingesetzt wird, erschließt sich nicht auf Anhieb und ist Gegenstand dieses Tipps.

XFCE zeigt unter „Einstellungen → Arbeitsflächen" auch eine Registerkarte „Ränder". Solche



Option „Ränder" in XFCE: Wer viel Monitorplatz hat, kann sich einen Desktopbereich für Symbole freihalten.

Ränder lassen sich an jeder der vier Bildschirmseiten reservieren, um sich dort einen Zugriff auf die Desktop-Schreibtischfläche zu bewahren, selbst wenn Programme im Vollbildmodus dargestellt werden. Ab einer größeren Pixelweite von etwa 60 aufwärts lassen sich damit auch Desktopsymbole stets erreichbar halten. Wie dies optisch am besten zu realisieren ist, bestimmt nicht nur die Pixelgröße für die „Ränder“, sondern auch die Symbolgröße, die unter „Einstellungen → Schreibtisch → Symbole“ definiert ist. Geht es nur darum, das Rechtsklick- oder Mittelklickmenü am Desktop auch bei Vollbildfenstern erreichbar zu halten, können auch ein, zwei Pixel als Rand ausreichen. Solcher Ränder sind zwar praktisch unsichtbar, aber durch Mausnavigation an den betreffenden Rand zuverlässig erreichbar. Diese Option ist auch unter LXQT sinnvoll, ein breiter Rand für den Symbolzugriff jedoch nicht: Unter LXQT werden nämlich nicht nur Programmfenster, sondern auch die Desktopicons von definierten Rändern verdrängt. Die Einstellung findet sich in LXQT und Lubuntu unter „Einstellungen → Fenstermanager Openbox → Ränder“. **-ha**



Jede Menge hübsche Hintergrundbilder: Hier wurden alle Bilder der R-, S-, T-, U-Versionen von Linux Mint eingesammelt, also von Version 17.x bis 20.x.

Cinnamon: Hintergrundbilder

Den Desktophintergrund von Cinnamon ändern Sie über „Systemeinstellungen → Hintergrundbilder“. Der kürzeste Weg ist ein Rechtsklick am Desktop und „Hintergrund der Schreibtisches ändern“. Das Angebot der Hintergrundbilder erweitern Sie beliebig durch eigene Bilder und Fotos sowie durch ältere Mint-Sammlungen.

Abgesehen von den vorgegebenen Bildern können Sie im Dialog „Systemeinstellungen → Hintergrundbilder“ mit dem kleinen Plus-Symbol (unten links) jederzeit einen eigenen Bilderordner hinzufügen. Sobald Sie nach Auswahl des Ordners auf „Öffnen“ geklickt haben, erscheint dieser in der Navigationsspalte des Hauptdialogs „Hintergrundbilder“ und erlaubt die Wahl des gewünschten Bildes.

Auch die zahlreichen Hintergrundbilder älterer Mint-Versionen sind nach wie vor verfügbar. So installiert etwa folgender Befehl

```
sudo apt install mint-backgrounds-u*
```

alle Hintergründe der mit „U“ benannten Mint-20-Versionen, also „Ulyana“ bis „Una“. Diese werden nach der Installation in den Anpassungsdialog „Systemeinstellungen → Hintergrundbilder“ einsortiert. **-ha**

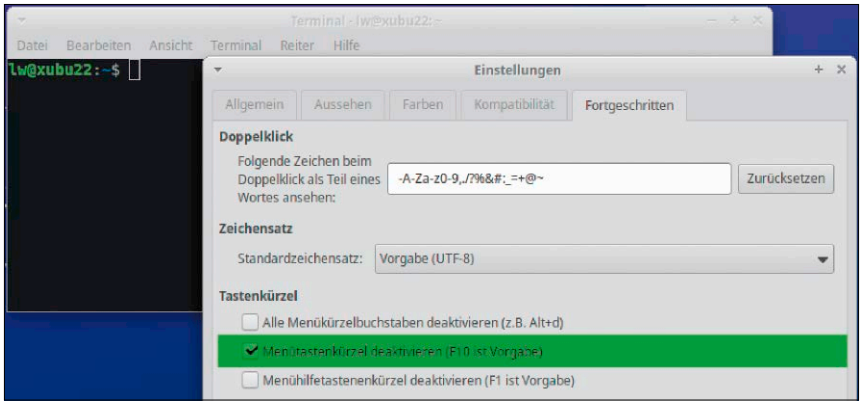
Grafisches Terminal: F10-Taste freigeben

Es gibt in den Terminals der meisten Desktopumgebungen kaum etwas Nervigeres als das vorkonfigurierte Verhalten der F10-Taste. Der Druck darauf öffnet die Menüleiste des Terminalfensters und dies dominiert über den wichtigen F10-Hotkey in Programmen wie dem Midnight Commander oder dem Prozessmonitor Htop.

Nur KDE und LXQT sind die Ausnahmen – dort ist F10 nicht vorbelegt. In allen anderen Gnome-affinen Terminals muss die voreingestellte Tastenbelegung geändert werden:

Die Desktops Gnome, Cinnamon und Budgie verwenden das Gnome-Terminal und hier findet sich über „Bearbeiten → Einstellungen → Allgemein“ die Option „Menütastenkombination aktivieren (Vorgabe: F10)“. Diese Option schalten Sie einfach ab.

Etwas tiefer ist die Option in den Menüs des Terminals von XFCE vergraben. Dort ist im Dialog „Bearbeiten → Einstellungen → Fortgeschritten“ der Punkt „Menütastenkombination aktivieren (Vorgabe: F10)“ untergebracht. Im Terminalprogramm von Mate findet sich der gesuchte Menüpunkt unter „Bearbeiten → Tastenkombinationen“.



F10-Taste für das Terminal freischalten: Jedes grafische Terminal (hier unter XFCE) hat irgendwo eine Option, um die Taste für Terminalprogramme freizugeben.

LXDE: Das Terminal dieses Desktops zeigt die Belegung der F10-Taste im Menü „Bearbeiten → Einstellungen → Verschiedenes → Tastenkürzel F10 für das Menü deaktivieren“. Der angetroffene Punkt macht, was er verspricht. **-ha**

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.

Xubuntu Core und Samba

Auf der Heft-DVD der letzten LinuxWelt war Xubuntu Core 22.10. Auf eine deutlich reduzierte Softwareausstattung war ich aufgrund der zugehörigen Distributionsvorstellung vorbereitet. Aber kann es tatsächlich sein, dass dieses Xubuntu standardmäßig keine Samba- und Windows-Freigaben öffnen kann?

Lutz W., per Mail

Ja, das trifft tatsächlich zu und ist sicherlich eine Sparmaßnahme an der falschen Stelle. Den einzigen Netzwerkclient, den Xubuntu Core standardmäßig mitbringt, ist der SSH-Zugriff – und diesen auch nur für Terminalbenutzung. Der Zugang zu Windows/Samba-Freigaben über den Dateimanager (Thunar) ist über zwei Pakete nachzurüsten:

```
sudo apt install gvfs-backends
 gvfs-fuse
```

Dabei werden automatisch weitere Komponenten, darunter auch bislang fehlende Samba-Bibliotheken mitinstalliert – insgesamt etwa 30 MB, die sich auch eine „Core"-Variante leisten sollte.

Wenn Sie Xubuntu Core nicht aus minimalistischen Motiven gewählt haben, können Sie mittels

```
sudo apt install xubuntu-desktop
```

die Defizite auch großzügiger beseitigen. Auch damit wird der Dateimanager Samba- und SSH/SFTP-tauglich.

Systeminfos ohne Grübeln

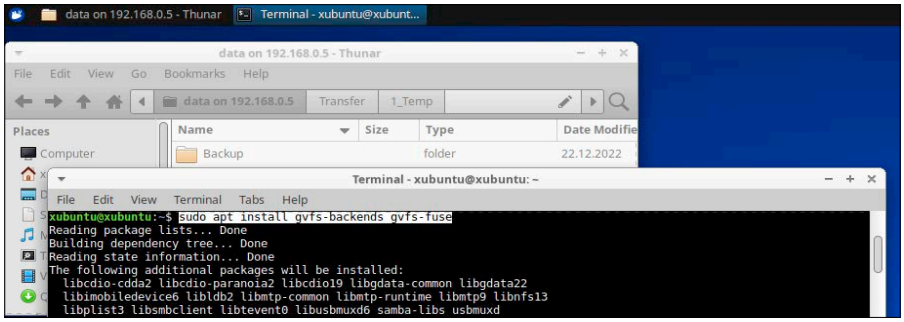
Wenn ich unter Linux bestimmte Systeminformationen einige Wochen nicht mehr benötigt habe, ist das zuständige Tool regelmäßig vergessen: „free", „ip", „dmidecode", „uname", „lsb_release", „lsblk", „lscpu" – geht das nicht einfacher?

Ulrich g., per Mail

Das Terminaltool inxi (zugleich Paketname) ist ein Wrapper für zahlreiche Spezialkommandos. Es kann nicht alles, sollte aber 95 Prozent aller typischen Fragen beantworten. Wer sich mit den Dutzenden von inxi-Schaltern nicht aufhalten will, nimmt am besten dieses Sammelkommando:

```
inxi -v8
```

Das hat zwar den Nachteil, dass man in der Infoflut suchen muss, aber die sollte wirklich alles Wesentliche enthalten: Sie finden Infos zu System (Uptime, Prozesse, Kernel), Distribution, Desktop, Displaymanager, Displayserver, Hardware (CPU, GPU, RAM, Bios, Audio, USB, Temperatursensoren, Laufwerke), Partitionen (Mountpunkte, Dateisystem, Speicherplatz), Netzwerkadapter, IP-Adressen, Hostname und mehr. ■



Xubuntu Core übertreibt seinen Sparkurs: Der Dateimanager kann mit Netzwerkprotokollen nichts anfangen, weil fundamentale Pakete fehlen. Nach deren Installation ist Thunar netzwerktauglich.

SERVICE

Heft-DVDs online
Sie finden die Heft-DVDs der aktuellen wie zurückliegenden LinuxWelt sowie die Extra-DVDs unter *https://github.com/LinuxWelt* als ISO-Dateien zum Download.

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
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

Bildnachweis:
Roisa – AdobeStock, sunftaka77 – AdobeStock, versusstudio – 123RF; 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 2570-4362

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

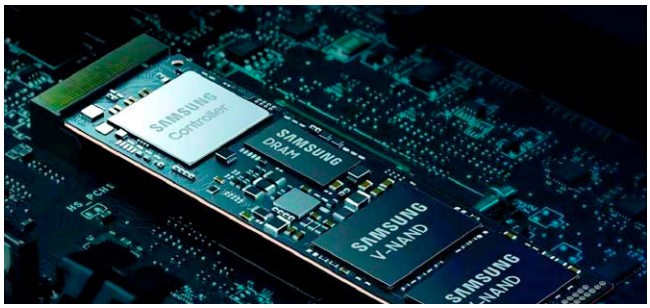
Sie können Ihr Abonnement jederzeit zur nächsten Ausgabe kündigen.
Bestellungen können innerhalb von 14 Tagen ohne Angabe von Gründen in Textform (zum Beispiel Brief, Fax, E-Mail) oder durch Rücksendung der Ware widerrufen werden.

LinuxWelt 3/2023 erscheint am 31. März 2023

Aus Aktualitätsgründen können sich Themen ändern.

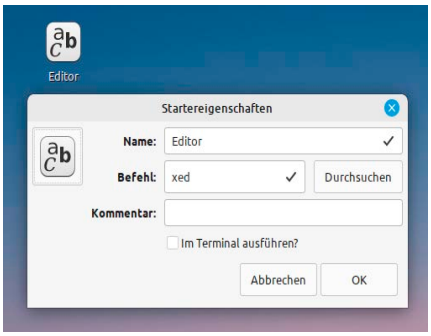
Interne und externe Datenträger

Ratgeber zur Hardware- und Datenträgerverwaltung: Neben mechanischen Festplatten und SSDs gibt es etliche weitere Laufwerkstypen wie NVME, M.2-SSD, externe USB- und Thunderbolt-Geräte unterschiedlicher Version, ferner auch eMMC- und SD-Karten für Platinenrechner. Der Hardwareteil des Schwerpunkts soll Kaufentscheidungen erleichtern und Einbauhilfen liefern. Im Softwareteil geht es um das optimale Partitionieren, Formatieren und Verschlüsseln von Datenträgern.



Programmstarter unter Linux

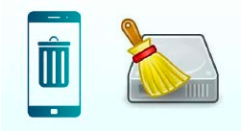
Grundlagen und Tipps zu „.desktop“-Verknüpfungen: Alles, was am Linux-Desktop im Menü, in Systemleisten, Docks oder an der Desktopoberfläche als Programmstarter erscheint, basiert auf Textdateien mit der Extension „.desktop“. Für diese Verknüpfungen gibt es systemweite und benutzerspezifische Sammelordner, weitere für Autostarts. Während einige Linux-Desktops den Umgang mit diesen Startern vorbildlich vereinfachen, ist auf anderen manuelle Handarbeit notwendig. Mit etwas Basiswissen kommen Sie unabhängig vom Desktop an die gewünschten Starter-Verknüpfungen.



Desktop LXQT 1.2

Schlanker Linux-Desktop mit Potenzial: Den Ressourcenvergleich mit dem puristischen LXDE-Desktop konnte LXQT nie gewinnen. Andererseits war es bislang optisch wie funktional dem bewährten XFCE-Desktop tendenziell unterlegen. Die jüngste Version LXQT 1.2 hat das Potenzial, den unbefriedigenden Status quo zu ändern. Die LinuxWelt zeigt anhand eines Lubuntu, was der Desktop dazugelernt hat, und diskutiert, ob er zur ernsten XFCE-Konkurrenz gewachsen ist.

Der Frühjahrsputz



Das große Aufräumen: Der Ratgeber nimmt sich mehr vor als das Entsorgen von temporären Daten, von Cachedateien oder überflüssiger Software. Jenseits typischer Tools wie Bleachbit oder Dublettensuche geht es um mehr Platz auf SSDs und Festplatten, um aufgeräumte Hardware und um reduzierte Komplexität für Netzwerk und Cloud. Einmal im Jahr ist es außerdem Zeit, Platinenrechner und Ausbau-PCs staubfrei zu fegen und Kabelsalat zu entwirren. Nicht zuletzt nehmen wir auch notorisch überfüllte Speicher von Smartphones und Tablets ins Visier.

PC-WELT

Die beste Software 2023

Jetzt am Kiosk!

Sonderheft
für nur
9,90 €

250 Top-Programme auf Heft-DVD

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 SH 2/23 Die beste Software 2023 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

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

tuxedocomputers.com