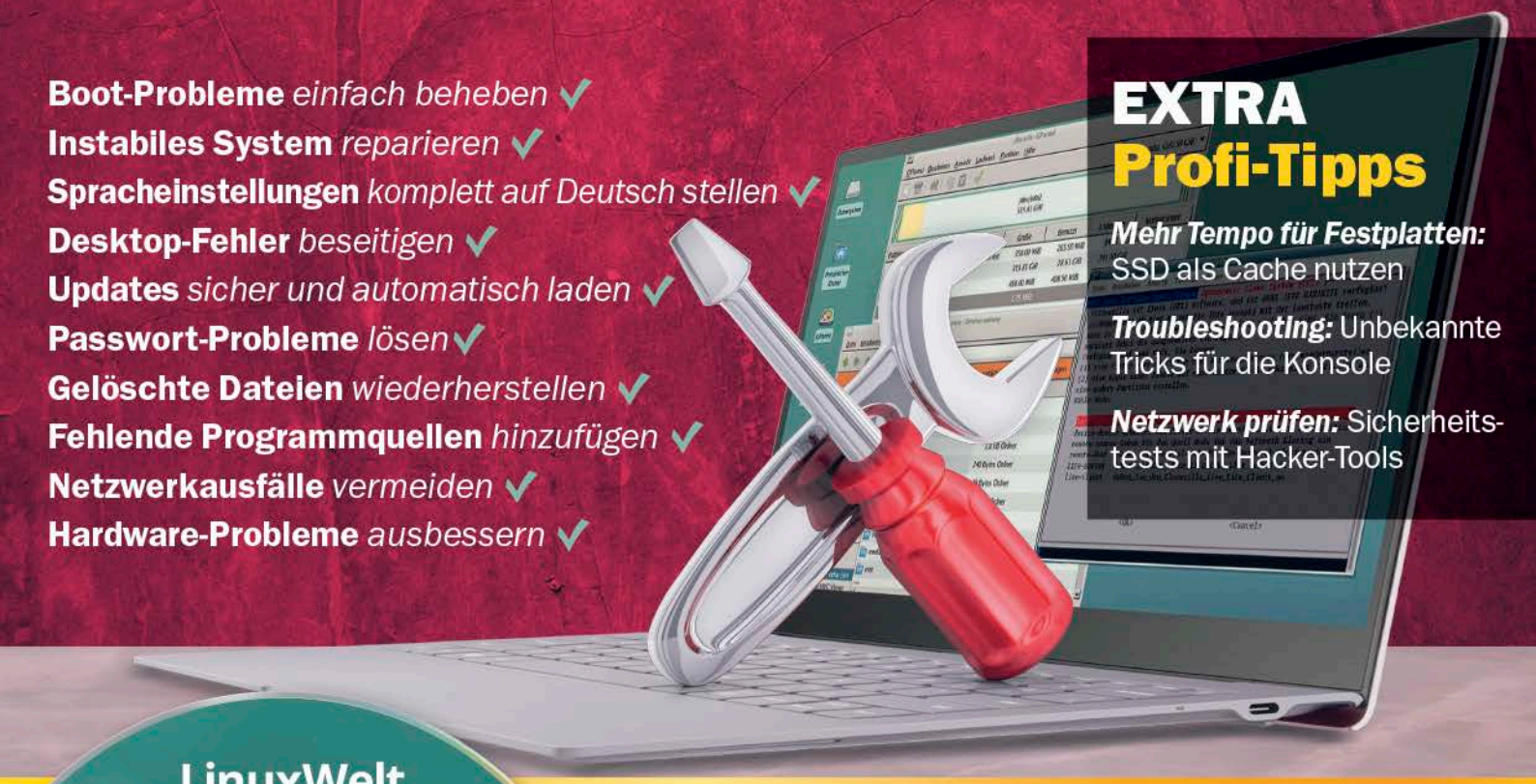
LINUX WELT Extra
SONDERHEFT 3/2021
September – November
€ 9,90 CH 19,90 sfr · Österreich, Benelux 10,95 €
4 190702 309900 03

Linux Systemhilfe

So lösen Sie die häufigsten Linux-Probleme

- **Boot-Probleme** *einfach beheben* ✓
- **Instabiles System** *reparieren* ✓
- **Spracheinstellungen** *komplett auf Deutsch stellen* ✓
- **Desktop-Fehler** *beseitigen* ✓
- **Updates** *sicher und automatisch laden* ✓
- **Passwort-Probleme** *lösen* ✓
- **Gelöschte Dateien** *wiederherstellen* ✓
- **Fehlende Programmquellen** *hinzufügen* ✓
- **Netzwerkausfälle** *vermeiden* ✓
- **Hardware-Probleme** *ausbessern* ✓



EXTRA
Profi-Tipps

Mehr Tempo für Festplatten: SSD als Cache nutzen

Troubleshooting: Unbekannte Tricks für die Konsole

Netzwerk prüfen: Sicherheitstests mit Hacker-Tools

Komplettes Hilfs-Paket

1. LinuxWelt-Rettungssystem – universeller Notfallhelfer
2. Rescuezilla – rettet Ihre Daten
3. Rescatux – repariert den Bootloader
4. Backbox – findet Netzwerkfehler
5. Ubuntu LTS – stabiles Ersatzsystem

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

PC-WELT

Virtuelle PCs

1 Rechner, mehrere Systeme

Jetzt am Kiosk!

Sonderheft
für nur
9,90 €

NEU:
Mega-Paket auf Download-DVD!

Bestellen unter
www.pcwelt.de/tech 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 Tech 7/21 Virtuelle PCs 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

BEZAHLEN

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

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

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

Selten nötig, aber unverzichtbar

Linux läuft sehr stabil. Viele Systeme arbeiten monatelang ohne Neustart und ohne Mucken. Das gilt vor allem für Serversysteme, aber auch auf dem Desktop ist Linux ein Dauerläufer.

Kommt es aber doch zu Problemen, dann hat man oft nicht gleich den passenden Befehl parat oder das richtige Tool in petto. Diese Dinge braucht man ja schließlich selten. Hier möchten wir mit unserem Heft „Linux Systemhilfe“ beispringen. Sie finden auf hundert Seiten unverzichtbare Tipps, Tricks und Tools gegen Systempannen, bockige Software und streikende Hardware. So können Sie alle auftretenden Linux-Probleme ganz einfach lösen.

Komplettes Hilfspaket auf DVD: Die Heft-DVD liefert fünf Systeme, mit denen Sie im Notfall Ihren Rechner wieder flottbekommen. Mit dabei ist auch eine neue Version des exklusiven Linux-Welt-Rettungssystems, das viele nützliche Tools vereint. Am besten ist es natürlich, wenn Sie diese Tools gar nicht benötigen und Ihnen ein Notfall erspart bleibt. Doch sollte es zu Problemen kommen, dann sind Sie mit der DVD und diesem Heft bestens vorbereitet.

Herzlichst, Ihr

Arne Arnold
Redakteur
aarnold@it-media.de

Linux-Systemhilfe

Das gesamte Heft liefert Tipps und Hilfen bei Linux-Problemen. Speziell in der Rubrik „Troubleshooting System“ sowie ab Seite 12 finden Sie Lösungen zu typischen Systemproblemen.

S. 18

Tempo für HDDs

Ein SSD-Cache mit LVM2 ist eine moderne Möglichkeit, HDDs deutlich schneller zu machen.

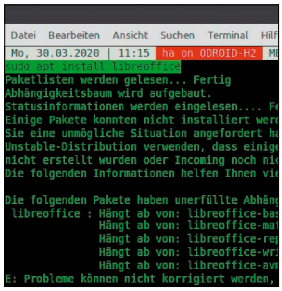
S. 58

Netzwerktests

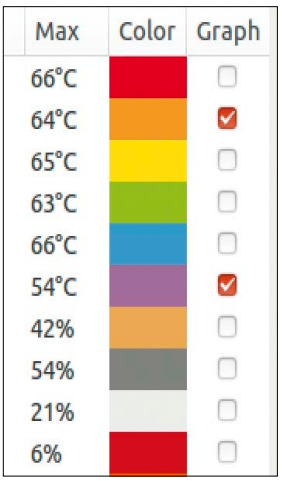
Sie können mit dem System Backbox auf unserer Heft-DVD Sicherheitstests Ihres Netzwerks durchführen.

S. 6

Grundlagen



Troubleshooting System



Desktop & Software

Die Highlights der DVD

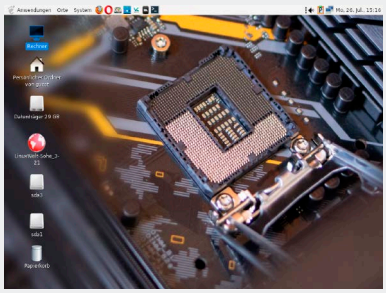
Auf Heft-DVD: Komplettes Hilfspaket mit fünf Systemen

Die Heft-DVD ist randvoll mit Systemen und bootfähigen Tools, mit denen Sie bei einem Notfall rettend eingreifen können. Mit dabei sind das LinuxWelt-Rettungssystem in der neuen Version 8.1, Rescuezilla, Rescatux, Blackbox und Ubuntu LTS, das als stabiles Ersatzsystem dienen kann.

S. 6

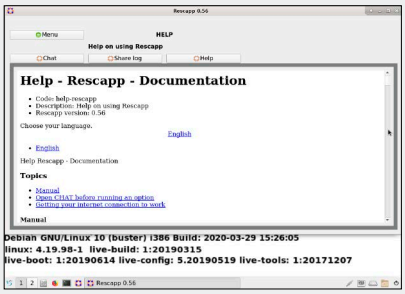
LinuxWelt-Rettungssystem 8.1

Das Highlight dieser Heft-DVD ist das überarbeitete LinuxWelt-Rettungssystem (64 Bit), das viele nützliche und wichtige Tools enthält.



Rescatux 0.73

Vom Entwickler der Super Grub Disk ist auch Rescatux, ein Livesystem zur Reparatur des Bootloaders Grub mit grafischer Oberfläche.



Rescuezilla 2.2

Dieses Livesystem greift die Idee von Clonezilla auf und bietet mit Partclone ein mächtiges Tool zum Backup von Partitionen.

Tempo-Probleme

Standards

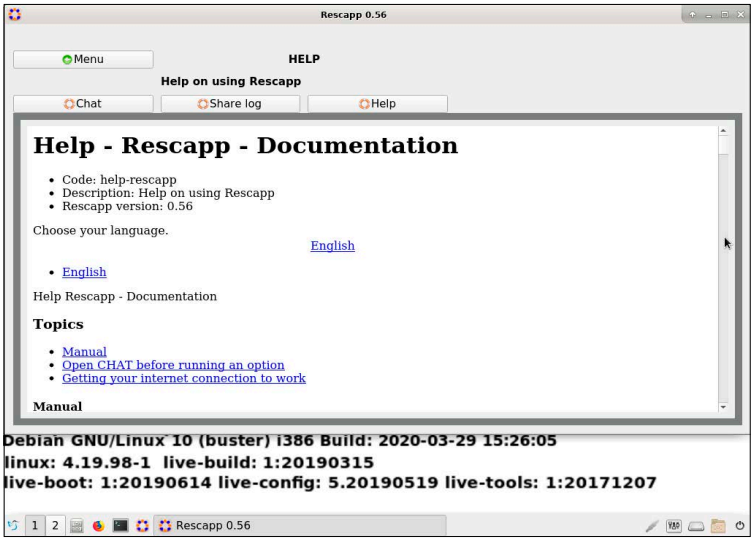
Datei-verwaltung

Hardware & Netzwerk

Terminal

Systemhilfe auch per DVD

In diesem Heft finden Sie Hunderte Tipps zur Systemhilfe bei Hard- und Softwareproblemen. Dazu liefern wir eine Heft-DVD, die randvoll ist mit Systemen und Tools für diese Zwecke. Sie helfen bei der Fehlersuche, beim Retten und beim Reparieren.



Das Reparatursystem Rescatux: Falls ein installiertes Linux-System wegen eines überschriebenen Bootloaders nicht mehr startet, hilft die Rescapp.

VON DAVID WOLSKI

Nicht schön, die Schattenseiten der IT: Hardwarehavarien und stolpernde Systeme dürften die meisten Anwender kennen, nicht nur von Linux-Rechnern, sondern hauptsächlich von den weit verbreiteteren Windows-10-PCs – zu Hause und im Büro. Sollte das Bios nervös piepen, die alternde Festplatten schon hörbar knirschen oder gar der Geruch verbrannter Elektronik in die Nase steigen, so ist ein Hardwareproblem als Ursache schnell ausgemacht.

Aber ganz so eindeutig sind Ausfälle in der Praxis selten. Einer der ersten Schritte bei der Fehleranalyse ist die Eingrenzung der Problemquelle auf Hardware oder Software. Wobei zur Software nicht nur Treiber, sondern auch das Betriebssystem selbst gehören.

Bootfähige Systeme auf Heft-DVD

Aber woher so schnell ein anderes Betriebssystem nehmen? Zu diesem Zweck sind Livesysteme auf Linux-Basis wie geschaffen: Sie können damit ohne Installation ein alternatives Betriebssystem von DVD oder USB-Stick starten und so die Funktionsfähigkeit der meisten Hardwarekomponenten und Festplatten ohne hohen Aufwand überprüfen. Oft noch wichtiger: Auf die Schnelle Dateien vom Datenträger des Rechners ziehen, wenn dessen System, Windows oder Linux, nicht mehr startet. Die gut gefüllte Sonderheft-DVD fasst alle wichtigen Livesysteme für diesen Zweck zusammen, zudem ein Reparatursystem für Bootloader und ein Imagingtool im Stil von Clonezilla.

LinuxWelt-Rettungssystem 8.1: Das eigentliche Highlight dieser Heft-DVD wird an dieser Stelle nur kurz der Vollständigkeit halber erwähnt, denn dem LinuxWelt-Rettungssystem 8.1 (64 Bit) widmet sich der darauf folgende Artikel noch im Detail. Schließlich umfasst es inzwischen zu viele wichtige Tools, als dass diese so kurz in dieser Übersicht sinnvoll vorgestellt werden könnten.

Rescatux 0.73: Vom Entwickler der Super Grub Disk ist auch Rescatux, ein Livesystem zur Reparatur des Bootloaders Grub mit grafischer Oberfläche. Nach dem Start des Systems aus dem Multibootmenü heraus begrüßt ein Assistent, dessen Standardeinstellung man mit „Ja“ übernimmt.

Wichtig zur Reparatur ist, dass Rescatux in 32 oder 64 Bit gestartet wurde, im Bios- oder Uefi-Modus (alles im Multibootmenü). Denn diese Modi müssen immer zum repa-

ALLES IM BOOT: UEFI- UND BIOS-MODUS

Die Sonderheft-DVD präsentiert alle Systeme beim Boot unter dem Bios- oder Uefi-Modus in einem komfortablen Multibootmenü. Allerdings gibt es einige wenige Notebooks, die wegen ihrer Firmwareversion die Heft-DVD nicht im Uefi-Modus starten können. Sollte dies passieren und die DVD nicht über die Anzeige des Bootmenüs hinauskommen, so starten Sie sie bitte im Bios-Modus. Dazu ist ein Umschalten der Bootoptionen in den Firmwareeinstellungen des Computers nötig. Die benötigte Option nennt sich „Legacy boot“, „CSM“ oder auch „BIOS compatibilty mode“ in den Bios-Einstellungen. Falls es dann immer noch Probleme gibt, hilft ein Workaround: Im Verzeichnis „Image-Dateien“ auf der DVD finden Sie alle Systeme auch in Form ihrer originalgetreuen ISO-Datei, zum Brennen auf DVD ohne Multiboot sowie zur Übertragung auf USB-Stick mit Balena Etcher (Open Source, für Windows und Linux, 64 Bit, auf Heft-DVD).

Backbox: Dieses installierbare Livesystem ist für die Jagd nach Sicherheitslücken im Netzwerk und auf Servern bestens ausgerüstet.

Rescuezilla, eine Alternative zu Clonezilla: Mittlerweile ist das grafische Rescuezilla zu Clonezilla voll kompatibel und kann auch dessen Datensätze öffnen.

raturbedürftigen fest installierten System auf dem Datenträger passen. Aus dieser Statusmeldung heraus lässt sich die Reparaturanwendung Rescapp mit „Start Rescapp“ starten.

Die Menüpunkte unter „Menu“ führen hier jeweils in die Untermenüs und zu den eigentlichen Funktionen. Die Rescapp kann kaputte und überschriebene Grub-2-Bootloader von installierten Linux-Systemen wieder flottmachen. Der Menüpunkt „Easy GNU/Linux Boot Fix“ schreibt einen frischen Grub-2-Bootloader auf den Datenträger und erkennt dabei die installierten Betriebssysteme (Linux und Windows). Zudem gibt es einige Reparaturoptionen für Windows-10-Installationen.

Backbox 7: Für Sicherheitsexperten gibt es für die Jagd nach Netzwerkproblemen eine besondere Klasse von Livesystemen: Backbox 7 ist ein Werkzeugkasten mit Tools für Netzwerk-Checks und zum Aufspüren von Sicherheitslücken im LAN und auf Servern. Zwar werden die enthaltenen Tools auch von der Hackerszene mitentwickelt, die Zielgruppen sind aber Administratoren und Sicherheitsexperten.

Der Einsatz der Werkzeuge auf dem eigenen PC, Server oder Netzwerk ist legitim und nützlich. Sie finden damit Sicherheitslücken in Ihren Systemen, bevor es jemand anderes tut. In diesem Kontext sind diese „Dual-Use“-Programme, die Gutes bewirken oder auch Schaden anrichten können, auch in Deutschland legal.

Rescuezilla 2.2: Dieses Livesystem greift die Idee von Clonezilla auf und bietet mit Partclone ein mächtiges Open-Source-Programm zum Backup von Partitionen mit grafischer deutschsprachiger Oberfläche. So wie Clonezilla eignet sich Rescuezilla ab Version 2.2 auch zum Wiederherstellen einzelner Partitionen aus dem Image eines Datenträgers.

Zum Speichern von Backups kann das Livesystem ein internes Laufwerk, angeschlossene oder externe Datenträger und auch Speicherorte im Netzwerk nutzen wie Windows-Freigaben und FTP-Server.

Ubuntu 20.04.2: Ein aktuelles Ubuntu soll natürlich auch nicht fehlen. Die aufgefrischte Ubuntu-Ausgabe ist ein Point Release, das alle bisher erschienenen Aktualisierungen in neuen Installationsmedien bereitstellt. Zudem gibt es ein Update des Betriebssystemkerns auf Kernel 5.8 und dessen Treibermodule. Dies ist ein optionales Update des ursprünglich ausgelieferten Kernels 5.4 und besonders für Desktopsysteme interessant. Zudem sind etliche Fehlerbehebungen enthalten, auch im Installer. Wer Ubuntu 20.04 schon installiert hat, bekommt alle diese Updates per Paketmanager.

Diese Installationsmedien sind also nur für Neuinstallationen wichtig. ■

Ein Ubuntu darf auch nicht fehlen: Als universelles Linux-System ist das aufgefrischte Ubuntu 20.04.2 (LTS) mit dem Gnome-Desktop mit von der Partie.

AUF DVD

Distributionen

LinuxWelt Rettungssystem 8.1 (64 Bit)
Rescatux 0.73 (32/64 Bit)
Backbox 7 (64 Bit)
Rescuezilla 2.2 (64 Bit)
Ubuntu 20.04.2 (64 Bit)

Extras und Tools

Super Grub Disk 2, Memtest86+, HDT, Plop Kexec, Shred-OS

50 Handbücher

Geballtes Linux-Know-how als PDFs

Das LinuxWelt-Rettungssystem

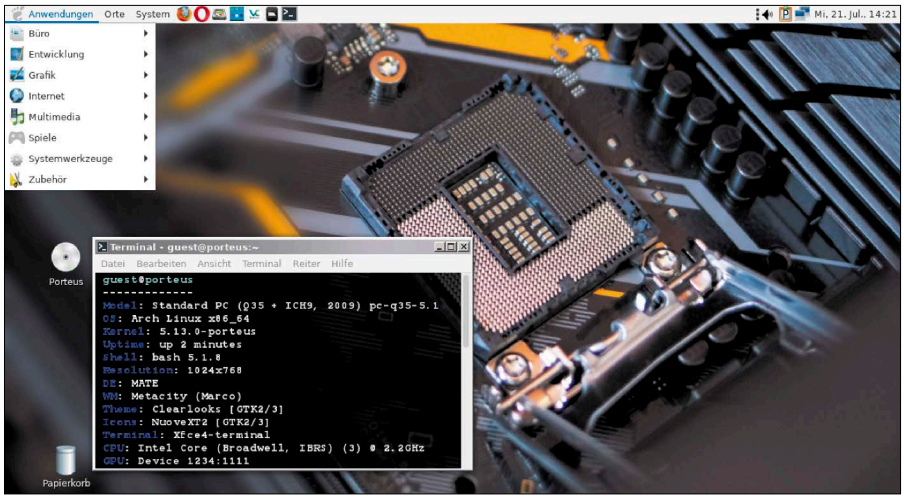
Was kann das neue Rettungssystem der LinuxWelt-Redaktion? In welchen Notfällen sind die enthaltenen Programme hilfreich? An dieser Stelle zeigen wir einige Tools im Detail, jeweils mit kurzen praxisorientierten Anleitungen.

VON DAVID WOLSKI

Das installierte Betriebssystem startet nicht mehr, beispielsweise wegen unpassender Treiber, Konfigurationsfehlern oder wegen eines Hardwareproblems. In diesen Fällen ist ein gut ausgestattetes Livesystem eine formidable Hilfe. Sofern die Datenträger intakt sind sowie unverschlüsselt, kann das Livesystem Dateien vom lahmgelegten Rechner auf einen anderen Datenträger oder auf eine Freigabe im Netzwerk kopieren. Und schließlich gibt es immer wieder Aufgaben, die nur aus einem Livesystem heraus funktionieren, wie die Wiederherstellung gelöschter Dateien, die Repartitionierung der Datenträger und das Klonen oder Speichern von Festplatten einer Abbilddatei als Komplettbackup.

Ein gut gefüllter Werkzeugkasten

Für diese Zwecke fasst das neue LinuxWelt-Rettungssystem 8.1 (in 64 Bit auf Heft-DVD) die wichtigsten Werkzeuge auf einem intuitiven Desktop zusammen. Es tritt wieder mit dem Anspruch an, ein möglichst unkompliziertes und dabei kompaktes Livesystem mit Wiederherstellungstools, Partitionierer und Browser von DVD zu starten. Der schlanke Mate-Desktop, Browser und die meisten Programme liegen dabei in deutscher Sprache vor. Von Heft-DVD ist ein Boot im Bios-Modus und auch im Uefi-Modus möglich. Neben dem normalen Start bietet das Menü den Punkt „Alles im RAM (ab 2 GB Arbeitsspeicher)“ an. Dabei handelt es sich um die empfohlene Startmethode, bei welcher das System alle Module in den Arbeitsspeicher lädt. Dies dauert etwas länger – dafür ist das laufende System aber blitzschnell, da es nicht mehr auf die DVD zugreifen muss.



Neuentwicklung aus der Redaktion: Das LinuxWelt-Rettungssystem basiert jetzt auf der Slackware-Variante Aporteus und ist mit vielen nützlichen Tools und Browsern auf der Heft-DVD vertreten.

Nach dem Start des Desktops wartet der Network-Manager rechts oben darauf, eine WLAN-Verbindung aufzubauen. Oben links gibt es ein ausklappendes Anwendungsmenü und für die wichtigsten Programme sind in der oberen Leiste Verknüpfungen angelegt: Firefox, Opera, der Partitionierer Gparted, Clonezilla, Veracrypt, Dateimanager und Terminalfenster stehen in dieser Reihenfolge für den schnellen Zugriff bereit. Der häufigste Grund, ein Livesystem zu starten, ist der Zugriff auf Datenträger und Dateien, wenn das fest installierte Betriebssystem nicht mehr starten will. Das Rettungssystem verfügt über einen NTFS-Treiber (NTFS-3G) und der Dateimanager kann Windows-Partitionen direkt zum Lesen und Schreiben per Klick öffnen.

Hilfe bei gelöschten Dateien

Egal, ob dieses Malheur unter Windows oder Linux passierte: Nach dem Löschen einer noch benötigten Datei hat es Vorrang, so schnell wie möglich weitere Schreibaktionen auf dem betroffenen Datenträger zu unterbinden. Das bedeutet, nicht mehr mit dem installierten System weiterzuarbeiten, sondern eiligst ein alternatives Livesystem wie das Rettungssystem mit Wiederherstellungstools zu booten. Das Rettungssystem hat zwei Programme mit an Bord zur Wiederbelebung gelöschter Dateien.

Photorec: Das Programm durchsucht die freien Bereiche von Dateisystemen und stellt von dort Dateien anhand ihres Typs und einer heuristischen Suche in ein Zielverzeichnis auf einem anderen Datenträger wieder her. Welche Bezeichnungen die Quell- und Zielpartitionen haben, ermittelt man zuerst im Dateimanager. In diesem

Beispiel soll die Quellpartition mit den gelöschten Dateien die Kennung „/dev/sda2“ haben. Anschließend geht es in ein Terminalfenster, in welchem dann zunächst der eingegebene Befehl

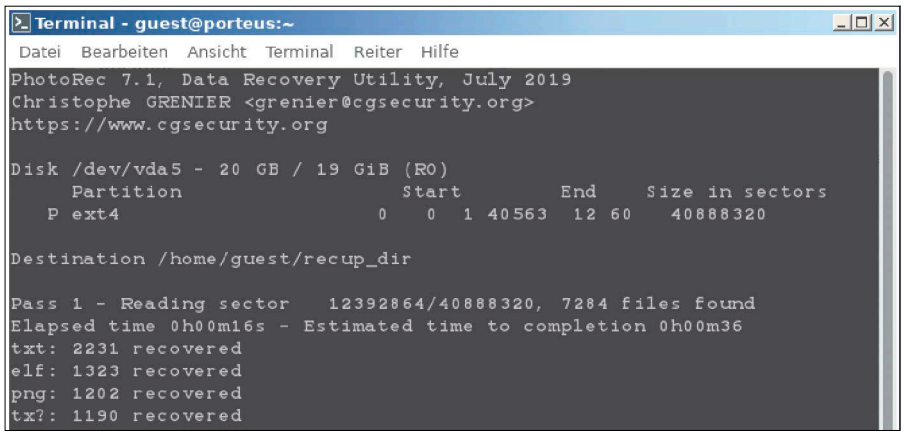
```
sudo umount /dev/sda2
```

die Partition erst aushängt, falls noch nicht geschehen, und dann mit

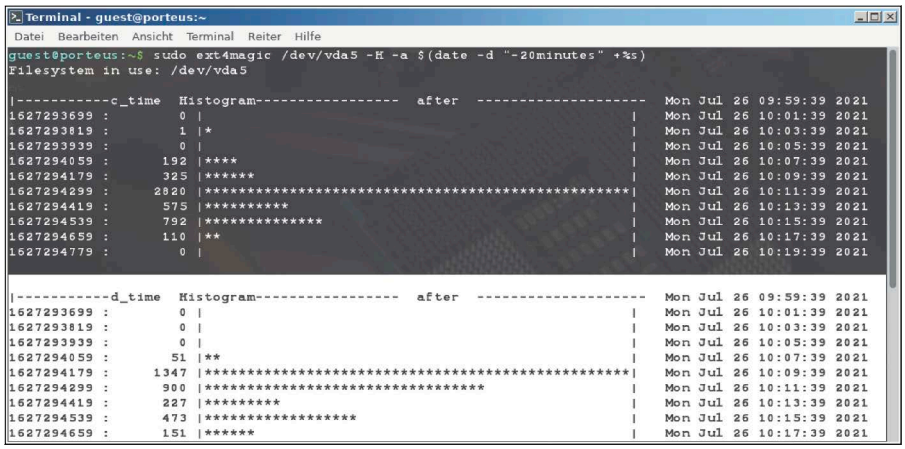
```
sudo photorec /dev/sda2
```

das Wiederherstellungstool Photorec darauf ausführt. Um gelöschte Dateien zu retten, verlangt Photorec noch in der Liste die Bestätigung der Partition und des enthaltenen Dateisystems mit Return. Auch die Auswahl des Dateisystemtyps muss passen, damit Photorec etwas findet. Es gibt dabei aber nur zwei Optionen, eine für Ext2/3/4 und eine für sämtliche andere Dateisysteme wie FAT32, NTFS und alle anderen. Nach der Auswahl des Dateisystems können Sie den freien Platz („Free“) oder das gesamte Laufwerk („Whole“) nach gelöschten Dateien untersuchen.

Für die gefundenen Dateien und Datenreste gehen Sie dann noch im Dateibrowser auf das gewünschte Zielverzeichnis und drücken dann die C-Taste, um die automatische Wiederherstellung zu starten. Je nach Größe des Datenträgers kann der Suchlauf bis zu Stunden dauern und findet meist sehr viele wiederherstellbare Dateien, die es danach zu sichten gilt.



Heuristische Suche nach Dateitypen: Das Shell-Tool Photorec arbeitet rigoros und findet viel. Eine Zielpartition sollte groß sein, denn Hunderte Megabyte sind schnell gefunden.



Dateiwiederherstellung aus dem Journal: Das Funktionsprinzip von Ext4magic fußt auf dem Änderungsprotokoll von Ext3/4, in dem sich oft noch Kopien gelöschter Dateien finden.

Ext4magic: Geht es darum, von einer Ext4- oder Ext3-Partition eine bestimmte Datei wiederzubeleben, die noch nicht lange gelöscht ist, so ist das Tool Ext4magic ein schnelles und zuverlässiges Werkzeug. Es arbeitet über die Analyse des Journals dieser Dateisysteme und kann deshalb gezielter Dateien wieder herstellen. Um Ext4magic sinnvoll einzusetzen, ist es aber nötig, ungefähr den Zeitpunkt zu kennen, wann die benötigte Datei gelöscht wurde. Denn man blickt anhand dieser Zeitangabe mit Ext4magic erst in das Journal, um Änderungsstempel der letzten Änderungen anzuzeigen.

```
sudo ext4magic /dev/sda2 -H -a
 $(date -d "-20minutes" +%s)
```

Dieser Befehl analysiert Änderungen der letzten 20 Minuten auf der (ebenfalls ausgehängten) Ext3/4-Partition „/dev/sda2“. Ext4magic zeigt nun ein Histogramm namens „c_time“ mit den letzten allgemeinen Änderungen an und darunter ein weiteres namens „d_time“ mit Löschungen. In diesem Fall sind nur die Zeitstempel von Änderungen unter „d_time“ interessant. Lautet dort der Zeitstempel vor dem letzten Löschen beispielsweise „1597491799“, so geben wir dem Tool mit dem Kommando

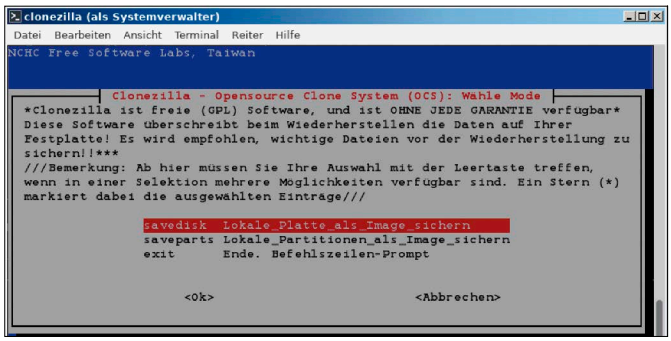
```
sudo ext4magic /dev/sda2 -a
 1597491799 -m -d gerettet
```

den Auftrag, alle Dateien ab dem angegebenen Zeitstempel in den neuen Unterordner „gerettet“ wiederherzustellen. Dateinamen gehen dabei zwar verloren, aber die Endungen nicht.

LINUXWELT-RETTUNGSSYSTEM 8.1: TOOLS IM ÜBERBLICK

Programm	Funktion/Einsatzbereich	Aufruf über
ATA Secure Erase	löscht SSDs am SATA-Port komplett	Menü → Systemwerkzeuge
Clonezilla 3.35	Backup- und Wiederherstellungstool	Schnellstartleiste
Ext4magic 0.3.2	Wiederherstellung gelöschter Dateien	„sudo ext4magic“ im Terminal
Firefox 90	Webbrowser, deutschsprachig	Schnellstartleiste
Gparted 1.3	mächtiger grafischer Partitionierer	Schnellstartleiste
Midnight Commander 4.8	Dateimanager und Netzwerkclient	„mc“ im Terminal
Nmap 7.91	Adress- und Portscanner im Netzwerk	„nmap“ im Terminal
Opera 74	Webbrowser mit eigenem VPN	Schnellstartleiste
Photorec 7.1	Wiederherstellung gelöschter Dateien	„sudo photorec“ im Terminal
Testdisk 7.1	stellt gelöschte Partitionen wieder her	„sudo testdisk“ im Terminal
Veracrypt 1.24-7	Verschlüsseler im Stil von Truecrypt	Schnellstartleiste

Einige der wichtigen Programme des Rettungssystems in der Übersicht: Einige der Tools für Fortgeschrittene sind nur über die Shell im Terminalfenster aufrufbar.



Clonezilla: Bei Uefi-Systemen die gesamte Platte sichern. Die Funktionen „savedisk/restoredisk“ beachten auch die EFI-System-Partitionen (ESP) und stellen auch die Booteinträge wieder her.

Clonezilla: Festplattenimages anlegen

Das Backuptool für ganze Festplatten oder auch nur einzelner Partitionen schreibt Abbilder in komprimierte Imagedateien, die es entweder lokal auf einer anderen Festplatte speichert oder auf einem USB-Medium. Es erkennt alle verbreiteten Dateisysteme aus dem Umfeld von Windows und Linux, wie Ext2, Ext3, Ext4, BTRFS, ReiserFS, XFS, JFS, FAT32 und NTFS. Die Backupimages kann Clonezilla gepackt als Dateien speichern und zu einem Umzug eine Festplatte 1:1 klonen.

Nach dem Aufruf von Clonezilla über die obere Schnellstartleiste, der übrigens gleich mit root-Rechten erfolgt, geht es auch schon los. Im textbasierten deutschsprachigen Menü wird „device-image“ und dann „local_dev“ ein Abbild auf einem lokalen Datenträger sichern.

Soll ein USB-Datenträger das Partitionsimage aufnehmen, stecken Sie das USB-Gerät jetzt an und drücken Sie die Return-Taste. Die Zielpartition und das Verzeichnis wählen Sie in den nächsten Schritten aus. Für das gepackte Image belassen Sie im nächsten Schritt die Einstellungen auf „Beginner Einsteiger“, gehen im nächsten Menü auf „saveparts“, geben den gewünschten Imagenamen an und wählen schließlich aus der Liste die Quellpartition aus, die Sie sichern möchten.

Wenn eine ganze Festplatte mit Betriebssystem und Datenpartitionen gesichert werden soll, speichert Clonezilla alles in einem Abbild. Nach der Auswahl der Zielpartition und den Einstellungen „Beginner Einsteiger“ brauchen Sie dazu den Punkt „savedisk“.

Im nächsten Schritt geben Sie wieder den gewünschten Dateinamen des Abbilds an und wählen dann die zu sichernde Festplatte aus. Sie erhalten auf der Zielpartition im ausgewählten Verzeichnis ein „gzip“-komprimiertes Abbild der gesamten Platte. Soll Clonezilla nur eine einzelne Partition sichern, so ist „saveparts“ dagegen der passende Menüpunkt.

Um eine gesicherte Partition mit Clonezilla wieder zurück auf die Platte zu schreiben, starten Sie das Tool wie zuvor mit den Optionen „device_image“ und „local_dev“. Wählen Sie dann die Partition und das Verzeichnis aus, in dem das zuvor gesicherte Image liegt, gehen auf „Beginner Einsteiger“ und dann allerdings auf die Option „restoreparts“. Clonezilla findet auf dem Backupmedium alle Abbilder automatisch und präsentiert sie in einer Liste. Danach wählen Sie noch die Zielpartition aus, in die das Image zurückgeschrieben werden soll. Die Wiederherstellung einer Festplatte aus dem gesicherten Image funktioniert ganz ähnlich. Nur wählen Sie statt „restoreparts“ die Option „restoredisk“ aus. Clonezilla listet wieder die gefundenen Imagedateien auf dem Backupmedium auf und fragt anschließend nach, welche Festplatte es überschreiben soll.

Zum Multitalent wird Clonezilla durch seine Netzwerkfähigkeit: Images können Sie nicht nur auf angeschlossenen Datenträgern speichern, sondern auch über eine Netzwerkverbindung auf einem anderen Rechner. Dazu gehen Sie bei der vorherigen Auswahl der Zielpartition für das Image nicht auf „local_dev“, sondern beispielsweise auf „samba_server“, wenn das Backup auf einer Netzwerkfreigabe von Windows landen soll.

ALTERNATIVER START: TRANSFER AUF EINEN USB-STICK

Viele moderne Rechner und Laptops haben kein optisches Laufwerk mehr. Deshalb läuft das LinuxWelt-Rettungssystem nicht nur von Heft-DVD, sondern ist auch im Nu auf einen USB-Stick übertragen, von welchem sich ein Rechner dann starten lässt – übrigens deutlich flotter als von DVD. Es gibt drei Möglichkeiten, das Rettungssystem auf USB-Sticks zu bringen.

Aus dem Livesystem heraus: Das Livesystem liefert unter „Anwendungen → Systemwerkzeuge → Bootfähigen USB-Stick erstellen“ ein Programm mit, um das Livesystem auf einem USB-Stick oder einer Speicherkarte bootfähig einzurichten. Nach dessen Start erwartet das erste Eingabefeld die Auswahl der ISO-Datei des Rettungssystems. Sie findet sich beim Boot von der Heft-DVD im Dateibrowser über den Pfad „sr0 → Image-Dateien → lw-rettungssystem-81.iso“. Darunter listet das Tool die angeschlossenen Wechselmedien auf, um den USB-Stick auszuwählen. Dieser wird dann automatisch neu partitioniert und muss über mindestens ein GB Kapazität verfügen. Schließlich gilt es noch auszuwählen, ob der resultierende Stick im Bios- oder Uefi-Modus starten soll. Ganz unten stehen Partitionierungsschemata zur Auswahl, wobei die erste Partition in der Standardeinstellung „Mini (ISO size)“ für das Livesystem reserviert ist und der Rest des USB-Sticks mit Ext4/3 oder FAT32 formatiert werden kann.

Mit Windows: Die Heft-DVD macht sich die fortgeschrittenen Fähigkeiten des Bootloaders Gub 2 zunutze und startet die Livesysteme anhand ihrer originalgetreuen ISO-Dateien. Auf Heft-DVD findet sich im Verzeichnis „Image-Dateien“ deshalb das Rettungssystem auch in Form der Datei „lw-rettungssystem-81.iso“. Auch damit ist ein bootfähiger USB-Stick schnell hergestellt: Der Windows-Explorer kann diese ISO-Datei gleich in einem Verzeichnis öffnen. Die enthaltenen Dateien und Unterverzeichnisse kommen dann auf einen USB-Stick, der mit FAT32 formatiert ist.

Jetzt gilt es noch, diesen USB-Stick mit einem Bootsektor bootfähig zu machen. Dazu dient das Programm „Porteus-Installer-

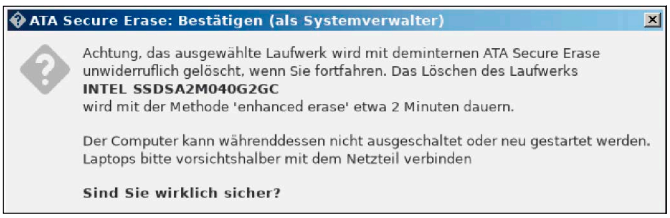
Zurücksetzen: ATA Secure Erase

Die Controllerlogik einer SSD steuert alle Schreibvorgänge der SSD, um Speicherzellen möglichst gleichmäßig zu nutzen. Der interne Befehl „ATA Secure Erase“ ist eine Erweiterung der Firmware und im Befehlssatz des Laufwerks untergebracht. Vor einer Weitergabe eines Datenträgers sorgt der Befehl dafür, dass keine wiederherstellbaren Dateireste auf dem Medium zurückbleiben. Auf SSDs hat der Befehl den zusätzlichen Nutzen, dass er das Laufwerk samt der reservierten Speicherzellen in den Werkszustand zurücksetzt. Das erhöht zwar nicht die Haltbarkeit der Flash-Speicherzellen, macht eine SSD aber wieder so schnell wie am ersten Tag.

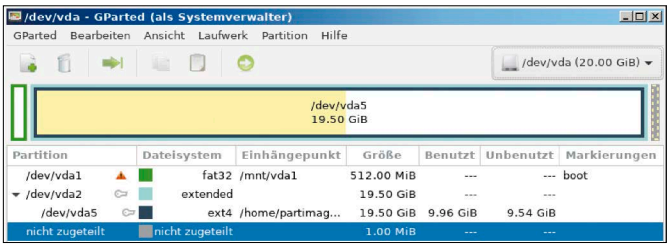
Im Rettungssystem findet sich im Anwendungsmenü unter „Anwendungen → Systemwerkzeuge → ATA Secure Erase“ ein grafisches Tool, das diesen Befehl ausführen kann. Nach dem Aufruf präsentiert das Tool eine Liste der erkannten SATA-Laufwerke. Es können dabei nur Laufwerke ausgewählt werden, die an SATA-Ports angeschlossen sind, NVME-Ports, USB-Laufwerke, E-SATA, SAS und Raid-Controller werden nicht unterstützt. Im nächsten Schritt wählen Sie das gewünschte Laufwerk aus, das zurückgesetzt werden soll. Vorsicht bei der Auswahl und der genauen Identifikation des Datenträgers anhand der angezeigten Geräte-ID sowie der Modellbezeichnung! Denn die Dateien auf dem ausgewählten Laufwerk werden später unwiederbringlich verloren gehen. Wenn in der Liste die Spalte „Eingefroren“ zu einer SSD den Zustand „ja“ anzeigt, so kann dieses Laufwerk nicht gleich gelöscht werden. Denn es bedeutet, dass ein angeschlossenes SATA-Laufwerk zunächst für den exklusiven Zugriff durch das Bios gesperrt ist. Dagegen hilft der Trick, den Rechner kurz in den Ruhezustand zu versetzen und wieder aufzuwecken. Das Tool bietet nach der Auswahl eines eingefrorenen Laufwerks automatisch an, das System in den Ruhezustand zu versetzen. Nach dem Aufwecken des Rechners hat sich der Status der Laufwerke geändert und Sie können nach dem erneuten Aufruf von „ATA Secure Erase“ wieder mit der Laufwerksauswahl fortfahren. Jetzt ist noch eine Bestätigung im Dialog „Sind Sie wirklich sicher“ nötig, um das nochmals angezeigte Laufwerk „ATA Secure Erase“ tatsächlich in Gang zu setzen oder abzubrechen. Der Löschvorgang dauert auf SSDs nur wenige Minuten. ■

ATA Secure Erase: Das Rettungssystem enthält dieses neue grafisches Tool, um SSDs am SATA-Port über den Controllerbefehl „Secure Erase“ mit „hdparm“ komplett zurückzusetzen.

Besser eine Bestätigung mehr: Es gilt, beim Einsatz von „ATA Secure Erase“ genügend Sorgfalt walten zu lassen und das richtige Laufwerk zum Löschen auszuwählen.



Der Partitionierer Gparted darf nie fehlen: Dieses Programm, im Rettungssystem in der neusten Version 1.3 enthalten, ist für Windows- und Linux-Anwender gleichermaßen nützlich.



for-Windows.exe“ im Unterordner „boot“, das einfach per Doppelklick gestartet wird. Anschließend verlangt das Programm noch eben eine Bestätigung per Tastendruck.

Mit Linux: Auch unter Linux entpackt man den Inhalt der ISO-Datei mit einem Packprogramm wie File-Roller (Gnome) oder Ark (KDE) auf einen FAT32-formatieren USB-Stick. Unter Linux sorgt dann das Kommandozeilenprogramm „Porteus-Installer-for-Linux.com“ für den Bootsektor auf dem Stick. Es wird in einem Terminalfenster im Unterordner „boot“ auf dem USB-Stick mittels

```
sudo ./Porteus-Installer-for-Linux.com
```

aufgerufen. Nach einer Bestätigung ist der Stick dann bootfähig.

Das USB-Transfertool des Livesystems: Bevor ein USB-Stick beschrieben wird, zeigt das Tool noch eine Zusammenfassung zur Bestätigung an und dann den Fortschritt im Terminal.

Die 20 häufigsten Linux-Probleme

Dieser Ratgeber orientiert sich an der Leserumfrage, die nach jeder LinuxWelt unter anderem die Frage stellt: „Was bereitet Ihnen unter Linux die meisten Probleme?“ Wir haben Antworten – nicht auf alle, aber doch auf die meisten Probleme.

VON HERMANN APFELBÖCK

1. Defekte Grub-Bootloader

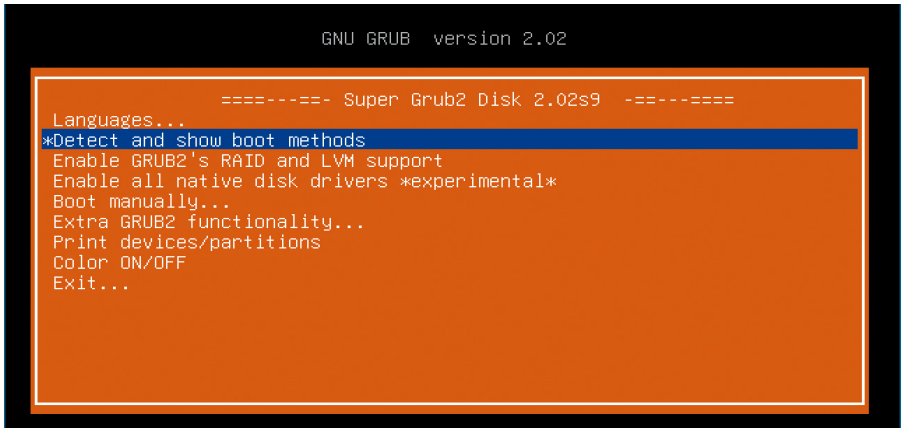
Der Grub-Bootmanager ist sehr robust, aber es gibt ein Szenario, das diesen regelmäßig vernichtet: Eine Windows-Installation ignoriert bei einer Parallelinstallation den Grub-Bootloader und ersetzt ihn durch den Windows-Bootloader, der nur Windows-Systeme bootet. Von den möglichen Reparaturmaßnahmen empfehlen wir die einfachste: Starten Sie den Rechner mit dem Tool Super Grub Disk (*www.supergrubdisk.org*, auch auf Heft-DVD unter „Extras und Tools“). Der Boothelfer durchsucht mit „Detect and show boot methods“ alle Datenträger nach Betriebssystemen und zeigt diese anschließend an. In der Liste markieren Sie das bootunfähige System und starten es mit der Eingabetaste.

Super Grub Disk beherrscht den Bios- und Uefi-Modus. Es ist aber notwendig, das Tool im richtigen Modus zu starten. Wenn es sich bei Ihrem Bootproblem um das typische Szenario nach einem Windows-Setup handelt, ging offenbar eine Bios-Installation voraus (Uefi und das GPT-Partitionsschema vermeiden das Problem).

Super Grub Disk findet und startet Systeme, repariert aber nicht die Bootumgebung. Dazu verwenden Sie nach der Starthilfe im laufenden Linux-System das Terminal. Für die Reparatur von **Bios-Installationen** helfen folgende Kommandos:

```
sudo grub-install --recheck /dev/
  sd[X]
sudo update-grub
```

Anstatt „[X]“ ist die Angabe des Datenträgers nötig, der zum Booten dient. In den allermeisten Fällen ist dies die erste interne Festplatte „/dev/sda“.



Der Boothelfer Super Grub Disk findet und startet Linux-Installationen. Die Reparatur des Grub-Bootloaders erledigen danach zwei Terminalbefehle im gestarteten System.

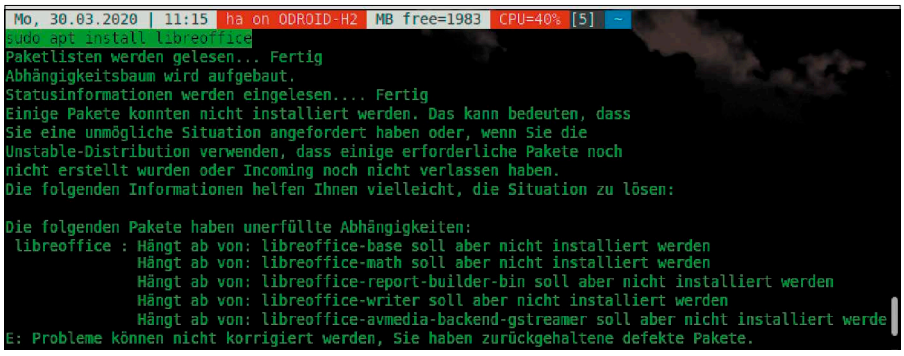
Uefi-Installationen reparieren Sie mit diesen Befehlen:

```
sudo grub-install
sudo update-grub
```

Ein Ziellaufwerk geben Sie in diesem Fall nicht an.

2. Paket-Dilemmas nach Updates und Installationen

Nicht nur Windows hat Updateprobleme, wenngleich bei Debian/Ubuntu/Mint die Systemaktualisierung zunächst sehr einfach erscheint: Der Befehl „sudo apt dist-upgrade“ oder ein Klick auf die automatische Meldung der „Aktualisierungsverwaltung“ genügt für ein Komplettupdate in-



Paket-Dilemmas: Wer Paketkonflikten aus dem Weg gehen will, bleibt am besten konsequent bei den Standardquellen oder installiert Containerformate.

klusive Software. Auch Systemupgrades meldet die Aktualisierungsverwaltung automatisch.

Bei der Vielzahl abhängiger Softwarepakete ist aber nie auszuschließen, dass es nach Installationen oder Updates zu Fehlern kommt. Fremdquellen wie PPAs erhöhen das Risiko. Solche Probleme äußern sich dann mit Meldungen wie „Pakete konnten nicht installiert werden".

Die Mehrzahl solcher Konflikte lässt sich unter Ubuntu/Mint mit

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

lösen. Der Schalter „-f" oder „--fix-broken" (Langform) korrigiert inkonsistente Paketabhängigkeiten und entfernt defekte Pakete. Wo das nicht funktioniert, verwenden Sie den spezielleren Befehl

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

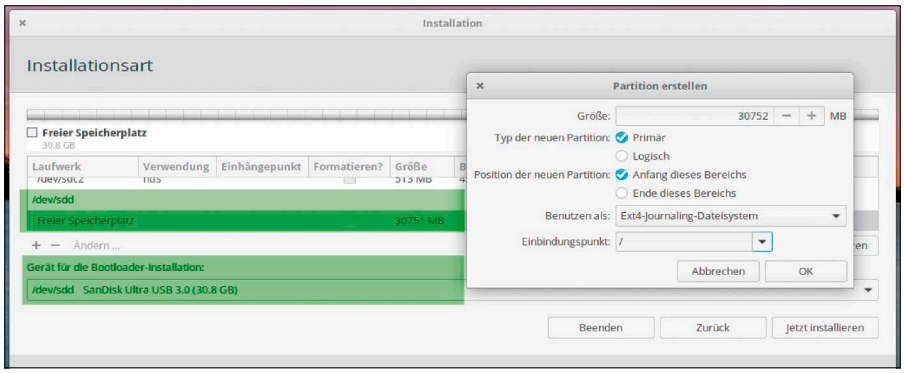
und löschen damit genau das eine genannte Paket ohne Prüfung der Abhängigkeiten. Wer Paketkonflikten für wichtige Anwendungen aus dem Weg gehen will, kann über die Softwareverwaltung Snap- oder Flatpak-Container installieren: Diese Container bringen alle notwendigen Pakete selbst mit. Der Preis ist ein deutlich (!) erhöhter Platzbedarf auf der Festplatte.

3. Installationen: Uefi und Bios

Bei der Linux-Installation dominiert das Problemfeld „Uefi-Bios". Mit anderen Worten: Die Installation als alleiniges System bereitet mit Installern wie Ubiquity und Calamares offenbar keine Probleme. Für das heiklere Multiboot gilt das einfache Grundprinzip, das Setup sofort abzubrechen, wenn der Installer keine Parallelinstallation vorschlägt, obwohl bereits ein System vorliegt.

Dies ist ein klares Indiz, dass der Installer im falschen Modus gebootet wurde und die vorhandene Partitionierung nicht versteht: Ein Bios-Boot versteht nur das alte MBR-Schema, Uefi-Boot nur die GPT-Partitionierung. Um den Installer im richtigen Modus zu booten, müssen Sie beim PC-Start das Bios-Bootmenü aktivieren (meistens eine F-Taste wie F8 oder F12) und dort das Installationsmedium im richtigen Modus starten: Es erscheint dort zweimal – mit und ohne „Uefi"-Angabe.

Wenn Sie nicht wissen, in welchem Modus das vorhandene System installiert ist, booten Sie bei Bedarf zweimal und installieren in dem Modus, wo der Installer das Parallelsystem erkennt.



Installation auf USB: Hier wird die Systempartition eingerichtet. Der Bootloader muss ebenfalls auf den USB-Datenträger (hier „/dev/sdd").

4. Installationen auf USB

Das Linux-Setup auf USB-Medien ist komplizierter als jene auf die interne Festplatte, weil der Installer diese Möglichkeit nicht von sich aus anbietet. Hier benötigen Sie bei der Partitionierung die Option „Manuell" oder „Etwas Anderes". Danach muss Klarheit über das richtige Laufwerk herrschen, weil dieses neu formatiert wird. Da die Kennung „/dev/sda" für die erste interne Festplatte steht, ist „/dev/sdb" der erste mögliche Kandidat, je nach Ausstattung mit internen Platten eventuell auch erst „/dev/sdc" oder „/dev/sdd". Bester Anhaltspunkt ist die angezeigte Kapazität des Laufwerks. Wichtig ist ferner, dass auch der Bootloader auf dem USB-Laufwerk landet. Ist das Laufwerk etwa als „/dev/sdc" als Installationsziel eindeutig erkannt, dann kommt der Bootloader auf „/dev/sdc" und das System auf Partition „/dev/sdc1".

5. Linux-Start mit langer Verzögerung

Der Start von Ubuntu/Mint sollte je nach Hardware nicht länger als etwa zehn bis 40 Sekunden dauern. Deutlich längere Ladezeiten sprechen für einen fehlerhaften Eintrag in der Datei „/etc/fstab", der entweder nach der Installation oder nach manuellem Editieren auftritt. Beweis dafür ist die Meldung „A start job is running for dev-disk-by...", die sich beim hängenden Start durch Druck der Esc-Taste offenbart oder durch einen Systemstart über „Erweiterte Optionen → recovery mode". Das System will eine Festplatte mounten, die es nicht vorfindet. Erste Abhilfe ist ein Auskommentieren der betreffenden Zeile in der „fstab" (mit „#"). Falls die Festplatte zwingend gemountet werden muss, ermitteln Sie mit *lsblk -f* deren korrekte UUID-Kennung und tragen diese ein. Kontrollieren Sie auch den Mountpunkt, da auch ein nicht existierendes Mountverzeichnis Starthänger verursacht.

6. Kompatible und inkompatible WLAN-Adapter

Die meisten in Notebooks integrierten WLAN-Chips arbeiten problemlos, externe USB-WLAN-Adapter sind hingegen nicht immer Linux-kompatibel. Wie die Übersicht auf *https://wiki.ubuntuusers.de/WLAN/Karten* zeigt, werden die USB-WLAN-Adapter von Asus, AVM, D-Link, TP-Link fast allesamt unterstützt. Durch praktischen Einsatz verifiziert haben wir die Tauglichkeit bei folgenden preisgünstigen (circa zehn bis 20 Euro), allerdings älteren Geräten:

- Asus N10 Nano WLAN-Stick
- TP-Link TL-WN823N N300 Mini WLAN
- CSL 300 Mbit/s USB 2.0 WLAN Stick
- Fritz Wlan USB Stick-N v2.4

Weitere, zunächst inkompatible WLAN-Sticks lassen sich über einen Trick in Betrieb nehmen. Das gilt etwa für Sticks von AVM wie dem Fritz WLAN USB Stick v 1.0 und v1.1. Der Trick besteht darin, Windows-Treiber unter Linux einzubinden. Es handelt sich um eine Notlösung, die nicht

WLAN per USB-Dongle: Nicht alle Billiggeräte werden von Linux unterstützt, die meisten Markengeräte wie hier von AVM jedoch schon.

Quelle: amazon.de

immer stabil funktioniert, aber einen Versuch wert ist.

Unter Ubuntu installieren Sie die Pakete „ndisgtk“, „ndiswrapper“, „ndiswrapper-utils-1.9“ und „ndiswrapper-dkms“. Bei Linux Mint sind diese Pakete bereits installiert. Den Windows-Treiber erhalten Sie auf *www.elektronenblitz63.de/html/fritzstick.html*. Entpacken Sie das „gz“-Archiv. Nach dem Terminalbefehl

```
sudo ndisgtk
```

klicken Sie auf „Neuen Treiber installieren“ und wählen hinter „Ort“ die Datei „fwlan64.inf“ (64 Bit) oder „avm_mod.inf“ (32 Bit) aus dem Ordner, wo Sie den Treiber entpackt haben. Klicken Sie auf „Installieren“. Danach erscheint in der Liste „Hardware verfügbar: Ja“. Danach können Sie eine WLAN-Verbindung herstellen.

7. Drucker und Scanner funktionieren nicht

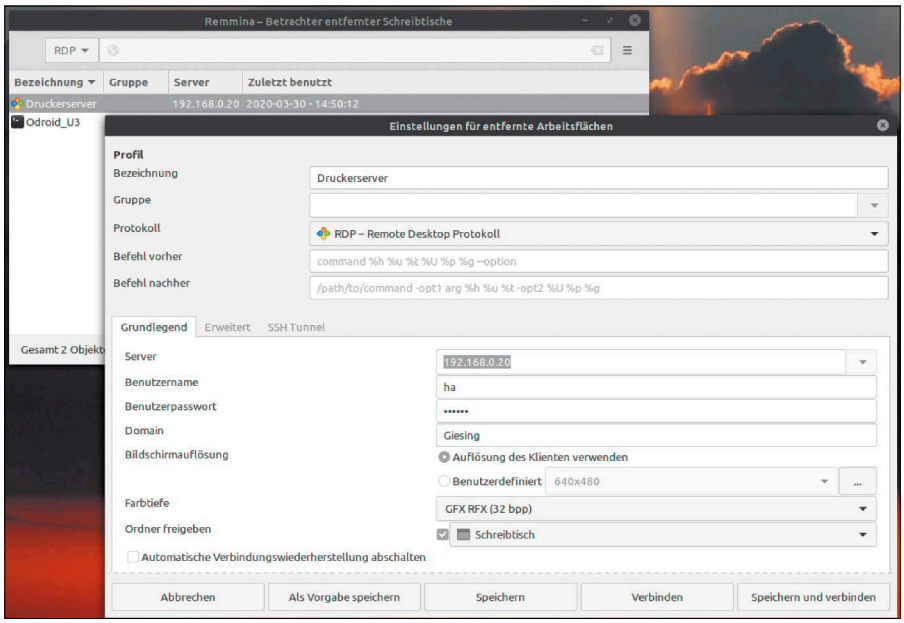
Wenn Druckerhersteller den Marktanteil von Linux als zu gering erachten, um dafür in kostspielige Treiberentwicklung zu investieren, dann arbeitet das Gerät gar nicht oder unbefriedigend. Der beste Rat ist es, schon beim Kauf auf Linux-Kompatibilität zu achten, wobei die Chancen bei Brother, Epson und HP am besten stehen. Eine detaillierte Übersicht finden Sie in der Datenbank *http://openprinting.org/printers*.

Was aber tun, wenn der störrische Drucker nun mal im Haus steht, aber unter Linux nicht arbeitet?

A. Wenn die Einrichtung über „Einstellungen → Drucker“ keinen Treiber anbietet, sollten Sie die Herstellerseite und dort den Downloadbereich aufsuchen. Eventuell gibt es dort bei der Suche nach dem genauen Modell ein DEB-Paket (Debian, Ubuntu, Mint) oder RPM-Paket (Open Suse, Fedora), das Sie herunterladen und installieren können.

B. Wenn der Drucker einen Standard wie Postscript oder GDL unterstützt, kann der bei der Einrichtung empfohlene generische Treiber genügen. Ob diese Variante ohne nativen Gerätetreiber funktioniert (und mit welcher Qualität), ist nur durch Ausprobieren zu verifizieren.

C. Hersteller wie Dell lizenzieren nur die Geräte anderer Hersteller. Es kann sich daher lohnen, das Druckermodell in der oben genannten Druckerdatenbank zu recherchieren und den passenden Treiber beim eigentlichen Hersteller zu suchen.



Drucken ohne Treibersorgen: Wenn ein Windows-Rechner im Dauerbetrieb vorhanden ist, ist der Remotedesktop der einfachste Weg zum Ausdruck.

8. Druckhilfe über Windows-PC

Die Druckerfreigabe eines Windows-PCs erreichen Sie über „Geräte → Netzwerkdrucker“ mit dem Unterpunkt „Windows-Drucker via SAMBA“. Dieser Weg hilft aber nicht weiter, wenn es keinen Linux-Treiber gibt – denn auch bei dieser Druckereinrichtung muss ein Treiber installiert werden. Ausnahmen sind Postscript-, GDL- oder GDI-taugliche Drucker, die eventuell auch mit einem generischen Open-Source-Treiber auskommen. Alle solchen Versuche, einen von Windows freigegebenen Drucker mit Linux anzusprechen, sind aber unnötig kompliziert und fehlerträchtig. Denn wenn für den Druck schon ein laufendes Windows vorausgesetzt wird, dann bietet sich eine viel einfachere Lösung an – die Desktopfreigabe des Windows-Rechners:

1. Der Windows-Rechner muss Remoteverbindungen erlauben. Dies ist unter „Systemsteuerung → System → Remoteeinstellungen → Remoteverbindung … zulassen“ zu aktivieren. Das gerade angemeldete Benutzerkonto erhält dabei automatisch Zugriff, weitere erlaubte Benutzer sind optional möglich. Konto und Kennwort brauchen Sie später beim Linux-Zugriff.

2. Auf dem Linux-System verwenden Sie am besten Remmina. Die Software ist bei Bedarf schnell nachinstalliert. Unentbehrlich für den Windows-Zugriff ist das RDP-Plug-in, aber am besten holen Sie gleich alle Plug-ins an Bord:

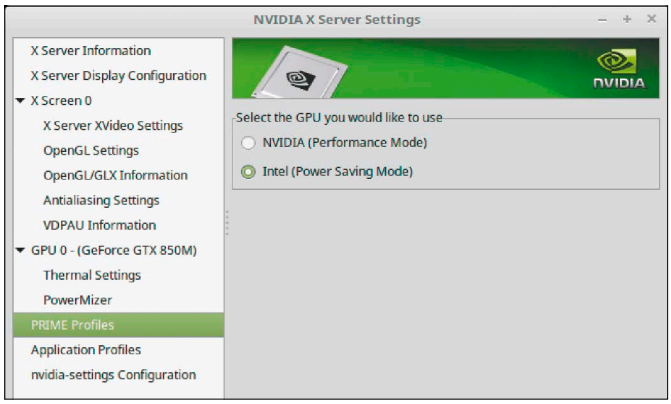
```
sudo apt install remmina remmina-plugin-rdp remmina-plugin-nx remmina-plugin-telepathy remmina-plugin-vnc
```

Danach legen Sie in Remmina eine Konfiguration mit dem Protokoll RDP an und hinterlegen dort die IP-Adresse, Konto und Passwort des Windows-Rechners. Den Austausch der Druckdateien können Sie weiter vereinfachen, indem Sie in Remmina die Option „Ordner freigeben“ aktivieren (etwa den „Schreibtisch“ des Linux-Rechners). Dann hat das Remote-Windows automatisch einen Austauschordner zur Hand, wo die zu druckenden Dateien liegen.

9. Unzureichende Grafikleistung

Linux-Desktopsysteme verwenden einen Open-Source-Grafiktreiber, der für Office und Web ausreicht. Wenn jedoch die Videowiedergabe ruckelt oder ein Spiel nicht die volle Auflösung zeigt, sollten Sie prüfen, ob ein proprietärer Treiber verfügbar ist („Systemeinstellungen → Treiberverwaltung“). Bei Grafikadaptern von Nvidia oder AMD ist dies die Regel, wobei Sie bei mehreren Angeboten den Treiber mit dem Zusatz „empfohlen“ wählen sollten.

Notebooks sind häufig mit Hybridgrafik ausgestattet. Standardmäßig sollte der Grafikadapter der Intel-CPU aktiv sein, um den Stromverbrauch zu minimieren. Voraussetzung dafür ist, dass Sie den Nvidia-Treiber über die Treiberverwaltung instal-



Bei Notebooks mit Hybridgrafik können Sie über „Nvidia X Server Settings“ den Intel-Grafikadapter aktivieren, um die Akkulaufzeit zu verlängern.

liert haben. Gehen Sie im Menü auf „Systemverwaltung → Nvidia X Server Settings“ und dann auf „PRIME Profiles“. Aktivieren Sie dort die Option „Intel (Power Saving Mode)“. Danach melden Sie sich neu an. Wenn Leistung gefragt ist, schalten Sie auf dem gleichen Weg auf den Nvidia-Adapter um, indem Sie die Option „NVIDIA (Performance Mode)“ aktivieren.

10. Grafikprobleme mit Herstellertreiber

Die Installation des Herstellertreibers ist nicht immer erfolgreich. In seltenen Fällen führt das zu Darstellungsfehlern oder verhindert den Start der Oberfläche. Dann hilft nur, die Treiber wieder zu deinstallieren. Dies können Sie in der virtuellen Konsole (Strg-Alt-F2) erledigen: Bei Nvidia-Treibern hilft der Befehl

```
sudo apt purge nvidia*
```

und bei Treibern von AMD verwenden Sie dieses Kommando:

```
sudo apt purge fglrx*
```

Nach einem Neustart wird der Desktop wieder funktionieren – allerdings nun wieder mit Open-Source-Treiber.

11. Die Akkulaufzeiten auf Notebooks

Mit Ubuntu & Co. erreichen Notebooks nicht die Akkulaufzeiten eines Windows-Systems. Daher sollten Sie die vorhandenen Stromsparoptionen maximal nutzen – die Bildschirmabschaltung und den S3-Suspend-Modus („Bereitschaft“). Unter „Systemeinstellungen → Energie“ finden Sie den Timer für den Bereitschaftsmodus. Nach der angegebenen Frist (ohne Nutzer-Aktivität) geht der Rechner in stromsparende Bereitschaft. Für das Verdunkeln und Ausschalten des Bildschirms bei Inaktivität finden Sie die Optionen an gleicher Stelle. Im S3-Modus („Bereitschaft“) verbrauchen Notebooks und PCs nur noch 0,5 bis ein Watt. Die Leistungsaufnahme zwischen einem maximal hellen Notebookdisplay und einem maximal abgedunkelten unterscheidet sich um drei bis vier Watt.

12. Probleme mit Samba-Freigaben

Die Samba-Konfiguration steht in der Liste der Problemfelder weit oben. Bei Samba-Freigaben gibt es zwei Methoden: die „persönliche“ Freigabe aus dem Benutzerkonto (*net usershare* oder direkt im Dateimanager) sowie die „administrative“ Freigabe. Auf die persönliche Freigabe gehen wir hier nicht näher ein, da sie sehr begrenzt nur im eigenen „Home“ und für das eigene Konto funktioniert. Für einen Datenserver, und sei es nur ein kleiner Platinenrechner, eignet sich nur die „administrative“ Freigabe. Zuständig ist die Konfigurationsdatei „/etc/samba/smb.conf“, deren Bearbeitung root-Recht erfordert. Freigaben werden am Ende unter „Share Definitions“ eingetragen. Eine Freigabe lässt sich im Minimalfall mit drei Zeilen erstellen:

```
[Daten]
path = /media/daten
writeable = yes
```

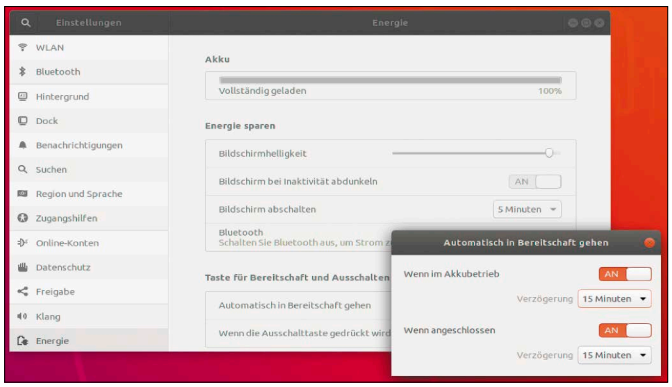
Das Beispiel gibt das Verzeichnis „/media/daten“ unter der Bezeichnung „Daten“ frei. Sollen auch Benutzer ohne Konto die Freigabe verwenden, so ergänzen Sie die Zeile „guest ok = yes“. Umgekehrt kann die Anweisung

```
valid users = ha sepp fritz
```

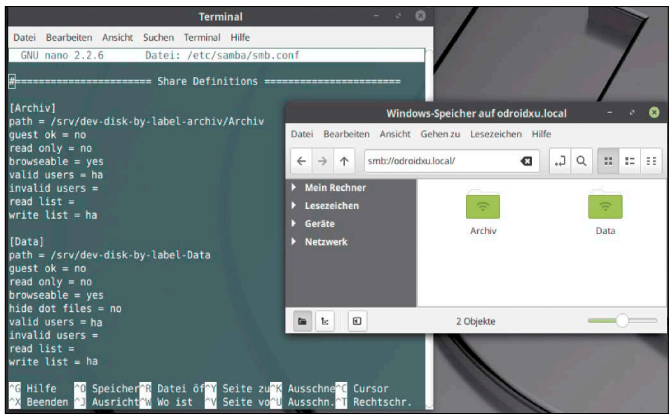
die zugriffsberechtigten Konten einschränken. Beachten Sie, dass manuelle Änderungen erst wirksam werden, wenn Sie Samba neu starten (sudo service smbd restart). Zugriffsprobleme ergeben sich fast nie durch die Netzwerkrechte. Viel häufiger fehlen die lokalen Dateirechte (siehe Punkt 14). Der zugreifende Nutzer muss für lokale Dateiberechtigungen ein Systemkonto auf dem Server besitzen (sudo adduser sepp). Außerdem muss das zugreifende Konto als Samba-User mit Passwort angelegt sein:

```
sudo smbpasswd -a sepp
```

Es vereinfacht den Überblick, System- und Samba-Passwort identisch zu wählen.



Stromsparen insbesondere auf Notebooks: Ubuntu-Systeme sparen immerhin dort, wo es sich am meisten lohnt – beim Bildschirm und beim Time-out für den Bereitschaftsmodus.



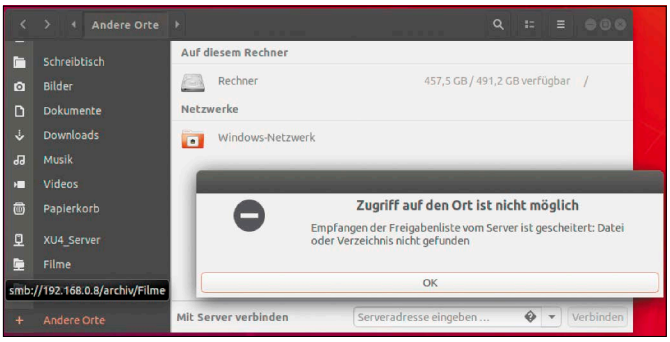
Administrative Freigaben in der „smb.conf“: In diesem Fall darf nur ein einziges Konto („ha“) zugreifen.

13. Samba-Problem unter Ubuntu & Co.

Seit Ubuntu 18.04 gibt es eine neue Samba-Version. Diese verhindert im Dateimanager die Verbindungsaufnahme zu Windows-Netzwerken. Konkret: Beim Klick auf das „Windows-Netzwerk“ im Dateimanager erscheint „Einhängen des Ortes nicht möglich“. Das Suchen nach Servern und Freigaben ist also nicht mehr vorgesehen. Stattdessen muss man sich mit einem Rechner direkt mit Hostnamen oder IP-Adresse verbinden. Das geht auch über das Adressfeld des Dateimanagers:

```
smb://[IP-Adresse]
```

Um sich ständige Eingaben dieser Art zu ersparen, sollten Sie wichtige Samba-Freigaben im Dateimanager als Lesezeichen ablegen (Strg-D in den meisten Dateimanagern).



Die Netzwerkübersicht scheitert. Sie können den Samba-Fehler kompensieren, indem Sie wichtige Freigaben als Lesezeichen ablegen.

14. Falsche lokale Dateirechte

Falsche Dateirechte sind Ursache für manche Zugriffsprobleme, zumal auch Netzfreigaben auch lokale Dateirechte voraussetzen. Linux-Einsteiger können nichts Klügeres machen, als manuelle Rechteänderungen zu vermeiden. Dabei helfen die Dateimanager, die lokale Datenträger und Netzwerklaufwerke automatisch so ins Dateisystem mounten, dass keine Rechtekonflikte entstehen. Solches Automount geht Rechteproblemen aus dem Weg und gilt bis zur Abmeldung.

Bei Zugriffsproblemen, wo statt dem normalen User nur root die nötigen Dateirechte besitzt, ist daher die richtige Antwort eine andere Mountmethode – und nicht das rekursive Ändern massenhafter Dateirechte. Dennoch ist das bei Bedarf natürlich möglich. Der Terminalbefehl chown ändert den Besitzer und arbeitet sich mit Schalter „-R“ rekursiv durch ganze Ordnerebenen:

```
sudo chown -R [Benutzer] [Pfad]
```

Zum Ändern der Rechte dient der Befehl chmod – mit leider zwei Beschränkungen. Er arbeitet nicht rekursiv, was sich mit Hilfe des find-Befehls kompensieren lässt. Chmod unterscheidet aber auch nicht zwischen Dateien und Ordnern. Wenn man Dateien und Ordnern dieselben Zugriffsrechte zuteilt, führt das zu dem Dilemma, dass sich entweder Ordner nicht öffnen lassen oder alle Dateien das „Ausführen“-Recht erhalten. Daher sind zwei Befehle notwendig:

```
find . -type f -exec chmod 664 {} \;
find . -type d -exec chmod 775 {} \;
```

„-type f“ bearbeitet Dateien, „-type d“ die Ordner. Die Beispielbefehle arbeiten ab dem aktuellen Verzeichnis (Punkt „.“).

15. Das ungeliebte Terminal

Viele LinuxWelt-Leser haben Probleme mit dem Terminal. Diese Tatsache ist aber durch den einen oder anderen Tipp nicht zu beheben, da Terminalkompetenz jahrelange Erfahrung erfordert. Eine Grundregel gibt es aber: Zumindest das, was man sich schon erarbeitet hat, sollte schnell wieder abrufbar sein. Um dies sicherzustellen, sollte man die Suchmechanismen für die Standarddatei „~/.bash_history“, ferner die Konfigurationsdatei „~/.bashrc“ optimieren:

Das Terminal vergisst so schnell nichts, weil alle Befehle in der „~/.bash_history“ gespeichert werden. Bei welcher Zeilenmenge Schluss sein soll, bestimmt diese Anweisung in der Datei „~/.bashrc“:

```
HISTFILESIZE=8000
```

Je höher die Zahl, desto umfangreicher ist das Gedächtnis.

Eine systematische Suche in der „bash_history“ bietet der Hotkey Strg-R: Nach Eintippen etwa von „apt“ erscheint der letztgenutzte apt-Befehl. Ist dieser passend, kann er mit Eingabetaste ausgeführt oder mit Alt-Eingabetaste auf den Prompt geholt werden. Ist der angezeigte History-Treffer nicht der passende, geht es mit Strg-R zum vorletzten und so fort.

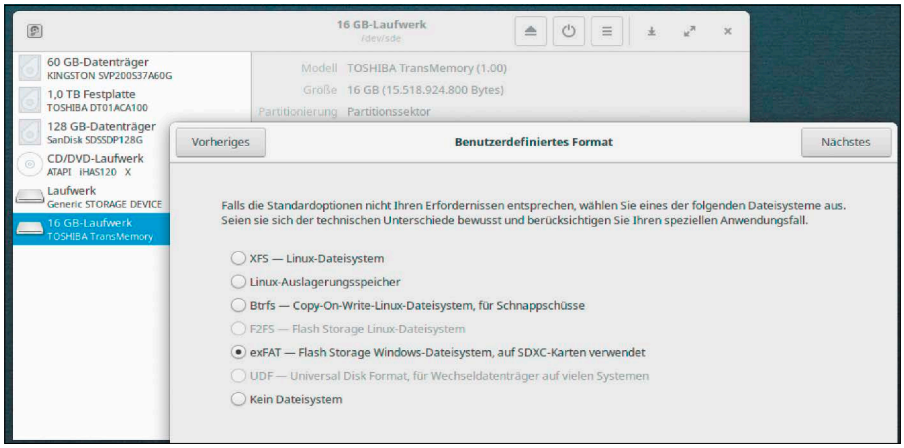
Eine nützliche Ergänzung ist die Filtersuche mit der Taste Bild-oben. Nach Eingabe etwa von „apt“ befördert diese Taste den letzten apt-Befehl auf den Prompt, ein weiteres Bild-oben den vorletzten und so fort. Solche Suche funktioniert aber nur, wenn Sie die Bild-Tasten entsprechend belegen – und zwar in der Datei „/etc/inputrc“. Das Editieren erfordert root-Recht. Sie werden dort die beiden Zeilen

```
\"e[5~\": history-search-backward
\"e[6~\": history-search-forward
```

antreffen und müssen nur das führende Kommentarzeichen „#“ entfernen.

16. Datenträger für Linux und Windows

Sollen interne Festplatten (bei Multiboot) oder mobile USB-Datenträger unter Linux und Windows genutzt werden, gibt es Einschränkungen, die sich aber durch richtige



exFAT unter Linux: Das einfache Microsoft-Dateisystem überwindet das Vier-GB-Limit von FAT32 und ist unter Linux umstandslos nachzurüsten.

Formatierung vermeiden lassen: Linux-Dateisysteme (Ext4) sind für Windows nicht lesbar. Sind nur Linux- und Windows-Rechner im Spiel, ist das Microsoft-Dateisystem NTFS erste Wahl. Linux wie Windows haben dort Lese- und Schreibzugriff, Mac-OS kann dort immerhin lesen.

Laufwerke mit dem alten Dateisystem FAT32 beherrschen alle Systeme. Allerdings gibt es dort das lästige Limit von vier GB pro Einzeldatei. Theoretisch kommt noch das Microsoft-Dateisystem exFAT in Betracht, das solches Limit nicht kennt. Unterstützung für exFAT ist unter Debian/Ubuntu/Mint mit

```
sudo apt install exfat-fuse exfat-
 utils
```

leicht nachzurüsten.

17. Fehlende Software und Spiele

Linux hat für jede Aufgabe eine reiche Auswahl geeigneter Software. Wenn es aber statt Gimp oder Libre Office eine Microsoft- oder Adobe-Software sein muss, kann Linux nicht dienen. Wer aus beruflichen Gründen uneingeschränkte Kompatibilität mit Excel oder Photoshop benötigt, wird mit Linux mittelfristig nicht froh: Der Austausch der Formate erfordert immer wieder lästige Detailkorrekturen (siehe Punkt 18).

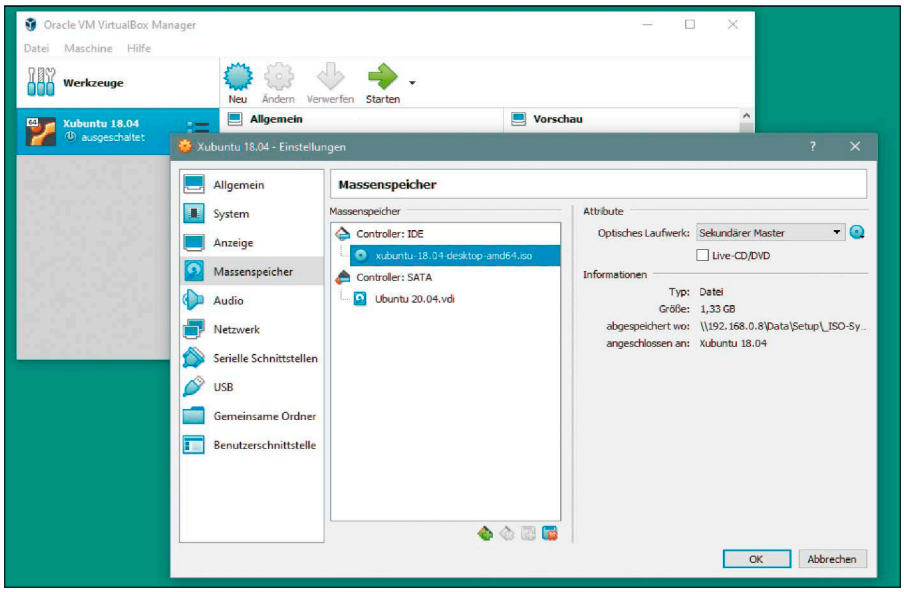
Die Erfolge, die das Projekt Wine mit dem Nachbau der Windows-API vorweisen kann (*https://appdb.winehq.org*), fallen sehr unterschiedlich aus: Dass hier genau die benötigte Version einer Windows-Software einen störungsfreien „Platinum"- oder „Gold"-Status erreicht, bleibt ein Glücksfall. Ferner ist die Benutzung von Wine durchaus komplex: Die Einrichtung ist einfach, der produktive Umgang aber keineswegs trivial.

Linux ist trotz Steam-Anbindung keine Gamingplattform. Das Angebot bleibt gegenüber Windows reduziert und leistungstechnisch kann selbst das Gaming-Linux SteamOS ein Windows nicht schlagen.

18. Kompatibilitätsprobleme mit MS Office

Libre Office lädt und bearbeitet mit Ausnahme von Access-Datenbanken im Prinzip alle Dateien, die mit MS Office erstellt wurden. Umgekehrt verarbeitet MS Office die Open-Document-Formate von Writer und Calc problemlos. Wo es nur um die Produktion von Text, Tabellen und Präsentationen geht, ist Libre Office uneingeschränkt für die Zusammenarbeit mit der Microsoft-Suite geeignet. Problematischer wird es, wenn Microsoft-Formate unter Libre Office weiterbearbeitet werden müssen, denn Word, Excel und Powerpoint bieten Formate, mathematische Funktionen, Diagramme oder Übergangseffekte, die Libre Office nicht kennt. Bei der Bearbeitung müssen Sie daher eventuell nachbessern.

Eine generelle Maßnahme kann den Korrekturaufwand verringern: Libre Office kommt mit den älteren Binärformaten DOC, XLS, PPT besser zurecht als mit dem jüngeren Office Open XML (OOXML) von Microsoft Office ab Version 2007. Daher sollten Libre-Office-Nutzer die Austauschdokumente von den Microsoft-Nutzern besser im älteren „97-2003"-Format anfordern.



VM unter Virtualbox: Technisch ist das Einrichten virtueller Maschinen eine einfache Übung. Windows-VMs benötigen im Dauerbetrieb allerdings eine kostenpflichtige Lizenz.

19. Probleme mit virtuellen Maschinen (VMs)

Virtualisierung ist für viele LinuxWelt-Leser eine Herausforderung. Das Thema ist ein weites Feld, zumal unsere Umfrage nicht zeigt, ob es sich um technische oder prinzipielle Probleme handelt. Nicht verhandelbar ist etwa die Tatsache, dass ein Windows nur 90 Tage als kostenlose Testversion läuft und für einen Dauereinsatz kostenpflichtig aktiviert werden muss. Für Adobe- und Microsoft-Programme, die oft unter virtuellem Windows laufen sollen, gelten noch deutlich kürzere kostenlose Testfristen (30 Tage und weniger). Technisch sind VMs unter einem Virtualisierer wie Oracle Virtualbox keine Aufgabe, die Profiwissen fordert. Im Prinzip ist eine VM nach Angabe des Betriebssystemtyps, der Speicherkapazität und der Festplattengröße bereits angelegt, wonach mit „Ändern → Massenspeicher" nur noch das Startmedium definiert werden muss. Der noch „leere" IDE-Controller erhält ein optisches Laufwerk („Sekundärer Master") und dort wird dann die ISO-Datei des Windows- oder Linux-Systems eingehängt. Ob das danach gestartete Windows- oder Linux-Installationsmedium dann zur Installation genutzt wird oder (im Falle von Linux) nur als Livesystem, entscheidet der Benutzer.

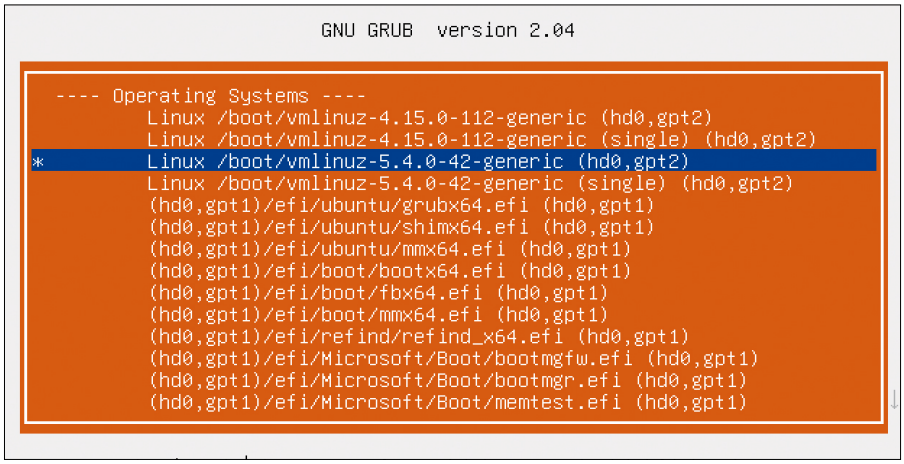
20. Bedienbarkeit der Oberfläche

Schwierigkeiten mit Linux-Desktops sind für LinuxWelt-Leser ein erwähntes, aber nachrangiges Problem. Daher können wir uns hierzu kurz fassen: Es gibt Linux-Desktops, die ungewöhnlich (Gnome, Moksha, Deepin), hermetisch (Gnome, Budgie, Pantheon) oder zu komplex ausfallen (KDE). Aber nichts ist einfacher, als diese ihren Fans zu überlassen und sich an Desktops mit klassischen Elementen zu halten. Der Desktop mit der derzeit umfassendsten Funktionalität ist Cinnamon, der Standard unter Linux Mint. Aber auch ein XFCE (Xubuntu) oder Mate (Ubuntu Mate) geben kaum Anlass zum Rätselraten. Nach unserer Erfahrung haben damit auch Nutzer, die Windows gewöhnt sind, kaum Orientierungsprobleme. ■

Boot- & Startprobleme beseitigen

Wenn ein Linux-System nicht mehr startet, bringen die geeigneten Tools das System wieder zum Laufen. Die Bootumgebung lässt sich mit wenigen Befehlszeilen wiederherstellen.

VON THORSTEN EGGELING



Externen Grub verwenden: Super Grub Disk 2 findet Kernel und Uefi-Bootloader auf der Festplatte. Linux lässt sich dann starten, auch wenn die installierte Bootumgebung defekt ist.

Der Start des Betriebssystems von der Festplatte ist eigentlich eine einfache Aufgabe. Das Bios lädt den Bootloader, der findet die Linux-Installation beziehungsweise den Kernel sowie die initiale Ramdisk und zum Schluss startet dann noch die Desktopumgebung. Es gibt jedoch Situationen, in denen Linux nicht mehr startet. Meist treten solche Fehler in Multiboot-Umgebungen auf, in denen sich die Systeme gegenseitig stören. Ein fehlgeschlagenes Update oder beschädigte Dateien kommen ebenfalls als Ursache infrage.

1. Linux trotz defektem Grub starten

Man kann Linux über Super Grub Disk 2 starten, wenn der installierte Bootloader defekt ist. Von der LinuxWelt-DVD lässt sich das Tool mittlerweile auch im Uefi-Modus booten. Das klappt allerdings nicht immer. Bei Problemen mit dem Uefi-Modus brennen Sie aus der ISO-Datei im Verzeichnis „Extras“ eine bootfähige CD/DVD oder Sie erstellen einen bootfähigen USB-Stick (siehe *www.pcwelt.de/2089747*).

Booten Sie den PC vom erstellen Medium. Achten Sie bei einem Uefi-System darauf, das Bootgerät mit dem vorangestellten „UEFI“ zu wählen. Gehen Sie im Menü auf „Detect and show boot methods“. Super Grub Disk 2 sucht nach bootfähigen Systemen und zeigt diese an. Es genügt dann, den gewünschten Eintrag unter „Operating Systems“ zu wählen, beispielsweise „Linux /boot/vmlinuz-5.4.0-42-generic (hd0, gpt2)“. Wählen Sie den Kernel mit der höchsten Versionsnummer. Grub lädt den Kernel direkt und startet das System. Das funktioniert bei Bios und Uefi-Systemen. Reparaturen kann Super Grub Disk 2 nicht durchführen. Das ist nur über ein laufendes System möglich (siehe Punkt 2).

2. Grub-Bootumgebung reparieren

Die meisten Grub-Probleme lassen sich durch Neuinstallation des Bootloaders beseitigen. Starten Sie das System zunächst über Super Grub Disk (Punkt 1) und öffnen Sie dann ein Terminal. Bei einem Bios-System verwenden Sie diese beiden Befehlszeilen:

```
sudo grub-install /dev/sd[x]
sudo update-grub
```

Für „[x]“ tragen Sie die Bezeichnung für die Bootfestplatte ein. Sollten Sie nicht sicher sein, verwenden Sie die Befehlszeile

```
mount | grep "on / type"
```

Wenn „/dev/sda“ in der Ausgabe auftaucht, ist Linux auf der ersten Festplatte installiert, bei „sdb“ auf der zweiten. Sie können auch die zweite Festplatte als Ziel der Grub-Installation angeben, müssen dann aber die Bootreihenfolge im Firmwaresetup entsprechend anpassen.

Uefi-System: Ermitteln Sie zuerst, ob die Uefi-Partition vorhanden und in das Dateisystem eingebunden ist:

```
mount | grep boot
```

Dann wird eine Ausgabe wie „/dev/sda1 on /boot/efi type vfat“ erscheinen. In Ordnern unterhalb von „/boot/efi/EFI“ liegen die Bootloader-Dateien mit der Dateinamenserweiterung „.efi“. Wenn das nicht der Fall ist, ermitteln Sie mit

```
sudo parted -l
```

(kleines „L“) die Partitionen auf der Festplatte. Es gibt eine kleine FAT32-Partiton meist mit der Bezeichnung „EFI System Partition“, beispielsweise mit der Nummer „1“. Binden Sie diese mit

```
sudo mount /dev/sda1 /boot/efi
```

in das Dateisystem ein. Danach verwenden Sie die folgenden beiden Befehlszeilen:

```
sudo grub-install
sudo update-grub
```

Ein Ziellaufwerk geben Sie bei einer Uefi-Installation nicht an. Das Script findet das Verzeichnis „/boot/efi“ für den Uefi-Bootloader automatisch.

3. Die Grub-Kommandozeile nutzen

Sollte Grub aufgrund einer Fehlkonfiguration den Kernel nicht finden, lässt sich Linux meist trotzdem starten. Voraussetzung dafür ist, dass der Rechner zumindest die Grub-Shell lädt, die sich mit dem Prompt „grub>“ zeigt. Der Befehl

```
ls
```

zeigt die Festplatten und Partitionen in Grub-Schreibweise an. „hd0“ ist die erste Festplatte, „hd1“ die zweite u. s. w. Der Befehl unterstützt die Tab-Vervollständigung.

```
ls (hd0,
```

gefolgt von der Tab-Taste ergänzt die möglichen Angaben oder listet sie auf.

```
ls (hd0,gpt2)/boot
```

beispielsweise zeigt nach Tab oder Eingabetaste den Inhalt des Ordners an. Mit den folgenden vier Zeilen geben Sie Kernel und Ramdisk an und starten das System:

```
set root=(hd0,gpt2)
linux /boot/vmlinuz-5.4.0-42-
 generic root=/dev/sd[XY] ro
initrd /boot/initrd.img-5.4.0-42-
 generic
boot
```

Die Dateinamen müssen Sie nicht vollständig eintippen. Verwenden Sie auch hier die Tab-Taste für die automatische Ergänzung. Den Platzhalter „/dev/sd[xy]“ ersetzen Sie durch den Gerätepfad der Linux-Installation. Bei „hd0,msdos1“ ist das „/dev/sda1“ (Bios/MBR), bei „hd0,gpt2“ verwenden Sie „/dev/sdb2“ (Uefi/GPT). Sobald das System gestartet ist, führen Sie eine Grub-Reparatur durch, wie in Punkt 2 beschrieben.

In der Grub-Shell gilt übrigens die englischsprachige Tastaturbelegung. „(“ beispielsweise geben Sie mit Umschalt-9 ein, „)“ mit Umschalt-0 und „=“ mit Umschalt-´ (rechts neben „ß“).

4. Grub verschwindet nach einem Neustart

Wenn Linux und Windows 10 auf dem PC installiert sind, können Sie über das Grub-Bootmenü zwischen den Systemen wählen. Nachdem Sie Windows gestartet haben, erscheint das Bootmenü jedoch nicht mehr und der Rechner bootet nur noch Windows. Tatsächlich ist Grub aber noch vorhanden, allerdings steht der Windows-Bootmanager in der Bootreihenfolge an erster Stelle. Das lässt sich zwar im Firmwaresetup ändern, die Reihenfolge ändert sich jedoch beim nächsten Windows-Start wieder.

Das Problem lässt sich umgehen, indem Sie Windows 10 starten und eine Eingabeaufforderung mit administrativen Rechten öffnen. Tippen Sie

```
bcdedit
```

ein und drücken Sie die Eingabetaste. Im Abschnitt „Windows-Start-Manager“ sehen Sie hinter „path“ den Eintrag „\EFI\Microsoft\Boot\bootmgfw.efi“. Ändern Sie den Pfad zum Bootloader mit dieser Befehlszeile:

```
bcdedit /set {bootmgr} path \EFI\
 ubuntu\grubx64.efi
```

Sollte Secure Boot aktiviert sein, verwenden Sie den Pfad „\EFI\ubuntu\shimx64.efi“. Für andere Linux-Systeme passen Sie den Pfad an. Sehen Sie unter Linux im Ordner „/boot/efi/EFI“ nach, was für Ihr System gilt. ■

Ausflug ins Terminal: Grub ist mit zwei Befehlszeilen schnell installiert und konfiguriert. Wenn dabei keine Hinweise auf Fehler auftauchen, sollte Linux wieder ohne Probleme starten.

Grub-Shell verwenden: Bei ungültigen Einträgen in der Grub-Konfiguration lassen sich Kernel und Initrd auch manuell starten. Die Tab-Vervollständigung vereinfacht die Befehlseingabe.

BOOTPROBLEME NACH UPDATES UND UPGRADES

Standardmäßig liegt der Ordner „/boot“ auf der Systempartition, außer man hat bei der Installation eine eigene Partition dafür eingerichtet. Bei jedem Kernel-Update kommen neue Dateien hinzu. Ist die Bootpartition zu klein gewählt, kann der Platz knapp werden. Ubuntu und Linux Mint scheinen nicht ausreichend zu prüfen, ob die neuen Dateien tatsächlich gespeichert wurden. In der Folge kann die Installation der Dateien unvollständig sein und der Systemstart scheitern.

Da die vorherigen Kernel-Installationen noch intakt sein sollten, booten Sie eine ältere Version. Im Grub-Bootmenü gehen Sie dann auf „Erweiterte Optionen für Ubuntu“ und auf den gewünschten Kernel. Sollte das Bootmenü nicht auftauchen, halten Sie kurz nach dem Start des PCs die Umschalt-Taste gedrückt. Sorgen Sie für genügend freien Platz auf der Festplatte. Mit

```
sudo apt autoremove
```

löschen Sie unnötige Pakete und veraltete Kernel-Dateien unter „/boot“.

Instabiles System und Abstürze

Auch ein Linux läuft nicht immer rund. Die Ursache für Systemhänger oder Komplettabstürze können bei der Hardware, beim Linux-System selbst oder bei einer Anwendung zu finden sein.

© David Wolski

VON THORSTEN EGGELING

Die meisten Linux-Distributionen sind gut getestet und laufen daher zuverlässig und stabil. Vor allem die Langzeitversionen (LTS) sind eher konservativ konfiguriert und setzen auf bewährte Komponenten. Aber auch eine LTS-Version kann instabil laufen – aus unterschiedlichsten Ursachen. Ein erster Schritt ist daher, den Auslöser eines Problems einzugrenzen.

Die Suche nach der Problemursache

Eine wichtige Unterscheidung betrifft den Zeitpunkt, ab dem ein Fehler auftaucht. Wenn ein neuer Rechner mit einem frisch installierten Linux unzuverlässig arbeitet, sollte man eine andere Distribution ausprobieren. Tritt der Fehler auch hier auf, kann man von einer generellen Inkompatibilität der Hardware mit Linux oder einem Hardwaredefekt ausgehen. In diesem Fall hilft die Suche im Internet nach den Erfahrungen anderen Nutzer mit ähnlicher Hardware eventuell weiter.

Ein Beispiel dafür ist ein Notebook in der Redaktion, bei dem sich USB-3.0-Festplatten im Betrieb immer wieder spontan und unregelmäßig abmelden. Es ist daher unmöglich, größere oder viele Dateien auf das Laufwerk zu kopieren. Das Problem tritt unter mehreren Linux-Distributionen und auch unter Windows auf, weshalb das System beziehungsweise ein Treiber als Ursache eher ausscheiden. Eine sinnvolle Analyse des Fehlers ist kaum möglich. Linux meldet in dieser Situation lediglich, dass das USB-Laufwerk entfernt wurde, aber nicht warum. Derartige Meldungen sind auch bei qualitativ minderwertigen USB-Kabeln oder SATA/USB-Adaptern zu beobachten. Da im Internet zahlreiche Besitzer des gleichen Notebookmodells den Ausfall beschreiben, kann man von einem Serienfehler beim USB-3.0-Port ausgehen, der sich per Software nicht beseitigen lässt. In diesem Fall bleibt nur, das Gerät zurückzugeben und ein anderes Notebook zu erwerben.

War dagegen die Linux-Installation zunächst erfolgreich und ein Fehler tritt erst nach mehreren Monaten auf, gibt es mindestens zwei Möglichkeiten. Ein kürzlich durchgeführtes Update kann verantwortlich sein, aber auch ein Problem mit der Hardware, etwa ein unzureichend gekühlter Prozessor. Linux bietet einige Tools und Protokolle, mit denen man dem Fehler auf die Spur kommen kann.

Die Logdateien auswerten

Standardmäßig zeichnet Linux fast alles auf, was für die Analyse wichtig ist. Die Protokolle sind im Ordner „/var/log“ zu finden. Je nach System und installierten Diensten sind hier unterschiedliche Dateien zu finden. Eines der interessantesten Protokolle ist „/var/log/syslog“, das bei einigen Systemen auch „/var/log/messages“ heißt. Den Inhalt lassen Sie sich in einem Terminal mit

```
cat /var/log/syslog
```

ausgeben. Scrollen Sie nach oben und halten Sie Ausschau nach möglichen Fehlermeldungen. Mit der Zeile

```
tail -f /var/log/syslog
```

erhalten Sie die letzten Logeinträge und die Anzeige wird aktualisiert, wenn neue Meldungen verfügbar sind. Damit lässt sich das System fortlaufend überwachen.

Das Kernel-Protokoll „/var/log/dmesg“ gibt Auskunft über erkannte Hardware, Laufwerke und Aktionen von Treibern. Es wird

bei jedem Bootvorgang neu erstellt. Stürzen Prozesse wegen fehlerhafter Treiber oder defekter Hardware ab, dann wird der Kernel dies hier melden. Die Datei lässt sich ebenfalls über cat betrachten, besser geht es jedoch so:

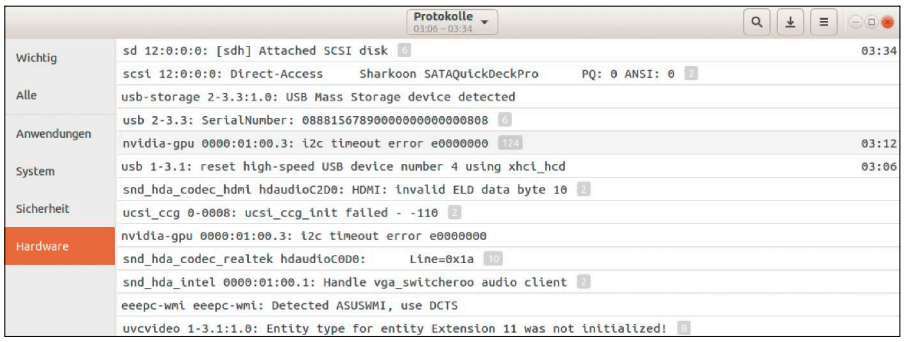
```
dmesg -T
```

Die Option „-T“ bewirkt eine Ausgabe mit Zeitstempel, was eine genaue Untersuchung des Zeitpunkts ermöglicht, an dem ein Fehler aufgetreten ist. Das Tool kennt einige Optionen, über die sich die Ausgabe eingrenzen lässt.

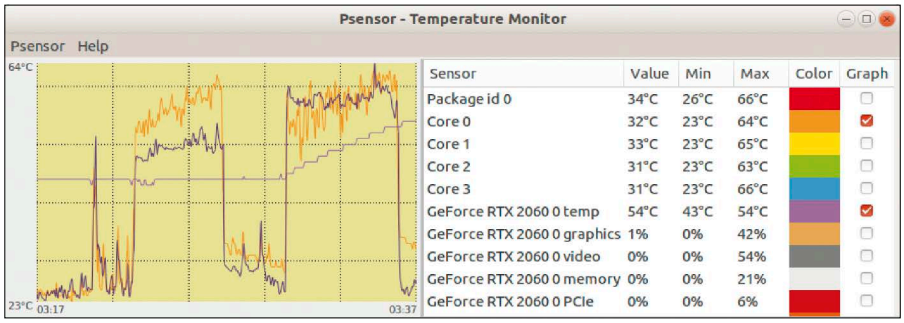
```
dmesg -T -l err
```

Dies filtert die Fehlermeldungen aus. Weitere Optionen liefert die Hilfe, die Sie sich mit dem Parameter „-h“ anzeigen lassen.

Wer eine grafische Oberfläche bevorzugt, startet unter Ubuntu/Linux Mint das Tool Gnome-Logs, das Sie über „Aktivitäten“ oder das Startmenü mit einer Suche nach „Protokolle“ finden. Über die Registerkarten kann man den gewünschten Bereich ansteuern, beispielsweise „System“ oder „Hardware“. Die Anzeige aktualisiert sich nicht automatisch, sondern erst, wenn man zwischen den Registerkarten wechselt.



Protokolle untersuchen: In den Linux-Protokollen sind Informationen und Fehlermeldungen zu finden. Viele Fehlermeldungen sind jedoch harmlos und können ignoriert werden.



Wärmeentwicklung: Eine zu heiße CPU kann einen Systemabsturz bewirken. Das Tool psensor zeigt die Temperaturen an und Sie sehen sofort, ob die Kühlung Ihres PCs ausreicht.

Nicht jeder Fehler hat ernste Auswirkungen

Die Linux-Logdateien enthalten zahlreiche Informationen, Warnungen und meist auch Fehlermeldungen. Die Kunst besteht darin, die relevanten Meldungen herauszulesen. Ansonsten besteht die Gefahr, dass man einem vermeintlichen Fehler nachjagt, der aber nichts mit dem aufgetretenen Problem zu tun hat. Dazu ein Beispiel: Einer unserer Testrechner ist mit einer Nvidia-Grafikkarte RTX 2060 ausgestattet. Diese läuft anscheinend ohne Auffälligkeiten mit einem aktuellen Nvida-Treiber. Im Kernel-Protokoll tauchen aber die Zeilen

```
kernel: ucsi_ccg 0-0008: ucsi_ccg_
  init failed - -110
kernel: nvidia-gpu 0000:01:00.3:
  i2c timeout error e0000000
```

auf (Kernel 5.4.0). Eine Recherche im Internet liefert die Info, dass es sich bei „ucsi_ccg“ um einen Treiber für den USB-C-Port auf der Nvidia-Grafikkarte handelt. Der dient vor allem für den Anschluss von VR-Brillen, könnte aber auch für andere Zwecke genutzt werden. Allerdings unterstützt der Treiber die Grafikkarte nicht. Der Kernel versucht den Treiber trotzdem zu laden, was dann diese Fehlermeldungen produziert. Das ist unserem Fall nur ein Schönheitsfehler, aber um dieses loszuwerden, hilft eine neue Datei „/etc/modprobe.d/blacklist-nvidia-usb.conf“ mit der Zeile

```
blacklist ucsi_ccg
```

als Inhalt. Der Treiber wird dadurch nicht mehr geladen. Mit einem neueren Kernel wird das Problem wahrscheinlich behoben sein. Der Treiber funktioniert dann auch mit unserer Grafikkarte oder er wird gar nicht erst geladen.

Temperaturen analysieren

Zu hohe Temperaturen bereiten immer Probleme. Wenn sich der Prozessor überhitzt, reduziert er zuerst die Taktfrequenz, um die Temperatur zu reduzieren. Wenn das nicht mehr hilft, schaltet er sich ganz aus – und das System stürzt ab. Es lohnt sich daher, die Temperaturen regelmäßig zu prüfen und wenn erforderlich, den Lüfter auszutauschen oder zu reinigen.

Für Temperaturmessungen installieren Sie das Paket „lm_sensors“, das Sie mit

```
sudo sensors-detect --auto
```

konfigurieren.

Das Tool psensor, das Sie über das gleichnamige Paket installieren, zeigt Werte wie CPU-, GPU- und Festplattentemperatur in einer grafischen Oberfläche an. ■

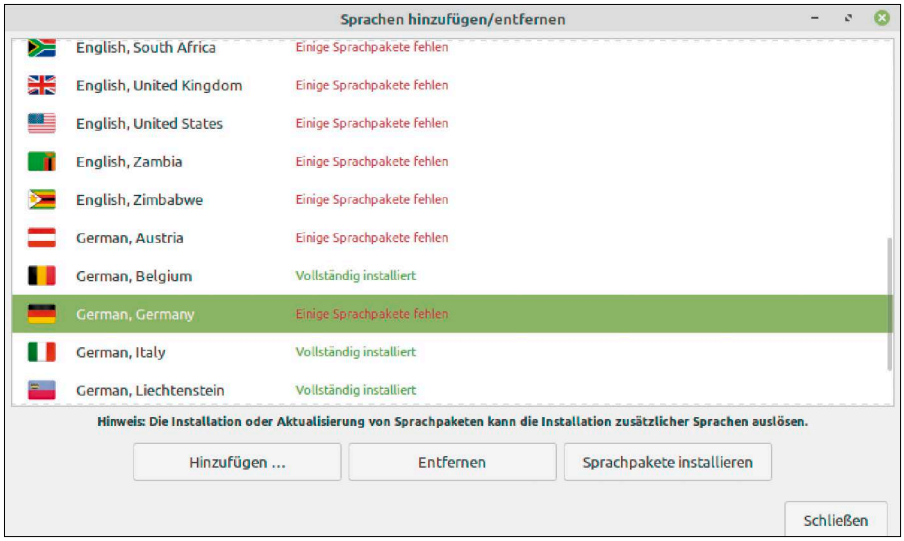
ABSTÜRZENDE ANWENDUNGEN

Programme stürzen ab, wenn sie fehlerhaft programmiert sind oder wenn eine defekte Datei geladen wird (was auch ein Programmierfehler ist). Unter Linux können außerdem fehlende Softwarebibliotheken oder eine fehlerhafte Konfiguration den Start von Anwendungen verhindern. Fehlermeldungen gibt es oft nicht. Zur Analyse empfiehlt es sich, auch ein Programm mit grafischer Oberfläche im Terminal zu starten. Meist gibt es Fehlermeldungen aus, die bei der Reparatur helfen. Im schlimmsten Fall erscheint nur „Segmentation Fault“ (Schutzverletzung). Das Programm ist dann defekt oder nicht für das System geeignet. Dann hilft nur, auf eine Aktualisierung zu warten oder eine ältere Version zu verwenden. Oft gibt es auch Alternativen, die stabiler laufen (Snaps, Flatpaks, Appimages).

Alles Deutsch? Zeit, Sprache & Tastatur

Linux-Systeme sind in vielen Ländern und Sprachen heimisch. Mit ein paar Mausklicks stellen Sie eine andere Sprache für Desktop und Anwendungen ein oder Sie ändern die Tastaturbelegung.

VON THORSTEN EGGELING



Sprachpakete für Linux Mint: Oft ist die Sprachunterstützung nicht vollständig installiert. Nach der Linux-Installation sollten Sie daher die Konfiguration prüfen und fehlende Pakete nachinstallieren.

Die Linux-Basissprache ist Englisch und nicht jedes Programm zeigt sich auch mit einer deutschsprachigen Oberfläche. Meistens lässt sich das ändern, indem man ein passendes Sprachpaket nachinstalliert. In Einzelfällen kann es aber auch sinnvoll sein, das System oder ein einzelnes Programm auf Englisch umzustellen, etwa um eine englischsprachige Fehlermeldung zu erhalten. Eine Internetsuche danach liefert oft bessere Ergebnisse.

Die Zeitzone legen Sie bereits bei der Installation fest. Davon hängen beispielsweise auch die Regionaleinstellungen wie Datumsformat und Währung ab. Bei Bedarf lässt sich die Zeitzone ändern, etwa wenn Sie sich gerade im Ausland befinden. Probleme beziehungsweise Abweichungen bei der Uhrzeit kann es geben, wenn Sie mehrere Betriebssysteme auf dem Rechner verwenden. Die korrekte Uhrzeit ist aber wichtig, etwa für Updates oder die Anmeldung bei Websites, insbesondere bei der Zwei-Faktor-Authentifizierung etwa über die Smartphone-App Google Authenticator.

Spracheinstellungen kontrollieren

Nach einer Linux-Neuinstallation sollte der erste Weg in die Spracheinstellungen führen. Auch wenn die Sprache bereits bei der Installation festgelegt wird, sind oft nicht alle Sprachpakete für die aktivierten Sprachen installiert.

Unter Ubuntu 20.04 rufen Sie die „Einstellungen“ nach einem Mausklick auf den rechten Bereich der Leiste oben auf dem Bildschirm auf. Gehen Sie auf „Region und Sprache“ und klicken Sie auf „Installierte Sprachen verwalten“. Ubuntu sucht automatisch nach fehlenden Sprachpaketen und bietet deren Installation an.

Meist fehlen jedoch keine deutschen Sprachpakete, sondern englischsprachige. Die kommen in der Regel allerdings nicht zum Einsatz. Es kann aber vorkommen, dass bei einem Softwareupdate das deutsche Sprachpaket noch nicht verfügbar ist. Ubuntu aktualisiert dann die Software und das englische Sprachpaket. Das Programm startet mit einer englischsprachigen Oberfläche, bis auch ein Update für das deutsche Sprachpaket bereitsteht. Bei anderen Linux-Distributionen finden sich entspre-

Sprachpakete für Ubuntu: Ubuntu signalisiert fehlende Sprachpakete in einem eigenen Dialog. Meist fehlen nur Pakete für andere Sprachen als Deutsch, die Sie aber trotzdem installieren sollten.

chende Einstellungen, je nach verwendetem Desktop. In Linux Mint 20 Cinnamon beispielsweise gehen Sie im Menü auf „Einstellungen → Sprachen“ und klicken auf „Sprachen hinzufügen/entfernen“. Wenn hinter „German, Germany“ die Angabe „Einige Sprachpakete fehlen“ steht, klicken Sie die Zeile an und dann auf die Schaltfläche „Sprachpakete installieren“.

Spracheinstellungen ändern

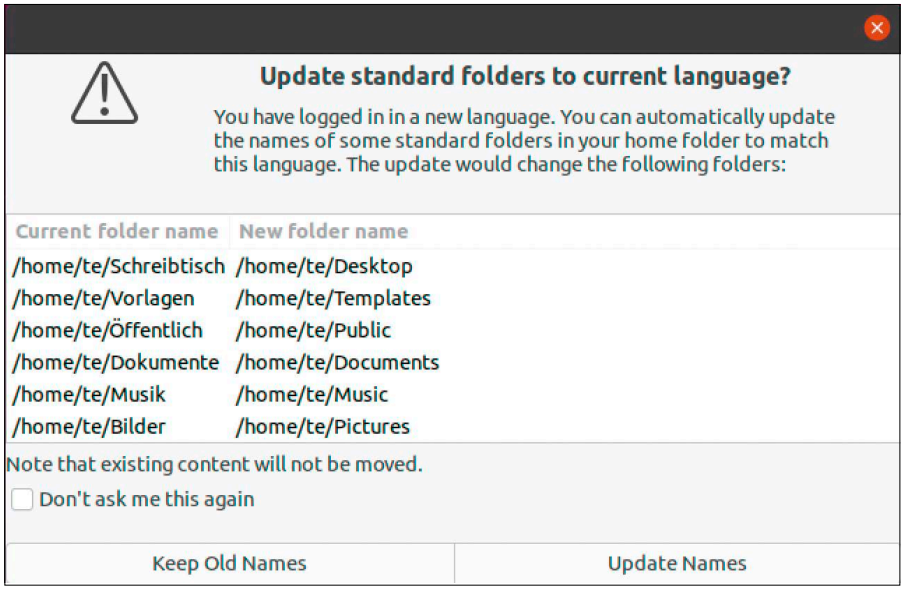
Die bei der Linux-Installation gewählte Sprache gilt systemweit und für alle Benutzerkonten. Wer etwas ändern möchte, geht unter Ubuntu 20.04 in den „Einstellungen“ auf „Region und Sprache“. Es öffnet sich das Fenster „Sprachen“, in dem man auf „Installierte Sprachen verwalten“ klickt. Unter „Sprache für Menüs und Fenster“ sind bei einer deutschsprachigen Ubuntu-Standardinstallation die Einträge „Deutsch (Deutschland)“, „English (United Kingdom)“ und „English“ zu sehen.

Die erste Sprache in der Liste ist der Standard für die Benutzeroberfläche. Sollte für ein Programm kein deutsches Sprachpaket vorhanden sein, verwendet es der Reihe nach die anderen Sprachen aus der Liste. Der letzte Eintrag ist immer „English“. Einträge darunter sind ausgegraut und werden ignoriert. Bei Bedarf lässt sich die Reihenfolge ändern, indem Sie eine Sprache mit der Maus an eine andere Position ziehen.

Die Einstellungen unter „Sprache für Menüs und Fenster“ gelten nur für den gerade angemeldeten Benutzer. Andere Benutzer des Systems können daher ihre eigenen Sprachpräferenzen festlegen. Änderungen werden erst wirksam, nachdem sich der Benutzer ab- und wieder angemeldet hat oder Linux neu gestartet wurde.

Per Klick auf „Systemweit anwenden“ übernehmen Sie die Spracheinstellungen für alle Benutzer sowie für den Start- und Anmeldebildschirm. Dafür ist das Passwort des Systemverwalters erforderlich. Ein Standardbenutzer kann diese Einstellung nicht ändern, aber für sein eigenes Konto eine beliebige Sprache wählen.

Die Umstellung der Sprache kann Auswirkungen auf einige Ordnernamen haben. Wenn Sie beispielsweise die Standardsprache auf „English (United States)“ ändern, fragt Ubuntu bei der nächsten Anmeldung, ob Sie die lokalisierten Bezeichnungen verwenden wollen. Wenn Sie auf „Update Names“ klicken, werden die Ordnernamen angepasst und leere Ordner gelöscht. Der Inhalt der bisherigen Ordner wird nicht verschoben. Das müssen Sie selbst erledigen und danach die nicht mehr benötigten Ordner löschen. Alternativ klicken Sie auf „Keep Old Names“, wenn Sie die deutschsprachigen Bezeichnungen behalten möchten. Auf Anwendungen hat das keine Auswirkungen. Dialoge wie „Datei öffnen“ oder „Datei speichern“ zeigen bei jeder Sprache automatisch einen passenden Ordner wie „Dokumente“ oder „Documents“, je nachdem, was vorhanden ist.



Sprachumstellung: Die Namen der Standardordner lassen sich für die jeweilige Sprache anpassen. Meist ist es besser, die bisherigen Namen zu behalten, damit Inhalte nicht verschoben werden müssen.

Im Fenster „Sprachen“ lassen sich auf der Registerkarte „Regionale Formate“ weitere Anpassungen vornehmen. Die Anzeige von Zahlen, Datumsangaben und Währungen erfolgt unabhängig von der Sprache der Oberfläche und kann hier geändert werden. Die Einstellungen gelten für den aktuellen Nutzer, nach einem Klick auf „Systemweit anwenden“ für alle Benutzerkonten.

Linux Mint 20 Cinnamon: „Einstellungen → Sprachen“ führt zum Fenster „Spracheinstellungen“, in dem Sie für „Sprache“, „Region“ und „Zeitformat“ jeweils eine andere

SPRACHEN UND ÜBERSETZUNGEN FÜR LINUX

Die meisten Programme und Tools unter Linux unterstützen mehrere Sprachen. In der ausführbaren Datei ist meist nur Englisch als Standardsprache enthalten. Die Sprachdateien mit den Übersetzungen werden je nach Spracheinstellung dynamisch geladen, wofür meist das Gettext-Framework zum Einsatz kommt.

Sprachdateien mit der Endung „.mo“, die in den einzelnen Programmpaketen enthalten sind, liegen in der Regel unterhalb von „/usr/share/locale“ in Ordnern mit der jeweiligen Länderkennung. „mo“-Dateien für Systemtools und die Desktopumgebungen werden über Sprachpakete installiert, beispielsweise „language-pack-[Länderkennung]“, „language-pack-gnome-[Länderkennung]“ „language-pack-kde-[Länderkennung]“. Die Datei liegen unter „/usr/share/locale-langpack“.

Für einige Anwendungen, beispielsweise Firefox, Thunderbird und Libre Office gibt es eigene Sprachpakete, beispielsweise „firefoce-locale-de“ oder „libreoffice-l10n-en-gb“.

In der Regel werden alle Sprachpakete automatisch installiert, wenn Sie eine neue Sprache hinzufügen. Sollte ein Programm nicht in der gewünschten Sprache erscheinen, sehen Sie nach, ob das zugehörige Pakete tatsächlich installiert ist und ob es dieselbe Versionsnummer trägt.

Sprache einstellen können. Nach einem Klick auf „Systemweit anwenden“ gelten die Einstellungen für alle Benutzer und den Anmeldebildschirm. Auch bei Linux Mint kann jeder Benutzer die eigenen Spracheinstellungen individuell ändern. Bei Standardbenutzern sind die Schaltflächen „Systemweit anwenden“ und „Sprachen hinzufügen/entfernen“ im Fenster „Spracheinstellungen“ nicht sichtbar.

Tastaturbelegung ändern

Die Belegung der Tastatur lässt sich bei Ubuntu 20.04 in den „Einstellungen“ unter „Region und Sprache“ unabhängig von der Sprache konfigurieren. Unterhalb von „Eingabequellen“ fügen Sie über die „+“-Schaltfläche weitere Belegungen hinzu. Die erste Sprache ist der Standard. Die Reihenfolge lässt sich per Klick und Ziehen mit der Maus ändern.

Rechts neben jedem Eintrag in der Liste befindet sich eine Schaltfläche mit einem Augen-Symbol. Nach einem Klick darauf erscheint ein Schema mit der zugehörigen Tastaturbelegung. Die meisten Tasten sind vierfach belegt. Die linke Spalte bei jeder Taste zeigt die Zeichen in Kombination mit der Shift-Taste, die rechte Spalte die zusammen mit der Alt-Gr-Taste (Super R).

Klicken Sie rechts neben „Eingabequellen“ auf die Schaltfläche mit dem Zahnradsymbol. Wählen Sie die Option „Verschiedene Quellen für jedes Fenster erlauben“, wenn Sie die Tastatur für unterschiedliche Fenster getrennt einstellen möchten. Die Eingabequelle lässt sich über das Menü der Schaltfläche mit dem Sprachkürzel am oberen rechten Bildschirmrand ändern.

Linux Mint 20 Cinnamon: Gehen Sie im Menü auf „Einstellungen → Tastatur“ und wechseln Sie auf die Registerkarte „Tastaturbelegungen“. Über die „+“-Schaltfläche fügen Sie weitere Sprachen hinzu, die Reihenfolge lässt sich über die Pfeil-Schaltflächen ändern. Im rechten Bereich des Fensters gibt es zwei Optionen. Sie können für alle Fenster die gleiche Tastaturbelegung verwenden oder unterschiedliche Belegungen für jedes Fenster. Die Umschaltung erfolgt über das Menü mit Landesflaggen in der Leiste am unteren Bildschirmrand.

Sprache im Terminal wechseln

Die bisher genannten Spracheinstellungen legen die Werte einiger Umgebungsvariablen fest. In einem Terminal (Strg-Alt-T) lassen Sie sich die Werte mit

```
locale
```

gefolgt von der Eingabetaste ausgeben. Bei einem deutschsprachigen Standardsystem enthalten alle LC_*-Variablen sowie „LANG“ den Wert „de_DE.UTF8“. „LANGUAGE“ besitzt den Wert „de_DE“ und „LC_ALL“ ist kein Wert zugewiesen. Die LC_*-Variablen sind für die unterschiedlichen Bereiche der Regionaleinstellungen zuständig.

Die Variablen lassen sich nutzen, um ein Programm schnell mit einer anderssprachigen Oberfläche zu starten oder die Sprache für nur ein Terminal zu ändern. Die Zeile

```
LANG=en_US.UTF-8 firefox
```

beispielsweise startet Firefox mit englischsprachiger Oberfläche. Programme im Terminal werten meist die Variable „LANGUAGE“ aus.

```
LANGUAGE=en_US.UTF-8 ping google.
  de
```

gibt Meldungen in englischer Sprache aus. Im Zweifelsfall verwendet man einfach beide Variablen:

```
LANGUAGE=en_US.UTF-8 LANG=en_US.
  UTF-8 gnome-terminal
```

Mit dieser Zeile öffnen Sie in neues Terminal, für das die geänderten Variablen gelten. Hier können Sie Programme mit grafischer Oberfläche oder Terminalprogramme starten und sehen Ausgaben in der angegebenen Sprache.

Schreibweisen: Variablen werden durchgehend in Großbuchstaben geschrieben, bei den Werten kann es unterschiedliche Schreibweisen geben. Der Befehl

```
locale -a
```

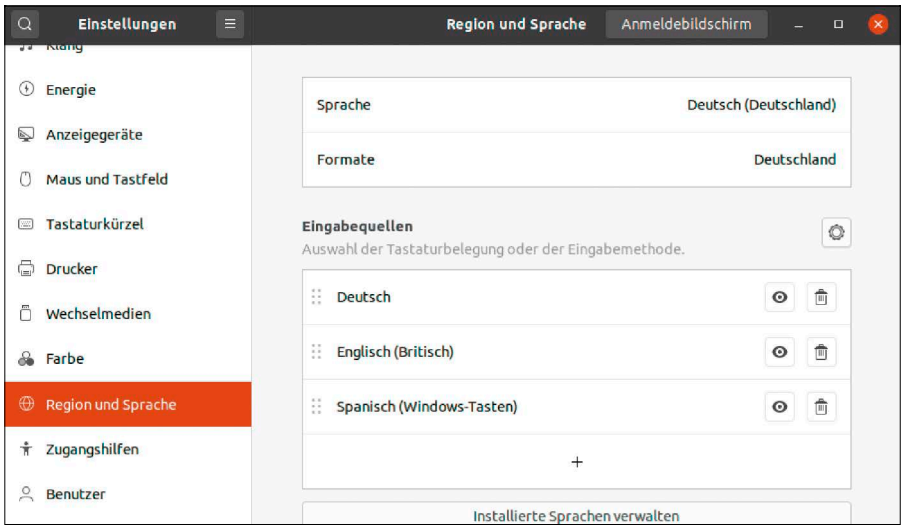
gibt Auskunft über die verfügbaren Locales. In der Ausgabe erscheint beispielsweise „en_US.utf8“, was als Wert für eine Variable ebenfalls gültig ist. Die durchgängige Kleinschreibung „en_us.utf8“ wird dagegen nicht akzeptiert.

Sprachunterstützung im Terminal einrichten: Eine Liste aller verfügbaren Locales ist in der Datei „/usr/share/i18n/SUPPORTED“ zu finden. Mit beispielsweise

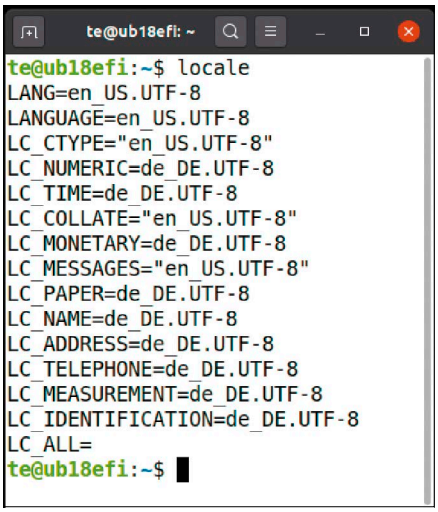
```
sudo locale-gen fr_FR.UTF-8
```

lässt sich eine neue Locale für Französisch erzeugen. Das wirkt sich jedoch nur auf Programme aus, für die bereits Sprachdateien vorhanden sind. Mit

```
sudo apt install language-pack-fr
```



Tastaturbelegung: Sie können mehrere Tastaturlayouts festlegen und die Belegung bei Bedarf schnell umstellen. Auf Wunsch funktioniert das auch für jedes Fenster individuell.



Umgebungsvariablen: Welche Spracheinstellungen gelten, wird über diese Variablen gesteuert. Programme lassen sich in einer anderen Sprache starten, indem Sie die Werte ändern.

installieren Sie beispielsweise das französische Sprachpaket.
Wer eine Sprache über die „Einstellungen“ und „Region und Sprache“ hinzufügt, muss keine Pakete manuell installieren. Die Einrichtung der Sprachunterstützung erfolgt dabei für Terminalprogramme und Desktopanwendungen automatisch.

Datum und Uhrzeit einstellen

Datum und Uhrzeit richten sich nach der Zeitzone, die Sie bei der Installation festgelegt haben. In den „Einstellungen“ lässt sich die Zeitzone bei Bedarf unter „Datum und Zeit“ ändern. Die Uhrzeit wird automatisch über einen NTP-Server (Network Time Protocol) synchronisiert, was eine Internetverbindung voraussetzt. Sollte die Uhrzeit zu stark abweichen, funktioniert das manchmal nicht. In diesem Fall setzen Sie unter „Datum und Zeit“ den Schalter hinter „Datum und Uhrzeit automatisch ermitteln“ auf „Aus“. Danach klicken Sie auf „Datum und Zeit“ und stellen die Uhr manuell ein. Anschließend setzen Sie den Schalter wieder auf „An“.
Bei Linux Mint 20 Cinnamon funktionieren die Zeiteinstellungen über „Einstellungen → Datum & Zeit“ entsprechend.
Wer auf einem Server beispielsweise über SSH die Zeit im Terminal korrigieren muss, verwendet diese drei Befehlszeilen:

```
timedatectl set-ntp false
timedatectl set-time "2020-10-10
 17:43"
timedatectl set-ntp true
```

Dies gilt für alle Systeme mit systemd (Debian, Ubuntu, Mint und viele mehr).

Uhrzeit bei Multiboot-Installationen

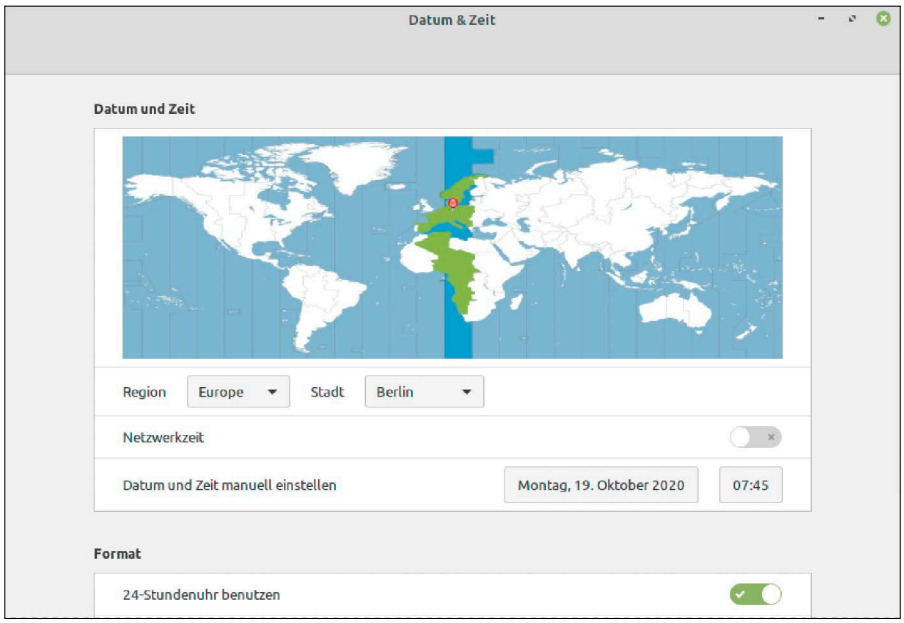
Datum und Uhrzeit erhalten Betriebssysteme von der Echtzeituhr auf der Hauptplatine (Real-Time Clock, RTC). Die Uhr geht meist nicht besonders genau, was die Synchronisierung mit einem NTP-Server erforderlich macht. Die korrigierte Uhrzeit wird auch an die Uhr auf der Hauptplatine übermittelt. Eine weitere Zeitkorrektur ist die Umstellung von Winter- auf Sommerzeit und wieder zurück. Dafür sorgt das Betriebssystem automatisch.
Linux und Windows interpretieren die Werte der Echtzeituhr auf der Hauptplatine unterschiedlich. Linux verwendet die koordinierte Weltzeit (UTC), Windows geht von der lokalen Zeit aus (Mitteleuropäische Zeit, MEZ, UTC+1). Zwischen beiden Zeitangaben liegen – je nach Sommer- oder Winterzeit – eine oder zwei Stunden. Im Terminal lässt sich mit

```
timedatectl
```

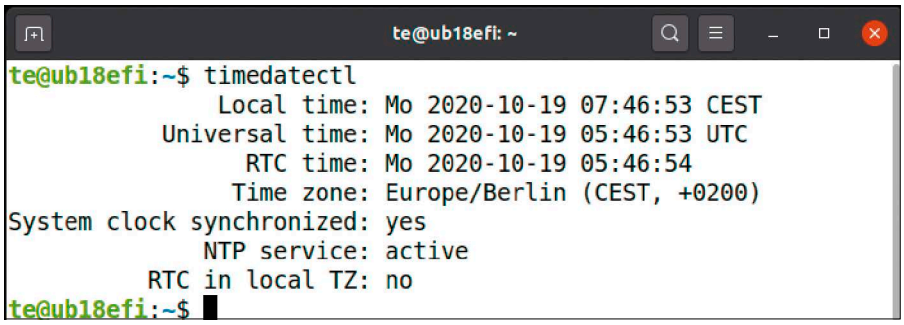
ermitteln, welche Zeiteinstellungen Linux verwendet. Steht hinter „RTC in local TZ:“ die Angabe „no“, basiert die Zeitangabe auf UTC.
Wenn Sie Windows starten, geht das System davon aus, das die Uhr auf UTC+1 eingestellt ist. Linux hat jedoch die UTC-Zeit eingestellt und die Uhr geht unter Windows eine Stunde oder bei Sommerzeit zwei Stunden nach. Windows korrigiert das mit einiger Verzögerung über NTP, was aber beim nächsten Linux-Start zu einer falsch eingestellten Uhr führt.
Zur Lösung des Problems können Sie unter Ubuntu oder Linux Mint das System mit

```
sudo timedatectl set-local-rtc 1
```

für die Verwendung der lokalen Zeit umstellen. Das hat jedoch den Nachteil, dass das System nicht mehr weiß, ob die Umstellung auf Sommer-/Winterzeit bereits erfolgt ist. Man muss dann erst auf den Abgleich mit dem Zeitserver warten, bis die korrekte Uhrzeit angezeigt wird.
Es erscheint daher sinnvoller, Windows UTC beizubringen. Dazu gehen Sie in der Registry auf „Hkey_Local_Machine\System\CurrentControlSet\Control\TimeZoneInformation“ und erstellen einen DWORD-Wert mit dem Namen „RealTimeIsUniversal“, den Sie auf „1“ setzen. Sollte Windows diesen nicht berücksichtigen, verwenden Sie einen QWORD-Wert.
Starten Sie Windows neu, öffnen Sie die „Einstellungen“ und gehen Sie auf „Zeit und Sprache → Datum und Uhrzeit“. Hier setzen Sie den Schalter unter „Uhrzeit automatisch festlegen“ auf „Aus“. ■



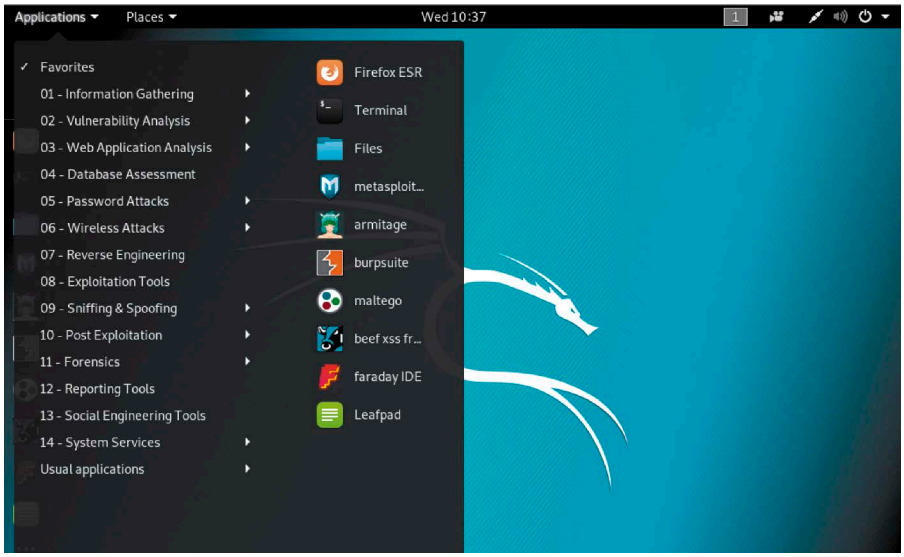
Uhrzeit einstellen (Linux Mint): Datum und Uhrzeit können Sie manuell ändern, nachdem Sie „Netzwerkzeit“ (NTP) deaktiviert haben. Die Zeitzone lässt sich hier ebenfalls wechseln.



Zeitquelle anpassen: Linux geht davon aus, dass die Hauptplatine die UTC-Zeit liefert. Wer parallel Windows nutzt, kann auch die lokale Zeit einstellen, um Konflikte zu vermeiden.

Hacken Sie Ihre eigenen Systeme!

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



VON STEPHAN LAMPRECHT

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

Die Grenzen des Erlaubten

Ein Pentest ist genau unter zwei Voraussetzungen erlaubt:

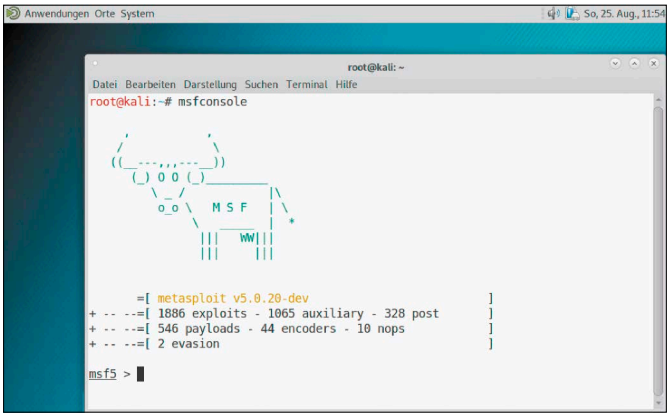
1. Sie bombardieren ein System, das Ihnen gehört und von Ihnen betrieben wird. Diesen Bereich verlassen Sie bereits, wenn Sie einen Webserver testen, der bei einem Provider steht. In den meisten günstigeren Tarifen teilen Sie sich einen physikalischen Rechner mit einer ganzen Reihe von anderen Kunden.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

2. Sie haben vom Inhaber und Betreiber einer Infrastruktur den offiziellen Auftrag erhalten, einen solchen Test durchzuführen.

Auf den nächsten Seiten zeigen wir Ihnen, wie Sie mit einem Framework handwerklich eigene Pentests planen und durchführen.

Metasploit stellt sich vor

Ein Framework sammelt verschiedene Werkzeuge rund um eine Aufgabenstellung. Zu dieser Kategorie gehört Metasploit, das unter einer Oberfläche verschiedene Tools versammelt, die für Pentests benötigt werden. Dazu gehören Programmkomponenten zur Informationsbeschaffung und auch die sogenannten Exploits. Das sind Programmbestandteile, mit denen sich bekannte Sicherheitslücken eines Systems ausnutzen lassen. Metasploit ist eine kommerzielle Anwendung. Es gibt aber eine kostenlose Version, die für Linux, Windows und Mac-OS angeboten wird und die Basisfunktionen zur Verfügung stellt. Das kommerzielle Produkt ist zusätzlich mit einer

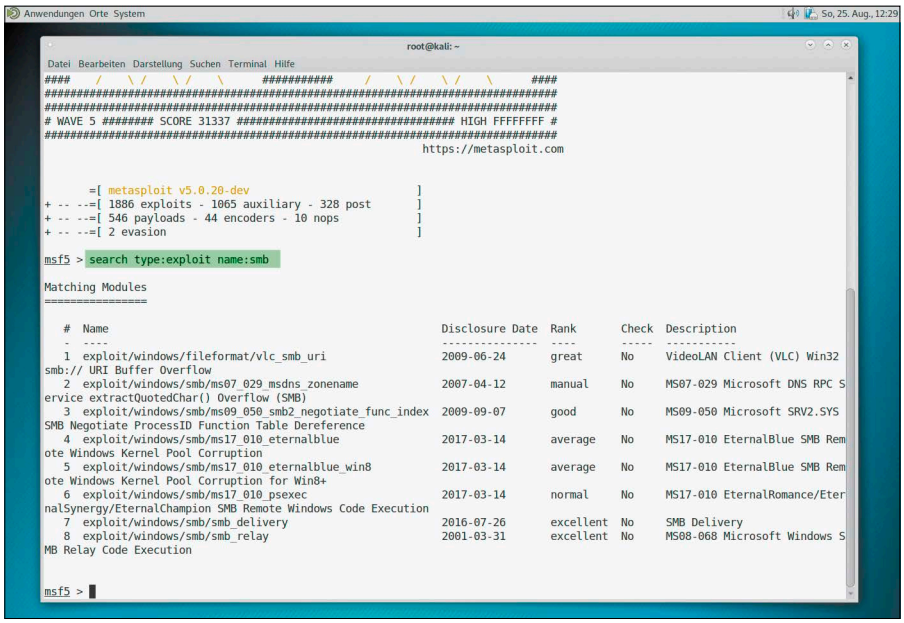


Wer ohne grafische Oberfläche auskommt, kann die Community-Edition von Metasploit nutzen. Zentrales Element ist die eigene Konsole.

Weboberfläche, Automatisierungsfunktionen und Assistenten ausgestattet.
Die Installation von Metasploit unter Linux besteht im Funktionsaufruf einer URL (Anleitung unter *https://github.com/rapid7/metasploit-framework/wiki/Nightly-Installers*), die einen Eintrag im Paketmanager vornimmt. Darüber kann dann das Programm installiert werden. Wenn Sie die Weboberfläche verwenden wollen, können Sie auch eine Trialversion des kommerziellen Produkts verwenden. Dazu ist aber ein Lizenzschlüssel erforderlich, den Ihnen der Hersteller an eine hinterlegte Mailadresse sendet.
Für diesen Artikel haben wir uns für die kostenlose Community-Edition entschieden, die ohne die Registrierung arbeitet. Abkürzen können Sie die Installation und die Arbeit mit dem Programm, wenn Sie sich für Kali Linux entscheiden. Dort ist das Metasploit-Framework bereits mit an Bord. Dazu später noch mehr.

So planen Sie eine Attacke

Wie würde ein Hacker vorgehen, wenn er ein nicht vertrautes System erforschen möchte? Der erste Schritt besteht in der Beschaffung von Informationen. Geht es darum herauszufinden, welche Server in einem Netzwerk überhaupt öffentlich zugänglich sind, kann Nmap die ersten Hinweise liefern (siehe ab Seite 86). Mit Nikto (*https://github.com/sullo/nikto*) könnten dann weitere Informationen dazu ermittelt werden, etwa, welche Software darauf läuft. Die Software würde auch Basisinfos liefern, wenn ganz gezielt ein spezieller Server untersucht werden soll. Und dann gibt es auch noch die Suchmaschine Shodan, die frei Haus Infos zu öffentlich zugänglichen Systemen aller Art bereitstellt. Shodan (*www.shodan.io*) sucht mit Crawlern aktiv nach Routern, allen Sorten von Internet-of-Things-Geräten und von außen erreichbaren Raspberry-Pi-Platinen.
Ist erst einmal bekannt, unter welcher Adresse und welchem Kanal das Ziel zu erreichen ist, und zusätzlich feststeht, welche Software darauf läuft, wird nach Schwachstellen gesucht. Dabei wollen wir keine neuen Schwachstellen aufdecken, sondern lediglich Systeme darauf untersuchen, ob die bekannten Sicherheitslücken verschlossen worden sind. Nach der Informationssammlung erfolgt dann der gezielte Versuch, eine solche Schwachstelle auszunutzen.



Metasploit auf der Suche: Über das Kommando „Search“ suchen Sie hier nach Modulen oder Lücken einer Software oder eines Systems.

Metasploit in Aktion: Passwörter testen

Sie starten Metasploit am besten in einem Terminal mit dem Kommando

```
msfconsole
```

Der erste Start nimmt etwas mehr Zeit in Anspruch, weil das System erst einmal seine Stammdaten aktualisiert. Danach werden Sie von einem eigenen Prompt begrüßt. Sie befinden sich damit sozusagen in einem Terminal innerhalb des Terminals. Eines der wichtigsten Basiskommandos für den ersten Schritt mit Metasploit ist „search“. Geben Sie keinen weiteren Parameter ein, erhalten Sie eine Liste der gültigen Kommandos. Sie setzen ein System ein, das per Samba Datenfreigaben im Netz zur Verfügung stellt? Dann sehen Sie doch einmal nach, welche Exploits Ihnen Metasploit zur Verfügung stellt. Das funktioniert gemäß der Hilfe zum Kommando so:

```
search type:exploit name:smb
```

Das System antwortet mit einer Liste potenzieller Angriffsvektoren. Um einen davon zu verwenden, wird das Kommando „use“ genutzt, dem dann der Name des Moduls folgt (Beispiel)

```
use exploit/windows/fileformat/
  vlc_smb_uri
```

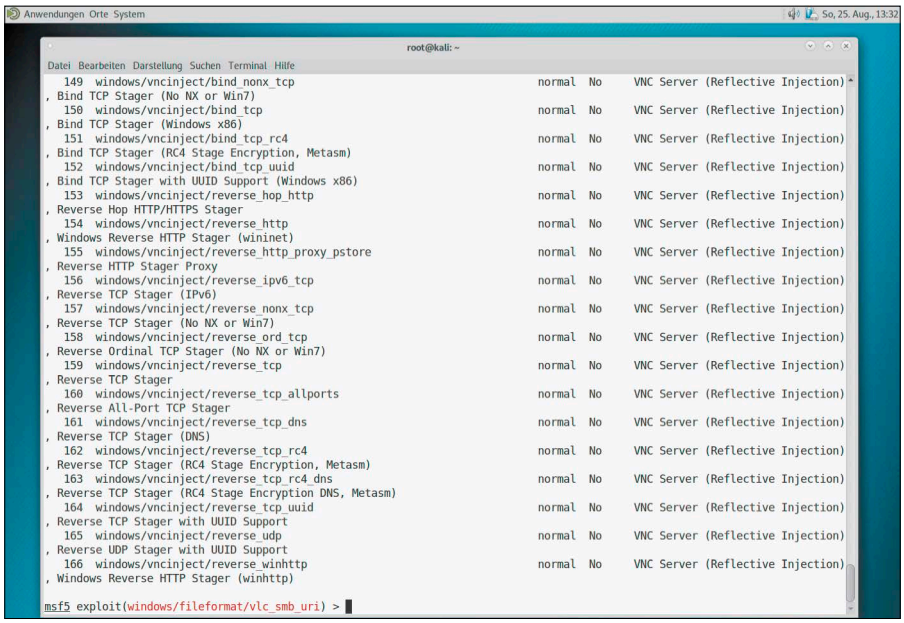
Nachdem das Modul geladen ist, wechselt die Farbe des Prompts zum Zeichen dafür, dass Sie sich jetzt in dem Modul befinden. Jedes Modul besitzt individuelle Optionen und Schalter, die Sie setzen müssen, um damit zu arbeiten. Innerhalb eines Moduls rufen Sie die Schalter mittels

```
show options
```

auf. Recht häufig werden Ihnen dabei zwei Optionen begegnen – „RHOST“ und „RPORT“. Das „R“ steht für Remote. Um das Modul einsetzen zu können, benötigen Sie die IP-Adresse des Hosts und den Port, der untersucht werden soll. Innerhalb eines Moduls setzen Sie die beiden Optionen jeweils mit dem Kommando „set“. Der Befehl

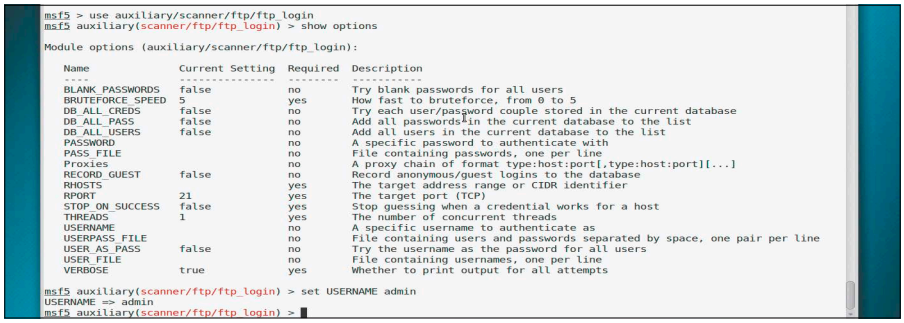
```
set RHOST 192.168.178.35
```

weist Metasploit an, den Server mit dieser IP-Adresse anzugreifen. Übrigens gelangen Sie aus der Konfiguration eines Moduls immer mit „back“ an den Prompt zurück. Die Suchfunktion ist auch dann nützlich, wenn Sie ein bekanntes System auf eine bekannte Lücke testen wollen. Mit „search“ suchen Sie beispielsweise auch nach Schwachstellen gemäß des Standards „Common Vulnerabilities and Exposures“ (CVE). Dazu müssen Sie nur das entsprechende Kürzel der Schwachstelle eintragen. Oder Sie rufen sich unter Angabe der eingesetzten Software alle Exploits passend zum System auf.
Von Bedeutung innerhalb eines Moduls sind noch die beiden Kommandos „show targets“ und „show payloads“. Unter Targets werden einzelne Programmversionen oder Komponenten einer Anwendung verstanden, die anfällig für den Exploit sind. So können Sie von vornherein überprüfen, ob die Attacke überhaupt sinnvoll ist. Denn

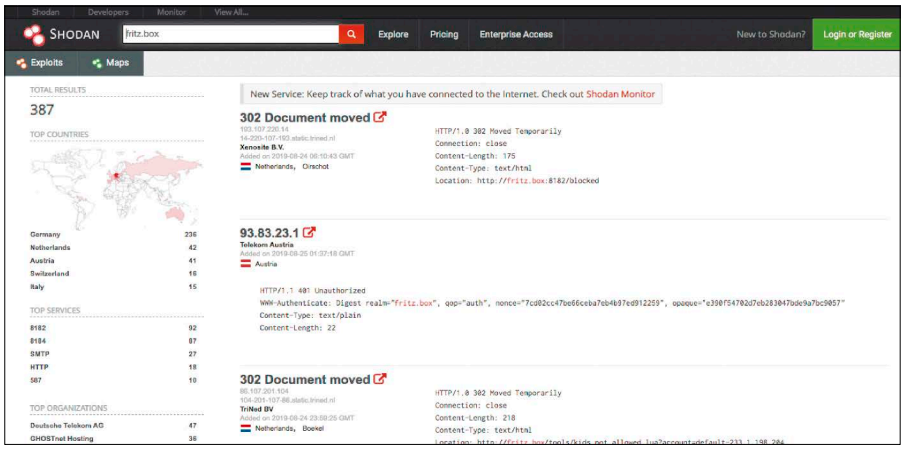


Die geänderte Farbe des Metasploit-Prompts signalisiert, dass Sie sich in einem Modul befinden. Mit Targets und Payloads sehen Sie sich Module an, die auf die Lücke angesetzt werden können.

wenn die notwendige Voraussetzung auf der Gegenseite gar nicht vorhanden ist, läuft der Angriff in Leere. Payloads sind Kommandos, die beim Angriff mitgeschickt werden, also sich beispielsweise im Zielsystem festsetzen. Haben Sie das Ziel definiert, führt „run“ dann den Angriff aus. Ist er erfolgreich, werden Sie dies direkt im Terminal sehen. Läuft er ins Leere, was bei einer Sicherheitsprüfung ja ein gutes Zeichen ist, probieren Sie einen anderen Exploit. Neben den konkreten kleinteiligen Exploits gehören zum Framework hilfreiche Zusatzprogramme. Mit diesen Scannern überprüfen Sie beispielsweise ein Log-in auf zu triviale Passwörter. So gibt es nach wie vor viele Router, die gemäß Auslieferungszustand dem Benutzer „admin“ das Passwort „admin“ zuordnen.



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



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

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

Nun zurück zur Suche nach trivialen Passwörtern. NAS-Systeme, Webserver und teilweise auch Router, die Filesharing anbieten, nutzen einen FTP-Zugang und besitzen in aller Regel ein Benutzerkonto für den Nutzer „admin“. Wie Sie gleich sehen werden, ist es immer günstig, wenn Sie einen eigenen Benutzer mit einem eigenen Namen einrichten, der über die Admin-Rechte verfügt. Denn mit Metasploit können Sie gezielt das Admin-Konto attackieren, um sich durch Brute Force Zugang zum System zu verschaffen. Dazu benötigen Sie nur eine Textdatei, in der sich die Passwörter befinden, die allesamt ausprobiert werden sollen. Über das Internet werden Sie schnell passende Wörterbücher finden können, wenn Sie nicht selbst eine solche Datei erzeugen wollen. Wie die Suche nach

```
search type:auxiliary path:scanner
```

oder der Blick in die Dateistruktur ergibt, gibt es eine Erweiterung mit dem Namen „ftp_login“, die im Verzeichnis „ftp“ liegt. Dieses Modul nutzen Sie mittels

```
use auxiliary/scanner/ftp/ftp_
  login
```

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

```
set PASS_File bsp.txt
```

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

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

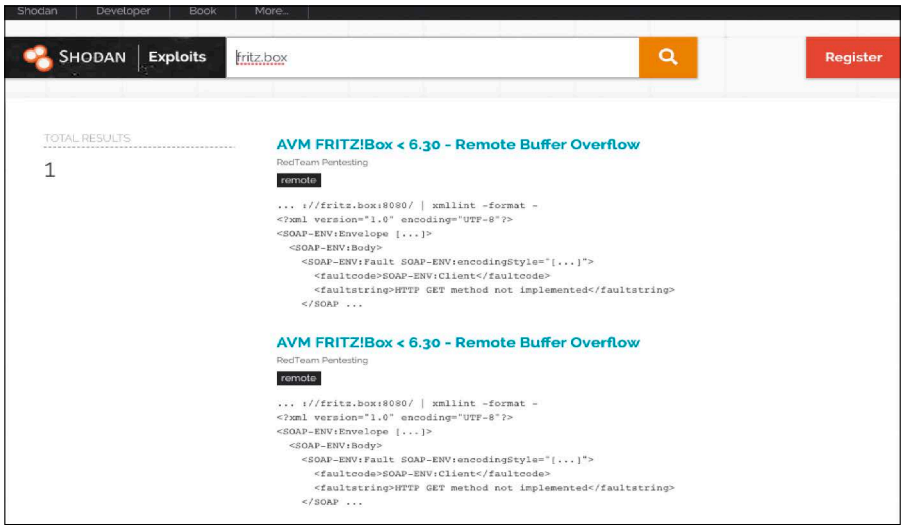
Mit Shodan verwundbare Geräte aufspüren

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

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

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

Wahrscheinlich fragen Sie sich jetzt, ob der Betrieb und die Nutzung eines solchen Systems überhaupt legal sind. Klare Antwort: ja. Es ist nicht illegal, das Internet nach öffentlich erreichbaren Systemen zu durchsuchen und das Ergebnis festzuhalten. Und es ist auch nicht illegal, sich darüber zu informieren. Verboten ist es allerdings, die Ergebnisse danach für einen Penetrationstest zu verwenden. Es sei denn, es handelt sich um Ihren eigenen Drucker oder Router. Hinter der Suchmaschine steckt auch ein Geschäftsmodell. Denn anders als bei Google sind nicht alle Funktionen kostenlos. Wer die Suchergebnisse mittels Filtern einschränken will, wird in der Regel auf die kostenpflichtige Variante hingewiesen. Wenn Sie Shodan besuchen, sehen Sie dort die klassische Eingabemaske. Geben Sie hier zum Test etwa „fritz.box“ ein.



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

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

```
Fritz.box country:DE city:Hamburg
```

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

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

Kali Linux: Der komplette Werkzeugkasten

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

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

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

Linux als Dauerläufer

In der Regel müssen Linux-Nutzer sich nur alle drei oder fünf Jahre um ein Upgrade der Distribution kümmern. Wer möchte, kann aber zwischenzeitlich trotzdem neuere Software installieren.

VON THORSTEN EGGELING

Distributionsauswahl: Den Wahl-O-Mat rufen Sie über die HTML-Oberfläche der Heft-DVD auf. Beantworten Sie die Fragen und lesen Sie die Informationen, die zu den Kriterien passen.

Die Auswahl einer geeigneten Linux-Distribution hängt vom Einsatzzweck ab. Auf einem produktiv eingesetzten Arbeitsrechner oder Server wird man ein stabiles und bewährtes System bevorzugen. Das Upgrade auf die nächste Version werden die meisten Nutzer dann vermeiden oder möglichst lange hinausschieben. Schließlich bedeutet jedes Upgrade eine längere Arbeitsunterbrechung – und möglicherweise funktioniert danach nicht mehr alles wie vorher.

Auf der anderen Seite des Spektrums stehen Nutzer, die meist technisch interessiert sind und die neuesten Versionen von Betriebssystem und Anwendungen bevorzugen. Für diesen Personenkreis gibt es Distributionen mit kürzerer Laufzeit und einer höheren Updatefrequenz. Wer es noch aktueller möchte, greift zu einem Rolling Release und hält damit das System fortlaufend auf dem aktuellen Stand (siehe Artikel ab Seite 32).

Der Fokus der nachfolgenden Artikel in diesem Special liegt jedoch auf der möglichst langen Nutzung einer Linux-Installation. Das gelingt mit geringem Aufwand, wenn man ein paar Regeln beachtet.

Linux-Distributionen für jeden Zweck

Die Standardeditionen von Ubuntu und Linux Mint bieten fünf Jahre Laufzeit und sind mit LTS gekennzeichnet (Long Term Support). Eine neue LTS-Version erscheint alle zwei Jahre (Ubuntu 16.04, 18.04, 20.04). Man kann dann ein Upgrade durchführen oder damit noch drei Jahre warten. Bei Bedarf lässt sich der Supportzeitraum für Ubuntu kostenpflichtig sogar auf bis zu zehn Jahre verlängern (*https://ubuntu.com/advantage*).

Wer ein System mit neueren Tools und Anwendungen bevorzugt, erhält es bei Ubuntu zweimal im Jahr (19.10, 20.10, 21,04), die Versorgung mit Updates erfolgt neun Monate lang. MX Linux beispielsweise basiert auf Debian, von dem es etwa alle zwei Jahre eine neue Ausgabe gibt. Das MX-Linux-Team stellt jedoch einmal im Jahr ein Upgrade mit neuer Software bereit. Manjaro ist ein Rolling Release, das fortwährend aktualisiert wird.

Die Distributionsvielfalt verstellt ein wenig den Blick dafür, dass die Basis oft identisch ist. Meist liefert Ubuntu den Unterbau, das wiederum mit Debian verwandt ist. Fedora basiert auf Red Hat Linux und Manjaro auf Arch Linux. Nur Open Suse ist eine unabhängige Entwicklung, die eng mit den kommerziellen Produkten Suse Linux Enterprise Desktop und Suse Linux Enterprise Server verbunden ist.

Bei der Entscheidung für eine bestimmte Distribution spielen mehrere Aspekte eine Rolle:

- der Nutzer ist Anfänger, erfahrener Anwender oder Profi
- die Distribution soll sich für einen Server oder Desktop eignen
- es werden eine breite Softwareauswahl oder nur gut getestete Paket gewünscht
- die Software soll entweder möglichst aktuell oder eher stabil sein

Bei der Auswahl der passenden Distribution hilft Ihnen unser Wahl-O-Mat, der sich über die HTML-Oberfläche der LinuxWelt-DVD im Browser aufrufen lässt.

Distributionen für Desktop oder Server

Es gibt zwar spezielle Serverdistributionen, jedoch ist die Basis der Server- und Desktopeditionen weitestgehend identisch. Unterschiede gibt es meist bei der Installation und der Vorauswahl der Software. Eine Desktopumgebung ist bei Servern oft entbehrlich, dafür möchte man dort aber Webserver, Datenbanken und E-Mail-Server bereits bei der Installation einrichten.

Das Installationsmedium beispielsweise von Debian 10 (*https://www.debian.org*) trägt dem Rechnung. Über das Installationstool wird zuerst ein Grundsystem eingerichtet, danach können Sie die gewünschten Pakete installieren – bei Bedarf mit Desktopumgebung oder ohne.

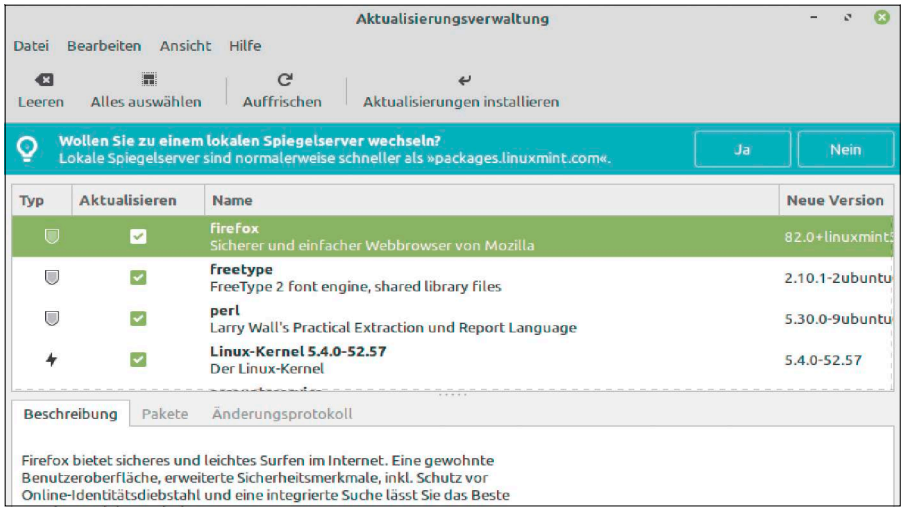
Bei Ubuntu Server (*https://ubuntu.com/download/server*) werden nur ein Grundsystem und der Open-SSH-Server einge-

richtet. Bei der Installation können Sie zusätzliche Snap-Pakete für die Serverrolle installieren und alles andere dann später im Terminal über apt.

Bei der Installation von Ubuntu Desktop und vielen anderen Desktopdistributionen werden Sie nicht nach einer Softwareauswahl gefragt. Das Installationstool richtet automatisch alle Pakete ein, die für einen Arbeitsrechner sinnvoll sind. Sie können später aber alle Pakete installieren, die auch für Ubuntu Server verfügbar sind.

Die meisten Rechenzentren, bei denen Sie root-Server oder virtuelle Server mieten können, bieten Debian 10 oder Ubuntu 20.04 LTS für die Installation an. Manchmal befindet sich auch Cent-OS 7 im Angebot, das bis Mai 2029 mit Updates versorgt wird. Etwas teurere Webhosting-Pakete für Geschäftskunden enthalten beispielsweise Lizenzen für Red Hat Enterprise Linux oder Suse Linux Enterprise Server, die zehn Jahre Support erhalten.

Server oder Desktop: Für Debian gibt es nur ein Installationsmedium. Softwarepakete lassen sich aber vorab auswählen – bei einem Server lassen Sie die Desktoppakete einfach weg.



System aktualisieren: Die regelmäßigen Updates schließen vor allem Sicherheitslücken. Für wenige wichtige Anwendungen wie Firefox gibt es aber auch neue Versionen.

Updates und Upgrades

Solange ein System vom Distributor offiziell unterstützt wird, gibt es Sicherheitsupdates und oft auch Updates für einige ausgewählte Programme. Ubuntu/Mint-Nutzer erhalten beispielsweise neue Versionen von Firefox und Thunderbird. Kernel-Upgrades gibt es ebenfalls in unregelmäßigen Abständen (siehe Artikel ab 36). Ist das Lebensende einer Distribution erreicht, liegen die Updates noch eine Zeit lang auf den Downloadservern. Es kommen aber wahrscheinlich keine neuen Updates hinzu, was ein Sicherheitsrisiko darstellen kann.

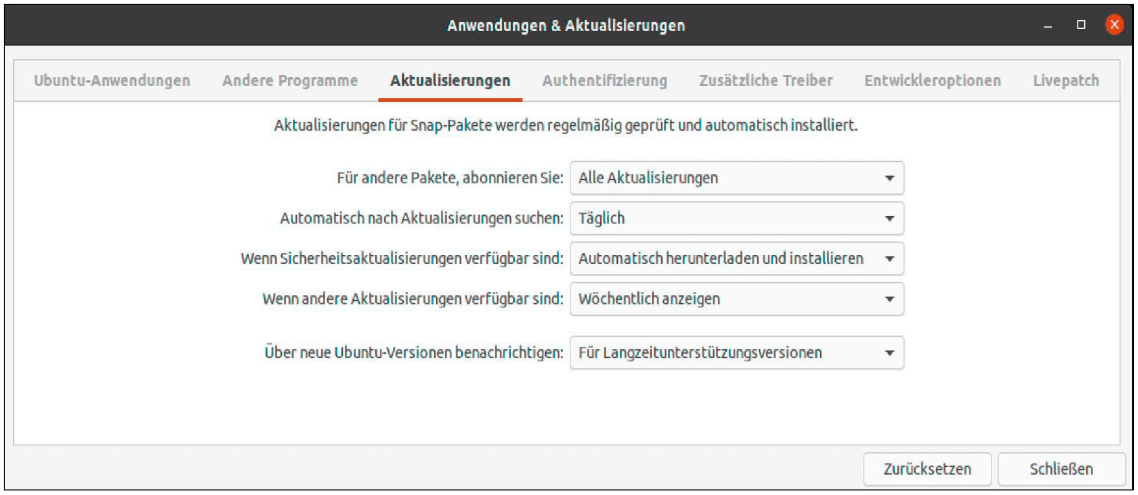
Ob man das System ohne Aktualisierungen einfach weiterbetreiben und sich das Upgrade sparen sollte, hängt vom Einsatzbereich ab. Wenn ein Linux-Server im Heimnetzwerk tatsächlich nur für den Datenaustausch etwa über Samba-Freigaben dient und aus dem Internet nicht erreichbar ist, kann das Upgrade auch ignoriert werden. Theoretisch besteht immer die Gefahr, dass ein Rechner über Sicherheitslücken im Kernel oder Fehler in der Serversoftware angegriffen wird. Die Gefahr geht dann aber eher von anderen Rechnern im Netzwerk aus, die von Schadsoftware betroffen sind. Für einige Geräte, beispielsweise ein älteres NAS, gibt es nach einiger Zeit auch keine Updates mehr. Privatanwender werden das Gerät trotzdem nicht gleich entsorgen wollen. Ganz anders sieht es bei Servern aus, die über das Internet erreichbar sind. Darauf muss immer ein aktuelles System inklusive aller verfügbaren Updates installiert sein. ■

NEUE SOFTWARE FÜR ÄLTERE SYSTEME

Software altert rasch: Fünf Jahre Laufzeit von LTS-Versionen sind für die Softwareentwicklung eine lange Zeitspanne. Allerdings benötigt nicht jeder unbedingt die neueste Version von Libre Office oder Gimp. Wenn doch, lassen sich aktuellere Programme über das Tool Ubuntu Software in einem Snap-Container installieren. Unter Linux Mint leisten die „Anwendungsverwaltung" und Flatpak-Pakete Ähnliches. Aktuellere Software für Ubuntu und Linux Mint lässt sich aber oft auch über externe PPAs installieren (Personal Package Archive). Eine Internetsuche nach der gewünschten Software zusammen mit dem Schlüsselwort „ppa" führt schnell zum passenden Angebot, das meist bei *https://launchpad.net* gehostet ist. Eine Beschreibung, wie sich das PPA einbinden und die Software installieren lässt, finden Sie auf der jeweiligen Webseite.

System und Software aktualisieren

Eine Linux-Installation kann man über einen langen Zeitraum nutzen. Regelmäßige Updates sind aus Sicherheitsgründen Pflicht und alle paar Jahre bringt man das System per Upgrade auf den neuesten Funktionsstand.



Grundeinstellungen: Ubuntu erledigt Download und Installation von Updates automatisch. Wer Kontrolle und manuelle Updates bevorzugt, kann die automatischen Updates auch abschalten.

VON THORSTEN EGGELING

Einer der größten Vorteile von Linux-Systemen ist die komfortable Updatefunktion. Die aktualisiert nämlich nicht nur das Betriebssystem, sondern auch die installierte Software. Das gilt für alle Programme, die über die Paketverwaltung beziehungsweise die konfigurierten Paketquellen eingerichtet wurden. Aktualisierungen lassen sich wahlweise automatisch beziehen oder auch manuell einleiten. Beides hat Vor- und Nachteile. Das gilt auch für Upgrades, also den Umstieg auf die nächste Version des Betriebssystems. Vor Updates und vor allem vor den umfangreichen Upgrades sollte man einige Sicherheitsmaßnahmen ergreifen, damit das System bei Fehlern nicht unbenutzbar wird. Wie immer vor größeren Änderungen, ist ein Backup anzuraten (siehe Punkt 6).

1. Automatische Updates für Ubuntu

Ubuntu 20.04 ist standardmäßig so eingerichtet, dass Sicherheitsupdates automatisch heruntergeladen und installiert werden. Vorsichtige Nutzer werden jedoch eher ein manuelles Update konfigurieren. Außerdem kann es wünschenswert sein, Updatedownloads zu reduzieren oder abzuschalten, beispielsweise wenn man viel mit dem Notebook unterwegs ist und deshalb keine schnelle Internetverbindung zur Verfügung steht.

Für die Konfiguration suchen Sie über die „Aktivitäten“ nach „Anwendungen“ und rufen „Anwendungen & Aktualisierungen“ auf. Dort gehen Sie auf die Registerkarte „Aktualisierungen“. Die erste Einstellung ist etwas seltsam mit „Für andere Pakete, abonnieren Sie:“ beschriftet. Standard ist hier „Alle Aktualisierungen“. Sie können die Updates aber auch auf „Sicherheits- und Empfehlungsaktualisierungen“ oder auf „Nur Sicherheitsaktualisierungen“ einschränken.

Ferner legen Sie hier fest, wie oft Ubuntu nach Aktualisierungen suchen soll. Stellen Sie „Niemals“ ein, wenn Sie den Download der Paketlisten und damit das automatische Update abschalten wollen. Hinter „Wenn Sicherheitsaktualisierungen verfügbar sind“ ist „Automatisch herunterladen und installieren“ eingestellt. Wählen Sie „Sofort anzeigen“, wenn Ubuntu mit dem Fenster „Aktualisierungsverwaltung“ über Updates nur informieren soll. Sie können Sie dann jederzeit auf „Jetzt installieren“ klicken oder das Update mit „Später erinnern“ vorerst verschieben.

Hinter „Über neue Ubuntu-Versionen benachrichtigen“ ist bei Ubuntu 20.04 LTS standardmäßig „Für Langzeitunterstützungsversionen“ eingestellt. Die nächste LTS-Version ist planmäßig im April 2022

verfügbar (22.04 LTS), die Benachrichtigung erfolgt meist drei Monate nach diesem Termin. Sie können dann ein Upgrade durchführen oder damit bis zum April 2025 warten. Wenn Sie keine Benachrichtigung über die Nachfolgeversion wünschen, stellen Sie „Niemals“ ein.

2. Update-Konfiguration bei Linux Mint 20

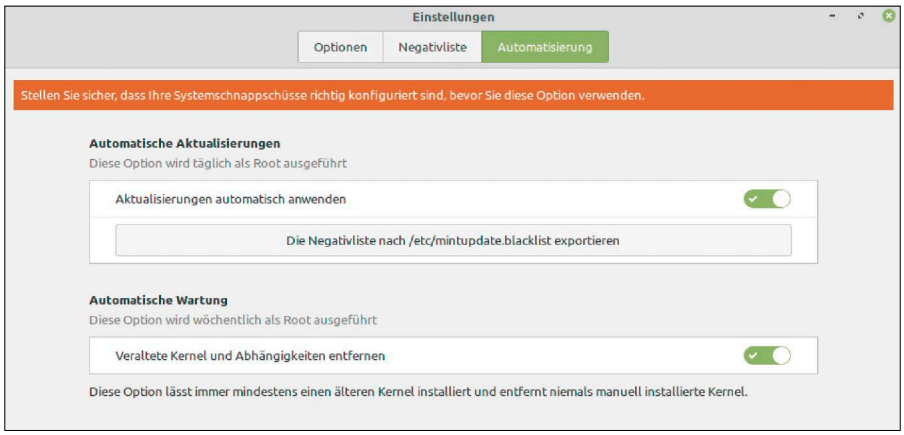
Bei Linux Mint 20 Cinnamon ist die Updateverwaltung vorsichtiger konfiguriert. Automatische Aktualisierungen sind standardmäßig deaktiviert. Sie werden über ein Icon rechts unten in der Leiste am unteren Bildschirmrand informiert, sobald Updates verfügbar sind. Klicken Sie das Icon an. Es öffnet sich das Fenster „Aktualisierungsverwaltung“, in dem Sie nur auf „Aktualisierungen installieren“ klicken.

Die Konfiguration der Aktualisierungsverwaltung lässt sich über den Menüpunkt „Bearbeiten → Einstellungen“ ändern. Wechseln Sie auf die Registerkarte „Automatisierung“. Linux Mint empfiehlt in einem farblich hervorgehobenen Hinweis, dass Sie Systemschnappschüsse konfigurieren sollen, bevor Sie das automatische Update aktivieren. Mehr dazu lesen Sie in Punkt 6. Wenn das erledigt ist, aktivieren Sie – wenn gewünscht – „Aktualisierungen automatisch anwenden“. Außerdem können Sie „Veraltete Kernel und Abhängigkeiten entfernen“ einschalten. Linux Mint löscht dann alle älteren Kernel bis auf den direkten Vorgänger des aktuellen. Sollten Problem mit einem neuen Kernel auftreten, lässt sich über das Grub-Bootmenü der funktionstüchtige Vorgänger wählen und der problematische Kernel danach deinstallieren.

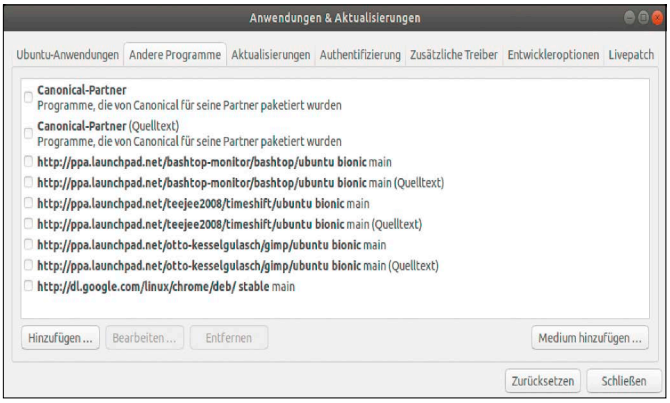
Auf der Registerkarte „Optionen“ legen Sie fest, wie oft Linux Mint die Paketliste auffrischen soll. Der Standard steht bei zehn Minuten nach dem Systemstart und danach alle zwei Stunden. Der Download der Paketliste lässt sich auch deaktivieren, wodurch dann auch keine automatischen Updates mehr erfolgen.

3. Pakete von Drittanbietern entfernen

Wer nur die Standard-Paketquellen verwendet, kann diesen Abschnitt überspringen. Sollte aber Software aus anderen Quellen installiert sein, sollten Sie vor einem großen Systemupgrade auf die nächsthöhere Version der Distribution zusätzliche Maßnahmen ergreifen. Probleme können nämlich auftreten, wenn ein PPA oder eine andere externe Paketquelle nicht nur eine bestimmte Software, sondern dabei auch Updates für Systembibliotheken installiert. Es ist nicht sichergestellt, dass das Systemupgrade die gleiche oder eine höhere Version nebst zugehörigen Abhängigkeiten installieren kann. Wird die passende Bibliothek nicht gefunden, bricht das Systemupgrade ab.



Linux Mint: Die automatische Aktualisierung ist standardmäßig deaktiviert. Bevor Sie die Funktion nutzen, sollten Sie Systemschnappschüsse mit Timeshift konfigurieren.



Zusätzliche Paketquellen: Ubuntu deaktiviert Fremdquellen vor dem Upgrade. Danach können Sie die Häkchen wieder setzen und bei Bedarf den Namen der Distribution anpassen.

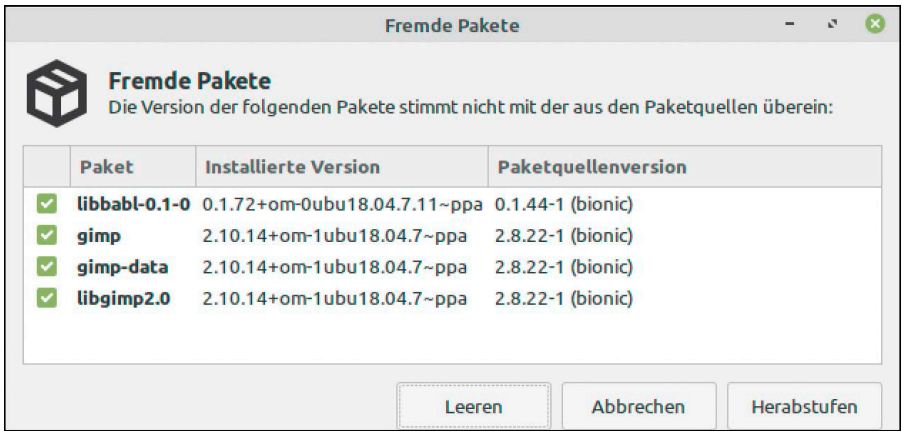
UPDATES EINZELNER PAKETE VERBIETEN

Manchmal sind bestimmte Paketupdates unerwünscht, etwa dann, wenn man selbst eine eigene Version mit anderen Optionen eingerichtet hat oder weil eine neue Version Probleme bereitet. Unter Linux Mint lassen sich Updateausnahmen in den Einstellungen der „Aktualisierungsverwaltung“ auf der Registerkarte „Negativliste“ konfigurieren. Über die „+“-Schaltfläche legen Sie Pakete und Versionen fest, die nicht aktualisiert werden sollen. Alternativ können Sie im Fenster „Aktualisierungsverwaltung“ über das Kontextmenü eines Pakets das Update genau dieser Paketversion oder auch aller zukünftigen Versionen unterbinden. Damit die Negativliste auch beim automatischen Update berücksichtigt wird, wechseln Sie auf die Registerkarte „Automatisierung“ und klicken auf „Die Negativliste nach /etc/mintupdate.blacklist exportieren“.

Ubuntu-Nutzer verwenden im Terminal diesen Befehl:

```
sudo apt-mark hold [Paketname]
```

Dies verhindert, dass „[Paketname]“ aktualisiert, automatisch installiert oder entfernt wird. Verwenden Sie „unhold“ statt „hold“, um eine Sperre wieder aufzuheben.



Vor dem Upgrade: Linux Mint bietet an, aktuellere Versionen aus fremden Quellen durch die älteren Versionen aus den Standard-Paketquellen zu ersetzen.

Ubuntu deaktiviert beim Upgrade automatisch alle zusätzlich eingebundenen PPAs und andere fremde Repositorien. Wenn Sie auf Software aus diesen Quellen angewiesen sind, prüfen Sie vor dem Upgrade, ob die Pakete auch für die neue Ubuntu-Version verfügbar sind. Nach dem Upgrade lassen sich die Quellen über „Anwendungen & Aktualisierungen“ auf der Registerkarte „Andere Programme“ wieder aktivieren. Bei einigen müssen Sie wahrscheinlich den Namen der Distribution anpassen. Ändern Sie beispielsweise „bionic“ auf „focal“, wenn Sie von Ubuntu 18.04 zu 20.04 wechseln.

Bei Ubuntu bleiben die Fremdpakete jedoch erhalten, auch wenn die Quellen deaktiviert sind. Die Entwickler verlassen sich darauf, dass das schon irgendwie gut gehen wird. In vielen Fällen wird das so sein, in einigen aber nicht. Wer auf der sicheren Seite sein will, folgt dem Vorbild Linux Mint. Installieren Sie dazu ein zusätzliches Tool:

```
sudo apt install ppp-purge
```

Mit der Befehlszeile

```
sudo ppa-purge [ppa-Name]
```

lässt sich eine externe Paketquelle deaktivieren und das Programm wird auf die Version aus den Standard-Paketquellen zurückgesetzt. Ist es dort nicht verfügbar, wird es deinstalliert. Ersetzen Sie den Platzhalter „[ppa-Name]“ durch die tatsächliche Bezeichnung des PPAs, die typischerweise mit „ppa:“ beginnt.

Linux Mint: Für ein Upgrade müssen bei Linux Mint Drittanbieterquellen zwingend deaktiviert sein und Software aus diesen Quellen muss entfernt werden. Das Risiko eines Fehlschlags beim Upgrade wird dadurch minimiert. Wenn Software aus zusätzlichen Quellen installiert ist, gehen Sie im Menü auf „Systemverwaltung → Anwendungspaketquellen“ und dann auf „PPAs“. Entfernen Sie alle Häkchen in der Spalte „Aktiviert“. Klicken Sie auf „OK“, um den apt-Zwischenspeicher zu aktualisieren. Unter „Zusätzliche Paketquellen“ gehen Sie entsprechend vor. Gehen Sie auf „Wartung“ und klicken Sie auf „Fremde Pakete herabstufen“. Wählen Sie alle Pakete aus und klicken Sie auf „Herabstufen“. Danach klicken Sie auf „Fremde Pakete entfernen“, wählen alles aus und klicken auf „Entfernen“.

4. Das Systemupgrade bei Ubuntu

Direkt vor einem Upgrade sollte man Sicherheitshalber ein Backup des gesamten Systems erstellen oder wenigstens das der persönlichen Dateien (siehe Punkt 6).

Installieren Sie außerdem alle verfügbaren Updates (siehe dazu auch den Beitrag ab Seite 36).

Sobald Ubuntu eine neue Systemversion meldet, genügt ein Klick auf „System jetzt aktualisieren“. Es kann immer nur auf die nächsthöhere Version aktualisiert werden, beispielsweise von Ubuntu 18.04 auf 20.04 (LTS-Versionen). Folgen Sie einfach den Anweisungen des Assistenten. Der Kernel und alle Softwarepakete werden dann auf den neuesten Stand gebracht. Wenn keine Upgradeinfo erscheint oder wenn Sie das Upgrade frühzeitig manuell durchführen wollen, verwenden Sie diese Befehlszeile im Terminal:

```
sudo update-manager -c
```

Das Upgrade lässt sich dann folgendermaßen auch ohne grafische Oberfläche im Terminal durchführen:

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

In der Regel gelingt das Upgrade problemlos. Es gibt jedoch einige Hürden, mit denen Sie rechnen müssen. Für die neue Linux-Version stehen unter Umständen nicht alle Softwarepakete zur Verfügung, die Sie bisher installiert hatten. Der Upgradeassistent informiert Sie über die nicht mehr unterstützten Pakete. Meist handelt es sich nur um einige veraltete Systembibliotheken, die ohnehin kein aktuelles Programm mehr verwendet. Sie sollten aber die Liste prüfen und im Internet nach Alternativen suchen, wenn Sie die genannte Software tatsächlich benötigen.

5. Das Systemupgrade bei Linux Mint

Installieren Sie alle verfügbaren Updates und erstellen Sie ein Backup (siehe Punkt 6). Damit sich Linux Mint auf die neueste Version (aktuell 20) aktualisieren lässt, muss das letzte Point-Release 19.3 installiert sein (siehe Artikel ab Seite 36).

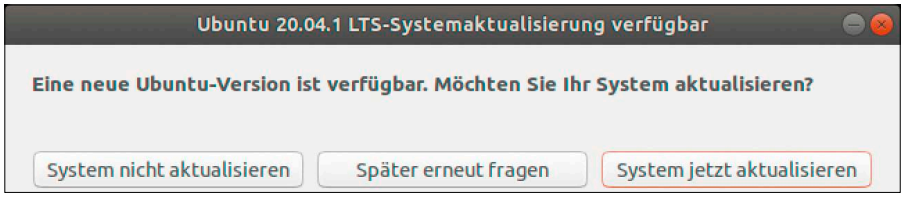
Upgradebereitschaft prüfen: Öffnen Sie ein Terminal und führen Sie die folgenden drei Befehle aus:

```
sudo apt update
sudo apt upgrade
sudo apt install mintupgrade
```

Das Tool mintupgrade erledigt ein Upgrade zur nächsthöheren Version – etwa von Linux Mint 19.3 auf 20. Starten Sie das Tool immer ohne vorangestelltes „sudo“. Höhere Rechte werden bei Bedarf angefordert:

```
mintupgrade check
```

Bestätigen Sie die Prüfung mit Y-Taste und Eingabetaste. Sollte bisher keine Sicherung mit Timeshift („Systemschnappschüsse“)



Upgrade einleiten: Kurze Zeit nach Erscheinen einer neuen Version wird deren Installation angeboten. Sie können das Angebot sofort annehmen oder das Upgrade verschieben.

konfiguriert sein (Punkt 6), erhalten Sie eine Fehlermeldung und der Vorgang bricht ab. Wurde eine Sicherung mit einem anderen Tool durchgeführt, können Sie dem System mit

```
echo "{}" | sudo tee /etc/timeshift.json
```

eine Timeshift-Sicherung vorgaukeln. Löschen Sie die Datei „timeshift.json“ später wieder, falls Sie Timeshift später verwenden möchten.

Mit der Option „check“ weisen Sie mintupdate an, die Paketquellen temporär für das neue System zu ändern und die Installation zu simulieren. Ansonsten wird nichts am System geändert. Unter „Die folgenden Pakete werden ENTFERNT“ gibt das Tool aus, welche Pakete von Linux Mint 20 nicht mehr unterstützt werden. In der Regel handelt es sich um veraltete Systembibliotheken, die ohnehin nicht mehr verwendet wird. Wenn etwas Auffälliges dabei ist oder benötigte Software, suchen Sie im Internet, ob die Software vom neuen System unterstützt wird. Die abschließende Meldung „Command ‚check‘ completed successfully“ signalisiert, dass Sie mit dem Upgrade fortfahren können. Andernfalls folgen Sie der Anweisung in der Fehlermeldung.

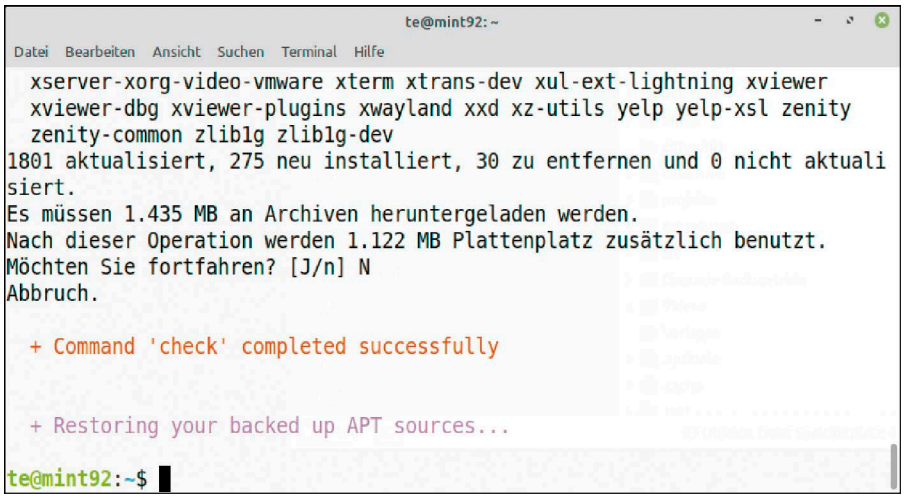
Upgrade durchführen: Im nächsten Schritt laden Sie mit

```
mintupgrade download
```

die Upgradedateien herunter, am installierten System ändert sich aber dadurch noch nichts. Erst das Kommando

```
mintupgrade upgrade
```

führt die Installation durch, was dann nicht mehr umkehrbar ist.



Upgradecheck unter Mint: Mit dem Tool mintupgrade prüfen Sie, ob das System für die Aktualisierung bereit ist. Wenn keine Fehler angezeigt werden, führen Sie das Upgrade durch.

6. Backups vor Updates oder Upgrades

Bei einem Arbeitsrechner genügt oft die Sicherung der persönlichen Dateien. Das Betriebssystem lässt sich nach einem Totalausfall oder einem Festplattendefekt oft schneller durch Neuinstallation als durch Rücksichern von Komplettbackups wiederherstellen. Sollten auf dem Rechner jedoch Serverdienste laufen oder sehr viel Software installiert sein, empfiehlt sich eine komplette Sicherung des Systems (siehe auch Artikel ab Seite 68) und zusätzlich ein Backup der Home-Verzeichnisse.

Ubuntu: Sie können das Programm „Datensicherungen“ verwenden, das für die automatische Sicherung des eigenen Home-Verzeichnisses konfiguriert ist. Unter „Zu ignorierende Ordner“ lassen sich Ordner einstellen, die nicht im Backup landen sollen. Über „Speicherort“ geben Sie den Zielordner an. Dieser kann auf einem Netzwerklaufwerk, einer lokalen Festplatte oder einem Cloudserver liegen.

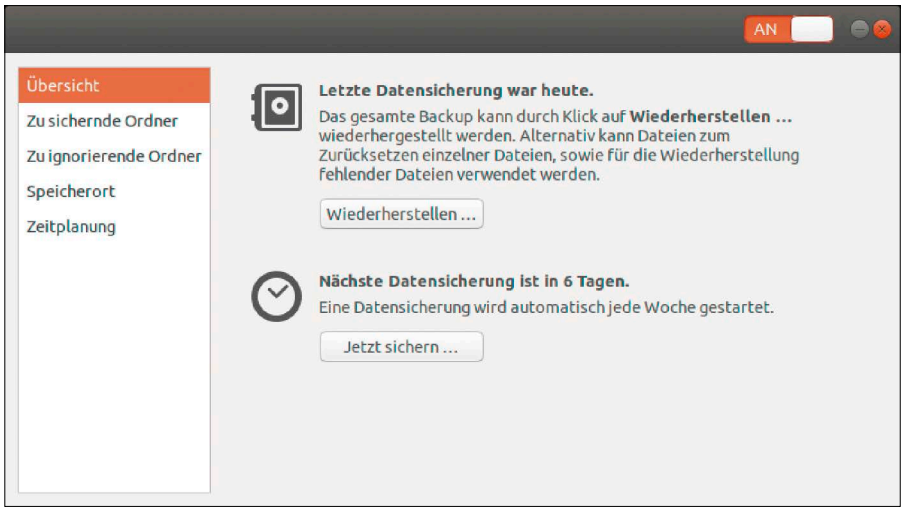
Für Komplettbackups empfiehlt sich ein Tool wie Timeshift. Ubuntu-Nutzer installieren es im Terminal mit diesen Befehlen:

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

Nach dem Start führt Sie ein Assistent durch die Konfiguration. Belassen Sie die Option „rsync“ und klicken Sie auf „Weiter“. Im nächsten Schritt geben Sie das Ziellaufwerk an. Am besten eignet sich eine zweite oder externe Festplatte, die mit einem Linux-Dateisystem formatiert sein muss, etwa Ext4. Netzwerklaufwerke werden nicht unterstützt. Im letzten Schritt definieren Sie einen Zeitplan und die Menge der Systempunkte.

Wiederherstellen: Die Backups bestehen aus unkomprimierten Ordnern und Dateien unter „/timeshift/snapshots“. Einzelne Dateiobjekte oder der komplette frühere Zustand lassen sich daher mit jedem Livesystem rekonstruieren, falls das primäre System nicht mehr funktioniert.

Linux Mint: Wer nur die persönlichen Daten sichern will, geht im Menü auf „Systemverwaltung → Datensicherungswerkzeug“ und klickt auf „Jetzt sichern“. Folgen Sie den Anweisungen des Assistenten. Timeshift zur Systemsicherung ist bei Linux Mint standardmäßig installiert. ■

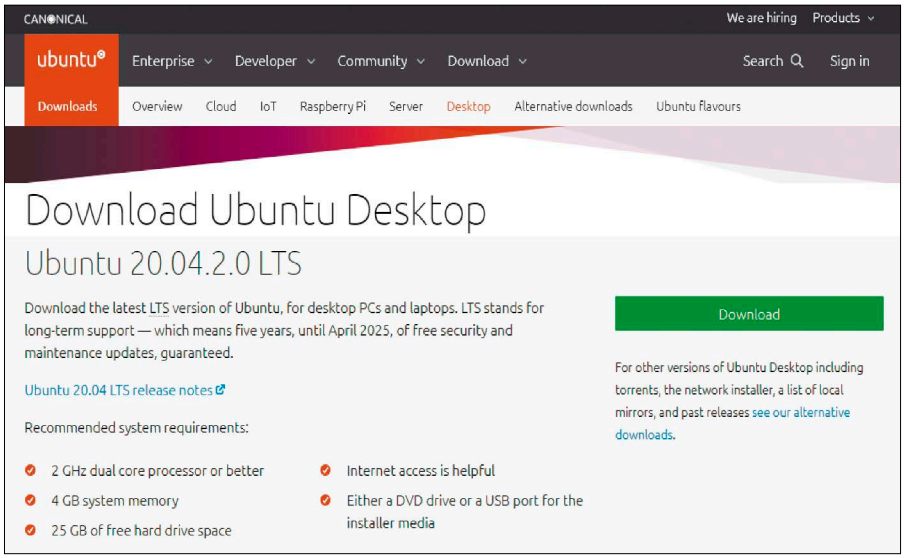


Persönliche Dateien sichern: Das Tool „Datensicherungen“ ermöglicht unter Ubuntu ein automatisches Backup der Dateien aus dem Home-Verzeichnis nach Zeitplan.

Point Releases und neue Kernel

Mit einem möglichst aktuellen Installationsmedium vermeiden Sie bei einer Neuinstallation umfangreiche Updates. Zumindest der Linux-Kernel lässt sich aber auch bei einem installierten System außerhalb der Reihe aktualisieren.

VON THORSTEN EGGELING



Neueste Version: Wer die Desktopausgabe von Ubuntu herunterlädt, erhält Version 20.04.2. Die ist ähnlich aktuell wie die erste Version vom April 2021 (Ubuntu 21.04), enthält aber noch keinen neuen Kernel.

Die langlebigen LTS-Versionen von Ubuntu und Linux Mint versprechen einen sorglosen Betrieb über mehrere Jahre. Wer allerdings eine LTS-Distribution ein oder zwei Jahre nach dem ursprünglichen Erscheinungsdatum neu installiert, muss zahlreiche Updates herunterladen, bevor er das System sicher nutzen kann. Um das zu vermeiden, stellen die Distributoren in unregelmäßigen Abständen aktualisierte Installationsmedien bereit. Die Bezeichnung enthält eine zusätzliche Nummer nach der Hauptversion. Aus Ubuntu 20.04 wird dann beispielsweise Ubuntu 20.04.1, auch erstes „Point Release“ genannt. Um nicht mehrere Versionen pflegen zu müssen, wird auch bei bestehenden Installation die Versionsnummer durch die standardmäßigen Updates angehoben. Es gibt allerdings bei einigen Komponenten Unterschiede zwischen Neuinstallation und Update.

1. Point Releases und neue Kernel für Ubuntu

Mit jedem neuen Linux-Kernel wird die Hardwareunterstützung ausgebaut oder verbessert. Bei einer funktionierenden Linux-Installation auf unveränderter Hardware gibt es keinen ernsthaften Grund, auf einen neuen Kernel umzusteigen. Anders sieht es aus, wenn neue Hardware dazukommt, die vom bisherigen Kernel nicht oder nur unzureichend unterstützt wird. Manchmal ist auch für neue Software ein neuerer Kernel Voraussetzung, wenn diese ein bestimmtes Kernel-Modul erfordert oder erstellen will.

Damit Nutzer nicht auf die nächste Hauptversion der Distribution warten müssen, installiert ein Point Release von Ubuntu-Desktop automatisch einen neueren Kernel als in der ursprünglichen Version. Teilweise gibt es zusätzlich aktuellere Versionen des X-Servers und einiger Grafikbibliotheken, wenn das im Zusammenspiel mit dem neuen Kernel nötig ist. Die Entwickler bezeichnen das als LTS Enablement Stack-Support oder HWE (Hardware Enablement).

Etwas anders sieht es bei Ubuntu-Server aus. Hier kann man beim Start der Installation von Ubuntu 18.04.5 im Bootmenü „Install Ubuntu Server with the HWE Kernel“ wählen (zur Zeit Kernel-Version 5.4). Andernfalls wird wie bei Ubuntu-Desktop der GA-Kernel 4.15 (General Availability) eingerichtet.

Wer auf seinem Rechner im April 2018 Ubuntu 18.04 LTS installiert hat, ist inzwischen durch Updates bei Version 18.04.05 LTS angelangt. Der Kernel trägt jedoch nach wie vor die Versionsnummer 4.15.0-122. Das Anhängsel „-122“ deutet auf einige Sicherheitsupdates hin, die ursprüngliche Revision war „-20“. Welche Kernel-Version das System verwendet, finden Sie im Terminal mit

```
uname -a
```

heraus. Mit

```
lsb_release -a
```

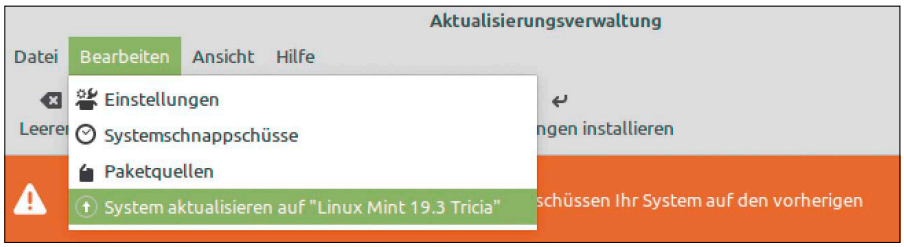
ermitteln Sie die genaue Version des Betriebssystems.

2. Point Releases und Kernel für Linux Mint

Auch die Entwickler von Linux Mint geben Point Releases heraus. Linux Mint 19 beispielsweise basiert auf Ubuntu 18.04. danach folgten Linux Mint 19.1, 19.2 und 19.3.

Datum der Veröffentlichung und Versionsnummer stimmen nicht mit Ubuntu überein. Anders als bei Ubuntu ändern die regulären Updates nichts an der Versionsnummer. Der Kernel wird über *sudo apt upgrade* ebenfalls nicht automatisch aktualisiert. War ursprünglich beispielsweise Linux Mint 19.2 installiert, bliebt es dabei. Das wird auch dadurch deutlich, dass die Point Releases eigene Codenamen tragen: Tara, Tessa, Tina, Tricia. Aus Sicht der Mint-Entwickler scheinen auch Zwischenversionen den Status einer neuen Ausgabe der Distribution zu besitzen.

Wer auf ein Point Release updaten möchte, muss das manuell einleiten. Dazu geht man über das Menü auf „Systemverwaltung → Aktualisierungsverwaltung“ und dann auf „Bearbeiten“. Im Menü erscheint beispielsweise „System aktualisieren auf ‚Linux Mint 19.3 Tricia‘“. Diese Aktualisierung ist auch Voraussetzung für das Upgrade auf Linux Mint 20.



Point Release für Linux Mint: Die Installation neuer Versionen erfolgt nicht automatisch, lässt sich aber über die „Aktualisierungsverwaltung“ manuell anstoßen.

3. Kernel bei Ubuntu aktualisieren

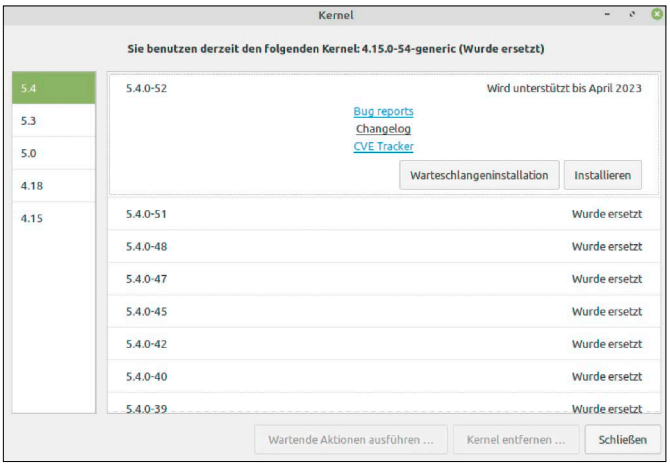
Wird eine Hardware vom installierten Kernel nicht unterstützt, kann man eine neuere Kernel-Version ausprobieren. Die Installation ist in der Regel unproblematisch, weil das System bei Fehlfunktionen jederzeit wieder mit dem älteren Kernel booten kann. Zur Installation des HWE-Kernels starten Sie bei Ubuntu 18.04 im Terminal

```
sudo apt-get install --install-
 recommends linux-generic-
 hwe-18.04 xserver-xorg-hwe-16.04
```

Der Kernel des letzten Point Release entspricht dem der nächsten LTS-Version. Die Kernel von Ubuntu 18.04.05 und 20.04 sind daher zur Zeit identisch (5.4.0-52). Sobald weitere Point Releases für Ubuntu 20.04 erscheinen, können Sie auch bei dieser Version den Kernel aktualisieren. Ersetzen Sie dafür in der Befehlszeile „18.04“ jeweils durch „20.04“.

Ubuntu bietet eine weitere Option, um auf einen noch aktuelleren Kernel zu wechseln. Das Paket „linux-generic-hwe-20.04-edge“ bietet eine Vorschau auf den kommenden HWE-Kernel. Zurzeit wird Version 5.8.0.25 ausgeliefert. Bei sehr neuem Kernel ist zu beachten, dass zusätzliche Treiber beispielsweise von Nvidia oder Virtualbox die Version unterstützen müssen. Ansonsten schlägt das Kompilieren fehl und die Hardware lässt sich nicht nutzen. Bei Problemen ruft man das Grub-Bootmenü auf. Sollte es nicht automatisch erscheinen, halten Sie die Umschalt-Taste nach dem Einschalten des PCs gedrückt. Im Menü gehen Sie auf „Erweiterte Optionen für Ubuntu“ und wählen einen älteren Kernel. Danach deinstallieren Sie die neuere Version.

Kernel für Linux Mint: Neue Kernel bietet das System in einem eigenen Fenster zur Installation an, weist aber darauf hin, dass Probleme mit zusätzlichen Treibern auftreten können.



4. Neue Kernel für Linux Mint

Linux Mint bietet etwas mehr Klarheit im Kernel-Wirrwarr. Aktuelle Kernel-Updates zeigt die „Aktualisierungsverwaltung“ an. Wer neuere Kernel benötigt, geht auf „Ansicht → Linux-Kernel“. Man erhält zuerst eine Warnung, dass ein neuer Kernel zu Problemen führen kann.

Eine Anleitung, wie sich das Problem über das Grub-Bootmenü beheben lässt (siehe Punkt 3), ist ebenfalls enthalten. Nach einem Klick auf „Fortsetzen“ erscheint ein Fenster, über das sich der gewünschte Kernel auswählen lässt.

Bei jedem Eintrag gibt es Links zu „Bug reports“ und „Changelog“, die über Fehler und Neuerungen informieren. ■

EXPERIMENTELLE KERNEL INSTALLIEREN

Traditionell kompiliert man experimentelle Kernel selbst, was aber sehr zeitaufwendig ist. Einfacher geht es über Downloads von *https://kernel.ubuntu.com/~kernel-ppa/mainline*. Bei Redaktionsschluss waren hier Kernel bis Version 5.10 als DEB-Pakete zu finden. Für ein 64-Bit-System laden Sie unter „amd64“ alle Pakete herunter, die „generic“ enthalten, und die Datei mit der Endung „all.deb“. Im Terminal erfolgt die Installation im Downloadverzeichnis per

```
sudo dpkg -i *.deb
```

Bitte beachten Sie, dass bei sehr neuem Kernel die Wahrscheinlichkeit geringer ist, dass sich damit zusätzliche Treiber kompilieren lassen.

Für mehr Komfort kann man über *https://github.com/teejee2008/ukuu/releases* das DEB-Paket für das Tool Ukuu herunterladen und installieren. Es ermöglicht die einfache Installation und Deinstallation der Kernel von *https://kernel.ubuntu.com* in Ubuntu und Linux Mint.

Mint 20: System-probleme lösen

Linux Mint 20 hatte nach seinem Erscheinen mit einigen Bugs und Eigenheiten zu kämpfen. Einige davon lassen sich durch ein Update auf Linux Mint 20.2 beheben. Bei anderen müssen Sie anderweitig tätig werden. Hier ein Überblick über bekannte Mint-Schwächen.

VON HERMANN APFELBÖCK

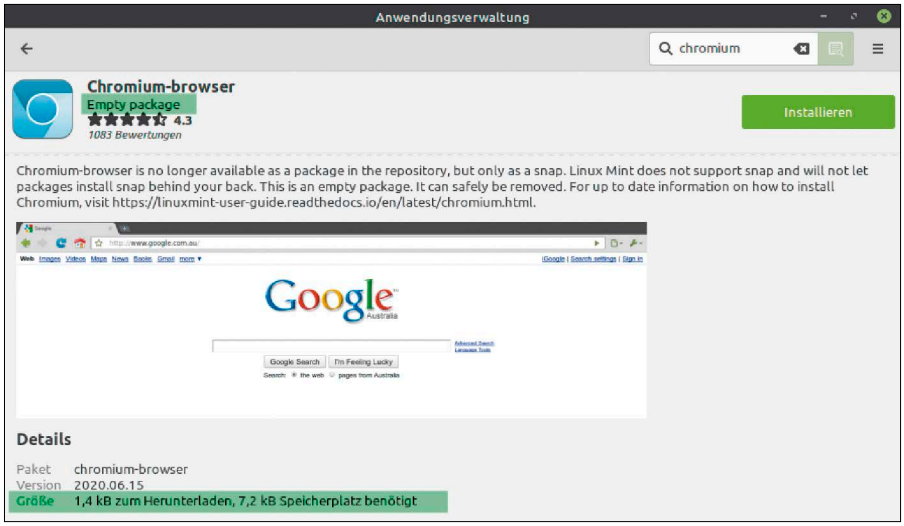
Die hier beschriebenen Bugs und Pannen sind zum größeren Teil speziell und selten gravierend. Nicht überall gibt es eine echte Lösung, aber überall Auswege oder Alternativen. Für typische Desktopprobleme hält die Cinnamon-Hauptedition außerdem eine Reihe interner Problemhelfer parat. Außerdem finden Sie im Kasten „Das Upgrade“ eine Anleitung, wie Sie älteres Mint 19.3 auf aktuelles 20 bzw. 20.2 hieven.

Chromium: Der verbotene Browser

Wer als Browser den freien Chromium bevorzugt, hat es unter Linux Mint 20 schwer: Die Ubuntu-Repositories, die Linux Mint mitbenutzt, bieten diesen Browser nicht mehr als klassisches DEB-Paket an, sondern nur noch als Snap-Paket. Snap wiederum verbietet Linux Mint 20, das sich auf das Containerformat Flatpak fokussiert hat. Um auf die Situation hinzuweisen, gibt es in Mint 20 sogar ein leeres Dummy-Paket von Chromium in der „Anwendungsverwaltung“. Es gibt drei Möglichkeiten, auf diese Situation zu antworten:

A. Aktualisieren Sie Linux Mint auf Version 20.1 oder 20.2. Denn in Version 20.1 hat das Mint-Team Chromium wieder in die „Anwendungsverwaltung“ integriert. Das nötige DEB-Paket wird nun von den Mint-Machern selbst und nicht mehr von Ubuntu gepfelt.

B. Das Snap-Verbot lässt sich umgehen, wie schon Mal in der LinuxWelt beschrieben: Es genügt, die verantwortliche Verbotsdatei zu löschen oder zu verschieben:



Browser-Dummy: Für Benutzer, die Chromium suchen, stellt Mint ein funktionsloses Paket bereit. Die Seite erklärt, warum es den Browser unter Mint nicht gibt und wo er notfalls zu beziehen ist.

```
sudo rm /etc/apt/preferences.d/
  nosnap.pref
```

Danach ist mit

```
sudo apt install snapd
```

die Installation der Snap-Umgebung wieder möglich und somit der Zugriff auf den Ubuntu-Snapstore und auf Chromium als Snap:

```
sudo snap install chromium
  chromium-ffmpeg
```

C. Am einfachsten ist es, auf Chromium sowie Canonical-Snaps zu verzichten und den weitgehend identischen Google-Browser Chrome zu installieren.

Den gibt es auf *www.google.com/chrome* als direkten Download, was dann allerdings den Eintrag einer Fremdquelle in die Paketquellen bedeutet. Dies ist notwendig, damit Chrome seine laufenden Updates beziehen kann.

Probleme beim Upgrade 19.3 auf 20

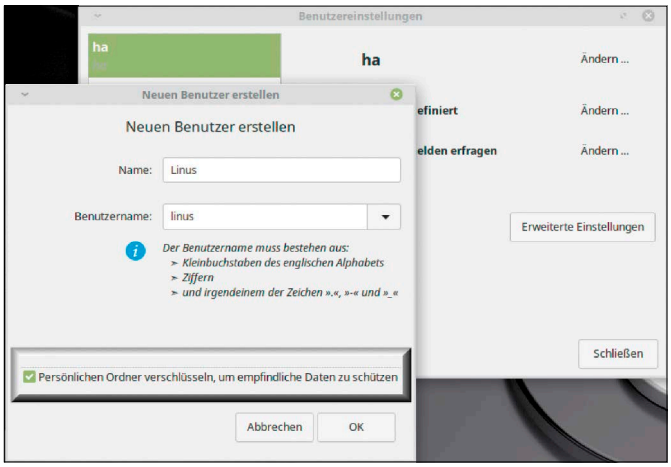
Das Upgrade der Version 19.3 auf aktuelles Mint 20 oder 20.2 funktioniert in den allermeisten Fällen schmerzfrei. Pannen sind dennoch nicht auszuschließen, wobei diese typischen Probleme dominieren:

1. Die Oberfläche friert ein, ist nicht mehr benutzbar und CPU, Lüfter, Festplatte laufen auf Höchstlast. In diesem Fall ist ein Gang zur virtuellen Konsole (Strg-Alt-F2) zu empfehlen und dort die Kontrolle des laufenden Upgrades mit *ps -elf* oder einem Tool wie top oder htop. Dort muss der aktive Prozess „mintupgrade“ angezeigt sein. Ist dies der Fall, genügt im Prinzip eine Portion Geduld: Das Upgrade läuft im Hintergrund weiter und sollte nach weiteren 20 bis 30 Minuten erfolgreich abgeschlossen sein. Wer CPU, Lüfter und Festplatte

entlasten will, kann in der Konsole die hängende Oberfläche gewaltsam beenden (etwa *killall cinnamon*).

2. Nach dem Upgrade erscheinen beim Bootvorgang kritisch klingende Hardwaremeldungen über „ACPI Errors“. Dies geht auf die Ubuntu-Basis zurück und kann laut Mint-Team als „kosmetisches“ Ärgernis ignoriert werden. Das Phänomen gilt nicht nur für das Upgrade, sondern auch für normale Installationen.

3. Auf (mit Cryptsetup) verschlüsselten Systemen wird nach dem Upgrade der erste Bootvorgang durch eine Fehlermeldung gebremst („Waiting for encrypted device / swapfile“). Schlimmstenfalls kommt der Bootvorgang über die initiale Ramdisk nicht hinaus, sondern bleibt mit einem Eingabeprompt stehen. Geben Sie *exit* ein, um den Start fortzusetzen. Das Problem sollte nach dem ersten Bootvorgang nicht mehr auftreten.



Neues Konto mit Home-Verschlüsselung: Was Mate und hier im Bild XFCE anbieten, lässt Cinnamon vermissen. Dort muss ein Terminalbefehl aushelfen.

4. Ernste Paketkonflikte können Fremdquellen wie PPAs verursachen. Einen Großteil dieser Probleme umgeht das Mint-Team inzwischen mit einer nachgeschobenen, sensibleren Version des Tools mintupgrade, das die Paketquellen unter „/etc/apt/sources.list.d/“ genauer analysiert und gegebenenfalls vorab warnt. Generell scheint die Empfehlung nicht paranoid, vor dem Upgrade alle Fremdquellen unter den „Anwendungspaketquellen“ zu entfernen – am besten auch die zugehörige Software.

DAS UPGRADE VON VERSION 19.3

Wer den Mint-Vorgänger 19.3 laufen hat, kann auf Version 20 upgraden. Beachten Sie aber, dass Mint 20 nur noch in 64 Bit vorliegt. Im Zweifel fragen Sie die Systemarchitektur mit

```
getconf LONG_BIT
```

ab. Die Antwort muss „64“ lauten. Wer ein 32-Bit-Mint laufen hat, muss bei der älteren Mint-Version 19.3 bleiben, das immerhin noch zweieinhalb Jahre bis April 2023 Updates erhält. Als Upgradewerkzeug hat das Mint-Team das Tool Mintupgrade bereitgestellt. Die Skepsis des Mint-Teams gegenüber dem Upgradeprozess hat sich aber nicht geändert, was sich in einer sehr vorsichtigen Upgradeanleitung niederschlägt.

1. Als Vorbereitung bringen Sie Version 19.3 auf den neuesten Stand, indem Sie in der Aktualisierungsverwaltung auf „Auffrischen“ und „Aktualisierungen installieren“ gehen. Nach dem „Auffrischen“ erscheint voraussichtlich der Hinweis, dass „eine neue Version der Aktualisierungsverwaltung“ verfügbar sei, die Sie nachrüsten und danach die restlichen angebotenen Updates installieren.

2. Ohne Timeshift-Sicherung wird sich das Upgrade später verweigern. Wenn Timeshift bereits benutzt wird, genügen der Aufruf des Tools und ein Klick auf „Erstellen“. Andernfalls muss Timeshift gestartet und konfiguriert werden, wonach der geforderte Schnappschuss erfolgen kann (Schaltfläche „Erstellen“).

3. Das Mint-Team empfiehlt, sämtliche Fremdquellen vom System zu entfernen. Das bedeutet konkret, im Tool „Anwendungspaketquellen“ unter „PPAs“ und „Zusätzliche Paketquellen“ alles zu löschen. Beachten Sie, dass Sie diese Quellen nach erfolgreichem Upgrade wieder nachtragen können.

4. Die eigentliche Aktion erfolgt im Terminal. Zunächst muss das Tool mit

```
sudo apt install mintupdate
```

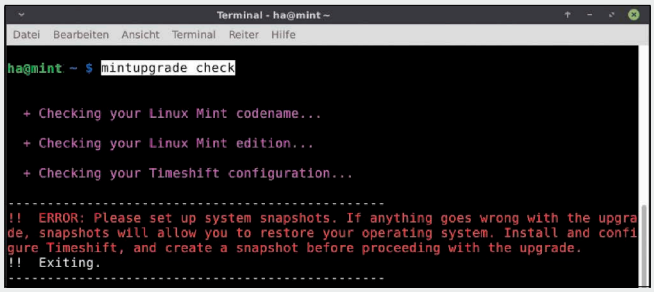
installiert werden. Ein erster Testlauf mit *mintupgrade check* kann eventuelle Probleme vorab anzeigen. Der nächste Befehl

```
mintupgrade download
```

bezieht die neuen Dateien aus dem Internet. Die Installation startet dann dieser Befehl:

```
mintupgrade upgrade
```

5. Der Vorgang muss interaktiv begleitet werden, da einige inhaltliche Abfragen erfolgen. So kann die Frage, ob laufende Dienste später neu gestartet werden sollen, der Einfachheit halber generell mit „Ja“ beantwortet werden. Ferner erscheint eventuell für einige Konfigurationsdateien (etwa „sshd_config“ oder „smb.conf“) die Abfrage, ob die alte Datei ersetzt werden darf. In aller Regel wird es sinnvoll sein, die „aktuell lokal installierte Version“ beizubehalten. Das ist vor allem dort unbedingt ratsam, wo Sie selbst eine Konfigurationsdatei aktiv und manuell bearbeitet haben.



Mintupgrade verlangt Timeshift: Eine Systemsicherung ist dringend zu empfehlen. Wer das partout nicht möchte, kann mit *sudo touch /etc/timeshift.json* ein konfiguriertes Timeshift vortäuschen.

Home-Verschlüsselung für Cinnamon

Die Installationsoption, das Home-Verzeichnis des Erstbenutzers zu verschlüsseln, hat die Mint-Version 20 weiter an Bord. Werden später in der grafischen Benutzerverwaltung zusätzliche Konten eingerichtet, haben Mate und XFCE diese Option ebenfalls im Angebot („Persönlichen Ordner verschlüsseln"). Ausgerechnet die Hauptedition mit Cinnamon lässt diese Einstellung an der grafischen Oberfläche vermissen. Hier hilft nur der Gang ins Terminal:

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

Anschließend legen Sie das Kontopasswort fest und bestätigen alle Abfragen mit Eingabetaste.

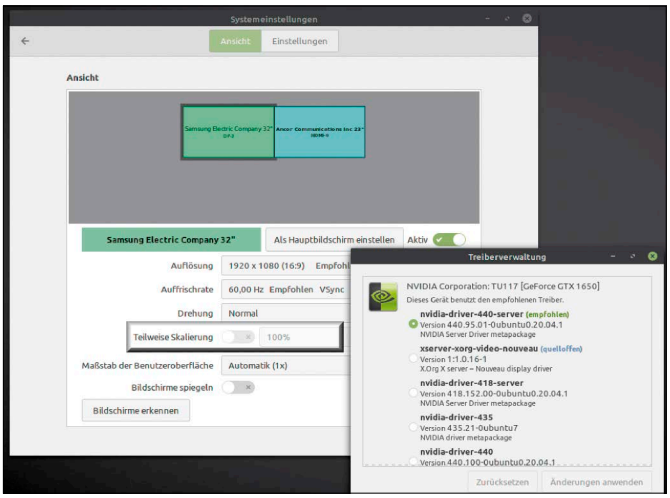
Home-Verschlüsselung: Abmeldung genügt nicht

Die praktische Home-Verschlüsselung (mit Ecrypt FS) leidet unter Linux Mint 20 weiterhin an einem Bug, den Sicherheitsbewusste kennen sollten: Eine Abmeldung vom System führt **nicht** dazu, dass die Daten unter „/home/[user]" entladen und unter „/home/.ecryptfs/[user]/.Private" nur noch unlesbar verschlüsselt vorliegen. Vielmehr hat ein anderes Systemkonto mit sudo-Recht vollen Zugriff auf alle Daten.

Das Verhalten entspricht nicht der Erwartung, dass die Kontenanmeldung die verschlüsselten Daten aufsperrt und eine Abmeldung diese wieder absichert. Es muss ein Neustart erfolgen, um die Daten vor Fremdzugriff zu schützen. Der Bug ist aber insofern nicht gravierend, da er nur auf einem Mehrbenutzersystem zutrifft, etwa einem Familienrechner mit mindestens zwei sudo-berechtigten Konten. Dort sollte das System komplett beendet werden, um den Datenschutz zu gewährleisten. Beachten Sie, dass die entscheidende Aufgabe der Ecrypt-FS-Verschlüsselung, nämlich die Daten eines mobilen Notebooks vor Fremdzugriff zu schützen (durch Livesystem oder nach Ausbau der Festplatte), uneingeschränkt erfüllt ist.

Nvidia-Treiber und Cinnamon-Skalierung

Die fraktionale Bildschirmskalierung, die in der Cinnamon-Edition Einzug gefunden hat, funktioniert nicht mit Nvidia-Grafiktreibern. Dieses Problem erbt Linux Mint 20 von Ubuntu 20.04. Bei installiertem Herstellertreiber bleibt der Punkt „Systemeinstellungen → Bildschirm → Teilweise Skalierung" schlicht inaktiv. Eine Lösung kann künftig nur von Ubuntu oder Nvidia kommen. Vorläufig muss sich der Nutzer entscheiden, was ihm wichtiger ist – die höhere Leistung des proprietären Treibers oder die erweiterten Skalierungsmöglichkeiten.



Skalierungsoption in Cinnamon und Nvidia-Treiber: Die neue fraktionale Skalierung bleibt inaktiv, wenn Nvidia-Herstellertreiber installiert sind.

Unsere Empfehlung: Der optimale Grafiktreiber sollte den Vorzug erhalten, zumal es unter Cinnamon mit „Systemeinstellungen → Schriftauswahl → Skalierungsfaktor der Schrift" noch eine weitere Option gibt, die Bildschirmdarstellung zu optimieren.

Secure Boot im Uefi-Bios

Die Mint-Community (*https://forums.linuxmint.com*, *www.linuxmintusers.de*) meldet eine Reihe von skurrilen und zum Teil schwer reproduzierbaren Hardwareproblemen mit Wi-Fi-Adaptern, Grafikchips und Notebookakkus. Obwohl ein kausaler Zusammenhang nicht offensichtlich ist, scheint die Uefi-Sicherheitseinstellung „Secure Boot" bei einigen dieser Probleme eine Rolle zu spielen. Obwohl Linux Mint eine „Secure Boot"-Signatur besitzt, empfehlen viele Betroffene das Abschalten dieser Uefi-Funktion. „Secure Boot", das den Systemstart von Rootkit-Schadsoftware verhindern soll, befindet sich im Uefi-Setup meist unter „Bios Features", „Security" oder ähnlich und lässt sich mit „Disabled" abschalten. Diesen Hinweis geben wir auf Basis unserer Recherche in den Mint-Foren ohne Gewähr weiter.

Kein Samba-Browsing

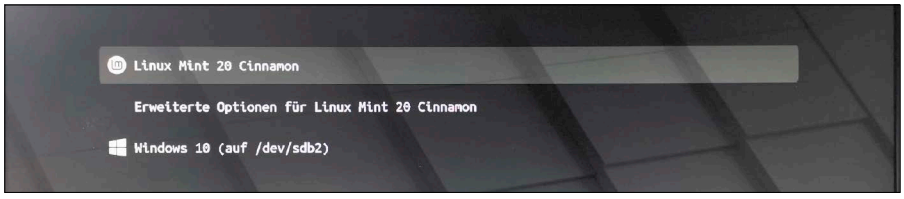
Schon seit Ubuntu 18.04 gibt es eine neue Samba-Version, welche die automatische Suche nach Samba-Freigaben verhindert. Die Mint-Dateimanager melden beim Klick auf das „Windows-Netzwerk" neuerdings gar nichts mehr, auch keinen Fehler. In der Adressleiste erscheint mit

```
smb:///
```

ein nicht ganz verkehrtes Basisangebot, jedoch mit einem Slash zu viel. Mit „smb://[Rechnername]" oder „smb://192.168.178.10" (Beispiel) kommen Sie aber jederzeit zur gewünschten Freigabe. Für häufig benötigte Freigaben empfiehlt es sich, die somit gemountete Netzwerkressource im Dateimanager dauerhaft als Lesezeichen abzulegen (Strg-D). Dann genügt künftig ein Klick auf dieses Lesezeichen.

Grub-Bootmenü größer und besser lesbar

Auf großen Bildschirmen fällt das Grub-Bootmenü sehr klein aus. Benutzbar ist es



Grub-Bootmenü aufhübschen: Die Darstellung der Bootoptionen wird durch ein vergrößertes Grub-Thema attraktiver und besser lesbar.

zwar durchaus noch, verliert sich aber etwas traurig am Bildschirm oben links. Für deutlich mehr Präsenz sorgt ein alternatives, größeres Grub-Thema, das sich mit

```
sudo apt install grub2-theme-mint-2k
```

leicht nachrüsten lässt.

Frische SSH-Clients für Windows

Wer auf Linux Mint 20 den Open-SSH-Server aktiviert hat und unter Windows die typischen SSH-Clients Putty, Kitty oder Filezilla für den Zugriff nutzt, scheitert eventuell bei der Anmeldung. Die Fehlermeldung über eine „key exchange group" ist nicht zielführend, das heißt: Ein Ändern des Algorithmus unter „Connection → SSH → Kex" bleibt erfolglos. Einfache Lösung ist es, das offenbar veraltete Putty/Kitty/Filezilla durch die aktuelle Version zu ersetzen (*www.putty.org/*, *www.9bis.net/*, *https://filezilla-project.org/*). Technischer Hintergrund ist eine geänderte Version von Open SSL, die Linux Mint von Ubuntu 20.04 erbt. Veraltetes Putty/Kitty/Filezilla ist damit nicht mehr kompatibel. Betroffen sind nur Anwender, die diese Clients über längere Zeit nicht aktualisiert haben.

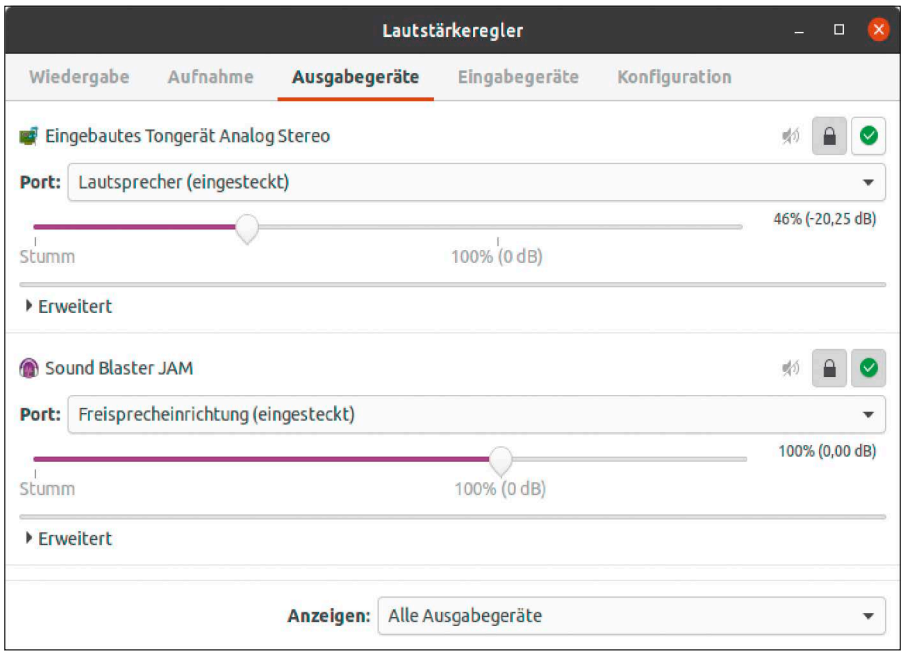
Pavucontrol: Soundausgänge aktivieren

Wie in nahezu allen Desktopdistributionen kümmert sich in Linux Mint „Pulse Audio" um die Klangausgabe. Das betrifft auch die Weiterleitung von Streams an Ausgabegeräte aller Art wie HDMI oder Bluetooth. Meist bleiben diese externen Audiogeräte nach der Verbindung aber erst einmal stumm. Die Auswahl des externen oder internen Audiogeräts, das zur Soundausgabe dienen soll, erfolgt üblicherweise über das Programm Pavucontrol, das zum Umfang von Pulse Audio gehört und die wichtigste Schaltzentrale für die Soundausgabe ist.

In Linux Mint 20 ist Pavucontrol nicht vorinstalliert und sollte mit

```
sudo apt install pavucontrol
```

nachgerüstet werden. Die Registerkarten „Wiedergabe" und „Aufnahme" zeigen jeweils aktive Anwendungen an, die mit Pulse Audio verbunden sind. „Ausgabegeräte" und „Eingabegeräte" listen die verfügbaren Geräte mit dem jeweiligen Ausgabeport und Reglern auf. Die wichtigste Einstellung verbirgt sich unter „Konfiguration". Dort aktivieren oder deaktivieren die auswählbaren Profile wichtige Ausgänge wie HDMI.



Das Tool Pavucontrol sollte man nachinstallieren, denn erst damit ist bei mehreren Ausgabeports und Geräten eine korrekte Konfiguration der Soundausgabe möglich.

Cinnamon-Reparaturen

Der Cinnamon-Desktop kann mit einfachen Handgriffen neu initialisiert werden, ohne die laufenden Anwendungen zu beenden. Aus technischer Sicht sind die folgenden Aktionen identisch:

A: Der Hotkey Strg-Alt-Esc lädt die Oberfläche komplett neu.

B. Der Rechtsklick auf der Systemleiste und die Option „Fehler suchen → Cinnamon neustarten" restauriert Cinnamon in gleicher Weise.

C. Schließlich löst nach Tastenkombination Alt-F2 (Minifenster für Befehle) die Eingabe „r" den Restart von Cinnamon aus.

Wenn diese sanftere Methode nichts bewirkt, hilft meistens der Hotkey Strg-Alt-Rücktaste, der allerdings die komplette Sitzung beendet und zum Anmeldebildschirm zurückführt. Zusätzliche Troubleshooting-Optionen bietet das Tool cinnamon-looking-glass. Es lässt sich durch Rechtsklick auf die Systemleiste und „Fehler suchen → Looking Glass" starten oder auch manuell über *cinnamon-looking-glass*. Hier gibt es unter der Schaltfläche „Actions" (ganz rechts) die zusätzliche Möglichkeit, die Cinnamon-Konfiguration auf den Standard zurückzusetzen („Reset Cinnamon Settings").

Ein kompletter Reset aller Cinnamon-Einstellungen, soweit sie in der Dconf-Konfigurationszentrale gespeichert sind, funktioniert aber auch in der virtuellen Konsole (Strg-Alt-F1), wenn die Oberfläche nicht mehr arbeitet:

```
dconf reset -f /org/cinnamon/
```

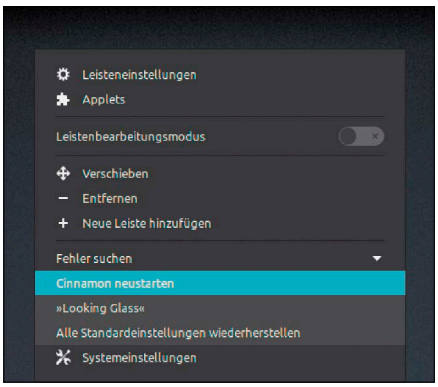
Wer vorgesorgt hat, kann Cinnamon aber auch weniger radikal auf einen funktionierenden Zustand zurücksetzen. Eine Sicherung aller Cinnamon-Einstellungen ist jederzeit mit dem folgendem Terminalbefehl möglich:

```
dconf dump /org/cinnamon/ > cinnamon_dconf.txt
```

Aus dieser Sicherungsdatei importieren Sie später mit

```
dconf load /org/cinnamon/ < cinnamon_dconf.txt
```

wieder alle Einstellungen. ■

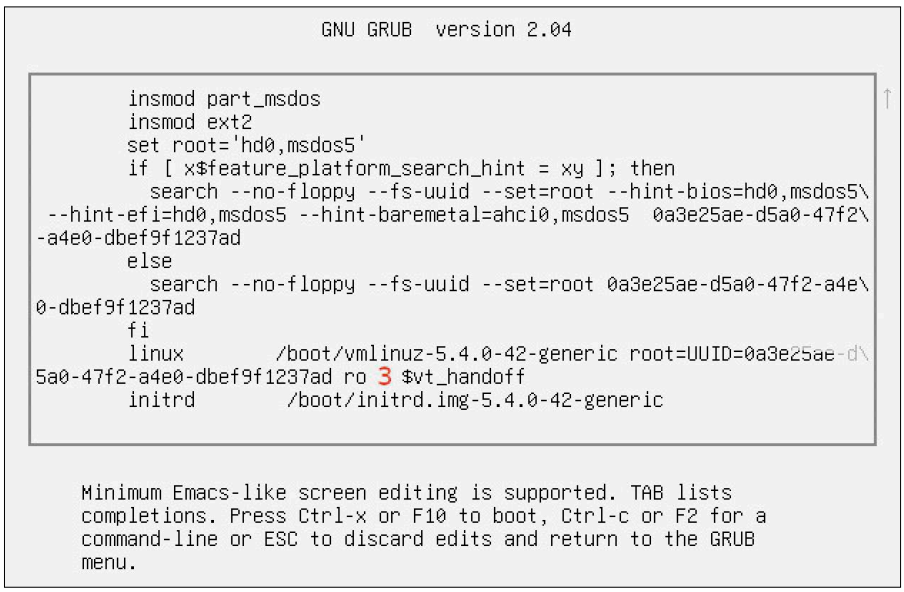


Eingebaute Problemlöser: Bei Desktophängern helfen spezielle Hotkeys sowie diese Optionen, die Sie über die Systemleiste erreichen.

Probleme mit Desktop und X-Server

Wenn der Desktop streikt, ist dafür in der Regel nur ein Fehler in der Konfiguration verantwortlich. In selteneren Fällen kann es an der Hardware oder einem unzulänglichen Treiber liegen.

VON THORSTEN EGGELING



Ohne Desktop starten: Für die Analyse startet man das System über Grub nur mit einer Textkonsole. Danach aktivieren Sie die Desktopdienste und untersuchen die Fehlermeldungen.

Unter Linux ist der Desktop zusätzliche Software, die vom System nachgeladen wird. Die Desktopumgebung läuft zwar nicht unabhängig von der Systembasis, stellt aber einen mehr oder weniger eigenständigen Aufsatz dar. Der besteht aus mehreren Komponenten. Der Anzeigeserver (Display-Server: meist Xorg, selten Wayland) ist die Basis der grafischen Oberfläche. Er wird vom Anzeigemanager (Display-Manager: meist Lightdm oder GDM) gestartet, der die Benutzeranmeldung ermöglicht. Ein Fenstermanager (Window-Manager: Compiz, Xfwm, Openbox) sorgt anschließend dafür, dass Anwendungen in einem Fenster erscheinen. Über die Fensterdekoration, die Darstellung der Bedienelemente sowie Menüs und Leisten entscheidet zuletzt die grafische Shell (Gnome, KDE, XFCE und andere).

Jeder der genannten Bestandteile kann aufgrund einer Fehlkonfiguration versagen, was sich aber unterschiedlich äußert. Am Anfang steht daher eine Untersuchung der Problemursache.

1. Desktopprobleme analysieren

Einen wichtigen Anhaltspunkt liefert die Phase, in der der Fehler auftritt. Wenn gar keine grafische Oberfläche erscheint beziehungsweise der Bildschirm nach dem Linux-Start schwarz bleibt, handelt es sich wahrscheinlich um ein Hardware- oder Treiberproblem (siehe Punkt 2). Gelangt man dagegen bis zum Anmeldebildschirm und der Desktop bleibt nach der Anmeldung leer, ist der Fehler bei der Software oder in der Konfiguration zu suchen (siehe Punkt 3).

Für die genauere Untersuchung bietet es sich an, Linux ohne grafische Oberfläche zu starten. Halten Sie kurz nach dem Einschalten des PCs die Umschalt-Taste gedrückt, damit das Grub-Menü erscheint. Drücken Sie die E-Taste, um den Standardmenüeintrag zu bearbeiten. Gehen Sie in die Zeile, die mit „linux“ beginnt. Tippen Sie hinter „ro“ ein Leerzeichen und eine „3“ ein. Entfernen Sie „quite splash“. Mit F10 booten Sie den Menüeintrag. Auf dem Bildschirm erscheinen die Meldungen des Kernels und Informationen zu den gestarteten Diensten, die eventuell sachdienliche Fehlermeldungen enthalten. Anschließen melden Sie sich auf der Konsole an. Mit dem Befehl

```
startx
```

starten Sie den X-Server und die grafische Oberfläche (ohne Anzeigemanager). Sollte das fehlschlagen, sehen Sie Meldungen, die das Problem näher beschreiben. Damit haben Sie einen Anhaltspunkt dafür, wonach Sie im Internet zur Problemlösung suchen können.

Sollte „startx“ zur grafischen Oberfläche führen, sind Treiber und X-Server offenbar in Ordnung. In diesem Fall melden Sie sich ab und gelangen so wieder zur Textkonsole. Mit der Befehlszeile

```
sudo service gdm3 start
```

starten Sie unter Ubuntu 20.04 den Anzeigemanager, der auch den X-Server startet. Sollte das nicht funktionieren, erhalten Sie eine Fehlermeldung oder Sie rufen per

```
sudo systemctl status gdm3
```

die Logmeldungen des Dienstes ab, die weiterführende Meldungen enthalten kann. Bei Linux Mint 20 funktioniert das entsprechend. Hier kommt jedoch ein anderer Anzeigemanager zum Einsatz, weshalb Sie „gdm3“ durch „lightdm“ ersetzen.

2. Den optimalen Grafiktreiber nutzen

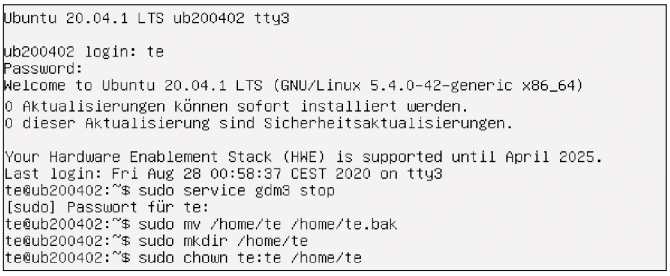
Ubuntu 20.04 und Linux Mint 20 verwenden bei der Installation einen Standardtreiber für Nvidia-Grafikchips („nouveau"). Der funktioniert in der Regel, bei einigen Chips startet das Livesystem jedoch nicht bis zum Desktop oder friert ein. Das Problem lässt sich umgehen, indem man beim Start vom Installationsmedium nach der Sprachauswahl „Ubuntu ohne Installation ausprobieren (abgesicherter Grafikmodus)" wählt (bei Linux Mint: „Start in compatibility mode"). Im Uefi-Modus wählen Sie den Eintrag mit dem Inhalt „safe graphics", bei Linux Mint „compatibility mode". Ubuntu-Nutzer setzen bei der Installation ein Häkchen vor „Installieren Sie Software von Drittanbietern für Grafik- und Wifi-Hardware und zusätzliche Medienformate". Die Installation sollte dann reibungslos ablaufen.

Ubuntu richtet den proprietären Nvidia-Treiber automatisch ein und der Desktop erscheint wie erwartet.

Unter Linux Mint müssen Sie zuerst das Grub-Bootmenü aufrufen, hinter „ro" die Option „nomodeset" eintragen und mit F10 starten (siehe Punkt 1). Nach dem Systemstart gehen Sie im Menü auf „Systemverwaltung → Treiberverwaltung". Wählen Sie den Treiber mit dem Zusatz „empfohlen", klicken Sie auf „Änderungen anwenden" und zum Abschluss auf „Neustarten".

Ubuntu-Nutzer sollten den verbesserten Treiber ebenfalls installieren, wenn noch nicht geschehen. Der Weg führt über „Aktivitäten", die Suche nach „Treiber" und Klick auf „Zusätzliche Treiber". Die Installation erfolgt dann wie bei Linux Mint.

Verbesserte Treiber: Für Nvidia-Grafikchips bieten Ubuntu und Linux Mint optimierte Treiber an. Einige Geräte zeigen nur mit einem dieser Treiber die grafische Oberfläche.



Test in einer Standardumgebung: Wenn Linux ein leeres Home-Verzeichnis vorfindet, werden alle Einstellungen neu erstellt. Das hilft bei der Analyse von Konfigurationsfehlern.

3. Fehler in der Konfiguration

Wenn der Desktop nach der Anmeldung nicht erscheint oder nicht reagiert, setzen Sie die Konfiguration zurück. Das gelingt am einfachsten, indem Sie Ihr Home-Verzeichnis umbenennen und mit einer frischen Konfiguration starten. Dazu wechseln Sie mit Strg-Alt-F3 auf eine Textkonsole („virtuelle Konsole") und melden sich an. Die Zeile

```
sudo service gdm3 stop
```

beendet unter Ubuntu 20.04 die laufenden Dienste für die grafische Oberfläche. Benutzer von Linux Mint ersetzen „gdm3" durch „lightdm". Danach verwenden Sie die folgenden drei Befehlszeilen:

```
sudo mv /home/[User] /home/[User].bak
sudo mkdir /home/[User]
sudo chown [User]:[User] /home/[User]
```

Den Platzhalter „[User]" ersetzen Sie jeweils durch Ihren Benutzernamen. Anschließend starten Sie den Desktop mit

```
sudo service gdm3 start
```

(Linux Mint: „lightdm" statt „gdm3"). Drücken Sie erneut Strg-Alt-F3, wenn die Konsole nicht mehr sichtbar ist. Melden Sie sich dann an und testen Sie das System. Wenn keine Probleme mehr auftauchen, liegt der Fehler offensichtlich an den Konfigurationsdateien. Damit beginnt der mühsame Teil der Problemanalyse. Sie können einzelne Ordner oder Unterordner nach und nach aus der Sicherungskopie in das neue Home-Verzeichnis kopieren. Die Konfigurationsverzeichnisse beginnen mit einem Punkt und werden erst sichtbar, wenn Sie im Dateimanager im Hamburger-Menü (drei horizontale Linien) ein Häkchen vor „Verborgene Dateien anzeigen" setzen. Sinnvoll ist das Wiederherstellen vor allem bei großen Verzeichnissen wie „.mozilla" und „.thunderbird", in denen Firefox beziehungsweise Thunderbird die Konfiguration ablegen.

Bei vielen anderen Programmen ist eine Neukonfiguration oft schneller. ■

ENERGIESPAREN DURCH TREIBERWECHSEL

Viele Notebooks verfügen über zwei Grafikchips. Die Intel-CPU-Grafik bietet weniger Leistung, dafür hält der Akku länger. Der Nvidia-Grafikchip verbessert die Darstellung von Spielen oder grafikintensiven Anwendungen, nimmt aber auch mehr Strom auf. Wenn der proprietäre Nvidia-Treiber installiert ist (siehe Punkt 3), kann man zwischen dem Nvidia- und Intel-Grafik umschalten. Linux Mint zeigt dafür ein Applet, über dessen Menü Sie den gewünschten Modus wählen. Ubuntu-Nutzer suchen über „Aktivitäten" nach „Nvidia" und starten „Nvidia X Server Setting". Gehen Sie auf „PRIME Profiles" und wählen Sie die gewünschte GPU. Nach der Änderung melden Sie sich bei Linux ab und wieder an.

Turbos für Programme

Wenn Programme zäh laufen, muss nicht die Hardware schuld sein. Am häufigsten liegt es an überladenen Benutzerkonfigurationen, die einen Reset des Profils nahelegen. Je nach Software gibt es noch weitere Tuningoptionen.

VON HERMANN APFELBÖCK

Die Gründe für träges Tempo von Anwendungen sind vielfältig. Der Browser wird Webinhalte nicht schnell laden, sofern es die Netzbrandbreite nicht hergibt. Die Filmwiedergabe wird stocken, wenn CPU und Grafikchip unterdimensioniert sind. Allgemeine Hardwareprobleme, die sich auf Software auswirken, sind aber hier nicht das Thema. Im Fokus stehen einige Beschleunigungsoptionen und Rücksetzaktionen für besonders prominente Programme.

Allgemeine Beschleunigung durch Preload

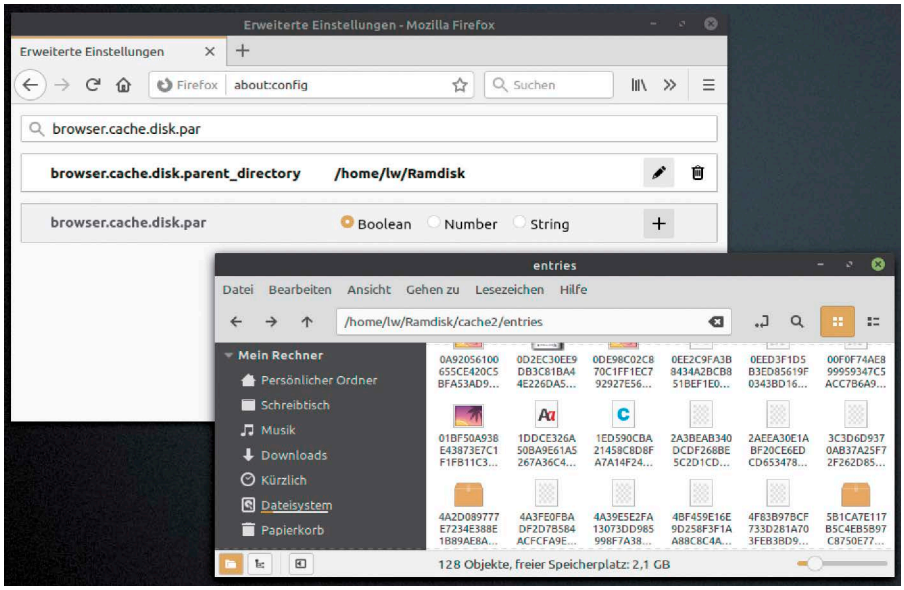
Das Tool Preload beschleunigt den Start von Software, die Sie häufig verwenden oder standardmäßig per Autostart laden. Der einfache Dienst protokolliert die Programmfavoriten und lädt deren Standardkomponenten vorab in den Arbeitsspeicher. Auf schnellen SSDs wird Preload kaum spürbare Effekte erzielen, während auf mechanischen Festplatten mindestens 15 und bis zu 50 Prozent Startbeschleunigung der Programmfavoriten zu erreichen ist. Preload ist über die Standardpaketquellen mit

```
sudo apt install preload
```

schnell nachinstalliert. Dies genügt. Für den künftigen automatischen Start sorgt Preload selbst. Manuelle Anpassung der Konfigurationsdatei „/etc/preload.conf“ ist möglich, kann aber mehr schaden als nützen.

Firefox beschleunigen

Zum Mozilla-Browser gibt es zahlreiche Detaileinstellungen über die Konfigurationszentrale „about:config“, die Firefox beschleunigen sollen. Seriöse, mit Messung belegte Leistungsvorteile durch geänderte Einstellungen unter „network.http.*“ oder „network.dns.*“ werden Sie jedoch nicht finden. Aus diesem Grund deuten wir diese Option nur an, ohne sie zu vertiefen, und beschränken uns auf nachhaltigere Maßnahmen.



Browserverlauf auf beliebiges Ziel schreiben: Firefox wie Chrome können die Surfchronik in einen benutzerdefinierten Ordner schreiben – etwa auf eine schnelle Ramdisk.

Tabula rasa: Einem langsamen Firefox helfen Sie durch ein neues Nutzerprofil auf die Sprünge. Nach

```
firefox --ProfileManager
```

und „Create Profile“ entsteht ein neues Profil mit Standardeinstellungen. Damit läuft der Browser wieder wie neu, Anpassungen und Lesezeichen gehen dabei aber verloren.

Erweiterungen abschalten: Firefox lädt beim Start alle eingerichteten Erweiterungen. Der Menüpunkt „Add-ons“ zeigt die installierten Erweiterungen und kann diese wieder entfernen.

Verlauf abschalten oder „Privates Browsen“: Wenn der Browser nichts aufzeichnen muss, läuft er schneller und entlastet die Festplatte. Über „Einstellungen → Datenschutz & Sicherheit → Chronik“ entscheiden Sie, ob Firefox einen Verlauf anlegt oder eben nicht. Am genauesten sind hier die „benutzerdefinierten Einstellungen“, die „Immer den Privaten Modus“ (ohne Verlaufsaufzeichnung) vorsehen oder eine Option, um nur Suchbegriffe und Formulardaten zu speichern.

Cacheverzeichnis verlegen: Eine interessante Tuningoption ist nicht mehr dokumentiert, funktioniert aber trotzdem noch. Wenn Sie über die Adresse „about:config“ den zusätzlichen Parameter

```
browser.cache.disk.parent_
  directory
```

neu anlegen (als „String“), können Sie danach den Ordner für die Verlaufsdaten manuell eintragen und somit frei wählen. Ideales Ziel wäre eine Ramdisk (siehe ab Seite 50), sofern der Verlaufsinhalt bei jedem System-Shutdown gelöscht werden darf – oder sogar soll.

Chrome/Chromium beschleunigen

Für Chrome gilt Analoges wie bei Firefox: Die „geheimen" Chrome-Seiten (Adresse „chrome:about") und dort insbesondere „chrome:flags" versprechen theoretisches Optimierungspotenzial. Praktiker werden mit folgenden Tuningmaßnahmen auskommen.

Tabula rasa: Der Google-Browser hat zwar keinen Profilmanager, aber es ist trotzdem ganz einfach, den Konfigurationsballast abzuwerfen, indem Sie den Ordner „~/.config/google-chrome" löschen oder verschieben. Ferner kann der Startschalter „--user-data-dir" ein beliebiges Verzeichnis festlegen, in das der Browser seine Daten schreibt:

```
google-chrome --user-data-dir=/
  home/lw/chrome
```

Auch das ergibt ein komplett neues Chrome/Chromium-Profil.

Erweiterungen oder Theme abschalten: Im Google-Browser zeigt der Menüpunkt „Weitere Tools → Erweiterungen" die Übersicht der installieren Add-ons, die sich per Schieberegler abschalten lassen.

„Inkognito-Fenster": Einstellungen für die Verlaufsaufzeichnung kennt Chrome nicht, aber bei konsequenter Verwendung des Inkognitomodus geht die Schreibaktivität des Browser ebenso gegen null. Interaktiv verwenden Sie dazu den Menüpunkt „Neues Inkognito-Fenster", einen generellen Inkognitomodus erreichen Sie mit dem Aufruf „google-chrome --incognito", den Sie als Starter oder Terminal-Alias ablegen.

Cacheordner verlegen: Chrome kann wie Firefox alle Verlaufsdaten auf ein beliebiges schreiben. Der Google-Browser erledigt das über einen Aufrufschalter:

```
google-chrome --disk-cache-dir=/
  home/lw/Ramdisk
```

Geschwindigkeitsvorteile ergeben sich, wenn es sich beim Ziel um eine Ramdisk oder SSD handelt.

Libre Office beschleunigen

Ob ein lahmendes Office-Paket durch eine fehlerhafte oder überladene Benutzerkonfiguration gebremst wird, lässt sich leicht nachprüfen:

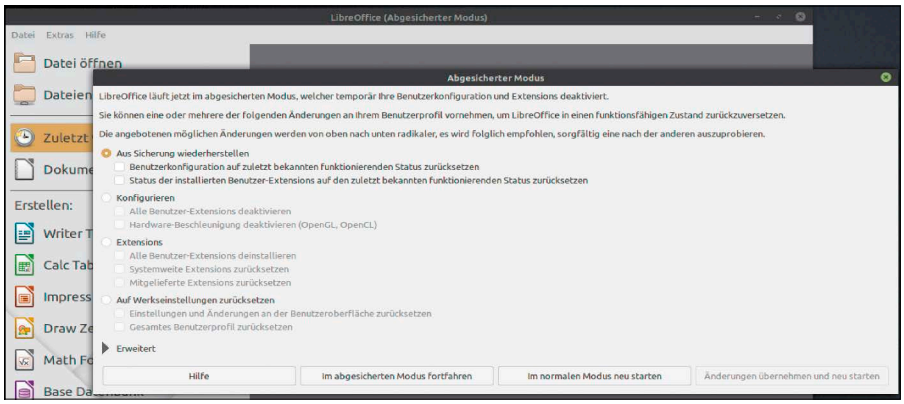
```
libreoffice
  -env:UserInstallation=file:///
  tmp/libreoffice
```

Damit entsteht ein neues Benutzerprofil im angegebenen Pfad. Wenn das Office damit einwandfrei läuft, sollten Sie Ihr normales Profil („~/.config/libreoffice") reparieren oder löschen. Dabei hilft dieser Start

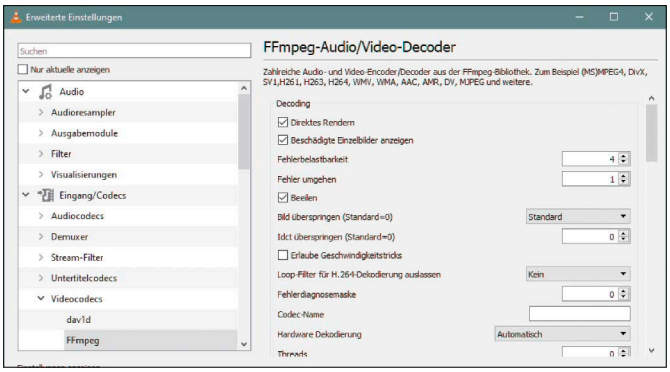
```
libreoffice --safe-mode
```

mit Reparaturoptionen wie „Benutzerkonfiguration [...] zurücksetzen" oder „Auf Werkseinstellungen zurücksetzen".

Alle Standardpfade von Libre Office, etwa für temporäre Dateien oder für automatische Sicherungskopien, lassen sich über „Extras → Optionen → LibreOffice → Pfade" in andere Ordner verlagern, die schneller zugänglich sind oder auf schnellerem Datenträger liegen. Wer das Datenbankmodul „Base" nie benutzt, kann unter „Extras → Optionen → LibreOffice → Erweitert" die Java-Laufzeitumgebung abschalten. Detailliertere Tuningoptionen hat Libre Office aus dem Hauptfenster verbannt und nach „LibreOffice → Erweitert → Experteneinstellungen" verlegt. Dort lässt sich etwa die Anzahl der Undo-Schritte (org.openoffice.Office.Common.Undo) anpassen oder die Speichernutzung für OLE-Objekte erhöhen (org.openoffice.Office.Common.Cache).



Libre-Office-Profil erneuern: Der Start im abgesicherten Modus erlaubt die Reparatur oder das Löschen der Benutzerkonfiguration.



Fehlertolerantere Filmwiedergabe: In den Tiefen der VLC-Konfiguration finden Sie Optionen für flüssigere Wiedergabe bei Filmfehlern und Hardwareengpässen.

VLC Player beschleunigen

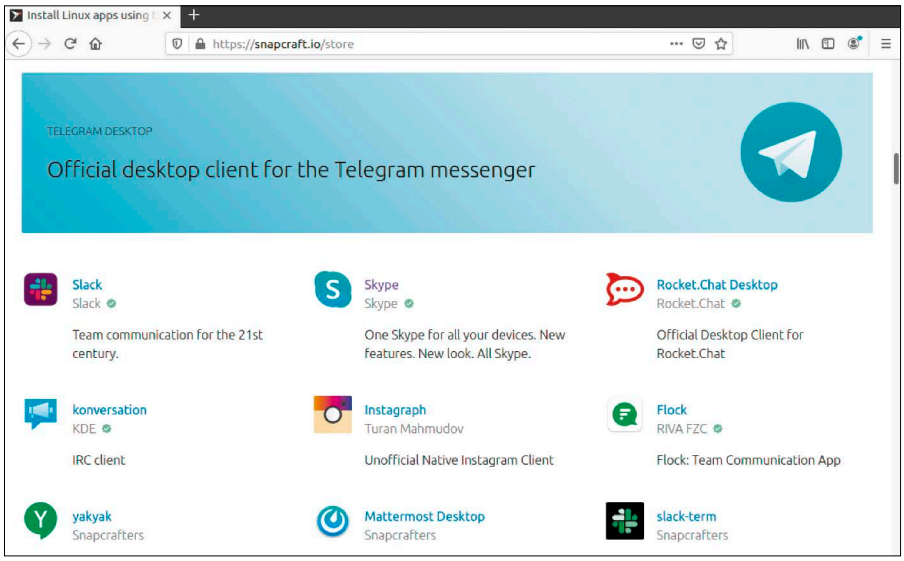
Eine lästige und häufige Bremse beim Start des VLC Players ist die Meldung, dass der Fontcache erneuert werden muss. Relevant ist der Fontcache nur für Filmuntertitel. Falls Sie diese nie benötigen, schalten Sie die Funktion einfach ab: Über „Werkzeuge → Einstellungen → Alle (links unten) → Video → Untertitel/Bildschirmanzeige" können Sie das „Textrenderer-Modul" auf „Deaktivieren" setzen. Eine Alternative ist die Option „Dummy-Font-Renderer", der Untertitel in einfacher Darstellung weiter ermöglicht.

Unter „Werkzeuge → Einstellungen → Eingang/Codecs" sollte stets die „Hardwarebeschleunigte Dekodierung" aktiviert sein, am einfachsten durch die Option „Automatisch". Weitere Verbesserungen erfordern wieder die Einstellungsoption „Alle" (links unten). Unter „Eingang/Codecs → Videocodecs → ffmpeg" gibt es für den meistgenutzten Decoder Optionen zur Fehlertoleranz: Aktivieren Sie „Direktes Rendern", deaktivieren Sie „Beschädigte Einzelbilder anzeigen" und erhöhen Sie die „Fehlerbelastbarkeit" auf „2" oder auf das Maximum „4". Die weiteren Optionen „Beeilen" an dieser Stelle und ein zweites Mal unter „Encoding" nehmen zugunsten flüssiger Wiedergabe Qualitätsabstriche in Kauf, wenn die Hardware überfordert ist. ■

Fehlende Software und Spiele

Linux-Distributionen bieten genügend Software für eine Basisausstattung. Wer neuere Programmversionen oder ganz spezielle Software benötigt, muss aber auch unter Linux auf (fast) nichts verzichten.

VON THORSTEN EGGELING



Zusätzliche Software: Über *https://snapcraft.io/store* finden Sie Programme, die sich über die Paketverwaltung nicht installieren lassen. Es gibt neuere Versionen und auch Closed-Source-Software wie Skype.

Ubuntu bietet mehr als 60 000 Softwarepakete zur Installation. Da sollte eigentlich für jeden Zweck etwas dabei sein. Bei einem großen Teil der Programme handelt es sich jedoch um Bibliotheken für Softwareentwickler oder um sehr spezielle Software. Trotzdem finden flexible Nutzer für fast jedes Einsatzgebiet geeignete Software. Wer neuere Versionen einer Anwendung benötigt oder in der Paketverwaltung nichts Passendes findet, kann auf alternative Installationsmethoden ausweichen. Auch PC-Spiele mit aufwendiger Grafik laufen unter Linux und die Unterstützung hat sich in den letzten Jahren deutlich verbessert. Allerdings sind längst nicht alle Titel für Linux verfügbar.

Mehr Software für Linux

Wer ein stabiles Linux-System bevorzugt, greift zu LTS Versionen wie Ubuntu 20.04. Der Nachteil: Über die Paketverwaltung erhalten Sie zwar regelmäßige Updates, aber keine neuen Programmversionen. Eine Lösung dafür sind Softwarecontainer, die mehr oder weniger unabhängig vom Betriebssystem laufen. Es besteht keine Gefahr, dass die neue Software Systemfunktionen beeinträchtigt oder standardmäßig installierte Pakete stört. Bei Ubuntu 20.04 ist Canonicals Snap-Format standardmäßig eingerichtet, Snap-Apps lassen sich daher über „Ubuntu Software“ oder auf der Kommandozeile installieren. Aktuellere Versionen gibt es als Snaps beispielsweise von Libre Office, Gimp oder VLC. Es sind auch Programme im Angebot, die sich über die Paketverwaltung nicht installieren lassen, beispielsweise Skype, Opera oder Plex Media Server.

Über den Snap Store (*https://snapcraft.io/store*) können Sie online nach der gewünschten Software suchen. Nach Klick auf „Install“ öffnet sich ein Fenster, das die Befehlszeile für die Installation über das Terminal anzeigt. Sie können aber auch auf „View in Desktop store“ und „Link öffnen“ klicken und gelangen damit zu „Ubuntu Software“. Dort genügt dann ein Klick auf „Installieren“, um die Software einzurichten.

In „Ubuntu Software“ können Sie ebenfalls nach Snap-Apps suchen. Im Suchergebnis tauchen die Programme meist zweimal auf: Eine Version aus den klassischen Paketquellen und die andere von snapcraft.io. Auf den ersten Blick sind die beiden Versionen nicht zu unterscheiden. Deshalb ist der Weg über *https://snapcraft.io/store* vorzuziehen, wenn Sie gezielt nach Snap-Apps suchen wollen.

In Linux Mint 20 ist die Snap-Umgebung nicht installiert, da Mint das ähnliche Containerformat Flatpak bevorzugt. Wie Sie auch hier Snap-Apps nutzen können, lesen Sie unter *www.pcwelt.de/1927768* im Abschnitt „Das Verbot für die Ubuntu-Snaps“.

Alternative Containerformate

Das Flatpak-Format, das bei Linux Mint 20 standardmäßig dabei ist, können auch Ubuntu-Nutzer nachinstallieren:

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

Linux Mint zeigt in der „Anwendungsverwaltung“ unter „Kategorien“ eine eigene Schaltfläche „Flatpak“, die zur Softwareauswahl führt. Alternativ können Sie auch direkt auf *https://flathub.org/home*

nach Flatpak-Software suchen. Per Klick auf „Install“ öffnen Sie das Paket im „Software Manager“ (Ubuntu: „Anwendungsinstallation“), über den die eigentliche Installation erfolgt.

Bei der Suche nach Programmen im Internet trifft man auch auf das Appimage-Format. Die Anwendung inklusive der benötigten Komponenten ist in einer einzigen Datei zusammengefasst, in der Regel mit der Endung „.appimage“. Man muss die Datei nur über den Dateimanger („Eigenschaften → Zugriffsrechte“) ausführbar machen und kann das Programm dann starten. Mehr ist nicht erforderlich.

Anlaufstellen für die gezielte Suche nach Appimage-Anwendungen sind *www.appimagehub.com* oder *https://appimage.github.io/apps*.

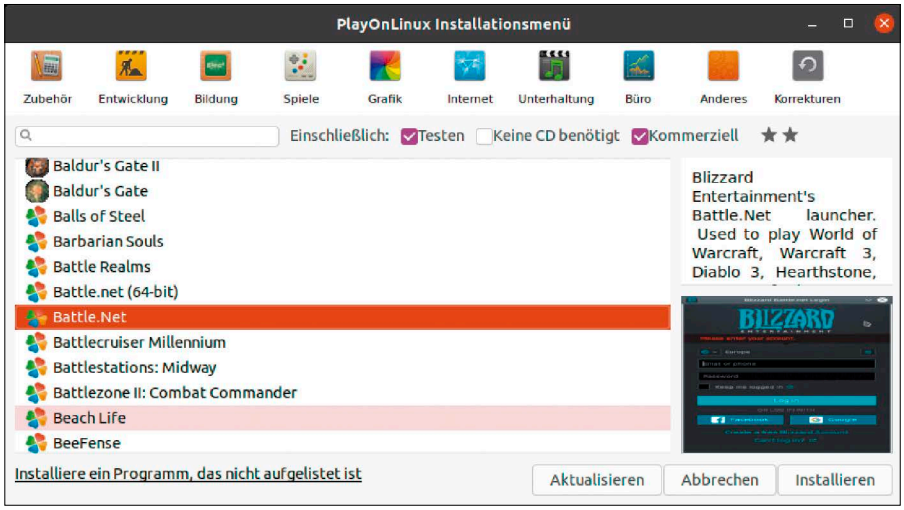
Wine statt Windows nutzen

Das Wine-Projekt (*www.winehq.org*) gibt es bereits seit 1993. Wine bildet die Windows-API (Application Programming Interface) nach, über die Anwendungen Systemaufrufe durchführen oder gemeinsam genutzte Komponenten einbinden.

Das Ziel ist, Windows-Software ohne Anpassungen direkt unter Linux starten zu können. Aufgrund der Komplexität der Windows-API und der unzureichenden Dokumentation ist das keine einfache Aufgabe. Im Ergebnis laufen aber viele ältere Windows-Programme stabil unter Wine, neuere oft nicht. Wer sich darüber informieren möchte, sucht in der Wine Application Database (*https://appdb.winehq.org*) nach der gewünschten Anwendung.

Wine ist über die Paketverwaltung schnell eingerichtet. Zusätzlich empfiehlt sich die Installation des Tools winetricks, das die Konfiguration erleichtert. Weiteren Komfort bietet Playonlinux, das sich ebenfalls aus den Standardrepositorien installieren lässt. Das Tool richtet automatisch die passende Wine-Version ein, wenn diese als stabiler für eine bestimmte Anwendung gilt. Nach dem Start des Programms klicken Sie auf „Installieren“ und dann auf die gewünschte Rubrik, beispielsweise „Büro“. Wählen Sie die gewünschte Anwendung, klicken Sie auf „Installieren“ und folgen Sie den Anweisungen des Assistenten. Wenn Sie dazu aufgefordert werden, geben Sie den Pfad der gemounteten Installations-CD/DVD oder der Setupdatei auf der Festplatte an.

Container-Apps: Bei Linux Mint 20 sind Flatpak-Pakete in die „Anwendungsverwaltung“ integriert. Die Programme lassen sich installieren wie klassische Softwarepakete auch.



Windows-Software unter Linux: Playonlinux ermöglicht die schnelle Installation von Windows-Anwendungen und Spielen. Die passende Wine-Version wird automatisch eingerichtet.

PC-Spiele unter Linux

Den Spielemarkt dominieren Windows und Konsolen. Der Hersteller Valve hat mit seiner Vertriebsplattform Steam (*https://store.steampowered.com*) versucht, dem eine Konsole auf Linux-Basis entgegenzusetzen. Die Entwicklung der Hardware wurde 2018 eingestellt, das zugehörige System Steam-OS soll jedoch weiterhin gepflegt werden.

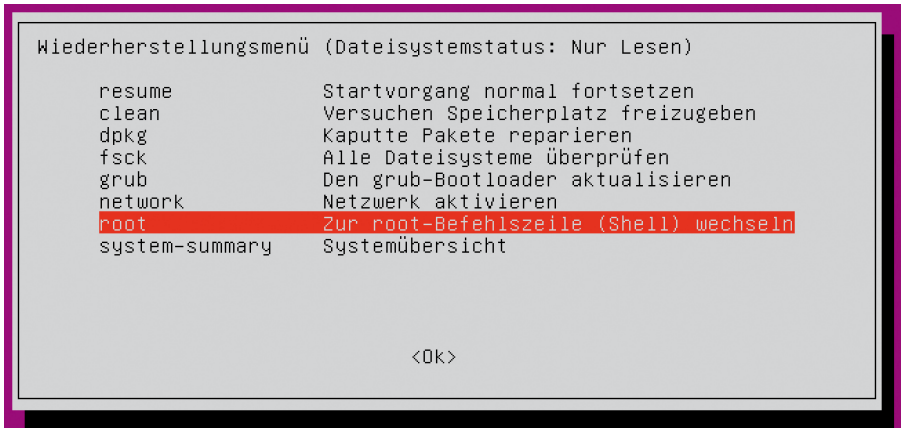
Für Desktop-PCs lässt sich unter Ubuntu oder Linux Mint der Steam-Client über die Standardrepositorien installieren. Sie sollten aber vorher herausfinden, ob das gewünschte Spiel unter Linux läuft. Unter *https://store.steampowered.com/linux* finden Sie eine Liste der Spiele für Linux und Steam-OS. Bei jedem Spiel sind die Systemanforderungen auch für Linux vermerkt. Für grafisch anspruchsvolle Spiele sind meist eine CPU ab Intel i3 oder AMD Phenom II X6 sowie ein Grafikchip von Nvidia oder AMD ab Geforce GTX 460 beziehungsweise Radeon R7 260X erforderlich. Einige Spiele sind auch unter Wine lauffähig, beispielsweise über Bizzard Battle.net, das sich mit Playonlinux installieren lässt. Damit kann man Spiele wie Starcraft oder World of Warcraft zocken.

Windows unter Linux mit Virtualbox

Virtualisierung ist eine zuverlässige Methode, Windows-Anwendungen auch unter Linux zu nutzen. Im Prinzip läuft hier alles außer Spiele, die eine hohe Grafikleistung erfordern. Anders als bei Wine benötigen Sie für Windows in Virtualbox (*www.virtualbox.org*) aber eine gültige Windows-Lizenz. Ohne Aktivierung lässt sich das System immerhin einige Wochen ohne große Einschränkungen nutzen, was beispielsweise für die Steuerberatungssoftware ausreicht. Einen Ratgeber mit ausführlicher Anleitung zum Thema Virtualbox finden Sie unter *www.pcwelt.de/2111217*. ■

Kleinere Linux-Pannen

Anmeldepasswort vergessen oder der Desktop reagiert plötzlich nicht mehr? Kleinere Probleme lassen sich meist über den Recovery-modus oder sogar nur über ein Tastenkürzel beseitigen.



Systemstart im Notfall: Im Wiederherstellungsmodus lässt sich eine root-Befehlszeile aufrufen. Sie können dort Konfigurationsdateien bearbeiten und Fehler beheben.

VON THORSTEN EGGELING

Nicht jeder Fehler endet in einer Katastrophe. Manchmal sind es nur kleine Hürden, die sich schnell aus dem Weg räumen lassen. Oft ist aber der Weg zur Lösung nicht auf den ersten Blick erkennbar.

1. Wiederherstellungsmodus starten

Nicht jede Reparatur lässt sich im laufenden System durchführen, schon gar nicht, wenn dieses nicht mehr startet oder man sich nicht mehr anmelden kann. Ubuntu und Linux Mint bieten für solche Fälle den Wiederherstellungsmodus: Halten Sie kurz nach dem Einschalten des PCs die Umschalt-Taste gedrückt, um das Grub-Menü aufzurufen. Wählen Sie „Erweiterte Optionen für Ubuntu“ und dann den ersten Eintrag mit dem Zusatz „recovery mode“. Gehen Sie auf „root“ und bestätigen Sie mit der Eingabetaste. Bei Linux Mint funktioniert das entsprechend, die Menüeinträge sind nur anders beschriftet.

Im Wiederherstellungsmodus ist das Dateisystem schreibgeschützt eingehängt, was sich mit der Befehlszeile

```
mount -o remount,rw /
```

ändern lässt. Danach können Sie Konfigurationsdateien mit einem Editor wie nano bearbeiten und speichern.

Abschließend geben Sie die folgenden drei Befehlszeilen ein:

```
sync
mount -o remount,ro /
exit
```

Damit stellen Sie sicher, dass die Änderungen tatsächlich auf die Festplatte geschrieben werden. Mit „exit“ kehren zum Wiederherstellungsmenü zurück. Wählen Sie dann „resume“, um den normalen Linux-Start fortzusetzen.

2. Das vergessene Passwort

Wer das Systempasswort vergessen hat, kann sich nicht mehr beim Linux-System anmelden. Es ist jedoch nicht besonders schwierig, das Passwort zu löschen und dann neu zu vergeben. Das funktioniert allerdings nur, wenn die Festplatte nicht verschlüsselt ist. Ohne Passwort kommt man an das System über den Ubuntu-Wiederherstellungsmodus (siehe Punkt 1), über den man auch das Passwort löschen oder ändern kann.

Passwort löschen: Mit der Befehlszeile

```
nano /etc/shadow
```

öffnen Sie die Passwortdatenbank im Editor. Hier sehen Sie Einträge wie „[Benutzer konto]:$6$9kSR4q[...]:16301:0:99999:7:::“.

Die lange Zeichenfolge hinter dem Benutzernamen und Doppelpunkt ist das verschlüsselte Passwort. Löschen Sie das Passwort. Die Zeile sieht dann so aus:

```
[Benutzerkonto]::16301:
 0:99999:7:::
```

Mit Strg-X und Bestätigung mit „j“ speichern Sie die Änderung. Danach verlassen Sie die Shell mit „exit“ und gehen auf „resume“. Im Anmeldebildschirm klicken Sie auf Ihren Benutzernamen. Ein Passwort ist jetzt nicht mehr erforderlich. Da Sie ohne Passwort keine root-Rechte anfordern können, müssen Sie ein Terminal öffnen (Strg-Alt-T) und mit „passwd“ ein neues Passwort vergeben.

3. Das Uhrzeit-Problem bei Multiboot-Installationen

Wenn auf Ihrem Rechner Linux und Windows parallel installiert sind, geht unter Windows die Uhr eine Stunde nach, bei Sommerzeit sogar zwei Stunden. Wenn Sie die Uhrzeit korrigieren und später wieder Linux starten, liegt hier die Zeit eine oder zwei Stunden in der Zukunft.

Die Ursache: Linux und Windows interpretieren die Werte der Echtzeituhr auf der Hauptplatine jeweils anders. Linux verwen-

det die koordinierte Weltzeit (UTC), Windows geht von der lokalen Zeit aus (Mitteleuropäische Zeit, MEZ, UTC+1). Zwischen beiden Zeitangaben liegen – je nach Sommer- oder Winterzeit – eine oder zwei Stunden. Im Terminal lässt sich mit

```
timedatectl
```

ermitteln, welche Zeiteinstellungen Linux verwendet. Steht hinter „RTC in local TZ:“ die Angabe „no“, basiert die Zeitangabe auf UTC.

Zur Lösung des Problems stellen Sie unter Ubuntu oder Linux Mint das System mit

```
sudo timedatectl set-local-rtc 1
```

für die Verwendung der lokalen Zeit um. Linux verhält sich dann wie Windows.

4. Apt-Blockaden bei der Paketinstallation

Sie wollen unter Ubuntu Software im Terminal mit „sudo apt install [Paketname]“ installieren. Das schlägt jedoch mit einer Meldung wie „Konnte keinen exklusiven Zugang zur Sperrdatei /var/lib/dpkg/lock-frontend erhalten“ oder ähnlich fehl. Die Ursache ist einfach: Wahrscheinlich installiert Ubuntu gerade Sicherheitsaktualisierungen, wodurch die Paketdatenbank gesperrt ist. Warten Sie einfach einige Zeit, bis der Vorgang abgeschlossen ist. Manchmal dauert die Aktualisierung sehr lange oder sie gibt den Zugriff auf die Paketdatenbank nicht mehr frei. Dann hilft nur ein Linux-Neustart.

Wer häufig apt im Terminal benutzt, kann das Problem vermeiden. Rufen Sie „Anwendungen & Aktualisierungen“ auf und gehen Sie auf „Aktualisierungen“. Hinter „Wenn Sicherheitsaktualisierungen verfügbar sind:“ stellen Sie „Sofort anzeigen“ ein. Sie erhalten dann eine Benachrichtigung, wenn Updates verfügbar sind, und sind für die eigentliche Aktualisierung selbst verantwortlich.

Passwort löschen: Die verschlüsselten Passwörter stehen in der Datei „/etc/shadow“. Wenn Sie ein Passwort entfernen, kann sich der betreffende Benutzer ohne Passwort anmelden.

5. Programme mit xkill abschießen

Es kommt unter Linux selten vor, aber manchmal passiert es doch: Ein Programm regiert nicht mehr und es lässt sich auch nicht beenden. Über das Tool xkill lassen sich grafische Programme beenden, deren Fenster nicht mehr reagieren. Beim Aufruf von xkill über das Terminal oder Alt-F2 („Befehl ausführen“) verwandelt sich der Mauszeiger in ein Kreuz, mit dem Sie das Programm mit linker Maustaste anklicken und damit beenden. Nicht gespeicherte Daten gehen dabei verloren. Die rechte Maustaste beendet xkill ohne Aktion.

Sie können auch ein Tastaturkürzel für das Tool festlegen. Gehen Sie unter Ubuntu 20.04 in den „Einstellungen“ auf „Tastaturkürzel“. Per Klick auf „+“ am unteren Bildschirmrand fügen Sie eine eigene Tastenkombination für den Befehl xkill hinzu, beispielsweise Strg-Alt-K. Nutzer von Linux Mint 20 gehen im Menü auf „Einstellungen → Tastatur“ und dann auf „Tastenkombinationen“. Klicken Sie auf „Eigene Tastenkombination erstellen“.

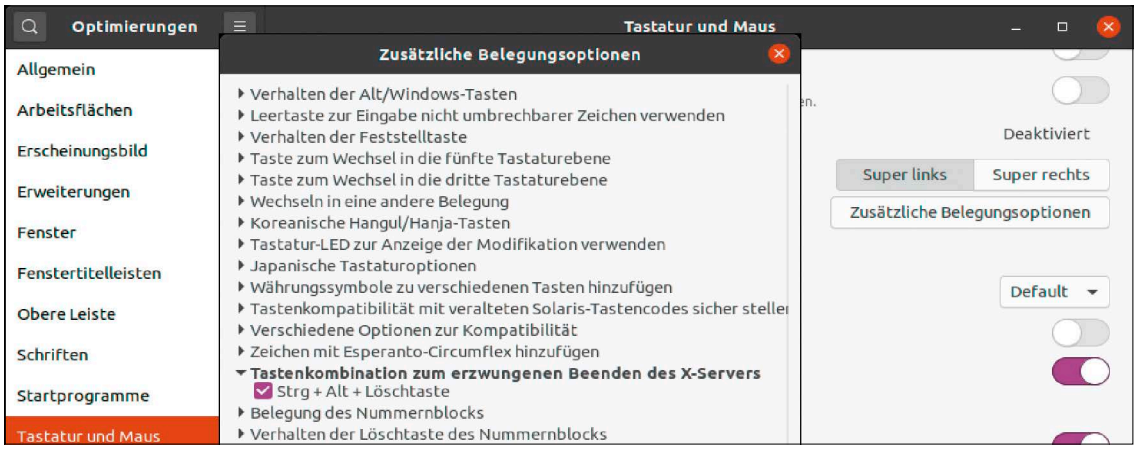
6. Desktopneustart bei Problemen

Bei Fehlfunktionen kann der Desktop einfrieren und nicht mehr reagieren. Laufende Anwendungen sind davon meist nicht betroffen, aber die Fenster lassen sich nicht mehr bewegen oder die Elemente im Fensterrahmen verschwinden.

Linux Mint 20 Cinnamon bietet mehrere Optionen beim Umgang mit Desktopproblemen. Über die Tastenkombination Strg-Alt-Esc lässt sich Cinnamon neu starten. Alternativ können Sie auch Alt-F2 drücken, „r“ eintippen und mit der Eingabetaste bestätigen. Beim Neustart des Cinnamon-Desktops laufen die gestarteten Anwendungen weiter. Daten sollten dabei nicht verloren gehen.

Die Desktop-Radikalkur unter Cinnamon ist die Tastenkombination Strg-Alt-Rücktaste. Damit beendet man die komplette Sitzung und kehrt zum Anmeldebildschirm zurück. Laufende Anwendungen werden zwangsweise geschlossen und nicht gespeicherte Daten gehen verloren.

Ubuntu 20.04: Der Gnome-Desktop lässt sich wie unter Linux Mint über Alt-F2 und „r“ neu starten. Der Hotkey Strg-Alt-Rücktaste ist hier allerdings nicht belegt. Wenn Sie das ändern möchten, installieren Sie das Paket „gnome-tweaks“ („Optimierungen“). Dort gehen Sie auf „Tastatur und Maus“ und klicken auf „Zusätzliche Belegungsoptionen“. Unter „Tastenkombination zum erzwungenen Beenden des X-Servers“ setzen Sie ein Häkchen vor „Strg + Alt + Löschtaste“. ■

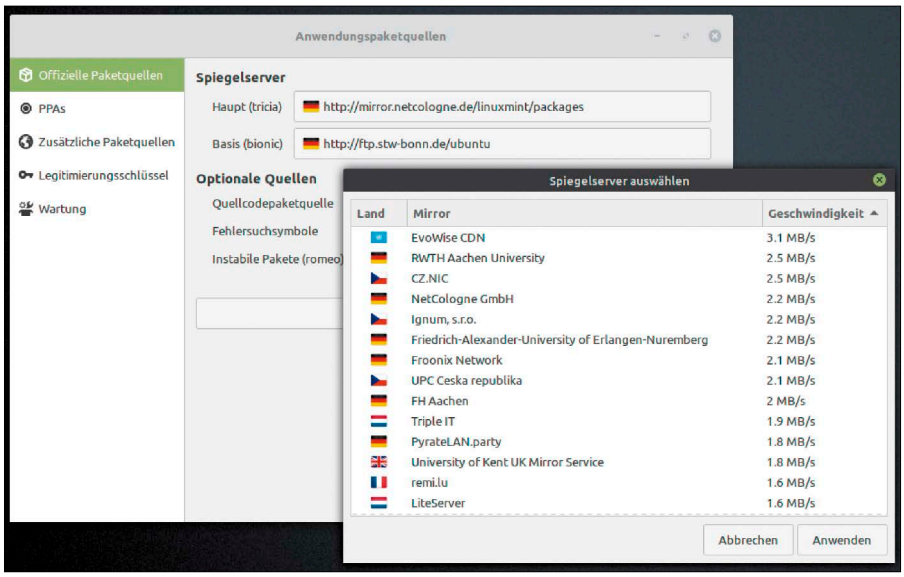


X-Server abschießen: Über das Tool Optimierungen („gnome-tweaks“) aktivieren Sie unter Ubuntu die Tastenkombinationen Strg-Alt-Rücktaste, mit der sich der X-Server beenden lässt.

Systemturbos für Ubuntu & Co.

Ubuntu, Mint & Co. sind schnell eingerichtet. Aber wie bei jedem System gibt es Optionen, die das System beschleunigen und die Benutzung effizienter machen. Im ersten Artikel in dieser Tempo-Rubrik geht es um systemnahe Leistungstipps.

VON HERMANN APFELBÖCK



Schnelle Server für Updates und Installationen: Ubuntu und Linux Mint zeigen durch Schnelltests die geeignetsten Kandidaten für den Softwarebezug.

Wenn Ubuntu und Mint auf einigermaßen aktuelle Hardware treffen, sind diese Linux-Distributionen bereits nach der Standardinstallation überzeugend schnell. Mit den nachfolgenden Tipps gewinnen Sie aber optional noch ein spürbares Stück Leistung hinzu.

Ein Hinweis vorab: Einige hier beschriebenen Eingriffe in die „sysctl.conf", in Systemdienste, Autostarts oder Dateisystemfunktionen bedeuten immer ein gewisses Risiko. Daher sollten Sie hier stets nur eine Maßnahme ausführen und ausreichende Zeit testen. Bei eventuellen Problemen können Sie die Systemänderung im Falle des Falles wieder gezielt rückgängig machen.

Schnelle Spiegelserver einstellen

Sämtliche Systemupdates und Softwareinstallationen verwenden den voreingestellten Spiegelserver, der die Ubuntu-Paketquellen bereitstellt. Je schneller Ihre Internetverbindung ist, desto mehr profitieren Sie von einem richtig schnellen Spiegelserver. Ubuntu & Co. können den geeignetsten deutschen Server selbst ermitteln: Dazu gehen Sie zu „Anwendungen & Aktualisierungen" (Ubuntu) oder „Anwendungspaketquellen" (Mint). Die dort vorangestellten Server können Sie anklicken, wonach automatisch die Suche nach einem deutschen Server beginnt, die auch gleich nach Downloadleistung sortiert. Wählen Sie den schnellsten Server (den ersten in der Liste). Beachten Sie aber, dass der Leistungstest eine Momentaufnahme ist, die gelegentliche Kontrolle verdient.

Optimale Treiber finden

Insbesondere bei Grafikkarten und WLAN-Chips können die mitgelieferten Open-Source-Treiber mit Herstellertreibern nicht mithalten. Ubuntu & Co. machen es aber recht einfach, Treiber zu finden und nachzuinstallieren. In den Systemeinstellungen finden Sie einen Punkt „Treiber" oder „Treiberverwaltung". Wenn Sie dieses Applet starten, beginnt automatisch eine Treibersuche. Wird ein passender Treiber gefunden, können Sie diesen nachinstallieren. Üblicherweise ist danach ein Neustart notwendig, damit der neue Treiber verwendet wird.

Schnellere Desktopalternativen

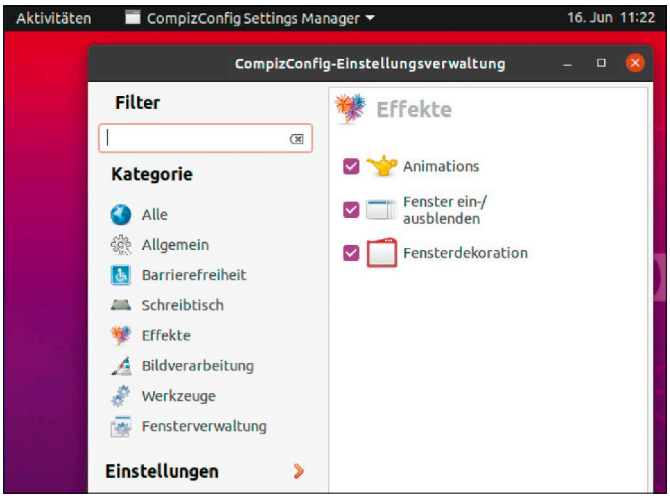
Oberflächen wie Gnome oder Budgie sind für ältere Hardware eine erhebliche Last. Größte Speicherersparnis erzielen Sie daher, wenn Sie einen sparsameren Desktop nachinstallieren. Einen guten Kompromiss zwischen Benutzerkomfort und Ressourcenökonomie bietet XFCE. Die Installation der Oberfläche können Sie über das Softwarecenter oder in der Konsole ausführen:

```
sudo apt install xfce4
```

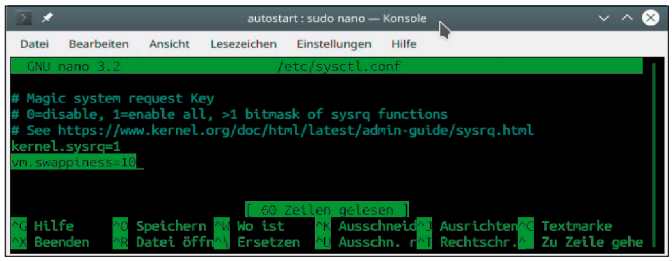
Beachten Sie, dass es sich bei diesem Metapaket nur um die Oberfläche handelt, während das größere Metapaket „xubuntu-desktop" auch das typische Zubehör mitinstalliert. Auf diesen Unterschied ist auch bei anderen Desktops zu achten: „lxqt" installiert nur die Oberfläche, „ lubuntu-qt-core" hingegen die komplette LXQT-Umgebung mit Zubehör. Nach er-

folgreichem Download melden Sie sich von der gewohnten Umgebung ab. Auf dem Anmeldebildschirm klicken Sie auf das Symbol neben Ihrem Benutzernamen und wählen „Xfce-Sitzung".

Grafische Effekte reduzieren: Wem der Ersatz der gewohnten Oberfläche zu weit geht, kann die Effekte seines Desktops reduzieren. Die meisten Desktops unterstützen dies: So zeigt etwa Cinnamon (Mint) in den Systemeinstellungen den Punkt „Effekte", KDE (Kubuntu) unter „Anzeige und Monitor" den Punkt „Composer". Hier lassen sich Effekte ganz oder teilweise deaktivieren. Die Ubuntu-Hauptedition mit Gnome lässt sich hingegen nur mit dem Zusatztool Gnome-Tweaks („Allgemein → Animationen") reduzieren, und das auch nur pauschal. Wer gezieltere Effektanpassung will, muss das weitere Tool CCSM (Compiz-Config-Settings-Manager) installieren.



Compiz-Konfiguration: Einige Mausklicks in diesem Zusatztool genügen, um die Effekte des Desktops abzuschalten und damit Grafikkarte und CPU zu entlasten.



Der Parameter „vm.swappiness" steuert die Auslagerungsaktivität. Bei viel RAM ist ein niedriger Wert angebracht, bei schneller SSD kann ein hoher Wert Leistungsvorteile bringen.

Swapping abschalten oder anpassen

Swapping, also das Auslagern länger ungenutzter Speicherseiten vom Arbeitsspeicher auf die Festplatte, ist ein Verfahren, das in die 90er-Jahre zurückgeht, als Speicher notorisch knapp war. Dieser Ansatz ist sinnvoll, solange RAM wertvoll ist: Der frei gewordene schnelle Arbeitsspeicher steht dann wieder für Programme und für den Festplattencache zur Verfügung.

Heute zeigt die Beobachtung der Swapaktivität im Taskmanager oder mit Kommandozeilentools (top, htop, free) meistens, dass keine Auslagerung stattfindet. Bei Rechnern mit acht und 16 GB ist das praktisch der Dauerzustand. Folglich können Sie dort die Swapdatei komplett abschalten. Das ist mit wenigen Handgriffen erledigt: Im laufenden System beenden die Terminalbefehle

```
sudo swapoff /swapfile
sudo rm /swapfile
```

die Auslagerung und löschen die Auslagerungsdatei. Zuletzt deaktivieren Sie in der Datei „/etc/fstab" die Zeile

```
/swapfile …
```

durch das Kommentarzeichen „#". Beachten Sie, dass der Ruhezustand „Bereitschaft" (Suspend to Ram) weiterhin funktioniert. „Hibernation" (Suspend to Disk) ist derzeit in den aktuellen Ubuntu-Varianten ohnehin nicht mehr vorgesehen, seit Ubuntu von der Swappartition auf die Swapdatei umgestellt hat.

Ihr System swappt? Wenn der Taskmanager auf älterer Hardware gelegentlich oder gar häufig die Anspruchnahme der Swapdatei anzeigt, sollten Sie dem Kernel das Swapping weiterhin zugestehen. Auch dann gibt es aber Optimierungschancen. Wie aktiv der Kernel auslagert, steuert der Parameter „Swappiness", dessen aktuellen Wert Sie mittels

```
cat /proc/sys/vm/swappiness
```

ermitteln. Unter Ubuntu & Co. voreingestellt ist „60", der Wert darf aber zwischen 0 und 100 liegen. Je höher der Wert, desto schneller schreibt der Kernel Speicherseiten aus dem RAM in die Swapdatei. Bei niedrigem Wert reagiert der Kernel erst bei ernster Speicherknappheit.

Dennoch lohnt sich die Swappiness-Anpassung nur in extremen Hardwaresituationen: Viel RAM bei langsamer mechanischer Festplatte legen es nahe, das Swappen zu reduzieren – etwa auf „10". Bei wenig RAM, aber schneller SSD empfiehlt sich hingegen ein hoher Wert –etwa „90". Um den Wert in der aktuellen Sitzung temporär zu erhöhen und zu testen, verwenden Sie dieses Terminalkommando:

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

Dauerhaft gilt der Swappiness-Wert, wenn Sie die Konfigurationsdatei „sysctl.conf" mit root-Recht bearbeiten:

```
sudo nano /etc/sysctl.conf
```

Vermutlich fehlt der Eintrag „vm.swappiness" noch – dann fügen Sie folgende Zeile einfach am Ende hinzu:

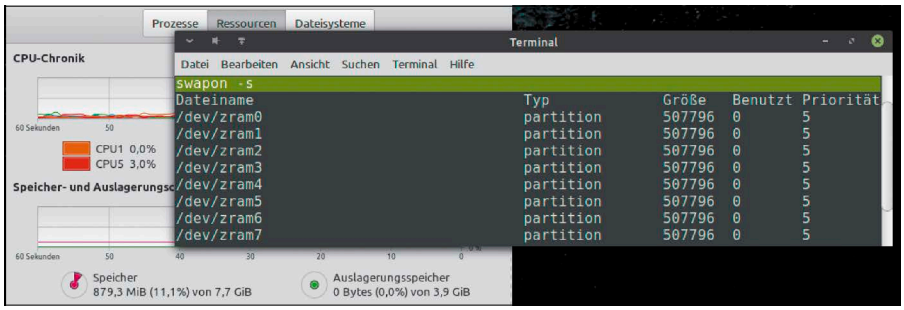
```
vm.swappiness=90
```

Das Systemverhalten lässt auf dem gleichen Weg jederzeit neu einstellen.

Komprimierte Auslagerung mit Zram

Wenn Sie bei guter RAM-Ausstattung das Swapping nicht komplett abschalten wollen, ist Zram eine interessante Alternative zum Swapping. Das Kernel-Modul reserviert einen Teil des Arbeitsspeichers, um dort mehrere RAM-Disks anzulegen, die als komprimierter Auslagerungsspeicher bei Engpässen dienen. Standardmäßig reserviert Zram die Hälfte des Arbeitsspeichers, teilt diesen durch die Anzahl der CPU-Kerne und richtet pro Kern ein Blockgerät ein. Bei einer CPU mit vier Kernen entstehen also vier Swapgeräte „/dev/zram0", /"dev/zram1" et cetera. Der Speicher wird dynamisch vergeben: Solange nichts auszulagern ist, nimmt Zram nichts in Anspruch. Erst wenn Auslagerung nötig wird, geht RAM nach Bedarf vom physikalisch vorhandenen RAM ab. Zram lässt sich mit minimalen Aufwand einrichten:

```
sudo apt install zram-config
```



Zram reserviert je nach RAM und CPU erhebliche Speicheranteile. Wie Sie im Bild sehen (0 Bytes von 3,9 GB), wird aber kein RAM abgezweigt, solange dies nicht angefordert ist.

Damit ist das Modul sofort aktiv, wie Sie mit

```
swapon -s
```

leicht kontrollieren können. Wir empfehlen Zram als Ersatz für die Auslagerungsdatei auf Rechnern mit guter RAM-Ausstattung. Zram soll aber auch auf Rechnern mit geringem Speicher (Raspberry & Co.) Vorteile bringen. Zram lässt sich durch Deinstallieren des Pakets „zram-config" wieder abschalten.

Ramdisk als Zwischendepot

16 GB RAM sind auf heutigen Rechnern keine Ausnahme. Für den typischen Einsatz mit Office, Mediaplayer, Bildbearbeitung ist das purer Luxus, mit dem sich aber Sinnvolles anfangen lässt. Wenn Sie einen zentralen Ordner, über den Sie den Datenaustausch inklusive Downloads abwickeln, in eine schnelle Ramdisk verlegen, entstehen mehrere Vorteile: mehr Leistung, Entsorgung beim Herunterfahren, Schonung von SSD/Festplatte, Nutzung des brachliegenden Speichers. Eine Ramdisk ist im Handumdrehen erstellt. Idealerweise liegt dieser Speicher zentral, etwa im Home-Verzeichnis oder gleich am Desktop:

```
sudo mount -t tmpfs -o size=2000M
  ramdisk ~/Schreibtisch/Ramdisk
```

Dieser Befehl genügt, um im Ordner „Ramdisk" (der existieren muss), Platz für maximal zwei GB Daten zu schaffen. Die angegebene Kapazität wird dynamisch abgezweigt – je nach Bedarf bis zum angegebenen Maximum. Die Ramdisk verbraucht also nur den Speicher, den die enthaltenen Dateien tatsächlich verursachen. Dauerhaft ist eine Ramdisk über die Datei „fstab" einzurichten:

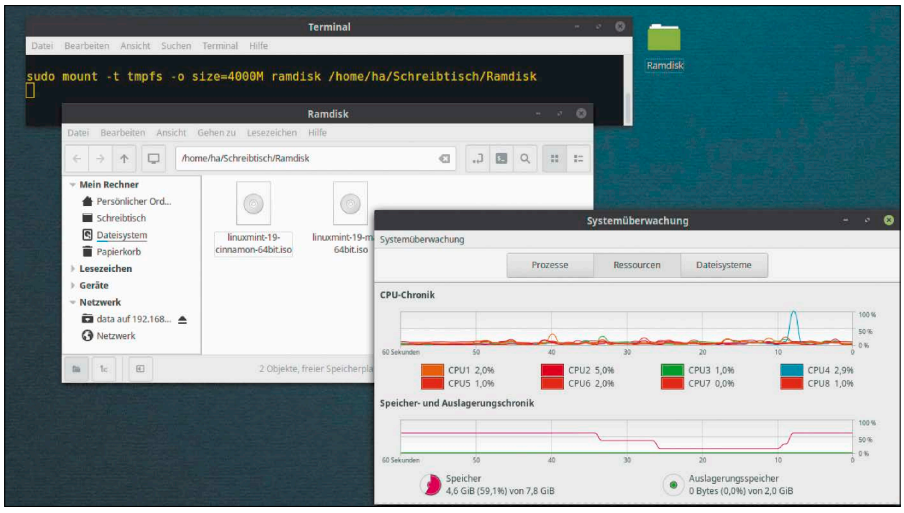
```
sudo nano /etc/fstab
```

Hier fügen Sie die weitere Zeile (Beispiel)

```
tmpfs /home/ha/Schreibtisch/
  Ramdisk tmpfs
  defaults,size=40%,mode=1777 0 0
```

hinzu (der Mountpfad darf keine Variablen enthalten). Nach dem Speichern starten Sie Linux neu.

Achtung: Der Umgang mit Ramdisk-Daten erfordert kompetente und disziplinierte Nutzer, weil die Daten beim Shutdown gelöscht werden.



Zwischendepot: Der Platz einer Ramdisk wird nach Bedarf dynamisch abgezweigt. Die Speicherchronik zeigt die Belegung nach Löschen und Kopieren großer ISO-Dateien.

Festplattenaktivität auf Ext4 reduzieren

Das Dateisystem Ext4 (ähnlich Ext3) bietet für Partitionen und Festplatten viele Detailoptionen über den Befehl tune2fs, die zum Teil mit eingehängten, zum Teil nur mit ausgehängten Datenträgern funktionieren. Eine Übersicht für eine Festplatte erhalten Sie mit diesem Befehl (Beispiel):

```
sudo tune2fs -l /dev/sda
```

Root-Recht ist für tune2fs grundsätzlich erforderlich.

Checks reduzieren: Ein erstes Beispiel, das die Automatismen von Ext4 steuert, reduziert die Datenträgerchecks:

```
sudo tune2fs -i60 -c100 /dev/sda
```

Eine Festplattencheck wird danach nur noch alle 60 Tage („-i60") oder nach 100 eboots („-c100") erfolgen – je nachdem, welches Ereignis früher erfüllt ist.

Journaling abschalten: Ein weiteres Beispiel ist das Abschalten der Journalingfunktion. Das Journaling dient zur Wiederherstellung von Dateien nach Abstürzen oder Stromausfällen und ist auf der Systempartition wünschenswert. Auf externen USB-Datenträgern oder reinen Datenpartitionen ist diese Funktion nicht ideal, da sie erheblichen Schreibaufwand verursacht:

```
sudo umount /dev/sdd?
sudo tune2fs -O ^has_journal /dev/
  sdd
```

Der erste Schritt ist „umount", weil das Dateisystem bei dieser Änderung nicht eingehängt sein darf. Der zweite Befehl schaltet das Journaling für das Gerät „/dev/sdd" ab, wovon Sie sich mit

```
sudo tune2fs -l /dev/sdd
```

in der Zeile „Filesystem features" überzeugen können. Umgekehrt lässt sich das Journaling mit diesem Befehl

```
sudo tune2fs -O has_journal /dev/
  sdd
```

aktivieren.

Journalingmodus ändern: Auch bei Verwendung der Ext-Journaling-Funktion verbleiben mehrere Abstufungen mit hoher bis niedriger Festplattenaktivität: Der Journalmodus schreibt nicht nur die Metadaten, sondern auch die Dateiinhalte. Diese aufwendigste Variante ist nicht Standard, aber mit (Beispiel)

```
sudo tune2fs -o journal_data /dev/
  sda
```

zu erzwingen. Standard ist „journal_data_ordered", das nur Metadaten ins Journal aufnimmt. Der schnellste Modus „journal_

data_writeback“ wartet erst gar nicht auf vorherige Journalsicherung, sondern schreibt Dateien sofort ins Dateisystem. Dieser Modus lässt sich mit (Beispiel)

```
sudo tune2fs -o journal_data_
  writeback /dev/sda
```

erzwingen. Solche Änderungen gelten ab dem nächsten Neustart.

Dateisystemoption „noatime“: Ext4-formatierte Partitionen speichern bei jeder Datei mehrere Zeitangaben. Erstelldatum und Änderungsdatum werden immer eingetragen (ctime und mtime: Creation und Modification). Optional ist hingegen das Erfassen des letzten Dateizugriffs (atime: Access). Diese Information ist nur dann relevant, wenn Sie mit „find -atime“ nach Zugriffszeiten von Dateiobjekten suchen. Wenn Sie das nie tun, kann die Festplattenaktivität reduziert werden. Es muss für die jeweilige Festplatte nur die Option „relatime“ oder „noatime“ in der „/etc/fstab“ gesetzt werden:

```
UUID=[…]  /  ext4  noatime  0  2
```

In aktuellen Ubuntu-Versionen ist die Option „relatime“ Standard. „relatime“ speichert die letzte Zugriffszeit nur dann, wenn dieser Zugriff vor der letzten Änderung der Datei erfolgte (mtime). Mit „noatime“ speichert das Dateisystem die Zugriffszeit (atime) generell nicht mehr.

Der Vollständigkeit halber: Es gibt auch noch die Option „nodiratime“, die bei Verzeichnissen darauf verzichtet, die Zugriffszeit zu vermerken. Wenn Sie die Aktivität der Festplatte reduzieren möchten, ist „noatime“ aber die weitreichendere Maßnahme.

Systemdienste abschalten

Jedes Linux lädt zahlreiche Systemdienste, die nicht jeder benötigt. Allerdings ist das Abschalten von Systemdiensten eine Wissenschaft für sich. Einblick in die aktiven Dienste auf einem System mit systemd-Daemon (Ubuntu, Mint) erhalten Sie so:

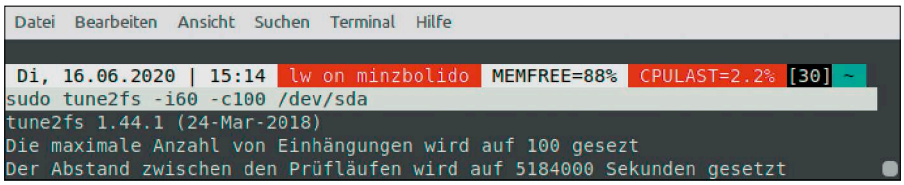
```
systemctl -a
```

Die Übersicht zeigt – unter anderem – die aktiven und inaktiven Dienste an. Dass Systemdienste in der Regel keine große Bootbremse darstellen, können Sie auf Ubuntu und Mint mit dem Befehl

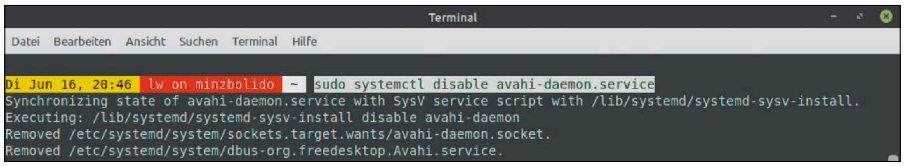
```
systemd-analyze blame
```

kontrollieren, der die Ladezeiten absteigend (längste bis kürzeste) auflistet. Trotzdem können Sie Dienste abschalten, um Speicher einzusparen:

```
sudo systemctl stop avahi-daemon.
  service
```



Festplattenchecks reduzieren: Das Tool tune2fs kann mit zahlreichen Optionen das Standardverhalten von Ext4-Datenträgern beeinflussen.



Systemdienste abschalten: Unter Ubuntu und Mint (mit systemd) ist das Tool systemctl das einschlägige Werkzeug zur Dienstverwaltung.

```
sudo systemctl disable avahi-
  daemon.service
```

Diese Befehle stoppen den angegebenen Dienst und deaktivieren ihn dauerhaft. Mit den Parametern „enable“ und „start“ ist er bei Bedarf wieder zu aktivieren.

Autostarts ausmisten

Desktops wie Gnome, KDE oder Cinnamon laden zahlreiche Programme bei der Desktopanmeldung. Das Abschalten solcher Autostarts spart Speicher und beschleunigt den Desktopstart. Über das Tool „Startprogramme“ können Sie bestehende Autostarts reduzieren. Besonders umfangreich fällt die Funktionalität unter KDE aus, das in den „Systemeinstellungen“ im Bereich „Starten und Beenden“ eine Reihe spezieller Optionen vorhält: So ist der Standard unter „Arbeitsflächen-Sitzung“, der alle Programme der letzten KDE-Nutzung automatisch wiederherstellt, in der Regel überflüssig und durch die Option „Mit leerer Sitzung starten“ zu ersetzen.

Wer rigoros ausmisten will, muss wissen, dass das Tool „Startprogramme“ die meisten systemnahen Komponenten ausblendet. Dafür sorgt die Anweisungszeile „NoDisplay=true“ in der jeweiligen Desktopdatei. Mittels

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

können Sie die Anweisung in allen Startern abschalten. Damit werden unter „Startprogramme“ alle Autostarts sichtbar und können deaktiviert oder komplett entfernt werden (die Programme selbst bleiben aber auf dem System). Theoretisch können Sie außer D-Bus, X-Settings-Plugin, Automount und den Sicherheitsdienst alles abschalten.

Protokoll IPv6 abschalten

Das Protokoll IPv6 spielt im Heimnetz in der Regel keine Rolle. Da ältere Router und andere Netzwerkhardware für IPv6-Pakete oft schlechterem Datendurchsatz bieten, kann man IPv6 auch abschalten. Bei Ubuntu & Co. lässt sich IPv6 über Kernel-Parameter steuern, also interaktiv über das Tool sysctl

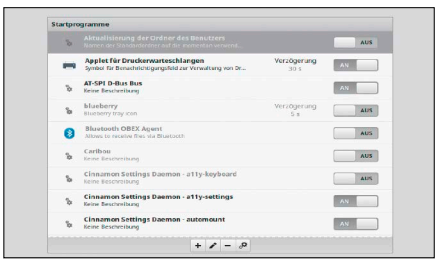
```
sudo sysctl net.ipv6.conf.all.
  disable_ipv6=1
```

oder dauerhaft über die Konfigurationsdatei „/etc/sysctl.conf“, indem Sie dort mit sudo-Recht die zusätzliche Zeile

```
net.ipv6.conf.all.disable_ipv6=1
```

eintragen. Nach einem Neustart ist die Änderung aktiv.

Noch ein Tipp für Systembastler: Der Befehl listet zahlreiche Parameter auf, die man mit dem Tool sysctl oder in der Systemdatei „/etc/sysctl.conf“ manipulieren kann. Unsere Tipps nennen zwei Beispiele – ipv6 an dieser Stelle und den Swappiness-Wert an früherer Stelle. ■



Alle Autostarts: „Startprogramme“ zeigt die ganze Menge der Komponenten erst an, wenn die Anweisung „NoDisplay“ in den Konfigurationsdateien abgeschaltet haben.

Schneller Systemstart

Im Verhältnis zu anderen Wartezeiten am PC, die durch Netzwerk, Backups, Updates, Programmstarts entstehen, scheint ein zögerlicher Rechnerstart eher nebensächlich. Aber erstens kann es nie schnell genug gehen, zweitens gibt es wirklich lästige Bremsen.

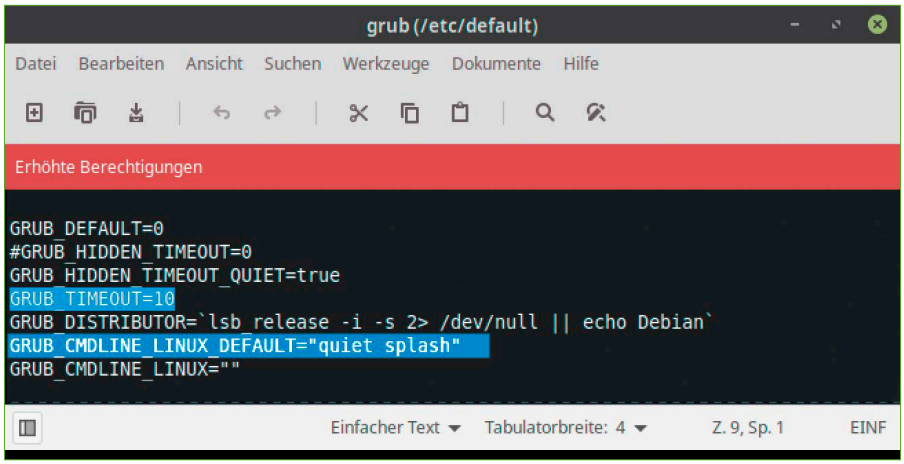
VON HERMANN APFELBÖCK

Systementwickler arbeiten permanent an der Bootoptimierung. Um nur einige Beispiele zu nennen: Ubuntu hat zuletzt an der Komprimierungsmethode gefeilt, der Init-Daemon Systemd ermöglicht parallelisiertes Laden der Systemdienste, Windows nutzt einen hybriden Shutdown zur Startbeschleunigung. Wenn es trotzdem nicht schnell genug geht, helfen schnellere Hardware, Fehlerbehebung oder alternative Startmethoden wie hier nachfolgend beschrieben. Allgemeinere, nicht eindeutig auf den Rechnerstart bezogene Optimierungsmaßnahmen finden Sie im voranstehenden Artikel.

Bootleistung und Hardware

Für den schnellen oder zähen Systemstart ist primär der Datenträger für die Systempartition, an zweiter Stelle der Prozessor verantwortlich. Moderne SSDs und Prozessoren garantieren bei Ubuntu & Co. schnelle Ankunft am Anmeldebildschirm: Zehn Sekunden und darunter sind das Ideal, 15 Sekunden sind auch mit nicht mehr ganz taufrischen Komponenten erreichbar.

An einer SSD kommen Anwender, die auf schnelle Bootzeiten und generell auf Systemleistung Wert legen, nicht vorbei. Aber es muss keine nach wie vor relativ teure SSD mit zwei, vier Terabyte oder mehr sein, die dann auch die kompletten Benutzerdaten aufnehmen soll: Ein Linux-System kommt dauerhaft mit 128 GB aus, sodass relativ günstige SSDs von 500 GB bis ein TB vollkommen ausreichen (50 bis 100 Euro). Für die Benutzerdaten kann dann eine langsame mechanische Festplatte dienen – eine sinnvolle Kombination, die man heute auch bei vielen Komplettangeboten antrifft.



Time-out ändern und gesprächiger Bootvorgang zur Fehleranalyse: Standardmäßig unterdrückt der „quiet"-Parameter die Startmeldungen. Der Time-out für Multiboot kann deutlich verkürzt werden.

Bootbremsen erkennen

Der Start von Ubuntu/Mint sollte je nach Hardware nicht länger als etwa 20 bis 40 Sekunden dauern, letzteres ohne SSD. Um eventuelle Bootbremsen zu erkennen, sollten Sie einen gesprächigen Bootvorgang erzwingen. Dauerhaft ist dies über die Datei „/etc/default/grub" möglich, indem Sie die Zeile mit dem Eintrag „quiet splash" mit dem Kommentarzeichen „#" deaktivieren. Eine einmalige Ad-hoc-Analyse erreichen Sie beim Systemstart, indem Sie „Erweiterte Optionen..." wählen und darunter den Eintrag mit dem Hinweis „recovery mode". Ebenfalls erhellend kann die Abfrage der Kernel-Meldungen mit

```
dmesg -T
```

sein, wobei Sie sich beim Booten die exakte Uhrzeit mit Sekundenangabe notieren sollten, wann der Boothänger auftritt. Dmesg zeigt nämlich die Zeit aller Systemereignisse sekundengenau, die Sie dann exakt zuordnen können.

Extrem lange Ladezeiten haben aber oft eine einfache Ursache, die sich relativ leicht beheben lässt: Sie sprechen für einen fehlerhaften Eintrag in der Datei „/etc/fstab", der entweder nach der Installation oder nach manuellem Editieren auftritt. Beweis dafür ist die Meldung „A start job is running for dev-disk-by...", die sich beim hängenden Start durch Druck der Esc-Taste offenbart oder durch einen Systemstart über „Erweiterte Optionen → recovery mode". Das System will eine Festplatte mounten, die es nicht vorfindet. Erste Abhilfe ist ein Auskommentieren der betreffenden Zeile in der „fstab" (mit „#"). Falls die Festplatte zwingend gemountet werden muss, ermitteln Sie mit *lsblk -f* die korrekte UUID-Kennung und tragen diese ein. Kontrollieren Sie auch den Mountpunkt, da auch ein nicht existierendes Mountverzeichnis Starthänger verursacht.

Bootloader-Wartezeit verkürzen

In Multiboot-Umgebungen wartet der Grub-Bootloader standardmäßig zehn Sekunden auf eine Auswahl, bis er das erste, oberste Default-System automatisch wählt. Vor allem dann, wenn man überwiegend dieses System nutzt, ist es sinnvoll, den Eintrag

`GRUB_TIMEOUT=10`
in der Datei „/etc/default/grub“ etwa auf „3“ (Sekunden) zu verkürzen und danach mit
`sudo update-grub`
die Bootumgebung neu zu initialisieren.

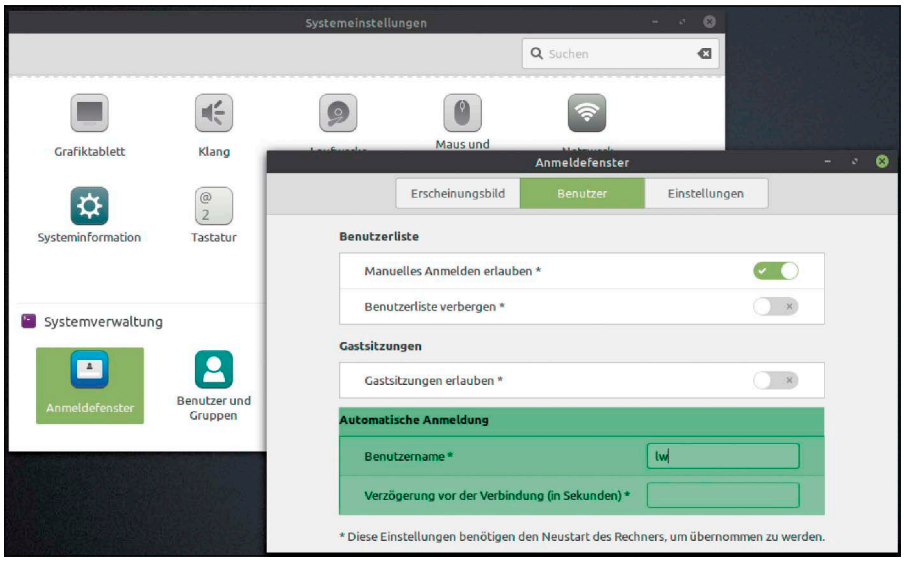
Vereinfachte Startvarianten

Folgende drei Lösungen starten zwar das System nicht schneller, es wird aber schneller benutzbar:

Luks-System ohne Systemanmeldung: Wenn ein Desktopsystem mit Datenträgerverschlüsselung installiert wurde, muss das Systemlaufwerk bei jedem Bootvorgang durch das Luks-Kennwort aufgesperrt werden. Dieser Zugangsschutz genügt, sodass die reguläre Systemanmeldung entfallen kann. Sie können daher eine automatische Anmeldung einrichten – etwa in Ubuntu unter „Systemeinstellungen → Details → Benutzer“, in Linux Mint unter „Anmeldefenster“. Um dadurch wirklich Zeit zu gewinnen, müssen Sie aber zusätzlich unter „Passwörter und Verschlüsselung“ (seahorse) nach Rechtsklick auf „Anmeldung“ und „Passwort ändern“ ein leeres Passwort definieren. Andernfalls wird der Schlüsselbund, der im Normalfall durch die Anmeldung geöffnet wird, jedes Mal nach dem Kennwort fragen.

Offenes System ohne Systemanmeldung: Ein PC zu Hause kann eventuell ebenfalls ohne Anmeldung zum Desktop durchstarten. Die Einrichtung erfolgt genauso wie oben bei Luks beschrieben. Auch hier muss das Schlüsselbund-Kennwort „leer“ sein, um ohne jede Abfrage loslegen zu können. Ein so eingerichtetes System verzichtet dann allerdings auf jeden Schutz von Konto und Passwortdaten.

PC in Dauerbereitschaft: Wer sein System jederzeit schnellstmöglich bedienen will, fährt es einfach gar nicht mehr herunter. Der einschlägige Ruhezustand nennt sich „Bereitschaft“ (technisch „Suspend to RAM“) und stellt nach Tastendruck oder Mausklick in wenigen (meist zwei bis drei) Sekunden den vorherigen Sitzungszustand wieder her. Wir messen für ein Notebook in „Bereitschaft“ ganze 0,7 Watt Stromverbrauch. Das wären kaum zwei Euro zusätzliche Stromkosten im ganzen Jahr, sofern Sie das Gerät überhaupt nicht mehr abschalten.



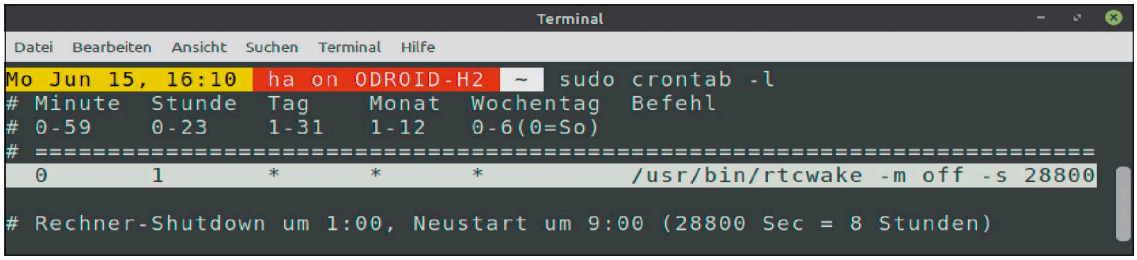
Auto-Log-in: Das lohnt sich zeitlich nur, wenn zusätzlich der Schlüsselbund ein leeres Passwort erhält. Jeder Kontenschutz entfällt damit, es sei denn, das System ist Luks-verschlüsselt.

Der automatische Systemstart

Bei relativ verlässlichen Nutzungszeiten eines Servers oder Desktop-PCs gibt es eine hübsche Alternative, sich um Shutdown und Neustart überhaupt nicht mehr zu kümmern. Das in der Regel vorinstallierte Linux-Tool rtcwake kann einen Rechner ausschalten (oder in einen Ruhezustand versetzen) und zur gewünschten Zeit wieder starten. Das „rtc“ im Namen steht für Real Time Clock und bezieht sich auf die physikalische Hardwareuhr. Diese läuft auch, wenn der Rechner komplett ausgeschaltet ist, und kann den Neustart auslösen, wenn ein definierter Zeitpunkt erreicht ist. Unter Linux ist dieser Zeitpunkt in der Datei „/sys/class/rtc/rtc0/wakealarm“ abgelegt.
Folgender Terminalbefehl
`sudo rtcwake -m off -s 60`
ist gut geeignet, um zu testen, ob die Hardware mitspielt (x86-Hardware praktisch immer, ARM-Rechner nicht immer). Der Schalter „-m“ bestimmt den ACPI-Modus. Mögliche Werte sind „standby“, „mem“, „disk“ oder „off“ (komplettes Ausschalten). Als zweiter Parameter ist hier „-s“ („seconds“) mit einer nachfolgenden Zeitangabe in Sekunden angegeben. Der obige Testbefehl wird also das System herunterfahren und nach einer Minute neu starten (60 Sekunden). Obwohl mit Schalter „-t“ („time) auch exakte Zeitangaben möglich ist, empfehlen wir, den geplanten Neustart immer mit Parameter „-s“ anzugeben. Es ist wenig Mühe, etwa zehn Stunden in Sekunden umzurechnen (10*3600=36 000).
Um Shutdown und Start zu automatisieren, kommt der Zeitplaner Cron ins Spiel: Nach dem Aufruf der Crontab-Editors mit
`sudo crontab -e`
schaltet folgender Eintrag

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

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

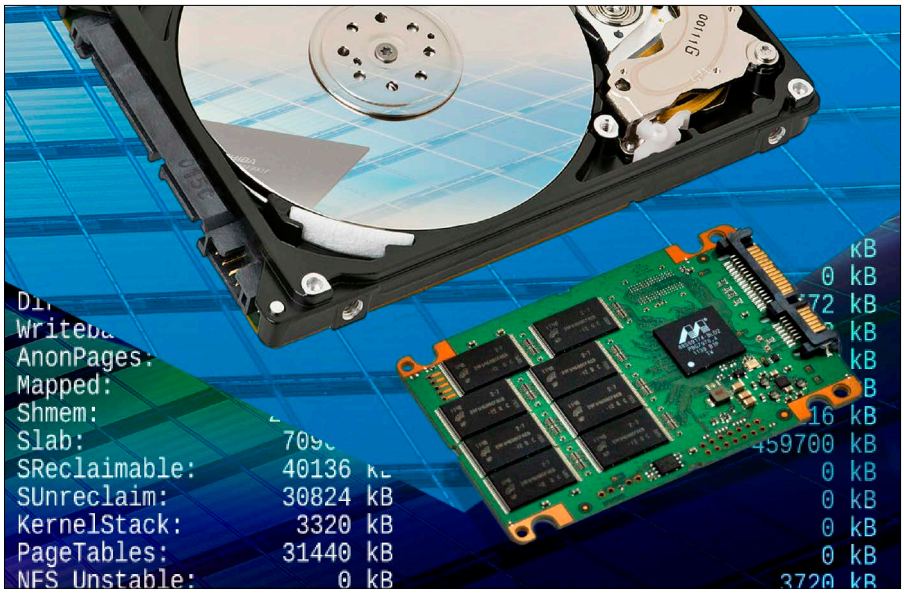


Das System läuft bereits, wenn Sie es brauchen: Das Tool rtcwake beendet und startet einen Rechner automatisch und erspart damit Wartezeiten.

Dm-Cache: Turbo mit Tücken

Auf Linux-Systemen mit hoher I/O-Auslastung kann eine SSD als manuell eingerichteter Cache langsame Festplatten über den Devicemapper beschleunigen. Der Dm-Cache ist eine vielversprechende, aber derzeit noch zu umständliche Methode.

VON DAVID WOLSKI



Dateiserver sind eine Paraderolle von Linux und es gibt mehrere Ansätze, langsamere Festplatten durch Flashspeicher als Cache zu beschleunigen. Im folgenden Artikel stellen wir den LVM-Cache vor, der einen Datenträgerverbund mit Cache über den Logical Volume Manager 2 (LVM2) erstellen kann. Diese Cacheform setzt eine LVM2-Partitionierung voraus – ein Datenträgersetup, das nicht gerade typisch ist für Linux-Systeme auf heimischen Servern oder Arbeits-PCs. Als Alternative gibt es die Möglichkeit, manuell über den Devicemapper einen Cache zusammenzusetzen. Diese Methode nennt sich „Dm-Cache" und ist auch die technische Grundlage für den LVM-Cache, verlangt aber bei der Einrichtung einige Schritte mehr in der Kommandozeile. Funktionsweise und Leistung sind aber identisch: Im Idealfall lassen sich so Geschwindigkeiten erreichen, die an hybride Festplatten heranreichen. Bis der Cache voll ist, entsprechen die Schreibgeschwindigkeiten jener einer SSD.

Der Nachteil des puristischen Dm-Cache soll nicht verschwiegen werden: Der Zusammenbau eines Caches auf einer SSD verlangt zwei Partitionen, eine für Cachedaten und eine weitere, sehr kleine für Metadateien. Deren Größen müssen manuell berechnet werden. Damit der Cache nach dem Systemstart aktiv wird, muss außerdem eine selbst geschriebene Systemd-Unit-Datei vorliegen. Bei einem zwischenzeitlichen Neustart bleibt der Cache aber erhalten, nach unseren Tests ohne Datenverlust. Es empfiehlt sich aber, den Cacheverbund immer komplett aufzulösen, damit das Dateisystem der Festplatte konsistent bleibt.

Konfiguration: Cache erstellen

Die Anleitung zeigt den Aufbau des Dm-Cache, die vorangehende Partitionierung einer SSD und die Berechnungen dazu. In diesem Beispiel erhält eine Festplattenpartition („/dev/sdd1") mit zwei TB eine SSD („/dev/sdb") mit 40 GB als Beiwagen. Die Festplatte wird dazu nicht neu formatiert und die Daten darauf bleiben intakt. Wichtig ist, dass die Festplatte stets ausgehängt ist, denn der Devicemapper wird ein neues, gecachtes Blockgerät als „/dev/mapper/[name]" erstellen, das ganz regulär eingehängt wird. Von den Daten auf der Festplatte muss ein lückenloses Backup bestehen – wie immer bei Eingriffen dieser Art. Die SSD muss für den Cache in zwei Partitionen unterteilt werden. Die aufgerundete Größe der kleineren der beiden Partitionen für Metadaten richtet sich ungefähr nach der Anzahl der Cacheblöcke zu 256 KB, die in das gesamten Cachelaufwerk passen. Dazu das Konfigurationsbeispiel unseres Testaufbaus:

1. Der Cache erwartet ein komplett leeres SSD-Laufwerk, das deshalb folgender Befehl mit Nullen überschreibt:

```
sudo dd if=/dev/zero of=/dev/sdb
```

2. Die Größe des gesamten Cachelaufwerks ermittelt dieser Befehl:

```
sudo blockdev --getsize64 /dev/sdb
```

3. Das Ergebnis (in Byte) wird durch die Blockgröße 262 144 (in Byte) geteilt, um die Anzahl der Cacheblöcke zu errechnen:

```
46137344000 / 262144 = 176000
```

4. Die Gesamtgröße der Metadaten-Partition ermittelt jetzt diese Formel

```
4 MB + 16 Byte * Cacheblöcke
```

und ergibt in diesem Beispiel eine Metadatengröße von 6,7 MB, aufgerundet 7 MB.

5. Nun wird auf der SSD eine kleine Partition mit sieben MB erstellt, hier auf „/dev/sdb1“, dann auf dem Rest der SSD eine zweite große Partition, in diesem Beispiel als „/dev/sdb2“. Dazu kann wahlweise der Partitionierer Gparted dienen oder auch fdisk in der Kommandozeile.

Festplatte und Cache zusammenfügen

Sind beide Partitionen auf der SSD erstellt, so gilt es, diese als Cache mit dem Befehl „dmsetup“ mit der Datenfestplatte zu verbinden. Dazu ist es nötig, die Größe der Festplatte in Sektoren zu ermitteln, was der Befehl

```
sudo blockdev --getsz /dev/sdd1
```

erledigt. In diesem Fall gibt das Kommando die Sektorzahl „1953521664“ zurück. Diese wird jetzt benötigt, um Festplatte und SSD-Partitionen zu einem Laufwerk zusammenzufügen:

```
sudo dmsetup create verbund --table
  '0 1953521664 cache /dev/sdb1 /
  dev/sdb2 /dev/sdd1 512 1 writeback
  default 0'
```

Die erste Zahl hinter der Null („--table ‚0 …“) muss der Sektorzahl der Festplatte entsprechen. Zudem ist die Reihenfolge der SSD-Partitionen wichtig. Es folgen nach der Angabe der Sektorenzahl der Festplatte erst die Metadaten auf „/dev/sdb1“, dann der eigentlich Cache mit „/dev/sdb2“ und schließlich das Festplattenlaufwerk mit „/dev/sdd1“. Das resultierende Blockgerät „verbund“ lässt sich dann mit

```
sudo mount /dev/mapper/verbund /
  mnt/verbund
```

in ein Zielverzeichnis, hier „/mnt/verbund“, einhängen und wie gewohnt beschreiben. Der Cache ist nun permanent und überdauert auch einen Neustart. Die beiden Befehle zum Erstellen und Einhängen des gecachten Laufwerks sind aber nach jedem Neustart notwendig.

Ohne Cache: Den Verbund auflösen

Um einen Verbund von Festplatte und SSD wieder komplett aufzulösen, also die Festplatte allein zu verwenden, muss das Cachelaufwerk komplett geleert sein. Ansonsten enthält die Festplatte „/dev/sdd1“ kein konsistentes Dateisystem. Es ist vor allem dieser Punkt, der Dm-Cache in der Praxis unhandlich macht, da es noch keine Tools zur Automatisierung dieser Schritte gibt: Zuerst hält

```
sudo umount /dev/mapper/verbund
sudo dmsetup suspend verbund
```

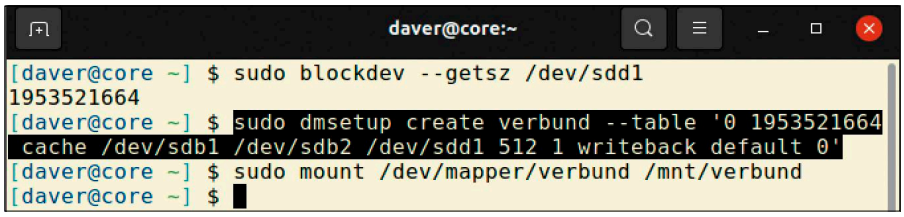
den Cache an und die beiden Kommandos

```
sudo dmsetup wipe_table verbund
sudo dmsetup wait verbund
```

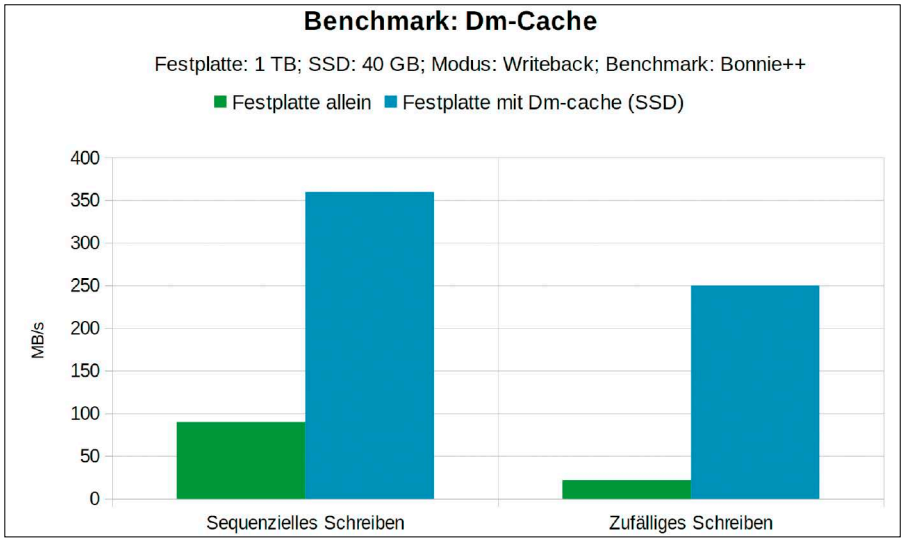
leeren den Cache auf die Festplatte. Schließlich entfernen die Kommandos

```
sudo dmsetup clear verbund
sudo dmsetup remove verbund
```

die SSD aus dem Verbund. Die Festplatte ist dann wieder allein benutzbar.



Cacheverbund mit „dmsetup“ zusammenfügen: Für die einzelnen Befehle gibt es noch keine Hilfsanwendungen, die den Weg zum gecachten Blockgerät vereinfachen.



Dm-Cache: Licht und Schatten

Zwar ist ein Cache immer eine gute Idee, doch macht die manuelle Einrichtung eines Dm-Cache diese Methode im Vergleich zum verwandten LVM-Cache wenig attraktiv. Die Berechnung der korrekten Parameter, das Zusammensetzen des gecachten Laufwerks sind aufwendig und die Notwendigkeit eines Ausleerens des Caches vor Neustarts und Herunterfahren des Systems eine zusätzliche Hürde – keine geringe, denn bei verworfenen Cacheinhalten droht Datenverlust. Dieser Umstand macht Dm-Cache trotz erheblichen Geschwindigkeitsgewinns weniger praktikabel als LVM-Cache. Es fehlen ein ausgereiftes Front-End und ein passender Systemd-Dienst in den Linux-Distributionen. Erst damit hätte der Dm-Cache ohne LVM2 und Konsolenakrobatik Potenzial für Linux-Systeme aller Art. ■

DM-CACHE: PRO UND CONTRA

+ benötigt keinen LVM-Verbund von Festplatte und SSD
+ ähnliche Beschleunigungsraten wie LVM-Cache
+ lässt sich jederzeit aktivieren und deaktivieren

– arbeitet nur als „Hot-Spot“-Cache für wiederholte Dateizugriffe
– anspruchsvollere Einrichtung als der LVM-Cache
– verlangt einen Systemd-Dienst zum Aktivieren und Deaktivieren

Festplatten mit SSD-Cache

Auf schwer arbeitenden Linux-Systemen mit hoher I/O-Last ist es immer von Vorteil, Festplattenzugriffe zu beschleunigen. Ein SSD-Cache mit LVM2 ist eine moderne Möglichkeit, HDDs über ein Flash-Laufwerk schneller zu machen.

VON DAVID WOLSKI

Unter den lohnenden Aufrüstungsmöglichkeiten für jedes System steht immer noch der Einbau einer SSD bei der zu erwartenden Leistungsverbesserung ganz vorne. Einst waren SSDs und NVME-Laufwerke klein, teuer, wenn auch schon immer angenehm schnell. Schneller Flash-Speicherplatz ist seit 2020 auch in größeren Portionen erschwinglich: So kostet eine SSD mit einer Speicherkapazität von einem TB gegenwärtig etwa 90 Euro (Stand Sommer 2021). Für ältere, kleinere SSDs zwischen 40 und 64 GB wird es dagegen schwerer, einen Verwendungszweck außer als Systempartition oder als Datenspeicher zu finden. Für ernstzunehmende Datenpartitionen reicht der Platz nicht. Aber es gibt eine ansprechende Verwendungsmöglichkeit für ältere SSD- oder NVME-Laufwerke als Cache für größere, langsame Festplatten oder für Raid-Systeme. Das Resultat ist ein Verbund, in welchem das schnelle Flash-Laufwerk als vorgelagerter Speicher für Lese- und Schreiboperationen fungiert. Im Idealfall lassen sich so die Geschwindigkeiten deutlich steigern.

Cache inklusive: Logical Volume Manager 2

Linux-Entwickler machten in den letzten zehn Jahren schon mehrere Ansätze, SSDs als Cache einzuspannen: Flashcache ist eine Entwicklung Facebooks zum Beschleunigen der eigenen Datenbankserver. Es wurde nie in den offiziellen Linux-Kernel aufgenommen, was die die Einrichtung zu einem unerfreulich komplexen Unterfangen macht. Ein anderer Kandidat ist Bcache, das als optionale Cachetechnik für Partitionen seit Linux Kernel 3.10 als Modul vertreten ist. Leider gab es seitdem wenig Weiterentwicklung und sogar Probleme, die zu Datenverlust führen können. Folglich gilt Bcache derzeit nicht mehr als attraktive Lösung.

Eine moderne Cachefunktion, die jener von Bcache ähnlich ist, dabei aber performanter, ausgereifter und einfacher konfigurierbar, ist im Logical Volume Manager 2 enthalten. Der LVM2 gehört unter jeder Linux-Distribution zum Standard-Repertoire, auch wenn nicht alle Distributionen dessen Methoden zur Festplattenverwaltung nutzen. Dennoch funktioniert diese Cachemethode in allen aktuellen Linux-Distributionen ohne zusätzliche Kernel-Module. Auch ist die Einrichtung nicht destruktiv – was bedeutet, dass sich ein schnelles Flash-Laufwerk zu einem vorhandenen LVM2-Setup ohne Neuformatierung hinzufügen und auch wieder ohne Datenverlust entfernen lässt. An Cachemethoden gibt es „Writethrough“, bei der nur Lesevorgänge zwischengespeichert werden, sowie „Writeback“. Letzteres ist ein Schreibcache, der zuverlässige SSDs voraussetzt. Denn ein defekter Datenträger wäre als Schreibcache für die Daten fatal, selbst wenn die Festplatten dahinter ein Raid1-Verbund sind. Allerdings können auch mehrere SSDs als cachendes Raid1 arbeiten – dank den Fähigkeiten von LVM2 gibt es da keine Einschränkungen.

Einen Pferdefuß gibt es aber: Die großen Distributionen wie Debian, Ubuntu und deren Abkömmlinge wie Mint haben einen Grub2-Bootloader, der den Boot von einem gecachten LVM2-Verbund nicht unterstützen. Eine bestehende Ubuntu-Installation,

die per Standard im Ubuntu-Installer auf der LVM2-Gruppe „vgubuntu“ eingerichtet wird, kann leider nicht mit einem hinzugefügten Cache umgehen (Stand Ubuntu 20.04). Der LVM2-Cache eignet sich also nur für LVM2-Gruppen mit Datenpartitionen, aber nicht die Systempartition.

Praxis: Festplatte plus SSD-Cache

In unserem Beispiel erhält ein Ubuntu-System eine neue LVM2-Gruppe namens „vgdata“ mit einer langsamen Festplatte (1 TB) als einzigen Datenspeicher, dem ein SSD-Laufwerk (40 GB) als Cache Beine machen soll. Die Festplatte hat hier die Laufwerkskennung „/dev/sdb“ und die SSD „/dev/sdc“. Alle Konfigurationsschritte finden im Terminal statt, mit den üblichen, vorinstallierten Tools von LVM2, die in Ubuntu standardmäßig vorhanden ist.

1. Festplatte vorbereiten: Gibt es schon eine LVM2-Gruppe mit Datenfestplatte(n), also ohne die Systempartition, so überspringt man diesen gesamten Schritt 1. Ansonsten initialisiert das Kommando

```
sudo pvcreate /dev/sdb
```

eine leere Festplatte für LVM2 als physikalisches Volumen (PV), das gleich im Anschluss einen SSD-Cache bekommen soll. Der Befehl

```
sudo vgcreate vgdata /dev/sdb
```

erstellt eine neue Volumengruppe (VG) namens „vgdata“ und

```
sudo lvcreate -n lvdata -l 100%FREE
  vgdata /dev/sdb
```

legt wieder ein logisches Volume (LV) darauf an, das hier den Namen „lvdata“ erhält. Das logische Volume ist erst mal leer. Deshalb erstellt nun der Befehl

```
sudo mkfs.ext4 /dev/vgdata/lvdata
  -L lvdata
```

ein Ext4-Dateisystem darauf. Ab jetzt kann man dieses Volume im Dateimanager und auf der Kommandozeile einhängen und wie eine gewöhnliche Festplatte nutzen.

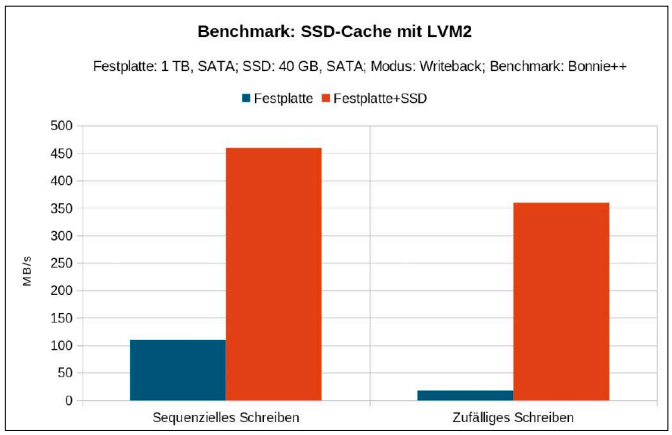
2. SSD vorbereiten: Ab jetzt gehen wir davon aus, dass eine Volumengruppe „vgdata“ und ein logisches Volume (LV) „lvdata“ bestehen und dort bereits Daten gespeichert sind, die natürlich nicht verloren gehen sollen. Die SSD mit der Laufwerkskennung „/dev/sdc“ wird aber neu initialisiert:

```
sudo pvcreate /dev/sdc
```

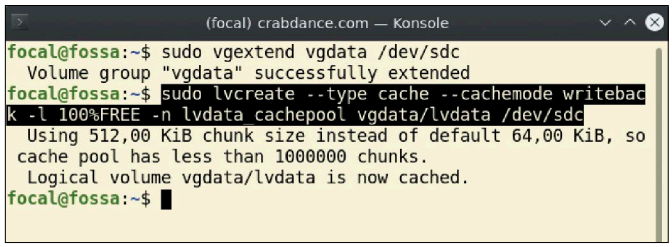
Dann erweitert das Kommando

```
sudo vgextend vgdata /dev/sdc
```

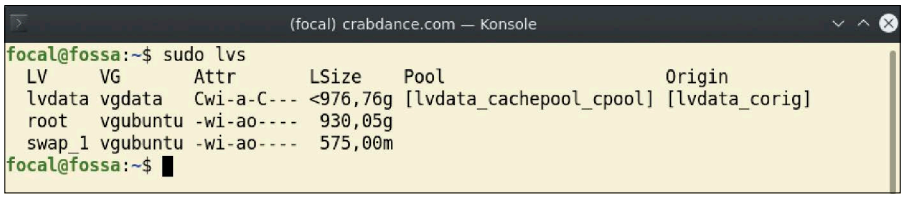
die Volumengruppe um die SSD – ohne Datenverlust auf der Festplatte.



Vergleich der Schreiboperationen auf Festplatte mit und ohne SSD-Cache: Im Modus „Writeback“ liefert der Cache von LVM2 eine signifikante Verbesserung des Datendurchsatzes.



Cache hinzuschalten: Dank LVM2 ist die Cachekonfiguration recht unkompliziert und kann auch im laufenden Betrieb erfolgen. Alle Daten des logischen Volumes bleiben erhalten.



Aktiver Cache für das logische Volumen „lvdata“: Leider kann Grub 2 als Bootloader nicht mit einer Systempartition plus LVM2-Cache umgehen, deshalb ist der Cache für „root“ nicht aktiviert.

3. Den Cache aktivieren: In diesem Fall arbeiten wir mit den Standardeinstellungen von LVM2 zum Anlegen eines Caches und verzichten auf die diversen Parameter zur Optimierung. Nach der Eingabe von

```
sudo lvcreate --type cache
  --cachemode writeback -l 100%FREE
  -n lvdata_cachepool vgdata/lvdata
  /dev/sdc
```

gehört die SSD als Cache zu „lvdata“. In diesem Fall im Modus „writeback“, der Lese- und Schreibaktionen zwischenspeichert. Eine sichere, wenn auch weniger performante Methode ist „writethrough“, die den Cache nur für Leseoperationen nutzt und direkt auf die Festplatte(n) schreibt.

Benchmarks und Fazit

Ein Lesecache mit („Writethrough“) ist nicht in allen Anwendungsfällen sinnvoll. Auf einem Desktopsystem mit vielen zufälligen Leseoperationen bringt der LVM2-Cache nach unseren Messungen nichts und Schreibaktionen sind unter Umständen sogar langsamer als eine Festplatte alleine. Diese Cachemethode ist für Server gemacht, die in schneller Folge stets die gleichen Dateien liefern sollen, was beispielsweise mit Git und Datenbanken aller Art der Fall ist. Ganz anders verhält es sich mit dem Schreibcache („Writeback“) von LVM2: Nach unseren Messungen sind Schreibaktionen bis zu viermal schneller als bei der Festplatte alleine.

LVM2 und dessen Tools in der Shell sind keine leichte Kost, weder für Anwender noch für Linux-Admins. Der Lohn einer Einarbeitung sind die überzeugende Performance des Writeback-Cache und die Flexibilität von LVM2 im Datenträgermanagement. Möchte man die SSD wieder ausbauen, so deaktiviert einfach der Befehl

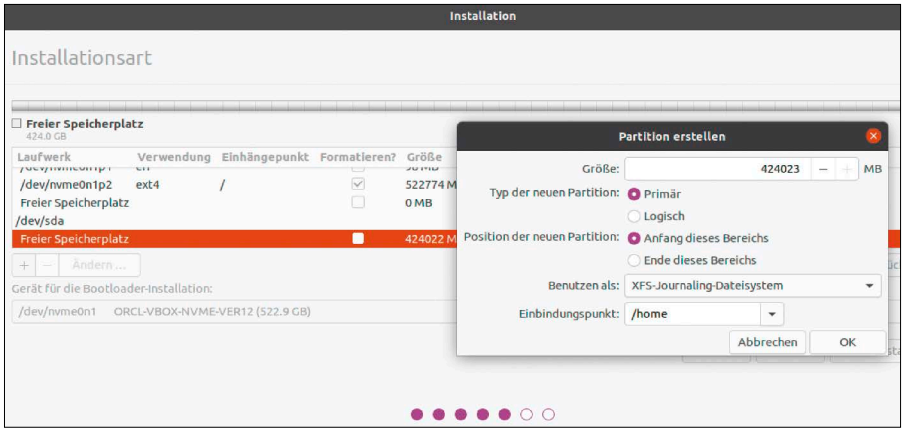
```
sudo lvconvert --uncache vgdata/
  lvdata
```

den Cache auf „lvdata“. Die dort gespeicherten Daten bleiben erhalten und die Aktion ist im Betrieb bei einem eingehängten Dateisystem auf „lvdata“ möglich. ■

Langlebiges Home-Verzeichnis

Partitionen lassen sich auch anders aufteilen, als das Setuptool bei der Installation standardmäßig vorschlägt. Insbesondere bietet eine separate Home-Partition Vorteile für nachhaltige Nutzerdaten trotz Neuinstallation.

VON THORSTEN EGGELING



Separates Home: Bei einer Neuinstallation lässt sich eine eigene Partition für die Home-Verzeichnisse konfigurieren. Die lässt sich dann bei späterer Neuinstallation wieder einbinden.

Bei der Linux-Installation gibt es viele mögliche Varianten. Distributionen wie Open Suse bieten beim „Geführten Setup" eine separate Home-Partition an. Ubuntu und Linux Mint gehen eher den konservativen Weg. Das gesamte System und auch die Home-Verzeichnisse werden standardmäßig gemeinsam auf einer Ext4-Partitition installiert. Die Trennung von System und Home-Verzeichnissen ist aber ebenfalls möglich und bietet Vorteile für die Datensicherheit und bei einer Neuinstallation des Systems.

Vorteile einer separaten Home-Partition

In aktuellen PCs stecken oft eine SSD mit relativ wenig Speicherplatz und eine deutlich größere Festplatte. Bei solcher Konfiguration ist es sinnvoll, das Home-Verzeichnis auf eine eigene Partition auszulagern. Die SSD gelangt dann wohl kaum an die Grenze ihrer Kapazität und die Festplatte bietet Platz auch für umfangreiche Datensammlungen. Das System startet von der SSD trotzdem sehr schnell und die Festplatte wirkt kaum als Bremse.

Bei allen PCs und Notebooks, auch mit nur einem Laufwerk, bietet die separate Home-Partition ebenfalls Vorteile. Bei einer Neuinstallation des Systems lässt sich die Partition einbinden, die Dateien darin bleiben erhalten und die Konfiguration von Programmen wie Thunderbird und Firefox sowie der Desktopumgebung steht sofort wieder zur Verfügung. Das funktioniert in der Regel auch, wenn man eine neuere oder sogar andere Distribution installiert. Die Desktopeinstellungen werden jedoch nur bei gleicher Desktopumgebung übernommen.

Ein Backup des Home-Verzeichnisses sollten Sie regelmäßig erstellen und bei Bedarf getrennt davon auch des gesamten Systems (siehe Artikel ab Seite 68). Eine eigene Home-Partition bietet dabei keinen Vorteil. Anders sieht es aus, wenn die vielleicht ältere Festplatte Fehler meldet und wahrscheinlich bald ausfällt. Sie können die Home-Partition oder deren Inhalt einfach auf eine neue Festplatte kopieren und diese in das Dateisystem einhängen (siehe nächste Seite).

Home-Partition bei der Neuinstallation

Wir gehen davon aus, dass Sie Ubuntu 20.04 neu auf einem Computer mit einem oder zwei unbenutzten Laufwerken installieren möchten. Bei Linux Mint läuft es entsprechend ab, andere Distributionen bieten ähnliche, aber meist abweichend bezeichnete Optionen.

Schritt 1: Booten Sie den Computer vom Installationsmedium und rufen Sie das Ubuntu Setuptool auf. Folgen Sie den Anweisungen des Assistenten. Im Dialog „Installationsart" wählen Sie die Option „Etwas Anderes" für die manuelle Partitionierung.

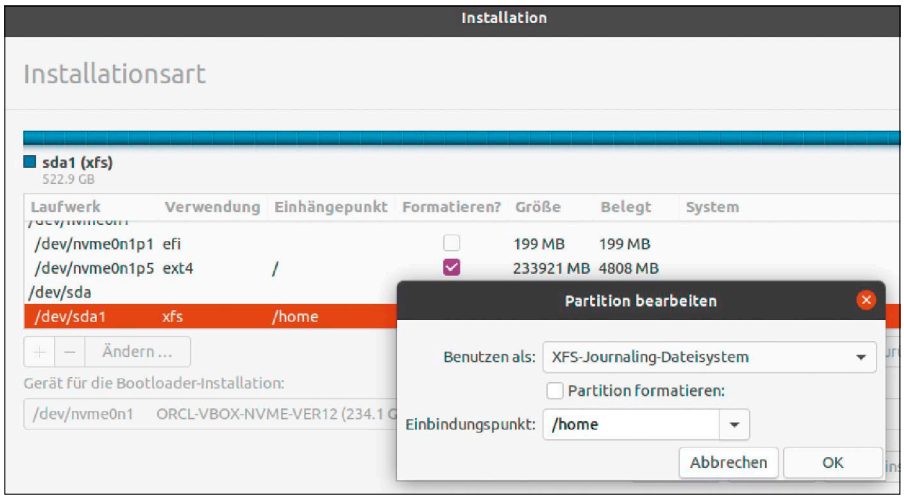
Schritt 2: Wählen Sie das Laufwerk, auf dem Sie das Betriebssystem installieren möchten. Sollten sich darauf Partitionen befinden, löschen Sie diese über die „-"-Schaltfläche. Oder Sie klicken auf „Neue Partitionstabelle", um alles auf einmal zu löschen. Alle bisherigen Daten auf der Festplatte gehen dabei verloren.

Schritt 3a: Wenn nur eine Festplatte zur Verfügung steht, klicken Sie auf „Freier Speicherplatz" und legen darin über die „+"-Schaltfläche neue Partitionen an. Bei einem Uefi-PC beginnen Sie mit einer „EFI-System-Partition", für die 100 MB ausrei-

chen. Danach folgt die Systempartition mit dem Dateisystem Ext4. Die Größe hängt vom Laufwerk ab. 50 GB sollten für einen Arbeitsrechner ausreichen. Wählen Sie hinter „Einbindungspunkt“ den Eintrag „/“.
Als Nächstes erstellen Sie die Home-Partition mit dem Einbindungspunkt „/home“ und dem Dateisystem Ext4. Alternativ können Sie auch XFS verwenden, was teilweise zu einer besseren Leistung führen kann. Deutlich spürbar ist das aber in der Regel nicht. Das Home-Verzeichnis kann den verbleibenden Platz auf der Festplatte füllen oder Sie lassen noch etwas Raum für eine Swappartition mit der Größe des eingebauten RAM. Auf einer SSD und mit genügend Hauptspeicher ist das nicht zwingend erforderlich.
Schritt 3b: Bei zwei Laufwerken gehen Sie wie in Schritt 3a vor, erstellen aber die Home-Partition mit dem Einbindepunkt „/home“ auf der anderen Festplatte beziehungsweise SSD.
Schritt 4: Klicken Sie auf „Jetzt installieren“, prüfen Sie die Partitionierung und klicken Sie auf „Weiter“. Danach absolvieren Sie die weiteren Schritte des Assistenten und starten abschließend das neu installierte Ubuntu.

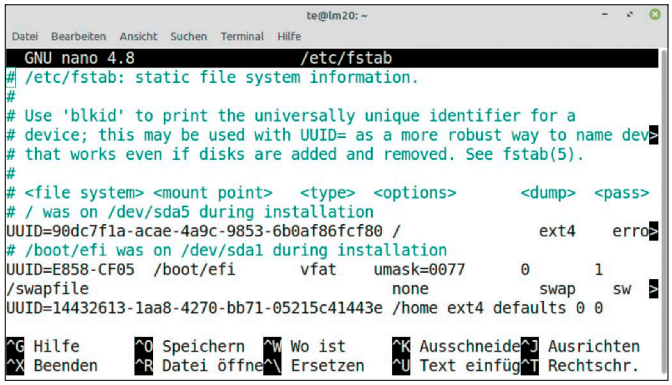
Neuinstallation mit vorhandener Home-Partition

Sollte eine Neuinstallation nötig oder gewünscht sein, verwenden Sie unter „Installationsart“ wieder „Etwas Anderes“. Klicken Sie die Systempartition an und dann auf „Ändern“. Wählen Sie hinter „Benutzen als:“ den Eintrag „Ext4-Journaling-Dateisystem“, als Einbindepunkt geben Sie „/“ an und setzen ein Häkchen vor „Partition formatieren“. Sie können auf die Formatierung auch verzichten. Dann wird eine Art Reparaturinstallation durchgeführt, bei der aber Verzeichnisse wie „/etc“, „/usr“ und „/var“ gelöscht werden. Zusätzliche Software müssen Sie danach neu installieren. Bei einem defekten System ist diese Methode der Reparatur jedoch einen Versuch wert. Erstellen Sie aber vorher ein Backup.
Bei der Home-Partition wählen Sie das zuvor genutzte Dateisystem und als Einbindepunkt „/home“. Das Häkchen vor „Partition formatieren“ darf nicht gesetzt sein. Nach einem Klick auf „Jetzt installieren“ prüfen Sie genau, dass die Home-Partition tatsächlich nicht neu formatiert wird. Klicken Sie auf „Weiter“ und fahren Sie mit der Installation fort.



Ohne Datenverlust: Achten Sie darauf, dass bei einer Neuinstallation kein Häkchen vor „Partition formatieren“ gesetzt ist, damit die Dateien auf der Home-Partition erhalten bleiben.

Home-Partition einbinden: In der Datei „/etc/fstab“ geben Sie an, welche UUID und welches Dateisystem die neue Partition besitzt und wo diese eingehängt werden soll („/home“).



Home-Partition nachträglich einbinden

Bei einer schon bestehenden Installation lässt sich das Home-Verzeichnis jederzeit auf eine eigene Partition auslagern. Über ein Tool wie Gparted (*sudo apt install gparted)* verkleinern Sie vorhandene Partitionen, um Platz dafür zu schaffen, oder Sie erstellen eine neue Home-Partition auf einer zweiten Festplatte.
Schritt 1: Ermitteln Sie zunächst im Terminal mit dem Befehl

```
blkid
```

die UUIDs der Partitionen.
Schritt 2: Öffnen Sie die Konfigurationsdatei für die Einbindung der Partitionen in einem Editor:

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

Fügen Sie folgende Zeile an:

```
UUID=[ID] /home ext4 defaults 0 0
```

Den Platzhalter „[ID]“ ersetzen Sie durch die zuvor ermittelte UUID der neuen Home-Partition. Setzen Sie „xfs“ statt „ext4“ ein, falls Sie XFS bei der Formatierung verwendet haben.
Schritt 3: Schließen Sie alle Anwendungen und beenden Sie die grafische Oberfläche. Ubuntu-Nutzer (20.04) verwenden dann

```
sudo service gdm3 stop
```

und Benutzer von Linux Mint 20 den folgenden Befehl:

```
sudo service lightdm stop
```

Drücken Sie Alt-F2, um eine Textkonsole einzublenden, bei der Sie sich anmelden.
Schritt 4: Benennen Sie „/home“ um und legen Sie ein neues Verzeichnis an:

```
sudo mv /home /home.bak
sudo mkdir /home
```

Schritt 5: Binden Sie die neue Home-Partition ein und kopieren Sie alle Dateien:

```
sudo mount -a
sudo rsync -aXS /home.bak/ /home/
```

Achten Sie auf die abschließenden Slash-Zeichen („/“). Starten Sie Linux mit

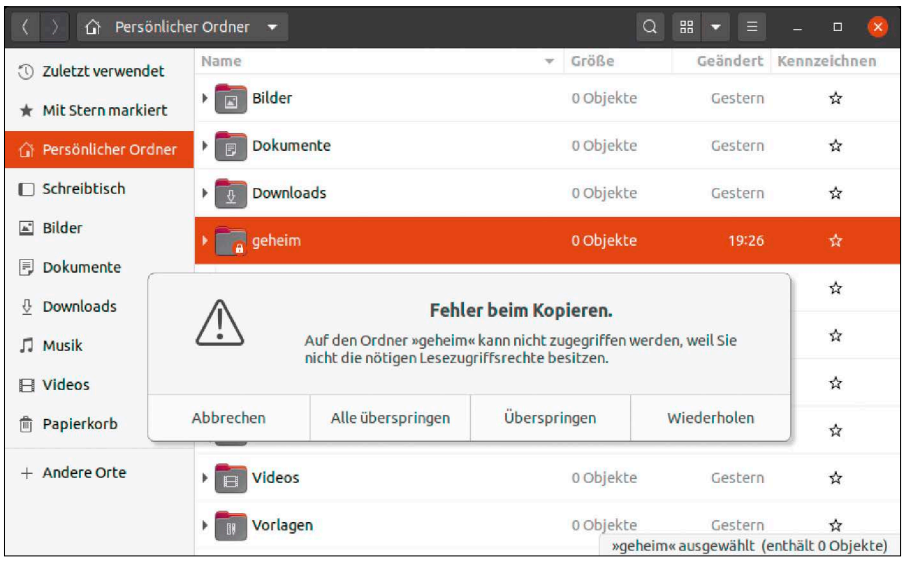
```
sudo reboot
```

neu. Das System verwendet jetzt die neue Partition für das Home-Verzeichnis. Die alten Dateien in „/home.bak“ können Sie danach löschen oder als Sicherungskopie aufbewahren. ■

Probleme mit Zugriffsrechten

Wenn sich ein Ordner nicht öffnen oder ein Programm nicht starten lässt, liegt meist ein Problem mit den Rechten im Dateisystem vor. Die lassen sich aber schnell anpassen.

VON THORSTEN EGGELING



Zugang verweigert: Wenn die Zugriffsrechte fehlen, meldet der Dateimanager beim Kopieren einen Fehler. Beim Öffnen des Ordners wird das root-Passwort für höhere Rechte angefordert.

Was ein Nutzer unter Linux darf, ist klar geregelt. Unbeschränkte Rechte gibt es im eigenen Home-Verzeichnis und sonst nur in wenigen anderen Ordnern. Das sorgt für maximale Sicherheit. Verwendet man sudo oder ein root-Konto, gilt dagegen maximale Unsicherheit. Denn der administrative Nutzer darf alles. Deswegen gilt die Regel, nur tatsächlich notwendige Aktionen mit administrativen Rechten durchzuführen. Andernfalls besteht die Gefahr, dass Zugriffsrechte so geändert werden, dass ein Standardnutzer bestimmte Ordner oder Dateien nicht mehr öffnen kann. Die typischen Zugriffsprobleme lassen sich aber auch schnell wieder beheben.

Geltende Rechte ermitteln

Unter Linux gehören Ordner und Dateien einem Benutzer („Besitzer“) und einer Gruppe. Die eigenen Dateien unter „/home/[User]“ beispielsweise gehören dem Benutzer „[User]“ und der gleichnamigen Gruppe. Der Platzhalter „[User]“ entspricht dem von Ihnen gewählten Benutzernamen. Für jedes Element im Dateisystem lassen sich Lese- und Schreibrechte vergeben, getrennt nach Besitzer und Gruppe. Zudem gibt es das Recht „Ausführen“. Ist es bei einer Datei gesetzt, darf ein Benutzer sie als Programm starten. Bei Ordnern gewährt es die Berechtigung, ihn zu öffnen beziehungsweise den Inhalt anzusehen. Außerdem lassen sich Rechte für „Andere“ festlegen. Damit sind Zugriffe von Benutzern gemeint, die weder Eigentümer sind noch zu der Gruppe gehören.

Im Terminal lassen sich die Zugriffsrechte schnell ermitteln.

Der Befehl

```
ls -al
```

zeigt Besitzer und Gruppe aller Elemente im aktuellen Verzeichnis an. In der ersten Spalte sind die Rechte mit „r“, „w“ und „x“ (lesen, schreiben, ausführen) zu finden, in der Reihenfolge „Besitzer“, „Gruppe“ und „Andere“. Der erste Buchstabe ist ein „d“, wenn es sich um einen Ordner handelt („Directory“), bei Dateien steht ein „-“.

Der Ausgabe „drwxr-x---“ beispielsweise ist zu interpretieren als: lesen („r“), schreiben („w“) und ausführen/suchen („x“) für den Besitzer. Die Gruppe darf lesen sowie ausführen/suchen („r-x“), „Andere“ haben keinen Zugriff („---“).

Zugriffsrechte im Terminal festlegen

Mit dem Befehl chmod ändern Sie die Zugriffsrechte im Terminal:

```
chmod o+rx /home/[User]
```

„Andere“ („o“), also alle Benutzer des PCs, dürfen dann auf das Home-Verzeichnis von „[User]“ zugreifen und Dateien lesen. Bei Ubuntu und Linux Mint ist das bereits der Standard. Mit

```
chmod o-rx /home/[User]
```

entziehen Sie „Anderen“ die Zugriffsrechte. Die anderen Benutzer des PCs können das Home-Verzeichnis von „[User]“ dann nicht mehr öffnen. Entsprechend setzen Sie statt „o“ die Buchstaben „u“ für Benutzer und „g“ für Gruppe ein.

```
chmod g+rw /home/[User]/Datei.txt
```

beispielsweise gibt der Gruppe Lese- und Schreibzugriff für eine Datei.

Wenn Sie die Rechte für Dateien/Ordner ändern möchten, die nicht Ihnen gehören, stellen dem Befehl ein „sudo“ voran.

Besitzer und Gruppe festlegen: Der Besitzer und die Gruppe einer Datei lassen sich

mit chown ändern. Die allgemeine Form lautet folgendermaßen:

```
chown [User]:[Gruppe] [Datei/
 Ordner]
```

Zusätzlich gibt es auch chgrp, womit sich nur die Gruppe ändern lässt. Die Befehle chmod, chgrp und chown kennen die zusätzliche Option „-R“. Der Befehl

```
sudo chown -R sepp:sepp /home/sepp
```

ändert bei allen Elementen unterhalb des angegebenen Pfades den Besitzer und die Gruppe auf „sepp“.

Das ist beispielsweise nützlich, wenn Sie fälschlich mit sudo im Home-Verzeichnis gearbeitet haben und dem Benutzer danach Zugriffsrechte fehlen.

Rechte für Dateien und Ordner ändern: Der Befehl chmod unterscheidet nicht zwischen Dateien und Verzeichnissen. Wendet man den Befehl rekursiv auf eine Ordnerstruktur an, kann das unerwünschte Auswirkungen haben. Verzeichnisse beispielsweise lassen sich nicht mehr öffnen, wenn man ihnen die Berechtigungen „Ausführen/Suchen“ entzieht. Um im aktuellen Ordner inklusive Unterordnern nur den Dateien Lese- und Schreibrecht für Besitzer und Gruppe zuzuweisen, verwenden Sie diesen Befehl

```
find . -type f -exec chmod ug+rw {}
 \;
```

Soll chmod nur auf Verzeichnisse angewandt werden, benutzen Sie beispielsweise

```
find . -type d -exec chmod ugo+x {}
 \;
```

Damit setzen Sie bei allen Ordnern „Ausführen/Suchen“ für „Besitzer“, „Gruppe“ und „Andere“.

Rechte im Dateimanager setzen

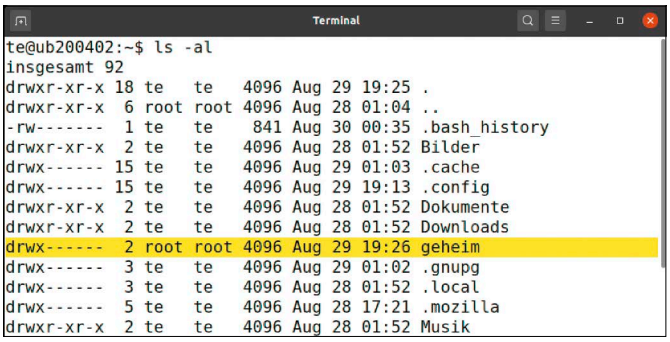
Welche Rechte für einen Ordner oder eine Datei gelten, lässt sich auch über den Dateimanager ermitteln und ändern. Klicken Sie ein Element im Dateisystem mit der rechten Maustaste an und wählen Sie „Eigenschaften“. Auf der Registerkarte „Zugriffsrechte“ sehen Sie die geltenden Rechte, die Sie auch ändern können. Bei Programmen, die Sie aus dem Internet heruntergeladen und entpackt haben, setzen Sie ein Häkchen vor „Datei als Programm ausführen“, damit sich die Anwendung starten lässt.

Über die Schaltfläche „Zugriffsrechte der enthaltenen Dateien ändern“, lassen sich unter Ubuntu bei Ordnern die Rechte rekursiv für alle enthaltenen Elemente in einem eigenen Dialog setzen – für „Besitzer“, „Gruppe“ und „Andere“ jeweils getrennt für die enthaltenen Dateien und Ordner.

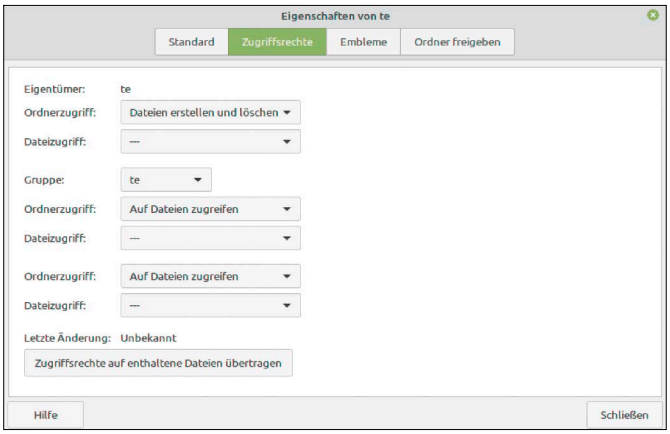
Bei Linux Mint funktioniert die Rechtevergabe über den Dateimanager Nemo ähnlich. Das Fenster „Eigenschaften→ Zugriffsrechte“ sieht nur etwas anders aus. Es gibt die drei Rubriken „Eigentümer“, „Gruppe“ und „Andere“, bei der letzten fehlt allerdings die Beschriftung. Hinter „Ordnerzugriff“ stellen Sie wie bei Ubuntu die Zugriffsrechte ein. Zusätzlich gibt es Auswahlfelder hinter „Dateizugriff“. Die Einstellungen gelten für alle Unterordner und Dateien, wenn Sie auf „Zugriffsrechte auf enthaltene Dateien übertragen“ klicken.

Sie können die Zugriffsrechte nur ändern, wenn Sie Besitzer des Elements sind. Andernfalls müssen Sie den Dateimanager als administrativer Benutzer starten. Das geht am einfachsten, indem Sie unter Ubuntu das Paket „nautilus-admin“ installieren. Melden Sie sich danach beim System ab und wieder an.

Im Kontextmenü von Ordnern finden Sie jetzt den neuen Eintrag „Als Systemverwalter öffnen“, bei Dateien gibt es „Als Systemverwalter bearbeiten“. Der Mint-Dateimanager Nemo bietet „Als Systemverwalter öffnen“ bereits standardmäßig an, der entsprechende Kontextmenüpunkt bei Dateien fehlt jedoch. ■



Welche Rechte gelten? Im Terminal gibt „ls -al“ Auskunft über Besitzverhältnisse und Zugriffsrechte. chmod und chown können Besitz- und Zugriffsrechte bei Bedarf ändern.



Nemo: Linux Mint bietet eine komfortable Oberfläche für die Zugriffsrechte. Datei- und Ordnerrechte lassen sich getrennt einstellen und auf enthaltene Dateien übertragen.

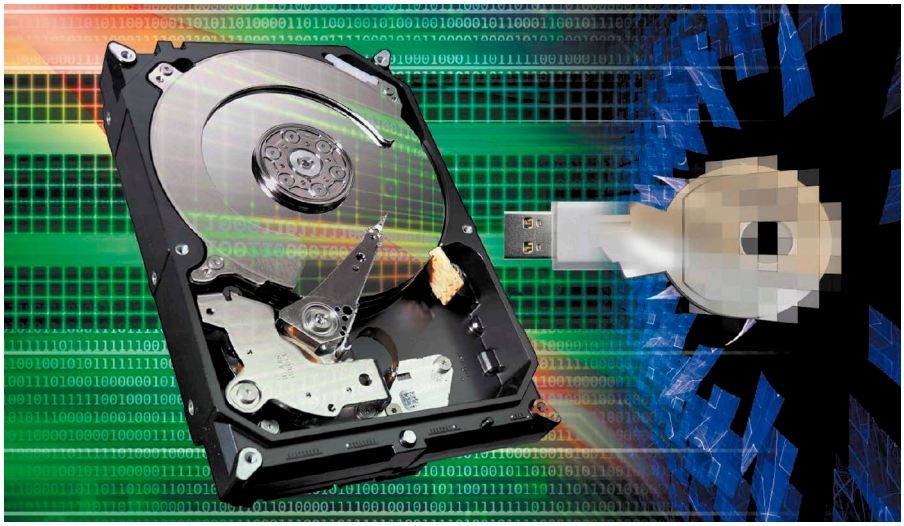
RECHTE FÜR SNAP-APPS

Eine Besonderheit gibt es bei Snap-Apps, die unter Ubuntu in einem Softwarecontainer laufen. Auf den ersten Blick gibt es keinen Unterschied zu herkömmlich installierten Programmen. Je nach Konfiguration kann es aber sein, dass eine Anwendung beispielsweise keinen Zugriff auf einen USB-Stick hat, obwohl dieser sonst über den Dateimanager möglich ist. Sie kontrollieren die Rechte, indem Sie „Ubuntu Software“ starten und nach der Snap-App suchen, beispielsweise nach Gimp. Bei Snap-Apps sehen Sie die Schaltfläche „Permissions“, über die Sie die Rechte einstellen können, beispielsweise „Read/write files on removable storage devices“ für den Zugriff auf USB-Laufwerke.

System mit USB-Stick aufsperren

Die folgende Maßnahme macht das System selbst zwar nicht schneller, aber den Systemstart vollverschlüsselter Luks-Systeme komfortabler. Eine Datei auf einem USB-Stick schließt die Systempartition automatisch auf.

VON DAVID WOLSKI



Bei einem verschlüsselten Linux-System, wie es die Installer von Debian, Ubuntu und dessen offizielle Abkömmlinge anbieten, ist beim Systemstart die Eingabe des Passworts nötig. Gleich nach dem Laden des Bootloaders Grub2 fragen diese Systeme das Passwort ab und erst nach korrekter Eingabe geht es mit dem Systemstart weiter bis zur Anmeldung. Die Verschlüsselung erledigt Cryptsetup/Luks, eine ausgereifte und sichere Methode, die komplette Systempartition samt Swap zu chiffrieren. Nur die kleine Bootpartition („/boot“) bleibt auf diese Weise unverschlüsselt, diese enthält aber nur den Bootloader, den Kernel sowie die initiale Ramdisk, die allesamt keinerlei Benutzerdaten enthalten.

Eine hardwarebasierte Lösung

Die Passwortabfrage beim Start schützt das komplette System, ist aber auch lästig, unterbricht sie doch einen flotten Neustart bis zur Benutzeranmeldung am Desktop. Wichtiger noch: Die interaktive Passwortabfrage ist ein Grund, warum sich diese Art der Vollverschlüsselung nicht für Server eignet. Denn zum einen soll ein Server ja auch mal per SSH aus der Ferne neu gestartet werden, ohne hilfreiche Hand vor Ort. Zum anderen arbeiten viele Linux-Systeme in einer Serverrolle ohne Monitor und ohne angeschlossene Tastatur. Wie lässt sich das Passwort automatisch eingeben?

Eine nicht besonders komplizierte Konfiguration von Cryptsetup löst das Dilemma mit Hilfe eines USB-Sticks als Schlüssel. Dazu brauchen Anwender lediglich einen zuverlässigen, beliebig kleinen USB-Stick und eine Handvoll Befehle zur Einrichtung anstatt eines Passworts. Cryptsetup wird dann während des Systemstarts nach dem eingesteckten USB-Stick und der dort vorbereiteten Schlüsseldatei suchen. Das Aufschließen der Systempartition und anderen Partitionen gelingt dann nur noch, wenn dieser USB-Stick am Rechner hängt. Die Passwortabfrage entfällt andererseits. Es handelt sich also um einen Wechsel weg vom interaktiven Passwort hin zu einer hardwarebasierten Entschlüsselung per Token. Als Token tut es hier aber jeder handelsübliche USB-Stick.

Die folgende Anleitung geht von einem Debian- oder Ubuntu-System aus, das per Installation Luks-verschlüsselt wurde. Für die hier gezeigte Lösung einer automatischen Entsperrung per USB-Stick sind auch keine externen Helfer-Scripts zum Auffinden des USB-Sticks notwendig. Alles funktioniert unter Debian, Ubuntu und den offiziellen Derivaten mit jenen Bordmitteln, die das Paket „cryptsetup“ bereits mitbringt. Eine Ausnahme macht Linux Mint, das sich immer weiter von seiner Ubuntu-Basis entfernt, hier in die ungünstige Richtung. Unter Linux Mint scheitert diese Methode.

Einen USB-Stick vorbereiten

Als Schlüssel ist ein beliebiger USB-Stick gefragt. Die Größe spielt dabei kaum keine Rolle, denn der dort hinterlegte Schlüssel wird lediglich 4096 Byte umfassen. Neben dem Schlüssel dürfen auf dem Stick auch andere Daten gespeichert werden. Ist das verschlüsselte Linux-System gebootet, schließt man den USB-Stick an und erstellt dort ein neues Dateisystem vom Typ Ext4. Die Wahl des nativen Linux-Dateisystems ist zwingend, denn die vom Kernel zum Sys-

temstart genutzte Ramdisk enthält auf allen Linux-Distributionen die nötigen Module für Ext4 und kann den Schlüssel somit einlesen.

1. In der Kommandozeile ermittelt der Befehl „lsblk" die Laufwerkskennung „/dev/sd[x]" des angeschlossenen USB-Sticks und der Befehl (Beispiel)

```
sudo mkfs.ext4 /dev/sdb1 -L
 keystore
```

erstellt dort ein neues Ext4-Dateisystem mit dem Label „keystore". Dieses Label wird im Anschluss gleich noch wichtig, um diesen Datenträger als Hardwareschlüssel zu hinterlegen, kann aber im Prinzip beliebig gewählt werden. Nach einem erneuten Einstecken des Sticks wird das Dateisystem in Debian, Ubuntu, Mint und Co. unter „/media/[User]/keystore" eingehängt, wobei der Platzhalter „[User]" dem eigenen Benutzernamen entspricht.

2. Die geforderte Schlüsseldatei von exakt 4096 Byte Länge (8 * 512) erstellt das Kommando

```
sudo dd if=/dev/urandom of=/media/
 [user]/keystore/sys.key bs=512
 count=8
```

aus dem Zufallsgenerator des Linux-Kernels direkt auf dem USB-Stick. Das vorangestellte „sudo" ist nötig, um Zugriffsrechte des zuvor erstellen Ext4-Dateisystems zu ignorieren. Es ist auch keine weitere Anpassung dieser Zugriffsrechte nötig, denn dem Linux-Systemstart sind diese egal.

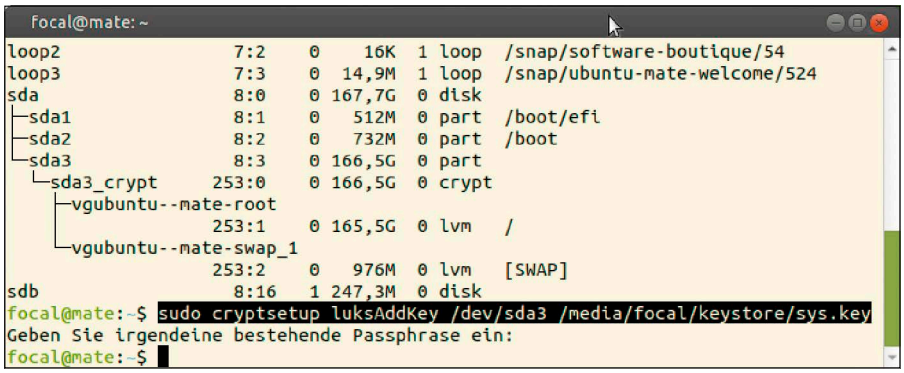
3. Jetzt wird der erzeugte Schlüssel auf dem eingehängten USB-Stick unter „media/[user]/keystore/sys.key" der verschlüsselten Partition als Entsperrmöglichkeit hinzugefügt. Dazu ist die Laufwerkkennung der verschlüsselten Systempartition gefragt, die wieder das Kommando lsblk ermittelt. In der Ausgabe ist jene Laufwerkskennung von Interesse, die mit „crypto_LUKS" als „FSTYPE" aufgelistet ist. Bei Ubuntu & Co. ist dies bei einer Vollverschlüsselung des Installers stets das Laufwerk „/dev/sda3". Das Kommando

```
sudo cryptsetup luksAddKey /dev/
 sda3 /media/[user]/keystore/sys.
 key
```

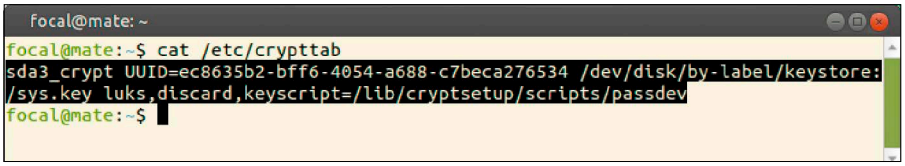
fügt die Schlüsseldatei hinzu.

4. Um beim Systemstart automatisch nach dem USB-Stick und der enthaltenen Schlüsseldatei zu zu suchen, benötigt die Konfigurationsdatei „/etc/crypttab" eine Modifikation. Das Kommando

```
sudo nano /etc/crypttab
```



Datei auf dem USB-Stick als weiteren Schlüssel hinzufügen: Das gesetzte Passwort bleibt bei dieser Aktion erhalten. Die Partition lässt sich weiterhin aus einem Livesystem heraus entsperren.



Konfigurationsdatei „/etc/crypttab": Dieser modifizierte Eintrag macht die Magie über das vorinstallierte Script „passdev", das beim Systemstart nach dem eingetragenen USB-Stick sucht.

lädt die Datei mit root-Recht in den Texteditor „Nano". Die dort eingetragenen Zeilen geben an, wie eine verschlüsselte Partition von Cryptsetup geöffnet werden soll. Der Standardeintrag führt zur interaktiven Passwortabfrage, die wir vermeiden wollen. Mit dem Script „passdev" im Repertoire von Cryptsetup kann stattdessen der präparierte USB-Stick als Schlüssel angegeben werden. Ist in der Datei die Zeile (Beispiel)

```
sda3_crypt UUID=5d492f5c-1d89-
 47f5-b77f-f093ae7fb6da none
 luks,discard
```

angegeben, so ändern Sie diese Zeile wie folgt ab (Beispiel):

```
sda3_crypt UUID=5d492f5c-1d89-
 47f5-b77f-f093ae7fb6da /dev/disk/
 by-label/keystore:/sys.key
 luks,discard,keyscript=/lib/
 cryptsetup/scripts/passdev
```

5. Während des Systemboots ist ohne Entschlüsselung nur die Partition „/boot" mit Kernel und initialer Ramdisk verfügbar. Die Ramdisk beherbergt deshalb alle für den Start wichtigen Scripts und Binaries, unter anderem auch für die Konfiguration von Cryptsetup.

Nach jeder manuellen Änderung der Datei „/etc/crypttab" ist es deshalb wichtig, die Ramdisk mit dem Kommando

```
sudo update-initramfs -k all -u
```

neu zu generieren.

Diesen Befehl führen Debian und Ubuntu übrigens nach einer Aktualisierung des Kernels automatisch aus.

Ab dem nächsten Neustart entfällt die interaktive Passwortabfrage und das System sucht stattdessen nachdem USB-Stick mit dem Label „keystore" und der dort enthaltenen Datei „sys.key". ■

HILFE, SCHLÜSSEL VERLOREN! BOOTEN MIT LIVESYSTEM

Bei der hier gezeigten Methode wird dem Luks-Schlüsselbund eine Schlüsseldatei zusätzlich zum bereits gesetzten Passwort hinzugefügt. Das bedeutet, dass das bisherige Passwort weiterhin gültig bleibt – es wird beim Systemstart nur nicht mehr abgefragt. Geht der USB-Stick mit der Schlüsseldatei also einmal verloren, so ist das noch kein Beinbruch: Mit einem Livesystem, etwa den Ubuntu-Installationsmedien, lässt sich das verschlüsselte System weiterhin booten und der Dateimanager kann die verschlüsselten Partitionen nach der Eingabe des weiterhin akzeptierten Passworts einhängen und öffnen.

Hilfe, Dateien gelöscht!

Wurden wichtige Dateien versehentlich aus dem Papierkorb oder in der Shell gelöscht, so gilt es, schnell und richtig zu handeln. Denn mit jeder Schreibaktion im Dateisystem könnten die gelöschten Daten unwiederbringlich verloren gehen.

VON DAVID WOLSKI

Moderne Dateisysteme wie Ext4, XFS oder BTRFS machen es nicht einfacher, Gelöschtes wiederherzustellen. Im Gegenteil: Diese Journaling-Dateisysteme sind darauf ausgelegt, ihre Struktur zu jederzeit konsistent zu halten, beispielsweise auch nach einem plötzlichen Stromausfall. Metadaten zu einer Datei, also die Infos zu den vormals belegten Blöcken, gehen bei Dateisystemen mit einem Journal schneller verloren als bei einfachen Dateisystemen wie FAT16, FAT32 oder dem alten Ext2. Erschwerend kommt noch die Controllerlogik von SSDs und NVME-Laufwerken mit Flashspeicher hinzu, die auf eigene Faust Schreibaktionen über das eigentliche Medium verteilt. Auch dies macht die Zuordnung von Blöcken einer gelöschten Datei schwieriger und verlangt nach einer schnellen Reaktion.

1. Konservieren: Schreibvorgänge vermeiden

Nach dem Löschen einer Datei hat es Vorrang, so schnell wie möglich weitere Schreibaktionen auf dem Datenträger zu unterbinden. Das bedeutet im Fall einer Datenpartition, den betroffenen Datenträger sofort auszuhängen. Auf Desktopsystemen gelingt das nach dem Schließen aller eventuell noch geöffneten Dateien über den jeweiligen Dateimanager und diesen Befehl:

```
sudo umount /dev/[ID]
```

Der Platzhalter „[ID]“ steht für die Laufwerkskennung, die mit der Eingabe von *lsblk* vor ermittelt werden kann. Falls es sich um die Systempartition handelt, auf der das System selbst läuft, so muss man dieses herunterfahren und mit einem Livesystem weiterarbeiten.

2. Flashspeicher: Image anlegen

Bei SSDs, NVME-Laufwerken, USB-Sticks und Speicherkarten ist eine zusätzliche Sicherheitsvorkehrung Pflicht: Die weiteren Wiederherstellungsaktionen sollte man nicht direkt auf dem physikalischen Laufwerk ausführen. Es könnte sonst passieren, dass der Controllerchip die freien Speicherbereiche unwiederbringlich mit einer internen Aufräumaktion löscht (Trim). Sicherer ist es, mit einem Image des Laufwerks zu arbeiten. Zum Anlegen dieses Abbildes soll hier das weniger bekannte Tool GNU ddrescue in der Kommandozeile dienen, ein Verwandter von dd, das den Inhalt einer Partition im Rohdatenformat in eine Datei schreibt. In Debian/Ubuntu ist das Programm über das Paket „gddrescue“ installierbar, in Fedora, CentOS und Arch Linux heißt das Paket schlicht „ddrescue“ und in Open Suse Leap „gnu_ddrescue“. Das Laufwerk darf zum Auslesen nicht mehr eingehängt sein und das Ziellaufwerk muss genügend Platz für das Image der gesamten Partition bieten. Angenommen, es soll das Laufwerk „/dev/sdb1“ ausgelesen werden, so speichert

```
sudo ddrescue -d /dev/sdb1 sdb1.img
```

die Partition „/dev/sdb1“ im aktuellen Verzeichnis in der Datei „sdb1.img“ ab. Die ausgelesene Datei übergibt man dann den weiteren Wiederherstellungsprogrammen zur Analyse – als ob sie ein Laufwerk unter „/dev/“ wäre.

3. Ext4magic: Erste Hilfe bei Ext4

Geht es darum, von einer Ext4- oder Ext3-Partition eine bestimmte Datei wiederzubeleben, die noch nicht lange gelöscht ist, so ist das Tool Ext4magic ein schnelles und zuverlässiges Werkzeug. Es arbeitet über die Analyse des Journals und ist unter Debian/Ubuntu über das gleichnamige Paket „ext4magic“ installierbar. Das alte Wiederherstellungstool Extundelete ist dagegen auf aktuellen Linux-Systemen nicht mehr lauffähig.

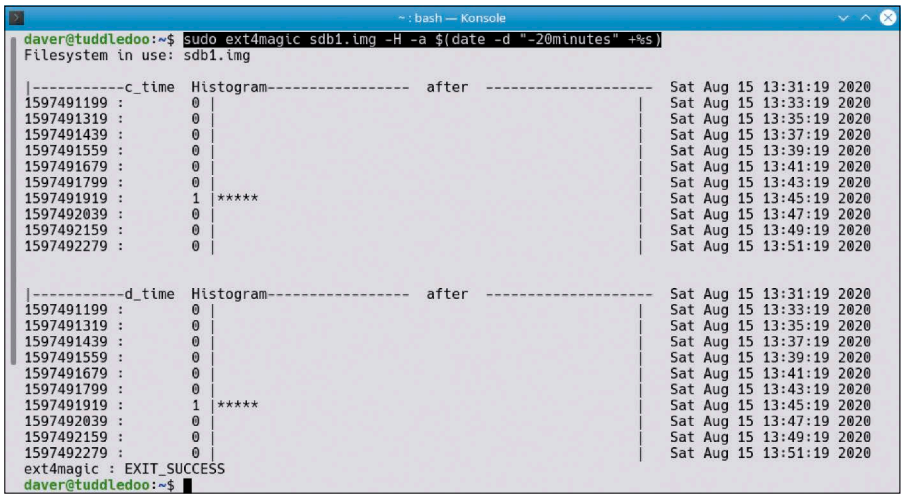
Um Ext4magic einzusetzen, ist es nötig, ungefähr den Zeitpunkt zu kennen, wann die benötigte Datei gelöscht wurde. Dann blickt man anhand dieser Zeitangabe mit Ext4magic erst in das Journal, um Änderungsstempel der letzten Änderungen anzuzeigen:

```
sudo ext4magic sdb1.img -H -a $(date
  -d "-20minutes" +%s)
```

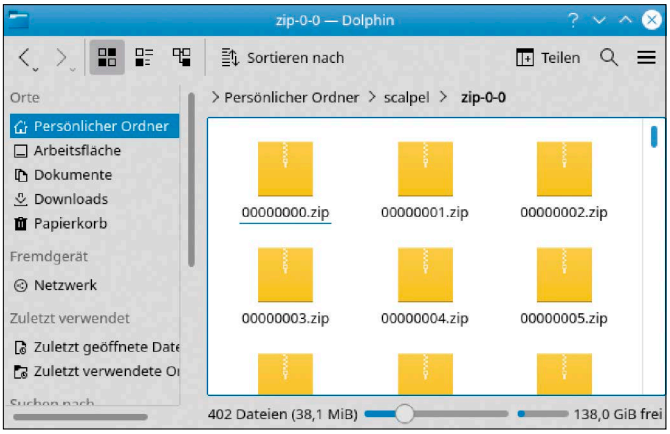
Dieser Befehl zeigt ein Histogramm der Änderungen der letzten 20 Minuten für das Ext3/4-Image „sdb1.img“ an. Bei (ausgehängten) Festplatten verwenden Sie statt der Imagedatei einfach direkt die Laufwerkskennung wie etwa „/dev/sdb1“. Ext4magic zeigt nun ein Histogramm namens „c_time“ mit den letzten allgemeinen Änderungen an und darunter ein weiteres namens „d_time“ mit Löschungen. In diesem Fall sind nur die Zeitstempel von Änderungen unter „d_time“ interessant. Lautet dort der Zeitstempel vor dem letzten Löschen beispielsweise „1597491799“, so geben wir Ext4magic mit dem Kommando

```
sudo ext4magic sdb1.img -a
  1597491799 -m -d gerettet
```

den Auftrag, alle Dateien hinter dem angegebenen Zeitstempel aus dem Image „sdb1.img“ oder aus einem nicht eingehängten Laufwerk in den neuen Unterordner „gerettet“ wiederherzustellen. Dateinamen gehen dabei verloren, Endungen dagegen nicht. Danach bleibt noch, die gesicherten Dateien in den angelegten Ordnern manuell zu überprüfen, um das Gesuchte zu finden.



Das Journal von Ext4 analysieren: Das Tool ext4magic verlangt die Angabe eines Zeitstempels aus den errechneten Histogrammen, ab dem die Dateien wiederhergestellt werden sollen.



Ausgrabungen: Das gründliche Scalpel hat hier ZIP-Dateien wiederhergestellt. Wir suchen nach einer Libre-Office-Datei und müssen manuell auf passende Dateitypen testen.

4. Magicrescue: Für alle Dateisysteme

Unabhängig vom Dateisystem arbeiten die Tools Photorec und Magicrescue, die gelöschten Dateien anhand ihrer Fingerabdrücke („Magic Bytes“) aus Fragmenten wiederherstellen können. Eine Anleitung zu Photorec liefert *www.pcwelt.de/1912252*, deshalb geht hier nur um Magicrescue. Es liegt unter allen Linux-Distributionen zur Installation den Standard-Paketquellen und ist in Debian/Ubuntu mit

```
sudo apt install magicrescue
```

zu installieren. Magicrescue analysiert Strukturen auf dem Datenträger und arbeitet entsprechend langsam. Für große Festplatten oder Images riesiger SSDs ist es deshalb weniger gut geeignet. Auch verlangt Magicrescue zur Identifizierung der Fingerabdrücke ein sogenanntes „Recipe“. Ohne „Rezept“ ist Magicrescue machtlos. Welche Recipes es für welche Dateitypen gibt, zeigt dieser Befehl:

```
ls /usr/share/magicrescue/recipes/
```

Es gibt ein „Recipe“ für Microsoft-Office-Dateien namens „msoffice“, aber beispielsweise keines für Libre-Office-Dokumente. Das Kommando

```
sudo magicrescue -r msoffice -d ./
  gerettet sdb1.img
```

stellt Microsoft-Office-Dateien aus dem angegebenen Image oder einem Laufwerk mit der jeweiligen ID wieder her.

5. Scalpel: Dateien nach Typ finden

Hat bisher alles versagt, so ist es Zeit, nochmal aufzurüsten: Das Werkzeug Scalpel basiert auf dem verwandten Open-Source-Programm Foremost, das von Forensikern der US Air Force für Beweisaufnahmen entwickelt wurde. Anders als Foremost arbeitet Scalpel, wie der Name nahelegt, speziell mit gesuchten Dateitypen, die aus einem Datenträger oder einem Image davon geschnitten werden. Scalpel ist in Linux-Distributionen über das Paket „scalpel“ installierbar. Wie auch Magicrescue basiert Scalpel auf einer Mustersuche. Leider bringt die freie Version nur eine Handvoll Muster mit, die in der Konfigurationsdatei „/etc/scalpel/scalpel.conf“ hinterlegt sind. Um einen bestimmten Dateityp aus den Rohdaten eines Dateisystems zu retten, muss das Kommentarzeichen „#“ am Zeilenanfang vor der angegebenen Dateiendung entfernt werden. Tipp: Libre-Office-Dateien sind ZIP-komprimiert und die Suche nach dem Dateityp „zip“ hat in unserem Test auch Libre-Office-Dokumente mit dem Kommando

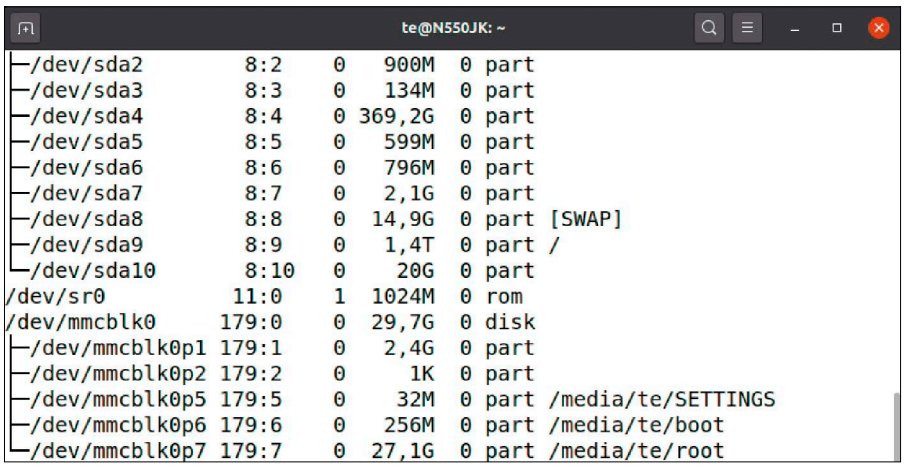
```
sudo scalpel sdb1.img -o ./scalpel
```

wiederhergestellt. Die Sichtung aller Dateien im hier angegebenen Unterordner „scalpel“ verlangt mehr Zeit, denn Scalpel arbeitet sehr gründlich, produziert aber auch etliche falsche Ergebnisse. ■

Imagebackups und Klonen

Abbildsicherungen von Laufwerken lohnen sich vor allem bei komplex konfigurierten Rechnern. Die Backups eignen sich beim Klonen aber auch für den Umzug auf neue Hardware.

VON THORSTEN EGGELING



Laufwerke oder Partitionen kopieren: Der Befehl lsblk -p liefert Informationen zu Gerätepfaden und Einhängepunkten. Sie benötigen diese Angaben für Backups mit dem Tool dd.

Alle Speichermedien haben nur eine begrenzte Lebensdauer. Man sollte Datenträger daher ab und zu auf Fehler prüfen und – wenn nötig – rechtzeitig austauschen. Regelmäßige Backups sind ein probates Mittel gegen Datenverlust. Wird ein Problem rechtzeitig erkannt, kann man den Inhalt einer vom Ausfall bedrohten Festplatte direkt auf ein neues Laufwerk kopieren und dann sofort weiterarbeiten. Oder man erstellt sicherheitshalber ein Imagebackup, das man später auf ein anderes Laufwerk überträgt.

1. Datenträger mit dd kopieren

Das Tool dd (disk dump) kopiert Datenträger bitgenau. Es arbeitet daher unabhängig von Dateisystemen und eignet sich zum Kopieren oder Klonen von Festplatten, SSDs und SD-Karten, etwa vom Raspberry Pi. Das funktioniert auch, wenn die Festplatte zwar noch ansprechbar ist, einige Dateien sich aber aufgrund von Lesefehlern nicht mehr kopieren lassen. Bei sehr vielen Defekten ist allerdings das Tool ddrescue besser geeignet (Paketname: „gddrescue“). dd kopiert alle Blöcke, ob sie belegt sind oder nicht. Bei großen Datenträgern arbeitet das Tool daher recht langsam und die Backupdatei hat die gleiche Größe wie die gesicherte Partition oder Festplatte. Für Laufwerke mit hoher Kapazität verwendet man besser Clonezilla, das nur die belegten Bereiche kopiert (siehe Punkt 3).

dd ist bei allen verbreiteten Linux-Distributionen standardmäßig installiert. Für Backups von SD-Karten, USB-Sticks oder anderen Laufwerken, die sich aus dem Dateisystem aushängen lassen, nutzen Sie das Tool im installierten Linux-System. Wenn Sie hingegen die Systemfestplatte sichern wollen, booten Sie den PC mit einem Livesystem, etwa dem ursprünglichen Installationsmedium.

Die allgemeine Syntax von dd lautet so:

```
dd if=[Quelle] of=[Ziel] [Optionen]
```

„if=“ legt die Eingabedatei beziehungsweise das Laufwerk oder die Partition fest. Hinter „of=“ steht die Zieldatei, das Laufwerk oder die Partition. Prüfen Sie diese Angaben sehr genau. dd legt immer sofort los und fragt vor dem Überschreiben nicht nach.

Um beispielsweise eine SD-Karte als Abbild zu sichern, gehen Sie so vor:

Schritt 1: Mit dem Befehl

```
lsblk -p
```

ermitteln Sie im Terminal den Gerätepfad zum SD-Kartenleser. In der Ausgabe sehen Sie beispielsweise „/dev/sdb1“ oder „/dev/mmcblk0“ bei internen Kartenlesern. Dahinter steht der Pfad im Dateisystem („/media/[user]/[Kennung]“).

Schritt 2: Hängen Sie die SD-Karte aus dem Dateisystem aus:

```
sudo umount /dev/sd[X]?
```

Der Platzhalter „[X]“ steht für den letzten Buchstaben der Gerätebezeichnung, beispielsweise „b“ bei „/dev/sdb“. Der Stellvertreter „?“ sorgt dafür, dass alle Partitionen des Geräts ausgehängt werden. Bei internen Kartenlesern verwenden Sie beispielsweise

```
sudo umount /dev/mmcblk0??
```

Damit hängen Sie die Partitionen „/dev/mmcblk0p1“ und „/dev/mmcblk0p2“ aus.

Schritt 3: Erstellen Sie ein Backup mit

```
sudo dd if=/dev/sdb of=[/Pfad/]sd-backup.img status=progress
```

Passen Sie den Beispielpfad „/dev/sdb“ für Ihr System an. Für den Platzhalter „[/Pfad/]“ tragen Sie den Pfad zum Ziellaufwerk ein. Die Option „status=progress“ sorgt für eine Fortschrittsanzeige. Die unkomprimierte „img“-Datei lässt sich über den Dateimanager und den Kontextmenüpunkt „Mit Einhängen von Laufwerksabbildern öffnen“ in das Dateisystem einbinden. Wenn Sie das

Backup platzsparend komprimieren möchten, verwenden Sie diese Variante:

```
sudo dd if=/dev/sdb status=progress
  | gzip -c > [/Pfad/]sd-backup.img.
  gz
```

Bei Laufwerken mit größerer Kapazität sollte man die Option „bs=4096“ hinzufügen. dd liest dann größere Blöcke, was den Kopiervorgang beschleunigt.

Weitere nützliche Optionen sind „conv=noerror,sync“, damit das Tool bei Kopierfehlern nicht abbricht.

Wenn Sie keine Imagedatei erstellen, sondern einen Datenträger klonen möchten, verwenden Sie eine Befehlszeile wie diese:

```
sudo dd if=/dev/sdb of=/dev/sdc
```

Das Ziellaufwerk muss mindestens so groß sein wie das Quell-Laufwerk. Wenn es größer ist, dehnen Sie die Partition später mit Gparted aus.

Sicherung wiederherstellen: Vertauschen Sie bei dd einfach Quelle und Ziel:

```
sudo dd if=[/Pfad/]sd-backup.img
  of=/dev/sdb status=progress
```

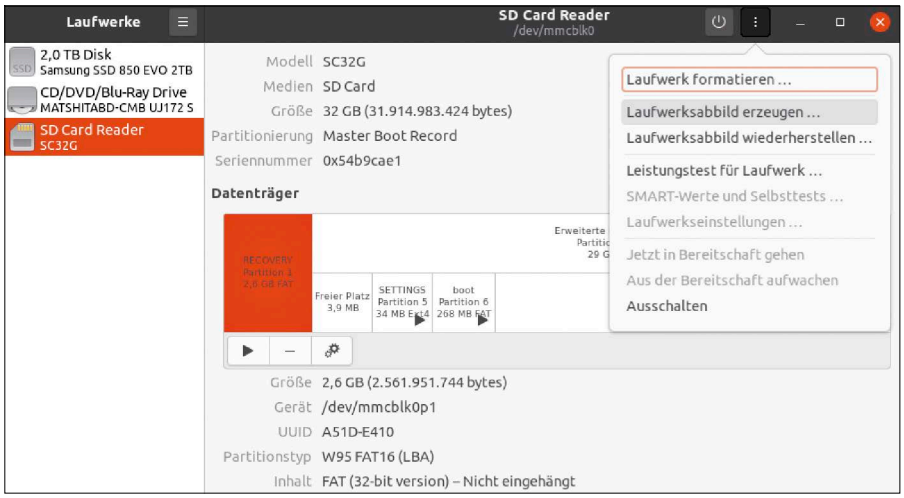
Dies überträgt das Abbild wieder auf das Ziellaufwerk „/de/sdb“.

2. Abbilder mit Gnome-Disks erstellen

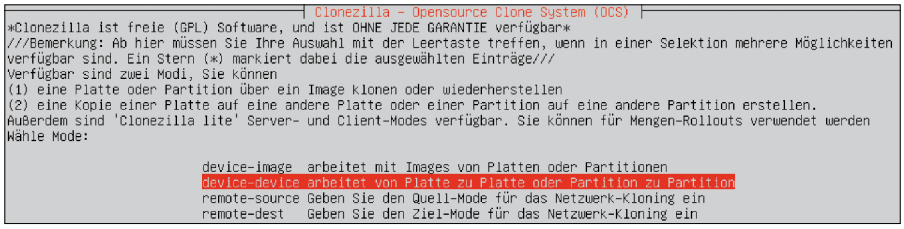
Wer eine grafische Oberfläche bevorzugt, sucht in Ubuntu oder Linux Mint nach „Laufwerke“. Dahinter verbirgt sich das Tool Gnome-Disks, mit dem Sie Laufwerke verwalten können. Über das Menü mit den drei vertikalen Punkten wählen Sie „Laufwerksabbild erzeugen“, um ein Abbild der ausgewählten Festplatte zu erstellen. Nach Auswahl einer Partition finden Sie nach Klick auf das Zahnradsymbol den Menüpunkt „Partitionsabbild erstellen“. Bei einem Systemlaufwerk funktioniert das nur über ein externes Zweitsystem. Gnome-Disks erstellt Abbilddateien im gleichen Format wie dd. Die „img“-Dateien lassen sich daher über den Dateimanager in das Dateisystem einbinden, wenn man etwa nur einzelne Dateien wiederherstellen möchte.

3. Festplatten klonen mit Clonezilla

Clonezilla startet von einer Live-DVD, die Sie unter *https://clonezilla.org* erhalten. Verwenden Sie die Version „alternative stable“ auf Ubuntu-Basis. Unter *https://clonezilla.org/clonezilla-live-doc.php* finden Sie zahlreiche detaillierte Anleitungen für die unterschiedlichen Einsatzgebiete. Clonezilla kann Laufwerke und Partitionen in komprimierte Imagedateien sichern oder klonen. Nachdem Sie einen Rechner mit Clonezilla gebootet haben, wählen Sie Sprache und Tastaturbelegung und starten dann Clonezilla. Um ein Laufwerk zu klonen, gehen Sie auf „device-device“, wählen „Beginner“ und danach „disk_to_local_disk“. Geben Sie dann Quell- und Ziellaufwerk an. Das Ziellaufwerk muss gleich groß oder größer als das Original sein. Ist es kleiner, müssen Sie einige Vorbereitungen treffen. Die nötigen Schritte haben wir unter *www.pcwelt.de/210432* beschrieben. ■



Backup in Imagedateien: Das Programm „Laufwerke“ (gnome-disks) erstellt ebenfalls Laufwerksabbilder. Die Größe eines Backups entspricht der Laufwerksgröße.



Das Tool Clonezilla läuft in einem Livesystem. Es kann platzsparende Abbilddateien erstellen und Laufwerke oder Partitionen für einen Umzug auf neue Hardware klonen.

DEN ZUSTAND DER LAUFWERKE PRÜFEN

Das Tool „Laufwerke“ (siehe Punkt 2) kann Diagnosedaten von Festplatten und SSDs auslesen. Wählen Sie ein Laufwerk auf der linken Seite aus. Klicken Sie dann auf die Schaltfläche mit den drei vertikalen Punkten und gehen Sie auf „SMART-Werte und Selbsttests“. Das Fenster zeigt die Temperatur des Laufwerks an und die Zeit seit der ersten Inbetriebnahme. Hinter „Allgemeine Einschätzung“ steht „Das Laufwerk ist in Ordnung“ oder eine Meldung, die auf Fehler hinweist.

Die Tabelle unter „SMART-Attribute“ zeigt die einzelnen Werte an. Bei SSDs steht hinter „wear-leveling-count“ in der Spalte „Normalisiert“ ein aussagekräftiger Wert. Neue SSDs starten bei „100“ und der Wert reduziert sich mit der Zeit. Geht er nahe „0“, sollten Sie das Laufwerk ersetzen.

Für SD-Karten und USB-Sticks verwenden Sie das Tool smartctl im Terminal (Paketname: „smartmontools“). Allerdings unterstützen nicht alle Medien SMART-Funktionen. Bei einem intakten Laufwerk liefert

```
sudo smartctl -H /dev/sd[x]
```

das Ergebnis „PASSED“.

Verwenden Sie die Option „-A“ für ausführlichere Informationen.

Linux-Hardware und Treiber

Meist lässt sich Linux auf PCs oder Notebooks problemlos installieren. Sehr neue oder exotische Hardware wird von Linux jedoch manchmal nicht erkannt. Prüfen Sie daher möglichst vor dem Kauf, ob die Hardware mit Linux kompatibel ist.

VON THORSTEN EGGELING

Die Linux-Installation bereitet auf den meisten PCs und Notebooks kaum Probleme. Zusätzliche Treiber sind oft nicht erforderlich, weil alles Nötige bei Linux bereits dabei ist. Peripheriegeräte, zumindest von bekannten Herstellern, werden von Linux ebenfalls gut unterstützt (siehe ab Seite 78). Es gibt jedoch keine Garantie dafür, dass ein bestimmtes Gerät von einem Linux-System erkannt und auch optimal eingebunden wird. Gegenwärtige und zukünftige Linux-Nutzer sollten daher vor dem Kauf neuer Hardware genau hinsehen und detaillierte Informationen einholen. Wenn Hardware, beispielsweise von Ubuntu 20.04 oder Linux Mint 20, nicht standardmäßig unterstützt wird, gibt es aber auch dafür Lösungen. Mit etwas Bastelarbeit lässt sich auch standardmäßig nicht unterstützte Hardware in Betrieb nehmen, wenn passende Treiber in einem neueren Linux-Kernel enthalten sind. Eine einfache Alternative ist der Umstieg auf eine andere Linux-Distribution mit aktuellerem Kernel.

1. Linux-Treiber und Kernel

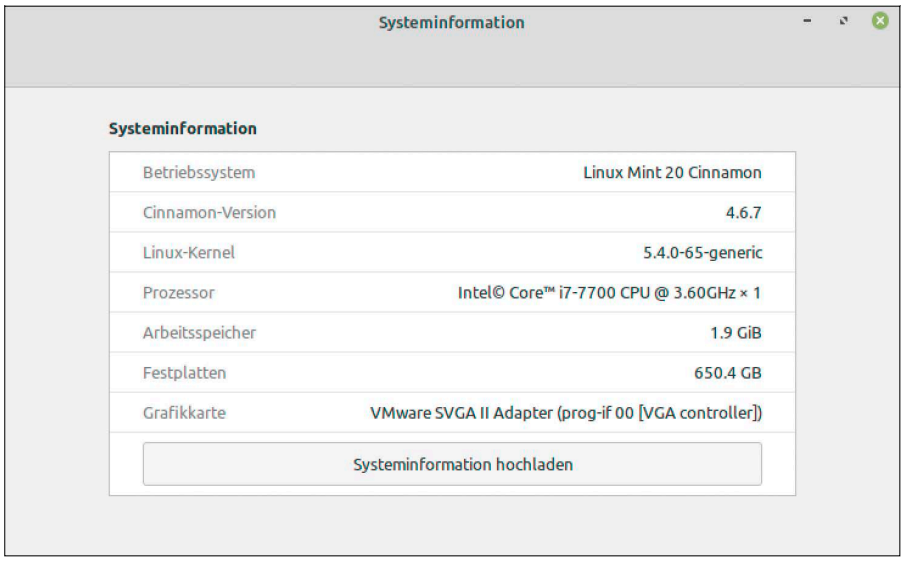
Ein Computer besteht aus zahlreichen Hardwarekomponenten und für alle ist ein eigener Treiber erforderlich. Unter Linux sind Treiber, die hier als Kernel-Module bezeichnet werden, im Betriebssystemkern (Kernel) enthalten oder werden von diesem bei Bedarf geladen. Neue Kernel erscheinen alle zwei bis drei Monate und enthalten neben Fehlerkorrekturen und Verbesserungen auch neue Module für aktuellere Hardware.

LTS-Distributionen (Long Term Support) wie Ubuntu 20.04 oder Linux Mint 20 sind auf lange Laufzeiten von fünf Jahren ausgelegt. Um die Stabilität des Systems sicherzustellen, beseitigen Updates nur Fehler und Sicherheitslücken. Die Hauptversionsnummern von Kernel und anderer Basissoftware bleiben standardmäßig gleich. Das hat zur Folge, dass Hardware nicht unterstützt wird, die erst kurz vor Erscheinen des Kernels auf den Markt kam oder für die zu diesem Zeitpunkt noch kein Linux-Treiber verfügbar war.

Im ungünstigsten Fall ist eine LTS-Version bei der Neuinstallation knapp zwei Jahre alt, der Kernel sogar noch etwas älter. Damit das auf neuer Hardware nicht zu Problemen führt, erscheint etwa alle sechs Monate ein Point Release von Ubuntu (18.04.4, 18.04.5, 20.04.1, 20.04.2). Die Version enthält alle bisherigen Updates und meist auch einen neueren Kernel. Das letzte Point Release einer Version wird mit dem Kernel des Nachfolgers ausgeliefert. Für Linux Mint, das auf Ubuntu basiert, gibt es ebenfalls Point Releases, wenn auch in etwas größeren Abständen.

Bestehende Installationen lassen sich bei Bedarf auf den Stand des jeweils aktuellen Point Release bringen (siehe Punkt 5). Ein Kernel-Upgrade ist sinnvoll, wenn zusätzlich eingebaute Hardware vom bisherigen Kernel nicht unterstützt wird oder Treiber eine neuere Kernel-Version erfordern.

Die von Ubuntu angebotenen Updates und Upgrades sind ausreichend getestet und gelten daher als sicher. Es ist aber möglich, noch neuere Kernel zu installieren (siehe Punkt 5). Damit ist jedoch nicht garantiert, dass das System stabil läuft und alle Komponenten zusammenpassen. Ein großes Risiko besteht jedoch nicht, weil man im Problemfall zum vorherigen Kernel zurückkehren kann.



Nicht wirklich aktuell: LTS-Versionen kommen mit sehr aktueller Hardware teilweise schlecht zurecht. Der Kernel 5.4 von Linux Mint 20 („Ulyana“) wurde bereits Ende 2019 veröffentlicht.

2. Distributionen mit besserer Hardwareunterstützung

Linux Mint und Ubuntu sind bewährte Distributionen, die sich auch für Einsteiger eignen. Wer Probleme mit sehr neuer Hardware vermeiden möchte, greift jedoch besser zu einer Distribution mit kürzeren Updatezyklen. Als Favorit kann Fedora (*https://getfedora.org*) gelten, das sich bei Installation und Nutzung nicht wesentlich von Ubuntu unterscheidet, aber aktuellere Kernel als regelmäßige Updates anbietet.

Für aktuelle Hardware ebenfalls empfehlenswert ist Open Suse Tumbleweed (*https://de.opensuse.org/Portal:Tumbleweed*), das als Rolling Release ständig auf dem aktuellsten Stand gehalten wird. Linux-Profis greifen gerne zu Arch Linux (*www.archlinux.de*), das für Einsteiger jedoch schwer zu installieren ist. Ein grafischer Installer fehlt und daher ist viel Handarbeit erforderlich. Eine Arch-Variante mit niedrigerer Einstiegshürde ist Endeavour-OS (*https://endeavouros.com*), das einen grafischen Installer in einem Livesystem bereitstellt.

Allen genannten Alternativen ist gemeinsam, dass sich Aktualität nur auf Kosten der Stabilität erreichen lässt. Damit ist nicht gemeint, dass sich die Systeme nicht produktiv nutzen lassen. Man muss jedoch aufgrund neuer und weniger getesteter Softwarepakete eher mit Problemen rechnen als beim konservativen Ubuntu oder Linux Mint.

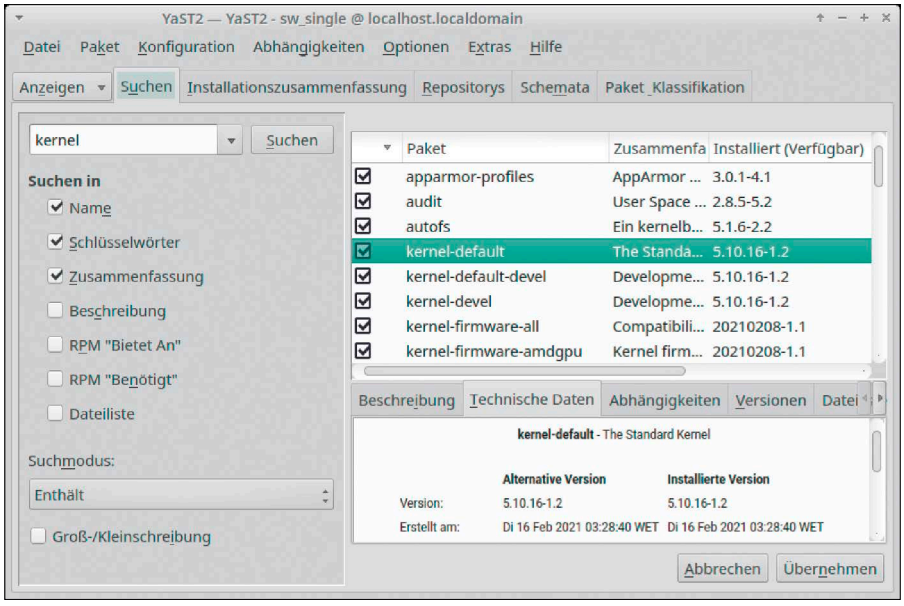
Ein Spezialfall liegt vor, wenn das Installationssystem den Netzwerkadapter nicht erkennt. Dann ist auch kein Update auf einen neueren Kernel möglich, der die Hardware unterstützt.

In diesem Fall ist es am einfachsten, vorübergehend einen externen Ethernet- oder WLAN-Adapter am USB-Port anzuschließen. Ältere oder besonders preisgünstige USB-Adapter für zehn bis 20 Euro funktionieren unter Linux meist problemlos (siehe ab Seite 78). Sollte das nicht möglich sein, laden Sie die Kernel-Pakete (siehe Punkt 5) auf einem anderen PC herunter und die Installation erfolgt dann manuell über einen USB-Stick.

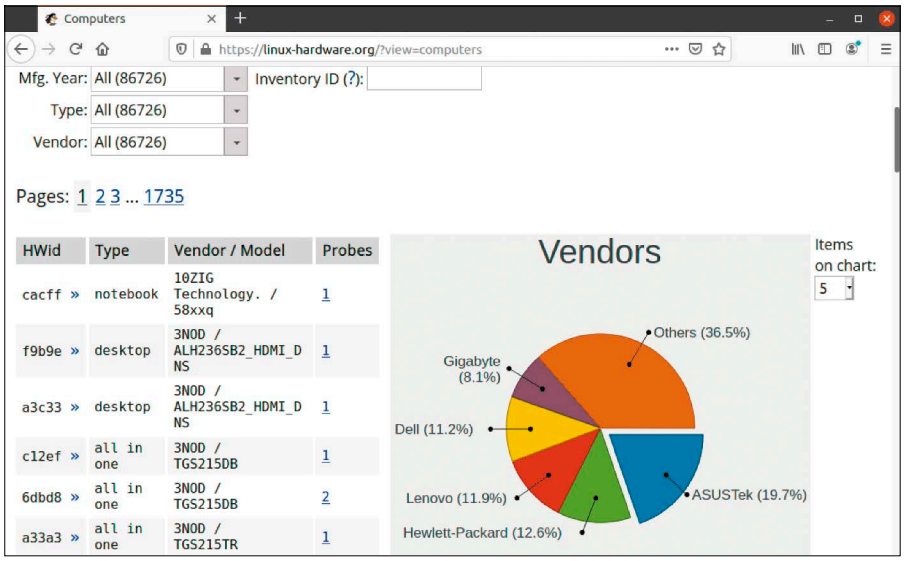
3. Geeignete Hardware für Linux finden

Wer sich mit der Hardware des PCs nicht selbst eingehend beschäftigen möchte, überlässt die Arbeit den Experten. Mehrere Hersteller bieten PCs und Notebooks mit vorinstalliertem Linux an oder sichern zumindest die Linux-Tauglichkeit zu. Canonical, das Unternehmen hinter Ubuntu, pflegt unter *https://certification.ubuntu.com/desktop* eine Liste mit zertifizierter Hardware. Die genannten Hersteller sind zurzeit Dell, Lenovo, HP, Intel und Acer. Zu jedem Gerät gibt es Angaben, mit welcher Ubuntu- und Kernel-Version es getestet wurde und welche Komponenten enthalten sind. Da Linux Mint auf Ubuntu basiert, sollte die Hardware auch mit dieser Distribution einsetzbar sein.

Einige Firmen und Händler bieten die Vorinstallation von Linux an, entweder auf Geräten bekannter Marken oder selbst zusammengestellter Hardware. Für Debian gibt es eine Liste von Firmen unter *https://www.debian.org/distrib/pre-installed*. Es handelt sich dabei aber meist um Anbieter für Unternehmens- und Serverlösungen. Ein umfangreiches Angebot für Firmen wie Privatkunden ist bei *https://www.tuxedocomputers.com* zu finden. Hier gibt es Linux-PCs und Notebooks für jeden Anwendungsbereich. Das System ist optimal auf die Hardware abgestimmt. Sollte doch einmal etwas klemmen, erhalten Sie Support per E-Mail oder Telefon.



Immer auf dem neuesten Stand: Rolling Releases wie Open Suse Tumbleweed werden ständig aktualisiert und eignen sich besonders gut für sehr aktuelle Hardware.



Was läuft unter Linux? Die Daten auf *https://linux-hardware.org* stammen von Einsendungen der Nutzer und liefern Information zu Hardware, die Linux unterstützt.

Bei einem beliebigen Gerät aus dem aktuellen Angebot eines Onlinehändlers oder lokalen Discounters kann niemand für die Linux-Unterstützung garantieren. Bis auf seltene Ausnahmen wird Ihnen auch der Händler nichts über Linux-Erfahrungen berichten können. Zurzeit gibt es keine zentrale Datenbank, in der die Kompatibilität jeder Hardware mit Linux-Distributionen oder Linux-Kerneln erfasst ist. Es ist daher nicht einfach möglich zu ermitteln, ob ein bestimmter PC oder ein Notebook in jeder Hinsicht perfekt unter Linux arbeitet. Trotzdem gibt es Hilfe und Infos:

Als Erstes sollte man eine Websuche nach dem gewünschten Computermodell kombiniert mit dem Suchbegriff „Linux" starten. Vielleicht haben andere Nutzer bereits Erfahrungen sammeln können und berichten von Erfolgen oder möglichen Problemen.

https://linux-hardware.org kann ebenfalls nützliche Informationen liefern. Die Datenbank basiert auf von Linux-Nutzern eingesendeten Testdaten und enthält daher nicht unbedingt die neusten Modelle. Über „Find Computer" kann man per Auswahl von „Type", „Vendor" (Hersteller) und „Model" eine Abfrage starten. Wählen Sie hinter „Mfg. Year" ein Jahr aus, um das Ergebnis auf einen Herstellungszeitraum zu beschränken.

https://linux-hardware.org zeigt an, mit welcher Linux-Distribution und welcher Kernel-Version der Test durchgeführt wurde. Unter „Devices" sind die einzelnen Komponenten aufgelistet. In der Spalte „Status" signalisiert „works", dass die Komponente funktioniert. Steht hier „detected", wird die Hardware zwar erkannt, es gibt jedoch noch keinen Test. Ein Ausrufungszeichen weist auf kleinere Probleme oder zusätzliche Anmerkungen hin. Per Klick auf das Feld gelangen Sie zur Detailansicht für das Gerät. Beim Status „failed" gibt es meist den Hinweis, dass kein Linux-Kernel diese Hardware unterstützt. Manchmal sind aber auch weiterführende Infos zu finden, wie man eine Komponente dennoch in Betrieb nehmen kann.

Eigene Hardware testen: Wer die Daten des PCs bei *https://linux-hardware.org* einsenden möchte, findet Informationen dazu über den Link „creating a probe". Nutzer von Ubuntu oder Linux Mint installieren das nötige Tool im Terminal:

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

Nach dem Start mit

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

erhalten Sie eine URL, die Sie im Webbrowser aufrufen.

4. Gezielte Suche nach Einzelkomponenten

Eine weitere Website, über Sie die Linux-Kompatibilität ermitteln können, ist *https://cateee.net/lkddb*. Die „Linux Kernel Driver Data Base" enthält Namen und numerische IDs von Hardware sowie deren Vorkommen im Kernel-Quellcode. Damit lässt sich ermitteln, ab welcher Kernel-Version eine Hardware unterstützt wird. Nutzbar ist das jedoch nur, wenn Sie die genaue Bezeichnung oder Hardware-ID einer Komponente kennen.

Letztere bekommen Sie heraus, wenn Sie bei *https://linux-hardware.org* nach einem PC oder Notebook suchen oder wenn Sie die Hardware bereits besitzen und Linux oder Windows auf dem Rechner läuft (siehe Kasten „Die Bedeutung von PCI- und USB-IDs" auf der nächsten Seite).

Ein Beispiel: lspci gibt folgende Info aus: „Realtek Semiconductor Co., Ltd. RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller [10ec:8168]", ferner den Hersteller des Mainboards mit „Subsystem: Micro-Star International Co., Ltd. [MSI] RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller [1462:7a70]". „Kernel driver in use: r8169" zeigt an, dass die Hardware erkannt und dafür das Kernel-Modul „r8169" geladen wurde.

Wichtig ist die Hardware-ID „10ec:8168". Eine Google-Suche bei *https://cateee.net/lkddb* kann dann mit der folgenden Suchanfrage erfolgen:

```
10ec 8168 site:cateee.net
```

Im ersten Suchergebnis sehen Sie im Abschnitt unter „LKDDb" mehrere Zeilen, die mit „lkddb pci 10ec 8168" beginnen. Am Ende jeder Zeile steht, in welchen Kerneln

```
te@ub1804: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
01:00.1 Audio device [0403]: NVIDIA Corporation GP106 High Definition Audio Controller [10de:10f1] (rev a1)
        Subsystem: ZOTAC International (MCO) Ltd. GP106 High Definition Audio Controller [19da:1438]
        Kernel driver in use: snd_hda_intel
        Kernel modules: snd_hda_intel
02:00.0 Ethernet controller [0200]: Realtek Semiconductor Co., Ltd. RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller [10ec:8168] (rev 15)
        Subsystem: Micro-Star International Co., Ltd. [MSI] RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller [1462:7a70]
        Kernel driver in use: r8169
        Kernel modules: r8169
te@ub1804:~$
```

Was steckt im PC? lspci gibt Bezeichnungen und Hardware-IDs der PC-Komponenten aus. Außerdem zeigt es an, welches Kernel-Modul geladen wurde.

die Hardware-ID gefunden wurde. In diesem Fall sind das die Versionen 3.17 bis 5.11.Bei USB-Geräten gibt es nur eine Hersteller- und Geräte-ID, aber keine Subsystem-ID. lsusb liefert die IDs, jedoch keine Infos über den geladenen Treiber. Dafür verwenden Sie

```
sudo usb-devices
```

Taucht in der Ausgabe „Driver=(none)“ auf, wurde kein Treiber geladen. Die Google-Suche beispielsweise für einen USB-WLAN-Adapter (TP-Link TL-WDN5200 T2U) mit

```
148f 761a site:cateee.net
```

zeigt, dass das passende Kernel-Modul „MT76x0U“ heißt und die Hardware erst ab Kernel-Version 4.20 unterstützt wird (siehe ab Seite 78).

5. Neue Kernel für neue Hardware

Abhängig von Ihren Recherchen installieren Sie einen neueren Kernel, um die Hardwareunterstützung zu verbessern. Vielleicht reicht der offizielle HWE-Kernel (Hardware Enablement) des nächsten Point Releases schon aus (siehe Punkt 1). Welcher Kernel aktuell verwendet wird, ermitteln Sie im Terminal:

```
uname -a
```

Mit der Zeile

```
apt search linux-generic-hwe
```

finden Sie Version des HWE-Kernels heraus. Ist der HWE-Kernel neuer als der installierte, installieren Sie ihn zusammen mit dem aktuellen X-Server:

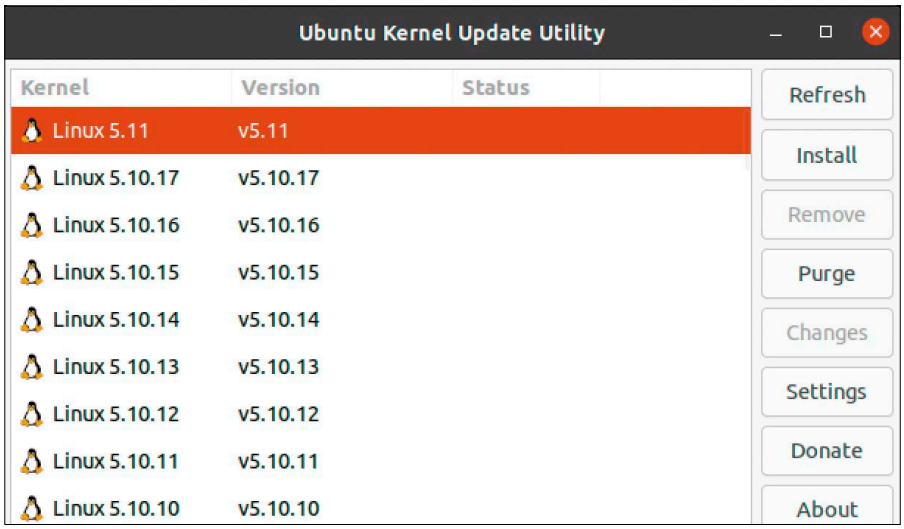
```
sudo apt-get install --install-
  recommends linux-generic-
  hwe-20.04 xserver-xorg-hwe-20.04
```

Die Versionsnummern passen Sie für andere Versionen an. Statt „20.04“ verwenden Sie beispielsweise „18.04“ für Ubuntu 18.04. Wer den HWE-Kernel unter Linux Mint installieren möchte, geht im Menü auf „Systemverwaltung → Aktualisierungsverwaltung“ und dann auf „Ansicht → Linux-Kernel“.

Die aktuellsten Kernel finden Sie unter *https://kernel.ubuntu.com/~kernel-ppa/mainline*. Bei Redaktionsschluss waren Kernel bis Version 5.11 als DEB-Pakete zum Download verfügbar. Für ein 64-Bit-System laden Sie unter „amd64“ alle Pakete herunter, die „generic“ enthalten, und die Datei mit der Endung „all.deb“. Neuere 32-Bit-Kernel werden nicht mehr bereitgestellt.

Im Terminal erfolgt die Installation im Downloadverzeichnis:

```
sudo dpkg -i *.deb
```



Kernel-Upgrade: Auch in LTS-Versionen lassen sich deutlich aktuellere Kernel installieren. Die gibt es bei *https://kernel.ubuntu.com*. Das Tool Ukuu vereinfacht die Installation.

Beachten Sie, dass bei sehr neuem Kernel die Wahrscheinlichkeit geringer ist, dass sich zusätzliche Treiber damit kompilieren lassen. Das kann Nutzer betreffen, die den proprietären Nvidia-Treiber (siehe ab Seite 74) oder Virtualbox verwenden.

Bei Problemen rufen Sie das Grub-Bootmenü auf. Sollte es nicht automatisch erscheinen, halten Sie die Umschalttaste nach dem Einschalten des PCs gedrückt. Im Menü gehen Sie auf „Erweiterte Optionen für Ubuntu“ beziehungsweise „Erweiterte Option für Linux Mint“ und wählen einen älteren Kernel. Danach deinstallieren Sie die neuere Version über die Paketverwaltung.

Wer neuere Kernel über die grafische Oberfläche installieren möchte, lädt sich das Tool Ukuu herunter (*https://github.com/teejee2008/ukuu*). Es ermöglicht die einfache Installation und Deinstallation der Kernel von *https://kernel.ubuntu.com* in Ubuntu und Linux Mint. ■

DIE BEDEUTUNG VON PCI- UND USB-IDS

Jede Hardware besitzt eine eindeutige ID, über die sich Hersteller und Gerätetyp ermitteln lassen. Die Verkaufsbezeichnung ist meist weniger eindeutig, weil einige Hersteller im Laufe der Fertigung andere Chips verbauen, ohne die Modellnummer zu ändern. Die Hardware-IDs ermitteln Sie unter Linux im Terminal mit diesen drei Befehlszeilen:

```
sudo lshw -numeric -html > lshw.html
sudo lspci -knn > lspci.txt
sudo lsusb -v > lsusb.txt
```

In der Datei „lshw.html“ finden Sie danach allgemeine Informationen zum PC, Typ der Hauptplatine, Bios-Version sowie Prozessor. „lspci.txt“ enthält Informationen zu den über PCI angebundenen Komponenten wie Soundchips („Audio device“), Grafikkarten („VGA compatible controller“) und Netzwerkchips („Ethernet controller“). In der Datei „lsusb.txt“ sehen Sie, welche Geräte mit den USB-Ports verbunden sind.

Unter Windows öffnen Sie den Gerätemanager (devmgmt.msc), rufen per rechten Mausklick die „Eigenschaften“ eines Gerätes auf und wechseln auf die Registerkarte „Details“. Unter „Eigenschaft“ stellen Sie „Hardware-IDs“ ein.

Eine Hardware-ID besteht aus der Vendor-ID (Chip-Hersteller) und einer Device-ID (Gerät). Beide nutzt der Linux-Kernel, um den passenden Treiber zu finden. Dazu kommt eine zweiteilige Subsystem-ID, die den Hersteller des Komplettgerätes enthält und die Sie nicht weiter beachten müssen.

Grafikkarten & Monitore optimal nutzen

Auch Grafikadapter benötigen Treiber und davon gibt es unter Linux gleich mehrere. Abhängig vom Einsatzbereich kann sich die Installation eines neueren und optimierten Treibers lohnen.

VON THORSTEN EGGELING

Die Anzahl der Anbieter von Grafikchips ist überschaubar. Die Basisausstattung steckt meist bereits im Hauptprozessor, der von Intel oder AMD stammt. Die Leistung genügt für Desktopanwendungen, Videowiedergabe in HD-Qualität und einfache Spiele. Wer mehr benötigt, vor allem für grafisch anspruchsvolle Spiele, greift zu Geräten mit einem zusätzlichen Grafikchip von Nvidia oder AMD. Der sitzt bei Notebooks auf der Hauptplatine, PCs lassen sich mit einer separaten Grafikkarte ausstatten. Aktuelle Linux-Systeme unterstützen alle genannten Grafikchips. Lediglich bei sehr neuen Modellen kann es zu Problemen bei der Linux-Installation kommen, was sich aber leicht beheben lässt. Die standardmäßig installierten Open-Source-Grafiktreiber reichen für die meisten Anwender aus, für optimale Leistung empfiehlt sich die Installation eines Treibers vom Hersteller.

1. Grafikchips und Treiber

Prozessorgrafik von Intel und AMD funktioniert dank Unterstützung durch die Hersteller in der Regel gut. Bei Grafikkarten geben viele Linux-Nutzer Nvidia-Chips den Vorzug, weil die Installation eines optimierten Treibers unter Ubuntu oder Linux Mint mit wenigen Mausklicks erledigt ist. Bei AMD-Grafikchips bietet allerdings schon der standardmäßige Open-Source-Treiber eine ausreichend gute Unterstützung. Wer möchte, kann trotzdem auch hier einen neueren Treiber installieren.

Eine Besonderheit bei Linux: Das System benötigt zwei Treiber. Der erste gehört zum Kernel und sorgt für die Darstellung der Textkonsole. Meist kommt der standardmäßige Vesa-Framebuffer-Treiber zum Einsatz. Der unterstützt keine speziellen Fähigkeiten des Grafikchips, genügt aber für eine höhere Auflösung in der Textkonsole. Die bekommen Sie in der Regel gar nicht zu sehen, weil das System gleich die grafische Oberfläche startet, deren Basis der Xserver ist. Hier wird ein Xorg-Treiber verwendet, der 2D-Beschleungigung für die bessere Darstellung der Fensterelemente und 3D-Beschleunigung für grafische Anwendungen bieten kann. Zudem kann der Treiber zusammen mit einigen Programmbibliotheken den Prozessor der Grafikkarte (GPU, Graphics Processing Unit) für die Decodierung (Abspielen) und Encodierung (Umwandeln) von Videos nutzen. Das entlastet den Hauptprozessor (CPU, Central Processing Unit) des Rechners und sorgt für die ruckelfreie Wiedergabe auch von hochauflösenden Videoinhalten.

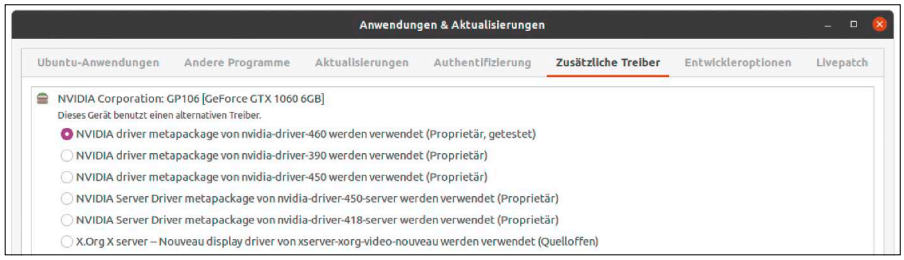
2. Grafikprobleme bei der Installation beheben

Ubuntu 20.04 und Linux Mint 20 verwenden bei der Installation einen Standardtreiber für Nvidia-Grafikchips („nouveau“). Der funktioniert in der Regel, bei einigen sehr neuen Chips startet das Livesystem jedoch nicht bis zum Desktop oder friert ein. Das Problem lässt sich umgehen, indem man beim Start vom Installationsmedium nach der Sprachauswahl „Ubuntu ohne Installation ausprobieren (abgesicherter Grafikmodus)“ wählt. Unter Linux Mint heißt die Option „Start in compatibility mode“). Im Uefi-Modus wählen Sie den Eintrag „safe graphics“, bei Linux Mint „compatibility mode“. Ubuntu-Nutzer setzen bei der Installation ein Häkchen vor „Installieren Sie Software von Drittanbietern für Grafik- und Wi-Fi-

Hardware und zusätzliche Medienformate". Die Installation sollte dann reibungslos ablaufen. Ubuntu richtet den proprietären Nvidia-Treiber automatisch ein und der Desktop erscheint wie erwartet.

Unter Linux Mint müssen Sie zuerst das Grub-Bootmenü aufrufen, indem Sie beim Neustart des PCs die Umschalt-Taste gedrückt halten. Drücken Sie die Taste E, um den Standardmenüeintrag zu bearbeiten. Gehen Sie in die Zeile, die mit „linux" beginnt, tragen Sie hinter „ro" die Option „nomodeset" ein und starten Sie dann Linux Mint mit Taste F10. Nach dem Systemstart gehen Sie im Menü auf „Systemverwaltung → Treiberverwaltung", wählen dort den Treiber mit der höchsten Versionsnummer und dem Zusatz „empfohlen", klicken auf „Änderungen anwenden" und schließlich auf „Neustarten".

Beim Start im abgesicherten Grafikmodus lädt Ubuntu keine Treiber, die den Start der grafischen Oberfläche verhindern. Der passende Treiber wird dann automatisch eingerichtet.



Verbesserte Treiber installieren: Ubuntu bietet mehrere Herstellertreiber zur Installation an. In der Regel wählen Sie die höchste Versionsnummer mit dem Zusatz „getestet".

3. Den optimalen Grafiktreiber nutzen

Für viele Nutzer ist der Nouveau-Standardtreiber für Nvidia-Chips ausreichend. Wenn Sie Spiele oder Videobearbeitungssoftware nutzen oder die Videowiedergabe ruckelt, sollten Sie aber auf den proprietären Nvidia-Treiber umsteigen. Der Weg führt unter Ubuntu über „Aktivitäten", die Suche nach „Treiber" und Klick auf „Zusätzliche Treiber", bei Linux Mint über „Systemverwaltung → Treiberverwaltung". Wählen Sie den Treiber mit der höchsten Versionsnummer und dem Zusatz „Proprietär, getestet" (Linux Mint „empfohlen"). Klicken Sie auf „Änderungen anwenden" und starten Sie Linux nach Abschluss der Installation neu.

Grafikchips von AMD: Linux-Distributionen verwenden automatisch den passenden Standardtreiber. Das Paket „xserver-xorg-video-ati" unterstützt sehr alte Grafikchips wie AMD/ATI Mach64, Rage128, Radeon, FireGL oder FireMV. „xserver-xorg-video-radeon" kommt bei Modellen wie R100 bis RV790 zum Einsatz. Der neueste Treiber steckt im Paket „xserver-xorg-video-amdgpu" und eignet sich für die Chipsatz-Familien Bonaire, Hawaii, Kaveri, Kabini Mullins, Iceland, Tonga, Carrizo, Fiji und Stoney. Nicht bei jedem Chipsatz werden bisher alle Funktionen unterstützt. Detaillierte Infos dazu liefert die Webseite *https://www.x.org/wiki/RadeonFeature*.

Grafikchips von Intel: Bei Chips ab Baujahr etwa 2007 wird nur der Kernel-Treiber geladen. Es ist zwar bei Ubuntu und Linux Mint auch das Paket „xserver-xorg-video-intel" installiert, die Treiber kommen aber bei neuerer Hardware nicht mehr zum Einsatz.

MONITORANSCHLÜSSE, KABEL UND 4K-AUFLÖSUNG

Einen Monitor verbinden Sie am besten über die digitalen Anschlüsse Displayport, HDMI oder DVI. Ubuntu oder Linux Mint erkennen die maximal mögliche Auflösung dann automatisch. Analoge VGA-Kabel sollten Sie nur benutzen, wenn ein älterer PC oder Monitor nichts anderes anbietet. Die Qualität ist schlechter, außerdem wird die passende Auflösung oft nicht erkannt und muss manuell justiert werden.

Für Auflösungen bis 1920 × 1200 Pixel genügt ein Single-Link-DVI-Kabel mit 18+1 Kontakten; für höhere Auflösung muss es ein Dual-Link-DVI-Kabel mit 24+1 Kontakten sein. Für einen hochauflösenden Monitor (Ultra-HD, 4K) nutzen Sie ein HDMI-2.0-Kabel, das den Hinweis „4k", „UHD" oder „2160p" auf der Verpackung trägt. Andernfalls liegt die Bildwiederholfrequenz nur bei 30 statt 60 Hz, was zu einer schlechteren Bildqualität führt. Bei der Grafikkarte ist dafür ein HDMI-2.0-Ausgang erforderlich. Alternativ verwenden Sie ein Displayport-Kabel. Für 60 Hz muss die Grafikkarte mindestens den Displayport-Standard 1.2 beherrschen.

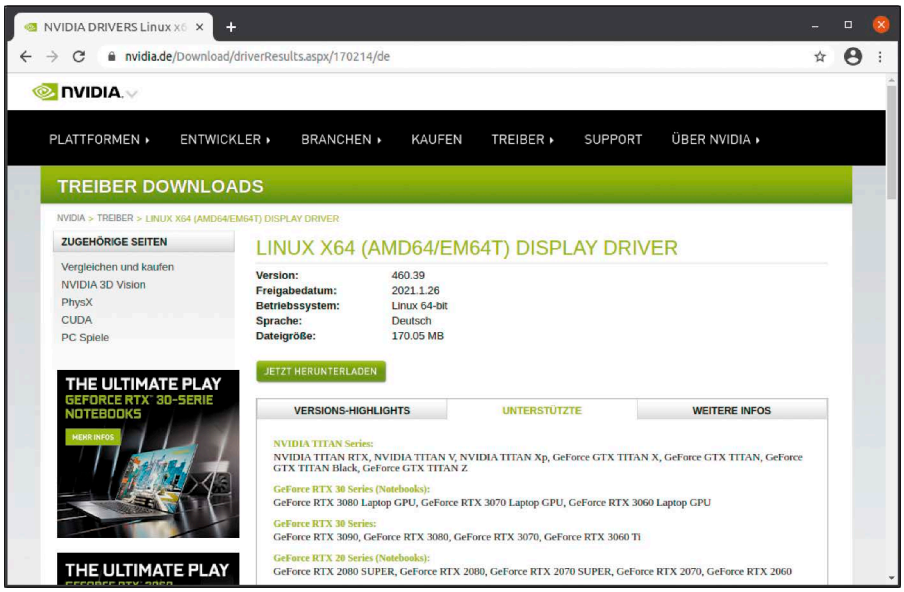
Bei voller 4K-Auflösung von 3840 × 2160 Pixeln sehen zwar Videos prima aus, Desktopelemente sind aber oft schwer zu erkennen. Bei Ubuntu 20.04 können Sie in den „Einstellungen" unter „Anzeigegeräte" die „Fraktionelle Skalierung" aktivieren. Hinter „Skalieren" stellen Sie dann beispielsweise „125 %" ein. Auf der gleichen Einstellungsseite lassen sich auch weitere Monitore aktivieren und bei Bedarf mit unterschiedlichen Auflösungen konfigurieren.

Linux-Mint-Nutzer finden die entsprechenden Optionen über „Einstellungen → Bildschirm".

Weitere Einstellungen ändern Sie unter Ubuntu über das Tool gnome-tweaks, das Sie per

```
sudo apt install gnome-tweaks
```

im Terminal installieren. Starten Sie das Tool über eine Suche nach „Optimierungen" unter „Aktivitäten". Gehen Sie auf „Schriften" und stellen Sie den gewünschten Skalierungsfaktor ein. Unter Linux Mint ist die Konfiguration über „Einstellungen → Schriftauswahl" möglich.



Welcher Treiber passt? Im Downloadbereich informiert Nvidia darüber, welche Grafikchips beziehungsweise Grafikkarten eine bestimmte Treiberversion unterstützt.

4. Herstellertreiber für Grafikchips verwenden

Ubuntu und Linux Mint bieten relativ aktuelle Treiber zur Installation an. Es ist daher nur in Ausnahmefällen erforderlich oder sinnvoll, einen neueren Treiber zu installieren, etwa für die Unterstützung eines sehr neuen Grafikchips. Aufgrund der zahlreichen Abhängigkeiten zum Xserver und anderen Programmbibliotheken kann die Installation eines Herstellertreibers leicht fehlschlagen und ist daher nur erfahrenen Linux-Nutzern zu empfehlen.

Für Nvidia-Chips rufen Sie *www.nvidia.de* auf und gehen auf „Treiber → Gforce-Treiber“. Wählen Sie das gewünschte Modell und hinter „Betriebssystem“ den Eintrag „Linux 64-Bit“. Klicken Sie auf „Suchen“ und dann auf „Unterstützte“. Vergewissern Sie sich, dass Ihre Grafikkarte in der Liste zu finden ist, und merken Sie sich die Versionsnummer. Gehen Sie dann zur Seite *https://launchpad.net/~graphics-drivers/+archive/ubuntu/ppa*. Hinter „Published in:“ wählen Sie die Ubuntu-Version, beispielsweise „Focal“ für Ubuntu 20.04/Linux Mint 20 oder „Bionic“ für Ubuntu 18.04/Linux Mint 19. Klicken Sie auf „Filter“ und prüfen Sie, ob die neueste Version der bei *www.nvidia.de* ermittelten entspricht.

Fügen Sie im Terminal das PPA hinzu:

```
sudo add-apt-repository
  ppa:graphics-drivers/ppa
sudo apt update
sudo apt upgrade
```

Ein Nvidia-Treiber mit der passenden Hauptversionsnummer wird damit aktualisiert. War ein älterer Treiber installiert, gehen Sie vor wie oben in Punkt 3 beschrieben, und installieren die neuste Version.

Über *https://www.nvidia.de/Download/Find.aspx?lang=de* finden Sie auch noch neuere Treiber, wenn Sie unter „Aktuelle“ den Eintrag „Beta“ wählen. Nvidia bietet einen Installer zum Download an. Klicken Sie auf „Weitere Infos“, um Informationen zum Treiber zu erhalten. Folgen Sie dem Link „See the README for more detailed instructions.“ für eine ausführliche Installationsanleitung.

Treiber von AMD nutzen: AMD bietet ebenfalls aktualisierte Treiber für Linux an. Auch hier lohnt sich die Installation nur, wenn die Hardware nicht standardmäßig unterstützt wird. Gehen Sie auf *https://www.amd.com/de/support* und wählen Sie die Grafikkarte in der Liste aus.

Nach einem Klick auf „Absenden“ gehen Sie auf „Ubuntu x86 64-Bit“ und laden „Radeon Software for Linux“ für Ubuntu 20.04 oder 18.04 herunter.

Eine Anleitung zur Installation finden Sie unter *https://amdgpu-install.readthedocs.io/en/latest*.

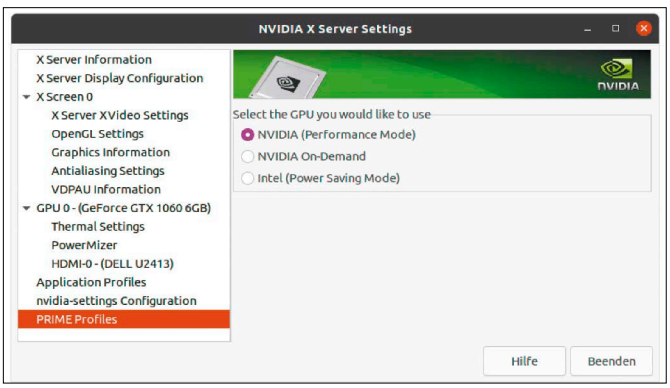
5. Energiesparen durch Treiberwechsel

In vielen Notebooks stecken zwei Grafikchips. Die CPU-Grafik bietet weniger Leistung, dafür hält der Akku länger. Der zusätzliche Grafikchip verbessert die Darstellung von Spielen oder grafikintensiven Anwendungen, nimmt aber auch mehr Leistung auf. Wenn die Open-Source-Treiber für die Grafikchips installiert sind, kommt standardmäßig die CPU-Grafik zum Einsatz, solange ein Programm nichts anderes fordert. Um einem Programm mehr Grafikleistung zuzuweisen, starten Sie es so:

```
DRI_PRIME=1 [Programmname]
```

Es verwendet dann den leistungsstärkeren Grafikchip von AMD oder Nvidia.

Ist der proprietäre Nvidia-Treiber installiert, kann man zwischen Nvidia- und CPU-Grafik umschalten. Linux Mint zeigt dafür ein Applet, über dessen Menü Sie den gewünschten Modus wählen. Ubuntu-Nutzer suchen über „Aktivitäten“ nach Nvidia, starten „Nvidia X Server Settings“ und gehen auf „PRIME Profiles“. Standardmäßig ist „Nvidia (Performance Mode)“ eingestellt. Wählen Sie „Intel (Power Saving Mode)“, wenn die Leistung nicht erforderlich ist. Die Option „Nvidia On-Demand“ – im Linux-Mint-Applet mit „Wechseln zu Nvidia auf Abruf“ bezeichnet – aktiviert ebenfalls die Intel-GPU. Anwendungen oder Spiele können dann bei Bedarf den Nvidia-Chip nutzen. Damit die Änderung wirksam wird, müssen Sie sich mindestens ab- und wieder anmelden.



GPU wählen: Über „Nvidia X Server Settings“ lässt sich wählen, welcher Grafikchip als Standard gelten soll. Der Intel-Chip bietet weniger Leistung, verlängert aber die Akkulaufzeit.

6. Feintuning für AMD-Grafikkarten

Das grafische Tool „Radeon-Profile“ dient zum Feintuning der AMD-Grafikchips über die Open-Source-Treiber unter Linux. Es unterstützt über den Treiber „radeon“ ältere AMD-Chips mit einer Handvoll Tuningoptionen.

Deutlich mehr Einstellungen gibt es, wenn der Treiber „amdgpu“ zum Einsatz kommt. Damit kann man beispielsweise manuell die Lüfterdrehzahl einstellen. Installieren Sie Radeon-Profile über ein PPA:

```
sudo add-apt-repository
 ppa:radeon-profile/stable
sudo apt update
sudo apt install radeon-profile
```

Zum Starten des Tools mit

```
sudo -H radeon-profile
```

sind root-Rechte erforderlich:

Tool für AMD-Grafikchips: Radeon-Profile zeigt Leistungsdaten sowie die Temperatur an und erlaubt auf vielen Karten die Anpassung der Energieprofile und der Lüfterdrehzahl.

7. Videos mit GPU-Unterstützung konvertieren

Schwächere Prozessoren sind mit der Darstellung hochauflösender Videos überfordert. Mediaplayer, Videoeditoren und Webbrowser nutzen daher – sofern vorhanden – die Hardwarebeschleunigung des Grafikprozessors. Die Programme erkennen, was der Grafikchip bietet, und passen die Einstellungen automatisch an. Die GPU lässt sich auch zum Encodieren von Videos nutzen, also für die Umwandlung in andere Formate. Im Vergleich zu einem Codec, der nur die CPU verwendet, ist die Geschwindigkeit etwa um den Faktor vier bis fünf höher. Allerdings leidet meist die Qualität etwas, weshalb viele Programme die GPU-Fähigkeiten nicht automatisch nutzen.

Wem es jedoch auf Geschwindigkeit ankommt, der kann beispielsweise den Videokonverter Handbrake verwenden. Sehen Sie zuerst unter *https://handbrake.fr/docs/en/1.3.0/technical/system-requirements.html* nach, ob die GPU in Kombination mit dem verwendeten Treiber unterstützt wird. Folgen Sie den Links im Abschnitt „Hardware encoders“.

Um die aktuellste Version zu erhalten, installieren Sie das Flatpak-Paket.

```
sudo apt install flatpak
flatpak --user install https://
 flathub.org/repo/appstream/fr.
 handbrake.ghb.flatpakref
```

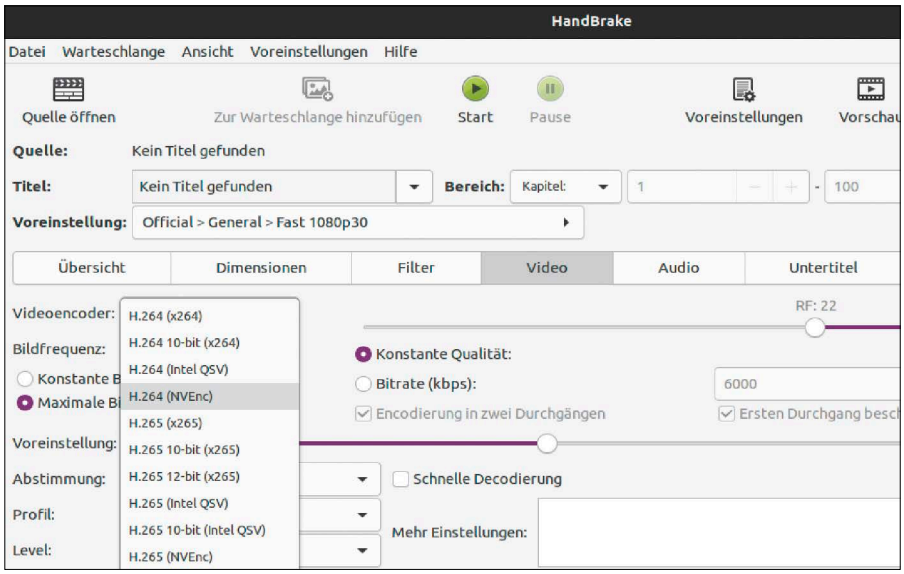
Nutzer von Linux Mint 20 können den ersten Befehl weglassen, weil dort Flatpak standardmäßig vorhanden ist. Wer die Intel-GPU (ab Intel Skylake, sechste Generation mit Intel HD Grafik oder besser) verwenden möchte, klickt zusätzlich unter *https://handbrake.fr/downloads.php* auf „QuickSync Plugin Download (64bit)“. Die Installation erfolgt mit

```
flatpak --user install Plugin.
 HandBrake.IntelMediaSDK-
 1.3.3-x86_64.flatpak
```

Anschließend starten Sie das Programm mittels

```
flatpak run fr.handbrake.ghb
```

Nach einem Klick auf „Open Source“ wählen Sie die Videodatei aus, die Sie konvertieren wollen. Klicken Sie auf „Video“ und stellen Sie hinter „Video Encoder“ beispielsweise „H.264 (NVEnc)“ (Nvidia), „H.264 (Intel QSV)“ (Intel-GPU) oder „H.264 (AMD VCE)“ (AMD-GPU) ein. Handbrake zeigt die Optionen nur an, wenn diese von Hardware und Treiber unterstützt werden. Prüfen Sie die anderen Einstellungen und klicken Sie abschließend auf „Start“. Bei einem Nvidia-Chip können Sie über „Nvidia X Server Settings“ (siehe Punkt 5) unter „GPU-0“ beobachten, wie die Auslastung hinter „Video Engine Utilization“ während der Verarbeitung steigt. ■



Videos umwandeln: Der Videokonverter Handbrake kann die Hardwarebeschleunigung des Grafikchips verwenden, was die Verarbeitung deutlich beschleunigt.

Probleme mit Hardware & Peripherie

Für Linux gibt es nur selten Treiberunterstützung durch die Hardwarehersteller. Trotzdem läuft die meiste Hardware ohne Probleme. In einigen Fällen muss man jedoch selbst nachbessern.

VON THORSTEN EGGELING

Linux bietet eine breite Unterstützung für fast jede Art von Hardware. Basiskomponenten wie Ethernet-Netzwerk- und SATA-Adapter, Maus und Tastatur sowie Grafikchips funktionieren fast immer auf Anhieb und ohne besondere Konfiguration. WLAN- oder Bluetooth-Adapter auf der Hauptplatine eines Notebooks stellen für Linux meist auch kein Problem dar, soweit es sich um weit verbreitete Bausteine von Intel oder AMD handelt. WLAN-Adapter für den USB-Port und WLAN-Karten werden aber teilweise nicht erkannt. Manchmal fehlt der Treiber, in einigen Fällen nur die Firmware, die sich aber nachinstallieren lässt. Aktuelle Drucker und Scanner lassen sich fast immer auch unter Linux nutzen. Mit den Standardtreibern stehen aber meist nicht alle Funktionen zu Verfügung. Zum Teil bieten Hersteller bessere Treiber und Software.

1. Hardware für Linux wählen

Von den Herstellern ist oft keine Linux-Unterstützung zu erwarten. Linux-Nutzer sind also auf die Arbeit der Kernel-Entwickler angewiesen. Denn alle Treiber gehören zum Linux-Kernel und eine Treiber-CD mit Setupprogramm, wie man es von Windows gewohnt ist, gibt es für Linux nicht. Nur in Einzelfällen stellen die Hardwarehersteller den Quellcode von Treibern bereit (siehe Punkt 5). Man sollte sich daher möglichst vor dem Kauf darüber informieren, ob eine Hardware unter Linux läuft und mit welchen Einschränkungen gegebenenfalls zu rechnen ist. Eine Suche im Internet hilft fast immer weiter. Bei Notebooks ist darauf zu achten, dass wirklich alle Komponenten unterstützt werden. Manchmal gibt es kleine, aber ärgerliche Fehlfunktionen. Bei einigen Modellen lässt sich beispielsweise die Bildschirmhelligkeit nicht regeln, der Lautsprecher bleibt stumm oder Bluetooth funktioniert nicht. Teilweise lässt sich das Problem mit einer Änderung der Konfiguration umgehen, manchmal ist aber keine Lösung verfügbar.

2. Treiber und Firmware finden

Wenn ein Gerät unter Linux nicht funktioniert, ermitteln Sie zuerst, um welches Gerät es sich genau handelt. Dazu starten Sie in einem Terminal

```
lsusb
```

Bei einer PCI-Steckkarte oder einer Onboard-Komponente verwenden Sie

```
lspci
```

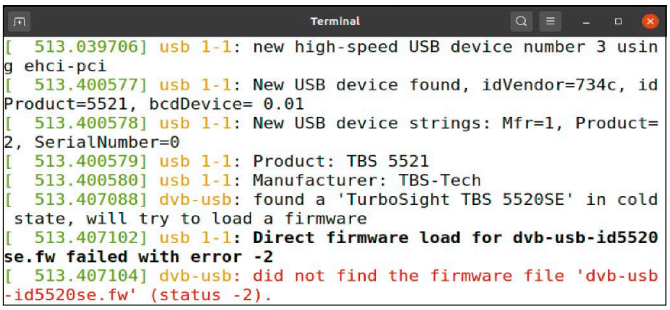
Hängen Sie den Parameter „-v“ an, um ausführlichere Informationen zu erhalten. Bei lspci verwenden Sie zusätzlich die Option „-n“, um sich auch die Geräte-ID ausgeben zu lassen. Eine Geräte-ID besteht aus zwei Werten, die mit einem Doppelpunkt getrennt sind, beispielsweise „734c:5521“. Der erste Teil gehört zum Hersteller, der zweite zum Gerät. Mit der ermittelten ID füttern Sie eine Suchmaschine, um weitere Informationen einzuholen.

Weitere Infos liefert der Befehl

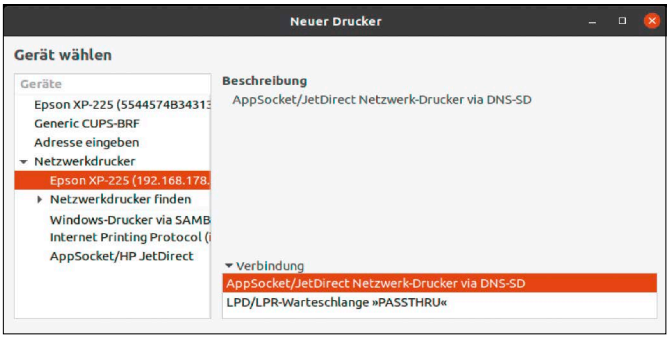
```
dmesg
```

Wenn es sich um ein USB-Gerät handelt, trennen Sie es vom Rechner und verbinden Sie es wieder. Dmesg gibt Kernel-Meldungen und Nachrichten geladener Treiber aus (siehe ab Seite 74). Erscheint hier beispielsweise nur „New USB device found“, aber kein Hinweis auf den Treiber, dann ist auch keiner verfügbar. Ihnen bleibt dann nur, auf einen neueren Kernel zu warten oder den Treiber aus dem Quelltext – wenn verfügbar – selbst zu erstellen (siehe Punkt 5). Manchmal sehen Sie eine Meldung wie „did not find the firmware file“, oft mit Angabe der benötigten Firmwaredatei. Das

kommt vor allem bei WLAN-Sticks oder TV-Adaptern vor. Suchen Sie nach der Firmware im Internet, laden Sie die Datei herunter und kopieren Sie sie iwn den Ordner „/lib/firmware“. Nach Trennen und Neuverbinden des USB-Geräts sollte es jetzt funktionieren.



Das Kernel-Protokoll (dmesg) gibt Auskunft über Fehler. Einige DVB-TV-Geräte und WLAN-Adapter benötigen neben dem Treiber auch noch eine Firmwaredatei.



Drucker einrichten: Viele Drucker findet Linux automatisch und richtet sogar einen Herstellertreiber ein. Netzwerkdrucker sind ebenfalls mit wenigen Klicks schnell konfiguriert.

3. Probleme mit WLAN-Adaptern

WLAN-Adapter erkennt Linux automatisch, wenn sie durch ein Kernel-Modul unterstützt werden. Bei den allermeisten Notebooks mit integriertem WLAN-Chipsatz ist das der Fall. Nach einem Klick auf das Netzwerksymbol sehen Sie die Funknetzwerke in der Umgebung. Klicken Sie das gewünschte WLAN an, geben Sie den WPA-Schlüssel ein und klicken Sie auf „Verbinden“.

Wird kein Funknetzwerk angezeigt, prüfen Sie, ob der Adapter aktiviert ist. Bei vielen Notebooks lässt sich der WLAN-Adapter über eine Tastenkombination zusammen mit einer F-Taste ein- und ausschalten. Sollte trotzdem kein WLAN auftauchen, fehlt der nötige Treiber oder die passende Firmwaredatei. Sehen Sie unter *www.pcwelt.de/NH3DEi* nach, ob es Informationen zu diesem Gerät gibt. Einige Adapter lassen sich über Tricks zur Zusammenarbeit bewegen. In der Regel ist es aber zuverlässiger, für wenige Euro einen von Linux unterstützten WLAN-Stick zu kaufen.

4. Drucker und Scanner einrichten

Netzwerkdrucker und Scanner richten Sie unter Ubuntu 20.04 in den „Einstellungen“ unter „Drucker“ ein. Ein USB-Drucker wird in der Regel automatisch erkannt und installiert. Bei einigen Modellen erscheint der Dialog „Treiber wählen“. Nach einem Klick auf „Anwenden“ lädt Ubuntu den Druckertreiber herunter und installiert ihn. Klicken Sie auf „Einen Drucker hinzufügen“. Dann werden Netzwerkdrucker oder USB-Geräte angezeigt, für die ein Treiber verfügbar ist. Wählen Sie den Drucker aus und klicken Sie auf „Hinzufügen“.

Für die manuelle Druckereinrichtung gehen Sie auf „Zusätzliche Druckereinstellungen“ und klicken auf „Hinzufügen“. Unter „Geräte“ tauchen USB-Drucker auf, nach einem Klick auf „Netzwerkdrucker“ sehen Sie auch Geräte, die Ubuntu im Netzwerk gefunden hat. Zur Einrichtung eines Druckers klicken Sie ihn an und dann auf „Vorwärts“. Folgen Sie den Anweisungen des Assistenten. Linux Mint erkennt Drucker am USB-Anschluss meist ebenfalls automatisch. Über das Menü und „Systemverwaltung → Drucker“ lassen sich Drucker so einrichten wie für Ubuntu beschrieben.

Taucht der Drucker nicht in der Liste auf, benötigen Sie einen Treiber des Herstellers. Diesen finden Sie über eine Suche im Downloadbereich des Herstellers etwa bei Epson, HP, Brother oder Canon (siehe Tabelle). Herstellertreiber bieten meist mehr Funktionen als der Standardtreiber.

5. Treiber selbst kompilieren

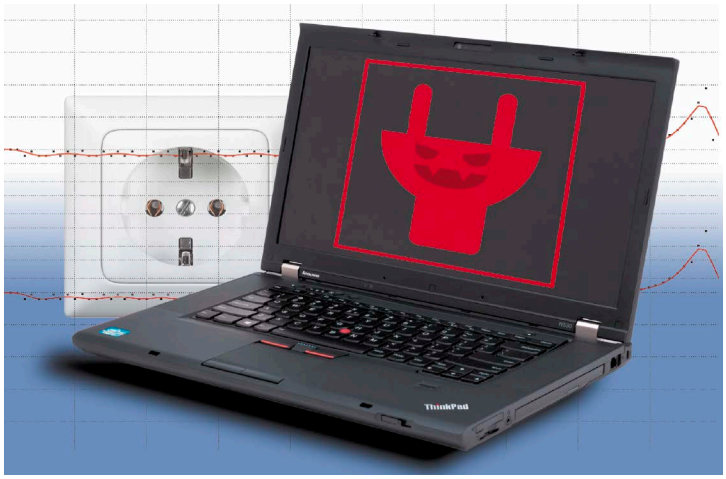
Wenn der Linux-Kernel ein Gerät nicht unterstützt, kann man den Treiber (Kernel-Modul) auch selbst kompilieren. Programmierkenntnisse sind nicht erforderlich, aber man sollte mit den Entwicklungswerkzeugen einigermaßen vertraut sein. Den Quellcode für den Treiber erhält man vom Hardwarehersteller oder es gibt bereits ein Projekt, das sich mit dem Treiber beschäftigt. Das findet man beispielsweise über die Suche nach der Geräte-ID (siehe Punkt 2) im Internet. Die erforderlichen Schritte sind bei jedem Treiber andere, sollten aber vom Entwickler dokumentiert sein.

Eine Herausforderung stellt Quellcode dar, der für ältere oder ganz aktuelle Kernel erstellt wurde. Bei Kompilieren wird die Kernel-Version abgefragt und dazu passender Code in den Treiber eingebaut. Ist dem Quellcode die Version unbekannt, lässt sich der Treiber nicht erstellen oder nicht laden. Es ist daher wichtig, die Dokumentation genau zu lesen, um zu sehen, für welche Linux- beziehungsweise Kernel-Version sich die Software eignet. ■

LINUX-TREIBER: DOWNLOADS UND INFOS

Hersteller	Geräteklasse	Internet
Alle	DVB-TV-Adapter	*www.pcwelt.de/yoA4A1*
Alle	für Ubuntu zertifizierte Hardware	*www.pcwelt.de/Z4Bc86*
Alle	WLAN-Adapter	*www.pcwelt.de/NH3DEi*
AMD	Grafikkarten	*www.pcwelt.de/lwsB48*
Brother	Drucker, Scanner	*www.pcwelt.de/AOve2K*
Canon	Drucker, Scanner	*www.pcwelt.de/9lx90f*
Epson	Drucker, Scanner, Multifunktionsgeräte	*www.pcwelt.de/po1lvX*
HP	Drucker, Multifunktionsgeräte	*www.pcwelt.de/ZIi0pr*
Intel	Grafikkarten	*www.pcwelt.de/maCHyY*
Nvidia	Grafikkarten	*www.pcwelt.de/vXxzwP*

Energiehunger von Notebooks bändigen



Notebooks laufen prima unter Linux. Im direkten Vergleich zu Windows auf demselben Gerät fällt aber oft die kürzere Akkulaufzeit auf. Mit ein paar Einstellungen lässt sich das verbessern.

VON THORSTEN EGGELING UND DAVID WOLSKI

Im Fokus der Linux-Entwickler stehen meist Server, wo Linux am häufigsten anzutreffen ist. Die knapp bemessene Zeit für die Treiberentwicklung wird daher vorwiegend in die Verbesserung der Rechenleistung investiert. Stromsparfunktionen, die zudem spezielle Anpassungen an das jeweilige Gerät erfordern, werden oft nicht ausreichend optimiert. Außerdem sind einige Stromsparfunktionen aus Kompatibilitätsgründen nach der Installation eines Linux-Systems noch nicht aktiviert. Wenn der Akku nicht lange genug durchhält, kann man das ändern. Zwei Tools helfen bei der Konfiguration.

Energiebedarf des Notebooks ermitteln

Vor der Optimierung sollte man den Leistungsbedarf des Geräts messen. Später lässt sich dann beurteilen, ob eine Maßnahme tatsächlich etwas bewirkt. Verwenden Sie in einem Terminal die Befehlszeile

```
cat /sys/class/power_supply/BAT?/
  power_now
```

Bei abgezogenem Netzteil erhalten Sie einen Wert in Mikrowatt, der den aktuellen Energiebedarf des Linux-Systems liefert. Teilt man den beispielsweise angezeigten Wert „19980000“ durch 1 000 000, ergibt das 19,98 Watt. Ebenfalls im Terminal arbeitet der Energiemonitor Powertop von Intel, der zahlreiche Informationen liefert. Das Tool liegt in den Standard-Paketquellen aller wichtigen Linux-Distributionen bereit. Nutzer von Debian, Ubuntu oder Linux Mint installieren Powertop mit

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

und erhalten nach dem Aufruf

```
sudo powertop
```

nach einigen Sekunden das Ergebnis. Sie sehen die Entladungsrate in Watt und den Energiebedarf einzelner Prozesse. Mit der Tab-Taste navigieren Sie zur jeweils nächsten Kategorie.

Auf der Seite „Einstellbarkeit“ gibt Powertop eine Reihe von Empfehlungen zur Systemkonfiguration aus, die aktivierte und deaktivierte Stromsparfunktionen zeigt. Temporär aktiviert ein Druck auf die Eingabetaste eine einzelne Option. Um alle vorgeschlagenen zusätzlichen Stromsparfunktion einzuschalten, verwenden Sie diesen Befehl:

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

Da dies nur für die aktuelle Sitzung gilt, sollte ein Cronjob diesen Befehl bei jedem Systemstart starten. Nach der Eingabe von

```
sudo crontab -e
```

tragen Sie den zusätzlichen Job

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

als weitere Zeile ein.

Ruhezustand zum Energiesparen nutzen

Wenn man den Rechner gerade nicht aktiv benutzt, hilft der Ruhezustand (Suspend) beim Stromsparen. Die Funktionen dafür sind standardmäßig konfiguriert. Bei Ubuntu 20.04 beispielsweise klicken Sie auf das Symbol rechts oben in der Leiste und gehen auf „Ausschalten / Abmelden → Bereitschaft“. In diesem Modus wird der Hauptspeicher weiter mit Strom versorgt. Wenn Sie den Rechner per Tastatur oder Maus wieder aufwecken, laufen weiterhin alle zuvor gestarteten Programme. Allerdings funktioniert das nicht immer ohne Probleme. Manchmal wacht der Rechner nicht auf oder die WLAN-Verbindung funktioniert nicht mehr. Sehen Sie im Firmwaresetup (Bios) nach, ob es Optionen für die Stromsparzustände gibt. Sofern vorhanden, sollte „Suspend to RAM (S3)“ aktiviert sein.

In den „Einstellungen“ können Sie bei Ubuntu 20.04 unter „Energie“ festlegen, ob der Rechner nach einer bestimmten Zeit automatisch in Bereitschaft gehen soll. Außerdem gibt es Optionen für die automatische Abschaltung von WLAN und Bluetooth bei Nichtbenutzung.

Nutzer von Linux Mint finden ähnliche Optionen über das Menü und „Einstellungen → Energieverwaltung“.

Schlafzustand (Hibernation) aktivieren

Dieser Modus ist standardmäßig nicht verfügbar und muss manuell aktiviert werden. Im Schlafzustand wird der Inhalt des Hauptspeichers auf die Festplatte geschrieben und der Rechner dann komplett ausgeschaltet. Dadurch lässt sich mehr Energie sparen als beim Ruhezustand. Ubuntu 20.04 und Linux Mint 20 verwenden die Swapdatei „/swapfile“ als Auslagerungsdatei. Darin wird auch der RAM-Inhalt beim Schlafzustand gespeichert.

Schritt 1: Die Swapdatei muss dafür doppelt so groß sein wie der Hauptspeicher im Gerät. Die Größe von Swapfile und RAM ermitteln Sie mit diesen beiden Befehlszeilen:

```
swapon -s
cat /proc/meminfo
```

Schritt 2: Ist die Swapdatei nicht vorhanden oder zu klein, erstellen Sie eine neue – bei acht GB RAM beispielsweise mit diesen vier Zeilen:

```
sudo dd if=/dev/zero of=/swapfile
  bs=1M count=16000
sudo chmod 600 /swapfile
sudo mkswap /swapfile
sudo swapon -v /swapfile
```

Schritt 3: Kontrollieren Sie die Einbindung der Swapdatei in der Datei „/etc/fstab“ und fügen Sie folgende Zeile bei Bedarf neu hinzu (*sudo nano /etc/fstab*):

```
/swapfile none swap sw 0 0
```

Starten Sie danach Linux neu.

Schritt 4: Installieren Sie jetzt zwei zusätzlich Softwarepakete:

```
sudo apt install hibernate uswsusp
```

Danach ermitteln Sie mit

```
sudo swap-offset /swapfile
```

den Offset und mit

```
findmnt -no SOURCE,UUID -T /
  swapfile
```

die UUID für die Partition, auf der die Datei liegt.

Schritt 5: Öffnen Sie die Grub-Konfigurationsdatei mit diesem Befehl:

```
sudo nano /etc/default/grub
```

Ändern Sie die Angaben wie folgt:

```
GRUB_CMDLINE_LINUX_DEFAULT="quiet
  splash resume=UUID=[UUID] resume_
  offset=[Offset]"
```

Für die Platzhalter in eckigen Klammern setzen Sie die in Schritt 4 ermittelte UUID und den Offset ein.

Schritt 6: Öffnen beziehungsweise erstellen Sie die Konfigurationsdatei für die initiale Ramdisk:

```
sudo nano /etc/initramfs-tools/
  conf.d/resume
```

Tragen Sie dort diese Zeile ein:

```
resume=UUID=[UUID] resume_
  offset=[Offset]
```

Die Platzhalter ersetzen Sie wieder wie in Schritt 5.

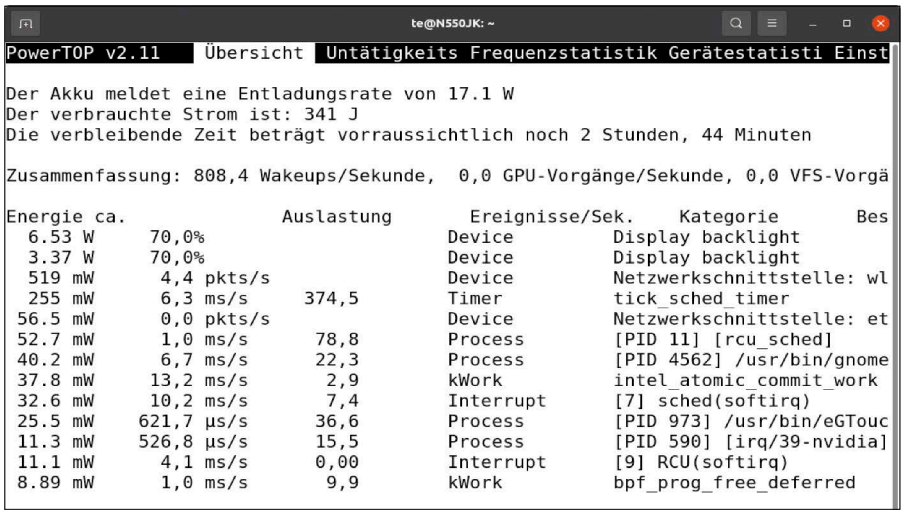
Schritt 7: Um die Konfiguration zu aktualisieren, verwenden Sie diese zwei Befehle:

```
sudo update-grub
sudo update-initramfs -u -k all
```

Starten Sie Linux neu. Danach aktivieren Sie den Ruhezustand:

```
sudo systemctl hibernate
```

Wenn das System nach dem Einschalten des Rechners anstandslos fortgesetzt wird, können Sie den Schlafzustand verwenden. Für die bequemere Nutzung installieren Sie unter Ubuntu 20.04 die Gnome-Erweiterung „Simpler Off Menu“ (*https://m6u.de/som*). „Hibernate“ lässt sich damit neben „Bereitschaft“ in das Menü der Systemleiste einbauen. Damit sich Gnome-Erweiterungen über die Website installieren lassen, aktivieren Sie zuerst das Firefox-Add-on „Gnome Shell integration“ (*https://m6u.de/gsi*) und installieren das Paket „chrome-gnome-shell“. Wer Linux Mint Cinnamon nutzt, installiert das Applet „Shutdown Menu with Icons“ („Herunterfahren-Menü mit Icons“). Wenn Sie bisher noch keine Applets eingerichtet haben, finden Sie eine Anleitung unter *www.pcwelt.de/2374433*.



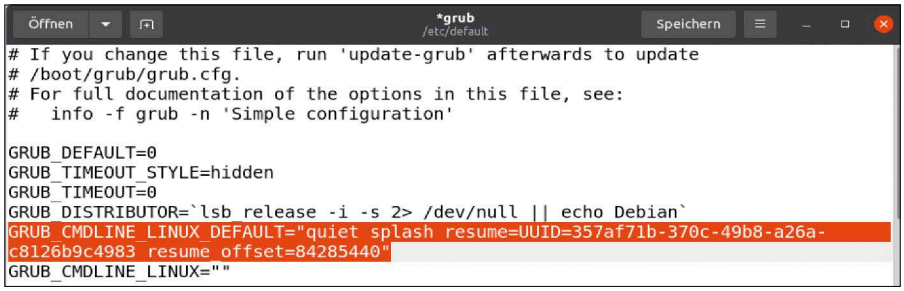
Energiebedarf ermitteln: Powertop zeigt die Entladungsrate des Akkus und die Leistungsaufnahme von Geräten und Prozessen an. Außerdem hilft das Tool bei der Optimierung.

Stromsparfunktionen über TLP aktivieren

Zahlreiche Feineinstellungen zum Betrieb mit möglichst wenig Energiebedarf fasst das Projekt „Linux Advanced Power Management“ (TLP) zusammen. Die Installation von TLP erfolgt unter Debian/Ubuntu/Mint mittels

```
sudo apt-get install tlp
```

und aktiviert ein grundlegendes Set an Stromsparfunktionen. Die Konfiguration erfolgt über die Datei „/etc/tlp.conf“, die englischsprachige Kommentare zu jeder Einstellung enthält. Ausführliche Erklärungen auf Deutsch finden Sie unter *http://thinkwiki.de/TLP_Einstellungen*. ■



Hibernate-Modus: Damit Linux weiß, wo der RAM-Inhalt für den Schlafzustand gespeichert werden soll, muss die UUID des Laufwerks in der Datei „/etc/default/grub“ konfiguriert sein.

Festplatten und SSDs unter Linux

Speicherlaufwerke jeder Art arbeiten unter Linux praktisch immer zuverlässig und ohne Auffälligkeiten. Einige Stellschrauben für die Optimierung bietet das System aber dennoch.

VON THORSTEN EGGELING

Festplatten und SSDs sind die wichtigsten Komponenten im Computer, weil sie für die verlässliche Datenspeicherung zuständig sind. Es ist mehr als ärgerlich, wenn eine Festplatte ausfällt und dabei wichtige Dateien verloren gehen. Die mechanischen Laufwerke sind empfindlich gegen Sturz oder Stoß und auch zu hohe Temperaturen können einen Ausfall herbeiführen. SSDs sind deutlich robuster, obwohl auch hier – wie bei allen elektronischen Bauelementen – die Wärmeabfuhr gewährleistet sein muss. Wie es um die Gesundheit eines Laufwerks bestellt ist und ob es die erwartbare Transferrate liefert, kann man unter Linux mit Bordmitteln und zusätzlichen Tools ermitteln.

Laufwerke und Kernel-Treiber

SATA-Controller für den Anschluss von Festplatten und SSDs sind in jedem PC oder Server zu finden. Die nötigen Treiber sind im Linux-Kernel enthalten und sorgen dafür, dass die Laufwerke frühzeitig beim Systemstart angesprochen werden können. Auch relativ neue Adapter für das schnelle USB 3.2 Gen2x2 oder für Thunderbolt bereiten unter Linux keine Probleme. Bei externen USB-Laufwerken sollte die grundsätzliche Inbetriebnahme immer gelingen. Wenn ein USB-Laufwerk sich im Betrieb spontan aushängt oder nicht automatisch erkannt wird, hat das meist andere Gründe: fehlerhafte USB-Ports, qualitativ minderwertige Kabel oder eine unzureichende Stromversorgung. Davon sind dann alle Betriebssysteme betroffen.

Laufwerke und Partitionen verwalten

Einen guten Überblick über die Laufwerke liefert das Tool Gnome-Disks (Paket: „gnome-disk-utility“). Ubuntu-Nutzer finden es mit einer Suche nach „Laufwerke“ über „Aktivitäten“, bei Linux Mint gehen Sie im Menü auf „Zubehör → Laufwerke“. Das Werkzeug kann Partitionen formatieren, löschen und die Größen ändern. Die Optionen erreichen Sie nach Auswahl einer Partition per Klick auf die Schaltfläche mit den Zahnrädern oder Umschalt-F10. Hier gibt es auch den Menüpunkt „Leistungstest für Partitionen“, über den Sie Lese- und Schreibgeschwindigkeit messen.

Weitere interne Festplatten erreichen Sie im Dateimanager unter „Andere Orte“ (Linux Mint: „Gehe zu → Rechner“). Soll eine Partition bereits beim Systemstart eingebunden werden, klicken Sie die gewünschte Partition an und gehen nach Umschalt-F10 auf „Einhängeoptionen bearbeiten“. Schalten Sie „Vorgaben der Benutzersitzung“ aus. Bei Bedarf ändern Sie den Pfad hinter „Einhängepunkt“ beispielsweise auf die Bezeichnung der Partition. Danach können Sie die Partition über die „Play“-Schaltfläche einhängen.

Gnome-Disks zeigt – sofern ein Sensor verfügbar ist – die Temperatur von Laufwerken an und gibt Infos zum Zustand. Wer es genauer wissen will, drückt die Tastenkombination Strg-S und kann dann die SMART-Werte ermitteln (Self-Monitoring, Analysis and Reporting Technology). Hinter „Allgemeine Einschätzung“ sollte „Das Laufwerk ist in Ordnung“ stehen. Andernfalls ist es Zeit, an einen Austausch zu denken. Bei SSDs sehen Sie sich die Zeile „wear-leveling-count“ an. In der Spalte „Normalisiert“ steht bei neuen SSDs der Wert „100“, der sich mit der Zeit reduziert. Bevor er nahe „0“ ist, sollten Sie das Laufwerk ersetzen.

Unbenutzte Laufwerke abschalten

Eine zweite Festplatte, die beispielsweise nur bei Backups zum Einsatz kommt, muss nicht ständig laufen. In Gnome-Disks rufen

Sie mit Strg-E die „Laufwerkseinstellungen“ auf. Aktivieren Sie die Option „Einstellungen für Bereitschaft-Wartezeit anwenden“ und stellen Sie darunter den Zeitraum ein, nach dem das Laufwerk automatisch in den Stand-by-Modus wechseln soll. Zusätzlich kann es auch die Registerkarte „APM“ (Advanced Power Management) geben, auf der Sie alternativ den Regler in Richtung „Energie sparen“ (schnelleres Stand-by) oder „Leistung verbessern“ schieben. Wenn Laufwerke diese Optionen nicht anbieten, sind die Einstellungen nicht verfügbar.

Über Strg-E und „Jetzt in Bereitschaft gehen“ lässt sich die Festplatte sofort abschalten, was in der Regel auch hörbar ist. Beachten Sie, dass zu viele Start/Stop-Zyklen zu vorzeitigem Verschleiß führen. Im Terminal lässt sich mit

```
sudo hdparm -C /dev/sd[x]
```

kontrollieren, ob die Abschaltung tatsächlich erfolgt ist. Bei einer laufenden Festplatte gibt das Tool „active/idle“ aus, „standby“ zeigt den Bereitschaftsmodus.

Sollte der Bereitschaftsmodus nicht funktionieren, hilft das Tool hd-idle weiter. Wie es sich installieren und verwenden lässt, lesen Sie auf der englischsprachigen Webseite *http://hd-idle.sourceforge.net*. hd-idle unterstützt auch USB-Laufwerke.

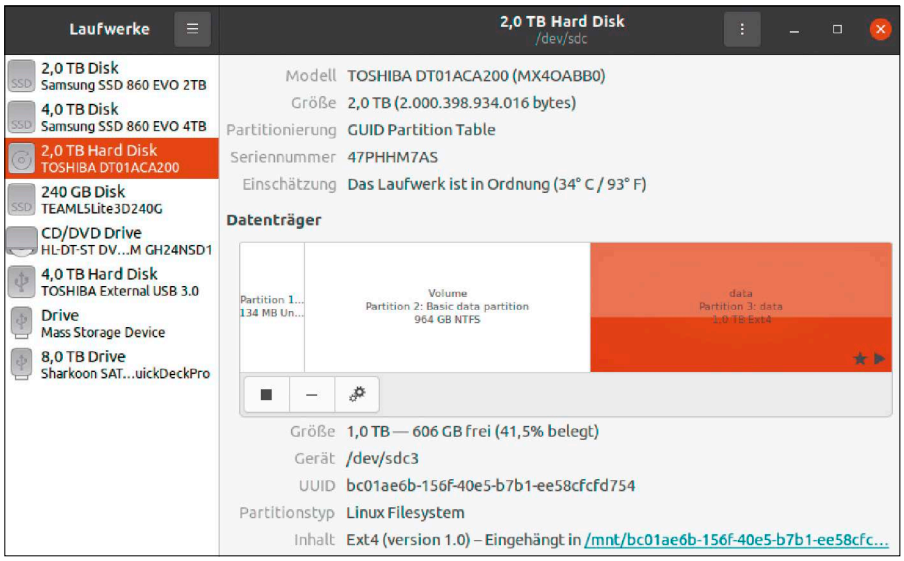
Tipp: Wer umgekehrt eine ständige Abschaltung von USB-Laufwerken verhindern möchte (um Wartezeiten beim Zugriff zu vermeiden), kann dafür einen Cronjob verwenden. Nach

```
sudo crontab -e
```

fügen Sie folgende Zeile an:

```
*/5 * * * * /bin/touch /dev/sd[x] &>/
 dev/null
```

Im Beispiel erfolgt ein Zugriff alle fünf Minuten. Ersetzen Sie den Platzhalter „[x]“ durch die Bezeichnung des Laufwerks.



Werkzeug für Laufwerke: Das Tool Gnome-Disks bietet die wichtigsten Funktionen rund um Festplatten und SSDs. Sie können Partitionen verändern oder Einhängepunkte festlegen.

Festplatten abschalten: Über Gnome-Disks legen Sie fest, wann ein Laufwerk automatisch in den Stand-by-Modus wechseln soll. Das funktioniert allerdings nicht mit allen Geräten.

Firmwareupdates unter Linux

Für Festplatten und SSDs gibt es Firmwareupdates, die Fehler beheben oder die Leistung verbessern. Die Hersteller stellen meist nur Windows-Tools bereit. Ubuntu 20.04 und Linux Mint 20 bringen ein Tool mit, über das sich die Updates auch unter Linux durchführen lassen. Es sollte standardmäßig installiert sein. Wenn nicht, holen Sie das mit

```
sudo apt install fwupdate
```

nach. Unter Gnome läuft fwupd automatisch im Hintergrund und das Gnome-Software-Center informiert über verfügbare Firmwareaktualisierungen. Wer das kontrollieren möchte, erhält im Terminal mit

```
sudo fwupdmgr get-devices
```

eine Liste der erkannten Geräte. Die drei Befehlszeilen

```
sudo fwupdmgr refresh
sudo fwupdmgr get-updates
sudo fwupdmgr update
```

bringen die Firmwaredatenbank auf den neuesten Stand, laden Updates herunter – wenn vorhanden – und führen die Installation durch. Bisher steuern noch nicht alle Hersteller zur Firmwaredatenbank bei. Zur Zeit sind vor allem Dell, HP, Lenovo und Logitech vertreten.

Für eine Suche in der Datenbank nach Hersteller und Gerätenamen gehen Sie auf *https://fwupd.org*. ■

SSDS MIT TRIM-BEFEHL OPTIMIEREN

Wenn Sie eine Datei löschen, wird der Platz im Dateisystem als wiederbeschreibbar markiert. Die SSD weiß davon jedoch nichts, daher muss zur Optimierung dem Controller ab und zu eine Liste mit den freien Blöcken übermittelt werden. Das funktioniert jedoch nur, wenn die SSD den Trim-Befehl unterstützt, was Sie mit

```
sudo hdparm -I /dev/sd[x] | grep -i TRIM
```

herausfinden. Die Ausgabe sollte „Data Set Management TRIM supported“ oder ähnlich lauten. Wenn nicht, lässt sich daran nur etwas über ein Firmwareupdate ändern. Andernfalls überlassen Sie Ubuntu oder Linux Mint die automatische Optimierung. Sie können fstrim auch manuell ausführen, etwa um sich von der korrekten Funktion zu überzeugen:

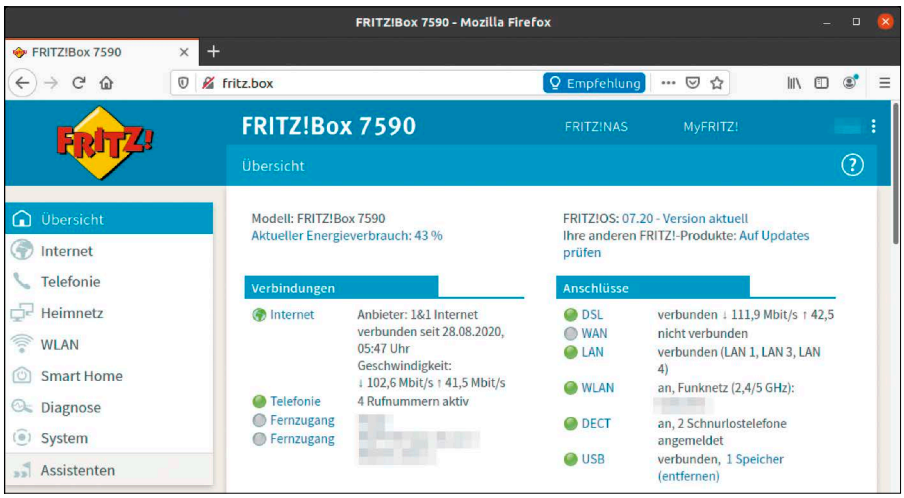
```
sudo fstrim -v -a
```

In der Ausgabe sehen Sie, wie viele Bytes freigegeben wurden. Es sollte sich nur um einen geringen Wert handeln, wenn das Tool periodisch und automatisch vom System ausgeführt wird.

Netzwerkprobleme lösen

Die Konfiguration des Netzwerks läuft unter Linux weitestgehend automatisch ab. Sollte das ausnahmsweise nicht zuverlässig klappen, hilft Ihnen dieser Artikel bei der Fehlersuche.

VON THORSTEN EGGELING



Internetzugriff: Der Router zeigt an, ob eine Internetverbindung besteht. Wenn nicht, ist die Verbindung zum Anbieter gerade unterbrochen oder die Zugangsdaten sind falsch.

Am Netzwerk sind mehrere Komponenten beteiligt: Router, Ethernet-Kabel, WLAN, Netzwerkadapter, Treiber für die Adapter, nicht zuletzt der Internetanbieter. Bei der Suche nach Fehlern führt nur eine systematische Herangehensweise zum Ziel. Dabei sollte man einige Fehlerursachen schnell ausschließen und sich Schritt für Schritt der Fehlerquelle nähern. Probleme mit Samba-Netzwerkfreigaben behandelt ein eigener Ratgeber unter *www.pcwelt.de/1903700*.

1. Netzwerkprobleme lokalisieren

Man kann im Netzwerk die folgenden Problembereiche unterscheiden:

A: Der Internetzugriff funktioniert bei keinem Gerät im Netzwerk. Der Browser meldet „Seite wurde nicht gefunden". Rechner im eigenen Netzwerk sind aber erreichbar, beispielsweise Dateifreigaben. Das Netzwerk funktioniert also grundsätzlich, aber der Internetzugang nicht. Hier liegt eine Störung beim DSL-Anschluss vor oder der Router ist falsch konfiguriert oder defekt (siehe Punkt 2 und 3).

B: Nur bei einem einzelnen Rechner funktioniert der Internetzugang über den Webbrowser nicht, andere Rechner im Netzwerk sind erreichbar. Hier ist wahrscheinlich der Browser falsch konfiguriert oder eine Einstellung verhindert den Internetzugang (siehe Punkt 7).

C: Ein einzelner Rechner hat keinen Internetzugriff, Geräte im lokalen Netzwerk sind dort ebenfalls nicht erreichbar. Der betroffene Rechner hat keine Netzwerkverbindung. Prüfen Sie die Netzwerkkonfiguration und die Funktion des Netzwerkadapters (siehe Punkt 6).

D: Kein Rechner kann auf das Internet zugreifen, das lokale Netzwerk ist auch nicht zu erreichen. Das Netzwerk funktioniert hier grundsätzlich nicht. Wahrscheinlich ist der Router defekt oder falsch konfiguriert (siehe Punkt 2, 3 und 4). Tritt das Problem im WLAN auf, prüfen, Sie die WLAN-Konfiguration des Routers (siehe Punkt 5).

2. Verbindung zum Router testen

Prüfen Sie, ob eine Verbindung zum DSL-Router möglich ist. Verbinden Sie einen PC oder ein Notebook direkt per Netzwerkkabel mit dem Router und starten Sie Linux neu. Geben Sie im Browser die IP-Adresse des Routers ein, etwa „http://192.168.0.1" oder „http://192.168.1.1". Bei einer Fritzbox lautet die Adresse standardmäßig „http://192.168.178.1", alternativ funktioniert auch „http://fritz.box". Wenn diese Verbindung nicht funktioniert und die Webseite des DSL-Routers nicht im Browser erscheint, ist der Router falsch konfiguriert oder defekt. Wiederholen Sie den Test mit einem anderen PC oder Notebook und einem anderen Ethernet-Kabel. Prüfen Sie auch mit dem Ping-Befehl (Punkt 6), ob Sie den DSL-Router erreichen können.

3. Konfiguration des DSL-Routers prüfen

Wenn Sie die Konfigurationsseite Ihres DSL-Routers aufgerufen haben, sollten Sie die wichtigsten Einstellungen prüfen und eventuell korrigieren. Die meisten Router zeigen schon auf der Übersichtsseite, ob eine Internetverbindung aufgebaut wurde. Bei einer Fritzbox beispielsweise steht unter „Verbindungen" hinter „Internet" dann „verbunden seit", andernfalls „nicht verbunden". Konnte keine Verbindung zum Internetanbieter aufgebaut werden, prüfen Sie, ob die Anmeldeinformationen unter „Internet → Zugangsdaten" wirklich stimmen. Unter „System → Ereignisse" finden

Sie Infos über die Ursache einer fehlgeschlagenen Verbindung. Der Fehler muss nicht unbedingt bei Ihnen liegen. Vielleicht ist gerade der Anschluss gestört.

4. DHCP-Einstellungen kontrollieren

Jedes Gerät im Netzwerk erhält seine Konfiguration vom Router per DHCP. Es darf nur einen DHCP-Server im Netzwerk geben, sonst erhalten die Rechner eine falsche Konfiguration. Prüfen Sie die DHCP-Einstellungen des Routers. Bei einer Fritzbox gehen Sie auf „Heimnetz → Netzwerk“. In der Tabelle sollten alle Netzwerkgeräte mit IP-Nummer auftauchen. Gehen Sie auf die Registerkarte „Netzwerkeinstellungen“ und klicken Sie auf „IPv4-Konfiguration“. Hier muss das Häkchen vor „DHCP-Server aktivieren“ gesetzt sein.

5. WLAN-Einstellungen prüfen

Damit eine WLAN-Verbindung klappt, müssen alle Geräte die gleiche Verschlüsselungsmethode und das gleiche Kennwort verwenden. In der Regel sollte das als ziemlich sicher geltende WPA2 aktiv sein, das von fast allen WLAN-Geräten unterstützt wird. Bei einer Fritzbox finden Sie die Einstellung unter „WLAN → Sicherheit“. Stellen Sie bei Ihrem PC ebenfalls WPA2 ein. Linux erkennt die Verschlüsselungsmethode in der Regel automatisch. Achten Sie darauf, dass die Option „Alle neuen WLAN-Geräte zulassen“ aktiviert ist. Andernfalls können sich neue Geräte nicht anmelden. Unter „WLAN → Funknetz“ sehen Sie – je nach Routermodell – die aktivierten Frequenzbänder. Hier sollten 2,4 und fünf GHz aktiviert sein, damit auch ältere Geräte das WLAN nutzen können.

6. Funktion des Netzwerks testen

Unter Linux gibt im Terminal der Befehl

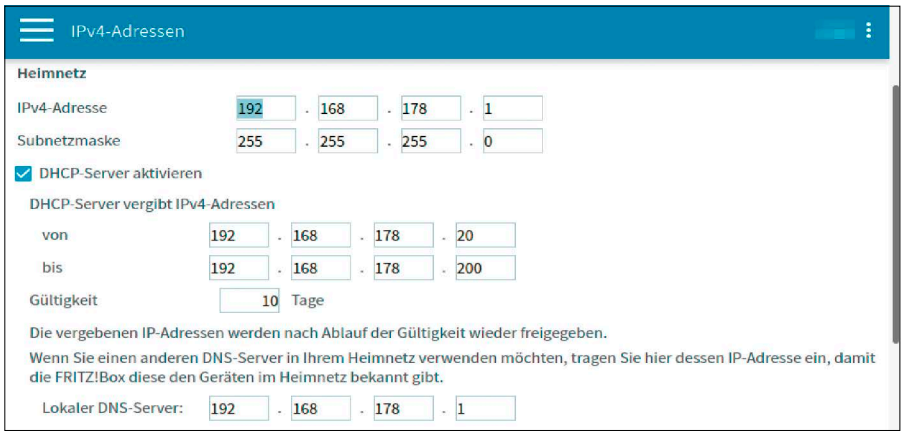
```
ip addr
```

Auskunft darüber, welche IP-Adresse der Netzwerkadapter erhalten hat. Der Befehl

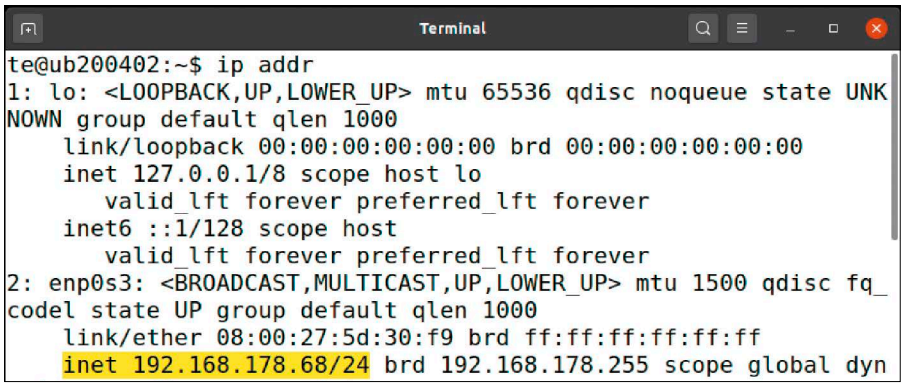
```
route -n
```

liefert die Information zum Default-Gateway. In der Spalte „Router“ muss die IP-Nummer des Routers stehen, beispielsweise „192.168.178.1“ bei einer Fritzbox.

Die IP-Adresse muss aus dem Bereich des Routers stammen, damit eine Verbindung möglich ist. Eine abweichende Adresse deutet auf einen zweiten DHCP-Server hin. Den sollte es in der Regel nicht geben, außer die Verbindung erfolgt über einen WLAN-Access-Point. In diesem Fall prüfen Sie, ob der Access Point eine Verbindung zum DSL-Router herstellen kann. Sollte keine IP-Adresse zu sehen sein, ist der Netzwerkadapter oder das Ethernet-Kabel defekt.



Adressverteilung: Damit alle Geräte im Netzwerk eine IP-Adresse erhalten, muss der DHCP-Server aktiviert sein. Er übermittelt auch die Gateway- und DNS-Adresse an die Netzgeräte.



Konfiguration des Netzwerkadapters: „ip addr“ zeigt die IP-Adresse an, die der Netzwerkadapter erhalten hat. Diese muss aus dem IP-Bereich des DSL-Routers stammen.

Testen Sie die Erreichbarkeit anderer Netzwerkgeräte mit der folgenden Befehlszeile im Terminal:

```
ping 192.168.178.1 -c 5
```

Die IP-Nummer ersetzen Sie durch die Ihres Routers oder eines anderen Geräts. Sie erhalten ein Ergebnis wie

```
64 Bytes von 192.168.178.1: icmp_
  seq=1 ttl=64 Zeit=0.882 ms
```

Diese Verbindung sollte in jedem Fall funktionieren, sonst könnten Sie auch die Konfigurationsoberfläche des Routers nicht im Browser aufrufen. Gibt ping „Zielhost nicht erreichbar“ aus, dann ist die Verbindung zum Router unterbrochen oder der andere PC ist nicht aktiv.

Wie das lokale Netz lässt sich auch der Internetzugang entsprechend testen:

```
ping google.de -c 5
```

Auch hier erhalten Sie eine Antwort in der Form „64 byte from“. Wenn nicht, besteht keine Internetverbindung oder die Namensauflösung funktioniert nicht.

7. Browserkonfiguration

Wenn ping erfolgreich war, dann funktionieren Internetverbindung und Namensauflösung über DNS. Sollte der Browser trotzdem keine Webseiten anzeigen, prüfen Sie dessen Konfiguration, insbesondere bei Firefox mit dessen eigener Proxy-Konfiguration. Klicken Sie in den „Einstellungen“ unter „Verbindungs-Einstellungen“ auf „Einstellungen“. Standardmäßig ist hier „Proxy-Einstellungen des Systems verwenden“ aktiviert. Im Heimnetz sollte „Kein Proxy“ aktiviert sein. Nur wenn Sie tatsächlich einen Proxyserver betreiben, müssen Sie die passenden Einstellungen unter „Manuelle Proxy-Konfiguration“ eintragen. Deaktivieren Sie außerdem Add-ons, die den Zugriff auf Webseiten verhindern können, beispielsweise Werbeblocker. ■

Offene Türen im Netzwerk

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

VON STEPHAN LAMPRECHT

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

Wann Sie Nmap brauchen

Mit Nmap können Sie einen Rechner oder ein gesamtes Subnetzwerk auf offene Ports untersuchen. Das Werkzeug für die Kommandozeile hilft Ihnen herauszufinden, ob ein bestimmter Port auf dem Zielsystem geöffnet ist. Wie bei allen Sicherheitswerkzeugen gilt auch hier, dass Sie Ihre Untersuchungen auf eigene Systeme beschränken sollten. Im lokalen Netzwerk ist Nmap jederzeit erlaubt. Die nachfolgenden Beispiele verwenden aus diesem Grund ausschließlich lokale Adressen. Beachten Sie aber, dass der eigentlich sicherheitsrelevante Scan der Ihrer öffentlichen Adresse darstellt. Beschränken Sie sich beim Scannen öffentlicher IP-Adressen aber immer auf diejenige, die Ihr Router als Ihre eigene anzeigt (etwa die Fritzbox unter „Übersicht"), oder gegebenenfalls auf diejenige Ihres eigenen Webauftritts bei einem Internethoster. Beim Nmap-Scan fremder Adressen begehen Sie nicht nur einen unfreundlichen Akt, sondern können sich strafbar machen. Linux-Nutzer finden Nmap in den Paketquellen der Distribution. Wer das Werkzeug unter Windows einsetzen will oder eine bestimmte Version aus dem Quellcode kompilieren möchte, muss die Projektseite aufsuchen (*https://nmap.org/download.html*). Nmap ist ein Kommandozeilenprogramm, es gibt aber mit Zenmap auch ein grafisches Front-End, das die Aufträge an Nmap weiterreicht und dabei auch über die Nmap-Syntax informiert.

Geöffnete Ports analysieren

Ein physikalischer Server kann verschiedene Dienste parallel anbieten. Das NAS im Wohnzimmer kann beispielsweise über ein Terminal erreicht werden (SSH-Sitzung) und stellt eine Weboberfläche zur Verfügung (HTTP-Zugang). Damit sich die Datenpakete, die in der Regel über das gleiche Protokoll abgewickelt werden (heute in der Regel TCP/IP), nicht in die Quere kommen, werden die Dienste auf unterschiedlichen Ports bereitgestellt. Hier hat sich eine Reihe von Standards etabliert. Beispielsweise werden die Anfragen an einen Webserver üblicherweise über Port 80 abgewickelt, SSH über Port 22 und viele weitere (*https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports*).

Für eine erste Abfrage genügt der Terminalbefehl *nmap [Adresse/Adressraum]*, etwa:

```
nmap 192.168.178.10
```

Wenn Sie Zenmap verwenden, tragen Sie Einzeladresse oder Adressraum in das Feld

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

```
nmap -Pn 192.168.178.10
```

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

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

```
nmap -p 22 192.168.178.10
```

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

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

Closed: Es sind keine Verbindungen auf diesem Port möglich.

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

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

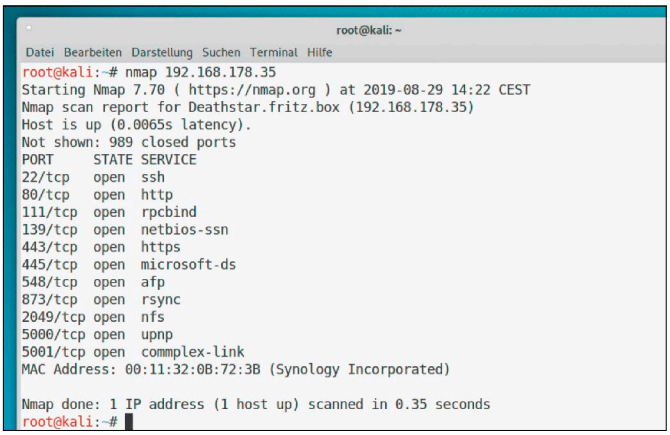
Alle Netzwerkgeräte finden

Die Annäherung eines Hackers an ein unbekanntes Netzwerk beginnt in der Regel mit der Abfrage der darin vorhandenen Rechner. Für diese „Host Discovery“gibt es mit Nmap verschiedene Wege. Der unauffällige Listscan geht lediglich alle IP-Adressen in einem Netzwerk durch und nutzt die sogenannte Reverse-DNS-Abfrage. Standardmäßig setzt Nmap einen Pingpefehl auf die Zieladresse ab, der bemerkt werden könnte. Wird auf den Ping verzichtet, ergibt sich aus Sicht des Netzbetreibers nur „normaler“ DNS-Verkehr.

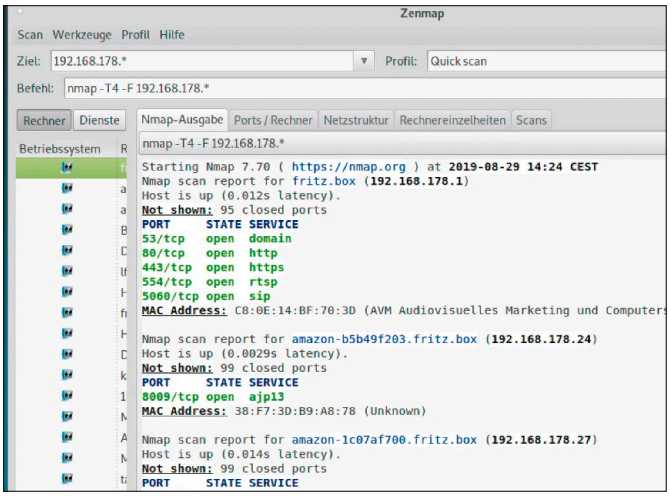
Schon eine solche einfache Liste kann Schwächen des Netzwerks zeigen. Denn bei der Installation eines Betriebssystems müssen die Anwender oft einen Hostnamen angeben. Wenn Sie diesen nicht editieren, wird dann ein vom Hersteller definierter Eintrag verwendet, der den Gerätetyp verrät. Viele Administratoren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

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

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



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



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

Detailanalyse in einem Netzwerk

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

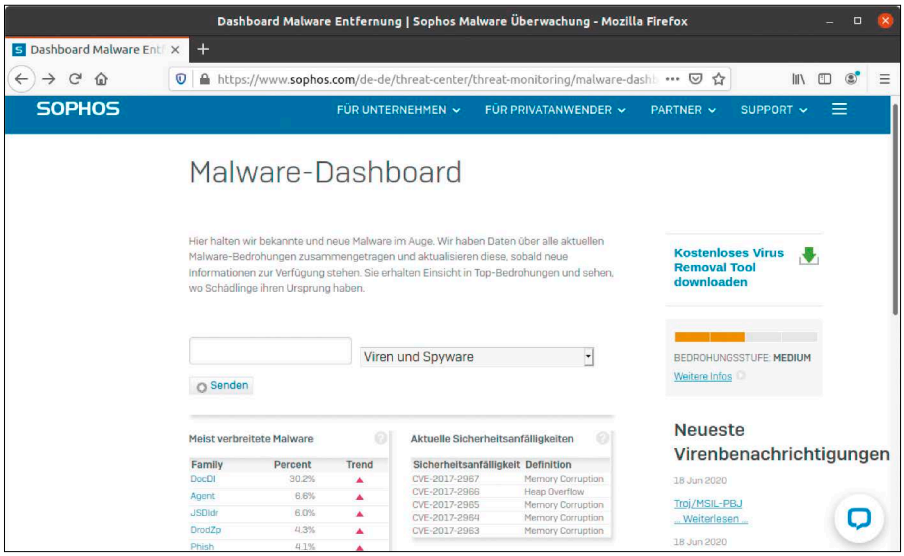
```
nmap -Pn -sV --version-all -v
  192.168.178.*
```

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

Virensicher im eigenen Netzwerk

Linux ist kaum von Viren, Würmern und Trojanern betroffen. Ein Linux-PC im eigenen Netzwerk kann jedoch dazu beitragen, den Schutz von beteiligten Windows-Rechnern zu verbessern.

VON THORSTEN EGGELING



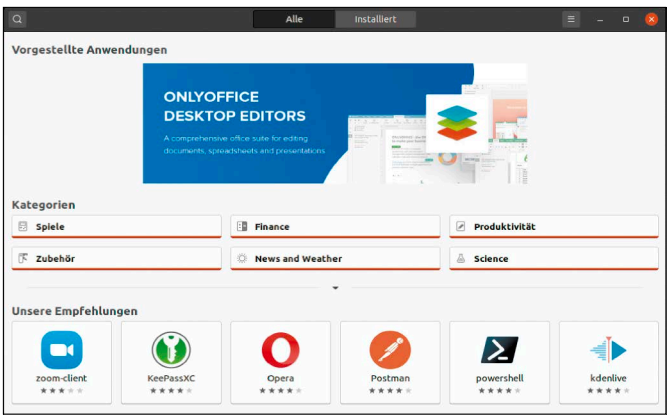
Permanente Bedrohungen: Die Hersteller von Antivirensoftware informieren über aktuelle Bedrohungen und Sicherheitslücken. Davon sind meist nur Windows-Systeme betroffen.

Jeden Tag entdecken die Virenlabore mehrere hunderttausend neue Viren und andere Schadsoftware. Die werden meist automatisch generiert und immer leicht verändert, damit Antivirensoftware sie nicht so leicht aufspüren kann. Ziel sind vor allem Windows-Rechner. Die sind zwar aus technischer Perspektive prinzipiell nicht viel unsicherer als Linux, aber das Nutzerverhalten ist dort ein anderes. Vor allem ist Windows für Angreifer lohnender, weil das System weitverbreitet ist. Wer in einem gemischten Netzwerk arbeitet, also mit Linux- und Windows-Rechnern, kann für etwas Entspannung sorgen. Dateifreigaben für Windows lassen sich unter Linux mit einem eigenen Virenscanner überwachen. Das sorgt für mehr Sicherheit, sollte die Schutzsoftware unter Windows aufgrund einer Infektion ausfallen.

Eine besondere Bedrohung, die auch Netzwerkfreigaben betrifft, stellen Verschlüsselungs-Trojaner dar. Vor dem Verlust wichtiger Dateien kann jedoch ein regelmäßiges Backup auf einen Linux-PC schützen.

Drohende Gefahren für Ihre Rechner

Es gibt im Wesentlichen nur zwei Angriffsszenarien auf Computer. Die größte Bedrohung geht vom Benutzer aus, der vor dem Bildschirm sitzt. Wer Software aus fragwürdiger Quelle ohne Prüfung installiert oder Programme aus E-Mail-Anhängen startet, holt sich am schnellsten Schadsoftware auf den Rechner. Das gilt im Prinzip für Windows und Linux gleichermaßen. Allerdings verwenden Linux-Anwender für die Softwareinstallation überwiegend die Paketquellen der jeweiligen Distribution. Dass darüber Viren auf den Rechner gelangen, ist so gut wie ausgeschlossen. Dateien aus E-Mail-Anhängen sind unter Linux standardmäßig nicht startfähig. Nur wenn der Benutzer selbst eine Datei als „ausführbar" kennzeichnet, lässt sie sich starten. Auch PDF-Dateien oder Makros in Office-Doku-



Sichere Software: Linux-Nutzer laden neue Programme nicht irgendwo aus dem Internet, sondern in der Regel über gut geschützte Paketquellen, die frei von Schadsoftware sind.

menten können Sicherheitslücken ausnutzen oder Schadsoftware mitbringen. Dagegen hilft nur, die Software stets aktuell zu halten und in den Sicherheitseinstellungen der Office-Software die Ausführung von Makros zu verbieten oder nur auf Nachfrage zu erlauben. Das ist jedoch die Standardeinstellung.

Das andere Szenario kommt ohne Mithilfe des Nutzers aus: Angriffe aus das Internet oder dem lokalen Netzwerk, etwa von einem infizierten Rechner aus, können Sicherheitslücken im Betriebssystem nutzen, um Schadsoftware zu verbreiten.

Reine Desktop- oder Büro-PCs sind davon in der Regel kaum betroffen, denn standardmäßig laufen dort keine Dienste, die von außen erreichbar sind (siehe Kasten „Schutz von Linux-Servern"). Daher gibt es auch keine Angriffsfläche. Das gilt für Linux wie Windows.

Sichere Netzwerkfreigaben unter Linux

Gewähren Sie nur die Zugriffsrechte, die wirklich erforderlich sind. Wenn Windows-Rechner keinen Schreibzugriff auf Netzwerkfreigaben besitzen, kann auch kein Schaden angerichtet werden. Wird der Linux-PC beispielsweise nur als Speicher für Backups genutzt, ist das problemlos möglich (siehe unten „Regelmäßige Backups erstellen"). Anders sieht es aus, wenn Freigaben zum Datenaustausch zwischen den Rechnern im lokalen Netzwerk dienen sollen. Dafür muss der Schreibzugriff möglich sein.

Wenn noch nicht geschehen, richten Sie auf Ihrem Linux-Rechner den Freigabedienst Samba in einem Terminal ein:

```
sudo apt install samba
```

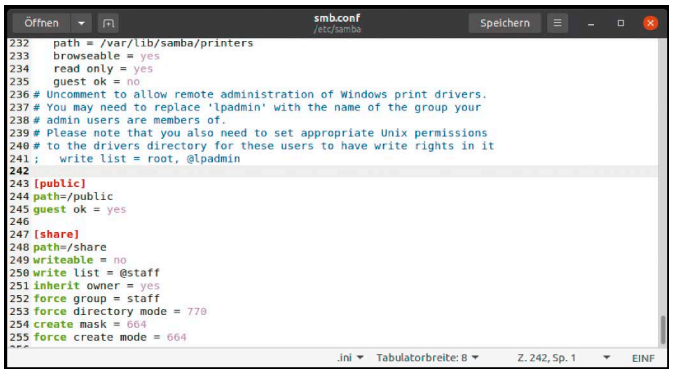
Bearbeiten Sie die Konfigurationsdatei mit einem Editor Ihrer Wahl:

```
sudo nano /etc/samba/smb.conf
```

Ändern Sie die Bezeichnung hinter „workgroup=" auf die Arbeitsgruppe, die Sie in Ihrem Netzwerk verwenden. Der Standard ist „WORKGROUP". Eine schreibgeschützte und ohne Anmeldung (Gastzugang) erreichbare Freigabe erzeugen Sie mit diesen Zeilen:

```
[public]
path=/public
guest ok = yes
```

Die Angabe hinter „path=" gibt den Pfad zu einem Ordner im Dateisystem an, den Sie als Speicherplatz im Netzwerk verwenden wollen. „guest ok = yes" ermöglicht den Zugriff für alle Windows- und Linux-Rechner ohne Benutzernamen und Passwort.



Freigaben (auch) für Windows: In der zentralen Konfigurationsdatei „smb.conf" legen Sie fest, welche Ordner Sie freigeben möchten und wer Schreib- oder nur Lesezugriff hat.

Die restriktivere Konfiguration für einen Ordner mit Schreibzugriff kann folgendermaßen aussehen:

```
[share]
path=/share
writeable = no
write list = @staff
inherit owner = yes
force group = staff
force directory mode = 770
create mask = 664
force create mode = 664
```

Hier erhalten nur Mitglieder der Gruppe „staff" den vollen Schreibzugriff. Neue und geänderte Dateien sowie Ordner versieht Samba mit passenden Zugriffsrechten. Damit das funktioniert, müssen einige Voraussetzungen erfüllt sein.

1. Benutzer müssen über ein Konto auf dem Linux-Rechner verfügen. Erstellen Sie neue Benutzer beispielsweise unter Ubuntu 20.04 in den „Einstellungen" unter „Benutzer".

2. Jeder Benutzer benötigt ein Samba-Passwort, das Sie mit

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

festlegen. Für den Platzhalter „[User]" setzen Sie den jeweiligen Benutzernamen ein.

3. Die Benutzer müssen in unserem Beispiel zur Gruppe „staff" gehören, die bei Ubuntu standardmäßig vorhanden ist. Fügen Sie Benutzer mit

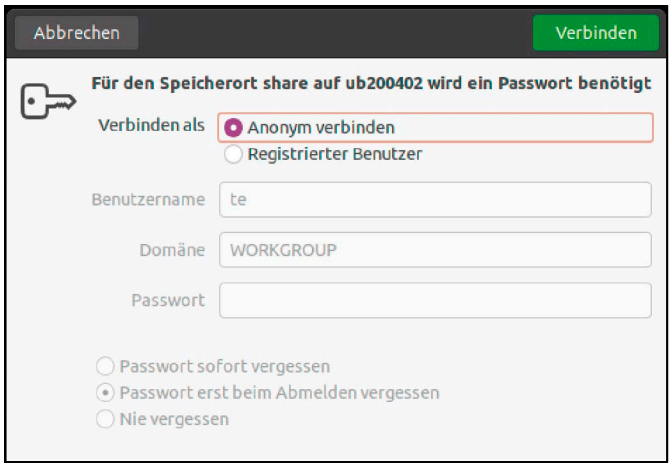
```
sudo usermod -a -G staff [User]
```

SCHUTZ VON LINUX-SERVERN

Sobald auf einem Rechner Serverdienste laufen, steigt die Gefahr. Besonders betroffen sind Webserver oder Fernsteuerungssoftware. Von außen ist ein Server durch die Routerfirewall geschützt beziehungsweise gar nicht ansprechbar. Angriffe aus dem lokalen Netzwerk sind jedoch möglich. Ist der Dienst auch über das Internet erreichbar, steigt das Risiko nochmal deutlich. Dafür muss man jedoch selbst eine Portfreigabe im Router einrichten. In diesem Fall muss der Server sehr sicher konfiguriert sein – stets aktuelle Software, sichere Passwörter, Zwei-Faktor-Authentifizierung, Basis-Angriffsschutz mit fail2ban (siehe *www.pcwelt.de/2321862*). Soll nur eine begrenzte Personenzahl auf den Server zugreifen, empfiehlt sich der Einsatz von VPN (*www.pcwelt.de/2448309*).

Öffentlich erreichbare Server sollten ab und zu auf Rootkits untersucht werden. Ein Rootkit eröffnet dem Angreifer die Option, sich auf dem kompromittierten System anzumelden, Netzwerkverkehr zu überwachen oder Programme zu starten.

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



Beim Server anmelden: Beim Zugriff auf einen Server über den Dateimanager haben Sie die Wahl zwischen einer anonymen Verbindung als Gast oder mit Benutzernamen und Passwort.

zur Gruppe hinzu. Sie können auch eine andere Gruppe verwenden oder mit „sudo groupadd“ eine neue Gruppe erstellen.

4. Der freigegebene Ordner, in unserem Beispiel „/share“, muss der gewählten Gruppe gehören. Legen Sie die Berechtigungen im Dateisystem mit

```
sudo chown -R root:staff /share
```

fest.

Wenn Benutzernamen und Passwörter auf den Client-PCs mit denen auf dem Server übereinstimmen, erfolgt der Zugang ohne die Abfrage von Anmeldeinformationen. Sollte das aus Sicherheitsgründen unerwünscht sein, legen Sie andere Benutzernamen und/oder Passwörter fest. Linux und Windows fragen dann nach den Anmeldeinformationen. Wenn Sie diese nicht speichern, erfolgt nach einem Neustart des Systems keine automatische Anmeldung. Die Freigabe ist dann zumindest nicht permanent für Schadsoftware erreichbar.

Hinweise: Wenn es einen Benutzer mit dem gleichen Namen auf dem Linux-Server gibt, aber mit einem abweichenden Passwort, fragt Windows nach Benutzernamen und Passwort. Soll nur die Verbindung zur Gastfreigabe erfolgen, tippen Sie als Benutzernamen beispielsweise „gast“ ein und lassen das Passwort leer. Für Samba spielt der Name des Gastbenutzers übrigens keine Rolle. Es werden alle unbekannten Benutzernamen als „bad user“ behandelt und damit als Gäste. Wenn es den Benutzer auf dem Linux-Server nicht gibt, versucht Windows eine automatische Anmeldung als Benutzer „Gast“ und Samba gewährt den Zugriff auf Gastfreigaben.

Unter Linux erscheint in jedem Fall ein Dialog, in dem Sie die Option „Anonym verbinden“ (Gast) wählen oder „Registrierter Benutzer“ und dann Benutzernamen und Passwort eintippen. Sollte im Ubuntu-Dateimanager der Zugriff auf Freigaben über „Andere Orte → Windows Netzwerk“ nicht klappen, drücken Sie Strg-L und tippen die Adresse der Samba-Freigabe in der folgenden Form

```
smb://[Server]/[Freigabe]
```

direkt ein.

Virenscanner I: Sophos Antivirus

Sophos bietet eine kostenlose Antivirenlösung für Linux an. Technischen Support gibt es aber nur bei der Bezahlversion. Für den Download über *https://m6u.de/sopho* müssen Sie sich registrieren. Das Programm lässt sich ausschließlich über die Kommandozeile steuern, eine grafische Oberfläche gibt es nicht. Entpacken Sie die heruntergeladene Datei, öffnen Sie ein Terminal und wechseln Sie in das Verzeichnis der Software. Dort starten Sie mit

```
sudo ./install.sh
```

die Einrichtung. Folgen Sie den Anweisungen des Assistenten. Übernehmen Sie alle Vorgaben per Druck auf die Eingabetaste, außer bei der Frage „Do you wish to install the Free (f) or Supported (s) version of SAV for Linux?“. Hier tippen Sie „f“ ein und bestätigen mit Eingabetaste. Nach der Installation starten Sie

```
sudo /opt/sophos-av/bin/savupdate
```

zum Update der Virensignaturen. Das müssen Sie später nicht manuell wiederholen, weil Sophos Antivirus automatisch alle 60 Minuten nach Updates sucht. Danach können Sie mit

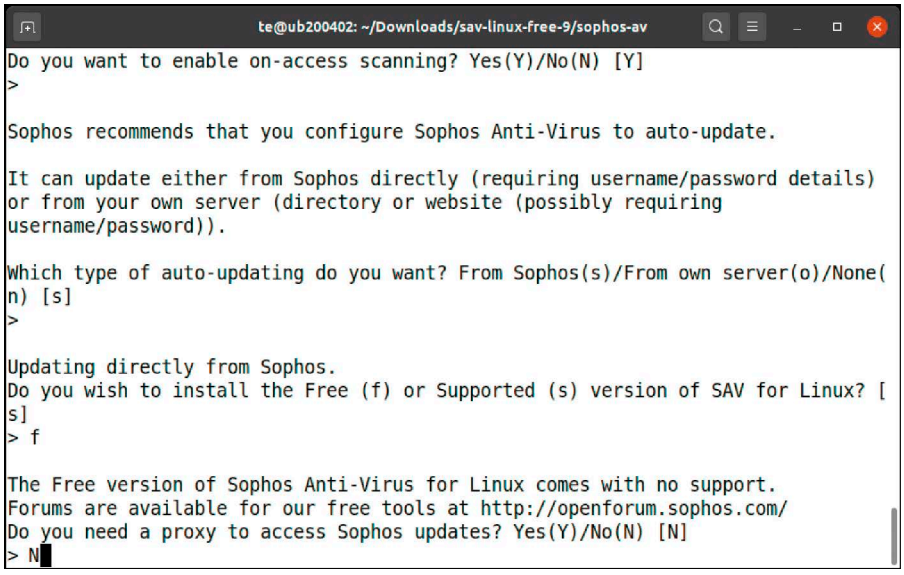
```
sudo /opt/sophos-av/bin/savscan /
```

das gesamte System auf Schadsoftware untersuchen. Standardmäßig ist die On-Access-Überprüfung aktiv. Sophos Anti-Virus prüft alle Dateioperationen, also jede Datei, die neu hinzukommt oder kopiert wird. Sollte Schadsoftware enthalten sein, wird die Datei blockiert, aber nicht gelöscht oder verschoben. Auch Windows-Nutzer, die eine infizierte Datei von einer Netzwerkfreigabe öffnen wollen, erhalten darauf keinen Zugriff. Mit

```
sudo /opt/sophos-av/bin/savlog
```

lassen Sie sich die Protokolle ausgeben.

Man sollte in regelmäßigen Abständen nach Schadsoftware suchen, betroffene Dateien verschieben, dann genauer untersuchen und gegebenenfalls löschen. Verwenden Sie die folgende Befehlszeile, wenn



Sophos Anti-Virus einrichten: Die Installation der Schutzsoftware erfolgt im Terminal. Ein Assistent fragt die Parameter ab, die Sie zum Großteil einfach mit der Eingabetaste bestätigen.

Sie nur den Ordner „/share“ prüfen und infizierte Dateien nach „/infected“ verschieben wollen:

```
sudo /opt/sophos-av/bin/savscan
  -nc -move=/infected /share
```

Die Option „-nc“ unterdrückt eventuelle Rückfragen. Informationen zu weiteren Optionen liefern

```
man savscan
```

sowie die Konfigurationsanleitung (*https://m6u.de/cgeng*) und die Startupanleitung (*https://m6u.de/sgeng*) für Linux.

Automatischer Scan: Laden Sie die Konfigurationsdatei des Crondienstes mit

```
sudo crontab -e
```

und tragen Sie dort diesen Auftrag ein (Beispiel):

```
0 1 * * * /opt/sophos-av/bin/savscan
  -nc -move=/infected /share >> /
  var/log/savscan.log
```

Dies würde den Virenscanner jede Nacht um 1:00 Uhr starten.

Virenscanner II: Eset Nod32 Antivirus

Von Eset gibt es einen Virenscanner für Linux, der auch eine grafische Oberfläche bietet. Über *www.eset.com/de/home/antivirus-linux* lässt sich eine kostenlose Version herunterladen, die Sie 30 Tage lang testen können. Für den Download ist eine Registrierung erforderlich. Die Vollversion kostet ab 29,95 Euro pro Jahr. Damit sich das Programm installieren lässt, müssen Sie unter Ubuntu oder Linux Mint ein zusätzliches Paket installieren:

```
sudo apt install libc6:i386
```

Danach verwenden Sie im Downloadverzeichnis diese beiden Befehle:

```
chmod 774 eset_nod32av_64bit_de.
  linux
sudo ./eset_nod32av_64bit_de.linux
```

Ein Assistent führt Sie durch die Installation. Zum Abschluss startet das Programm automatisch und aktualisiert selbständig die Virensignaturen. Über „Computer prüfen → Standardprüfung“ führen Sie einen ersten Virenscan auf allen lokalen Laufwerken durch.

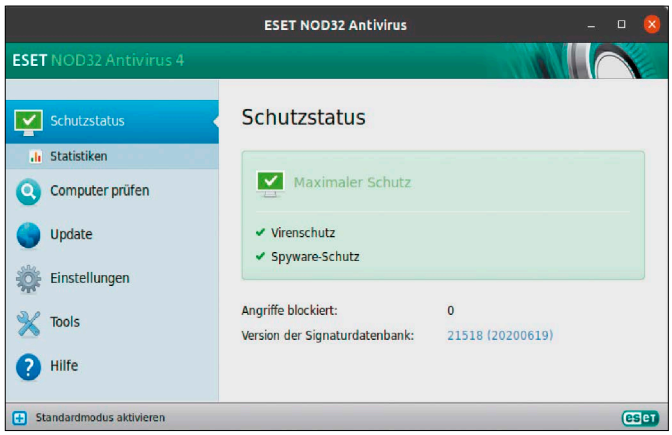
Eset Nod32 Antivirus schützt den Rechner mit dem Echtzeit-Dateischutz. Neue Dateien werden automatisch geprüft, auch in den im Netzwerk freigegebenen Ordnern. Wird eine Bedrohung erkannt, versucht das Programm, die Datei zu säubern. Wenn das nicht gelingt, landet die Datei in Quarantäne. Klicken Sie links unten im Fenster auf „Erweiterten Modus aktivieren“. Damit blenden Sie zusätzliche Optionen ein. Gehen Sie auf „Tools → Log-Dateien“. Hier sehen Sie Meldungen zu den erkannten Bedrohungen. Unter „Tools → Quarantäne“ finden Sie eine Liste mit Dateien, die in Quarantäne verschoben wurden. Sollten Sie Vireninfektionen als Irrtum verifizieren, lassen sich solche Dateien wiederherstellen. Mit

```
sudo /opt/eset/esets/sbin/esets_
  scan [Pfad]
```

starten Sie einen Virenscan auf der Kommandozeile.

Das ist nützlich, wenn Sie per SSH mit dem Server verbunden sind und gezielt bestimmte Ordner untersuchen wollen. Wenn die Echtzeitprüfung aktiv ist, sollte das jedoch in der Regel nicht nötig sein.

Tipp: Laden Sie über *http://2016.eicar.org/85-0-Download.html* eine Testdatei herunter, beispielsweise „eicar.com“. Sobald Sie die Datei speichern, sollte jeder Virenscanner Alarm schlagen. Wenn nicht, prüfen Sie die Konfiguration.



Eset Nod32 Antivirus: Dieser Virenscanner bietet eine grafische Oberfläche, die Sie aber nur selten bemühen müssen. Die Echtzeitprüfung beseitigt Schadsoftware automatisch.

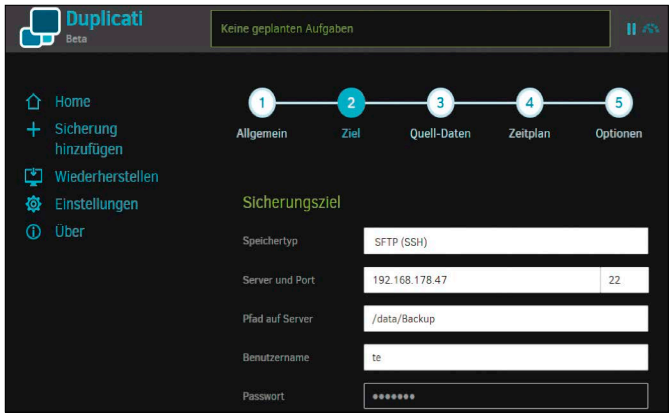
Regelmäßige Backups erstellen

Backups auf Freigaben, für die standardmäßig der Schreibzugriff erlaubt ist, sind keine gute Idee. Backups sollten möglichst auf Laufwerken gespeichert werden, die nicht ständig mit dem Windows-PC verbunden. Die Gefahr, dass Backups unter die Kontrolle von Schadsoftware geraten, lässt sich nur reduzieren, wenn Dateien von Windows-Rechnern auf anderem Wege gesichert werden.

Ein empfehlenswertes Tool zum Sichern persönlicher Dateien ist Duplicati (*www.duplicati.com*). Die Software läuft unter Windows, Linux und Mac-OS. Konfiguration und Bedienung erfolgen über eine Weboberfläche im Browser.

Als Backupziel unterstützt das Programm lokale Ordner und Laufwerke, aber auch Onlinespeicher wie Google Drive oder Dropbox. Zum Datenschutz lassen sich die Backups verschlüsseln.

Im lokalen Netzwerk mit einem Linux-Server empfiehlt sich die Sicherung mit Duplicati über SFTP (SSH). Unter Linux muss dazu das Paket „openssh-server“ installiert sein und unter Windows Duplicati. Standardmäßig hat Windows über SSH keinen Zugriff auf den Linux-Server. Die Backups können somit auch nicht durch Schadsoftware kompromittiert werden. ■



Backuptool: Duplicati beherrscht auch die Datensicherung über SFTP (SSH). Windows hat auf den Backupordner keinen Zugriff, weshalb eventuelle Schadsoftware nichts ausrichten kann.

Tipps und Tricks für ein besseres Terminal

Im Terminal lassen sich fast alle Aufgaben der Systemwartung und zum Troubleshooting ausführen. Aber auch das Terminal braucht von Zeit zu Zeit Aufmerksamkeit. Hier finden Sie Tipps, mit denen Sie die Konsole von Mint, Ubuntu & Co. verbessern.

Andere Shells: Fish, Zsh und Co.

Die Bourne Again Shell (Bash) ist in Linux-Systemen der Quasistandard, aber nicht die einzige Shell für Linux-Systeme.
Ein Wechsel ist nicht weiter kompliziert. Für Einsteiger ist beispielsweise die Friendly Interactive Shell (Fish) mit ihren Eingabehilfen und Syntaxhervorhebung gut geeignet, während sich Fortgeschrittene über die gut konfigurierbare Zsh freuen. Eine der angesagten alternativen Shells ist schnell installiert, denn sie finden sich üblicherweise in den Standard-Paketquellen von Linux-Distributionen.
Die beliebte Fish-Shell ist mit

```
sudo apt-get install fish
```

in Debian, Ubuntu & Co. leicht nachzurüsten.
Um diese Shell zum aktiven Kommandointerpreter im eigenen Benutzerkonto zu machen, ist aber noch ein weiterer Schritt nötig. Der Befehl „chsh" ändert die Standard-Shell auf eine andere, neu installierte Shell um. Um zunächst alle verfügbaren Interpreter zu sehen, dient dieses Kommando:

```
cat /etc/shells
```

Es zeigt dann beispielsweise den Pfad „/bin/fish" für die Fish-Shell. Mit dem Kommando

```
chsh -s /bin/fish
```

machen Sie die Fish-Shell ab der nächsten Anmeldung zur Standard-Shell. **-dw**

Sixel: Bilder im Terminal

Grafische Anwendungen wie Bildbetrachter sind nicht die einzige Möglichkeit, Bilder auszugeben. Eine in Unix-Systemen schon lange genutzte Möglichkeit, Bilder in einem Terminal auszugeben, arbeitet mit Sixel und funktioniert auch wieder in Linux-Systemen – allerdings nicht mehr in jedem Terminal.
Ein Sixel ist ein Muster von sechs Pixeln Höhe und einem Pixel Breite und eine von DEC entwickelte Methode, Bilder in textbasierten Terminals darzustellen, per Ascii zu codieren und über sieben Bit breite serielle Schnittstellen an Nadeldrucker zu übertragen. Diese uralte Methode zur Grafikdarstellung unterstützt unter Linux noch der Terminalemulator xterm, der in den meisten Distributionen vorhanden ist. Über den Ausführen-Dialog der Desktopumgebung ruft das Kommando

```
xterm -ti vt340
```

den Terminalemulator mit Sixel-Unterstützung auf. Nun kann der Befehl

```
convert [datei].jpg
  -geometry 800x480
  sixel:-
```

eine JPG-Datei in Sixel umwandeln und im Terminal anzeigen. Das ist nicht nur eine Kuriosität aus grauen Unix-Urzeiten. Das Script „lsix" hat die Methode verfeinert, um Grafikdateien aller Art in Xterm anzuzeigen. Es findet sich auf Github unter *https://github.com/hackerb9/lsix* und muss nach dem Herunterladen nur mit

```
chmod +x lsix
```

ausführbar gemacht werden. Der Aufruf von

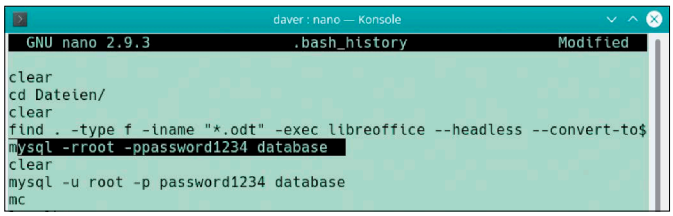
```
./lsix
```

stellt alle Bilder im aktuellen Verzeichnis grafisch im Sixel-Format dar. **-dw**

Sixel statt Pixel: Eine uralte Technologie aus den 80er-Jahren funktioniert weiterhin im Terminal Xterm. Das ist eine Kuriosität, die sich kein Terminalfreak entgehen lässt.

Bash: Zeilen aus dem Verlauf löschen

Wer mit öfters mit My SQL hantiert, schreibt möglicherweise Passwörter aus Bequemlichkeit direkt in die Kommandozeile und damit in den Befehlsverlauf der Kommandozeile. Passwörter sollten aber auf Mehrbenutzersystemen und Systemen ohne Vollverschlüsselung nie in die History kommen, da dies immer einen potenziellen Ver-



Befehlsverlauf ausmisten: Gerade auf Mehrbenutzersystemen sollten Sie darauf achten, dass sich keine wichtigen Passwörter in die Datei „~/.bash_history“ verirren.

lust vertraulicher Informationen darstellt.

Es müssen aber nicht gleich Passwörter sein, die im Befehlsverlauf unerwünscht sind. Auch sonst sammeln sich über die Zeit etliche Kommandos in der History, die auf Dauer bei der Suche nach einem bestimmten, wieder benötigten Befehl stören. Hin und wieder ist es also keine schlechte Idee, den Befehlsverlauf der Shell aufzuräumen und überflüssige Kommandos zu löschen. Dies ist nicht schwer, denn in der Bourne Again Shell (Bash), die in den meisten Linux-Distributionen der Standard ist, liegt die Datei „~/.bash_history“ mit dem Befehlsverlauf als schlichte Textdatei in Home-Verzeichnis. Jede Zeile entspricht einem Befehl. Um dort aufzuräumen, öffnet man diese Datei einfach in einem beliebigen Texteditor und löscht die unerwünschten Zeilen.

Alternative Tastenkombination in der Bash: Mit der Cursor-Oben-Taste zeigt die Shell die zuletzt eingegebenen Befehle vom neuesten bis zum ältesten Kommando an. Stößt man dabei auf einen unerwünschten Befehl, so drückt man einfach die Kombination Strg-U, um die betreffende Zeile aus der History zu entfernen.

History sauber halten: Soll ein Befehl gleich gar nicht im Befehlsverlauf landen, bietet sich in Debian, Ubuntu und Konsorten ein Trick an: Ein vorangestelltes Leerzeichen am Zeilenanfang eines Befehls verhindert, dass dieses Kommando in der History landet. Die Shell selbst stört sich nicht am Leerzeichen und führt das Kommando ganz normal aus. Dieses Verhalten ist besonders praktisch, wenn sich die Eingabe von Passwörtern in der Shell nicht ganz vermeiden lässt. Wichtig ist aber, im Hinterkopf zu behalten, dass dieser Trick auf anderen Distributionen wie Fedora, Cent-OS, Open Suse und Red Hat Enterprise Linux nicht funktioniert. **-dw**

Terminalfarben invertieren

Bei ungünstigen Lichtverhältnissen oder ermüdeten Augen hilft es, die Bildschirmfarben zu invertieren. Am Desktop gibt es dafür Tools wie xcalib (xcalib -a -i), das die komplette Monitorausgabe invertiert. Aber auch exklusiv für das Terminal steht ein passender Befehl bereit, der dann – im Unterschied zu grafischen Tools – auch in der virtuellen Konsole funktioniert.

Der Standardbefehl „setterm“ ist historisch und stammt noch aus der Zeit früher Farbmonitore mit nur acht oder 16 Farben. Das Tool ist weitgehend obsolet, kann aber mit

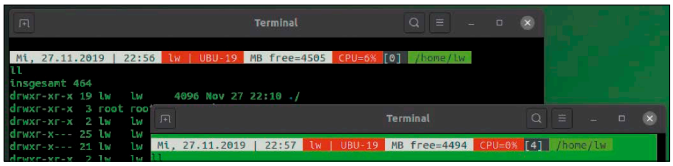
```
setterm -inversescreen on
```

und zurück mit dem Parameter „off“ schnell für andere Terminalfarben sorgen, auch in den virtuellen Konsolen.

Wer oft mit schlechten Lichtverhältnissen rechnen muss, kann sich mit

```
alias hell='setterm
  -inversescreen on'
alias dunkel='setterm
  -inversescreen off'
```

zwei schnelle Aliases „hell“ und „dunkel“ zum Hin- und Herschalten zurechtlegen. **-ha**



Farben invertieren im Terminal: Die Old-School-Methode mit setterm hat den Vorteil, dass sie auch in der virtuellen Konsole funktioniert.

Textdateien: Ausgabe mit Bat statt Cat

In der Kommandozeile ist es oft hilfreich, zur schnellen Kontrolle die Inhalte von Konfigurations- oder Script-Dateien ohne Editor mit dem Befehl cat anzuzeigen. Allerdings ist cat extratrocken und gibt einfach den unformatierten Textinhalt einer Datei aus.

Es geht schöner und übersichtlicher: Das Programm Bat (*https://github.com/sharkdp/bat*) macht Textdateien in vielen Formaten durch Syntaxhervorhebung im Terminal viel zugänglicher.

Alle bekannten Textdateien erhalten eine farbige Inhaltsauszeichnung. Dabei erkennt Bat die Syntax von Dutzenden Dateiformaten, von der einfachen Script-Datei über Konfigurationsdateien bis hin zu Quelltexten. Außerdem versieht Bat angezeigte Texte mit Zeilennummern und kann für Vergleiche mehrere Dateien übereinander anzeigen. Die Standardfarben sind für dunkle Terminals mit schwarzem Hintergrund geeignet. Es gibt aber noch einige weitere Themen für die Konfiguration von Bat, die sich für Terminalfenster mit dunkler Schrift auf hellem Grund eignen.

Die Installation ist unter Ubuntu und Debian (alle Versionen) dank eines vorbereiteten DEB-Paket kein Problem: Nach dem Download der passenden DEB-Datei von *https://github.com/sharkdp/bat/releases* für die eigene Linux-Distribution installiert das Kommando

```
sudo dpkg -i bat_0.9.0_
  amd64.deb
```

das Programm – im Beispiel die Version für Ubuntu/Debian mit 64 Bit. Der Aufruf erfolgt genau so einfach wie bei cat

```
bat [Datei]
```

und die Navigation erfolgt mit Cursor- und Bildtasten. Ein Druck auf „Q“ beendet den Betrachter. **-dw**

Farbig und übersichtlich: bat (statt cat) macht die Anzeige von Quelltexten und Konfigurationsdateien im Terminal wesentlich freundlicher.

Tmate: Das geteilte Terminal

Die Fernwartung von Linux-PCs und die Pflege von Servern finden üblicherweise über SSH im Terminal statt. Bei kniffligen Problemen und bei der Serveradministration ist es immer wieder mal nützlich, Freunde oder Kollegen zur Unterstützung einzuladen. Das Tool Tmate erlaubt die gemeinsame Arbeit in der Shell.
Bei Tmate handelt es sich um eine Abspaltung des bekannten Werkzeugs Tmux, das die Shell um eine ausgewachsene Sitzungsverwaltung erweitert. Im Unterschied zum ursprünglichen Programm enthält es einen SSH-Client, der die gemeinsame Arbeit in einer Shell über eine Internetverbindung möglich macht. Tmate arbeitet dabei über die zentrale Vermittlerstelle *https://tmate.io*, sodass eine Portweiterleitung für den Linux-Rechner nicht nötig ist. Das Konzept erinnert an andere Supportwerkzeuge wie Teamviewer und Chrome Remote Desktop, allerdings haben die Tmate-Entwickler auch den Code für den Vermittlungsserver als Open Source herausgegeben. Sollte jemand Zweifel an der Vertrauenswürdigkeit an *https://tmate.io* haben oder im Firmenumfeld höhere Datenschutzansprüche erfüllen müssen, so ist der Betrieb des Vermittlungsservers also auch in Eigenregie möglich. Diese Vermittlungsstelle muss im Internet direkt per SSH wie ein SSH-Server erreichbar sein. Die damit verbundenen Tmate-Clients allerdings nicht.

Die Installation von Tmate ist dank vorbereiteter Pakete für viele Linux-Distributionen und auch für Mac-OS X und Free BSD nicht kompliziert. In Ubuntu und seinen Varianten erledigen die drei Befehle

```
sudo add-apt-repository
  ppa:tmate.io/archive
sudo apt-get update
sudo apt-get install tmate
```

die Installation aus einem externen Repository der Entwickler. Weil Tmate Gebrauch von SSH-Bibliotheken macht, muss auch der Open-SSH-Server installiert sein.

Teamarbeit im Terminal: Tmate ist ein Vermittlungsdienst, der die Verbindung mehrerer Anwender in einem Terminal per SSH erlaubt. Auch die Serverkomponente dafür ist Open Source.

Auf frisch installierten Ubuntu-Systemen fehlt der Serverdienst zunächst und muss erst noch mittels des Befehls

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

nachinstalliert werden.
Danach ist das Tool sofort mit dem Aufruf von

```
tmate
```

einsatzbereit.
Nun gilt es, flott die unten in der Fußzeile eingeblendete ID mit der Maus im Terminalfenster zu markieren und über die Tastenkombination Strg-Umschalt-C in die Zwischenablage zu kopieren. Denn diese ID dient zur Verbindungsaufnahme mit dem Partner und muss diesem per Instant Messenger oder per SMS mitgeteilt werden. Die ID wird aber nur zehn Sekunden angezeigt, sodass man schnell reagieren muss.
Auf dem anderen Rechner, der sich in das gemeinsame Terminal verbinden soll, wird Tmate nicht benötigt – ein herkömmlicher SSH-Client genügt. Dieser verbindet sich über die zuvor mitgeteilte ID und dem Befehl

```
ssh [ID]@am2.tmate.io
```

mit der laufenden Tmate-Sitzung auf dem Zielrechner. **-dw**

BASH: BEFEHLSVERLAUF ABSCHALTEN

Einer der Vorzüge der Linux-Shells ist ihr Befehlsverlauf, der früher getätigte Kommandos mit der Suchfunktion (Strg-R) oder mit den Pfeiltasten wieder hervorholt.
Es gibt aber auch Fälle, in welchen man den eingegebenen Befehl nicht im Verlauf haben möchte – beispielsweise die Eingabe von Befehlen, die Passwörter als Parameter enthalten. Wichtige Zugangsdaten sollten niemals im Klartext im Befehlsverlauf landen. Es gibt mehrere Möglichkeiten, dies zu verhindern:

1. Bevor Sie ein Kommando eingeben, das nicht im Verlauf gespeichert werden soll, schalten Sie mit

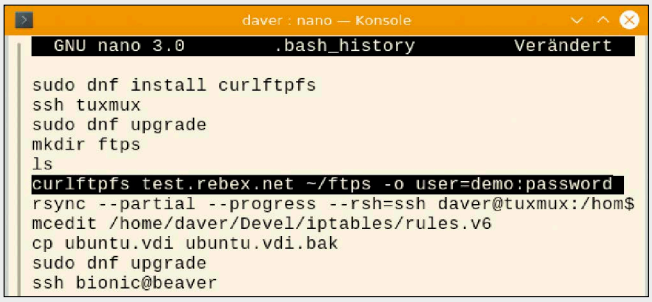
```
unset HISTFILE
```

den Verlaufsspeicher für die aktuelle Shell-Sitzung ab.

2. Haben Sie den Befehl bereits eingegeben, der eigentlich nicht in den Verlauf kommen sollten, dann schließt das Kommando

```
HISTSIZE=0 && exit
```

die aktuelle Shell, ohne deren Verlaufsspeicher mit den letzten Befehlen zu sichern.



Aufräumen im Verlauf: Wenn unerwünschte Kommandos im Befehlsverlauf gelandet sind, kann man sie mit jedem Texteditor aus der „.bash_history“ entfernen.

3. Sind bereits mehrere unerwünschte Befehle im Verlauf der Bash (oder Sie möchten dies überprüfen), so können Sie immer noch eine manuelle Aufräumaktion starten. Der Terminalbefehl

```
nano ~/.bash_history
```

lädt die Datei mit dem Befehlsverlauf in den Texteditor Nano.

PC-WELT

Sonderheft-Abo

Für alle Sonderausgaben der PC-WELT

Sie entscheiden, welche Ausgabe Sie lesen möchten!

Die Vorteile des PC-WELT Sonderheft-Abos:

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

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

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

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

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

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PWSJO14130

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

Weniger tippen: Vereinfachte Autovervollständigung

Niemand tippt gerne zu viel in der Kommandozeile. Das ist auch nicht nötig, denn die Kommandozeile kennt eine intelligente Form der Autovervollständigung, die Pfade und Dateinamen mit einem mehrfachen Druck der Tab-Taste ergänzen kann. Das geht auch noch schneller.

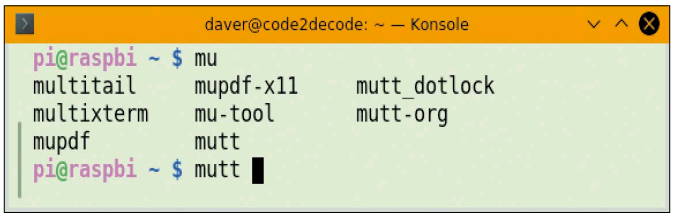
Mit einer kleinen Anpassung der Konfigurationsdateien der Bourne Again Shell reagiert die Autovervollständigung schon auf einen einzigen Druck der Tab-Taste. Die erste Änderung dazu ist eine neue Konfigurationsdatei mit dem Namen „.inputrc" im Home-Verzeichnis, die man beispielsweise mit dem Texteditor Nano so erstellt:

```
nano ~/.inputrc
```

Als Inhalt erhält diese neue Datei nur eine Zeile und zeigt damit eine Liste aller Vervollständigungsoptionen mit einem einzigen Druck auf Tab an:

```
set show-all-if-ambiguous
  on
```

Das ist schon mal recht nützlich. Optional kommt dazu noch in die Datei „.bashrc" im Home-Verzeichnis ganz ans Ende folgende Zeile:



Bessere Autovervollständigung: Nach zwei kleineren Ergänzungen in der Bash-Konfiguration reagiert die intelligente Vervollständigung auf einen einzigen Druck der Tab-Taste.

```
[ $- = *i* ]] && bind
  TAB:menu-complete
```

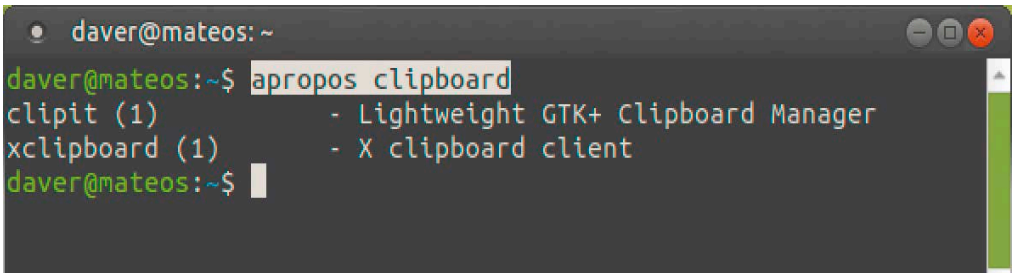
Diese Anweisung listet alle weiteren Optionen auf, ergänzt dabei aber die erste schon mal. Ein weiterer Druck auf Tab springt dann zur zweiten Option und so weiter. Aktiv werden alle diese Änderungen erst nach Schließen und erneutem Öffnen der Shell beziehungsweise des Terminalfensters. **-dw**

Apropos: Welchen Befehl brauche ich?

Eine der Hürden bei der Verwendung der Shell ist schlicht der Einstieg, welches Kommando für welche Aufgabe geeignet wäre. Ist das Kommando ungefähr bekannt, dann führt eine Recherche im Web auf *https://stackoverflow.com* zu anschaulichen Beispielen und konkreten Lösungen.

Für eine Suche ins Blaue hinein ist der Befehl apropos geschaffen, der die Datenbank der Hilfeseiten (Manpages) von Shell-Befehlen nach Stichwörtern durchsucht.

So hält apropos für Einsteiger erste Infos parat und liefert eine allgemeine Übersicht zu einem Stichwort. Fortgeschrittene finden mit dem Kommando schnell alternative Shell-Tools und Befehle, die eventuell für das konkrete Problem besser geeignet sind.



Findet oft den passenden Befehl: Das Kommando apropos ist einer der Schätze der Befehlszeile und findet Befehle anhand ihrer Beschreibung in der Dokumentation.

Einen ersten Blick in die Werkzeugkiste der Kommandozeile wirft der Befehl

```
apropos [Stichwort]
```

So zeigt

```
apropos clipboard
```

beispielsweise alle Befehle an, die für den Zugriff auf die Zwischenablage (Clipboard) taugen.

Es genügt auch, nur den Teil eines gesuchten Wortes oder Befehl anzugeben. Generell kann das Stichwort in Englisch oder auch in Deutsch angegeben werden, sofern die deutschsprachigen Manpages nachinstalliert werden. Bei Bedarf erledigt das dieser Installationsbefehl:

```
sudo apt-get install man-
  pages-de
```

unter Debian/Ubuntu. **-dw**

Ein Bash-Alias umgehen

Wenn Sie einen Standardbefehl wie mc, ls oder lsblk durch ein gleichlautendes Bash-Alias ersetzen, das Ihre bevorzugten Schalter gleich mitbringt (etwa alias mc='mc /srv/ /home/'), kann das zu Irritationen führen. Das Kommando scheint zu versagen, wenn Sie ausnahmsweise andere Parameter übergeben.

Ein Aliasname, der mit dem eigentlichen Befehlsnamen übereinstimmt, scheint erst mal praktisch, weil man sich dann keinen Extra-Namen einprägen muss. Früher oder später werden Sie damit aber solche Irritationen erleben, weil das Alias über den normalen Befehl dominiert.

Das Standardverhalten erreichen Sie dann immer über den Vorsatz „command" – etwa:

```
command mc
```

Ebenso ist es möglich, zunächst den Pfadnamen mit

```
which mc
```

zu ermitteln und das Programm sodann mit seinem Pfadnamen zu starten („/usr/bin/mc"). **-ha**

PC-WELT PLUS

Stellen Sie uns auf die Probe!

3 x PC-WELT Plus zum Testpreis

Jetzt testen:
3x PC-WELT Plus
gedruckt & digital
16,99€

Satte **22%** gespart!

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

- ✓ **3x PC-WELT Plus als Heft frei Haus** mit je 2 Doppel-DVDs und 32 Seiten Spezialwissen
- ✓ **3x PC-WELT Plus direkt aufs Smartphone & Tablet** mit interaktivem Lesemodus

Jetzt bestellen unter
www.pcwelt.de/testen 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 Plus Testabo für 16,99€.

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

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PWPMA14141

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

Verlag

IT MEDIA PUBLISHING GMBH & CO KG

IT Media Publishing GmbH & Co. KG
Gotthardstr. 42, 80686 München
E-Mail: *info@it-media.de*
www.it-media.de

Chefredakteur: Sebastian Hirsch
(v.i.S.d.P – Anschrift siehe Verlag)

Druck: Mayr Miesbach GmbH
Am Windfeld 15, 83714 Miesbach
Tel. 08025/294-267

Inhaber- und Beteiligungsverhältnisse: Alleinige Gesellschafterin der IT Media Publishing GmbH & Co. KG ist die IT Media Publishing Verwaltungs GmbH, München, Geschäftsführer Sebastian Hirsch.

WEITERE INFORMATIONEN

Redaktion

Gotthardstr. 42, 80686 München
E-Mail: *info@it-media.de*
www.it-media.de
Chefredakteur: Sebastian Hirsch (verantwortlich für den redaktionellen Inhalt)
Stellvertretender Chefredakteur: Thomas Rau
Chef vom Dienst: Andrea Kirchmeier
Redaktion: Arne Arnold
Redaktionsbüro: MucTec (*hapfelboeck@googlemail.com*)
Freie Mitarbeiter Redaktion: Dr. Hermann Apfelböck, Thorsten Eggeling, Stephan Lamprecht, David Wolski
Titelgestaltung: Schulz-Hamparian, Editorial Design / Thomas Lutz
Freier Mitarbeiter Layout/Grafik: Alex Dankesreiter
Freie Mitarbeiterin Schlussredaktion: Andrea Röder
Freier Mitarbeiter digitale Medien: Ralf Buchner
Herstellung: Melanie Arzberger
Redaktionsassistenz: Manuela Kubon

Einsendungen: Für unverlangt eingesandte Beiträge sowie Hard- und Software übernehmen wir keine Haftung. Eine Rücksendegarantie geben wir nicht. Wir behalten uns das Recht vor, Beiträge auch auf anderen Medien, etwa auf DVD oder online, zu veröffentlichen.

Haftung: Eine Haftung für die Richtigkeit der Beiträge können Redaktion und Verlag trotz sorgfältiger Prüfung nicht übernehmen. Die Veröffentlichungen in der LinuxWelt erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Auch werden Warennamen ohne Gewährleistung einer freien Verwendung benutzt.

Bildnachweis: AdobeStock – Vlad Kochelaevskiy, AdobeStock – electriceye, AdobeStock – Kamjana, 123rf – amadeus542, AdobeStock – noppadon; sofern nicht anders angegeben: Anbieter

Anzeigen

Anzeigenleitung:
Brigitta Reinhard
RMS GmbH
Tel. 089/464729
E-Mail:
brigitta.reinhart@mnet-online.de

Vertrieb

Vertrieb Handelsauflage:
MZV GmbH & Co. KG, Ohmstraße 1
85716 Unterschleißheim
Tel. 089/31906-0
Fax 089/31906-113
E-Mail: *info@mzv.de*
Internet: *www.mzv.de*
Druck: Mayr Miesbach GmbH
Am Windfeld 15, 83714 Miesbach
Tel. 08025/294-267

Verlag

IT Media Publishing GmbH & Co. KG
Gotthardstr. 42, 80686 München
E-Mail: *info@it-media.de*
www.it-media.de
Sitz: München, Amtsgericht München, HRA 104234
Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949:
Alleinige Gesellschafterin der IT Media Publishing GmbH & Co. KG ist die **IT Media Publishing Verwaltungs GmbH,** Sitz: München, Amtsgericht München, HRB 220269
Geschäftsführer: Sebastian Hirsch
ISSN 1860-7926

KUNDENSERVICE

LinuxWelt-Kundenservice für Einzelheft-Käufer:
DataM-Services GmbH
Postfach 9161
97091 Würzburg
Tel.: 0931/4170-177
Fax: 0931/4170-497
(Mo bis Fr, 8 bis 17 Uhr)
E-Mail: *idg-techmedia@datam-services.de*

LinuxWelt-Kundenservice für Abonnenten: Fragen zum bestehenden Abonnement / Premium-Abonnement, zum Umtausch defekter Datenträger, zur Änderung persönlicher Daten (Anschrift, E-Mail-Adresse, Zahlungsweise, Bankverbindung) bitte an
Zenit Pressevertrieb GmbH
LinuxWelt-Kundenservice
Postfach 810580
70522 Stuttgart
Tel: 0711/7252-233
(Mo bis Fr, 8 bis 18 Uhr)
Fax: 0711/7252-333
E-Mail: *linuxwelt@zenit-presse.de*
Erscheinungsweise:
6x jährlich

Jahresbezugspreise LinuxWelt mit DVD: 51,00 € (D)
57,00 € (A, CH, Benelux)
inkl. Versandkosten

Bankverbindung für Abonnenten:
Postbank Stuttgart, IBAN
DE56 6001 0070 0029
0547 04, BIC PBNKDEFFXXX

Sie können Ihr Abonnement jederzeit zur nächsten Ausgabe kündigen.
Bestellungen können innerhalb von 14 Tagen ohne Angabe von Gründen in Textform (zum Beispiel Brief, Fax, E-Mail) oder durch Rücksendung der Ware widerrufen werden.

LINUX WELT

Mini-Angebot!

Satte **33 %** gespart!

3x LinuxWelt inkl. Prämie*

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

Jetzt testen:

3 x LinuxWelt als Heft frei Haus mit Gratis-DVD +
3 x LinuxWelt direkt aufs Smartphone & Tablet mit interaktivem Lesemodus +
10,- € Geldprämie*

=17,- € (anstatt 25,50 EUR)

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

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

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

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

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

LWPM062018

* 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

Schärfen Sie Ihren Blick!

TUXEDO InfinityBook Pro 14

Intel Core i7-1165G7
Intel Iris Xe Graphics

3K Omnia Display
16:10 | 2880 x 1800 Pixel

Robustes
Magnesiumgehäuse
1,5 cm dünn | 1 kg

Thunderbolt 4
Full featured USB-C 4.0

100%
Linux

5
Jahre
Garantie

Lifetime
Support

Gefertigt in
Deutschland

Deutscher
Datenschutz

Support
vor Ort

TUXEDO COMPUTERS

tuxedocomputers.com