AUF DVD: LINUX MINT 18 UND 6 WEITERE SYSTEME

4 196691 608505 05

ANDROID WELT Sonderheft
5/2016 · August / September
Deutschland 8,50 €
Schweiz 16,90 sfr · Österreich + Benelux 9,45 €

LINUX WELT

Konsolen-Tricks

Speicherfresser killen, Logdateien auswerten, Downloads beschleunigen

Geniale Linux-Power-Tipps

- Uefi und Bios sicher updaten
- Dateien schlauer kopieren
- Mausrad-Tuning u.v.m.

Mini-Server fürs Heimnetz

Raspberry & Co. verwenden als NAS, Gruppenkalender u.v.m.

NEU: Linux mobil

Aquaris M 10: Das neue Ubuntu-Tablet im Praxistest

Linux-Notfallhilfe!

So helfen Sie sich bei Linux-Problemen

- Startprobleme beseitigen · Fehlende Codecs nachrüsten
- Hardware-Probleme lösen · WLAN-Bugs beheben
- Tuning für Windows-Virtualisierung

So wird Ihr System sicher & stabil

- Router-Lücken schließen · WLAN schützen
- Passwortmanager nutzen · Linux-Konten absichern · Mails verschlüsseln

Neu: Linux Mint 18

Das beliebteste Linux mit optimierter Oberfläche, X-Apps, neuen Software-Paketen und Langzeit-Support bis April 2021

Linux doppelt so schnell!

- Holen Sie mehr aus Ihrer SSD heraus
- So verlängern Sie die Lebensdauer des Flash-Speichers

Auf DVD: Mint 18 und 6 weitere Systeme
Fedora Workstation, KDE Neon User Edition, Bunsenlabs „Hydrogen“, Antergos, Icebox, Rescatux

PLUS: Notfallsystem für Ihren PC
Daten retten, Fehler finden, Startprobleme beheben, System reparieren

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

PC-WELT PLUS

GRATIS! Eine Ausgabe gedruckt & digital

Jetzt kostenlos die gedruckte & digitale Ausgabe bestellen!

Jetzt bestellen unter
www.pcwelt/gratis oder per Telefon: 0711/7252277 oder ganz einfach:

1. Formular ausfüllen — **2. Foto machen** — **3. Foto an shop@pcwelt.de**

Ja, ich bestelle die PC-WELT gratis.

Möchten Sie die PC-WELT Plus anschließend weiter lesen, brauchen Sie nichts zu tun. Sie erhalten die PC-WELT Plus für weitere 12 Ausgaben zum aktuellen Jahresabopreis von z.Zt. 79,90 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

PWPNA14140

PC-WELT erscheint im Verlag IDG Tech Media GmbH, Lyonel-Feininger-Str. 26, 80807 München, Registergericht München, HRB 99187, Geschäftsführer: York von Heimburg.
Die Kundenbetreuung erfolgt durch den PC-WELT Kundenservice, ZENIT Pressevertrieb GmbH, Postfach 810580, 70522 Stuttgart, Geschäftsführer: Joachim John

Arne Arnold
Redakteur
aarnold@it-media.de

Ist Linux stabil und sicher?

Linux stabil: Wenn Sie Ihr Linuxsystem erst einmal perfekt eingerichtet haben, dann läuft es lange, lange Zeit vollkommen stabil. Vor allem in seiner Paraderolle als Server macht Linux hier eine sehr gute Figur. Die wenigen Notfälle eines Linux-Systems treten meist zu Beginn einer perfekten Konfiguration auf.

Damit Ihnen solche Notfälle möglichst erspart bleiben, finden Sie in dieser LinuxWelt Einrichtungstricks für das neue Ubuntu 16.04 sowie viele Notfalltipps bei Startproblemen eines Linux-Systems.

Linux sicher: Der Ubuntu-Entwickler Oliver Grawert hatte vor rund drei Jahren scharf gegen Linux Mint geschossen. Er meinte: „Mit Linux Mint würde ich kein Onlinebanking machen". Er bezog sich dabei auf die vorgeblich schleppende Update-Politik von Linux Mint (*http://bit.ly/29Nz03E*). Gegen diesen Vorwurf wehrte sich der Linux-Mint-Initiator Clement Lefebvre vehement – zu Recht, wie die Linux-Welt findet. Mit Linux Mint lässt sich sehr wohl sicheres Onlinebanking betreiben.

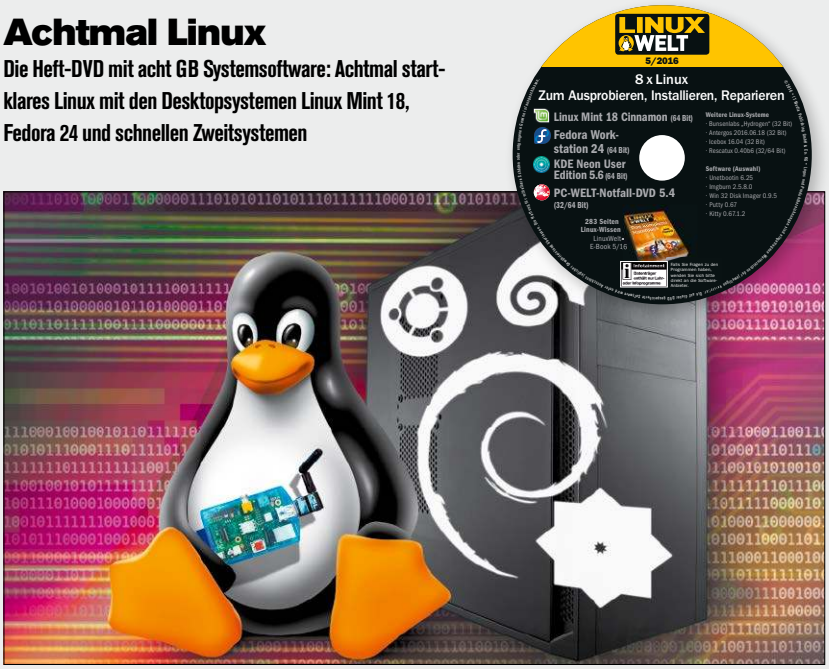
Dennoch steckt in der Kritik ein wahrer Kern: Die Update-Einstellungen von Mint sind etwas eigen. Im neuen Linux Mint 18 haben die Entwickler das Update-Tool nun überarbeitet. Welche Einstellung in Version 18 für Sie sinnvoll ist, verrät der Beitrag zum neuen Mint 18 ab Seite 16.

Diese Neuerung zeigt auch: Linux ist sicher – es lässt sich aber noch einiges verbessern, wenn man die richtigen Einstellungen wählt. Welche das genau sind, das erfahren Sie in dieser Ausgabe in unserem ausführlichen Special zum Thema Sicherheit.

Viel Spaß beim Lesen!

Achtmal Linux

Die Heft-DVD mit acht GB Systemsoftware: Achtmal startklares Linux mit den Desktopsystemen Linux Mint 18, Fedora 24 und schnellen Zweitsystemen



54 | Special Sicherheit III: Server im Internet

Wachdienste für Ihren Webserver: Öffentliche Server benötigen wachsame Aufsicht. Mit diesen Maßnahmen schützen Sie Internetserver und freigegebene Heimserver mit Apache, Wordpress & Co.

Special: Sicherheit III

Server im Internet

Software

Hardware

Praxis

Standards

Software auf Heft-DVD

LinuxWelt 5/2016

Achtmal Linux

Ausprobieren, Installieren, Reparieren

Linux Mint Cinnamon 18 (64 Bit)
Linux Mint 18 präsentiert sich in einem komplett renoviertem Outfit und tauscht Minzgrün gegen dunkles Pastell ein. Als Oberfläche dient der neueste Cinnamon-Desktop 3.0. Als Unterbau dient Ubunt 16.04 LTS. Das installierbare Livesystem liegt auch als ISO auf DVD.

Fedora 24 Workstation (64 Bit)
Die experimentierfreudige Distribution aus dem Umkreis von Red Hat zeigt sich auf dem Linux-Desktop stets als Vorreiter. In der vorliegenden Workstationvariante läuft das neue Gnome 3.20 mit optionaler Wayland-Unterstützung. Das installierbare Livesystem auf Heft-DVD ist bereits mit deutschen Sprachpaketen ausgestattet. Auch als ISO-Datei auf DVD.

KDE Neon User Edition 5.6 (64 Bit)
Für KDE-Fans: Die KDE Neon User Edition kombiniert stets die brandaktuellen KDE-Pakete mit der stabilen Basis von Ubuntu 16.04. Die neue Distribution genießt ganz offiziell die Unterstützung der KDE-Entwickler, liefert KDE Plasma 5.6 auf dem Desktop und wird vom ehemaligen Kubuntu-Team gepflegt. Auch als ISO-Datei auf DVD.

PC-WELT-Notfall-DVD 5.4 (32/64 Bit)
Das aktualisierte Livesystem aus eigener Entwicklung ist das beste Rettungssystem für defektes Windows, kann aber auch Linux-Systeme unterstützten. Der gut gefüllte Werkzeugkasten rettet Daten mit Photorec, überprüft das System mit Antivir auf Viren und setzt Windows-Passwörter zurück. Auch als ISO-Datei auf DVD.

Bunsenlabs „Hydrogen“ (32 Bit)
Die junge Debian-Variante tritt die Nachfolge der einst beliebten Distribution „Crunchbang“ an, die mit dem Erscheinen von Debian 8 eingestellt wurde. Bunsenlabs ist ein aktuelles Debian-System für Puristen mit einem extrem reduzierten, aber eleganten Openbox als Window-Manager.

Antergos 2016.06.18 (32 Bit)
Arch Linux steht normalerweise für viel Arbeit auf der Kommandozeile, bis das System installiert. Mit seinem grafischem Installer macht der Arch-Abkömmling Antergos den Einstieg deutlich einfacher. Auch als ISO-Datei mit auf DVD.

Icebox 16.04 (32 Bit)
Die inoffizielle Ubuntu-Variante macht sich für fortgeschrittene Anwender, aber auch für ältere PCs besonders schlank auf dem Desktop und präsentiert eine sehr schlichte Openbox-Umgebung. Als Basis dient hier Ubuntu 16.04 LTS. Das Installierbare Livesystem ist auch als ISO-Datei auf DVD.

Quirky 8 (64 Bit)
Eine Weiterentwicklung von Puppy Linux, das für den geringen Ressourcenverbrauch optimiert ist, aber trotzdem einen voll funktionsfähigen Desktop liefert: Quirky teilt viele Merkmale mit dem Livesystem Puppy, etwa die Möglichkeit, zur Laufzeit weitere Pakete nachzuinstallieren.

Rescatux 0.40b6 (32/64 Bit)
Dieses Rettungssystem ist für den Grub-Bootloader maßgeschneidert: Rescatux ist ein schlichtes Livesystem auf Debian-Basis, das kaputte oder überschriebene Bootloader von installierten Linux-Systemen mit Hilfe eines Assistenten wieder flottmacht. Liegt zudem als ISO-Datei auf DVD.

Extras & Tools

Super Grub Disk 2.02
Die Super Grub Disk 2 bietet eine Boothilfe für Linux-Systeme, bei welchen der Bootloader vom Typ Grub 2 nicht mehr intakt ist oder von Windows überschrieben wurde. Das Tool ist direkt aus dem Multibootmenü auf DVD unter „Extras und Tools“ startklar.

Plop Bootmanager 5
Dieser Bootmanager kann von USB-Geräten booten, auch wenn dies das Bios des Rechners nicht unterstützt. Plop bietet dafür ein eigenes Bootmenü und lässt sich von DVD starten, um ein angeschlossenes USB-Laufwerk zu booten.

Hardware Detection Tool (HDT)
Einen Überblick zur kompletten Hardware eines Systems bietet das startfähige Hardware Detection Tool (unter „Extras und Tools“), auch wenn kein Betriebssystem installiert ist. In einem englischsprachige Fenster zeigt HDT Kategorien wie PCI, RAM, Prozessor und Bios an.

Memtest 86+ 5.01
Der aktuelle Memtest 86+ testet den Arbeitsspeicher und unterstützt auch moderne Intel-Chipsätze. Das Diagnoseprogramm läuft auf jedem PC mit 32-Bit- als auch 64-Bit-CPUs sowie mit allen verbreiteten RAM-Typen. Es beginnt sofort nach dem Start mit den Tests, die jederzeit unterbrochen werden können.

DBAN 2.3
Darik's Boot and Nuke (DBAN) löscht Daten auf magnetischen Datenträgern endgültig durch Überschreiben. Auch Wiederherstellungstools können danach keine Daten mehr rekonstruieren. DBAN eignet sich nur für Festplatten. Auf Flash-Speichern, SSDs und USB-Sticks ist das Tool wirkungslos.

Software auf DVD

Imgburn 2.5.8.0
Kompaktes deutschsprachiges Brennprogramm für alle Windows-Versionen, um Imagedateien auf CDs/DVDs zu schreiben. **Hinweis:** Werbefinanzierte Freeware – die Installation bietet optional die Einrichtung der Ask-Toolbar und von Werbelinks auf dem Desktop an.

Unetbootin 6.25
Das nützliche Tool mit grafischer Oberfläche transferiert mit wenigen Klicks die ISO-Images von Ubuntu und seinen Abkömmlingen sowie weiteren Distributionen auf USB-Stick oder Speicherkarten und macht diese mit einem eigenen Bootmenü startfähig. Auf DVD befinden sich 32-Bit- und 64-Bit-Varianten für Linux (alle Linux-Distributionen) und Versionen für Windows und Mac-OS X.

Putty 0.67
Ein Terminalclient für SSH und Telnet, der für alle Windows-Systeme geeignet ist. Putty liegt in Form einer EXE-Datei vor und braucht nicht installiert zu werden. Das Open-Source-Programm ist englischsprachig.

Kitty 0.67.1.2
Als Abspaltung von Putty ist Kitty ebenfalls ein Terminalclient für SSH, allerdings mit einigen zusätzlichen Funktionen. Wie Putty wird es einfach über seine EXE-Datei gestartet.

Win 32 Disk Imager 0.9.5
Das grafische Windows-Tool überträgt hybride ISO-Images (für DVD und USB) und IMG-Dateien (für USB und Speicherkarten) wie unter Linux mit dd direkt auf USB-Sticks.

PDF-E-Booklet 5/2016

283 Seiten zum Nachschlagen, Nachsehen und Nachlesen: Die Zusammenfassung von früheren Beiträgen aus der LinuxWelt liefert zeitlose Grundlagenartikel und viel Neues aus der letzten Ausgabe, so etwa eine Artikelserie zum aktuellen Ubuntu 16.04 LTS. Auch die Rubriken zur Hardware unter Linux und zum Raspberry Pi sind um frische Beiträgen erweitert: Eine Kaufberatung hilft, das perfekte Notebook für Linux zu finden, und eine Kurzvorstellung präsentiert den Raspberry Pi 3.

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

Infotainment
Datenträger enthält nur Lehr- oder Infoprogramme

Weitere Infos Ausführliche Beschreibungen der Linux-Systeme auf DVD lesen Sie im Heft ab Seite 10. Weitere Details zu den Distributionen und Livesystemen liefert die HTML-Oberfläche auf Heft-DVD, die Sie über die Datei „index.html“ in einem Browser öffnen. Das Special im Heft dreht sich diesmal um das facettenreiche Thema Sicherheit und ist dreigeteilt: Der erste Teil ab Seite 22 zeigt die Grundlagen der System- und Datensicherheit unter Linux. Der zweite Teil ab Seite 36 handelt über Netzwerke und Internet. Im Teil drei ab Seite 54 geht es um Linux in seiner Paraderolle als gut abgesicherter Server im Internet und LAN.

PC-WELT PLUS

ANDROID WELT

Sonderheft-Abo

Für alle Sonderausgaben der PC-WELT und AndroidWelt

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: 0711/7252277 oder ganz einfach:

1. Formular ausfüllen **2. Foto machen** **3. Foto an shop@pcwelt.de**

Ja, ich bestelle das PC-WELT Sonderheft-Abo.

Wir informieren Sie per E-Mail über das nächste Sonderheft der PC-WELT bzw. AndroidWelt. 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

BEZAHLEN

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

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

PWSJO14130

PC-WELT erscheint im Verlag IDG Tech Media GmbH, Lyonel-Feininger-Str. 26, 80807 München, Registergericht München, HRB 99187, Geschäftsführer: York von Heimburg.
Die Kundenbetreuung erfolgt durch den PC-WELT Kundenservice, ZENIT Pressevertrieb GmbH, Postfach 810580, 70522 Stuttgart, Geschäftsführer: Joachim John

Sicherheit an jedem Ort

Mit der Entscheidung für Linux verschließen Sie einer Armada von digitalem Ungeziefer die Tür. Aber Linux ist kein Allheilmittel: Mit verlorenen USB-Sticks, gehackten Cloudkonten und belauschtem WLAN muss man rechnen – und aktiv vorbeugen.

Von **Hermann Apfelböck**

Eine LinuxWelt ganz im Zeichen des Themas Sicherheit: In 20 Beiträgen und auf insgesamt 44 Seiten geht es um Systemschutz und Datenschutz. Warum nur ist IT-Sicherheit so komplex und vielschichtig? In erster Linie deshalb, weil es so viele Orte und Wege gibt, auf welchen unsere Daten liegen und übertragen werden. Die Grundlagenartikel und praktischen Tipps in diesem Heft haben das Ziel, alle wesentlichen Aspekte anzusprechen, die Ihnen die Kontrolle und – wo nötig – den alleinigen Besitz der System- und Benutzerdaten garantieren.

Unsicher ist nicht gleich unsicher

Was nicht überall ausdrücklich explizit zur Sprache kommen kann, sind die fundamentalen graduellen Unterschiede der Datenunsicherheit.

Man kann es sich so veranschaulichen: Alles was physisch und digital die eigenen vier Wände verlässt, wird öffentlich und verdient bestmögliche Absicherung – es sei denn, es ist reproduzierbar und inhaltlich wertlos. Mails gehen nach draußen und wenn sie vertraulich sind, sollten sie geschützt werden. Daten auf Notebooks und USB-Datenträgern verlassen das Haus und bleiben irgendwann irgendwo liegen: Wenn sie persönliche Daten enthalten, müssen diese verschlüsselt werden. Über Daten auf Webservern und Cloudspeichern haben Sie keine Kontrolle: Auch diese sind zu schützen, wenn sie es inhaltlich wert sind.

Alles was im lokalen Netz und auf stationären PCs liegt, ist hingegen im Prinzip (WLAN geschützt?) sicher vor der Öffentlichkeit: Lokale Rechte des Dateisystems und Samba-Rechte im lokalen Netzwerk sind daher für typische Heimnetze nicht wirklich kritisch. Die Kenntnis darüber ist aber insofern wichtig, als manche Standards mehr verbieten als im Heimnetz gewünscht.

Diese freizügige Ansicht über Netzrechte gilt natürlich ausschließlich für private Heimnetze: In Firmen verlässt der „engagierte“ Mitarbeiter sein Büro mit allem, was er mit den eingeräumten Rechten abgreifen kann – und damit sind die Daten im Prinzip öffentlich.

Ein Punkt für sich sind eigene Server. Auch hier gilt wieder die fundamentale Unterscheidung zwischen einem unkritischen lokalen Datenserver im LAN-Netz und einem Web- oder Datenserver, der über das Internet öffentlich erreichbar ist (egal ob bei einem Provider oder durch Portfreigabe eines

Überblick Auf DVD

Heimservers). Wer Daten öffentlich ausliefert, darf nicht öffentlich ausgeliefert sein: Die Administration per Fernwartung muss rigoros abgesichert werden und auch die Daten, die der Server preisgibt, benötigen kritische Überwachung.

Nicht zuletzt ist typische Software für öffentliche Server wie Wordpress und Apache (ganz anders als das Linux-Basissystem) ein beliebtes Angriffsziel für Internetganoven. Hier hilft nur die Kenntnis über aktuelle Sicherheitslücken und entsprechende Updatepflege.

Die Heft-DVD mit brandaktuellem Linux Mint 18

Die neue Version von Linux Mint hat vergleichsweise lange auf sich warten lassen. Der Unterbau mit Ubuntu 16.04 TLS stand seit April bereit, dennoch wurde Mint 18 erst am 30.6. finalisiert und freigegeben.

Wir freuen uns, das beliebte Desktop-Linux auf der Heft-DVD dieser Ausgabe noch ganz aktuell mitliefern zu können, und haben dafür mit einem späten Neubau der bereits fertigen DVD keine Mühen gescheut. Es handelt sich um die Mint-Hauptausgabe in 64-Bit-Ausführung mit dem angestammten Cinnamon-Desktop. Eine Erstvorstellung von Linux Mint 18 finden Sie im Heft ab Seite 16.

Weitere Highlights auf DVD sind die neue Fedora Workstation 24, das aktualisierte PC-WELT-Notfallsystem 5.4 für havarierte Windows-Rechner und der Crunchbang-Nachfolger Bunsenlabs für Linux-Anwender, die es puristisch und funktional mögen. Hinzu kommen bewährte Service- und Reparatursysteme wie Super Grub Disk unter „Extras und Tools“.

Um ein Livesystem zu starten, legen Sie die DVD ins Laufwerk und booten den Rechner von DVD. Dazu rufen Sie entweder beim Rechnerstart per Tastendruck das Bios-Bootmenü auf oder Sie ändern die Bootreihenfolge im Bios. Im Menü der Heft-DVD wählen Sie dann eine Distribution aus. In der Regel gelingt der Systemstart mit der Standardoption „Normaler Start“.

Die meisten Systeme liegen auch als ISO-Images auf der DVD vor (im Verzeichnis „Image-Dateien“) und lassen sich mit einem Linux- oder Windows-System bootfähig auf CD/DVD oder auf USB-Stick schreiben. Die einschlägigen Windows-Tools Imgburn und Unetbootin finden Sie ebenfalls auf der Heft-DVD. Unter Linux hilft das Kommandozeilenprogramm dd.

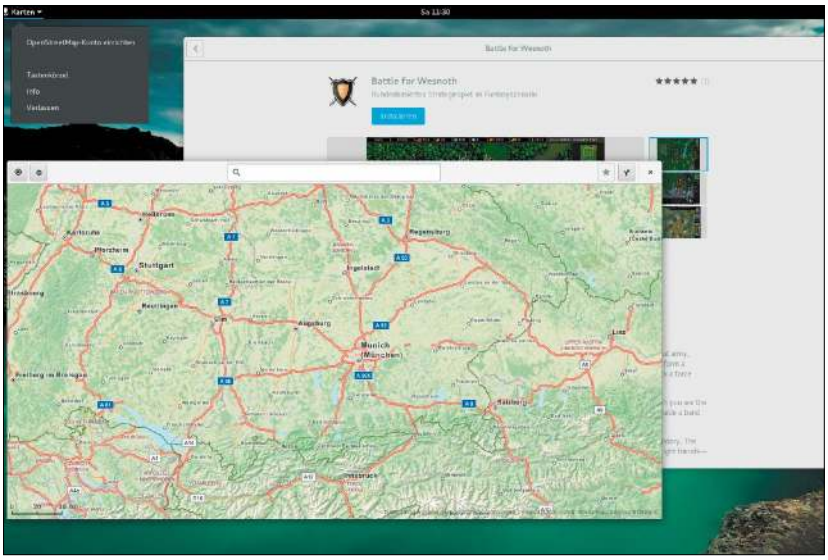
Bootmenü der Heft-DVD: Alle Distributionen starten als Livesysteme direkt von DVD. Desktopsysteme wie Mint, Fedora, KDE Neon bieten die Installation auf Festplatte an.

Fedora 24 Workstation

Die von Red Hat unterstütze Distribution zeigt gerne die neuesten Entwicklungen auf dem Linux-Desktop, ist aber nicht immer leicht zu bändigen. Fedora 24 ist ein Stück zahmer geworden, da Technologien wie Wayland gereift sind.

Von **David Wolski**

Auf dem Desktop zeigt sich das stets vorauseilende Fedora weiterhin experimentierfreudig und spricht ebensolche Anwender an. In seiner neuen Ausgabe 24 gibt sich das System aber gereifter und ist mit weniger Nacharbeiten zufrieden. Der Grund dafür auch sein, dass sich die Entwickler auf eine Verschiebung um einen Monat einigten, um den letzten Bugs mehr Zeit zu widmen. Das ist eine Menge – sogar für diese schon traditionell oft verspätete Distribution. Fedora 24 haben die längeren gründlicheren Arbeiten an den letzten Kleinigkeiten aber offensichtlich gut getan.



Geizt nicht mit Neuigkeiten: Fedora präsentiert ein neues Gnome 3.20 und erlaubt erste Tests mit Flatpak-App-Containern, die den neuen Snappaketen von Ubuntu ähneln.

Desktop und Software

Auf dem Desktop präsentiert die reguläre Workstationausgabe ein brandneues Gnome 3.20 mit schönerem Schriftrendering und überarbeiteten Gnome-Anwendungen: Gnome Maps blendet die Karten von Open Street Map ein und erlaubt die Bearbeitung von Einträgen. Das Tool Gnome Fotos hat eine Bearbeitungsfunktion, die allerdings bislang nur einfache Retuschen ausführen kann. Die Bildverwaltung Shotwell ist in Fedora 24 Workstation ebenfalls noch vorhanden, denn diese kann Gnome Fotos vorläufig nicht ersetzen. Ein Flair von Apple verbreitet der neue Konfigurationsdialog für Eingabegeräte, denn dort ist jetzt auch eine Funktion für inverses Scrollen auf Touchpads untergebracht. Die Tastenkombination Strg-F1 zeigt in Gnome-Anwendungen jetzt eine Übersicht der jeweiligen Tastenkombinationen an.

Bei der Softwareauswahl bleibt Fedora 24 Workstation bei bewährten Komponenten wie Firefox, Evolution für E-Mail, Rhythmbox als Musikplayer und Libre Office 5.1.

Zur Fotoverwaltung dient eine neue Version von Shotwell, die jetzt unter der Ägide von Gnome steht. Patentrechtlich geschützte Codecs und auch einige Player wie VLC sind in Fedora nicht enthalten, stehen aber über externe Paketquellen wie *http://rpmfusion.org* bereit.

Neues Paketformat: Flatpak

Das App-Format namens Flatpak ergänzt die grundlegende RPM-Paketverwaltung des Systems um einen neuen Installationsweg, der an Apps für Smartphones erinnert.

Flatpaks, die während der Entwicklungsphase noch „xdg-app“ hießen, erlauben die Installation von Programmen in eigenen Verzeichnissen, die von anderen Systemkomponenten isoliert sind. Diese Pakete sind zudem unabhängig von einer bestimmten Distribution. Zwar ist Flatpak erst in der Testphase und muss mit

```
sudo dnf install flatpak
```

explizit nachinstalliert werden, aber es gibt bereits Programme wie Libre Office, Inkscape, Gnome- und KDE-Basisprogramme als Flatpak. In die grafische Paketverwaltung Gnome Software ist es noch nicht aufgenommen worden und so erfolgen die Schritte zur Installation eines Flatpaks vorerst manuell über die Befehlszeile. Eine weitere Schwierigkeit bei Flatpak: Es gibt noch kein zentrales App-Verzeichnis. Quellen für Flatpaks müssen auf *http://flatpak.org* gesucht und eingetragen werden. Da ist Ubuntu mit seinen „Snaps“ im Vergleich schon einen Schritt weiter.

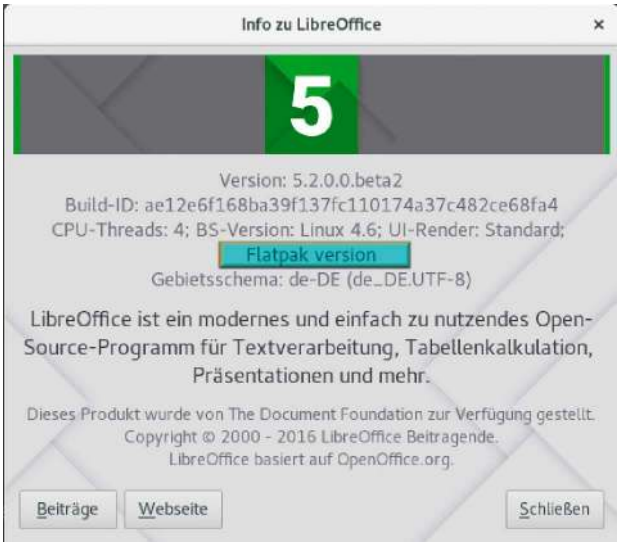
Updates werden einfacher

Für die Verwaltung der regulären Softwarepakete dienen Gnome Software und das Tool dnf auf der Kommandozeile, das auch die Aktualisierung von Fedora 23 auf 24 ohne Neuinstallation erledigen kann. Diesen Aktualisierungsweg auf eine neue Fedora-Ausgabe gab es zwar früher schon, war aber stets ein Drahtseilakt. Gerade für eine schnell fortschreitende Distribution mit Halbjahresrhythmus war dies stets ein wunder Punkt. Nun kann der Paketmanager dnf den Wechsel auf Fedora 24 erledigen und hat dafür ein neues Plug-in bekommen, dessen Verwendung unter *https://fedoraproject.org/wiki/DNF_system_upgrade* schon ausführlich dokumentiert ist. Der Sprung auf Fedora 24 ist damit mit vier Befehlen in der Kommandozeile zu erledigen. Der Paketmanager lädt neue Pakete herunter, was eine Datenmenge von rund 1,2 GB umfasst, und startet dann das System neu in eine minimale Bootumgebung. Das eigentliche Upgrade aller Pakete bleibt dann Systemd überlassen. In Zukunft wird dieses Systemupdate auch grafisch über Gnome Software möglich sein und auch Fedora 23 soll den grafischen Weg noch per Update erhalten.

Wayland: Beinahe alltagstauglich

Eigentlich war geplant, den neuen Displayserver Wayland, der baldmöglichst Xorg als Grundlage für den grafischen Desktop ersetzen soll, schon jetzt zum Standard zu küren. Davon sieht Fedora 24 jedoch noch ab und liefert in der Hauptausgabe mit Gnome wieder die Option „Gnome unter Wayland“ als separate Session.

Auf einem Testrechner von Tuxedo mit aktuellem Intel-Chipsatz (Skylake) gibt es an Wayland wenig auszusetzen: Endlich klappt Copy und Paste zwischen Programmen, die Wayland und die Kompatibilitätsschicht Xwayland verwenden, über einen gemeinsamen Buffer. Nur manchmal will Ctrl-V auf Anhieb nicht gleich Inhalte aus der Zwischenablage einfügen. Auch die mittlere Maustaste hat unter Wayland wieder eine Funktion und fügt mit der Maus markierte Inhalte ein – eine Funktion, die viele Anwender unter Wayland bisher vermisst haben. Mit proprietären Grafiktreibern von Nvidia und AMD funktioniert Wayland allerdings noch nicht.



Geizt nicht mit Neuigkeiten: Fedora präsentiert ein neues Gnome 3.20 und erlaubt erste Tests mit Flatpak-App-Containern, die den neuen Snappaketen von Ubuntu ähneln.

Upgrade ohne Neuinstallation: Die Aktualisierung eines Fedora 23 auf Version 24 über dnf in der Kommandozeile klappt bereits problemlos. Ein grafischer Weg soll folgen.

Fazit: Zugängliches Fedora 24

Es ist kein Geheimnis, dass in der Fedora-Entwicklung ambitionierte Sprünge im Vordergrund stehen und nicht die möglichst benutzerfreundliche Zusammenstellung altbewährter Komponenten. Schließlich gibt es dafür Red Hat Enterprise Linux und dessen frei verfügbaren Abkömmling Cent-OS, für die Fedora mit seinen Experimenten als Vorstufe gilt. Trotzdem ist Fedora 24 eine der pflegeleichteren Ausgaben dieser Distribution geworden. Klar, die Zielgruppe ist immer noch der fortgeschrittene Anwenderkreis. Aber auch wer diesem gerade erst entwachsen ist, wird von Fedora 24 nicht vor unlösbare Aufgaben oder frustrierende Bugs gestellt. Mit sehr aktueller Hardware funktioniert das System dank des frischen, als Update nachgereichten Kernel 4.6.3 ausgesprochen gut.

Mehr Infos

Auf Heft-DVD liegt Fedora 24 Workstation in 64 Bit. Es handelt sich um eine von der LinuxWelt-Redaktion angepasste Version, die das Livesystem bereits in Deutsch startet. Ansonsten gibt es keine Unterschiede zu den offiziellen Installationsmedien. Die zahlreichen anderen Fedora-Ausgaben mit weiteren Desktops wie KDE, Cinnamon und dem schlanken LXDE liefert die Projekt-Webseite.

Website: *https://getfedora.org*

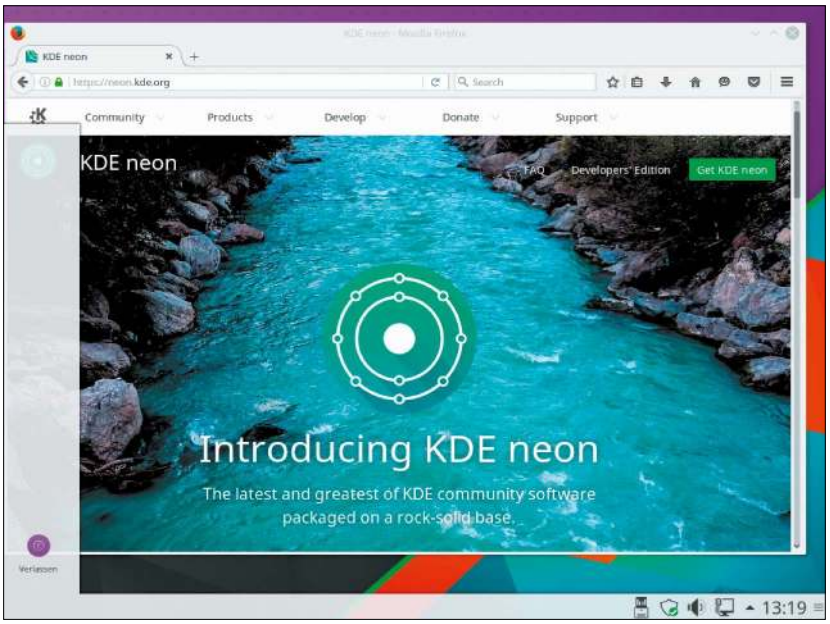
Dokumentation: *http://docs.fedoraproject.org*

KDE Neon User Edition 5.6

Mit dieser Distribution erhält die Desktopumgebung KDE Plasma 5 ein Vorzeigesystem. KDE Neon User Edition 5.6 ist eine Neuvorstellung, nutzt Ubuntu als Unterbau und versorgt KDE-Fans ab jetzt mit besonders frischen KDE-Paketen.

Von **David Wolski**

Drei Kräfte haben sich bei diesem regelmäßig aktualisiertem System zusammengetan: Jonathan Riddell als ehemaliger Kopf hinter Kubuntu, die KDE-Entwickler und deren Sponsoren. Diese prominente Aufstellung soll dafür sorgen, dass KDE Neon neben Open Suse und Kubuntu ein vielversprechendes Vorzeigesystem für diese Desktopumgebung wird. Denn KDE hat ganz offensichtlich ein Problem mit den üblichen Distributionen, die in ihrem eigenen Rhythmus erscheinen: Das aktuelle KDE Plasma 5.x entwickelt sich enorm schnell und ist entsprechend dieser Geschwindigkeit immer wieder von Bugs beeinträchtigt.



Aushängeschild für KDE Plasma: Die KDE Neon User Edition will ab sofort ein stets aktuelles und stabiles KDE liefern und verlässt sich bei den Systemkomponenten auf Ubuntu.

KDE in neuer Kadenz

Unter den genannten Voraussetzungen ist es von Vorteil, mit möglichst frischen KDE-Paketen zu arbeiten. Distributionen wie Kubuntu oder Open Suse Leap können hier nicht Schritt halten. Das stets aktuelle Arch Linux und dessen Abkömmlinge wie Manjaro oder Netrunner sind dagegen oft zu experimentell und können zwischenzeitlich keinen stabilen Desktop für die tägliche Arbeit bieten. KDE Neon soll nun diese Lücke füllen, denn die vorliegende User Edition hat KDE-Pakete an Bord, die zwar frisch, aber bereits getestet sind.

So ist in der vorliegenden ersten öffentlichen Ausgabe der KDE Neon User Edition KDE Plasma 5.6 enthalten. Daneben gibt es auch noch die experimentelle Developer Edition, die ihren KDE-Desktop aus den Entwicklerquellen schöpft und eher für neugierige Anwender und fortgeschrittene KDE-Fans gedacht ist. Unter anderem lässt sich hier KDE nach der Installation einiger Zusatzpakete auch schon unter Wayland ausprobieren.

Ubuntu als Systembasis

Trotz dem Zerwürfnis zwischen einigen ehemaligen Kubuntu-Köpfen und der Ubuntu-Gemeinde samt Canonical ist KDE Neon kein Abschied von Ubuntu. Als Grundlage dient auch hier Ubuntu 16.04 LTS, das den Kernel, wichtige Betriebssystemkomponenten und einige Anwendungen außerhalb des KDE-Umfelds mitbringt.

KDE Neon wird auch in der User Edition teilweise als Rolling Release gepflegt: KDE-Komponenten bekommen also laufende Updates, während der Ubuntu-Kern bei den erprobten Programmversionen der letzten LTS-Ausgabe bleibt.

Das Installationsprogramm ist eine KDE-Version des bewährten Ubiquity, die auch im offiziellen Kubuntu die Einrichtung auf Festplatte übernimmt. Das Livesystem (in 64 Bit auf Heft-DVD) enthält deutsche Sprachpakete und bietet die gesamte Oberfläche auch in Deutsch an.

Die Hardwareanforderungen fallen nicht anders als bei Kubuntu oder Open Suse aus: Eine 64-Bit-CPU und zwei GB RAM sollten es mindestens sein. Mehr ist besser, denn KDE hat einen stattlichen Speicherhunger.

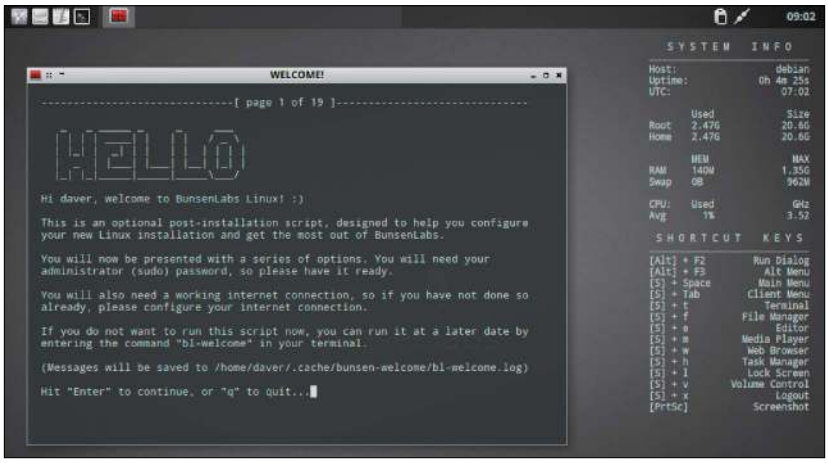
Website: *https://neon.kde.org*
Dokumentation:
https://neon.kde.org/faq

Bunsenlabs „Hydrogen“

Wer Feuer und Flamme für minimalistische Arbeitsumgebungen ist, bekommt mit Bunsenlabs „Hydrogen“ einen Nachfolger des einst beliebten, aber inzwischen eingestellten Crunchbang. Für einen soliden Unterbau sorgt ein Debian 8.

Von **David Wolski**

Die Rezeptur ist gleich geblieben, die Zutaten sind frisch: Bunsenlabs „Hydrogen“ ist ein solides Debian-System mit einem möglichst reduzierten Desktop. Die Optik ist durchgehend in Grau und Anthrazit gehalten, um den Desktop möglichst unaufdringlich zu halten. Um den Desktop kümmert sich der Window-Manager Openbox, das Anwendungsmenü wird mit einem Rechtsklick auf den Desktophintergrund geöffnet. Auf der Arbeitsoberfläche zeigt der Systemmonitor Conky die Auslastung und einige nützliche Tastenkürzel an. Die Zielgruppe sind dabei eher fortgeschrittene Debian-Anhänger.



Ganz schön grau: Bei Bunsenlabs spielt der Openbox-Desktop eine bewusst dienende Rolle. Im Hintergrund zeigt der Systemmonitor Conky Infos zur Auslastung der Ressourcen.

Ein Debian für Puristen

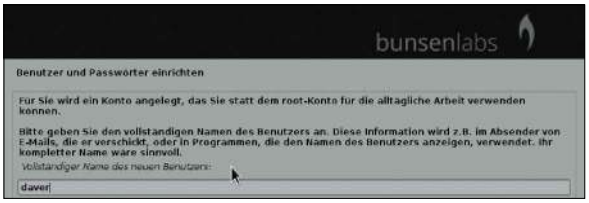
Bunsenlabs ist ein Debian 8 „Jessie“ und nutzt dessen Paketquellen, die mit eigenen Repositories ergänzt werden. Das System wird noch die gesamte Unterstützungszeit von Debian 8, die mindestens bis 2020 gehen soll, mit Updates versorgt. Wie auch bei Debian 8 geht es hier nicht um die allerneuesten Programmversionen, sondern um stabile, bewährte und lange getestete Pakete. So ist der Kernel wie im regulären Debian noch bei 3.16, Libre Office ist auf dem Stand 4.3.3, als Webbrowser dient ein Iceweasel (Firefox) 38.8 ESR. Thunar, der Dateimanager von XFCE, kommt standardmäßig auch in Bunsenlabs zum Einsatz. Anders als bei einem Debian von der Stange sind hier schon der Videoplayer VLC enthalten und die proprietären Firmwarepakete aus dem Non-Free-Repository. Das vereinfacht die Verbindung über WLAN-Chips ungemein. Um das fertige System möglichst schlank zu halten, sind außer dieser Grundausstattung kaum Anwendungen vorinstalliert: Von Libre Office ist nur der Writer vorhanden, die anderen Komponenten des Büropakets müssen bei Bedarf nachinstalliert werden. Der Reiz des minimalen Systems ist, gezielt nur die benötigten Anwendungen einzurichten. Für diesen Zweck ist die grafische Paketverwaltung Synaptic enthalten.

Livesystem und Installation

Bunsenlabs liegt in der 32-Bit-Ausführung auf DVD. Bei der Installation benötigt es nur drei GB Speicherplatz auf der Festplatte. Das Livesystem dient zur Demonstration des Desktops und bringt einen separaten Installer mit. Wie bei Openbox nicht anders zu erwarten, sind die Hardwarevoraussetzungen minimal; der Desktop verlangt nur rund 200 MB RAM.

Der Installer ist von Debian übernommen und kann über einen separaten Eintrag im Multibootmenü der Heft-DVD gestartet werden, allerdings nicht aus dem Livesystem heraus. Neben dem grafischen Installationsprogramm gibt es wie bei Debian auch eine textbasierte Installation.

Website: *www.bunsenlabs.org*
Dokumentation:
www.bunsenlabs.org/installation.html



Separater Installer: Bunsenlabs „Hydrogen“ läuft als Livesystem, bietet aber den Debian-Installer im Grafik- sowie Textmodus als eigenen Bootmenüpunkt.

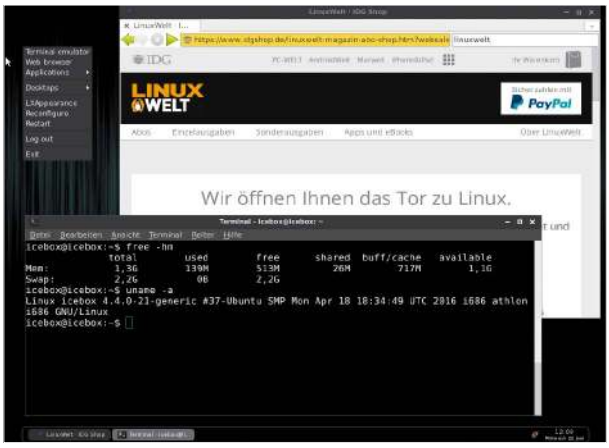
Antergos 2016.06.18

Diese Variante von Arch Linux ist eine attraktive Option für ambitionierte Anwender, die eine vollständig manuelle Installation des Arch-Vorbilds scheuen. Während pures Arch bei der Einrichtung ein längeres Textadventure sein kann, senkt Antergos die Einstiegshürde und liefert ein durchdachtes Installationsprogramm mit. Der Installer sieht jenem von Ubuntu recht ähnlich und startet aus einem schlichten Livesystem heraus. Schon im Installer stehen für das fertige System mehrere Desktops zur Auswahl: Gnome 3.20, KDE Plasma 5.6, Cinnamon 3, Mate 1.14 und XFCE 4.12. Das Resultat ist trotzdem ein echtes Arch Linux mit vielen seiner Vorzüge: Die Pakete sind sehr aktuell, denn das Paketformat von Arch erlaubt es den Entwicklern, fertige Pakete ohne großen Aufwand aus dem Quellcode von Programmen zu erzeugen. Als Rolling Release lässt sich die Distribution allein über den Paketmanager aktuell halten und bleibt, einmal installiert, über Jahre ohne Neuinstallation frisch. Antergos nutzt die originalen Repositories von Arch und keine eigenen Quellen. Für das Paketmanagement steht auf dem Desktop Pacman XG zur Verfügung und auf der Kommandozeile das Arch-Tool pacman. Antergos überlässt es den Anwendern, die benötigte Software nachzurüsten. Wie Arch verzichtet auch Antergos auf grafische Werkzeuge zur Systemadministration. Das Livesystem liegt komplett in Deutsch vor (als 32-Bit-Ausführung auf Heft-DVD).

Website: *http://archbang.org*
Dokumentation:
http://wiki.archbang.org

Icebox 16.04

Diese Distribution spricht eine ähnliche Zielgruppe an wie Bunsenlabs. Statt Debian 8 kommen hier aber die Betriebssystemkomponenten von Ubuntu 16.04 LTS zum Einsatz, die der Entwickler von Icebox mit dem besonders schlichten Openbox kombiniert hat. Damit kommt Ubuntu für schwächere Rechner in Betracht, für die sich ansonsten nur das ebenfalls sparsame Lubuntu anbietet. Auf Heft-DVD bieten wir daher auch ein Icebox 16.04 in der 32-Bit-Ausführung an. Der Desktop ist auf die nötigsten Elemente reduziert und noch eine Spur schlichter als jener von Bunsenlabs. Die Einstellungsdialoge zur gelungenen Optik der Programmfenster sowie der Dateimanager Pcmanfm sind von Lubuntu übernommen. An vorinstallierter Software gibt es gerade mal Terminals und den Webbrowser Xombrero, der sich dank der verwendeten Webkit-Engine durchaus sehen lassen kann. Um das System nach den eigenen Wünschen einzurichten, führt kein Weg am Terminal vorbei, denn es gibt zunächst keinen grafischen Paketmanager. Zur Softwareinstallation dient apt auf der Kommandozeile. Icebox verwendet nicht nur die Standard-Paketquellen von Ubuntu, sondern fügt auch zwei weitere Repositories hinzu. Voraussichtlich soll Icebox wie Xubuntu, Lubuntu und die anderen kleinen Ubuntu-Ausgaben Updates bis 2019 erhalten. Der Desktop ist nicht komplett in Deutsch übersetzt, sondern liegt teilweise in Englisch vor. Die installierbaren Programme sprechen hingegen Deutsch.



Website:
https://unit193.net/icebox/download
Dokumentation:
https://unit193.net/icebox

PC-WELT-Notfall-DVD 5.4

Aufgefrischt: Wie ein Feuerlöscher für den Notfall braucht auch ein Reparatursystem von Zeit zu Zeit eine Inspektion. Dieses Livesystem aus der LinuxWelt-Redaktion hat mit Version 5.4 den Linux-Kernel 4.1, einen frischen Firefox 45 und weitere Updates für Gparted und Clonezilla bekommen. Generell stehen hier Tools im Mittelpunkt, die dabei helfen, Windows-Katastrophen zu überstehen und PCs nach Havarien wieder flottzumachen. So bietet die PC-WELT-Notfall-DVD die Werkzeuge für einen unkomplizierten Virencheck auf Windows-Partitionen und zum Wiederherstellen von gelöschten Dateien.

Gegen Malware sind die Scanner Avira und Clam AV vorhanden und über eine Internetverbindung jederzeit schnell mit neuen Definitionsdateien versorgt. Zur Datenrettung gibt es Photorec mit einem grafischen Front-End.

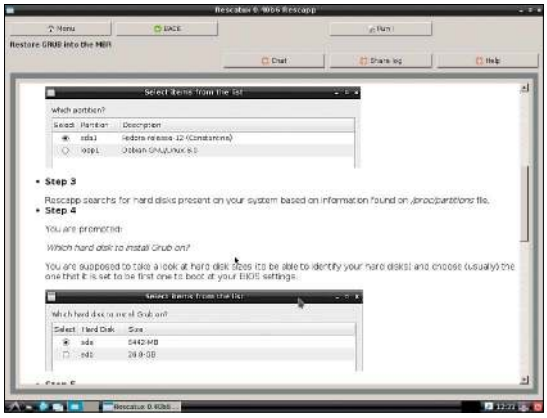
Die PC-WELT-Notfall-DVD stellt für die intuitive Bedienung einen XFCE-Desktop bereit, auf dem Sie die wichtigsten Tools über das ausklappende Menü „Rettungswerkzeuge“ im oberen Panel erreichen. Zur Verbindungsaufnahme mit einem Netzwerk und WLAN ist Wicd vorhanden. Speziell für Windows ist das Tool Chntpw über den Punkt „Kennwort neu (neue Version)“ vorhanden, um Administratorpasswörter von Windows zurückzusetzen. Zum Einhängen von Partitionen aller Art gibt es ein grafisches Einhängetool im oberen Panel (drittes Symbol von links). Über das Multibootmenü der Heft-DVD startet das Livesystem als 32-Bit-Variante oder auch mit 64 Bit für neuere Systeme.

Website: www.pcwelt.de/1168242
Dokumentation:
www.pcwelt.de/1753246

Rescatux 0.40b6

Gäbe es einen Schönheitswettbewerb für Live- und Reparatursystem, dann würde Rescatux sicher auf einem der letzten Plätze landen. Was dem System an optischer Finesse fehlt, macht es aber durch seinen Nutzwert wett. Rescatux stellt überschriebene und defekte Grub-Bootloader wieder her, wenn diese beispielsweise von einer Windows-Installation im Dualboot-Betrieb überschrieben wurden. Zwar lassen sich defekte Grub-Bootloader mit praktisch jeder aktuellen Live-CD auf manuellem Weg reparieren, jedoch macht Rescatux die Reparatur deutlich einfacher und fehlertoleranter.

Nach dem Start von Rescatux startet die englischsprachige Reparaturanwendung Rescapp automatisch. Im Menüpunkt „Grub (+)“ können Sie mit „Restore Grub“ einen neuen Grub-Bootloader schreiben und dabei alle automatisch erkannten Betriebssysteme (Linux und Windows) in ein neues Bootmenü einbinden. Die Funktion „Update Grub Menus“ greift zur Restaurierung der Bootmenüs auf die Konfigurationsdateien des installierten Linux-Systems zurück.



Für Ubuntu-Systeme ist unter „Expert Tools“ zudem das Tool „Boot-Repair“ vorhanden, das den Bootloader eines Ubuntu-Systems wiederherstellen kann. Im Multibootmenü stehen jeweils eine Version für 64 Bit und 32 Bit zur Auswahl. Diese muss passend zum installierten System ausgewählt werden, dessen Bootloader repariert werden soll. Mit der 32-Bit-Version lässt sich kein 64-Bit-System reparieren. Für den Start auf Uefi-Rechnern und für USB-Sticks ist Rescatux auch als ISO-Datei auf DVD.

Website: *http://sourceforge.net/projects/rescatux/files*
Dokumentation:
www.supergrubdisk.org/rescatux

Das neue Linux Mint 18

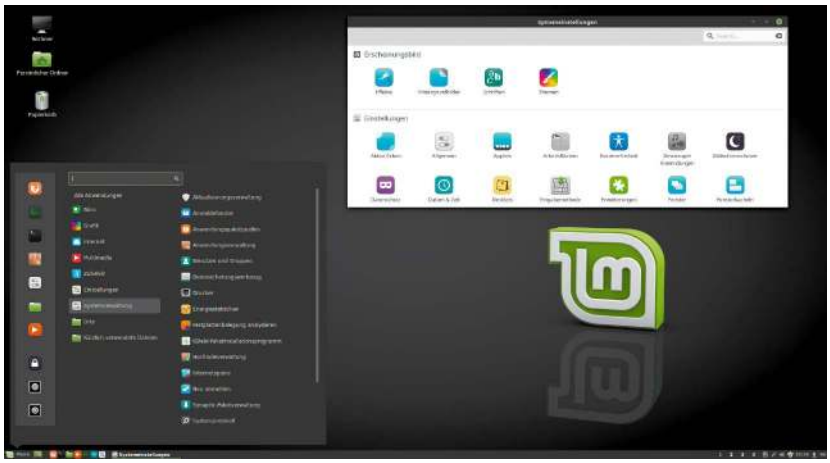
Linux Mint 18 wurde am 30.6. fertiggestellt: Mint ist das Desktop-Linux schlechthin, hat sich im Gegensatz zu Ubuntu ganz dieser Rolle verschrieben und steht auf distrowatch.com auf Platz eins der Linux-Distributionen. Kann Mint 18 diesen Platz verteidigen?

Von **Hermann Apfelböck**

Linux Mint basiert auf Ubuntu und zwar mittlerweile ausschließlich auf den Ubuntu-Langzeitversionen (LTS). Das jüngste Ubuntu 16.04 LTS erschien im April, so dass nun wieder eine neue Mint-Version anstand (Version 18 mit Codenamen „Sarah"). Das von Heft-DVD startende Livesystem ist die Standardedition von Linux Mint mit dem angestammten Cinnamon-Desktop in der 64-Bit-Ausführung. Weitere Varianten mit Links zu Spiegelservern für den Download zeigt wie gewohnt die Projektseite *https://linuxmint.com*. Bei Redaktionsschluss Anfang Juli war neben der Cinnamon-Variante nur die Mate-Edition bereits fertiggestellt (Downloadgröße etwa 1,6 GB). Die Editionen mit KDE und XFCE werden in Kürze folgen.

Die guten Nachrichten zuerst: Linux Mint 18 stellt sich wieder auf eine aktuelle Ubuntu-Systembasis mit Kernel 4.4.0 und bringt eine renovierte Oberfläche (Cinnamon 3.0.6) sowie frische Softwarepakete mit (etwa Firefox 47, VLC 2.2.2 und Libre Office 5.1.4). Mint 18 erhält genau wie Ubuntu 16.04 Langzeitsupport für fünf Jahre bis April 2021 (die Variante mit Mate-Desktop nur bis 2019). Und wer Linux Mint bereits jahrelang nutzt, wird eine absolut vertraute Umgebung vorfinden, die keinerlei Umstellung abverlangt.

Die schlechte Nachricht: Mint 18 bringt wenig Neues, das sich unmittelbar auf den Benutzeralltag auswirkt. Wer von den neuen X-Apps (die es durchaus gibt) funktional Neues erwartet hat, wird enttäuscht werden.



Modernisierung mit Cinnamon 3

Die angestammte Mint-Oberfläche Cinnamon ist in Version 3.0.6 enthalten. Der Versionsschritt über die „3" bringt aber nur marginale Verbesserungen – vorwiegend in Applets der Systemeinstellungen, die Sie unten im Punkt „Kleine Neuerungen und Verbesserungen" nachlesen können. Cinnamons Fenstermanagement hat das Einrastverhalten von Fenstern optimiert, so dass nun auch eine Skalierung von geviertelter Bildschirmgröße möglich ist. Die automatische Größenanpassung erfolgt, wenn das Fenster mit der Maus gezogen und dabei gleichzeitig die Taste Strg gedrückt wird (die gewünschte Taste ist einstellbar).

Auffälliger und wesentlicher als solche Detailverbesserungen ist die optische Modernisierung des Desktops. Cinnamons neue Designelemente sind unter „Systemeinstellungen -> Themen" als „Mint-Y" erkennbar, während die klassischen Themen als „Mint-X" erscheinen. Insbesondere die neuen Symbolthemen, die sich im Hauptmenü, in den Systemeinstellungen (cinnamon-settings), in der Systemleiste präsentieren, geben dem tendenziell konservativen Cinnamon-Desktop einen überraschend modernen Anstrich. Allerdings gelingt noch nicht jedes Symbol wirklich aussagekräftig (Firefox?).

Ein seit Jahren gewünschtes Feature war zwar ursprünglich angekündigt, ist aber erneut nicht realisiert: Die Leisteneinstellungen (die übrigens nach wie vor das umständliche Aktivieren des „Bearbeitungsmodus" erfordern) ermöglichen zwar eine zweite Leiste, aber eine vertikale Anordnung von Systemleisten ist weiterhin unmöglich. Auf heutigen Breitbildschirmen ist das ein echtes Manko.

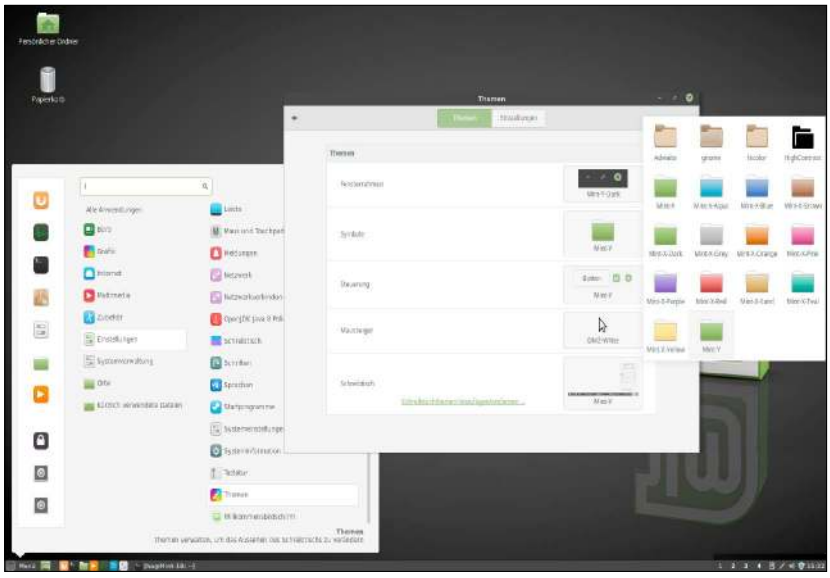
Mint 18 mit den ersten X-Apps

Für Entwickler ist das Thema X-Apps eine wichtige und produktive Neuerung, weil es die Chance eröffnet, (Gnome-)Programme zu schaffen, die auf diversen Gnome-affinen Oberflächen laufen. Auf lange Sicht sollte damit die Abhängigkeit von Distributionen und Desktopumgebungen

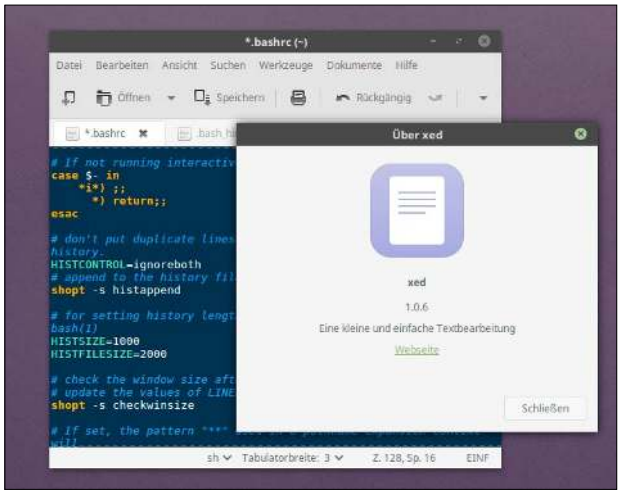
wegfallen, wobei es dem Mint-Team wohl primär um die Desktops Cinnamon, Mate und XFCE gehen dürfte. Die X-Apps haben nicht den Anspruch auf funktionale Innovation, ja nicht mal den, neue Software zu sein. Es geht darum, bewährte Programme desktopunabhängig zu machen und dabei abwärtskompatibel zu bleiben.

Linux Mint 18 präsentiert nun mal schon die ersten fünf X-Apps, nämlich den Texteditor Xed (deutsch: „Textbearbeitung“) auf der Basis von Pluma/ Gedit, den Player Xplayer (deutsch „Videos“) auf der Basis von Totem, ferner den Bildviewer Xviewer (deutsch: „Bildbetrachter“) auf der Basis von Eog und den Xreader (deutsch: „Dokumentenbetrachter“) auf der Basis von Atril/ Evince. Schließlich gibt es noch den exzellenten Bildviewer Pix (deutsch ebenfalls „Pix“), der auf Gthumb basiert.

Für den Anwender ist die Diskussion über die neuen X-Apps von geringem Interesse. Funktional haben diese ersten fünf X-Kandidaten nichts Neues zu bieten. Positiv ist aber anzumerken, dass Xed, Pix und Co. keinerlei Umstellungsschwierigkeiten zeigen – sie funktionieren genauso schnell und zuverlässig wie ihre Vorgänger Gedit, Gthumb und Co.



Neue Cinnamon-Themen: Die Mint-Y-Themes für Symbole und Schreibtisch (siehe „Systemeinstellungen -> Themen“) modernisieren die Oberfläche frappierend.



X-App Xed ist nichts anderes als Gedit: Für Anwender spielt die Portierung bekannter Gnome-Programme in das X-App-Format keine wesentliche Rolle.

Neues in der „Aktualisierungsverwaltung“

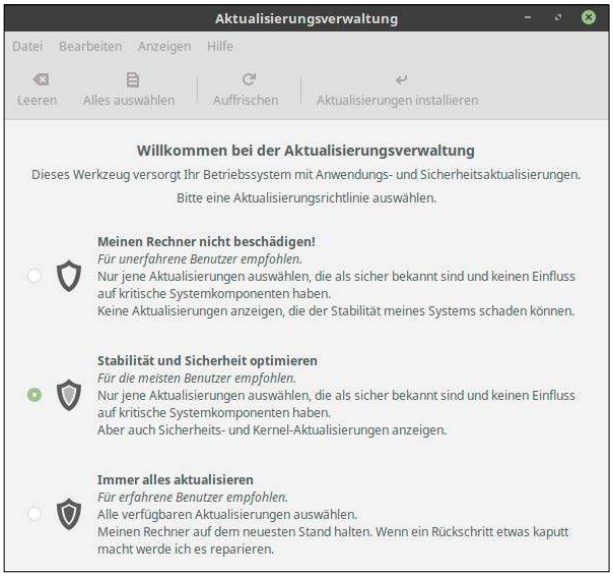
Beim Update geht Linux Mint schon lange eigenwillige Wege. Die „Aktualisierungsverwaltung“ (mintupdate) mit ihrer Level-Kategorisierung ist ein Eigengewächs des Mint-Teams. Standardmäßig zeigt und installiert das Tool nur Updates, die Linux Mint nach den Levels 1, 2 und 3 klassifiziert. Alles, was nicht selbst vom Mint-Team getestet wurde, sondern beispielsweise aus den Ubuntu-Repositories stammt, wird mit Stufe 4 oder 5 bewertet. Kernel-Updates fallen in Level 5 und bleiben daher unsichtbar.

Mit der Realität stimmt die Einschätzung des Mint-Teams, was stabil ist, nicht immer überein. So landen etwa in den offiziellen Ubuntu-Repositories keine experimentellen Pakete, und Probleme nach Updates aus diesen Quellen sind deshalb selten.

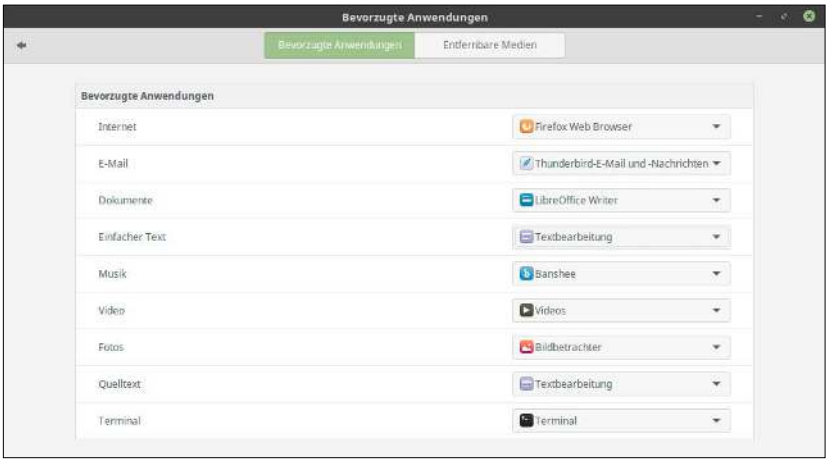
Nun war es zwar schon immer möglich, in der „Aktualisierungsverwaltung“ mit „Bearbeiten -> Einstellungen -> Ebenen“ auch Level 4 und 5 als „Sicher“ und „Sichtbar“ zu markieren und damit auch solche Updates zu beziehen. Das Mint-Team hat aber offenbar eingesehen, dass das Levelkonzept für die typische Anwenderklientel des Mint-Systems eher undurchsichtig blieb. Insbesondere ist für einen Desktopanwender psychologisch heikel, etwas selbst als sicher zu erklären, was die Systementwickler als unsicher einstufen. Anstatt sich vom Levelkonzept zu verabschieden, hat Mint jetzt nochmal eine vereinfachende Richtlinie eingeschoben. Die erreichen Sie über „Aktualisierungsverwaltung -> Bearbeiten -> Aktualisierungsrichtlinie“.

Anstatt die einzelnen Levels zu bearbeiten, gibt es hier drei recht simple Ansagen wie „Meinen Rechner nicht beschädigen!“ Wird eine solche Policy gewählt, setzt das Updatetool automatisch die entsprechenden Level. Das genannte Beispiel führt wieder zu einer restriktiven Updatepolitik, die nur Level 1 bis 3 zulässt.

Diese vereinfachende „Aktualisierungsrichtlinie“ setzt aber nicht nur



Neue Aktualisierungsrichtlinie: Mint 18 hält eisern an seiner eigenwilligen Updatestrategie fest und versucht mit dem abgebildeten Dialog eine Konfigurationsvereinfachung.



Editoren für unterschiedliche Textformate: Mit „Dokumente“, „Einfacher Text“ und „Quelltext“ gibt es jetzt drei Typen, die Sie passenden Standardeditoren zuweisen können.

die dazu passenden Levels, sondern aktiviert und deaktiviert eventuell auch Optionen, die unter „Bearbeiten -> Einstellungen -> Optionen“ gesetzt waren – etwa „Kernel-Aktualisierungen immer anzeigen“. Mit anderen Worten: Das Hantieren mit den detaillierten Updateregeln wird sinnlos, wenn man eine „Aktualisierungsrichtlinie“ festlegt.

Unser Tipp für Mint-Einsteiger: Nutzen Sie die mittlere Richtlinie „Stabilität und Sicherheit optimieren“ und lassen Sie das System künftig einfach machen. Der Tipp für erfahrene Mint-Anwender kann hingegen nur so lauten:

```
sudo apt-get update
sudo apt-get dist-upgrade
```

Die Kommandozeile und apt kümmern sich nicht um die Mint-Levels und installieren alle neuen Pakete.

Kleine Neuerungen und Verbesserungen

Codecs: Linux Mint hat sich jahrelang als besonders benutzerfreundliche Distribution bewiesen, die unter anderem auch alle Multimedia-Codecs vorinstalliert mitbringt. Entgegen mancher Meldungen im Vorfeld ist das auch in Version 18 wieder der Fall. Richtig ist aber, dass die Codecs nicht mehr im ISO-Image des Live- und Installationssystems enthalten sind. Wenn man aber bei der Installation die Option aktiviert, Software von „Drittanbietern“ zu übernehmen, ist alles wieder an Bord.

Cinnamon-Menü anpassen: Das Hauptmenü hat eine neue Funktion erhalten. Nach Rechtsklick auf das Menüsymbol und „Einrichten“ gibt es die neue Option „Favoriten und Beendenoptionen anzeigen“. Die ist standardmäßig aktiv, lässt sich aber abschalten. In der Tat können die Favoriten das Menü vertikal überdimensionieren, aber das ist besser durch zurückhaltende Bestückung zu verhindern. Die Kombination, mit den Favoriten auch die Shut-down-Schalter auszublenden, halten wir für unglücklich.

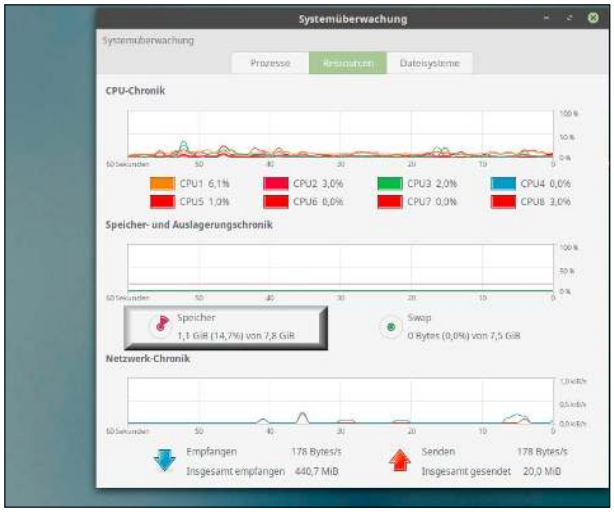
Applets in den Systemeinstellungen (cinnamon-settings): Hier gibt es eine kleine Reihe marginaler Detailverbesserungen. Die Punkte „Maus und Touchpad“, „Barrierefreiheit“ und „Klang“ bieten jeweils erweiterte Einstellungsmöglichkeiten, wobei Touchpads nun auch hardwaretechnisch besser unterstützt werden. Dass sich batteriebetriebene Geräte individuell umbenennen lassen, gehört eher zur Kategorie „nebensächlich“.

Desklet „Digitaler Bilderrahmen“ (photoframe): Der skalierbare Bilderrahmen für den Desktop berücksichtigt nun auch die Unterordner des angegebenen Quellverzeichnisses.

Dateisysteme exFAT und BTRFS: Das einfache Dateisystem exFAT stammt aus der Windows-Welt und wurde dort hauptsächlich eingeführt, um Dateigrößenlimits älterer, simpler Dateisysteme (FAT, FAT32) zu überwinden. Linux Mint 18 kann standardmäßig mit exFAT umgehen (via exfat-fuse und exfat-utils). Außerdem wurde nach zwischenzeitlicher Absenz das fortschrittliche, aber immer noch experimentelle Linux-Dateisystem BTRFS wieder als Standard integriert.

Standardprogramme: Der Dialog „Systemeinstellungen -> Bevorzugte Anwendungen“ unterscheidet jetzt bei Textdokumenten zwischen Dokument, Text und Quelltext. Dies erlaubt es, für diese unterschiedlichen Texttypen jeweils einen speziellen Editor als Standardprogramm zu definieren.

Starter in der Hauptleiste mit Zusatzoptionen: Der Firefox-Launcher bietet nach Rechtsklick zwei Startmöglichkeiten.



Cinnamon plus Firefox: Damit ist bereits mehr als ein GB RAM belegt. Für Hardwarerecycling oder für Netbooks ist Mint 18 mit Cinnamon nicht geeignet.

Starter in der Hauptleiste: Die Programmfavoriten in der Hauptleiste zeigen nach Rechtsklick bereits softwarespezifische Optionen an – so etwa der Firefox-Browser neben „Ein neues Fenster öffnen“ auch das Angebot „Ein neues privates Fenster öffnen“. Längst nicht alle Programme unterstützen diese neue Funktion, bei den meisten bleibt es beim Standardstart.

Vorinstallierter Thermald: Dieser Dienst überwacht die Temperatursensoren der Hardware und insbesondere der CPU und schützt den Prozessor vor Überhitzung. Thermald ist im Prinzip überall schnell nachinstalliert, aber bei Mint 18 jetzt bereits ab Installation Standard.

Empfehlungen zur Hardware und Installation

Linux Mint 18 mit Cinnamon (oder auch Mate) ist in der 64-Bit-Ausführung kein ausgesprochenes Leichtgewicht, hat aber noch moderate Mindestanforderungen: Eine Dualcore-CPU mit über einem GHz Taktfrequenz ist empfehlenswert sowie mindestens zwei GB RAM. Die Systemüberwachung (gnome-system-monitor) meldet nach der Benutzeranmeldung knapp 600 MB Speicherbedarf für das pure System – dies allerdings auf einem gut ausgestatteten Rechner mit acht GB RAM. Wird dort noch der Firefox gestartet, ist bereits das erste GB belegt.

Nur in der 32-Bit-Ausführung und bei geringen Anforderungen der Software kommen Sie notfalls auch noch mit einem GB Speicher aus (Netbooks). Für den standardmäßigen Cinnamon-Desktop ist ein 3D-fähiger Grafikchip von Vorteil, damit die Oberfläche flott läuft. Das pure System fordert zunächst etwa acht GB Speicher auf dem Installationsmedium, daher sind auf kleineren Datenträgern wie SSD oder USB insgesamt etwa 32 GB aufwärts zu empfehlen, um Reserven für Softwareinstallationen und Benutzerdateien zu haben.

Zwei wichtige Hinweise zu Uefi:
1. Die 64-Bit-Versionen von Linux Mint unterstützen zwar Uefi-Firmware uneingeschränkt, jedoch kein Secure Boot (bei parallelem Windows 8/10), Die Option muss gegebenenfalls im Uefi-Setup deaktiviert werden.
2. Die beiliegende Heft-DVD bootet im Bios-Modus. Somit erfolgt auch eine Installation aus dem Mint-Livesystem heraus ausschließlich im Bios-Modus. Das ist kein Problem, wenn Sie einen Rechner oder einen USB-Datenträger ausschließlich mit Mint 18 betreiben wollen. Für eine Parallelinstallation neben einem bereits existierenden Windows, das im Uefi-Modus installiert ist, ist hingegen unbedingt eine Installation von Mint 18 ebenfalls im Uefi-Modus zu empfehlen. Dies erreichen Sie nur, indem Sie das ISO-Image von Mint (unter „Image-Dateien“ auf Heft-DVD) auf eine eigene DVD oder einen USB-Stick kopieren. Einschlägige Hilfsmittel sind dd unter Linux oder der Win 32 Diskimager unter Windows (auf Heft-DVD).

Das Upgrade von 17.3: Bei Redaktionsschluss gab es noch keine Upgrademöglichkeit von der Vorgängerversion 17.3 auf Version 18. Vermutlich wird noch im Laufe des Monats Juli über die Aktualisierungsverwaltung ein Upgradepfad eröffnet. Nach einem kleinen Update wird dann die Aktualisierungsverwaltung im Menü „Bearbeiten“ eine zusätzliche Option anzeigen, die das Onlineupgrade auf Version 18 auslösen kann.

Linux Mint 18: Nicht mehr als ein solides Upgrade

Zurück zur Eingangsfrage: Kann die neue Version ihre Anhänger halten? Höchstwahrscheinlich ja. Mint 18 stellt sich wieder auf einen aktuellen Unterbau von Ubuntu 16.04 LTS mit Kernel 4.4. und relativ frischer Software wie Firefox 47 oder Libre Office 5.1.2. Die Bedienung ist wie gehabt und fordert keinerlei Umgewöhnung. Die Cinnamon-Oberfläche kann trotz Hauptversionsnummer „3“ nicht viel mehr als früher, ist aber optisch signifikant aufgefrischt. Alle Modernisierung bleibt aber ein offenes Angebot: Konservative Mint-Nutzer schalten in den Systemeinstellungen mit wenigen Klicks die neuen Fenstereffekte ab und kehren optisch zu den Standards älterer Versionen zurück. Mint mit Cinnamon hält damit weiter einen Haupttrumpf gegenüber Ubuntus Unity in der Hand: seine enorme Anpassungs- und Wandlungsfähigkeit. ●

Logs lügen nicht

Läuft auf dem Linux-System wirklich alles wie gewünscht? Die Logs von System- und Serverdiensten geben darüber Auskunft. Aber wo steht was? Es gibt zahlreiche Hilfen, die wertvolle Infos aus den Datenmengen sieben.

Von **David Wolski**

Quelle: JoJan, Titel: „Grand Turk". Lizenz: GNU Public License (Lizenztext auf Heft-DVD).

Ein regelmäßiger Blick in die Logdateien ist bei der Fehlersuche auf Desktopsystemen nützlich, bei Servern eine Pflichtübung, selbst wenn alles in bester Ordnung scheint. Linux-Systeme sind ja durchaus gesprächig: Der Kernel hat ein Logbuch, Mailserver und Webserver sowieso. Aber wo steht was? Der Rsyslog-Dämon legt alle Logdateien unterhalb des Ordners „/var/log an" und die meisten Dateien liegen im Textformat vor, die sich mit root-Privilegien über einem Betrachter wie less öffnen und mit grep durchsuchen lassen.

Ein Sonderfall ist Fedora, das die Protokollierung von Systemereignissen aller Art dem neuen Init-Dämon Systemd überlässt und sich vom klassischen Logformat verabschiedet hat. (siehe Kasten „Journald: Das neue Logging von Systemd"). Aber jede Linux-Distribution bietet Werkzeuge, die Datenberge der Logdateien zu meistern und über ungewöhnliche Ereignisse zu informieren.

Mit Logrotate die Datenflut eindämmen

Bevor es um die Inhalte der Logdateien geht, sollten diese in handliche Portionen aufgeteilt werden. Ein Webserver, der über Monate läuft, produziert auf öffentlichen Servern schnell Hunderte MB an Logdaten. Der Dienst „Logrotate", der über das Paket „logrotate" zu installieren ist (in den meisten Distributionen Standard), kümmert sich um den Wildwuchs. Hat eine Logdatei ein bestimmtes Alter erreicht, dann wird sie von Logrotate umbenannt, meist noch komprimiert und mit einer Zahl am Dateiende versehen. Die neuen Meldungen kommen in eine neue Logdatei. Als Archiv hält Logrotate eine bestimmte Anzahl alter Logdateien mit fortlaufenden Nummern vor. Bei jeder Rotation, die üblicherweise täglich erfolgt, wird die älteste Datei überschrieben. Das spart Speicherplatz und sorgt für kleinere, chronologisch sortierte Dateien.

Überblick: Grundlegende Werkzeuge

Einsteiger auf der Suche nach Infos machen sich am besten mit dem Dateimanager Midnight Commander (Paket „mc") mit den Logdateien vertraut:

```
sudo mc /var/log
```

Die Taste F3 öffnet eine Logdatei im Textbetrachter.

Einträge in Logdateien werden stets mit Zeitstempel ans Ende der Datei geschrieben. Die neuen Infos sind also immer an Ende der Datei zu finden. Ein wichtiges Werkzeug in der Shell ist daher der Befehl tail, der die zehn letzten Einträge einer Logdatei ausgibt. Genügt das nicht, so kann das Kommando

```
sudo tail -n 20 [Logdatei]
```

auch zwanzig Zeilen ausgeben. Um den laufenden Betrieb zu überwachen, hilft die Kombination mit watch, das einen Befehl in einem Intervall von zwei Sekunden ausführt und mit

```
sudo watch tail [Logdatei]
```

fortlaufende Änderungen einer Logdatei anzeigt. Geht es um die Fehlersuche speziell bei Webservern mit Access- und Errorlog, so gibt es mit multitail ein Tool für Fortgeschrittene:

```
sudo multitail [Logdatei1] [Log
  datei2]
```

Multitail zeigt und aktualisiert gleichzeitig mehrere Logdateien.

Der Spezialist Log File Navigator

Die genauesten Informationen nützen nichts, wenn sie im Rauschen der Masse untergehen. Bei einem Blick in umfangreiche Logdateien mit einem universellen Textbetrachter wie less oder mcview passiert das aber schnell. Für eine Recherche in Logs ist das Kommandozeilenprogramm Log File Navigator besser geeignet. Es ist mit

```
sudo apt-get install lnav
```

in Debian/Ubuntu schnell nachinstalliert. Der Aufruf *sudo lnav* ohne Parameter öffnet das allgemeine Syslog mit den Meldungen aller Sysloginstanzen. Die Einträge macht der Log File Navigator durch Farben übersichtlicher. Der folgende Befehl

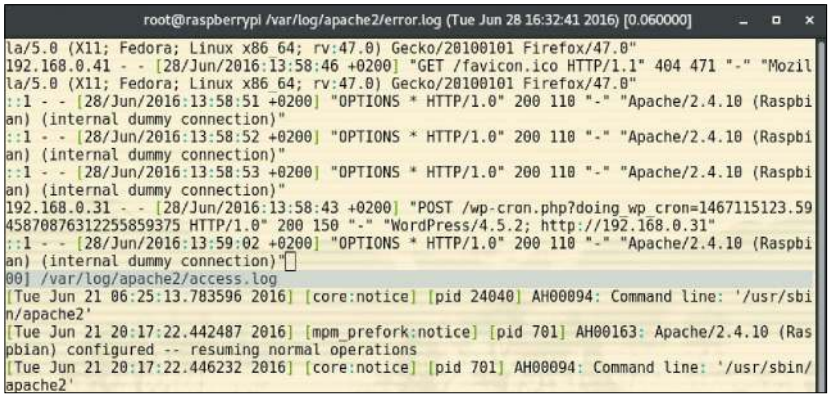
```
sudo lnav [Logdatei]
```

öffnet eine bestimmte Logdatei und die Pfeiltasten oder das Mausrad scrollen durch die Zeilen. Entscheidend ist aber die syntaktische Kenntnis des Programms zum Format der verbreiteten Logdateien und damit die Unterscheidung von Hinweisen, Warnungen und Fehlern. So springt die Taste E (und Umschalt-E) zwischen Fehlermeldungen vor und zurück. Taste W (Umschalt-W) interessiert sich nur für Warnungen. Taste I wechselt zwischen der Listenansicht und einer Übersicht, wann und wo Fehler aufgetreten sind.

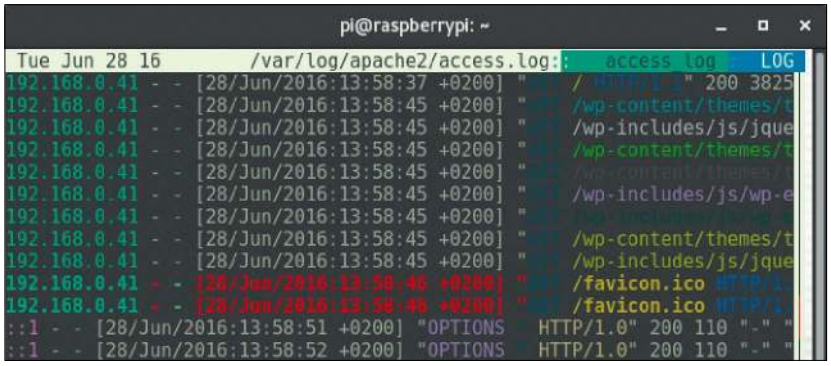
Mit Logwatch Infos frei Haus

Für gezielte Fehlersuche ist die manuelle Auswertung von Logdateien hilfreich. Um aber ein System längere Zeit zu überwachen, gibt es das Programm Logwatch, das sich als täglicher Cronjob installiert. Es erstellt einen jederzeit abrufbaren Bericht als Zusammenfassung. Auf Servern mit einem Mailserver wie Postfix/Sendmail/Exim2 kann es den Bericht auch per Mail senden. Soll ein Benutzer wie root auf dem System die Zusammenfassung im lokalen Postfach erhalten, so genügt auch ein lokaler Mailserver ohne Verbindung nach außen zu einem SMTP-Server im Internet.

Debian, Raspbian, Ubuntu, Fedora, Open Suse und Arch bieten das Paket „logwatch“ in ihren Paketquellen. In



Mehrere Logs im Blick: multitail zeigt und aktualisiert Logdateien in einem Terminalfenster. Ideal ist das Tool zur Fehlersuche auf Webservern mit diversen Logs.



Nicht nur bunt, sondern auch informativ: Der Log File Navigator versteht die Syntax der meisten Logdateien, bietet Filter und springt bei Bedarf zu Warnungen und Fehlern.

seinen Standardeinstellungen trägt sich Logwatch unter „/etc/cron.daily ein. Der Befehl

```
sudo logwatch
```

präsentiert im Terminal eine Übersicht zu ungewöhnlichen Ereignissen. Möchte man die per Mail erhalten, ist die Konfigurationsdatei „/usr/share/logwatch/default.conf/logwatch.conf“ anzupassen.

Öffnen Sie die Datei mit sudo in einem Texteditor, gehen Sie zur Zeile „MailTo = root“ und tragen Sie statt root die gewünschte Mailadresse ein oder bei einem lokalen Mailserver den Benutzernamen des Administrators.

Journald: Das neue Logging von Systemd

Mit dem Wechsel zu Systemd als Init-System schlagen Distributionen wie Fedora ein neues Kapitel im Logbuch auf. Um die Protokollierung kümmert sich jetzt nicht mehr das klassische Syslog/Rsyslog, sondern Systemd selbst beziehungsweise dessen Modul Journald als zentrale Loginstanz.

Leider verabschiedet sich Journald vom allgemein gebräuchlichen Textformat für Logs. Diese werden bei Systemd, ähnlich einer Datenbank, in einem binären Format unter „/var/log/journal“ gespeichert. Zur Betrachtung genügt folglich ein Texteditor nicht mehr. Stattdessen ist ein Spezialtool wie journalctl nötig, das mit

```
sudo journalctl -xb
```

beispielsweise das gesamte Syslog anzeigt, aber auch Filterfunktionen bietet. Genau das ist auch bei der Diskussion während der Umstellung von Debian und Ubuntu zu Systemd einer der Hauptkritikpunkte der Systemd-Gegner gewesen. Unter Debian, Raspbian, Ubuntu ist deshalb weiterhin Rsyslog aktiv, obwohl alle zu Systemd umgestiegen sind.

Was Linux so sicher macht

Linux gilt als sicheres Betriebssystem – sicherer als Windows. Stimmt das wirklich? Und wenn ja: Was sind die Gründe? Dieser Startbeitrag zum großen Sicherheitsspecial fasst die wichtigsten Aspekte zusammen.

Von **Hermann Apfelböck**

Jeden Tag werden Horden neuer digitaler Schädlinge bekannt. Linux-Anwender dürfen das weitestgehend ignorieren: Gelegentlich ist das ebenfalls unixoide Mac-OS betroffen, aber in der Regel zielen Viren und Trojaner auf Windows. Dabei handelt es sich doch bei allen drei Systemen um Multiuser-Umgebungen mit sauberer Rechteverwaltung, die für das Laden und Installieren (oder „Einnisten“) von neuer Software Administrator-/root-Rechte voraussetzen. Die technischen Unterschiede, wenngleich vorhanden, sind folglich nur ein Aspekt. Die Sicherheitsvorteile von Linux haben noch andere Gründe.

Vielfalt und Kompetenz einer Minderheit

Schlüpft man gedanklich in die Rolle eines Virenprogrammierers, dann wird sehr deutlich, warum Windows das lohnendere Ziel ist:

- Auf dem PC/Notebook-Desktop kommt Linux seit Jahren nicht über einen Marktanteil von maximal zwei Prozent hinaus. Windows liegt bei knapp 90 Prozent.
- Linux erschwert Programmierern von Schadsoftware die Arbeit durch zusätzliche Vielfalt und Heterogenität. Das Minderheitensystem spaltet sich weiter auf in diverse Distributionen, die sich technisch deutlicher unterscheiden als etwa ein altes Windows XP vom aktuellen Windows 10. Eine Schadsoftware, die Ubuntu befallen kann, funktioniert wahrscheinlich nicht unter Arch, Fedora oder Open Suse. Das Windows-Biotop ist hingegen so homogen, dass ein für Windows 98 geschriebener Virus theoretisch auch noch unter Windows 10 lauffähig ist. Lediglich uralte 16-Bit-Software funktioniert definitiv nicht mehr.
- Der Benutzer, der vor einem Linux-Desktop sitzt, ist meistens technisch kompetenter als der typische Windows-Nutzer. Plumpe Aufforderungen, mal schnell das sudo-Kennwort abzunicken, haben weniger Aussicht auf Erfolg als beim Windows-User ein unbedachtes „Ja“ bei der Abfrage der Benutzerkontensteuerung.

Unterm Strich erreicht ein Linux-Virenprogrammierer für seine „harte Arbeit“ viel weniger Masse, hat deutlich höhere technische Hürden und muss auch noch mit misstrauisch-kompetenten Systembenutzern rechnen. Die Chance, auf dem Zielsystem überhaupt anzukommen, ist – aus seiner Sicht – frustrierend gering.

Sichere Installationsquellen – einfaches Update

Standardmäßig bezieht der Linux-Anwender zusätzliche Software ausschließlich aus den sicheren Paketquellen seiner Linux-Distribution. Das ist mitunter einschränkend, weil die Distributionen oft mit der Aktualisierung der Paketquellen hinterherhinken und daher nicht die allerneuesten Versionen anbieten. Aber es ist sicher, weil dort nur seriöse und geprüfte Programme vorliegen. Ein weiterer entscheidender Vorteil der Paketquellen ist das einfache Systemupdate inklusive aller installierten Programme, das sich mit einer Kommandozeile (*apt-get dist-upgrade* auf Debian-Systemen) oder sogar vollautomatisch erledigen lässt (Ubuntu).

Das Konzept der verbindlichen Paketquellen wird in Debian/Ubuntu-basierten Systemen durch Launchpad-PPAs (Personal Package Archives) punktuell unterwandert, da es sich

dabei streng genommen um Fremdquellen handelt. Das Bereitstellen von Software über PPAs folgt aber sauberen Regeln inklusive Signatur, die einen Missbrauch praktisch ausschließen. Die Qualität solcher PPA-Pakete mag unterschiedlich sein, aber aggressive Schadsoftware ist dort nicht zu befürchten.

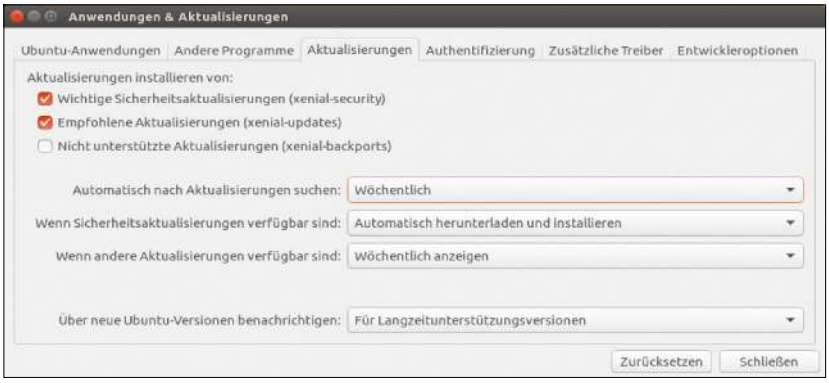
Linux-Nutzer, die noch einen Schritt weiter gehen und Quellcode zu ausführbarem Binärcode kompilieren, müssen natürlich wissen, was sie tun und woher der Code stammt. Dies ist aber praktisch immer der Fall, weil die Suche des Quellcodes und das Kompilieren ein zielgerichtetes und bewusstes Handeln darstellt.

Darüber hinaus ist es unter Linux ausgeschlossen, dass ein bösartiges Script aus dem Internet versehentlich gestartet wird. Der Download ist nicht ausführbar, bis der Benutzer der Datei mit root-Recht explizit das Executable-Bit einräumt, sei es auf Kommandozeile oder im grafischen Dateimanager.

Windows? Als fatale Kehrseite dieser sehr offenen Softwareplattform darf hier jede EXE-Datei aus den dunkelsten Internetecken gestartet werden. Wenn sich das Programm mit dem Userkontext zufriedengibt, erfolgt nicht einmal eine Abfrage der Benutzerkontensteuerung. Flankierende Schutzmaßnahmen, die schon vorab beim Download warnen („Smartscreen"), sind Flickschusterei und können nicht darüber hinwegtäuschen, dass letztlich der vorsichtige User entscheiden muss, ob er den Virus haben will oder nicht.

Open Source versus proprietäre Software

Der Quellcode von Windows und der kommerzieller Programme ist Verschlusssache. Daher ist auch die Beseitigung von Sicherheitslücken Sache der Hersteller. Viele Unternehmen fahren hier die Strategie „Security through Obscurity." Sie hoffen darauf, dass Schwachstellen schwerer zu finden sind, wenn niemand die genauen Funktionen der Software kennt. Das ist aber ein Trugschluss, wie die Sicherheitslücken in proprietärer Software immer wieder zeigen. Angreifer finden die Schwachstellen auch ohne Einblick in den Quellcode.



Sicherheit leicht gemacht: Das Linux-Paketmanagement erlaubt die Aktualisierung sämtlicher System- und Softwarekomponenten – bei Ubuntu auch vollautomatisch.

Standardmäßig nicht ausführbar: Heruntergeladenen Scripts fehlt das Recht, als Programm zu starten. Das Executable-Bit muss erst bewusst gesetzt werden.

Der Linux-Kern und die meisten Linux-Programme sind Open Source: Der Quellcode kann also von jedem eingesehen und geprüft werden. Sicherheitslücken gibt es überall, aber die Wahrscheinlichkeit, Fehler im Open-Source-Code frühzeitig zu entdecken, ist höher als bei kommerzieller Software.

Sicherheit und Nutzerpflichten

Jeder Linux-Anwender genießt ein Plus an Sicherheit gegenüber Windows-Usern – und dies ganz ohne Antivirensoftware und Softwarefirewall. Das heißt aber nicht, dass das Ziel „Sicherheit" mit der Linux-Installation erledigt wäre: Bei physischem Zugriff auf ein verlorenes Notebook sind die Daten unter einem gebooteten Fremdsystem genau so offen wie bei Windows. Selbst der Zugang mit dem regulären Benutzerkonto ist hier nach vorheriger Bearbeitung der Datei „/etc/shadow „möglich – und dies ist sogar einfacher als bei Windows. Dagegen hilft wie bei Windows nur das Verschlüsseln der Benutzerdaten, wobei Linux mehr Optionen anbietet als Windows mit Bitlocker. Ähnliches gilt für Mails oder Onlinekennwörter, über deren Sicherheit nicht Linux oder Windows entscheiden, sondern Software wie das Mailprogramm oder der Browser. Auch hier ist Verschlüsselung die richtige Antwort. Auch auf Linux-Servern sind es Softwarekomponenten, die durch Sicherheitslücken oder schlampige Konfiguration Scheusen öffnen. Apache, SSH, Portfreigaben lassen sich widerstandsfähiger absichern, als dies der Standard vorsieht. Gegen singuläre Programmfehler wie den fatalen Heartbleed-Bug in Open SSL ist letztlich kein Kraut gewachsen bis zur Erkennung und Korrektur durch ein Update. Auch in Content-Management-Systemen wie Wordpress gibt es immer wieder Sicherheitslücken im Coresystem und bei den Plug-ins, die nur durch konsequente Updatepflege zu beantworten sind.

Mit dem Basissystem Linux selbst haben solche Serverlücken genau genommen nicht viel zu tun. Die nachfolgende Artikelsammlung wird sich aber mit allen Sicherheitsaspekten befassen – vom Datenschutz lokaler Daten über sichere Heimnetz- und Webkommunikation bis hin zu abgehärteten Home- und Webservern. ●

Maßnahmen zum Systemschutz

Backups müssen weder lästig noch langweilig sein, insofern sie einfach unbemerkt geschehen. Mit den richtigen Tools richten Sie die Datensicherung nur einmal ein und überlassen den Rest dem System.

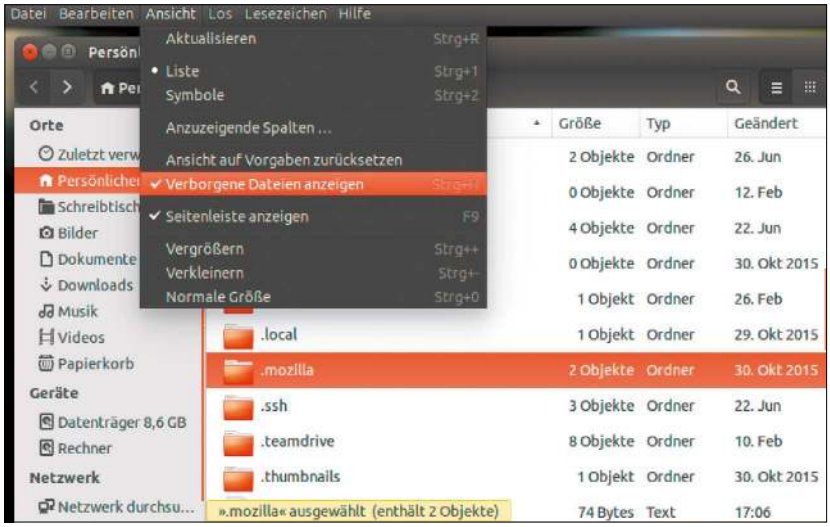
Von **Thorsten Eggeling**

Eine fehlerhafte Konfiguration, etwa nach einem Upgrade der Distribution, kann den Linux-Start verhindern. Und auch mit Festplattendefekten müssen Sie jederzeit rechnen. Damit sich im Notfall das System oder wenigstens wichtige Dateien schnell wiederherstellen lassen, sollten Sie regelmäßig Sicherungskopien erstellen.

Sinnvolle Backupstrategien

Sie haben die Wahl zwischen einem kompletten Backup des Systems, einem Backup der persönlichen Daten oder einer Kombination aus beidem. Was Sie sichern sollten, hängt von der Art ab, wie Sie Linux nutzen. Stehen Textverarbeitung, Webbrowser und E-Mail im Vordergrund, ist vor allem die regelmäßige Sicherung der persönlichen Dateien im Home-Verzeichnis wichtig. Dient der PC als Webserver oder Datenspeicher für andere PCs im Netzwerk, müssen Sie weitere Verzeichnisse sichern. Wichtig ist dann beispielsweise der Ordner „/etc“, in dem die Linux-Konfigurationsdateien und die des Webservers liegen.

Ein Backup sollte nicht nur die Dateien unter „~/Dokumente“ erfassen. Wichtige Konfigurationsdateien von Anwendungen und Desktop liegen unter „/home“ in versteckten Dateien oder Ordnern, die mit einem Punkt beginnen. Dateimanager wie Nautilus zeigen diese erst, wenn Sie im Menü „Ansicht“ ein Häkchen vor „Verborgene Dateien anzeigen“ setzen. So speichert etwa Firefox im Verzeichnis „.mozilla“ die Profildateien eines Benutzers. Wenn Sie den Browser Lesezeichen, Kennwörter und Formulardaten speichern lassen, ist ein regelmäßiges Backup des Profilordners empfehlenswert. Das können Sie zwischendurch auch manuell erledigen, indem Sie „.mozilla“ einfach in einen Backupordner kopieren.



Versteckte Ordner: Dateimanager zeigen Konfigurationsverzeichnisse standardmäßig nicht an. Für manuelle Backups blenden Sie diese über „Ansicht“ oder mit Hotkey Strg-H ein.

Ein komplettes Systembackup ist anzuraten, wenn viele zusätzliche Programme installiert sind oder das System aufwendig konfiguriert ist. Ansonsten ist eine Neuinstallation und nachfolgende Wiederherstellung der eigenen Dateien oft schneller als ein Restore des ganzen Systems.

Inkrementelles Backup mit Timeshift

Für regelmäßige Backups empfehlen wird Timeshift. Das Tool erstellt Momentaufnahmen des Dateisystems, die beim Zurückspielen einen vorherigen Zustand wiederherstellen. Der erste Sicherungspunkt ist immer ein komplettes Backup der Systemverzeichnisse und mit einigen Gigabyte recht groß. Die weiteren Wiederherstellungspunkte sind dann aber deutlich kleiner, da Timeshift nur noch die Unterschiede zum vorherigen Sicherungspunkt speichert. Zur Installation unter Ubuntu verwenden Sie die folgenden Terminalbefehle:

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

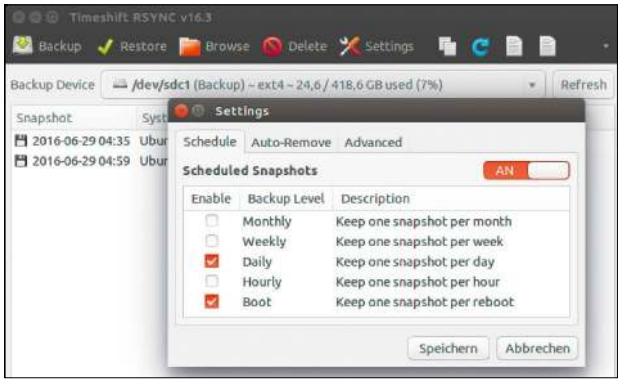
```
sudo apt-get install timeshift
```

Informationen zur Installation bei anderen Linux-Systemen finden Sie auf der Webseite des Entwicklers *(www.teejeetech.in/p/timeshift.html)*.

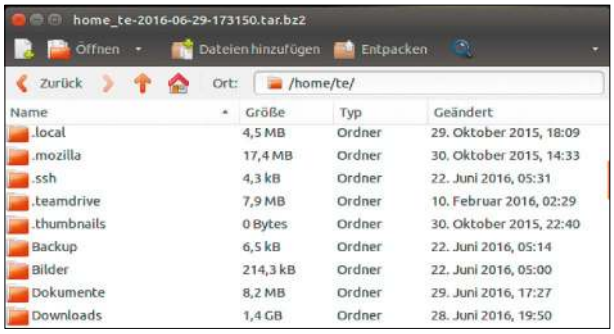
Starten Sie das Tool mit *sudo time shift*. Hinter „Backup-Device“ wählen Sie die Festplatte aus, auf der Sie sichern wollen. Voraussetzung ist, dass ein externes Laufwerk mit einem Linux-Dateisystem wie Ext3, Ext4, XFS oder BTRFS formatiert ist. Die Home-Verzeichnisse sind standardmäßig ausgeschlossen, lassen sich aber über „Settings -> Advanced -> Include“ hinzufügen. Klicken Sie auf „Backup“, um die Sicherung zu starten.

Nach dem ersten Backup legen Sie über „Settings -> Schedule“ einen Zeitplan fest. Die regelmäßigen Sicherungen werden dann automatisch per Cronjob durchgeführt.

Wiederherstellung: Die Backupsätze von Timeshift bestehen einfach aus Ordnern und Dateien. Im Notfall lässt sich ein früherer Zustand daher mit jedem Livesystem rekonstruieren, selbst wenn Timeshift dort nicht verfügbar ist. In der Liste der Momentaufnahmen zeigt Timeshift alle Punkte auf dem Backuplaufwerk nach Alter geordnet an, mit den jüngsten Wiederherstellungspunkten am Ende der Liste. Über „Browse“ öffnen Sie den Standarddateimanager des Linux-Systems, um die Verzeichnisstruktur manuell nach Dateien zu durchforsten. Für die komplette Wiederherstellung schließen Sie zuerst alle anderen noch geöffneten Anwendungen. Wählen Sie den gewünschten Punkt in der Liste der Momentaufnahmen aus und klicken Sie auf „Restore“. Bevor die Wiederherstellung beginnt, zeigt Timeshift eine Zusammenfassung der Aktionen mit Backuplaufwerk und Ziellaufwerk an.



Automatische Sicherung: In Timeshift stellen Sie ein, wann und wie oft das Tool Backups erstellen soll. Kurze Intervalle sind möglich, weil die Sicherungen nur wenig Platz benötigen.



Wiederherstellung: Ein Tar-Archiv lässt sich im Archivmanager öffnen. Sie können einzelne Dateien oder Ordner extrahieren oder das komplette Archiv entpacken.

Backup mit Tar: Einfach und zuverlässig

Sicherungskopien legen Sie am besten auf einer zweiten Festplatte ab, die auch über USB angeschlossen sein kann. Für die schnelle Sicherung zwischendurch eignet sich das Tool tar:

```
tar -cvjpf /media/[User]/[USB-
  Laufwerk]/home_[User].tar.bz2 /
  home/[User]
```

Damit sichern Sie den Inhalt von „/home/[User]“ in das Verzeichnis „/media/[User]/[USB-Laufwerk]“. Dabei entsteht eine Datei mit der Endung „tar.bz2“, die platzsparend mit Bzip komprimiert ist. Für die Wiederherstellung entpacken Sie die Archivdatei im Dateimanager über den Kontextmenüeintrag „Hier entpacken“ in einen beliebigen Ordner. Sie können dann einzelne Dateien oder Verzeichnisse in Ihr Home-Verzeichnis zurückkopieren. Um das komplette Home-Verzeichnis zu rekonstruieren, wechseln Sie auf der Kommandoziele mit

```
cd \
```

in das Root-Verzeichnis und nutzen dann folgenden Befehl:

```
tar -xvjf /media/[User]/[USB-Lauf
  werk]/home_[User].tar.bz2
```

Bereits vorhanden Dateien werden überschrieben. Verwenden Sie diese Methode daher nur, wenn sich im Zielverzeichnis keine neueren Dateien befinden.Tar eignet sich auch für automatisierte Scripts. Die folgenden vier Zeilen sichern das Home-Verzeichnis. Der Dateiname wird zusätzlich mit Datums- und Zeitangabe versehen. Außerdem speichert das Script die Backupzeit in einer Logdatei.

```
#!/bin/bash
DATE=$(date +%Y-%m-%d-%H%M%S)
tar -cjpf /media/$USER/[USB-Lauf
  werk]/home_$USER-$DATE.tar.bz2
  $HOME
echo $DATE Backup ausgeführt >>
  $HOME/backup.log
```

Erstellen Sie das Script in einem Texteditor und speichern Sie es in Ihrem Home-Verzeichnis etwa als „backup.sh“. Machen Sie es danach ausführbar:

```
chmod 755 backup.sh
```

Passen Sie die Pfadangabe für das Backup-Verzeichnis entsprechend Ihrer Konfiguration an. Damit das Script automatisch startet, rufen Sie im Terminalfenster *crontab -e* auf. Tippen Sie folgende Zeile ein

```
0 16 * * * nice -n 19 ionice -c2
  -n7 $HOME/backup.sh >/dev/null
  2>&1
```

und speichern Sie die Änderung. Damit startet das Script jeden Tag um 16:00 Uhr. Wenn Sie statt „0 16“ den Wert „53 2“ eingeben, wird das Script um 2:53 Uhr ausgeführt. ●

Rechtevergabe im Dateisystem

Linux ist als Mehrbenutzersystem konzipiert. Die Rechte im Dateisystem spielen daher eine große Rolle – als Schutz vor den neugierigen Blicken anderer Benutzer und wichtiger noch vor Schadsoftware.

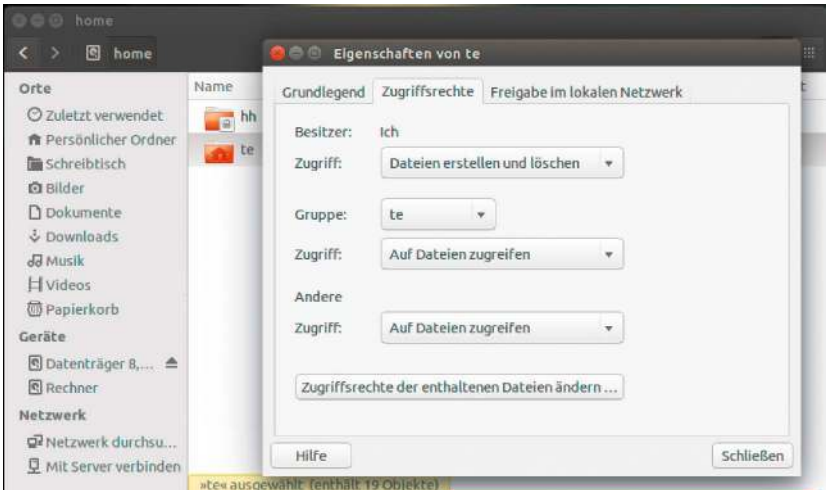
Von **Thorsten Eggeling**

Die Rechtevergabe im Dateisystem ist ein wichtiger Bestandteil des Linux-Sicherheitskonzepts. Linux-Nutzer, aber auch Dienste wie Web- oder FTP-Server sollen nur in den wirklich nötigen Bereichen Dateien erstellen oder ändern dürfen. Damit die Sicherheit erhalten bleibt, sollten Sie die grundlegenden Prinzipien des Berechtigungssystems kennen.

Eigentümer, Gruppen und Rechte

Das Rechtesystem von Linux ist relativ einfach und überschaubar. Eine Datei oder ein Ordner kann nur einem einzigen Benutzer („Eigentümer“) und nur einer Gruppe gehören. Für beide lässt sich das Lese- und Schreibrecht getrennt festlegen. 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 und den Inhalt anzusehen. Außerdem lassen sich Rechte für „andere“ festlegen. Damit sind Zugriffe gemeint, die weder vom Eigentümer noch von der Gruppe aus erfolgen. Es lassen sich daher insgesamt neun Zugriffsrechte vergeben: „Lesen“, „Schreiben“ und „Ausführen/Durchsuchen“ jeweils für den Eigentümer, die Gruppe und für andere Benutzer.

Die Rechte für Ordner wirken sich indirekt auch auf die darunter liegenden Ordner aus. Wenn Sie „Ausführen/Durchsuchen“ verbieten, gilt das auch für die darunter liegenden Ordner. Es



Zugriffsrechte: Über einen Dateimanager wie Nautilus ermitteln Sie, welche Rechte bei Dateien und Ordnern gesetzt sind. Sie können die Berechtigungen hier auch ändern.

gibt eine Besonderheit: Ist „Ausführen/Durchsuchen“ bei einem Ordner erlaubt, aber „Lesen“ nicht, kann ein anderer Benutzer eine darin liegende Datei öffnen, wenn ihm der Pfad beziehungsweise Dateiname bekannt ist.

Für sehr spezielle Einsatzbereiche lassen sich noch drei zusätzliche Sonderrechte festlegen. Das Set-UID-Recht und Set-GID-Recht bewirken, dass eine ausführbare Datei immer mit den Rechten des Besitzers beziehungsweise der Gruppe läuft, egal wer sie startet. Das kommt beispielsweise beim Programm sudo zum Einsatz. Der Eigentümer ist der administrative Benutzer „root“, mit dessen Rechten es startet, auch wenn ein nicht-privilegierter Benutzer es aufruft. Es liegt dann beim Programm zu prüfen, ob der Benutzer das Recht dazu hat. sudo verwendet dafür die Datei „/etc/sudoers“, in der etwa bei Ubuntu-Systemen die Rechte dem Benutzer „root“ und den Gruppen „admin“ sowie „sudo“ eingeräumt werden. Grundsätzlich sollten Sie beide Rechte nicht selbst ändern, vor allem bei Dateien, die „root“ gehören. Es sei denn, Sie wissen genau, dass das Programm die Prüfung für eine erhöhte Berechtigung ordnungsgemäß durchführt.

Das dritte Sonderrecht heißt „Stick-Bit“. Es wird beispielsweise für den Ordner „/tmp“ verwendet. Ist es bei einem Ordner gesetzt, kann nur der Besitzer die darin enthaltenen Elemente ändern oder löschen.

Benutzerrechte über den Dateimanager setzen

Welche Rechte für Ordner und Dateien gelten, lässt sich über einen Dateimanager wie Nautilus ermitteln. Wählen Sie eine Datei oder einen Ordner mit

der rechten Maustaste aus, gehen Sie im Menü auf „Eigenschaften“ und dann auf die Registerkarte „Zugriffsrechte“. Hinter „Zugriff“ können Sie die Rechte für „Besitzer“, „Gruppe“ und „Andere“ festlegen, außerdem lässt sich die Gruppe ändern. Standardmäßig sind Gruppe und Benutzer im Home-Verzeichnis identisch.

Per Klick auf die Schaltfläche „Zugriffsrechte der enthaltenen Dateien ändern“ lassen sich bei Ordnern die Rechte rekursiv für alle enthaltenen Elemente setzen. Anders als die Beschriftung vermuten lässt, gelten die Änderungen auch für den Ordner, für den Sie „Eigenschaften“ aufgerufen haben. Sie werden bemerken, dass bei Ubuntu die Rechte für „Andere“ mit „Auf Dateien zugreifen“ eingestellt ist. Andere Benutzer können daher den Inhalt fremder Home-Verzeichnisse einsehen und Dateien darin öffnen, aber nicht ändern. Wenn Sie das nicht möchten, setzen Sie für Ihr Benutzerverzeichnis unter „/home“ die Rechte für „Andere“ hinter „Zugriff“ auf „Keiner“. Das gilt dann auch für alle Unterverzeichnisse.

Zugang verweigern: Unter Ubuntu können Benutzer auf den Inhalt anderer Home-Verzeichnisse zugreifen. Um das zu verhindern, entziehen Sie anderen Benutzern die Zugriffsrechte.

```
te@teub14043: ~
te@teub14043:~$ stat -c '%A %a %U %G %n' /var/www/wordpress/*
-rw-r--r-- 644 www-data www-data /var/www/wordpress/index.php
-rw-r--r-- 644 www-data www-data /var/www/wordpress/license.txt
-rw-r--r-- 644 www-data www-data /var/www/wordpress/liesmich.html
-rw-r--r-- 644 www-data www-data /var/www/wordpress/readme.html
-rw-r--r-- 644 www-data www-data /var/www/wordpress/wp-activate.php
drwxr-xr-x 755 www-data www-data /var/www/wordpress/wp-admin
-rw-r--r-- 644 www-data www-data /var/www/wordpress/wp-blog-header.php
-rw-r--r-- 644 www-data www-data /var/www/wordpress/wp-comments-post.php
```

Rechte ermitteln: Mit dem Tool stat lassen Sie sich anzeigen, welche Zugriffsrechte in einem Ordner oder für eine Datei vergeben sind. stat gibt auch die oktalen Werte aus.

Tools für die Kommandozeile verwenden

Als Administrator eines Linux-Systems werden Sie für die Rechtevergabe das Terminal bevorzugen. Mit chown ändern Sie den Besitzer von Dateisystemobjekten:

```
chown -R www-data:www-data /var/
  www/wordpress
```

Der Parameter „-R“ steht für rekursiv. Damit wirkt sich der Befehl auf alle enthaltenen Ordner und Dateien aus. Dahinter stehen der neue Besitzer und die Gruppe für den angegebenen Ordner. Die Befehlszeile aus dem Beispiel verwenden Sie, wenn Sie einen Webserver betreiben und das Blogsystem Wordpress nach „/var/www/wordpress“ kopiert haben.

Der Apache-Server läuft unter Ubuntu und Debian mit der Benutzerkennung „www-data“, der zur gleichnamigen Gruppe gehört. Indem Sie den Besitz aller Ordner und Dateien an „www-data“ übertragen, haben Apache und damit auch Wordpress das Recht, hier Konfigurationsdateien zu erzeugen und Dateien zu erstellen. Das ist für die Erstkonfiguration und auch für Dateiuploads nötig.

Sensible Dateien sollten Sie danach schützen, indem Sie Rechte wieder entziehen. Die Wordpress-Konfigurationsdatei „wp-config.php“ sollten mögliche Angreifer nicht manipulieren dürfen. Dem Server genügt der Lesezugriff, wenn Wordpress eingerichtet ist:

```
chmod a-w /var/www/wordpress/wp-
  config.php
chmod go-r /var/www/wordpress/wp-
  config.php
```

Parameter „a“ bezieht sich auf „Alle“, also auf den Besitzer, die Gruppe und andere Benutzer. „-w“ entzieht das Schreibrecht. In der zweiten Zeile entfernen Sie das Recht „Lesen“ für die Gruppe und andere Benutzer. Es bleibt nur das Leserecht für den Eigentümer übrig. Die möglichen Angaben bei chmod sind „u“ für den Eigentümer, „g“ für die Gruppe und „o“ für andere. Diese kombinieren Sie mit den Rechten „r“ (Lesen), „w“ (Schreiben) und „x“ (Ausführen/Durchsuchen). Ein „-“ entfernt das Recht, „+“ fügt es hinzu und „=“ setzt die Rechte neu. Damit Sie nicht zwei Befehlszeilen verwenden müssen, empfiehlt sich die oktale Schreibweise:

```
chmod 400 /var/www/wordpress/wp-
  config.php
```

Der Wert „4“ steht für „Lesen“ und „0“ für keine Rechte. Die erste Stelle bezieht sich auf den Eigentümer, die zweite auf die Gruppe und die dritte auf andere Benutzer. Verwenden Sie den Wert „600“, um dem Eigentümer wieder Schreibrechte zu gewähren. Eine Übersicht mit der Bedeutung der numerischen Werte finden Sie über *www.pcwelt.de/8P42PF*.

In einem Terminalfenster können Sie prüfen, welche Rechte für Dateien und Ordner gelten. Die gesetzten Rechte in einem Ordner prüfen Sie mit

```
ls -al /var/www/wordpress
```

ls zeigt die Rechte in der ersten Spalte mit „r“, „w“ und „x“ (Lesen, Schreiben, Ausführen) in der Reihenfolge Eigentümer, Gruppe und andere an. Um sich die Rechte zusätzlich in oktaler Schreibweise anzeigen zu lassen, verwenden Sie diese Befehlszeile:

```
stat -c '%A %a %U %G %n' /var/www/
  wordpress/*
```

Informationen zu einer einzelnen Datei lassen Sie sich mit *stat <Dateiname>* ausgeben. ●

Sicher verschlüsselte Daten

Vergessene Notebooks, verlorene USB-Sticks, öffentliche Cloud: Vertrauliche und private Daten müssen auf die Eventualität vorbereitet sein, dass sie in fremde Hände gelangen. Verschlüsselung ist nicht bequem, aber unerlässlich.

Von **Hermann Apfelböck**

Quelle: D. Wolski

Wenn persönliche Daten persönlich bleiben sollen, ist das immer mit gewissem Organisationsaufwand und Komfortverlust zu bezahlen. Das ist leider logisches Gesetz, aber Sie können durch die Wahl der richtigen Werkzeuge den Aufwand gering halten. Generell ist der technische Anteil keine ernste Hürde und kommt erst an zweiter oder dritter Stelle der Verschlüsselungsstrategie. Das Richtige mit dem passendem Werkzeug zu verschlüsseln, ist zu allererst eine Frage der Ordnung und Disziplin: Die erste Frage lautet „Was muss ich verschlüsseln?“, die zweite „Wo (auf welchen Geräten) brauche ich die verschlüsselten Daten?“ und erst zuletzt kommt die dritte Frage: „Was ist in diesem Fall das angemessene und bequemste Werkzeug?“

Strategischer Überblick: Was – wo – wie?

Es gibt für wirksamen Datenschutz nur zwei Methoden, nämlich Vermeidung und Reduktion öffentlicher Daten und die Verschlüsselung der verbleibenden öffentlichen (oder potenziell öffentlichen) Daten. Vereinfachung durch Vermeidung ist die erste Grundregel:

- Nutzen Sie unterwegs immer nur ein und dasselbe mobile Gerät (ein Notebook, einen USB-Stick).
- Cloudspeicher sind entbehrlich, wenn Sie eine private Alternative in Form einer Homepage oder eines heimischen Linux-Servers haben. Wenn Sie einen Clouddienst benötigen, genügt das Kontingent eines Anbieters.
- Beschränken Sie sich auf allen Geräten auf einen Browser. Das gilt insbesondere dann, wenn Sie die Browsersynchronisierung nutzen und somit die Browserdaten bei Google oder Mozilla speichern.
- Mails müssen nach draußen – das ist nun einmal ihre Bestimmung. Damit private Mails weder direkt abgehört noch durch gehackte Mailserver öffentlich werden, nutzen Sie Mailverschlüsselung mit GnuPG.

Beachten Sie unsere Spezialbeiträge auf Seite 40, 42 und 48 (sichere Passwörter, Browser und Mailverschlüsselung). An dieser Stelle geht es ausschließlich um die Datenverschlüsselung auf PC/Notebook, USB-Datenträger und Cloudserver. Denn auch nach der Reduktion der zu schützenden Daten auf ein Minimum werden Kandidaten verbleiben, die zu verschlüsseln sind:

- Mobile Linux-Notebooks, bei Bedarf natürlich auch PCs, können bei der Linux-Installation so eingerichtet werden, dass alle Benutzerdateien automatisch verschlüsselt sind („Meine persönlichen Daten verschlüsseln“ unter Ubuntu, Mint und Co.). Näheres zur Home-Verschlüsselung lesen Sie auf Seite 32. Bei dieser Luks-Verschlüsselung (Linux Unified Key Setup) entsperrt die Benutzeranmeldung transparent und automatisch die Daten: Bei einem physischen Zugriff über ein Fremdsystem (ohne korrekte Benutzeranmeldung) sind die Dateien folglich unlesbar. Wer die Installeroption für Luks nicht genutzt hat, kann Luks theoretisch manuell einrichten, jedoch sind dann andere Werkzeuge einfacher und komfortabler.
- Bei mobilen USB-Datenträgern spielt es eine wesentliche Rolle, ob die Daten nur unter Linux, unter Linux und Windows, unter Linux und Mac-OS oder für alle Systeme lesbar sein

sollen. Eine Lösung für alle drei Systeme bietet der nachfolgend beschriebene Truecrypt-Nachfolger Veracrypt (*https://veracrypt.codeplex.com/*), der sich wie Luks auch für große Datenmengen eignet.

• Für Clouddaten reichen in der Regel Werkzeuge für kleinere Datenmengen. Erste Wahl ist Enc FS (Encrypted Filesystem), das sich für Linux, Mac-OS und sogar Android eignet, für Windows weniger. Für Linux und Windows sowie geringe Datenmengen können Sie aber auch auf einfache Packerverschlüsselung zurückgreifen. Zum optimalen Einsatz von Enc FS und 7-Zip lesen Sie nachfolgend mehr.

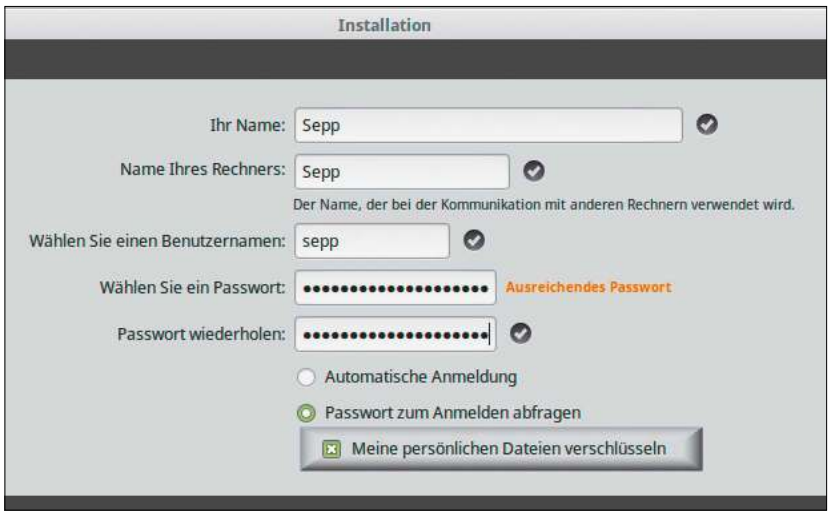
Verschlüsselungswerkzeuge in der Praxis

Die folgenden Kryptographiemethoden sind populär und verbreitet, aber nur ein Ausschnitt zahlreicher Verschlüsselungsoptionen. Es ist aber zu empfehlen, genau solche verbreitete Methoden zu verwenden, weil nur sie langjährige Kontinuität versprechen.

Kennwortschutz in Officesoftware

Libre Office und Microsoft Office bieten eine integrierte Verschlüsselung. Diese Methode, Dateien ad hoc einzeln zu verschlüsseln, eignet sich nur für wenige sensible Texte oder Tabellen, für größere Datenmengen ist sie zu unbequem. Libre Office bietet die Option „Datei -> Speichern unter -> Mit Kennwort speichern“. Das Kennwort muss dann jeweils beim Öffnen eingegeben werden. Dass das Dokument geschützt ist, ist Libre Office bei der Weiterbearbeitung klar: Es genügt künftig, normal zu speichern. In Microsoft Office erledigt den Job „Datei -> Speichern unter -> Tools -> Allgemeine Optionen“. Solche softwareinterne Kryptographie hat den Nachteil, dass Sie genau diese Software brauchen, um ein Dokument lesen zu können.

Libre Office ist eine Ausnahme, denn es kann auch passwortgeschützte Microsoft-Dateien öffnen. Umgekehrt ist das nicht der Fall.



Option des Ubuntu/Mint-Installers: Die Luks-Verschlüsselung von „/home“ ist mit die bequemste Methode, vor allem auf Notebooks alle lokalen Benutzerdaten abzusichern.

7-Zip-Verschlüsselung für Linux und Windows

Packer wie 7-Zip können zuverlässig verschlüsseln. Dies eignet sich für kleinere und mittlere Datenmengen, denn immerhin sind mehrere Dateien oder komplette Ordner problemlos möglich. Wichtig für USB und Cloud: 7-Zip-Archive lassen sich zwischen Linux und Windows austauschen.

Falls 7-Zip noch nicht vorliegt, installieren Sie den Packer unter Ubuntu und Co. mittels

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

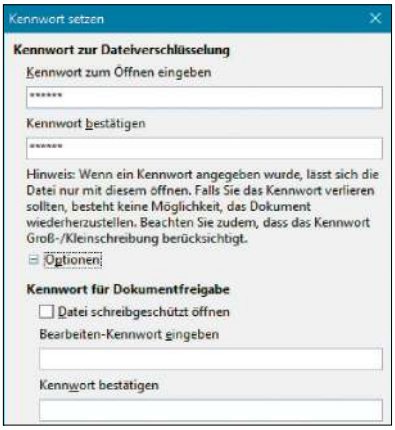
nach, für Windows gibt es unter *www.7-zip.de/download.html* mehrere Downloadvarianten. In Zusammenarbeit mit dem file-roller („Archivverwaltung“) unter Linux, worunter sich 7-Zip integriert, beziehungsweise dem 7z-Filemanager („7zFM.exe“) unter Windows ist Verschlüsseln und Entschlüsseln recht komfortabel: Sie ziehen Datei oder Ordner einfach mit der Maus in das Fenster („Archivverwaltung“ oder „7-Zip“), bestätigen unter Linux, dass damit ein neues Archiv angelegt werden soll. und geben dann das Format „7z“ und ferner unter „Erweiterte Einstellungen“ das Passwort an.

So leicht wird Privates öffentlich

Tatort Werkstoffhof: Hermann A. entsorgt einen Platinenrechner, der nach Fehlverhalten durch Überspannung abgeraucht ist. Ein, zwei Tage später fällt ihm ein, dass er die SD-Karte mit dem Betriebssystem in der Platine vergessen hat. Das ist kein finanzieller Ruin, und die SD-Karte enthält ja keine Benutzerdaten – oder?

Bei genauerer Überlegung doch: In der „~/.bashrc“ könnte das eine oder andere Samba-Kennwort für das lokale Netzwerk stehen. Unproblematisch. Bedenklicher: Für das bequeme Mounten des Strato-Hidrive via SSHFS dürften in dieser Datei User und Kennwort ersichtlich sein. Sicherheitshalber ändert Hermann A. das Kennwort seiner Hidrive-Cloud. Was die vergessene SD-Karte eventuell sonst noch über ihn verrät, wird er nicht mehr verifizieren können. So unwahrscheinlich es ist, dass sich irgendjemand intensiv und kompetent mit dieser SD-Karte beschäftigen wird, bleibt doch ein Unbehagen, das mit Paranoia nichts zu tun hat.

Die Konsequenz dieser Real-Anekdote? Lassen wir unsere Daten zu Hause. Und alles Persönliche, was wir aus dem Haus tragen oder ins Internet kopieren (was dasselbe ist), gehört verschlüsselt. Aber: Pannen mit nachfolgendem Unbehagen wird es immer geben ...



Einzeldateien unter Libre Office verschlüsseln: Diese Ad-hoc-Maßnahme ist ein Notbehelf für ganz geringe Datenmengen (hier Libre Office unter Windows).

Packer 7-Zip als Sicherheitstool: In der Archivverwaltung muss das Format „7z" gewählt werden, damit die Verschlüsselungsoptionen angeboten werden.

Die Option „Dateiliste ebenfalls verschlüsseln" sorgt dafür, dass der fileroller später auch keine Dateinamen verrät. Beim späteren Doppelklick des Archivs wird automatisch das Kennwort abgefragt und nur bei Kenntnis desselben entpackt. Unter Windows ist der Vorgang im Prinzip analog.

Wer sich die Aktion lieber auf der Kommandozeile mit dem einen oder anderen Alias zurechtlegen will, was die direkte Übergabe des Kennworts ermöglicht, kann unter Linux und Windows auf identische Syntax bauen:

```
7z a -p"Pass+w0rt" -mhe
 "Zielarchiv.7z"
 "Quelldatei|Ordner"
```

„a" ist der wesentliche Schalter, der 7-Zip zum Anlegen eines neuen Archivs anweist. Mit Schalter „-p" wird das Kennwort übergeben, danach folgen der Archivname und schließlich die Quelldaten. Schalter „-mhe" sorgt dafür, dass das Archiv keine Dateinamen anzeigt. Der Befehl

```
7z x -p"Pass+w0rt" "[name].7z"
```

entpackt ein Archiv.

Enc FS für Linux, Mac-OS und Android

Beim bewährten Enc FS herrscht seit 2014 Verunsicherung: Ein Sicherheitsexperte hatte nachgewiesen, dass die Enc-FS-Verschlüsselung knackbar sei, wenn mehrere Versionen derselben Datei vorliegen. Daher gibt es bei der Installation des Tools nach

```
sudo apt-get install encfs
```

einen entsprechenden Warnhinweis. Version 2.0 soll die Angriffsfläche beheben, aktuell erhalten Sie etwa unter Ubuntu/Mint noch Version 1.8.1. Wir vertreten hier den Standpunkt, dass es sich um ein akademisches Problem handelt, das normale Anwender ignorieren können: Den Aufwand, Enc-FS-Dateien zu entschlüsseln, wird man vielleicht bei der Terrorfahndung oder Industriespionage betreiben, aber gewiss nicht bei einem in der U-Bahn vergessenen Notebook.

Enc FS ist gut geeignet für kleinere und mittelgroße Datenmengen und vor allem für Anwender ideal, die auch mit dem Android-Smartphone ver- und entschlüsseln wollen. Dafür gibt es die Android-App Cryptonite (*https://goo.gl/RttwL*). Enc FS ist auch mit Mac-OS X kompatibel, auf Windows-Systemen läuft es hingegen nur mangelhaft (*http://goo.gl/djpLB*).

Enc FS ist als komplexes Kommandozeilenprogramm komplett über das Terminal zu bedienen (siehe *man encfs*). Die Kernsyntax

```
encfs [/Pfad1/verschlüsselte/Da
 ten/] [/Pfad2/unverschlüsselte/
 Daten/]
```

ist nicht schwierig, wonach man im Mountverzeichnis „Pfad2" arbeitet und in „Pfad1" die verschlüsselten Dateien liegen. Die Terminalbedienung bietet unterm Strich eine Reihe von Vorteilen, insbesondere die freie Wahl der Ordnerpfade. Trotzdem werden die meisten Desktopanwender das grafische Front-End Cryptkeeper bevorzugen, das sich insbesondere unter Ubuntu vorbildlich integriert. Nach

```
sudo apt-get install cryptkeeper
```

und dem Aufruf *cryptkeeper* präsentiert sich dieser dauerhaft als Schlüsselsymbol in der Hauptleiste. Die Option „Erstelle verschlüsselten Ordner" richtet ein neues verschlüsseltes Verzeichnis ein, wobei Sie in der oberen Zeile des Dialogs den Ordnernamen vergeben und unten zum gewünschten Ort navigieren, etwa zu einem USB-Stick.

Anmerkung: Beim Cryptkeeper müssen Sie an dieser Stelle ein neues leeres Verzeichnis verwenden; auf Kommandozeile ist auch ein existierendes Verzeichnis möglich, wobei hier aber bereits vorhandene Dateien nicht nachträglich verschlüsselt werden.

Mit der Schaltfläche „Vor" geht es dann weiter zur Passwortvergabe. Der noch leere Mountordner wird danach automatisch im Dateimanager geöffnet und kann befüllt werden. In diesem Mountordner arbeiten Sie mit unverschlüsselten Dateien. Die verschlüsselten Dateien liegen auf gleicher Ebene in einem versteckten Ordner „.[name]_enfcs". Um einen Enc-FS-Ordner wieder auszuhängen und damit zu schützen, klicken Sie auf das Cryptkeeper-Symbol und dann auf den betreffenden Eintrag.

Über die „Einstellungen" legen Sie fest, ob Mountordner nach dem Entladen („Aushängen") gelöscht werden sollen und ob ein nicht genutzter Enc-FS-Ordner nach einer bestimmten Frist automatisch entladen werden soll. Vor allem diese zweite Maßnahme erhöht die Sicherheit.

Aufgrund der typischen Arbeitsweise von Enc FS mit verschlüsselten Ordnern und unverschlüsselten Arbeitsordnern bietet es sich an, Sync-

ordner einer Cloud wie Dropbox als Enc-FS-Ordner zu definieren. Dann landen alle Dateien verschlüsselt auf dem Cloudserver.

Der Truecrypt-Nachfolger Veracrypt

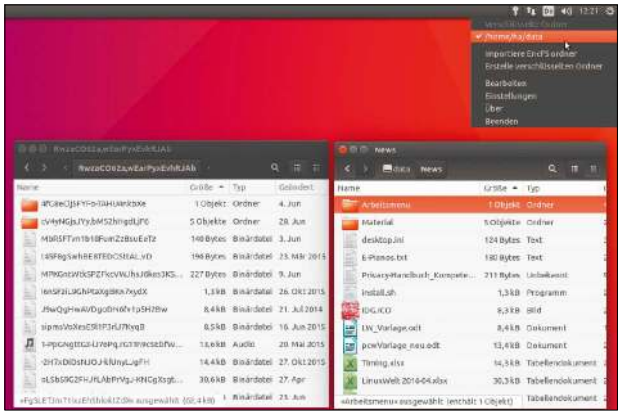
Verschlüsselte Container mit der Open-Source-Software Veracrypt eignen sich für große und sehr große Datenmengen, allerdings nur auf lokalen Rechnern oder im lokalen Netzwerk. Um umfangreiche verschlüsselte Container in der Cloud oder auf Webservern abzulegen, müsste man die Container ständig hin und her kopieren, um enthaltene Dateien zu lesen oder zu bearbeiten.

Veracrypt gibt es für Linux, Windows und Mac-OS. Anlaufstelle ist die Projektseite *https://veracrypt.codeplex.com/*, jedoch ist für Ubuntu und Co. die Installation über ein PPA deutlich einfacher:

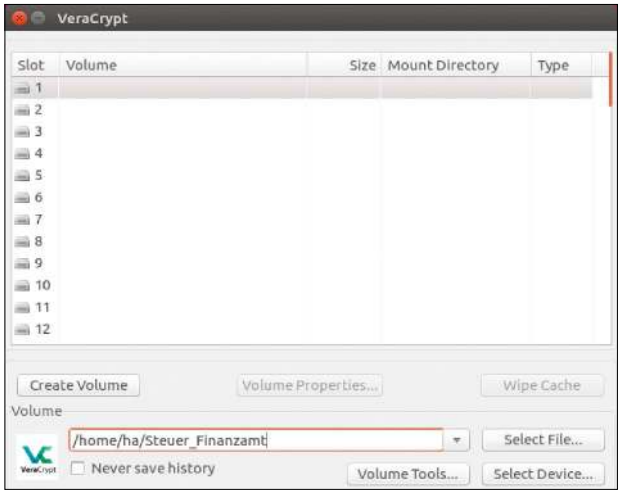
```
sudo add-apt-repository
  ppa:unit193/encryption
sudo apt-get update
sudo apt-get install veracrypt
```

Langjährige Truecrypt-Nutzer werden es begrüßen, dass Veracrypt die Oberfläche von Truecrypt komplett übernimmt (unter Linux nur englischsprachig). Noch wichtiger ist, dass Veracrypt auch alte Truecrypt-Container laden kann, sofern man beim Mounten eines Truecrypt-Containers die Option „TrueCrypt Mode“ aktiviert.

Container erstellen: Etwas Planung ist ratsam, weil verschlüsselte Container die Größe nicht mehr ändern können. Um nicht ständig neue Container anlegen zu müssen, sollten Sie angemessene Kapazitäten planen. Die Vorgehensweise ist wie bei Truecrypt: Nach „Create Volume -> Create […] file container -> Standard VeraCrypt volume“ geben Sie Pfad und Namen einer bisher nicht existierenden Datei an. Das wird der Container für die verschlüsselten Daten. „Encryption Option“ belassen Sie auf den Standardvorgaben und danach geben Sie die Größe des Containers an. Wenn Sie schon wissen, welche Dateien dort landen sollen, analysieren Sie den Umfang mit einem Dateimanager und rechnen dann noch einen großzügigen Puffer dazu. Danach kommt die Passwortvergabe („keyfiles“ sind eine interessante Alternative, deren Erläuterung aber hier zu weit führt).



Der Cryptkeeper mit seinem Schlüsselsymbol in der Ubuntu-Leiste vereinfacht Enc FS erheblich. Der untere Bildteil zeigt einen Enc-FS-Ordner und den zugehörigen Mount- und Arbeitsordner.



Noch nie intuitiv, aber wohlvertraut: Das Laden von Veracrypt-Containern entspricht exakt der Vorgehensweise unter dem Vorgänger Truecrypt („Select File“ und „Mount“).

Zur Schlüsselerstellung auf Basis des Passworts will Veracrypt Mausbewegungen im eigenen Fenster, was sie nach beendeter Fortschrittsanzeige mit „Format“ abschließen. Damit ist der Container einsatzbereit.

Container mounten und nutzen: Mit „Select File“ im Hauptdialog navigieren Sie zur Containerdatei. Mit Klick auf „Mount“ wird diese geladen und sofort im Dateimanager geöffnet (falls nicht, lässt sich das unter „Preferences -> System Integration“ einstellen). Linux mountet Container nach „/media/veracrypt[nummer]“, Windows auf freie Laufwerkbuchstaben. Auf diesem virtuellen Datenträger lesen, arbeiten, kopieren Sie wie auf einem normalen Laufwerk. Mit „Dismount“ im Hauptdialog entladen Sie den Container, der somit wieder geschützt ist. Oft genutzte Container lassen sich als „Favorites“ definieren, die sich dann über das gleichnamige Menü mit einem Klick laden lassen. Das ist aber nur bei Containern sinnvoll, die dauerhaft im gleichen Ordner verbleiben.

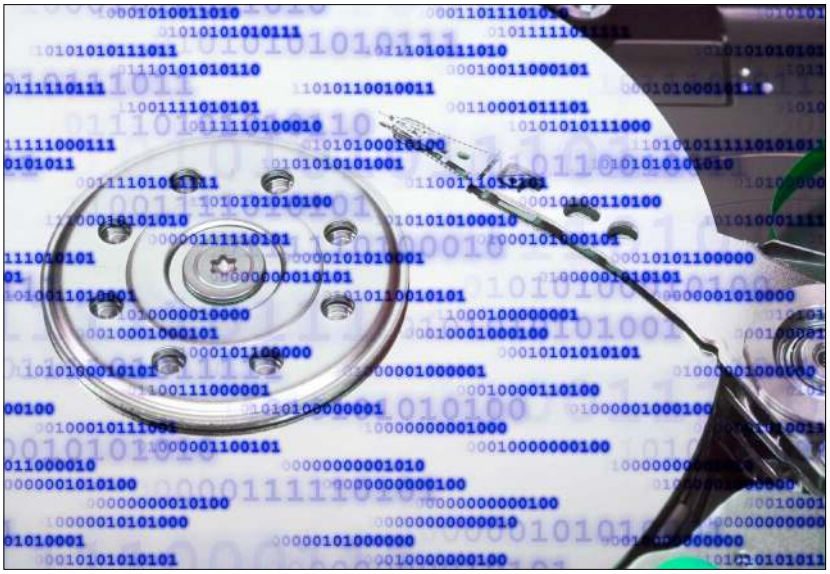
Hinweis 1: Wer lieber auf der Kommandozeile arbeitet oder dort via SSH arbeiten muss, kann Veracrypt auch komplett im Terminal bedienen (siehe *veracrypt --help*). Unter Windows funktionieren immerhin die wichtigsten Aktionen auch auf der Kommandozeile.

Hinweis 2: Beachten Sie, dass Sie zum Mounten von Veracrypt-Containern nach dem sudo-Kennwort gefragt werden, das mit dem Containerpasswort nichts zu tun hat und vermutlich anders lautet. ●

Benutzerdaten sicher ablegen

Wird das Notebook gestohlen oder geht verloren, können Unbefugte in Ruhe versuchen, das Benutzerverzeichnis auszulesen, um an vertrauliche Dokumente zu gelangen. Gegen dieses Risiko schützt eine Verschlüsselung der Daten.

Von **Stephan Lamprecht**



© Foto-Ruhrgebiet - Fotolia.com

Jeder Anwender speichert auf seinem System Dateien, deren Inhalt niemanden etwas angeht. Liegen die Dokumente unverschlüsselt auf der Festplatte, genügt bereits der Systemstart mit einer Rettungs-CD, um sich Dateien anzusehen und zu kopieren. Eine sichere Verschlüsselung beugt vor.

Verschlüsseltes Verzeichnis anlegen

Jeder Nutzer kann einen verschlüsselten Container in seinem Benutzerverzeichnis anlegen, um darin vertrauliche Dateien abzulegen. Dieses besondere Verzeichnis wird bei der Anmeldung automatisch entschlüsselt und bei der Abmeldung wieder verschlüsselt. Aus Anwendersicht ändert sich beim Arbeiten mit den Dateien nichts. Sie können normal bearbeitet, geöffnet und verschoben werden. Und auch die Einrichtung ist sehr einfach. In einem Terminal genügt bereits die Eingabe von

```
ecryptfs-setup-private
```

Das Kommando muss durch die Eingabe des Benutzerpasswords bestätigt werden. Danach möchte das Werkzeug die „Passphrase“, also das Kennwort für das Einbinden des verschlüsselten Laufwerks wissen. Dieses wird zweimal eingegeben. Jetzt genügt es, sich einmal ab- und dann wieder anzumelden. Als Ergebnis erscheint im Benutzerverzeichnis der neue Ordner „/Private“. Alle Dateien darin werden bei der Abmeldung verschlüsselt. Geht die Passphrase verloren, gibt es allerdings keine Möglichkeit mehr, an die Dateien heranzukommen. Deswegen sollte der Inhalt des versteckten Verzeichnisses „./.ecryptfs“ gesichert werden. Wurde keine eigene Passphrase gewählt, sondern eine vom System angelegt, wechseln Sie in einem Terminal in dieses versteckte Verzeichnis und lassen sich mit

```
ecryptfs-unwrap-passphrase
```

den Schlüssel anzeigen. Diesen müssen Sie unbedingt notieren, um im Falle eines Falles wieder an die Dokumente heranzukommen.

Das Home-Verzeichnis verschlüsseln

Nutzer mit einem noch größeren Sicherheitsbedürfnis können auch das gesamte Home-Verzeichnis verschlüsseln. Diese Maßnahme bieten die meisten Distributionen bereits während der Installation oder der Einrichtung eines neuen Benutzers an. Es ist der einfachste Weg, seine Daten sicher zu verwahren, die nur bei korrekter Anmeldung unverschlüsselt in ein Verzeichnis gemountet werden.

Je nachdem, wie viel Zeit seit der Anlage des Benutzers oder der Installation vergangen ist, gibt es zwei gangbare Wege, nachträglich zu verschlüsseln, die sich allerdings stark im Aufwand unterscheiden. Wenn für alle Benutzerdateien ein vollständiges Backup zur Verfügung steht, kann das Benutzerverzeichnis nachträglich einfach auf Verschlüsselung umgestellt werden. Dabei gehen aber die Einstel-

lungen und Dateien verloren. Wenn die Installation oder Anlage des Benutzers noch nicht lang zurückliegt, ist dies aber der einfachste Weg. So geht's:

Starten Sie das System zunächst im Recovery-Modus. Dazu muss während des Systemstarts in dem Moment, während der Bootmanager angezeigt wird, die Umschalt-Taste gedrückt werden. Bei Ubuntu-Systemen, die den Bootmanager vor den Augen des Anwenders verstecken, sollte das Drücken der Umschalt-Taste während des Systemstarts ausreichen.

Im Menü von Grub sind die verschiedenen Kernel-Versionen und deren Recovery-Modus aufgelistet. Wählen Sie dort den Eintrag aus, der mit dem Zusatz „Recovery" versehen ist. Damit startet das System und zeigt den Wiederherstellungsmodus an. Hier entscheiden Sie sich für „root", um eine entsprechende Konsole anzuzeigen. Jeder Nutzer eines Systems gehört zu einer Reihe von Gruppen, die vom System eingerichtet werden. Diese Gruppenzugehörigkeit regelt den Zugriff auf Systemressourcen. Die Zugehörigkeit ist in der Datei „/etc/group" geregelt. Von dieser Datei sollte am besten eine Kopie angelegt werden

```
cp -f /etc/group /etc/group.bak
```

Später können Sie die Datei mit einem Texteditor öffnen und sich ansehen, zu welchen Gruppen die Benutzer gehört haben, um deren Gruppenzugehörigkeit wiederherzustellen. Der Benutzer, um den es geht, wird nämlich zunächst gelöscht:

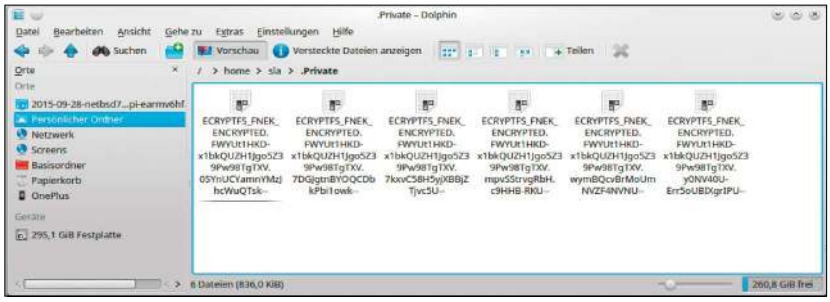
```
deluser --remove-home [Benutzerna
 me]
```

Hierbei wird auch das Home-Verzeichnis entfernt. Anschließend kann dieser Benutzer wieder neu angelegt werden – und dabei wird sein Home-Verzeichnis verschlüsselt:

```
adduser --encrypt-home [Benutzer
 name]
```

Details zum Benutzer können später noch hinterlegt werden. Wichtig ist aber, dass dem Nutzer root-Rechte zugewiesen werden, wenn er später auch die Systemverwaltung übernehmen soll. Dies erledigen Sie mit

Verschlüsseltes Verzeichnis: Es genügt ein kurzes Terminalkommando, um im Benutzerverzeichnis einen eigenen Ordner anzulegen, der vollständig verschlüsselt ist.



Vergeblicher Blick in den Ordner: Nicht nur der Inhalt der Dateien ist verschlüsselt, auch die Dateinamen verraten im Dateimanager nichts über deren Inhalt.

```
adduser [Benutzername] sudo
```

Mit Strg+D kehren Sie zum Ausgangsbildschirm zurück und wählen dort „resume". Damit startet der gewohnte Anmeldevorgang.

Der beschriebene Weg über die Recovery-Konsole ist nur notwendig, wenn lediglich ein Benutzer vorhanden ist. Geht es um die Anlage eines neuen Benutzers, kann dies auch jederzeit über ein Terminal erfolgen oder Sie verwenden die Benutzerverwaltung auf der grafischen Oberfläche, die Sie in den Systemeinstellungen finden.

Migration von Home ohne Datenverlust

Die nachträgliche Umstellung unter Beibehaltung aller Benutzerdateien und Einstellungen ist ebenfalls möglich, aber mit mehr Aufwand verbunden. Im ersten Schritt legen Sie ein vollständiges Backup des Benutzerverzeichnisses an, das geändert werden soll. Danach legen Sie einen neuen Benutzer an, der ebenfalls root-Rechte erwerben darf. Ist das erledigt, sollte man diesen Benutzer einmal testen. Funktioniert alles, melden Sie sich ab.

Auf dem Anmeldebildschirm rufen Sie mit Strg-Alt-F1 eine Konsole auf. Melden Sie sich mit dem neuen Benutzer an. Für die nachfolgenden Kommandos benötigen Sie root-Rechte. Stellen Sie also bei allen folgenden Befehlen jeweils ein *sudo* voran. Im Terminal wird zunächst der grafische Fenstermanager mit

```
service lightdm stop
```

beendet. Jetzt kann das Verzeichnis des ersten Benutzers migriert werden:

```
ecryptfs-migrate-home -u [Benut
 zername]
```

Danach starten Sie wieder den Fenstermanager mit *service lightdm start*.

Mit Strg-Alt-F7 gehen Sie wieder auf die grafische Oberfläche. Bevor das System neu gestartet oder heruntergefahren wird, melden Sie sich unbedingt mit dem ursprünglichen Benutzer an und testen das System ausgiebig. Die Anmeldung schließt die Migration ab – dieser Schritt ist also notwendig.

Kontrollieren Sie die Dateien im Home-Verzeichnis auf Vollständigkeit und Lesbarkeit. Hat alles wie erwartet funktioniert, kann das angelegte Backup natürlich wieder gelöscht werden. Von jetzt an kann auch der Diebstahl des Rechners der Vertraulichkeit der Daten nichts anhaben, da das Benutzerverzeichnis verschlüsselt vorliegt und erst bei der Anmeldung des Benutzers entschlüsselt wird. ●

Hochsicherheitstrakt Linux

Aufgrund der Architektur von Linux sind kaum Schadprogramme bekannt, die Unbefugten Informationen übermitteln können. Es gibt aber zusätzliche Möglichkeiten, das Sicherheitsniveau eines Linux-Rechners anzuheben.

Von **Stephan Lamprecht**

© GKSD - Fotolia.com

Für normale Benutzer eines Linux-Systems dürften die integrierten Sicherheitsfunktionen mehr als ausreichen. Über das Rechtesystem ist genau festgelegt, wer der Eigentümer von Ordnern und Dateien ist. Veränderungen an den Optionen des Systems sind dem Superuser root vorbehalten. Und schließlich kann durch die Verschlüsselung von Dateien oder von Partitionen das Risiko minimiert werden, dass sich Dritte einfach die gespeicherten Informationen ansehen.

Überall dort, wo höchstes Sicherheitsniveau herrschen muss, gibt es zusätzliche Programme, um ein System gegen unbefugte Zugriffe abzusichern. Und zwar gerade gegen solche aus dem Inneren des Systems. So kann theoretisch eine vom Benutzer gestartete Anwendung eine Hintertür enthalten, die auf Bereiche zugreift, die für die Erledigung der eigentlichen Aufgabenstellung nicht notwendig sind. Das Risiko, Opfer solcher Hintertüren zu werden, ist im Umfeld von Open Source gering, aber nicht vollständig auszuschließen. Banken, Versicherungen und Großunternehmen, die regelmäßig personenbezogene Daten verarbeiten, können ein solches Risiko schon aus Gründen der Haftung nicht eingehen.

Um solche Gefährdungspotenziale auszuschließen, wird dort oft auf das Sicherheitskonzept „Mandatory Access Control“ gesetzt.

Zwei Konzepte: App Armor und Selinux

Das Konzept des Mandatory Access (MAC) ist mit einer guten Firewall zu vergleichen. Bei einfachen Modellen kann der Nutzer den Datenverkehr lediglich auf Ebene eines Ports regeln. Entweder ist der Port geschlossen und ein Datenaustausch nicht möglich. Oder der Port wird geöffnet, dann haben aber alle Anwendungen darauf Zugriff. Bei besser ausgestatteten Modellen kann der Zugriff auf einen Port bis auf Ebene eines Programms festgelegt werden. Während das eine Programm den Port nutzen darf, ist dies bei einem anderen ausgeschlossen. Ähnlich fein steuert Mandatory Access den Zugriff auf die Ressourcen eines Linux-Systems. Dabei geht es nicht allein um den Zugriff auf das Netzwerk, sondern bis auf Datei- und Ressourcenebene hinab. Um Mandatory Access Control unter Linux umzusetzen, existieren zwei Lösungen mit unterschiedlichen Ansätzen, die beide auf eine lange Geschichte zurückblicken:

Security-Enhanced Linux (Selinux) ist eine Erweiterung des Kernels und wurde maßgeblich von der amerikanischen NSA und dem Hersteller Red Hat entwickelt. Es ist unter Red-Hat-Linux und dessen Abkömmlingen der bevorzugte Ansatz für das Abhärten des Systems. Selinux ergänzt das Rechtesystem von Linux um mehrere Schutzmechanismen. Type Enforcement definiert, ob ein Prozess auf ein Objekt zugreifen darf. Dazu werden Subjekten und Objekten in Form eines zusätzlichen Attributs Klassen zugeordnet. Ein Prozess darf nur dann auf ein Objekt zugreifen, wenn eine Regel den Zugriff auf die Klasse gestattet. Was nicht explizit erlaubt ist, ist verboten.

Ein weiterer Schutzmechanismus durchbricht das klassische Rollensystem unter Linux. Ein Benutzer befindet sich unter Selinux immer in einer von mehreren möglichen Rollen. Die Rolle des Benutzers definiert, auf welche Objekte er zugreifen kann.

Root darf in der Administratorrolle nur Systemverwaltungsaufgaben wahrnehmen. Obwohl er root ist, hat er keinen Zugriff auf die Home-Verzeichnisse der Nutzer. Die Erweiterung um die Sicherheitsattribute geschieht tief im System.

Application Armor (App Armor) gilt gemeinhin als einfacher zu administrieren und zu verstehen. Dabei operiert App Armor unabhängig vom Dateisystem. Umbauten daran, wie bei der Installation von Selinux, sind nicht notwendig. Auch am Rollenkonzept von Linux selbst gibt es keine Änderungen. App Armor arbeitet mit Regelwerken. Anders als bei Selinux erfolgt nicht eine Umstellung zu einem festen Zeitpunkt, sondern die Überwachung und die Regeln können nach und nach ausgebaut werden. Die Regeln legen fest, welche Rechte die Anwendung hat, beispielsweise welchen Netzwerkport sie nutzen, auf welche Dateien zugreifen darf und so fort. Da App Armor auch für normale Anwender praktikabel ist, folgt ein etwas genauerer Blick auf dieses Sicherheitskonzept.

App Armor einrichten und erkunden

Sie können App Armor über den Paketmanager oder in der Konsole nachrüsten:

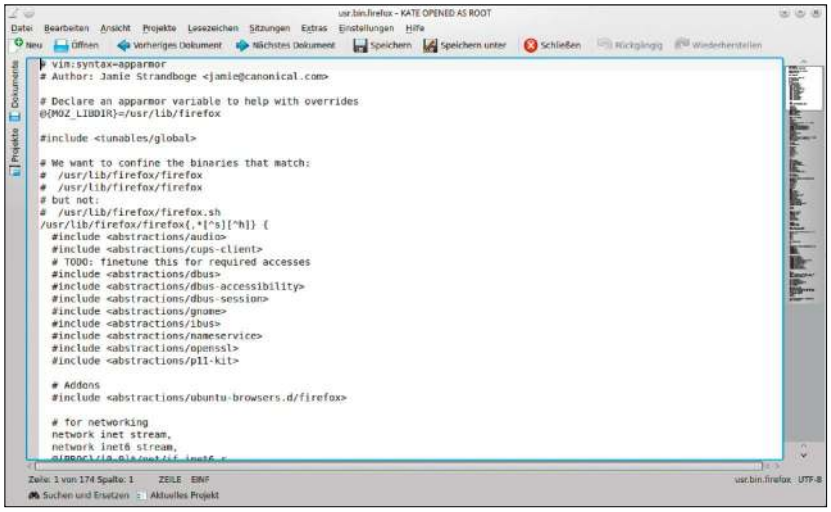
```
sudo apt-get install apparmor
```

Nützlich ist es, auch noch die zusätzlichen Pakete „apparmor-utils“ und „apparmor-profiles“ zu installieren. Mit dem Kommando

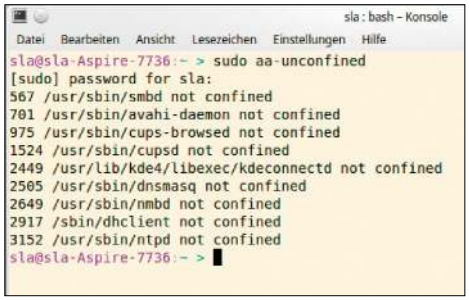
```
sudo aa-status
```

können Sie auf der Konsole abfragen, ob App Armor läuft.

Auf einem völlig abgesicherten System existiert im Idealfall für jede Anwendung ein Profil. Jedem Profil kann wiederum einer von drei erlaubten Modi zugewiesen werden. Der „Enforce-Modus“ unterbindet alle Aktionen, die gegen die im Profil definierten Regeln verstoßen. Im „Complain-Modus“ darf eine Anwendung an sich verbotene Aktionen ausführen, die protokolliert werden. Der „Audit-Modus“ dient der Protokollierung von Regelverstößen und Regelanwendungen. Während des Einrichtens der Profile wird zweckmäßig zunächst der Complain-Modus genutzt. So kann im Benutzeralltag und über das Protokoll geprüft werden, ob die Rechtebeschränkung praktikabel ist oder zu Problemen führt. Die Anwendungsprofile für App Armor liegen gemeinsam im Verzeichnis „/etc/apparmor.d/“. Der Dateiname des Profils entspricht dabei dem Namen und Pfad der Anwendung, auf die es sich bezieht.



Firefox-Profil: Die Profile von App Armor lassen sich mit jedem beliebigen Texteditor bearbeiten und sind nach etwas Einarbeitungszeit auch gut verständlich.



App-Armor-Kontrolle: Ein einfaches Terminalkommando zeigt alle laufenden Prozesse, für die es noch kein aktives Profil gibt. Diese sollten als Erstes untersucht werden.

Sie können sich mit einem beliebigen Texteditor eines der Profile ansehen, um es zu bearbeiten, benötigen Sie root-Rechte. Wenn Sie etwa das Profil von Firefox bearbeiten wollen, nutzen Sie dieses Kommando:

```
sudo gedit /etc/apparmor.d/usr.
  bin.firefox
```

Auf den ersten Blick wirkt ein solches Profil ziemlich kompliziert, doch die Struktur ist logisch. Zu Beginn wird mit dem Kommando „#include“ häufig auf den Ordner „/tunables/global“ verwiesen. Darin ist eine Reihe von Variablen gespeichert, was beim Anlegen von Profilen viel Zeit spart. Erst danach folgen die Anweisungen, die für den Prozess, der geschützt werden soll, typisch sind. Dabei werden die aus dem Dateisystem bekannten Kürzel benutzt.

Ein Eintrag

```
/etc/passwd rw
```

bedeutet etwa, dass der Prozess auf das Verzeichnis lesenden („r“) und schreibenden („w“) Zugriff haben darf. Zusätzlich arbeitet App Armor mit einigen internen Bezeichnungen und Kommandos. Wenn der Netzwerkverkehr verboten werden soll, würde dies ein Eintrag wie

```
deny network tcp,
```

regeln. Lautet der Eintrag dagegen nur „network“, ist der Netzwerkzugriff ohne jegliche Einschränkung möglich. Wenn Sie sich intensiver für die Absicherung mittels App Armor interessieren, können Sie sich als root die Prozesse mit Netzwerkzugriff ansehen, die noch nicht durch ein Profil geschützt sind. Der Befehl

```
sudo aa-unconfined
```

gibt eine entsprechende Liste aus. Diese Prozesse sind erste Kandidaten für neue App-Armor-Profile. ●

Router unter der Lupe

Der Router ist das Gateway ins Internet und die Schnittstelle zwischen den sicheren Gewässern des lokalen Netzwerks und den Untiefen des Internets. Damit das so bleibt, muss der Router sicher konfiguriert sein.

Von **David Wolski**

Ein typischer Router übernimmt üblicherweise mehrere Aufgaben, denn er kombiniert das Kabel-/ADSL-Modem mit einem Switch und DHCP-Server, um im lokalen LAN die Clients zu einem Netzwerk zusammenzuschließen. Im heimischen Netzwerk ist der Router also der zentrale Zugangspunkt. Damit dieser Zugangspunkt nicht zum Einfallstor wird, ist es wichtig, den Router einigen Checks zu unterziehen. Da viele Anwender den Router ohne große Änderungen an der Konfiguration in Betrieb nehmen, laufen die Geräte meist mit Standardeinstellungen. Diese sind nicht immer optimal und schlimmstenfalls unsicher.

Firmware: Update oder Ausschuss

Im Auslieferungszustand weist die Firmware vieler Router Sicherheitslücken auf. Der erste Schritt besteht immer darin, im Internet zu überprüfen, ob es eine neue Firmware des Herstellers gibt. Hersteller schließen bekannte Sicherheitslücken zwar meist rasch, aber leider installieren viele Administratoren oder Benutzer diese Aktualisierungen nicht. Viele Hersteller wie auch AVM für die Fritzbox bieten in der Konfigurationsoberfläche die Möglichkeit, direkt eine Aktualisierung durchzuführen. Wo das nicht der Fall ist, lassen sich Updatedateien aus dem Internet herunterladen und über die Konfigurationsoberfläche installieren.

Aufschlussreich ist auch immer eine Websuche nach bekannten Lücken. Eine umfangreiche Datenbank bekannter Schwachstellen bietet die englischsprachige Open Source Vulnerability Database (*http://osvdb.org*). Seit April 2016 wird die Datenbank zwar nicht mehr erweitert, die Informationen bleiben aber trotzdem eine Fundgrube. Weitere Lücken finden sich in der Exploit-DB (*https://www.exploit-db.com*). Alte Router mit bekannten Sicherheitslücken, gegen die es kein Firmwareupdate mehr gibt, sollten besser ausgemustert werden. Vor diesem Schritt lohnt sich aber die Suche nach inoffizieller Firmware für das veraltete Modell.

Log-in: Nur komplexe Kennwörter

Einer der ersten Schritte bei der Routereinrichtung sollte die Änderung des Standardpassworts und des vorgegebenen Log-in-Namens sein, damit die Routerverwaltung nicht einfach über die Standardanmeldung gelingt, die im Handbuch steht. Router nutzen zunächst ganz simple Log-in-Daten, etwa die Kombination User=admin und Passwort=admin oder auch gar kein Passwort. Auch wenn der Hersteller ein weniger leicht zu erratendes Passwort gesetzt hat, bietet dieses keinerlei Schutz, denn Webseiten wie *http://www.routerpasswords.com* sammeln bekannte Anmeldedaten zu Routern zur einfachen Recherche. Die Passwortänderung ist selbst dann empfehlenswert, wenn Sie einen WLAN-Router nur selbst nutzen.

Einige Router lassen den Verwaltungszugriff über das Internet zu. Es ist in den seltensten Fällen sinnvoll, die Administration eines Heimrouters über das Internet zu erlauben.

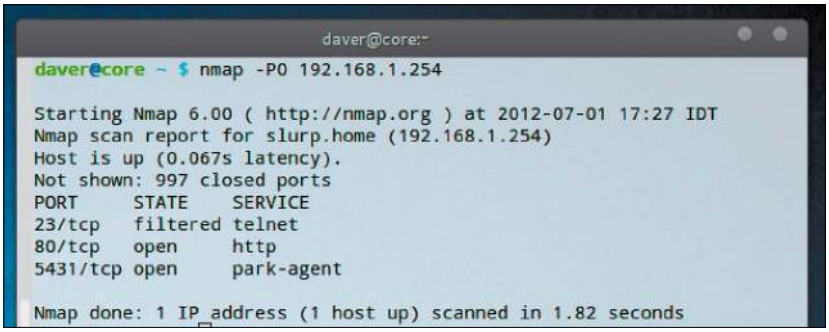
Wichtig: Gerne werden weitere Access Points im Netzwerk übersehen, die ebenfalls eine Verwaltungsoberfläche haben und mit Standardpasswörtern ausgestattet sind. Dazu gehören beispielsweise auch Powerline-Adapter mit WLAN-Funktion, die in vielen Netzwerken versehentlich offenstehen.

Verschlüsselt: Administration per SSL

Die Anmeldung an der Verwaltungsoberfläche sollte auch aus dem LAN heraus über HTTPS erfolgen, sofern der Router das anbietet, damit die Log-in-Daten nicht unverschlüsselt übertragen werden. Ansonsten besteht das Risiko, dass LAN-Teilnehmer oder

Anmeldedaten zum Nachschlagen: Passwortdatenbanken wie http://www.routerpasswords.com zeigen schön übersichtlich die bekannten Standardpasswörter und Admin-Log-ins von Routern an.

Gut gelöst: Bei den Geräten von AVM gibt es auch für nicht mehr ganz frische Modelle noch Updates der Firmware. Die Routeradministration zeigt, ob es eine neue Firmware gibt.



Bewährtes Tool bei der Suche nach Lücken: Der Portscanner nmap prüft hier einen Router auf offene Ports und entdeckt neben dem Webzugang einen laufenden Telnet-Server.

ungebetene Besucher, die über andere Sicherheitslücken bereits ins Netz kamen, die Zugangsdaten mitprotokollieren. Nicht alle Geräte für den Gebrauch zu Hause unterstützen HTTPS über ein SSL-Zertifikat. Erfreulicherweise verfügt aber die AVM Fritzbox über diese Sicherheitsfunktionen. Sie ist in der Oberfläche im Menü „Internet -> Freigaben -> Fritz!Box-Dienste“ untergebracht.

Das Zertifikat der Fritzbox ist nicht von einer CA signiert und beim ersten Aufruf der HTTPS-Adresse, etwa mit *https://fritz.box*, wird sich der Browser über ein ungültiges Zertifikat beschweren. Eine Aufnahme des Zertifikats als Ausnahme lässt diese Warnung verschwinden, und die Verbindung ist dann sicher verschlüsselt.

Portscan: Der Router im Check

Welche Dienste der Router im lokalen Netzwerk anbietet, finden Sie mit einem Portscanner heraus. Das bekannteste Programm für diesen Zweck ist der Portscanner Network Mapper – kurz nmap. Es ist Bestandteil aller Linux-Distributionen und lässt sich in Ubuntu und Debian mit

```
sudo apt-get install nmap
```

nachinstallieren. Um einen Scan zu starten, geben Sie den Befehl

```
sudo nmap -P0 [IP-Addresse]
```

ein. Der Parameter „-P0“ weist nmap an, nicht auf eine Ping-Antwort des Routers zu warten. Dies verhindert einen Abbruch des Scans, falls der Router ICMP-Anfragen (Pings) verwerfen sollte. In der darauffolgenden Ausgabe auf der Kommandozeile sehen Sie dann die Ergebnisse des Scans mitsamt den eventuell geöffneten Ports des Routers. Wenn die IP-Adresse des Routers zunächst nicht bekannt ist, dann hilft folgender Terminalbefehl:

```
mtr google.de
```

Der Befehl zeigt alle Zwischenstationen zwischen dem Rechner und dem Zielserver unter der angegebenen Adresse an. Die allererste IP-Adresse ist jene des Routers.

Inoffizielle Firmware: DD-WRT und Co.

Auf handelsüblichen Routern läuft ein vom Hersteller angepasstes Linux-System als Betriebssystem, das nicht immer alle Möglichkeiten ausschöpft. Alternative Routerfirmware zielt darauf ab, alle Funktionen und Einstellungen offenzulegen. Mittlerweile gibt es alternative Firmwarevarianten für Hunderte Routermodelle. Das Aufspielen ist bei einigen Geräten so einfach wie ein Softwareupdate, bei anderen sind Geduld und Experimentierfreude gefragt. Einige Router, wie der Belkin (Linksys) WRT1900AC, bewirbt der Hersteller sogar ausdrücklich mit der Kompatibilität zu Open-Source-Firmware. Drei Open-Source-Firmwares haben sich als gut gepflegte Projekte etabliert: DD-WRT (*https://www.dd-wrt.com/site*), Open WRT (*https://openwrt.org*) und Tomato USB (*http://tomatousb.org*).

In einer anderen Liga spielen die Router von AVM, die als Fritzbox, Speedport oder 1&1 Home Server vermarktet werden. Inoffizielle Firmwareimages können aus rechtlichen Gründen nicht zum Download angeboten werden, sondern erfordern das Kompilieren auf eigene Faust (*http://pcwelt.de/1955419*).

Sichere Netze und Funknetze

Zu Hause und in kleinen Unternehmen ist es meistens der Router, der für LAN und WLAN sorgt. Auch wenn diese Geräte über eingeschränkte Verwaltungs- und Überwachungsfunktionen verfügen, muss die Sicherheit hier nicht zu kurz kommen.

Von **David Wolski**

Netzwerke sind gewachsene Strukturen und wachsen meist noch gerne ein Stück weiter – mit einem weiteren Access Point hier und einem Raspberry Pi dort. Typische Heimnetze mit LAN und WLAN sind selten generalstabsmäßig geplant, sondern nach Bedarf zusammengestellt und erweitert. Dementsprechend divers sind die teilnehmenden Geräte, selbst wenn das Netzwerk nur den eigenen Geek-Gerätepark, ein paar PC-Arbeitsplätze oder das familiäre WLAN bedient. Um diese Netzwerke geht es in diesem Beitrag, zumal die Dokumentation zum Management und Audit von großen Netzwerken schnell ganze Ordner füllt. Heimnetze müssen aber nicht unsicher sein, sofern Router, WLAN und sorgfältig konfiguriert werden. Generell gibt es drei Szenarien zu, auf die zu achten ist:

- unautorisierte Zugriffe von außen auf das WLAN wegen Konfigurationsfehlern
- unerwünschte Zugriffe aus dem Internet wegen laxer Portfreigaben
- unkontrollierte Portfreigaben durch Programme über UPnP

WLAN-Sicherheit: WPA oder WPA2?

Bei der Einrichtung eines WLAN, das nicht allen offen stehen soll, ist Verschlüsselung nach WPA beziehungsweise WPA2 Pflicht. Der Unterschied von WPA2 zu WPA liegt im vorgeschriebenen Verschlüsselungsstandard: AES (Advanced Encryption Standard) von WPA2 gilt als sehr sicher, das ältere TKIP (Temporal Key Integrity Protocol) von WPA ist mit dem verwendeten RC4-Verschlüsselungsverfahren nicht ganz so robust. WPA mit der alten TKIP-Verschlüsselung zwackt außerdem bis zu 17 Prozent Netzwerkperformance ab.

Ideal ist also WPA2 mit AES. Wenn dies bei Altgeräten nicht zur Verfügung steht, ist auch WPA mit der oft angebotenen AES-Erweiterung eine gute Wahl. Zudem muss bei schnellen 802.11n-Netzwerken gemäß Spezifikation sowieso AES verwendet werden, ansonsten schaltet der Router automatisch einen Gang zu 802.11g herunter.

Authentifizierung besser ohne WPS

Zur vereinfachten Konfiguration bieten viele Router WPS (WiFi Protected Setup), das mit Hilfe einer PIN oder sogar mit einem automatischen, kurzzeitig freigeschaltetem Setup per Knopfdruck die Eingabe von langen WLAN-Passwörtern auf dem Client erspart. Nützlich ist WPS dann, wenn Anwender nicht in der Lage sind, Passwörter korrekt bei der Konfiguration einzugeben. Unter Linux wird WPS vom NetworkManager generell nicht unterstützt. Zudem ist WPS auf vielen Routern unsicher umgesetzt und hat Sicherheitslücken, die unautorisierten Clients per Brute-Force-Angriffen die PIN verraten können. Um davor sicher zu sein, sollten Sie WPS im Router beziehungsweise Access Point abschalten.

Übersicht aller Teilnehmer im Netzwerk

Wer ist mit dem Netzwerk verbunden oder am WLAN angemeldet? Viele Router, aber nicht alle, geben darüber bereitwillig Auskunft. Falls der Router diese Funktion nicht bietet oder kein

Zugriff auf die Administrationsoberfläche besteht, dann hilft der Angry IP Scanner weiter. Das Java-Programm zeigt alle Teilnehmer in Netzwerk mit IP-Adresse an und führt auf Wunsch auch gleich einen Portscan auf die gefundenen IP-Adressen aus. Auf der Projekt-Webseite *http://angryip.org/download/#linux* stehen DEB- und RPM-Pakete zur Installation unter Debian, Ubuntu, Mint, Fedora und Open Suse bereit. Eine installierte Java-Runtime, die Linux-Distributionen über ihre eigenen Paketquellen liefern, wird vorausgesetzt. Der Angry IP Scanner findet nicht nur alle Netzteilnehmer, sondern hilft auch bei der Identifikation von möglicherweise unerwünschten Serverdiensten.

Angry IP Scanner: Das Java-Programm nimmt eine Inventur der Netzwerkteilnehmer vor und kann dabei offene Ports ausmachen. Ein kompletter Portscan dauert eine Weile.

Außenansicht: Um Portfreigaben zu testen und versehentlich geöffnete Ports auf dem Router zu entdecken, lohnt sich ein Scan von außen, etwa über www.speedguide.net/scan.php.

UPnP durch die Firewall

Eine manuelle und daher bewusst eingerichtete Portfreigabe im Router ist nicht der einzige Weg, durch die Firewall des Routers Serverdienste nach außen anzubieten. Mit UPnP (Universal Plug and Play) ist dies ebenfalls möglich. Ein Risiko ist, dass Malware auf Clients im Netzwerk ebenfalls diese Technik nutzen, um temporär Ports zu öffnen. Um das zu verhindern, genügt es, UPnP als Protokoll in der Routeradministration abzuschalten. Bei der AVM Fritzbox findet sich die Einstellung dazu im Menü „Internet -> Freigaben -> Portfreigaben“ unter dem Namen „Alle Geräte im Heimnetz dürfen Portfreigaben selbständig verändern“. Standardmäßig ist diese Option inaktiv, was allerdings nicht bei allen Routern der Fall ist. Hilfreich ist übrigens ein Portscan von außen gegen den eigenen Router, um versehentlich Portfreigaben zu entdecken. Einen Scan nimmt die Seite *www.speedguide.net/scan.php* vor.

Clientisolation für Gäste

Ein Gast-WLAN, das getrennt vom internen WLAN arbeitet, lässt Ihre Besucher ins Internet, aber nicht ins lokale Netzwerk. Zudem ist eine weitere Sicherheitsvorkehrung empfehlenswert: Im Gast-WLAN sorgt die Clientisolation dafür, dass alle Clients nur sich selber und den Zugangspunkt im lokalen Netzwerk sehen, nicht aber andere Clients. In der Konfigurationsoberfläche von Access Points und WLAN-Routern heißt diese Einstellung meist „Wireless Isolation“, „Clients Isolation“, „AP Isolation“ oder „Station Isolation“. In der AVM Fritzbox und dem Telekom Speedport nennt sich die Funktion „Die mit dem Gastzugang verbundenen WLAN-Geräte dürfen untereinander kommunizieren“ im Menü „WLAN -> Gastzugang“. Ist die Clientisolation aktiviert (oder – gleichbedeutend – in der Fritzbox die Clientkommunikation abgeschaltet), erreichen WLAN-Geräte über den Router zwar das Internet, können sich aber nicht mit anderen Teilnehmern verbinden.

Störerhaftung: Abmahnungen weiterhin möglich

Werden über die eigene Internetverbindung Urheberrechtsverletzungen oder Straftaten verübt, heißt es vor Gericht meist: im Zweifel gegen den Angeklagten – also gegen den Anschlussinhaber. Dieser ist anhand der IP-Adresse, die ein Geschädigter dem Gericht vorlegt, schnell ausgemacht. Internetprovider unterliegen in Deutschland seit 2008 einem zivilrechtlichen Auskunftsanspruch und müssen die Identität eines Kunden hinter einer IP-Adresse preisgeben, auch ohne richterlichen Beschluss. Das Bundeswirtschaftsministerium hatte 2015 einen Gesetzesvorschlag ausgearbeitet, der die Situation für WLAN-Betreiber entschärfen sollte. So sollten Privatpersonen und Betreiber öffentlicher Netze nicht mehr selbst haften, wenn sie die Gäste in ihrem WLAN namentlich kennen.

Daraus wurde nun doch nichts: Die aktuelle Gesetzesvorlage für den Paragraf 8 TMG schafft keine Sicherheit vor Unterlassungsansprüchen gegen Anschlussinhaber, also vor Abmahnungen. Daher muss sich weiterhin jeder gut überlegen, ob er Gäste in sein WLAN lässt.

Sichere Passwörter

Ein vielschichtiges Thema: Welche Kennwörter sind sensibel, welche nicht? Ist der Ort, an dem die Passwörter gespeichert sind, sicher und vertrauenswürdig? Wie viele Geräte brauchen Zugriff auf wie viele Kennwörter?

Von **Hermann Apfelböck**

Zum Thema „Passwort" kann man jede Menge punktueller Ratschläge erteilen, die alle für sich genommen richtig sind: Das Passwort soll komplex sein. Es muss verschlüsselt gespeichert sein, damit es kein anderer lesen kann. Das Passwort kann durch Zwei-Wege-Authentifizierung unterstützt werden (Google). Verschiedene Log-ins benötigen unterschiedliche Kennwörter. Passwortmanager reduzieren den Aufwand …

Das trifft alles zu, aber es vermittelt keine Strategie. Wer mit einem Notebook und einem Smartphone mit einem Google-Konto durchs Leben kommt, hat völlig andere Voraussetzungen als ein Poweruser mit vielen Clientgeräten, Server, Websites, FTP-Zugängen und einer dreistelligen Anzahl von Onlinekonten. Die Strategie muss lauten, eine für das Nutzerprofil sichere Lösung mit geringstmöglicher Komplexität zu finden.

Welches Passwort für welchen Zweck?

Was in heimischen Netzwerken für System-Log-ins (Linux, Windows), Netzwerkfreigaben (Samba, Windows), Administrationsoberflächen (Router, Netzdrucker, Access Points, Apache-/Nginx-Dienste) an Kennwörtern benötigt wird, ist nicht sonderlich sicherheitskritisch. Hier ist es durchaus vertretbar, sich die Log-ins für viele Zugänge mit einem gemeinsamen Kennwort zu vereinfachen, das noch nicht mal hohe Komplexitätsansprüche erfüllen muss. Wichtige Ausnahme ist nur das WLAN-Passwort, das den Zutritt Fremder ins Heimnetz verhindert: Dieses muss lang und komplex ausfallen, zumal es auf jedem Clientgerät nur einmal eingegeben werden muss.

Solche Vereinfachung ist nur zulässig, solange Daten und Geräte das Haus nicht verlassen: Jede Öffnung nach außen via Portfreigabe im Router erfordert sichere Passwörter und jedes Notebook, das das Haus verlässt, verdient einen gut abgesicherten Systemzugang.

Onlinekennwörter sind ebenfalls nicht über einen Kamm zu scheren: Der Zugang zu einem Diskussionsforum oder einer Vereinshomepage ist unkritisch. Hier müssen Sie sich nicht mit einem Sonderzeichenmonster verkünsteln und können auch ein Standardpasswort für verschiedene Zugänge nutzen. Besonders sensibel ist hingegen das Mailkonto: Ein gehacktes Mailkonto legt nicht nur die private Korrespondenz offen, sondern ermöglicht zudem den Zugriff auf weitere Online-Log-ins: Denn bei den meisten Diensten genügt die Mailadresse, um sich („Kennwort vergessen?") einfach ein neues Passwort zu beschaffen, das dann wiederum an das gehackte Mailkonto geschickt wird. Ebenfalls sensibel sind Bank-, Paypal-, Onlineshop-Log-ins, eventuell (je nach Nutzung) auch Konten in sozialen Netzen.

Wer die unterschiedlichen Sensibilitätsstufen berücksichtigen will, kann eine Passwortstrategie nach folgendem Muster verfolgen: Ein einfaches Standardpasswort dient für die meisten lokalen Anmeldungen im Heimnetz. Ein anderes einfaches Kennwort nutzen Sie für unkritische Onlineanmeldungen (Forum, Schule, Verein, Stadtwerke). Für alle kritischen Zugänge verwenden Sie komplexe Passwörter. Um es sich hier einfacher zu machen, kann ein Masterkennwort herhalten, das Sie in rekonstruierbarer Weise jeweils für den einzelnen Zugang variieren. Das könnte etwa so aussehen: „wien+bonn-kiel=ltrn" – wobei „wien+bonn-kiel=" das Masterkennwort wäre, und „ltrn" den zweiten, vierten, sechsten und achten Buchstaben der Anmelde-URL von „elsteronline.de" übernimmt (als Beispiel). Ein solches Schema ist dann bei jeder Anmelde-URL jederzeit ohne fremde Hilfe rekonstruierbar.

Komplexe Kennwörter schützen gegen Wörterbuchangriffe, sind aber leider kein Allheilmittel: Oft werden komplette Datenbanken inklusive aller Zugangsdaten gehackt. Dann ist das Passwort in fremden Händen – sei es schwach oder stark. Daher ist es so wichtig, für eine halb private Vereinsseite oder einen kleinen Onlineshop, die keine anspruchsvolle Sicherheitsadministration erwarten lassen, ein anderes Kennwort zu verwenden als beim Google- oder Amazon-Konto.

Wo werden die Kennwörter gespeichert?

Die Komplexität von Passwörtern spielt – scheinbar – keine Rolle, weil sich die Software die Kennwörter merkt: So landen etwa die Zugangsdaten für lokale Netzfreigaben im gnome-keyring oder kwalletmanager, in Filezilla ist ein FTP-Serverzugang nur einmal samt Kennwort einzutragen, Browser wie Firefox oder Chrome speichern auf Nachfrage die Log-in-Daten von Onlinediensten und tragen diese beim nächsten Besuch der Seite automatisch ein.

Sich auf die Software zu verlassen, hat aber Nachteile und erhöht die Komplexität: Wer nur einen PC oder ein Notebook nutzt, fährt damit sicher bequem – solange das System funktioniert. Bei mehreren Geräten muss man dafür sorgen, dass dieselbe Software überall bereitsteht und die Passwörter kennt. Richtig bequem ist das nur beim Browser, sofern Sie sich bei Firefox Sync oder Chrome Sync anmelden und die Passwörter synchronisieren lassen. Dabei übermittelt der Browser die Passwörter an Mozilla oder Google beziehungsweise empfängt sie von dort. Dies geschieht verschlüsselt, schafft aber auch eine nachhaltige Abhängigkeit vom jeweiligen Browser.

Wer die Browser-Synchronisierung unterwegs auf Notebooks nutzt, muss außerdem wissen, dass sich alle Passwörter unter „Einstellungen -> Sicherheit -> Gespeicherte Zugangsdaten“ (Firefox) oder „Einstellungen -> Erweiterte Einstellungen -> Passwörter verwalten“ (Chrome/Chromium) auslesen lassen. Chrome fordert dabei unter Windows das Windows-Kennwort, unter Linux stehen die Kennwörter hingegen offen. Die Firefox-Daten sind gut zu schützen, indem man das zusätzliche Masterpasswort einrichtet.

Gespeicherte Passwörter in Firefox: Wäre kein Masterpasswort vergeben, wären sämtliche Kontodaten bei physischem Rechnerzugriff zugänglich.

Anlegen der Datenbank in Keepass: Der erste Schritt ist die Vergabe des Masterpasswortes. Damit wird die KBD-Datenbankdatei des Passwortmanagers verschlüsselt.

Trotz mancher Tücken ist es der bessere Weg, die Onlinekennwörter einem Chrome oder einem Firefox anzuvertrauen als einen zusätzlichen Online-Passwortmanager wie Lastpass einzusetzen. Auch hier müssen Sie die (verschlüsselten) Kennwörter auf einem amerikanischen Server speichern, der aber nicht die Reputation etwa einer Mozilla-Foundation genießt. Lastpass musste Mitte 2015 einen Hackerangriff einräumen und seine Benutzer zum Ändern des Masterpassworts aufrufen.

Keepass-X mit Synchronisierung

Die Browsersynchronisierung hat zwei Mängel, die eine Ergänzung ratsam erscheinen lassen: Erstens weiß niemand, ob es Google und Mozilla morgen noch gibt, vor allem aber ob es deren Dienste noch kostenlos gibt. Zweitens speichern Firefox und Chrome keine lokalen Kennwörter. Wenn Sie alle Passwörter im Griff haben wollen, brauchen Sie zusätzliche Hilfe. Der Passwort-Manager Keepass-X, der in gängigen Distributionen in den Paketquellen liegt (Ubuntu/Mint: *sudo apt-get install keepassx*), arbeitet als lokale Software. Das Öffnen der lokalen KBD-Datenbankdatei erfordert die Eingabe des Keepass-Masterpassworts und ist daher auch bei physischem Fremdzugriff geschützt. Die Synchronisierung mehrerer Rechner ist nicht vorgesehen, lässt sich aber über einen Trick erreichen, etwa über den lokalen Synchronisierungsordner von Dropbox. Dann genügt es, Keepass-X mit der aktuellen KBD-Datei über den Aufruf

```
keepassx ~/Dropbox/[name].kbd
```

zu laden. Dieser direkte Aufruf der Datenbankdatei funktioniert ebenfalls unter Windows.

Wer selbst einen Server besitzt, kommt ohne Clouddienst aus und kann mit einem simplen Bash-Wrapper wie zum Beispiel

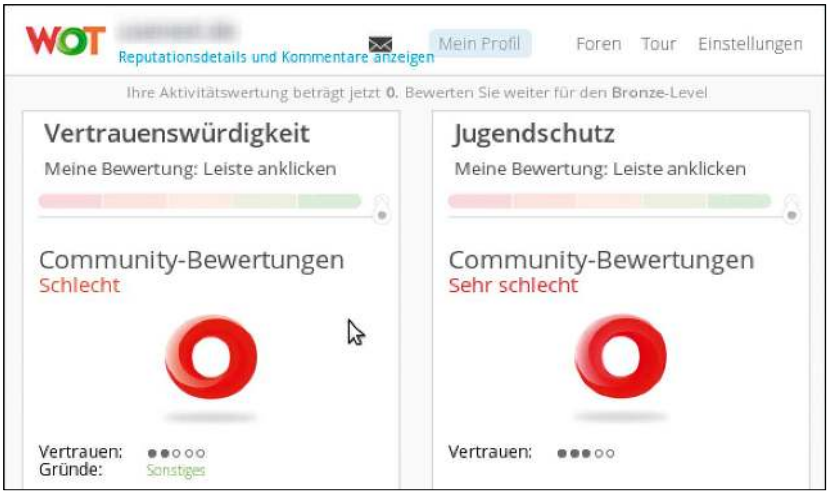
```
cd ~
curl -O ftp://server.de/ordner/
  [name].kbd --user
  ftpuser:ftpkennwort
keepassx ~/[name].kbd
curl -T [name].kbd ftp://server.
  de/ordner/[name].kbd --user
  ftpuser:ftpkennwort
```

dafür sorgen, dass Keepass immer die aktuelle Datenbank nutzt und Änderungen wieder auf den Server zurückschreibt. ●

Der sichere Browser

Moderne Browser filtern das Web und schützen vor gefährlichen Downloads und Webseiten. Dieser Beitrag erklärt elaboriertere Techniken in Chrome/Chromium und Firefox.

Von **Hermann Apfelböck**



WOT – Web of Trust: Die WOT-Erweiterung ist Pflicht für alle Browser. Bevor Sie auf eine der Community bekannte Betrügerseite geraten, kommt das große Stoppschild.

Sicherheit im Browser hat zwei Aspekte: Einmal geht es darum, das System vor Schadsoftware zu schützen, zweitens um den Schutz der privaten Daten und Kennwörter. Dieser Artikel erklärt Sicherheitsfunktionen für Firefox und Chrome/Chromium.

Insgesamt nehmen sich die beiden Browser in puncto Sicherheit nicht viel: Chrome schützt besser vor riskanten (Windows-)Downloads; Firefox bleibt unter Linux mit Masterpasswort und besserem Scriptschutz (mit Noscript) erste Wahl.

Schutzmechanismen von Chrome und Firefox

Firefox bietet unter „Extras -> Einstellungen -> Sicherheit“ drei Optionen, um betrügerische Webseiten zu blockieren. Hier sollten unter „Allgemein“ alle Kästchen aktiviert sein. Es handelt sich allerdings nur um einen Grundschutz, der unbedingt durch Add-ons erweitert werden sollte.

Chrome zeigt unter „Einstellungen -> Erweiterte Einstellungen anzeigen -> Datenschutz“ die Option „Mich und mein Gerät vor schädlichen Websites schützen“. Früher hieß diese Option technisch klarer „Phishing- und Malware-Schutz aktivieren“. Sie sorgt dafür, dass Chrome den Zugang auf gefährliche Sites blockiert und vor „ungewöhnlichen“ Downloads warnt. Ob es sich letztlich um eine harmlose Datei handelt, welche die Google-Datenbank nur nicht kennt, können Sie dann selbst entscheiden. Unter Linux ist dieser Downloadschutz nicht wirklich relevant.

Sicherheitserweiterungen für Firefox und Chrome

Bei den wichtigsten Sicherheitstools für Browser hat sich seit Jahren nichts Wesentliches geändert. Alle nachfolgend empfohlenen Browsererweiterungen finden und installieren Sie über „Add-ons“ in Firefox oder über „Einstellungen -> Erweiterungen“ in Chrome/Chromium.

WOT – Web of Trust: Rechtzeitig zu erkennen, dass eine Webseite betrügerisch ist, kann Gold und Geld wert sein. WOT basiert auf einer großen Communitydatenbank mit betrügerischen oder jugendgefährdenden Websites. Ist diese Erweiterung installiert, erhalten Sie schon bei der Google-Suche neben dem Link einen grünen oder roten Ring. Beim Zugang auf die Seite (direkt oder via Suchmaschine) erscheint eine deutliche Warnung, die Sie entweder ignorieren können oder zum Anlass nehmen, besser abzubrechen. WOT ist für jeden Browser unbedingt zu empfehlen, wenngleich es nicht nur technisch, sondern auch moralisierend filtert.

Noscript: Das Firefox-Add-on Noscript verhindert, dass Webseiten Javascript, Java oder andere ausführbare Inhalte automatisch starten. Sie haben die Kontrolle, ob solche Scripts starten dürfen. Das ist nicht immer bequem, da auf vielen interaktiven Seiten mit Formularen oder Votings die Scripts explizit erlaubt werden müssen. Einmal erlaubte Sites landen aber in der Whitelist und müssen später nicht mehr bestätigt werden.

Chrome zeigt unter „Einstellungen -> Erweiterte Einstellungen -> Inhaltseinstellungen -> JavaScript“ eine Option, Javascript generell zu verbieten. Das ist nicht praktikabel, da dann sehr viele interaktive Webseiten nicht mehr funktionieren (prominent etwa Google Drive, Google Store). Eine alltagstaugliche, mit Firefox-Noscript vergleichbare Lösung steht nach der Einstellung von Notscript 2014 aus: Die aktuell verfügbaren Add-ons

Kein Banking ohne grüne Adresse: Grünes „https:“ zeigt, dass PINs und TANs verschlüsselt übertragen werden.

„Noscript Suite Lite“, „ScriptSafe“, „ScriptBlock“ sind in Technik oder Bedienung allenfalls ausreichend.

HTTPS Everywhere: Die Erweiterung wählt, wo immer verfügbar, eine verschlüsselte HTTPS-Verbindung zu einer Website, auch wenn dies vom Benutzer nicht so angefordert wurde. Verschlüsseltes HTTPS ist vor allem bei Bankgeschäften und Einkäufen im Internet unverzichtbar, weil Sie Zugangsdaten oder Kreditkartendaten über das Netz versenden müssen. Der Browser zeigt eine verschlüsselte Verbindung zur zertifizierten Gegenstelle in der Adresszeile grün gefärbt. Verifizieren Sie das immer, bevor Sie Ihre Daten eingeben. Legen Sie ferner, um Irrtümer zu vermeiden, die Anmelde-URL Ihrer Bank als Lesezeichen ab und verwenden für den Zutritt ausschließlich dieses Lesezeichen.

Die Bedeutung des „Inkognito-Modus“

Das Browsen im „Inkognito-Fenster“ (Chrome) oder im „Privaten Fenster“ (Firefox) ist eine Datenschutzmaßnahme: Es vermeidet Surfspuren auf dem Rechner, die Mitbenutzer lesen könnten, zweitens unterbindet es den Großteil der Tracking-Schnüffelei der Website-Betreiber. Ein manchmal wichtiger Nebenaspekt ist ferner, dass Sie hier ohne Cookies und Webprotokolle unterwegs sind und daher neutrale und ungefilterte Ergebnisse erhalten (gelegentlich wichtig bei Suchmaschinen und Onlineshops). In Chrome und Firefox starten die Tastenkombinationen Strg-Umschalt-N und Strg-Umschalt-P am schnellsten ein privates Fenster.

„Inkognito“ Surfen bietet aber keinerlei technischen Schutz vor digitalen Schädlingen oder betrügerischen Webseiten. Es anonymisiert auch nicht die IP-Nummer und verschleiert keine strafbaren Handlungen.

Firefox-Masterpasswort: Diese Maßnahme schützt vor Datenklau auf dem lokalen Gerät. Das Masterpasswort ist nur einmal pro Firefox-Sitzung erforderlich.

Firefox: Masterpasswort gegen Datenklau

Jeder Browser fragt bei einer Webanmeldung nach, ob das Passwort gespeichert werden soll. Solches Speichern ist bequem, weil Sie sich das Passwort dann nicht länger merken müssen. Andererseits bedeutet das, dass jeder, der Zugriff auf Ihr Gerät hat, auch Ihre persönlichen Zugänge nutzen kann. Schlimmer noch: Unter „Einstellungen -> Sicherheit -> Gespeicherte Zugangsdaten“ lassen sich alle Kennwörter auch noch in Gesamtschau bequem auslesen.

Beim Firefox hilft das Masterpasswort, das Sie über „Firefox > Einstellungen > Sicherheit -> Master-Passwort verwenden“ einrichten. Das Masterpasswort schützt und verschlüsselt die in Firefox hinterlegten Webkennwörter. Der Komfortverlust dieser Sicherheitsmaßnahme ist vertretbar: Das Masterpasswort wird pro Firefox-Sitzung grundsätzlich nur einmal abgefragt, eventuell auch gar nicht, falls Sie keinen Zugriff auf die gespeicherten Kennwörter benötigen.

Skepsis gegenüber der Synchronisierung?

Die Browsersynchronisierung von Lesezeichen, Einstellungen, Erweiterungen bedeutet für Nutzer mehrerer Geräte einen unschätzbaren Komfort. Weniger erfreulich ist der Nebenaspekt, dass dabei Mengen von persönlichen Daten auf Google- oder Mozilla-Servern hinterlegt werden müssen.

Firefox: Der Mozilla-Browser verschlüsselt standardmäßig alle Daten, wobei der Schlüssel auf dem Gerät des Benutzers verbleibt. Generell darf die Mozilla-Foundation zu den „Guten“ gerechnet werden, die ein Auswerten von Nutzerdaten nicht selbst betreibt, sondern allenfalls zulassen muss.

Chrome/Chromium: Standardmäßig werden nur Kennwörter verschlüsselt. Aber unter „Einstellungen -> Erweiterte Synchronisierungseinstellungen“ (vorherige Google-Anmeldung vorausgesetzt) gibt es die zusätzliche Option „Alle synchronisierten Daten […] verschlüsseln“, bei der Sie ein individuelles Kennwort zur Sync-Verschlüsselung vergeben, das unabhängig vom Google-Kennwort ist. Der Komfortverlust ist nicht gravierend, da Sie dieses Kennwort auf jedem weiteren Gerät nur ein einziges Mal eingeben müssen. Alle Daten landen dann verschlüsselt auf dem Google-Server, der Schlüssel dazu (Kennwort) verbleibt auf dem lokalen Gerät.

Wohlgemerkt: Es handelt sich um eine Datenschutzmaßnahme gegen die Datenschnüffelei von Google. Die Maßnahme hilft nichts gegen Datenklau am lokalen Gerät. ●

Samba sicher einrichten

Samba ermöglicht den bequemen Datenaustausch zwischen allen Geräten im Netzwerk. Sicherheitsprobleme sind nicht zu befürchten, wenn Sie sich an ein paar einfache Regeln halten.

Von **Thorsten Eggeling**

Schon von Haus aus ist Samba so konfiguriert, dass nicht jeder einfach auf einen anderen PC zugreifen kann. Die Anmeldung mit dem Benutzernamen und Passwort ist in der Regel erforderlich. Für Gäste sind aber auch Freigaben ohne Authentifizierung möglich.

Samba-Server für Freigaben einrichten

Die Samba-Clientsoftware ist in populären Linux-Distributionen vorinstalliert, so dass Sie über den Dateimanager sofort auf Samba-Freigaben im Netzwerk zugreifen können. Die Serverkomponente ist in der Regel nicht installiert. Vor deren Einrichtung aktualisieren Sie zunächst das System:

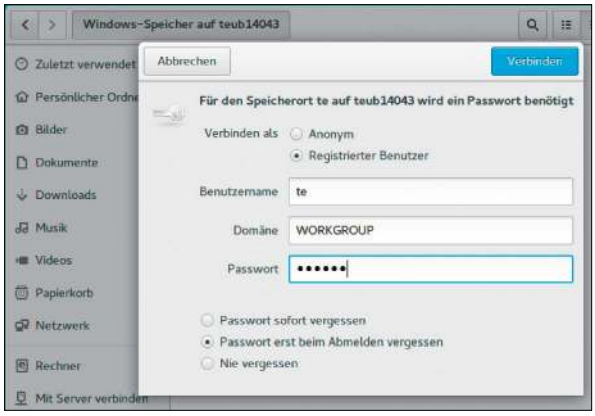
```
sudo apt update
sudo apt upgrade
```

Das ist vor allem bei Ubuntu 14.04 wichtig, weil Samba Programmbibliotheken einer bestimmten Version benötigt, etwa libtalloc2 2.1.5. Ist diese veraltet, kann der Serverprozess abstürzen. Installieren Sie dann Samba:

```
sudo apt-get install samba-common
  samba libpam-smbpass
```

Samba verwendet eigentlich eigene Passwörter, aber libpam-smbpass kann für den automatischen Abgleich der Samba- und Systempasswörter sorgen, wenn sich ein Nutzer bei Linux anmeldet oder sein Passwort ändert. Melden Sie sich daher jetzt ab und wieder an, damit das Passwort synchronisiert wird.

Unter neuestem Ubuntu 16.04 lassen Sie libpam-smbpass weg. Dieses Paket steht hier nicht zur Verfügung. Ohne libpam-smbpass müssen Sie mit



Passwortschutz: Auf dem Server müssen Sie für jeden Benutzer ein Samba-Passwort festlegen. Beim Zugriff fordert der Dateimanager Benutzernamen und Passwort an.

```
sudo smbpasswd -a [Benutzer]
```

neue Benutzer in die Samba-Konfiguration eintragen. Jeder Benutzer darf über *smbpasswd* sein eigenes Samba-Passwort unabhängig vom Systempasswort ändern. Um den Überblick zu behalten, sollten Sie auf allen PCs die gleiche Kombination von Benutzernamen und Passwörtern verwenden.

Serverkonfiguration und globale Freigaben

Samba verwendet die globale Konfigurationsdatei „/etc/samba/smb.conf“, die Sie mit jedem beliebigen Editor bearbeiten können:

```
sudo gedit /etc/samba/smb.conf
```

Ändern Sie im Abschnitt „[global]“ bei Bedarf den Namen der Arbeitsgruppe, zu der der Server gehören soll. Vorgegeben ist „workgroup = WORKGROUP“. Änderungen in der „smb.conf“ werden erst wirksam, wenn Sie den Samba-Service neu laden:

```
sudo service smbd restart
```

Home-Verzeichnisse freigeben: In der „smb.conf“ gibt es einen auskommentierten Abschnitt, der mit „;[homes]“ beginnt. Entfernen Sie die Kommentarzeichen („;“), wenn Sie alle Home-Verzeichnisse freigeben möchten. Soll auch der Schreibzugriff erlaubt sein, ändern Sie „read only = yes“ auf „read only = no“. Jeder authentifizierte Benutzer sieht beim Netzwerkzugriff nur sein eigenes Home-Verzeichnis.

Allgemeine Freigaben: Eine neue Freigabe lässt sich über diese drei Zeilen erstellen, die Sie am Ende der Datei „smb.conf“ einfügen:

```
[data]
path = /data
writeable = no
```

Hier wird das Verzeichnis „/data“ mit dem Freigabenamen „data“ freigegeben. Der Ordner muss existieren und die Benutzer müssen auf der Ebene des Dateisystems wenigstens Leserechte besitzen. Das ist standardmäßig der Fall, wenn Sie das Verzeichnis mit *sudo mkdir /data* erstellen. Dürfen auch Benutzer ohne Konto die Freigabe verwenden, so ergänzen Sie die Freigabe-Definition um „guest ok = yes“.

Freigaben mit Schreibberechtigung erstellen

Damit Benutzer Dateien über das Netzwerk neu erstellen oder ändern

können, genügt aus der Sicht von Samba die Änderung von „writeable = no“ auf „writeable = yes“. Das alleine reicht jedoch noch nicht für den vollen Zugriff aus. Der Ordner „/data“ im vorigen Beispiel gehört nämlich dem Benutzer und der Gruppe „root“, alle anderen Benutzer haben auf der Ebene des Dateisystems nur Leserechte. Um das zu ändern, verwenden Sie folgende vier Befehlszeilen:

```
sudo groupadd smbadmin
sudo chown -R root:smbadmin /data
sudo find /data -type d -exec ch
 mod 775 {} +
sudo find /data -type f -exec ch
 mod 664 {} +
```

Die letzten drei Befehle arbeiten rekursiv, berücksichtigen also alle unter „/data“ vorhanden Ordner und Dateien. Die neue Gruppe „smbadmin“ – die Bezeichnung können Sie frei wählen – und der Besitzer „root“ erhalten Vollzugriff, andere Benutzer und Gäste dürfen weiterhin nur lesen. Fügen Sie Ihr eigenes Benutzerkonto und weitere Konten, die eine Schreibberechtigung erhalten sollen, zur Gruppe „smbadmin“ hinzu:

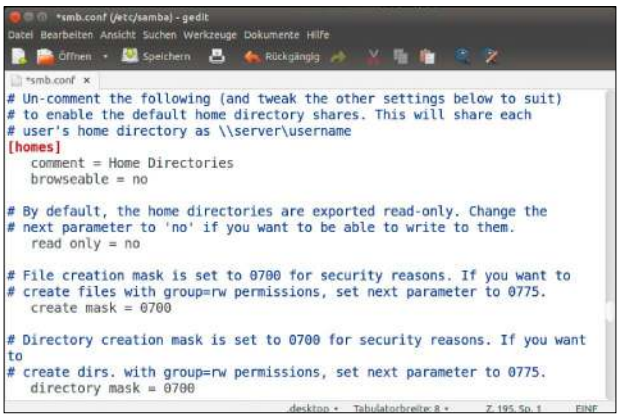
```
sudo usermod -aG smbadmin [Benut
 zer]
```

Den Platzhalter ersetzen Sie dabei jeweils durch den Benutzernamen. Melden Sie sich ab und wieder an, damit Linux die neue Gruppenzugehörigkeit berücksichtigt.

Eine Schreibberechtigung für Gäste ist in Kombination mit „guest ok = yes“ möglich, wenn Sie die lokalen Rechte für Ordner auf „777“ und für Dateien auf „666“ setzen.

Berechtigungen erhalten: Der Schreibzugriff durch mehrere Benutzer hat unerwünschte Nebenwirkungen. Erstellt ein Benutzer Dateien neu oder ändert er deren Inhalt, wird er zum Besitzer. Danach haben andere Benutzer dann nur noch Leserecht. Folgende Freigabedefinition löst dieses Problem:

```
[data]
path = /data
writeable = no
write list = @smbadmin
inherit owner = yes
```



Eigener Speicher: Freigaben für die Home-Verzeichnisse der Benutzer sind in der „smb.conf“ schon enthalten. Sie müssen nur die Kommentarzeichen entfernen.

```
force group = smbadmin
force directory mode = 770
create mask = 664
force create mode = 664
```

„write list = @smbadmin“ gewährt der Gruppe „smbadmin“ Schreibzugriff. Für alle anderen Benutzer und Gruppen bleibt es durch „writeable = no“ beim Lesezugriff. Die weiteren Optionen sorgen dafür, dass neu erstellte Elemente dem Besitzer des darüber liegenden Ordners („inherit owner“) sowie der Gruppe „smbadmin“ gehören und beide Vollzugriff erhalten.

Individuelle Benutzerfreigaben erlauben

Auch ohne root-Recht lassen sich eigene Ordner aus dem Home-Verzeichnis im Netzwerk freigeben. Die Berechtigung dazu haben unter Ubuntu alle Benutzer, die zur Gruppe „sambashare“ gehören. Mit

```
sudo usermod -aG sambashare [Be
 nutzer]
```

nehmen Sie weitere Benutzer in diese Gruppe auf, der Standardbenutzer ist

Benutzerfreigaben: Mitglieder der Gruppe „sambashare“ dürfen über den Dateimanager selbst Freigaben erstellen. Dabei ist für andere Benutzer auch der Schreibzugriff möglich.

bereits Mitglied. Im Dateimanager können Sie im Kontextmenü eines Ordners den Eintrag „Freigabe im lokalen Netzwerk“ wählen und die Freigabe aktivieren. Der Konfigurationsdialog bietet außerdem Optionen, über die sich der Schreibzugriff für alle authentifizierten Benutzer und Gäste aktivieren lässt. Wenn Sie aus Sicherheitsgründen die Freigabe für Gäste nicht ermöglichen wollen, tragen Sie in der Datei „smb.conf“ hinter „usershare allow guests =“ den Wert „no“ ein.

Samba-Freigaben und Passwortschutz

Samba-Freigaben sind nur im lokalen Netzwerk zu sehen und nicht über das Internet erreichbar. Ist ferner das WLAN über einen WPA-Schlüssel gut abgesichert, ist ein Datenzugriff von außen ausgeschlossen. Ist Ihr Netz für Fremde zugänglich, sollten Sie die Sicherheitsregeln für komplexe Passwörter einhalten. In einem privaten Netz genügen einfache Passwörter – eventuell können Sie mit einem Gastzugang auf die Authentifizierung ganz verzichten. Erlauben Sie den Schreibzugriff dennoch nur, wo es erforderlich ist. Bei Windows-Rechnern im Netz besteht immer die Gefahr, dass ein Trojaner Dateien auch auf Netzfreigaben verschlüsselt. Das funktioniert jedoch nur mit Schreibrecht des jeweiligen Benutzers.

Sicherer Datentransfer über das Netz

Linux kennt viele Methoden, um Dateien von einem Rechner auf einen anderen zu übertragen. Auch der verschlüsselte und damit sichere Transfer lässt sich schnell konfigurieren.

Von Thorsten Eggeling

Der Klassiker für den Datentransfer heißt FTP (File Transfer Protokoll). Allerdings bietet FTP von Haus aus keine Verschlüsselung und auch Benutzernamen und Passwörter gehen im Klartext über das Netzwerk. Es ist daher sicherer, den Datentransport verschlüsselt über SSH abzuwickeln (Secure Shell) – vor allem dann, wenn ein Server auch aus dem Internet erreichbar ist.

Open-SSH-Server für den Fernzugriff einrichten

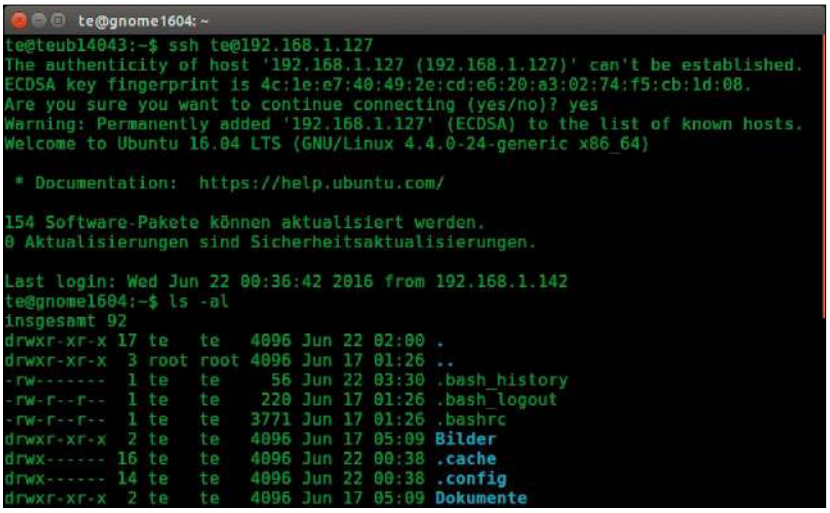
Der Open-SSH-Server ist Voraussetzung für den Zugriff auf die Linux-Shell und den Dateitransfer über das Netzwerk. Ein SSH-Client ist bei allen Linux-Distributionen standardmäßig installiert. Der SSH-Server fehlt jedoch oft, so etwa bei Ubuntu. Zur Installation genügen unter Ubuntu/Debian folgende Befehlszeilen:

```
sudo apt-get update
sudo apt-get install openssh-ser
 ver
```

Am einfachsten ist es, die Serversoftware auf allen Linux-PCs im Netzwerk einzurichten. Dann ist der Datenaustausch in alle Richtungen möglich. Nach erfolgter Installation ist der Open-SSH-Server standardmäßig aktiviert. Probieren Sie die Funktion auf dem Server oder einem anderen Linux-Rechner im Netzwerk aus, indem Sie auf der Kommandozeile

```
ssh [benutzer]@[hostname]
```

eingeben, wobei Sie die Stellvertreter durch den tatsächlichen Kontonamen und den Hostnamen (die IP-geht auch) ersetzen. Beim allerersten Zugriff ist dem Client der Server noch nicht bekannt und Sie müssen die Verbindung mit „yes“ bestätigen. Tippen Sie Ihr Passwort für die Anmeldung auf dem Server ein und bestätigen Sie mit der Eingabetaste. Beenden Sie die SSH-Verbindung mit *exit*. Wenn der Zugriff über ssh funktioniert hat, ist das System auch bereit für den Dateitransfer über SFTP.



Fernzugriff: Über ssh stellen Sie die Verbindung zu einem anderen Linux PC her. Im Terminalfenster können Sie dann so arbeiten, als ob Sie vor dem entfernten PC säßen.

SCP und SFTP auf der Kommandozeile

Der Open-SSH-Server bietet nicht nur den Shellzugang, sondern auch zwei Methoden für den Dateitransfer an. SCP (Secure Copy Protocol) kommt meist dann zu Einsatz, wenn einzelne Dateien übertragen werden sollen, etwa für Backups.

SFTP (Secure File Transfer Protocol) orientiert sich dagegen an FTP und erlaubt der Clientsoftware komplexere Kommandos, etwa zur Anzeige von Verzeichnisinhalten. Das Tool scp lässt sich wie folgt nutzen:

```
scp test.tar.gz [benutzer]@[host
 name]:~/
```

Dies lädt die Datei „test.tar.gz“ aus dem aktuellen Verzeichnis in das Home-Verzeichnis auf dem Server hoch. Die Stellvertreter ersetzen Sie durch den Benutzernamen und den Namen des PCs, auf den Sie die Datei übertragen wollen. scp funktioniert ähnlich wie cp in der allgemeinen Form „scp Quelle Ziel“ in beide Richtungen. scp kann auch Wildcards wie „*“ verarbeiten. Folgender Befehl ko-

piert alle PNG-Dateien unter „~/Bilder „auf den Server:

```
scp ~/Bilder/*.png [benutzer]@
  [hostname]:~/Bilder
```

Das Tool sftp ist eine Alternative zu scp. Sie starten es mit

```
sftp [benutzer]@[hostname]
```

und melden sich mit Ihrem Passwort an. sftp arbeitet interaktiv. *help* liefert eine Übersicht der verfügbaren Kommandos. Befehle wie *ls* und *cd* oder auch die automatische Ergänzung mit der Tab-Taste arbeiten wie in einer lokalen Shell. Das Kopieren erfolgt mit *get* (Download) und *put* (Upload).

SFTP mounten: Ordner eines SSH/SFTP-Servers lassen sich über Fuse (Filesystem in Userspace) auch direkt in das lokale Dateisystem einbinden, wenn die nötige Software sshfs installiert ist:

```
sudo apt-get install sshfs
```

Damit ein Benutzer ohne root-Rechte Fuse nutzen darf, fügen Sie ihn mit

```
sudo usermod -aG fuse Benutzer
```

zur Gruppe „fuse“ hinzu. „Benutzer“ ersetzen Sie durch den tatsächlichen Anmeldenamen. Melden Sie sich ab und wieder an. Danach können Sie das Dateisystem mit

```
mkdir ~/fusessh
sshfs Benutzer@Server.de:/Pfad ~/
  fusessh
```

lokal einhängen und mit *fusermount -u ~/fusessh* jederzeit wieder lösen.

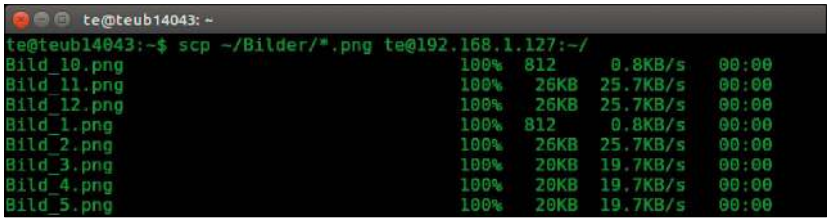
SSH und Dateitransfer ohne Passwort

Bei einer Verbindung per SSH besteht die Möglichkeit, sich über einen Schlüssel zu autorisieren. Das ist sicherer und erspart die Passworteingabe – auch bei scp und sftp. Erstellen Sie über folgenden Befehl einen Schlüssel für SSH auf dem Client-PC:

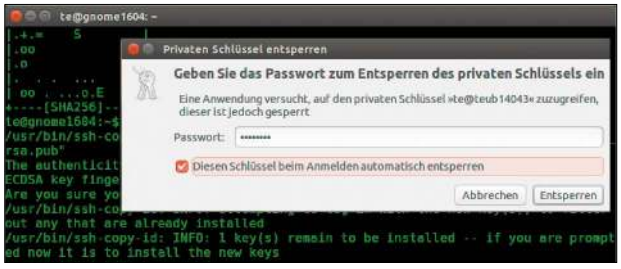
```
ssh-keygen -t rsa -b 4096
```

Bestätigen Sie die Vorgabe für den Schlüsselnamen „~/.ssh/id_rsa.pub“ mit der Eingabetaste und tippen Sie ein Passwort zum Schutz des Schlüssels ein. Anschließend kopieren Sie den öffentlichen Schlüssel „id_rsa.pub“ auf den Server:

```
ssh-copy-id -i ~/.ssh/id_rsa.pub
  [benutzer]@[hostname]
```



Dateien übertragen: Mit scp kopieren Sie Dateien über das Netzwerk. Per Wildcard („*.png“) lassen sich mehrere Dateien auswählen, die dem Muster entsprechen.



Ohne Passwort: Erzeugen Sie den Schlüssel auf dem Client und übertragen Sie ihn auf den Server. Das Passwort müssen Sie nur einmal eingeben.

Diese Aktion bestätigen Sie mit dem regulären Anmeldepasswort. Starten Sie dann eine SSH-Sitzung:

```
ssh [benutzer]@[hostname]
```

Das System fragt nach dem eben vergebenen Passwort für den Schlüssel. Setzen Sie ein Häkchen vor „Diesen Schlüssel beim Anmelden automatisch entsperren“, damit Sie das Passwort nicht wieder eingeben müssen. Solche Anmeldung per Schlüssel ist auch für Server empfehlenswert, die über das Internet erreichbar sind. Angreifer haben dann kaum eine Chance, sofern Sie die Anmeldung mit Passwort ausdrücklich verhindern. Dazu öffnen Sie als root die Datei „/etc/ssh/sshd_config“ in einem Editor und ergänzen oder ändern dort die folgenden Optionen:

```
PasswordAuthentication no
UsePAM no
```

Die Änderung gilt erst, nachdem Sie mit *sudo /etc/init.d/ssh reload* die Konfiguration neu einlesen.

Verwendung von SFTP einschränken

Standardmäßig hat jedes Benutzerkonto SSH- und SFTP-Zugriff. Sie können aber für einzelne Benutzer oder Gruppen den Shellzugang über SSH verbieten und SFTP auf ein bestimmtes Verzeichnis beschränken, etwa für den Datenaustausch mit Mitarbeitern. Dazu öffnen Sie die Datei „/etc/ssh/sshd_config“ als root in einem Editor und fügen am Ende diese sechs Zeilen an:

```
Match Group sftpgroup
ChrootDirectory /home/sftphome
ForceCommand internal-sftp
AllowTcpForwarding no
PermitTunnel no
X11Forwarding no
```

Erstellen Sie mit *addgroup sftpgroup* eine neue Gruppe und mit den folgenden fünf Zeilen einen neuen Benutzer mit Passwort sowie das Verzeichnis „/home/sftphome“ mit den erforderlichen Rechten:

```
sudo useradd -s /bin/false -g
  sftpgroup sftpuser
sudo passwd sftpuser
sudo mkdir /home/sftphome
sudo chown root:root
  /home/sftphome
sudo chmod 755 /home/sftphome
```

Der Benutzer sftpuser kann sich jetzt über einen SFTP-Client anmelden und Dateien aus „/home/sftphome“ herunterladen. Wenn er auch Dateien hochladen soll, führen Sie diese Befehle aus:

```
mkdir /home/sftphome/upload
chown root:sftpgroup /home/sft
  phome/upload
chmod 775 /home/sftphome/upload
```

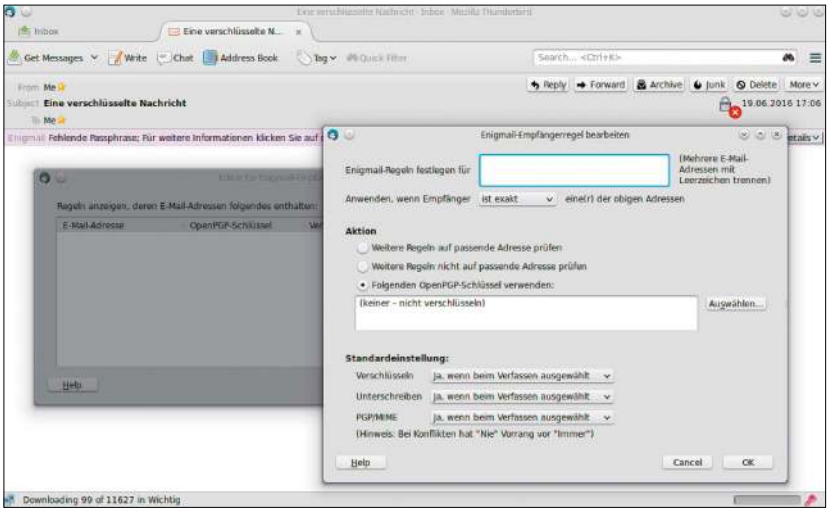
Damit erhalten Mitglieder der Gruppe sftpgroup Schreibrechte unter „/home/sftphome/upload“. Eine Anmeldung über SSH ist für diese Gruppe nicht möglich. ●

Sichere Post mit Thunderbird

Vertrauliche Informationen per E-Mail zu verschicken, ist keine gute Idee. Obwohl das die meisten Anwender wissen, machen sich nur wenige die Mühe, ihre elektronische Post zu verschlüsseln. Dabei ist das unter Linux wirklich einfach.

Von **Stephan Lamprecht**

Wer Mitleser seiner E-Mails ausschließen will, sollte sich mit dem Thema Verschlüsselung beschäftigen. Dank einer durchdachten Software als Ergänzung zum E-Mail-Programm Thunderbird ist die Einrichtung einer wirkungsvollen Chiffrierung der Mails kein Problem.



GPG und Thunderbird einrichten

Auf den meisten Linux-Systemen ist bereits das Programm GNU Privacy Guard (Gnu PG) standardmäßig installiert. Es verwendet für die Chiffrierung zwei Schlüssel: Der öffentliche Schlüssel eines Empfängers wird vom Absender dafür genutzt, eine Nachricht an den Adressaten zu verschlüsseln. Die codierte Botschaft entschlüsselt der Empfänger mit seinem geheimen privaten Schlüssel. Anders als beim Verfahren S/MIME, das mit GPG nicht kompatibel ist, kümmert sich hier keine zentrale Instanz um die Herausgabe von Schlüsseln und Zertifikaten. GPG ist dezentral organisiert. Die Nutzer vertrauen sich untereinander.

Die Erweiterung Enigmail integriert sich nahtlos in das Mailprogramm Thunderbird. Es setzt ein installiertes GPG voraus. Falls dies fehlt, wird der Nutzer bei der Einrichtung des Programms aber darüber informiert. Dann kann die Basiskomponente jederzeit mittels des Befehls

```
sudo apt-get install gnupg
```

nachinstalliert werden. Um Enigmail zu installieren, klicken Sie in Thunderbird auf die Menüschaltfläche und wählen „Add-ons“ aus. Geben Sie danach „Enigmail“ in das Suchfeld ein und installieren Sie die Erweiterung. Daraufhin muss Thunderbird einmal neu gestartet werden. Nach dem Neustart begrüßt das Programm den Anwender mit einem Einrichtungsassistenten. Entscheiden Sie sich hier für „Ausführliche Konfiguration“.

Im ersten Schritt geben Sie Ihre „Passphrase“ ein. Dieses Passwort benötigen Sie später, um auf Ihre Schlüssel zugreifen zu können. Es bildet auch die Grundlage für die Schlüssel selbst. Nutzen Sie daher ein möglichst sicheres und langes Passwort. Nach der doppelten Eingabe beginnt Enigmail damit, das notwendige Schlüsselpaar anzulegen. Dieser Vorgang dauert eine Weile. Arbeiten Sie in dieser Zeit einfach normal mit dem System weiter. Ist der Vorgang abgeschlossen, blendet Enigmail einen Dialog ein, um ein Zertifikat für die Entsperrung des Schlüssels anzulegen. Auch dies wird mit einer Passphrase gesichert. Vergleichbar mit der PUK einer SIM-Karte dient es dazu, erneut an den Schlüssel heranzukommen, falls Sie die ursprüngliche Passphrase vergessen haben sollten. Ist dieser Schritt erledigt, können Sie die Software sofort einsetzen.

Nachrichten verschlüsseln und signieren

Dank Enigmail können Sie in Thunderbird Ihre Nachrichten signieren und verschlüsseln. Öffnen Sie dort wie gewohnt den Editor zum Verfassen von Nachrichten. Dort hat Enigmail jetzt eine weitere Symbolleiste platziert. Um Ihre E-Mail zu signieren, um damit zu beweisen, dass diese tatsäch-

lich von Ihnen stammt, genügt es, auf das Stiftsymbol zu klicken. Drücken Sie dann später auf „Senden“, bittet Enigmail um die Eingabe Ihrer Passphrase, um den Zugriff auf die Schlüssel zu erlauben. Damit der Empfänger die Signatur überprüfen kann, muss er Ihren öffentlichen Schlüssel in seiner Schlüsselverwaltung importiert haben. Kann der Schlüssel einer signierten E-Mail bestätigt werden, weist Enigmail den Nutzer direkt im Header der Nachricht darauf hin.

Möchten Sie eine ausgehende E-Mail verschlüsseln, benötigen Sie den öffentlichen Schlüssel des Empfängers. Diesen kopieren Sie beispielsweise in eine Textdatei. Über das Menü „Enigmail, Schlüssel verwalten“ rufen Sie sich dann den Schlüsselbund auf. Dort nutzen Sie aus dem Menü „Datei“ das Kommando „Importieren“ und wählen die Datei aus. Nach erfolgreichem Import ist der Empfänger dem System bekannt und sein Schlüssel kann für Chiffrierung verwendet werden. Im Editor klicken Sie beim Verfassen der Nachricht dann auf das Symbol mit dem Schloss. Wird die Mail versendet, müssen Sie wieder Ihre Passphrase eingeben.

Erhalten Sie umgekehrt eine E-Mail, die verschlüsselt wurde, erkennt Enigmail das automatisch. Wenn Sie im Vorschaubereich von Thunderbird auf das Element klicken, werden Sie dazu aufgefordert, Ihre Passphrase einzutragen. Wenige Augenblicke später erscheint die Nachricht.

GPG verschlüsselt auch lokale Dokumente

Praktischerweise kann GPG auch lokal Dateien verschlüsseln. Dazu nutzen Sie das Terminal und Ihren persönlichen Schlüssel:

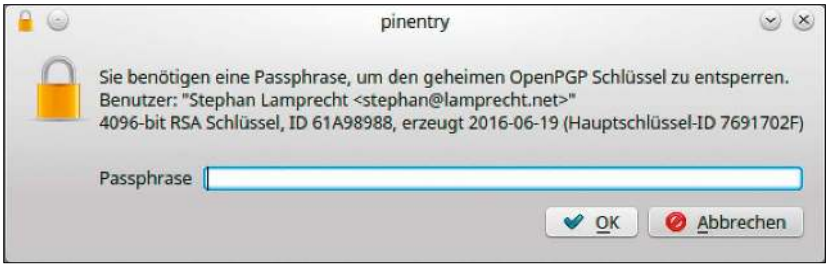
```
gpg -e -r stephan@tld.de [Datei]
```

Dies macht den Inhalt der Datei unlesbar. Der Parameter „-e“ kümmert sich um die Chiffrierung, während Sie mit „-r“ den öffentlichen Schlüssel angeben, der verwendet werden soll. Auf die gleiche Weise könnten Sie auch Dateien verschlüsseln, die nur vom jeweiligen Empfänger entschlüsselt werden können. Beim Entschlüsseln einer Datei müssen Sie beachten, dass das System versuchen wird, deren Inhalt direkt im Terminal anzuzeigen. Um stattdessen eine Datei zu erhalten, muss die Ausgabe umgeleitet werden:

```
gpg -d -r stephan@tld.de [Ver
  schlüsselte Datei] > [Entschlüs
  selte Datei]
```

Der Parameter „d“ steht für das Entschlüsseln (Decrypt).

Ein Einrichtungsassistent begleitet Sie durch die Erstellung Ihrer Schlüssel. Während der Anlage der Schlüssel nutzen Sie den Rechner einfach weiter.



Passphrase-Abfrage: Erhalten Sie eine verschlüsselte Mail ,werden Sie automatisch dazu aufgefordert, das Kennwort einzugeben, um den Klartext sichtbar zu machen.

Schlüsselserver und -export auf die Homepage

Damit Ihnen andere Personen eine verschlüsselte Nachricht schicken können, müssen diese ebenfalls GPG einsetzen und zur Verschlüsselung Ihren öffentlichen Schlüssel verwenden. Enigmail ergänzt Thunderbird um die praktische Funktion, den öffentlichen Schlüssel auch per E-Mail zu versenden. Um den Schlüsselaustausch weiter zu erleichtern, existiert ein Netz an Schlüsselservern, auf denen öffentliche Schlüssel geladen werden können. Um dort nach Schlüsseln anderer suchen oder Ihren eigenen Schlüssel zu hinterlegen, rufen Sie die Schlüsselverwaltung von Enigmail auf. Markieren Sie Ihren eigenen Schlüssel und nutzen Sie „Schlüssel hochladen“ aus dem Menü „Schlüsselserver“. Der Vorgang dauert nur einen Augenblick. Aus dem gleichen Menü können Sie mit „Schlüssel suchen“ nach den Mailadressen von Korrespondenzpartnern suchen, um sich deren Schlüssel zu importieren. Dazu genügt es, einen Treffer mit der Maus anzuwählen und den Dialog mit „OK“ wieder zu verlassen.

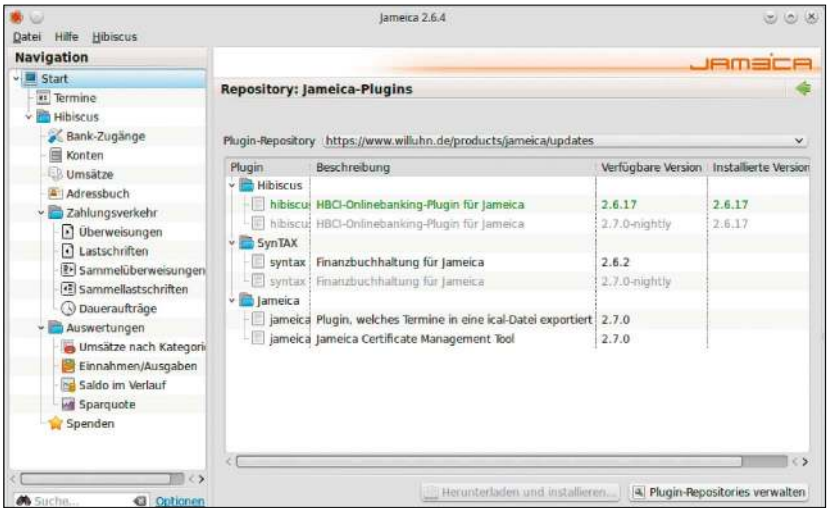
Sie können den öffentlichen Schlüssel zusätzlich auf Ihrer Homepage veröffentlichen. So erreichen Sie auch Personen, mit denen Sie noch keinen Kontakt hatten. Klicken Sie dazu in Thunderbird auf „Enigmail -> Schlüssel verwalten“, dort markieren Sie Ihren eigenen Schlüssel und wählen aus dem Menü „Datei“ den Eintrag „Exportieren“. Das Programm fragt nun, welche Schlüsselart exportiert werden soll, was Sie mit „Nur öffentliche Schlüssel exportieren“ beantworten. Die exportierte Datei legen Sie dann in einem Verzeichnis Ihrer Wahl auf Ihrer Homepage ab. ●

Sicheres Banking mit Linux

Für die meisten Kunden gehört der Besuch einer Bank heute eher zu den Ausnahmen. Bargeld stellen Automaten bereit und der bargeldlose Zahlungsverkehr wird online abgewickelt – trotz potenzieller Sicherheitsrisiken.

Von **Stephan Lamprecht**

Das Girokonto ist für den Kunden bequem und notwendig, für das Kreditinstitut aber ein Kostentreiber, der sich betriebswirtschaftlich nicht lohnt. Daher haben Banken und Sparkassen in den vergangenen 20 Jahren alles unternommen, um den Aufwand zu reduzieren. In SB-Service-Bereichen besorgen sich die Kunden Bargeld aus dem Automaten und geben in Terminals Überweisungen und Daueraufträge ein. Wer das noch bequemer möchte, entscheidet sich für das Onlinebanking seines Instituts.



Das Homebankingprogramm Hibiscus ist als Plug-in umgesetzt: Voraussetzung ist die Software Jameica, die wiederum eine Java-Umgebung benötigt.

Aktuelle Sicherheitsverfahren

Beim Thema Onlinebanking wird das HBCI-Verfahren meist als die sicherste Form des Bankings gepriesen. Oft klingt es so, als genüge die Entscheidung für HBCI – und schon könne nichts mehr passieren. Ganz so einfach ist es nicht. Tatsächlich gehört HBCI zu den Verfahren, die viel Sicherheit eingebaut haben. Allerdings ist es kaum verbreitet und wird von vielen Instituten nur noch auf Nachfrage angeboten. Ernstzunehmende Schätzungen der Universität Tübingen gehen davon aus, dass HBCI nur einen Marktanteil von sechs Prozent besitzt. Fast die Hälfte der Transaktionen wird heute mit SMS-TANs abgesichert. Hier werden die Transaktionen im Back-End der Bank vorbereitet und der Server des Instituts versendet eine SMS mit der TAN, die dann wieder in den Dialog des Servers eingetragen werden muss. Das ist bequem und schnell – ist es auch sicher?

Unterstellt, dass die Server der Bank nicht kompromittiert werden können, lauern die größten Gefahren auf dem System des Nutzers und auf der Wegstrecke zwischen dem Computer des Bankkunden und dem Server des Instituts. Auf dem System des Nutzers können Keylogger und Trojaner die Eingabe der Tastatur damit Transaktionsnummern und PINs abfangen. Auf der Wegstrecke zwischen den beteiligten Systemen wäre ein sogenannter Man-in-the-middle-Angriff denkbar, der die übermittelten Daten abfängt, manipuliert und dann erst an den Bankserver weiterleitet. Und hier lauern auch Gefahren für das HBCI-Verfahren in seinen ersten Entwicklungsstufen. Bei der ersten Generation wurden einfache Chipkartenleser genutzt. Die Eingabe des notwendigen Schlüssels zum Zugriff erfolgt über die Tastatur des Computers. Diese Zahlen können von Trojanern aber ausgelesen werden. Die zweite Generation der Chipkartenlesegeräte besitzt ein eigenes Eingabefeld. Ein Keylogger geht in diesem Fall also leer aus, der Nutzer erhält aber keine Rückmeldung, ob die richtige Überweisung (Betrag, Konto) erfolgt ist, da kein Display enthalten ist. Ein Man-in-Middle-Angriff ist also nicht völlig auszuschließen. Erst die Lesegeräte der dritten Generation, die über ein Display verfügen, gelten als sicher gegenüber Trojanern.

HBCI unter Linux mit Hibiscus

Kommerzielle Hersteller von Homebankingprogrammen haben Linux

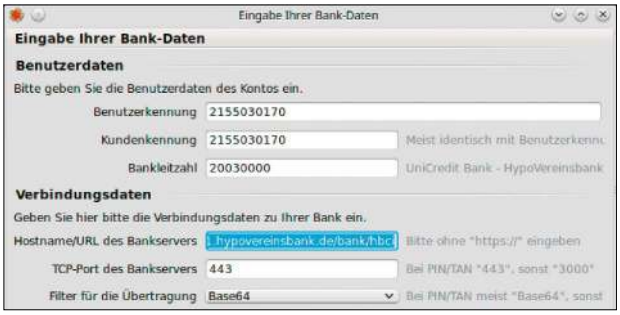
lange vernachlässigt. Als letzter Vertreter eines kommerziellen Herstellers ist das Unternehmen Matrica mit seiner Software Moneyplex übrig geblieben. Aber es gibt eine Reihe von freien Alternativen. Eine der bekannteren ist Gnucash, das auch mit HBCI nachgerüstet werden kann. Allerdings verlangt Gnucash einiges an Einarbeitung ab, schließlich ist es ursprünglich als Buchführungsprogramm konzipiert worden.

Einfacher geht es mit der Software Hibiscus, die alle wesentlichen Funktionen des Onlinebankings mitbringt und Kontostandsabfragen und Überweisungen nach HBCI-Standard ermöglicht. Ist das Konto HBCI-fähig, ist die Einrichtung von Hibiscus nicht schwer. Es setzt Java voraus: Kontrollieren Sie im Terminal mit *which java*, ob Java installiert ist. Falls nicht, holen Sie das mit

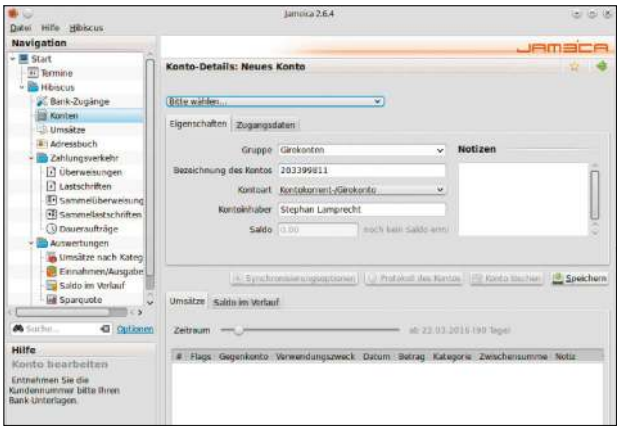
```
sudo apt-get install java
```

nach. Laden Sie sich dann von *https://www.willuhn.de/products/hibiscus/download.php* die Software Jameica herunter. Es handelt sich um ein einfaches ZIP-Archiv, dessen Inhalt Sie an einer beliebigen Stelle des Systems entpacken. Achten Sie nur darauf, dass die Verzeichnisstruktur des Archivs erhalten bleibt. Starten Sie Jameica mit einem Doppelklick auf das Shellscript „jameica.sh“ in dem Ordner, in dem Sie das Archiv entpackt haben. Gehen Sie dann auf „Datei -> Plugins online suchen“ und markieren Sie dort „hibiscus“. Laden Sie sich diese Erweiterung herunter und installieren Sie diese.

Beim ersten Start müssen Sie ein Verzeichnis auswählen, in das die Benutzerdaten abgelegt werden. Ist das Plugin installiert, starten Sie Jameica neu. Dort finden Sie dann den neuen Eintrag „Hibiscus“. Darin legen Sie über „Bank-Zugänge“ ein Bankkonto an. Sie müssen lediglich Ihre Bankleitzahl wissen und welche Absicherung Sie verwenden (Chipkarte, PIN/TAN). Der Assistent hilft bei der weiteren Einrichtung. Am Ende ist das Konto erfolgreich angelegt und steht damit zur Bearbeitung zur Verfügung.



Die Einrichtung eines Kontos in Hibiscus ist nicht schwierig: Sie müssen nur Ihr Sicherheitsverfahren kennen und die eigene Bankleitzahl.



Neue Bankkonten können aus den HBCI-Daten ausgelesen und eingerichtet werden. Sie lassen sich aber auch manuell anlegen.

Die Benutzeroberfläche von Hibiscus ist einfach. Alle Funktionen finden Sie in der übersichtlichen Baumstruktur auf der linken Seite. Darüber erreichen Sie die Bereiche für den Zahlungsverkehr, der Ihnen auch die Anlage von Daueraufträgen und deren Verwaltung erlaubt. Welche Funktionen Sie bei Ihrer Bank nutzen können, ist aber vom Kreditinstitut abhängig. Es muss beispielsweise eine „Änderung eines Dauerauftrags“ online anbieten, damit Hibiscus darauf zugreifen kann.

Live-CD als sichere Alternative

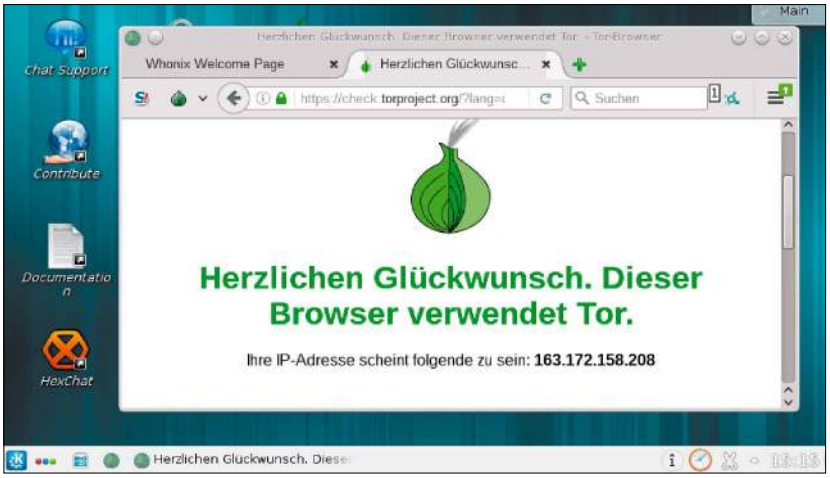
Sie gehören zu den Bankkunden, die Überweisungen und Umsatzabfragen direkt im Browser ohne HBCI erledigen? In diesem Fall ist der Browser die wichtigste Schnittstelle zur Bank. Die Kreditwirtschaft war in den vergangenen Jahren recht kreativ, was die Entwicklung von Sicherheitsverfahren anbelangt. Neben dem bereits erwähnten Verfahren mit der mobilen TAN (als SMS) gibt es Methoden, bei denen eine TAN mit einem externen Gerät erzeugt wird. Oder ein Code auf der Seite der Bank muss mit der Smartphone-Kamera fotografiert werden. Einige dieser Verfahren gelten bei Sicherheitsexperten zumindest als angreifbar. Eine der Schwachstellen ist hier der Browser, dessen Sicherheitslücken potenzielle Angreifer ausnutzen könnten.

Voraussetzung bei allen bisher bekannten Angriffsmethoden ist immer, dass vorher schädlicher Code auf dem System eingeschleust wurde. Dazu muss der Trojaner einen permanenten Platz auf der Festplatte haben und sich automatisch laden. Daher haben Schädlinge keine Chance, wenn Sie Bankgeschäfte mit einer schreibgeschützten Live-CD erledigen. Für Downloads etwa von elektronischen Kontoauszügen lässt sich ein zusätzlicher USB-Stick verwenden. Eine besonders geeignete Distribution ist etwa das bekannte Tails (*https://tails.boum.org/index.de.html*), das besonderen Wert auf sichere Komponenten legt. Im Prinzip minimiert aber jedes beliebige Livesystem wie etwa ein Knoppix (*www.knoppix.org*) alle Risiken drastisch. Absolute Sicherheit wird es beim Onlinebanking technisch nie geben. ●

Anonym und sicher im Netz

Völlige Anonymität kann es im Internet nicht geben. Sie können aber so viele Informationen wie möglich verbergen. Dabei helfen spezialisierte und seit Jahren bewährte Linux-Systeme.

Von **Thorsten Eggeling**



Tor-Netzwerk zur Anonymisierung: Tails und Whonix fußen auf Tor. Der Datenverkehr in diesem Netzwerk geht immer über drei Zwischenstationen zum Ziel und wieder zurück.

Im Internet hinterlässt Ihr Rechner Spuren. Sobald Sie eine Webseite öffnen, erfasst der Webserver Ihre IP-Adresse und protokolliert, welche Seiten Sie aufrufen. Anhand typischer Merkmale von Betriebssystem und Browser können beispielsweise Werbenetzwerke Ihren PC wiedererkennen und Ihren Weg durch das Internet verfolgen. Webseiten speichern auf dem PC zudem Informationen in Cookies. Das ist manchmal technisch notwendig, etwa für die Authentifizierung des Benutzers, kann aber auch zur Steuerung personalisierter Werbung genutzt werden.

Wem es vor allem in bestimmten Situationen auf mehr Privatsphäre ankommt, etwa bei der Nutzung fremder WLANs im Urlaub oder eines Gastzugangs im Firmennetzwerk, greift am besten zu einem auf Sicherheit spezialisierten Linux-Livesystem. Das lässt sich von DVD, USB-Stick oder in einer virtuellen Maschine starten.

Tails: Anonym und spurlos surfen

Tails (*https://tails.boum.org*) ist ein Linux-System, das auf anonymisiertes Surfen im Web spezialisiert ist. Die Anonymisierung läuft über das Tor-Netzwerk (*www.torproject.org*). Alle übertragenen Daten werden verschlüsselt und über mehrere Server des Netzwerks geleitet, bevor sie über einen Endpunkt ins offene Internet beziehungsweise zurück auf Ihren PC gelangen. Eine logische Einschränkung ist allerdings, dass die Geschwindigkeit der Datenübertragung darunter leidet. Das Laden von Webseiten und Dateien dauert deutlich länger.

Tails herunterladen und installieren: Tails gibt es als ISO-Datei zum Download, aus der Sie eine bootfähige DVD brennen. Oder Sie verwenden einen USB-Stick. Gehen Sie auf *https://tails.boum.org* und klicken Sie auf „Installieren Sie Tails 2.4“. Folgen Sie den Anweisungen des Assistenten, der Ihnen die unterschiedlichen Installationsvarianten erklärt. Für Debian und Ubuntu beispielsweise gibt es einen Tails-Installer, der das System auf einen USB-Stick kopiert und bei Bedarf auch aktualisieren kann. Am einfachsten ist es, Tails über *www.pcwelt.de/5ozMAb* herunterzuladen und aus der ISO-Datei mit folgender Befehlszeile einen bootfähigen USB-Stick zu erstellen:

```
sudo dd if='~/Downloads/tails-
  i386-2.4.iso' of=/dev/sd[x]
  bs=16M && sync
```

Passen Sie den Pfad zur ISO-Datei und die Datenträgerkennung für Ihr System an. Der Inhalt des Sticks wird dabei überschrieben, alle darauf befindlichen Dateien gehen verloren. Ein auf diesem Weg erstellter Stick kann jedoch nicht als Speicher für Benutzerdaten dienen, was aus Sicherheitsgründen vielleicht auch unerwünscht ist. Wenn Sie etwa die Netzwerkkonfiguration und persönliche Dateien trotzdem speichern möchten, benötigen Sie einen zweiten USB-Stick.

Über das Menü „Anwendungen“ und „Tails -> Tails Installer“ starten Sie ein Tool, über das Sie Tails auf den Stick kopieren. Wenn Sie das System von diesem starten, lässt sich über „Anwendungen -> Tails -> Configure

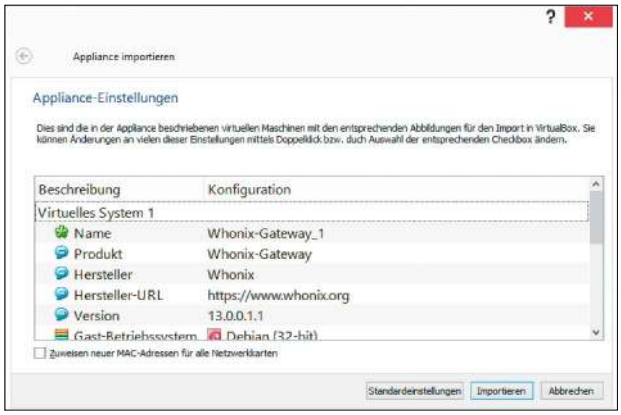
persistent volume“ ein permanenter Datenspeicher einrichten.

Tails verwenden: Booten Sie den PC von der Tails-DVD oder dem Tails-Stick. Sobald das Fenster „Welcome to Tails“ erscheint, können Sie in die Leiste am unteren Bildschirmrand „Deutsch“ als Sprache auswählen. Klicken Sie auf „Anmelden“. Über das Ausklappmenü rechts oben stellen Sie eine Verbindung zum WLAN-Netz her. Ist der PC über ein Ethernet-Kabel angeschlossen, erfolgt der Verbindungsaufbau automatisch. Warten Sie, bis das Kreuz beim Tor-Symbol (Zwiebel) in der Leiste verschwunden ist. Dann besteht eine Verbindung zum Tor-Netzwerk.

Die für die Nutzung von Tor nötige Software ist in Tails bereits vorkonfiguriert enthalten. Der mitgelieferte Tor-Browser basiert auf Firefox und ist ebenfalls für das Tor-Netzwerk konfiguriert. Sie starten ihn über „Anwendungen -> Internet -> Tor-Browser“. Auf der Startseite klicken Sie auf „Verbindung testen“. Sie sehen dann Ihre öffentliche IP-Nummer aus dem Tor-Netzwerk, die sich von der öffentlichen IP Ihres DSL-Routers unterscheidet. Klicken Sie in der Symbolleiste des Browsers auf das Zwiebel-Symbol und wählen Sie im Menü „Neuer Kanal für diese Seite“. Die Seite lädt neu und zeigt eine andere IP-Nummer an.

Whonix: Anonymität und sicheres System

Whonix (*www.whonix.org*) verwendet wie Tails das Tor-Netz zur Verschleierung der IP-Adresse im Internet. Der Ansatz geht jedoch noch ein Stück weiter. Whonix besteht aus zwei getrennten Betriebssystemen: Im Whonix-Gateway läuft die Tor-Instanz, die den gesamten Datenverkehr über das Tor-Netzwerk abwickelt. Das System ist außerdem durch eine Firewall und eine besonders sichere Konfiguration geschützt. Das zweite System, Whonix-Workstation, kann nur über Whonix-Gateway mit dem Internet Daten austauschen und enthält die Anwendungen für den Nutzer, beispielsweise



Virtualisiertes System: Zuerst importieren Sie Whonix-Gateway in Virtualbox. Dieses System stellt die Verbindung zum Tor-Netzwerk her und sorgt für den sicheren Datentransport.

den Tor-Browser, ein E-Mail- und ein Chat-Programm. Enigmail für die PGP-Verschlüsselung im Thunderbird-Ableger Icedove ist ebenfalls mit dabei.

Whonix installieren: Da Whonix zwei getrennte PCs benötigt, erfolgt die von den Entwicklern empfohlene Installation in einer virtuellen Umgebung. Am sichersten ist die Verwendung von Qubes-OS (*www.qubes-os.org*). Dieses System basiert auf Fedora und dem Virtualisierer Xen. In Qubes-OS lassen sich mehrere Betriebssysteme in abgeschotteten virtuellen Umgebungen nebeneinander installieren. Der Installationsaufwand ist jedoch erheblich. Deshalb empfehlen wir, das System erst einmal in Virtualbox auszuprobieren. Das ist zwar weniger sicher, weil auch unter Linux virtuelle Maschinen kompromittiert werden können, aber für eine anonyme Surfumgebung reicht die Sicherheit aus.

Gehen Sie auf *www.whonix.org/wiki/Download* und klicken Sie hinter „Linux“ auf den Link „VirtualBox“. Laden Sie die OVA-Dateien von Whonix-Gateway und Whonix-Workstation herunter. Beide Systeme basieren auf Debian. Installieren Sie Virtualbox über die Paketverwaltung Ihres Linux-Systems, unter Ubuntu beispielsweise im Terminal:

```
sudo apt-get install virtualbox
```

Importieren Sie beide OVA-Dateien per Doppelklick in Virtualbox. Starten Sie zuerst Whonix-Gateway. Es erscheint ein Meldungsfenster, das Sie mit den weiteren Schritten vertraut macht. Folgen Sie diesen Anweisungen und installieren Sie alle Aktualisierungen für das System. Über das Desktop-Icon „WhonixCheck“ können Sie jederzeit den Status des Systems und auch die Verbindung zum Tor-Netzwerk testen. Sobald die Einrichtung abgeschlossen ist, starten Sie die virtuelle Maschine mit Whonix-Workstation. Auch hier folgen Sie den Anweisungen im Meldungsfenster für das Systemupdate. Der Tor-Browser ist noch nicht installiert, was Sie über das gleichnamige Desktopicon nachholen.

Hinweis: Der Standardbenutzer in beiden Whonix-Systemen heißt „user“, das Passwort ist „changeme“.

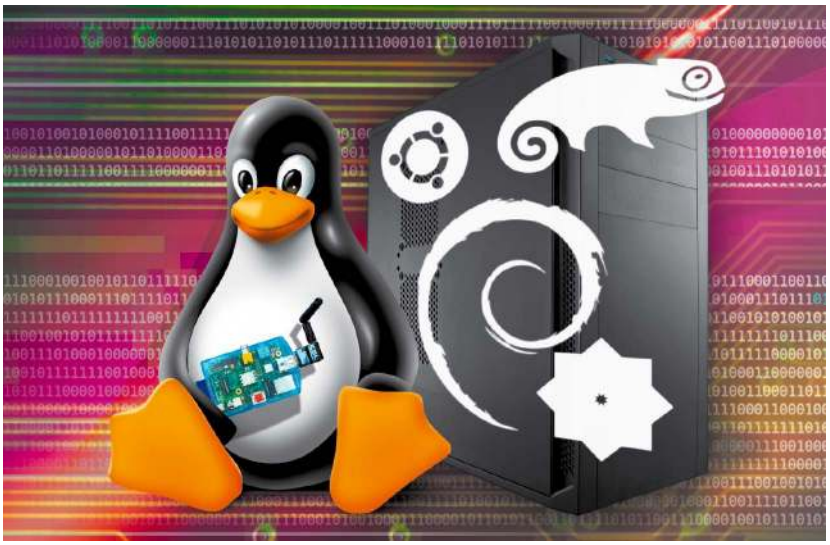
Die Grenzen der Anonymität

Tails und Whonix erhöhen die Sicherheit und können Ihre Identität wirkungsvoll verschleiern. Absoluten Schutz kann aber kein Dienst garantieren. Das gilt insbesondere für das Abfangen oder Auslesen persönlicher Daten, wenn diese nicht verschlüsselt sind oder Metadaten enthalten. Das Thema unsicherer Zugangsdaten wird durch die Dienste ebenfalls nicht gelöst: Wer ein schwaches Passwort beim Onlinebanking oder bei Paypal verwendet, muss natürlich trotzdem damit rechnen, dass sein Zugang geknackt wird. Eine Liste mit den Grenzen und Möglichkeiten von Tails finden Sie über *www.pcwelt.de/45SCbm*.

Geschützte Server

Die sichere Konfiguration eines Linux-Servers ist von dessen Rolle abhängig. Dennoch gibt es universelle Maßnahmen, die jeder Administrator kennen sollte. Egal ob es um Hobby-, Heimnetz- oder um ausgewachsene Mietserver geht.

Von **David Wolski**



Ein Linux-Server ist heute schnell eingerichtet. Kleine Platinenrechner mit genügend Leistung für eine Handvoll Aufgaben im heimischen Netzwerk sowie günstige virtuelle Server bei Cloudanbietern haben den Weg zum eigenen Linux-System enorm verkürzt. Doch auch wenn Hürden und Kosten heute niedriger sind: Es nicht einfacher geworden, den eigenen Server sicher zu betreiben. Trotz sinnvoller Grundkonfiguration der Serverdistributionen müssen angehende Linux-Administratoren selbst einige Sicherheitsvorkehrungen treffen – vor allem bei Servern, die aus dem Internet erreichbar sind.

1. Benutzer: Arbeiten mit sudo

Herrscher über ein Linux-System ist der Benutzer „root“. Es ist aber nicht empfehlenswert, die Administration unter diesem Systemkonto zu erledigen. Auf Mehrbenutzersystemen und Servern ist sudo das ideale Tool zur Delegation von Administratorrechten. Das Programm erlaubt einem Benutzer, einen einzelnen Befehl als root-User auszuführen. Für die tägliche Arbeit heißt das, dass sich niemand mehr als root anzumelden braucht, auch nicht zur Installation, Konfiguration oder für den Start von Programmen und Prozessen, die eigentlich nach root-Rechten verlangen. Der Vorteil: Das root-Passwort kann geheim bleiben und Benutzer können bei Bedarf sudo-Rechte bekommen, die sich auch wieder entziehen lassen.

Auch auf kleinen Servern hat sudo seine Vorzüge: Anders als bei root protokolliert das Linux-System die mit sudo aufgerufenen Aktionen.

Ubuntu brachte sudo einem großen Anwenderkreis näher, denn bei dieser Distribution ist sudo vorkonfiguriert, der Erstbenutzer automatisch sudo-berechtigt und die Anmeldung als root ist schlicht deaktiviert, damit Anwender gar nicht erst auf die Idee kommen, den root-Account zu nutzen. Auch Raspbian folgt diesem Beispiel und stattet den Standardbenutzer „pi“ mit sudo aus. Bei Fedora sowie Cent-OS gibt es vor der Installation die Option „Diesen Benutzer zum Administrator machen“ und bei Open Suse „Dieses Passwort für den Systemadministrator verwenden“, um das erstellte Benutzerkonto für sudo freizuschalten.

Welche einzelnen Benutzer und welche Gruppen sudo verwenden dürfen, ist in der Datei „/etc/sudoers“ festgelegt. Es empfiehlt sich jedoch nicht, einzelne Einträge für individuelle Benutzerkonten zu erstellen. Der einfachere Weg ist, die gewünschten Benutzer stattdessen zu jener Gruppe hinzuzufügen, die bereits Privilegien für sudo besitzt. Das hält den Administrationsaufwand niedrig, da eine entsprechende Gruppe auf den meisten Linux-Distributionen bereits vorhanden ist. Zudem ist es einfacher, sudo-Rechte einem Benutzer auch wieder zu entziehen, ohne abermals die Datei „/etc/sudoers“ zu bearbeiten.

Debian, Raspbian, Ubuntu und Derivate: Die Gruppe für sudo nennt sich in diesen Systemen schlicht ebenfalls „sudo“ und einen Benutzer nehmen Sie mit dem Kommando

```
sudo usermod -a -G sudo [Benutzer
  name]
```

in diese privilegierte Gruppe auf.

Fedora, Cent-OS und RHEL: In der Welt von Red Hat nennt sich die Gruppe mit sudo-Berechtigungen nach ganz alter Unix-Tradition „wheel“; der Be-

fehl, um die Zugehörigkeit eines Benutzers auf diese Gruppe auszudehnen, lautet folgendermaßen:

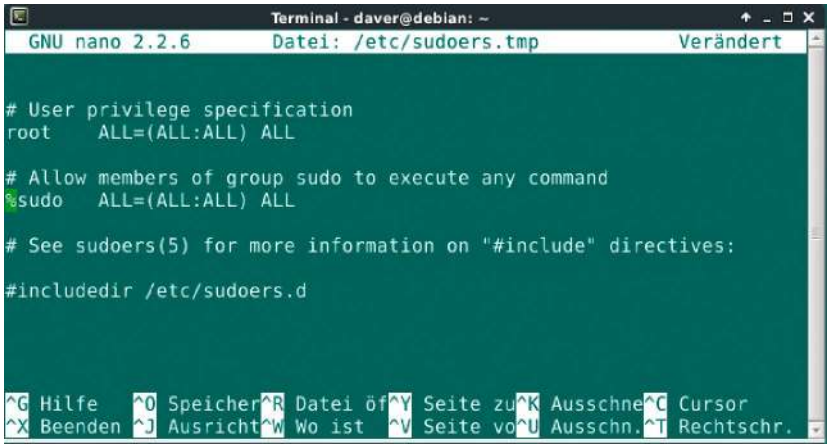
```
sudo usermod -a -G wheel [Benut
 zername]
```

Open Suse: Die Ausgangskonfiguration von sudo ist hier eigenwillig und verlangt noch eine manuelle Nachbearbeitung der Datei „/etc/sudoers“, die nicht mit dem grafischen Yast erfolgen kann, da die grafischen Menüs nicht fehlerfrei arbeiten. Starten Sie in Open Suse in der Shell erst den Editor für sudo mit dem Kommando

```
sudo visudo
```

und entfernen Sie gegen Ende der Datei das Kommentarzeichen „#“ vor der Zeile. Der Standardeditor für die Kommandozeile ist unter Open Suse vim. Fall Ihnen dieser Editor mit gewöhnungsbedürftiger Bedienung nicht behagt, können Sie auch den Editor Nano verwenden. Rufen Sie dazu visudo mit diesem Befehl auf:

```
sudo sh -c "export EDITOR=nano;
 visudo"
```



Gruppe statt einzelner Benutzer: In der Konfigurationsdatei von sudo ist in Debian/Ubuntu die Benutzergruppe „sudo“ vordefiniert. Hier können Sie weitere Benutzer aufnehmen.

Danach nehmen Sie den gewünschten Benutzer wie unter Fedora, Cent-OS und RHEL in die jetzt freigeschaltete Gruppe „wheel“ auf.

2. Serverdienste: Nur Benötigtes starten

Ein sauber eingerichteter Server führt nur jene Dienste aus, die für den Betrieb des Servers und seine Rolle im Netzwerk wichtig sind. Ein Webserver braucht etwa keinen Proxy- DNS-, POP- oder SMTP-Dienst anzubieten. Trotzdem kann es vorkommen, dass nach Experimenten oder Umbauten mehr läuft als nötig. Der Befehl

```
sudo netstat -tulp
```

gibt unter „PID/Program name“ und

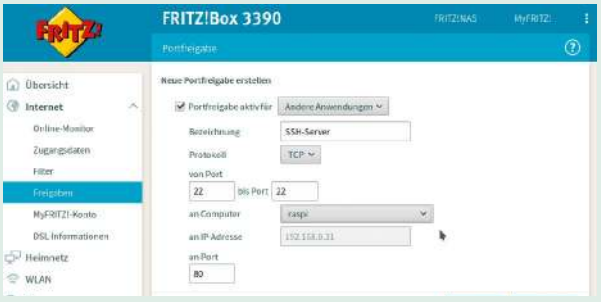
Server zu Hause: Portfreigaben ins Internet

Auch zu Hause müssen die Dienste eines Linux-Rechners oder eines Mini-PCs im Format eines Raspberry Pi nicht auf das LAN begrenzt sein. Eine Portfreigabe auf dem Router und ein dynamischer Hostname macht den Linux-Rechner von außen und von unterwegs erreichbar.

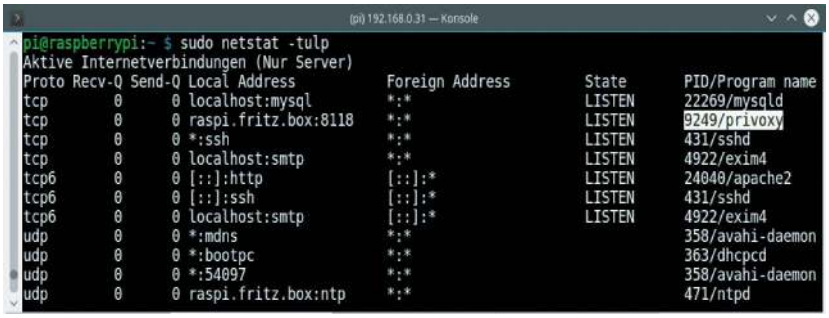
Die Aufgabe, den eingehenden Verkehr von außen über das Internet auf dem richtigen Port an den Rechner im lokalen Netzwerk weiterzuleiten, kommt im Heimnetzwerk dem Router zu. Die Einstellungen nehmen Sie in der Administrationsoberfläche des Routers vor. Kommt die verbreitete Fritzbox zum Einsatz, dann gehen Sie dafür auf der Administrationsoberfläche von *http://fritz.box* zunächst auf „Einstellungen -> System -> Ansicht“. Stellen Sie hier die „Expertenansicht“ ein. Dann können Sie über „Internet -> Portfreigabe -> „Neue Portfreigabe“ einen Port auf dem Router öffnen und an eine Rechner-IP im Netzwerk weiterleiten. Bei Routern anderer Hersteller funktioniert die Portfreigabe ähnlich, aber die Namen der Menüpunkte unterscheiden sich. Die Einstellungen an der Konfiguration finden sich meist unter einem Menüpunkt namens „Portforwarding“, „Portmapping“, „Forward“ „Custom Service“ oder „Virtual Server“. Wenn die Portweiterleitung steht und der Serverdienst im eigenen Netzwerk läuft, ist das eigene Netzwerk bereits aus dem Internet erreichbar.

Allerdings bleibt noch ein Problem: Der DSL- oder Kabelprovider vergibt bei jedem Verbindungsaufbau eine neue IP-Adresse. Diese Adresse müssten Sie jedes Mal herausfinden, etwa über die Webseite *http://ifconfig.me* – und das ist umständlich.

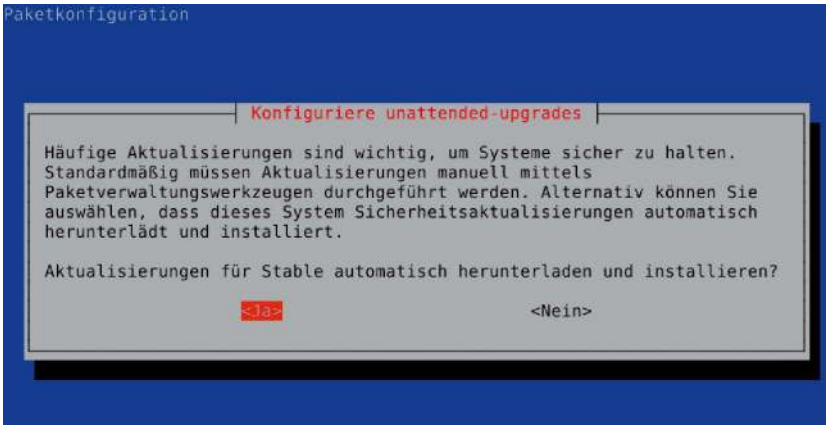
Für Abhilfe sorgt der Dienst von DNS-Anbietern, die bei der Einwahl des Routers die Internet-IP-Adresse einem dynamischen Hostnamen zuordnen. In den letzten Jahren war dazu Dyn DNS (*www.dyndns.org*) die erste Wahl. Mittlerweile akzeptiert dieser Service aber keine kostenlosen Neuanmeldungen mehr, sondern bietet nur noch kostenpflichtige Konten ab 25 US-Dollar an sowie befristete Testaccounts. Eine kostenlose Alternative ist *www.noip.com*. Ob der Router dies unterstützt, überprüfen Sie in der Administrationsoberfläche. Die Fritzbox bietet den Dienst in jedem Fall an.



Portweiterleitung auf der Fritzbox: Der Router ist im heimischen Netzwerk dafür verantwortlich, die Ports von Rechnern aus dem LAN, hier SSH mit Port 22, nach außen anzubieten.



Sehen, was läuft: netstat zeigt aktive Serverprozesse mit geöffneten Ports auf einem Linux-System an. In diesem Fall ist auf dem System ein längst vergessener Proxyserver aktiv.



Unbeaufsichtigt auf dem neuesten Stand: Debian-und Ubuntu-Systeme liefern für regelmäßige Sicherheitsaktualisierungen per Cronjob ein Konfigurationsscript mit.

„State“ an, welche Serverprozesse laufen. Steht vor dem Prozessnamen ein „LISTEN“, so lauscht der Prozess auf eingehende Verbindungen. Nach einer Überprüfung, ob ein aufgelisteter Dienst wirklich gebraucht wird, lassen sich die nicht benötigten Dienste mit

```
sudo service [Name] stop
```

anhalten und mit

```
sudo service [Name] disable
```

so abschalten, dass sie beim nächsten Neustart nicht wieder aktiv werden. Der Platzhalter „[Name]“ entspricht dabei der Angabe unter „PID/Program name“.

3. Unbeaufsichtigt: Automatische Updates

Ein Linux-System kann sehr sicher sein, solange es regelmäßig Updates erhält. Andererseits kann ein vorbildlich konfiguriertes Linux-System durch neu entdeckte Bugs angreifbar werden. Obwohl die Paketmanager ein Systemupdate sehr komfortabel machen, werden Aktualisierungen im Alltag gerne mal aufgeschoben. Für Server bietet sich eine unbeaufsichtigte Aktualisierung im Hintergrund an, die neue und als Sicherheitsupdates markierte Pakete regelmäßig einspielt.

Debian, Raspbian und Ubuntu: Vorbereitete Scripts für unbeaufsichtigte Updates installiert dieser Befehl:

```
sudo apt-get install unattended-
  upgrades
```

Danach verlangt das System nur noch kleinere Anpassungen. Rufen Sie das Konfigurationsscript mit

```
sudo dpkg-reconfigure
  --priority=low unattended-up
  grades
```

auf und beantworten Sie die Rückfrage nach dem automatischen Herunterladen und Installieren mit „Ja“. Die benötigten Einträge für einen täglichen Cronjob, der um 6:25 Uhr ausgeführt wird, erstellt das Konfigurationsscript nun selbständig. Testen können Sie dies mit diesem Befehl:

```
sudo unattended-upgrades --dry-run
  -d
```

Die Logdatei „/var/log/unattended-upgrades/unattended-upgrades.log“ protokolliert die Updates. Eine komplette Distributionsaktualisierung, die auch geänderte Abhängigkeiten unter Paketen beachtet, müssen Sie hin und wieder manuell mit

```
sudo apt-get dist-upgrade
```

ausführen.

Cent-OS: Im Klon von Red Hat Enterprise Linux gibt es das Paket „yum-cron“, das unbeaufsichtigte Updates aktiviert. Sie installieren es mit

```
sudo yum install yum-cron
```

und finden die zugehörige kommentierte Konfiguration unter „/etc/yum/yum-cron.conf“.

Per Standard holt das Script alle Aktualisierungen und nicht nur Sicherheitsupdates. Mit

```
sudo systemctl enable yum-cron.
  service
sudo systemctl enable yum-cron.
  service
```

schalten Sie den Dienst für Updates ein.

Open Suse: Egal ob Server oder Desktop – die Konfiguration eines Open-Suse-Systems erfolgt mit dem Tool Yast, das auch als textbasierte Version auf der Kommandozeile zur Verfügung steht. Um diese Version zu nutzen, installieren Sie zuerst mit dem Kommando

```
sudo zypper install yast2-online-
  update-configuration
```

das Yast-Modul für automatische Updates und rufen dann mit

```
sudo yast
```

Yast in der Shell auf. Dort gehen auf „Software -> Konfiguration der Online-Aktualisierung“ und können mit „Automatische Online-Aktualisierungen“ (Tastenkombination Alt-A) die Updates einschalten und noch das Intervall auswählen. Voreingestellt ist ein wöchentliches Intervall.

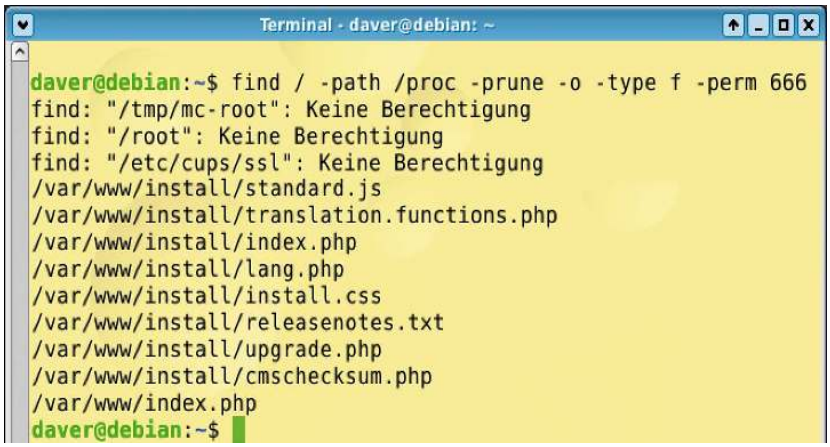
4. Updates: PHP-Projekte und Co

Linux-Distributionen machen über den Paketmanager das regelmäßige Systemupdate für Kernel, Serverdienste und Bibliotheken zu einer leichten Auf-

gabe. Anders ist es bei den diversen PHP-Projekten und anderen Frameworks, die üblicherweise auf Webservern laufen. Um diese auf dem neuesten Stand zu halten, muss der Administrator selbst aktiv werden, da nach gravierenden Sicherheitslücken nicht viel Zeit bleibt, die eigene Site abzusichern. Nachrichten zu Updates gibt es auf der Webseite des verwendeten PHP-Projekts oder der anderweitigen Scripts. Besonders wichtig ist es, auch Plug-ins auf dem neuesten Stand zu halten, da dort bei allen CMS und Blogsystemen die meisten Sicherheitslücken lauern. Newsseiten berichten meist nur über die großen Systeme – und auch nicht immer ganz aktuell. Für die Suche nach neuen Sicherheitslücken in bestimmten Versionen von Webseiten-Frameworks und deren Plug-ins ist die Mailingliste Full Disclosure eine gute Anlaufstelle, die sich unter *http://seclists.org/fulldisclosure* durchsuchen lässt. Abonnieren kann man die umfangreiche Liste unter *http://www.grok.org.uk/full-disclosure*. Bekannte Exploits für viele Projekte nimmt auch das Archiv von *http://www.exploit-db.com* unter „Web Application Exploits“ auf.

5. Zugriffsrechte: Kein Vollzugriff für alle

Wer keine Gruppen für gemeinsame Zugriffsrechte für Verzeichnisse und Dateien einrichtet, behilft sich oft mit einer simplen, aber unsicheren Abkürzung: Dateien bekommen kurzerhand die Zugriffsrechte 666 oder gar 777 zugewiesen, Verzeichnisse die Rechte 777. Damit sind Lese- und Schreibrechte ausgehebelt, da alle Prozesse und Benutzer auf dem System Vollzugriff auf diese Dateisystem-Objekte haben. Auf einem Server ist das keine gute Idee und schlicht ein Konfigurationsfehler, auch wenn nachlässig geschriebene Anleitungen diese Rechte empfehlen. Sie können Dateien und Verzeichnisse mit unbeschränkten Zugriffsrechten einfach ausfindig machen und benötigen dazu noch nicht mal root-Rechte. Das Kommando



Diese Zugriffsrechte sollte es nicht geben. find durchsucht hier das gesamte Dateisystem („/proc“ ausgenommen) nach Dateien mit den oktalen Rechten 666 (Schreibrecht für alle).

Welche Benutzer gibt es? Die Datei „/etc/passwd“ enthält auf den Unix-ähnlichen Systemen die Namen aller Benutzerkonten. Jene mit Home-Verzeichnis sind interessant.

```
find / -path /proc -prune -o -type
  f -perm 666
```

findet alle Dateien im gesamten Dateisystem, ausgenommen „/proc“, die von allen gelesen und beschrieben werden dürfen.

```
find / -path /proc -prune -o -type
  f -perm 777
```

listet Dateien auf, die zusätzlich ausführbar sind. Genauso findet

```
find / -path /proc -prune -o -type
  d -perm 777
```

Verzeichnisse, die zum Lesen und Schreiben offenstehen.

Anstatt für Dateien und Verzeichnisse uneingeschränkten Vollzugriff zu setzen, ist es besser, Gruppen für gemeinsam genutzte Dateien zu verwenden. Der Befehl

```
sudo chgrp [Gruppe] [Datei/Ver
  zeichnis]
```

ändert die Gruppe von Dateisystem-Objekten. Für den Vollzugriff für Besitzer und Gruppe genügen bei Verzeichnissen die Rechte 770 sowie bei Dateien 660.

6. Altlasten: Vergessene Benutzer löschen

In Teams mit wechselnder Besetzung kann es vorkommen, dass auch längst weitergezogene Exkollegen noch ein Benutzerkonto auf dem Server haben. Im schlimmsten Fall ist das Konto auch noch für sudo freigeschaltet. Bei Servern mit mehreren Admins und wechselnder Besetzung ist es nicht verkehrt, die eingerichteten Benutzerkonten auf dem Server zu überprüfen. Diese stehen in der Datei „/etc/passwds“ und lassen sich mit

```
cat /etc/passwd |grep "/home"
```

anzeigen, wobei es hier nur auf Benutzer mit einer numerischen ID über 1000 ankommt – die anderen sind Accounts von Systemdiensten.

Nicht mehr benötigte Accounts löscht der Befehl

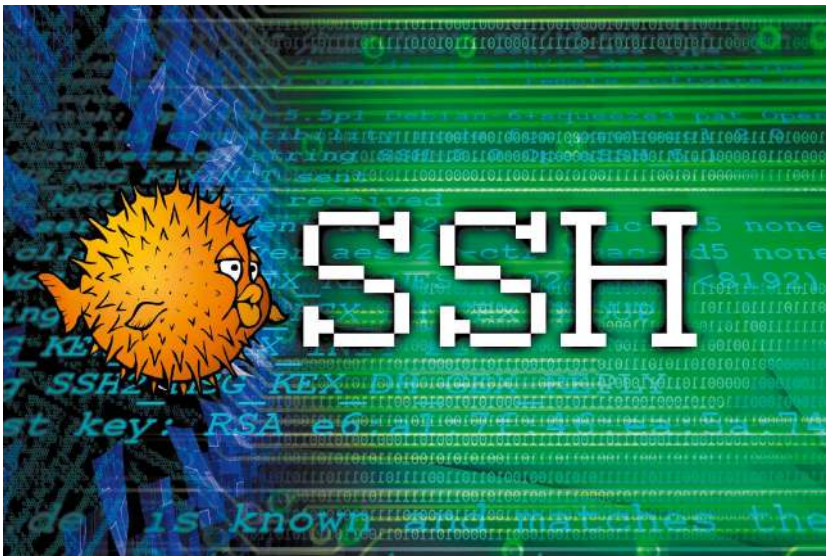
```
userdel -rf [Benutzername]
```

samt zugehörigem Home-Verzeichnis. Der Parameter „f“ führt die Löschaktion auch dann aus, wenn der Benutzer gerade noch angemeldet ist. ●

Sichere Secure Shell

Die Secure Shell, kurz „SSH“, ist das verbreitete Protokoll zur sicheren Fernadministration per Kommandozeile über das Netzwerk. Vor allem Rechner, die per SSH auch über das Internet erreichbar sind, sollten gut abgesichert sein.

Von **David Wolski**



SSH ist der Standard, um sich an einem Linux über das Netzwerk anzumelden. Die Voraussetzungen für SSH sind minimal: Ein Linux-System kann sowohl Client als auch Server sein, wobei die üblichen Linux-Distributionen erst mal nur der Client vorinstallieren und der Server über das Paket „openssh-server“ nachgerüstet wird. Entwickelt wurde das verschlüsselte Protokoll schon in grauer Unix-Vorzeit als Alternative zu Telnet. Seither hat es sich als Möglichkeit durchgesetzt, sich über ein unsicheres Netzwerk mit einem Server zu verbinden, um dort Befehle auszuführen.

Während das verschlüsselte SSH-Protokoll nach wie vor als sicher gilt und nur die Clients und Server von Zeit zu Zeit die obligatorischen Aktualisierungen der Open-SSH-Pakete verlangen, ist die effektive Sicherheit auch von der Serverkonfiguration abhängig. Die folgenden Punkte helfen dabei, SSH auf einem Linux-Server optimal abzusichern.

Türsteher: Benutzer ausschließen

Standardmäßig kann sich jeder Benutzer, der ein Konto auf dem Linux-Rechner hat, auch per SSH mit seinem Namen und Passwort dort anmelden. Dies ist enorm praktisch, aber nicht immer gewünscht. Der Benutzer root beispielsweise sollte sich nicht anmelden können, denn hier ist von den beiden Zugangshürden (Benutzer plus Kennwort) schon mal eine bekannt. Wenn hier ein Angreifer das Passwort durch eine Wörterbuchattacke erraten hat, ist das System komplett kompromittiert. Um root und auch andere Benutzer von SSH auszuschließen, ist eine Anpassung an der Konfigurationsdatei von Open SSH nötig.

Öffnen Sie die Konfigurationsdatei „/etc/ssh/sshd_config“ mit root-Rechten in einem Texteditor. Tragen Sie dann die Zeile

```
PermitRootLogin no
```

an einer beliebigen Position ein, um einen root-Log-in zu verbieten. Wichtige Voraussetzung für diese Maßnahme ist, dass sudo für einen oder mehrere Benutzer eingerichtet ist, damit man sich als Admin nicht selbst über das Netzwerk aussperrt. Bei Ubuntu und Co ist ein root-Log-in übrigens sowieso nicht vorgesehen, bei Debian, Open

SSH zur Dateiübertragung

SSH sorgt für eine verschlüsselte Übertragung der Anmeldeinformationen und für die sicherere Datenübertragung. Damit eignet es sich auch als Ersatz für das unverschlüsselte FTP. Das Kommandozeilenprogramm für die Dateiübertragung vom Client auf den Server per SSH heißt scp („secure copy“). Mit dem Befehl

```
scp datei.ext [name]@[server]:/
  home/[name]/
```

kopieren Sie eine Datei namens „datei.ext“ als Benutzer „[name]“ auf einen Server in das Verzeichnis „/home/[name]“. Mehr Komfort gefällig?

Die Dateimanager Midnight Commander, Nautilus unter Gnome und Dolphin sowie Krusader unter KDE können ebenfalls Dateien per SSH übertragen. Für Mac und Windows eignet sich Filezilla (auf Heft-DVD, Download unter *www.pcwelt.de/298277*) als Client.

Suse, Red Hat und anderen Distributionen dagegen schon.

Weitere Benutzer schließen Sie durch die Zeile

```
DenyUsers [Benutzer] [Benutzer]
```

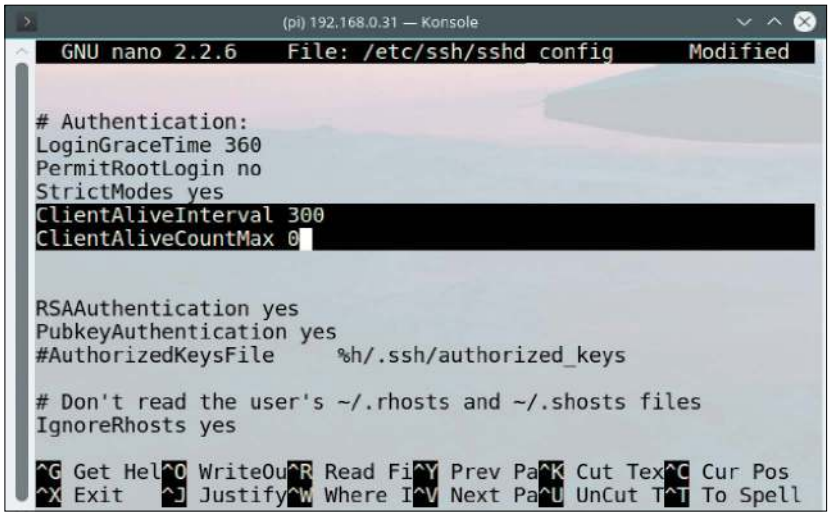
aus, wobei die Platzhalter „[Benutzer]“ durch die tatsächlichen Namen der Benutzerkonten ersetzt werden. Anschließend erwartet der Open-SSH-Serverdienst noch einen Neustart mit

```
sudo service ssh restart
```

in Debian, Ubuntu, Raspbian beziehungsweise mit

```
sudo service sshd restart
```

in Fedora, Cent-OS, Red Hat und Open Suse.



Und tschüss: Ein Zeitlimit für inaktive Sitzungen ist nützlich, um vergessene SSH-Verbindungen nach definierter Frist zu trennen – hier nach hier 300 Sekunden.

Inaktivität: Automatisch abmelden

Vergessene Konsolenfenster mit geöffneten SSH-Verbindungen sind eine Sicherheitslücke, sobald andere Personen an den Rechner kommen. Mit einer kleinen Ergänzung in der Konfiguration des SSH-Servers kann dieser eine inaktive SSH-Verbindung automatisch nach einer bestimmten Anzahl von Minuten trennen. Bei Open SSH genügt in der Konfiguration „/etc/ssh/sshd_config“ die Ergänzung der folgenden beiden Zeilen:

```
ClientAliveInterval 300
ClientAliveCountMax 0
```

Im Beispiel wird die Verbindung nach 300 Sekunden (fünf Minuten) getrennt, wenn keine Eingaben erfolgen.

Fail2ban: Angriffe abblocken

Jeder, der einen Linux-Server betreibt, der über eine Internetverbindung erreichbar ist, kennt das Problem: Einfallslose Angreifer probieren über Dictionary-Attacken, sich auf dem SSH-Port mit dem Server zu verbinden. Bei ausreichend komplexen Passwörtern und dem Verzicht auf sehr einfache Benutzernamen wie „Gast“ oder „User“ sind diese Angriffe nicht erfolgreich. Bei mehreren Hundert gescheiterten Verbindungsversuchen täglich wird das Security- beziehungsweise Access-Logfile allerdings unnötig unübersichtlich. Dagegen ist ein Kraut gewachsen: Das Tool fail2ban ist ein Hintergrundprozess (Daemon), der die Logdateien auf erfolglose Log-in-Versuche überprüft und die IP-Adresse dieser Versuche nach einer definierbaren Zahl von fehlgeschlagenen Anmeldungen für einige Zeit blockt. Das Paket „fail2ban“ steht unter Ubuntu, Debian, Fedora und Open Suse über den Paketmanager zur Verfügung und muss nicht einmal mehr konfiguriert werden: In den Standardeinstellungen kommt ab fünf Versuchen für zehn Minuten die IP-Adresse des Clients in den Giftschrank und wird mittelt iptables geblockt. In der Konfigurationsdatei „/etc/fail2ban/jail.conf“ lässt sich die erlaubte Anzahl der Versuche und eine Liste von nicht zu blockenden IP-Adressen festlegen. Eine Protokolldatei gibt es unter „/var/log/fail2ban.log“.

Yubikey: Absicherung durch Hardware

Die Authentifizierung an einem SSH-Server ist üblicherweise an ein Passwort oder an einen hinterlegten Public Key gebunden. Soll ein Benutzer auf dem SSH-Server keinen Zugriff mehr haben, etwa wenn ein Projekt oder ein Arbeitsvertrag endet, so muss auf dem Server eine Passwortänderung erfolgen oder der Public Key gelöscht werden. Mit dem USB-Dongle Yubikey wird die SSH-Anmeldung an ein Stück Hardware gebunden, denn nur mit dem angesteckten USB-Stick ist es möglich, sich an einem SSH-Server anzumelden.

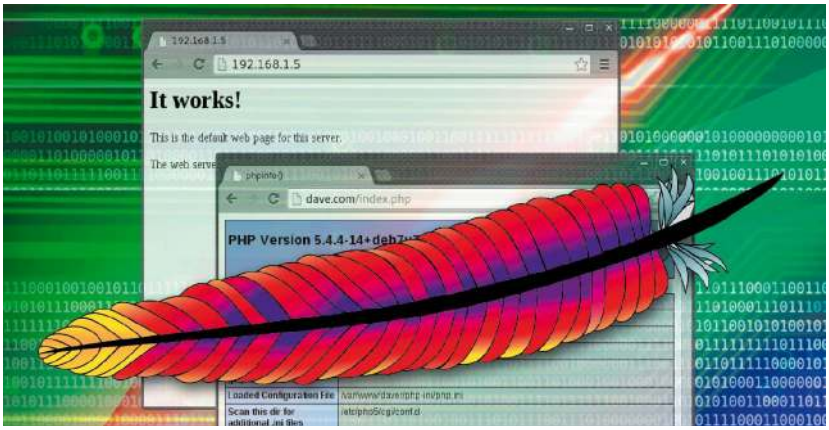
Ganz ohne Software funktioniert das natürlich auch nicht: Der Hersteller des Yubikey bietet für Linux- und BSD-Systeme PAM-Module für die Anmeldeprozedur an. Diese Module sind Open Source und liegen bei Github. Soll ein Anwender keinen Zugriff mehr auf einen bestimmten SSH-Server haben, so genügt es, einfach den Yubikey wieder einzusammeln, denn dieser kann nicht vervielfältigt werden. Ist ein Yubikey verlorengegangen, dann kann ein Schlüssel auch weiterhin auf der Serverseite gesperrt werden. Yubikeys sind je nach Modell ab 50 Euro zu haben (*http://amzn.to/25lyont*).

Yubikey als Hardwareschlüssel für SSH. Die USB-Dongles arbeiten auch als Schlüssel für SSH und arbeiten auf dem Client mit jedem Betriebssystem, das USB-Eingabegeräte unterstützt.

Apache-Webserver absichern

Ein Webserver wie Apache soll zwar Inhalte servieren, darf dabei aber nicht zu viele Informationen preisgeben oder gar angreifbar sein. Der Beitrag zeigt die wichtigsten Schritte zu einer sicheren Konfiguration.

Von **David Wolski**



Keine Überraschung: Der Webserver Apache dominiert das Web, wie der Branchendienst Netcraft (*http://www.netcraft.com*) nach der Auswertung von fast einer Milliarde Sites im Februar 2016 wieder bestätigt hat. Trotz der sinnvollen Standardkonfiguration, mit der Apache und dessen Module von diversen Distributionen ausgeliefert werden, ist der Webserver nicht per se sicher. Sicherheit ist davon abhängig, welche Art von Anfragen der Webserver beantworten soll und wie sorgfältig die Konfiguration gelungen ist. Die folgenden Punkte helfen, typische Apache-Server besser zu abzusichern.

Header: Die Informationen reduzieren

Apache stellt sich bei HTTP-Anfragen im Antwortheader höflich mit Namen und Versionsnummer vor – und die aktivierten Module wie PHP ebenfalls. Diese Infos, die Rückschlüsse auf das verwendete System, Version und schlimmstenfalls auf veraltete Software hinweisen, gehen aber außer dem Administrator niemanden etwas an. Diese standardmäßig aktivierten Infos sind schnell deaktiviert. In Debian/Ubuntu/Raspbian ist die Konfigurationsdatei „/etc/apache2/conf-available/security.conf“ dafür verantwortlich. In der Datei muss nur die Zeile „ServerTokens OS“ zu

```
ServerTokens Prod
```

geändert werden, gefolgt von einem Apache-Neustart. Danach sind Angaben zu Apache-Version und Modulen aus dem Header getilgt.

Verzeichnisse: Den Index abschalten

In der Standardkonfiguration zeigt Apache für Ordner im Document-Root (bei Debian/Ubuntu/Raspbian unter „/var/www/html“) eine Verzeichnisübersicht an, sofern dort keine Datei namens „index.html“ beziehungsweise „index.php“ liegt. Diese Auflistung von Verzeichnisinhalten präsentieren Besuchern auf dem Webserver schlimmstenfalls Dateien, die nicht öffentlich sein sollten.

Um Verzeichnislisten generell abzuschalten, ist unter Debian/Ubuntu/Raspbian eine Anpassung der Konfigurationsdatei „/etc/apache2/apache2.conf“ nötig: Unter der Zeile „<Directory /var/www/>“ muss die Zeile „Options Indexes FollowSymLinks“ nach „Options FollowSymLinks“ geändert werden, gefolgt von einem Apache-Neustart. Bei einer Site-Konfiguration im Apache-Verzeichnis „/etc/apache2/sites-available“ lässt sich diese Änderung auch gezielt für die gewünschten Verzeichnisse eintragen.

Aufräumen: Karteileichen löschen

Während des Aufbaus eines Webservers oder eines ganzen Webangebots ist es immer mal nötig, Verzeichnisse und Scripts zum Testen anzulegen, etwa um eine im Hintergrund arbeitende Datenbank per Phpmyadmin bequem über den Browser anzulegen und zu pflegen. Sobald ein Webserver dann öffentlich über das Internet erreichbar ist, müssen diese Testverzeichnisse und Admin-Oberflächen verschwinden oder per Passwort gesichert werden. Bei einem Webprojekt, an dem mehrere Leute gearbeitet haben, ist das keine einfache Aufgabe. Aber findet diese Verzeichnisse überhaupt jemand? Die Erfah-

rung zeigt, dass auch obskure Datei- und Verzeichnisnamen keinen Schutz darstellen. Denn es gibt bewährte Tools, die per Dateilisten einen Webserver gründlich nach vergessenen Verzeichnissen und Karteileichen abklappern. Wie wichtig Aufräumarbeiten sind, zeigt der Einsatz eines Tools gegen den eigenen Server.

Das Java-Programm Dirbuster wurde vom gemeinnützigen Verein OWASP entwickelt und ist ein Klassiker unter den Pentestingtools, das allerdings schon länger kein Update mehr bekommen hat. Für den Hausgebrauch ist die letzte Version von 2013 aber immer noch gut geeignet. Dirbuster liegt unter *https://sourceforge.net/projects/dirbuster* als tar.bz2-Archiv vor und verlangt eine Java-Runtime, die in Debian/Ubuntu/Mint das Paket „default-jre“ liefert. Nach dem Entpacken startet der Befehl

```
java -jar DirBuster-0.12.jar
```

das Programm im Terminalfenster. Das Feld „Target URL“ erwartet die IP-Adresse oder den Hostnamen des eigenen Servers. Unter „File with list of dirs/files“ wird eine Wörterbuchdatei mit den gewünschten Einträgen für den Scan angegeben. Dirbuster bringt einige Wörterbücher mit der Endung „.txt bereits mit. Die kleinere Datei „directory-list-2.3-small.txt“ reicht meistens schon aus.

Per Modul: Extraschutz für Apache

Wer immer einen Dienst, sei es nur einen Webserver mit statischen oder dynamischen Inhalten, per PHP anbietet, wird irgendwann die Bekanntschaft mit automatisierten Scanprogrammen machen, die ungebetene Besucher auf den Webserver schicken. Schlimmstenfalls kann sich ein penetranter Scan sogar als Denial-of-Service-Attacke auf den eigenen Server auswirken.

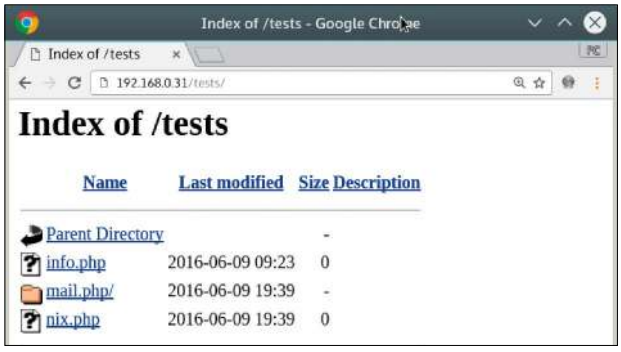
Mit dem Extramodul „libapache2-mod-evasive“ weicht Apache typischen Angriffen selbständig aus. Die Erkennung von Angriffsmustern funktioniert über eine bei jedem Zugriff aktualisierte Tabelle der IP-Adressen, von welchen eine HTTP-Anfrage ausging. Wird eine Seite in schneller Folge von einer IP-Adresse aus mehrmals pro Sekunde angefordert oder werden 50 gleichzeitige Requests pro Apache-Prozess ausgelöst, dann landet diese IP einige Sekunden auf einer schwarzen Liste und erhält nur noch eine 403-Forbidden-Meldung. Die Erweiterung lässt sich unter Ubuntu/Debian/Raspbian mit dem Befehl

```
sudo apt-get install libapache2-
  mod-evasive
```

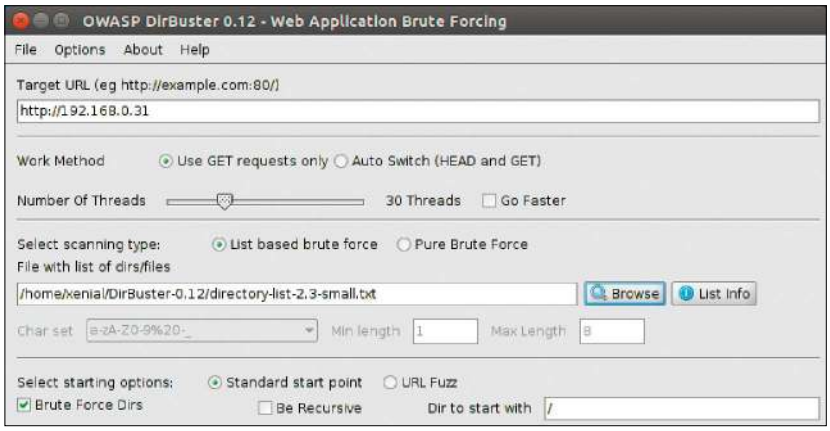
leicht installieren und durch einen Apache-Neustart mit

```
sudo service apache2 restart
```

aktivieren. Die Funktion lässt sich im Browser durch mehrfachen Druck auf die F5-Taste leicht testen. Auch CentOS kennt das Modul unter diesem Namen und unter Open Suse nennt es sich „apache2-mod-evasive“.



Unerwünschte Verzeichnislisten: Ist in einem Verzeichnis keine „index.html“ oder „index.php“ enthalten, zeigt Apache dennoch eine Auflistung. Verantwortlich dafür ist die Option „Indexes“.



Findet vermeintlich Unauffindbares: Dirbuster sucht öffentliche Webserver hartnäckig nach typischen Verzeichnisnamen ab, die in einer Wörterbuchdatei definiert sind.

Nikto: Check für den Webserver

Linux und die verwendeten Serverkomponenten wie Apache können noch so sorgfältig entwickelt und sicher sein – meist sind es Flüchtigkeitsfehler oder Pannen aus Unkenntnis, welche die größten Lücken reißen. Ein Tool, das systematisch bei der Analyse von möglichen Konfigurationsfehlern hilft, ist das Sicherheitsprogramm Nikto (*https://cirt.net/Nikto2*) für die Linux-Kommandozeile, das Webserver auf 6700 typische Risiken prüft. Installiert ist Nikto in den verbreiteten Linux-Distributionen schnell über den jeweiligen Paketmanager, in Debian/Ubuntu/Mint/Raspbian mit diesem Kommando:

```
sudo apt-get install nikto
```

Um einen Webserver zu untersuchen, dient dieser Aufruf:

```
nikto -h [Hostname/IP]
```

Nikto wird dann im Terminal nach seinen Checks ein ausführliches Protokoll mit weiterführenden Infos (in Englisch) ausgeben.

Wordpress schützen

Die mit Abstand beliebteste PHP-Blogsoftware ist Wordpress, das vielerorts auch als Content-Management-System Verwendung findet. Die große Popularität macht Wordpress – und besonders dessen Plug-ins – zum beliebten Angriffsziel.

Von **David Wolski**

Quelle: David Wolski

Während große Sites mit viel Verkehr meist auf maßgeschneiderte Lösungen auf der Basis von Django und Ruby und Rails setzen, ist Wordpress bei kleinen Webseiten die bevorzugte Lösung. Es ist nach einer Studie von W3techs im Sommer 2016 bei 26 Prozent der untersuchten zehn Millionen Sites im Einsatz.

Diese Popularität ist leicht erklärt: Wordpress setzt auf einem typischen Webserver wie Apache, My SQL sowie PHP auf, ist schnell eingerichtet und der PHP-Code ist vergleichsweise klar strukturiert. Die Entwickler- und Anwendergemeinde macht das Open-Source-Projekt zum Selbstläufer. Es gibt zahllose Themes und ein Plug-in-System, das Wordpress mit wenig Aufwand erweitert und für den anvisierten Einsatzzweck fit macht.

Diese Flexibilität hat aber ihren Preis, denn oft sind es diese Plug-ins aus der großen Entwicklergemeinde, die sich angreifbar zeigen und immer wieder Sicherheitslücken in eine Wordpress-Installation reißen.

Updates: Auf dem Laufenden bleiben

Zur Pflege einer Wordpress-Site gehört nicht nur die regelmäßige Aktualisierung der Kernkomponenten, sondern auch ein akribischer Check der Erweiterungen. Wordpress selbst bekommt seitens seiner Entwickler häufig Aktualisierungen: 2016 gab es im Januar, Februar und Mai Sicherheitsupdates. Die Verwaltungskonsole von Wordpress informiert nicht nur über neue Versionen, sondern kann diese auch einspielen. Seit Wordpress 3.7 gibt es eine automatische Aktualisierungsfunktion innerhalb von Versionsnummern. Nur größere Versionssprünge warten dann noch auf die manuelle Genehmigung, beispielsweise von 4.4 zu 4.5.

Tipp: Wer nicht regelmäßig die Administrationsoberfläche von Wordpress aufsucht, kann über den RSS-Feed *https://wordpress.org/news/feed* über neue Wordpress-Versionen auf dem Laufenden bleiben.

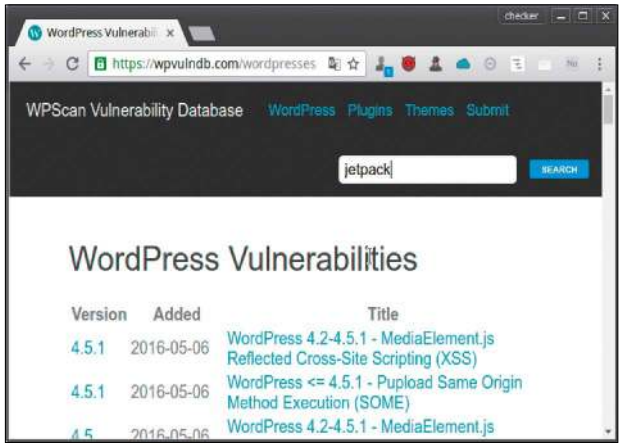
Themes und Plug-ins nicht vergessen

Zügige Updates gibt es bei fremden Wordpress-Komponenten nicht immer. Eine schlecht gewartete Kollektion von fremdem PHP-Code ist neben groben Konfigurationsfehlern die Hauptursache für Einbrüche in Wordpress. Im Juni 2016 machte beispielsweise eine kritische Lücke im WP Mobile Detector über 10 000 Wordpress-Sites verwundbar – und ein Sicherheitsupdate für dieses Plug-in gab es nicht. Es blieb den vielen Betroffenen nur, das Plug-in so schnell wie möglich zu deinstallieren.

Zwar zeigt die Wordpress-Verwaltungsoberfläche auch an, wenn es Updates für installierte Plug-ins gibt, das aber nur dann, wenn deren Entwickler tätig werden. So ist es nicht einfach, zu Schwachstellen in schlecht gepflegten Plug-ins und Themes rechtzeitig Informationen zu finden. Dieses Manko will die Online-Datenbank *https://wpvulndb.com* beheben. Es handelt sich dabei um ein laufend aktualisiertes Nachschlagewerk zu Sicherheitslücken in Wordpress selbst, in Plug-ins und Themes.

Automatischer Check per Script

Die Datenbank der Wordpress-Sicherheitslücken entstand aus einem älteren Projekt: WP Scan (*http://wpscan.org*)



Wordpress-Betreiber sollten diese Adresse kennen: https://wpvulndb.com ist eine laufend aktualisierte Datenbank bekannter Sicherheitslücken in Wordpress, Themes und Plug-ins.

Auf Schwachstellen abklopfen: WP Scan untersucht Wordpress, aktivierte Themes und Plug-ins auf alle Sicherheitsprobleme, die unter https://wpvulndb.com dokumentiert sind.

ist ein Ruby-Script, das einen automatischen Check von Wordpress-Installationen von einem Client aus über HTTP erlaubt und bekannte Sicherheitslücken findet. Die Dokumentation unter *https://github.com/wpscanteam/wpscan/blob/master/README.md* liefert auch Installationsanleitungen für Ubuntu, Debian, Fedora und Arch Linux. In Ubuntu 16.04 und Co. installieren Sie in einem Terminalfenster mit

```
sudo apt-get install git libcurl4-
  openssl-dev libxml2 libxml2-dev
  libxslt1-dev ruby-dev build-es
  sential libgmp-dev zlib1g-dev
```

zunächst die benötigten Abhängigkeiten. Dann laden Sie mit dem Befehl

```
git clone https://github.com/wp
  scanteam/wpscan.git
```

das Programm von Github in das Verzeichnis „wpscan“ herunter. Nach einem Wechsel in dieses Verzeichnis mit *cd wpscan* installiert das Kommando

```
sudo gem install bundler && bundle
  install --without test
```

die weiteren Ruby-Module (RubyGems) nach und macht WP Scan einsatzbereit:

```
./wpscan.rb --update
```

Dies aktualisiert die interne Datenbank vor dem ersten Aufruf. Einen umfassenden Scan von Wordpress, Plug-ins und Themes auf Ihrem Zielserver mit der Adresse „[Domain]“ starten Sie folgendermaßen:

```
./wpscan.rb --url http://[Domain]/
  --random-agent  --enumerate
```

Nur die Plug-ins überprüft dagegen dieses Kommando:

```
./wpscan.rb --url http://[Domain]/
  --random-agent  --enumerate p
```

Ein Scan kann einige Minuten dauern; die Ergebnisse werden im Terminalfenster hübsch aufbereitet angezeigt – mit Links zu Problembeschreibungen.

Checkliste: Wordpress sicherer machen

Viele Angriffe auf Wordpress-Webseiten gehen gar nicht so weit, erst nach ungepatchten Sicherheitslücken zu suchen. Automatisierte Attacken nehmen sich meist einfach die Log-in-Seite unter „/wp-admin“ vor, um dort häufige Passwort-Benutzer-Kombinationen abzuarbeiten. Die folgenden Punkte helfen dabei, Wordpress gegen diese Art von Belästigung zu schützen:

Keine Standardnamen für den Admin: Ein aktuelles Wordpress richtet keinen Admin-Benutzer mit leicht zu erratendem Namen mehr ein. Den Namen kann man sich bei der Installation selbst aussuchen. Auf Benutzerkonten wie „Admin“, „Administrator“ und Ähnliches sollten Sie dabei verzichten.

SSL nutzen: Die schönsten Passwörter nützen wenig, wenn diese im Klartext übertragen werden. Eine Wordpress-Site sollte deshalb per HTTPS erreichbar sein, zumindest mit einem selbst signierten Zertifikat für den Admin-Zugang. Kostenlose SSL-Zertifikate gibt es von Let's Encrypt (*https://letsencrypt.org*) mit 90 Tagen Laufzeit und von Start SSL (*https://www.startssl.com*) für ein Jahr.

Zwei-Faktor-Authentifizierung: Ein weiterer Schutz gegen Anmeldungen über gestohlene Zugangsdaten ist eine Zwei-Faktor-Authentifizierung, bei der ein weiterer Zugangscode für jeden Log-in nötig ist. Beim Plug-in Two-Factor Auth (*https://de.wordpress.org/plugins/two-factor-auth*) dient dazu ein TOTP/HOTP-Generator wie der Google Authenticator (*http://bit.ly/19dDzPR*) auf einem Smartphone.

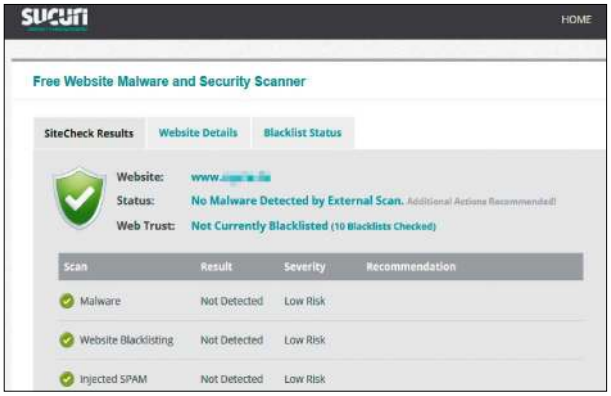
Anmeldeversuche reduzieren: Zahllose gescheiterte Anmeldeversuche deuten darauf hin, dass ein Angreifer per Script Passwörter durchprobiert. Per Plug-in kann dessen IP-Adresse ab einer bestimmten Zahl an erfolglosen Log-ins blockiert werden. Das Plug-in Login Lockdown (*https://de.wordpress.org/plugins/login-lockdown*) für Wordpress sperrt standardmäßig eine IP eine Stunde lang, wenn von dort aus die Anmeldung dreimal innerhalb von fünf Minuten fehlschlug. Die Werte können Sie individuell anpassen.

Tools für den Sicherheits-Check

Über das Internet erreichbare Server sind permanenten Angriffen ausgesetzt. Sie sollten daher regelmäßig prüfen, ob eine Serverinstallation den aktuellen Sicherheitsansprüchen noch genügt.

Von **Thorsten Eggeling**

Ein eigener Webserver erfordert regelmäßige Kontrolle und Wartung. Angriffe erfolgen teilweise im Sekundentakt. Wenn Sie Sicherheitslücken nicht zeitnah schließen oder der Server durch eine Fehlkonfiguration angreifbar ist, dauert es nicht lange, bis Hacker Ihren Server übernehmen. Es gibt aber Tools und Webdienste, die Sie bei einer sicheren Konfiguration unterstützen.



Website-Status: Der Onlinedienst sitecheck.sucuri.net informiert Sie, ob Ihre Website Schadsoftware oder Spam verbreitet und ob die Domain in Blacklists aufgeführt wird.

Sicherheitsprüfung mit Open VAS

Open VAS (Vulnerability Assessment System) ist eine bewährte Open-Source-Lösung zur Schwachstellenanalyse. Das System sucht nach Sicherheitslücken und liefert einen Bericht über die gefundenen Probleme. Die Installation kann auf einem beliebigen Linux-PC erfolgen, da die Analyse über das Netzwerk erfolgt.

Für den schnellen Einstieg empfiehlt sich eine virtuelle Maschine für Virtualbox, die Sie über *www.openvas.org/vm.html* herunterladen können. Virtualbox muss bereits installiert sein. Wenn nicht, laden Sie das Programm über *www.virtualbox.org* herunter und richten die Software ein. Die OVA-Datei importieren Sie einfach per Doppelklick in Virtualbox.

Schritt 1: Nach dem Start von Open VAS in Virtualbox melden Sie sich als Benutzer „openvas“ mit Passwort „openvas“ an. Merken Sie sich die angezeigte IP-Adresse. Danach wechseln Sie mit *sudo -i* in den root-Kontext. Mit *switchkdb de* stellen Sie zunächst die deutsche Tastaturbelegung ein und erzeugen dann mit

```
openvas-mkcert -f
openvas-mkcert-client -i -n
```

die notwendigen Zertifikate. Mit

```
openvasmd --get-scanners
```

ermitteln Sie die UUID des Open-VAS-Scanners, die Sie in folgende Befehlszeile einsetzen:

```
openvasmd --modify-scanner <UUID>
  --scanner-ca-pub /usr/local/var/
  lib/openvas/CA/cacert.pem
  --scanner-key-pub /usr/local/
  var/lib/openvas/CA/servercert.
  pem --scanner-key-priv /usr/lo
  cal/var/lib/openvas/private/CA/
  serverkey.pem
```

Schritt 2: Nun aktualisieren Sie mit

```
openvas-nvt-sync
openvas-scapdata-sync
openvas-certdata-sync
```

Open VAS auf den neuesten Stand und starten den Dienst mit

```
openvassd
```

Schritt 3: Öffnen Sie die IP-Adresse (-> Schritt 1) in einem Browser im lokalen Netzwerk. Da die SSL-Verschlüsselung über selbst signierte Zertifikate erfolgt, müssen Sie diese Zertifikate im Browser als Ausnahme akzeptieren. Der Einstiegsbildschirm bietet einen „Schnellstart“: Sie geben an dieser Stelle lediglich die IP-Adresse eines Servers ein; Open VAS führt dann alle Tests eigenständig durch und präsentiert die Ergebnisse. Die „Schnellstart“-Tests gehen nicht in die Tiefe, aber geben Auskunft über den allgemeinen Sicherheitszustand des Systems. Der Scan kann einige Minuten dauern, da mehrere Zehntausend Überprüfungen durchgeführt werden. Danach klicken Sie unter „Berichte“ auf das aktuelle Datum. Sollten Schwachstellen vorhanden sein, klicken Sie auf den zugehörigen Link, beispielsweise „Check for SSL Weak Ciphers“. Sie erhalten dann Informationen, mit deren Hilfe Sie das Sicherheitsproblem beseitigen können.

Nach dem Scan können Sie auf Basis der Erkenntnisse eine detaillierte Prüfung einzelner Fehlergruppen durch-

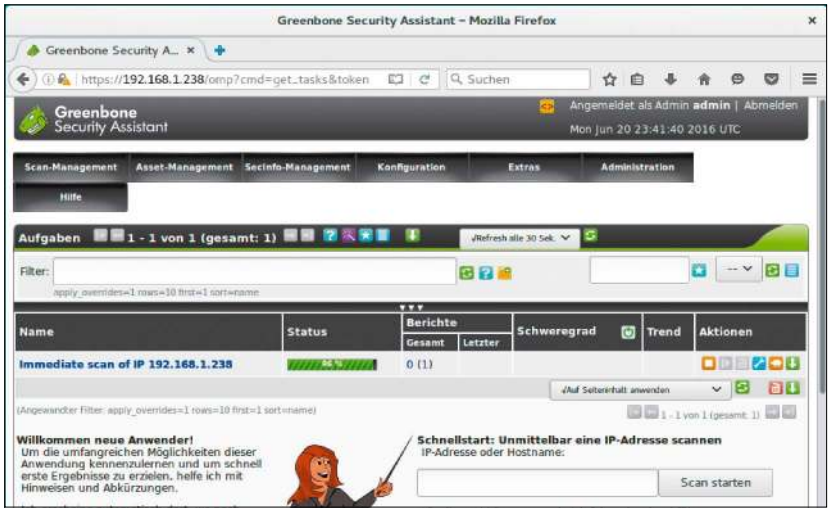
führen. Legen Sie dazu über „Konfiguration/Scan Konfiguration“ eine neue Scankonfiguration an und wählen Sie im nächsten Schritt die gewünschten Fehlergruppen. Zum Abschluss erhalten Sie einen Bericht, welcher die Schwachstellen des Servers zeigt. Open VAS kategorisiert die Probleme in drei Gruppen: High, Medium und Low. Der Gesamtbericht („Full Report“) liefert einen Überblick aller gefunden Schwachstellen.

SSL-Verschlüsselung und HTTP-Header

Einen entscheidenden Beitrag zu mehr Sicherheit im Internet leistet die Verschlüsselung von Webseiten per SSL. Das Verfahren bietet für den Besucher Ihrer Website Schutz vor ungewollten Mitlesern. Außerdem werden auch Passwörter verschlüsselt, etwa für die Anmeldung beim Wordpress-Blog. Die Einrichtung von SSL ist jedoch nicht ohne Fallstricke.

Einige Server verwenden in der Standardkonfiguration veraltetete Protokolle, die als unsicher gelten. Zertifikate können außerdem ablaufen, was Besucher verunsichert und vom Aufruf Ihrer Website abhält.

Wie Sie ein kostenloses Zertifikat für Ihren Webserver erhalten, haben wir unter *www.pcwelt.de/2189443* beschrieben. Einen Test des Servers können Sie über *www.ssllabs.com* durchführen. Klicken Sie auf „Test your server“, tippen Sie den Domainnamen



Sicherheitslücken finden: Open VAS ist nicht ganz einfach einzurichten. Ein Basis-Check lässt sich über die Weboberfläche jedoch schnell durchführen.

ein, und klicken Sie auf „Submit“. Sie erhalten einen Bericht mit Hinweisen zum Problem und Wegen zur Beseitigung. Nachdem Sie die erforderlichen Maßnahmen durchgeführt haben, starten Sie den Test erneut, bis die Einstufung „A+“ erreicht ist.

Weitere Tests führen Sie über *http://securityheaders.io* durch. Der Dienst liefert Informationen zu HTTP-Headern Ihres Servers und zu Headern, die für eine sichere Konfiguration empfehlenswert sind.

Status der eigenen Website ermitteln

Sicherheitsrisiken bleiben nicht lange unentdeckt. Sollte Ihr Server nach einem Hackerangriff Schadsoftware verbreiten, registrieren dies auch Suchmaschinen wie Google oder Bing. Besucher Ihres Internetangebots erhalten dann unter Umständen eine Warnmeldung: Der Zugriff ist erst nach einem Extra-Klick möglich – sofern jemand das Risiko eingeht. Ob Ihr Server Schadsoftware verbreitet oder sogar schon auf einer schwarzen Liste steht, prüfen Sie beispielsweise über *https://sitecheck.sucuri.net*. Tippen Sie die Adresse Ihrer Site ein und klicken Sie auf „Scan Website!“ Sollte das Ergebnis negativ ausfallen, nehmen Sie den Server vom Netz. Prüfen Sie, welche Schadsoftware auf welchem Wege auf Ihren Server gelangt ist. In der Regel stellt nur eine Neuinstallation den sicheren Zustand wieder her.

Sicherheit von Mailservern testen

Fehler in der Konfiguration eines E-Mail-Servers lassen sich besonders leicht ausnutzen. Sollte der Server beispielsweise E-Mails von fremden Domains weiterleiten, landet Ihre E-Mail-Adresse schnell auf einer Spamliste. Daher sollte der Server immer SSL-Verschlüsselung verwenden und E-Mails nur von den eigenen Domains und nur nach Authentifizierung des Benutzers versenden. Das lässt sich relativ leicht über Anfragen mit Telnet an den eigenen Mailserver testen:

```
telnet mail.meinedomain.de 25
```

Danach tippen Sie folgende drei Zeilen ein und bestätigen jeweils mit Eingabetaste:

```
HELO test.xx
MAIL FROM: xx@test.xx
RCPT TO:<user@mail.de>
```

In der letzten Zeile verwenden Sie eine gültige Mailadresse, die aber nicht von Ihrem Server verwaltet wird. Das Ergebnis sollte „Relay access denied“ lauten. Erscheint dagegen „ok“, sendet Ihr Server E-Mails auch an Adressen, für die er nicht zuständig ist. Da es noch mehr Methoden gibt, dem Server unberechtigte E-Mails unterzuschieben, sollten Sie für Tests ferner den Dienst *www.mailradar.com* verwenden. Klicken Sie auf „SysAdmin Tools“ und dann auf „Open Relay Test“. Tippen Sie die IP-Adresse Ihres Mailservers ein und dann auf „Test“. Auch hier sollte das Ergebnis immer „Relay access denied“ lauten.

Starthilfe für Linux

Linux will nicht mehr starten oder lässt sich gar nicht erst installieren. Mit den richtigen Werkzeugen und unseren Tipps reparieren Sie die Bootumgebung oder die Linux-Konfiguration.

Von **Thorsten Eggeling**

Ohne Fremdeinwirkung wird die Linux-Bootumgebung selten zerstört. Meist führt die Installation anderer Betriebssysteme auf dem PC zu Problemen oder ein fehlgeschlagenes Update oder Upgrade ist schuld. Oft sind es auch nur Kleinigkeiten, die den Start von Linux verhindern, etwa eine falsche Bios-Einstellung (-> Punkt 1) nach einem Stromausfall oder ein loses Kabel im PC. Liegt ein Fehler in der Bootloader-Konfiguration vor, hilft das Linux-Installationsmedium oder ein anderes Notfallsystem. Die Bootumgebung lässt sich darüber wiederherstellen (-> Punkte 7 und 8).

Startprobleme können auch nach der Linux-Neuinstallation auftreten. Der Bildschirm bleibt dann beispielsweise dunkel, nachdem Sie das Installationssystem von der DVD booten oder Linux das erste Mal nach der Installation starten.

Mit einiger Hardware kommt Linux nicht auf Anhieb zurecht, was sich aber durch spezielle Startparameter beheben lässt. Informationen dazu finden Sie im Kasten „Bootoptionen bei Linux-Systemen“. Ein schwarzer Bildschirm zeigt sich beispielsweise auch nach einer missglückten Installation des Grafiktreibers. Auch hier ist ein Notfall- oder Zweitsystem hilfreich, über das Sie Konfigurationsdateien ändern oder den Treiber zurücksetzen können (-> Punkt 5).

Wir beziehen uns in diesem Artikel hauptsächlich auf Ubuntu 16.04. Die Gnome-Version finden Sie auf der Heft-DVD. Die Tipps gelten sinngemäß aber auch für andere Systeme.

© VRD - Fotolia.com

1. Die Einstellungen im Bios prüfen

Der erste Weg bei Startproblemen sollte immer in die Bios/Firmware-Einstellungen führen. Sie gelangen in das Bios-Setup, indem Sie die Tasten Entf (Del), Esc oder F2 kurz nach dem Einschalten des PCs drücken. Die genaue Tastenkombination finden Sie im Handbuch zur Hauptplatine, eventuell auch am Bildschirm.

Die Einstellungen fürs Booten finden sich meist unter „Advanced BIOS Features“, „Boot Features“, „Boot“ oder ähnlich lautend. Suchen Sie die Option für die Reihenfolge der Bootgeräte und setzen Sie das Bootlaufwerk an die erste Stelle.

Sollte die Bootfestplatte nicht auftauchen, kontrollieren Sie im PC, ob Stromversorgung und Datenkabel richtig an die Festplatte angeschlossen sind. Bei laufendem PC kontrollieren Sie auch, ob der Laufwerksmotor einer Festplatte läuft oder ob die Festplatte ungewöhnliche Geräusche von sich gibt. Letzteres weist auf einen Schaden hin, der dazu führen kann, dass das Laufwerk vom Bios nicht mehr erkannt wird. In diesem Fall können Sie die Festplatte nur austauschen und die Daten aus einem Backup wiederherstellen.

Bei neueren Rechnern, die mit Windows 8 oder 10 ausgeliefert wurden, ist meist Uefi und Secure-Boot aktiviert. Die meisten Linux-Versionen laufen mit diesen Einstellungen problemlos. Sollte die auf Ihrem PC installierte Linux-Distribution Secure-Boot nicht unterstützen, müssen Sie die Funktion abschalten, sonst startet das System nicht. Das Gleiche gilt, wenn Sie Linux im Bios-Modus installiert haben. Sie müssen dann – wenn vorhanden – eine Option wie beispielsweise „UEFI only“ auf „UEFI and legacy“ oder ähnlich setzen.

Bootverhinderung: Die meisten Linux-Systeme starten auch bei aktiviertem Secure-Boot. Im Zweifelsfall sollten Sie die Option im Firmwaresetup des PCs jedoch abschalten.

2. System über Super Grub Disk 2 starten

Alle aktuellen Linux-Distributionen verwenden Grub 2 als Bootmanager. Bei der Installation im Bios-Modus ersetzt Grub einen eventuell schon vorhandenen Linux- oder Windows-Bootloader, baut aber bei einer Multiboot-Umgebung die anderen Systeme in das Bootmenü ein.

Wenn Sie hingegen Windows nach Linux installieren, wird Grub durch den Windows-Bootloader ersetzt und Sie können Linux nicht mehr starten. Erfolgt die Installation auf neueren PCs im Uefi-Modus, spielt die Installationsreihenfolge keine Rolle. Die Bootloader sind hier in der EFI-Partition untergebracht und stören sich nicht gegenseitig.

Bei einem defekten Bootloader hilft Super Grub Disk 2 weiter. Dabei handelt es sich um einen eigenständigen Grub-Bootloader. Die Software sucht automatisch nach bootfähigen Partitionen und nach Bootloadern. Über ein Menü steuern Sie die gewünschte Startumgebung an.

Super Grub Disk 2 lässt sich von der LinuxWelt-DVD („Extras und Tools“) nur im Bios-Modus booten. Für den Uefi-Modus müssen Sie aus der ISO-Datei selbst eine bootfähige CD brennen. Die Datei liegt auf der Heft-DVD im Verzeichnis „/Extras“. Oder Sie erstellen einen bootfähigen USB-Stick. Dazu kopieren Sie die ISO-Datei zuerst in Ihr Home-Verzeichnis. Verbinden Sie einen USB-Stick mit dem PC und sichern Sie alle darauf befindlichen Daten. Öffnen Sie ein Terminalfenster und ermitteln Sie mit folgendem Befehl, über welchen Gerätepfad der USB-Stick erreichbar ist:

```
sudo mount
```

Das kann beispielsweise „/dev/sdd“ sein. Hängen Sie dann den Stick mit

```
sudo umount /dev/sdd
```

aus dem Dateisystem aus. Starten Sie in einem Terminalfenster folgenden dd-Befehl:

```
sudo dd if=~/super_grub2_disk_hy
 brid.iso of=/dev/sd[x]
```

Den Dateinamen der ISO-Datei ersetzen Sie durch den Namen der von der Heft-DVD kopierten Datei. Bei „[x]“ tragen Sie die Kennung des USB-Laufwerks ein.

Super Grub Disk 2 verwenden: Booten Sie den PC von der Heft-DVD, der selbst erstellten CD/DVD mit Super Grub Disk 2 oder dem USB-Stick. Achten Sie bei einem Uefi-System darauf, das Bootgerät mit dem vorangestellten „UEFI“ zu wählen. Nach dem Start gehen Sie im Menü auf „Detect and show boot methods“. Super Grub Disk 2

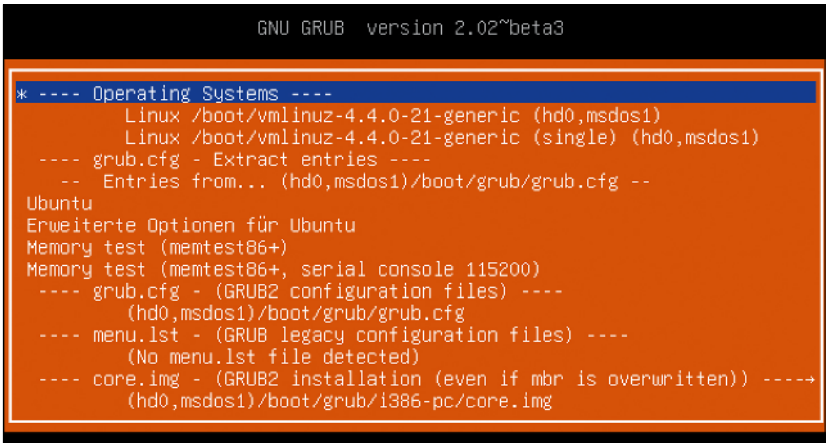
Bootoptionen bei Linux-Systemen

Linux-Installationssysteme sind so konfiguriert, das sie auf den meisten PCs und Notebooks problemlos starten. Gelingt dies nicht, weil das Bios oder Hardwarekomponenten Schwierigkeiten verursachen, steht ein Arsenal weiterer Optionen zur Verfügung. Diese können Sie bei manchen Systemen über vorgefertigte Menüeinträge auswählen oder in jedem Fall manuell über eine Eingabezeile ergänzen.

Bei Ubuntu beispielsweise erscheint kurz nach dem Start vom Installationsmedium nur ein Symbol am unteren Bildschirmrand. Das Menü blenden Sie ein, indem Sie eine beliebige Taste drücken. Danach wählen Sie die gewünschte Sprache. Mit der Taste F6 blenden Sie ein Menü mit gebräuchlichen Zusatzparametern ein. „nomodeset“ wählen Sie beispielsweise, wenn das System nach der Anzeige des Ubuntu-Logos hängenbleibt. „acpi=off“ deaktiviert alle ACPI-Funktionen (Advanced Configuration and Power Interface), die vor allem bei Notebooks zu Startproblemen führen können. Mit der Esc-Taste verlassen Sie das Menü wieder. Diese Parameter und einige mehr können Sie auch in die Zeile hinter „Startoptionen“ eintragen. Bei Problemen etwa mit dem Grafikchip ist oft die Kombination aus „nomodeset“ und „xforcevesa“ empfehlenswert. Nach der Installation des Systems und eines optimierten Treibers (-> Punkt 5) sind die Optionen in der Regel nicht mehr erforderlich.

Bei einem installierten System funktionieren die gleichen Optionen. Im Grub-Bootmenü drücken Sie die Taste E, um in den Editormodus zu wechseln. Tragen Sie die Werte in die Zeile ein, die mit „linux“ beginnt. Die Angaben werden jedoch nicht dauerhaft gespeichert.

Sollten sie für den reibungslosen Systemstart erforderlich sein, tragen Sie die Parameter in die Datei „/etc/default/grub“ hinter „GRUB_CMDLINE_LINUX_DEFAULT“ ein und übernehmen die Änderungen mit *sudo update-grub*. Eine Übersicht mit allen Ubuntu-Bootoptionen und Tipps dazu finden Sie über *www.pcwelt.de/VMWpYN*.



Ersatz-Grub: Ist der Bootloader Grub defekt oder falsch konfiguriert, booten Sie den PC mit Super Grub Disk 2 und wählen im Menü das gewünschte System.

sucht nach Linux-Systemen und zeigt diese in einem Menü an. In der Regel genügt es, den gewünschten Eintrag unter „Operating Systems“ oben in der Liste zu wählen, beispielsweise „Linux /boot/vmlinuz-4.4.0-21-generic (hd0, msdos1)“. Wenn das nicht funktioniert, probieren Sie den Eintrag unterhalb von „---- core.img“ aus.

Super Grub Disk 2 dient nur für den Systemstart im Notfall, repariert aber nichts. Sie können jedoch Grub im System reparieren, das Sie über Super Grub Disk 2 gestartet haben (-> Punkt 3). Sollte das nicht funktionieren, verwenden Sie Rescapp in Rescatux oder Boot Repair Disk (-> Punkt 8).

3. Grub 2 im laufenden System reparieren

Wenn Grub 2 Fehler zeigt, sich das System aber noch booten lässt, installieren Sie Grub 2 neu. Alternativ starten Sie das installierte System über Super Grub Disk 2 (-> Punkt 2).

Bei einem Bios-System verwenden Sie in einem Terminalfenster die zwei Befehlszeilen

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

Für „[x]“ tragen Sie die Bezeichnung für die Bootfestplatte ein. Bei nur einer Festplatte verwenden Sie „sda“. Ist beispielsweise Linux auf „/dev/sdb“ und Windows auf „/dev/sda“ installiert, können Sie auch die Linux-Festplatte als Ziel angeben. Setzen Sie im Bios die Linux-Festplatte in der Liste der Bootgeräte an die erste Stelle. Über das Grub-Bootmenü starten Sie dann Linux oder Windows. Der Vorteil: Wenn Sie Windows neu installieren, bleibt der Grub-Bootloader auf der Linux-Festplatte erhalten.

Bei einem Uefi-System reparieren Sie Grub 2 und die EFI-Dateien im Terminalfenster so:

```
sudo grub-install
```

Ein Ziellaufwerk geben Sie nicht an. Das Script findet das Verzeichnis „/boot/efi“ mit dem Uefi-Bootloader automatisch.

4. Minimales Rettungssystem starten

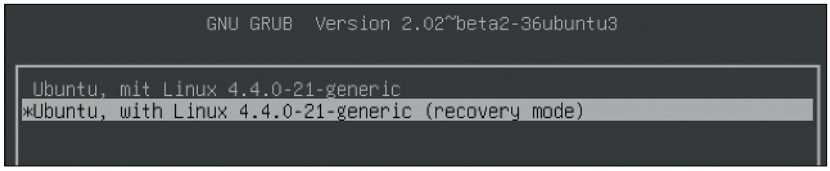
Für einige Reparaturen genügt es, Linux ohne grafische Oberfläche in einem Minimalmodus zu starten. Voraussetzung dafür ist, dass die Bootumgebung noch in Ordnung ist. Wenn nicht, verwenden Sie Super Grub Disk 2 (-> Punkt 2). Nach „Detect and show boot methods“ wählen Sie aus der Liste „Erweiterte Optionen für Ubuntu“ und dann beispielsweise „Ubuntu, with Linux 4.4.0.24-generic (recovery mode)“. Sollte das nicht funktionieren, starten Sie ein Notfallsystem vom USB-Stick oder einer DVD (-> Punkte 6 und 8).

Um das Minimalsystem bei funktionstüchtiger Bootumgebung zu starten, verwenden Sie das Menü des Bootmanagers. Ist nur ein System installiert, erscheint bei Ubuntu das Menü nicht auf dem Bildschirm. Drücken Sie dann kurz nach dem Einschalten des PCs die Tasten Esc oder Shift. Manchmal ist es heikel, den richtigen Zeitpunkt dafür zu finden. Halten Sie einfach die Shift-Taste gedrückt und schalten Sie den Computer ein.

Über das Menü wählen Sie den Eintrag für das Wiederherstellungssystem aus. Bei Ubuntu beispielsweise gehen Sie auf „Erweiterte Optionen für Ubuntu“ und dann auf „Ubuntu, mit Linux 4.4.0-24-generic (recovery mode)“. Die angezeigte Kernel-Version („4.4.0-24-generic“) variiert je nach Ubuntu-Version. Sollten einige Kernel-Updates installiert sein, nehmen Sie den Eintrag mit der höchsten Versionsnummer.

Recoverysystem verwenden: Nach erfolgreichem Start sehen Sie das Wiederherstellungsmenü mit mehreren Optionen. Sie können hier etwa den Netzwerkzugriff aktivieren (Menüpunkt „network“), das Dateisystem überprüfen lassen („fsck“) oder die Konfiguration des Grub-Bootloaders aktualisieren und ihn damit reparieren („grub“). Für Reparaturarbeiten auf der Kommandozeile wählen Sie den Menüpunkt „root Zur root-Befehlszeile (Shell) wechseln“.

Über die Kommandozeile lassen sich Dateien ändern oder kopieren. Das Dateisystem ist im Minimal-Linux jedoch schreibgeschützt eingehängt. Das müssen Sie mit diesem Befehl



Ubuntu reparieren: Im Grub-Bootmenü wählen Sie unter „Erweiterte Optionen für Ubuntu“ den Eintrag mit dem Zusatz „recovery mode“. Damit starten Sie das Reparatursystem.

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

ändern.

5. Grafische Oberfläche reparieren

Bei Problemen mit dem Grafiktreiber hilft es oft, die Standardeinstellungen wiederherzustellen. Dazu setzen Sie einfach die Konfiguration des Xservers außer Kraft:

```
mv /etc/X11/xorg.conf /etc/X11.
  xorg.conf.bak
```

Oft ist die Datei „xorg.conf“ nicht vorhanden und Sie erhalten eine entsprechende Fehlermeldung. Das ist so auch in Ordnung, weil das Grafiksystem (Xserver) sich automatisch konfiguriert und keine Konfigurationsdatei benötigt.

Ist sie jedoch vorhanden, berücksichtigt der Xserver den Inhalt. Die automatische Konfiguration erfolgt auf Basis der gefundenen Hardware und der verfügbaren Treiber.

In einem funktionstüchtigen Ubuntu-System wählen Sie den Treiber in den „Systemeinstellungen“ über „Anwendungen & Aktualisierungen“ auf der Registerkarte „Zusätzliche Treiber“ aus. Meist stehen hier Herstellertreiber von Nvidia, AMD (ATI) oder Intel zur Verfügung (proprietäre Treiber). Diese Treiber leisten mehr als die Standardtreiber, können aber auch Fehler aufweisen, die bei bestimmten Grafikchips zu Fehlfunktionen führen. In diesem Fall kehren Sie wieder zum Standard zurück, indem Sie beispielsweise für einem Nvidia-Grafikchip die Option „X.Org-X-Server - Anzeigetreiber Nouveau“ wählen.

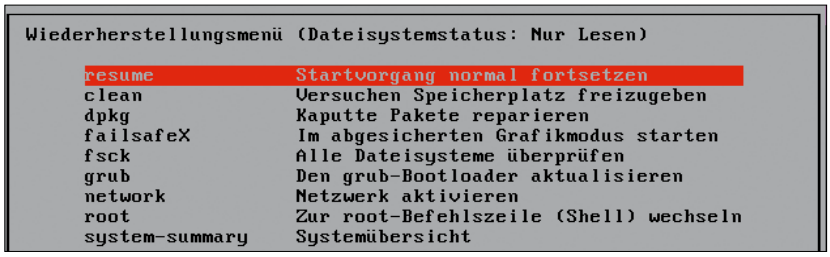
Im Recoverysystem steht auf der Kommandozeile das Tool ubuntu-drivers zur Verfügung, mit dem sich Treiber nur auflisten und installieren, aber nicht wieder entfernen lassen. Das lässt sich jedoch mit folgender Befehlszeile erledigen:

```
sudo apt-get purge nvidia*
```

Bei einem AMD/ATI-Chipsatz verwenden Sie den Befehl

```
sudo apt-get purge fglrx*
```

Fehlt der proprietäre Treiber, verwendet Linux den Standardtreiber.



Wiederherstellungsmenü: Im Recovery Mode zeigt Ubuntu ein Menü, über das Sie nützliche Reparaturfunktionen oder eine Kommandozeile aufrufen können.

Grafikprobleme: Proprietäre Treiber können die Leistung des Systems verbessern, aber auch Fehler verursachen. Der Standardtreiber lässt sich jedoch reaktivieren.

Konfigurationsfehler beheben: Für Fehlfunktionen der grafischen Oberfläche kann nicht nur der Treiber, sondern auch die Konfiguration der Desktopoberfläche verantwortlich sein. Das ist vor allem dann wahrscheinlich, wenn Sie sich zwar anmelden können, danach aber der Desktop nicht erscheint. Legen Sie im Recoverysystem einfach einen neuen Benutzer an:

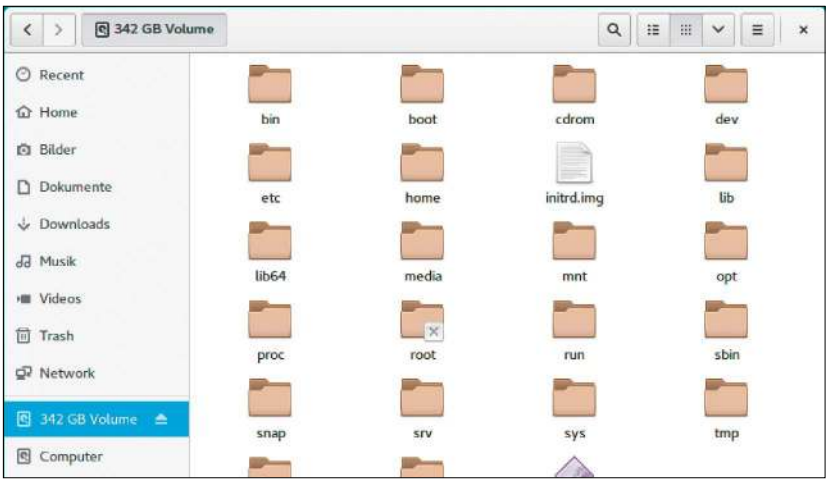
```
adduser Benutzername
```

Verlassen Sie die root-Kommandozeile mit *exit* und melden Sie sich beim neu erstellten Benutzerkonto an. Dessen Einstellungen entsprechen dem Standard. Jetzt funktioniert alles? Dann verwenden Sie in Zukunft dieses Benutzerkonto.

6. Live-DVD für Rettung und Reparaturen verwenden

Reparaturen lassen sich bequem vom Livesystem aus durchführen, das Sie ursprünglich für die Linux-Installation verwendet haben. Die genaue Version spielt keine große Rolle. Wichtig ist nur, dass es sich um die gleiche Architektur handelt, also 32 oder 64 Bit. Starten Sie das gewünschte Livesystem von einer DVD oder erstellen Sie einen Bootstick mit Unetbootin (auf Heft-DVD). Wir beziehen uns in diesem Artikel auf Ubuntu 16.04 mit Gnome-Desktop. Die 64-Bit-Version lässt sich von der Heft-DVD im Bios-Modus booten. Für einen Uefi-PC erstellen Sie aus der ISO-Datei eine bootfähige DVD oder Sie verwenden einen USB-Stick.

Nach dem Start des Ubuntu-Gnome-Livesystems öffnen Sie den Dateimanager über „Aktivitäten“ und das drittletzte Icon „Files“. In der Navigation auf der linken Seite taucht die Linux-Partition auf der Festplatte unter der Bezeichnung auf, die Sie ihr gegeben haben. Sollte es keine Bezeichnung geben, steht hier beispielsweise „Datenträger 500 GB“. Per Klick darauf binden Sie die Partition ein. Diese wird unterhalb von „/media/ubuntu-gnome“ in ein Verzeichnis mit der Bezeichnung oder der ID eingehängt. Bei einem Standard-Ubuntu heißt der Ordner „/media/ubuntu“. Wenn sich die Partition einhängen lässt und eingehängt bleibt, ist die Festplatte in Ord-



Dateien bearbeiten oder retten: Im Livesystem binden Sie über den Dateimanager die Systempartition ein, um Dateien zu kopieren oder Konfigurationsdateien zu bearbeiten.

nung und Sie können im Notfall wichtige Dateien auf einen USB-Stick kopieren. Andernfalls prüfen Sie die Verbindung der Festplatte zur Stromversorgung und zum SATA-Adapter. Sollte sich die Partition nicht einhängen lassen und sind von der Festplatte ungewöhnliche Geräusche zu hören, liegt ein Defekt vor. Die Daten sind dann verloren und Sie müssen das Laufwerk austauschen.

Da Sie im Gnome-Livesystem als Benutzer „ubuntu-gnome“ ohne root-Rechte arbeiten, haben Sie über den Dateimanager keinen Schreibzugriff. Um das bei Bedarf zu ändern, öffnen Sie unter Ubuntu mit Strg-Alt-T ein Terminalfenster und verschaffen sich mit dem Befehl

```
sudo -i
```

root-Rechte. Ein Passwort ist nicht erforderlich. Jetzt lassen sich Dateien über die Kommandozeile öffnen und bearbeiten. Wenn Sie die grafische Oberfläche bevorzugen, tippen Sie *nautilus* ein, um den Dateimanager mit root-Rechten zu starten. Sie können jetzt Konfigurationsdateien mit der rechten Maustaste anklicken und im Kontextmenü „Mit gedit öffnen“ wählen, die Datei bearbeiten und die Änderungen speichern.

Installiertes System bearbeiten: Für einige systemnahe Aufgaben ist es nötig, die Linux-Partition in einer chroot-Umgebung zu bearbeiten. In einem Terminalfenster mit root-Rechten verwenden Sie den Befehl

```
chroot /media/ubuntu-gnome/Ubuntu
  System
```

Das root-Verzeichnis „/“ zeigt jetzt den Inhalt des Systems von der Festplatte, und wenn Sie ein Programm starten, stammt dieses ebenfalls vom installierten System. Daher können Sie beispielsweise den Befehl *passwd* verwenden, um ein Passwort zu ändern. Mit *exit* verlassen Sie die chroot-Umgebung wieder.

Sollten innerhalb der chroot-Umgebung Zugriffe auf das Netzwerk oder Geräte unter „/dev“ nötig sein, müssen Sie einige Verzeichnisse einbinden, bevor Sie chroot verwenden:

```
mount -t devtmpfs /dev /System/dev
mount -t devpts /dev/pts /System/
  dev/pts
mount -t sysfs /sys /System/sys
mount -t proc /proc /System/proc
mount -t tmpfs /run /System/run
mv /System/etc/resolv.conf /Sys
  tem/etc/resolv.conf.bak
cp /etc/resolv.conf /System/etc/
  resolv.conf
```

„/System“ ersetzen Sie jeweils durch den Pfad zum installierten System, etwa „/media/ubuntu/UbuntuSystem“. Die letzten beiden Zeilen sind nötig, damit die Namensauflösung im Internet über DNS funktioniert. Wechseln Sie dann mit

```
chroot /media/ubuntu-gnome/Ubuntu
  System
```

in die chroot-Umgebung. Hier können Sie jetzt beispielsweise mit *apt update* die Softwareliste aktualisieren und mit *apt install Paketname* Software installieren. Die Reparatur der Grub2-Bootumgebung ist nach diesen Vorbereitungen ebenfalls möglich (-> Punkt 7). Nachdem Sie die chroot-Umgebung mit *exit* verlassen haben, stellen Sie mit

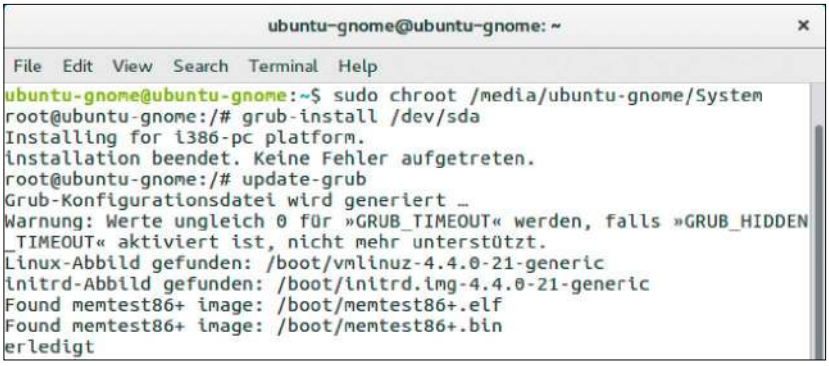
```
mv /System/etc/resolv.conf.bak /
  System/etc/resolv.conf
```

die Originaldatei wieder her.

7. Bootumgebung über eine Live-DVD wiederherstellen

Sie haben den PC von einer Linux-Installations-DVD gebootet und wollen den Bootmanager Grub neu installieren oder konfigurieren? In diesem Fall binden Sie die Dateisysteme ein, wie im -> Punkt 5 beschrieben. Bei einem Uefi-System mounten Sie zusätzlich die EFI-Partition mit

```
sudo mount /dev/sdxy /media/ubun
  tu-gnome/UbuntuSystem/boot/efi
```



Grub reparieren: Im Livesystem wechseln Sie mit dem Befehl chroot in den Verzeichnisbaum des installierten Systems und stellen Grub mit zwei Befehlen wieder her.

Ersetzen Sie „/dev/sdxy“ durch den Pfad zur EFI-Partition. Wenn Sie diesen nicht kennen, verwenden Sie *sudo parted -l*. Das Tool zeigt eine Liste der Partitionen an. Den Pfad zum eingehängten Systemlaufwerk passen Sie ebenfalls für Ihr System an.

Führen Sie sodann folgende vier Befehlszeilen aus:

```
sudo chroot /media/ubuntu-gnome/
 UbuntuSystem
grub-install /dev/sdx
update-grub
exit
```

„System“ ist wieder der Einbindepunkt der Ubuntu-Partition, für „sdx“ setzen Sie den Pfad zum Bootlaufwerk ein. Bei einem Uefi-System lassen Sie „/dev/sdx“ weg.

8. System mit Rescatux reparieren

Rescatux ist ein kleines Notfallsystem, das auf die Reparatur der Linux-Bootumgebung spezialisiert ist. Von der Heft-DVD („Extras und Tools“) lässt sich Rescatux im Bios-Modus starten. Für Uefi-Systeme erstellen Sie aus der ISO-Datei eine bootfähige DVD oder Sie übertragen das System mit dd auf einen USB-Stick, wie in -> Punkt 2 für Super Grub Disk beschrieben.

Rescatux meldet sich nach dem Start mit der Reparaturzentrale „Rescapp“. Hier klicken Sie für die Reparatur der Bootumgebung auf „Restore Grub“ und dann auf „Run“. Wählen Sie die Partition mit der Linux-Installation aus und klicken Sie auf „OK“.

Danach geben Sie die Festplatte an, auf der Sie Grub installieren wollen und klicken auf „OK“. Grub ist danach frisch installiert sowie konfiguriert und Sie können Linux wieder von der Festplatte starten.

Rescatux enthält noch einige weitere Tools, über die Sie das Dateisystem prüfen, das Linux-Anmeldepasswort ändern oder ein System deinstallieren können. Ebenfalls mit dabei ist das Tool Boot Repair, das die Grub-Reparatur mit erweiterten Optionen ermöglicht und ein Backup von Partitionstabelle und Bootsektor erstellen kann.

Notfallsystem: In Rescatux rufen Sie die Reparaturfunktionen über Rescapp auf. Sie können beispielsweise Grub reparieren oder das Anmeldepasswort neu setzen.

Bootumgebung wiederherstellen: Boot Repair ermöglicht die Grub-Reparatur mit einem Klick. Unter „Advanced Options“ stehen aber auch Profifunktionen zur Verfügung.

Boot Repair gibt es in Form von Boot Repair Disk auch als eigenständiges System zum Download (*www.pcwelt.de/FAy1WB*). Wenn Sie Boot Repair Disk im Uefi-Modus starten, ist auch die Reparatur einer EFI-Bootumgebung möglich.

In der Regel genügt in Boot Repair ein Klick auf „Recommended repair“. Das Tool führt dann alle Aufgaben automatisch aus.

Wer mehr Kontrolle über den Prozess haben möchte, klickt auf „Advanced options“.

Um beispielsweise einen fehlenden Windows-Uefi-Bootloader in die Grub-Konfiguration zu integrieren, gehen Sie auf die Registerkarte „GRUB location“. Wählen Sie das Betriebssystem aus, das Sie standardmäßig starten möchten. Hinter „Separate /boot/efi-Partition“ ist bereits die EFI-Partition eingetragen, meist ist das „sda1“. Klicken Sie auf „Apply“, um die Reparatur durchzuführen.

Bei einer Bios-Installation gehen Sie ähnlich vor. Hier legen Sie auf der Registerkarte „GRUB location“ das Standardsystem fest. Wählen Sie die Option für den Grub-Speicherort. In der Regel liegt Grub auf der ersten Festplatte („sda“).

Reparaturinstallation als letzte Rettung

Sollten die in diesem Artikel genannten Reparaturversuche scheitern, versuchen Sie eine Neuinstallation ohne Datenverlust. Dazu booten Sie den PC vom Ubuntu-Installationsmedium und rufen den Installer wie bei der Erstinstallation auf. Folgen Sie den Anweisungen des Assistenten. Im Fenster „Installationsart“ wählen Sie die Option „Ubuntu <Version> neu installieren“. Ihre persönlichen Daten sowie die von Ihnen eingerichteten Programme bleiben dabei erhalten, die Systemeinstellungen werden jedoch zurückgesetzt.

Das funktioniert in der Regel zuverlässig, eine Garantie gibt es aber nicht. Deshalb ist es empfehlenswert, wichtige Dateien vorher zu sichern (-> Punkt 6).

Problemlöser für Ubuntu 16.04

Eigentlich sollte Ubuntu 16.04 als LTS-Version (Langzeitunterstützung) stabiler und unproblematischer sein als reguläre Ausgaben der Distribution. Ubuntu 16.04 läuft aber keineswegs reibungslos und verlangt Nacharbeiten.

Von **David Wolski**

Quelle: Basiert auf „Cape ground squirrel", Yathin S Krishnappa (http://bit.ly/1Zs6BBD), CC-BY-SA

Nach einem festen Rhythmus schickt Canonical alle zwei Jahre eine Ubuntu-Version mit einem Unterstützungszeitraum von fünf Jahren ins Rennen. Diese LTS-Versionen sollen die bisherigen Entwicklungen in Ubuntu auf Desktop und Server konsolidieren und besonders zuverlässig sein – schließlich sollen die Anwender das System jahrelang ohne Neuinstallation einsetzen. Diese Versionen bringen üblicherweise wenig Neues und orientierten sich bei der Auswahl vieler Pakete an den Paketquellen des stabilen Zweiges von Debian, auf dem Ubuntu basiert.

Bei Ubuntu 16.04 hat Canonical mit dieser Tradition gebrochen: Das neue Ubuntu schöpft aus den Paketquellen von Debian „Stretch" und „Sid", aus dem erst das nächste stabile Debian 9 entsteht. Zudem leistet sich Ubuntu 16.04 ganz untypisch für seine Versionsnummer ein ganzes Bündel experimenteller Neuerungen: Es führt „Snaps" als neues Paketformat ein, wechselt auf dem Server zu PHP 7 und liefert ein natives vorkompiliertes Modul zur Unterstützung des Dateisystems ZFS aus. Das sind alles Schritte, die eher zu den kurzlebigen Ubuntu-Ausgaben gepasst hätten, die alle sechs Monate erscheinen. Den Vorwurf, dass die Distribution stagniert, kann man Ubuntu aber nicht mehr machen. Im Dauerbetrieb und bei der Installation auf Notebooks drängt sich jedoch der Eindruck auf, dass Ubuntu 16.04 nicht völlig ausgereift erschienen ist. Dieser Beitrag greift besonders häufige und lästige Hürden bei der Einrichtung und Verwendung des aktuellen Ubuntus heraus und zeigt die Lösungen.

Netzwerk: Das WLAN kommt und geht

In allen Ubuntu-Varianten kümmert sich der Network-Manager um die Verbindung zu Ethernet- und Drahtlosnetzwerken. In Ubuntu 16.04 ist der Network-Manager Quelle vielfältiger Verbindungsprobleme. Auf Notebooks bricht die WLAN-Verbindung regelmäßig ab, das Symbol des Network-Managers stellt die Funktion ein und nach der Rückkehr des Rechners aus dem Ruhezustand gibt es kein WLAN mehr.

Lösung durch Service-Neustart: Bevor ein aktualisiertes Paket für Ubuntu die Bugs im Network-Manager beheben wird, springt als erste Hilfe ein Neustart des Network-Managers ein. Fällt der WLAN-Chip wieder einmal unvermittelt aus, so setzt ihn dieser Terminalbefehl wieder in Gang:

```
sudo service network-manager re
  start
```

Es kann danach einige Sekunden dauern, bis die WLAN-Verbindung wieder steht und das Symbol des Network-Managers rechts oben auch funktionstüchtig ist.

Lösung für Ruhezustandsfehler: Ein verwandtes Problem ist ein lahmgelegter WLAN-Chip nach dem Aufwachen des Rechners. In diesem Fall hilft eine Ergänzung der Systemd-

Keine Verbindung mehr: Ein Bug im Network-Manager legt in Ubuntu 16.04 regelmäßig den WLAN-Chip lahm. Das Problem tritt auch nach der Rückkehr aus dem Ruhezustand auf.

Scripts für den Ruhezustand weiter, die den Network-Manager automatisch neu startet. Dazu öffnet der Befehl

```
sudo -H gedit /etc/systemd/system/
  wlan-resume.service
```

den Texteditor Gedit mit root-Rechten. In die neu angelegte, noch leere Scriptdatei „/etc/systemd/system/wlan-resume.service“ kommen die Zeilen aus dem Kasten „Listing: Network-Manager neu starten“.

Der Inhalt des Kastens ist für bequemes für Copy & Paste als Codeschnipsel auch unter *http://pastebin.com/A2jv5T4z* hinterlegt. Nach dem Speichern des Scripts muss dieses noch mit dem Kommando

```
sudo systemctl enable wlan-resume.
  service
```

aktiviert werden. Ab jetzt wird Systemd den Network-Manager nach dem Erwachen des Rechners selbständig neu starten.

Verlorener Mauszeiger nach Ruhezustand

Eine weitere Komplikation nach dem Ruhezustand wirkt sich auf den Mauszeiger aus, der bei vielen Ubuntu-Systemen nach dem Aufwachen nicht mehr sichtbar ist. Das Problem tritt in Ubuntu 16.04 bei verschiedenen Intel-Grafikchips auf, egal ob auf Desktop-PCs oder Notebooks.

Lösung: Fehlt der Mauszeiger, dann helfen ein Wechsel auf eine textbasierte Konsole und die Rückkehr auf die grafische Benutzeroberfläche schnell weiter. Die Tastenkombination Alt-Strg-F1 springt zur ersten Konsole. Hier ist nichts weiter zu tun, als mit der Kombination Alt-Strg-F7 wieder zurück zum Desktop zu gehen, der jetzt wieder einen Mauszeiger anzeigt.

Notebooks mit flackerndem Bildschirm

Wer mit einem Notebook arbeitet, in dem einer der verbreiteten und in Linux üblicherweise unproblematischen Intel-Grafikchips arbeitet, wird oft von einem besonders lästigen Flackern des Bildschirms heimgesucht. Je nach Modell des Intel-Chips kann das Flackern in Ubuntu 16.04 so heftig ausfallen, dass produktives Arbeiten unmöglich wird. Besonders Intel Core-i-Prozessoren der 6. Generation sind betroffen (Skylake).

Lösung: Ein Kernel-Update mit neuen Intel-Treibern wird das Flackern in absehbarer Zeit gewiss beheben. Bis es soweit ist, hilft vorerst eine Änderung an der Methode der Grafikbeschleunigung. Anstatt die neuere, schnelle Methode „SNA“ zu verwenden, die standardmäßig aktiv ist, kann die langsamere Methode „UXA“ Bildschirmflackern und andere Darstellungsfehler vermeiden.

Der Wechsel zu UXA erfordert eine Konfigurationsänderung an Xorg. Ubuntu 16.04 bringt dafür schon eine Datei mit: Das Terminal-Kommando öffnet

```
sudo -H gedit /usr/share/X11/xorg.
  conf.d/10-quirks.conf
```

die Datei „0-quirks.conf für kleinere Xorg-Anpassungen. Hier müssen Sie

Listing: Network-Manager neu starten

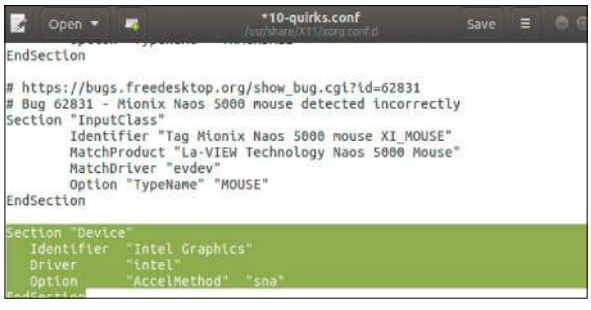
```
[Unit]
Description=Network-Manager neu
  starten
After=suspend.target
After=hibernate.target
After=hybrid-sleep.target

[Service]
Type=oneshot
ExecStart=/bin/systemctl restart
  network-manager.service

[Install]
WantedBy=suspend.target
WantedBy=hibernate.target
WantedBy=hybrid-sleep.target
```

Listing: Intel-Grafikbeschleunigung

```
Section "Device"
   Identifier  "Intel Graphics"
   Driver      "intel"
   Option      "AccelMethod"  "uxa"
EndSection
```

am Ende der Datei die fünf Zeilen aus dem Kasten „Listing: Intel-Grafikbeschleunigung“ eingeben. Anschließend ist noch eine Ab- und Anmeldung am System nötig, um die Änderung zu aktivieren.

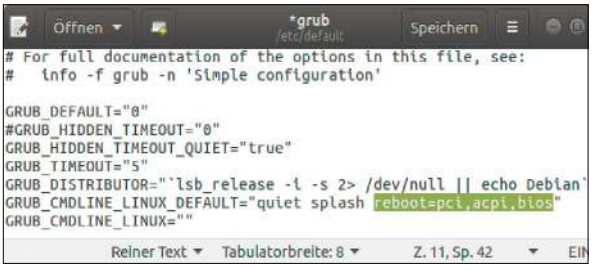
Sonderfall VLC: Die Änderung der Grafikbeschleunigung hat keine Auswirkungen auf die Darstellungsfehler von Videos in VLC unter den neuesten Intel-Core-i-Prozessoren (Skylake). Bis neue Skylake-Treiber in Ubuntu 16.04 über ein Kernel-Update zur Verfügung



Grafikbeschleunigung auf Intel-Hardware wechseln: Wenn der Bildschirm eines Notebooks unentwegt flackert, dann hilft diese Änderung am Grafiktreiber in der Konfiguration von Xorg.

Probleme mit Videos unter Intel-Skylake-CPUs: Die Ausgabe von Videos mit Hardwarebeschleunigung ist bei den Treibern, die Ubuntu 16.04 derzeit mitbringt, noch nicht fertig.

Neustart ohne Hänger: Der Linux-Kernel kennt mehrere Methoden, einen Reboot auszulösen. Die drei Methoden „pci, „acpi“, „bios“ haben sich bei Notebooks vieler Hersteller bewährt.



DVDs abspielen: In den Paketquellen von Ubuntu gibt es keinen DVD-Codec. Diesen gibt es aber noch als Quelltext, der einfach selbst zu einem Paket kompiliert wird.

stehen, muss in VLC die „Beschleunigte Videoausgabe“ unter „Werkzeuge -> Einstellungen -> Video“ abgestellt werden.

Das System hängt beim Abschalten

Auf bestimmter Hardware funktioniert ein reguläres Abschalten oder Neustarten nicht, da Ubuntu auf dem Shut-down-Bildschirm verharrt. Ohne Betätigung der Powertaste geht es nicht weiter.

Lösung: Der Grund für die Hänger ist ein Bios oder eine Firmware, welche(s) auf den Neustart durch den Kernel nicht reagieren. Für diese Kandidaten liefert der Linux-Kernel eine Reihe an Parametern mit, um einen Neustart oder ein Abschalten über vorgegebene Methoden zu erzwingen. Diese Parameter müssen aber schon beim Booten des Systems angegeben werden. In Ubuntu 16.04 öffnen Sie dazu die Datei „/etc/default/grub“:

```
sudo -H gedit /etc/default/grub
```

Die Zeile „GRUB_CMDLINE_LINUX_DEFAULT=“ enthält die Kernel-Parameter. An deren Ende kommt nun noch die Ergänzung

```
reboot=pci,acpi,bios
```

innerhalb des abschließenden Anführungszeichens. Damit der Rechner das nächste Mal mit diesen Parametern startet, muss der Bootloader Grub noch mit dem Kommando

```
sudo update-grub
```

aktualisiert werden.

Anmeldung: Den Gast entfernen

Ubuntu und seine offiziellen Varianten bieten auf dem Anmeldebildschirm die Option eines Gastzugangs. Der erlaubt eine Anmeldung ohne Passwort und eine eingeschränkte Nutzung des Systems mit einem temporären Home-Verzeichnis. Wer die Gastsitzung loswerden möchte, sucht in den Systemeinstellungen vergeblich, denn das Gastkonto taucht dort unter „Benutzer“ nicht auf.

Lösung: Die Gastsitzung von Ubuntu basiert nicht auf einem normalen Benutzerkonto, sondern auf einer Funktion des Anmeldemanagers Light DM. Der Gast ist mit strengen Einschränkungen belegt. Beispielsweise ist es nicht möglich, vom Gastkonto mit „su“ in ein anderes Konto zu wechseln. Alle gespeicherten Dateien und Einstellungen werden bei der Abmeldung wieder gelöscht. In der Konfiguration von Light DM lässt sich der Gastzugang deaktivieren. Dazu ist in einem Terminal nur die Eingabe von

```
echo "allow-guest=false" | sudo
  tee --append /etc/lightdm/light
  dm.conf
```

nötig. Ab dem nächsten Neustart ist das Gastkonto verschwunden.

DVDs abspielen: Codec nachrüsten

Ein Codec zum Abspielen von DVDs ist in Ubuntu 16.04 wie schon beim Vorgänger aus patentrechtlichen Gründen nicht mehr enthalten. Es gibt auch kein fertiges binäres Paket in den Ubuntu-Paketquellen, um es selbst nachzurüsten.

Lösung: Es bleibt weiterhin die Möglichkeit, den Codec für DVDs aus einem Quellcodepaket selbst zu kompilieren. Ubuntu 16.04 vereinfacht diesen Weg mit einem Installationsscript, das im Terminal mit dem Befehl

```
sudo apt-get install libdvdread4
```

installiert wird. Dem eigentlichen DVD-Codec baut dann das folgende Kommando

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

zusammen und installiert anschließend das fertige Paket.

Systemupgrade: Codecs werden nicht erkannt

Nach einer Aktualisierung von Ubuntu 14.04 oder 15.10 auf die neueste Ausgabe 16.04 bleiben viele Abspielprogramme stumm beziehungsweise bei Videos schwarz. Das System findet die passenden Codecs nicht.

Lösung: Eine zwischengespeicherte Konfigurationsdatei zur Codec-Konfiguration unter Unity und Gnome bleibt bei einem Systemupdate erhalten und verhindert, dass Programme die passenden Gstreamer-Codecs finden. Der Befehl

```
rm -r ~/.cache/gstreamer-1.0
```

entfernt den veralteten Zwischenspeicher, der nach einer erneuten Anmeldung am System neu aufgebaut wird.

Wine: Aktuell ist besser

Obwohl Ubuntu bei der Auswahl vieler Pakete auf eigene Versionen oder neue Pakete von Debian Unstable zurückgreift, liegt ausgerechnet Wine nur einer abgehangenen Version 1.6 vor. Bei Wine sind aber aktuelleren Versionen wichtig, da sie stets mit einer besseren Kompatibilität zu Windows-Programmen aufwarten.

Lösung: Das neuere, stabile Wine 1.8 liegt zwar nicht in den Standard-Paketquellen bereit, dafür aber in einem externen Repository (PPA). Der Befehl

```
sudo add-apt-repository
 ppa:ubuntu-wine/ppa
```

Front-End für Wine: Playonlinux ist nicht nur eine Konfigurationshilfe, um Windows-Programme in Gang zu bringen. Es kann auch die aktuellsten Wine-Versionen nutzen.

nimmt dieses PPA auf und über

```
sudo apt-get update
sudo apt-get install wine
```

ist von dort das neuere Wine 1.8 schnell installiert.

Alternative: Einige Windows-Programme verlangen nicht nur eine aktuelle Wine-Version, sondern auch weitere DLLs von Windows. Für diese Programme mit einem komplizierten Installationsweg ist es meist besser, sich von Playonlinux helfen zu lassen, da dieses Front-End einige Konfigurationen für beliebte Windows-Software mitbringt. Mittels

```
sudo apt-get install playonlinux
```

wird das Tool installiert. Im Menü „Werkzeuge -> Wine-Versionen verwalten“ erlaubt auch Playonlinux die Einrichtung neuer Ausgaben von Wine, die dann aber nur innerhalb von Playonlinux zur Verfügung stehen. Ideal ist das für Experimente mit widerspenstigen Windows-Programmen.

Unity: Unsichtbare Menüzeilen

Bei Gnome-Programmen kann es vorkommen, dass in Ubuntu 16.04 auf der Desktopumgebung Unity die Menüleisten des Programmfensters komplett verlorengehen. Auch ein erneuter Start des betroffenen Programms bringt die Leiste nicht zurück.

Lösung: Ein Neustart des Unity-Panels bringt auch die Menüleiste wieder zurück. Der Neustart ist mit dem Kommando

```
initctl restart unity-panel-ser
 vice
```

in einem Terminal schnell erledigt und betrifft dabei nur die obere Leiste. sudo-Rechte sind dazu nicht nötig. Alle Programme und der Desktop laufen dabei weiter, ohne sich zu beenden.

Automatischer Hinweis auf Systemupgrade

Einer der großen Vorzüge Ubuntus ist das Distributionsupdate, das ein bestehendes System ohne Neuinstallation auf die nächste Ubuntu-Ausgabe bringt. Die Aktualisierungsverwaltung blendet einen Hinweis ein, sobald eine neue Version vorliegt, und startet auf Wunsch den Wechsel auf das neue Ubuntu. Wer mit einer regulären Ubuntu-Version wie 15.10 gearbeitet hat, wird den Hinweis bereits erhalten haben, dass 16.04 bereitliegt. Die Anwender, die mit der letzten LTS-Ausgabe Ubuntu 14.04 arbeiten, haben noch keine Benachrichtigung. Denn Canonical ist sich bewusst, dass die ersten Monate nach einer Veröffentlichung der Distribution noch von hektischen Fehlerbehebungen und Bugreports geprägt sind.

Die neue LTS-Ausgabe soll erst dann in der Aktualisierungverwaltung für ein automatisches Update erscheinen, wenn die ersten Kinderkrankheiten ausgestanden sind. Das ist typischerweise erst rund drei Monate nach der Veröffentlichung einer LTS-Version der Fall. Bei Ubuntu 16.04 ist es voraussichtlich Ende Juli soweit und Anwender von Ubuntu 14.04 können ab dann das System aktualisieren. Bleibt der Hinweis der Aktualisierungsverwaltung dauerhaft aus, so ist in den Systemeinstellungen ein Besuch unter „Anwendungen & Aktualisierungen“ nötig. Unter „Aktualisierungen -> Über neue Ubuntu-Versionen benachrichtigen“ muss „Für Langzeitunterstützungsversionen“ ausgewählt sein.

Tipp: Generell lässt sich aber ein Systemupdate zur nächsten LTS-Version auch vor dem Ablauf der drei Monate erzwingen. Folgender Terminalbefehl

```
sudo update-manager -d
```

startet die Aktualisierungsprozedur auf die neue LTS-Ausgabe.

Libre Office automatisch

Libre Office bietet Automatismen wie Speicherfunktionen, Tastenkombinationen, Autotext- und Autofill-Funktionen sowie eine Makro-Programmierumgebung. Wo und wie man diese Möglichkeiten optimiert – oder auch abstellt –, lesen Sie hier.

Von **Hermann Apfelböck**

Bei der Arbeit mit Writer und Calc werden typische Buchstabendreher korrigiert, Aufzählungen, Datumsangaben oder Nummerierungen automatisch erkannt, Zellen intelligent ausgefüllt und Wortvorschläge gemacht. Die Voreinstellungen, die viele Nutzer unkritisch belassen, sind zwar sinnvoll, aber naturgemäß nicht optimiert für individuelle Arbeitsabläufe. Genau wie bei Microsoft Office sind viele Anwender vom gut gemeinten Mitdenken der Software oft sogar genervt. Abschalten? Nein! Mit etwas Anpassung erweisen sich die Autofunktionen als wirkliche Helfer. Die Tipps beziehen sich auf Libre Office 5.1.3.2, wie es das aktuelle Ubuntu 16.04 mitbringt, sollten aber uneingeschränkt auch für ältere Versionen gelten.

Auto-Ersetzen für alle Office-Komponenten

Das Auto-Ersetzen hat eigentlich die Aufgabe, typische Tippfehler wie Buchstabendreher automatisch zu korrigieren. Dafür nutzt Libre Office eine globale Ersetzungsliste, die für alle Komponenten gleichermaßen gilt. Sie können die Autokorrektur unter „Extras -> AutoKorrektur-Optionen“ auf der Registerkarte „Ersetzen“ aber auch als Autotext-Zentrale nutzen.

Libre Office geht an dieser Stelle selbst weit über die Fehlerkorrektur hinaus, wenn es etwa Hunderte von Einträgen wie

```
:Schach Turm weiß:
```

anbietet, die dann durch passende Sonderzeichen ersetzt werden.

Um besonders häufige genutzte Namen und Wörter hier einzutragen, geben Sie unter „Kürzel“ die Kurzform ein wie etwa „#a“ und unter „Ersetzen durch“ das tatsächliche Wort wie etwa „Aminosäure“. Mit „Neu“ und „OK“ ist die Abkürzung gespeichert. Folgt künftig der Eingabe „#a“ eine Leer-, Eingabe- oder Tab-Taste, so schreibt jede Office-Komponente das Wort „Aminosäure“. Ein Sonderzeichen wie hier „#“ ist nicht unbedingt notwendig, stellt aber sicher, dass solche Ersetzungsautomatismen nicht beim Schreiben normaler Wörter ausgelöst werden.

Die Autokorrektur-Liste befindet sich als „DocumentList.xml“ unter „~/.config/libreoffice/4/user/autocorr“ und kann hier auch manuell editiert oder auf andere Rechner übertragen werden.

Wortergänzungen im Writer

Automatische Wortergänzungen unterstützen insbesondere Fachautoren und Studenten, die mit vielen Spezialbegriffen und Personennamen zu tun haben. Das Prinzip der Wortergänzung ist einfach: Der Writer indiziert jeden geladenen Test, sammelt die im aktuellen Text enthaltenen Wörter in einer Liste und schlägt sie beim Tippen vor. Dann genügt die Eingabe weniger Buchstaben, bis ein passender Wortvorschlag erfolgt, den Sie (standardmäßig) mit der Eingabetaste in den Text übernehmen. Je umfangreicher und komplexer der Text, desto umfangreicher fällt die Wörterliste aus.

Anders als Autokorrektur oder Autotext ist die Wortergänzung keine feststehende Liste, sondern eine dynamische Funktion, die sich auf das oder die geöffnete(n) Dokument(e) bezieht. Wenn Sie die Dateien schließen, spätestens wenn Sie Libre Office beenden, löscht Libre Office die Liste. Feineinstellungen über Umfang und Verhalten können Sie unter „Extras -> AutoKorrektur -> AutoKorrektur-Optionen“ auf der Registerkarte „Wortergänzung“ vornehmen. Unter anderem gibt es auch eine Option, die Wortliste beim Schließen eines Dokuments zu löschen, was sich aber nur dann empfiehlt, wenn Sie Texte unterschiedlicher inhaltlicher Ausrichtung erstellen.

Wer das Prinzip verstanden hat, erhält mit der „Wortergänzung“ eine unschätzbare Hilfe, die wenig Arbeit macht: Beim Anlegen neuer Texte genügt es, vorher eine thematisch ähnliche, möglichst umfangreiche Datei zu laden. Deren Wörterliste gilt dann auch für die neue Datei. Wer die Methode optimieren will, kann sich auch eine spezielle Datei „Wörterliste“ anlegen (bei Verlagen oft Standard), die

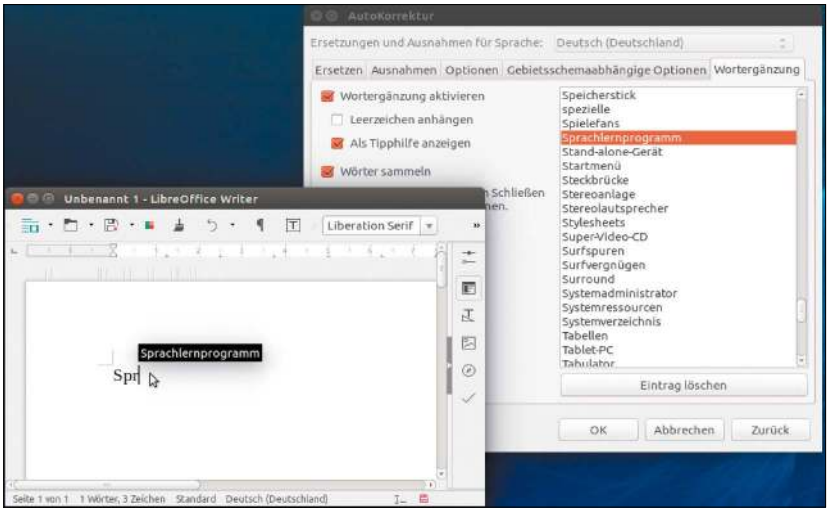
dann wirklich nur die notwendigen Fachbegriffe enthält. Nimmt man einen normalen Text als Basis, sind nämlich stets auch unnötige Wörter und Flexionsformen dabei.

Textbausteine für den Writer

Als umfassende Schreibhilfe gibt es in der Komponente Writer den „AutoText“ (unter „Extras“). Damit erstellte Textbausteine gehen über Wortergänzungen weit hinaus und erlauben den Abruf ganzer Absätze inklusive Formatierung nach Eingabe eines Kürzels. Typische Kandidaten sind etwa Adressen. Um einen neuen Autotext abzulegen, schreiben und formatieren Sie die Passage zunächst optimal, wobei auch Feldfunktionen möglich sind – etwa „Einfügen -> Feldbefehl -> Datum“. Den fertigen Text markieren Sie und starten dann „Extras -> AutoText“ (Strg-F3). Hier vergeben Sie einen beschreibenden Namen und das maßgebliche „Tastaturkürzel“ – etwa „adr“ für die Adresse. Nach Klick auf die Schaltfläche „AutoText“ erscheint die Option „Neu“, die den Textbaustein einfügt, und nach „Schließen“ des Dialogs ist er dauerhaft gespeichert. Die weiteren Möglichkeiten des Dialogs, etwa das Ändern oder Löschen von Bausteinen, erschließen sich weitgehend selbst. Abgerufen wird ein Autotext-Baustein über die Eingabe des Kürzels an der gewünschten Stelle und Drücken der Funktionstaste F3. Autotext ist rechnerübergreifend transportabel, da Libre Office die Bausteine unter „~/.config/libreoffice/4/user/autotext“ speichert.

Autofunktionen in Libre Office Calc

Die Automatismen bei der Zahleneingabe in Calc-Tabellen folgen den üblichen Spreadsheet-Standards. So werden einfache arithmetische oder geometrische Reihen wie „3 – 7 – 11“ erkannt und nach Markieren und Ziehen automatisch mit „15 – 19 …“ erweitert. Für Texteingaben bietet Libre Office Calc die Funktion „AutoEingabe“, die grundsätzlich alle in einer



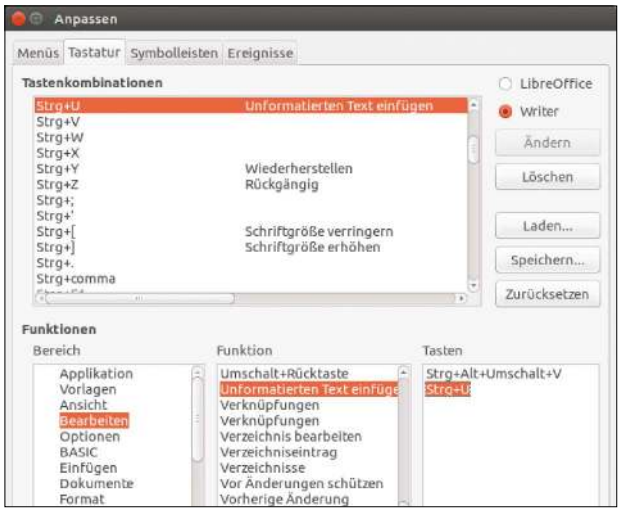
Wortergänzung: Jede (inhaltlich passende) geöffnete Datei kann das Schreiben neuer Dokumente vereinfachen, weil der Writer einen Index erstellt, der auch für andere Dateien gilt.

Standardlisten für Calc: Die Eingabe eines einzigen Eintrags genügt. Danach lässt sich die komplette Liste durch Ziehen mit der Maus in die Nachbarzelle einfügen.

Spalte bereits enthaltenen Einträge erneut anbietet, wenn der Anfangsbuchstabe übereinstimmt. Der Service lässt sich über „Extras -> AutoEingabe“, in älteren Versionen unter „Extras -> Zellinhalte -> AutoEingabe“ abschalten.

Calc scheint auch zu verstehen, dass Sie nach der Eingabe „Januar“ in der Regel die Monatsnamen „Februar“, „März“ benötigen: Es genügt, die Zelle mit dem Eintrag „Januar“ zu markieren und dann mit der Maus nach unten zu ziehen. Diese „Intelligenz“ beruht aber auf einigen simplen vorgegebenen Listen. Über „Extras -> Optionen -> LibreOffice Calc -> Sortierlisten“ können Sie über „Neu“ eigene Listen anlegen – etwa mit sämtlichen Mitarbeitern Ihrer Abteilung, mit Produktnamen, mit Software oder mit Fußballmannschaften. Der Dialog kann auch einen aktuell in Calc markierten Bereich mit „Liste kopieren aus:“ ohne Tipparbeit importieren. Danach genügt dann ein einziger Eintrag der Liste – und Calc wird nach Ziehen dieser Zelle sämtliche weiteren Namen automatisch eintragen.

Die automatische Konvertierung von Eingaben wie „5.1.“ in das Datumsformat „05.01.2016“ ist in der Regel eine begrüßenswerte Vereinfachung, kann aber auch stören – etwa wenn Sie ein Spalte mit Versionsangaben zu Software anlegen wollen. Hier hilft das bewährte Hochkomma (') zu Beginn der Zelle. Um dieses eingeben zu können, müssen Sie aber eine Einstellung ändern: Unter „Extras -> AutoKorrektur-Optionen -> Gebietsschemaabhängige Optionen“ muss das typografische Ersetzen von Anführungszeichen deaktiviert werden. Ein eingegebenes '*5.1.* wird als dann als Text akzeptiert – und das Hochkomma bleibt in Calc unsichtbar.



Tastenkombinationen optimieren: Häufig benötigte Funktionen können Sie hier für den schnelleren Abruf auf den Hotkey Ihrer Wahl legen.

Automatisches Speichern

Bearbeitungsfehler, die man versehentlich gespeichert hat, können zeitaufwendige manuelle Korrekturen nach sich ziehen. Die einfachste Rückversicherung sind automatische Sicherheitskopien des letzten Zustands. Libre Office unterstützt dies durch die Option „Extras -> Optionen -> Laden/Speichern -> Allgemein -> Sicherungskopie immer erstellen“. Ist diese Option aktiv, wird stets die vorherige Dateiversion in das Backupverzeichnis kopiert, sobald eine aktuelle Version gespeichert wird.

Noch mehr Sicherheit entsteht dadurch, dass Sie das Backupverzeichnis auf einem externen Datenträger oder im Netzwerk definieren. Die Einstellungen finden Sie unter „Extras -> Optionen -> LibreOffice -> Pfade ändern“. Tragen Sie beim Eintrag „Sicherungskopien“ nach „Bearbeiten“ den neuen Pfad ein. Dabei ist auch ein ins Dateisystem eingebundener Netzwerkpfad möglich. Die Netzfreigabe sollte dann aber standardmäßig gemountet und immer verfügbar sein.

Tastenkombination optimieren

Libre Office enthält Hunderte von kleinen Funktionen, die man bei Bedarf nur prominenter zugänglich machen muss. Ein typisches Beispiel ist etwa das für Vielschreiber essenzielle Einfügen von purem Text ohne Formatierung und Bildelementen. Das funktioniert einwandfrei mit „Bearbeiten -> Inhalte einfügen -> Unformatierter Text“, nur ist dieser Weg viel zu umständlich. Über „Extras -> Anpassen ->Tastatur“ können Sie den Vorgang auf einen griffigen Hotkey wie etwa Strg-U verkürzen. Klicken Sie dazu unten bei den „Funktionen“ auf den Bereich „Bearbeiten“ und suchen Sie dann daneben die Funktion „Unformatierten Text einfügen“. Danach gehen Sie oben unter den „Tastenkombinationen“ auf „Strg-U“ und klicken auf „Ändern“. Fertig!

Sie werden feststellen, dass die Funktion bereits den Hotkey Strg-Alt-Umschalt-V besitzt, den wir allerdings unhandlich finden und kurzerhand gelöscht haben. Sie werden ferner feststellen, dass Strg-U standardmäßig für das Unterstreichen vorgesehen ist: Wenn Sie das häufig benutzen, sollten Sie natürlich einen anderen Hotkey für das unformatierte Einfügen wählen. „Unformatiert einfügen“ ist nur ein Beispiel: Da jeder Office-Benutzer andere Lieblingsfunktionen alltäglich benötigt, lohnt sich das exemplarisch beschriebene Optimieren auf der „Tastatur“-Registerkarte aber in jedem Fall.

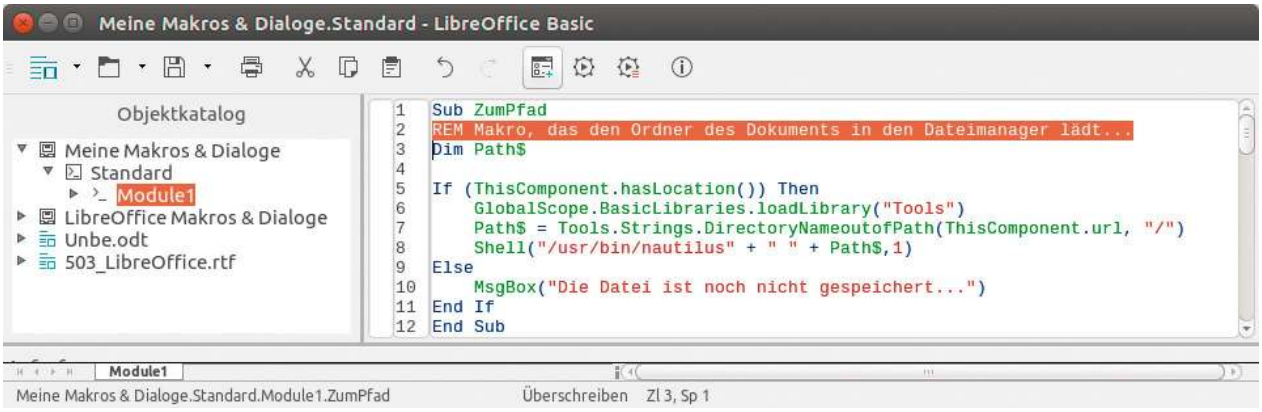
Einfache Makros erstellen

Die Basic-Programmiersprache von Libre Office ermöglicht umfassende Automatisierung – was diesen Beitrag freilich sprengen würde. Wir beschränken uns daher auf grundsätzliche Anregungen und ein sehr einfaches Beispielmakro. Starten Sie die Makroverwaltung mit dem Hotkey Alt-F11 oder über „Extras -> Makros -> Makros verwalten -> LibreOffice Basic“. Wenn Sie noch nie ein Makro erstellt haben, landen Sie auf „Meine Makros -> Standard“ und gelangen mit „Neu“ zum Code-Editor.

Beispiel 1: Um mit einem nützlichen Beispiel Appetit zu machen, verwenden Sie etwa das abgebildete Beispiel: Es öffnet den Ordner des aktuellen Dokuments im Ubuntu-Dateimanager Nautilus (Nemo unter Mint wäre genauso möglich wie der Explorer unter Windows). Dies ist ein typisches Anliegen, um schnell die zum Dokument gehörigen Bilder, Notizen oder URLs zu erreichen. Tragen Sie den Code manuell ein oder kopieren Sie ihn von *http://paste.ubuntu.com/16988469*.

Für den bequemen Zugriff sind solche Makros am besten in die Symbolleiste einzubauen oder per Hotkey abzurufen. Für den Einbau in die Symbolleiste verwenden Sie „Extras -> Anpassen -> Symbolleisten“. Nach „Hinzufügen“ geht es unter „Bereich“ ganz nach unten zu den „LibreOffice Makros“. Unter „Meine Makros -> Standard“ finden Sie das ebene erstellte Makro und binden es mit „Hinzufügen“ in die Symbolleiste ein. In der Symbolleiste können Sie dann mit „Ändern -> Symbol austauschen“ noch ein passendes Icon auswählen. Ein Klick auf das Symbol öffnet den Ordner des Dokuments im Nautilus-Dateimanager.

Beispiel 2: Die Makroverwaltung (Alt-F11) zeigt unter „LibreOffice Makros“ eine Anzahl von Beispielen und praktischen Tools. So kann etwa das Makro unter „Gimmicks -> Autotext“ eine Liste aller aktuellen Autotexte im Writer ausgeben. Wählen Sie dazu einfach das Modul „Autotext -> Main“ und klicken Sie auf „Ausführen“. Es handelt sich um eine reine Übersicht. Für Änderungen der Autotext-Sammlung müssen Sie den Dialog „Extras -> Autotext“ benutzen wie oben beschrieben.



Kleines Beispielmakro: Der Code öffnet den Quellordner des aktuellen Dokuments im Dateimanager und sollte über eine Schaltfläche oder einen Hotkey erreichbar sein. Die wenigen Codezeilen können Sie auch von http://paste.ubuntu.com/16988469 abholen.

Beispiel 3: Das dritte hier erwähnte Makro ist für Engagierte unentbehrlich, verspricht aber weder Spaß noch schnellen Nutzen. Hier geht es um die Objekteigenschaften der Office-Dokumente und darum, dass etwa ein Writer-Text ganz andere Basic-Eigenschaften hat als eine Calc-Tabelle. Um einen Überblick zu erhalten, was Sie in Libre Office Basic mit Texten, Tabellen, Präsentationen und Datenbanken anstellen können, verwenden Sie folgenden Makrocode:

```
Sub Properties
GlobalScope.BasicLibraries.
  LoadLibrary("Tools")
x=ThisComponent
WritedbgInfo(x)
End Sub
```

Wenn Sie diesen Code mit F5 auslösen, erhalten Sie im Writer eine Property-Liste. Beachten Sie, dass diese anders ausfällt, je nachdem, ob ein Writer-Text, eine Calc-Tabelle oder eine Impress-Präsentation aktiv war. Die Listen bieten keine Syntaxanleitung, aber eine Basis, mit der Sie weiter recherchieren und nach konkreten Codebeispielen suchen können. Einschlägige Informationsquellen sind *https://help.libreoffice.org*, *http://api.libreoffice.org/examples/examples.html* und *www.pitonyak.org*.

Hilfestellung durch Makroaufzeichnung

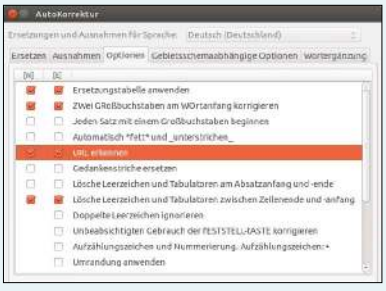
Die Makroaufzeichnung gilt noch als experimentell und ist daher nicht standardmäßig aktiviert. Sie kann aber bei kleingliedrigen Aktionen wie etwa beim Navigieren und Ausfüllen von Calc-Zellen viel Codeecherche und Tipparbeit ersparen. Unter „Extras -> Optionen -> LibreOffice -> Erweitert“ finden Sie die Einstellung „Ermöglicht eine Makroaufzeichnung (eingeschränkt)“. Danach ist unter „Extras -> Makros“ der zusätzliche Menüpunkt „Makro aufzeichnen“ verfügbar. Klicken Sie darauf und führen Sie dann die Menü- und Bearbeitungsaktionen aus, die Sie für Ihr Makro benötigen. Anschließend beenden Sie die Aufzeichnung mit der gleichnamigen Schaltfläche. Damit öffnet sich die Makroverwaltung, wo Sie einen Namen vergeben und das Makro „Speichern“. Über die Makroverwaltung (Alt-F11) können Sie nun Teile des aufgezeichneten Codes in andere Makros einbauen oder das aufgezeichnete Makro manuell ausbauen.

Die Aufzeichnung eignet sich meist nur als Codegenerator für einzelne Aktionen. Ein komplexes Makro werden Sie auf diese Weise nicht erzielen.

Weitere Autokorrektur-Optionen

Bei weiteren Writer-Korrektureinstellungen unter „Extras -> AutoKorrektur -> AutoKorrektur-Optionen -> Optionen“ geht es nicht um schnelles Schreiben, sondern um automatische Formatierungen wie etwa das Erkennen von Webadressen und Umwandeln in klickfähige Hyperlinks. Im genannten Optionsdialog können Sie wählen, welche Aktionen während der Texteingabe erfolgen sollen. Diese werden in der Spalte „[E]“ für Eingabe angezeigt. Generell arbeiten Eingabeautomatismen nur, wenn die Option „Extras -> AutoKorrektur -> Während der Eingabe“ aktiv ist. In der Praxis eher zweitrangig ist die Spalte „[N]“ für spätere Nachbearbeitung, die Sie mit „Extras -> AutoKorrektur -> Anwenden“ auslösen können.

Während eine aktive Autokorrektur meist erwünscht ist, sind manche Details je nach Umfeld eher störend – so etwa das Erkennen und Umformatieren von nummerierten Absätzen. Dies lässt sich an dieser Stelle gezielt abschalten.



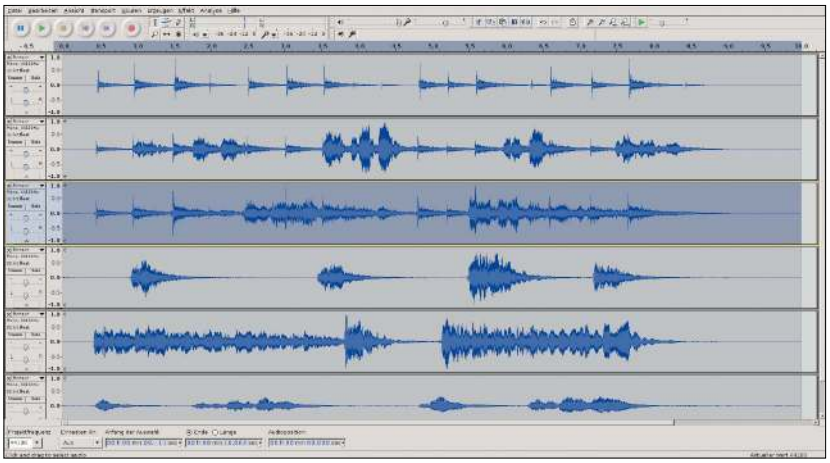
Nicht alle Writer-Automatismen eignen sich für jeden: Einige Details lassen sich hier abschalten.

Musikproduktion mit Linux

Musik am PC muss nicht über Apple- und Microsoft-Software produziert werden. Daniel Schlep, Profimusiker der Rhythmus-Szene, zeigt in diesem Beitrag, dass Linux und freie Linux-Software alle Tools für kreatives Musikschaffen mitbringen.

Von **Daniel Schlep**

Wirft man einen näheren Blick auf das Material professioneller Musiker und Tontechniker, strahlen einem meist „leuchtende Äpfel" entgegen, häufig genug auch ein Windows-Logo. Der Grund hierfür liegt zum einen in der guten Treiberunterstützung, wenn komplexe und speziell angepasste Hardware kommerzieller Firmen zum Einsatz kommt. Zum anderen liegt es aber auch an einer gewissen Ignoranz der Musiker bezüglich möglicher Alternativen. Inzwischen regt sich aber auch in dieser Klientel Kritik an der Firmenpolitik mehrerer kommerzieller Anbieter. Das ist klar, denn Musik basiert auf Freiheit und Kreativität. Wird diese durch zu stark einschränkende Wirtschaftsmechanismen beschnitten, merken das irgendwann auch technisch eher weniger bewanderte Künstler. Linux-Nutzer hingegen sind dafür bekannt, Probleme zu lösen und neue Wege zu suchen, anstatt nur zu konsumieren.



Aufnahme: Der Audioeditor Audacity ermöglicht Mehrspuraufnahmen und hat bereits viele professionelle Features und Effekte zur Nachbearbeitung an Bord.

Arbeitsfeld 1: Die Aufnahme

Im Bereich der freien Software gibt es eine Vielzahl von kreativen Anwendungen, die ein Musiker für sein Schaffen nutzen kann. Diese bieten Lösungen für die Bereiche Audio, Video, Grafik oder auch Kommunikation (etwa für Online-Lessons). All diese Themen sind relevant für den modernen Musiker.

Dieser Überblick konzentriert sich auf das Thema Audio und auf die interessanten Tools für die Aufnahme, die Komposition und die Erzeugung von Musik. Beginnen wir mit einem einfachen Einstieg in den Arbeitsbereich der Tonaufnahme. Tontechniker im Studio arbeiten meist mit zwei Standardmethoden: Entweder wird etwa eine Band direkt komplett live aufgezeichnet oder es werden alle Instrumente und Gesänge in Spuren nach und nach produziert. Audacity ist ein weitverbreiteter Klassiker und wird meist nur als einfacher Audioeditor genutzt. Dabei kann das Programm weitaus mehr. Audacity bietet die Möglichkeit, auch mit zeitversetzten Mehrspuraufnahmen zu arbeiten. So kann man mit diesem Tool nicht nur kleine Audioaufnahmen erstellen, sondern eine ganze Band produzieren.

Für die spätere Nachbearbeitung hält Audacity eine große Auswahl an Effekten parat. Von einem Equalizer über einen Kompressor bis hin zur Rauschentfernung gibt es hier sinnvolle Optionen, um die aufgenommenen Spuren zu verändern.

Eines der größten und oft besprochenen Probleme im Bereich der Aufnahme ist die Latenz, also die zeitliche Verzögerung, die bei der Übertragung von Daten im Computer entsteht. Zur Regulierung gibt es proprietäre Treiber, aber auch freie „Low-latency"-Lösungen. Audacity bietet hier eine spezielle Option, um die Latenz zu kontrollieren. In den Einstellungen finden Sie die „Latenzkorrektur". In diesem Feld kann der User die Latenz manuell in Form von Millisekunden korrigieren.

Das praktische Vorgehen: Man nimmt zwei Spuren nacheinander auf, vergleicht mit Hilfe des Markers und der Zeitanzeige die Länge der optisch sichtbar gewordenen Verzögerung und trägt diesen Wert in die Latenzkorrektur ein. Von nun an ist die Latenz des jeweiligen PC-Systems bestimmt und zukünftige Aufnahmen haben keinen weiteren Zeitversatz.

Mit diesem Vorgehen kann man mit ganz einfachen Mitteln (wie der eingebauten Soundkarte und auch älteren PC-Systemen) gute Ergebnisse erzielen.

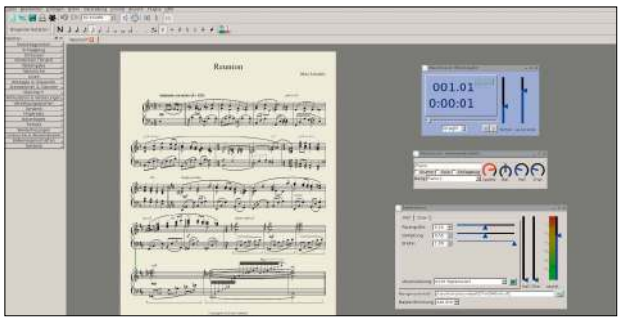
Wem die schon breit gefächerten Funktionen von Audacity nicht genügen, der kann sich auf die gleiche Art und Weise mit einer komplexeren DAW-Software auseinandersetzen. Digital Audio Workstations sind speziell für die Nutzung mit hochwertiger Zusatzhardware ausgelegt. Wie der Name schon sagt, ist diese Sorte von Musikprogrammen tatsächlich als vollständiger Studioersatz gedacht – also als klassisches Tonstudio in digitaler Form. Als freie Software bietet sich etwa das professionell ausgerichtete Programm Ardour an.

Audacity-Website:
www.audacityteam.org
Ardour-Website: *www.ardour.org*
Terminalinstallation unter Debian/Ubuntu & Co:

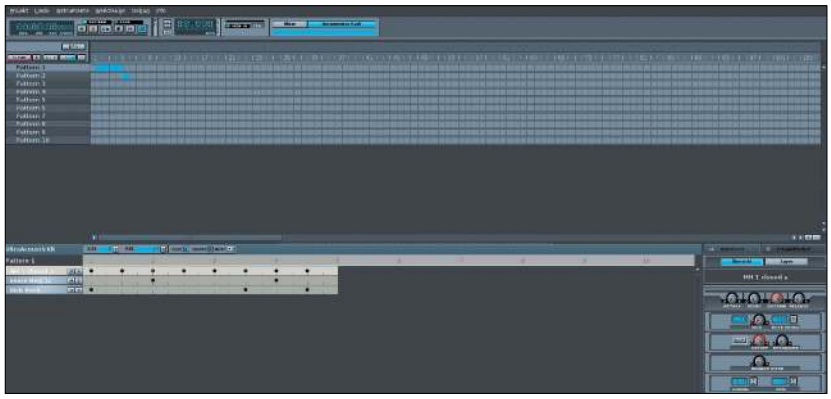
```
apt-get install audacity
apt-get install ardour
```

Arbeitsfeld 2: Die Komposition

Eine zweite Kerndisziplin des Musikers ist das Komponieren im klassischen Sinne. Wer in der Schule gut aufgepasst oder vielleicht auch bereits zusätzlichen Musikunterricht erlebt hat, dem werden klassische Noten nicht fremd sein. Die Welt der freien Software bietet auch hier verschiedene Programme, mit denen Kompositionen niedergeschrieben und arrangiert werden können. Ein bekanntes Tool ist Musescore. Bei dieser Lösung kommt die Midi-Technologie zum Einsatz, die es im Gegensatz zu einer Audioaufnahme ermöglicht, nach Beendigung der Produktion noch Sounds und Stimmen zu wechseln und im Arrangement später noch sehr frei Änderungen durchführen zu können. So ist es auch möglich, Midi-Files anderer Komponisten in die Software zu laden und die Werke nicht nur als Notation zu sehen, sondern auch als Audiodatei zu hören. Für eine klassische Arbeitsweise gibt es hier auch die Option, die Notation auszudrucken. Eine Alternative zu Musescore ist Rosegarden. Dieses Programm ist speziell als Kompositionstool gedacht, bietet aber auch Funktionen für das Aufnehmen von Audiodateien wie im vorherigen Bereich beschrieben.



Komposition: Für die Arbeit mit Midi-Dateien und klassischen Noten ist das Kompositionstool Musescore gut geeignet.



Erzeugung: Mit dem Drum-Sequencer Hydrogen kann man Rhythmik schnell verstehen und erzeugen – auch ohne klassische Notation (siehe Beispiel www.danielschlep.de/Beat6.ogg).

Musescore-Website:
www.musescore.org
Rosegarden-Website:
www.rosegardenmusic.com
Terminalinstallation unter Debian/Ubuntu & Co:

```
apt-get install musescore
apt-get install rosegarden
```

Arbeitsfeld 3: Die Tonerzeugung

Eine weitere Basisdisziplin ist die Erzeugung von Musik. Rhythmus ist eine der ältesten Musikformen und kann dennoch moderner zum Einsatz kommen als viele andere Bereiche. Rhythmus und Rhythmusgefühl befinden sich quasi von Geburt an im Menschen und benötigen nicht zwangsläufig viel Theorie, um verstanden zu werden. Rhythmusinstrumente sind daher ein perfekter Einstieg in die Musik. Produzenten und DJs benutzen Sequencer, die Rhythmus nicht klassisch in Noten, sondern in ein einfaches grafisches Raster fassen. Um auf diese Art und Weise einen Drum-Beat zu erstellen, gibt es die freie Software Hydrogen. Dieses Programm wirkt zunächst unscheinbar, trägt aber viele professionelle Details für Rhythmiker in sich und bietet dabei Sounds von akustischen Schlagzeugen etwa für Rockgenres bis hin zu elektronischen Sounds etwa für Hip-Hop. Auch kann man neben der manuellen Eingabe von Inhalten ein E-Drum als Midi-Controller anschließen und die Funktionen so noch erweitern. Hat man das System der Rhythmik einmal verstanden, kann man schnell selbst kreativ werden. Man setzt einfach einen weiteren Akzent in die vorhandenen Instrumente oder ergänzt an passender Stelle einen neuen Sound aus der Bibliothek.

Hydrogen-Website:
www.hydrogen-music.org
Terminalinstallation unter Debian/Ubuntu & Co:

```
apt-get install hydrogen
```

Neue Software

Linux-Programme als App: Unter den zwölf Softwarevorstellungen sind mit Krita 3.0 und Etcher 1.0 bereits zwei Projekte, die nicht nur in Paketen für bestimmte Distributionen vorliegen, sondern schon in den neuen App-Formaten.

Von **David Wolski**

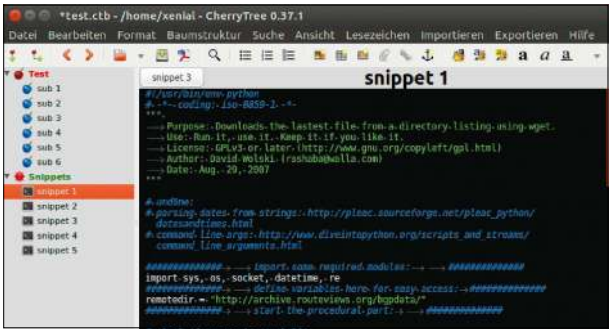
Was müsste auf dem Linux-Desktop geschehen, um dem freien Betriebssystem auf die Sprünge zu helfen? Die illustren Open-Source-Entwickler samt Chef-Pinguin Linus Torvalds sind sich in dieser Sache einig: Die Installation von Software, die nicht von Distributionen fertig paketiert ist, muss viel einfacher werden. Noch einfacher als unter Windows, aber dennoch sicherer als unter Windows. Das App-Modell von Smartphones, Tablets und Chromebooks gilt jetzt für Anwendungen als heiße Alternative zu den klassischen Paketformaten RPM und DEB. Die erfolgreichen Verwandten von Linux-Distributionen machen es vor – schließlich handelt es sich bei Android und Chrome-OS ebenfalls im weitesten Sinne um Linux-Systeme. Nur sind dort Programme als App in einem gut eingerichteten App-Store verfügbar. Dessen App-Format ist weitgehend standardisiert und Entwickler müssen nicht, wie unter Linux, eine Anwendung für jede Art und Version eines Systems einzeln bauen. Mittlerweile sind Android-Apps sogar bei Chromebooks angekommen, denn Google überträgt Google Play derzeit auf seine Netbooks.

Die App-Container kommen

Jetzt freunden sich die großen Linux-Distributionen mit Anwendungen als App an. Zweifellos wird das Anwendern und Entwicklern das Leben auf dem Linux-Desktop einfacher machen. Zähes Tauziehen ist aber bereits vorprogrammiert: Da es hier um Open-Source-Technologien geht, gibt es gleich drei unterschiedliche Ansätze, denn die tonangebenden Softwarehäuser hinter Distributionen entwickeln ihre eigenen Standards: Canonical hat zusammen mit Ubuntu 16.04 den Paketmanager Snappy für Snappakete einer größeren Anwenderschaft zugänglich gemacht. Inspiriert ist Snappy von Ubuntu Touch für Smartphones und Tablets, auf welchen das Basissystem unangetastet bleibt und Apps im Stil von Android separat installiert werden.

Beinahe zeitgleich ist aus dem Gnome-Umfeld mit kräftiger Unterstützung vom Linux-Platzhirsch Red Hat das App-Format Flatpak erschienen, das zuvor als „xdg-app“ auch schon einige Jahre in der Entwicklung war. Der dritte Kandidat ist Appimage, das einen pragmatischen Ansatz für übergreifende Programmpakete wählt und sie einfach nur samt allen Bibliotheken im Benutzerkontext installieren lässt. Alle drei sind der Testphase entwachsen. Es gibt bereits Software, wie etwa das hier vorgestellte Malprogramm Krita 3.0, das schon in allen drei Formaten vorliegt.

Für Linux-Anwender wäre es wünschenswert, wenn sich zumindest Red Hat und Canonical auf ein gemeinsames Format einigten und einen universellen App-Store einrichteten. Das könnte Linux auf dem Desktop tatsächlich einen Schub geben.



Sammeln und ordnen: Cherrytree bringt Ordnung in Notizen und speichert Textschnipsel aller Art in einer Datenbank.

Cherrytree 0.37.1

Organisiert Notizen in Baumstrukturen

Webseite: *www.giuspen.com/cherrytree*

Der digitale Zettelkasten erlaubt eine übersichtliche Kategorisierung und hierarchische Baumstrukturen sowie Verknüpfungen von Aufzeichnungen untereinander. Gut geeignet ist Cherrytree auch für Programmierer, die Beispiele und Codeschnipsel als Referenz sammeln, denn der integrierte Texteditor unterstützt auch Syntaxhervorhebung. Auf der Projekt-Webseite liefert der Entwickler den Quelltext (GPL 3), fertige DEB- und RPM-Pakete sowie ein PPA für Ubuntu.

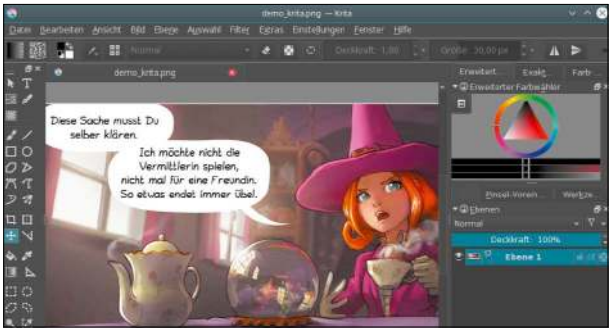
In drei Schritten zum bootfähigen USB-Stick: Etcher überträgt ISO-, IMG- und Archivdateien von Linux-Distributionen.

Etcher 1.0

Schreibt ISO-Dateien auf USB-Sticks

Webseite: *http://etcher.io*

Hybride ISO-Dateien von Linux-Distributionen, also Images, die für den Start von CD/DVD und von USB-Medien geeignet sind, schreibt man am besten mit dd auf das Ziellaufwerk. Das grafische Etcher vereinfacht dies und ist ein plattformübergreifender Ersatz (Linux und Windows) für das Kommandozeilentool dd zur bequemen Übertragung in drei Schritten von ISO-, IMG- und Archivdateien. Die Projekt-Webseite liefert die Linux-Versionen bereits als Appimages aus.



Bilder lernen laufen: Krita 3.0 bringt Animationsfunktionen, verbessert seine Ebenenverwaltung und zeigt Filter in einer Vorschau.

Krita 3.0

Zeichenprogramm für professionelle Ansprüche

Webseite: *http://krita.org*

Das Open-Source-Programm Krita finanziert sich per Kickstarter und wird mittlerweile von einigen Comic-, Animations- und Filmstudios eingesetzt. Im Vordergrund stehen Malwerkzeuge zur Illustration, Zeichentabletts und Filterfunktionen für Zeichnungen, nicht die Fotoretusche. Version 3.0 ist auf Qt5 portiert und bringt einen besseren Dialog für Ebenen und 2D-Animation. Auf der Webseite gibt es Krita als Appimage, in Ubuntu 16.04 als Snappaket und in Fedora als Flatpak.

Beste Beschallung: Mixxx ist ein professionelles DJ-Pult, unterstützt Jack-Audio und arbeitet mit externen Mixern per USB zusammen.

Mixxx 2.0

Player mit Mixer und Crossfader

Webseite: *www.mixxx.org*

Drei Jahre war diese Version des DJ-Players in Arbeit – das Ergebnis kann sich sehen lassen. Das freie Programm (GNU Public License) emuliert ein digitales DJ-Pult und kombiniert bis zu vier MP3-Player. Ein Sampler, Equalizer und Effektgerät können auf der Oberfläche ebenfalls aktiviert werden. Eine Synchronisationsfunktion sorgt dafür, dass alle Tracks im Takt bleiben. Mixxx 2.0 ist in der aktuellen Version bereits in Ubuntu 16.04, Linux Mint 18 und Fedora 24 verfügbar.

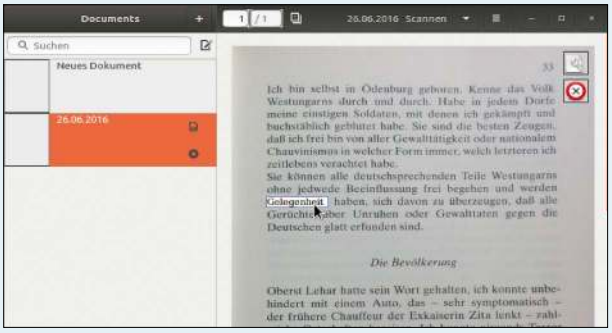
Kompatibel zu Firefox: Palemoon kann trotz aller Unterschiede mit einer Menge Add-ons umgehen. Es hat eine eigene Sync-Funktion.

Palemoon 26.3.1

Schneller alternativer Firefox-Browser

Webseite: *www.palemoon.org*

Langsam, speicherhungrig und zu viele Funktionen: Viele ehemalige Firefox-Anwender sind mit dem Browser unzufrieden und suchen Alternativen. Palemoon ist aus Firefox entstanden, blieb bei der alten grafischen Oberfläche von Firefox 24, hat aber die Browserengine der aktuellen Version übernommen und kann mit viele Firefox-Erweiterungen umgehen. Auf der Projekt-Webseite gibt es Palemoon als ausführbare Binärdatei mit Installer, für Ubuntu und Co. auch ein PPA.



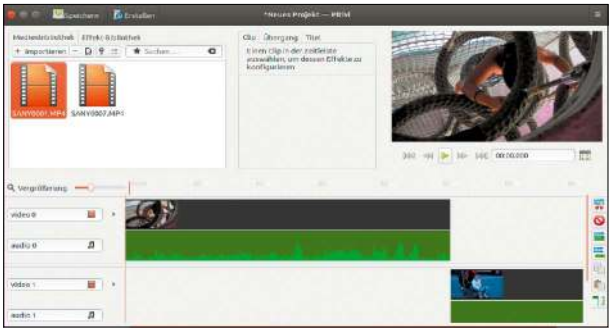
Paperwork erspart unzählige Einzelschritte: Vom Scannen über Texterkennung zum fertigen PDF sind alle Schritte im Nu erledigt.

Paperwork 0.3.0

OCR-Werkzeug mit komplettem Workflow

Webseite: *https://github.com/jflesch/paperwork*

Das Python-Programm Paperwork bildet mit simpler grafischer Oberfläche den Workflow vom Scannen eines Dokuments über Schrifterkennung zur Erstellung einer fertigen PDF-Datei ab. Die eigentliche Arbeit überlässt es bewährten Tools wie etwa Tesseract-OCR zur Schrifterkennung. Eine Vorschau zeigt jede Dokumentseite und den umgewandelten Text an. Die Installation erfolgt in allen Distributionen per Python-Pip. Anleitungen liefert die Projekt-Webseite.



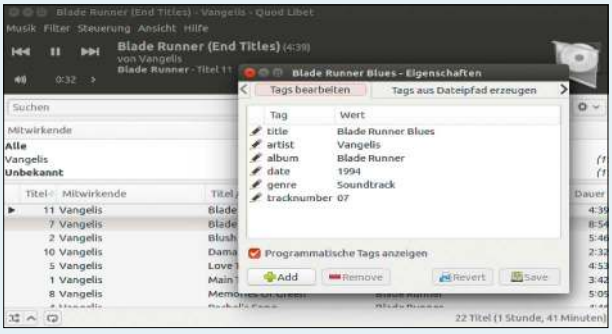
Flotte Einarbeitung: Pitivi verbindet eine gute GUI mit vielen Gestaltungsmöglichkeiten und ist auch für Anfänger bedienbar.

Pitivi 0.95

Nicht-linearer Videoeditor

Webseite: *www.pitivi.org*

Nachdem die letzte Version zu instabil war, ist Pitivi 0.95 wieder brauchbar und in den Paketquellen von Ubuntu 16.04, Mint 18 und Fedora 24 verfügbar. Der Videoeditor erlaubt unkompliziertes Schneiden und Editieren von Clips. Das Überblenden zweier Clips mit Übergangseffekten ist schnell erledigt. Der Editor unterstützt mehrere Spuren und nutzt die Codecs des Gstreamer-Frameworks. Für den Export stehen die wichtigsten Videoformate bereit.



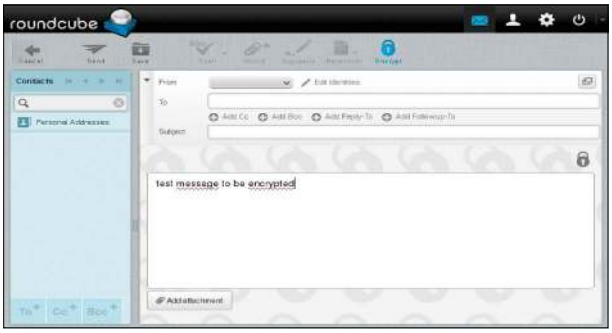
Ordnung für die Musiksammlung: Quodlibet ist ein Player und Tageditor mit fortgeschrittenen Funktionen und zahlreichen Plug-ins.

Quodlibet

Tageditor und Player

Webseite: *http://quodlibet.readthedocs.io*

„Was immer du willst“ (lat. „Quod libet“) nennt sich dieser in der Tat mächtige Tageditor mit fortgeschrittenen Funktionen. Zu den unterstützten Dateiformaten gehören MP3, Ogg Vorbis, Opus, Flac, Musepack, WMA, Wavpack und AAC. Aus den Onlinedatenbanken von Musicbrainz und CDDB können Tags automatisch eingelesen werden. Quodlibet dient auch als Player und kann den Replay Gain berechnen. Pakete für alle wichtigen Linux-Systeme liefert die Webseite.



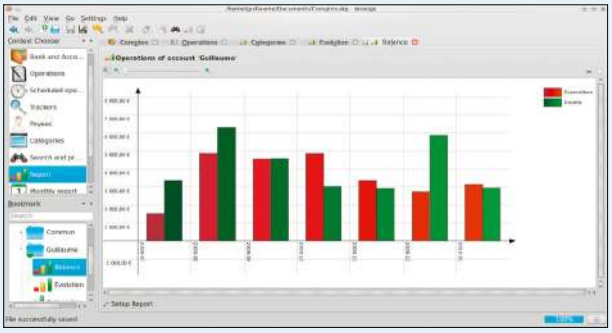
Mailverschlüsselung: Über die Browsererweiterung Mailvelope können jetzt die GPG-Funktionen von Roundcube genutzt werden.

Roundcube 1.2.0

Webbasierender Mailclient mit GPG

Webseite: *https://roundcube.net*

Roundcube ist eine freie PHP- und Java-Software, um per Webmail ein IMAP-Konto zu nutzen. Es ist eine Alternative zu Google Mail und anderen Maildiensten, die Administratoren auf ihrem eigenen Server betreiben können. Das neue Roundcube bietet Mailverschlüsselung per GPG und arbeitet dazu auf dem Client mit der Browsererweiterung Mailvelope (*www.mailvelope.com/de*). Roundcube 1.2.0 ist kompatibel zu PHP 7 und verlangt ein typisches LAMP-Setup.



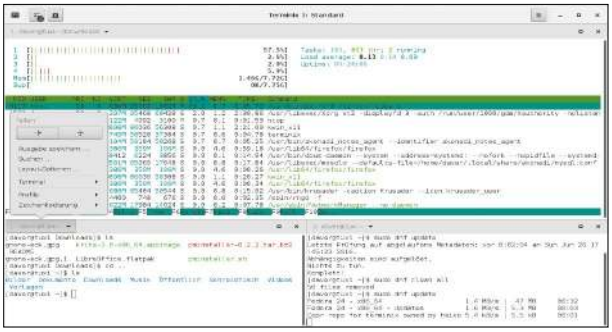
Skrooge ist eine KDE-Finanzverwaltung: Schön (zumindest optisch) ist die Visualisierung von Einnahmen und Ausgaben.

Skrooge 2.4.0

Persönliche Finanzverwaltung

Webseite: *http://skrooge.org*

Das KDE-Programm hat in der neuesten Version den Sprung auf Qt5 für KDE Plasma 5 geschafft. Skrooge verschafft einen Überblick über die Finanzen, auch bei mehreren Konten. Ausgaben und Einnahmen sortiert man in Kategorien oder legt selbst welche an. Wiederkehrende Kosten kann das Programm automatisch in Intervallen buchen und Berichte zeigen, wie es um die Finanzen steht. Die Webseite nennt PPAs für Ubuntu sowie Quellen für Arch Linux und Open Suse.



Terminal teilen: Terminix macht es leicht, auch bei zahlreichen laufenden Shells und SSH-Verbindungen den Überblick zu behalten.

Terminix 1.0

Multiterminal für Gnome

Webseite: *https://github.com/gnunn1/terminix*

Bei der Administration von Servern genügt nur selten ein Terminalfenster. Terminix ist ein Programm für Gnome (GTK3), das eine übersichtliche Aufteilung des Fensters in viele Unterterminals erlaubt. Das Layout lässt sich für die spätere Wiederverwendung sichern. Sind viele Shells geöffnet, zeigt eine seitliche Leiste alle Terminals in einer Miniaturansicht an. Terminix ist derzeit über die Webseite für Fedora, Open Suse und Arch Linux verfügbar, noch nicht für Ubuntu.

Künstliche Intelligenz: Die Computergegner fahren so realistisch, dass Torcs sogar in Forschungsprojekten zum Einsatz kommt.

Torcs 1.3.7

Rennspiel mit realistischem Fahrverhalten

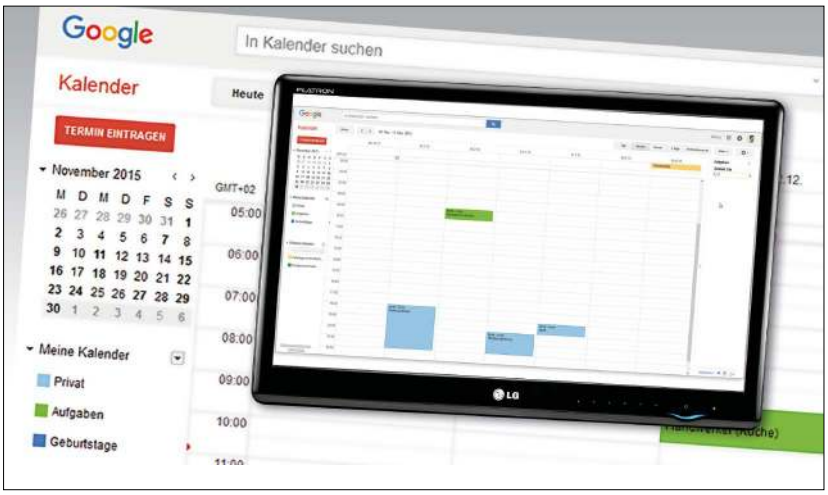
Webseite: *http://torcs.sourceforge.net*

Dass eine aufwendige Rennspielsimulation nicht von großen Spielestudios kommen muss, beweist Torcs („The Open Racing Car Simulator"). Dessen Entwickler begannen schon vor fast 20 Jahren mit Torcs und statteten die Computergegner mit bemerkenswerter künstlicher Intelligenz aus Die Grafik ist nicht aufwendig, aber sehr schnell, und für Langzeitmotivation sorgen insgesamt 41 Strecken und ein Meisterschaftsmodus. Ein PPA liefert Pakete für Ubuntu und Co. ●

Pünktlich dank Raspberry

Wieder mal einen Termin verpasst, weil der Kalender an der Wand nicht umgeschlagen war? Solche Pannen sind mit dem Raspberry Pi Vergangenheit: Der kleine Pi kann mit Hilfe von Google zum elektronischen Jahreskalender umgebaut werden.

Von **Markus Fasse**



Mit diesem Projekt kommen Sie nie mehr zu spät. Und hinter einem Monitor angebracht stören auch keine überflüssigen Kabel. Mit Ausnahme der Stromversorgung empfängt der kleine Rechenknecht Signale und Infos über das WLAN etwa per Fernwartung. In wenigen Schritten zeigt er rund um die Uhr Ihre aktuellen Termine an. Die folgende Anleitung startet bei null. Wenn Sie bereits einen Raspberry nutzen, entfallen in jedem Fall die Punkte 1 bis 3, eventuell auch noch Punkt 4.

1. Der Einkaufszettel

Der wichtigste Teil des Wandkalender-Projekts ist ein Raspberry Pi inklusive Micro-SD-Karte sowie Stromversorgung. Ob Sie zum aktuellen Modell 3 greifen oder einen älteren Pi verwenden, ist für dieses Projekt unerheblich. Möchten Sie den Minicomputer allerdings neben seinem Job als Wandkalender noch mit weiteren Aufgaben betrauen, sollten Sie zum aktuellen Modell greifen.

Darüber hinaus benötigen eventuell einen USB-WLAN-Stick zwecks räumlicher Unabhängigkeit (beim neuesten Raspberry-Modell 3 ist WLAN standardmäßig an Bord), ferner einen Monitor mit HDMI-Anschluss, ein HDMI-Kabel und optional eine Wandhalterung für den Bildschirm.

Da der Raspberry Pi ständig mit dem Internet verbunden ist, sollten Sie ein entsprechendes Heimnetzwerk installiert und betriebsbereit haben. Eine USB-Maus und -Tastatur ergänzen die Ausstattung.

2. Die ersten Schritte

Zunächst müssen Sie den Minicomputer mit einem Betriebssystem ausstatten. Laden Sie sich dafür die aktuelle Version von Raspbian herunter (*www.raspberrypi.org/downloads/raspbian/*). Die bei Redaktionsschluss aktuelle Version war Raspbian Jessie mit circa 1,3 GB. Der Download ist ein gepacktes ZIP-Archiv, das Sie unter Linux mit der Standard-Archivverwaltung ebenso mühelos entpacken wie unter Windows mit der eingebauten ZIP-Unterstützung.

Die resultierende Imagedatei mit knapp vier GB schreiben Sie dann bootfähig auf eine SD-Karte. Dies geschieht mit dem Terminalbefehl

```
sudo dd if=[image] of=/dev/sd[xy]
```

unter Linux, also etwa mit:

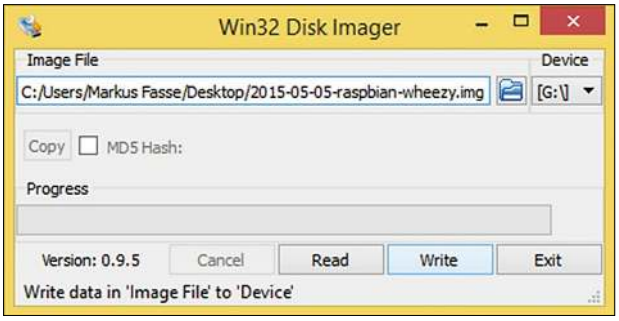
```
sudo dd if=~/2016-05-10-raspbian-
  jessie.img of=/dev/sdc1
```

Das Zielgerät (hier „/dev/sdc1“) ist wie immer in solchen Fällen genau zu kontrollieren, weil es bei der Aktion komplett überschrieben wird. Unter Windows verwenden Sie den Win 32 Disk Imager (auf Heft-DVD, Download unter *http://sourceforge.net/projects/win32diskimager)*.

3. Den Raspberry vorbereiten

Schließen Sie nun Tastatur, Maus, ein LAN-Kabel und gegebenenfalls den WLAN-USB-Stick an den Raspberry Pi an. Verbinden Sie ferner den Minicomputer per HDMI-Kabel mit dem Monitor. Anschließend booten Sie den Pi durch Anschluss an die Stromversorgung. Zunächst sind ein paar Feineinstellungen beim frisch installierten Raspbian nötig: Expandieren Sie zuerst das Dateisystem, damit das Betriebssystem die gesamte SD-Karte ausnutzt. Dies erledigen Sie über den Punkt 1 „Expand Filesystem“. Darüber hinaus müssen Sie noch den Desktopstart aktivieren (Punkt 3 „Enable Boot to Desktop“), damit der Google-Kalender später sofort angezeigt wird. Ferner sollten Sie im Setup ein sicheres Passwort vergeben (Punkt 2 „Change User Pass-

word“). Folgen Sie in allen Fällen einfach den Anweisungen auf dem Bildschirm. Zu guter Letzt aktivieren Sie SSH. Über die Secure Shell können Sie auf Ihren Raspberry jederzeit über das Netzwerk zugreifen. Das ist praktisch bis unentbehrlich, um Wartungsarbeiten durchzuführen. Den entsprechenden Punkt finden Sie im Menü „Advanced Options“.

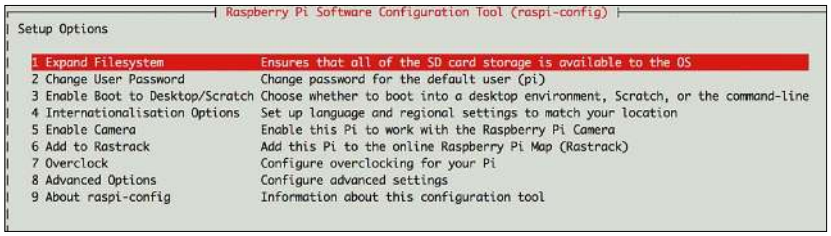


Bootfähiges Image auf die Karte schreiben: Mit dem Programm Disk Imager kopieren Sie das Raspbian-Image unter Windows auf eine SD-Karte.

4. WLAN installieren

Der Raspberry Pi ist bereits über das LAN-Kabel mit dem Internet verbunden. Um Kabelsalat zu vermeiden, sollte der Kalender aber später über WLAN laufen. Ohne Umstand funktioniert das mit dem Raspberry 3 und seinem integriertem WLAN-Chip. Für ältere Modelle gibt es WLAN-USB-Sticks, die in der Regel nach einem Neustart des Systems automatisch erkannt werden.

Zur Kontrolle geben Sie im Terminal den Befehl *lsusb* ein. Sie sehen nun sämtliche angeschlossenen USB-Geräte und der WLAN-Adapter sollte mit der Typenbezeichnung des Herstellers zu finden sein. Erfahrungsgemäß tadellos funktionieren beispielsweise der Edimax EW-7811UN für rund acht Euro oder der CSL 300 MBit/s WLAN-Stick für rund 13 Euro.



Ersteinrichtung: In der Konfiguration des Raspberry Pi nehmen Sie wichtige Einstellungen vor, die für dieses Projekt nötig sind – etwa das Booten in den grafischen Desktop.

Um den Raspberry mit dem WLAN zu verbinden, klicken Sie in der grafischen Oberfläche auf das Programm Wifi Config. Wählen Sie im Feld „WLAN-Adapter“ Ihren Stick aus und scannen Sie anschließend nach der SSID des kabellosen Netzwerkes. Klicken Sie in der Ergebnisliste Ihr Funknetz doppelt an und tragen Sie das Passwort ein.

Ins WLAN per SSH-Terminal: Wenn Sie den Raspberry Pi ohne grafische Oberfläche konfigurieren, geben Sie im Terminal den Befehl

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

ein. Der Editor zeigt eine Konfigurationsdatei, an dessen unteren Zeilen folgende Informationen zu finden sein sollten:

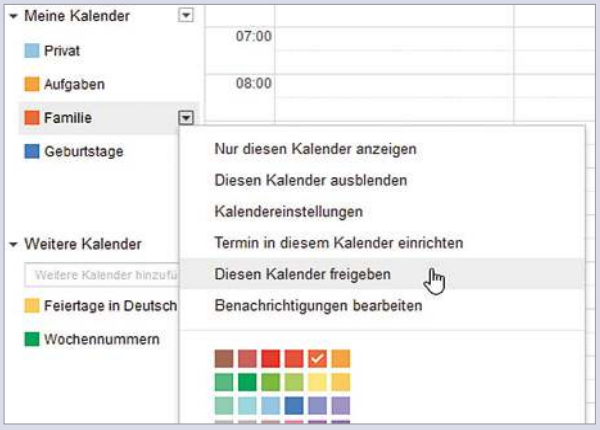
```
allow-hotplug wlan0
iface wlan0 inet manual
wpa-roam /etc/wpa_supplicant/wpa_
  supplicant.conf
iface default inet dhcp
```

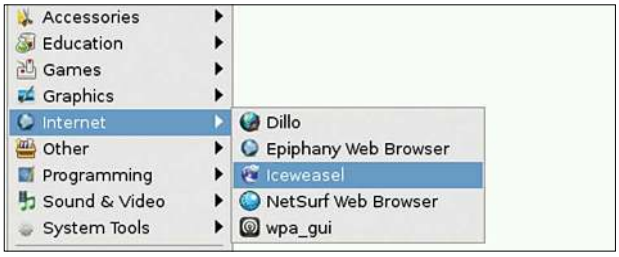
Das steht dort so nicht? Kein Problem!

Google-Kalender mit der ganzen Familie nutzen

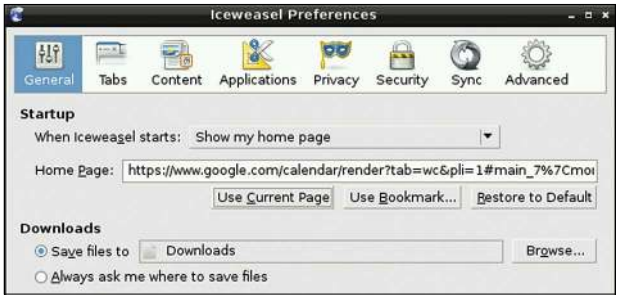
Was wäre ein ordentlicher Wandkalender für die ganze Familie ohne die Termine der lieben Verwandtschaft? Damit Sie immer wissen, was bei Ihrer Familie so anliegt, können Sie einen eigenen Kalender für die Familie anlegen und via Google mit allen anderen teilen. So kann jedes Familienmitglied Termine für die Allgemeinheit eintragen und sie werden alle am Monitor angezeigt. Ihre privaten Termine bleiben hingegen weiterhin nur für Sie sichtbar.

Und so geht's: Loggen Sie sich bei Google ein und klicken Sie über das gekachelte Quadrat oben rechts auf „Kalender“. Klicken Sie links neben der Überschrift von „Meine Kalender“ auf das abwärts zeigende Dreieck. Wählen Sie aus dem Menü den Eintrag „Neuen Kalender erstellen.“ Geben Sie dem Kalender im folgenden Menü einen treffenden Namen und füllen Sie bei Bedarf die übrigen Felder wie „Beschreibung“ oder „Ort“ aus. Wichtig: Tragen Sie im Feld „Für bestimmte Personen freigeben“ die Googlemail-Adressen Ihrer Familienmitglieder ein, mit denen Sie den neuen Kalender teilen möchten. Alle Adressen werden benachrichtigt und können fortan Termine in den gemeinsamen Kalender eintragen. Alternativ können Sie über das Dreiecks-Menü auch bereits bestehende Kalender freigeben.





Der Browser Iceweasel ist kein Bordmittel von Raspbian. Lesen Sie hier, wie Sie den Firefox-Ableger installieren.



Damit Iceweasel nach einem Neustart sofort den Google-Kalender anzeigt, legen Sie diesen als Startseite im Browser fest.

Ergänzen Sie die obigen Zeilen in Ihrer Datei, aber löschen Sie nicht die vorhandenen Einträge, die mit „auto lo“, „iface lo“ und „iface eth0“ beginnen. Speichern Sie die Datei über Strg-X ab, und laden Sie dann den Netzwerkdienst neu:

```
sudo /etc/init.d/networking reload
```

Suchen Sie nun Ihr WLAN mit dem folgenden Befehl:

```
sudo iwlist wlan0 scan
```

Tragen Sie dann mit dem Editor nano die SSID samt Passwort in die Datei „wpa_supplicant.conf“ ein:

```
sudo nano /etc/wpa_supplicant/wpa_
  supplicant.conf
```

Hier sollten Sie unter der Zeile „update_config=1“ diese Einträge sehen:

```
network={
ssid="WLAN-Name"
psk="WLAN-Passwort"
key_mgmt=WPA-PSK
}
```

Falls nicht, tragen Sie diese Zeilen nach. Ergänzen Sie den Platzhalter „WLAN-Name“ mit dem tatsächlichen WLAN-Namen (SSID) und tragen Sie statt „WLAN-Passwort“ das Kennwort Ihres Netzwerkes ein. Speichern Sie auch diese Datei via Strg-X. Danach laden Sie wieder mit

```
sudo/etc/init.d/networking reload
```

den Netzwerkdienst neu. Damit haben Sie sich auch ohne grafische Oberfläche mit Ihrem WLAN verbunden.

5. Iceweasel und weitere notwendige Hilfstools

Im Grunde ist nun alles angerichtet. Damit der Google-Kalender aber permanent und stets synchron auf dem Monitor angezeigt wird, sollten Sie zuvor noch Iceweasel installieren. Das ist ein Browser auf Grundlage von Mozillas Firefox, den Sie mit dem folgenden Terminalbefehl

```
sudo apt-get install Iceweasel
```

installieren. Damit der Browser bei jedem Neustart des Minirechners automatisch lädt, tragen Sie ihn in den Autostart des Systems ein. Laden Sie dazu die passende Konfigurationsdatei in den Editor nano:

```
sudo nano /etc/xdg/lxsession/LXDE/
  autostart
```

Hier tragen als die beiden Schlusszeilen der Datei die folgenden Zeilen

```
@iceweasel
@Unclutter
```

ein. Speichern Sie die Datei mit Strg-X. Ab sofort ist Iceweasel bei jedem Systemstart dabei. Die Funktion des Tools Unclutter erklärt sich nachfolgend.

Bevor Sie den Google-Kalender einrichten, sorgen Sie für etwas Ordnung: Falls der Browser einmal abstürzt, soll er nicht den üblichen Wiederherstellungsmodus anwerfen, sondern sofort wieder den Google-Kalender. Starten Sie Iceweasel und geben Sie in der Adresszeile *about:config* ein. Scrollen Sie in der Liste zum Eintrag „browser.sessionstore.resume_from_crash“ und setzen Sie den Wert auf „false“. Schließen Sie danach den Tab.

Nun stört noch der ständig abgebildete Mauscursor. Auch dafür ist wieder ein kleines Stück Software nötig: Installieren Sie zunächst das Tool Unclutter:

```
sudo apt-get install unclutter
```

Starten Sie das Programm manuell mit dem Befehl

```
unclutter
```

Sobald Sie nun die Maus für ein paar Sekunden nicht bewegen, blendet sich der Mauscursor automatisch aus.

Letzter Schritt der Vorbereitung: Der Energiesparmodus mit seinem Dimmen oder gar Ausschalten des Bildschirm muss weg. Die Darstellung des Kalenders soll konstant hell und konstant sichtbat bleiben.

Um den Energiesparmodus zu vermeiden, müssen Sie die Datei „lightdm.conf“ bearbeiten. Geben Sie den Befehl

```
sudo nano /etc/lightdm/lightdm.
  conf
```

im Terminal ein. Bewegen Sie den Cursor ganz ans Ende der Datei zur Rubrik „[SeatDefaults]“. Ändern Sie dort die Zeile

```
"#xserver-command=X"
```

nach

```
"xserver-command=X -s 0 -dpms".
```

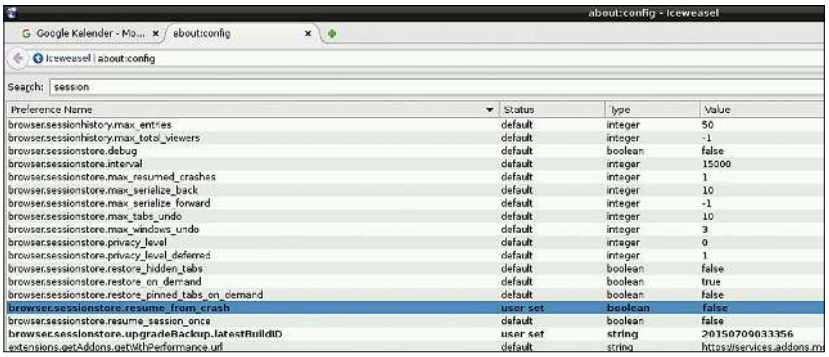
Speichern Sie die Datei mit Strg-X.

6. Google-Kalender einrichten und ausreizen

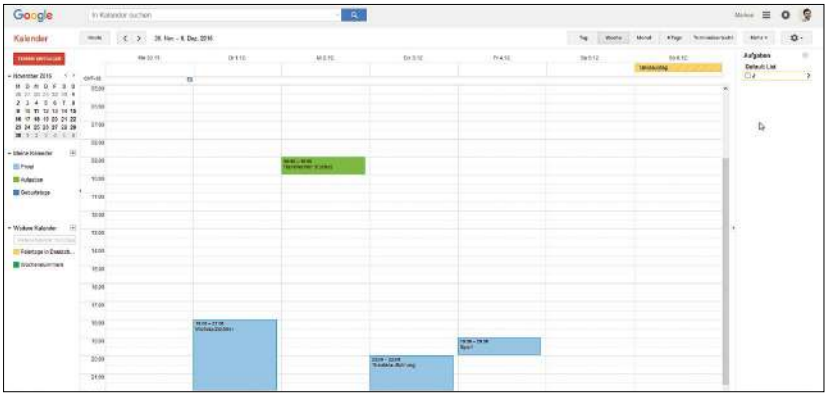
Rufen Sie im Iceweasel-Browser die URL *www.google.de* auf und loggen Sie sich mit Ihrem Google-Konto ein. Klicken Sie anschließend oben rechts innerhalb der Google-Seite auf das gekachelte Quadrat und wählen Sie „Kalender“. Dieser ist dank der einfachen Struktur selbsterklärend.

Richten Sie nun exakt diese Kalender-Webseite als Startseite von Iceweasel ein. Klicken Sie dafür auf das Symbol mit den drei Balken oben rechts. Im Menü „General“ können Sie mit einem Klick auf „Use Current Page“ den Google-Kalender als Homepage festlegen. Bestätigen Sie die Änderung mit einem Click auf „Close“ und drücken

Sie auf der Tastatur die Taste F11. Der Browser geht nun in den Vollbildmodus – so stört Sie keine unnötige Menüzeile. Über die Schaltfläche „Termin eintragen“ können Sie nun ein Ereignis datieren. Es taucht dann auch gleich in der Gesamtübersicht auf. Auch Termine, die über die App auf einem Smartphone eingetragen wurden, werden hier angezeigt. Die Synchronisation kann aber schon einmal ein paar Minuten dauern. Besonders schön ist die Möglichkeit, einzelne Kalender zu färben. Wichtige Aufgaben könnten so beispielsweise in einem feurigen Rot erscheinen, während ein dezentes Grün Feiertage und Geburtstage ankündigt.



Falls Iceweasel oder der Raspbery Pi mal den Dienst quittieren: Der Browser soll anstelle der Tab-Wiederherstellung immer den Google-Kalender präsentieren.



Ein neuer Google-Kalender im Vollbildmodus wirkt aufgeräumt und wartet darauf, Ihre Termine und Aufgaben abzuspeichern.

7. Raspberry Pi und Monitor anbringen

Die Raspberry-Pi-Installation kann nun an die Wand geschraubt werden. Verwenden Sie am besten ein Gehäuse: So verstaubt er nicht und lässt sich unbeschadet und stabil an der Rückseite des Monitors befestigen. Nehmen Sie als Befestigung ein bis zwei großzügig zugeschnittene Streifen doppelseitiges Klebeband. Achtung: Mit dem Raspberry-Pi-Huckepack vergrößert sich auch die Tiefe des Monitors. Bedenken Sie dies bei der Wahl der Schrauben und der Dübel. Dies ist natürlich hinfällig, sollten Sie eine eigene Wandhalterung des Monitormodells – womöglich gar mit Teleskoparm – verwenden.

Fertig an die Wand gedübelt überprüfen Sie noch einmal alle wichtigen Einstellungen: Ist Iceweasel samt Google-Kalender im Vollbildmodus? Alle anderen Fenster – etwa das Terminal – sind geschlossen? Dann können Sie Maus und Tastatur vom Raspberry Pi entfernen. Um neue Termine einzutragen, verwenden Sie am besten ein Smartphone inklusive Google-App. Der Kalender ist auf einem Mobiltelefon mit Android standardmäßig mit dem Google-Konto verknüpft. Wer ein iPhone verwendet, kann seinen Google-Kalender mit der Kalender-App von iOS verknüpfen.

Wer Termine direkt per Maus und Tastatur eintragen möchte, nutzt dazu am besten kabellose Geräte, die zudem kleiner und unauffälliger sind als ihre Schreibtischableger. Die gibt’s für kleines Geld beim (Online)-Händler Ihres Vertrauens.

Mit Apps alles im Griff

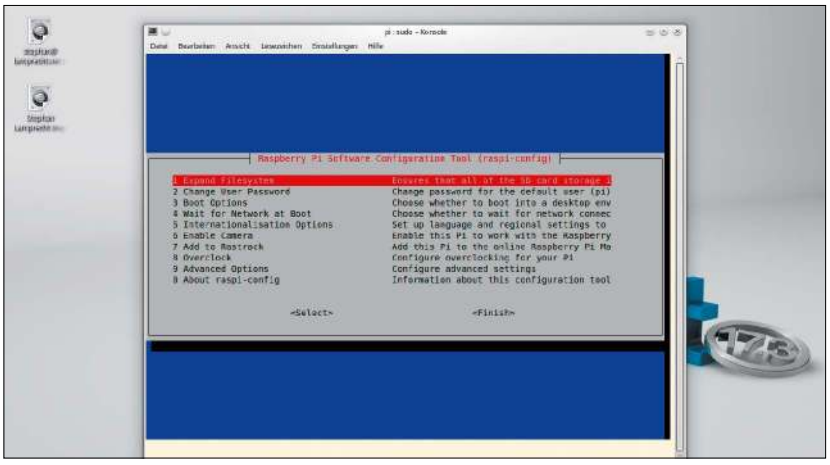
Ein neuer Termin oder eine neue Aufgabe steht an? Nehmen Sie nicht den Umweg über SSH oder die sperrige Tastatur. Ihr Smartphone erledigt das am bequemsten. Wenn Sie ein Android-Handy besitzen, ist die Kalender-App Ihres Smartphones bereits mit Ihrem Google-Konto verknüpft: Sämtliche Kalender und Termine sind somit auch auf Ihrem Smartphone zu sehen. Neue Termine, die Sie über die App eintragen, finden auch direkt den Weg auf den Monitor des Raspberrys.

Wenn Sie ein iPhone verwenden, benötigen Sie die kostenlose App Google Kalender. Sie ermöglicht, dass iOS-Fans verschiedene Kalender darstellen können. In der nativen Kalender-App von iOS werden keine zusätzlichen Kalender, etwa der geteilte Jahresweiser Ihrer Familie, dargestellt. Innerhalb der offiziellen Google-Kalender-App ist das aber kein Problem und auch neue Termine finden dank automatischer Synchronisation den Weg zum Raspberry Pi.

Virtueller Raspberry

Virtualisierung ist ein alter Hut: Ganze Arbeitsplätze inklusive System und Desktop werden in Unternehmen heute als virtuelle Rechner übers Netzwerk gestartet. Mit dieser Technik können Sie auch mit einem Raspberry experimentieren.

Von **Stephan Lamprecht**



Wer mit einem Raspberry Pi experimentieren möchte, kann das auch ohne Hardware tun. Möglich macht dies die Virtualisierung, die die Ressourcen eines PCs dem Betriebssystem des Pi zur Verfügung stellt. Mit einigen Einschränkungen muss man dabei rechnen. Diese betreffen vor allem die Soundausgabe und alle Funktionen, die das GPIO-Board der Platine verwenden. Beides ist mit einem Virtualisierer nicht nachzubilden. Je nach verwendeter Hardware des Host, also des physikalisch genutzten PCs, mag die Bildschirmausgabe vielleicht nicht auf Anhieb funktionieren. Typische Serverrollen lassen sich aber auch virtuell befriedigend testen.

Qemu statt Virtualbox

Im Internet kursieren Imagedateien für Virtual Box. Abgesehen davon, dass es sich um hoffnungslos veraltete Raspbian-Versionen handelt, tut man sich damit auch aus Leistungsgründen keinen Gefallen. Sehr viel schneller arbeitet die Virtualisierungssoftware Qemu. Zunächst brauchen Sie jedoch ein paar Pakete:

```
sudo apt-get install qemu qemu-
  user-static binfmt-support
```

Mit *update-binfmts --display* lassen Sie sich anzeigen, ob Sie die Möglichkeit besitzen, ARM-Architekturen zu virtualisieren. Der Raspberry arbeitet ja mit einem ARM-Prozessor, während auf Ihrem Linux-System wahrscheinlich eine Intel- oder AMD-CPU verbaut ist, die eine völlig andere Architektur besitzt. Der ARM-Interpreter von Qemu erlaubt aber dem Betriebssystem des Raspberry, den PC-Prozessor zu verwenden.

Raspberry-Image besorgen und anpassen

Sie benötigen ein aktuelles Image für den Raspberry Pi. Noobs ist in diesem Fall nicht brauchbar. Laden Sie sich stattdessen Raspbian als ZIP-Archiv auf den Rechner (*www.raspberrypi.org*). Dessen Inhalt entpacken Sie in einen Ordner Ihrer Wahl. Überprüfen Sie anschließend das Image (der bei Redaktionsschluss aktuelle Name kann in Ihrem Fall anders lauten):

```
fdisk -lu 2016-05-27-raspbian-jes
  sie.img
```

Sie erhalten mehrere wichtige Informationen: Die Sektorengröße beträgt typischerweise 512 Bytes. Das Image enthält eine kleine Bootpartition und die größere Systempartition. Beide besitzen jeweils einen Startsektor, dessen Wert Sie in der Spalte „Anfang“ finden. Damit Sie auf der „virtuellen“ Festplatte des Systems ausreichend Platz haben, vergrößern Sie diese Partition. Dazu müssen Sie sich die Ergebnisse des Wertes unter „Anfang“ des vorangegangenen Kommandos notieren. Um dem Dateisystem jetzt beispielsweise ein GB an zusätzlichem Speicher zu gönnen, geben Sie dies ein:

```
dd if=/dev/zero bs=1M count=1024 >>
  2016-05-27-raspbian-jessie.img
```

Der geschaffene zusätzliche Platz kann aber erst genutzt werden, wenn der Speicher den integrierten Dateisystemen zugewiesen wird. Da Linux nur auf Dateisysteme zugreifen kann, die sich auf einem Blockdevice befinden, müssen Sie die Imagedateien des Pi zu einem Loopdevice machen. Ein Loopdevice verhält sich wie ein Blockgerät, so dass ein darauf gespeicherte Dateisystem gemountet werden kann. So legen Sie für die beiden Images je ein Loopdevice an:

```
losetup -f --show 2016-05-27-rasp
  bian-jessie.img
losetup -f --show -o
  $((137216*512))  2016-05-27-rasp
  bian-jessie.img
```

Die beiden Werte für den Startsektor und die Sektorgröße sind dem obigen fdisk-Befehl zu entnehmen.

Loop-Devices können jetzt wie physikalische Festplatten partitioniert und bearbeitet werden. Starten Sie mit

```
sudo parted /dev/loop0
```

den Partitionsmanager. Mit *print* erhalten Sie einen Einblick in die vorhandenen Partitionen. Sie sehen darin zwei Einträge. Merken Sie sich den Wert unter „Anfang“ für die zweite Partition – also etwa 70,3 MB (siehe Abbildung). Außerdem finden Sie die Gesamtgröße des Systems unter „Festplatte“. Dieser Wert hat sich durch die Vergrößerung geändert, in unserem Beispiel soll die Gesamtgröße 6167 MB betragen. Auch diesen Wert benötigen Sie gleich. In Parted führen Sie danach folgende Befehle aus (Beispiel):

```
rm 2
mkpart primary 70.3 6167
quit
```

Maßeinheiten wie KB oder MB sind nicht nötig. Jetzt überprüfen Sie das neue Dateisystem mit

```
sudo e2fsck -f /dev/loop1
```

und vergrößern es dann:

```
sudo resize2fs /dev/loop1
```

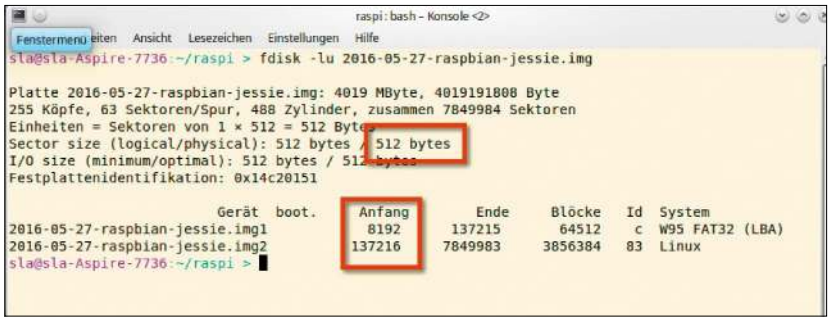
Danach können Sie die Loopdevices wieder vom System entfernen (*sudo losetup -d /dev/loop0 /dev/loop1*). Die Arbeiten an der Imagedatei sind damit abgeschlossen.

Raspberry-Image einbinden

Damit Qemu auf das Image zugreifen kann, muss es mit einem Mountpunkt versehen werden. Legen Sie in Ihrem Home-Verzeichnis einen Ordner an, der als Mountpunkt dienen soll (etwa *mkdir ~/rpi_mnt*). An dieser Stelle binden Sie jetzt das Image ein. Dazu benötigen Sie wieder den ersten Sektor der größeren Partition mit dem Dateisystem:

```
sudo mount 2016-05-27-raspbian-
 jessie.img -o
 loop,offset=$((137216*512)),rw
 ~/rpi_mnt
```

Wiederholen Sie die Einbindung für die Bootpartition des virtuellen Raspberry. Hier tragen Sie den Anfangssektor der kleineren Partition ein. Der Befehl dürfte in den meisten Fällen folgendermaßen lauten:



Hantieren mit dem Raspbian-Image: Sie benötigen die beiden exakten Startsektoren für die Boot- und Systempartition zum Vergrößern und Mounten des Systemabbilds.

```
(parted) print
Modell: Loopback device (loop)
Festplatte  /dev/loop0:  6167MB
Sektorgröße (logisch/physisch): 512B/512B
Partitionstabelle: msdos

Nummer  Anfang  Ende    Größe   Typ      Dateisystem  Flags
 1      4194kB  70,3MB  66,1MB  primary  fat16        LBA
 2      70,3MB  6167MB  6096MB  primary  ext4

(parted) rm 2
(parted) mkpart primary 70.3 6167
(parted) print
Modell: Loopback device (loop)
Festplatte  /dev/loop0:  6167MB
Sektorgröße (logisch/physisch): 512B/512B
Partitionstabelle: msdos

Nummer  Anfang  Ende    Größe   Typ      Dateisystem  Flags
 1      4194kB  70,3MB  66,1MB  primary  fat16        LBA
 2      70,3MB  6167MB  6096MB  primary  ext4

(parted) quit
```

Image als virtuelles Gerät: Mit dem Terminal-Partitionsmanager Parted formatieren Sie die als Loopdevice eingebundenen Partitionen des Images.

```
sudo mount 2016-05-27-raspbian-
 jessie.img -o
 loop,offset=$((8192*512)),rw ~/
 rpi_mnt/boot
```

Wenn Sie nun mit einem Dateimanager in das Verzeichnis wechseln, werden Sie dort die Ordner des Images finden, ganz so, als befände es sich auf einer SD-Karte, die Sie eingelegt haben.

Damit das Zusammenspiel mit Qemu klappt, müssen Sie noch eine Kleinigkeit an der Raspbian-Konfiguration anpassen. Öffnen Sie mit einem beliebigen Texteditor als root die Datei „~/rpi_mnt/etc/ld.so.preload“. Darin wird sich wohl nur ein Eintrag befinden. Diesen kommentieren Sie mit dem #-Zeichen aus. Danach verbinden Sie das Image mit Qemu:

```
cp /usr/bin/qemu-arm-static ~/rpi_
 mnt/usr/bin
```

Jetzt kann es losgehen. Um auf den virtuellen Rechner zuzugreifen, wird das Kommando chroot verwendet. Wechseln Sie in einem Terminal in das Mountverzeichnis des Raspi (*cd ~/rpi_mnt*) und führen Sie dort den folgenden Befehl aus:

```
sudo chroot . bin/bash
```

Jetzt können Sie alle Kommandos benutzen, die Ihnen auch in einem Terminal oder per SSH-Zugriff auf dem Raspberry zur Verfügung stünden. Melden Sie sich beispielsweise als Standardnutzer „pi“ und seinem Passwort „raspberry“ an. Dazu geben Sie *login pi* und das Passwort ein. Damit befinden Sie sich jetzt in einem Terminal auf dem Raspberry, wobei das Terminal in einem Terminal auf Ihrem Linux-System läuft.

Sie können jetzt nach Herzenslust Programme installieren oder Dienste starten. Auch das Ausführen von „raspi-config“ ist möglich. Selbst das Starten von grafischen Programmen dürfte in den meisten Fällen kein Problem sein. Um etwa den Browser Dillo zu starten, genügt das Kommando „DISPLAY=:0 dillo“. Um das System wieder zu verlassen, geben Sie *exit* ein, um sich vom Raspberry abzumelden, dann erneut *exit*, um die chroot-Umgebung zu verlassen. Melden Sie anschließend die gemounteten Laufwerke wieder mit *umount* ab. ●

Odroid-XU4 als Top-NAS

USB 2.0 und Fast Ethernet des Raspberry Pi sind nicht überall ausreichend. Für einen leistungsstarken Homeserver wird man andere Platinenrechner bevorzugen. Dieser Beitrag wirft einen kritischen Blick auf das Odroid-Spitzenmodell XU4.

Von **Hermann Apfelböck**

Quelle: www.pollin.de

Die Platinenfamilie Odroid des koreanischen Herstellers Hardkernel (*www.hardkernel.com*) gehört mit Recht zu den populärsten Raspberry-Konkurrenten. Die Odroid-Hardware ist solide und ausgewogen konzipiert, die offiziellen Systemimages werden durch eine aktive Community um zahlreiche Systemalternativen erweitert und Forum, Wiki und das kostenlose „Odroid Magazine" bieten Tipps und Infos. Das einfache Odroid-Grundkonzept war schon immer, für etwas mehr Geld deutlich mehr Leistung als der Raspberry zu liefern. Das Spitzenmodell XU4 ist freilich deutlich teurer als ein Raspberry – ist es auch deutlich besser?

Die technischen Daten des Odroid XU4

Der Odroid-XU4 bleibt nur knapp unter der psychologischen Schmerzgrenze von 100 Euro: Inklusive dem empfehlenswerten Gehäuse liegt er mit circa 95 plus acht Euro bei etwa 103 Euro (*www.pollin.de*). Dafür gibt es aber eine Achtkern-CPU (Samsung Exynos 5422), deren vier schnelle Kerne (Cortex-A15) mit zwei GHz takten, und vier sparsame Kerne (Cortex-A7) mit 1,4 GHz. Der Arbeitsspeicher beträgt zwei GB, und als GPU-Chip arbeitet ein Mali-T628 MP6, der auch in hochpreisigen Samsung-Tablets zum Einsatz kommt. Fast noch wichtiger für den Einsatz als Server sind der Gigabit-Netzadapter und die beiden USB-3.0-Anschlüsse (plus einer mit USB 2.0). Nicht jedermanns Sache ist der aktive CPU-Lüfter, der zwar akustisch recht dezent bleibt, aber unter Last recht häufig anläuft. Insgesamt scheint diese Hardware in Kombination mit ein, zwei externen Festplatten an USB 3.0 ideal für einen richtig schnellen, NAS-ähnlichen Datenserver im Gigabit-Netz.

Die Auswahl des Betriebssystems

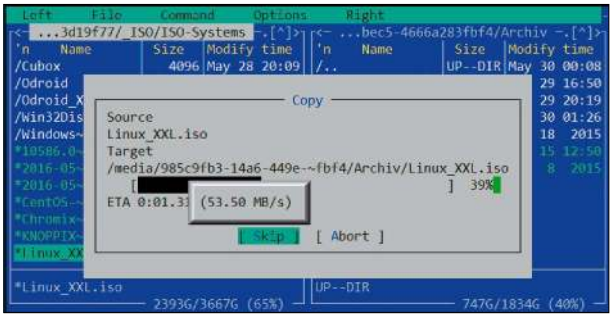
Die Auswahl an offiziellen Systemen des Herstellers und weiteren inoffiziellen Alternativen ist mehr als zufriedenstellend und deckt alle Bereiche ab (siehe *http://odroid.com/dokuwiki/doku.php?id=en:odroid-xu4*). Unter anderen finden sich hier mehrere Android-Versionen, Ubuntu 14.04 und 15.10 (aller Voraussicht nach auch 16.04 bis Erscheinen dieses Hefts), ferner das NAS-System Open Media Vault 2.1.1, Odrobian (ein Debian 8.3 „Jessie" mit vorinstalliertem Kodi und Mate-Desktop), Ubuntu Server sowie schlanke Debian-8-Server-Varianten. Damit lässt sich die Platine ohne viel Handarbeit sowohl für Desktop- wie für Serveraufgaben nutzen. Für den Serverbetrieb sind Open Media Vault (OMV, Download *https://sourceforge.net/projects/openmediavault/files/Odroid-XU3_XU4/*) oder ein Debian/Ubuntu erste Wahl. Wer für die Verwaltung mit dem SSH-Terminal auskommt, wird sich für eines der letztgenannten Systeme entscheiden. Das voreingestellte Passwort für root ist in der Regel „odroid", das Odroid-Forum gibt dazu Auskunft für jeden Einzelfall. OMV hat den Vorteil einer attraktiven Konfigurationsoberfläche, die via Nginx-Server auf dem OMV-System im Netzwerk über jeden Browser erreichbar ist (standardmäßig ist der User „admin" mit dem Passwort „openmediavault" zugangsberechtigt). Ein Datenserver in einem nicht sicherheitskritischen Heimnetz oder Home Office ist aber über das SSH-Terminal mit einigen „net usershare"-Befehl oft schneller eingerichtet als über OMV. Das unentbehrliche Samba ist bei Serversystemen wie OMV oder Ubuntu-Server vorinstalliert, muss aber etwa bei Odrobian noch mit

```
apt-get install samba samba-common
```

nachinstalliert werden.

Die Odroid-Images kommen wie üblich als gz-Archive, die auf Linux-Systemen mit der vorinstallierten Archivverwaltung zu entpacken sind. Unter Windows ist dafür der freie Packer 7-Zip erforderlich (auf Heft-DVD). Unter Linux nutzen Sie dann das Tool dd zum bootfähigen Übertragen des entpackten Systems auf SD-Karte, unter Windows den Win 32 Disk Imager (auf Heft-DVD). Acht GB auf der SD-Karte sollte für alle erwähnten Systeme und für einen Servereinsatz ausreichen. Für einen Desktopeinsatz sollte wenigstens das Doppelte bereitstehen.

Klickfreundliches Serversystem für Odroid-XU4: Für die Platine gibt es ein gutes Dutzend Systemimages. Wer die SSH-Administration scheut, kann zu Open Media Vault greifen.



Die Schreibleistung ist suboptimal: Wie internes Kopieren zwischen den angeschlossenen Festplatten (ohne Netzwerk) zeigt, bleibt die Platine hier unter den Möglichkeiten der Datenträger.

Datenträger einrichten und Leistung messen

Kommerzielle NAS-Systeme bestehen bei der Nutzung der eingeschobenen Festplatten obligatorisch auf ihrem Linux-eigenen Dateisystem – heute meist Ext4. Das heißt, dass Datenträger mit anderen Dateisystemen wie etwa NTFS zwangsläufig neu formatiert werden müssen. Im Hinblick auf eine optimale Leistung ist dies auch für jeden Platinenserver dringend zu empfehlen: Der getestete Odroid-XU4 erreichte mit NTFS- und exFAT-Partitionen nicht etwa relativ schlechtere, sondern dramatisch schlechte Durchsatzwerte von kaum fünf MB pro Sekunde.

Das Formatieren unter OMV geschieht unter „Datenspeicher -> Dateisysteme“, im SSH-Terminal mit *mkfs.ext4 /dev/sd[xy]* oder auch mit X11-Forwarding und dem Tool Gparted. Für die Netzwerkfreigaben aktivieren Sie in OMV zunächst Samba unter „Dienste -> SMB/CIFS -> Einstellungen“ und geben unter „Dienste -> SMB/CIFS -> Freigaben“ die Datenträger im Netz frei. Dazu muss vorher unter „Zugriffskontrolle -> Benutzer“ mindestens ein Benutzer angelegt sein. Die Vorgehensweise im SSH-Terminal mit *smbpasswd -a [user]* (Samba-User anlegen) und *net usershare add [name] /[Mountpunkt]/ "[Name]" [user]:f* (Samba-Freigabe) ist analog.

Nach diesen Vorbereitungen sind durch Messungen von Netzwerkkopien praktische Aussagen über die Leistung des Odroid-XU4 möglich: Die Platine ist flott, leistet aber nicht ganz, was sie verspricht: Sehr schnell ist das Kopieren vom Platinenrechner zum Samba-Client (im Gigabit-Ethernet): Diese Kopien erreichen 80 bis maximal 95 MB pro Sekunde – dieser Durchsatz liegt mit etwas Wohlwollen nahe am Gigabit-Bereich. Beim Kopieren vom Client zum Odroid-XU4-Platinenserver erreicht wir hingegen nur maximal 45 MB/s, im Schnitt eher nur 40 MB/s. Dies liegt ziemlich eindeutig an den USB-3.0-Schnittstellen, wie Kopiervorgänge direkt am Odroid-XU4 zwischen den beiden angeschlossenen Festplatten belegen: Auch hier kommt die Platine nur auf etwa 55 MB pro Sekunde. Die von uns genutzten Festplatten sind keine Topgeräte (WD Mybook 4 TB und Intenso Memory 2 TB), sollten aber beim Schreiben 110 MB/s beziehungsweise 80 MB/s erreichen. Einen Teil des eher durchschnittlichen Schreibdurchsatzes rechnen wir daher der Platine an.

Aber lassen wir die Kirche im Dorf: Unterm Strich hat der Odroid-XU4 das Attribut eines Top-Datenservers trotzdem verdient. Er liefert die Daten acht- bis neunmal schneller aus als ein Raspberry Pi und empfängt sie vier- bis fünfmal schneller. Durch Top-Festplatten ist dies eventuell noch zu steigern. CPU und Speicher bieten deutlich mehr als typische kommerzielle Home-NAS-Geräte und sind beim Einsatz als Datenserver kaum ernsthaft gefordert. Leistung und aktiver Lüfter schlagen sich allerdings nicht nur beim Preis nieder, sondern auch beim Stromverbrauch: Die Platine kommt im Idle-Betrieb kaum unter vier Watt und fordert bei Last und laufendem Lüfter bis zu zehn Watt – das ist jeweils circa der doppelte Verbrauch eines Raspberry. ●

Ubuntu auf dem Tablet

„Konvergenz“ klingt nicht sexy, doch ist das Konzept durchaus charmant, in einem Gerät Desktop und Tablet zu vereinen. Vom Hersteller Bq gibt es das erste Ubuntu-Tablet, das dieses Konzept mit Ubuntu Touch 15.04 umsetzt.

Von **David Wolski**

Ein halbes Jahrzehnt feilt Canonical schon an der Idee, mit Ubuntu den PC-Desktop wie auch Tablets und Smartphones zu bedienen. Das gleiche Betriebssystem soll auf einem Gerät ganz nach Bedarf mal eine Oberfläche für Touchbedienung zeigen und sich nahtlos in einen beinahe klassischen Desktop mit Programmfenstern verwandeln. Ubuntu Touch mit der grafischen Oberfläche Unity 8 ist das Betriebssystem aus dem Hause Canonical für diese Geräteklasse, die gegen die Android- und Apple-Geräte zumindest eine Nische erobern sollen. Seit Februar 2015 gibt es Smartphones mit Ubuntu Touch vom chinesischen Hersteller Meizu und vom spanischen Hersteller Bq.

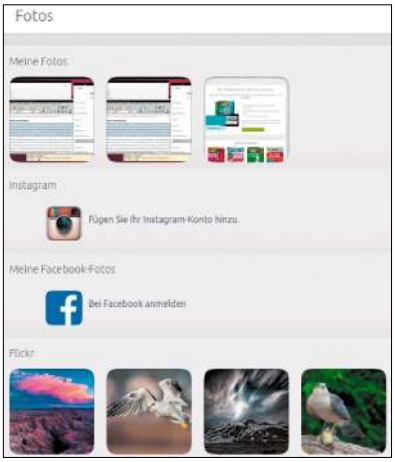
Von Bq stammt nun auch das im Frühsommer vorgestellte Tablet Aquaris M10 „Ubuntu Edition“, das in zwei Ausführungen mit unterschiedlichen Auflösungen über den Webshop von Bq erhältlich ist. Die Tablets mit Ubuntu Touch 15.04 zeigen die angekündigte Konvergenz in Aktion, und zwar nicht nur mit ein paar auserwählten Apps, sondern mit den regulären Linux-Programmen Libre Office, Firefox, Gimp und Gedit. Das ist beeindruckend, doch merkt man im Langzeittest noch deutlich, dass Ubuntu für Mobilgeräte in einem frühen Stadium der Entwicklung ist.

Ubuntu Touch: Scopes statt Apps

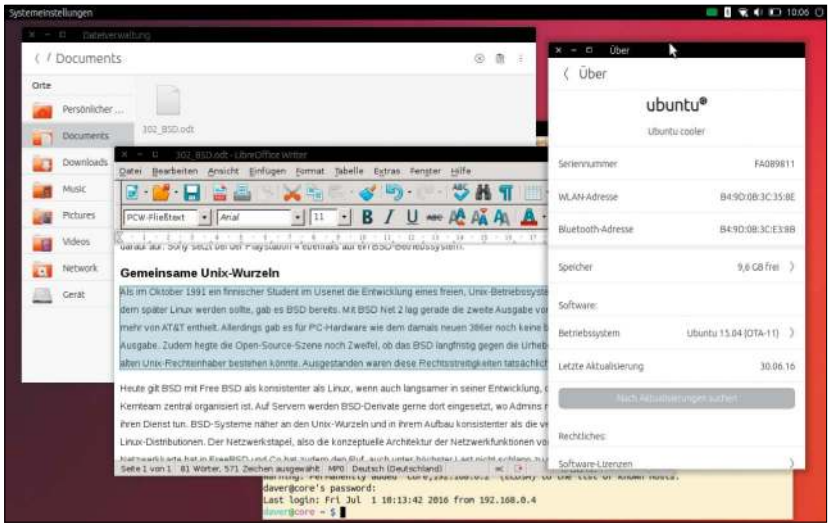
Seit der Vorstellung des aktuellen Tablets hat Ubuntu Touch 15.04 im Juni bereits das elfte Update bekommen, das eine Menge kleinerer Bugs behob und Leistung sowie Reaktionszeit deutlich verbesserte. Ubuntu Touch arbeitet mit dem neuen Displayserver Mir, der Canonicals eigener Nachfolger für das alternde X-Window-System ist. Darauf läuft als Desktop Unity 8, das wie eine schlichtere Ausgabe des regulären Ubuntu-Desktops wirkt. Das Gerät begrüßt Anwender im Tabletmodus und präsentiert nach einer sympathischen animierten Vorstellung des Bedienkonzepts die typischen Elemente von Ubuntu Touch: Eine Ansicht die sich „Scopes“ nennt, zeigt nicht wie bei anderen Mobilsystemen die Symbole der installierten Apps, sondern strukturiere Informationen verschiedener Webdienste nach Themenschwerpunkt. Eine Wischbewegung wechselt zwischen den Themen, die auf ihren Übersichtsseiten aktuelle Infos wie Nachrichten und Wetterbericht abrufen, sich aber zu Facebook, Flickr, Instagram und Twitter verbinden können. Die Auswahl der „Scopes“ bleibt den Anwendern überlassen und im Ubuntu Store gibt es auch noch einige mehr dieser Scopes. Die Auswahl der Webdienste ist derzeit aber noch beschränkt und für deutsche Nutzer zum Teil irrelevant.

Anwendungen: Ein Hauch Desktop

Neben Scopes gibt es auch noch Apps sowie eine Handvoll traditioneller Linux-Anwendungen, die in ihrem eigenen Programmfenster laufen. Einige Dutzend Apps hat der Ubuntu Store derzeit zu bieten. Firefox 44, Libre Office 4.4, Gimp 2.8, Gedit 3.10, Xchat und ein Terminal sind bereits vorinstalliert. Bei diesen Programmen erweist sich die Desktopfähigkeit des Tablets, welche die eigentliche Besonderheit von Ubuntu Touch ist: Über das obere Infomenü gibt es unter „System“ einen Schalter für den Schreibtischmodus, in



Scopes: Ubuntu Touch zapft mit seinen Scopes Onlinedienste und soziale Netzwerke an. Scopes präsentieren die Infos dann seitenweise, thematisch geordnet.



Schreibtischmodus: Die Scopes verschwinden in ihrem eigenen Fenster und geben den Blick frei auf den Desktop. Hier laufen vorinstallierte Anwendungen wie Libre Office.

den das Tablet auch selbständig schaltet, sobald eine USB- oder Bluetooth-Maus angeschlossen wird. Laufende Scopes und Apps wandern in eigene verschiebbare Fenster auf einer Arbeitsfläche. Dieser Desktop ist benutzbar und intuitiv.

Ein vollwertiges Ubuntu wird aus Ubuntu Touch so aber noch nicht, denn es fehlen schlicht die Anwendungen. Ferner ist die Mittelklasse-Hardware des Bq Aquaris M10 für Android ausreichend, unter Ubuntu Touch gibt es im Desktopmodus hingegen Verzögerungen bei der Größenänderung von Programmfenstern. Die kurze Akkulaufzeit erlaubt dem Tablet nur einige Stunden außer Reichweite einer Steckdose oder eines USB-Ports.

Erweitern mit eigenen App-Containern

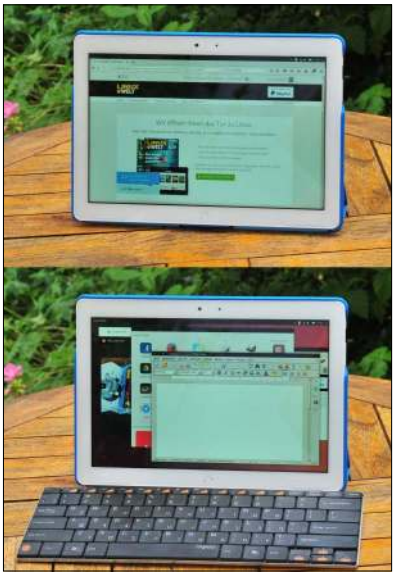
Ubuntu Touch arbeitet nicht mit DEB-Paketen und der Paketverwaltung Apt, sondern mit Clickpaketen, die ein Vorläufer der Snappakete sind. Anwender müssen sich daher vorerst mit der Handvoll Linux-Programme begnügen, die vorinstalliert sind. Wer basteln will, kann aber von einem Ubuntu-PC per USB im Entwicklermodus auf das Tablet zugreifen und über den Containermanager in Ubuntu Touch einen beschreibbaren Container für eigene Anwendungen erstellen. In diesen Container lassen sich dann weitere DEB-Pakete aus dem Ubuntu-Touch-Repository installieren und über die seit Juni verfügbare App Libertine starten. Der Weg ist unter *https://wiki.ubuntu.com/Touch/Libertine* dokumentiert und im Test konnten wir so immerhin Inkscape und das Terminal Lxterminal nachrüsten.

Fazit: Zu wenig Linux

Einer kleineren Firma wie Canonical muss klar sein, dass die Konkurrenz bei Tablets und Smartphones uneinholbar ist. Dazu fehlen Entwickler und Budget. Ubuntu-Touch-Geräte könnten sich aber eine Nische erobern, sofern sie sich auf die Tugenden von Linux-Distributionen besinnen. Eine Reihe bewährter Linux-Anwendungen, ein mächtiger Dateimanager, einige Netzwerktools und Programme für den Remotezugriff machen aus dem Ubuntu-Tablet ein passables Zweitgerät für Linux-Fans und professionelle Anwender.

All das gibt es rund um Linux bereits und müsste nur sorgfältig für Ubuntu Touch paketiert werden. Stattdessen will Canonical das Rad neu erfinden und ignoriert naheliegende Chancen für Ubuntu-Mobilgeräte.

Für Ubuntu Touch ist Linux momentan ein Mittel zum Zweck. Aber die damit verbundenen Stärken eines großen Angebots bewährter Open-Source-Software weiß es auf dem Tablet derzeit noch nicht zu nutzen.



Doppelfunktion: Mit Bluetooth-Tastatur und Maus verwandelt sich das Ubuntu-Tablet (beinahe) in einen Desktop. Der Übergang erfolgt im laufenden Betrieb.

Bq Aquaris M10 HD
Display: 10,1 Zoll (1280 x 800 Pixel)
RAM: 2 GB RAM, **Speicher:** 16 GB
CPU: Mediatek Quad Core 1,3 GHz
Gewicht: 470 Gramm
Infos: *www.bq.com/de/tablets*
Preis: 229,90 Euro (279,90 für die FHD-Variante mit 1920 x 1200 Pixeln) ●

Tuning für SSDs & Festplatten

Linux richtet bei der Installation schon fast alles für die optimale Nutzung der Datenträger ein. Bei bestimmten Konfigurationen lohnt es sich jedoch, manuell nachzubessern.

Von **Thorsten Eggeling**

In der Regel erfordern weder Festplatte noch SSD bei einem Linux-System besondere Aufmerksamkeit von Seiten des Benutzers. Es gibt aber einige Maßnahmen, mit denen sich die Lebensdauer der Laufwerke verlängern oder die Leistung verbessern lässt.

Dateisystem für mehr Platz komprimieren

Auf SSDs mit wenig Kapazität sorgen Sie für mehr freien Platz, indem Sie bei der Linux-Installation BTRFS (B-Tree-Filesystem) als Dateisystem wählen und dessen Komprimierung aktivieren. Die Komprimierung erhöht auch die Geschwindigkeit, weil weniger Daten transportiert werden müssen. Dafür steigt die CPU-Last etwas, was aber bei aktuellen PCs kaum zu bemerken ist.

Das Installationstool von Ubuntu bietet standardmäßig keine Option zur Auswahl des BTRFS-Dateisystems. Sie müssen die Partition daher manuell erstellen. Wählen Sie bei der Ubuntu-Installation im Fenster „Installationsart“ die Option „Etwas Anderes“. Klicken Sie das Laufwerk an, auf dem Sie Linux installieren wollen, beispielsweise „/dev/sda“, dann auf „Neue Partitionstabelle“ und anschließend auf „Weiter“. Damit löschen Sie alle Partitionen auf dem Laufwerk. Erstellen Sie über die „+“-Schaltfläche eine etwa 500 MB große Ext4-Partition mit dem Einbindungspunkt „/boot“. Außerdem erstellen Sie eine Swappartition mit einer Größe, die dem Hauptspeicher entspricht. Zuletzt legen Sie die Systempartition mit dem Dateisystem BTRFS und dem Einbindungspunkt „/“ an und klicken auf „Jetzt installieren“.

Im neu installierten System führen Sie in einem Terminalfenster folgende Befehlszeile aus:

```
sudo gedit /etc/fstab
```

Sie sehen, dass der Installer zwei BTRFS-Volumes erstellt hat: Eins für „/“ (subvol=@) und eins für „home“ (subvol=@home). Ergänzen Sie die Einbindeoptionen für „/“ mit dem Wert „compress“. Die Zeile sieht dann beispielsweise so aus:

```
UUID=<Partitions-ID> / btrfs
 defaults,compress,subvol=@ 0 1
```

Wenn Sie möchten, können Sie die Option auch für „/home“ hinzufügen, was aber keinen großen Gewinn verspricht. Große Benutzerdateien wie Videos oder MP3-Audio sind bereits komprimiert und können durch die BTRFS nicht weiter verkleinert werden. Speichern Sie die Änderungen und starten Sie Linux neu.

Die nachträglich aktivierte Komprimierung wirkt sich nur auf neu erstellte Dateien aus. Um die vorhandenen Dateien zu komprimieren, verwenden Sie einmalig folgende Befehlszeile:

```
sudo btrfs filesystem defragment
 -r -v -czlib /
```

Hinweis: Mithilfe des Tools btrfs-convert ist es von einem Livesystem aus möglich, das Ext4-Dateisystem eines bereits installierten Linux nach BTRFS zu konvertieren. Diese Methode ist noch sehr unsicher und kann zu Datenverlust führen. Wir raten ab.

Festplatte bei Nichtgebrauch abschalten

Die Mechanik von Festplatten unterliegt im Betrieb einem ständigen Verschleiß. Es ist daher empfehlenswert, Laufwerke abzuschalten, die gerade nicht verwendet werden. Das ist für zusätzliche Daten- oder Backupplatten sinnvoll, nicht jedoch für die Systemfestplatte. Denn hier finden ständig Laufwerkszugriffe statt und die Festplatte würde nach dem Abschalten schnell wieder anlaufen. Die Folge wäre mehr Verschleiß statt weniger.

Testen Sie in einem Terminalfenster, ob sich eine Festplatte zuverlässig in den Standbymodus versetzen lässt. Mit dem Befehl

```
sudo fdisk -l
```

ermitteln Sie die Laufwerkspfade: Ist die gewünschte Festplatte „/dev/sdb“, dann aktivieren Sie mit

```
sudo hdparm -y /dev/sdb
```

den Ruhezustand. Wenn Sie danach

```
sudo hdparm -C /dev/sdb
```

ausführen, erscheint die Ausgabe „/dev/sdb: drive state is: standby“. Greifen Sie über den Dateimanager auf das Laufwerk zu und führen Sie dann erneut *sudo hdparm -C /dev/sdb* aus. Diesmal erhalten Sie die Ausgabe „/dev/sdb: drive state is: active/idle“.

Wenn das funktioniert hat, können Sie die automatische Abschaltung nach einem bestimmten Zeitraum festlegen:

```
sudo hdparm -S 60 /dev/sdb
```

Der Wert hinter „-S“ steht für 60 mal fünf Sekunden, also fünf Minuten.

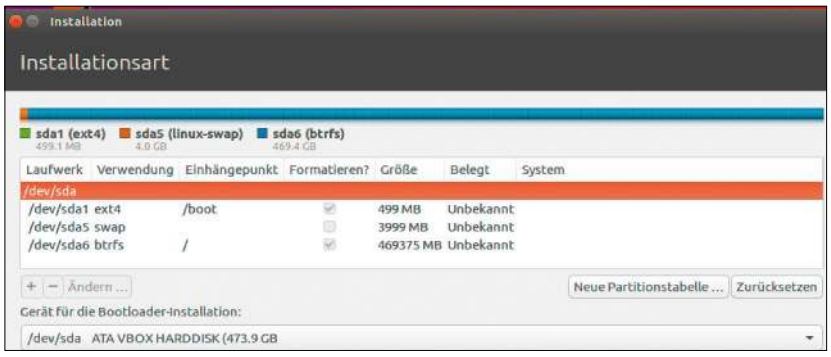
Die Konfiguration über hdparm wirkt nur bis zum nächsten Neustart des Systems. Für eine dauerhafte Änderung ermitteln Sie mit blkid die eindeutige UUID der gewünschten Partition. Führen Sie dann folgende Befehlszeile aus:

```
sudo gedit /etc/hdparm.conf
```

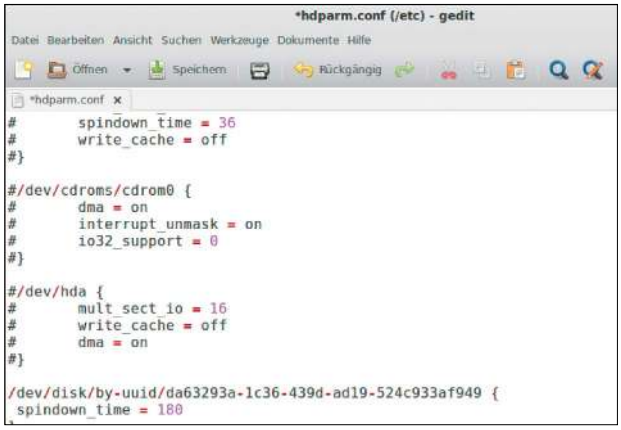
Fügen Sie im Editor folgende Zeile am Ende der Datei an:

```
/dev/disk/by-uuid/<Partitions-ID>
 { spindown_time = 60 }
```

Den Platzhalter „<Partitions-ID>“ ersetzen Sie durch die ermittelte UUID.



Platz sparen: BTRFS bietet eine eingebaute Komprimierung. Um das Dateisystem BTRFS zu nutzen, müssen Sie die Partitionierung bei der Installation jedoch selbst durchführen.



Abschaltzeit: In der Datei „/etc/hdparm.conf“ legen Sie hinter „spindown_time“ die Zeit fest, nach der eine Festplatte automatisch in den Standbymodus geht.

SSDs mit dem Trim-Befehl optimieren

Beim Löschen von Dateien wird im Dateisystem der frei gewordene Platz als wiederbeschreibbar markiert, der Inhalt aber nicht tatsächlich gelöscht. Der Controller auf der SSD weiß nichts davon und schreibt neue Dateien nur in Bereiche, die er für frei hält. Das ist nicht optimal, weil dadurch nach und nach immer mehr eigentlich unbelegter Speicherplatz nicht mehr zur Verfügung steht. Über den Trim-Befehl kann der Treiber des Dateisystems eine Liste mit unbenutzten Blöcken an den SSD-Controller übermitteln.

Aktuelle Linux-Systeme starten Trim einmal pro Woche automatisch. Bei Ubuntu ist dafür die Datei „/etc/cron.weekly/fstrim“ zuständig. Sie enthält nur den Befehl „exec fstrim-all“ oder „/sbin/fstrim --all“. Das Script fstrim-all beziehungsweise das Tool fstrim prüft, ob die SSD den Trim-Befehl überhaupt beherrscht und ob es sich um ein Modell von Intel, Samsung, OCZ, Sandisk oder Patriot handelt. Wenn nicht, wird der Trim-Befehl nicht abgesetzt. Hintergrund dieses Verfahrens ist, dass bei einigen SSDs, etwa von Crucial oder Micron, Trim fehlerhaft in der Firmware implementiert ist und die Anwendung zu Datenverlust führen kann.

Wer möchte, kann fstrim auch manuell ausführen, etwa um sich von der korrekten Funktion des Cronjobs zu überzeugen. Dazu verwenden Sie folgendes Terminalkommando:

```
sudo fstrim -v -a
```

Bei älteren Toolversionen, die den Parameter „-a“ nicht kennen, verwenden Sie *sudo fstrim -v /*. In der Ausgabe sehen Sie, wie viele Bytes freigegeben wurden. Es sollte sich in der Regel nur um einen geringen Wert handeln, wenn das Tool über den Cronjob erst kürzlich automatisch ausgeführt wurde.

So gesund ist Ihre Festplatte oder SSD

S.M.A.R.T ist die Abkürzung für Self-Monitoring, Analysis and Reporting Technology – eine Technologie, die in allen modernen Festplatten enthalten ist. Smart-Werte geben Auskunft über den Zustand der Festplatte oder SSD. Starten Sie das Tool gnome-disks, indem Sie bei Ubuntu im Dash oder bei Linux Mint im Startmenü nach „Laufwerke“ suchen. In der Übersicht klicken Sie das gewünschte Laufwerk auf der linken Seite des Fensters an und dann in der oberen Leiste auf die Menüschaltfläche. Wählen Sie „Smart-Werte und Selbsttests...“. Das Fenster gibt Auskunft über die Betriebsstunden sowie Temperatur des Laufwerks. Die Tabelle unter „SMART-Attribute“ zeigt die einzelnen Werte an.

Hinter „Allgemeine Einschätzung“ sollte „Das Laufwerk ist in Ordnung“ stehen – wenn nicht, ist es Zeit, an einen Austausch zu denken.

Sagen Sie uns Ihre Meinung – und gewinnen Sie!

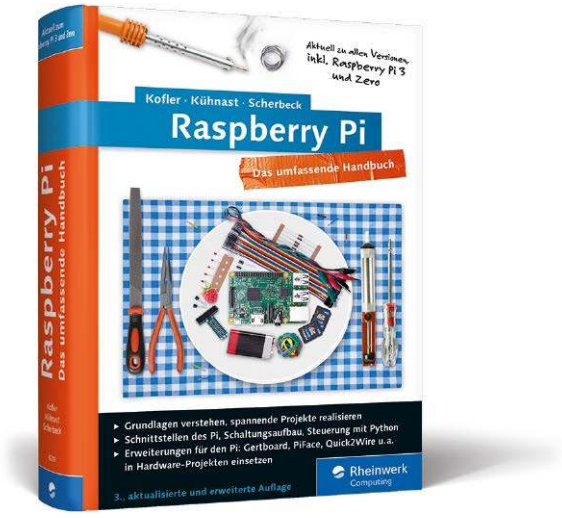
Wir möchten Linux-Hefte machen, die ganz Ihren Bedürfnissen und Interessen entsprechen. Dabei können Sie uns helfen! Füllen Sie einfach unseren Fragebogen im Internet aus. Das Beantworten der Fragen dauert nur rund zehn Minuten.

Das bewährte Standardwerk zum Raspberry Pi

3 x Raspberry Pi

Das umfassende Handbuch

- **Grundlagen verstehen, spannende Projekte realisieren**
- **Schnittstellen des Pi, Schaltungsaufbau, Steuerung mit Python**
- **Erweiterungen für den Pi: Gertboard, PiFace, Quick2Wire u. a. in Hardwareprojekten einsetzen**
- **Aktuell zu allen Versionen des Raspberry Pi – inkl. Modell 2**



Autoren: Michael Kofler, Charly Kühnast, Christoph Scherbeck

Verlag: Rheinwerk Verlag, 1088 Seiten, 3., aktualisierte Auflage 2016, gebunden, in Farbe, mit CD

ISBN ISBN 978-3-8362-4220-2, **39,90 Euro**

Zu allen Raspberry-Pi-Varianten erwartet Sie hier Bastelwissen in seiner umfassendsten Form. Es gibt Ihnen Grundlagen und Kniffe zu Linux, Hardware, Elektronik und Programmierung an die Hand und fügt alles in überragenden Bastelprojekten zusammen. Weit über 1000 Seiten zum Raspberry Pi: nicht live, aber in Farbe! Klingt spannend? Dann steigen Sie direkt ein ...

Aus dem Inhalt

▪ Inbetriebnahme, Desktop und Mediacenter, Terminal ▪ Linux mit Raspbian ▪ Die Raspberry-Pi-Hardware (CPU/GPU, GPIO u. v. m.); nun auch zur Raspi-Version 2 ▪ Crashkurs Elektronik: LEDs, Motoren, Relais ... ▪ Erweiterungsboards: Kamera, Atmega, Gertboard, Piface & Co. ▪ Sensoren, z. B. Ultraschall- und Wasserstandssensor, Bewegungsmelder ▪ Monitorboards ▪ Programmieren lernen: Python, C, PHP und Shell-Scripts ▪ Inkl. Kapitel zu Mathematica und Wolfram-Language ▪ Projekte: Heimautomation, Luftraumüberwachung, FM-Transmitter, IPv6-Router u. v. m.

Jeder Teilnehmer bekommt als Dankeschön die PC-WELT Extra 7/2016 PC-WELT Hacks 2016 als PDF (ohne Datenträger). Sie finden den Link zum Download des Hefts am Ende der Leserbefragung.

So funktioniert's:

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

Einsendeschluss für das Gewinnspiel
in LinuxWelt 5/2016 ist der 26.09.2016.

Datenschutz: Wenn Sie gewinnen, schicken wir Ihnen den Preis per Post zu. Deshalb fragen wir Sie auch nach Ihrer Adresse. Datenschutzerklärung: Alle auf unserer Webseite erhobenen Daten werden entsprechend den Vorschriften des Bundesdatenschutzgesetzes (BDSG) und des Informations- und Telekommunikationsdienstegesetzes (IuTDG) behandelt. Eine Weitergabe der Daten an Dritte ohne ausdrückliche Einwilligung des Betroffenen erfolgt nicht. Weitere Infos finden Sie unter *www.pcwelt.de/datenschutz*

LINUX WELT

Stellen Sie uns auf die Probe!

2x LinuxWelt zum Testpreis

Jetzt testen:
2x LinuxWelt
gedruckt & digital

11,90 €

Satte **30 %** gespart!

Als Print-Abonnent der **LinuxWelt** erhalten Sie Ihre Ausgabe in der PC-WELT App **IMMER GRATIS** inklusive DVD-Inhalte zum Download.

- ✓ **2x LinuxWelt als Heft frei Haus** mit Gratis-DVD
- ✓ **2x LinuxWelt direkt aufs Smartphone & Tablet** mit interaktivem Lesemodus

Jetzt bestellen unter
www.pcwelt.de/linuxtesten oder per Telefon: 0711/7252277 oder ganz einfach:

1. Formular ausfüllen — **2. Foto machen** — **3. Foto an shop@pcwelt.de**

Ja, ich bestelle das LinuxWelt Testabo für 11,90 €.

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. 49,50 EUR. Danach ist eine Kündigung zur übernächsten Ausgabe jederzeit möglich.

ABONNIEREN

Vorname / Name

Straße / Nr.

PLZ / Ort

Telefon / Handy | Geburtstag TT MM JJJJ

E-Mail

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

BEZAHLEN

Geldinstitut

IBAN

BIC

Datum / Unterschrift des neuen Lesers

LWPMA14147

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

Oberflächen optimieren

Linux Mint 18 bringt den Desktop Cinnamon 3.0 mit: Dieser kann auch in andere Linux-Distributionen eingebaut werden. Im Übrigen stehen Gnome/Unity bei den nachfolgenden Tipps im Fokus.

Von **David Wolski**

Cinnamon-Installation

Ubuntu, Fedora Open Suse

Zwar ist der alternative Desktop Cinnamon eine Eigenentwicklung der Macher von Linux Mint, hat aber seit seiner Vorstellung vor fünf Jahren über diese Linux-Distribution hinaus Freunde gefunden. Der Desktop ist nicht nur Mint vorbehalten, sondern steht auch unter anderen Linux-Systemen wie Ubuntu, Open Suse oder Fedora zur Verfügung.

Wer zu Cinnamon 3.0 wechseln will, das sich ganz bequem im Livesystem von Linux Mint 18 (auf der Heft-DVD) ausprobieren lässt, muss in den großen Distributionen jetzt nicht mehr lange suchen:

Debian: Die ältere Version 2.2.4 von Cinnamon hat es bei Debian 8 in die Standard-Paketquellen geschafft. In einem Terminalfenster installiert das Kommando

```
sudo apt-get install cinnamon-
  desktop-environment
```

die gesamte Desktopumgebung mit Programmen. Der Platzbedarf auf der Festplatte beträgt bis zu einem GB.

Ubuntu: Das aktuelle Cinnamon 3.0 steht hier über ein PPA bereit, also über ein externes Repository. Dessen Einrichtung erfolgt mit dem Befehl

```
sudo add-apt-repository
  ppa:embrosyn/cinnamon
```

über die Kommandozeile. Danach erledigen die beiden Kommandos

```
sudo apt-get update
sudo apt-get install cinnamon
```

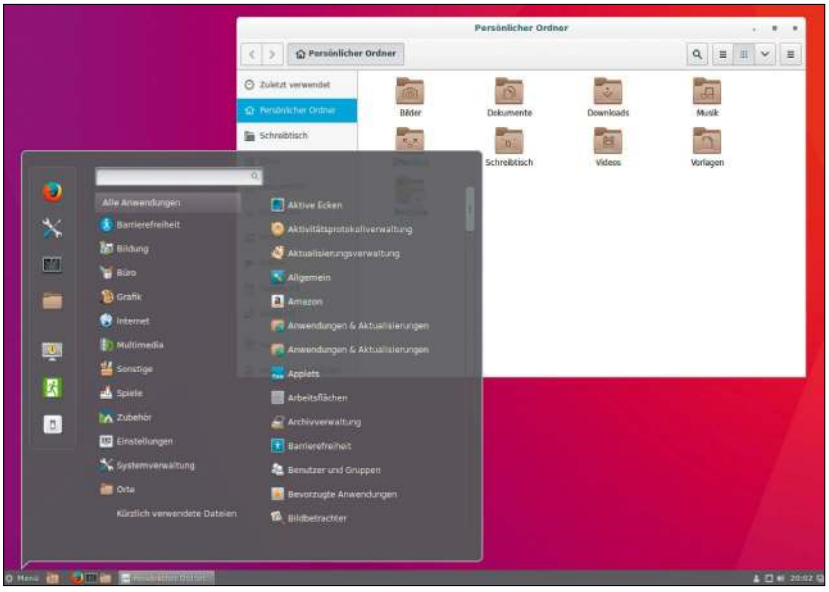
die Installation. Cinnamon belegt rund 280 MB zusätzlich auf der Festplatte und steht dann auf der Log-in-Seite als weitere Desktopsession bereit. Mit einem bereits installierten Unity oder anderen Desktopmgebungen gibt es keine Konflikte.

Fedora: Über seine Standard-Paketquellen kommt Fedora ebenfalls in den Genuss von Cinnamon. Die Installation erfolgt recht komfortabel über den Paketmanager dnf im Terminal:

```
sudo dnf install @cinnamon
```

Das @-Zeichen dient hier dazu, eine Paketgruppe anzugeben, die mehrere Pakete enthält. Die Installation von Cinnamon 3.0 verlangt rund 500 MB auf der Festplatte.

Open Suse: Sowohl für 42.1 Leap als auch für den Rolling Release „Tumbleweed“ gibt es eigene Paketquellen, die Yast mit einigen Klicks aufnehmen kann. Ausflüge in die Kommandozeile sind in diesem Fall nicht nötig, sondern ein Besuch der Webseite *https://en.opensuse.org/Portal:Cinnamon*. Ein Klick auf eine der Schaltflächen „1-Click-Installation“ neben der passenden Paketquelle für die laufende Open-Suse-Version startet die Installation. Yast springt nach einigen Bestätigungen und Rückfragen automatisch an, um alle benötigen Komponenten nachzurüsten. Die Gesamtgröße der Pakete beläuft sich auf rund 800 MB.



Cinnamon in Ubuntu 16.04: Ein PPA liefert die Desktopumgebung von Linux Mint in der neuesten Version auch für Ubuntu. Mit dem vorinstallierten Unity gibt es keine Konflikte.

Externe Bildschirme

Profile erstellen

Nach dem Anschluss eines TV-Bildschirms per HDMI oder eines Beamers per VGA erlaubt die Desktopumgebung die Konfiguration des externen Anzeigegeräts. Das System merkt sich diese Einstellungen, kann aber nicht zwischen mehreren unterschiedlichen HDMI- oder VGA-Ausgabegeräten unterscheiden.

HDMI-Ausgabe konfigurieren: Desktopumgebungen, hier Mate, merken sich die letzten Einstellungen von externen Anzeigegeräten, können aber nicht mehrere Profile verwalten.

Wer einmal ein TV-Gerät an HDMI anschließt und dann wieder einen externen Monitor, muss die Einstellungen zu Auflösung und Anordnung des externen Displays neu vornehmen, denn bisher unterstützt kein Linux-Desktop einzelne Profile für Anzeigegeräte. Es gibt aber das Kommandozeilentool xrandr, das die Ausgabeparameter einer Schnittstelle direkt beeinflussen kann. Mit diesem Tool ist es möglich, die gewünschten Einstellungen per Parameter wieder aufzurufen. Weil das Zusammentragen der Parameter für mehrere Anzeigegeräte recht umständlich ist, hat der Entwickler Stefan Tomanek ein Script geschrieben, das die Monitoreinstellungen für xrandr in ein Profil schreibt und dieses Profil bei Bedarf wieder aufruft. Das Script liegt auf der Github-Seite des Entwicklers und wird mit

```
wget https://raw.githubusercon
  tent.com/wertarbyte/autorandr/
  master/autorandr
```

heruntergeladen und anschließend mit

```
chmod +x autorandr
```

ausführbar gemacht. Die Parameter sind schnell erklärt: Mit

```
./autorandr -s [Profilname]
```

sichert das Tool die Konfiguration von primärer und sekundärer Ausgabe unter dem angegebenen Profilnamen. Die Daten dafür legt es übrigens im Home-Ordner unter „/.autorandr“ ab. Der Aufruf

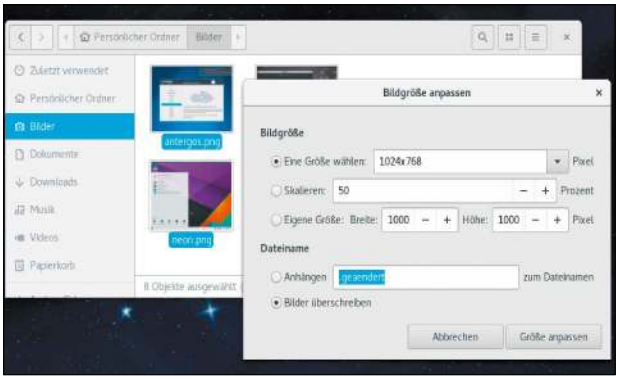
```
./autorandr -l [Profilname]
```

kann dann ein Profil für ein bestimmtes Anzeigegerät wieder aktivieren. Diese Befehle verlangen keine root-Rechte, denn das zugrunde liegende Tool xrandr funktioniert mit gewöhnlichen Benutzerrechten.

Gnome/Unity

Bildgrößen in Nautilus per Kontextmenü ändern

Unter Gnome und Unity ist es nicht unbedingt nötig, für die Verkleinerung von Bilddateien vor dem Verschicken per Messenger oder E-Mail eine Bildbearbeitung aufzurufen. Eine Erweiterung für den Dateimanager Nautilus holt die Funktion ganz komfortabel in ein Kontextmenü.



Bilder in Form bringen: Eine Erweiterung für den Dateimanager Nautilus kann Bilder an Ort und Stelle auf eine gewünschte Größe bringen. Das klappt auch mit mehreren markierten Dateien.

Basteleien mit Scripts und Konfigurationsdateien sind hier nicht nötig, denn die prominenten Distributionen mit Gnome und Unity als Desktop haben die Erweiterung für Nautilus zum Ändern von Bildgrößen bereits in ihren Paketquellen. In Ubuntu ist sie in der Kommandozeile mit

```
sudo apt-get install nautilus-
  image-converter
```

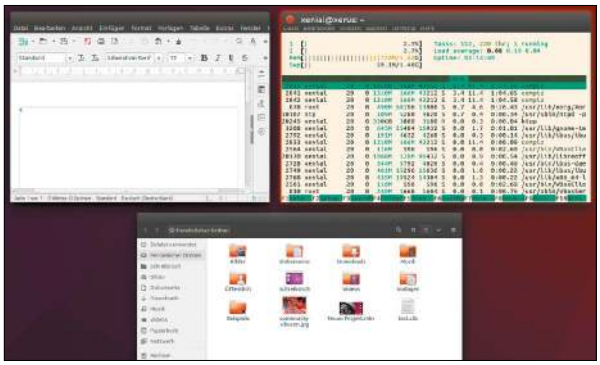
schnell installiert auch danach auch schon einsatzbereit. In Fedora gibt kommt das Paket mit dem Befehl

```
sudo dnf install nautilus-image-
  converter
```

auf das System. Nun genügt ein Rechtsklick in Nautilus auf eine oder mehrere markierte Bilddateien, um über die neuen Kontextmenüpunkte „Bildgröße anpassen“ und „Bilder drehen“ eine Bildmanipulation direkt im Dateimanager auszulösen.

Unity-Fenster

Übersicht im Eck



Alle Fenster in der Übersicht: Diese Alternative zu Alt-Tab lässt sich über die Tastenkombination Windows-W aufrufen oder wie bei Gnome über eine Bildschirmecke.

Der Launcher in Unity ist nicht optimal, um einzelne Fenster laufender Programme zu wählen, weil dort mehrere Unterfenster immer zu einem Symbol gruppiert werden. Besser ist die Fensterübersicht mit der Tastenkombination Windows-A, die Programme aller Arbeitsflächen verkleinert zur Auswahl anzeigt.

Wer eine alte mechanische Tastatur ohne Windows-Taste besitzt, kann die Fensterübersicht, die auch eine nützliche Alternative zu Alt-Tab ist, auch mit der Maus einblenden. Unity, das von Gnome abstammt, kennt aktive Bildschirmecken: Fährt der Mauszeiger genau in eine der konfigurierten Ecken, dann kann auch die Mauszeigerposition die Übersicht einblenden. Folgender Befehl legt die Fensterübersicht in die linke obere Bildschirmecke:

```
dconf write /org/compiz/profiles/
  unity/plugins/scale/initiate-
  all-edge "'TopLeft'"
```

Statt des Werts „TopLeft“, der genau so in einfachen und doppelten Anführungszeichen stehen muss, gibt es auch für die anderen Bildschirmecken entsprechende Werte. Im Uhrzeigersinn sind das „TopRight“, „BottomRight“ und „BottomLeft“. Ein leerer Wert setzt die Einstellung wieder zurück.

Alternative: Die Konfiguration aktiver Ecken ist auch auf grafischem Weg mit dem Unity Tweak Tool möglich, das Sie mit

```
sudo apt-get install unity-tweak-
  tool
```

nachinstallieren können. Die betreffende Einstellung finden Sie dort unter „Aktive Ecken“.

Anwendungsstarter Gnome-Do

Suchen und Starten

Multitalent Gnome-Do: Für Desktopumgebungen mit magerem Ausführen-Dialog ist Gnome-Do eine gute Ergänzung. Bei Ubuntu und Mint liegt es in den Standard-Paketquellen.

Desktopumgebungen wie Unity, Gnome und KDE verfügen über vielseitige Ausführen-Dialoge, die nicht nur als simple Programmstarter dienen, sondern auch nach Anwendungen und Dokumenten im Home-Verzeichnis suchen. Auf Desktops wie Mate, Cinnamon, XFCE und LXDE kompensiert ein Zusatztool diese Lücke.

Das Programm Gnome-Do ist eine kleine Desktopanwendung, die weit mehr kann, als nur Programme zu starten. Die Ergänzung ist optimal für Anwender, die auch auf einer grafischen Oberfläche die Tastatur der Maus vorziehen. Ursprünglich wurde Gnome-Do noch für ältere Gnome-Versionen mit dem .NET-Framework Mono entwickelt. Es wird aber immer noch gelegentlich gepflegt und mit Plug-ins erweitert. Für schlichte Desktopumgebungen ist Gnome-Do eine gute Ergänzung. Mit Unity ist es allerdings nicht kompatibel. Der Befehl

```
sudo apt-get install gnome-do gno
  me-do-plugins
```

installiert Gnome-Do in Debian, Ubuntu-Varianten und Linux Mint samt allen Abhängigkeiten und den verfügbaren Plug-ins. Zum ersten Aufruf und zu Konfiguration muss das Tool noch mittels *gnome-do* im herkömmlichen Ausführen-Dialog gestartet werden. Rechts über den Pfeil gelangt man zu den Einstellungen, wo sich Gnome-Do auch gleich als Autostart einrichten lässt. Das Tool läuft üblicherweise im Hintergrund, und die Tastenkombination Windows und Leertaste holt es auf den Bildschirm. Der Ausführen-Dialog besteht aus zwei Feldern nebeneinander: Im linken Eingabefeld ist zu sehen, auf welche Anwendung, Datei oder Objekte die bisherigen Tastatureingaben passen. Falls es mehrere Möglichkeiten gibt, klappt die Pfeil-unten-Taste eine Liste aus. Das rechte Feld zeigt die vorgeschlagene Aktion für die Angabe im linken Feld an. Bei Anwendungen ist dies beispielsweise „Ausführen“ und bei Webadressen „URL öffnen“. Mit der Tab-Taste wechseln Sie zwischen

rechtem und linkem Feld. Die Plug-ins von Gnome-Do erweitern dessen Funktionen, damit es mit weiteren Anwendungen zusammenspielen kann. Beispielsweise kann Gnome-Do mit der Erweiterung „Files and Folders“ das Dateisystem durchsuchen und „Gnome Session Management“ kann den Rechner auf Befehl neu starten, abschalten, in den Ruhezustand versetzen oder den Benutzer anmelden. Viele Plug-ins haben allerdings keinerlei Dokumentation und erschließen sich erst durch Experimentieren.

Gnome

Maximierte Fenster ohne Titelleiste

Erweiterung Maximus für Gnome: Das Tool ist einfach über die Extensions-Webseite zu beziehen und versteckt bei maximierten Fenstern die Titelleiste eines Fensters.

Richtig gut arbeiten lässt es sich in Gnome 3 mit maximierten Programmfenstern. Die Desktopumgebung verzichtet auf eine klassische Taskleiste und schafft dadurch Platz. Allerdings zeigen maximierte Fenster weiterhin die Titelleiste – besonders auf kleinen Notebookdisplays verschenkter Platz.

Eine Ergänzung für Gnome kann die Titelleiste automatisch ausblenden, wenn das Fenster maximiert ist: Maximus NG steht über das Onlineverzeichnis der Gnome-Erweiterungen (*https://extensions.gnome.org/*) zur Installation bereit und funktioniert in allen aktuellen Gnome-Versionen bis Gnome 3.20.

KDE-Kshutdown

Geplantes Abschalten

Wenn vor dem Ausschalten des PCs noch einige Aktionen erforderlich sind, etwa Downloads oder Systemaktualisierungen, dann kann KDE den Rechner zur gewünschten Zeit selbständig abschalten.

Das KDE-Tool Kshutdown bietet einen Timer, der das System automatisch herunterfährt, neu startet oder in den Ruhezustand versetzt. Die gewünschte Aktion kann zu einem bestimmten Zeitpunkt ausgeführt werden und ist über einen übersichtlichen Dialog schnell eingerichtet.

Kubuntu: In der aktuellen Ausgabe 16.04 steht kshutdown noch nicht in den Standardpaketquellen zur Verfügung. Es funktionieren aber die Pakete aus der Vorgängerversion, die unter *https://launchpad.net/ubuntu/wily/+package/kshutdown* im DEB-Format bereitstehen.

Fedora: In dieser Distribution ist das Tool über den Paketmanager verfügbar und mit *sudo dnf install kshutdown* zu installieren.

Open Suse: Kshutdown ist hier nicht in den Standard-Paketquellen enthalten. Es gibt aber für die Versionen 42.1 Leap und Tumbleweed ein passendes Paket über den Build Service unter *https://build.opensuse.org/package/show/KDE:Extra/kshutdown*.

LXDE-Papierkorb

Per Menüpunkt ausleeren

Müllabfuhr per Kontextmenü: Der Menüpunkt „Empty Trash“ fehlt auf dem LXDE-Desktop. Das Tool trash-cli und ein Installationsscript rüsten diese Funktion nach.

Hier wurde etwas vergessen: Ein Rechtsklick auf das Papierkorb-Symbol von LXDE zeigt keine Funktion zum Ausleeren des Papierkorbs. Diesen Menüpunkt gibt es in LXDE bisher nur im Dateimanager Pcmanfm.

Erst die nächsten Versionen von LXDE sollen den bislang fehlenden Menüpunkt im Papierkorb nachliefern. Bis es soweit ist, kann eine geschickte Kombination aus dem Kommandozeilentool trash-cli, einem Script und einer Verknüpfung den Menüpunkt nachrüsten. Das Team um Lubuntu hat einen Fix in Form eines weiteren Shellscripts veröffentlicht, das alle Änderungen in Lubuntu 14.04/16.04 vornimmt. Der Fix liegt unter (*https://goo.gl/27LHA7*) und der Befehl

```
wget https://github.com/Nicolas
  Bernaerts/ubuntu-scripts/raw/ma
  ster/lubuntu/trash-empty/ask-
  trash-empty-install.sh
```

lädt das Script in das aktuelle Verzeichnis herunter. Dort starten Sie die Datei mit diesem Kommando:

```
sh ask-trash-empty-install.sh
```

Zur Installation von trash-cli fragt das Installationsscript nach sudo-Berechtigungen und legt zudem die zwei weiteren Scripts „/usr/local/bin/ask-trash-empty“ und „~/.local/share/file-manager/actions/ask-trash-empty.desktop“ ab. Nach einer Neuanmeldung zeigt ein Rechtsklick auf den Papierkorb den Eintrag „Empty Trash“. ●

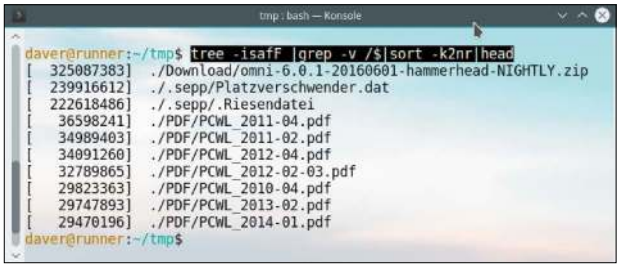
Solide Shell

Eine Menge Aufgaben lassen sich mit ein paar genialen Kniffen in der Shell eines Linux-Systems effektiver lösen als auf der grafischen Oberfläche. Diesmal geht es um nützliche Kommandos rund um die Dateiverwaltung.

Von **David Wolski**

Platzfresser

Die größten Dateien finden



Die zehn größten Dateien im aktuellen Ordner ermitteln: Der Befehl tree kann Dateigrößen in Byte ausgeben. grep, sort und head machen dann eine sortierte Liste daraus.

Welche Dateien belegen den meisten Platz? In Zeiten erschwinglicher, aber vergleichsweise kleiner SSDs und auf Platinenrechnern mit bescheidener Speicherkarte wird diese Frage jetzt wieder aktuell. Auf der Kommandozeile gibt es unter Linux gleich mehrere Wege, Platzfressern auf die Spur zu kommen.

Die Tools tree und du sind bestens dazu geeignet, sich eine Übersicht zum Inhalt zur Größe von Verzeichnissen zu verschaffen. Der Befehl tree zeigt hübsche Baumansichten zur Visualisierung von Dateien und Ordnerstruktur – zusammen mit den Parametern

```
tree -fash
```

auch mit Größenangabe pro Datei, ausgehend vom aktuellen Verzeichnis. Auf schlichte Listen ist dagegen das Tool du spezialisiert, das kurz für „Disk usage“ steht. Das schlichte Listenformat ist ganz gut zur einfachen Sortierung durch verknüpfte Kommandos zu gebrauchen. So erstellt beispielsweise das verknüpfte Kommando

```
du -aS | sort -n -r | head
```

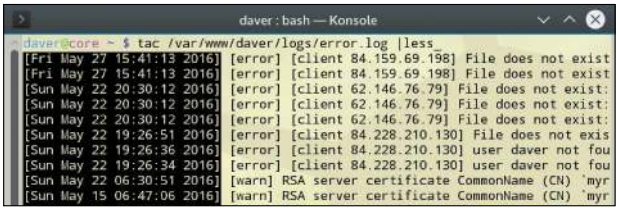
eine Top Ten der größten Dateien und Ordner im aktuellen Verzeichnis und sortiert nach Größe in Kilobyte. Sollen Auflistungen dieser Art nur Dateien und keine Ordnergrößen enthalten, dann ist wiederum tree das geeignete Werkzeug. Die verknüpften Befehle zur Sortierung fallen mit

```
tree -isafF |grep -v /$|sort
 -k2nr|head
```

etwas umfangreicher aus, aber die Ausgabe (nach Byte sortiert) kann sich sehen lassen.

Logdateien

Mit cat und tac Inhalte anzeigen



Auf den Kopf gestellt: tac ist das Gegenstück zum bekannten Befehl cat und gibt die Zeilen einer Datei, hier eine Logdatei, in umgekehrter Reihenfolge aus – mit den neuesten Zeilen am Anfang.

Auf Servern oder Mini-PCs, die einen Serverdienst im LAN anbieten, geben Logdateien am schnellsten Aufschluss über mögliche Probleme. Die Ausgabe von Textdateien aller Art in der Shell erfolgt meist mit dem Kommando cat, das eine Datei von Anfang bis Ende ausgibt.

Die interessantesten (weil neuesten) Einträge einer Logdatei stehen üblicherweise am Ende des Protokolls. Eine Auflistung des Inhalts zeilenweise in umgekehrter Reihenfolge erledigt tac, das Gegenstück zu cat. Das Tool gehört zum Standardrepertoire aller Linux-Distributionen, denn es ist Teil der GNU Coreutils. Wichtig ist, die umgekehrte Auflistung von Textdateien in der Shell mittels tac noch mit einem Anzeigetool wie less zu verbinden:

```
tac [Datei] | less
```

Die Ausgabe erfolgt nun seitenweise, und die Pfeil-ab- und Pfeil-auf-Taste kann den Inhalt abrollen. Die Taste Q beendet less.

Internetdownloads

Multitalent Aria2

Der übliche Weg, Dateien von einem Server herunterzuladen, führt über den Browser oder gelegentlich über wget in der Shell. Für den Download größerer Dateien von mehreren Servern gleichzeitig ist Aria2 ein weniger bekanntes Tool: Dieses Multitalent kann auch mit FTP, Bittorrent und Bittorrent-Metalinks umgehen, die zum Download von Linux-Distributionen öfter mal angeboten werden.

Von zwei Servern gleichzeitig laden: Das Multitalent Aria2 kann nicht nur mit den wichtigsten Protokollen für Downloads umgehen, sondern auch mehrere Spiegelserver nutzen.

Ein Programm für die Kommandozeile zum Herunterladen ist nicht nur für Rechner ohne grafische Benutzeroberfläche interessant. So ist es für langwierige Downloads auch nützlich, das Programm samt dem laufenden Download unabhängig von Browsern und grafischer Benutzeroberfläche per screen oder tmux in den Hintergrund zu verschieben. Der Download läuft so auch dann weiter, wenn man sich zwischenzeitlich abmeldet. Der Vorteil von Aria2 gegenüber dem einfachen wget liegt nicht nur bei der Unterstützung des Bittorrent-Protokolls. Das Tool kann auch von mehreren unterschiedlichen URLs zu einer identischen Datei parallel gleichzeitig herunterladen. In den verbreiteten Distributionen wie Debian, Ubuntu, Mint, Fedora ist Aria2 über den Paketmanager zu erreichen, so etwa mit

```
sudo apt-get install aria2
```

bei den Debian-Abkömmlingen. Nach erfolgter Installation hört das Programm auf den Namen aria2c und erwartet einfach die Angabe einer Download-URL, einer Bittorrent-Datei oder eines Magnet-Links:

```
aria2c ftp://ftp.fau.de/ubuntu-re
  leases/16.04/ubuntu-16.04-ser
  ver-amd64.iso
```

Gibt es mehrere URLs für die gleiche Datei, dann können etwa mit

```
aria2c ftp://ftp.fau.de/ubuntu-re
  leases/16.04/ubuntu-16.04-ser
  ver-amd64.iso ftp://ftp.fu-ber
  lin.de/linux/ubuntu/re
  leases/16.04/ubuntu-16.04-ser
  ver-amd64.iso
```

ganz einfach beide Quellen angegeben werden.

Sonderzeichen

Saubere Dateinamen

Ein typisches Linux-Dateisystem wie Ext2/3/4, XFS, BTRFS kommt mit allen Sonderzeichen in Datei- und Verzeichnisnamen zurecht – aber nicht alle Programme unter Linux. Auch bei der Kopie einer Datei auf einen FAT-formatierten USB-Stick oder auf eine Netzwerkfreigabe machen viele Sonderzeichen Probleme, weil sie auf dem Zieldateisystem nicht zulässig sind.

Dateinamen in Form bringen: Detox entfernt problematische Sonderzeichen aus Dateinamen. Das Tool arbeitet rekursiv und eignet sich für umfangreiche Dateisammlungen.

Der MP3-Player beschwert sich über ungültige Zeichen, die Windows-Freigabe mag eine ganze Reihe an Sonderzeichen nicht und Smart-TVs stolpern auch hin und wieder über Dateinamen an angesteckten USB-Sticks. Wenn eine Datensammlung wild zusammengewürfelte Namen enthält, ist es zu mühsam, unerwünschte Zeichen manuell auszutauschen. Das Rename-Tool Detox hilft weiter. Es verfügt über Filter gegen unerwünschte Zeichen in Dateinamen und steigt auf Wunsch auch rekursiv in beliebig viele Ordnerebenen hinab. Die Installation ist in Debian, Ubuntu und Mint schnell mit

```
sudo apt-get install detox
```

erledigt. Auch Fedora und Arch Linux kennen das Tool unter diesem Namen in ihren Paketquellen. Für Open Suse liegt Detox derzeit nur in dessen Build-Service als inoffizielles Paket vor (*https://build.opensuse.org/package/show/home:winski/detox*). Detox verfügt über Standardfilter, die rigoros alle Sonderzeichen der Zeichensätze ISO 8859-1 nach Ascii umwandeln, ferner Leerzeichen in Unterstriche, und somit alle möglichen Probleme mit Sonderzeichen beseitigen. Außerdem gibt es für vorsichtige Naturen einen Schalter („n“), sich die Änderungen erst mal ohne tatsächliche Änderungen auflisten zu lassen. Mit

```
detox -nrv Musik/
```

geht Detox sämtliche Unterordner des Ordners „Musik“ durch und listet die neuen Dateinamen zunächst nur auf. Die Option „-s“ erlaubt die Angabe von Filtern für Sonderzeichen und die vorhandenen Filter listet der Befehl

```
detox -L
```

auf. Generell liefert der Filter „utf_8“ gute Ergebnisse bei Dateinamen mit Unicode-Zeichen:

```
detox -nrv -s utf_8 ~/Musik/
```

Um die Änderungen tatsächlich durchzuführen, muss nur der Parameter „n“ gestrichen werden. ●

Hilfen zur Hardware

Für ältere Hauptplatinen gibt es seitens der Hersteller meist nur Windows-Programme zum Update der Firmware. Das Tool Flashrom kann aber auch unter Linux eine neue Firmware in das Flash-ROM vieler Platinen schreiben.

Von **David Wolski**

Notebook im Freien

Schatten für den Bildschirm

Die warmen Monate laden zur Arbeit am Notebook im Freien ein. Das ist aber nicht mit allen Notebookbildschirmen ein Vergnügen. Matte Bildschirme bieten bei hellem Umgebungslicht und direkter Sonne oft keinen ausreichenden Kontrast.

Bei der Arbeit im Freien ist Schatten der beste Freund des Bildschirms. Wenn sich ein Schattenplätzchen nicht finden lässt, dann hilft es, nur das Notebook unter einen Sonnenschutz zu stellen. Ein Schattenspender ist ganz schnell aus einem leeren Karton improvisiert, der auf der Rückseite oder an den Seiten nur noch einige Ausschnitte für Strom- und Anschlusskabel braucht. Zusammengefaltet sind Kartons auch eine Lösung für unterwegs.

Wem ein umfunktionierter Karton zu schmucklos oder nicht haltbar genug ist: Die Firma Tabrella stellt freistehende Mini-Sonnenblenden im Strandlook speziell für Notebooks und Tablets her (*http://amzn.to/24eRfAo*).

Nicht hübsch, aber wirksam: Ein Pappkarton spendet dem Notebook im Freien genügend Schatten und sorgt bei matten Bildschirmen für besseren Kontrast.

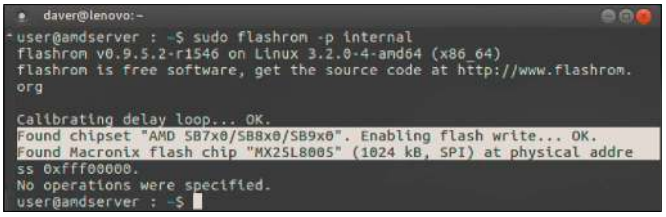
Das schicke Accessoire ist allerdings genau 35 Euro teurer als ein ausrangierter Pappkarton.

Bios/Uefi

Mit Flashrom Firmware aufspielen

Hersteller von Hauptplatinen haben in vielen ihrer Modelle ein Flash-Utility in der Firmware untergebracht. Das Aufspielen einer neuen Uefi-Version gelingt dann über einen FAT16-formatierten USB-Stick, der die neue Firmwaredatei enthält. Was aber, wenn die Hauptplatine ein älteres Modell ist und das Bios oder die Firmware per Windows-Programm aktualisiert wird?

Für Linux gibt es zum schreibenden Zugriff auf das Flash-ROM von Hauptplatinen das herstellerunabhängige Tool Flashrom, das bereits 15 Jahre stetig weiterentwickelt wird und gerade erst in einer neuen Version erschienen ist.



Chipsatz und Flash-ROM-Chip erkennen: Der erste Schritt mit Flashrom ist immer die Suche nach unterstützter Hardware. Das Tool erkennt mehrere Hundert Chips, Boards und Chipsätze.

Das Tool kennt alle wichtigen Protokolle für den Zugriff auf Flashchips und unterstützt in der Version 0.9.9 vom März 2016 immerhin 500 Hauptplatinen verschiedener Hersteller. Die neue Version ist erfreulicherweise bereits in den Paketquellen von Ubuntu 16.04 enthalten.

Es gibt auch einige Platinen, die explizit nicht unterstützt werden oder deren Kompatibilität noch nicht verifiziert ist. Eine aktuelle Liste findet sich unter *https://www.flashrom.org/Supported_hardware*.

Eine Warnung vorab: Ein Bios-Update geschieht immer auf eigene Gefahr. Wenn eine falsche Firmware geschrieben wird oder der Schreibvorgang fehlschlägt, wird das System nicht mehr booten. Flashrom gehört schon fast zur Standardausrüstung aller populären Linux-Distributionen und ist in Debian/Ubuntu/Mint schnell über den Paketmanager mit

```
sudo apt-get install flashrom
```

nachinstalliert. Das Tool lässt sich auch von einem Ubuntu-Live-System aus installieren (auf Heft-DVD) und verwenden, falls die verwendete Distribution nur eine alte Version des Tools im Repertoire hat.

1. Der erste Schritt ist die Identifizierung des Platinen-Chipsatzes und des Flash-ROM-Bausteins. Dazu dient in einem Terminalfenster dieser Befehl:

```
sudo flashrom -p internal
```

Sie erhalten die Info, ob Chip und Hauptplatine unterstützt werden. Bei Erfolg gibt Flashrom „Found“ und die Typenbezeichnung zurück. Generell sind Meldungen, die mit „Warning“ beginnen, noch kein Anzeichen, dass ein schreibender Zugriff nicht möglich wäre. Die Meldung „Writes have been disabled for safety reasons“ ist hingegen eine ernstzunehmende Gegenanzeige.

2. Zur Überprüfung, ob der Flashzugriff tatsächlich gelingt, kann Flashrom die bestehende Uefi/Bios-Version zunächst in eine Datei sichern, was der Befehl

```
sudo flashrom -r original.rom
```

erledigt.

3. Wenn dieser Zugriff gelungen ist, dann kann es ans Aufspielen der neuen Firmware gehen:

```
sudo flashrom -w [Firmware]
```

Für den Platzhalter „[Firmware]“ setzen Sie die tatsächliche Datei des Herstellers ein.

USB-Datenträger

Verlässliche Fortschrittsanzeige

Größere Dateien auf ältere USB-Sticks zu übertragen, kann quälend lange dauern. Die meisten Dateimanager unter Linux schreiben eine Datei zunächst anscheinend sehr schnell auf das Medium – doch dann bleibt der Fortschrittsbalken geraume Zeit bei 100 Prozent stehen.

Tatsächlich landen die Daten zunächst im Cache des Kernels. Danach dauert es, bis die Schreibaktionen auf dem USB-Stick abgeschlossen sind. Die Fortschrittsanzeigen vieler Dateimanager sind deshalb bei der Übertragung auf USB-Sticks nicht aussagekräftig. Während die Schreibaktion noch läuft, gibt es aber trotzdem eine Möglichkeit, den Fortschritt zu verfolgen. Der Befehl

```
watch grep "Dirty" /proc/meminfo
```

zeigt den Wert „Dirty“ der Kernel-Speicherverwaltung an.

Wie lange dauert's noch? Bei Dateiübertragungen auf USB-Sticks zeigen Dateimanager den Fortschritt nicht an. Hier hilft der Blick in die Speicherverwaltung unter „/proc/meminfo“.

Dies sind jene Speicherseiten in Kilobyte, die darauf warten, auf Datenträger geschrieben zu werden. Durch das vorangestellte Kommando „watch“ wird dieser Wert alle zwei Sekunden aktualisiert.

Wenn sich der Wert der Null nähert, ist die Übertragung auf den USB-Stick abgeschlossen.

Mausrad

Scrollgeschwindigkeit einstellen

Zu träge oder zu flott? Wie sich ein Dreh am Mausrad ganz subjektiv auf die Scrollbalken in Programmen auswirkt, ist nicht nur vom Mausmodell, sondern auch von Bildschirmgröße und Auflösung abhängig. Nicht jede Desktopumgebung für Linux bietet aber eine Einstellungsmöglichkeit für das Scrollverhalten des Mausrads.

Wer KDE nutzt, wird zur Scrollgeschwindigkeit in den Systemeinstellungen fündig: Unter „Eingabegeräte -> Maus -> Erweitert“ ist die gesuchte Einstellung als „Mausrad erzeugt Bildlauf“ untergebracht. Was ist aber zu tun, wenn auf dem Desktop kein KDE zum Einsatz kommt?

Unter Debian, Ubuntu und Linux Mint gibt es das Tool Imwheel, das die Konfiguration vieler Detaileinstellungen von Mäusen beherrscht. Mit

```
sudo apt-get install imwheel
```

ist es schnell installiert. Imwheel benötigt seine Instruktionen in der Konfigurationsdatei „.imwheelrc“ im Home-Verzeichnis. Tragen Sie daher alle Änderungen oder Ergänzungen der Mausfunktionen mit einem Editor in diese Datei ein. Zum Beschleunigen des Mausrades sind die folgenden drei Zeilen nötig:

```
".*"
None, Up, Up, 3
None, Down, Down, 3
```

Der Wert „3“ gibt die Geschwindigkeit an, mit welcher das Mausrad Fensterinhalte abrollt. Je größer der Wert, desto höher die Geschwindigkeit. Der Aufruf *imwheel* in einem Terminalfenster aktiviert die neue Konfiguration und nach Änderungen übernimmt

```
imwheel -k
```

die neuen Werte. Damit Imwheel immer beim Start der grafischen Oberfläche aktiv wird, muss es in der verwendeten Desktopumgebung als Autostart-Programm eingetragen werden. ●

Software im Einsatz

Die Softwaretipps zeigen dieses Mal den Aufbau eines interaktiven Tabellenblatts mit Auswahlbox in Libre Office Calc, eine Alternative zu Whatsapp Web und nachträglich eingefügte Seitenzahlen in PDF-Dokumenten.

Von **David Wolski**

Whatsapp-Client

Whatsie für Linux

Ob man will oder nicht – vor dem Messengerdienst Whatsapp scheint es momentan kein Entrinnen zu geben, da sich immer mehr Leute im Kollegen- und Bekanntenkreis in Whatsapp-Gruppen zusammenschließen. Ein Chatprogramm für Whatsapp gibt es jetzt auch für den Linux-Desktop.

Das Programm Whatsie (*https://whatsie.chat*) ist ein inoffizieller Client, der auf dem offiziellen Whatsapp Web aufsetzt, aber wie eine eigenständige Desktop-App erscheint. Dabei bleibt der eigentliche Client das Smartphone mit dem eingerichteten Whatsapp-Konto. Whatsie ist lediglich ein Front-End für die App auf dem Smartphone, das auch hier Voraussetzung zur Teilnahme ist. Der entscheidende Vorteil von Whatsie ist, den Messenger mit „Drag & Drop"-Unterstützung auf dem Desktop einzubinden und bei Bedarf zu einem Symbol im Infobereich zu verkleinern.

Die Installation von Whatsie auf verbreiteten Distributionen ist nicht weiter kompliziert, da der Entwickler der Projekt-Webseite fertige DEB- sowie RPM-Pakete für 32- und 64-Bit-Systeme bereitstellt. Nach dem Download wird das DEB-Paket unter Debian/Ubuntu/Mint mittels

```
sudo dpkg -i [Paket].deb
```

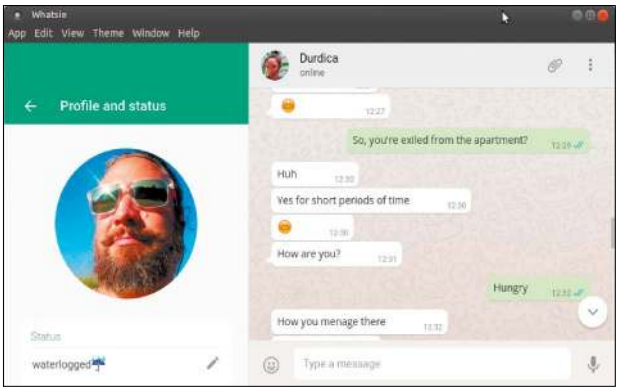
installiert, in Fedora und Open Suse auf diesem Weg:

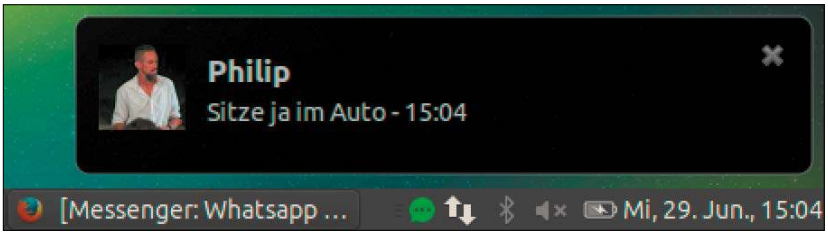
```
sudo rpm -ivh [Paket].rpm
```

Nach dem ersten Aufruf verlangt Whatsie genauso wie Whatsapp Web die Verbindung zur App auf dem Smartphone, die per abfotografiertem QR-Code hergestellt wird. Whatsie zeigt dann die Chats auf seinem Programmfenster an.

Das Smartphone muss unterdessen immer eingeschaltet bleiben.

Alternativer Client: Whatsie nutzt das Electron-Framework, um Whatsapp Web in einem Programmfenster darzustellen. Hier funktioniert auch Drag & Drop für Bilddateien.





Whatsapp-Nachrichten auf dem Linux-Desktop: Wenn das Programmfenster von Whatsie minimiert oder auf sein Symbol reduziert ist, zeigen Pop-ups die neuen Nachrichten.

Whatsie 2.0 Beta: Inoffizieller Desktopclient für Whatsapp. Download des Quellcodes und von fertigen Linux-Pakete unter *https://github.com/Aluxian/Whatsie* (50 MB, englischsprachig, MIT-Lizenz).

Firefox-Suche

Zurück zum alten Suchfeld

Die neue Suche neben der Adresszeile in Firefox behagt nicht allen Anwendern. Wenn jemand routinemäßig mit mehreren Suchmaschinen arbeitet, dann ist das neue Untermenü zur Auswahl des Suchanbieters sehr umständlich.

Das Problem mit dem neuen Suchfeld ab Firefox 43: Es merkt sich die letzte Auswahl nicht, sondern schickt die Anfragen immer zur Standardsuchma-

schine, sofern die Suchmaschine nicht bei jeder Suche manuell ausgewählt wird. Um das Verhalten des alten Suchfelds wiederherzustellen, haben Firefox-Anwender die Erweiterung „Old Search Fixed 2“ erstellt. Nach deren Installation und einem Neustart des Browsers ersetzt die Erweiterung die neue Suche durch die alte.

Old Search Fixed 2: Stellt in Firefox ab Version 43 das alte Suchfeld wieder her. Installation unter *https://addons.mozilla.org/de/firefox/addon/old-search-fixed2*.

Gewohnte Suche: Das herkömmliche Suchfeld, das Firefox 43 durch ein verzweigtes Menü zur Auswahl der Suchmaschinen ersetzt hat, kommt per Add-on zurück.

Twitter und Co

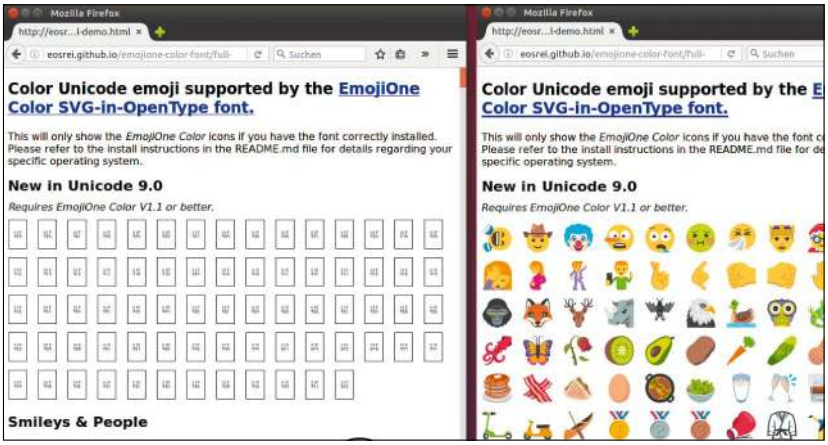
Emojis für Linux

Während die von Smartphone-Apps bekannten Emojis, also farbige Grafiken für Emoticons in Messengerprogrammen, unter Linux meist tadellos dargestellt werden, ist im Webbrowser davon nichts zu sehen: Emojis sind dort beispielsweise auf Twitter nur durch einen leeren UTF-8-Platzhalter vertreten, denn den üblichen Linux-Distributionen fehlen die Emoji-Fonts.

Der Entwickler Brad Erickson hat aus frei verfügbaren SVG-Grafiken den Font „Emojione Color“ zusammengestellt und auf Github veröffentlicht (*https://github.com/eosrei/emojione-color-font*). Der Font sorgt in Firefox und Thunderbird für bunte Emojis, in Google Chrome/Chromium und anderen Anwendungen immerhin für eine monochrome Darstellung der Minibilder, da hier SVG-Grafiken in Unicode-Fonts noch nicht unterstützt werden.

Es genügt nicht ganz, den Font lediglich als zusätzliche Schriftart in Linux einzurichten. Damit Emojis sichtbar werden, ist zusätzlich noch die Änderung des Standardfonts auf Bitstream Vera nötig.

In Ubuntu und Linux Mint erledigt die Installation des Fonts ein PPA des



Vorher und nachher: Die Schriftart Emojione Color sorgt in Firefox für bunte Emoticons (Emojis). In Ubuntu und Co. ist die freie Unicode-Schriftart per PPA schnell installiert.

Entwicklers. Mit den folgenden drei Befehlen

```
sudo apt-add-repository
  ppa:eosrei/fonts
sudo apt-get update
sudo apt-get install fonts-emoji
  one-svginot
```

ist die neue Symbolschriftart eingerichtet. Eine Demo unter *http://eosrei.github.io/emojione-color-font/full-demo.html* zeigt eine Übersicht der neuen Emojis. Eine Nebenwirkung ist, dass der Font „DejaVu“ gegen den beinahe identischen Font „Bitstream Vera“ ausgetauscht wird. Für andere Linux-Distributionen als Ubuntu/Mint gibt es auf der Github-Webseite des Entwicklers unter *https://github.com/eosrei/emojione-color-font/releases* ein „tar.gz“-Archiv für Linux, das ein Installationsscript („install.sh“) und das dazugehörige Deinstallationsscript enthält („uninstall.sh“).

Emojione Color 2.2.1: Unicode-Font für grafische Emoticons. Download und Installationsscript unter *https://github.com/eosrei/emojione-color-font/releases* (3 MB, Creative Commons Attribution 4.0 International).

PDF-Seitenzahlen

Nummern nachtragen

Ist ein PDF in einem Reader geöffnet, dann sind Seitenzahlen im Dokument nicht weiter wichtig. Schließlich zeigt der Betrachter schon an, auf welcher Seite man gerade ist, und die Reihenfolge gerät auch nicht durcheinander. Für Ausdrucke sollten Dokumente aber ordentliche Seitenzahlen haben.

Seitenzahlen lassen sich auch nachträglich noch in PDF-Dokumente eintragen. Je nachdem, um wie viele Seiten es geht, eignen sich verschiedene Herangehensweisen. Der einfachste, aber bei mehreren Seiten schnell umständliche Ansatz ist die manuelle Nachbearbeitung eines PDFs mit dem Programm Xournal. Das Programm kann PDF-Dateien aller Art öffnen, sofern diese nicht passwortgeschützt sind, und dann im Stil einer simplen Bildbearbeitung nachbearbeiten. In den populären Linux-Distributionen wie Debian, Ubuntu, Fedora und Open Suse liegt das Programm in den Standard-Paketquellen bereit. Unter Debian/Ubuntu installieren Sie es mit diesem Kommando:

```
sudo apt-get install xournal
```

Nach dem Laden einer PDF-Datei im Xournal erlaubt das Texttool die manuelle Platzierung einer Seitenzahl auf jeder einzelnen Seite. Damit der Drucker die Zahlen auch noch zu Papier bringt, sollte der Abstand zum Rand nicht zu knapp ausfallen und über einem Zentimeter liegen.

Sollen viele Seiten in einem PDF Seitenzahlen bekommen, dann hat Libre Office die bessere, wenn auch anspruchsvollere Lösung parat: Die Büro-Suite lädt PDFs in die Anwendung Draw und macht aus jeder PDF-Seite eine Folie wie für eine Präsentation. Über die Bearbeitung der Masterfolien können alle Seiten nachträglich eine fortlaufende Foliennummer erhalten. So funktioniert es:

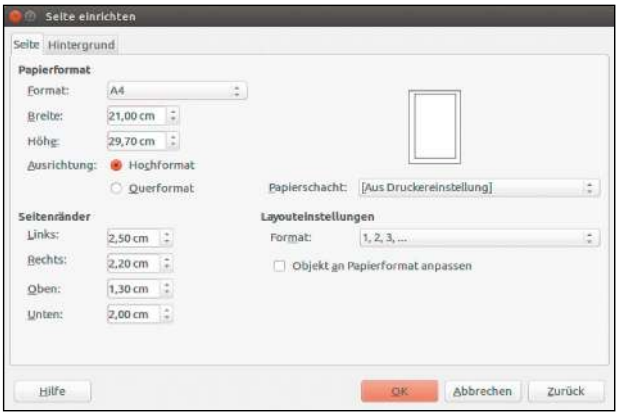
1. Ist das PDF über „Datei -> Öffnen“ in Libre Office Draw geladen, dann muss erst der Druckbereich angepasst werden, der als hellgrauer Rahmen auf jeder Dokumentseite eingeblendet ist. Der Menüpunkt „Format -> Seite“ beziehungsweise „Format -> Folieneigenschaften“ (ab Libre Office 5.1) erlaubt diese Anpassung unter „Seite -> Seitenränder“. Damit oben oder unten noch Seitenzahlen in den druckbaren Bereich passen, muss dort der Seitenrand reduziert werden, etwa auf einen Zentimeter.

2. Nun geht es an die Masterfolie(n), die sich nach dem Wechsel des Bearbeitungsmodus über „Ansicht -> Master“ bearbeiten lassen. In den meisten PDFs gibt es mehr als eine Masterfolie. Alle sind in der Spalte links angeordnet.

3. Innerhalb des druckbaren Bereichs, aber nicht in den eigentlichen, auf der Masterfolie ausgeblendeten PDF-Inhalt hinein, fügen Sie jetzt die fortlaufende Seitenzahl ein. Dies erledigt der Menüpunkt „Einfügen -> Feldbefehl -> Foliennummer“. Nun muss der Positionsrahmen mit der enthalten Nummer noch an den Rand verschoben, und über die „Eigenschaften“ in der rechten Seitenleiste formatiert werden.

4. Damit die fortlaufende Nummer auch auf jeder Seite des PDFs auftaucht, ist es nötig, den Positionsrahmen per Kopieren und Einfügen (Strg-C, Strg-V) auf jeder Masterfolie in der linken Spalte einzufügen. Keine Sorge – die gewählte Position kopiert Draw dabei gleich mit.

5. Nach einem Ansichtswechsel mit „Ansicht -> Normal“ sind nun die eingefügten Seitenzahlen zu sehen und das Dokument kann über „Datei -> Exportieren als PDF“ wieder als PDF gespeichert werden. Sind wider Erwarten keine Seitenzahlen zu sehen, dann prüfen Sie in der Masteransicht, dass der Positionsrahmen mit der Foliennummer innerhalb des grauen Rahmens liegt und sich nicht mit dem PDF-Inhalt überschneidet.

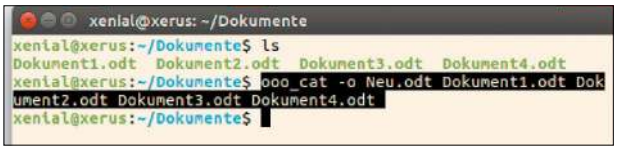


Randexistenz: Damit die eingefügten Seitenzahlen im PDF Platz finden, muss der bedruckbare Bereich weiter an den Rand rücken. Es sollte mehr als ein Zentimeter Rand bleiben.

Angezählt: Libre Office Draw kann per Folienmaster in ein bestehendes PDF nachträglich fortlaufende Seitenzahlen mit vertretbarem Aufwand einfügen.

Libre Office Writer

Dokumente zusammenfügen



Vereint mehrere ODT-Dateien zu einem Dokument: Das Python-Script der Sammlung Ooopy fügt Einzeldokumente zusammen. Meist sind dann noch Anpassungen bei der Formatierung nötig.

Aus einer Menge einzelner Seiten oder Kapiteln soll ein zusammenhängendes Dokument entstehen. Was bei einer Handvoll Dateien noch auf manuellem Wege gelingt, wird bei einer größeren Anzahl an Einzeldateien mühsam.

Die manuelle Methode, Dokumente im Libre Office Writer zusammenzufügen, ist im Menüpunkt „Einfügen -> Dokument“ untergebracht. Ein Dateibrowser erlaubt die Auswahl einer Datei, deren Inhalt dann an der aktuellen Stelle im Dokument erscheint. Es muss sich dabei um Textdokumente handeln, also um Dateien im Format ODT, SXW, DOC oder DOCX. Tabellendateien oder Präsentationen akzeptiert Libre Office an dieser Stelle nicht.

Sollen viele Einzeldateien zu einem Dokument verschmelzen, dann hilft die Python-Scriptsammlung Ooopy (*www.runtux.com/ooopy.html*) weiter. Unter anderem findet sich in der Sammlung das Script „ooo_cat“ für die Kommandozeile, das Libre-Office-Dokumenten mittels XML-Parser zusammenfügt.

Nach dem Download des „tag.gz“-Archivs und dem Entpacken mit einem grafischen Packprogramm oder in der Shell mit

```
tar xzvf OOoPy-1.11.tar.gz
```

liegt im Unterverzeichnis „OooPy-1.11“ das Installationsscript. Starten Sie dieses mit diesem Kommando:

```
sudo python setup.py install
```

Danach sind die Tools einsatzbereit: Der Befehl

```
ooo_cat -o Neu.odt Dok1.odt Dok2.
 odt Dok3.odt Dok4.odt
```

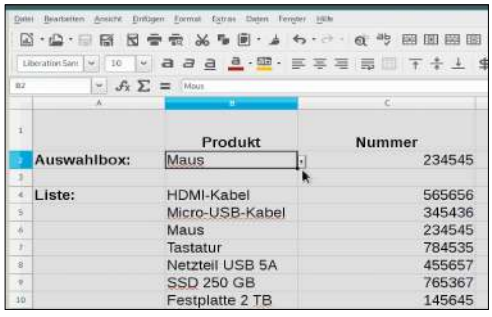
fügt die Dateien „Dok1.odt“ bis „Dok4.odt“ zur neuen Datei „Neu.odt“ zusammen. Das Script erwartet immer ODT-Dateien, mit Dokumenten in fremden Formaten sowie mit ODS-Tabellen und ODP-Präsentationen kann es nicht umgehen. Meistens gibt es im neu angelegten Dokument noch einige Korrekturen an Formatierungen und Seitenwechseln zu erledigen.

Übrigens: Wenn das Material nicht in Form von ODT-Dokumenten vorliegt, sondern in Formaten wie DOC und DOCX von Microsoft Office, dann hilft Libre Office bei der Konvertierung nach ODT. Unter „Datei -> Assistenten -> Dokumentkonverter“ findet sich ein Serienkonverter für alle Typen von Dokumenten, die Libre Office unterstützt. Der Konverter schreibt die neuen Dateien in einen ausgewählten Zielordner, es werden also keine Originaldateien überschrieben.

Ooopy 1.11: Python-Scriptsammlung zur Änderung von ODT-Dokumenten. Download unter *https://sourceforge.net/projects/ooopy* (260 KB, Lesser GNU Public License).

Libre Office Calc

Auswahlbox für Zellen



Einträge aus Tabellen per Klick auswählen: Mit einer Auswahlbox und einer Matrixabfrage mit der Funktion „SVERWEIS“ statten Sie Artikellisten mit einem praktischen Suchwerkzeug aus.

Lange Tabellen wie Artikel- und Preislisten werden durch eine interaktive Auswahlbox übersichtlicher. Die Box dient in der Kopfleiste einer Tabelle zum Nachschlagen eines Eintrags und dessen zugehöriger Daten.

Auswahlboxen in Libre Office Calc erlauben die schnelle Navigation per Tastatureingaben zum gesuchten Eintrag. Um den Aufbau einer Auswahlbox zu erläutern, geht dieses Beispiel von einer Tabelle aus, in welcher von Zelle B4 bis B10 Artikelnamen stehen und in der benachbarten Spalte C die Artikelnummern. Die Auswahlbox soll nun alle Artikelnamen in einer Liste anbieten und in der nebenstehenden Zelle beim Anklicken eines Eintrags dessen Nummer anzeigen. Der erste Schritt ist die Markierung der Zelle, welche die Auswahlbox enthalten soll. Dann geht es weiter in das Menü „Daten -> Gültigkeit“. In diesem Dialog wählen Sie im Feld „Zulassen“ die Option „Zellbereich“. Darunter wählt man im Feld „Quelle“ mit dem Symbol rechts daneben den Bereich in der Spalte B mit allen Artikelnamen aus, in diesem Beispiel B4 bis B10. Nach einem Klick auf „OK“ ist die Auswahlbox schon in der Tabelle. Damit die Auswahl die richtige Artikelnummer aus der Tabelle holt, bekommt die nebenstehende Zelle folgende Formel zugewiesen:

```
=SVERWEIS(B2;B4:C10;2;0)
```

Die Formel holt jetzt automatisch aus der angegebenen Matrix B4:C10 den passenden Eintrag zum Suchbegriff in der interaktiven Auswahlbox (B2). ●

Leserbriefe

Haben Sie Fragen zum Heft, oder möchten Sie uns Ihre Meinung dazu mitteilen? Schreiben Sie bitte an *linux@it-media.de* oder per Post an Redaktion LinuxWelt, IT Media, Gotthardstr. 42, 80686 München. Von den vielen Zuschriften können wir nur eine Auswahl veröffentlichen. Sinnwahrende Kürzungen behalten wir uns vor.

Support für Ubuntu-Varianten

In der letzten LinuxWelt wurde ein reduziertes Xubuntu Core 16.04 vorgestellt als „Ubuntu LTS mit XFCE auf dem Desktop“. Was dort unklar blieb: Ist der Unterstützungszeitraum fünf Jahre wie beim Standard-Ubuntu oder drei Jahre wie bei Xubuntu LTS?
Peter Knoll, per Mail

Bei Xubuntu Core handelt es sich wie bei der regulären Ausgabe von Xubuntu 16.04 um eine LTS-Ausgabe mit drei Jahren Unterstützung, also bis April 2019. Hierbei unterscheidet sich Xubuntu Core nicht von den anderen offiziellen Ubuntu-Varianten. Allein die Hauptausgabe mit Unity-Desktop erhält von Canonical fünf Jahre Unterstützung.

Da allerdings Xubuntu und Xubuntu Core genau auf den gleichen Paketquellen aufbauen wie die reguläre Ubuntu-Ausgabe, bekommen Kernkomponenten wie Kernel, Subsysteme, Serversoftware und Programme wie Firefox ebenfalls fünf Jahre Aktualisierungen. Das sind jene Pakete, die bei Ubuntu in den Repositories „main“ und „restricted“ vorliegen. Alle anderen Pakete, die zu XFCE gehören und die vom Xubuntu-Team gepflegt werden, erhalten ab 2019 keine Updates mehr. Das betrifft alle Pakete, die in den Ubuntu-Repositories „universe“ und „multiverse“ liegen.

Ein genereller Tipp: Wer sich über die Laufzeit seiner Ubuntu-Variante im Unklaren ist, muss nicht lange im Web recherchieren. Das Kommandozeilentool ubuntu-support-status zeigt die verschiedenen Supportzeiträume aller installierten Pakete. Das Tool ist in Ubuntu und Co. vorinstalliert und Sie können es für eine knappe Übersicht im Terminal mit

```
ubuntu-support-status
```

aufrufen. Das Terminalprogramm arbeitet auf Wunsch aber noch detaillierter. Mit dem zusätzlichen Parameter „--list“ zeigt es für jedes einzelne installierte Paket den verbleibenden Supportzeitraum. Interessant ist ferner der Schalter „--show-unsupported“, der nicht mehr unterstützte Software anzeigt.

Unsicher über den Supportzeitraum? Das Terminaltool ubuntu-support-status listet die unterschiedlichen Supportfristen eines Ubuntu-Systems auf.

Probleme mit Linux?

Haben Sie Probleme mit Linux?
In unserem Forum unter *www.pcwelt.de/forum* stehen Ihnen unter „Betriebssysteme -> Linux-Distributionen“ neben Linux-Experten auch andere Linux-Anwender mit Rat und Tat zur Seite und helfen bei Schwierigkeiten mit Linux.
Aktuelle News rund um das Thema lesen Sie unter *www.pcwelt.de/computer-technik/betriebssystem-software/linux.*

Kontakt zur Redaktion
Wir freuen uns über jede Mail! Bei Fragen zum Heft LinuxWelt wenden Sie sich am besten an *linux@it-media.de.* Bitte beachten Sie, dass wir keinen Support für spezielle Hardware oder die Linux-Systeme auf der Heft-DVD leisten können.

Heftbestellung & Abonnement
Sie können die Reihe LinuxWelt auch unabhängig von PC-WELT abonnieren. Für den Abo-Preis von 49,50 € (D), 64,50 CHF (CH) und 53,50 € (A) erhalten Sie sechs Hefte im Jahr versandkostenfrei zugesandt.
Haben Sie eine Ausgabe von LinuxWelt verpasst? Hier können Sie einzelne Hefte nachbestellen:
Tel.: 0711/7252-277
Österreich: Tel.: 01/2195560
Schweiz: Tel.: 071/31406-15
oder schreiben Sie an den PC-WELT-Kundenservice, Postfach 810580, 70522 Stuttgart, Mail: *linuxwelt@zenit-presse.de.*

Digitalabo in der App
https://shop.pcwelt.de/portal/linuxwelt-ipad-jahresabo-zukunft-ist-jetzt--2636

IMPRESSUM

VERLAG

IT Media Publishing GmbH & Co. KG
Gotthardstr. 42, 80686 München,
Tel. 089/3398052-10,
Fax 089/3398052-70, E-Mail: *info@it-media.de*, *www.it-media.de*

Chefredakteur: Sebastian Hirsch (v.i.S.d.P – Anschrift siehe Verlag)

Gesamtanzeigenleitung:
IDG Tech Media GmbH, Lyonel-Feininger Str. 26, 80807 München,
Tel. 089/36086-0, Fax 089/36086-118,
Stefan Wattendorff, E-Mail: *swattendorf@idgtech.de*

Druck: Mayr Miesbach GmbH, Am Windfeld 15, 83714 Miesbach,
Tel. 08025/294-267

Inhaber- und Beteiligungsverhältnisse: Alleinige Gesellschafterin der IT Media Publishing GmbH & Co. KG ist die IT Media Publishing Verwaltungs GmbH, München, Geschäftsführer Sebastian Hirsch.

WEITERE INFORMATIONEN

REDAKTION

Gotthardstr. 42, 80686 München,
Tel. 089/3398052-10, Fax 089/3398052-70,
E-Mail: *info@it-media.de*, *www.it-media.de*

Chefredakteur: Sebastian Hirsch
(verantwortlich für den redaktionellen Inhalt)
Stellvertretender Chefredakteur: Thomas Rau
Chef vom Dienst: Andrea Kirchmeier
Redaktion: Arne Arnold

Redaktionsbüro: MucTec (hapfelboeck@googlemail.com)
Freie Mitarbeiter Redaktion: Dr. Hermann Apfelböck, Thorsten Eggeling, Markus Fasse, Stephan Lamprecht, Daniel Schlep, David Wolski

Titelgestaltung: Schulz-Hamparian, Editorial Design / Thomas Lutz

Freier Mitarbeiter Layout/Grafik: Alex Dankesreiter
Freie Mitarbeiterin Schlussredaktion: Andrea Röder
Freie Mitarbeiterin Herstellung: Claudia Pielen
Freier Mitarbeiter digitale Medien: Ralf Buchner
Redaktionsassistenz: Manuela Kubon

ANZEIGENREPRÄSENTANZ

IDG Tech Media GmbH, Lyonel-Feininger Str. 26, 80807 München,
Tel. 089/36086-210, Fax 089/36086-263,
E-Mail: *media@pcwelt.de*
Gesamtanzeigenleitung:
Stefan Wattendorff (-212)
(verantwortlich für den Anzeigenteil)

Digitale Anzeigenannahme – Datentransfer:
Zentrale E-Mail-Adresse: *AnzeigendispoPrint@pcwelt.de*
Digitale Anzeigenannahme – Ansprechpartner:
Walter Kainz (-258), E-Mail: *wkainz@idg.de*

Anzeigenpreise: Es gilt die Anzeigenpreisliste 33 (1.1.2016).
Bankverbindungen: Deutsche Bank AG,
Konto 666 22 66, BLZ 700 700 10;
Postbank München, Konto 220 977-800,
BLZ 700 100 80
Anschrift für Anzeigen: siehe Anzeigenabteilung
Erfüllungsort, Gerichtsstand: München

Verlagsrepräsentanten für Anzeigen in ausländischen Publikationen
Europa: Shane Hannam, 29/31 Kingston Road, GB-Staines, Middlesex TW 18 4LH, Tel.: 0044-1-784210210. USA East: Michael Mullaney, 3 Speen Street, Framingham, MA 01701, Tel.: 001-2037522044. Taiwan: Cian Chu, 5F, 58 Minchuan E Road, Sec. 3, Taipei 104 Taiwan, R.O.C., Tel.: 00886-225036226. Japan: Tomoko Fujikawa, 3-4-5 Hongo Bunkyo-Ku, Tokyo 113-0033, Japan, Tel.: 0081-358004851

VERTRIEB

Vertrieb Handelsauflage:
MZV GmbH & Co. KG, Ohmstraße 1, 85716 Unterschleißheim
Tel. 089/31906-0, Fax 089/31906-113
E-Mail: *info@mzv.de*, Internet: *www.mzv.de*

Druck: Mayr Miesbach GmbH, Am Windfeld 15, 83714 Miesbach,
Tel. 08025/294-267

VERLAG

IT Media Publishing GmbH & Co. KG
Gotthardstr. 42, 80686 München,
Tel. 089/3398052-10, Fax 089/3398052-70,
E-Mail: *info@it-media.de*, *www.it-media.de,*
Sitz: München, Amtsgericht München, HRA 104234

Veröffentlichung gemäß § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949:
Alleinige Gesellschafterin der IT Media Publishing GmbH & Co. KG ist die **IT Media Publishing Verwaltungs GmbH**, Sitz: München, Amtsgericht München, HRB 220269

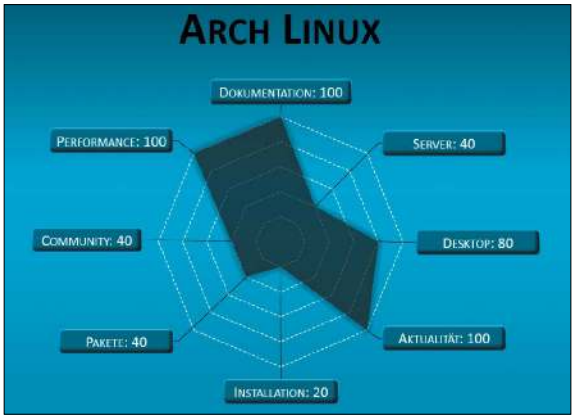
Geschäftsführer: Sebastian Hirsch

ISSN 1860-7926

Kundenservice: Fragen zu Bestellungen (Abonnement, Einzelhefte), zum bestehenden Abonnement / Premium-Abonnement, Umtausch defekter Datenträger, Änderung persönlicher Daten (Anschrift, E-Mail-Adresse, Zahlungsweise, Bankverbindung) bitte an
Zenit Pressevertrieb GmbH
Kundenservice
Postfach 810580
70522 Stuttgart
Tel: 0711/7252-277
(Mo bis Fr, 8 bis 18 Uhr; aus dem deutschen Festnetz nur € 0,14 pro Minute, Mobilfunkpreise maximal € 0,42 pro Minute),
Fax: 0711/7252-377
Österreich: 01/2195560
Schweiz: 071/31406-15
E-Mail: *linuxwelt@zenit-presse.de*
Internet: *www.pcwelt.de/shop*

LinuxWelt 6/2016 erscheint am 30.09.2016

Linux im Radar



Der große Distributions-Überblick: Welche Stärken und Schwächen haben welche Linux-Distributionen? Unser Orientierungsbeitrag mit den wichtigsten Desktop- und Spezialsystemen visualisiert die besonderen Talente und Nachteile populärer Linux-Distributionen mit einprägsamen Radargrafiken. Es gibt triftige Gründe für die Neuauflage dieses Distributions-Checks der LinuxWelt 3/2013, der das PDF-Booklet auf DVD seither einleitete: Zum einen hat sich mittlerweile so manche Einzelbewertung deutlich verschoben, zum anderen drängen neue Kandidaten in den Vordergrund.

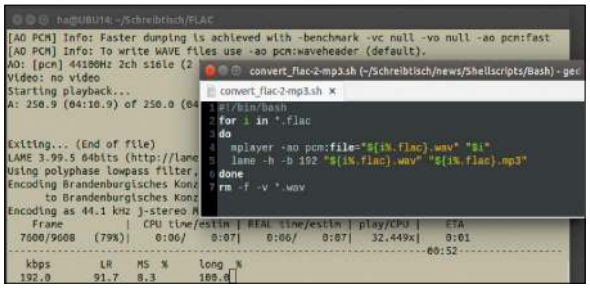
Produktiv mit Linux Mint 18

Der große Ratgeber zu Linux Mint 18: Die nächste Linux-Welt nimmt das neue Linux Mint 18 „Sarah“ genau unter die Lupe. Der Ratgeber bespricht die optimale Einrichtung, die Möglichkeit zum Upgrade älterer Versionen, wichtige Erstmaßnahmen nach der Installation und die individuelle Anpassung von Desktop und System. Besonderes Augenmerk erhalten neue Komponenten wie die aufgefrischte Oberfläche, die neuen X-Apps und Änderungen bei der Aktualisierungsverwaltung und dem Paketmanagement.

Datenträger und Dateisysteme im Griff

Komplettratgeber zu Festplatten, USB-Geräten, SSDs und Netzressourcen: Die ersten Fragen stellen sich schon beim Partitionieren und Formatieren von Datenträgern. Ist eine Aufteilung des Datenspeichers sinnvoll und welches Dateisystem eignet sich für die geplante Aufgabe am besten? Im laufenden Betrieb mag es zwar ausreichen, sich auf das Automount grafischer Desktopsysteme zu verlassen, doch wer die Kontrolle behalten will, wird sich mit dem Mountbefehl und der fstab anfreunden müssen. Ein weiterer wichtiger Aspekt ist das Einhängen von Netz- und Serverressourcen in das lokale Dateisystem. Weitere Themen des Ratgebers erklären den Einsatz von Raid-Verbänden, die Verwendung von Diskquota, den Umgang mit Analysetools und die Optimierung von Festplatten und SSDs hinsichtlich Leistung, Kapazität und Energieverbrauch.

Alles konvertieren



Video – Audio – Bilder – Office – PDF – Text: Digitale Daten liegen nicht immer im Wunschformat vor. Das zeigt sich spätestens dann, wenn die Abspiel- oder Anzeigegeräte beziehungsweise die dort zuständigen Programme ihren Job verweigern. Erfreulicherweise gibt es für praktisch jedes Multimedia- oder Textformat einschlägige Werkzeuge zur Umwandlung. Die LinuxWelt zeigt die beste Konvertersoftware und ihre Benutzung, vor allem aber die besten Methoden für eine automatisierte Massenkonvertierung.

Aus Aktualitätsgründen können sich Themen ändern.

PC WELT PLUS | ANDROID WELT | LINUX WELT

PC-WELT Plus Digital

Alle aktuellen & bisherigen Ausgaben in der Magazin-App und im Webbrowser lesen

PC-WELT Plus Digital Abo

6,99 € pro Monat

App erhältlich für:

Lesen Sie einen Monat lang **alle Ausgaben** der **PC-WELT Plus**, **LinuxWelt** und **Android-Welt** sowie alle **PC-WELT Sonderhefte** in der **Magazin-App** oder im **Webbrowser**.

Jetzt bestellen unter **www.pcwelt.de/plus-monat**
oder per Telefon: 0711/7252277 oder ganz einfach:

1. Formular ausfüllen **2. Foto machen** **3. Foto an shop@pcwelt.de**

Ja, ich bestelle das PC-WELT Plus Digital Abo für 6,99 €.

Möchten Sie nach Ablauf des Monats Ihr PC-WELT Plus Digital-Abo anschließend weiter lesen, brauchen Sie nichts zu tun. Sie erhalten das PC-WELT Plus Digital-Abo für weitere 12 Ausgaben zum aktuellen Jahresabopreis von z.Zt. 69,99 EUR. Danach ist eine Kündigung zur übernächsten Ausgabe jederzeit per Post an PC-WELT Kundenservice, Postfach 810580, 70522 Stuttgart oder per E-Mail an kundenservice@pcwelt.de 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

PW1MO15231

PC-WELT erscheint im Verlag IDG Tech Media GmbH, Lyonel-Feininger-Str. 26, 80807 München, Registergericht München, HRB 99187, Geschäftsführer: York von Heimburg.
Die Kundenbetreuung erfolgt durch den PC-WELT Kundenservice, ZENIT Pressevertrieb GmbH, Postfach 810580, 70522 Stuttgart, Geschäftsführer: Joachim John

3% Rabatt auf Ihre Bestellung:
Gutscheincode:
TUXMEUPLXWELT

TUXEDO COMPUTERS

Mehr als Hardware

TUXEDO Computers sind individuell gebaute Computer und Notebooks, die vollständig Linux-tauglich sind.
Windows natürlich auch, das kann ja jeder, wir natürlich auch :) Aber es steckt noch mehr dahinter:

+ Assemblierung und Installation in unserem Haus
+ Eigens programmierte Treiber, Scripte und Addons
+ Individueller Support und eigene Repositories
+ 100 % Funktionalität aller Hardware-Bestandteile:
  - Aller Sondertasten
  - Helligkeitseinstellung
  - Stand-By-Modus / Ruhezustand
  - Energiesparfunktionen, usw.
+ **Pinguin-Sondertaste** :-)
+ Exklusiver Zugang zur ***myTUXEDO.de*** Cloud
  - Deutsche Server & Verschlüsselung
  - RAID-Systeme & mehrfach Backups
  - Sync-Clients, Browseranwendungen, webdav
  - Kalender, Aufgaben, Kontakte, Media-Player
  - Dokumentenbearbeitung, Mail, Galerie
  - 10GB Speicherplatz kostenlos

Andere Betriebssysteme kann ja jeder, wir natürlich auch...
Aber wir können vor allem Linux!
Und zwar so, dass alles einfach funktioniert, alles!
Und um das "Drumherum" kümmern wir uns auch gleich :-)

TUXEDO Book XC14 | XC15 | XC17

+ 14", 15,6" oder 17,3" Full-HD IPS matt
+ Metallgehäuse; beleuchtete Tastatur
+ Intel Core i7 Quad-Core
+ bis zu 4 HDD/SSD, HDMI + 2x DisplayPort
+ bis zu 64 GB DDR4 Arbeitsspeicher
+ bis zu GeForce GTX 980M

ab 1.249 €*

TUXEDO InfinityBook

+ 13,3" oder 15,6" Full-HD IPS matt
+ Aluminiumgehäuse Unibody Ultrabook
+ bis zu 15 Std. Akkulaufzeit
+ inkl. Intel Core i7-6500U CPU
+ USB3.1 Typ-C, HDMI, USB3.0
+ inkl. beleuchteter Tastatur

ab 899 €*

* Preise inkl. MwSt. zzgl. evtl. anfallender Versandkosten. Irrtümer und Fehler vorbehalten, Angaben ohne Gewähr!

Mehr Infos unter **www.Linux-Onlineshop.de** und **www.TUXEDOComputers.com**